

# EGOSECURE

A MATRIX42 COMPANY

## EgoSecure Full Disk Encryption

---

### Administration and Usage 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](mailto:helpdesk@matrix42.com)  
Self Service Portal: [support.matrix42.com](https://support.matrix42.com)  
Internet: [www.matrix42.com](https://www.matrix42.com)

# CONTENTS

<b>1. Administration and Usage .....</b>	<b>5</b>
1.1. How the Boot Process is affected by EgoSecure Full Disk Encryption .....	5
1.2. The Initial Start and User Capturing .....	5
1.3. The Boot Sequence.....	6
Smart card boot procedure.....	6
Smart card boot procedure – error dialogs.....	9
Windows credentials boot procedure .....	13
Windows credentials boot procedure – error dialogs .....	14
1.4. Advanced PBA Features .....	16
Log viewer .....	16
Advanced PBA configuration options .....	18
Changing keyboard layout.....	19
Operating system boot selection .....	20
PBA user management.....	21
1.5. The Control Center .....	23
1.6. PBA Administration.....	25
1.7. PBA Initialization/De-initialization .....	28
1.8. FDE Initialization - Boot Security .....	30
Installing boot security .....	30
Updating boot security configuration.....	31
Removing boot security .....	34
1.9. Changing the Administration Password .....	36
1.10. FDE Status Query .....	38
The FDE status query GUI .....	39
Start a status query via the commandline.....	41
FDE query log file.....	41
1.11. Hard Disk Encryption.....	45
Encrypting a hard disk partition .....	46
Decrypting a hard disk partition .....	54
1.12. Emergency Recovery Information (ERI).....	57
Creating an ERI file .....	58
Defining an automatic ERI file naming convention.....	61
Creating a WinPE emergency recovery boot CD or USB flash drive (Windows Vista/Windows 7/8/8.1/10) .....	64
1.13. Performing emergency recovery.....	69
Recovery via the HelpDesk option .....	69
Emergency recovery via boot CD or USB stick .....	75
1.14. Remote Administration .....	92

---

Deploying Full Disk Encryption policies .....	93
Deploying Pre-Boot Authentication policies .....	94
<b>2. Building Policy for Deployment.....</b>	<b>95</b>
2.1. The Full Disk Encryption Policy Builder .....	96
Creating an initialization policy.....	96
Creating a configuration policy .....	113
Creating a de-initialization policy.....	129
Editing policies .....	136
2.2. The Pre-Boot Authentication Policy Builder .....	139
Creating an initialization or configuration policy .....	140
Creating a de-initialization policy.....	161
Editing an existing PBA policy .....	167
2.3. Creating an upgrade policy .....	169
<b>3. Trusted Platform Module (obsolete) .....</b>	<b>172</b>
Introduction .....	172
3.1. Overview .....	172
Introduction .....	172
Requirements.....	173
Limitations .....	173
Tested systems.....	173
3.2. TPM installation .....	173
Attended installation.....	174
Unattended installation .....	174
3.3. Removal .....	174
3.4. TPM usage .....	174
TPM administration module (attended mode) .....	175
Remote TPM functionality (unattended mode) .....	176
3.5. TPM utilities .....	178
Obtain TPM status.....	178
Test TPM compatibility .....	179
3.6. Boot Code Errors.....	180
3.7. Creating policy for TPM (Full Disk Encryption Policy Builder) .....	180
<b>4. The Integrated Boot Manager.....</b>	<b>183</b>
4.1. Overview .....	183
Graphical interface .....	183
Manual approach .....	183
4.2. Step 1: Creating a configuration file .....	184
Notes .....	184
Understanding the bootmgr.ini.....	184

---

---

4.3. Step 2: Create a configurator.exe file .....	188
4.4. Step 3: Executing the configurator.exe file on the target system.....	190
<b>5. Helper Applications .....</b>	<b>191</b>
5.1. Changeeripw .....	191
5.2. GUS.....	192
Usage.....	192
5.3. PSEnc .....	193
Usage.....	193
Examples.....	194
Specific example.....	194
5.4. Dmiconfig (hardware compatability mode) .....	195
Mechanisms .....	195
Screen parameters.....	196
Kernel parameters .....	196
Default computers.....	196
Dmiconfig tool .....	197
5.5. Systemcheck.....	198
5.6. TMP_test .....	200
5.7. Tcosconfig.....	200
<b>6. Appendix .....</b>	<b>207</b>
6.1. Bootmgr.ini example.....	207
6.2. Key usage.....	208

## 1. ADMINISTRATION AND USAGE

### 1.1. How the Boot Process is affected by EgoSecure Full Disk Encryption

EgoSecure Full Disk Encryption is the ultimate security measure for notebooks - the notebook no longer boots directly to Windows but rather to a secure system image that controls the access to Windows.

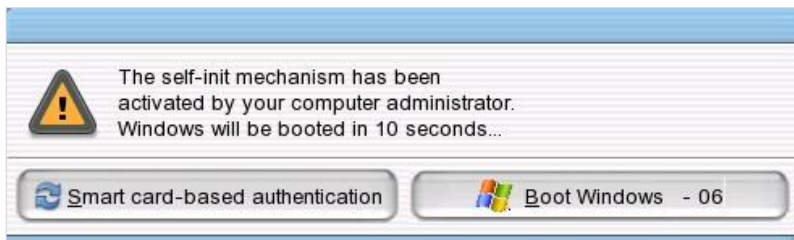
Although EgoSecure Full Disk Encryption is compact, it still takes time to load, to enter the Windows credentials or smart card PIN, to check the validity of the information, and to boot to Windows.

### 1.2. The Initial Start and User Capturing

PBA has a "capture mode" called "user capturing". This mode is activated when the PBA option **Enable smart card user capturing** (for smart cards), or **Enable user ID/password capturing** (for Windows credentials), is enabled either during installation or configured later via the Control Center.

When activated, PBA does not prompt for authentication during startup, but rather displays the following dialog:

**Figure 1. Self initialization dialogs –Windows credentials and smart card**



After 10 seconds, the dialog will automatically boot to the Windows logon dialog. It is here that the "capture" takes place – when the user enters their password, and clicks **OK**. Once the user credentials are successfully captured, the computer boots into Windows. As from this point on, for every logon, the user must enter their credentials into the PBA as stated in section [1.3](#).



#### ATTENTION

#### Preventing users from being incorrectly captured

In certain installations, for example "Netinstall" installations, it is possible that user may be incorrectly captured.

- ◆ For details about how to blacklist users to prevent them from being captured or from being able to access EgoSecure Full Disk Encryption installation, refer to the [EgoSecure FDE – Installation and Troubleshooting Guide](#).

## 1.3. The Boot Sequence

This section details the PBA boot sequence. The boot sequence differs according to the type of authentication, which is configured in PBA – either smart card or Windows credentials. This section also details any error dialogs you may encounter.



### ATTENTION

#### **Disconnect external hard disks and USB sticks**

Disconnect or turn-off any external hard disks or USB sticks before starting the computer, because leaving them connected may prevent EgoSecure Full Disk Encryption from starting (risk detection).

When starting EgoSecure Full Disk Encryption for the first time you will not be prompted for authentication in PBA because EgoSecure Full Disk Encryption is in “capture mode” (the exception to this rule is when smart card self-initialization is active - which may be the case after installation). When in this mode EgoSecure Full Disk Encryption bypasses logon and takes you straight to the Windows logon dialog. In the Windows logon dialog, you must enter your credentials as normal for the EgoSecure Full Disk Encryption to capture them. When you next shut down/start the computer, EgoSecure Full Disk Encryption is active, and you must authenticate as stated above. For details about capture mode, see section 1.2. If you enabled the single sign-on option during initialization, then authentication to the standard Windows logon dialog will be performed automatically. If you did not enable this feature, then you must enter your Windows credentials into the Windows logon dialog before you can access the system.



### INFO

#### **Achieving maximum security**

To achieve maximum security, ALWAYS shut down the computer when you do not need it.

### CONTENTS

- ◆ [Smart card boot procedure](#)
- ◆ [Smart card boot procedure – error dialogs](#)
- ◆ [Windows credentials boot procedure](#)
- ◆ [Windows credentials boot procedure – error dialogs](#)

### Smart card boot procedure

This section details the boot procedure using a smart card for authentication.



### ATTENTION

#### **Using Simple PBA with smart card authentication**

If Simple PBA boot mode was selected during system boot, smart card authentication is supported only in the graphical Simple PBA (UEFI). For details about Simple PBA boot mode, see EgoSecure FDE – Installation and Troubleshooting Guide, chapter 4.15.

1. Make sure that the smart card is in the reader, and the reader is connected to the computer (if necessary).
2. Start the computer as normal.
  - After a moment, the EgoSecure Full Disk Encryption background image (or the custom image defined during installation/initialization) appears.
  - The PBA startup screen appears (the startup screen may vary according to the background image chosen during either installation or configuration).
  - After a short while the following dialog appears:



This dialog presents you with the following options:

Option	Description
Click here to display options	Click this text to display the extended options (see the next page).
Helpdesk	When you have problems with the logon process, you can click Helpdesk (or press Alt+H keys) to start the HelpDesk process (providing that you have installed this feature). Helpdesk is not working in the text-based Simple PBA boot mode (BIOS). For details about Simple PBA, see <a href="#">EgoSecure FDE – Installation and Troubleshooting Guide</a> , chapter 4.15.
Restart	Click <b>Restart</b> (or press Alt+R keys) if you need to restart the computer (e.g. if you have connected the wrong smart card reader).

3. Enter your smart card PIN and click **OK**.

- The EgoSecure Full Disk Encryption will now check the validity of the information. If valid, the computer will automatically boot to Windows.

### Problems with single sign-on

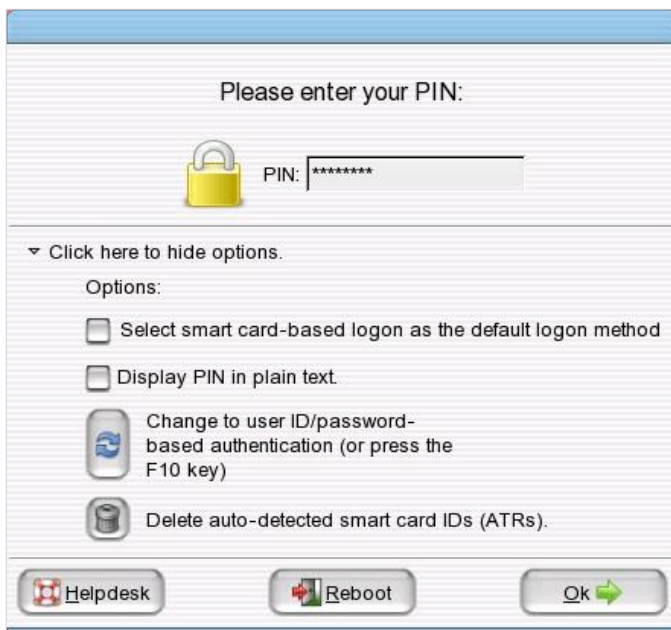
If after the initial capture has been performed and you have successfully logged on to EgoSecure Full Disk Encryption, you are still confronted with the standard Windows logon dialog, then the most likely cause is that the 'Windows secure logon' feature is active and must be disabled for single sign-on to succeed. For further details, see the [EgoSecure FDE – Installation and Troubleshooting Guide](#).

## Issues with PBA loading

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. That is why EgoSecure utilizes the Grub boot loader in BIOS systems and the UEFI boot manager in UEFI systems to resolve the problem with Windows start. For details about available boot methods, see chapter 4.15 of the [EgoSecure FDE – Installation and Troubleshooting Guide](#).

## Extended options

The following menu unfolds when you select **Click here to display options:**



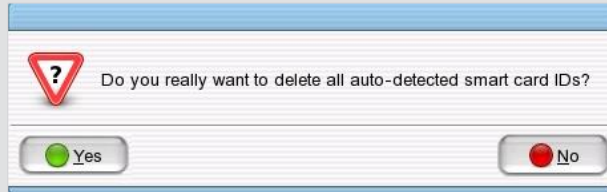
This menu presents you with the following extra options:

Extended options	Description
Select smart card-based logon as the default logon method	Check this box to define smart card logon as the default authentication method.
Display PIN in plain text	Select this option to display an entry made (or to be made) in the Password field.
Change to user ID/password-based authentication (or press the F10 key)	Click this (or press F10) to switch to the <i>Windows</i> credentials logon method (click the link for details about <a href="#">Windows credentials boot procedure</a> ). Switching the authentication method can be permanently disabled via the Pre-Boot tab of the PBA Administration module in the EgoSecure Full Disk Encryption Control Center. For details, follow the link <a href="#">PBA Administration</a> .



Delete auto-detected smart card IDs (ATRs)

Click this button to delete the smart card IDs auto detected by PBA. This results in PBA prompting you to select another provider:



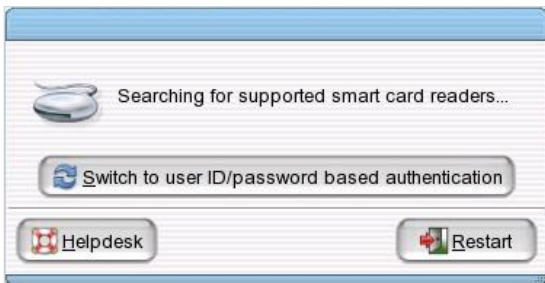
## Smart card boot procedure – error dialogs

The dialogs described in this part indicate problems with the smart card authentication method.

- ◆ [No smart card reader](#)
- ◆ [No smart card](#)
- ◆ [No matching certificate](#)
- ◆ [No PKCS#11 provider](#)
- ◆ [PKCS#11 provider not recognized](#)
- ◆ [Incorrect PIN](#)
- ◆ [Enter PIN correctly after wrong entry](#)

### No smart card reader

If no smart card reader is found, the following dialog appears:



PBA will continue to check the USB/PCMCIA bus for readers until one is found (if one is not found it is probable that the reader has been defined incorrectly during the installation procedure). The following options are available:

Option	Description
Switch to user ID/password based authentication	If you click <b>Switch to user ID/password based authentication</b> you can switch to the <i>Windows</i> credentials logon method (click the link for details <a href="#">Windows credentials boot procedure</a> ).
Helpdesk	When you have problems with the logon process, you can click Helpdesk (or press Alt+H keys) to start the HelpDesk process (providing that you have installed this feature). Helpdesk is not working in the text-based Simple PBA boot mode (BIOS). For details about Simple PBA, see <a href="#">EgoSecure FDE – Installation and Troubleshooting Guide</a> , chapter 4.15.

Restart

Click **Restart** (or press Alt+R keys) to restart the computer (e.g. if you have connected the wrong smart card reader).

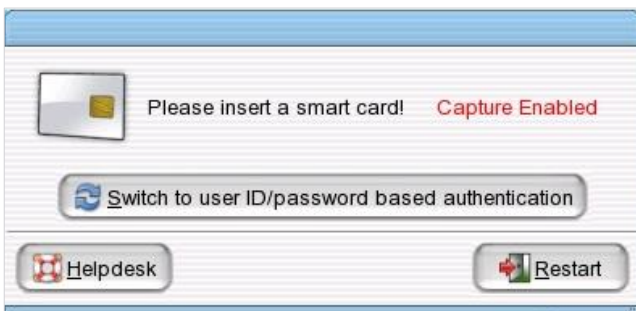
### No smart card

If no smart card is found in the reader, the following dialog appear:

**Figure 2. Error dialog - no smart card found**



**Figure 3. Error dialog – no smart card found (when self-initialization of smart card is enabled)**



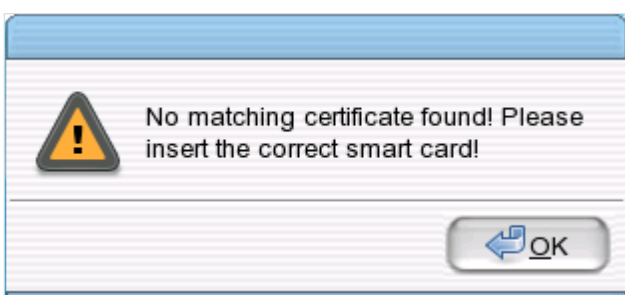
PBA will continue to check the reader for a smart card until one is found (if one is not found it is probable that the smart card provider (PKCS#11) has been defined incorrectly during the installation procedure). If a smart card is already inserted in the reader, and this dialog still appears (i.e. the smart card cannot be detected by the PBA), this has nothing to do with which provider (PKCS#11) has been selected during installation. The reason for such behavior is most probably a communication problem with the smart card. Re-inserting the card may help.

The options available to you are the same as described above (no smart card reader can be found).

### No matching certificate

If no matching certificate is found on the smart card/token the following dialog appears:

**Figure 4. Error dialog - no matching certificate found**

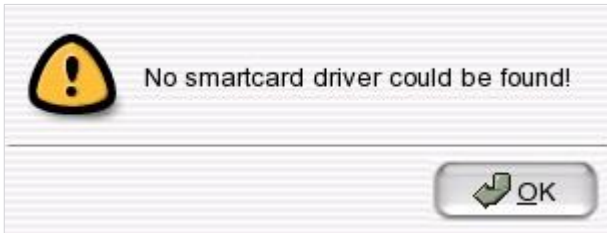


This means that the PIN entered by the user is correct, but the certificate on the smart card/token does not match the user information and/or key usage/label information located in the PBA. The correct certificate must be used for authentication. Either re-enable user capturing in the PBA or use another smart card/token with the correct certificate.

## No PKCS#11 provider

If no PKCS#11 provider is found on the smart card the following dialog will appear:

**Figure 5. Error dialog - no PKCS#11 provider found**

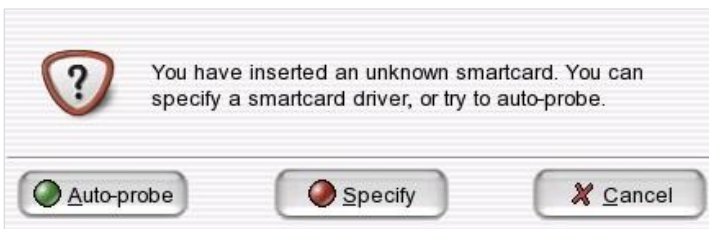


It is probable that the smart card provider (PKCS#11) has been defined incorrectly during the installation procedure. Either check the card, or use Windows credentials to logon (click the [link](#) for details). If Windows credentials logon is not active then use either the HelpDesk or an ERD to access the computer. Click **OK** to return to the PIN entry dialog (see [Smart card boot procedure](#)).

## PKCS#11 provider not recognized

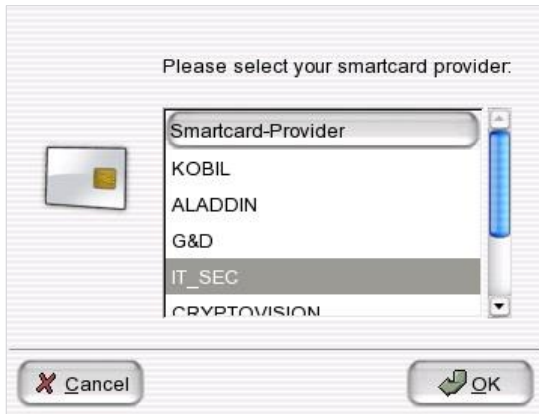
The following dialog indicates that the reader has been found but the smartcard PKCS#11 provider has not been recognized:

**Figure 6. Error dialog - PKCS#11 provider not recognized**



1. Click **Auto-probe** to let PBA select the provider, or click **Specify** to select a provider manually.
2. If you click **Specify** the following dialog appears:

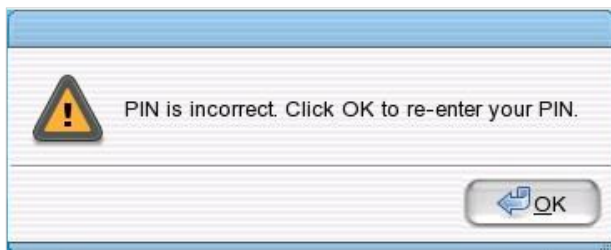
**Figure 7. Manual provider selection dialog**




3. Select the provider from the list and click **OK**.

### **Incorrect PIN**

The following dialog indicates an incorrect PIN:

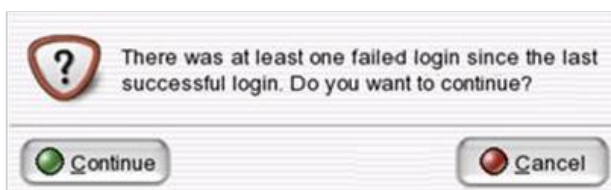


- Click **OK** to return to the PIN entry dialog, and enter the correct PIN.

 <b>ATTENTION</b>	<p><b>Limited number of PIN retries</b></p> <p>Smart cards have a limited number of PIN retries, after which you can only use Windows credentials or the HelpDesk to access your computer. For further information about smart card limitations please refer to the card issuer.</p>
---	--

### **Enter PIN correctly after wrong entry**

This dialog informs the user of attempts to authenticate to the computer. The following dialog will appear after a PIN has been entered incorrectly one or more times before being entered correctly.



The dialog will appear **before** the next login is actually performed. Click **Continue** to boot to Windows, or login to the card.



## WARNING

### Possible card misuse

This dialog informs you of possible card misuse! Please contact your system administrator.

## Windows credentials boot procedure

This section details the boot procedure using Windows credentials for authentication.

1. Start the computer as normal.

- After a moment the PBA background image will appear (or the image designated during installation/initialization).
- After a while you will be prompted to enter your Windows credentials (username/password/domain):



This dialog presents you with the following options:

Option	Description
Click here to display options	Click this text to display the extended options (see below).
Helpdesk	When you have problems with the logon process, you can click Helpdesk (or press Alt+H keys) to start the HelpDesk process (providing that you have installed this feature). Helpdesk is not working in the text-based Simple PBA boot mode (BIOS). For details about Simple PBA, see <a href="#">EgoSecure FDE - Installation and Troubleshooting Guide</a> , chapter 4.15.
Restart	Click <b>Restart</b> (or press Alt+R keys) if you need to restart the computer (e.g. if you have connected the wrong smart card reader).

2. Enter your user name and password in the respective fields and click **OK**.

- EgoSecure Full Disk Encryption will now check the validity of the information. If valid, the computer will automatically boot to Windows.

- If, after the initial capture has been performed and you have successfully logged on to EgoSecure Full Disk Encryption, you are still confronted with the standard Windows logon dialog, then the most likely cause is that the “Windows secure logon” feature is active and must be disabled for single sign-on to succeed. For further details, refer to the [EgoSecure FDE – Installation and Troubleshooting Guide](#).
- The following dialog appears when you select **Click here to display options**:



This dialog presents you with the following extra options:

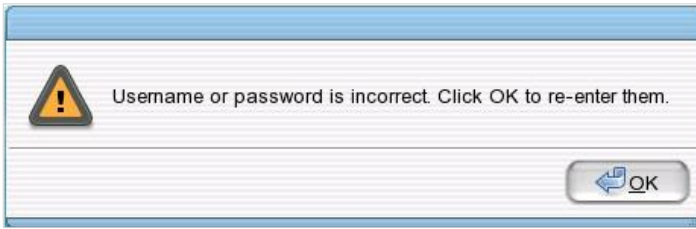
Extended options	Description
Select user ID/password-based logon as the default logon method	Check this box to define Windows credentials as the default authentication method.
Display password in plain text	Check this option to display an entry made (or to be made) in the field Password.
Change to smart card-based authentication (or press the F10 key)	Click this (or press F10) to switch to the smart card logon method (click the link <a href="#">Smart card boot procedure</a> for details). Switching the authentication method can be permanently disabled via the Pre-Boot tab of the PBA Administration module in the EgoSecure Full Disk Encryption Control Center. For more details, see <a href="#">PBA Administration</a> .

## Windows credentials boot procedure – error dialogs

The following dialogs indicate problems with the Windows credentials authentication method.

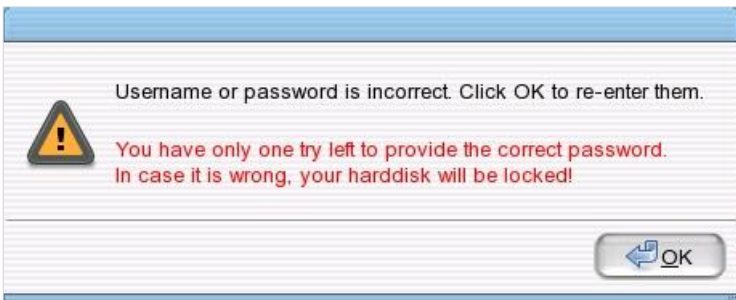
### Invalid Windows credentials

- If the credentials have been entered incorrectly the following dialog will appear:



Click **OK** to return to the Windows credentials logon dialog and re-enter your password.

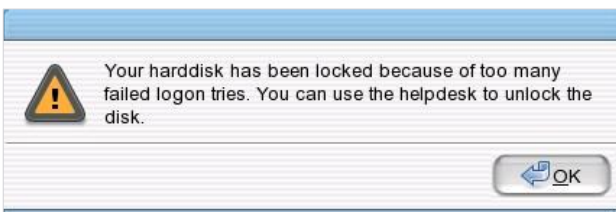
- The following error message appears if you are about to exceed the maximum number of failed login.



Click **OK** to return to the Windows credentials logon dialog and re-enter your password.



Be aware that your hard disk will be locked if again entered a wrong password.



Click **OK**. The **Recovery** dialog appears:



For details about recovery process, see chapter [1.13](#).

## 1.4. Advanced PBA Features

This section details the advanced features in the PBA – The log viewer and advanced configuration options.

Both of the following PBA features can be permanently disabled via the Pre-Boot tab of the PBA Administration module in the EgoSecure Full Disk Encryption Control Center. For more details, see [PBA Administration](#).

### CONTENTS

- ◆ [Log viewer](#)
- ◆ [Advanced PBA configuration options](#)
- ◆ [Changing keyboard layout](#)
- ◆ [Operating system boot selection](#)
- ◆ [PBA user management](#)

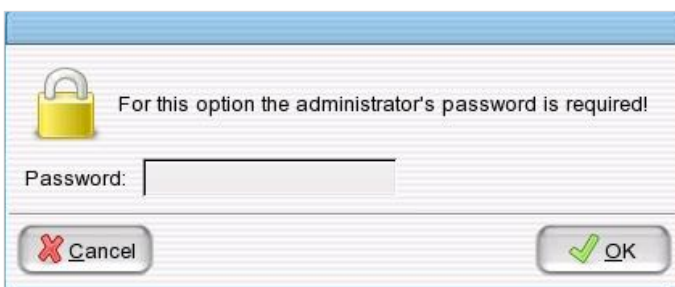
### Log viewer

This section details the log viewer functionality in the PBA.

The log viewer is a diagnostics tool to help administrators locate any problems with PBA, for example, if a supported smart card reader has been successfully recognized by the Linux kernel, or that the boot process has been successful. This information may be needed by the local administrator or by the HelpDesk personnel in an emergency.

1. To open the log viewer, press the Ctrl+F12 key while still in the PBA logon dialog.

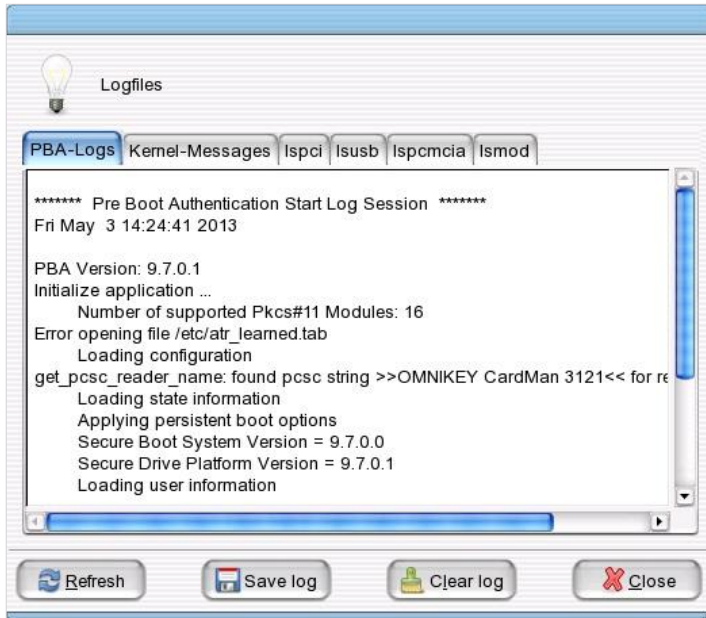
→ The Administration password dialog appears:





2. Enter the credentials and click **OK**.

→ The **PBA** dialog appears. The tabs represent the Linux functionality used by the PBA component.



