



EGOSECURE FULL DISK ENCRYPTION

Installation and Troubleshooting Guide

Version 22.0.1

Updated: October 2022

Matrix42 AG
Elbinger Street 7
60487 Frankfurt am Main

Telephone: +49 69 667738 222
E-Mail: helpdesk@matrix42.com
Self Service Portal: support.matrix42.com
Internet: www.matrix42.com

CONTENTS

1. Introduction	5
1.1. About EgoSecure Full Disk Encryption	5
What is EgoSecure Full Disk Encryption?	5
What does EgoSecure Full Disk Encryption not do?	5
EgoSecure Full Disk Encryption characteristics	5
1.2. EgoSecure Full Disk Encryption components and features	6
Full Disk Encryption (FDE)	6
Pre-Boot Authentication (PBA)	7
Boot and authentication scenarios	8
HelpDesk and data recovery methods	10
2. Installation, Upgrade and Removal	12
2.1. Before installing EgoSecure Full Disk Encryption	12
2.2. Installation overview	12
2.3. Installation requirements	13
2.4. Installation	14
Customizing	14
Prerequisites for <i>Windows 7</i> installations	16
Manual installation	17
Unattended installation	50
2.5. Upgrade	54
Manual upgrade	54
Unattended upgrade	58
2.6. Removal	60
Manual removal	60
Manual removal (Quick)	66
Unattended removal	69
3. Windows Upgrade	71
4. Troubleshooting	72
Additional tools to get configuration details	73
4.1. The limit of 4 primary partitions is reached	75
4.2. If the BSOD happens on a first reboot after the installation	76
4.3. If the system fails to boot Windows after disk encryption	77
4.4. Problems with image creation	78
4.5. Problems when copying an image back to the hard disk	79

4.6. Characters cannot be entered into the HelpDesk dialogs	80
4.7. How to prevent specific users from being “captured” during self initialization ...	81
4.8. User capturing fails	83
4.9. Partition creation fails after FDE has been initialized	84
4.10. Incorrect GUI language/Change GUI language.....	85
4.11. Administrator password forgotten.....	86
4.12. How to change PBA boot method	87
4.13. PBA fails to start in RAID mode.....	93
4.14. FDE initialization fails – very fragmented disk.....	95
4.15. PBA error	97
4.16. BitLocker hang after BSOD.....	98
Glossary.....	99

1. INTRODUCTION

EgoSecure Full Disk Encryption provides unmatched data-at-rest protection for standard hard disks via full-disk encryption.

This chapter gives you an overview of the product, detailing why it has been created and how it works.

1.1. About EgoSecure Full Disk Encryption

Although *EgoSecure Full Disk Encryption* can protect desktop computers the primary use is for notebooks. The mobility of information is quickly becoming more of a success factor in daily business. Notebook computers fulfill the requirement of mobility and thus, may contain business-critical information.

Unfortunately, a large number of notebooks are lost or stolen each year. In most cases, the information stored on those notebooks is much more valuable than the hardware itself. Companies and institutions are aware of the need to protect their data against unauthorized access even if the hardware is lost or stolen.

What is EgoSecure Full Disk Encryption?

EgoSecure Full Disk Encryption is a data protection solution for "data-at-rest". This means that it will protect data from malicious intent when the computer is turned-off or in hibernation mode.

EgoSecure Full Disk Encryption provides strong authentication and protection for standard hard disks via sector-based Full Disk Encryption (FDE) and Pre-Boot Authentication (PBA). This provides perfect 'turn-off-protection', which means that the implemented security mechanisms provide the highest security for the operating system, as well as for the data – provided the computer is turned off at the time of theft. The optional use of a security token or smart card at pre-boot is the high-end solution for secure key management in conjunction with two-factor authentication.

What does EgoSecure Full Disk Encryption not do?

EgoSecure Full Disk Encryption does not protect the computer against data theft or attack once authorization to the pre-boot component is successful and the system has booted into *Windows*. The user or administrator is responsible for ensuring that *Windows* is adequately protected (anti-virus, firewalls, remote data encryption, etc.).

EgoSecure Full Disk Encryption characteristics

- Enterprise-wide deployment and remote configuration (for laptops as well as desktop computers) via policies or via the EgoSecure Data Protection Console.
- Easy-to-implement protection: Installation wizards help you through the installation and configuration.

- Transparent to the user: The end user only needs to authenticate to Windows via the EgoSecure Pre-Boot Authentication. Encryption/decryption tasks are performed on the fly in the background.
- Easy to configure and administrate: All aspects of EgoSecure Full Disk Encryption are controlled via the Control Center in the Windows Control Panel.
- Extendible to the highest level of security using PBA and smart cards as well as the ability to block unauthorized external media.
- Comprehensive HelpDesk and self-help recovery methods.

1.2. EgoSecure Full Disk Encryption components and features

EgoSecure Full Disk Encryption has the following features:

- FDE support (FDE uses sector-based encryption). For further information, refer to the section below.
- Support for the encryption of multiple internal hard disks.
- Strong PBA via a hardened *Linux* operating system (protected against manipulation via the use of MD5 checksums). For details, see chapter [PBA](#).
- Smart card/token or *Windows* credentials used for authentication. For details, see chapter [PBA](#).
- Single Sign-On (SSO) from the PBA component to *Windows*. For details, see chapter [PBA](#).
- Emergency recovery via:
 - HelpDesk application
 - Emergency Recovery CD (plug-ins for WinPE).
For details about emergency recovery, see [EgoSecure FDE - Administration and Usage Guide](#), chapter 1.12.
- Optional policy-based deployment and configuration.
For details, see [EgoSecure FDE - Administration and Usage Guide](#).
- Secure data erasure so that the hard disk on which *EgoSecure Full Disk Encryption* is installed may be reused without having to worry about data being recovered by third parties. For details, see [EgoSecure FDE - Administration and Usage Guide](#).

Full Disk Encryption (FDE)

Full Disk Encryption (FDE) provides access protection and encryption for sensitive business information. It stops unauthorized users from gaining access to any part of the (encrypted) hard disk – provided the computer is either turned-off or in stand-by/hibernation mode.

‘Full Disk Encryption’ is the term used to describe the encryption of the whole disk or partition – literally everything – including temporary files, swap files, and the operating system itself. Because of this, the data cannot be accessed when booting the computer from media such as a CD-ROM, floppy disk, or USB stick. Hacker tools that crack or reset the system password do not have a chance to compromise the system. If the hard disk is built into another computer as a second disk, access to encrypted partitions would also be impossible. For authorized users, disk access will be no different to that of unencrypted systems.

FDE applies to hard disks that DO NOT utilize a hardware encryption chip – in other words 'standard' hard disks. The advantage of *EgoSecure Full Disk Encryption* is that it can be installed on ANY hard disk regardless of size or manufacturer. Once the hard disk has undergone an initial encryption, further encryption/decryption of new data is performed on the fly with little or no impact on system performance.

Unlike other encryption products that encrypt specific files on your hard disk, EgoSecure FDE uses a sector-for-sector encryption method. That means that FDE encrypts all the data written to your hard disk and decrypts all the data read from the disk at a very low level – all directly at physical hard disk access.

Pre-Boot Authentication (PBA)

The *EgoSecure Full Disk Encryption* PBA component extends FDE to the highest level of security via *Windows* credentials/smart card/token authentication to a hardened *Linux* system at pre-boot time.

The *EgoSecure Full Disk Encryption* installer places a fully functional and secure *Linux* system to a small partition on the hard disk pre-prepared by the installer.

Once the PBA has loaded the user can enter either *Windows* credentials or smart card PIN; this information is compared to the encrypted information in the PBA. If the credentials/PIN matches the information in the PBA, the PBA will terminate and *Windows* will be booted.

Advantages of using Linux for the PBA

Using a hardened *Linux* system for PBA has a huge advantage when compared to normal *Windows* logon. For example, it is common knowledge amongst hackers how to extract a *Windows* password. Not only does the *EgoSecure* FDE component encrypt the hard disk making password extraction impossible, but *EgoSecure* PBA goes one step further by providing a secure authentication system that cannot be manipulated. The same component protection for the PBA applies as already stated above (MD5 checksums and strong encryption for the keys).

EgoSecure Full Disk Encryption gives the user the security needs – safe with the knowledge that the password is securely encrypted in PBA, and without it no one can access their computer.

Authentication

Two forms of authentication can be used in EgoSecure PBA:

- Smart card authentication based on international standards such as X.509, PKCS#11, and PC/SC

The smart card, or token, authentication method is the alternative to *Windows* credentials. This method has the advantage of separability - the 'key' (the smart card) can be taken with you. As the keys are stored solely on the smart card or token, if the computer is stolen, it is impossible to access the data without the card and PIN. The only theoretical way to obtain

the data in such a case would be to use brute force method, which is considered useless if a key length of 128 bits or more has been used to encrypt the data.

After entering the smart card PIN in the PBA, the PIN is used to decrypt a so called 'Data Encryption Key (DEK)' (the key used to encrypt data on the hard disk) by the smart card. Only if successful will *Windows* be booted.

The PBA component is able to perform the decryption/encryption of the Data Encryption Key on the basis of symmetric encryption or asymmetric encryption mechanisms, so called 'public key' mechanisms. In the case of asymmetric encryption, X.509 certificates (and the corresponding private key) are used for encryption and decryption. This guarantees the highest degree of interoperability with most PKIs on the market.

- Windows credentials authentication based on the user's current user ID, password, and optionally – domain

The *Windows* credentials authentication method is the ideal way to improve security and usability at the same time. The user has no need to remember another password or learn a new PIN – user simply enters the user ID and password used for *Windows*.

Boot and authentication scenarios

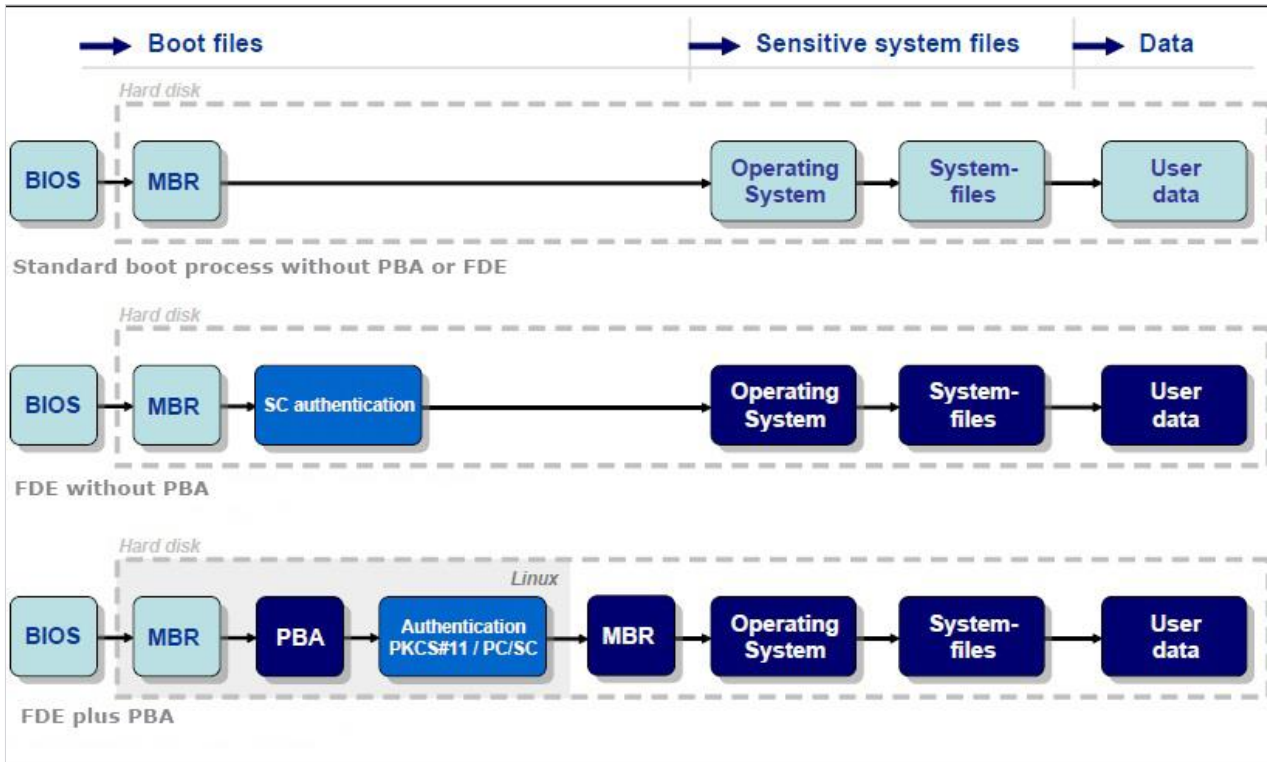
This section details the PBA boot and authentication procedure.

The following figure (Figure 1) illustrates the difference between:

- Booting normally to *Windows* (no encryption, no PBA = high security risk)
- Booting to an encrypted hard disk with a Windows-smart card interface without PBA (medium security risk)
- Booting to an encrypted hard disk with PBA using the PBA

Dark blue indicates protected components and data, while light blue indicates components and data that are unprotected:

Figure 1. Boot and authentication process comparison



■ The first row illustrates the standard *Windows* boot procedure. This method offers no data protection whatsoever. *Windows* logon can easily be overcome using readily-available hacker tools –leaving your data open. Even if the attacker does not have these tools a third party can remove the hard disk from the computer and attach it as a secondary drive to another computer to copy the data (these are just a few examples of how to hack a computer that is not protected).

■ The second row illustrates the *EgoSecure Full Disk Encryption*. Up to the point of successful authentication the sensitive system files and user data are inaccessible. Due to this encryption the data cannot be retrieved by connecting the hard disk to another computer as a secondary drive - the contents of the drive are unreadable without the disk key! The only weakness that remains with this method is the *Windows* logon dialog.

■ The third row illustrates the full *EgoSecure Full Disk Encryption* approach to data protection with PBA. User login is processed within the Linux PBA component. This stops any attack via the *Windows* logon dialog.

The PBA partition is not encrypted. To protect the PBA, only those components needed to complete the secure authentication via *Windows* credentials or smart card/token exist in the system. No networking components are available making hacking the PBA via a network impossible. USB and CD drivers are implemented strictly for the purpose of emergency recovery and are protected as such. All PBA system components are protected against manipulation.

HelpDesk and data recovery methods

An *EgoSecure Full Disk Encryption* user is supported in an emergency situation through several recovery methods. Remote assistance via a HelpDesk is the method most likely to be used in an enterprise, but self-help recovery methods are also available.

These recovery methods may become necessary when a user stumble into one of the following situations:

- Defective smart card readers, lost/forgotten/broken smart cards;
- Forgotten Windows credentials;
- Forgotten/blocked smart card PIN;
- Failed *EgoSecure Full Disk Encryption* installation/ encryption/ decryption.

EgoSecure Full Disk Encryption offers several methods of data recovery in an emergency:

HelpDesk Application

■ The PBA HelpDesk application can be used to assist a user in starting his/her computer in an emergency, for example, should the user have forgotten password or lost smartcard, the user receives HelpDesk contact information (telephone-based, contained within the PBA) displayed on his/her screen. A challenge–response process between the user and the HelpDesk personnel is used to verify the installation as well as the identity of the user and consequently start the computer.

■ HelpDesk in the EgoSecure Data Protection Console (**Product Settings | FDE | Helpdesk**).

Use **Helpdesk** to permit the user a certain number of boot actions without authenticating in the “EgoSecure boot system”.

During PBA the user can launch the helpdesk to select the **request code (request ID)** and send it to the administrator.

Then, administrator enters the challenge ID that was received from the user.

Challenge			
a	<input type="text"/>	b	<input type="text"/>
c	<input type="text"/>	d	<input type="text"/>
e	<input type="text"/>	f	<input type="text"/>
g	<input type="text"/>	h	<input type="text"/>
i	<input type="text"/>	j	<input type="text"/>
k	<input type="text"/>	l	<input type="text"/>
m	<input type="text"/>	n	<input type="text"/>
o	<input type="text"/>	p	<input type="text"/>

After that, administrator sends the **response (response ID)** that contains the number of boot actions, available to the user without PBA logging.

Response			
a	<input type="text"/>	b	<input type="text"/>
c	<input type="text"/>	d	<input type="text"/>
e	<input type="text"/>	f	<input type="text"/>
g	<input type="text"/>	h	<input type="text"/>
i	<input type="text"/>	j	<input type="text"/>
k	<input type="text"/>	l	<input type="text"/>
m	<input type="text"/>	n	<input type="text"/>
o	<input type="text"/>	p	<input type="text"/>

It is also possible to activate **self-init** (automatic initialization), which means that the next user, who logs in via the Windows logon function successfully is automatically added to the PBA list and can be used in the PBA during the next boot process.

Emergency Recovery Disk (ERD)

This is a hands-on method of data recovery. The ERD should only be used in situations in which the HelpDesk is no longer of help, for example, when the PBA can no longer be started, or if the initial encryption on a standard hard disk has been interrupted prematurely (due to power failure).

EgoSecure has developed add-on for *WinPE* (for *Windows Vista, Windows 7 and higher*). To recover a computer in such an emergency scenario, it is necessary to use an Emergency Recovery Information (ERI) file created either by the *EgoSecure Full Disk Encryption* installer during the installation or afterwards via the *EgoSecure Full Disk Encryption* control center. The ERI file contains the specific recovery information necessary to clear any major problems with the computer.

2. INSTALLATION, UPGRADE AND REMOVAL

This chapter details the steps necessary to install, upgrade, and remove *EgoSecure Full Disk Encryption* using either manual or unattended methods.

2.1. Before installing EgoSecure Full Disk Encryption

Please ensure that the following conditions are met before you install *EgoSecure Full Disk Encryption*:

- Run CHKDSK/f on all the drives you wish to encrypt. This will check the hard disk and the file system for errors and if necessary, correct them.
- Check if the AHCI mode rather than legacy mode is enabled on in BIOS. If you want to use AHCI, *EgoSecure* recommends using the *standard Microsoft* default driver.
- Check if the target computer meets the installation requirements described in Section [2.3](#).

In addition to the above, the following tasks must be performed:

- If the hard disk has been encrypted by a product other than *EgoSecure Full Disk Encryption*, decrypt the hard disk and remove the encryption application. This will avoid conflicts between the applications and close any possible security holes that may be opened when using two applications.



ATTENTION

Backup before installing EgoSecure Full Disk Encryption

Backup any important data from the fixed drive(s) of your computer before installing *EgoSecure Full Disk Encryption* (if the installation or the initial encryption on standard hard disks fails, the information on the computer will be inaccessible without an Emergency Recovery Disk. Also, despite the fact that the installation process being made as safe as possible, a disk or power failure during the installation could result in a loss of data).

Be aware that one reboot is necessary after the installation of the FDE component. This is because the installer creates a small partition on which the PBA component is installed and it is necessary to let Windows check the disk (CHKDSK) BEFORE initializing the PBA component on this small partition. Optionally, further reboot is necessary after the initialization of the PBA component to capture user credentials (this does not apply if you either enter user credentials or certificates directly into the PBA component, or pass credentials onto the PBA component via an initialization policy).

2.2. Installation overview

The first installer will place an integrated FDE mechanism to the hard disk as well as a hardened *Linux*-based PBA system to a specific, new partition on the hard disk. Once running, *EgoSecure Full Disk Encryption* will boot to this system first and will prompt for authentication. If successful, the computer will automatically boot to *Windows* and use the SSO method to authenticate the user to *Windows* with no further need to enter credentials.



ATTENTION

EgoSecure Full Disk Encryption is delivered in several languages and you can install any of them on a computer that has a different keyboard layout, i.e. the English version can be installed on a computer with a German keyboard layout.

Caution is needed when either connecting an external keyboard that has a different layout, or when deploying EgoSecure Full Disk Encryption to computers that have a different keyboard layout to that on which the deployment policies have been created.


Bear in mind that when defining passwords, the keyboard layout used to define the password may differ from the keyboard layout used at a later date (special characters have keys/key combinations that differ - for example, a QWERTZ keyboard layout differs greatly from a QWERTY keyboard layout).

2.3. Installation requirements

In this section the hardware and software requirements for *EgoSecure Full Disk Encryption* are described.

Required for the...	Details
Operating System	<ul style="list-style-type: none"> ■ Windows Vista 32-bit/64-bit with Service Pack 2 ■ Windows 7 32-bit/64-bit ■ Windows 8 32-bit/64-bit ■ Windows 8.1 32-bit/64-bit ■ Windows 10 32-bit/64-bit ■ Windows 11 32-bit/64-bit
Firmware	Both UEFI and BIOS firmware are supported.
Hardware	Device with x86 or x64 architecture.
File System	The file system must be formatted as NTFS.
Hard Disk Space/Partitions	<p>EgoSecure Full Disk Encryption has the following hard disk space/partition requirements:</p> <ul style="list-style-type: none"> ■ FDE (without and with PBA): 500 MB (system disk) ■ FDE (without and with PBA): 650 MB (system partition) ■ Free space in an unpartitioned area of the hard disk or free space at the end of an NTFS partition. ■ <i>Additionally, for the MBR partition style.</i> The system with MBR may have 4 primary partitions at most. EgoSecure Full Disk Encryption needs one entry in the primary partition table; three other partitions on the hard disk are left for other operating systems. <p>NOTE: Windows 7 installs a 100MB boot partition per default. EgoSecure Full Disk Encryption works successfully with this partition. For those users who want to install to Windows 7 systems that do not have this boot partition, it is necessary to manually edit the boot sequence with the</p>

	Microsoft onboard utility 'BCDedit' before installing EgoSecure Full Disk Encryption. For details, see Prerequisites for Windows 7 .
Supported Keyboard Layouts	Linux-based PBA has over 100 keyboard layouts. Graphical Simple PBA supports the following keyboard layouts: <ul style="list-style-type: none"> ■ en_US - English (United States) ■ de_DE - German (Germany) ■ de_CH - German (Switzerland) ■ fr_CH - French (Switzerland)
Unsupported configurations	<ul style="list-style-type: none"> ■ Dynamic disks ■ Windows Server operating systems ■ Computers encrypted with other 3rd party encryption solutions (exclusion: BitLocker Drive Encryption) ■ Microsoft Device Encryption ■ Non-NTFS drives: FAT, exFAT ■ BIOS MBR with 4 primary partitions ■ RAID configurations (not supported on BIOS systems; on UEFI systems it is supported, but PBA works only in the Simple PBA mode). ■ 32-bit UEFI systems



ATTENTION

- Only the **basic** disk type is supported for the second hard disk (for further information about 'basic' disk types refer to your Windows documentation or online help).
- If the primary disk is damaged, the partitions on second hard disk can be decrypted using the ERD application with the respective ERI file.
- Up to 10 partitions, on multiple hard disks, can be encrypted.

2.4. Installation

This section details how to install *EgoSecure Full Disk Encryption* either manually, or via the EgoSecure Data Protection Console.

Customizing

This section details how to customize the setup in preparation for rollout. There are two main ways to customize the MSI package:

- If you intend to rollout to multiple hardware configurations, we recommend that you test each configuration for compatibility beforehand. This enables you to locate any configuration that EgoSecure does not support using the standard setup and allows you to test alternative setups using 'Hardware Compatibility Mode' or an alternative bootloader. For further information, see [Installation options for FDE](#).
- The PBA component can also be customized with an individual background image and company-specific HelpDesk texts. For further information, see [PBA customization](#).

Installation options for FDE

To provide system administrators with methods of installing EgoSecure Full Disk Encryption successfully on the new and legacy hardware several new mechanisms have been

implemented. There is no absolute guide as to which mechanism should be used on which computer. The standard mechanism will work on most computers, but there are some computers that need help. The mechanisms available are:

- Hardware compatibility mode (DMI config)

As of EgoSecure Full Disk Encryption 'Hardware compatibility mode' is available. This allows a system administrator to use two alternative methods of booting from the PBA to Windows. This means that it is possible to identify computers on which the standard method does not work, test the alternatives, and incorporate the details for such computers into the rollout package for automatic identification.

For further information, see [EgoSecure FDE - Administration and Usage Guide](#).

- Alternative bootloader

An even smaller number of computers may need an alternative bootloader to boot correctly.

PBA customization

This section details how to customize EgoSecure Full Disk Encryption to:

- Incorporate a PBA new background;
- Incorporate new EgoSecure Full Disk Encryption PBA HelpDesk texts.
- Rebranding mechanism for OEM use implemented. The customization detailed in this section is a subset of the rebranding mechanism.

If you are a customer with an interest in rebranding EgoSecure as an OEM version, then please contact your nearest EgoSecure representative for further details.

The customizing mechanism is a simple one. The file 'fsebrand.bin' must be placed in the same directory as the EgoSecure Full Disk Encryption MSI package before the installation starts.



ATTENTION


Failure to place the fsebrand.bin file in the same directory as the EgoSecure Full Disk Encryption msi package will result in the EgoSecure Full Disk Encryption background and standard HelpDesk texts being installed to the end-user computer.

It is not possible to enter a remote location for the fsebrand.bin file via the command line!

1. Locate and open the file fsebrand.bin located in the Customizing directory. The fsebrand.bin file is actually a ZIP file that has had the extension renamed to *.bin. To open the file either open the file directly using an intelligent ZIP/archiving application or rename the extension from *.bin to *.zip and then open it using your archiving utility of choice.
2. Unpack the contents of the file to produce the directory fsebrand.
 - The fsebrand directory contains the following files needed to rebrand EgoSecure Full Disk Encryption:

Directory/file	Details
PBA customization files	The following file is used to rebrand the default PBA background image: pba_bkgd_image.png(800x600 pixels) NOTE: If the picture size does not match the above mentioned standard size (pixels), FDE will scale down the original size to standard size.
Country-specific directories identified by an RFC 1766 identifier (i.e. en_US)	Each directory contains the following file: helpdesk_snb.txt HelpDesk text message file for the PBA HelpDesk.

3. Edit the default message in the HelpDesk file helpdesk_snb.txt in each of the languages you wish to use, as well as the background image.




To display the HelpDesk correctly in the PBA component, the HelpDesk file must be saved using the following formatting information (it is recommended to use a text editor such as UltraEdit for this):

INFO

- ◆ Unix terminators-LF
- ◆ UTF-8 encoding

4. Once finished, select all the files and directories in the fsebrand directory and re-zip them. Rename the resulting file to fsebrand.bin. The customization is now complete.



Make sure that you re-zip the files and directories directly IN the fsebrand directory and NOT the fsebrand directory itself. This is because the installation mechanism expects to find the rebranded files directly in the fsebrand.bin file and not within another directory inside it.

ATTENTION

Prerequisites for *Windows 7* installations

This section details the prerequisites for the successful installation of *EgoSecure Full Disk Encryption* under *Windows 7*.

- EgoSecure Full Disk Encryption does not support the standard Windows 7 boot screen that contains the twirling/glowing Windows logo. This is because the standard boot screen calls on graphics libraries before the EgoSecure Full Disk Encryption driver can be loaded. To solve this issue, the EgoSecure Full Disk Encryption installer will call the Microsoft utility BCDedit to switch the boot screen to "basic" mode, which results in a Vista-like progress bar instead of the twirling Windows logo. The above applies to "standard" Windows 7 setups that have a small, active 100MB boot partition before the system partition. In such a scenario, the BCDedit utility can be successfully called to change the start screen because the active boot partition is not the Windows partition (access right issues).

Manual installation

- [Installation of EgoSecure Full Disk Encryption components](#)
- [Installing Boot Security \(initializing FDE\)](#)
- [Configuring PBA components](#)

This section details how to install the *EgoSecure Full Disk Encryption* on standard hard disks. No hard disk encryption is started during the initial installation. This enables easy recovery should anything go wrong during the installation. Encrypt the hard disk only when you see that the PBA has installed and initialized correctly, and you have successfully authenticated to the EgoSecure Full Disk Encryption PBA at least once. If everything is all right, then you can encrypt the hard disk. For further information, refer to [EgoSecure FDE - Administration and Usage Guide](#).

Be aware that one reboot is necessary after the installation of the FDE component. This is because the installer creates a small partition on which the PBA component is installed and it is necessary to let Windows check the disk (CHKDSK) BEFORE initializing the PBA component on this small partition. An optional further reboot is necessary after the initialization of the PBA component to capture user credentials (this does not apply if you either enter user credentials or certificates directly into the PBA component, or pass credentials onto the PBA component via an initialization policy).



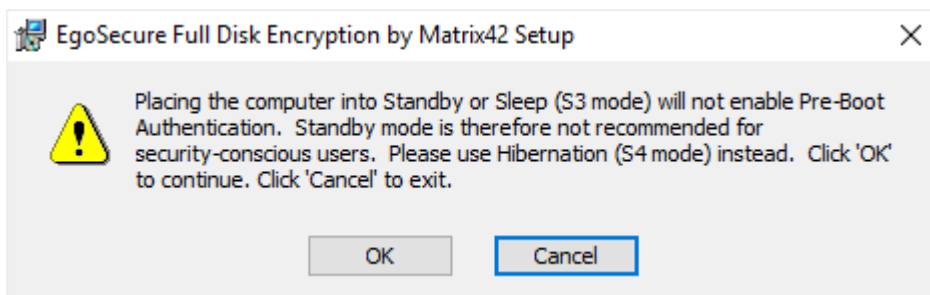
ATTENTION

- The FDE installation requires a user account with administrator privileges.
- For Windows Vista, Windows 7 and higher: By default, the security feature "User Account Control (UAC)" is enabled. This means that it will be necessary to confirm any such dialogs throughout the installation..

Installation of Full Disk Encryption components

1. Double-click the executable file EgoSecure FDE by Matrix42 Setup.exe.
 - The GUI language will be automatically selected by the installer to fit that of the operating system. If you have an operating system other than English, German, the default language – English – will be installed.
 - A warning message appears if standby is enabled on the computer.
2. Read the warning carefully and click **OK** to continue.

Figure 2. FDE Installation – Standby Warning Dialog



→ The **Welcome** dialog appears.

3. Click **Next** to proceed with the next step.

Figure 3. FDE Installation - Welcome Screen



→ The **License Agreement** dialog appears.

4. Select **I accept the terms in the License Agreement**, and then press **Next** to continue.

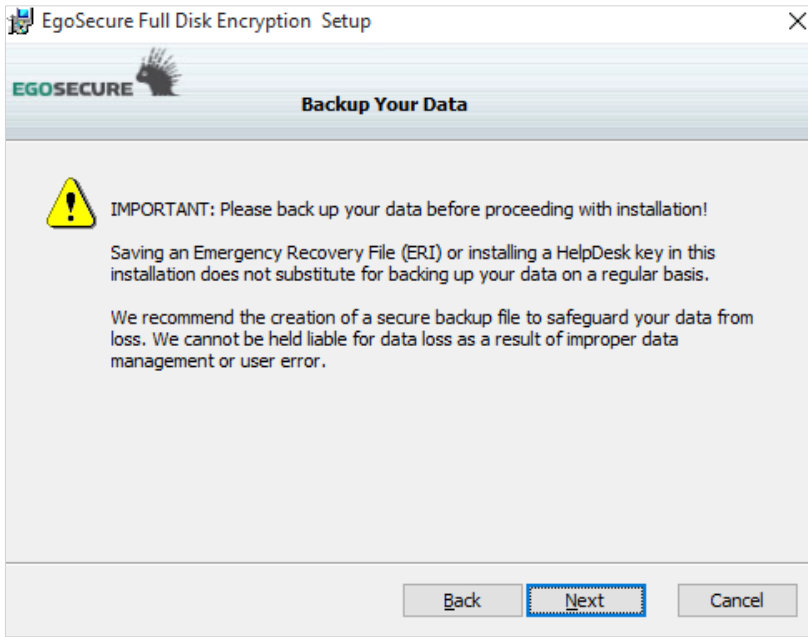
Figure 4. FDE Installation - License Agreement Dialog



→ The **Data Backup** dialog appears.