The tabs display the following information:

Tab	Details
PBA-Log	This is the only tab that is purely for EgoSecure Full Disk Encryption. It details the log messages generated by PBA application, from loading the PKCS#11 modules to initializing the card reader.
Kernel-Messages	Linux core boot messages relevant to EgoSecure Full Disk Encryption.
Ispci	An enumeration of all devices connected to the PCI bus.
Isusb	An enumeration of all devices connected to the USB bus.
Ispcmcia	An enumeration of all devices connected to the PCMCIA bus.
Ismod	All currently loaded kernel modules.


The buttons have the following functionality:

Function	Details
Refresh	Use this function to update the input to the log viewer. This is useful to see if a new smart card or reader has been recognized by PBA.
Save log	Use this function to save the log messages to a file. These files can only be saved to a USB mass storage device. NOTE: Press Ctrl+F1 key while still in the PBA logon dialog without providing administrator password. <b>! Only FAT32 file system is supported.</b>

Clear log	Use this function to clear the dialog of all log input up to that point in time. This is useful if you want to view new log messages.
Close	Close the log viewer dialog.

## Advanced PBA configuration options

This section details the advanced configuration options in the PBA. This feature will enable you to alter a few specific features to help speed-up the PBA loading time and/or secure the PBA further.

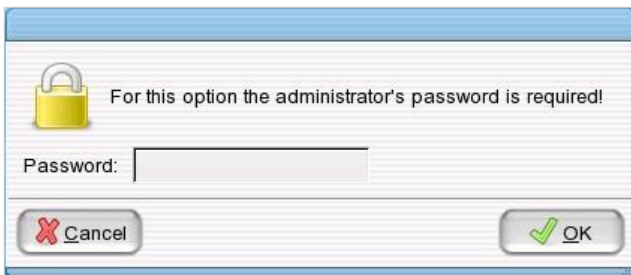


**WARNING**

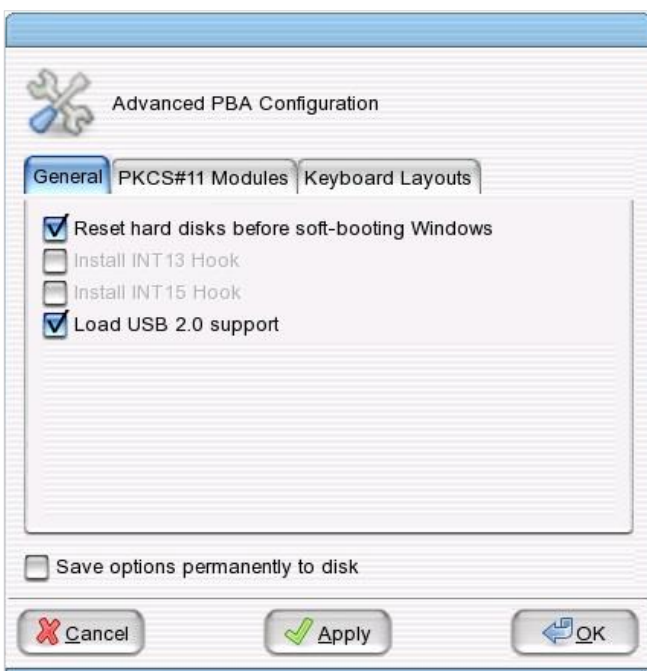
**PBA damage risk**

These options can damage the PBA if set incorrectly! If you have not already done so, it is recommended to contact your administrator or EgoSecure support before setting any options.

- To open the advanced options, press the Ctrl+F11 key while still in the PBA logon dialog.  
→ The **Administration password** dialog appears:



- Enter the EgoSecure Full Disk Encryption administration password and click **OK**.  
→ The Advanced PBA Configuration dialog appears:



The tabs display the following information:

Tab	Details
General	<p>This option is usually of no interest but may be of used on specific notebooks to overcome some issues during soft-booting to <i>Windows</i>:</p> <ul style="list-style-type: none"><li>■ Load USB 2.0 support</li></ul> <p>Check this option if you are having problems with some USB smart card readers. This option stops the USB 2.0 drivers being loaded into the <i>Linux</i> PBA.</p>
PKCS#11 Modules	<p>Click this tab if you want to change the order in which the smart card provider modules (PKCS#11 modules) are scanned during smart card auto-detection. Select a provider you want scanned first from the list and click <b>Up</b> until the entry is at the top of the list.</p>
Keyboard Layouts	<p>Click this tab if you want to change the keyboard layout used for PBA authentication.</p> <ul style="list-style-type: none"><li>■ Keyboard layout.</li></ul> <p>The current keyboard layout is displayed above the list.</p> <ul style="list-style-type: none"><li>■ Test [field]</li></ul> <p>Once a layout has been selected from the list (and Apply is clicked) you can test the new layout in this dialog.</p>

The remaining options/buttons have the following functionality:

Function	Details
Save options permanently to disk	Check this option before clicking <b>Apply</b> or <b>OK</b> to permanently save any changes you make to the PBA. If you do not check this option, any changes you make will apply only to this session.
Cancel	Click <b>Cancel</b> to return to the PBA logon dialog.
Apply	Click <b>Apply</b> to confirm any changes, but remain in the <b>Advanced PBA Configuration</b> dialog.
OK	Click <b>OK</b> to confirm any changes and return to the PBA logon dialog.

## Changing keyboard layout

This feature enables a user to change the keyboard layout while still in the PBA – without the need for authentication.

1. To open the keyboard layout dialog, press the Ctrl+F9 key while still in the PBA logon dialog.
  - The **Keyboard layouts** dialog appears:



The following options are available:

Option	Details
Keyboard layouts	Check this option before clicking <b>Apply</b> or <b>OK</b> to permanently save any changes you make to the PBA. If you do not check this option, any changes you make will apply only to this session.
Test [field]	Click <b>Cancel</b> to return to the PBA logon dialog.
Save options permanently to disk	Check this option before clicking Apply or OK to permanently save any changes you make to the PBA. If you do not check this option, any changes you make will apply only to this session.
Cancel	Click <b>Cancel</b> to return to the PBA logon dialog.
Apply	Click <b>Apply</b> to confirm any changes, but remain in the <b>Advanced PBA Configuration</b> dialog.
OK	Click <b>OK</b> to confirm any changes and return to the PBA logon dialog.

## Operating system boot selection

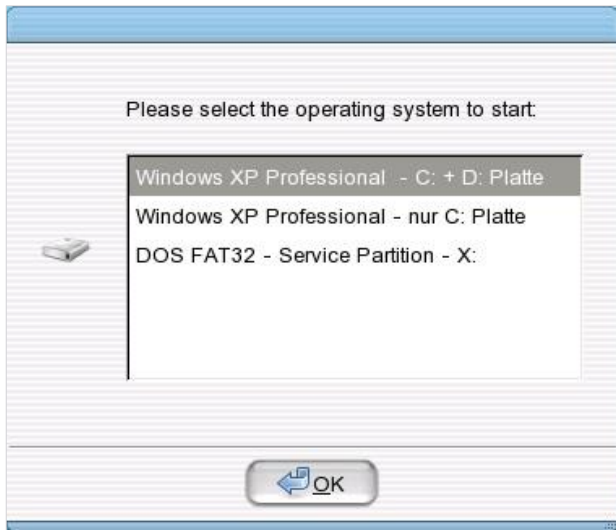
This section details how to select the operating system to boot via the PBA.

This feature enables a user to boot the operating system (on selected partition) while still in the PBA – without the need for authentication.

1. Perform the steps described in chapter 4 "[The Integrated Boot Manager](#)".

To open the **Operating System Boot Selection** dialog, press the F8 key while still in the PBA logon dialog.

→ The Operating System Boot Selection dialog appears:



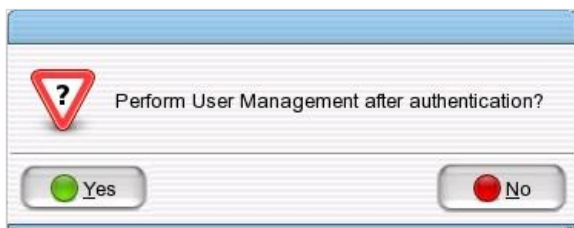
Select the operating system in specific partition to boot, and click **OK**.

## PBA user management

This section details how to perform User Management via the PBA. An admin user is allowed to add a new user, promote as well as delete an existing PBA user(s).

A new user will be captured during his/her logon to the computer as a registered user. Only user who has User Admin rights will be able to perform User Management.

1. To perform User Management, press the F7 key while still in the PBA logon dialog.
  - A confirmation message to perform User Management appears after authentication:



2. Click **Yes** to perform User Management, or **No** to exit the dialog.

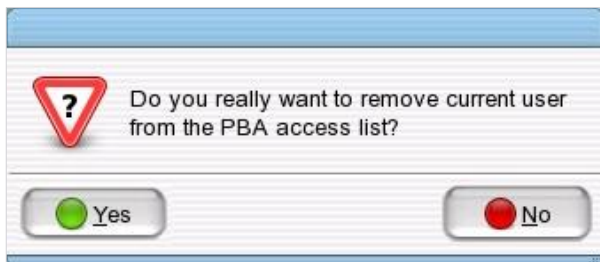
→ The **PBA logon** dialog re-appears.

Enter your Windows credentials (username, password, and domain) to login.

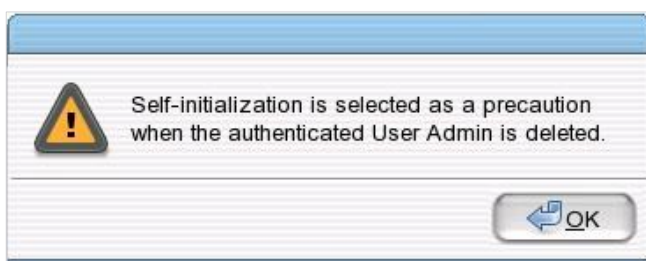
→ After successful login, the **User Management** dialog appears. The **Registered Users** tab lists all the existing users in the PBA access control list.



3. Select a user, and click **Promote** to promote the user as a User Admin in the PBA access list. The selected user will be promoted as an Admin in the PBA access list.
4. If you want to delete the current logged-in user, click **Delete** in the **PBA access control list**.



5. Click **Yes**.  
→ The following message appears:



6. Click **OK**.

7. Click **Enable self-initialization and register the next user to logon** option to capture the next user who logon to the computer to be self-initialized as a valid user.

→ On selecting this option, the other two options get enabled.



- Select **Perform user registration with a Smart Card** option to register the captured user with Smart Card authentication.
- Select **Grant User Admin privileges to the next user registered** option to register the captured user with User Admin privileges.

8. Click **OK** to save.

- If a normal PBA user tries to perform User Management, the following message appears. Click **Continue** to proceed with the logon process. The User Management dialog will not appear after successful logon.



## 1.5. The Control Center

The EgoSecure Full Disk Encryption Control Center is the central point of configuration and administration for EgoSecure Full Disk Encryption. The modules cover all aspects of administration and configuration. Once EgoSecure Full Disk Encryption is configured and running, there should be little need to use the Control Center.

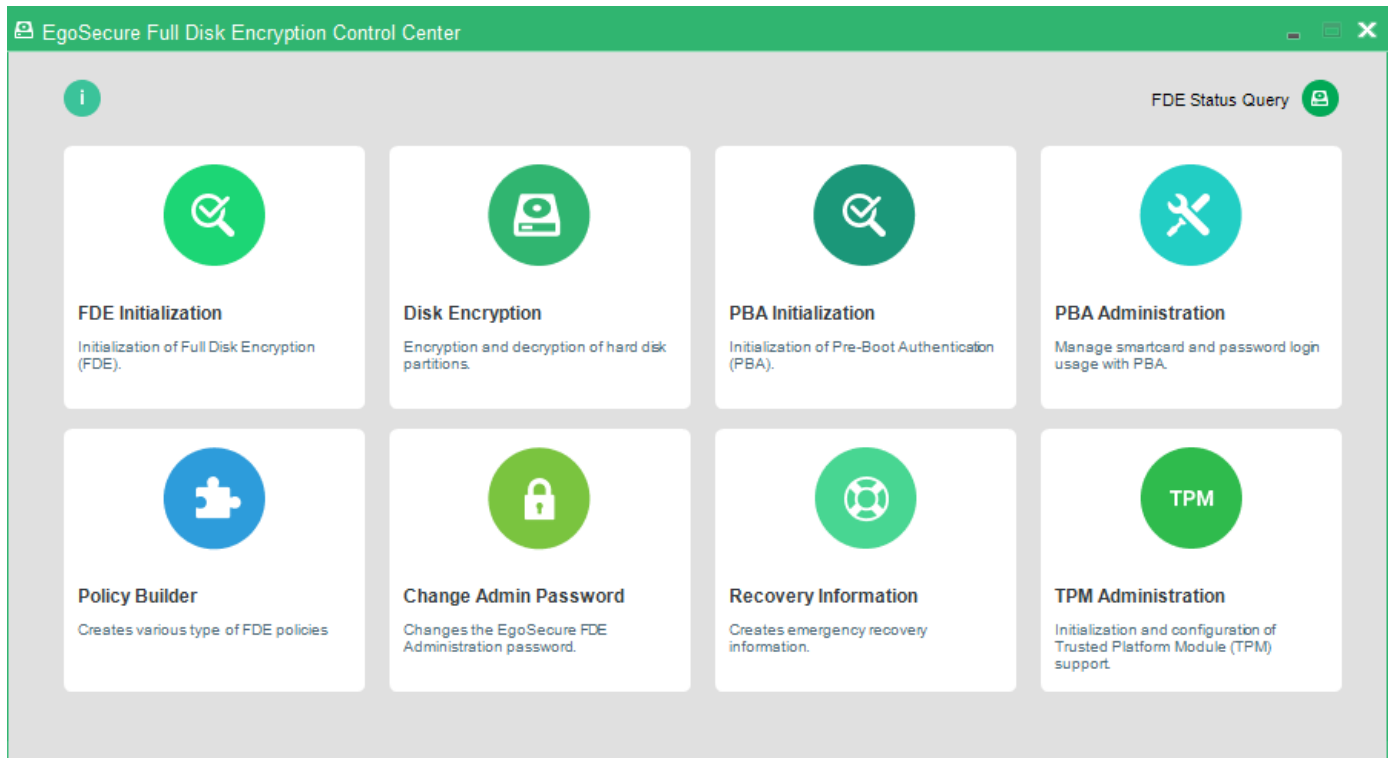
The FDE Control Center can be opened via the Windows control panel as follows:

1. Open the Windows Control Panel:

2. Double-click the EgoSecure Full Disk Encryption control center icon:



→ The Control Center window appears:



The modules have the following functions:

Option	Details
FDE Initialization	This module is used for the administration, installation, and removal of boot security. Boot security is necessary for PBA and is also a prerequisite for the encryption of any hard disk partition. For details about FDE Initialization module, see <a href="#">FDE Initialization - Boot Security</a> .
Disk Encryption	This module is used to configure the encryption of hard disk partitions.
PBA Initialization/De-initialization	This module is used to enable and disable the PBA component. Click <a href="#">PBA Initialization/De-initialization</a> for details.
PBA Administration	This module allows you to alter the PBA configuration. For example, to add an authorized user to PBA, or change the smart card provider. For details, see <a href="#">PBA Administration</a> .
Policy Builder	This tool is used to create and edit policies for the purpose of configuration, initialization, and de-initialization of FDE and PBA components. The purpose of these policies is to allow for an administrator to remotely control and ensure the consistent, central deployment, and configuration of FDE and PBA with no need for user interaction.
Change Admin Password	This module is used to change the administration password. For details, see <a href="#">Changing the Administration Password</a> .
Recovery Information	This module is used to create ERI files and ERD, which in turn can be used to repair or decrypt a damaged system.
TPM Administration	This module offers you a way to utilize and bind the TPM chip on the most business computer motherboards to EgoSecure Full Disk Encryption.
FDE Status Query	This option gives you a simple overview of the system. For details, see chapter <a href="#">1.10</a> .



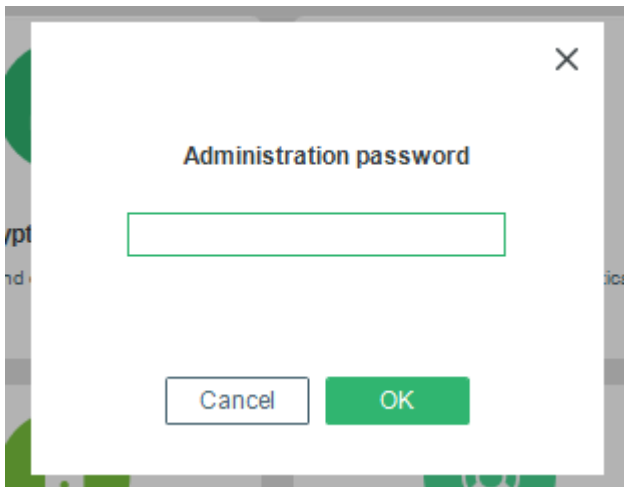
## 1.6. PBA Administration

Use the Control Center module PBA Administration to configure, re-configure, and administrate the PBA component of EgoSecure Full Disk Encryption.

### Modifying PBA

1. If you have not already done so, open the Control Center (as described in Section [1.5](#)).
2. Double-click the **PBA Administration** icon.

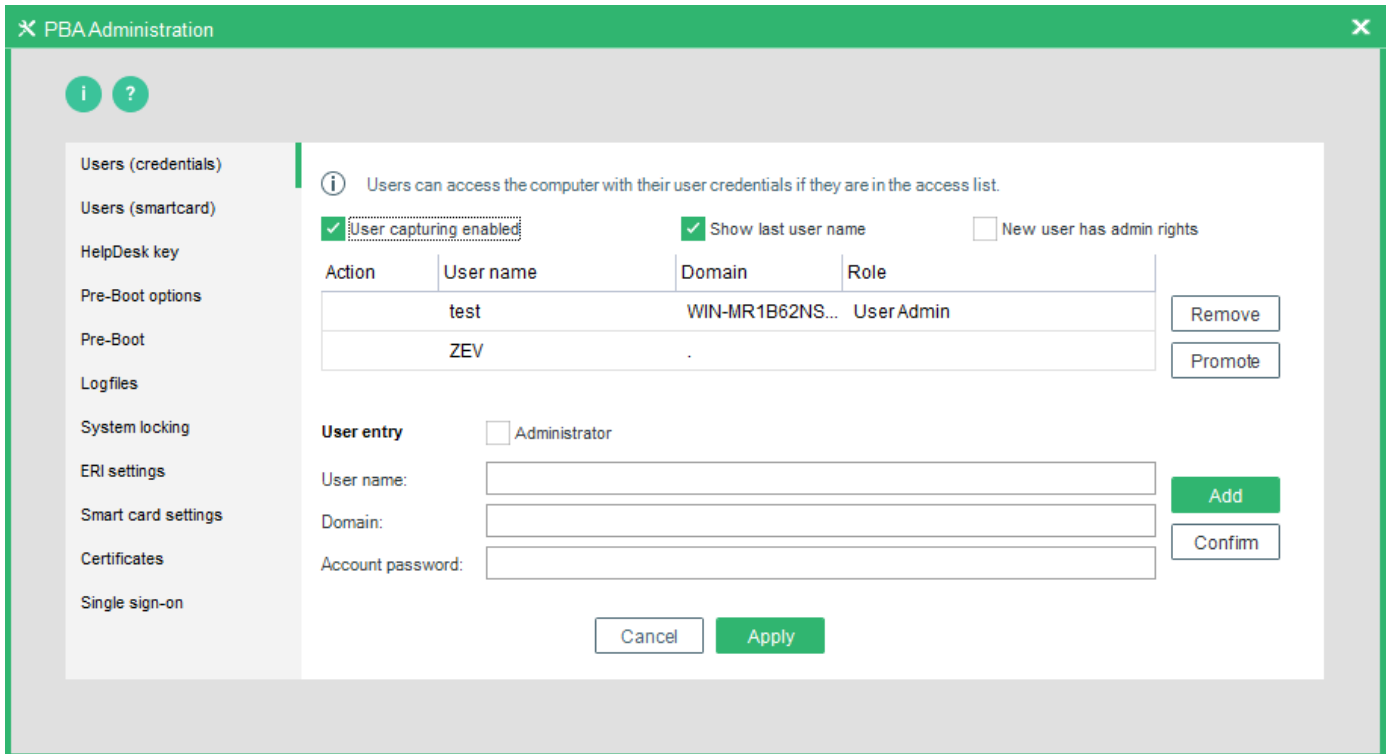
→ The Administration password dialog appears:



3. Enter the password and click **OK**.

→ The **PBA Administration** dialog appears (Figure 8):

Figure 8. PBA Administration Window



The options available in each of the tabs above have already been configured during installation. The descriptions for each tab/option can therefore be found in the relevant step in the installation chapter (refer to [Related information](#) below).

### Related information

Refer to the following sections for further information about the options available for configuration in each of the tabs above:

Option	Details
Users (credentials)	This tab allows you to configure which users are allowed to login to PBA using their Windows credentials. If the options are greyed-out, you must uncheck the option <b>Disable PBA</b> in the <b>Pre-boot options</b> tab (and click <b>Apply</b> ) before setting this. The password for PBA must be no longer than 32 symbols. <b>User name</b> must not contain any of the following characters: / \ [ ] " : ;   < > + = , ? * % @
Users (smartcard)	This tab allows you to configure which smart card user is allowed to authenticate to PBA. If the options are greyed-out, you must uncheck the option <b>Disable PBA</b> in the <b>Pre-boot options</b> tab. For further information, refer to <a href="#">EgoSecure FDE – Installation and Troubleshooting Guide</a> .
HelpDesk key	This tab allows you to configure the HelpDesk keys used for communication with a HelpDesk administrator in an emergency scenario. Once the HelpDesk is configured, you can activate Friendly Network. For details about Friendly Network, see <a href="#">EgoSecure FDE – Installation and Troubleshooting Guide</a> .

Pre-Boot options	<p>This tab allows you to configure user interface options in the PBA such as PIN reset for smart cards, disabling switching between authentication methods, specifying screen resolution, etc.</p> <p>You can also configure the following options:</p> <ul style="list-style-type: none"> <li>■ <i>Disable PBA</i>: temporarily deactivate PBA so that the computer can be rebooted without the need for authentication in the PBA. This can be permanent or configurable for 'n' reboots.</li> <li>■ <i>Reenable PBA after 'n' reboots</i>: use this option together with <i>Disable PBA</i> to allow the user/admin to reboot the computer a specific number of times before the PBA is automatically re-enabled.</li> <li>■ <i>Power off PBA after 'n' seconds</i>: set whether the PBA should power off the computer if the PBA is left unattended for a configurable number of seconds.</li> </ul> <p>For details about all options, see <a href="#">EgoSecure FDE – Installation and Troubleshooting Guide</a>.</p>
Pre-Boot	This tab allows you to configure the background image, keyboard layout, and Integrity checking used in PBA.
Logfiles	This tab allows you to configure if the PBA should generate log files and if so, the size, filename, and location of the log files.
System locking	This tab allows you to configure how many times a user may enter a password incorrectly before being either locked out, or penalized by a time penalty. This locking feature is applicable only to user name/password authentication and not applicable for smartcard PIN.
ERI settings	This tab allows you to configure whether the password used to protect ERI files should be used, and if it is used, the minimum number of characters the password should have. If the options are greyed-out, you must uncheck the option <b>Disable PBA</b> in the <b>Pre-boot options</b> tab (and click <b>Apply</b> ) before setting this.
Smart card settings	This tab allows you to configure which smart card reader and PKCS#11 provider <i>EgoSecure Full Disk Encryption</i> should use for authentication. For further information, refer to <a href="#">EgoSecure FDE – Installation and Troubleshooting Guide</a> .
Certificates	This tab allows you to configure the methods of certificate recognition that are to be used for authentication.
Single sign-on	This tab allows you to configure which SSO mechanism <i>EgoSecure Full Disk Encryption</i> is to use. If the options are greyed-out, you must uncheck the option <b>Disable PBA</b> in the <b>Pre-boot options</b> tab. For further information, refer to <a href="#">EgoSecure FDE – Installation and Troubleshooting Guide</a> .
Perform configuration	This tab automatically appears (or is switched to) when you click <b>Apply</b> to transfer any settings to the PBA component. It only displays the status of the data transfer.

If you temporarily disable PBA, no configuration can be performed during this time. If you want to configure the PBA, reactivate it.

If you intend to make configuration changes to PBA and also disable it then this must be done in two steps:

- Make any configuration changes to PBA (and click Apply)

- Disable PBA (and click Apply)

Or if the PBA is already deactivated...

- Reenable PBA (and click Apply)
- Make any configuration changes (and click Apply)
- Disable PBA (and click Apply)

Once you have made your selection, click **Apply** to transfer them to the PBA component. The new settings will be available at the next restart. Click **OK** to close the PBA administration dialog.

## 1.7. PBA Initialization/De-initialization

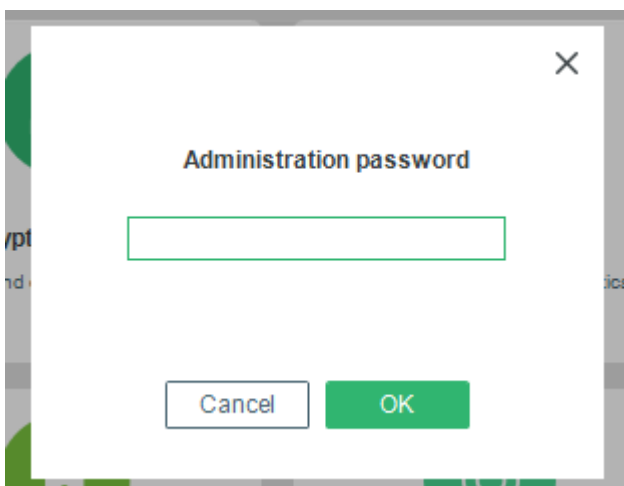
Use the **PBA Initialization** Control Center module to initialize, or de-initialize the PBA component. Use this module in one of the following scenarios:

- You have installed the FDE and PBA components, but you have not yet initialized the PBA component (task ->enable PBA, refer to the table below).
- You have disabled PBA to perform other administration tasks, and you now want to re-enable it (task ->re-enable PBA, refer to the table below).
- You simply want to disable the PBA (task ->de-initialize PBA, refer to the table below).

Follow these steps to de-initialize PBA (the de-initialization screens appear only if you have already initialized the PBA):

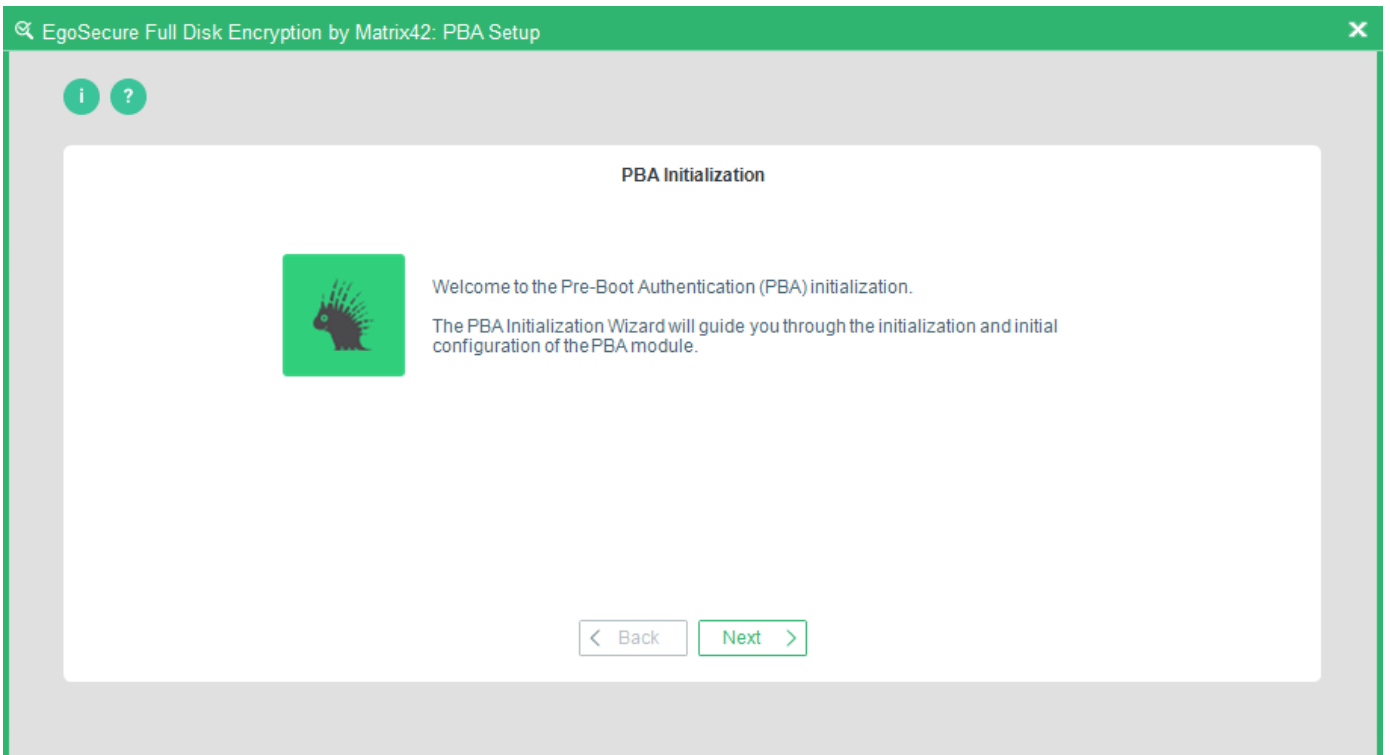
1. Open the **Control Center** (as described in Section 1.5).
2. Double-click the **PBA Initialization** icon.

→ The **Administration password** dialog appears:



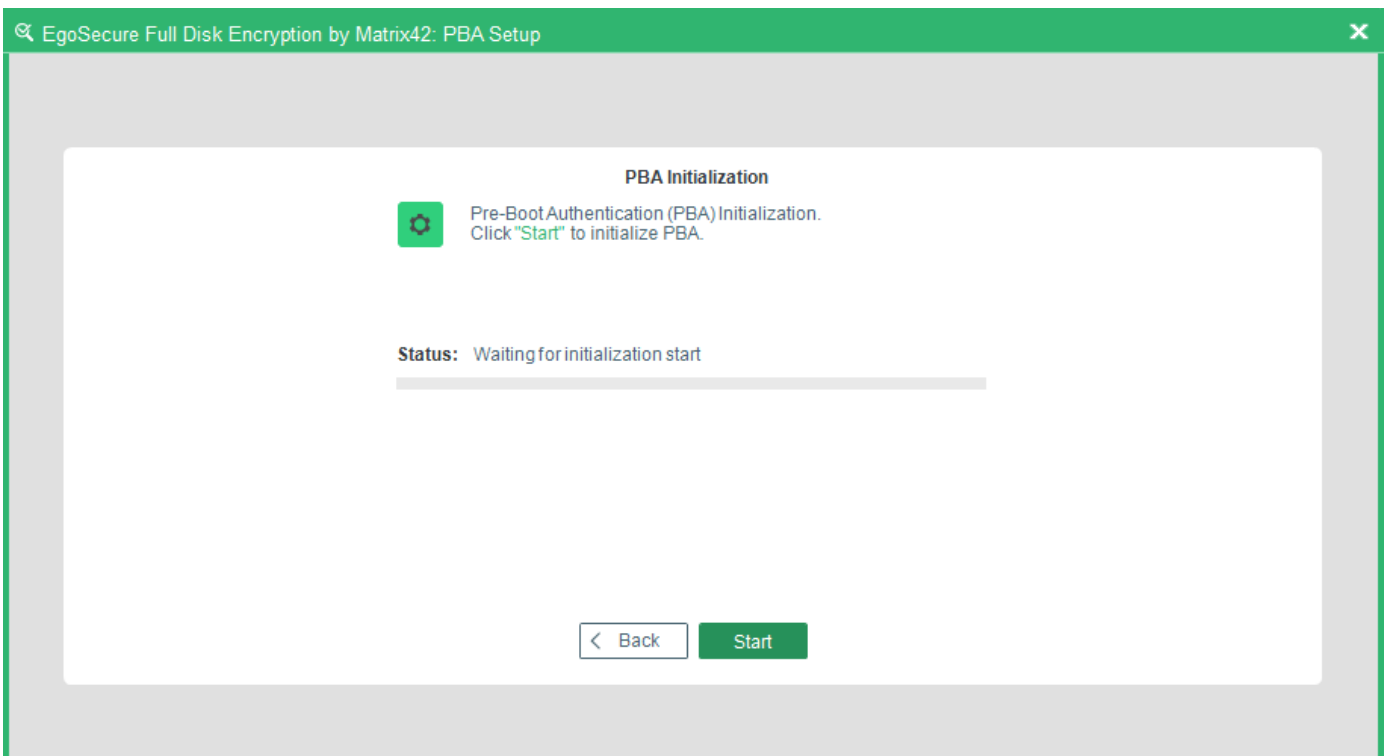
3. Enter the password, and click **OK**.

→ The **PBA Initialization/PBA Deinitialization** dialog appears.



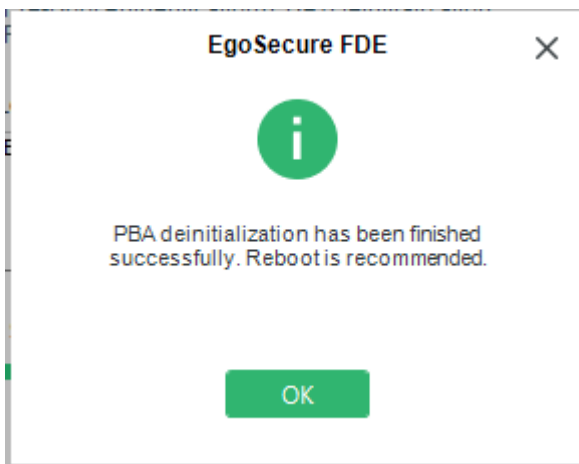
4. Click **Next** to continue.

→ The PBA Initialization Status/PBA Deinitialization Status dialog appears.



5. Click **Start**. The initialization/deinitialization may take a while so please be patient.

→ If the initialization/deinitialization is successful, the following dialog appears:



6. Click **OK** to close the dialog and finish the procedure.

## 1.8. FDE Initialization - Boot Security

This section contains tasks related to boot security.

### CONTENTS

- ◆ [Installing boot security](#)
- ◆ [Updating boot security configuration](#)
- ◆ [Removing boot security](#)

### Installing boot security

Normally, the boot security installation is performed as a part of the initial product installation. Installing boot security is available in the following scenarios:

- Boot security has been disabled and must be re-enabled.
- Boot security was not enabled during the installation.

Follow the steps below to initialize boot security:

1. Open the Control Center (as described in Section [1.5](#)).
2. Double-click the **FDE Initialization** icon.

→ The **Welcome** dialog appears:

Read about the steps of FDE initialization in the [EgoSecure FDE – Installation and Troubleshooting Guide](#), description “Installing Boot Security”.



#### INFO

#### Boot security was previously installed

If boot security was previously installed on the computer, it is possible that the EgoSecure Full Disk Encryption partition already exists. If so, the partition will be reused (this is quite quick as no new partition must be created).



## ATTENTION

### Computer restart required

The computer needs to be restarted after the installation and before any hard disk partition can be encrypted. If you click No, do not forget to restart the computer before you try to encrypt a hard disk partition!

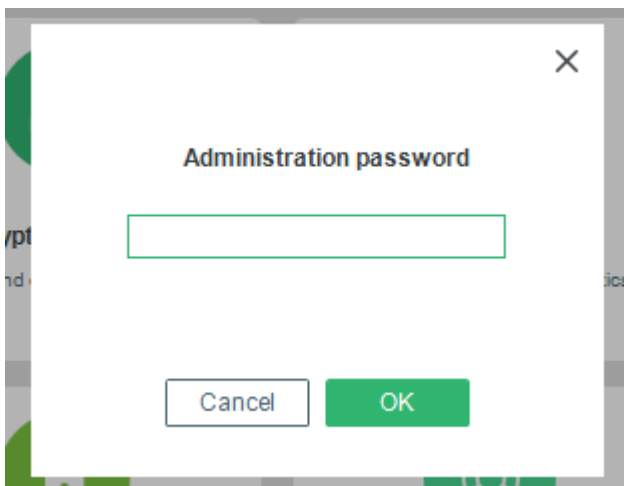
## Updating boot security configuration

This section details how to make changes to the configuration of EgoSecure Full Disk Encryption boot security. Boot security settings can be updated via the Control Center. This function does not update the EgoSecure Full Disk Encryption on your computer.

Follow the steps below to update a boot security configuration:

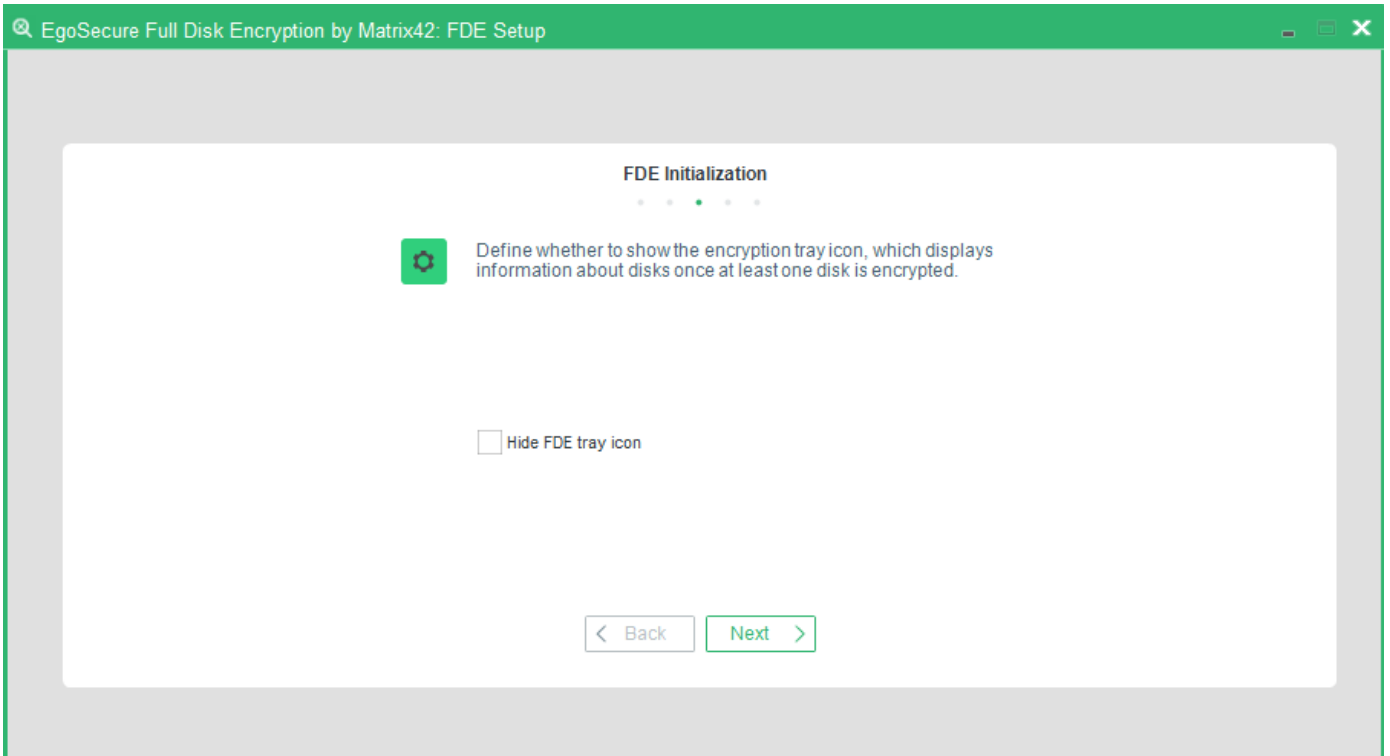
1. Open the **Control Center** (as described in Section [1.5](#)).
2. Double-click the **FDE Initialization** icon.

→ The Administration password dialog appears.



3. Enter the password and click **OK**.

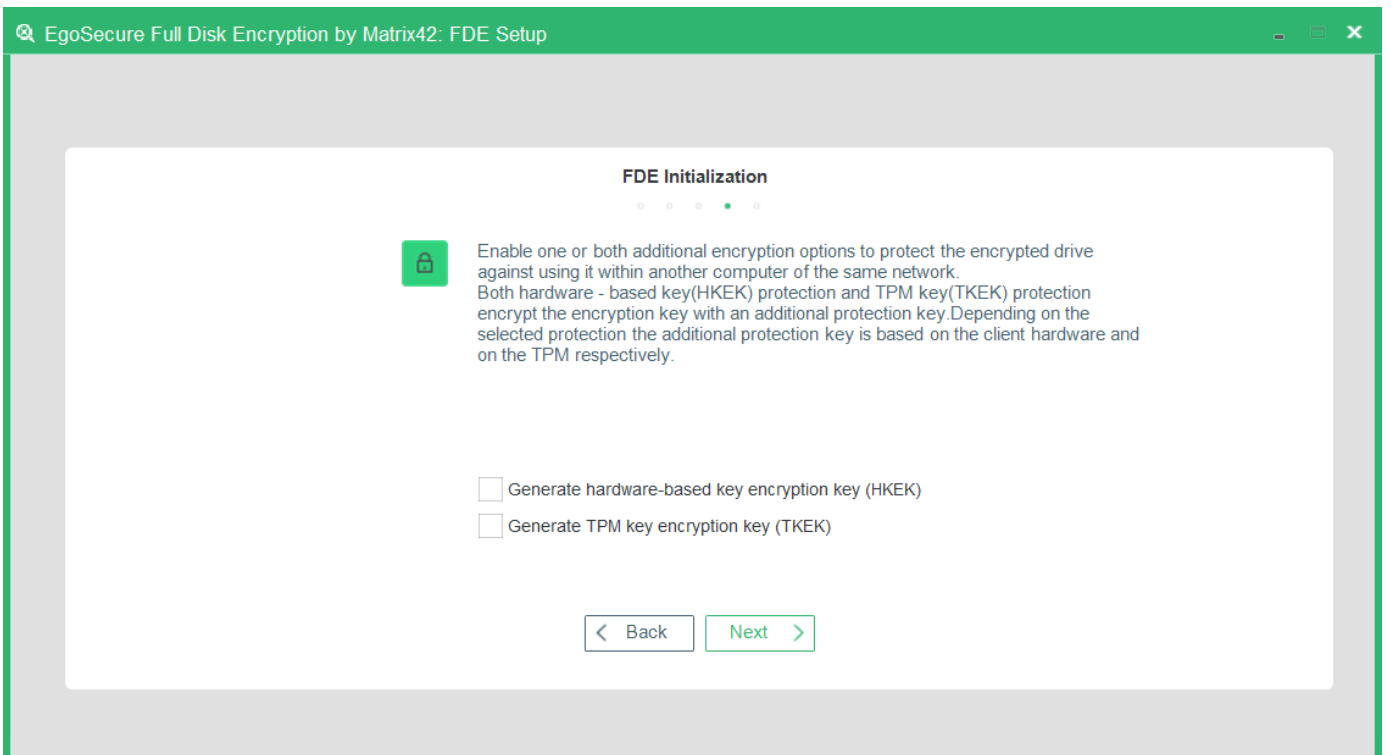
→ The step for hiding encryption tray appears.



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.

4. 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.

## 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.



### ATTENTION

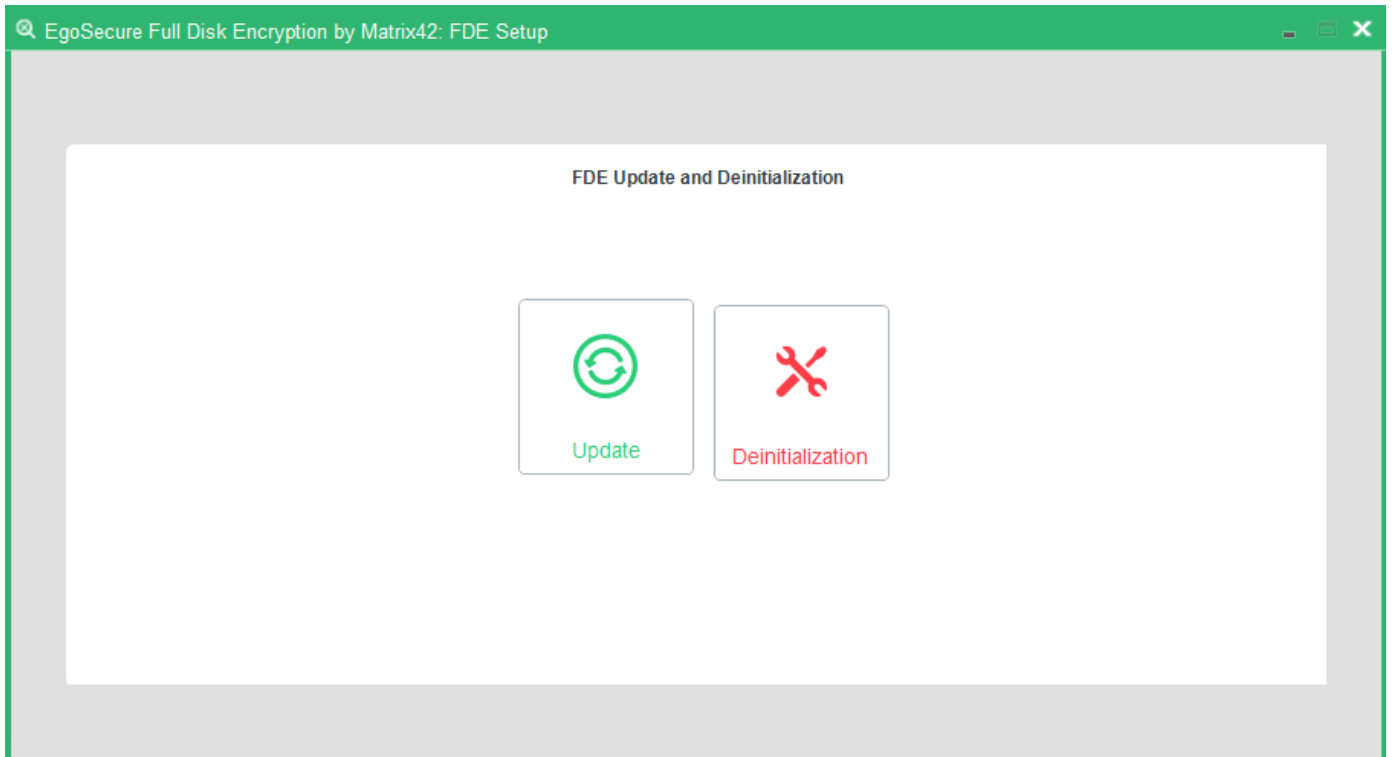
#### Before updating BIOS or replacing hardware

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.

4. Enable the **Generate hardware-based key encryption key (HKEK)** option and/or **Generate TPM-based key encryption key (TKEK)**, and then click **Next**.

→ The **FDE Update and Deinitialization** dialog appears.



5. Click **Update**.
6. Close the dialog once the update finishes.

### Removing boot security

This section details how to remove EgoSecure Full Disk Encryption boot security. Boot security can be re-installed via the Control Center. This function does not remove the EgoSecure Full Disk Encryption from your computer.



#### ATTENTION

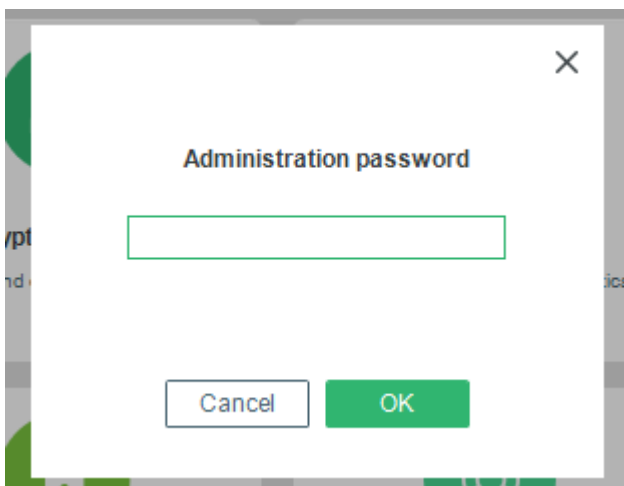
#### Decrypt the drives

If one or more drives are encrypted, you have to decrypt them before you can remove the boot security.

Follow the steps below to remove boot security:

1. Open the **Control Center** (as described in Section [1.5](#)).
2. Double-click the **FDE Initialization** icon.

→ The **Administration password** dialog appears.

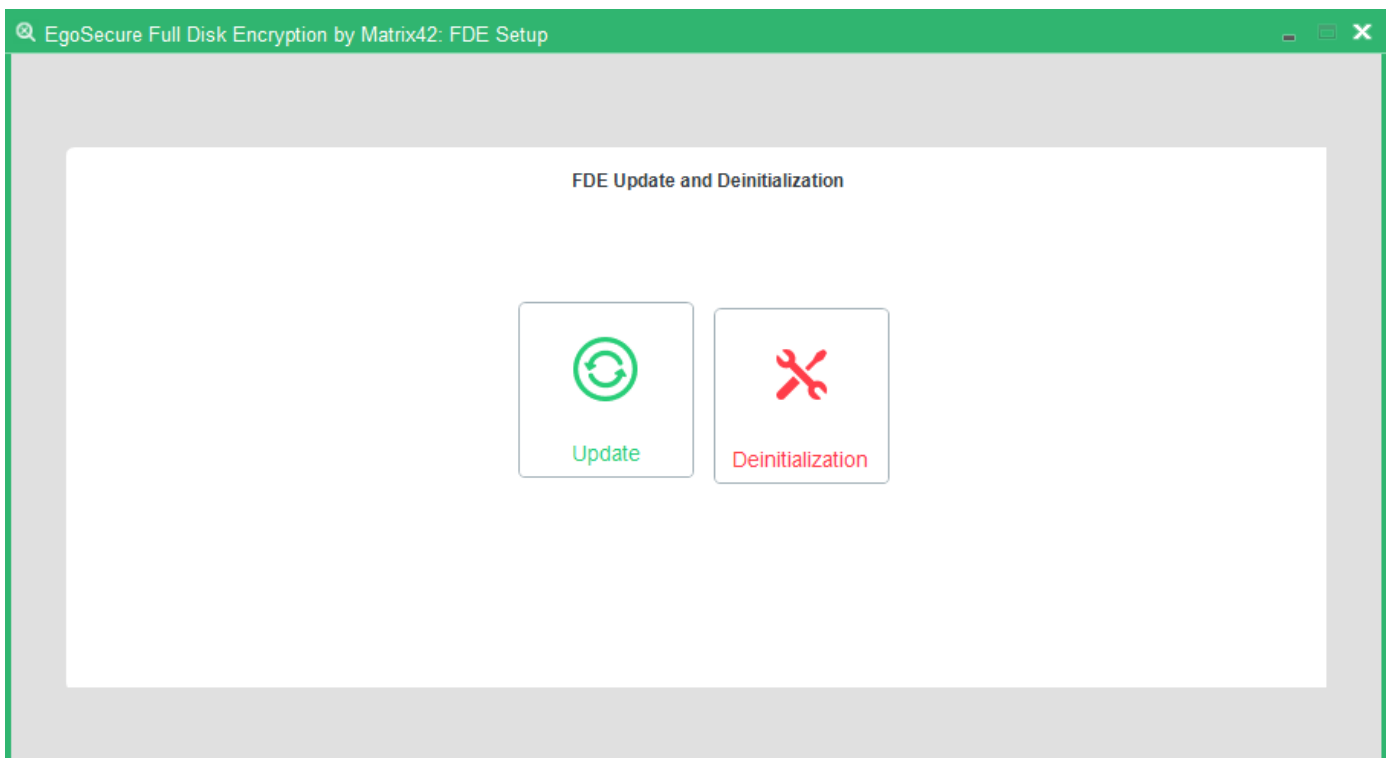


3. Enter the password and click **OK**.

→ The two steps for configuring additional protection for disk encryption key and hiding encryption tray appear.

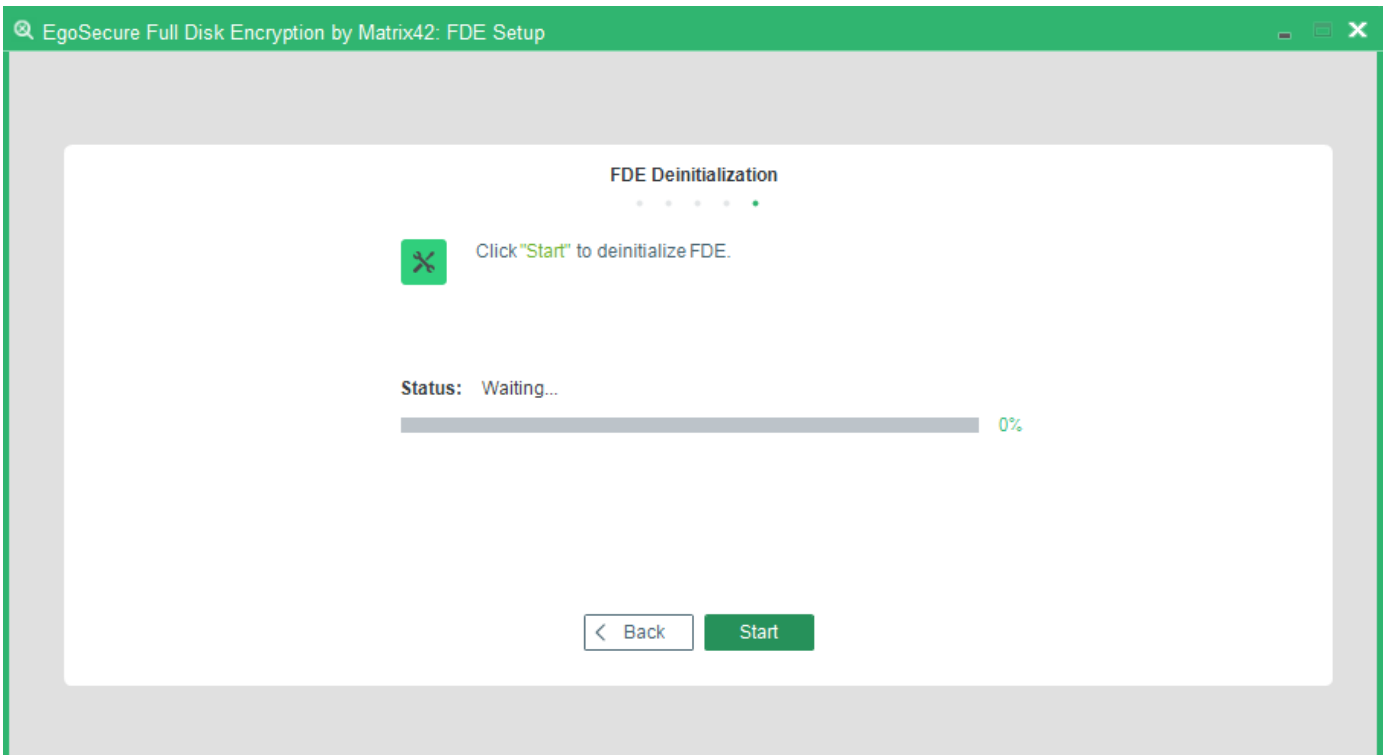
4. Skip them via clicking **Next**.

→ The **FDE Update and Deinitialization** dialog appears.



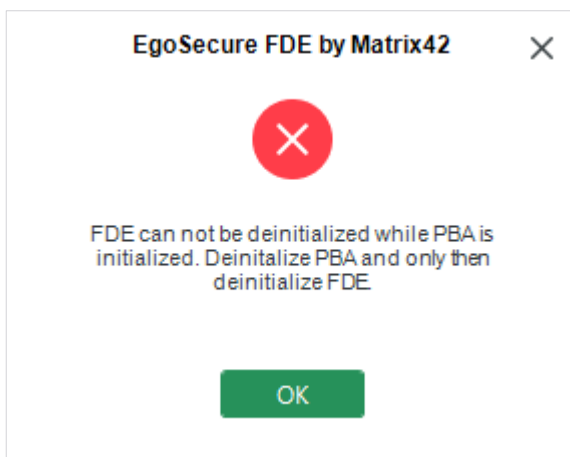
5. Click **Deinitialization**.