5. Read the warning carefully, and if you have not already done so, click **Cancel**, create a backup of your data before restarting the installation. Press **Next** to continue.

Figure 5. FDE Installation - Data Backup Dialog



→ The **Setup Type** dialog appears. This dialog allows you to choose which *EgoSecure* components should be installed.

Figure 6. FDE Installation – Setup Type Dialog

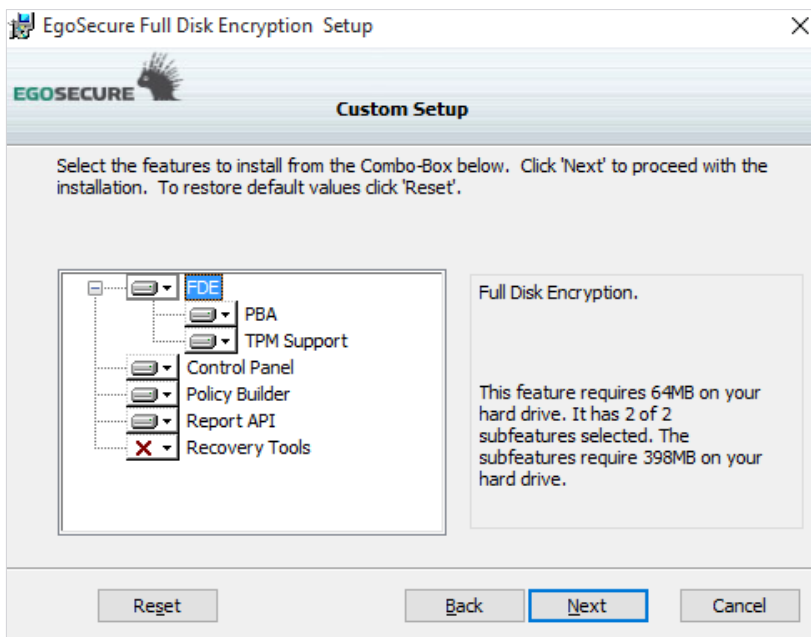


6. Click **Complete** to install all the features. The easiest way to secure your computer. This also requires the most disk space (approximately 200MB). If you select this option, go directly to the next step.

Note: The **Complete** mode will not install “Recovery Tools” of the *EgoSecure* package.

7. Click **Custom** to select which features will be installed. **This is recommended for advanced users only!** This dialog allows you to perform the following tasks:

Figure 7. FDE Installation – Custom Setup Dialog



- Context menu for specific component selection:
 - If you want to select/re-select a component for installation, click the hard drive icon next to the component and select either **Will be installed on local hard drive** or **Entire feature will be installed on local hard drive** from the context menu.
 - If you want to prevent the installation of a component, select **Entire feature will be unavailable** from the context menu.

The following components can be installed:

FDE: The Full Disk Encryption components (base components).

PBA: The PBA component (optional component).

TPM Support: Support for Trusted Platform Module (optional component).

Control Panel: This refers only to the EgoSecure Full Disk Encryption Control Center plugin for the Windows control panel.

Policy Builder: Install the Policy builder components.

Report API: Install support for status information retrieval via third-party applications (not recommended).

Recovery Tools: This allows installing the recovery tools (PE ERD, Secure Erase and Secure Wipe).

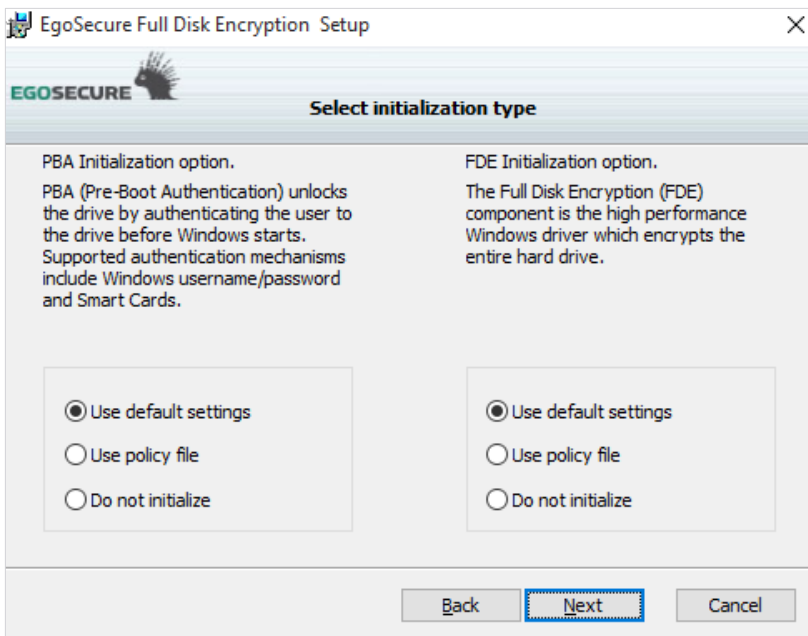
- To return to the default selection click **Reset**.

8. Once you have made your selection click **Next**.

- The **Select Initialization Type** dialog appears. This dialog allows for selecting the following types of initialization:

Initialization type/ Option	Option/details
PBA initialization options	<ul style="list-style-type: none"> ■ Use default settings Manually configure and initialize PBA before installing its components. ■ Use policy file Start the initialization and configuration of the PBA component according to pre-defined settings in a policy. For further information about <i>EgoSecure Full Disk Encryption</i> policies refer to EgoSecure FDE - Administration and Usage Guide. ■ Do not initialize Only install the PBA components - leave the initialization and configuration of the PBA component until later. (Initialization and configuration can be performed via the Control Center - refer to EgoSecure FDE - Administration and Usage Guide).
FDE initialization options	<ul style="list-style-type: none"> ■ Use default settings Manually configure and initialize FDE before installing its components. ■ Use policy file Start the initialization and configuration of the FDE component according to pre-defined settings in a policy. For further information about <i>EgoSecure Full Disk Encryption</i> policies refer to EgoSecure FDE - Administration and Usage Guide. ■ Do not initialize Only install the FDE components - leave the initialization and configuration of the FDE component until later. (Initialization and configuration can be performed via the Control Center - refer to EgoSecure FDE - Administration and Usage Guide).

Figure 8. FDE Installation – Select Initialization Type Dialog



■ If this is an initial installation and you want to manually install, initialize, and configure *EgoSecure Full Disk Encryption* in one procedure, it is recommended to check the option **Use default settings for** both FDE and PBA. Continue with step 10.

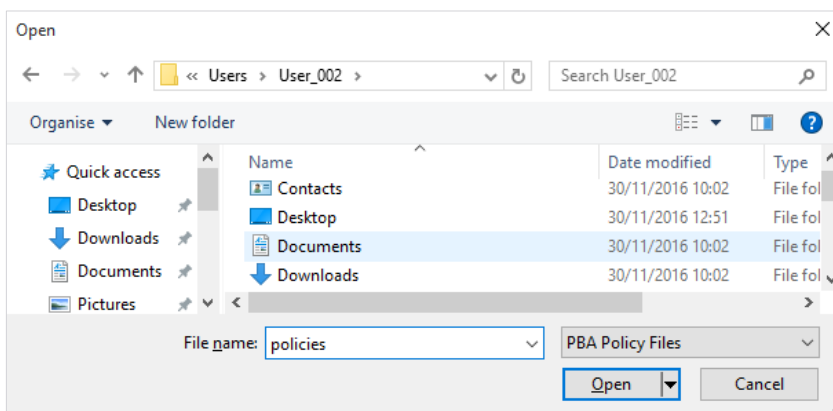
■ If you want to install and initialize the FDE and/or the PBA components according to settings in pre-defined policies, check the option **Use policy file**. Continue with the next step (the dialogs prompting for the location of the policy files will appear after the main components have been installed).

■ If you want to initialize and configure *EgoSecure Full Disk Encryption* at a later date, check the option **Do not initialize** for both FDE and PBA. Continue with step 10.

9. Once you have made a selection, click **Next** to continue.

→ If you have selected the **Use policy file** option in the previous step, then the following dialog appears in sequence prompting you to locate the respective policy file for the FDE (*.nbs) and PBA (*.pba) components:

Figure 9. FDE Installation – FDE/PBA Policy Prompt Dialog



10. Locate and open the necessary policy files.

→ The Complete Installation dialog appears.

11. Click **Install**.

→ The Installation Status and Installation Complete dialogs will appear.

12. Click **Finish**.

→ The installer finishes here. The FDE initialization starts automatically, and once successfully completed the **Operation was successful** dialog appears.



ATTENTION

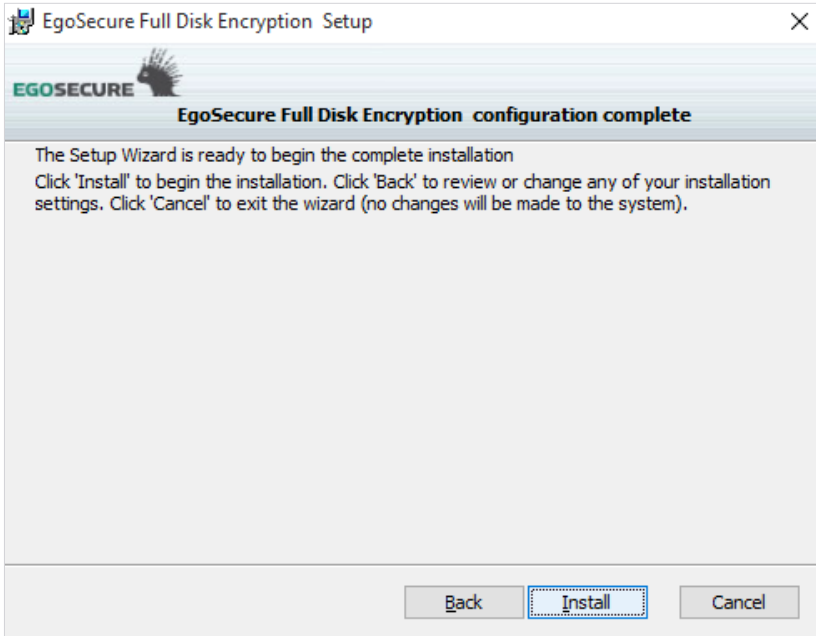
When you restart the computer, it will boot to the Windows logon dialog as normal. Log on as normal. The Windows desktop will not appear for a couple of minutes because the PBA component is being initialized. **Your computer has not crashed!** Please be patient and let the process finish. You will be taken to the desktop as soon as the PBA component has been initialized.

■ If you have selected to use policy file-based initialization for just the FDE component, continue with the next step to initialize the PBA component (refer to the dialog and notes above). The setup finishes here.

■ If you have selected to use policy file-based initialization for just the PBA component, continue with the next step.

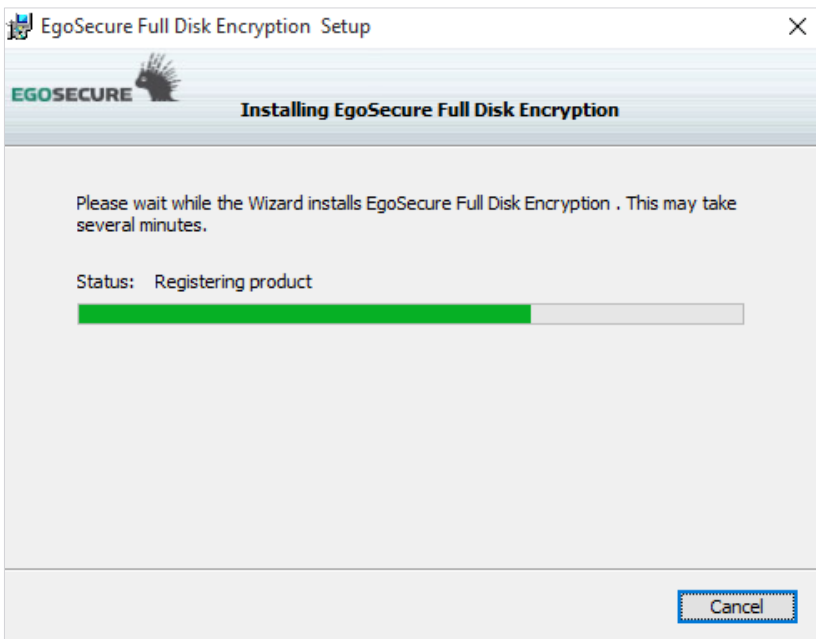
13. The **Complete Installation** dialog appears. Click **Install** to begin installing files.

Figure 10. FDE Installation – Complete the Installation Dialog



→ The **Installation Status** dialog appears. Please wait while EgoSecure is installed. This may take several minutes.

Figure 11. FDE Installation – Installation Status Dialog



→ If the installation is successful, the following dialog appears:

Figure 12. FDE Installation – Installation Completion Dialog

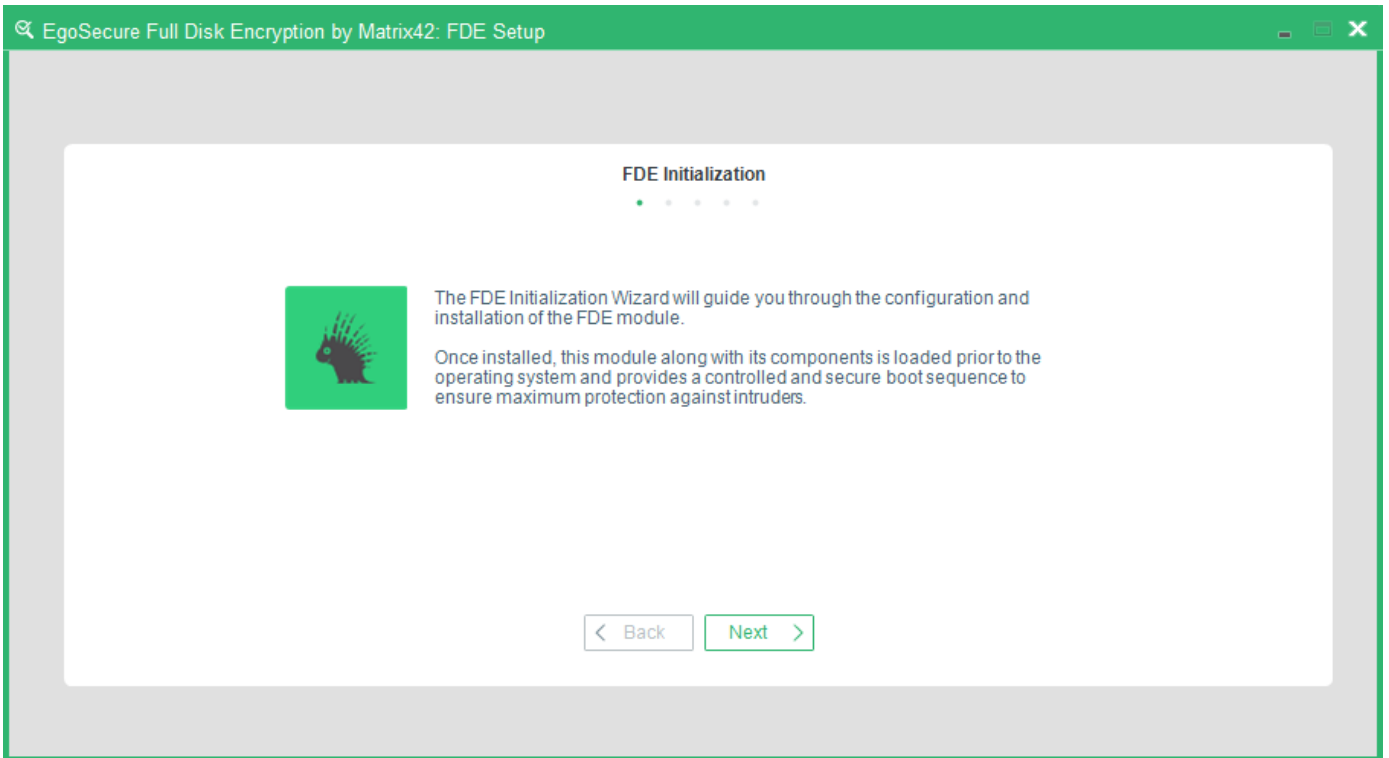
➤ The initial part of the installation is now complete.

- If you have selected **Use default settings** for both FDE and PBA components in step 6, the initialization and configuration will now continue. Continue with [Installing Boot Security](#).
- If you have selected **Do not initialize** for both FDE and PBA in step 6, you can initialize the FDE and PBA components via the Control Center at a later date. The installer finishes here.

Installing Boot Security (initializing FDE)

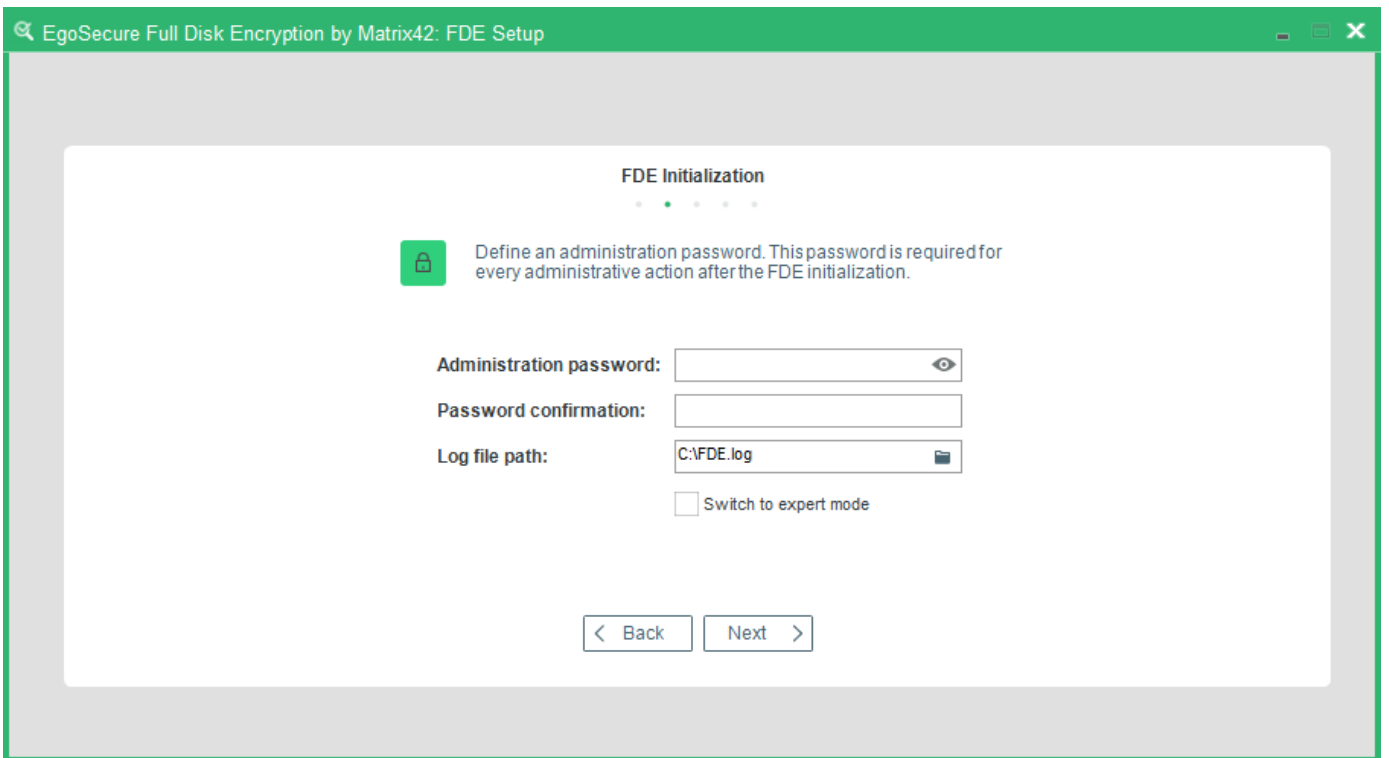
1. If **Use default settings** for the FDE component was selected in step 6, the following dialog appears. If a disk is encrypted with BitLocker, the dialog displays a warning that BitLocker protection will be disabled till the moment FDE initialization finishes (reboot included).
2. Click **Next** to continue.

Figure 13. FDE Initialization – Welcome Dialog



→ The **Administration Password** dialog appears:


Figure 14. FDE Initialization – Administration Password Dialog



3. Use this dialog to define the administration password for *EgoSecure Full Disk Encryption* and to define the location for the installation log file. This password will be required for every

administrative action after *EgoSecure Full Disk Encryption* has been configured and running. You will also need this password to install and configure the PBA component after the computer has been restarted (providing you have chosen to install it).

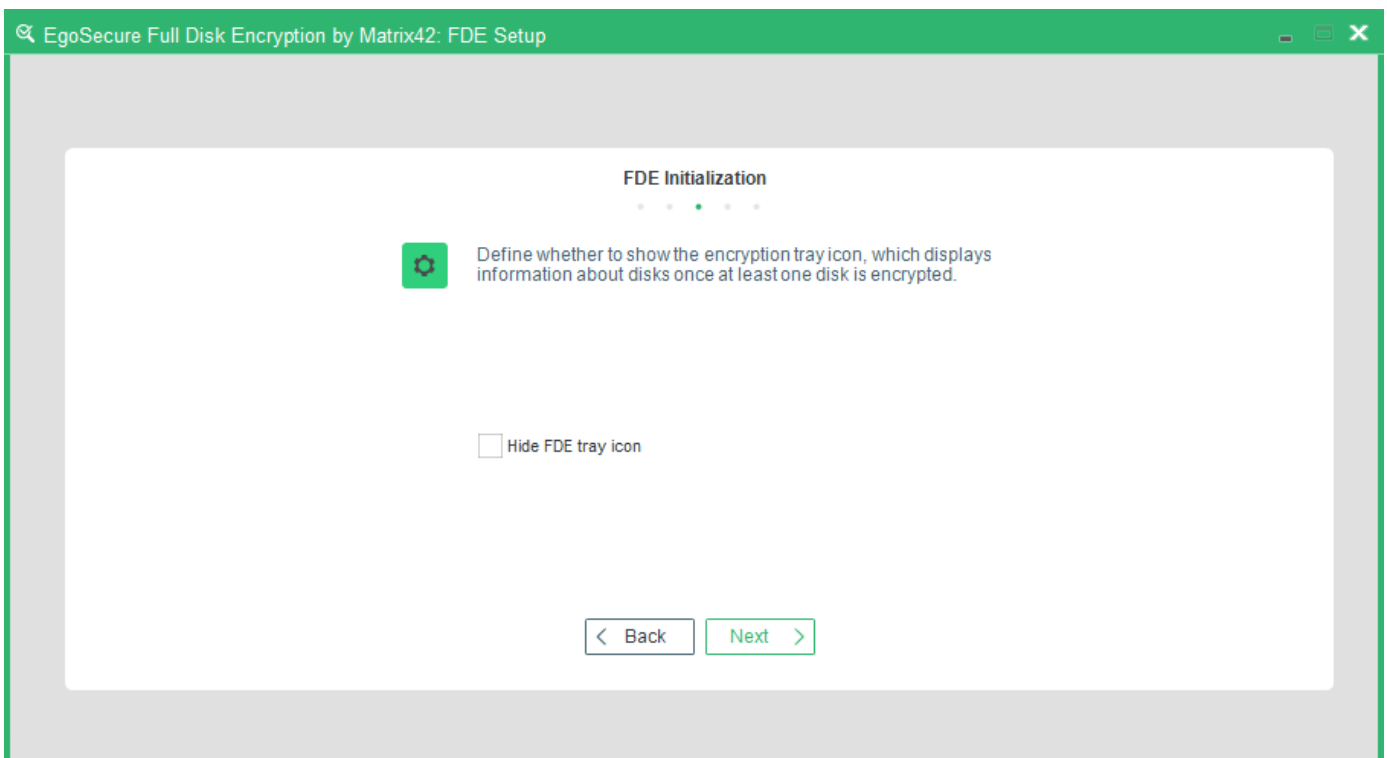
4. Click **Next** to continue.



WARNING

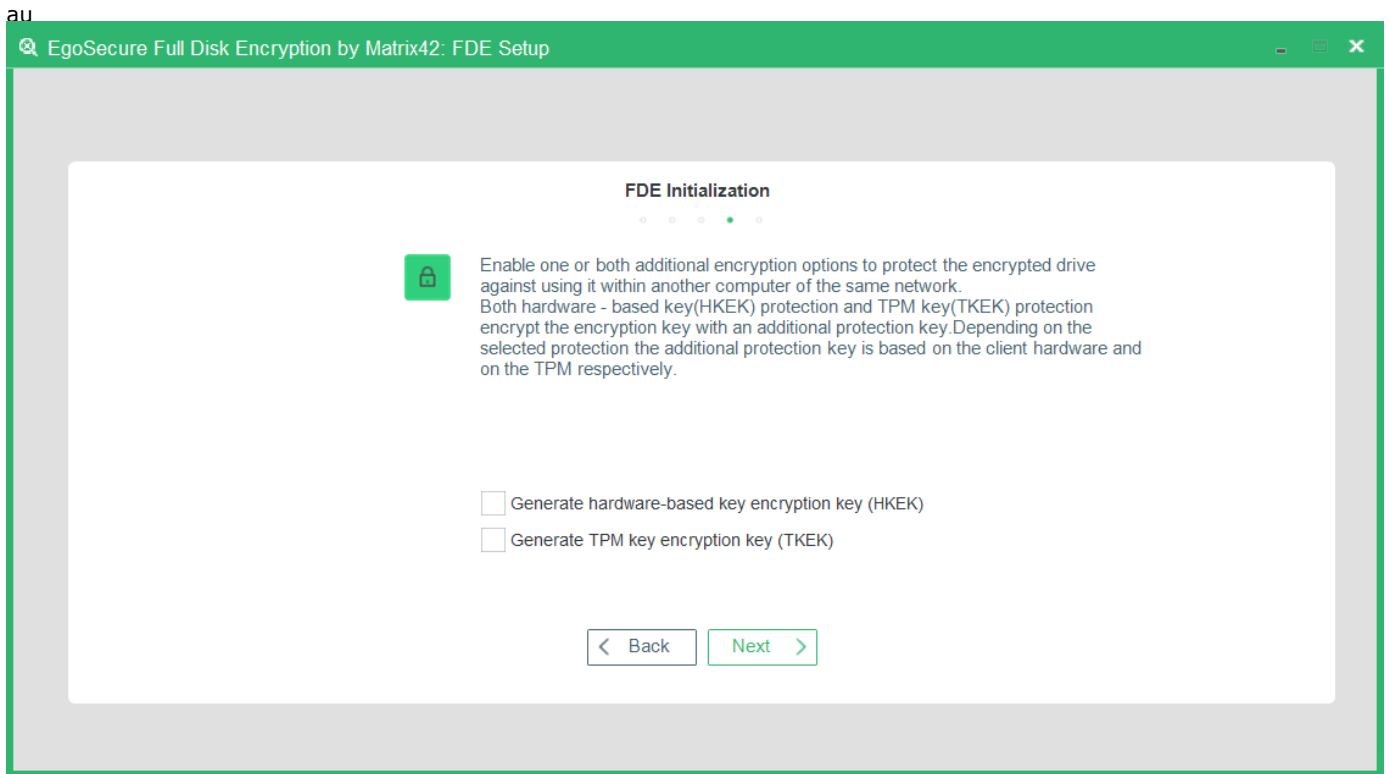
Keep the administration password in a secure location.

→ The step for hiding an encryption tray icon appears.



5. By default, the encryption tray appears on the Windows taskbar once a disk is encrypted and shows information about the state of all disks on a computer. To hide the icon, check the **Hide FDE tray icon** box and click **Next**.

→ The step for configuring additional encryption key protection appears.



Enable an additional layer of security to the disk encryption key (DEK).

The HKEK option utilizes unique hardware-based information from the client to generate an additional hardware-based key encryption key (HKEK).

The TKEK option uses unique TPM information from the client for generating a TPM-based key encryption key (TKEK). Check [TPM system requirements](#) before enabling the option.

The options protect against moving the encrypted drive into another computer within the same network, where the same KEK is used.

You can use both options at a time for the protection.