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



6. Click **Start**.

**Note:** If PBA is still installed, you will end up with the following warning message:



→ Upon successful removal the success dialog appears.

7. Click **OK** to close the dialog.

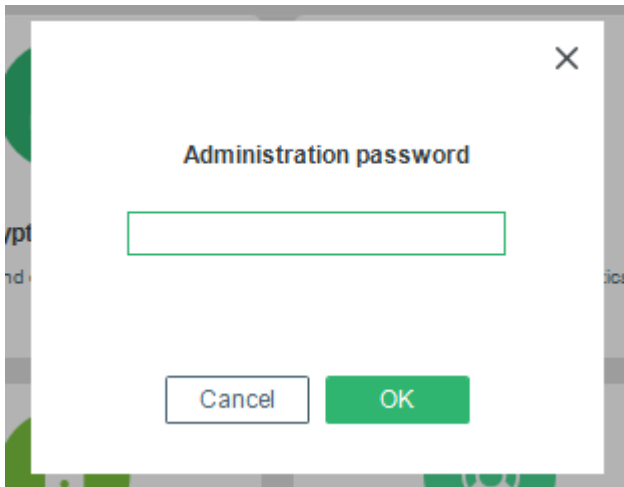
## 1.9. Changing the Administration Password

Use the **Change Admin Password** module of the Control Center to change the global password used to configure any EgoSecure Full Disk Encryption setting. Follow these steps to modify the administration password:

1. Open the **Control Center** (as described in Section [1.5](#)).

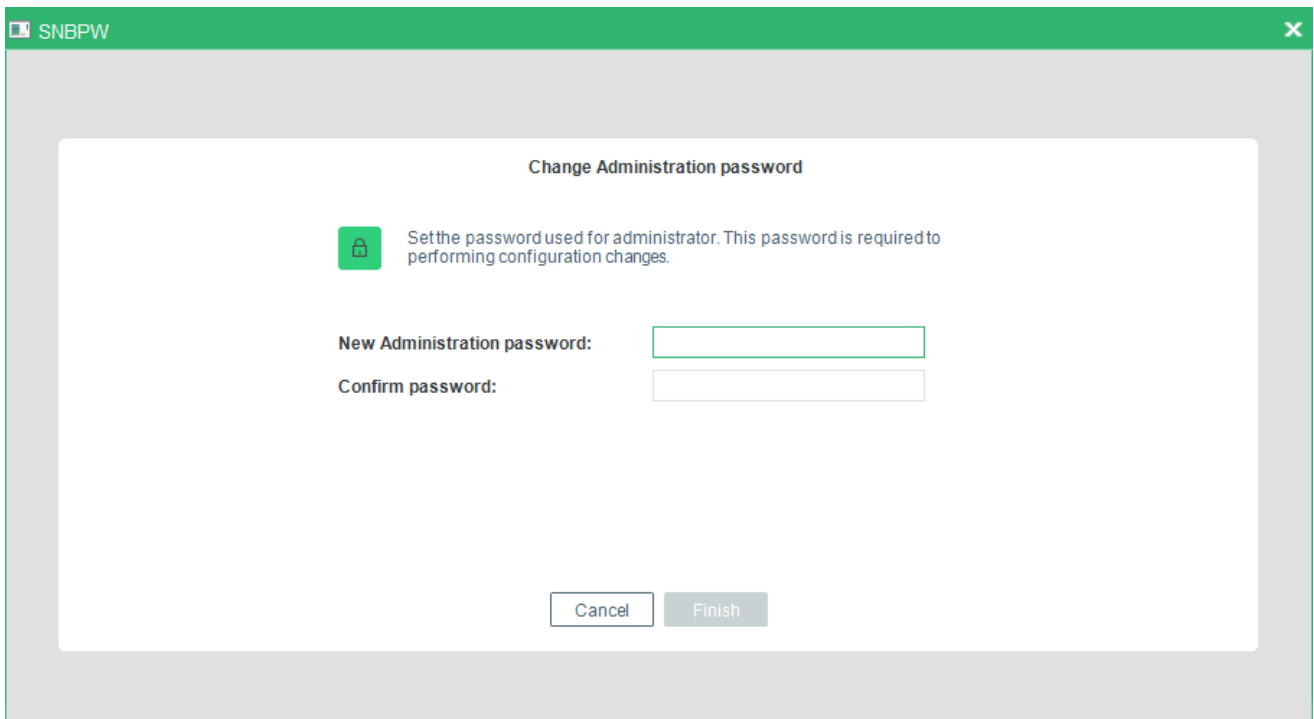
2. Double-click the **Change administration password** icon.

→ The **Administration password** dialog appears.



3. Enter the current administration password and click **OK**.

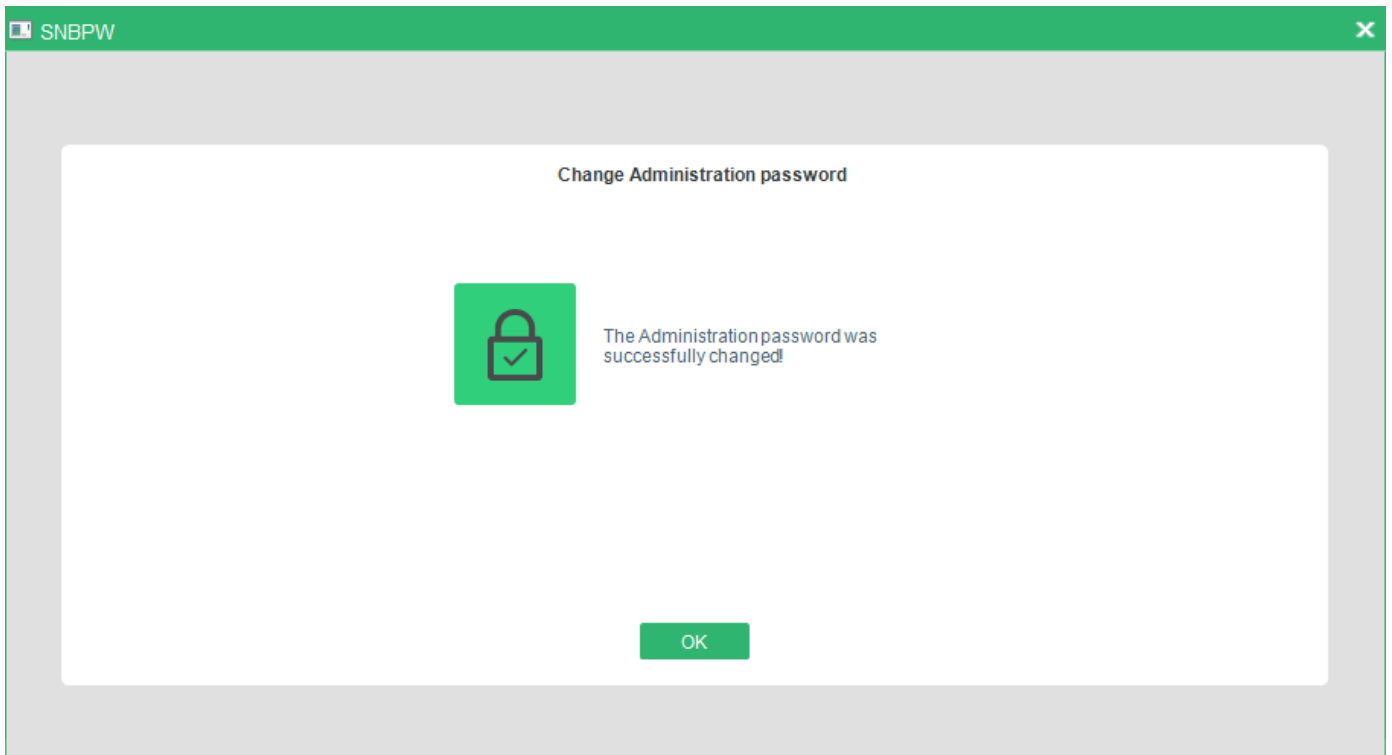
→ The **Change Administration Password** dialog appears.



4. Enter and confirm the new password in the fields **New Administration Password**, and **Confirm Password** respectively.

5. Click **Finish** to apply the new password for EgoSecure Full Disk Encryption administration.

→ The **Success** dialog appears.



6. Click **OK**.



**INFO**

**Taking care of the administration password**

Once running, FDE rarely needs any administrative action. It is logical to assume that the administration password is not used very often and could therefore be easily forgotten. Once you have changed the password, it is recommended to keep a copy of it in a safe place.

## 1.10. FDE Status Query

Use the **FDE status query** module of the Control Center to identify the status of a hard disk protected by the EgoSecure Full Disk Encryption. The following information can be identified:

- Status of the installation
- Status of the boot protection
- Encryption status of the drives

This module can also be used transparently by administrators to log (and consequently audit) the status of the EgoSecure Full Disk Encryption.

**CONTENTS**

- ◆ [The FDE status query GUI](#)
- ◆ [Start a status query via the commandline](#)
- ◆ [FDE query log file](#)

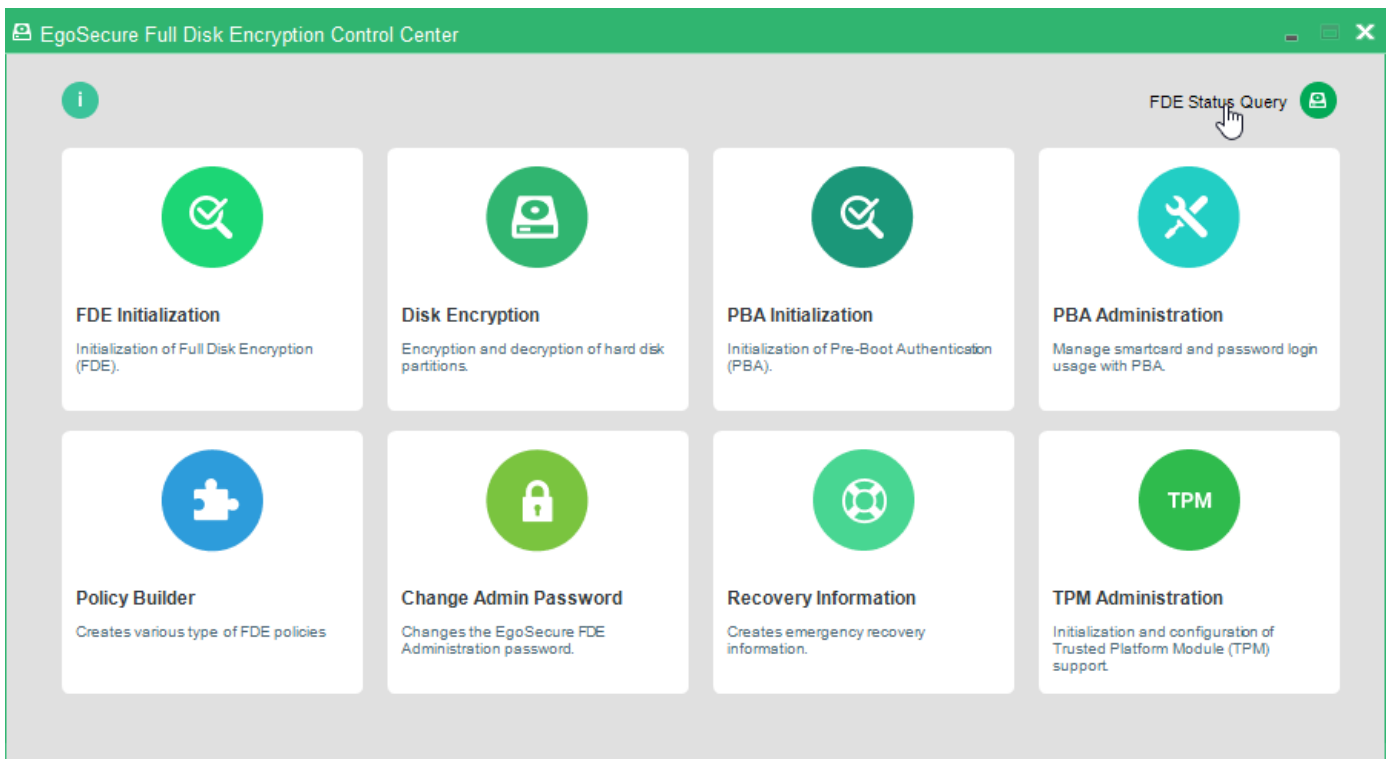
## The FDE status query GUI

The FDE status query GUI is an easy and quick way to view information about the status of the local EgoSecure Full Disk Encryption installation.

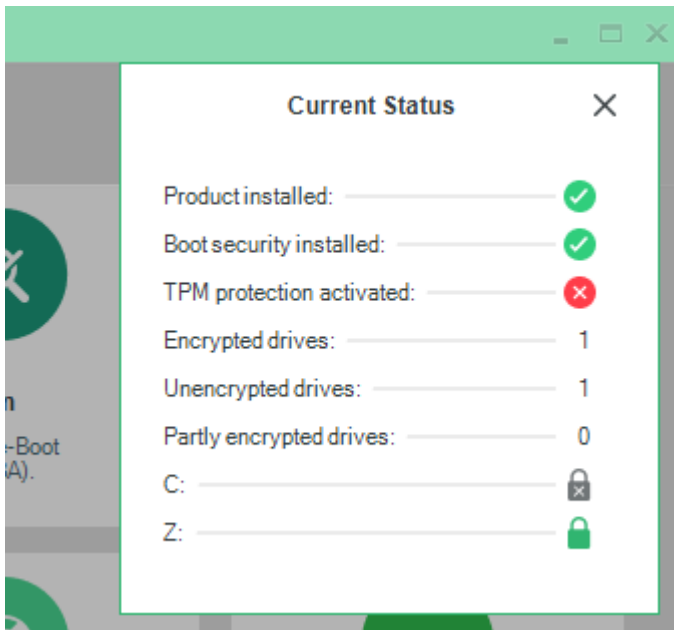
Every time the FDE Status Query application is started, it will generate an entry in the log file NBSTATUS.LOG, by default located directly under the C: drive. The name and location of the log file can be changed (see [FDE query log file](#)).

Follow the steps below to query the status of the EgoSecure Full Disk Encryption installation on your computer:

1. Open the Control Center (as described in section 1.5).
2. Double-click the **FDE Status Query** icon.



→ The following dialog appears:



→ The application automatically gathers and displays information about the EgoSecure Full Disk Encryption installation on your computer. This dialog displays the encryption status of the first six partitions. If there are more than six drives available, the sum of the values is displayed.






The dialog displays the following FDE characteristics:

Characteristic	Details
Product installed	Is EgoSecure Full Disk Encryption installed? <b>NOTE:</b> <i>EgoSecure Full Disk Encryption may be installed but is not yet active.</i>
Boot security installed	Is boot security installed? In other words, is the FDE component active?
TPM Protection activated	Shows the status of the TPM protection for EgoSecure Full Disk Encryption.
Encrypted drives	The total number of encrypted partitions on the hard disk.
Unencrypted drives	The total number of unencrypted partitions on the hard disk.
Partly encrypted drives	The total number of partitions on the hard disk that have only been partly encrypted. This may be due to a loss of power during the encryption of a partition.
Drive (x)	Encryption status for a specific partition: fully encrypted, just used sectors, or unencrypted.

The icons you may encounter in the status dialog have the following meaning:

Icon	Description
	Yes / OK / Active.



	No / Not OK / Not enabled.
	Drive unencrypted.
	Drive encrypted.
	Encryption status of drive cannot be determined.
	Activating or activation error (TPM only).

## Start a status query via the commandline

The commandline functionality for the status query application is primarily for administrators that need frequent information about the status of the EgoSecure Full Disk Encryption installations in the company.

When the commandline syntax is executed, it will generate an entry in the log file NBSTATUS.LOG, by default located directly under the C: drive. The name and location of the log file can be changed (for details, see [FDE query log file](#)).

Follow these steps to start a status query via the commandline:

1. Open a **Command Prompt** window.
  - The **Command** window opens.
2. To start the application, enter the following string in the **Command** window: nbstatus [-NOGUI]

Command line option	Details
-NOGUI	Hide the GUI. The current status is written to the log file and provided as return value. If you do not enter this option, the GUI will be displayed.

**Example.** C:\WINDOWS\NAC\nbstatus -nogui

## FDE query log file

This section details how to interpret the log file entries as well as how to define a log file path.

### Log file interpretation

The Nbstatus application, via GUI or commandline, updates the log file each time it is execution. When opened, a typical log file entry appears as follows:

```
Error status = 0
Driver letter = C
Encrypt status = 0x1
Algorithm:
-----
-----
```

```
Error status = 0
Driver letter = E
Encrypt status = 0x1
Algorithm:
```

```
-----
Computer name: MB-WINXP-02
Date: 20090429
Exit code = 9
FDE installed: Yes
Boot security installed: Yes
Unencrypted drivers = 2
Encrypted drivers = 0
Partly encrypted drivers = 0
Boot security errors = 0
Encrypted errors = 0
-----
```

```
MB-WINXP-02 20090429 9 1 1 2 0 0 0 0
```

The last line of an entry can be broken down into the following:

- Computer name
- Date
- Exit code
- FDE installed
- Boot security installed
- Number of unencrypted partitions
- Number of encrypted partitions
- Number of partly encrypted partitions (process of initial encryption or decryption is ongoing)
- Boot security error code
- Encrypted error code

The listed entries are as follows:

Log file entry	Details
Error Status	0 = Error found 1 = No errors found
Driver letter	Partition/drive letter for which information has been gathered
Encrypt Status	0x0= Status unknown 0x1= Partition is unencrypted 0x2= The whole partition is encrypted 0x3= The encryption of the whole partition is not yet completed 0x4= The decryption of the whole partition is not yet completed 0x102=The used sectors of the partition are encrypted 0x103= The encryption of used sectors on the partition is not yet completed 0x104=The decryption of used sectors on the partition is not yet completed
Algorithm	The algorithm used to encrypt the partition
Computer name	Name of the computer

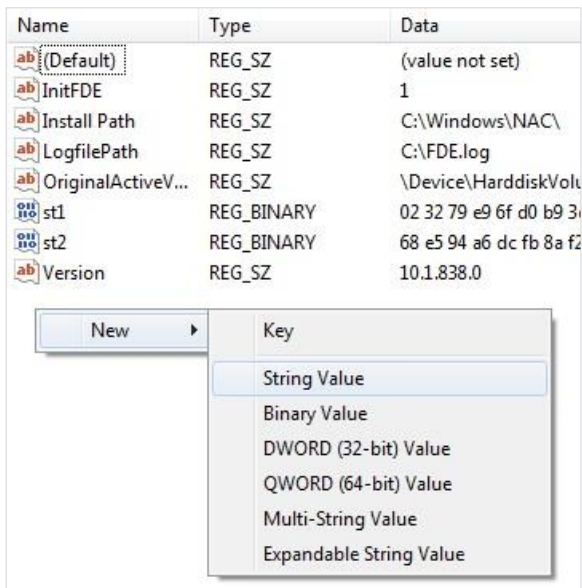
Date	Date on which the status query was run
Exit code	Exit codes have the following meaning: 1 – Unencrypted partitions exist 2 – Encrypted partitions exist 4 – Partly encrypted partitions exist 8 – Boot protection is installed 16 – The encryption status of some partitions could not be obtained 32 – The status of the Boot protection could not be obtained 64 – FDE is not installed  In the example, The value 9 (8+1) has the following meaning: Boot protection is installed + Unencrypted partitions exist The value 11 (8 + 2 + 1) has the following meaning: Boot protection is installed Unencrypted partitions exist Encrypted partitions exist
FDE installed	0= no 1= yes
Boot security installed	0= no 1= yes
Unencrypted drivers	The number of partitions that are unencrypted
Encrypted drives	The number of partitions that are encrypted
Partly encrypted drivers	The number of partitions that are only partly encrypted
Boot security errors	0 = no error
Encrypted errors	0 = no error

### Defining log file path and name

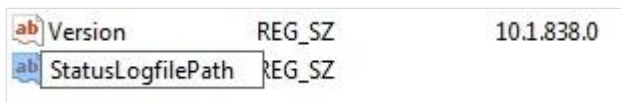
This section details how to tweak the log file location for NBSTATUS.LOG. By default, the log file is written to C:\NBSTATUS.LOG. You may however, want to save the log file to a specific directory.

To specify an alternate log file location:

1. Open the Windows Registry Editor by either selecting Start -> Run and entering regedit into the Open field, or by opening the editor directly from the directory:  
C:\WINDOWS\regedit.exe
2. In the Registry Editor open the entry:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Mobsec\_NB\Notebook\General\
3. Make a new entry by right-clicking the mouse in an open space on the right-hand panel and choose New -> String Value from the menu:

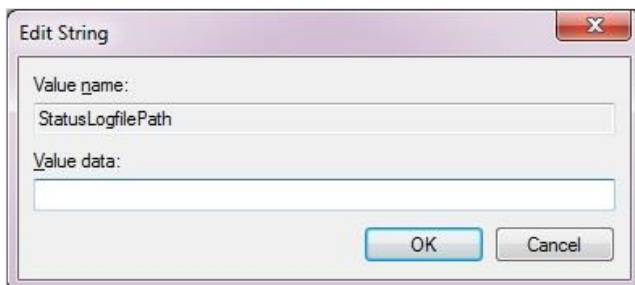


4. Define the string name: *StatusLogfilePath*.



5. Double-click the new entry.

→ The **Edit String** window opens:



6. Enter the path and filename, to which the log file will be saved (for example: C:\EgoSecure Log\nb status log files\), into the **Value Data** field:



7. If you do not want Nbstatus to write a log file, then simply enter NOLOG into the **Value Data** field. Click **OK** to apply the value.

**INFO****Reverting to default log file destination**

If, at any time after you have made this change, you decide to revert to the default log file destination (C:\NBSTATUS.LOG), just delete the entry made in this section from the registry.

## 1.11. Hard Disk Encryption

Encrypting the hard disk ensures that all the data remains secure from unauthorized users. Data on a hard disk encrypted by FDE cannot be hacked via boot CDs, floppy disks, USB devices, or by removing the hard disk completely for installation in another computer. Also, resetting the Windows user or administrator passwords with some well-known tools does not work on hard disks encrypted by EgoSecure Full Disk Encryption.

Encrypted hard disks display information only to authorized users, or to users who have accessed the disk using a password-protected ERI file either via the HelpDesk or via the ERD. The data on an encrypted hard disk cannot be accessed if you do not have EgoSecure Full Disk Encryption installed, or do not know the key.

Once a hard disk has undergone its initial encryption, EgoSecure Full Disk Encryption will automatically encrypt data newly added to the disk on-the-fly. This means that it functions in a completely transparent manner to the user. As an option, each hard disk partition can be encrypted by a different algorithm.

Hard disk encryption applies to IDE, SATA, and SCSI hard disks formatted using the NTFS file system under Windows. Hard disks formatted using the FAT file system are not supported.

You can encrypt a disk either with EgoSecure FDE or with Windows BitLocker. It means that if one disk is encrypted with EgoSecure FDE and another disk is encrypted with BitLocker they will co-exist in one system.

### Algorithms

EgoSecure Full Disk Encryption offers the following range of software FDE encryption algorithms:

Algorithm	Description
Blowfish	A strong, fast, and compact algorithm that supports key lengths of up to 448 bits.
DESX	A widely used cryptosystem and uses a key length of up to 128 bit.
DES	A widely used cryptosystem and uses a key length of up to 56 bit.
AES	Provides the most effective protection using a 256 bit key. <i>The AES (Advanced Encryption Standard) provides the highest security coupled with fast encryption speed. This algorithm is the optimal choice for most users.</i>

If you intend to install the PBA component to raise security to a maximum, then please wait until the PBA component is installed and working BEFORE encrypting the hard disk. The reason for this is that if you were to encrypt before installing PBA it is possible that something in the authentication process may fail, you will be unable to access the computer, and you will be forced to perform an emergency recovery procedure. Such typical causes of failure are incorrect smart card provider or incorrect certificates.

## CONTENTS

- ◆ [Encrypting a hard disk partition](#)
- ◆ [Decrypting a hard disk partition](#)

## Encrypting a hard disk partition

- EgoSecure Full Disk Encryption can only encrypt a hard disk partition if you have local Windows administrator privileges!
- EgoSecure Full Disk Encryption supports the integrated power management mechanisms of Windows 'Suspend to RAM' and 'Suspend to Disk' with enabled, as well as disabled, PBA.
- If your hard disk is already encrypted using a third-party product, please, decrypt it BEFORE re-encryption with EgoSecure Full Disk Encryption.
- You cannot apply hard disk encryption to the following:
  - A remote (network) hard disk
  - A drive that uses software BIOS, for example: EZ-Drive, Drive-Pro or Disk Manager.
- Do not encrypt drives, which are already encrypted! This will result in data loss.
- Do not encrypt system logical drives where the operating system is installed.
- Only the "basic" disk type is supported for the second hard disk (for details about "basic" disk types, see Windows documentation or online help).
- Once the encryption process is started, a valid ERI file is created and cached in the PBA partition. This allows users to recover the partition if anything goes wrong during the encryption process. However, the ERI file presents a security risk. Once the encryption process is complete, you should start the Recovery Information module in the Control Center and save an ERI file to external media or a network drive (this will also remove the cached ERI created at the start of the encryption process).
- Make sure that you close, or stop, applications that perform hard disk intensive operations before you start the INITIAL ENCRYPTION.
- Do not turn off the computer or work on the computer while the initial encryption is in progress. Doing so would result in data corruption.



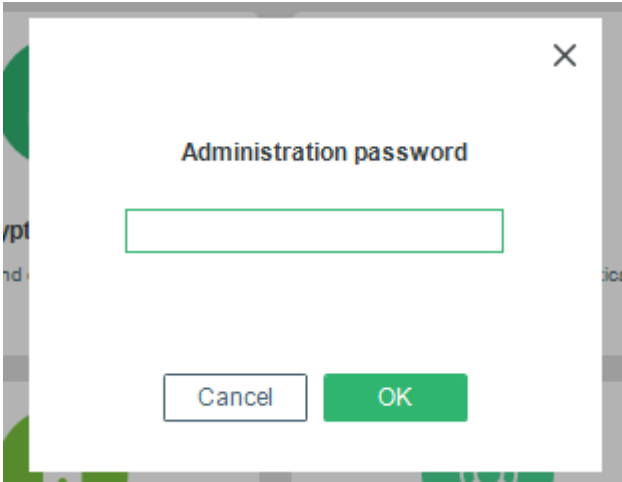
### WARNING

#### Data loss risk

Do NOT modify the encrypted partitions (size change, shrink, etc.). It may lead to data loss.

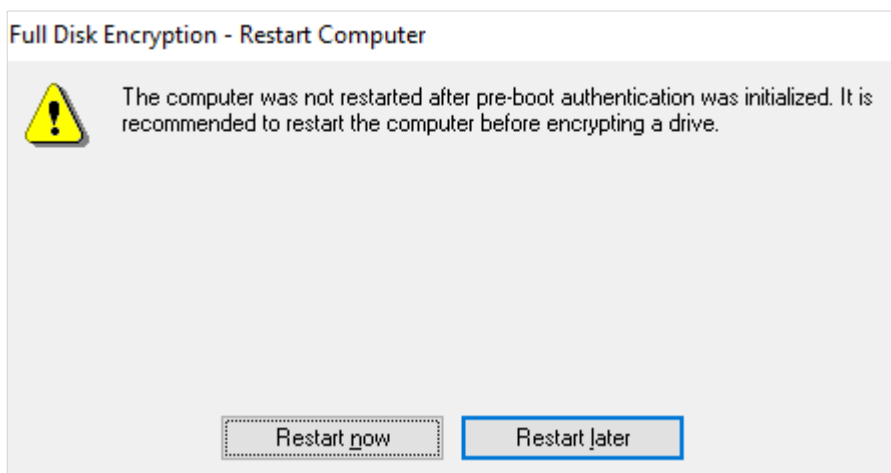
## Encrypting a hard disk partition with FDE

1. Open the Control Center (as described in Section 1.5).
2. Double-click the **Disk Encryption** icon.
  - The Administration password dialog appears.
3. Enter the password and click **OK**.



→ When you try to encrypt the disk before re-starting the system after PBA initialization, a message stating to restart the computer appears.

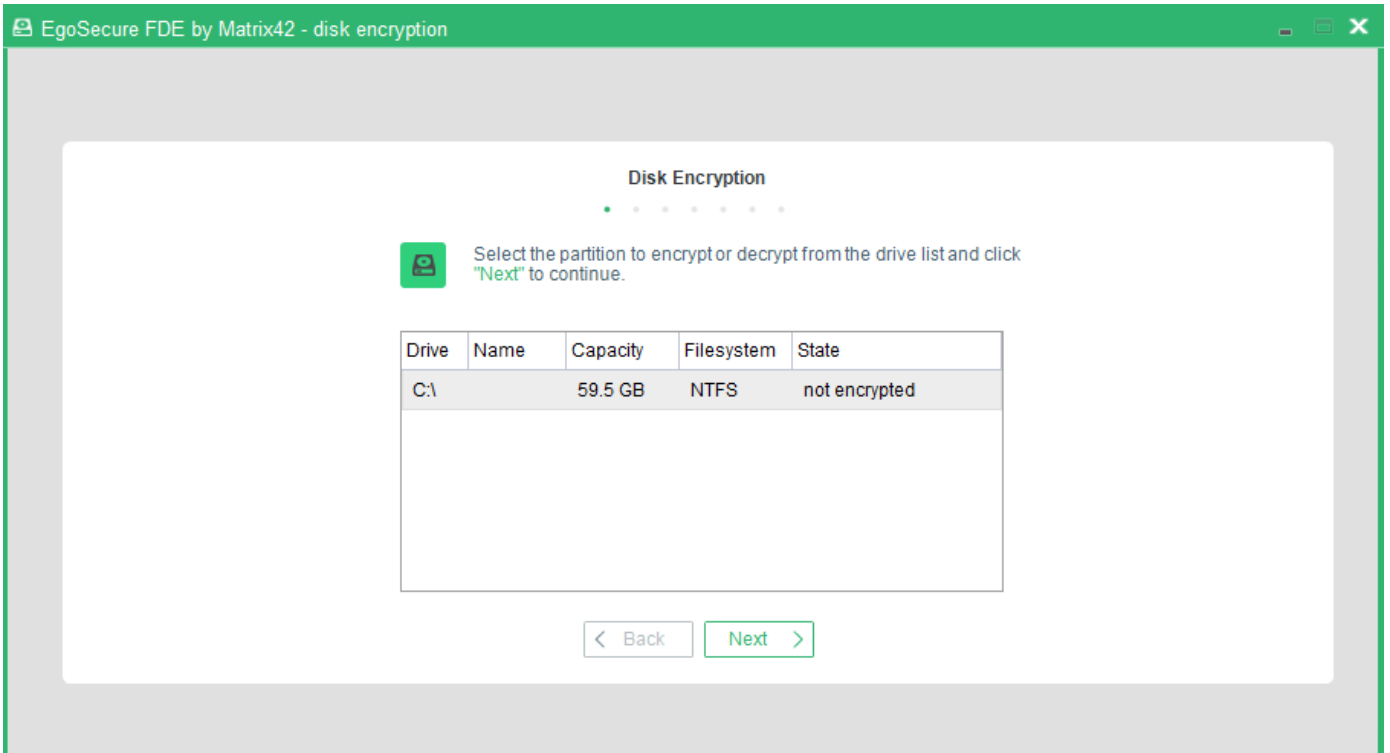
4. (Recommended) Click **Restart now** to restart the system before encrypting the drive.



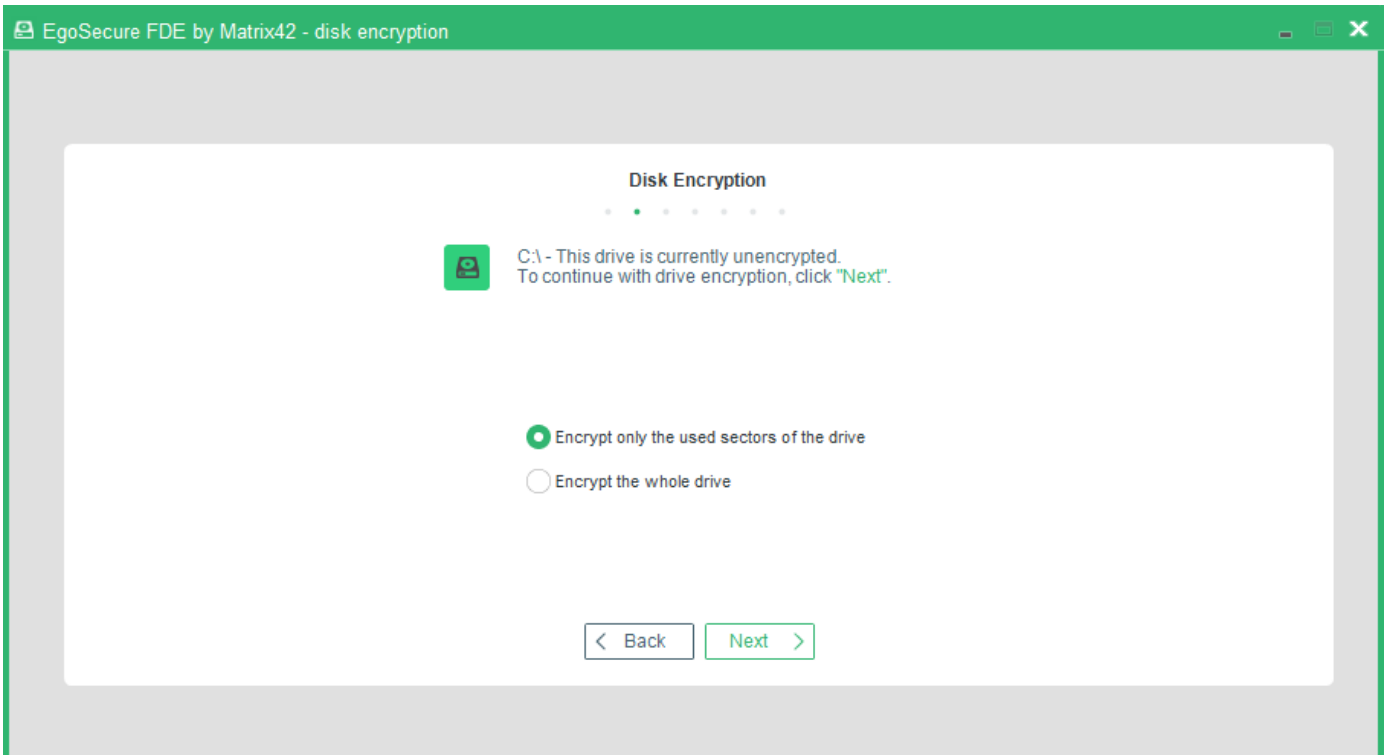
→ The **Disk Encryption** dialog appears (Figure 9). This dialog lists all the available NTFS partitions/disks on your computer. Plain (unencrypted) hard disk partitions are displayed using a hard disk icon. Encrypted partitions are displayed using a lock icon.

5. Select a plain hard disk to encrypt and click **Next** to continue.

**Figure 9. Encrypt a Hard Disk - Disk Encryption Dialog**



→ The **Information** dialog appears. This dialog enables you to select, whether the whole drive or only used parts of the drive should be encrypted:



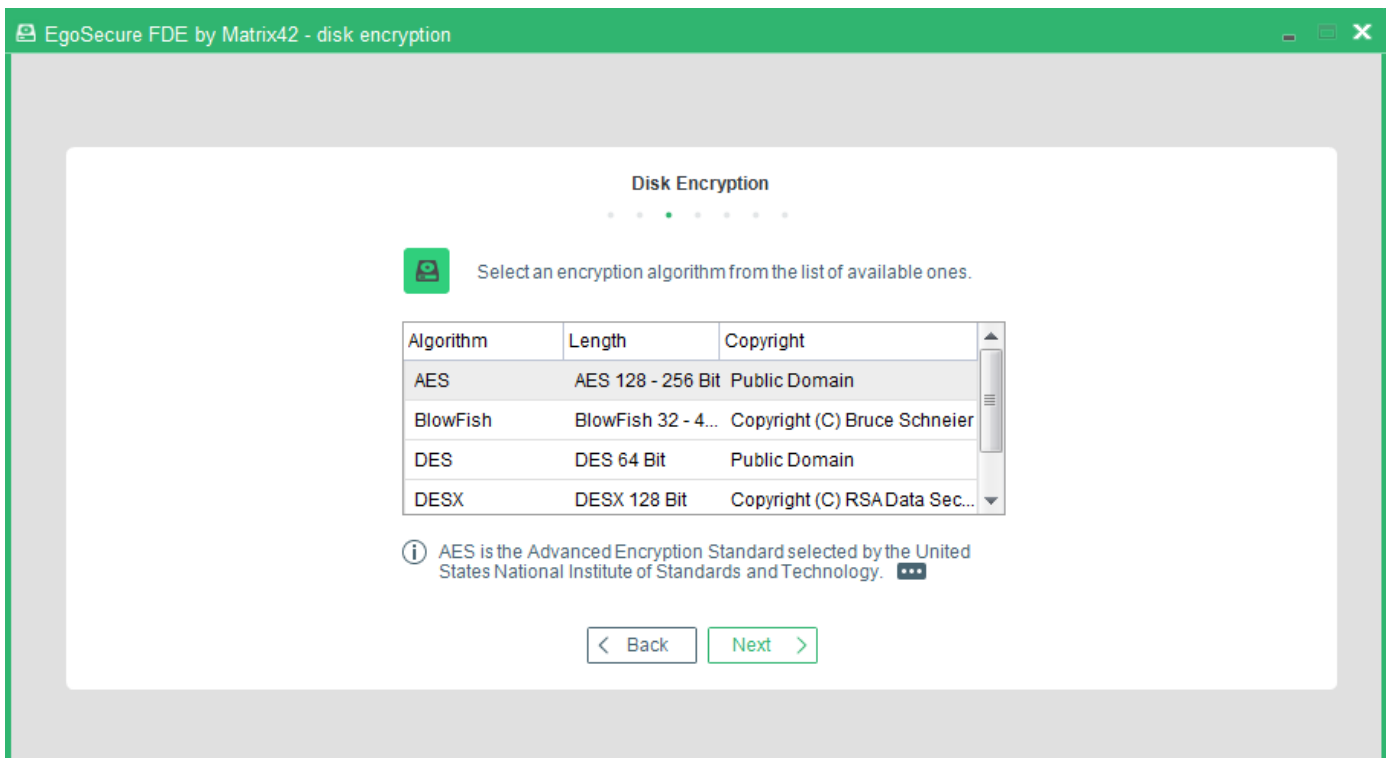
GUI option	Details
Encrypt only the used sectors of the drive	When a drive is initially encrypted, either all the sectors (regardless of whether they contain data or not) or only those sectors that contain



	data, can be encrypted. Encrypting only those portions of the drive that are used is much faster in most of the cases. Select this option if you want to encrypt only the currently used sectors during the initial encryption.
Encrypt the whole drive	Encrypting all sectors of the drive provides more security because even such things as already deleted data will be encrypted. Select this option to encrypt all the sectors of the selected partition.

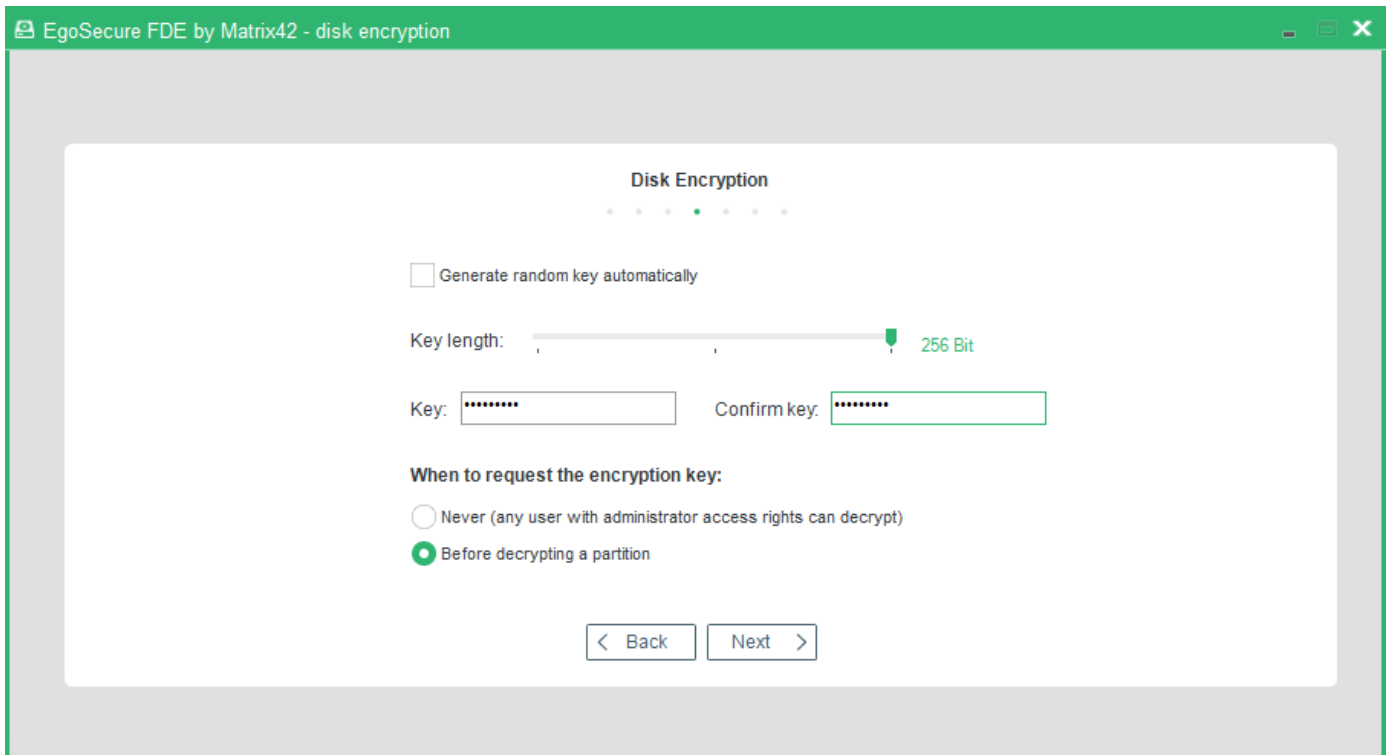
6. Click **Next** to proceed with the next step.

- The **Algorithm** dialog appears. This dialog allows you to select which algorithm will be used for the encryption of the selected drive. For further information about each algorithm refer to the beginning of this section.



7. Select an algorithm and click **Next**.

- ! The AES (Advanced Encryption Standard) provides the highest security coupled with fast encryption speed. This algorithm is the optimal choice for most users.
- The **Key** dialog appears:



This dialog enables you to specify the encryption key that should be used for hard disk encryption. The following settings are available:

GUI option	Sub-option and details
Properties	<ul style="list-style-type: none"> <li>■ Key length Some encryption algorithms support different key lengths. Use the slider to define the preferred key length for the selected algorithm. The key that will be generated out of the password will be of this length.</li> <li>■ Generate random key automatically With this option you do not have to enter an encryption password. The encryption key will be generated randomly when encryption takes place.</li> <li>■ Key, Confirm key The encryption key will be generated from, but is not a copy of, the password you enter (and confirm) here. The encryption password should be different to the <i>EgoSecure Full Disk Encryption</i> administration password.</li> </ul>
Options	<p>Define when encryption key input is required:</p> <ul style="list-style-type: none"> <li>■ Never (any user with administrator access rights can decrypt) This option is totally transparent for the user. The encryption password is not required to decrypt the drive or start the system. This option also means that every user with administrator privileges may start a decryption of the hard disk.</li> <li>■ Before decrypting a partition As with the option <i>Never</i>, this option is also totally transparent for the user. It provides the same protection as the option <i>Never</i>, but to decrypt a partition requires the input of the encryption password (see above).</li> </ul>

- **Key length:** It is recommended to choose the maximum key length for the selected algorithm. This provides the highest security with no remarkable performance loss.
- **Passwords:** If you decide to define your own encryption password choose one that is hard to guess. Use a mix of digits, letters and special characters. The password has to have at least a length of eight characters. A strong password must fulfill the following:
  - Be as long as possible (we suggest 16 characters)
  - Include mixed case letters, digits, and punctuation marks
  - Not be based on any personal information or any word found in a dictionary (in any language)

It is recommended to keep a copy of this password in a safe place. It might be required at a later time for decryption (if the respective option for Key input is selected), or in an emergency.

- **Generate random key automatically:** This option is only possible if the key (password) is never requested later on (see the option NEVER in the key **Options** field). Because nobody knows the random key, it is not possible to enter the key (password) during the startup sequence or to decrypt.
- **Before decrypting a partition:** The **Before decrypting a partition** option assumes that the user knows the encryption key (password). Therefore, the **Generate random key automatically** option should not be checked! Doing so would prevent the user from either decrypting a partition/drive or logging onto the computer.

If you want to enable an additional layer of security to the disk encryption key, enable the **Generate hardware-based key encryption key (HKEK)** option and/or **Generate TPM-based key encryption key (TKEK)** when:

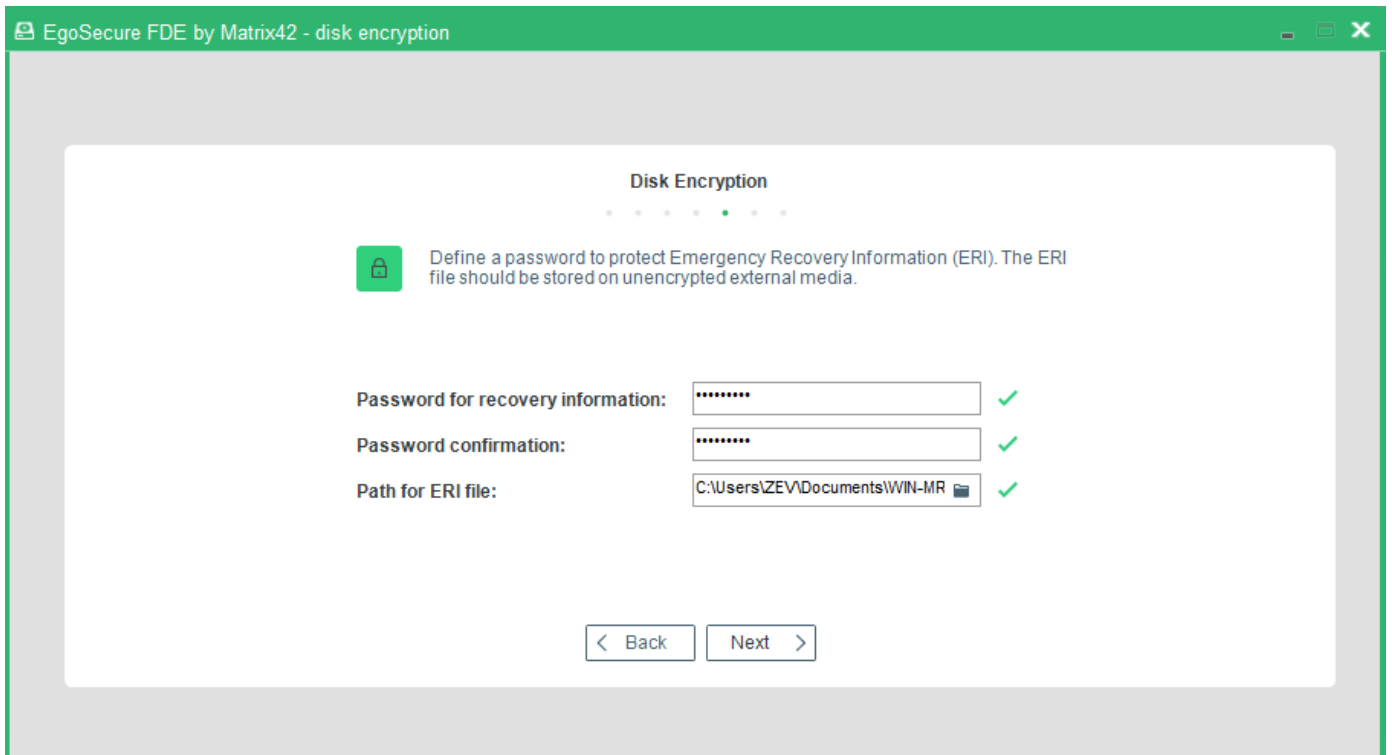
- Initializing FDE or
- Updating FDE settings or
- Creating FDE policies

It means that HKEK and/or TKEK can be added both before and after encrypting a disk partition.

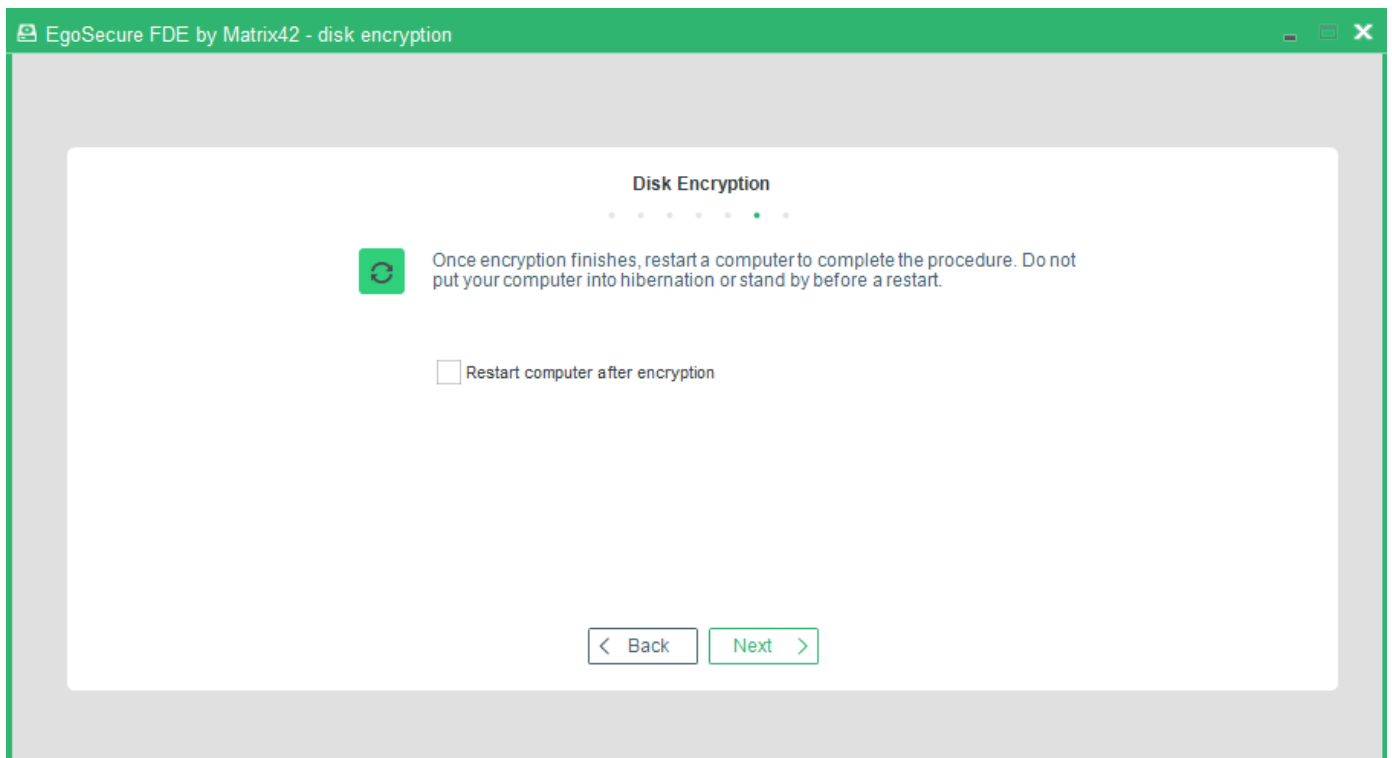
This protects against moving the encrypted drive into another computer within the same network, where the same KEK is used.

8. Select you preferred options and click **Next** to continue.

- The **Key** dialog appears. This dialog allows for creating the ERI file used for the recovery of the disk in case of emergency. Save this file to a flash card or to a network folder.

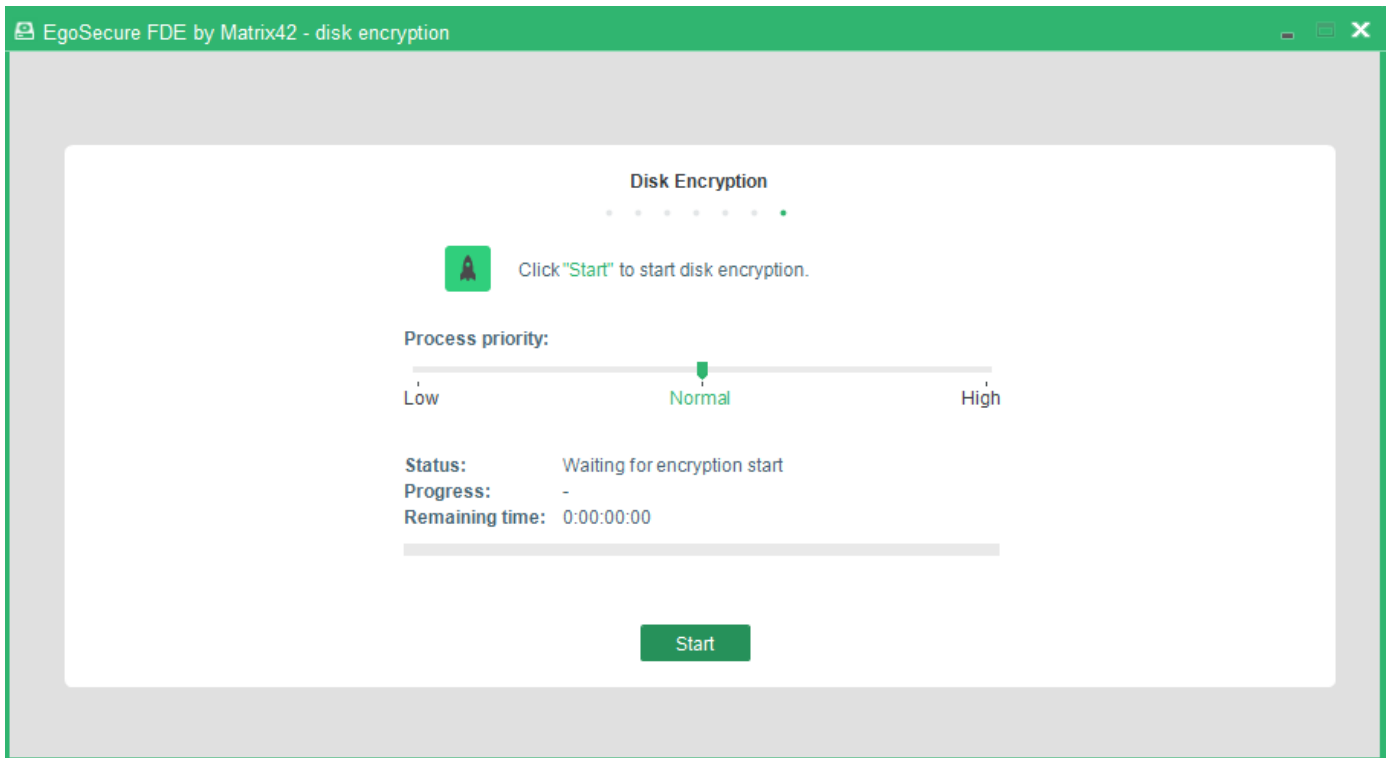


9. Enter the password for the ERI file, confirm it and specify the path for saving the file. Click **Next**.  
Only the English keyboard layout is supported in the recovery application, that is why please enter the ERI password, which contains no symbols from other languages.




10. Set the check box to restart the computer shortly after finishing the disk encryption.

→ The **Encryption** dialog appears:

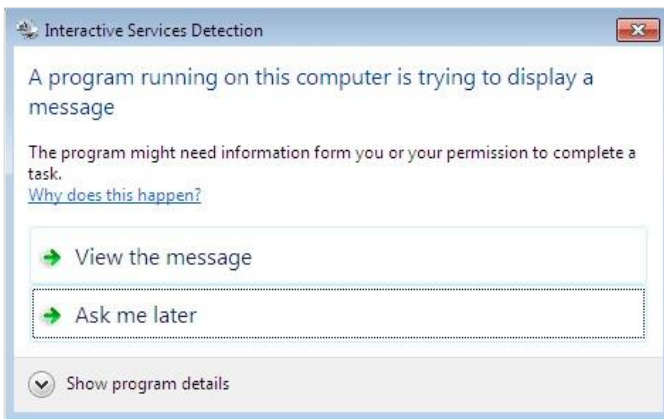


11. Click **Start**. You can adjust the CPU priority given to the encryption process by adjusting the **Priority** slider.