ATTENTION

Before updating BIOS or replacing hardware

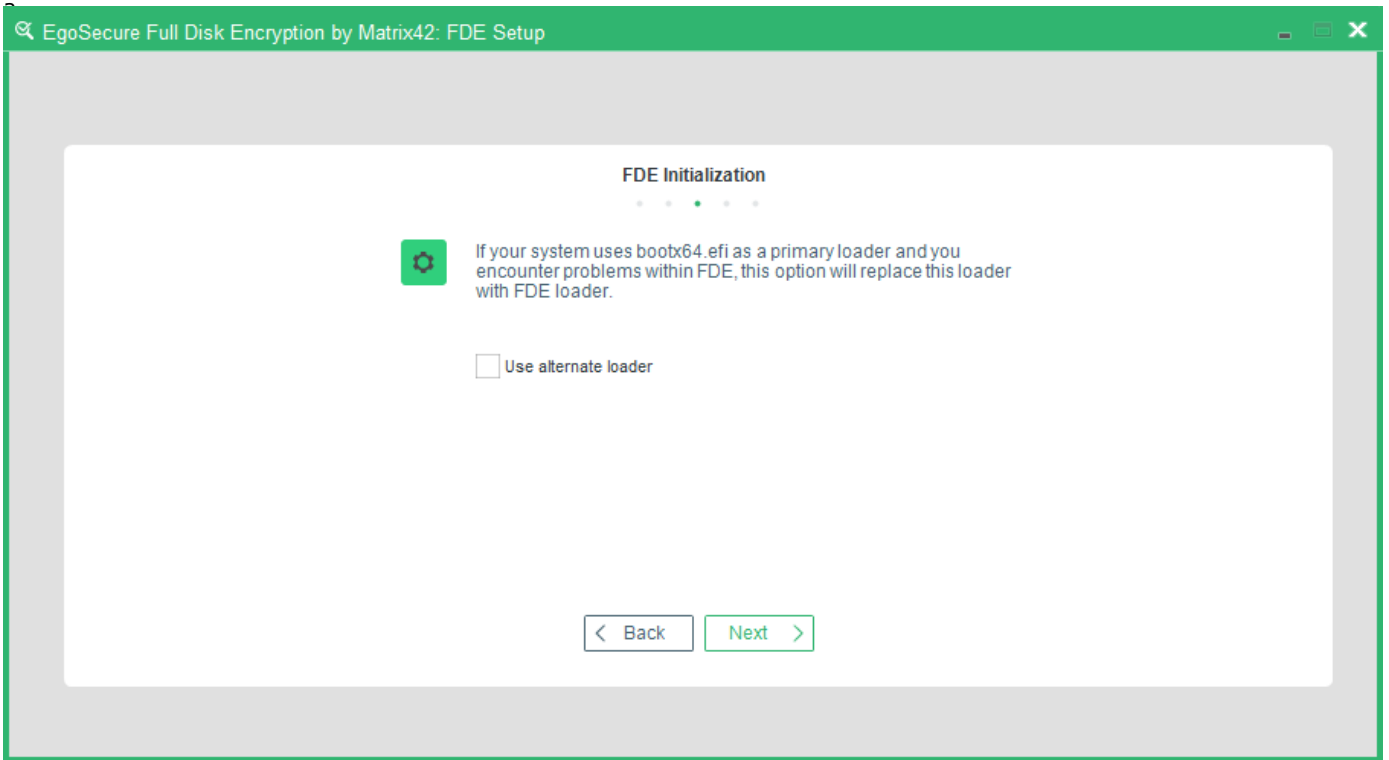
When updating BIOS or replacing hardware, the information used for key generation changes and **disk recovery will no longer be possible**. That is why, please, follow the steps below to avoid it:

1. Decrypt the disk.
2. Update BIOS or replace hardware.
3. Encrypt the disk.

System requirements for computers with TKEK

- UEFI systems starting with Windows 10 and later
- TPM devices with specification version 2.0 are supported only
- TPM must implement the following set of commands:
 - TPM2_CreatePrimary

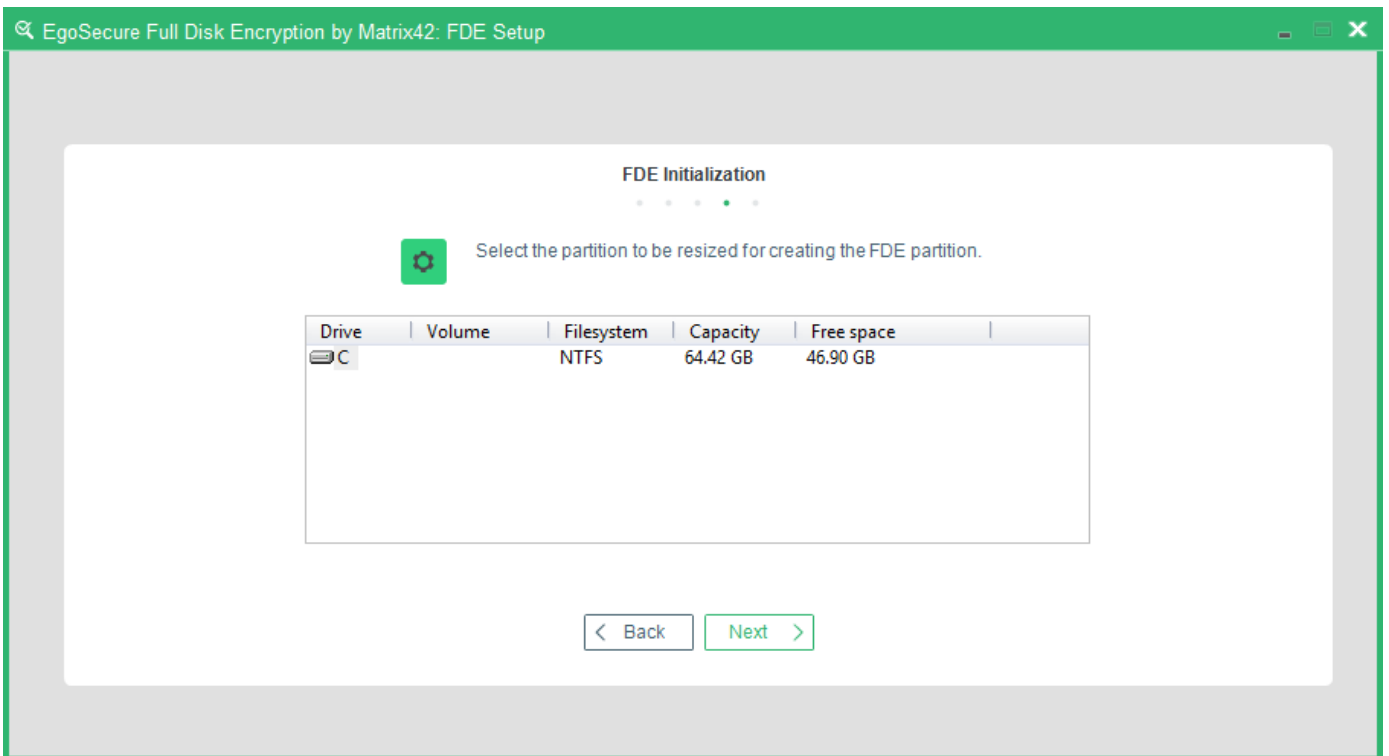
-
- TPM2_Create
 - TPM2_Load
 - TPM2_EvictControl
 - TPM2_FlushContext
 - TPM2_GetRandom
 - TPM2_RSA_Encrypt
 - TPM2_RSA_Decrypt
 - TPM2_ObjectChangeAuth
- TPM must support the following set of algorithms:
 - TPM_ALG_SHA256
 - TPM_ALG_RSA
 - TPM_ALG_OAEP
 - TPM_ALG_AES
 - TPM_ALG_CFB
 - TPM device must be in the **Ready** state.
6. Enable the **Generate hardware-based key encryption key** (HKEK) option and/or **Generate TPM-based key encryption key** (TKEK), and then click **Next**.
- The following dialogs appear if **Switch to expert mode** option was selected in the previous step.
7. Check **Use alternate loader** if PBA loading with current motherboard failed and you are now reinitializing FDE or your motherboard is considered as an old one.



→ The dialog, which informs, whether there is enough free disk space to install the PBA partition appears. You cannot use this dialog to select a partition for repartitioning – the free space available will be used to create new PBA Linux partition.

8. Select any of the drives, and click **Next**.

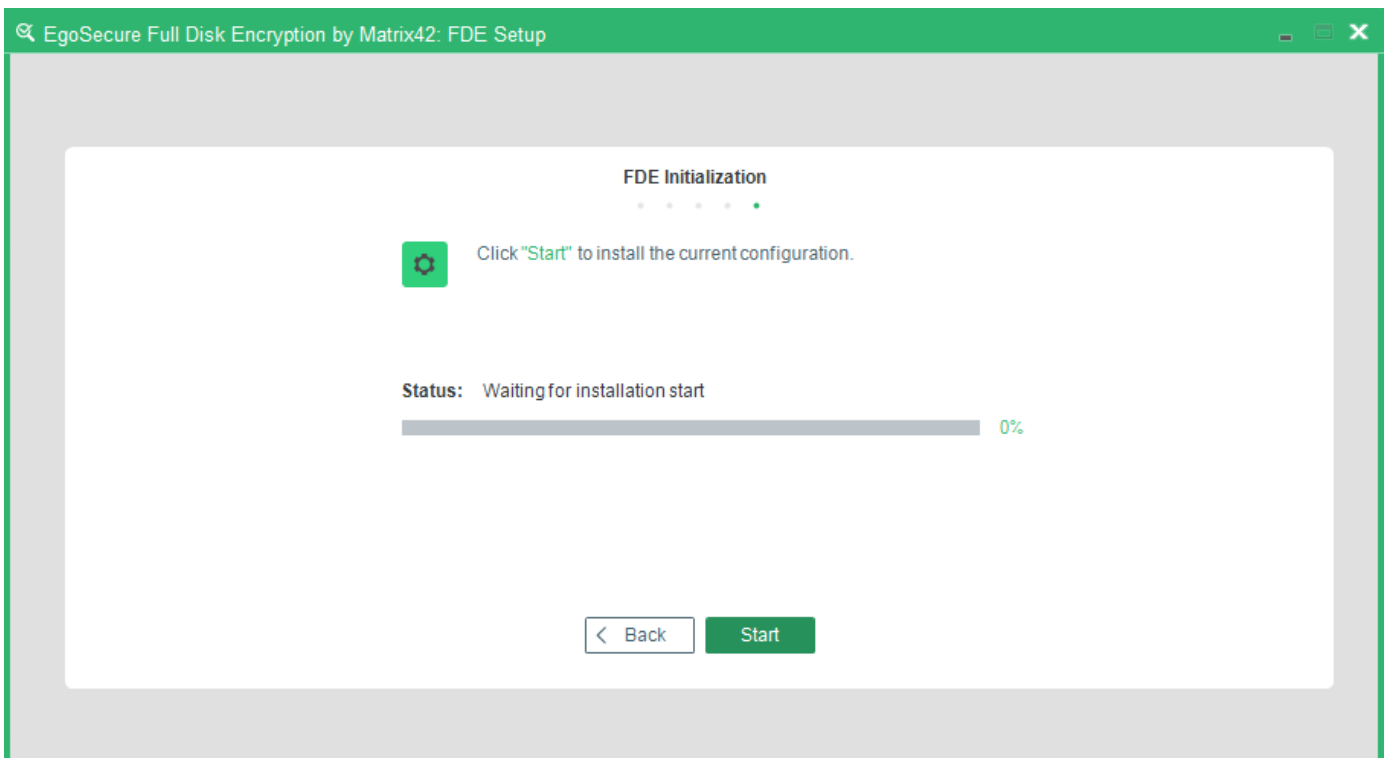
Figure 15. FDE Initialization – Display Partitions Dialog



- The selected partition will be cut to 500MB disk space for creating PBA Linux partition.
- The **Finish Initialization** dialog appears. The configuration parameters for FDE are now set.

9. Click **Finish** to install the FDE component.

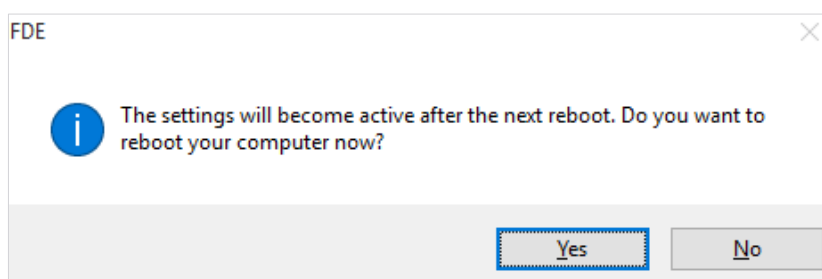
Figure 16. FDE Initialization (Expert Mode) – Finish Initialization Dialog



- If you selected to prepare the hard disk for FDE initialization, repartitioning is a complicated process and may take a few minutes to complete.


10. Once the initialization has finished, the following dialog appears:


Figure 17. FDE Initialization (Expert Mode) – Reboot Dialog



- The installation and initialization of the EgoSecure Full Disk Encryption component is now complete. You have also activated the configuration procedure for the PBA component – ready to be configured after you reboot the computer.

11. Click **Yes** to automatically reboot the computer and refer to the next step to guide you through the initialization of PBA.

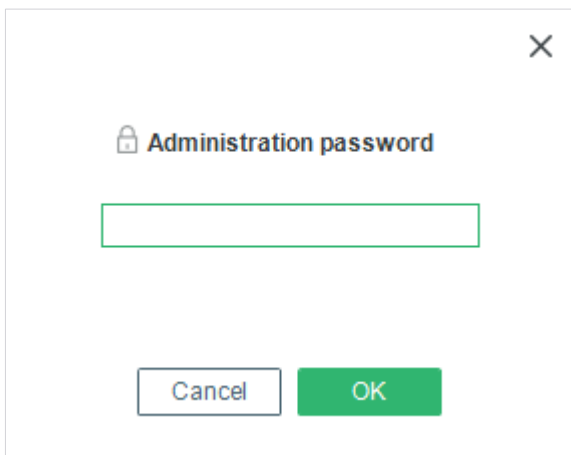
 WARNING	This reboot is absolutely necessary after the initialization of the FDE component. This is because the installer creates a small partition and it is necessary to let Windows check the disk (CHKDSK) BEFORE installing or initializing the PBA component on this small partition.
---	--

 INFO	Windows may prompt you to check the integrity of the hard disk after the computer has been restarted (CHKDSK utility). This is normal! Let Windows perform this check. Once the check is finished, Windows boots as usual.
--	--

Configuring PBA components

1. Once a computer is rebooted after FDE initialization and log on to *Windows* is performed as usually, the configuration of the PBA component starts. You will be prompted to enter the *EgoSecure Full Disk Encryption* administration password defined before.

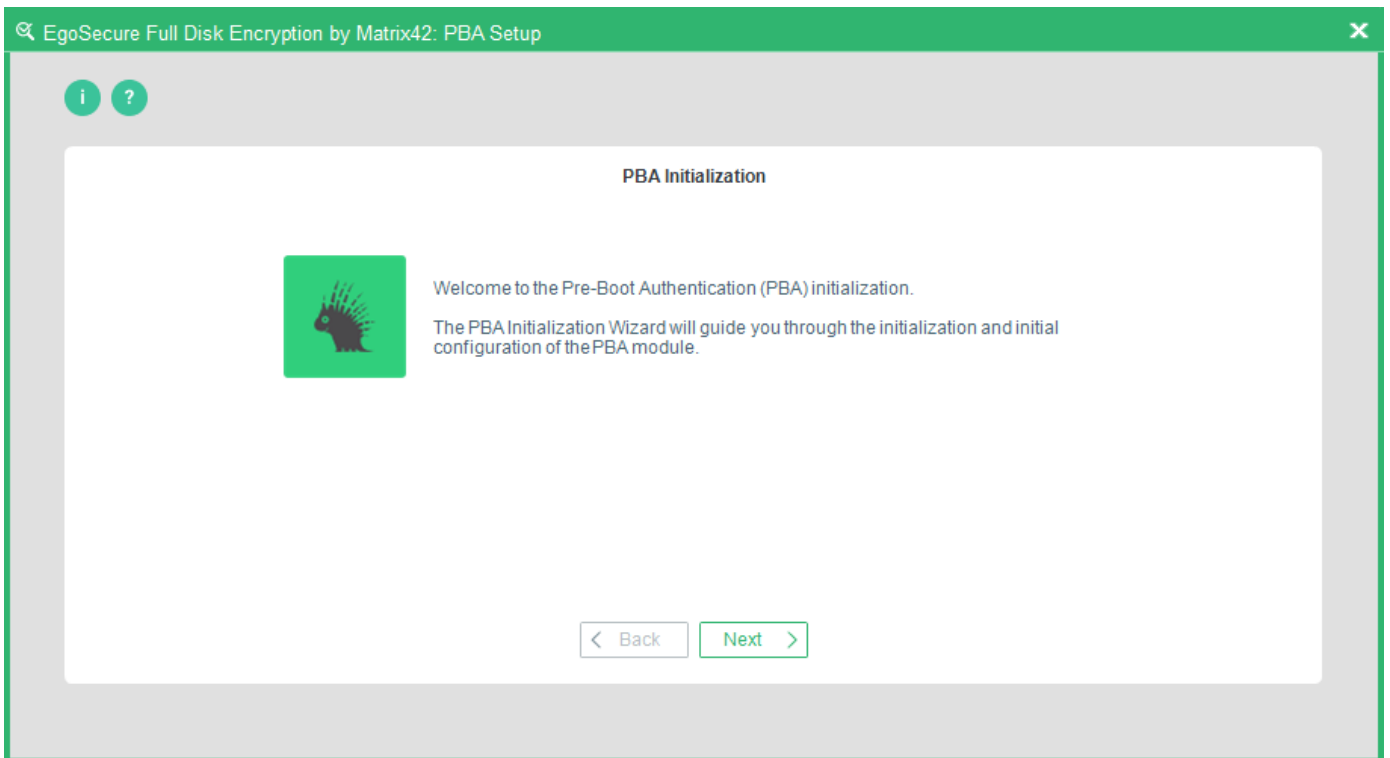
Figure 18. PBA Setup Wizard – Enter Administration Password Dialog



2. Enter the password and click **OK**. Click **Cancel** if you do not want to initialize the PBA component at this time. The **PBA Setup** welcome dialog appears.

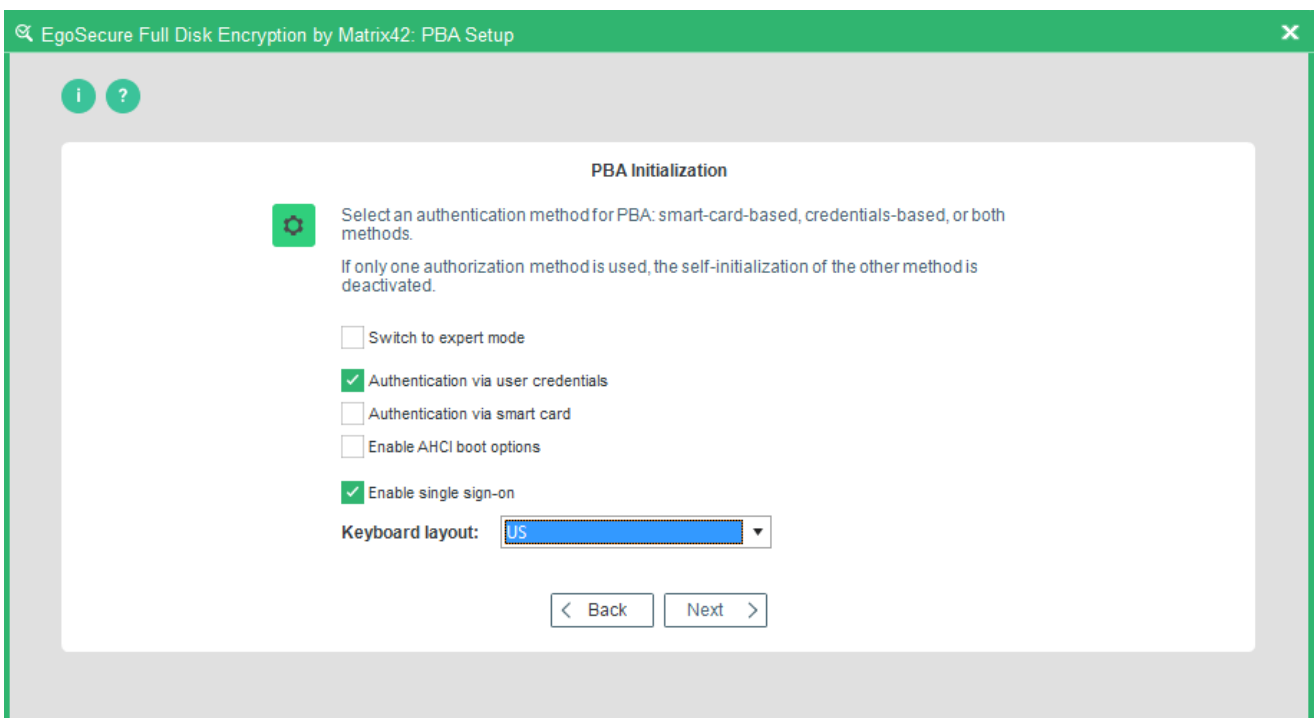
→ This wizard will guide you through the steps necessary to configure PBA for secure authentication and sign-on. Click **Next** to continue.

Figure 19. PBA Setup Wizard – Welcome Dialog



→ The **Authentication method** dialog appears.

Figure 20. PBA Setup Wizard – Select Authentication Method Dialog



This dialog allows for selecting the authentication method and keyboard layout for PBA. Please select whether you want to use smart card, user ID/password, or both authentication methods. You can also choose to activate SSO for user ID/password authentication.

The following options are available:

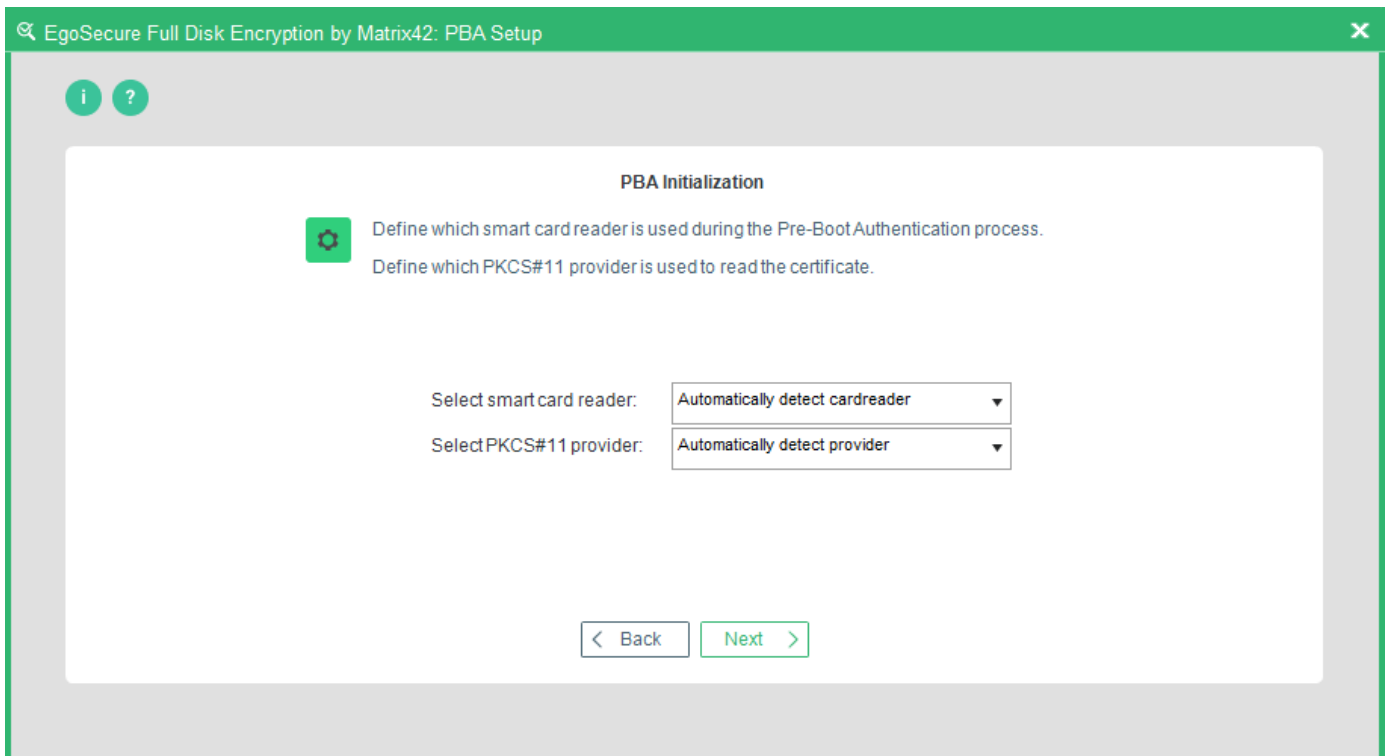
Option	Details
Switch to expert mode	Check this option if you want to configure further PBA options in this wizard (If you did not select this option, the wizard only displays the Finish button - in this case you will end up at step 13).
Authentication via user credentials	Check this option if you want to implement the user ID/password (<i>Windows</i> credentials) authentication method. The password for PBA must be no longer than 32 symbols.
Authentication via smart card	Check this option if you want to implement the smart card authentication method (If this option is not selected, the wizard will redirect you to step 5).
Enable AHCI boot options	This option will be enabled only if the BIOS is set to AHCI-mode: It gives you the possibility to easily test and use an alternative PBA configuration that could improve hardware compatibility (KICKSTART=KEXEC and Kernel parameter: AHCI-to-legacy). There is no guarantee that this option will resolve all hardware compatibility issues or the PBA boots up after that. The mechanism used here is Dmiconfig (refer to EgoSecure FDE - Administration and Usage Guide). Using this option creates a dmi.ini for the current hardware platform with the configuration stated above. If there is already an existing dmi.ini file, the user may be asked to overwrite it.
Enable single sign-on	Check this option if you want to activate the SSO method for smart card or user ID/password-based authentication.
Keyboard layout	Select the keyboard layout of the target computer to be used for PBA. <i>Keyboard layout for text-based and graphical Simple PBA (UEFI)</i> : only German and English layouts are supported. Directly in the mode, language switch is available only in graphical Simple PBA. <i>Keyboard layout for text-based Simple PBA (BIOS)</i> : only English layout is supported.

3. Once you have made your selection click **Next** to continue (or **Finish** if you did not select **Switch to expert mode** in which case you will end up at [step 13](#)).

In case you did not select **Authentication via smart card**, then proceed to [step 5](#).

- The **Smart card reader/provider** dialog appears if **Switch to expert mode** and **Authentication via smart card** options have been selected.

Figure 21. PBA Setup Wizard – Smart Card Reader/Provider Dialog



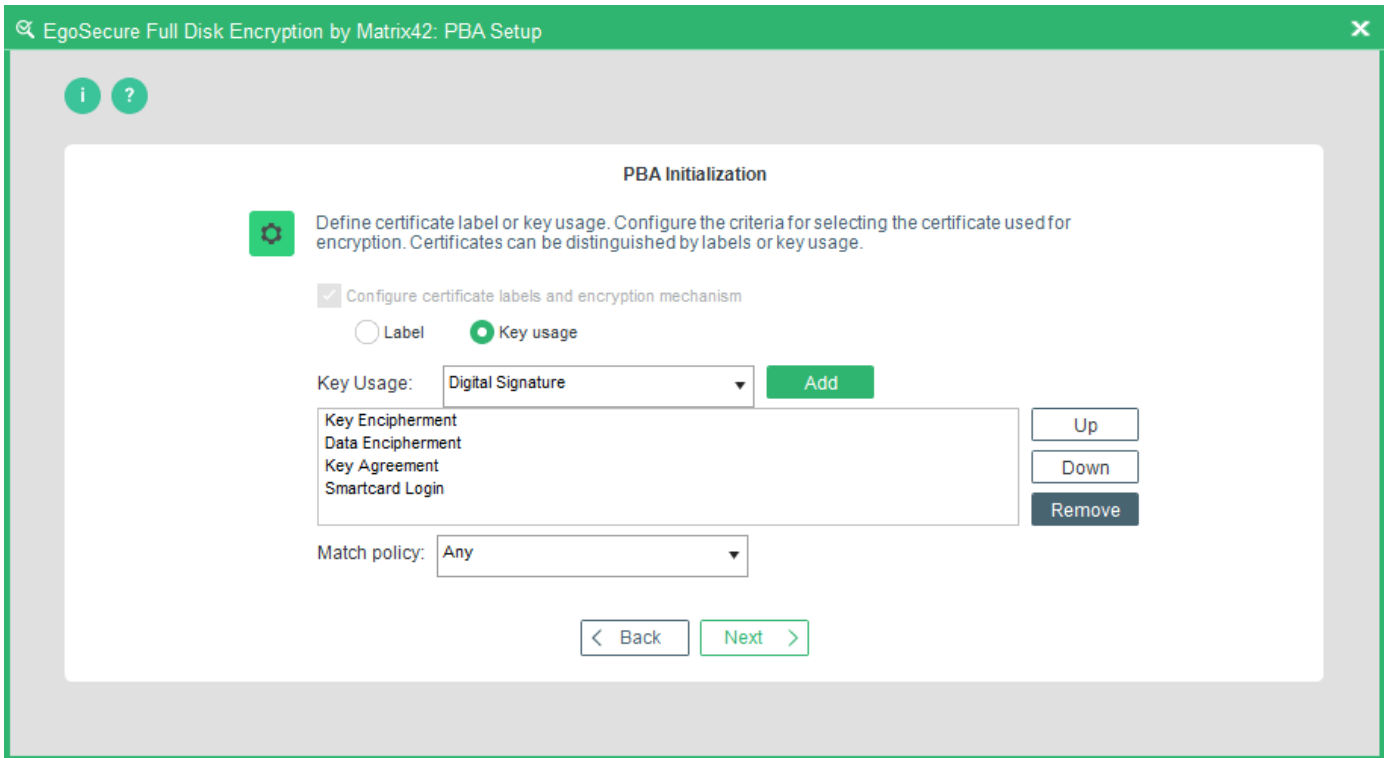
Use the following options to determine the smart card reader and provider:

Option	Details
Select smart card reader	Select the card reader you want to use for PBA from the drop-down list. Selecting a specific card reader vendor will decrease the amount of time it takes the computer to start; selecting Automatically detect card reader will increase the startup time because all the CCID-compliant readers contained in the generic CCID bundle delivered with <i>Linux</i> will be scanned until the correct one is found. NOTE: The <i>Linux</i> CCID bundle used in this version of <i>EgoSecure Full Disk Encryption</i> is version 1.3.11.
Select PKCS#11 provider	Select the PKCS#11 provider mechanism on the smart card by selecting it from the combo box. Choosing Automatically detect provider will mean that all the providers will be checked upon startup - this setting does not work with several smart cards. For further information, refer to the known issues in the release notes.

4. Once you have made your selection click **Next** to continue.

- The **Certificates** dialog appears (only applicable if you selected **Authentication via smartcard** before):

Figure 22. PBA Setup Wizard – Certificate Label or Key Usage Dialog



This dialog enables you to define the criteria for selecting the certificate used for encryption. Certificates can be distinguished by labels or key usage:

Option	Details
Label	<p>The term 'Label' refers to the filename of the certificate file on the smart card, for example User_Certificate.</p> <p>Follow these steps to add a certificate based on a Label:</p> <ul style="list-style-type: none"> ■ Select Label (the GUI will change). ■ Enter the label into the field Label and click Add. If the smart card contains more than one certificate (multi-user access) then you should add the labels for those as well. <p>If you have mistakenly entered a false label, select it from the list and click the Remove button to remove it from the list.</p> <p>To sort label preference, select a label in the list and click either Up or Down - the certificate that will be used for authentication is the first one in the list that matches the label criteria.</p>

Key usage

Key usage extensions define the purpose of the public key contained in a certificate. You can use them to restrict the public key to as few or as many operations as needed. For example, if you have a key used only for signing, enable the **Digital signature** and/or **Non-repudiation** extensions. Alternatively, if a key is used only for key management, enable **Key encipherment**. Follow these steps to add a certificate based on Key usage:

- Select Key usage.
- Choose a standardized form of key usage from the **Key usage** combo box, for example **Data Encipherment**, and click **Add**. To give preference to a specific key usage, select it from the list and click either **Up** or **Down**. Key usages at the top of the list have preference (the certificate that will be used for authentication is the first one whose key usage matches the criteria in the list). If you have mistakenly entered a false certificate label, select it from the list and click **Remove**.

The following warning messages appears if there is no certificate key /Label selected:

Warning ×


There is no certificate label defined ! Do you want to proceed with the already defined key usages ?

For further details about the key usages supported by EgoSecure Full Disk Encryption smart card authentication refer to [EgoSecure FDE - Administration and Usage Guide](#).

Match policy

Select one of the following policies:

- **Any**: The first certificate that contains any key usage from the list will be used.
- **All**: The certificate must fulfill all the key usages in the list.
- **None**: No certificate may contain any of the key usages from the list.



ATTENTION

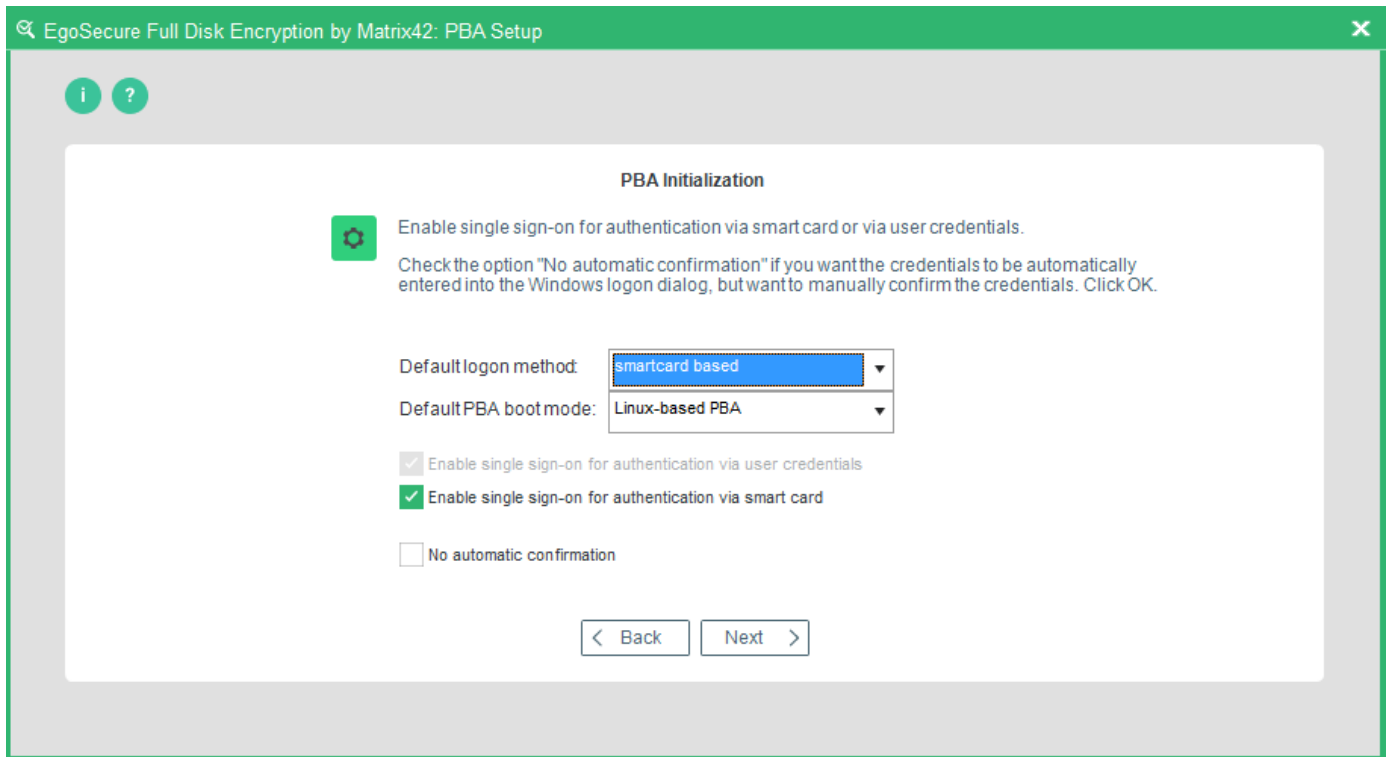
The certificate label and key label entries are case sensitive! Bear this in mind when defining the certificate labels or the key labels. If the labels are configured incorrectly it will prevent the successful authentication of the user and therefore the system will not start. If the **Key usage** is set to the wrong values, i.e. no certificate on the smart card matches the usage set in the list, then authentication is also not possible and the system will not start.