→ The **Initial encryption** process starts. Additionally, the icon  appears in the notification area of the Windows taskbar (if the **Hide FDE tray icon** option hasn't been enabled). When clicking this icon, the **EgoSecure FDE** dialog appears, where the encryption progress is shown.

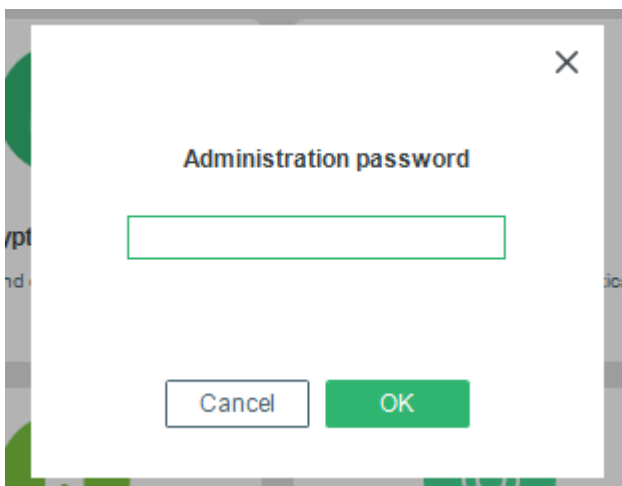
Should the power fail during the encryption process or should the process be interrupted for any other reason this may cause data corruption. However, the encryption procedure can still be continued via the WinPE recovery CD.

The initial encryption of a hard disk takes time. Depending on the amount of data on the hard disk and the speed of the computer, the time needed can be an hour or more. On Windows 7 systems (32 or 64-bit), if the FDE encryption is triggered by the FDE service via policy or after a reboot AND the policy has the 'Show message'-flags set, the user will be notified by the following **Interactive Services Detection** dialogs below. The same can happen if the FDE encryption is triggered through a third-party agent running with "local service" privileges using the public-API provided by EgoSecure. If the 'Show Message'-flags are not set, the user will not be notified with any messages.



## Decrypting a hard disk partition

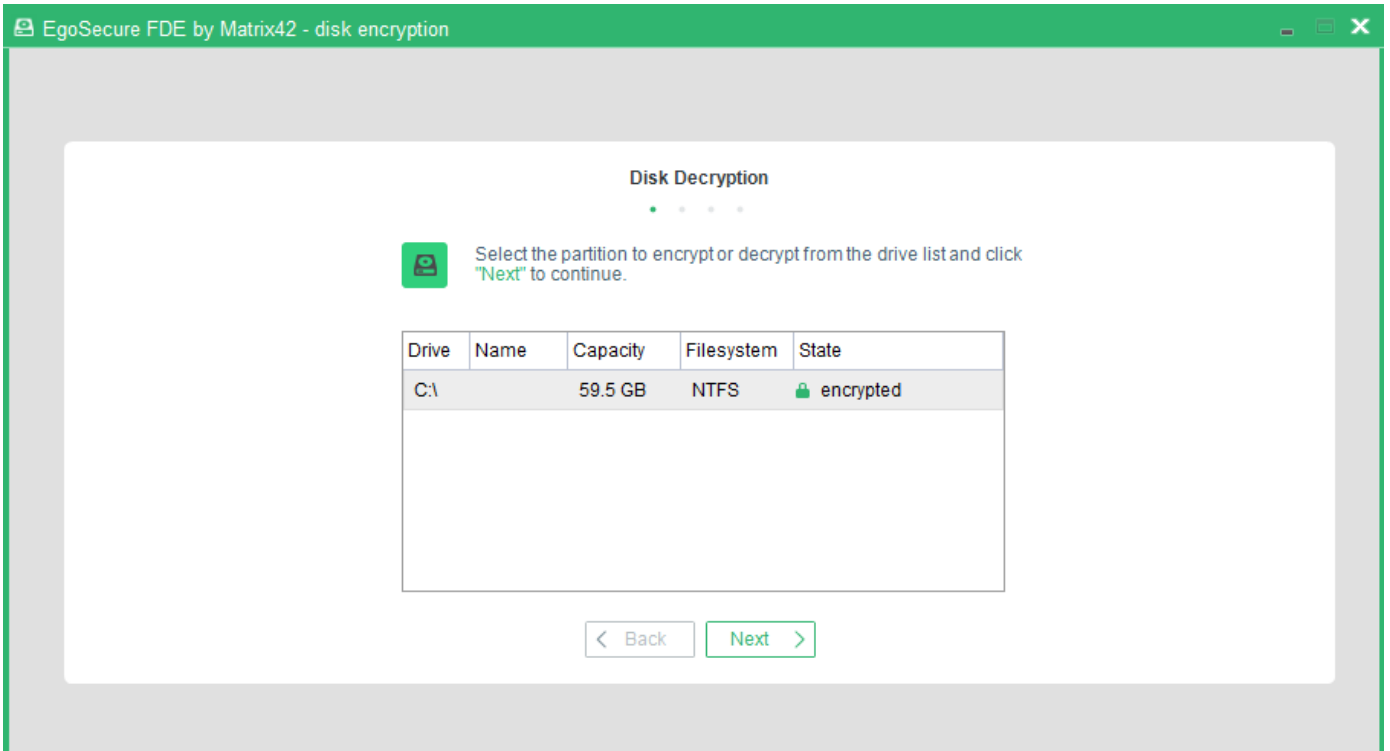
1. Open the **Control Center** (as described in Section [1.5](#)). Double-click the **Disk Encryption** icon.  
→ The Enter administration password dialog appears.
2. Enter the password and click **OK**.



→ The **Disk Encryption** dialog appears.

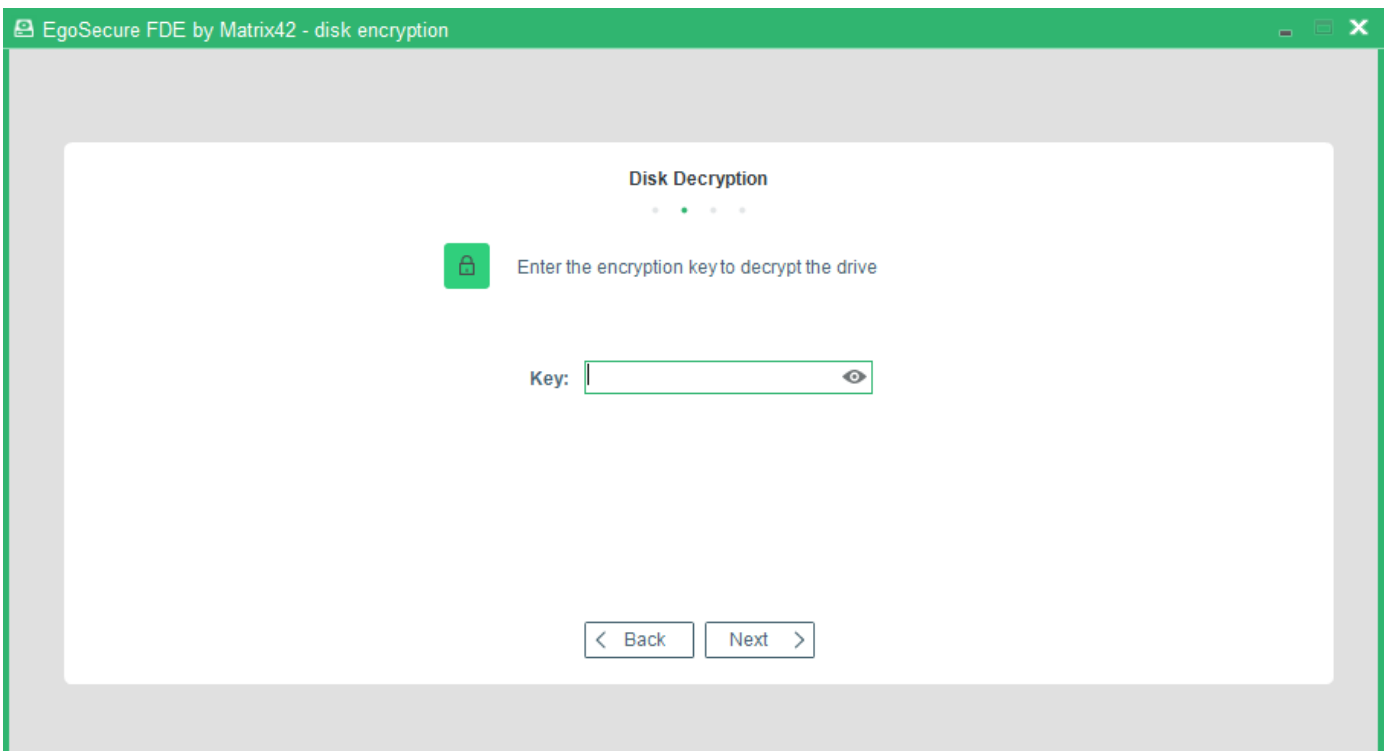
All the available NTFS partitions on your computer are listed in the **Drives** list:

- Plain hard disk partitions are displayed with a hard disk icon.
- Encrypted partitions are displayed with a lock icon.



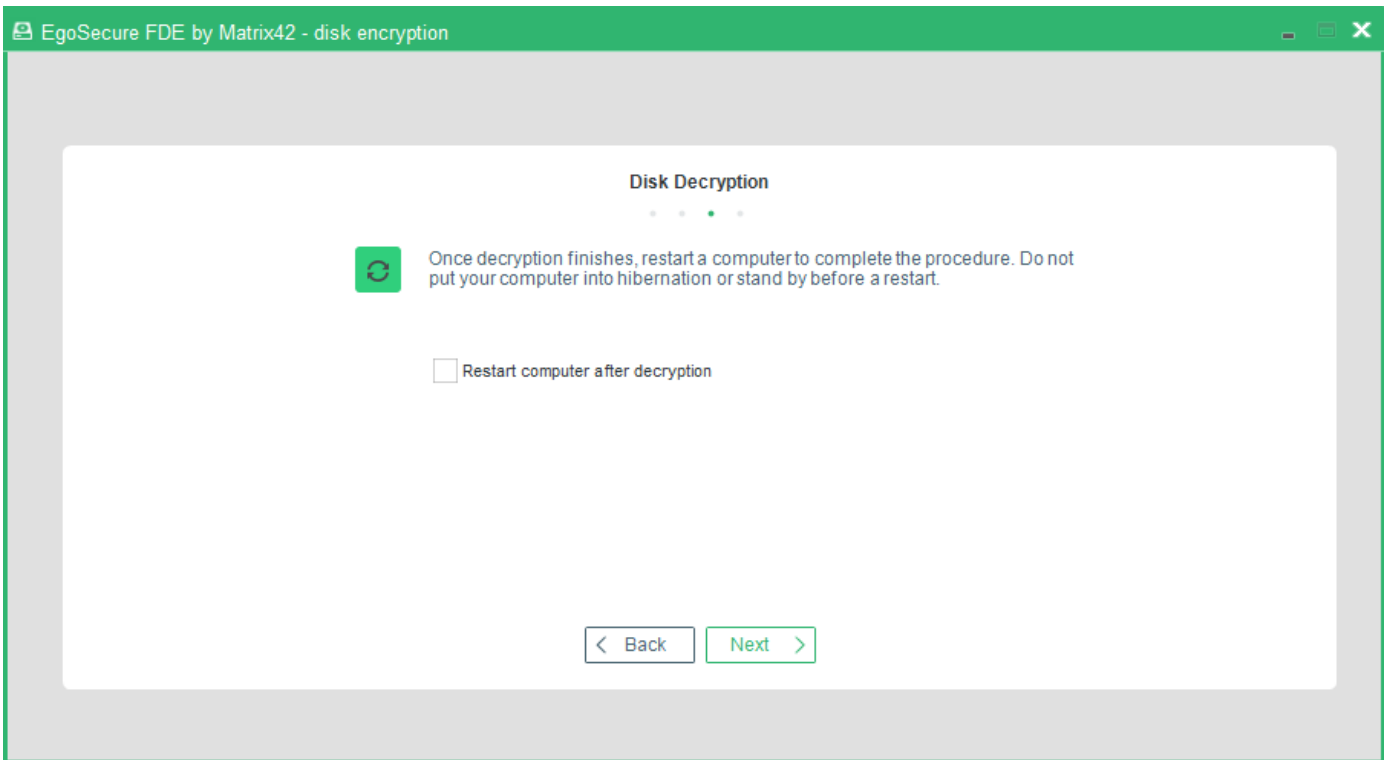
3. Choose an encrypted drive to decrypt and click **Next** to continue.

→ The **Key** dialog appears if during disk encryption the **Before decrypting a partition** option was selected, see [step 8](#) for details.



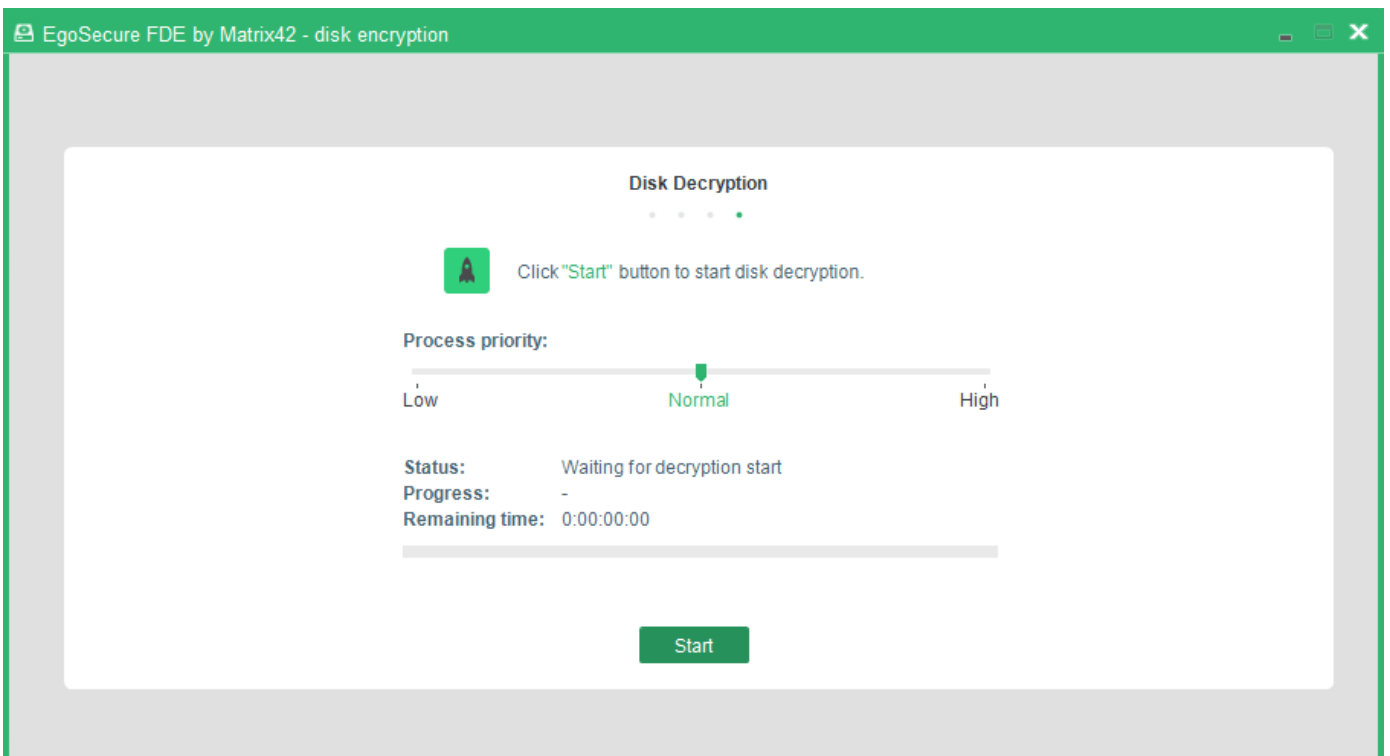
4. Enter the key defined for drive encryption.

→ The **Restart** dialog appears.



5. Set the check box to restart the computer shortly after finishing the disk decryption.
6. Click **Next** to continue.

→ The Encryption / decryption dialog appears:



7. Click **Start** to begin the decryption of the selected drive. You can adjust the CPU priority given to the decryption process by adjusting the **Priority** slider.



→ The decryption starts.

! Do not shut the computer down or work on the computer while decryption is in progress. If not, it would result in data corruption.

→ Once the decryption is complete, a success message appears or the restart starts automatically (if the respective check box was set).

## 1.12. Emergency Recovery Information (ERI)

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

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

- The computer does 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, or decryption was interrupted due to a power failure.

### Solutions

The EgoSecure Full Disk Encryption emergency recovery application is based on Microsoft Windows PE. Both are freely available and reliable tools that enable the administrator to build, and expand a boot CD based on Windows components. EgoSecure Full Disk Encryption has developed plug-ins for both that enable you to start the emergency recovery application from CD.

For details about creating an emergency recovery boot CD or USB flash drive, see [Creating a WinPE emergency recovery boot CD or USB flash drive \(Windows Vista/Windows 7/8/8.1/10\)](#).

### Emergency recovery information (ERI)

To perform an emergency recovery, an ERI file is needed for the damaged computer. An ERI file is a password protected file that contains the encryption keys to the encrypted partitions of the hard disk (each partition has its own encryption key).

The ERI file can be generated during either the installation or at a later time. The file is the 'key' to getting back into your computer should an emergency arise, so a backup copy of the ERI file should be made to a secure location (network directory or external drive) (see [Creating an ERI file](#)).

The emergency application accesses the ERI file to either decrypt the local partitions or to turn PBA off.

To perform emergency recovery, the ERI file must contain the latest encryption details for the damaged computer. Therefore, it is recommended to create a new ERI file every time the encryption settings are changed on the target computer.

If a “company key” is used for encryption (a single key used for the encryption of all, or many computers within a company), only one ERI file has to be created. This ERI file can be used for emergency recovery on any computer that shares the same encryption key. In the case of individual keys for each computer, an ERI file has to be created for each one.

## CONTENTS

- ◆ [Creating an ERI file](#)
- ◆ [Defining an automatic ERI file naming convention](#)
- ◆ [Creating a WinPE emergency recovery boot CD or USB flash drive \(Windows Vista/Windows 7/8/8.1/10\)](#)

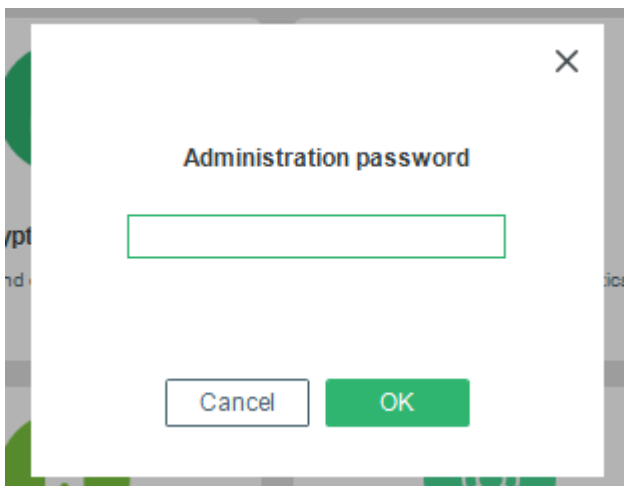
## Creating an ERI file

This section details the ERI file creation procedure.

To create an ERI file and an ERD, Windows local administrator privileges are required.

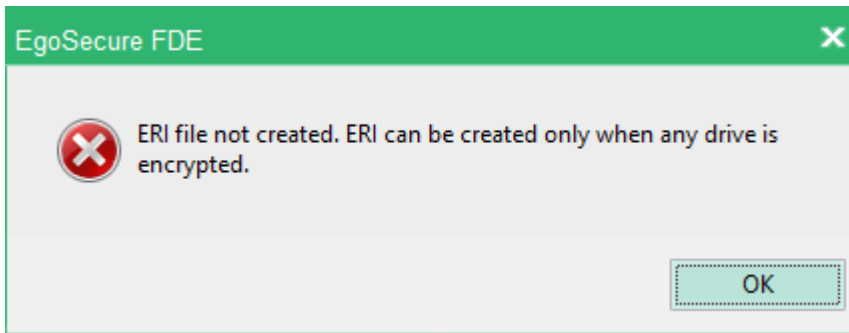
Follow the steps below to create an ERI file, and/or to create an ERD:

1. Open the **Control Center** (as described in section [1.5](#)).
2. Double-click the **Recovery Information** icon.
  - The Administration password dialog appears.

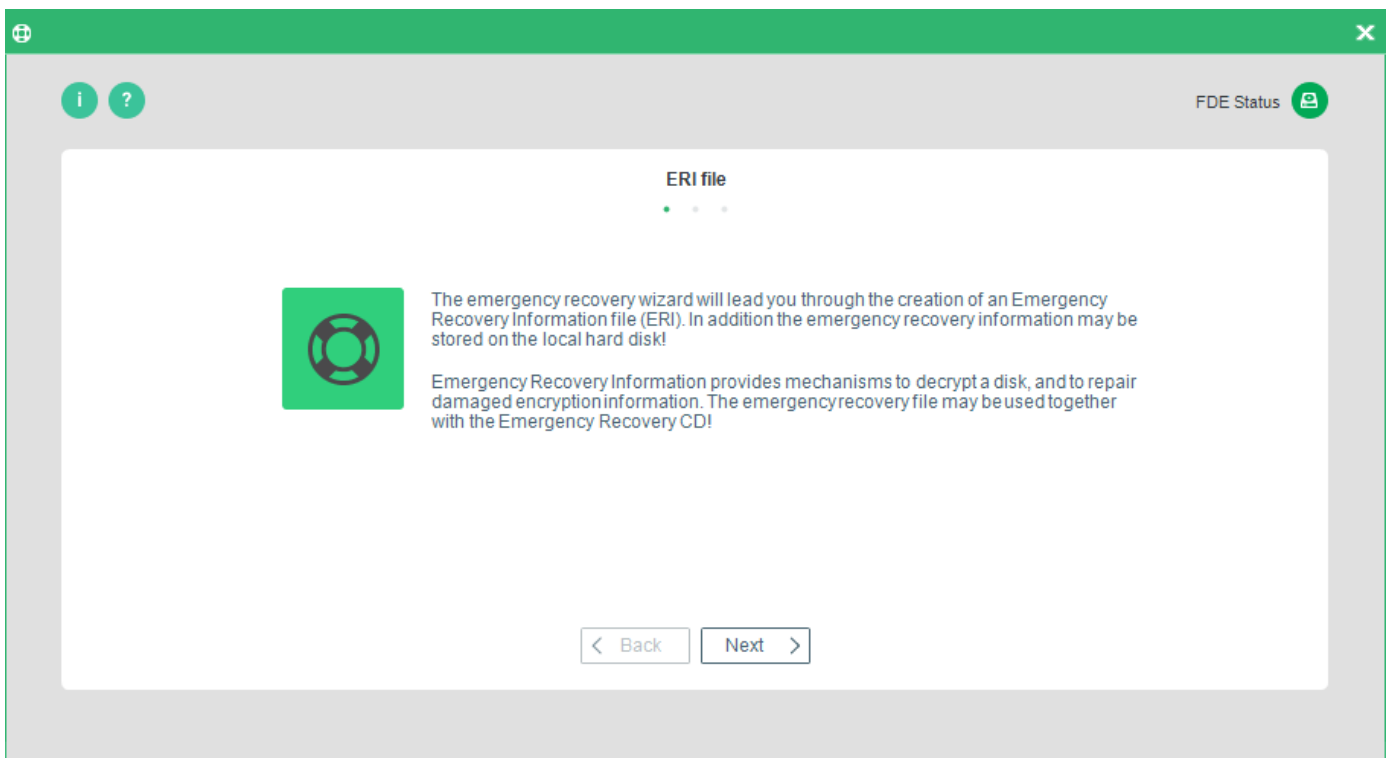


3. Enter the password and click **OK**.

! ERI file can be created, only if any one of the drives in the system is encrypted. If you try to create an ERI file without encrypting any drive, an error message will appear



→ The Save Emergency Recovery Information dialog appears:



4. Read the information in the dialog and click **Next** to continue.

→ The **ERI Password/File Destination** dialog appears.

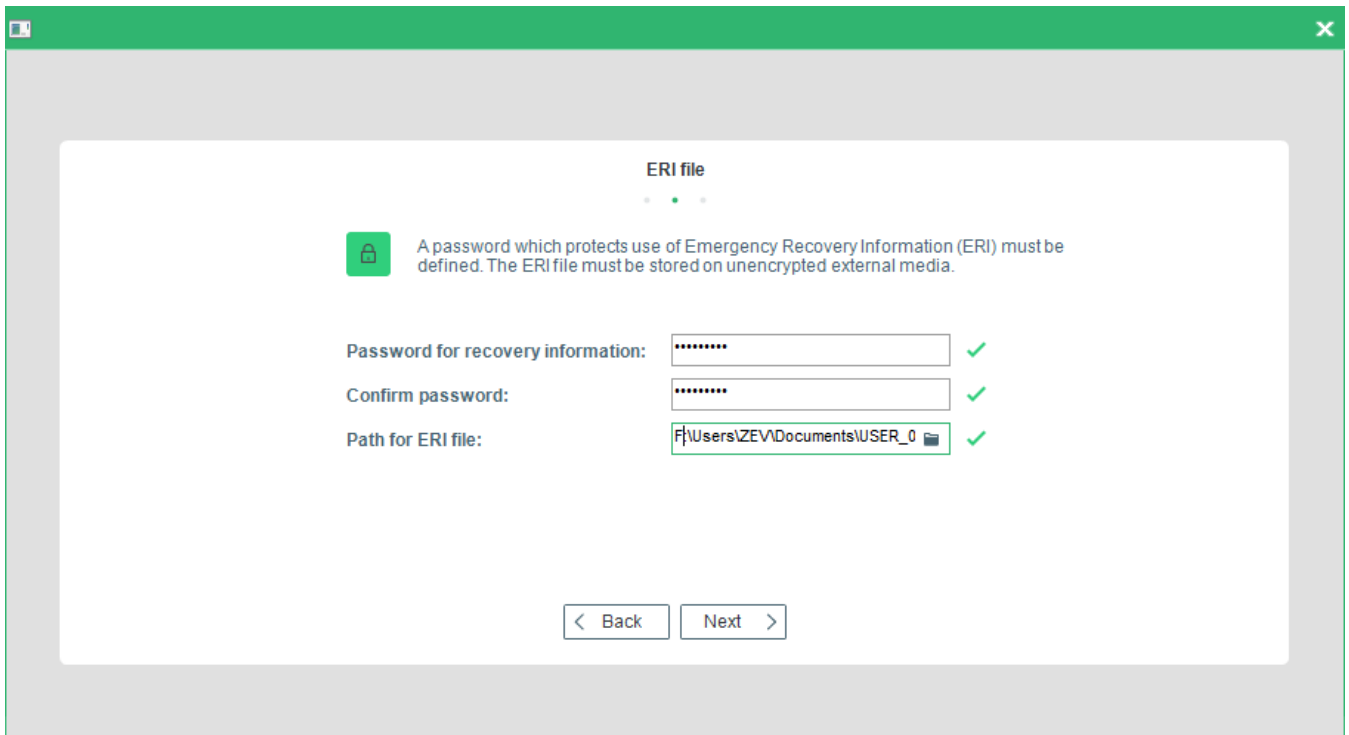
This dialog helps you specify the password to protect the ERI file from third parties, as well as the destination directory for the file.

5. Enter and confirm a password for recovery information.

Only the English keyboard layout is supported in the recovery application, that is why please enter the password, which contains no symbols from other languages.