→ The **Single sign-on** dialog appears. Use the following options to determine an SSO method to *Windows*:

Option	Details
Default logon method	Select the default logon method from the combo box. Choose between Windows credentials (user ID/password based) or smart card-based logon. Both logon methods can be available at boot time.

Default PBA boot mode	<p>Select the default PBA boot method.</p> <ul style="list-style-type: none"> ■ Linux-based PBA: usual pre-boot authentication with its graphical user interface. ■ Text-based Simple PBA: simple pre-boot authentication without a graphical user interface. ■ Graphical Simple PBA: simple pre-boot authentication with a graphical user interface. Available only for UEFI systems. <p>For details, see Boot mechanisms</p>
Enable single sign-on for user ID/password authentication	<p>Check this option if you want PBA to take care of the traditional user name/password/domain logon to Windows (you will be required to enter the password only once at startup, make sure that the password is no longer than 32 symbols.).</p>
Enable single sign-on for smart card authentication	<p>Check this option if you already use a smart card (with X.509 certificates) to logon to the Windows domain.</p>

Figure 23. PBA Setup Wizard – Activate Single Sign-on Dialog



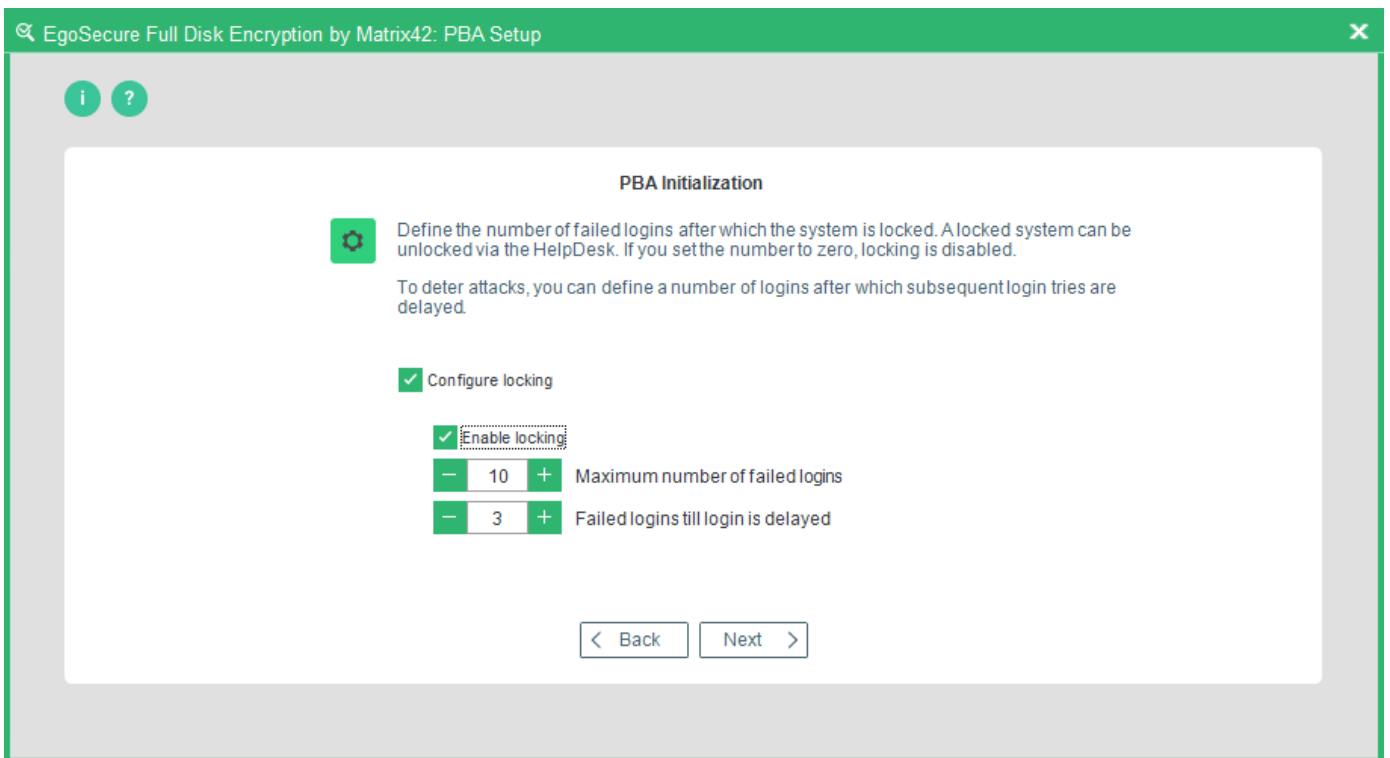
5. Once you have made your selection, click **Next** to proceed to the next step.

→ The **Configure Locking** dialog appears. Use the following options to help you configure how failed authentication attempts are handled:

Option	Details
Configure locking	Check this option to activate the locking feature (leaving this option unchecked allows the user to enter their password incorrectly a limitless number of times without penalty).
Maximum number of failed logins	Enter the number of times a user may attempt to enter the correct password. This number should be greater than that for Failed attempts

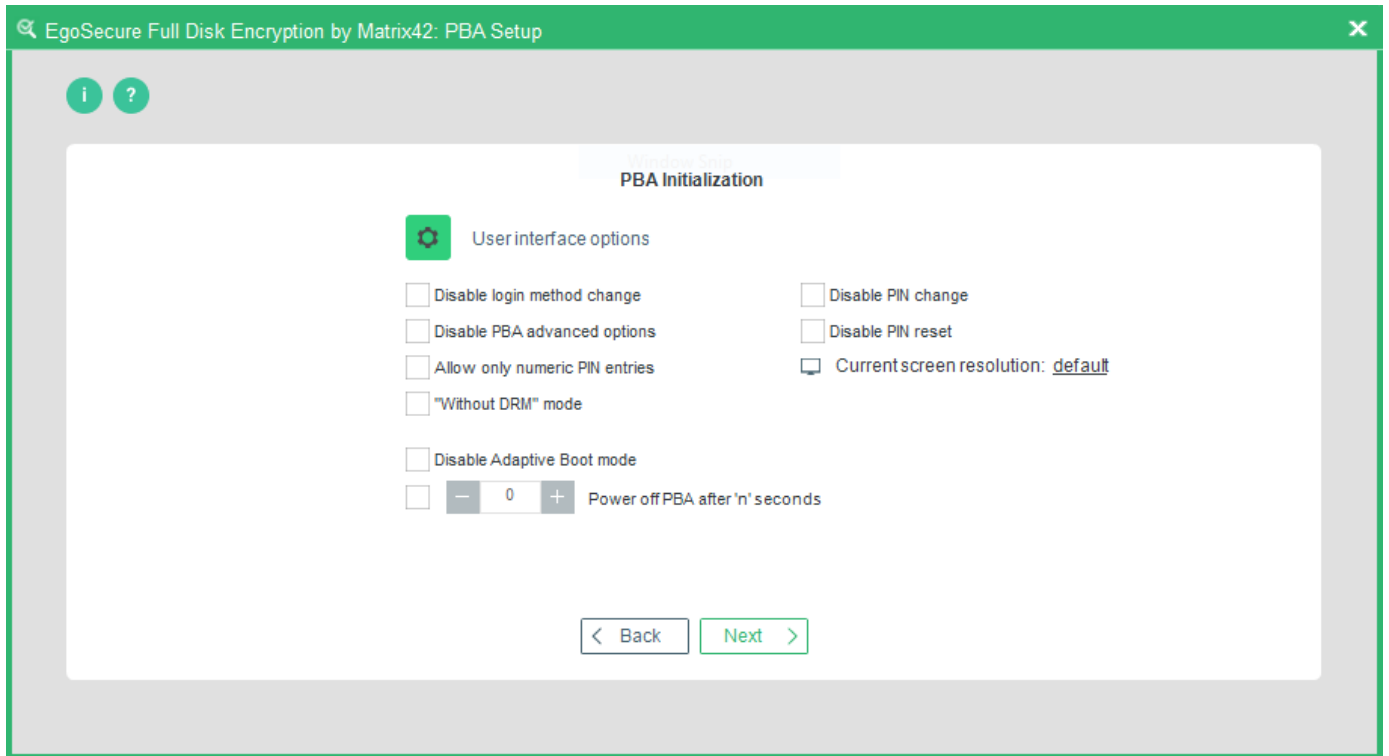
	after which login is delayed. Entering the value 0 means that locking is deactivated!
Failed logins till login is delayed	Enter the number of times a user may enter an incorrect password before being penalized with a time penalty the next time they logon. This number should be smaller than that for Maximum number of failed attempts .

Figure 24. PBA Setup Wizard – Configure Locking Dialog



- Once you have made your selection, click **Next** to continue.
→ The first PBA **Pre-Boot Options** dialog appears.

Figure 25. PBA Setup Wizard – Pre-Boot Options Dialog #1



Use the following options to determine which options should be available to the end user in the PBA component as well as the PBA state (dialog 1 of 2):

Option	Details
Disable login method change	Check this option to disable switching between authentication methods in the PBA component. NOTE: This means that once a specific authentication method has been selected together with this option, there is NO CHANCE to select the other authentication method in the PBA.
Disable PBA advanced options	Check this option to disable access to the PBA advanced options. NOTE: Enabling this option means that there is NO CHANCE to enter the advanced PBA options in the PBA.
Allow only numeric PIN entries	Check this option to allow only numeric smart card PIN entries.
Disable PIN change	Check this option to prevent smart card users from changing their PIN during the PBA-HelpDesk procedure.
Disable PIN reset	Check this option to prevent smart card users from resetting their PIN during the PBA-HelpDesk procedure.
Screen resolution	If a screen resolution is not specified, the default value take effect. It means that EgoSecure specifies screen resolution automatically, but in some cases this resolution doesn't fit. E.g. 800x600 is a good selection for laptop devices. <i>Limitations for BIOS systems:</i> the option for changing the screen resolution works only with ACPI kernel where DRM is enabled.
"Without DRM" mode	Enable this boot mode option if there are problems with graphic card and PBA loading.
Disable Adaptive Boot mode	Adaptive Boot mode is used to automatically select the PBA boot mode that is needed for correct operating system boot. If the

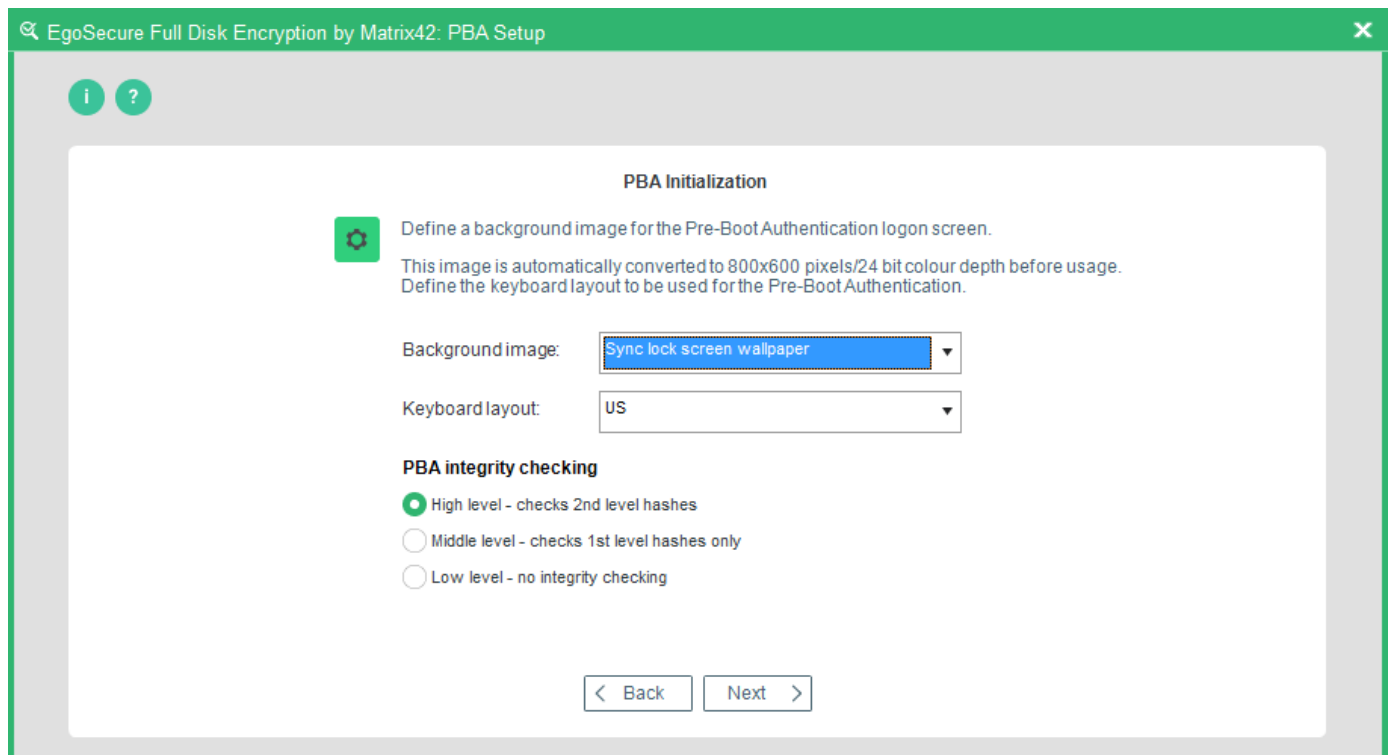
problem phase is identified, a user is informed. By default, Adaptive boot mode is enabled. For details about available boot modes, see *boot mechanisms* in the [EgoSecure FDE - Administration and Usage Guide](#).

Power off PBA after 'n' seconds


Check this option to allow the PBA to shutdown the computer if the PBA remains unattended. Also enter the number of seconds the PBA should wait before shutting down the computer.

→ The second **PBA Pre-Boot Options** dialog appears:

Figure 26. PBA Setup Wizard – Pre-Boot Options Dialog #2



7. Configure the following options (dialog 2 of 2):

Option	Details
Background image	Use this option to select an optional background for the PBA screen. Click '...' to open the file browser and to select an image of your choice (the image will be automatically resized to the correct resolution and color depth for the PBA screen - 800x600 pixels, 24-bit). <ul style="list-style-type: none"> ■ Default to use a default PBA image. ■ Sync desktop wallpaper to use an individual desktop wallpaper of each computer where PBA is launched. ■ Sync lock screen wallpaper to use an individual lock screen wallpaper of each computer where PBA is launched. ■ Custom to select an optional background image. The image is automatically resized to the correct resolution and color depth for the PBA screen: 800x600 pixels, 24-bit.
Custom image path	If you selected Custom in the field above, click  in the Custom image path field to define a path for a background image.
Keyboard layout	Use the combo box to select which keyboard layout to be used for PBA.

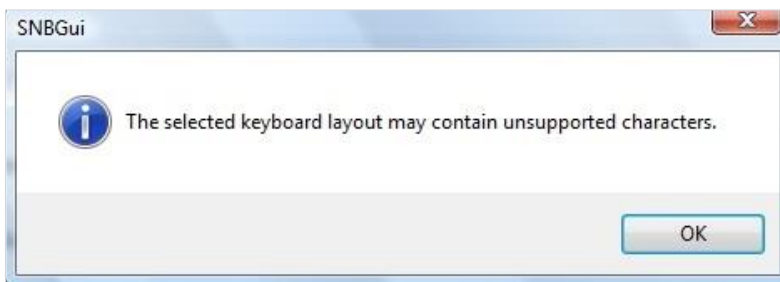
Keyboard layout for text-based and graphical Simple PBA (UEFI): only German and English layouts are supported. Directly in the mode, language switch is available only in graphical Simple PBA.
Keyboard layout for text-based Simple PBA (BIOS): only English layout is supported.

PBA integrity checking

'Integrity checking' is the guarantee that the Linux PBA components are protected against tampering by third parties. The following levels are available:
High Level (highly recommended) will check first and second-level hashes and offers the most security, but is slower than the other two. This is the default parameter.
Middle level will check first-level hashes only and offers a compromise between speed and security.
Low level (not recommended) -No integrity checking is performed which means the PBA will boot quicker, but there is no security against tampering by third parties.

8. Once you have made your selection click **Next** to continue.

→ The following dialog may appear:



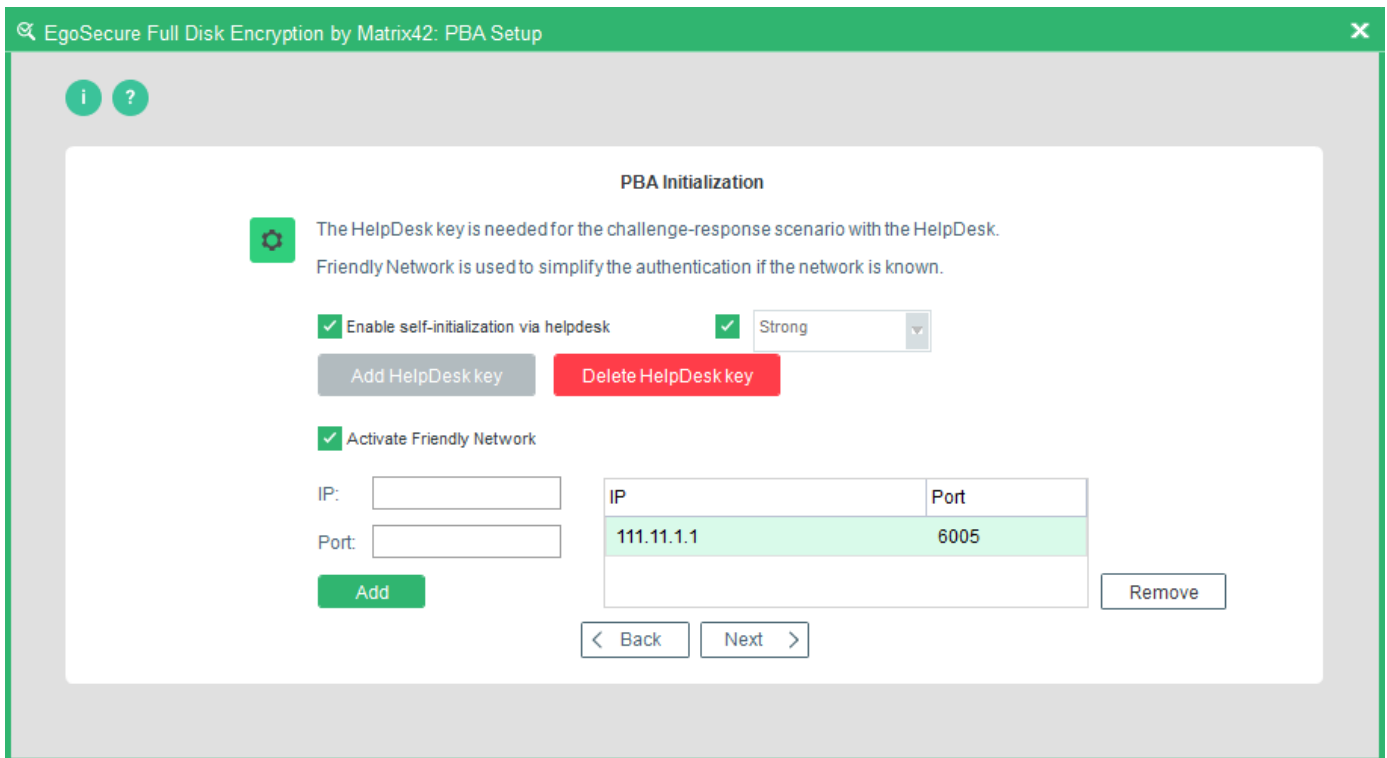
This dialog informs you that the selected keyboard layout does not match that of the operating system and may cause problems (different character positions) when used in the PBA (the installer assumes that the keyboard layout matches the language of the operating system). If you are sure about your selection click **OK** and continue with the next step. If you are not sure, click **OK** and then **Back** to review your selection.

The background image in this step is solely for an installation on the local hard disk. If you intend to deploy the same background image to several target computers in an unattended installation (click the [link](#) for details), then make sure you either copy the image to each target computer per software distribution first or create a branding file to be placed together with the installer.

EgoSecure recommends that you copy the image to the C:\WINDOWS\NAC directory, create a policy, and then deploy (see [EgoSecure FDE - Administration and Usage Guide](#) for details).

→ The HelpDesk Keys and Friendly Network dialog appears.

Figure 27. PBA Setup Wizard – Helpdesk Keys and Friendly Network Dialog



This dialog is for configuring the HelpDesk keys for use in an emergency. The HelpDesk is a central point of contact (in-house or third party) that can be contacted when you have forgotten a password, misplaced or broken the smart card, or if the smart card reader is defective. If you do not have an enterprise-wide HelpDesk, then ignore this feature. The HelpDesk uses a challenge–response process to unlock your hard disk. Once you configure HelpDesk, you can activate Friendly Network.

EgoSecure Full Disk Encryption HelpDesk (via HelpDesk Key)

This HelpDesk is used when a user has mislaid or lost smart card, or forgotten the *Windows* credentials. Furthermore, the PBA HelpDesk can also place PBA in 'user capture' mode. This means either the user can register a new smart card, or after a successful *Windows* logon, the user's credentials are newly embedded in the PBA component. The HelpDesk key is provided as a file by the respective *EgoSecure Full Disk Encryption* HelpDesk administrator to be imported into PBA for such an event.

Friendly Network

Friendly network simplifies the process of booting if the network is known. If computer is outside the known network, the PBA asks for authentication. PBA authentication phase is skipped with the help of Helpdesk. When PBA is booted, helpdesk request is generated and sent to the Server. An attempt to sign in to the system on the basis of a server response is made. If the attempt is successful, the computer is restarted followed by *Windows* boot. If the attempt is unsuccessful (incorrect network configuration, no connection to the Server etc.), PBA authentication is needed as usually.



ATTENTION

Restrictions:

- ◆ Not compatible with BIOS Simple PBA (text-based mode).
- ◆ The ACPI boot mode is not supported.
- ◆ Not compatible with Linux-based PBA if SSL is enabled.

Recommended (only BIOS): disable Quick Boot (Fast Boot) in BIOS settings as it skips the network drivers necessary for Friendly Network.

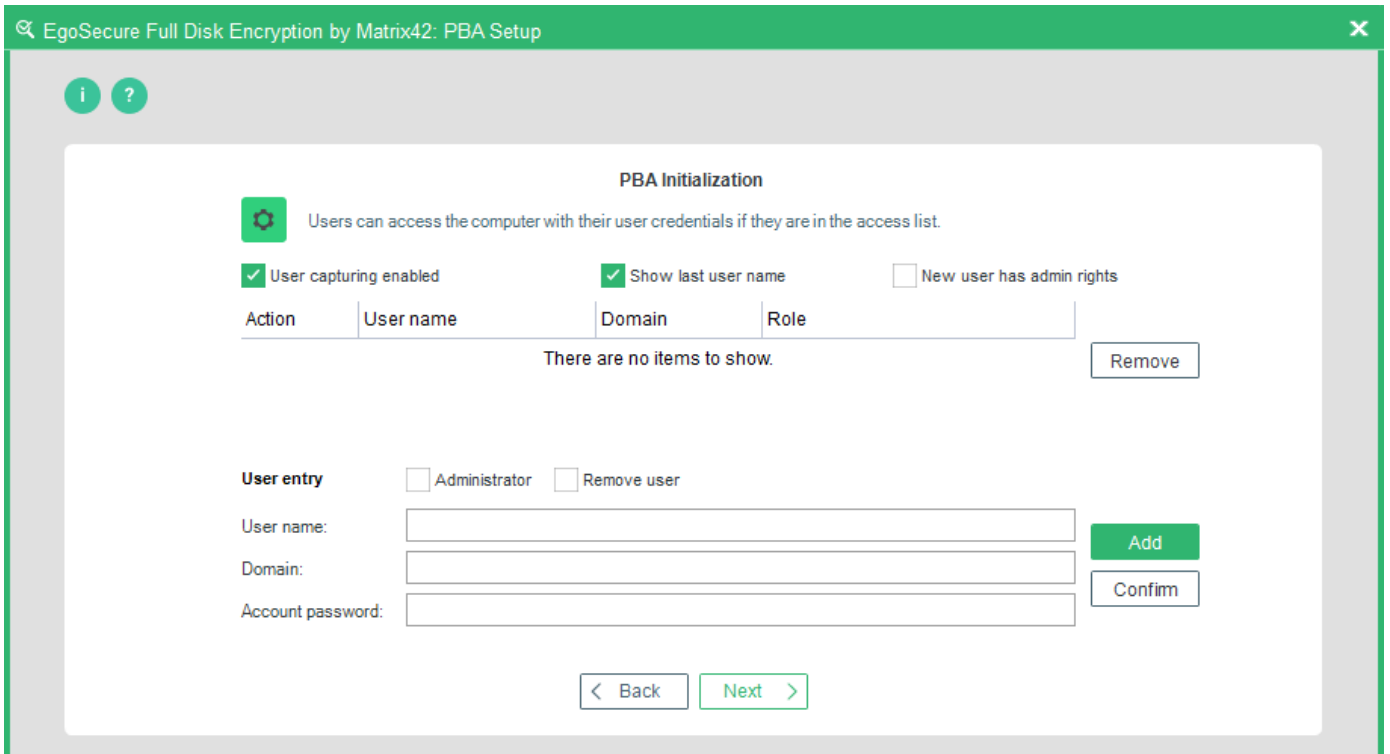
The following options are available:

Option	Details
Add Helpdesk key	Import a HelpDesk key from a password-protected HelpDesk file. The helpdesk file is exported from a PBA HelpDesk application or from the EgoSecure Data Protection Console (Product settings FDE Helpdesk). NOTE: The HelpDesk feature has two different types of HelpDesk communication: <i>Comfort</i> - quick with good security, and <i>Strong</i> - very secure. It is important that you choose a method BEFORE you import the HelpDesk key file. The Import HelpDesk Key dialog will appear. Click the `...` button to open the file explorer. Select the HelpDesk file and click Open . Enter the password for the file into the Key password field and click Import .
Delete Helpdesk key	Delete a HelpDesk key that has been imported into PBA.
Enable self-initialization via helpdesk	Check this option if you want the HelpDesk administrator to 'allow' the user to capture their <i>Windows</i> credentials/smart card details in an emergency. This means that the user is allowed to re-authorize himself/herself (smart card or Windows credentials) when the computer is next booted.
Activate Friendly Network	Activate Friendly Network so that if connection to the Server can be established during PBA, the authentication is skipped and boot into Windows occurs.
IP	Enter the IP address of the management server. This can be the EgoSecure Server or your own one.
Port	Enter the IP address of the management server.

9. Once you have made your selection, click **Next** to continue.

→ The Windows Credentials dialog appears.

Figure 28. PBA Setup Wizard – Windows Credentials Dialog



This dialog helps you to define the users to be authenticated to the system via their *Windows* user account details.

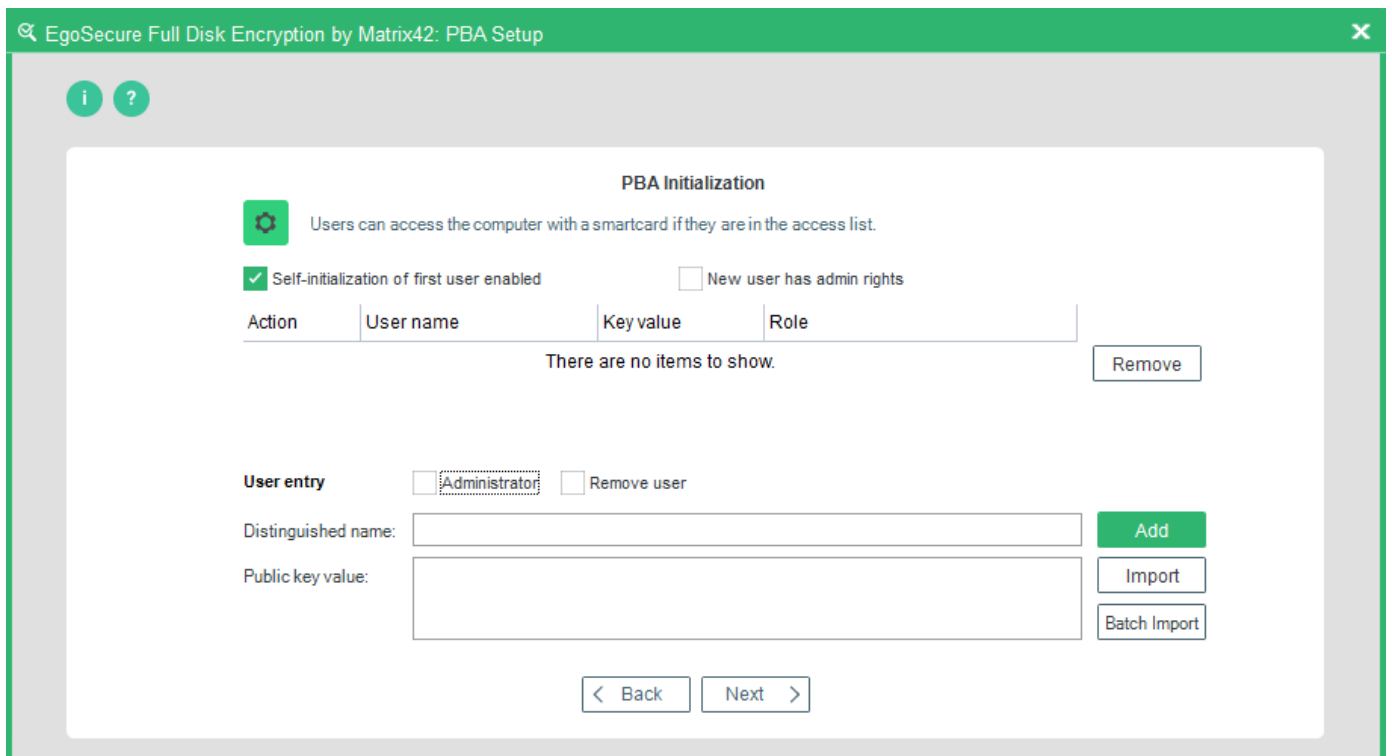
The following options are available:

Option	Details
User capturing enabled	Check this option to allow the next user who logs on to the computer to be initialized as a valid user (this means that it is not necessary to add a user to the list).
New user has admin rights	Check this option to allow the next new user who logs on to the computer to have Admin rights.
Show last user name	Check this option to always display the user name of the last known logged-on user in the PBA logon dialog.
User entry [area]	<p>If you do not check User capturing enabled, then you must enter your <i>Windows</i> account details in this area to be able to log on to the computer.</p> <p>Follow these steps to add a user to the list:</p> <ol style="list-style-type: none"> 1. Enter the User name, Account Password, and Domain in the respective fields. The password for PBA must be no longer than 32 symbols. User name must not contain any of the following characters: / \ [] " : ; < > + = , ? * % @ 2. Click New user has admin rights to enable the user to have administrator rights. Admin has the right to capture new user and delete user from the PBA user management list.

3. Click **Add** to complete the entry. The user will be added to the PBA management list.
4. Click **Confirm** to confirm the user's account password. You can remove any user who has already been added to the list by selecting the user and clicking **Remove**. You can promote any user already added to the list as a **User Admin** by selecting the user and clicking **Promote**.

10. Once you have made your selection (and optionally added users), click **Next** to continue.
 - The **Smart Card user** dialog appears. This dialog helps you to define the smart card users to be authenticated to the system.

Figure 29. PBA Setup Wizard – Smart Card User Dialog



The following options are available:

Option	Details
Self-initialization of first user enabled	Check this option to allow the user that logs onto the computer at the next start with a valid smart card (correct PKCS#11 provider and credentials – key or certificate label), to be automatically initialized as a valid user (this means that it is not necessary to enter a user into the list via the User entry area).
New user has admin rights	Check this option to allow the next new user who logs on to the computer to have Admin rights.
User entry	If you did not check Self initialization of first user enabled , then you must manually enter the user certificate details in this area to be able to log on to the computer. Follow these steps to add a user to the list: <ol style="list-style-type: none"> 1. Check New user has admin rights to enable the user to have administrator rights. Admin has the right to capture new user and delete user from the PBA user management list.

2. Now you can:
 - a. enter the certificate information manually,
-OR-
 - b. import a certificate.

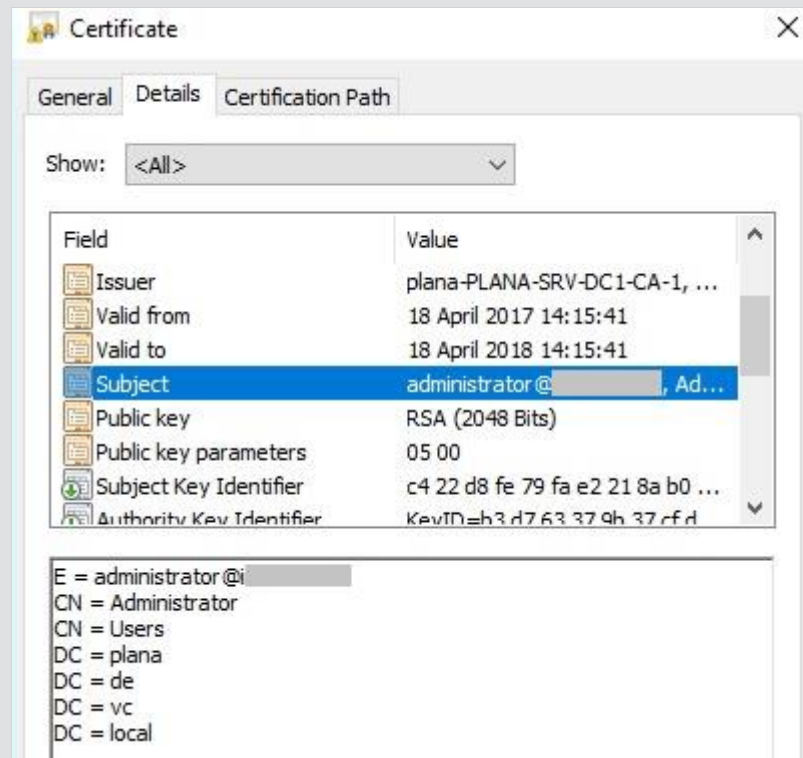
To fill in the **Distinguished name** and **Value of public key** fields:

1. Right-click a certificate and select *Properties* from the context menu.
2. In the *Certificate* dialog, navigate to the *Details* tab.
3. Copy the data from the *Value* column of the *Subject* entry to the **Distinguished name** field.
E.g.: local, vc, de, plana, Users, Administrator, administrator@....
4. Copy the data of the **Public key** entry to the **Value of public key** field.

Special characters and order



- ◆ In most cases, the values of the **Subject** field are pasted in the reverse order. Test if it works, if not - import a certificate (as described below) to see which order is the right one, because it depends on the smart card specification.
- ◆ Special characters are not supported. Check if there are any special characters in the required fields.



- b. *Importing a certificate*: Click **Import**, select the X.509 certificate (*.cer; der-encoded) from the file explorer [**Open**],

then click **Add**. The user details are now in the list, but not yet in the system. Click **Apply** to complete the entry.

- You can remove any user who has already been added to the list by selecting the user and clicking **Remove**.
- You can promote any user already added to the list as a **User Admin** by selecting the user and clicking **Promote**.

11. Press **Next** to continue.

As an alternative to importing each certificate separately, you can import all of them in a single step via the Batch Import function as follows:

- Make sure all the certificate files are in a single directory.
- Click **Batchimport** to open the file explorer.
- Select the certificates directory and click **OK**. A dialog will appear informing you about how many certificates have been found in the directory:



12. Click **OK**.

→ An import success dialog will appear:



13. Click **OK**. The user entry list now contains the users:

Action	User name	Key value
	DE, █████ IT security GmbH, Jon	
Add	DE, █████ GmbH, Stephan	30 8102 02 0A ...
Add	DE, █████ GmbH, █████ Trustfactory ST...	82 01 0A 02 02 ...

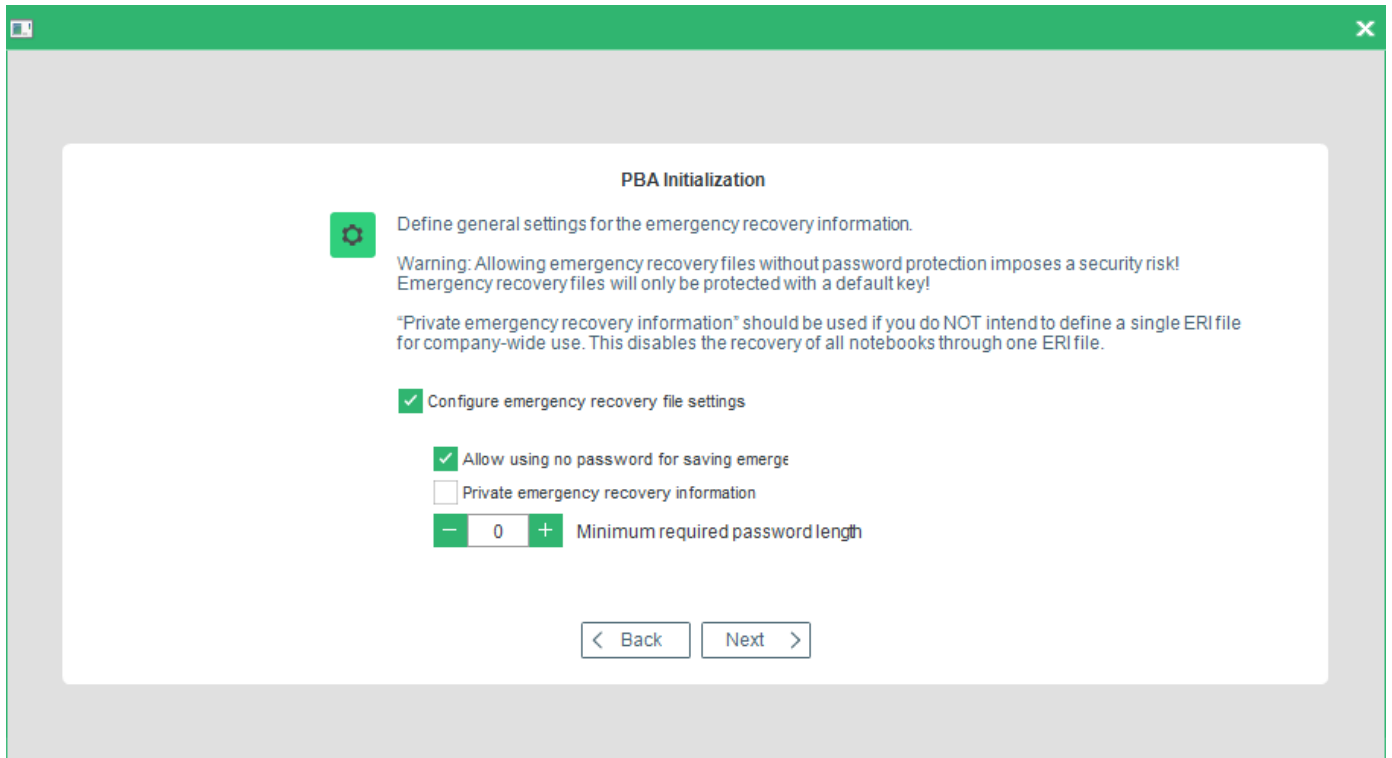
14. Click **Apply** to confirm the entries.

→ The ERI settings dialog appears. The following options are available:

Option	Details
Configure emergency recovery files settings	Check the option to allow the use of ERI files (recommended).
Allow using no password for saving emergency recovery information	Allow user to save unprotected ERI files (not recommended).
Minimum required password length	Length of ERI password. Use the up/down arrows in the number field to set a minimum password length for the ERI file (at least 8 characters are recommended).
Private emergency recovery information	Check this option if you want ERI files generated on this computer to be able to recover this computer only (recommended for a strict security policy). If you leave this option unchecked, an administrator

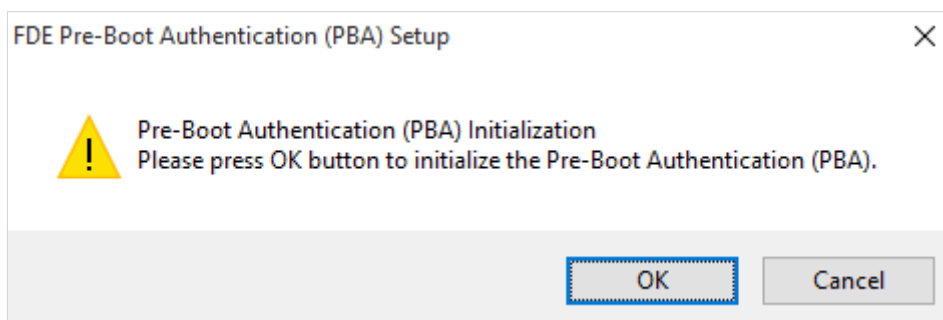
can access this computer using an ERI file generated on a similar system.

Figure 30. PBA Setup Wizard –ERI Settings Dialog



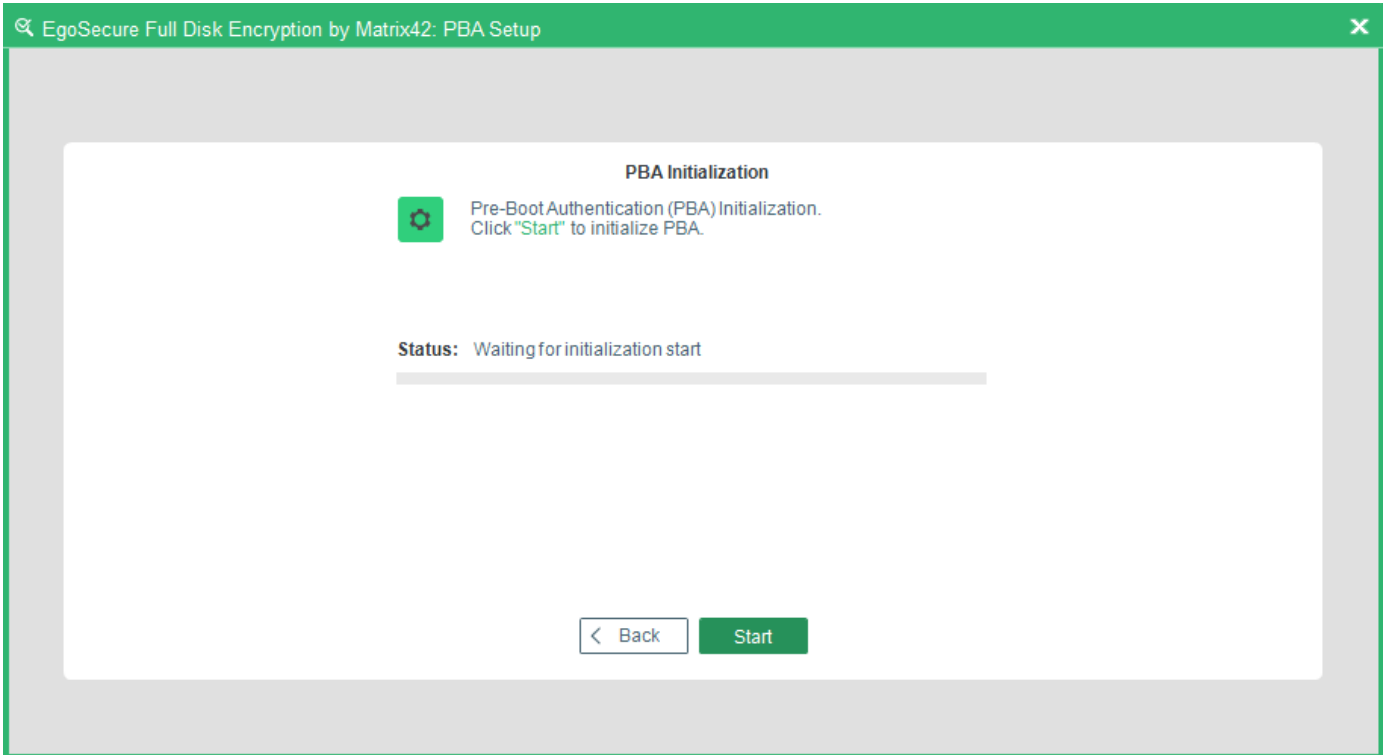
→ The **Pre-Boot Authentication** message dialog appears.

15. Click **OK** to initialize Pre-Boot Authentication.



→ The **Initialization** dialog appears. The initialization should start automatically. If not, click **Finish** to start the initialization procedure. It may take a while to complete - please be patient.

Figure 31. PBA Setup Wizard – Initialization (Status) Dialog



→ If the initialization is successful, the dialog prompting to restart appears:

- The initialization of the PBA component is now complete. The new PBA settings will become active after the shutdown or restart of the computer. If you have selected **Enable smart card user capturing** or **Enable user ID/password capturing** options during the initialization, there is no need for authentication upon the initial PBA start (EgoSecure Full Disk Encryption will capture the user credentials of the first user who logs-on to the computer).



ATTENTION

Shutdown and then restart the computer after the initialization of the PBA component to, optionally, capture user credentials (this does not apply to if user credentials or certificates have been passed onto the PBA component via an initialization policy).



WARNING

Please uninstall FDE immediately if PBA initialization fails for any reason. Do not shutdown the system unless an ERI file was successfully generated.

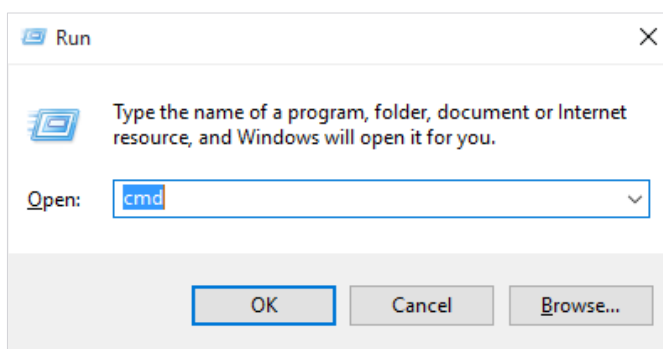
Unattended installation

To start an unattended installation of FDE, you may need an initialization policy generated by the *EgoSecure Full Disk Encryption Policy Builder* – this means that you must install (but not initialize) *EgoSecure Full Disk Encryption* once to access each of the Policy Builder. For details about deploying policies, see the [EgoSecure FDE - Administration and Usage Guide](#), chapter 1.14 “Remote administration”.

Be aware that the computer will reboot after the initialization of the FDE component. This is because the installer needs to create a small partition outside of the Windows runtime (this is also used for the PBA and is needed even if the PBA is not installed), as well as letting Windows register the encryption driver correctly. An optional, further reboot is necessary after the initialization of the PBA component to capture user credentials (this does not apply if user credentials or certificates have been passed onto the PBA component via an initialization policy).

Follow these steps below to perform an unattended installation:

- 1. Customizing (optional):** You can customize your setup through the following steps:
 - If you have created a dmi.ini file for computers set for ‘Hardware Compatibility Mode’ then place it in the same directory as the *EgoSecure Full Disk Encryption [version].msi* package so that computers that need specific installation setting will be automatically recognized by the installer. For further information about how to create alternative installation parameters (also known as ‘Hardware Compatibility Mode’) refer to [EgoSecure FDE - Administration and Usage Guide](#).
 - If you have a specific background image for the PBA or HelpDesk text files that must be deployed, then place the EHDDbrand.bin file in the same directory as the MSI package.
- 2.** Prepare the **EgoSecure Full Disk Encryption** installation file.
- 3.** Open a **Command** window (select **Start>Run**). The following dialog appears. Enter *cmd* in the **Open** field, and click **OK**.



- 4.** The **Command** window appears. Navigate to the directory, where the *EgoSecure Full Disk Encryption* installation package is located. Two installer packages are available: for 32-bit systems use *Full Disk Encryption.msi*, and for 64-bit systems use *Full Disk Encryption x64.msi*.

- 5.** Use the following syntax to call the setup:

```
msiexec /i "<full path to the msi package, file name, file extension>" /qn  
[<PROPERTY>=<value>] /! *vx "<full path to log file>"
```

For example, enter the following:

```
msiexec /i "C:\FDE versions\EgoSecure Full Disk Encryption by Matrix42 [version].msi" /qn
ADDLOCAL=FeatureFde,FeaturePba INITFDEQ=1 /!*vx "C:\log files\log.txt"
```


The following *Microsoft* installer-related options are available:

Command line option	Details
/i, /qn, /qf	<p>Microsoft installer parameters:</p> <ul style="list-style-type: none"> ■ /i [package]: Install a specific package. ■ /qn: Quiet mode -no user interface (the same as /q). ■ /qf: Quiet mode with full user interface.
Full Disk Encryption by [version].msi, Full Disk Encryption [version]x64.msi	The file name of the EgoSecure Full Disk Encryption installer package according to system (32-bit/64-bit).
/!*vx log.txt	<p>Create a very detailed log file of the unattended installation under the file name log.txt. vx stands for a detailed log file. If you do not want to have a detailed log file, remove this parameter.</p>

The following EgoSecure Full Disk Encryption related options are available:

Command line option	Details
ADDLOCAL	<p>To install only FDE or both FDE and PBA for standard hard disks use the following (!the commands are case-sensitive):</p> <ul style="list-style-type: none"> ■ ADDLOCAL=FeatureFde to install only FDE. ■ ADDLOCAL=FeaturePba to install only PBA. ■ ADDLOCAL=FeatureFde, FeaturePba to install both FDE and PBA. ■ ADDLOCAL=FeatureAPI to install the API libraries (snbreportapi.dll, policyencryptor.dll) necessary for third-party consoles to interact with <i>EgoSecure Full Disk Encryption</i> (deprecated). ■ ADDLOCAL=FeatureTpm to install TPM support. ■ ADDLOCAL=FeatureCPL to install control panel. ■ ADDLOCAL=FeaturePolicyBuilder to install Policy builder (FDE Policy Builder, PBA Policy Builder and Upgrade Policy Builder) ■ ADDLOCAL=FeatureRecovery to install recovery tools (PE ERD, Secure Erase and Secure Wipe) <p>NOTE: If this property is not entered the FDE/PBA components will not be installed. HINT: If those combinations don't fit your needs it might help to use the MSI-switch 'REMOVE=' in combination with 'ADDLOCAL=All'</p>
ADMINPWD	<p>This option allows you to provide the administration password for FDE initialization/de-initialization. For example: ADMINPWD=12345678 This property can only be used without property FDEPOLICY.</p>

<i>FDEPOLICY</i>	Provide the file name and path of an FDE initialization policy, for example: <code>FDEPOLICY="c:\fdeinit.nbs"</code> . NOTE: This property must be used together with <code>INITFDEQ</code> .
<i>INITFDEQ</i>	Initialize FDE after installation. Enter: <ul style="list-style-type: none"> ■ <code>INITFDEQ=1</code> to start initialization ■ <code>INITFDEQ=0</code> to leave initialization until later <p>This property can only be used in combination with <code>ADDLOCAL</code>. If this property is not entered FDE will not be initialized.</p>
<i>INITPBAQ</i>	Initialize PBA after installation. Enter: <ul style="list-style-type: none"> ■ <code>INITPBAQ=1</code> to start initialization ■ <code>INITPBAQ=0</code> to leave initialization until later <p>This property can only be used in combination with <code>ADDLOCAL</code>. If this property is not entered PBA will not be initialized.</p>
<i>PBAPOLICY</i>	Provide the file name and path to PBA initialization policy, for example: <code>PBAPOLICY="c:\pba.pba"</code> . NOTE: This property can only be used if the property <code>INITPBAQ=1</code> is also used.
<i>LANG</i>	The property is used to select the language. Enter: <ul style="list-style-type: none"> ■ <code>LANG=de_DE</code> to select German <p>If you do not set this property the default language (<code>en_US-English</code>) will be used.</p>
<i>WMIQUERY</i> (Advanced users only!)	Enable/Disable WMI queries made by the installer. Under certain rollout scenarios in which no remote administrator permissions have been granted, you can disable WMI querying made by the installer. <ul style="list-style-type: none"> ■ Enter <code>WMIQUERY=1</code> to enable querying (default, even if not entered). ■ Enter <code>WMIQUERY=0</code> to disable querying. NOTE: Turning-off WMI querying will only work with certain hardware!
<i>DMIINIPATH</i>	The path to the <code>dmi.ini</code> file used to specify computers targeted for hardware compatibility mode. This is only necessary if the <code>.ini</code> file is not in the same directory as the MSI package. For information about hardware compatibility modes refer to EgoSecure FDE - Administration and Usage Guide .
<i>SYS420A=1</i>	Alternative boot loader to specific (or problem) configurations.



INFO

The only way to completely install EgoSecure Full Disk Encryption without the need for user interaction for dialogs is to use policies for the FDE and PBA components. Refer to [EgoSecure FDE - Administration and Usage Guide](#). See below for examples of the command line syntax for such installations.

Example syntax for installation:

- For Standard hard disks

- Install FDE only, initialize FDE, do not display GUI, and log the whole procedure to a log file on the local hard disk:

```
msiexec /i "<full MSI file path, name, and extension>" /qn  
ADDLOCAL=FeatureFde INITFDEQ=1 FDEPOLICY="c:\fdeinit.nbs" /l*  
"<full log file path, name, and extension>"
```

- To install FDE and PBA, initialize FDE and PBA according to policies, do not display a GUI, and log the whole procedure to a log file on the local hard disk, you must deploy two policies:

```
msiexec /i "<full MSI file path, name, and extension>" /qn /l*  
"<full log file path, name, and extension>"  
ADDLOCAL=FeatureFde,FeaturePba INITFDEQ=1  
FDEPOLICY="c:\fdeinit.nbs" INITPBAQ=1  
PBAPOLICY="c:\pbainit.pba" /forcerestart
```

NOTE: A third [configuration] policy must be deployed to perform encryption.

- To install all features of Full Disk Encryption and initialize both FDE and PBA

```
msiexec.exe /i "<full MSI path, name, and extension>" /qn /l*  
"<full og file path, name, and extension>" ADDLOCAL=All  
INITFDEQ=1 INITPBAQ=1 ADMINPWD=12345678
```

- To uninstall and update FDE and PBA use the following command line options:

```
fdeinit [-uninstall|-update] -silent <admin password>  
fdeinit @<fdeinit policy>|<fdedeinit policy>  
fdeinit @<upgradepolicy>  
Pbainit [-uninstall|-update] -silent <admin password>  
Pbainit @<PBA init policy>|<PBA deinit policy>  
Pbainit @<upgradepolicy>
```

update: performs an update of the PBA/FDE.

uninstall: EgoSecure Full Disk Encryption PBA/FDE will be deinitialized with this version.

If the above two options are omitted then the mode will be automatically selected based on the current state of initialization as given below.

- For PBAInit, if PBA is already initialized deinitialization will be performed, else initialization will be performed.
- For FDEInit, if FDE is already initialized update will be performed, else initialization will be performed.

Note:

Full Disk Encryption must be installed before running *fdeinit* and *pbainit* command.

To run *fdeinit*, a current directory must be changed to C:\Windows\NAC

To run *pbainit*, a current directory must be changed to C:\Windows\NAC\SBS

**INFO**

If you have a custom dmi.ini file you wish to deploy with the EgoSecure Full Disk Encryption MSI package, then make sure that it resides in the same installation directory as the MSI package. This will ensure that the file is recognized and EgoSecure Full Disk Encryption will use the correct boot parameters for those computer models defined in the dmi.ini file.

Collecting FDE installer logs

1. Run cmd as an administrator.

2. Execute the following command:

```
msiexec.exe /i "e:\files\EgoSecure Full Disk Encryption by Matrix42 [version].msi" /l*vx "c:\fde-install-log.txt"
```

3. Collect the logs in the specified path.

2.5. Upgrade**Manual upgrade**

The following steps detail the manual installation of the software-based FDE components:

1. **Customizing:** If you have created a new DMI file for unusual computer configurations then place the dmi.ini file in the same directory as the EgoSecure Full Disk Encryption [version].msi package so that computers set for 'Hardware Compatibility Mode' will automatically be installed accordingly. For details about Hardware Compatibility Mode, see [EgoSecure FDE - Administration and Usage Guide](#).

2. Double-click the file EgoSecure FDE by Matrix42 Setup.exe.

**INFO**

The GUI language will be automatically selected by the installer to fit that of the operating system. If you have an operating system other than English, German, or Hungarian, the default language – English – will be installed..

**ATTENTION**

Be aware that you will need to reboot the computer after the upgrade is complete.

→ The **Welcome** dialog appears.

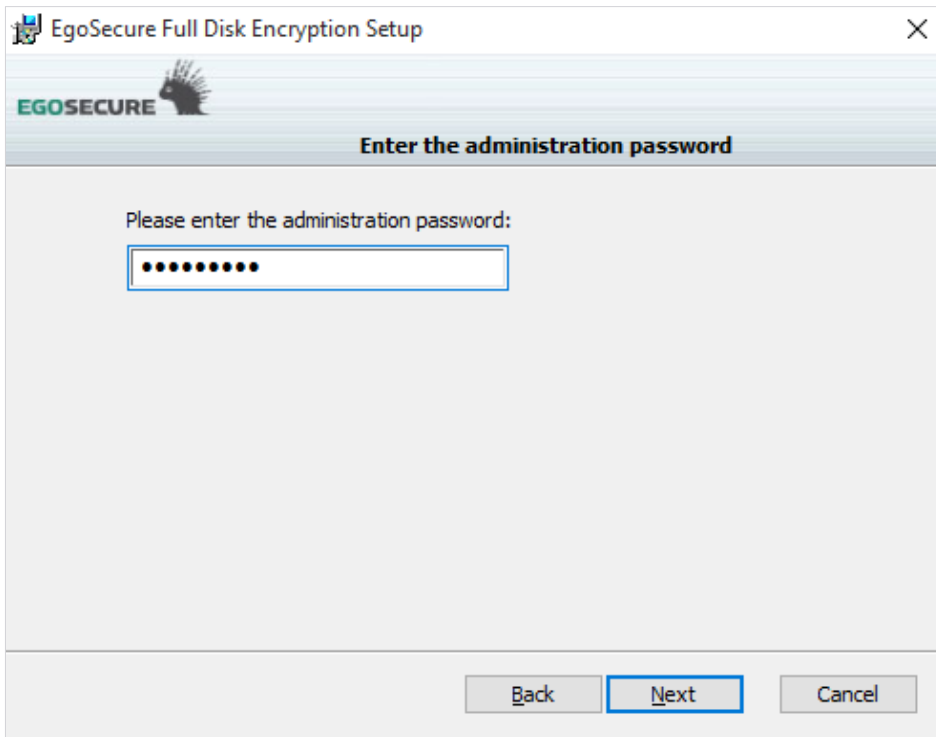
3. Click **Next**.



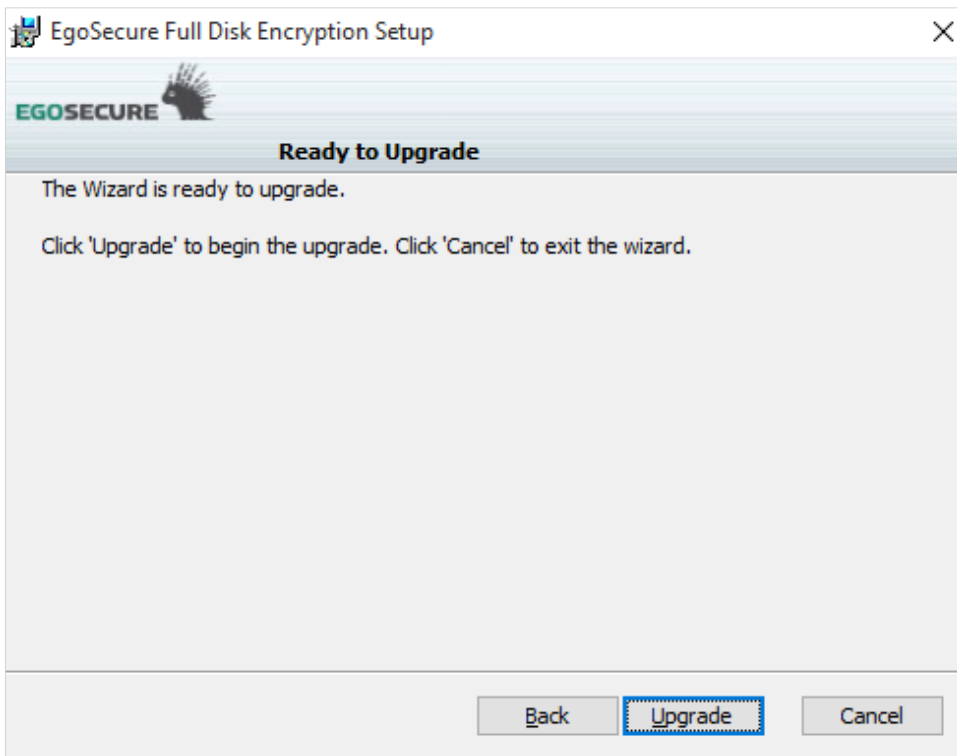
→ The Administration password dialog appears.

4. Enter the password and click **Next**.

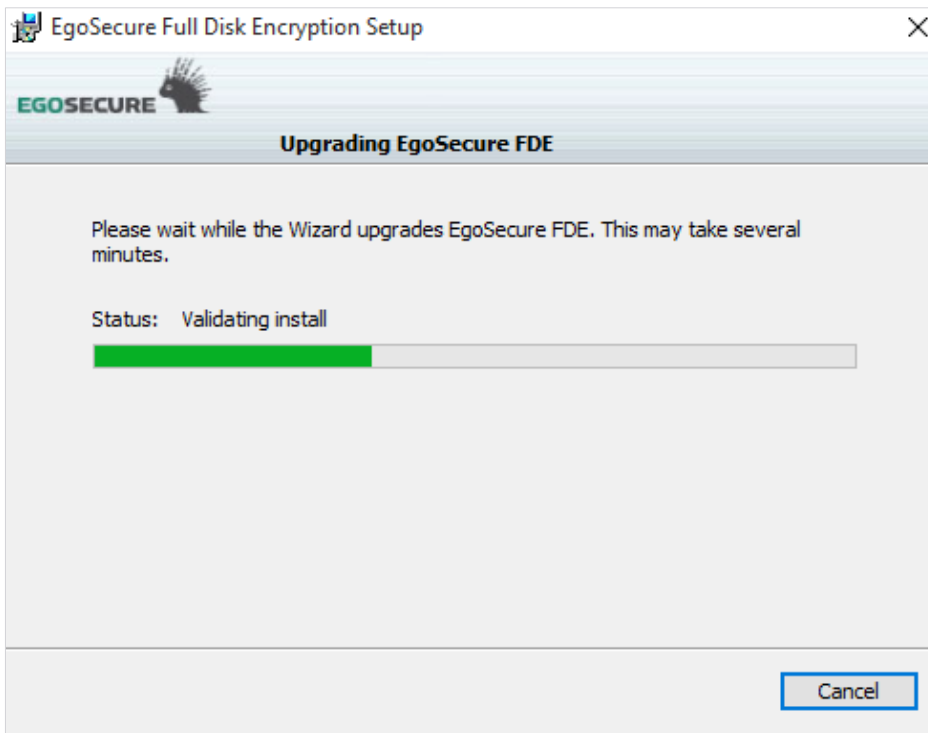
Figure 32. FDE upgrade - administration password



5. The **Ready to Upgrade** dialog appears. Click **Upgrade**.



6. The **Upgrading EgoSecure FDE** status dialog appears. Let the installer upgrade the components (this may take a few minutes).