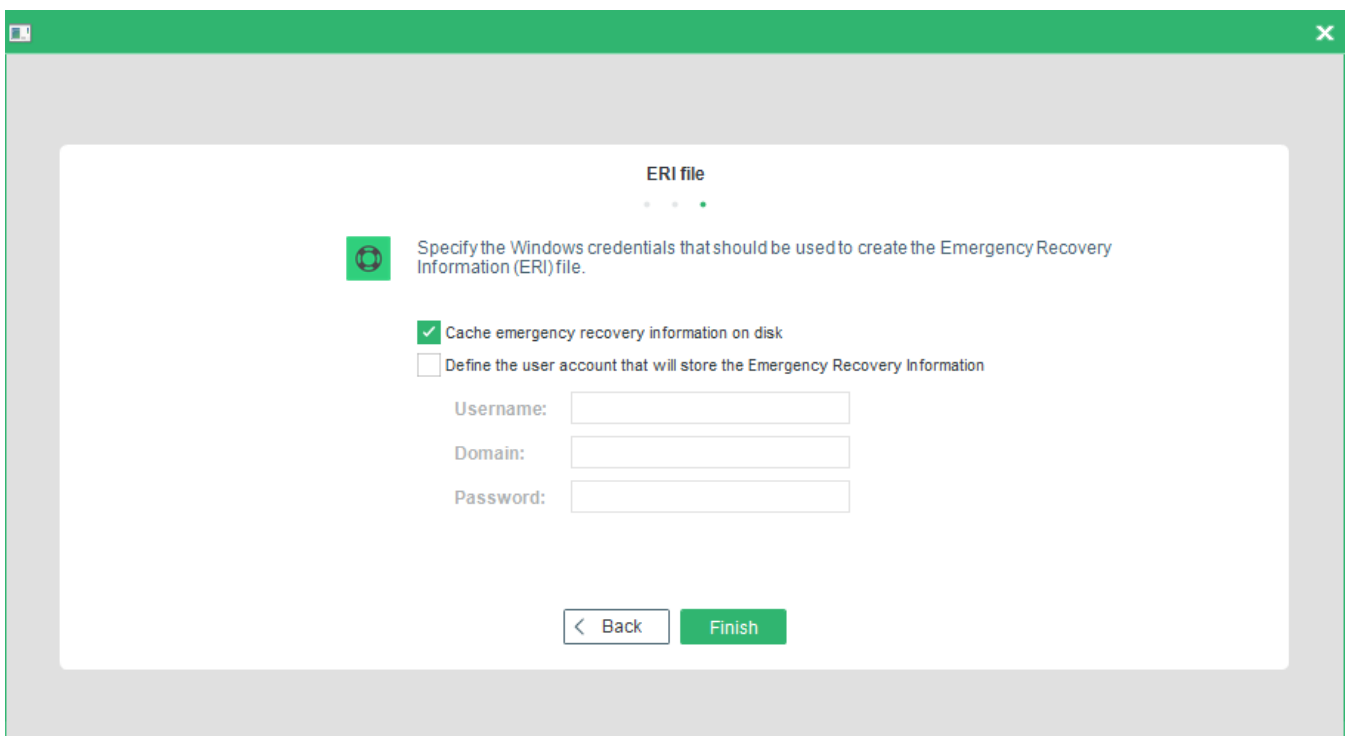
6. Enter a full path for the ERI file either directly into the field **Path** or click "..."/> to open a file explorer.

7. Click **Next** to continue.



8. (optional) If you want to make use of a 'pattern' (click [Defining an automatic ERI file naming convention](#) to see the description), make sure that the path ends with a simple backslash ( \ ) - the filename will be completed automatically using the pattern defined in the registry entry `ERIFilePattern`.

→ The **Cache ERI/Specify User** dialog appears. This dialog allows you to specify a user (via their Windows credentials) for storing the ERI file and whether to cache the ERI to the hard disk.

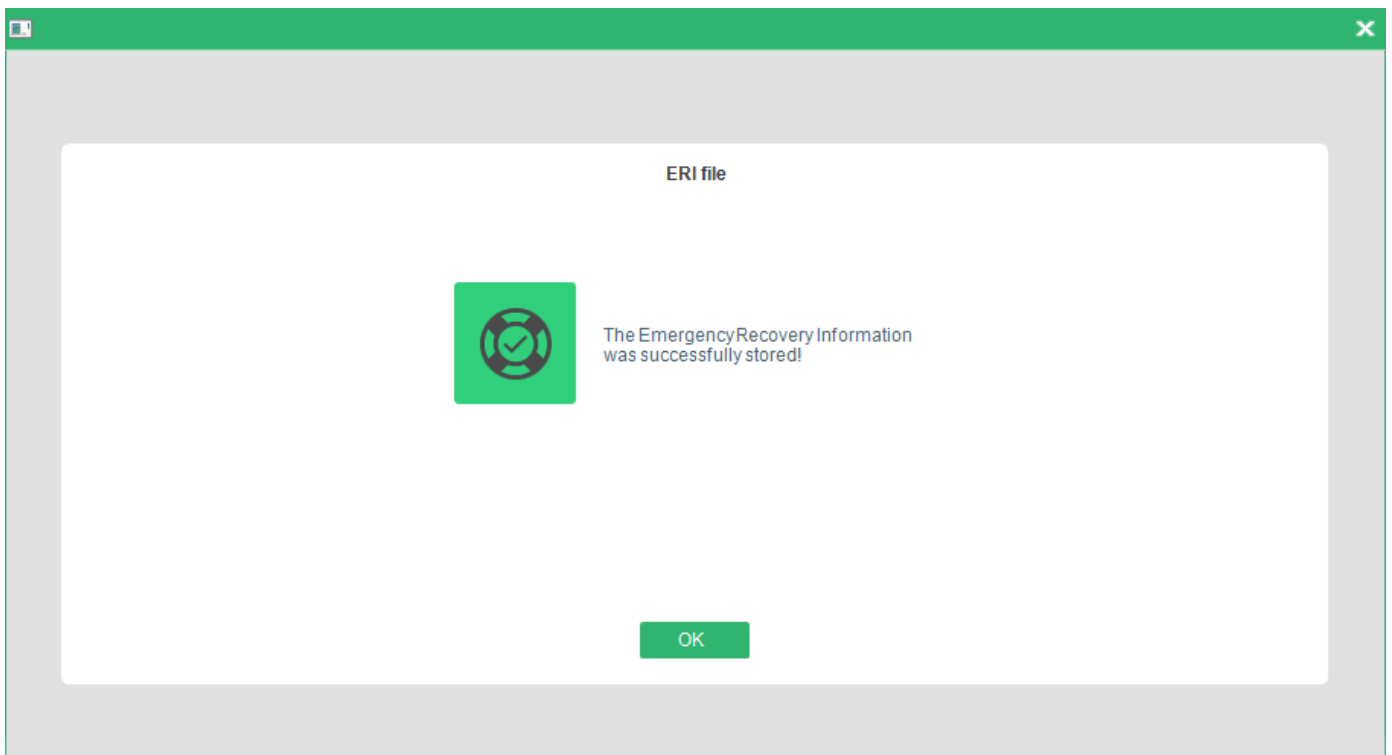


The following options are available:

Option	Details
Cache emergency recovery information on disk	This option allows you to cache the ERI on the PBA partition in encrypted form.
Define the user account that will store the Emergency Recovery Information	If you check this option, a user account will be assigned to the emergency recovery file copy, as an additional security measure (this only functions if the recovery information copy is saved on a network drive). To be able to create the account, a username, domain and password must already exist to be specified in the fields <b>Username</b> , <b>Domain</b> and <b>Password</b> , respectively.

9. Once you have made your selection click **Finish** to complete ERI file creation.

→ A confirmation dialog appears if the ERI creation is successful:



Note: It is not possible to create an ERI file on a network path with mapped drive path. For example, Y:\ERI (Y mapped to \\FDE001\Product).

## Defining an automatic ERI file naming convention

This section is an extension of step 5 – How to define an automatic naming convention for ERI files via the use of 'patterns'.

A 'pattern' is a placeholder that can be used as part of the path to keep certain elements of the filename consistent. These placeholders must be 'delimited' via the use of angled brackets (< >) and can be of the following type:

- <computername>
- <username>
- <date>

These placeholders already exist as a part of every Windows system. The pattern simply uses this information to name the ERI file.

Patterns can be used directly in the **Path for ERI file** field and in the registry entry for the automatic naming convention.

Follow these steps to define an automatic ERI naming convention:

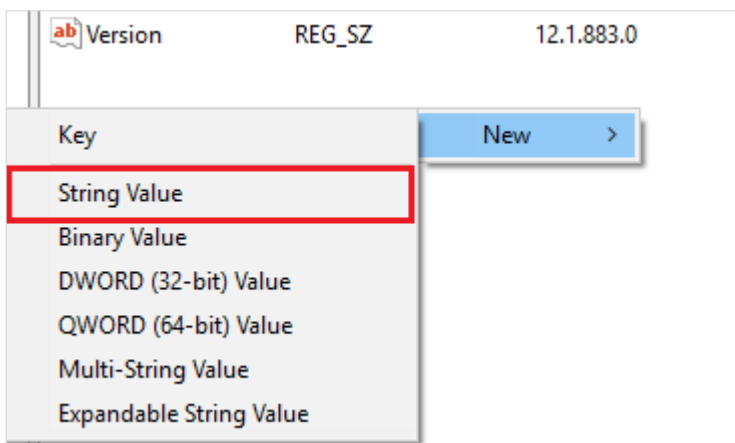
1. Open the Windows Registry Editor by either selecting Start > Run and entering `regedit` into the **Open** field, or opening the editor directly from the directory:

C:\WINDOWS\regedit.exe

In the Windows Registry Editor, open the entry:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Mobsec\_NB\Notebook\General\

Create a new entry by right-clicking in an open space on the right-hand panel and choose **New > String Value** from the menu:



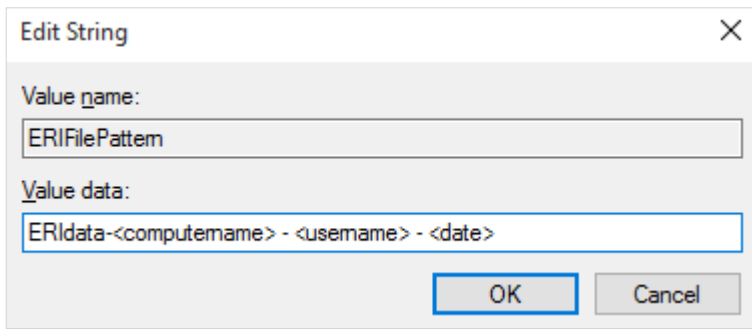
2. Enter `ERIFilePattern` as the value name:

Name	Type	Data
(Default)	REG_SZ	(value not set)
InitFDE	REG_SZ	1
Install Path	REG_SZ	C:\WINDOWS
LogfilePath	REG_SZ	C:\FDE.log
OriginalActiveV...	REG_SZ	\Device\Hard
st1	REG_BINARY	02 8f de 8c 6a
st2	REG_BINARY	e9 b0 da 6e e:
Version	REG_SZ	12.1.883.0
ERIFilePattern	REG_SZ	

3. Double-click the new entry.

→ This will open a window in which you can enter the naming convention you wish to use for filenames.

4. Enter the naming convention ('pattern') in the **Value data** field (see examples on next page). Click **OK** to close the window and set the value.



5. Close registry editor.

### Path examples

Here are some examples of paths that either use patterns directly or use automatic naming (the filename will automatically be appended with the extension `.eri` if this was not already included in the path):

Dialog Entry (entered directly in the 'Path for ERI file' field)	Registry Entry	Result
x:\dir\erifile<date>	-----	x:\dir\erifile20050928.eri
x:\dir\	erifile	x:\dir\erifile.eri
x:\dir\	ERI_<computename>_<username>.eri	x:

It is possible that the ERI file will fail to copy to the specified path, for example, if a network drive has been specified but the computer is unable to connect to the network at the time the ERI file is created. In such a scenario, the ERI file will be temporarily stored in the EgoSecure Full Disk Encryption PBA partition until the computer can successfully locate the specified path. Once copied to the specified path, the local copy on the PBA partition is deleted.

If there is an emergency before the ERI file can be successfully copied to the specified path, the local copy of the ERI file will be detected and used by the ERD. For details about performing emergency recovery, see chapter [1.13](#).



#### WARNING

#### Taking care of ERI files

It is recommended to keep copies of all ERI files in a safe place.  
If an ERI file is damaged or lost, no emergency recovery will be possible!

## Creating a WinPE emergency recovery boot CD or USB flash drive (Windows Vista/Windows 7/8/8.1/10)

This section details on how to create a WinPE (Windows Preinstalled Environment) ERD. This includes how to adapt WinPE to use a plug-in in preparation for recovering/repairing data from a damaged partition.



### WARNING

#### WinPE and Full Disk Encryption update

Create WinPE each time when updating Full Disk Encryption. WinPE created in the latest FDE version is valid for the emergency recovery in previous FDE versions.

But: disks encrypted with the latest FDE version can NOT be decrypted with WinPE of lower versions.



### ATTENTION

#### SCSI adapters not supported

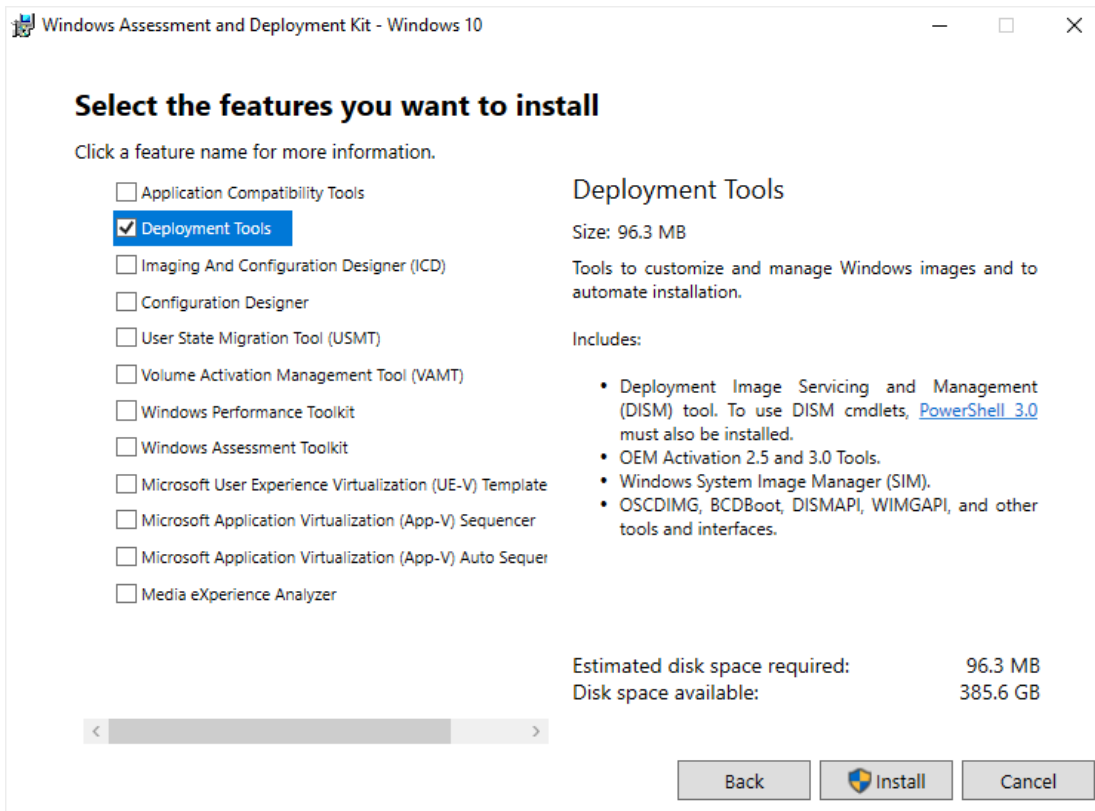
SCSI adapters are not supported for creating WinPE, reconnect your device as IDE.

### Preparation steps

WinPE is a part of the Windows Assessment and Deployment Kit (ADK). That is why download ADK and install its features.

1. Download ADK:
  - Windows ADK 10, version 1903 is used for creating WinPE by default ([click to start the download of the Windows ADK 10](#)).
  - Windows ADK 8 is used for creating WinPE if Windows ADK 10 installation failed ([download Windows ADK 8](#)).
2. Install the following features, once the ADK is downloaded:
  - **Deployment Tools:** includes the Deployment and Imaging Tools Environment.
  - **Windows Preinstallation Environment:** includes the files used to install Windows PE (*only for ADK 8*).
3. *Only for Windows ADK 10, version 1903 and higher:* install Windows PE add-on for ADK ([click to start the download](#)).



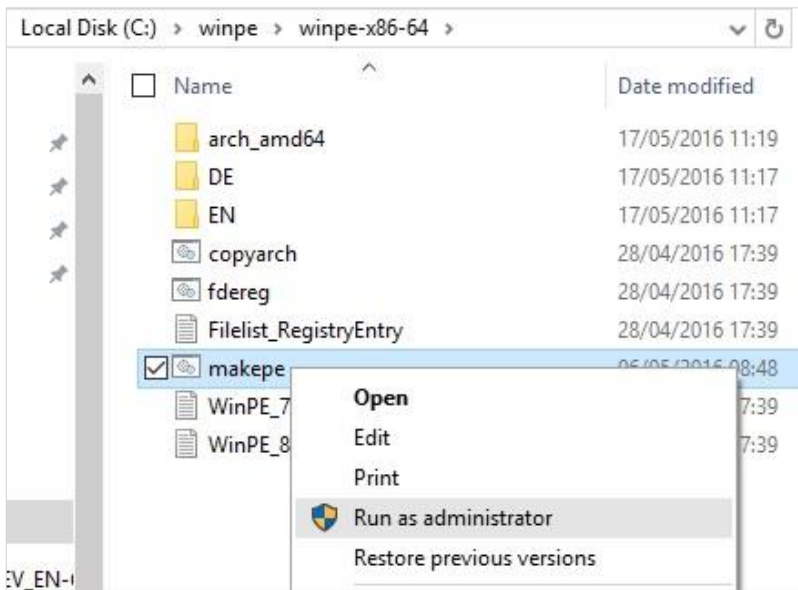


## Creating a WinPE ERD

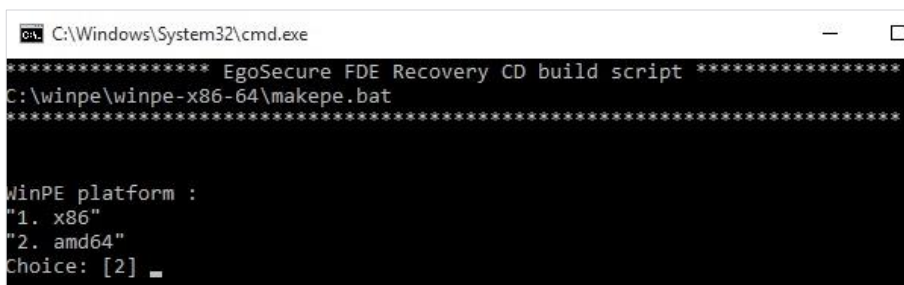
1. Before starting the procedure, make sure that you have already installed Full Disk Encryption and generated the ERI files necessary for recovery (for details, see [Creating an ERI file](#)).

*Additional step for users with Windows ADK 10:* Right-click a **makepe.bat** file and select **Edit** from the context menu. In the text editor, replace the path "c:\Program Files (x86)\Windows Kits\8.0\Assessment and Deployment Kit\Deployment Tools" with "c:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Deployment Tools" in two places.

Unzip the Full Disk Encryption package to C:\winpe folder and run the **makepe.bat** file as administrator.



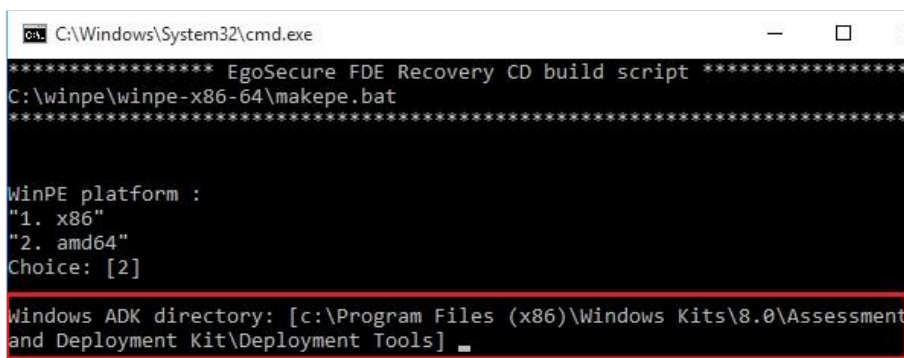
→ The dialog appears. On the first step, the system detects the WinPE platform type.



## 2. Type **Enter**.

→ In the next step, the path for Windows ADK directory is identified automatically and the following is displayed:

- For Windows ADK 8: c:\Program Files (x86)\ Windows Kits\8.0\Assessment and Deployment Kit\Deployment Tools
- For Windows ADK 10: c:\Program Files (x86)\ Windows Kits\10\Assessment and Deployment Kit\Deployment Tools



## 3. Press **Enter**.

- At the next 2 steps, the paths for EgoSecure WinPE directory and EgoSecure WinPE ERI directory are detected.

```
C:\Windows\System32\cmd.exe

Windows ADK directory: [c:\Program Files (x86)\Windows Kits\8.0\Assessment
and Deployment Kit\Deployment Tools]

EgoSecure WinPE directory: [C:\winpe\winpe-x86-64]
EgoSecure WinPE ERI directory : [C:\winpe\winpe-x86-64\ERI]
```

4. Enter the number which is referred to media type you want to create (1 for ISO image, 2 for USB flash drive). [1] is used by default.

```
C:\Windows\System32\cmd.exe

Windows ADK directory: [c:\Program Files (x86)\Windows Kits\8.0\Assessment
and Deployment Kit\Deployment Tools]

EgoSecure WinPE directory: [C:\winpe\winpe-x86-64]
EgoSecure WinPE ERI directory : [C:\winpe\winpe-x86-64\ERI]

Media type:
'1. ISO"
'2. USB Flash Drive"
Choice: [1] 2_
```

5. Press **Enter**.

6. Creating ISO:

- a. Type **Y** to agree.

```
Media type:
"1. ISO"
"2. USB Flash Drive"
Choice: [1]

Copy amd64 ADK architecture to directory 'C:\winpe\winpe-x86-64\arch_amd64
...
Delete directory 'C:\winpe\winpe-x86-64\arch_amd64'...
C:\winpe\winpe-x86-64\arch_amd64, Are you sure (Y/N)? y_
```

- b. Press any key to close the window.

```
100% complete

Success

ISO file: C:\winpe\winpe-x86-64\arch_amd64\winpe.iso

Done!

Press any key to continue . . . _
```

7. Creating USB:

- a. Enter the letter of the drive.

- If your flash drive has the MBR partition layout, just type **yes** to agree that all data on the USB drive will be lost.
- If your flash drive has the GPT partition layout, type **yes** to agree that all data on the USB drive will be lost and the drive partition layout will be changed to MBR.
- If your flash drive has the partition layout other than GPT or MBR, the warning message is displayed. Change the partition layout manually and start the procedure again.

```
EgoSecure WinPE directory: [C:\winpe\winpe-x86-64]
EgoSecure WinPE ERI directory : [C:\winpe\winpe-x86-64\ERI]
Media type:
"1. ISO"
"2. USB Flash Drive"
Choice: [1] 2
USB drive letter: [F] E
All data on E: will be lost! Are you sure (yes/no)? : [no] yes_
```

b. Type **Y** to agree.

**Figure 10. Deleting directory**

```
USB drive letter: [F] E
All data on E: will be lost! Are you sure (yes/no)? : [no] yes
Using '' !
Copy amd64 ADK architecture to directory 'C:\winpe\winpe-x86-64\arch_amd64'...
Delete directory 'C:\winpe\winpe-x86-64\arch_amd64'...
C:\winpe\winpe-x86-64\arch_amd64, Are you sure (Y/N)? y_
```

c. Answer **Y** again to agree with formatting of disk drive.

**Figure 11. Disk formatting and finishing of the process**

```
C:\Windows\System32\cmd.exe
The operation completed successfully.
The operation completed successfully.

Deployment Image Servicing and Management tool
Version: 6.2.9200.16384

Saving image
[=====100.0%=====]
Unmounting image
[=====100.0%=====]
The operation completed successfully.

MakeWinPEMedia /UFD "C:\winpe\winpe-x86-64\arch_amd64" E:
WARNING, ALL DATA ON DISK DRIVE E: WILL BE LOST!
Proceed with Format [Y,N]?Y
Formatting E:...

Setting the boot code on E:...

Copying files to E:...

Success
USB Flash Drive: E:
Done!
Press any key to continue . . . _
```

d. Once the process is finished, press any key to close the window.



**ATTENTION**

**If flash drive is more than 2 GB and error occurs**

If your flash drive is more than 2 GB and an error occurs while creating the WinPE, delete all partitions on this flash drive and create one partition for 2 GB. This partition must be formatted with the FAT32 file system.

## 1.13. Performing emergency recovery

This section details the emergency recovery process. Emergency recovery may be needed in one of the following situations:

Situation	Solution
Remote recovery: You have forgotten your password or lost/misplaced your smart card.	In this case you can recover the system via either the Helpdesk option (for details, see <a href="#">Helpdesk</a> ) or the recovery CD or USB stick (for details, see <a href="#">Recovery via CD or USB stick</a> ).
On-site: The boot code/pre-boot system is damaged/cannot boot to <i>Windows</i> after the system has been reinstalled.	In this case you can recover the system via the recovery CD or USB only (for details, see <a href="#">Recovery via CD or USB stick</a> ).



**WARNING**

**Valid ERI file**

The prerequisite for on-site emergency recovery is a valid ERI file! If you have not created one to a secure location (i.e. USB stick or CD) then this section is useless to you – your data is LOST!

For details about generating an ERI file, see [Creating an ERI file](#).

### Recovery via the HelpDesk option

#### HelpDesk scenarios

The PBA component has built-in functionality to help you start the computer in the following emergency scenarios:

- Defective smart card readers, lost/forgotten/broken smart cards (via PBA HelpDesk). PBA HelpDesk will help you start the system a predefined number of times without a smartcard or a smart card reader (after successful authentication via the HelpDesk). For details, see [Scenario 1](#).
- Forgotten Windows credentials (via PBA HelpDesk). PBA HelpDesk will help you start the system a predefined number of times without a smart card or a smart card reader (after successful authentication via the HelpDesk). For details, see [Scenario 1](#).
- Forgotten/blocked smart card PIN (cards issued via Third-Party). For details, see [Scenario 2](#).

- For smart Card PIN change refer to [Change PIN of your Smart Card](#).

### Challenge and response

The methodology behind the PBA HelpDesk is called 'challenge and response' - the user must relay a 'challenge sequence' to a HelpDesk administrator and in return receives a "response sequence" that authorizes PBA to set a specific recovery procedure in motion. This process offers you the following:

- A more secure challenge-response process than in previous versions while still being 50% shorter. This is known as 'Strong' in the PBA admin GUI.
- A very short challenge-response process that offers a compromise between speed and security. This is known as 'Comfort' in the PBA admin GUI.
- Compatibility to HelpDesk keys generated in previous generations of the HelpDesk application.

The HelpDesk feature only applies if the following criteria are met:

- You have access to this form of remote assistance.
- The HelpDesk application has been installed, HelpDesk keys have been exported from it, and these keys have been correctly imported into PBA either during or after installation.
- The following procedure only describes the process as seen by the user. For further information about the HelpDesk application what both sides of the challenge-response process involves, refer to the [EgoSecure Console Manual](#), description "Using Helpdesk".

### Scenario 1: Misplaced/lost/stolen smart card reader/smart card – forgotten/compromised User ID-password (disable PBA)

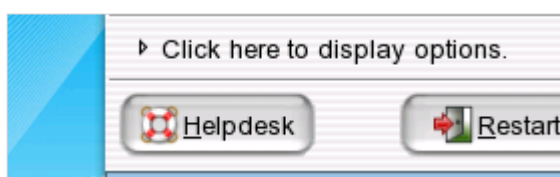
This section will guide you through the HelpDesk procedure to be used if you have problems with the smart card reader, mislaid or lost your smart card, or have forgotten your user ID/password.

Both you and the HelpDesk administrator share one or more secrets for the purpose of identification. As to how the secret is administrated and stored is up to the parties involved and is not part of this guide or the EgoSecure Full Disk Encryption product.

If you use smart card authentication, after this process is implemented, the computer will be able to boot without a smart card – but only a limited number of times. This means that the system security status is set to 'transparent encryption'. This is a much weaker security status! Re-implement smart card authentication as soon as possible.