7. Once FDE is upgraded the following dialog appears:



8. The upgrade is now almost complete. The last dialog indicates the final step. Click **Yes** to restart.



ATTENTION

- ◆ A reboot is necessary after the initialization of the PBA component to capture user credentials and apply the new settings.
- ◆ Please uninstall FDE immediately if PBA initialization fails for any reason. In other words, do not shutdown the system unless an ERI file was successfully generated. Given the logic in the current product it is possible that the FDE.x drive is locked in such a case.

Unattended upgrade

An upgrade has been defined to fit the new software architecture and to aid the further development of this product. The following now applies:

- [Unattended upgrade](#) details steps to upgrade from one major version to another and also within a major version.
- [Command line parameters for upgrade](#) details the command line parameters for the above.

Unattended upgrade

This section details steps to upgrade from one major version to another. The same procedure is applicable for upgrading it within a major version.

1. Open a command prompt and navigate to the directory in which the EgoSecure FDE setup files are located. There are two similar methods to upgrade that differ only in that you can choose to enter the administration password into the command line in plain text or in encrypted form. Follow the method that is best for you:

- **Using plaintext password:** Open a command prompt and enter the following syntax into the command line:

```
msiexec.exe /i "<full MSI file path, name, and extension>"
ADMINPWD=<EgoSecure FDE administration password> /l* "<logfile
location\logfile name.txt>" /passive /forcerestart
```

For example:

```
msiexec.exe /i "C:\FDE files\EgoSecure Full Disk Encryption by
Matrix42 [version].msi" ADMINPWD=12345678 /l* "C:\log
files\FDE update.log" /passive /forcerestart
```

- **Using encrypted upgrade policy:**

To upgrade EgoSecure Full Disk Encryption using an encrypted administration password, you must first create an upgrade policy via either the Upgrade Policy Builder (or the helper application `GUS.exe` (*EgoSecure FDE - Administration and Usage Guide*)). Press **Return** when you are done.

2. Save the policy to a common location accessible by the installer.

3. Navigate to the directory where the EgoSecure Full Disk Encryption package is located.
4. Start the update upgrade procedure by entering the following in the command line:

```
msiexec.exe /i "<full MSI path, name, and extension>"  
UPGDPOLICY="<full policy path, name, and extension>" /l*  
<logfile location\logfile name.txt> /passive /forcerestart
```

For example:

```
msiexec.exe /i "C:\FDE versions\EgoSecure Full Disk Encryption  
by Matrix42 [version].msi" UPGDPOLICY="C:\update.upd" /l*  
"C:\FDE.log" /passive /forcerestart
```



ATTENTION

- ◆ Make sure that you enter the correct package in the command line for the operating system you intended to deploy to –32 or 64-bit? The 32-bit version of EgoSecure FDE CANNOT be installed on 64-bit versions of Windows, and vice versa.
- ◆ It is recommended to restart the computer once an upgrade is complete. This will allow the new encryption driver to be loaded into Windows (this cannot be done until a restart has taken place). Because a restart is not mandatory, make use of the options /forcerestart or /promptrestart to force a restart.

Command line parameters for upgrade

The following Microsoft installer removal options are available for upgrading EgoSecure Full Disk Encryption:

Command line option/property	Details
/qf, /qn, /i, /l	<i>Microsoft</i> installer parameters. <ul style="list-style-type: none">■ /i<package>: a specific package.■ /qn: quiet mode –no user interface(the same as /q).■ /qf: quiet mode with full user interface.■ /l* <log.txt>: Log file of the upgrade.
EgoSecure Full Disk Encryption by Matrix42 [version].msi, EgoSecure Full Disk Encryption by Matrix42 [version] x64.msi	The file name of the EgoSecure Full Disk Encryption installer package according to system (32-bit/64-bit).

The following *EgoSecure* installation options are available:

Command line option/property	Details
ADMINPWD	This option allows you to provide the administration password for the current installation. For example: ADMINPWD=12345678 If you do not use this option, the administration password must be entered when prompted by the installer.
UPGDPOLICY	This option allows you to enter the path and policy name to an upgrade policy (created using either the Upgrade Policy Builder or the helper application GUS.exe (EgoSecure FDE Administration and Usage Guide)). The syntax is: UPGDPOLICY=<full policy path, name, and extension> For example: UPGDPOLICY="C:\update.upd"
WMIQUERY (Advanced users only)	Enable/Disable WMI queries made by the installer. Under certain rollout scenarios in which no remote administrator permissions have been granted, you can disable WMI querying made by the installer. <ul style="list-style-type: none"> ■ Enter WMIQUERY=1 to enable querying (default, even if not entered). ■ Enter WMIQUERY=0 to disable querying. NOTE: Turning off WMI querying will only work with certain hardware!
forcerestart, promptrestart	Use either of these commands to force a restart after the upgrade procedure is complete (recommended).



INFO

The 'Rollback' takes place only when anything fails during the upgrade procedure, then the installer will roll back the installation files so that the system is unaffected and remains with previous version. The installer also gives out an appropriate message.

2.6. Removal

This section details how to remove *EgoSecure Full Disk Encryption* using manual and unattended methods.

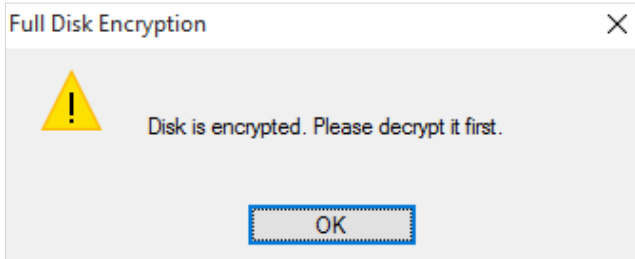
Manual removal

1. Open the Windows Control Panel (according to the Windows version):
2. Scroll to, and select the entry *EgoSecure Full Disk Encryption* [version] (or *Full Disk Encryption*), and click **Uninstall**.

3. The installer will prompt you to confirm the removal. Click **Yes**. Information about the installation type will then be gathered by the removal application - this may take a while so please be patient. *Windows Vista/7/8*: Accept any User Access Control prompts that may appear.

→ The following dialog may appear:

Figure 33. Decrypt Hard Disk Before Removal Dialog

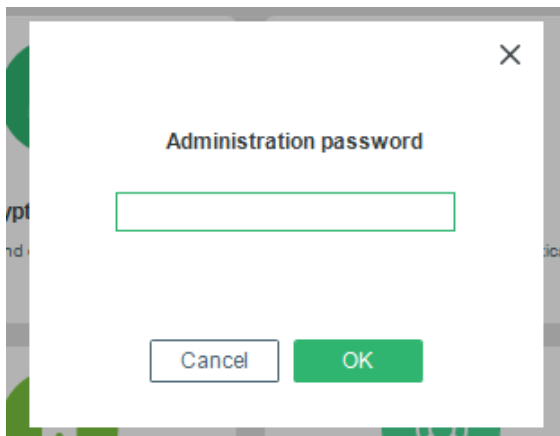


This indicates that the hard disk partitions are still encrypted. Click **OK** to close the dialog. For details about hard disk decryption, see [EgoSecure FDE - Administration and Usage Guide](#). Once the decryption is finished continue with the steps below.

1. One of the following removal scenarios is possible:
 - If your *Full Disk Encryption* installation has not yet been initialized, or PBA/FDE has been deactivated, the removal application will simply remove *EgoSecure Full Disk Encryption* and request to restart your computer once it is finished. The removal procedure ends here.
 - If your *Full Disk Encryption* installation is still active, continue with the next step.
2. If FDE and PBA are still initialized, they must first be deinitialized to successfully remove the application data.
3. Click **PBA initialization** in the FDE Control Center.

→ The **Administration password** dialog appears:

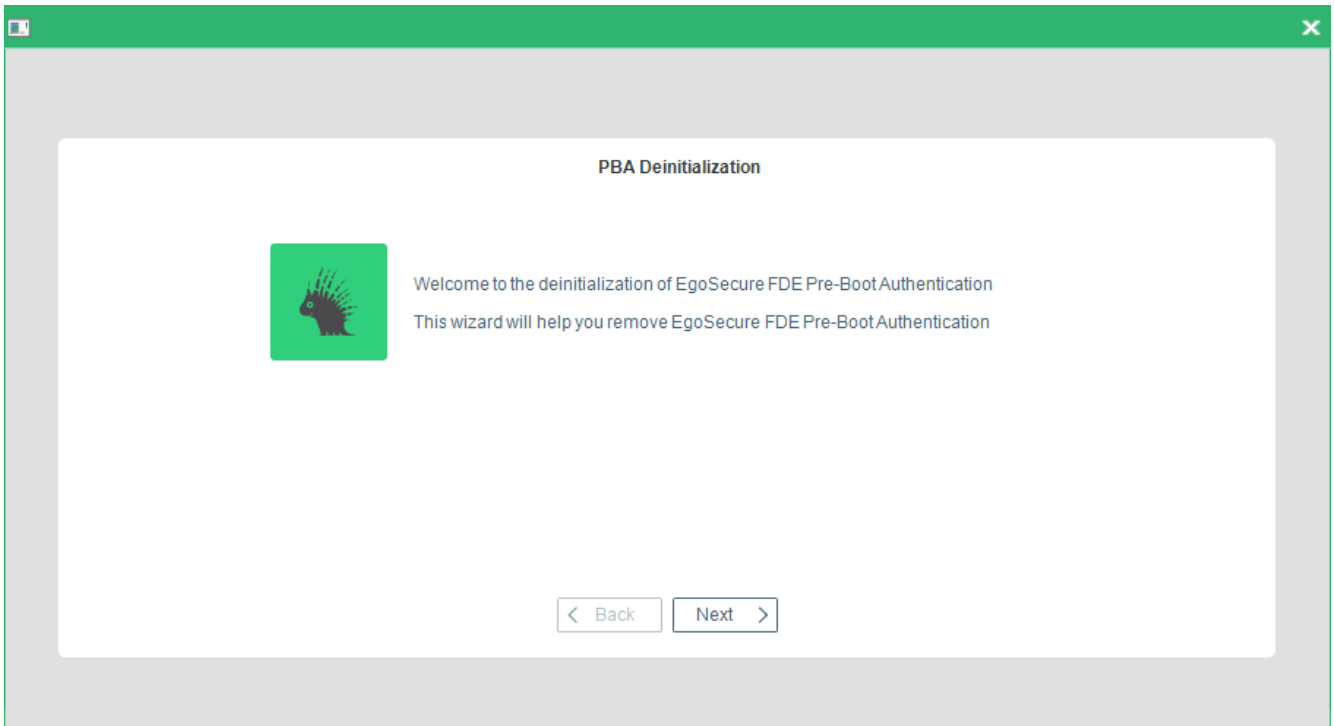
Figure 34. Enter Administration Password Dialog



- To remove both the PBA and FDE components, continue with the next step.
 - To remove only the FDE component, proceed with the step [8](#).
- The EgoSecure Full Disk Encryption PBA Setup dialog appears.

4. Click **Next** to continue.

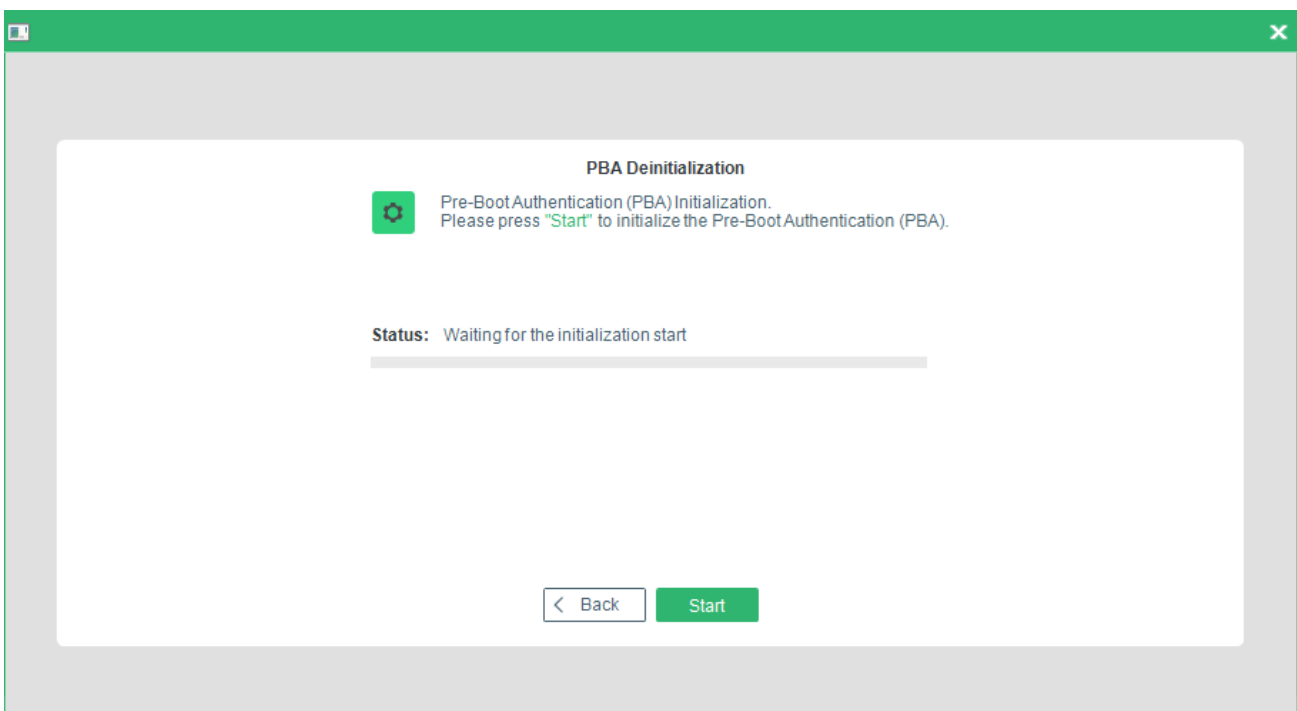
Figure 35. De-initialize PBA – Welcome Dialog



→ The **De-initialization Status** dialog appears.

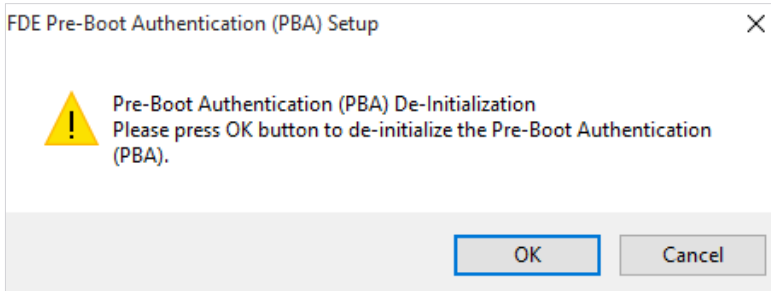
5. Click **Start**.

Figure 36. De-initialize PBA – Status Dialog



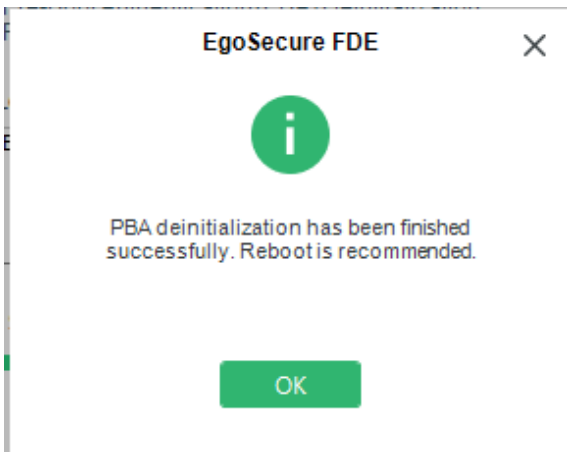
→ A confirmation dialog appears:

Figure 37. De-initialize PBA – Confirmation Dialog



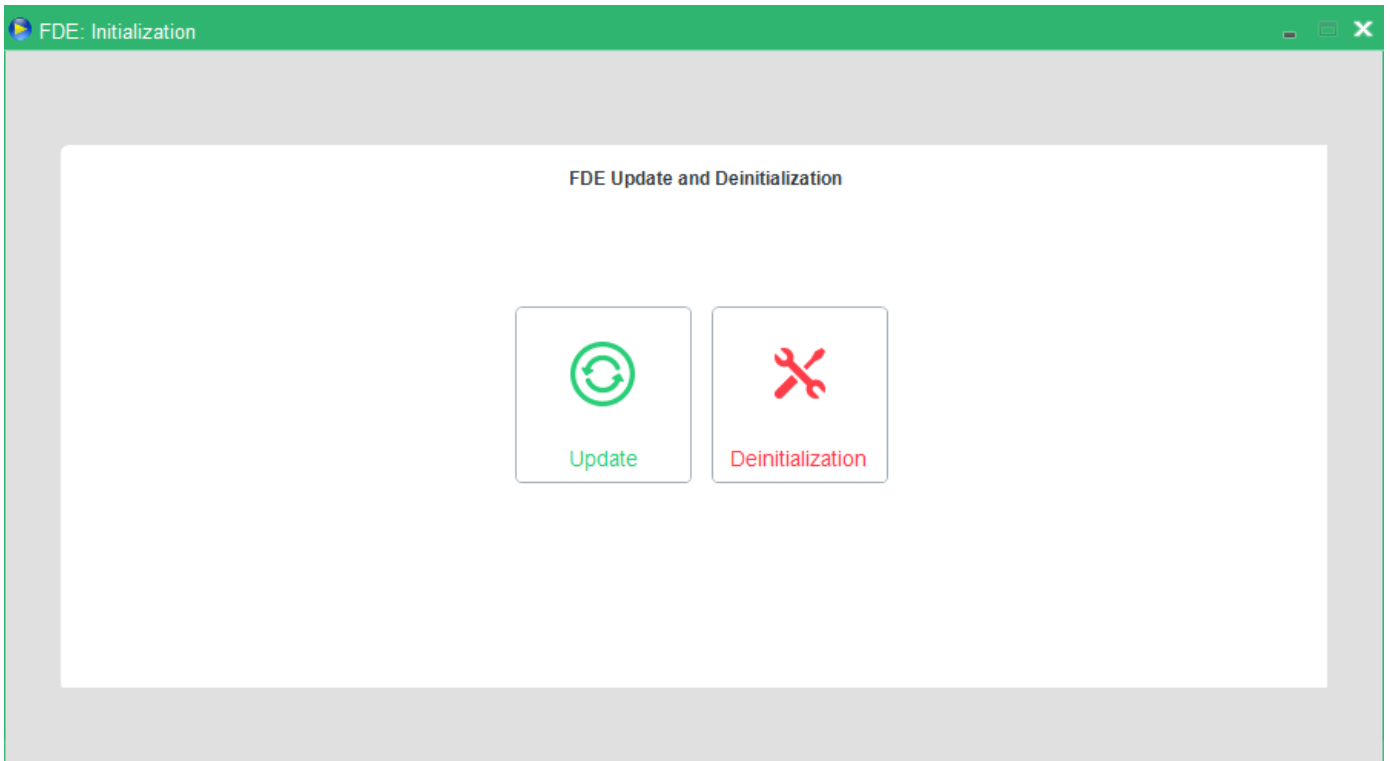
6. Click **OK** to continue. The de-initialization may take a while so please be patient.
→ If the de-initialization is successful, the following dialog appears:

Figure 38. De-initialize PBA – Success Dialog

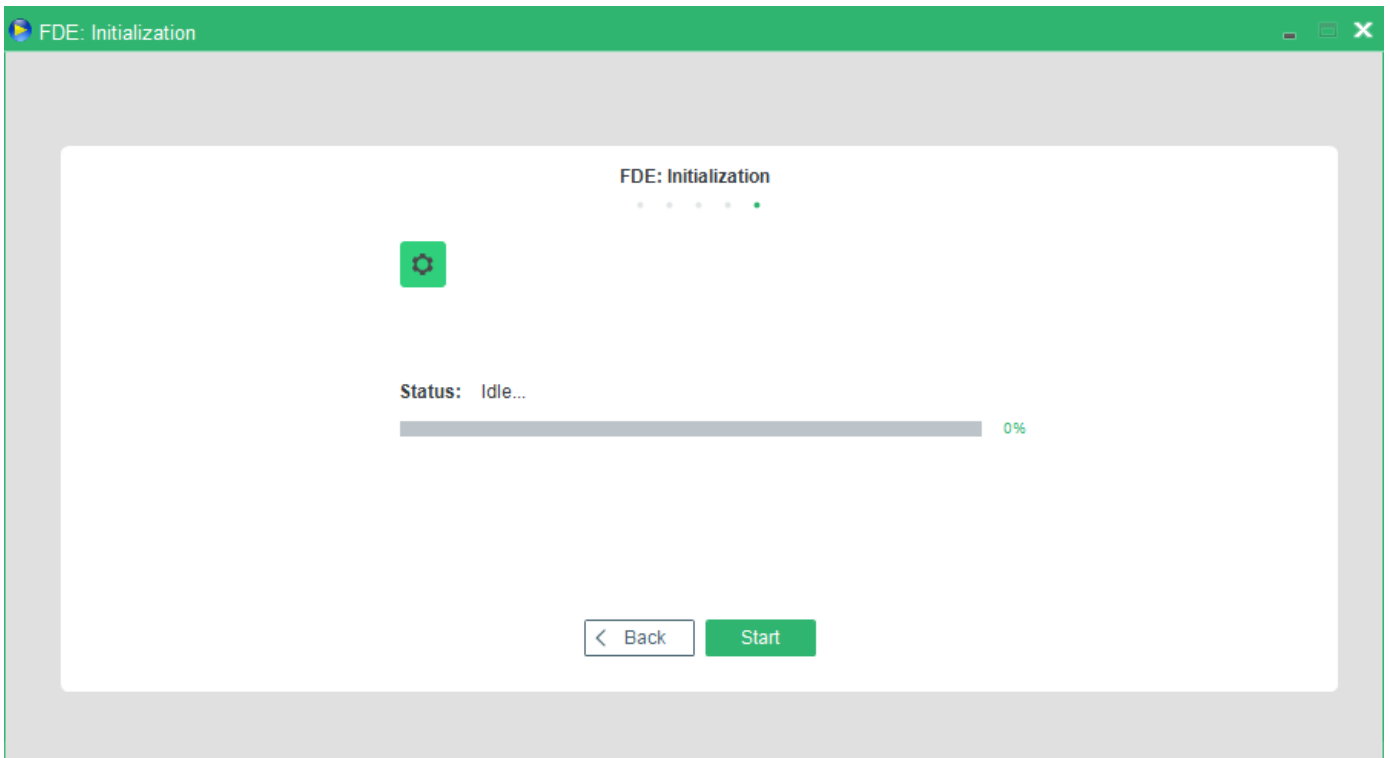


7. Click **OK** to close the dialog.
→ The setup application will finish removing files.
8. Click **FDE initialization** in the FDE Control Center.
→ The Administration password dialog appears.
9. Enter the password and click **OK**.
→ The **FDE Update and Deinitialization** dialog appears. Click **Deinitialization**.

Figure 39. FDE Deinitialization Dialog

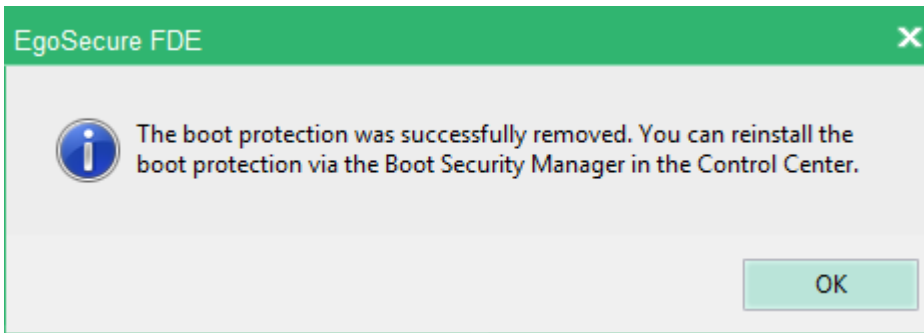


→ The **FDE Deinitialization Status** dialog appears.




10. Click **Start**.

→ Once finished, a success dialog appears. Click **OK** to close the dialog.



It is recommended, but not essential, to restart the computer to complete the removal. *EgoSecure Full Disk Encryption* cannot be reinstalled if the computer is in a freshly-removed state.

 After removing EgoSecure Full Disk Encryption it is highly recommended to re-enable the Windows secure logon mechanism..

INFO

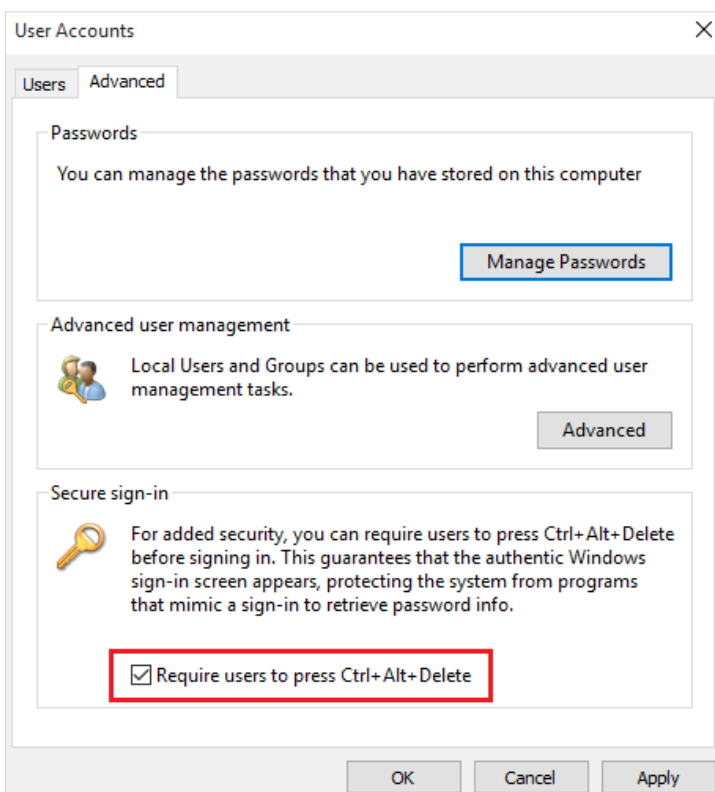
Re-enabling secure logon functionality

1. For Windows 7: `control userpasswords2`

For Windows 10: run `netplwiz` command

→ The **User Accounts** dialog appears:

Figure 40. Enabling Secure Logon (sign-in)



2. In the Advanced tab, check Require users to press Ctrl+Alt+Delete and click OK. Cancelling the removal of the FDE can leave the EgoSecure Full Disk Encryption product in an undefined state. It is recommended to reinstall, or remove the EgoSecure Full Disk Encryption.

Manual removal (Quick)

EgoSecure Full Disk Encryption also offers a quick method of removal via the installer file.

	Use this method of removal only if your hard disk already decrypted.
WARNING	

Follow these steps to quickly remove *EgoSecure Full Disk Encryption*:

1. Double-click the EgoSecure FDE by Matrix42 Setup.exe.
→ The **Welcome** dialog appears.
2. Click **Next**.

Figure 41. Removal - Welcome Page



- The **Modify, Repair, or Remove** dialog appears.
3. Click the **Remove** icon.

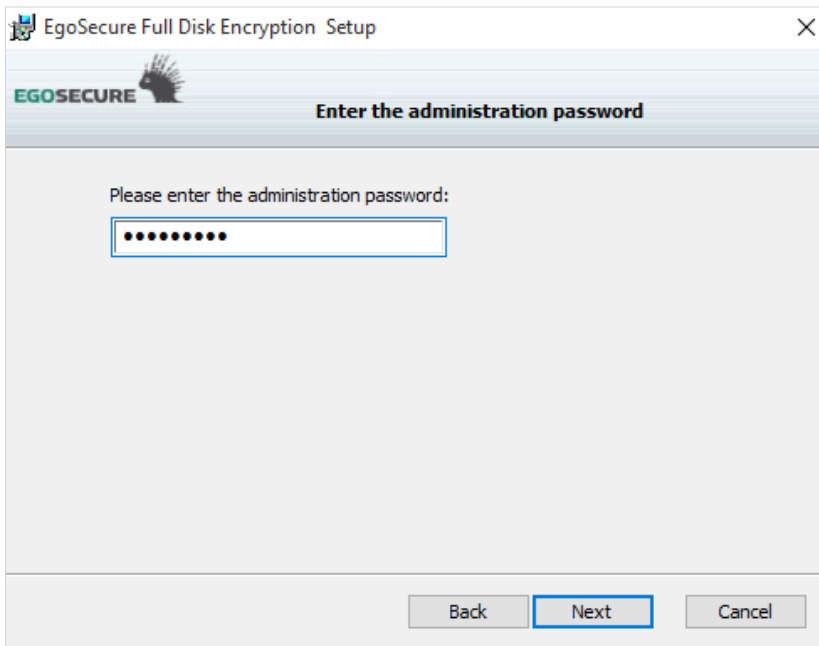
Figure 42. Removal – Modify, Repair, or Remove Options Dialog



→ The installer will now prompt for the *EgoSecure Full Disk Encryption* administration password to authenticate the removal of the components.

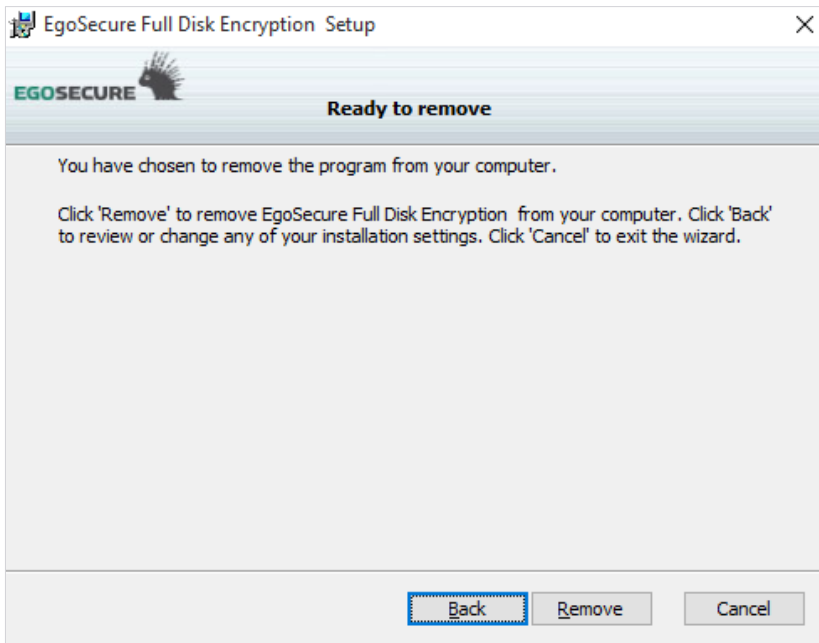
4. Enter the password, and click **Next**.

Figure 43. Removal - Administration Password Dialog



→ An information dialog appears to inform you for the last time of the action you are about to perform.

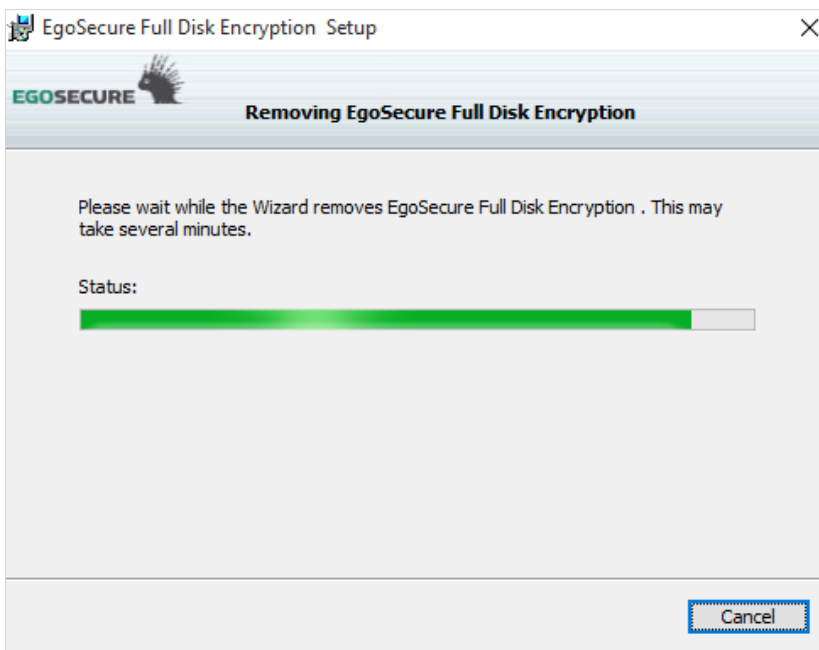
Figure 44. Removal – Confirmation Dialog



5. Click **Remove**.

→ The status of the removal will be displayed.

Figure 45. Removal - Status



WARNING

Avoiding data loss during removal

To avoid data loss, do not turn-off the computer during the removal process.

→ A success dialog appears once the components have been cleanly removed.

6. Click **Finish**.

Figure 46. Removal – Uninstallation Success Message



If you have used custom dmi.ini during installation, repairing an existing installation after manually removing dmiconfig from the \sbs directory will also remove the dmi.ini config from the PBA and correspondingly the system may not boot anymore. So manually copy the dmi.ini in to c:\windows\nac\sbs before repairing an existing installation.

Unattended removal

This section details the Microsoft installer syntax necessary to perform an unattended removal of EgoSecure Full Disk Encryption.

Before starting this procedure, make sure that:

- the EgoSecure Full Disk Encryption Control Center is closed and that no Control Center module is currently active;
- PBA and FDE are deinitialized.

Follow these steps to perform an unattended removal:

1. Open a command prompt.
2. Navigate to the directory in which the *EgoSecure FDE* msi package is located.
3. To start the removal use the following syntax with options:

```
msiexec /x "<full MSI file path, name, and extension>" /qn /l*  
"<full log file path, name, and extension>"  
[<PROPERTY>=<value>]
```

For example, enter the following:

```
msiexec /x "C:\FDE versions\EgoSecure Full Disk Encryption by Matrix42 [version].msi" /qn /l* "C:\log files\log.txt" ADMINPWD=12345678 -forcerestart
```

or

```
msiexec /x "C:\FDE versions\EgoSecure Full Disk Encryption by Matrix42 15.1.943.0 x64.msi" /qn /l* "C:\log files\log.txt" REMOVEPOLICY="C:\FSEremove.upd"
```

The following *Microsoft* installer removal options are available:

Command line option/property	Details
/q, /qn, /x, /l	<p><i>Microsoft</i> installer parameters.</p> <ul style="list-style-type: none"> ■ /x <package>: remove a specific package. ■ /qn: quiet mode –no user interface (the same as /q). ■ /qf: quiet mode with full user interface. ■ /l* log.txt: Log file of the unattended removal
EgoSecure Full Disk Encryption 12.1.883.0.msi EgoSecure Full Disk Encryption 12.1.883.0 x64.msi	The name of the installer package.

The following *EgoSecure FDE* removal options are available:

Command line option/property	Details
ADMINPWD	<p>This option allows you to provide the administration password for FDE de-initialization. For example: ADMINPWD=12345678 If you do not use this option, a de-initialization will be attempted without the administration password.</p>
REMOVEPOLICY	<p>Define the full path, filename, and extension of the upgrade policy (encrypted administration password). Upgrade policies can also be used for this purpose (dual use for the upgrade policy file). For further information about how to create an upgrade policy, GUI version, and command line helper application refer to EgoSecure FDE - Administration and Usage Guide.</p>
forcerestart	<p>Use this command to force a restart after the removal procedure is complete (recommended).</p>



INFO

Restart recommended

It is recommended to restart the computer (with Vista/Win7) after a successful uninstall by FDE policy. Restart will allow the removal of driver from the computer memory.

3. WINDOWS UPGRADE



WARNING

Data loss risk

Before upgrading your operating system (e.g.: from Windows 8 to Windows 10), follow the steps below. Otherwise, you may lose all your data.

Please, differentiate between an operating system upgrade and an update. When performing an operating system **update** (e.g.: Windows 10 from build 1703 to 1709), all the steps described below are not needed.

1. Decrypt the encrypted drive (refer to the [EgoSecure FDE - Administration and usage guide](#), chapter "Decrypting a hard disk partition").
2. Remove the EgoSecure Full Disk Encryption (to get further information, see chapter [2.6](#)).
3. Upgrade your operating system.
4. Install the EgoSecure Full Disk Encryption (to get further information, see chapter [2.4](#)).
5. Encrypt the necessary drive (refer to the [EgoSecure FDE - Administration and usage guide](#), chapter "Encrypting a hard disk partition").

4. TROUBLESHOOTING

- | | |
|---|---|
| 4.1. The limit of 4 primary partitions is reached | 4.7. How to prevent specific users from being "captured" during self initialization |
| 4.2. If the BSOD happens on a first reboot after the installation | 4.8. User capturing fails |
| 4.3. If the system fails to boot Windows after disk encryption | 4.9. Partition creation fails after FDE has been initialized |
| 4.4. Problems with image creation | 4.10. Incorrect GUI language/Change GUI language |
| 4.5. Problems when copying an image back to the hard disk | 4.11. Administrator password forgotten |
| 4.6. Characters cannot be entered into the HelpDesk dialogs | 4.12. How to change PBA boot method |
| | 4.13. PBA fails to start in RAID mode |
| | 4.14. FDE initialization fails – very fragmented disk |

This chapter will help you overcome the most common problems with *EgoSecure Full Disk Encryption*.

**INFO****Check that version is up-to-date**

As a first step in troubleshooting, make sure that your Full Disk Encryption version is up to date.

EgoSecure has some requirements and unsupported software or hardware configurations. The following configurations are not supported:

- Dynamic disks
- Computers encrypted with other 3rd party encryption solutions
- Microsoft Device encryption
- Non-NTFS drives like: FAT, exFAT
- BIOS MBR with 4 primary partitions
- RAID configurations (not supported on BIOS systems; on UEFI systems it is supported, but PBA works only in the Simple PBA mode)

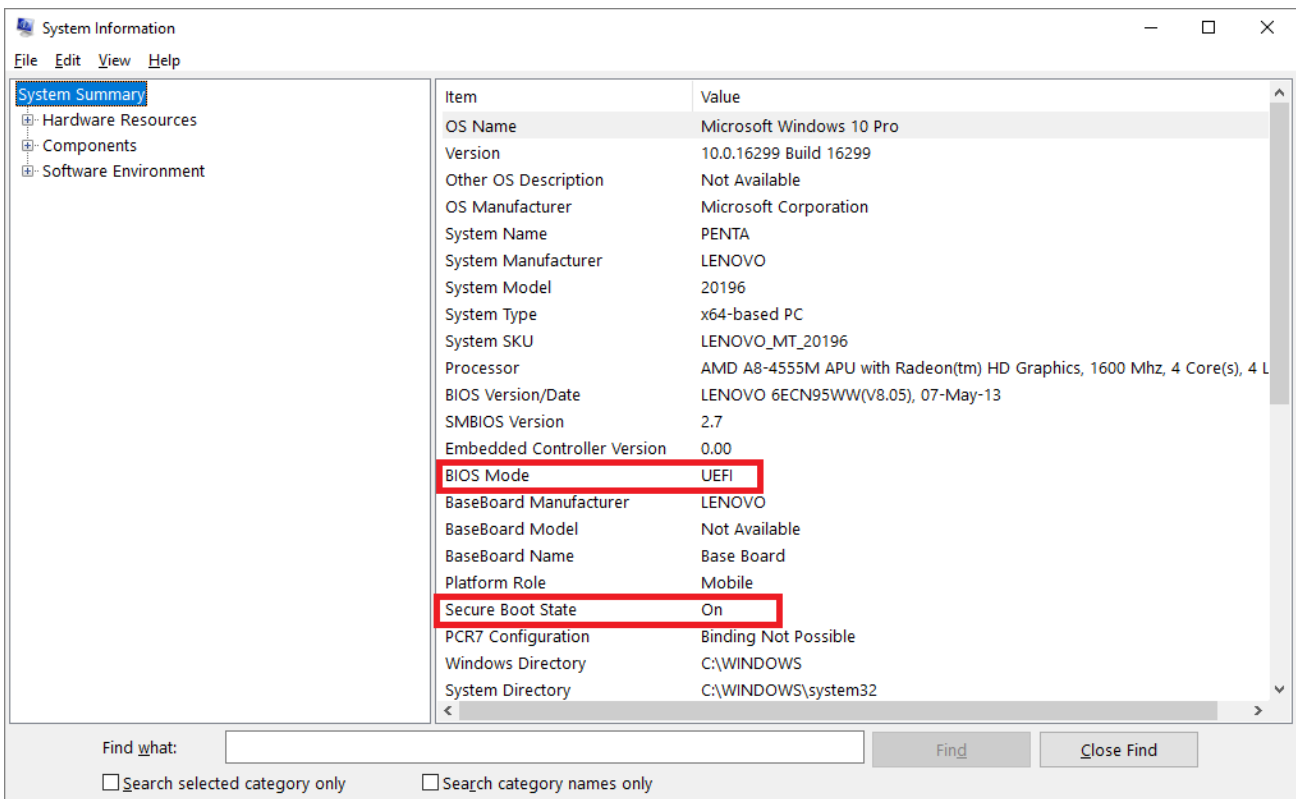
In most cases EgoSecure FDE installation package can detect incompatible configurations during the installation or initialization and return the error messages explaining why the installation was not possible. Sometimes additional tools are required to understand why the installation or initialization fails.

New installation cannot be performed if the previous version of EgoSecure was uninstalled and reboot is pending.

Additional tools to get configuration details

System Information

To start, press Windows + R and start msinfo32.exe. The tool can show the current status of Secure Boot, BIOS type.



Disk Management

To start, right-click the **Windows** icon and select **Disk Management**.

- Only Basic disks are supported in EgoSecure FDE. Dynamic Disks are not supported. You can check the disk type in the Disk Management tool.
- Disk Management can show the file system, only NTFS is supported.
- It also shows the status of BitLocker in the File System Column for the drives if BitLocker is Enabled.
- BIOS MBR with 4 primary partitions can also be seen in this tool.
- The presence of EFI partition usually is a sign of UEFI system.

Disk Management

File Action View Help

Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(D:)	Simple	Basic	Unknown (B...	Healthy (Primary Partition)	25.00 GB	25.00 GB	100 %
(Disk 0 partition 1)	Simple	Basic		Healthy (Recovery Partition)	1000 MB	1000 MB	100 %
(Disk 0 partition 2)	Simple	Basic		Healthy (EFI System Partition)	260 MB	260 MB	100 %
(Disk 0 partition 3)	Simple	Basic		Healthy (OEM Partition)	1000 MB	1000 MB	100 %
(Disk 0 partition 6)	Simple	Basic		Healthy (Recovery Partition)	450 MB	450 MB	100 %
(Disk 0 partition 8)	Simple	Basic		Healthy (Recovery Partition)	20.00 GB	20.00 GB	100 %
(Disk 0 partition 9)	Simple	Basic		Healthy (Primary Partition)	502 MB	502 MB	100 %
amd (C:)	Simple	Basic	NTFS (BitLo...	Healthy (Boot, Page File, Crash Du...	417.49 GB	139.89 GB	34 %
WinPE-907-1 (E:)	Simple	Basic	NTFS	Healthy (Active, Primary Partition)	3.76 GB	3.47 GB	92 %

Disk 0 Basic 465.64 GB Online	1000 MB Healthy (Rec	260 MB Healthy (f	1000 MB Healthy (OEM	amd (C:) 417.49 GB NTFS (BitLocker Healthy (Boot, Page File, C	502 MB Healthy (Pr	450 MB Healthy (R	(D:) 25.00 GB Unknown (20.00 GB Healthy (Recovery P
	Disk 1 Removable 3.76 GB Online WinPE-907-1 (E:) 3.76 GB NTFS Healthy (Active, Primary Partition)							

■ Unallocated ■ Primary partition

4.1. The limit of 4 primary partitions is reached

Problem. BIOS MBR scheme has a limit of 4 primary partitions. EgoSecure PBA requires additional primary partition, which is created after the EgoSecure installation and during the FDE initialization. If there are 4 primary partitions in the system, the EgoSecure PBA partition cannot be created.

Solution. In most cases it is possible to delete one of the primary partitions to let EgoSecure FDE create required partition. For example, some HP laptops with MBR have 4 partitions used. One of the partitions is HP Tools. You can copy HP tools content to some local folder or removable media and erase the partition.

New systems with UEFI and GPT don't have a limitation of 4 primary partitions.

4.2. If the BSOD happens on a first reboot after the installation

Problem. The EgoSecure FDE was installed, but the blue screen happened during the next reboot.

Solution. Disable filter drivers via Windows PE recovery tool.

1. Boot the system using Windows PE removable media (you can use EgoSecure Recovery USB or CD which is also based on Windows PE).
2. call: REG LOAD HKLM\fdesys c:\windows\system32\config\system
3. call: regedit.exe
4. delete "nbfdec" filter name only from
HKEY_LOCAL_MACHINE\fdesys\ControlSet001\Control\Class\{71A27CDD-812A-11D0-BEC7-08002BE2092F}\LowerFilters
Leave other filters!
5. delete "nbfdec" filter name only from
HKEY_LOCAL_MACHINE\fdesys\ControlSet001\Control\Class\{4D36E967-E325-11CE-BFC1-08002BE10318}\UpperFilters
Leave other filters!
6. close regedit
7. call: REG UNLOAD HKLM\fdesys
8. Restart Windows.

4.3. If the system fails to boot Windows after disk encryption

If the systems fail to boot from the encrypted drive, there is an option to decrypt drive using EgoSecure Recovery Media. It might be a bootable USB stick or CD/DVD. For details, see [the EgoSecure FDE - Administration and Usage Guide](#), chapter 1.12.

Always save ERI (Emergency Recovery Information) files and keep them in a safe place. This allows to decrypt encrypted drives. Once it is done, you can continue troubleshooting using other methods described in this document.



ATTENTION

If there is no ERI file, ERI cache is not available, Helpdesk is not available or you do not remember the encryption key length and algorithm you cannot recover your data. Your data is lost.

- ◆ In case of an encrypted drive the data can be recovered only if the ERI file has been saved to an external and secure location (to removable media). Remove the NTFS compression to gain access to encrypted files.

4.4. Problems with image creation

Problem. An image of the complete hard disk has been made (to include the *Windows* and PBA partitions) using an imaging application such as *Norton Ghost* or *Acronis TrueImage*. When the image is transferred back to the same computer or to another computer of the same model, the computer does not boot.

Cause. Imaging applications use varying methods of data backup, compression, and optimization – using such methods may change the internal data structure of the encrypted partition and/or PBA partition.

Solution. There are two methods of imaging that are dependent on whether you want to encrypt the complete hard disk or just the system partition:

- If you want to make an image of the Windows partition AND our Linux (PBA) partition, you have to create an image using a sector-for-sector, uncompressed method.
- If you want to make an image of only the system partition and leave the Linux (PBA) partition as it is, then you have to create an image using a sector-for-sector method, but you have the option to use compression to make the image smaller. For more details, refer to [EgoSecure FDE - Administration and Usage Guide](#).

4.5. Problems when copying an image back to the hard disk

Problem. The hard disk image (that you wish to re-apply) was created at a time when *EgoSecure Full Disk Encryption* was not installed on the computer (i.e. *EgoSecure Full Disk Encryptions* not in the image file). At the time you want to copy the image back to the target computer, *EgoSecure Full Disk Encryptions* installed and the PBA is initialized.

After the image has been applied the computer will not boot from the PBA into *Windows*.

Cause. The PBA can no longer locate the necessary boot files.

Try one of the following:

- Use either the *EgoSecure* ERD to remove the PBA and reinstall *EgoSecure Full Disk Encryption* once you can boot to *Windows*, or...
- Perform a secure erase on the complete hard disk and re-copy the image back to the drive.

Applies to standard hard disks only (FDE with PBA).

Problem. The data contained in the hard disk image was encrypted by *EgoSecure* at the time the image was created (i.e. the image contains encrypted data). *EgoSecure Full Disk Encryptions* installed and the PBA is initialized on the target computer. The intention is to simply copy the data back to the hard disk and use the existing PBA.

After the image has been applied the computer will not boot from the PBA into *Windows*.

Cause.

- The PBA can no longer locate the necessary boot files.
- The *EgoSecure Full Disk Encryption* versions (between the image file and the current PBA) are incompatible.

Solution. Try one of the following:

- Use either the *EgoSecure* ERD (plus a valid ERI file) to remove the PBA and, if necessary, decrypt the drive, or...
- Perform a deletion/secure erase on the complete hard disk and re-copy the image back to the drive. Afterwards, decrypt the drive using the ERD (plus ERI file that is valid for the data contained in the image).

4.6. Characters cannot be entered into the HelpDesk dialogs

Problem.

- I am having trouble with the characters I pass on to the HelpDesk administrator. The computer keeps beeping.
- I am having trouble with the characters the HelpDesk administrator gives me. The computer keeps beeping.

Cause. Certain letters have been removed from the challenge/response process because they can be confused with another letter or number.

Solution. The following letters cannot be entered into the challenge/response fields in the HelpDesk GUIs:

B, D, O, Y

Every time you press a key for one of these letters the computer will beep to let you know that the entry is incorrect. The correct characters for each of the letters removed are:

Problem Letter	Correct character
B (for B ravo)	8 (eight)
D (for D elta)	0 (zero)
O (for O scar)	0 (zero)
Y (for Y ankee)	V (for V ictor)

4.7. How to prevent specific users from being “captured” during self initialization

Problem. When the computer boots into the PBA component an unknown user entry is visible in the PBA login dialog.

Solution. You can define users to be ‘blacklisted’ to prevent them being ‘captured’ upon PBA self initialization, for example netinstall or ‘__vmware_user__’. This is achieved by editing a EgoSecure registry entry that acts as a blacklist (the entry ‘__vmware_user__’ has already been added to the list).

Follow these steps to add a user to the blacklist:

1. Open the *Windows registry editor* by either selecting **Start>Run** and entering *regedit* into the **Open** field, or double-clicking the *regedit.exe* directly in the directory:

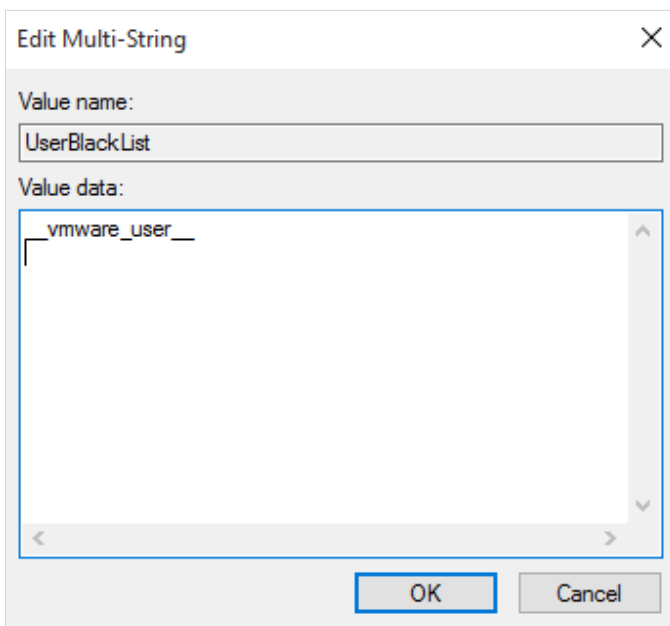
C:\WINDOWS\regedit.exe

2. In the registry editor open the entry:

HKEY_LOCAL_MACHINE\SOFTWARE\cpsd\SBS\scopen\UserBlackList

3. The **Edit Multi String** dialog appears:

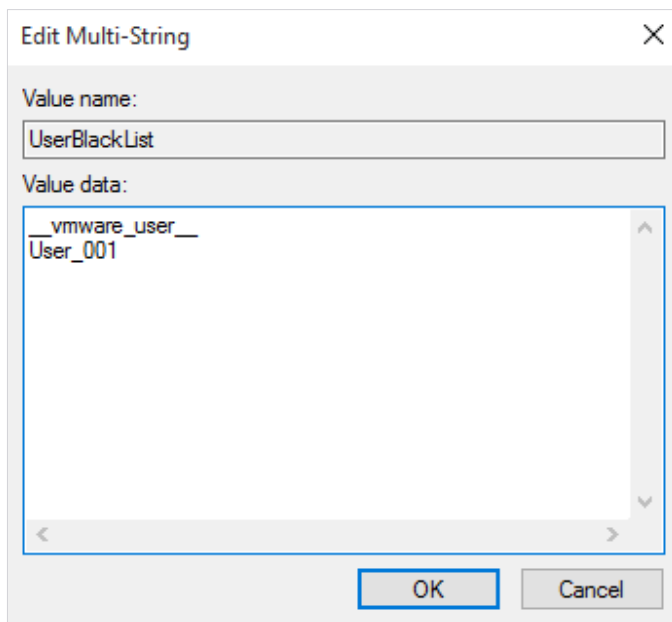
Figure 47. User Blacklist Dialog



4. Place and click the cursor under the last, current entry in the **Value data** pane and enter the exact characters for the user to be blacklisted. If you want to create more than one entry, make sure that each entry starts on a new line.

Click **OK** to apply the entries.

Figure 48. User Blacklist - Enter Username



5. Close the registry editor.

Revert to original settings. If, at any time after you have made this change, you decide to revert to the default blacklist entries, then just delete all the registry entries except `__vmware_user__` .

4.8. User capturing fails

The problem is [currently] specific to some Intel chipsets, for example chipsets used in DELL 630+830 computers.

Problem #1. 'User capturing' (i.e. *Windows* credentials) has been enabled and upon restart the following problems may occur:

- User capturing is apparently successful, but upon restarting the computer the self-initialization dialog reappears –i.e. user capturing was not successful.
- Either the PBA login screen does not appear or PBA itself does not appear.

Solution. This problem usually occurs because the *Intel* ICH 8 (AHCI) drivers are installed but the BIOS is configured for ATA mode.

If you download the ICH 8 driver from Intel, the package will not install unless the BIOS has configured the chipset for AHCI (you will be prompted that your system does not meet the minimum requirements). The driver on the DELL driver CD has no such restriction. The result is an installed ICH 8 driver that expects AHCI-mode but instead encounters an ATA-mode chipset.

It is recommended to remove EgoSecure Full Disk Encryption (if necessary using the Bart PE recovery CD) and reinstall Windows. The native Windows driver will allow you to install and perform user capturing without error.

Problem #2. "User capturing" (i.e. *Windows* credentials) has been enabled. When restarting the computer, the self-initialization dialog keeps reappearing – i.e. user capturing was not successful.

There is a conflict between the Intel 'Network Provider Credentials Manager' (*IntelNetProvCredMan*) and the EgoSecure capture driver. Follow these steps to change the provider order and enable successful user capturing:

1. Click Start -> Control Panel -> Network Connections.
2. From the menu, click Advanced -> Advanced Settings.
3. The **Advanced Settings** dialog appears. Click the **Provider Order** tab.
4. Make sure the entry *EgoSecure* is above the entry *IntelNetProvCredMan*. If not select the entry *EgoSecure*, and click the 'up' arrow button until the entry appears above *IntelNetProvCredMan*.
5. Click **OK**.
6. Restart the computer to capture the *Windows* credentials. Start the computer again to confirm that you must enter the password in the PBA component.

Alternative solution. As an alternative you can use the following registry key to change the provider order:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order

4.9. Partition creation fails after FDE has been initialized

Problem. Data copied to a partition that was created after the EgoSecure FDE component has been initialized fails to appear in Windows.

Solution. The cause of this is most likely to be the sector-based encryption. A workaround is to perform a restart after creating the new partition. If the new partition contained sectors which were previously encrypted, then reformat the new partition after the restart.

4.10. Incorrect GUI language/Change GUI language

Problem. The control center GUI has the wrong language. The installer has incorrectly recognized the language of the operating system. This may happen if you are using a Windows MUI language pack on top of the original system language.

Solution. A registry entry needs to be changed.

1. Open the Windows Registry Editor and navigate to:
HKEY_LOCAL_MACHINE\SOFTWARE\SECUDE\SNB.
2. Create new string Value with the name **lang** (or double-click it if it already exists) and enter the correct language into the field **Value Data**.

EgoSecure Full Disk Encryption currently supports the following languages:

- English (use en_US)
 - German (use de_DE)
3. Click **OK** when finished and close the editor.
 4. Restart the EgoSecure Full Disk Encryption Control Center.

Alternative way

Alternatively, you can:

1. Open a simple text editor and copy/paste the following text to change the GUI to German (with spaces and gaps):

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\SECUDE\SNB]
"lang"="de_DE"
```

2. Enter 'en_US' instead of 'de_DE' to change the GUI language to English
3. Save the file and close the text editor.
4. Change the extension of the file just created from *.txt to *.reg.
5. Double-click the file to set the registry correctly.

4.11. Administrator password forgotten

Problem. Administrator password for Full Disk Encryption has been forgotten.

Solution. Decrypting partition with the help of the ERI file -> deleting FDE partition -> initializing FDE again.

For details about ERI file, see [EgoSecure FDE - Administration and Usage Guide](#), chapter 1.12.

- If FDE was installed locally, the path for the ERI file is defined during ERI-file creating.
- If FDE was installed using EgoSecure Data Protection Console, the ERI file can be exported from the Console (**Computer management | FDE | Administrator**).

The screenshot shows the 'Administrator' settings page in the EgoSecure Data Protection Console. The page has a navigation bar with tabs for 'Administrator', 'Pre-Boot Authentication', 'PBA settings', 'Full Disk Encryption', and 'Drives'. The 'Administrator' tab is active. Below the navigation bar is a 'Save' button. The main content area is divided into two sections: 'Administration password' and 'Emergency recovery'. In the 'Administration password' section, there is a password input field with masked characters, a 'Change' button, and a 'Reset' button. Below the input field is a checkbox labeled 'Generate random password automatically'. In the 'Emergency recovery' section, there is a text description: 'In case you forget your username or account password, you can set an Emergency Recovery Password and save Emergency Recovery Information (ERI file)'. Below this is a password input field with three masked characters and a 'Change' button. There are two checkboxes: 'Automatically save ERI file' and 'Cache emergency recovery information on disk'. Below these is the text 'Copy ERI file into the database:' followed by two buttons: 'Copy' and 'Export...'. A mouse cursor is pointing at the 'Export...' button.

4.12. How to change PBA boot method

Problem. To date, general support of new computers is a costly and time consuming process – the sheer number of new notebook models grows every day. Each model brings new hardware and software with it – a challenge for any software that works so closely with the hardware.

That’s why after the PBA initialization, some problems with Windows starting may occur.
Solution.

EgoSecure utilizes the Grub boot loader in BIOS systems and the UEFI boot manager in UEFI systems. See solutions for:

- [BIOS](#)
- [UEFI](#)

BIOS

Call the grub menu to select the boot method, which will start your system correctly. To call the grub menu, press **Ctrl + G** key combination or only **G** key before the PBA boot image appears.

Figure 49. Grub menu



In this menu, select one of the following boot methods, and then press **Enter**.

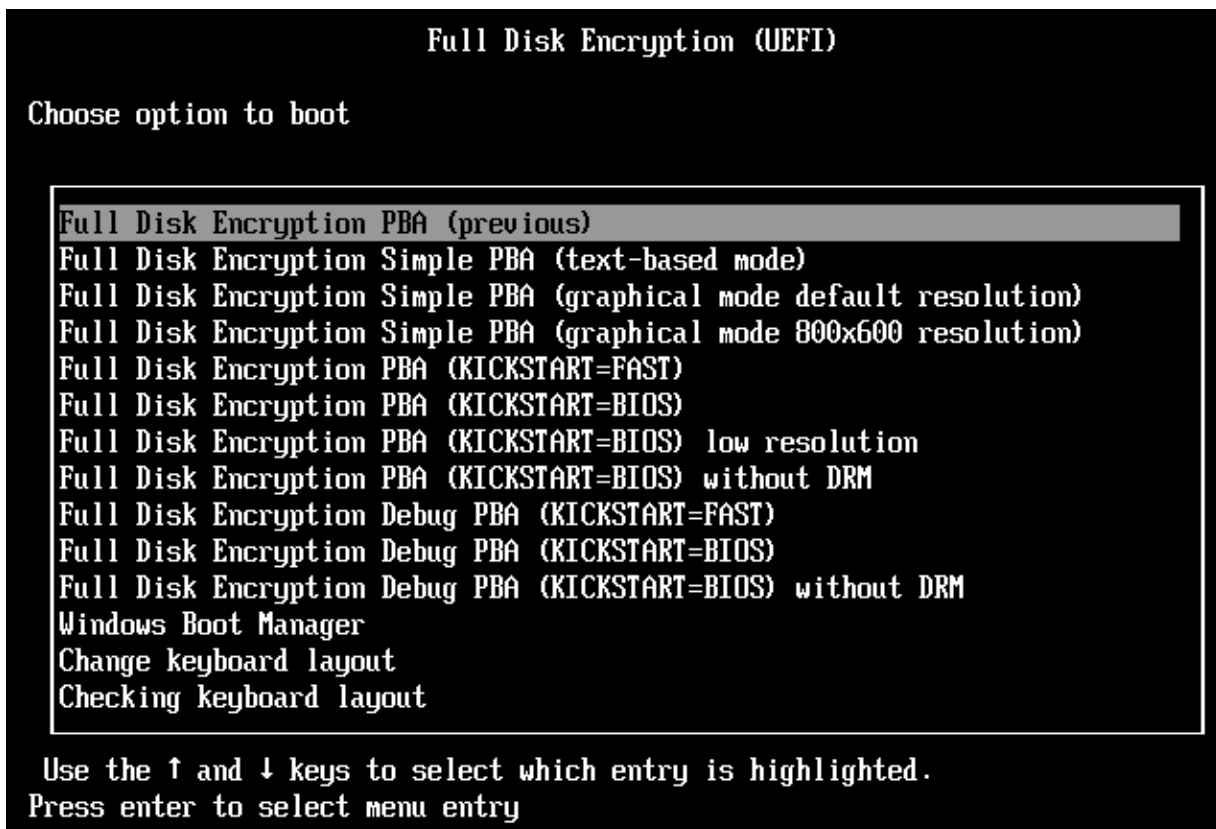
UEFI

When the UEFI FDE entry appears on the screen (Figure 50), press the **Ctrl + G** combination or only **G** key. In the boot menu (Figure 51), select one of the methods.

Figure 50. Starting PBA



Figure 51. PBA boot menu



Boot mechanisms description

Boot method	Details	
	BIOS	UEFI
[any of the methods]	The boot method that was selected the previous time. <i>Full Disk Encryption PBA</i> is a default value.	
Full Disk Encryption PBA (dmi. ini/dmi. default. ini)	The system is booted with the settings, which has been defined in the <i>dmi.ini</i> file.	-
Full Disk Encryption Simple PBA (text-based mode) – in both BIOS and UEFI	Simple PBA is an alternative PBA with a minimal feature set used to avoid possible hardware incompatibilities. During PBA, hardened Linux is used and during Simple PBA (SPBA), the EgoSecure Credentials manager is used. For details about PBA and SPBA in UEFI and BIOS systems, see Figure 52 and Figure 53 .	
Full Disk Encryption Simple PBA (graphical mode) – only for UEFI		

	<p>How it works? User authenticates with user name and password in a GUI-less login mask (in case of text-based mode) or in a GUI dialog (in case of graphical mode). HelpDesk works in all SPBA modes and smart card authentication works only in the graphical mode.</p> <p>What sources are used? Simple PBA utilizes the Grub boot loader in BIOS systems and the UEFI boot manager in UEFI systems. For details about PBA and SPBA comparison, see Figure 52 and Figure 53.</p>	
Full Disk Encryption PBA (KICKSTART=BIOS)	This is a standard mechanism used by EgoSecure Full Disk Encryption and should not be edited. This involves rebooting the computer a second time so that the BIOS hardware settings can be passed to <i>Windows</i> .	
Full Disk Encryption PBA (KICKSTART=KEXEC)	This mechanism is similar to KICKSTART=BIOS but does not need a reboot.	-
Full Disk Encryption PBA (KICKSTART=FAST)	This mechanism has been implemented for systems that have unusual hardware configurations not supported by the KEXEC mechanism.	
Full Disk Encryption PBA (ACPI, KICKSTART=BIOS)	This will automatically select an alternative Linux kernel configuration that enables ACPI support. This is something found almost exclusively in desktop computers and is rarely needed. ACPI mode is not compatible with Friendly Network.	-
Low resolution	Select this mode if during a previous boot, text and images of FDE dialogs were unreadable on the monitor (e.g.: on laptops). All boots after that will be performed in the selected mode with low screen resolution. For details about changing a screen resolution in PBA settings, see screen resolution .	
Without DRM	Select a mode without DRM if there are problems with graphic card and PBA loading.	
Debug PBA	Select a mode with this option to identify boot errors. Kernel loading messages will be displayed in this case.	
HDD 1 Partition 1	A bootloader on the partition 1 of the hard drive 1 will be used to start the system.	-
HDD 1 Partition 2	A bootloader on the partition 2 of the hard drive 1 will be used to start the system.	-
HDD 1 Partition 3	A bootloader on the partition 3 of the hard drive 1 will be used to start the system.	-
Windows Boot Manager	-	This mechanism uses default Windows Boot Manager, without PBA.
Change keyboard layout	-	Select the keyboard layout for entering PBA credentials: German or English.

Checking keyboard layout

-

Check what keyboard layout is currently used.

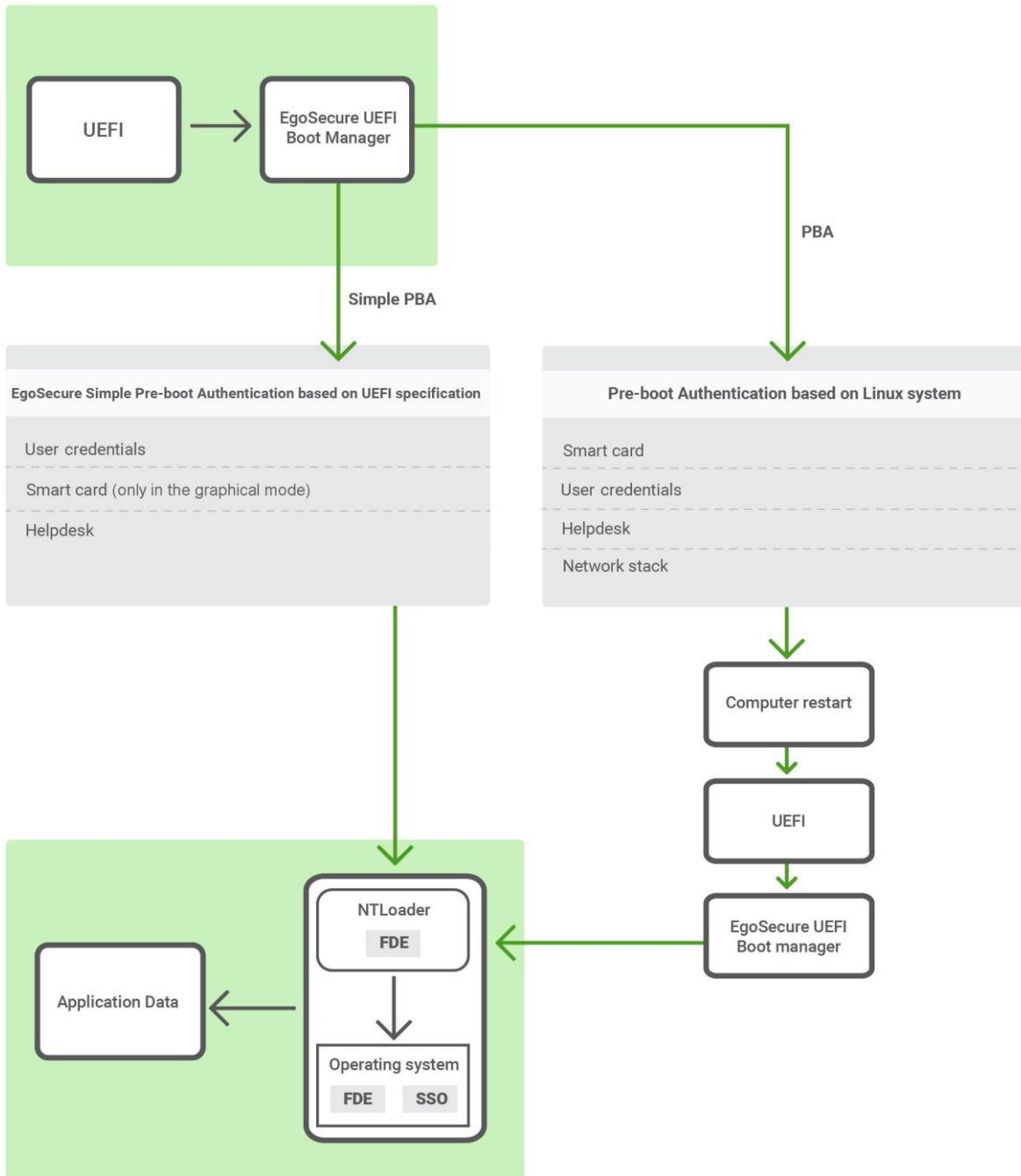


INFO

Using KEXEC and FAST

The KEXEC and FAST mechanisms should be used only if the standard mechanism (BIOS) does not work.

Figure 52. PBA and SPBA comparison - UEFI

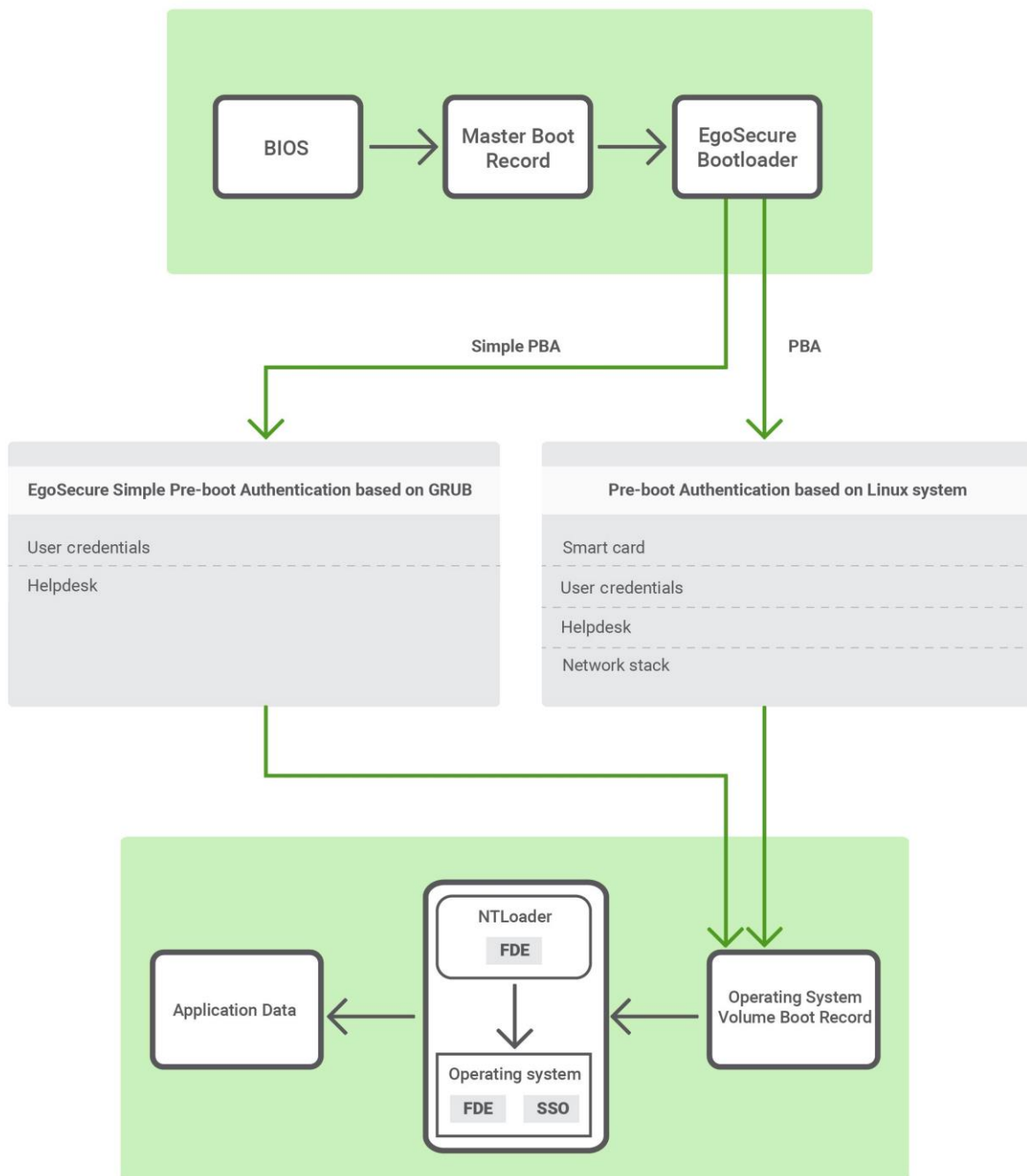


When loading WITHOUT PBA:

- only green blocks are functioning;
- SSO is not used.

SSO - Single sign-on
PBA - Pre-boot authentication

Figure 53. PBA and SPBA comparison - BIOS



When loading WITHOUT PBA:

- only green blocks are functioning;
- SSO is not used.

SSO - Single sign-on
PBA - Pre-boot authentication

4.13. PBA fails to start in RAID mode

Problem. EgoSecure FDE installation completes successfully. Partition is created. Once PBA is activated, the system hangs on startup. Caps lock is flashing and nothing happens. There is no chance to press **Ctrl + G** key combination (or only **G** key) to change PBA boot method, because the system hangs before this phase.

Solution. Changing System Drive from RAID to AHCI.

Applies to EgoSecure Full Disk Encryption 11.2 and higher.



ATTENTION

Enabling safe mode to avoid Windows crash

Before changing SSD type in BIOS, switch to safe mode. If not, Windows fails to boot and crashes. See the details below.



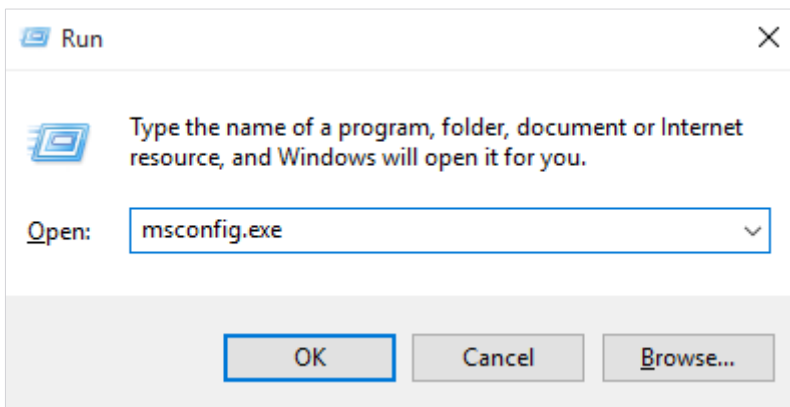
INFO

Prepare local administrative account

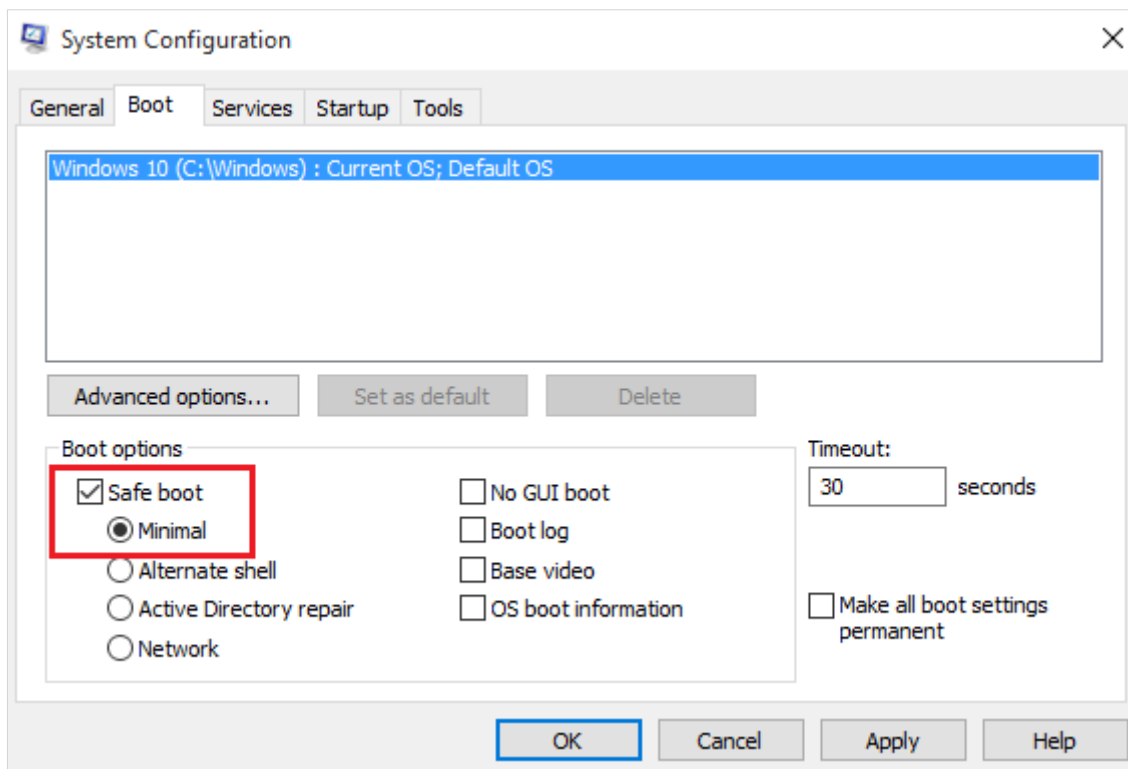
Please, make sure that local administrative account exists on the laptop and you know the password for this account. Network is disabled in this Safe Minimal mode and it might be not possible to authenticate and log in to the system.

Preparing Windows to start in safe mode

1. Run `msconfig.exe`. The **System configuration** dialog appears.



2. In the **Boot** tab, check **Safe boot** and set **Minimal** radio button.



3. Click **Apply** and reboot the system.
4. Press the key to Enter BIOS system setup (Esc, F1, F2, F10 or F12, depends on the device model). Change **Storage Configuration** option in BIOS from **RAID** to **AHCI**. Save settings and proceed with booting Windows.
5. Once Windows is started successfully, run msconfig.exe and clear the **Safe boot** check box.

4.14. FDE initialization fails – very fragmented disk

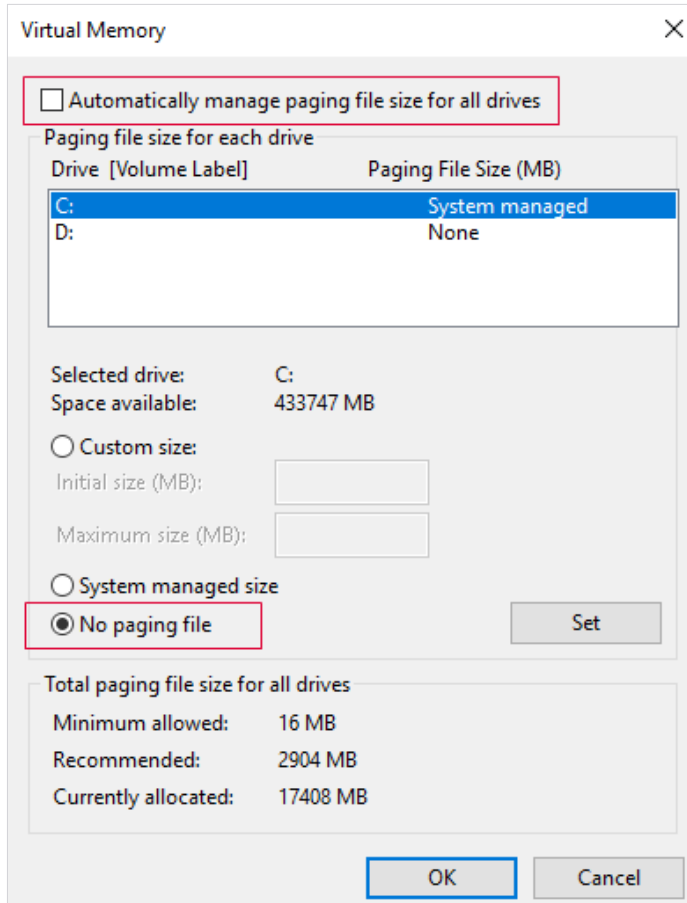
Problem. FDE initialization fails, because a disk is very fragmented.

1st solution.

1. Defragment the drive, using the **Optimize** option (for details, see the Microsoft article [Defragment your Windows 10 PC](#)).
2. Shrink the volume manually (minimum size is 510 MB).
3. Initialize FDE.

2nd solution (if 1st solution haven't helped).

1. Clear the Automatically manage paging file size for all drives check box.
2. Go to Control Panel | System and Security | System.
3. Click Advanced system settings.
 - The **System Properties** dialog appears.
4. In the **Advanced** tab, click **Settings** in the **Performance** area.
 - The **Performance Options** dialog appears.
5. Navigate to the **Advanced** tab and click **Change** button.
 - The **Virtual Memory** dialog appears.



6. Clear the Automatically manage paging file size for all drives option.
7. Select the drive and then select the **No paging file** radio button.
8. Click **OK** to save the changes and close the dialog.
9. Restart a computer.
10. Defragment the drive, using the **Optimize** option (for details, see the Microsoft article [Defragment your Windows 10 PC](#)).
11. Shrink the volume manually (minimum size is 510 MB)
12. Restore the settings the Virtual Memory settings to previous ones: enable the **Automatically manage paging file size for all drives** option and the previously selected radio button.
13. Initialize FDE.

4.15. PBA error

Problem. The PBA ERROR message is displayed on the whole screen when loading an operating system.

The reason is that the PBA protection has triggered in response to the issues with the FDE loader.

Solution.

1. Start the emergency recovery application (for details, see chapter “Emergency recovery via boot CD or USB stick” of the [EgoSecure FDE - Administration and Usage Guide](#)).
2. Click Disable PBA load check under BootChain.
 - The dialog appears.
3. Click **Start**.
4. Close the emergency recovery application.
5. Continue the system loading.

4.16. BitLocker hang after BSOD

Problem. In certain circumstances BitLocker encryption/decryption may hang. In our test environment BSOD happened when FDE was uninstalled during BitLocker decryption; after that BitLocker decryption hung.

Solution. Use BitLocker `manage-bde` commands in the commandline to pause encryption/decryption and then start the reverse process. After that you can repeat disk encryption or decryption that hung.

1. Run cmd as administrator.
2. Enter `manage-bde -pause` command. E.g: enter `manage-bde -pause C:` to pause encryption/decryption on disk C.
3. Start the reverse process.
 - a. If decryption was performed, start encryption using the command `manage-bde -on`. E.g.: enter `manage-bde -on C:` to start encryption on disk C.
 - b. If encryption was performed, start decryption using the command `manage-bde -off`. E.g.: enter `manage-bde -off C:` to start decryption on disk C.

Glossary

A **Administrator**

The 'administrator' – in *EgoSecure Full disk encryption* terms – is responsible for the installation, configuration and maintenance of the product. This person is responsible for (among other tasks) the following:

- ERI generation and storage
- Emergency recovery
- Remote installation and maintenance

Advanced Encryption Standard (AES)

In cryptography, the Advanced Encryption Standard (AES), also known as Rijndael, is a block cipher adopted as an encryption standard by the U.S. government. AES has a fixed block size of 128 bits and a key size of 128, 192 or 256 bits.

AES

See 'Advanced Encryption Standard'.

Algorithm

Algorithms are essential to the way computers process information, because a computer program is essentially an algorithm that tells the computer what specific steps to perform (in what specific order) in order to carry out a specified task.

An encryption algorithm is known as a cipher (see '*cipher*').

autoconf.nbs (temporary name)

A policy created by the FDE Policy Builder to automatically configure certain options for a number of computers.

This policy is the last of three policies to be executed for unattended installation:

- The first policy (setup.iss) is used to perform an unattended installation of the product on all the target computers.
- The second policy (bootconf.nbs) is used to integrate the boot security configuration in the installation process.
- The third policy (autoconf.nbs) continues with the rest of the configuration (encryption, ERI) after the computer has been restarted (the computer needs to be restarted before hard disk encryption can be performed).

B **Blowfish**

Blowfish is a keyed, symmetric block cipher, has a 64-bit block size and a key length of anywhere from 32 bits to 448 bits.

Boot

To load the first piece of software that starts a computer. Because the operating system is essential for running all other programs, it is usually the first piece of software loaded during the boot process.

Boot manager

The *EgoSecure* boot manager is an editor to prepare the computer to boot/display different systems and partitions. The boot manager has a similar graphical user interface to the Windows 2000/XP boot menu.

Boot time

The time it takes to turn on the computer to either the PBA logon dialog, or the *Windows* logon dialog.

bootconf.nbs (temporary name)

A policy created by the FDE Policy Builder to automatically configure the boot security options for a number of computers.

This policy is the second of three policies to be executed for unattended installation:

- The first policy (setup.iss) is used to perform an unattended installation of the product on all the target computers.
- The second policy (bootconf.nbs) is used to integrate the boot security configuration in the installation process.
- The third policy (autoconf.nbs) continues with the rest of the configuration (encryption, ERI) after the computer has been restarted (the computer needs to be restarted before hard disk encryption can be performed).

C Control Center

The *EgoSecure Control Center* is a console in which all the *EgoSecure* administration modules reside. These modules include:

- PBA administration

This module configures every aspect of PBA such as the smart card provider or configuring the HelpDesk.

- Policy Builder

This module is used to create and edit FDE, PBA, and Upgrade policies for unattended/remote configuration or removal of FDE components.

- *Boot Security Manager* (FDE Initialization)

This module is used for the administration, installation and removal of boot security.

- Recovery information

This module is used to create ERI.

- Disk encryption

This module is used to encrypt and decrypt internal hard disk partitions.

Cipher

A cipher (or cypher) is an algorithm for performing encryption and decryption -a series of well-defined steps that can be followed as a procedure. In most cases, that process is varied depending on a key which changes the detailed operation of the algorithm. *EgoSecure* uses the following ciphers:

- Blowfish
- DESX
- DES
- AES

Credentials

Used to establish the identity of a party in communication. Usually they take the form of machine-readable cryptographic keys and/or passwords. Cryptographic credentials may be self-issued, or issued by a trusted third party; in many cases the only criterion for issuance is unambiguous association of the credential with a specific, real individual or other entity. Cryptographic credentials are often designed to expire after a certain period, although this is not mandatory. See also 'Windows Credentials'.

Cryptographic erase

A secure method of data deletion to ensure that hard disks can be safely redeployed or discarded. Also known as 'secure erase', and 'digital shredding'.

D Data Encryption Key (DEK)

A cryptographic key that is used to encipher application data. (See 'key-encrypting key').

Data Encryption Standard (DES)

The Data Encryption Standard (DES) is a cipher (a method for encrypting information) selected as an official Federal Information Processing Standard (FIPS) for the United States in 1976.

DES is now considered to be insecure for many applications. This is chiefly due to the 56-bit key size being too small; DES keys have been broken in less than 24 hours.

Decryption

Cryptographically restore cipher text to the plaintext form it had before encryption (see 'Encryption').

DEK

See 'Data encryption key'.

Deploy

To install, test and implement a computer system or application. The term can be used to refer to any installation and testing, such as setting up a new network in an enterprise, to installing a server farm, to implementing a new application over a distributed computing network.

DES

See 'Data encryption standard'.

DESX

DES-X (or DESX) is a variant on the DES (Data Encryption Standard) block cipher intended to increase the complexity of a brute force attack using a technique called key whitening.

E Emergency Recovery Disk (ERD)

A boot CD to aid in re-accessing the data on the *EgoSecure* encrypted computer. In a situation in which the hard disk has been fully encrypted using *EgoSecure Full Disk Encryption*, and the user has forgotten the credentials necessary to access the computer (with or without PBA), the emergency recovery application can be used to gain access to the data on the computer.

You may need to use the emergency recovery application if the following occurs:

- The computer will not start correctly.
- The encryption/decryption key (or the password that leads to the encryption/decryption key) has been damaged, forgotten or lost.
- FDE has been removed without decrypting the hard disk first.

Encryption

Cryptographic transformation of data (called 'plaintext') into a form (called 'ciphertext') that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called 'decryption', which is a transformation that restores encrypted data to its original state.

Encryption key

A varying set of characters, numbers, and special characters used by an encryption algorithm as a 'key' to encrypt data. See also '*algorithm*'.

ERD

See 'Emergency Recovery Disk'

External media

All devices connected to, or inserted into, a computer. This includes USB hard disks, USB flash drives, and PCMCIA drives.

F FDE

See 'Full Disk Encryption'

Full Disk Encryption (FDE)

The Full Disk Encryption module for *EgoSecure*. FDE uses a sector-based encryption principle encrypt all the data written to the hard disk, and decrypt all the data read from the hard disk at a very low level, all directly at physical hard disk access.

This technology enables the encryption of the whole disk or partition, to include temporary files, swap files, and the operating system itself. Due to the encryption of whole partitions, no one can access the data by starting the

computer from media such as a CD-ROM, floppy disk or USB stick. Hacker tools that crack, or reset the system password, no longer have a chance to compromise the system. If the hard disk is built into another computer as a second disk, the access to encrypted partitions is also impossible.

H HelpDesk

In an emergency in which the user has lost their smart card or forgotten their *Windows* credentials and/or has no access to administrator resources, *EgoSecure FDE* offers the user the chance to access their notebook via a HelpDesk. The HelpDesk is usually a telephone hotline that can be reached by the user via information in the PBA dialog. The HelpDesk administrator will use information from the user (called the 'challenge') and relays a 'response' that the user enters in the PBA help-dialog to bypass the authentication mechanism for a limited number of times.

HelpDesk Administrator

A person with administrator access to the HelpDesk application to aid users in obtaining access to their computers in an emergency.

K KEK

See 'Key Encrypting Key'.

Key Encrypting Key (KEK)

A cryptographic key that is used to encrypt other keys, either DEKs or other KEKs, but usually is not used to encrypt application data.

Key length

The number of symbols (usually bits) needed to be able to represent any of the possible values of a cryptographic key.

L Log file

A file to which system/component messages are collected for the purpose of evaluation. The following log files are created by *EgoSecure Full Disk Encryption*:

- *setup.log*—used to evaluate the correctness of the policy recording procedure.
- *notebook.log/FDE.log*—The main log file for *EgoSecure Full Disk Encryption*. It contains information about every administrative action performed in *EgoSecure* (such as deployment) and also details the parameters used for any operation.
- *sbs.log/PBA.log*—This file is created by the PBA component. The file details all the actions performed in the PBA component, from installation to any configuration changes.
- *sbsnotm.log*—This log file is created by the *EgoSecure* Notification Manager. The Notification Manager is an *EgoSecure* developed plug-in for the *Windows* GINA responsible for single sign-on. *EgoSecure* oversees the size of the file. When the file becomes larger than a predefined size 50% of the entries (oldest entries) are deleted.

M **Module**
See 'Control Center'

P **PBA**
See 'Pre-Boot Authentication'

PBA HelpDesk
See 'HelpDesk'

PKCS#11

'PKCS' refers to a group of Public Key Cryptography Standards devised and published by RSA Security. 'PKCS#11' is an API defining a generic interface to cryptographic tokens.

Pre-Boot Authentication (PBA)

A means to authenticate a person to a computer before the computer boots to the primary operating system. The Pre-Boot Authentication (PBA) module is an extension of EgoSecure Full Disk Encryption (FDE). A choice of two authentication methods is possible:

- *Smart card authentication* based on international standards such as X.509, PKCS#11 and PC/SC.
- *Windows credentials authentication* based on the user's current user ID and password.

PBA is supported by the PBA HelpDesk (See 'HelpDesk').

Policies

See 'autoconf.nbs', 'bootconf.nbs', and 'setup.iss'.

R **Remote administration**

An administrator has the possibility to deploy and/or configure EgoSecure Full Disk Encryption to any number of computers from a single computer. This helps maintain a consistent security policy throughout the company and saves time.

S **Secure erase**

See 'Cryptographic erase'
setup.iss

This policy is the first of three policies to be executed for unattended installation:

- The first policy (setup.iss) is used to perform an unattended installation of the product on all the target computers.
- The second policy (bootconf.nbs) is used to integrate the boot security configuration in the installation process.
- The third policy (autoconf.nbs) continues with the rest of the configuration (encryption, emergency recovery information) after the computer has been restarted (the computer needs to be restarted before hard disk encryption can be performed).

Single sign-on

A method of access that administrates authentication information allowing a user to logon to systems and open programs without the need for re-authentication.

For *EgoSecure FDE*, single sign-on is for *Windows* credentials.

Smart card

A credit-card sized device containing one or more integrated circuit chips, which perform the functions of a computer's central processor, memory, and input/output interface.

Smart card reader

Smart card readers are used as a communications medium between the smart card and a host, e.g. a computer, a point of sale terminal, or a mobile telephone.

T Token

A security token (or sometimes a hardware token, authentication token or cryptographic token) may be a physical device that an authorized user of computer services is given to aid in authentication. The term may also refer to software tokens.

Smart card-based USB tokens (which contain a smart card chip inside) provide the functionality of both USB tokens and smart cards. They enable a broad range of security solutions and provide the abilities and security of a traditional smart card without requiring a unique input device (smart card reader). From the computer operating system's point of view such a token is a USB-connected smart card reader with one non-removable smart card present.

U User

An individual who uses a computer. This includes expert programmers as well as novices. An end user is any individual who runs an application program. The user usually cannot configure, remove, or change any *EgoSecure Full Disk Encryption* component.

W Windows Credentials

A unique set of information authorizing a user to access the *Windows* operating system on a computer. The credentials usually comprise a user name, a password, and a domain name (optional).

PBA allows the user to authenticate themselves via their *Windows* credentials. The 'single sign-on' function of PBA allows the user to enter their credentials once in PBA with no need to re-enter them in the *Windows* logon dialog.