Follow these steps to help you through the HelpDesk process:

1. Click the **Helpdesk** button (or press the **Alt+H** keys) in the PBA logon dialog for remote assistance:



- The following dialog appears:

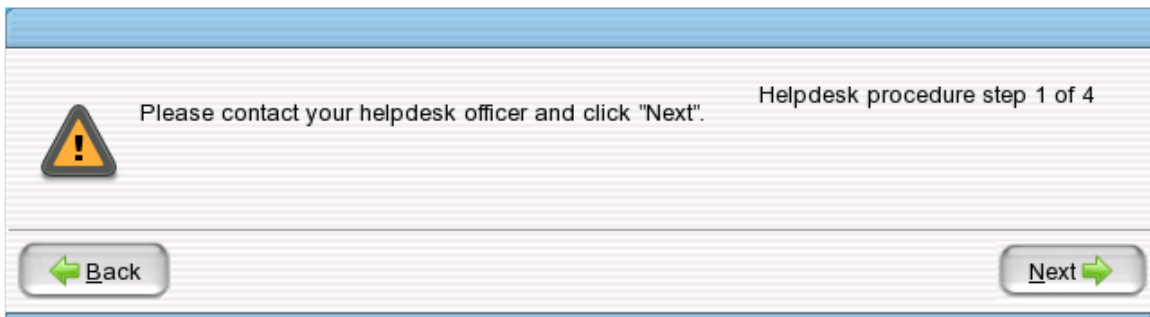


2. Select **Deactivate pre-boot authentication**.

! If **Deactivate pre-boot authentication** is not active (greyed-out) then you have not imported HelpDesk keys into PBA. Helpdesk keys cannot be imported into PBA while EgoSecure Full Disk Encryption is in this state. Either you have to wait until smart card authentication can take place or use an ERD to bypass PBA (see [Emergency recovery via boot CD or USB stick](#) for details).

3. Click **Next**.


→ The HelpDesk contact details dialog appears:



4. Contact the HelpDesk using the information provided in the dialog. Identify and authenticate yourself to the HelpDesk administrator. After successful authentication, click **Next**.

→ The **Request ID** dialog appears:

Helpdesk procedure step 2 of 4

 Please relay the Request-ID below to your helpdesk officer and click "Next"!

Request-ID

a  b  c  d  e

▼ Click here to hide the input guide.

ALFA BRAVO CHARLIE DELTA ECHO FOXTROT GOLF HOTEL INDIA  
JULIET KILO LIMA MIKE NOVEMBER OSCAR PAPA QUEBEC ROMEO  
SIERRA TANGO UNIFORM VICTOR WHISKEY XRAY YANKEE ZULU

5. Relay the **Request ID** sequence (fields a & b) to the HelpDesk administrator.
6. Once the sequence has been relayed to the HelpDesk, click **Next**.


The **Request ID** has a specific sequence to it. Should the user relay the sequence incorrectly to the HelpDesk administrator, or the HelpDesk administrator enter the sequence incorrectly in the HelpDesk application on their side, the computer will 'beep', alerting the user and the HelpDesk administrator that the sequence must be clarified.

The cause of an incorrect entry usually applies to the characters entered into each field. The letters B, D, O, Y have been removed from the challenge-response process because they can be confused with another letter or number. If one of these characters is entered the computer will beep.

7. Read and relay the request ID carefully! For example, a '1' can look like an 'I'.

→ The **Challenge sequence** dialog appears:

Helpdesk procedure step 3 of 4

 Relay the Challenge sequence below (fields a to p) to your helpdesk officer and click "Next".

Challenge sequence

a  b  c  d

e  f  g  h

i  j  k  l

m  n  o  p

▶ Click here to display the input guide.



8. Relay the **Challenge sequence** (fields a & b) to the HelpDesk administrator and then click **Next**.

The **Challenge sequence** has a specific sequence to it. If you relay the sequence incorrectly, the HelpDesk administrator will ask you to clarify the sequence (as stated above).

Once the sequence has been successfully relayed to the HelpDesk, the HelpDesk administrator may query you as to when, if possible, you can next authenticate yourself via the smart card and will set the number of reboots (without a smart card – transparent mode) accordingly.

→ The **Response sequence** dialog appears.

The HelpDesk administrator will relay the response sequence to you field-by-field (**a** to **n**).

Helpdesk procedure step 4 of 4

Carefully enter the response sequence from the helpdesk officer in these fields:

Response sequence

a	9J136	b	7GMF6	c	93758	d	K33XP
e	8K7R7	f	ZFPKF	g	CQWTZ	h	X4K6A
i	TLXVU	j	NVUZW	k	QQARJ	l	8G9R9
m	IVJIC	n	1NI84				

Back Cancel Clear values Finish

9. Enter the sequence carefully. Once the sequence is entered click **Finish** to complete the process. You are now able to start the computer and bypass PBA for a limited number of reboots.

! If you cannot authenticate within the reboot limit set by the HelpDesk, then the HelpDesk process must be repeated.

## Scenario 2: Forgotten/compromised/blocked smart card PIN (PIN reset with PUK)

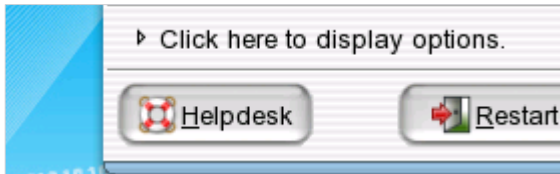
This section will guide you through the HelpDesk procedure to be used if you have forgotten or lost your smartcard, or if the smart card PIN has been blocked.

It is possible to reset the smart card PIN only if the following conditions have been met:

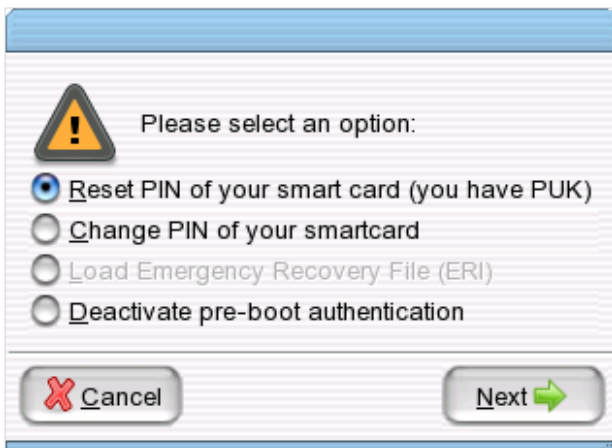
- The smart card issued by Third-party.
- PUK to reset the PIN.

Follow these steps in the PBA logon dialog;

1. Click the **Helpdesk** button (or press the **Alt+H** keys) in the PBA logon dialog for remote assistance:



→ The following dialog appears:



2. Select Reset PIN of your smart card (you have PUK) and click Next.

→ The **PUK detail** dialog appears:

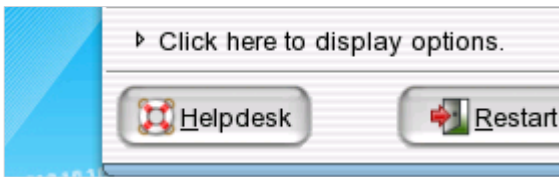


3. Enter the **PUK**.
4. Enter the **New PIN** and confirm it.
5. Click **OK**.

### **Change PIN of your Smart Card**

This section will guide you to change smart card pin in PBA dialog.  
Follow these steps in the PBA logon dialog:

1. Click the **Helpdesk** button (or press the **Alt+H** keys) in the PBA logon dialog for remote assistance:

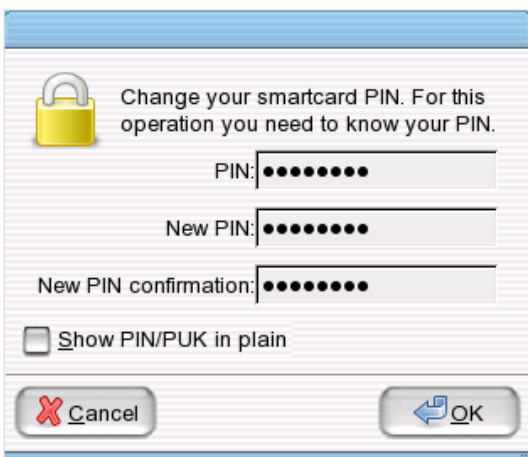


→ The following dialog appears:



2. Select Change PIN of your smartcard and click Next.

→ The **PIN detail** dialog appears:



3. Enter the **PIN**.
4. Enter the **New PIN** and confirm it.
5. Click **OK**.

## Emergency recovery via boot CD or USB stick

In an emergency in which the computer will not start properly, or the PBA is damaged, you can access the hard disk using a customized boot media that contains the emergency recovery application. This is referred to as the ERD.

- The ERD will enable you to perform a number of repair operations, provided that you have either a valid ERI file for the damaged computer (see [Load ERI](#)), or know the

encryption keys so you can enter them manually (see [Enter the encryption key manually](#)).

- To perform any of the tasks detailed in this section you need to create an ERD. For details see [Creating a WinPE emergency recovery boot CD or USB flash drive](#).

There are two types of emergency recovery application supplied with *EgoSecure Full Disk Encryption*:

- `pe_erd_w32.exe` – This is a GUI-based recovery application. This is the recommended application as it provides a full feature set for the administrator.
- `pe_erd_console.exe` – This is a commandline-based recovery application created to provide only certain functions for scripted, remote recovery.

## CONTENTS

- ◆ [The emergency recovery console \(commandline\)](#)
- ◆ [Start the emergency recovery application \(GUI\)](#)
- ◆ [Menu commands](#)
- ◆ [Workbench for standard hard disks](#)
- ◆ [Load ERI](#)
- ◆ [Enter the encryption key manually](#)
- ◆ [Decrypt a drive in silent mode](#)
- ◆ [Repair MBR](#)
- ◆ [Restore original MBR](#)
- ◆ [Set active partition](#)
- ◆ [Set the administration password](#)

## The emergency recovery console (commandline)

The commandline console has been developed to help administrators perform basic, scripted recovery tasks from within the *WinPE* environment.

Parameter	Details
<code>eripath</code>	The path of ERI file. <b>Note:</b> If the ERI path contains spaces, it must be enclosed in quotation marks.
<code>Eripwd</code>	The ERI file password. <b>Note:</b> If the ERI password contains spaces, it must be enclosed in quotation marks.
<code>partition</code>	The partition to be decrypted.
<code>/H</code>	Display information in the command prompt about each parameter listed here.
<code>/L</code>	Load keys to memory for all encrypted partitions.
<code>/injectkey</code>	Inject the encryption keys from an ERI file. An automatic comparison takes place to add only the keys of any partition that has been encrypted by a previous FDE installation but is unavailable in the new one.
<code>/tpmoff</code>	Deactivate TPM protection.

/tpmon	Configure activation of TPM protection for next boot.
/tpmrebind	Deactivate TPM protection and configure reactivation for next boot.

■ To decrypt a specific partition, use:

- `pe_erd_console.exe eripath=f:\fde.eri eripwd=12345678 partition=d`
- `pe_erd_console.exe eripath=f:\fde.eri eripwd=12345678 /L`

→ The command prompt will return if the partition is decrypted successfully. If unsuccessful an error will appear followed by the help information in the command prompt.

■ To inject the encryption keys in the ERI file (to re-enable the partitions encrypted by a previous FDE installation), use:

- `pe_erd_console.exe eripath=A:\fde.eri eripwd=12345678 /injectkey`

1. Start the emergency recovery application (GUI).

! If you have stored your ERI file(s) on removable storage media (i.e. USB stick), then insert the media into the computer before starting from the ERD.

2. The first step in performing an emergency recovery with the ERD, is to open the recovery application:

3. Insert the ERD into the CD/DVD drive, start the computer, and allow the computer to boot from the CD. The ERD interface will of course, differ according to which ERD you are using: the WinPE CD only has a commandline interface.

→ The EgoSecure Recovery application should start automatically, but if not, use the command prompt to navigate to the directory: `X:\Program Files\FDE\`  
Enter `pe_erd_w32.exe` <press Enter>. Go to step 4.

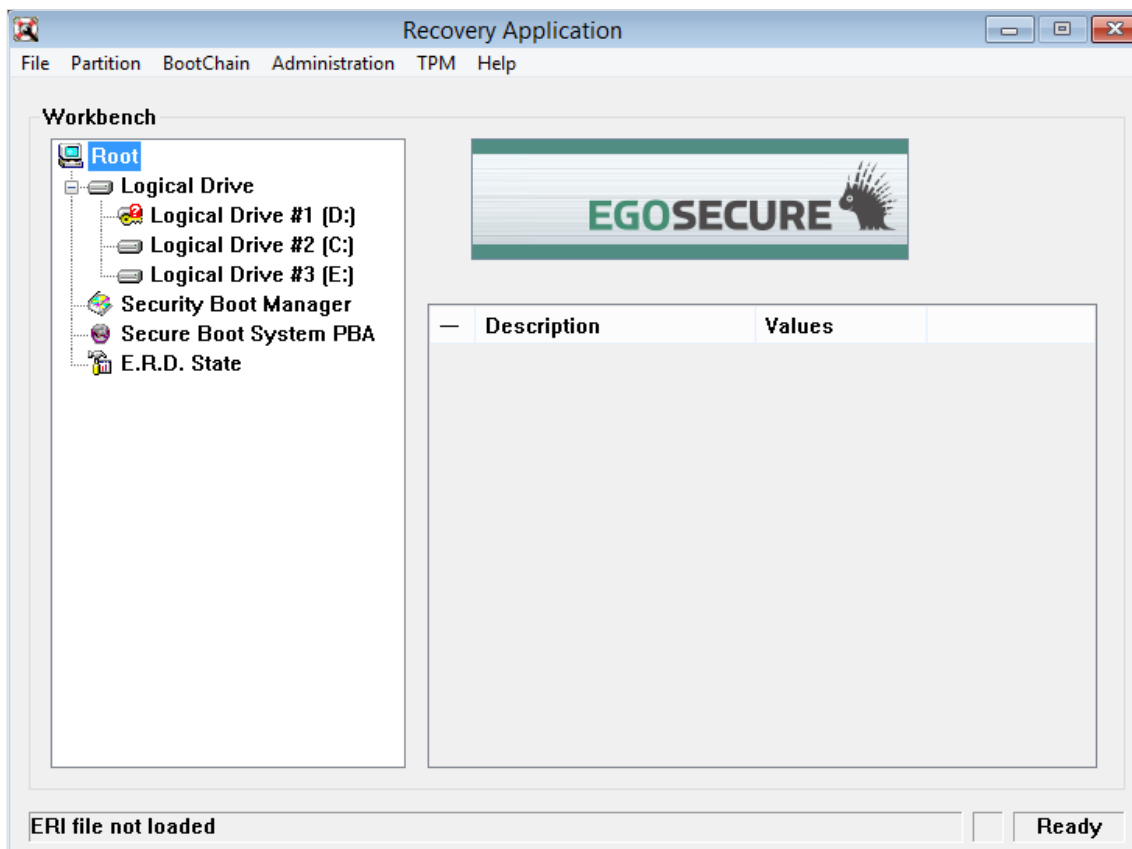
! If the computer does not boot from the CD, then it is likely that the device is not set as the primary boot device in the BIOS. If so, change the BIOS settings accordingly, or possibly start the computer from a 'one-time boot menu'.

4. Open the menu entry `Go>Programs> EgoSecure ERD (ENG)`.

→ The emergency recovery application will start by scanning the *EgoSecure Full Disk Encryption* configuration on the computer:



- The application gathers information about the hard disk as well as information about the PBA and FDE components. The scan may last for a minute so please be patient.
- Once the scan is complete, the main window appears:



The main window enables you to select and perform the operations necessary for recovery. This window has the following functionality:

- Menu commands

The heart of the recovery application. See [Menu commands](#) for details.

- Workbench

This area allows you to choose a topic/node in the left-hand pane to display the information about that node in the right-hand pane. It is possible to right-click each node and select a command specific to that node from the context sensitive menu. However, the **Workbench** area is used mainly to display information specific to a node in the right-hand pane. For further details about each node, refer to the end of this section.

For details about the workbench nodes visible for standard hard disks, see [Workbench for standard hard disks](#).

5. Before proceeding with any recovery task you must first authenticate yourself via one of the following methods:

- Load the ERI file. For details, see [Load ERI](#).
- Enter the encryption keys manually (software FDE). For details, refer to [Enter the encryption key manually](#).

The following commands are the heart of the recovery application.

Menu Command	Details
File	<ul style="list-style-type: none"> <li>■ <b>Open ERI file</b> This option opens an explorer window to locate and load the ERI (.eri) file.</li> <li>■ <b>Load ERI file from cache</b> This option loads the cached, and encrypted, ERI (.eri) information directly from the hard disk.</li> <li>■ <b>End</b> Exit the application.</li> </ul>
Partition	<ul style="list-style-type: none"> <li>■ <b>Repair VBR</b> This option restores a damaged VBR sector of a partition using one of the methods: <i>Generate new VBR</i> (creates a new VBR sector using a template) or <i>Use VBR backup</i> (uses a backup of a VBR sector from the same partition).</li> <li>■ <b>Decrypt drive</b> This option decrypts the drive selected in the left-hand pane of the window. Refer to <a href="#">Decrypt a drive</a> for details.</li> <li>■ <b>InputKey</b> This option allows you to input keys manually.</li> <li>■ <b>Key Injection</b> Inject the encryption keys from an ERI file, the automatic comparison takes place to add only the keys of the any partition that has been encrypted by a previous FDE installation but is unavailable in the new one. See <a href="#">Enter the encryption key from ERI file</a> for details.</li> </ul>
BootChain	<ul style="list-style-type: none"> <li>■ <b>Repair UEFI (only for UEFI systems)</b> This option changes the boot order so that the Secure Boot Manager becomes the first one in the list of loaders.</li> <li>■ <b>Repair MBR (only for BIOS systems)</b> This option allows you to repair the Master Boot Record. See <a href="#">Repair MBR</a> for details.</li> <li>■ <b>Restore original MBR (only for BIOS systems)</b> This option is available only after successful ERI authentication. This</li> </ul>

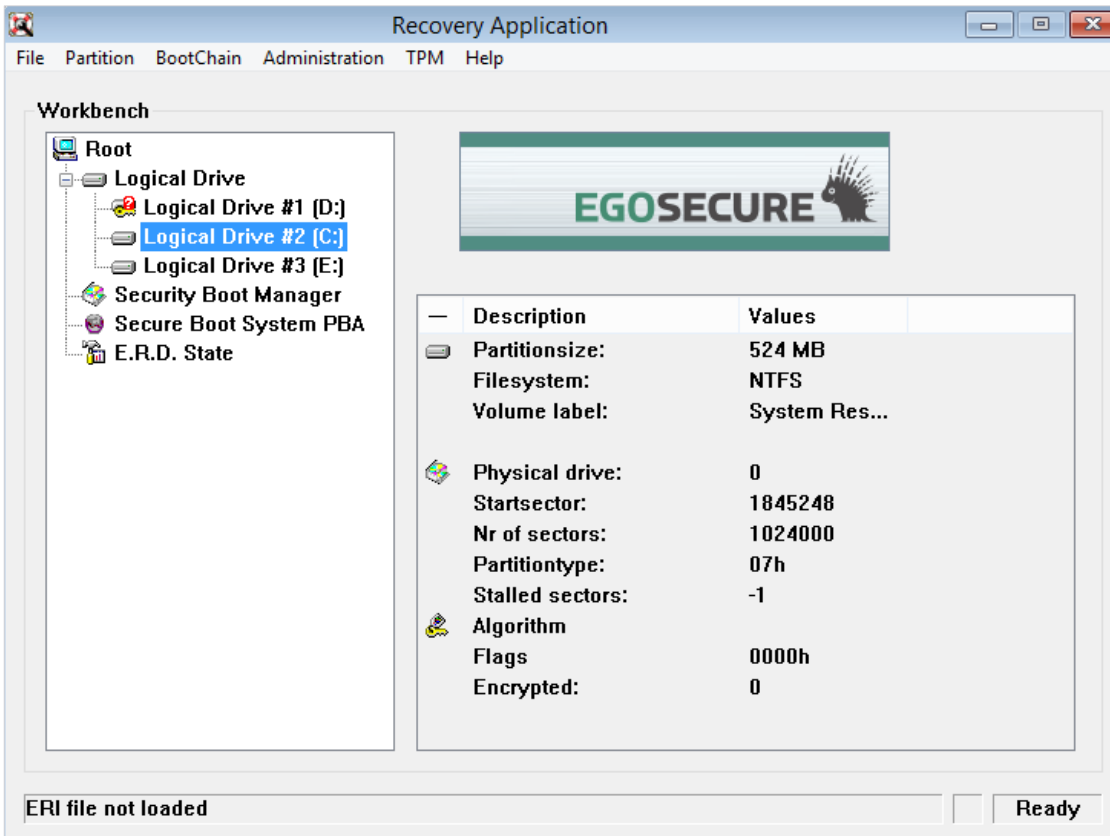
Menu Command	Details
	<p>option searches for backed-up MBR file and once found it will extract the MBR and overwrite the EgoSecure MBR with the 'old' one. Refer to <a href="#">Restore original MBR</a> for details.</p> <ul style="list-style-type: none"> <li>■ <b>Set Active Partition</b> This option allows you to set the active partition. For details, see <a href="#">Set active partition</a>.</li> <li>■ <b>Disable PBA load check</b> This option disables the security measure, which checks whether the Secure Boot Manager loaded the system (if the system was loaded by any other loader, BSOD occurs). If the system disk is encrypted decrypt it before disabling PBA load check. (To decrypt, load ERI file, select the system disk from the list and click Partition &gt; Decrypt drive).</li> </ul>
Administration	<ul style="list-style-type: none"> <li>■ <b>Set admin-password</b> This option allows you to set the Control Center administration password. For details, see <a href="#">Set the administration password</a>.</li> <li>■ <b>Collect log files</b> This option allows to collect the log files of the recovery application. The WinPE log files are necessary for the support to investigate issues with a recovery process.</li> </ul>
TPM	<ul style="list-style-type: none"> <li>■ <b>Activate</b> Activate TPM functionality in <i>EgoSecure Full Disk Encryption</i>. A restart is necessary to complete this function.</li> <li>■ <b>Deactivate</b> Deactivate TPM functionality in <i>EgoSecure Full Disk Encryption</i>.</li> <li>■ <b>Rebind</b> This deactivates and re-activates the TPM in one command. For details about TPM usage, see Chapter 3 'Trusted Platform Module'.</li> </ul>
Help	<ul style="list-style-type: none"> <li>■ <b>About</b> This displays version and copyright information.</li> </ul>

## Workbench for standard hard disks

Each node in the left-hand pane has a self-explanatory label. When selected, the details about that node are displayed in the right-hand pane:

- Logical drives





The **Logical Drive** node displays the internal partitions/hard disks on the computer. The hard disk/partition icon can change according to the hard disk state:

**Table 1. Status of the encryption**

Icon	Meaning
	Partition is encrypted and the disk encryption key (DEK) is available.
	Partition is encrypted but the disk encryption key (DEK) is not available.
	Hard disk is currently unlocked.
	The hard disk has a problem or is in an undefined state. This icon appears if the EgoSecure Full Disk Encryption is not yet installed.

The following information is displayed when a partition/hard disk is selected:

**Table 2. Partition/Hard Disk Status**

Attribute	Values
Partitionsize	The size of the selected partition.
Filesystem	The format of the selected partition.
Volume Label	The name of the partition (if any).
Physical Drive	The index of the physical hard disk. The primary hard disk is indicated by the value 0. Any other value indicates a secondary hard disk.
Startsector	The sector on the hard disk that is first used to store data.

Number of Sectors	The total number of sectors on the selected partition.
Partitiontype	The file system used in the partition. <i>07h</i> means NTFS, <i>95</i> is our own proprietary partition, and <i>0E</i> is FAT32.
Stalled Sector	The sector on the hard disk that is last used to store data.
Algorithm	The algorithm used to encrypt the partition. An algorithm will only be recognized if the partition was encrypted using EgoSecure Full Disk Encryption.
Flags	This is a bitmap that indicates if the drive is encrypted, partly encrypted or plain (last bit is set) and how it is encrypted. For instance <i>601</i> means the drive is CBC encrypted.
Encrypted	<i>0</i> = partition is not encrypted <i>1</i> = partition is encrypted

■ Security Boot Manager

This node displays the following boot manager information:

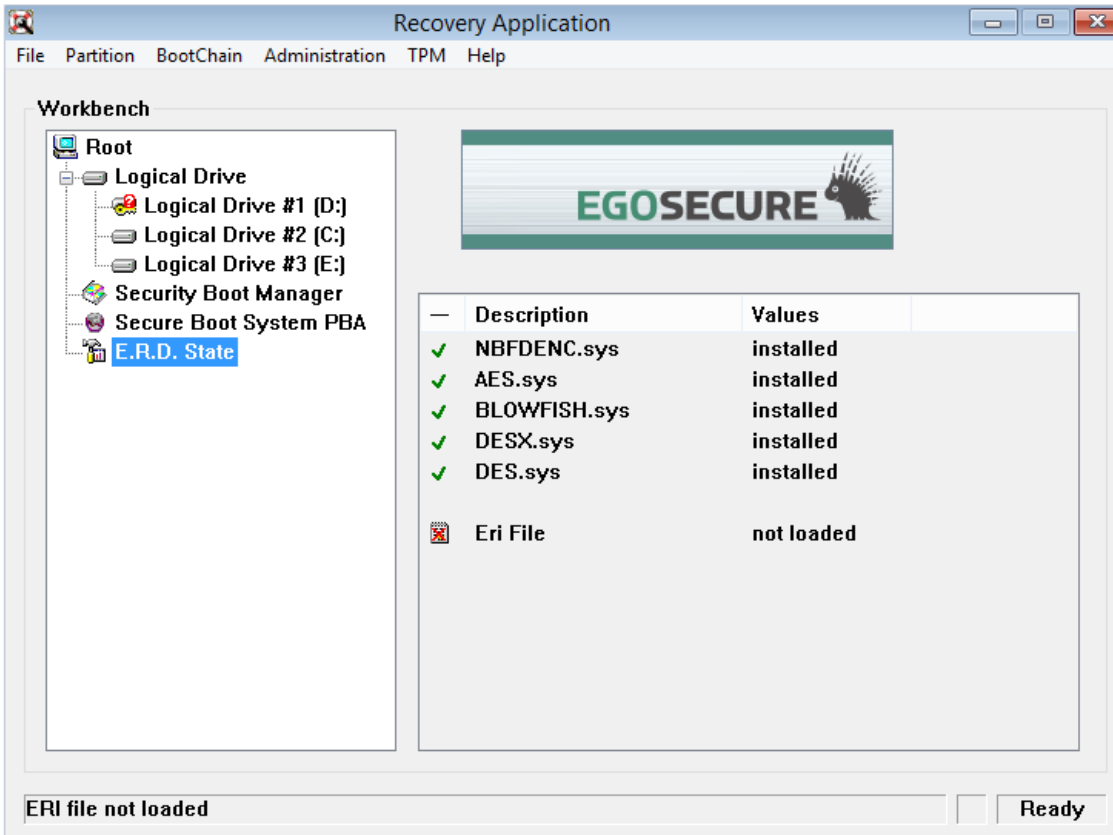
Attribute	Values
FDE-Partition	This entry is visible twice in the list. The first entry states whether an FDE partition is available, the second if it is active (i.e. encrypted).
KEK-Information	This entry indicates if the structure where the keys are stored exists.
FDE Bootstrap	This entry indicates if the section where the FDE bootcode is stored exists.
PBA Bootstrap	This entry indicates if the boot sector of the 95 Partition (Linux boot loader) exists.
PBA loader	This entry indicates if the 16 bit code which is executed after the Linux PBA was finished.
Real-Mode-PBA	This entry indicates if the bootcode that starts Windows exists.
16Bit-Algorithms	This entry indicates if the 16 bit implementation of the encryption algorithms exists.

■ Security Boot System PBA

This node displays the following PBA component information:

Attribute	Values
Security Boot System PBA	A short message to inform whether the PBA components is installed.

## ■ ERD State



This node displays information about the encryption algorithms loaded into the environment as well as if an ERI file has been successfully loaded into the emergency recovery application.

This following information is available:

Attribute	Values
NBFDENC.sys	This entry indicates if the 32 Bit encryption driver for full-disk encryption exists.
AES.sys, Blowfish.sys, DESX.sys, DES.sys	These entries state whether each of the encryption components has been loaded by the emergency recovery application.
ERI File	This entry states whether the ERI file has been loaded into the emergency recovery application.

### Load ERI

Once the application is started, the next task you have to perform is to load the ERI file into the emergency recovery application. The ERI file can be loaded [from computer](#) or emergency recovery information (ERI) can be loaded [from cache](#).



**Loading ERI required**

Without loading an ERI file, none of the recovery functions are active.

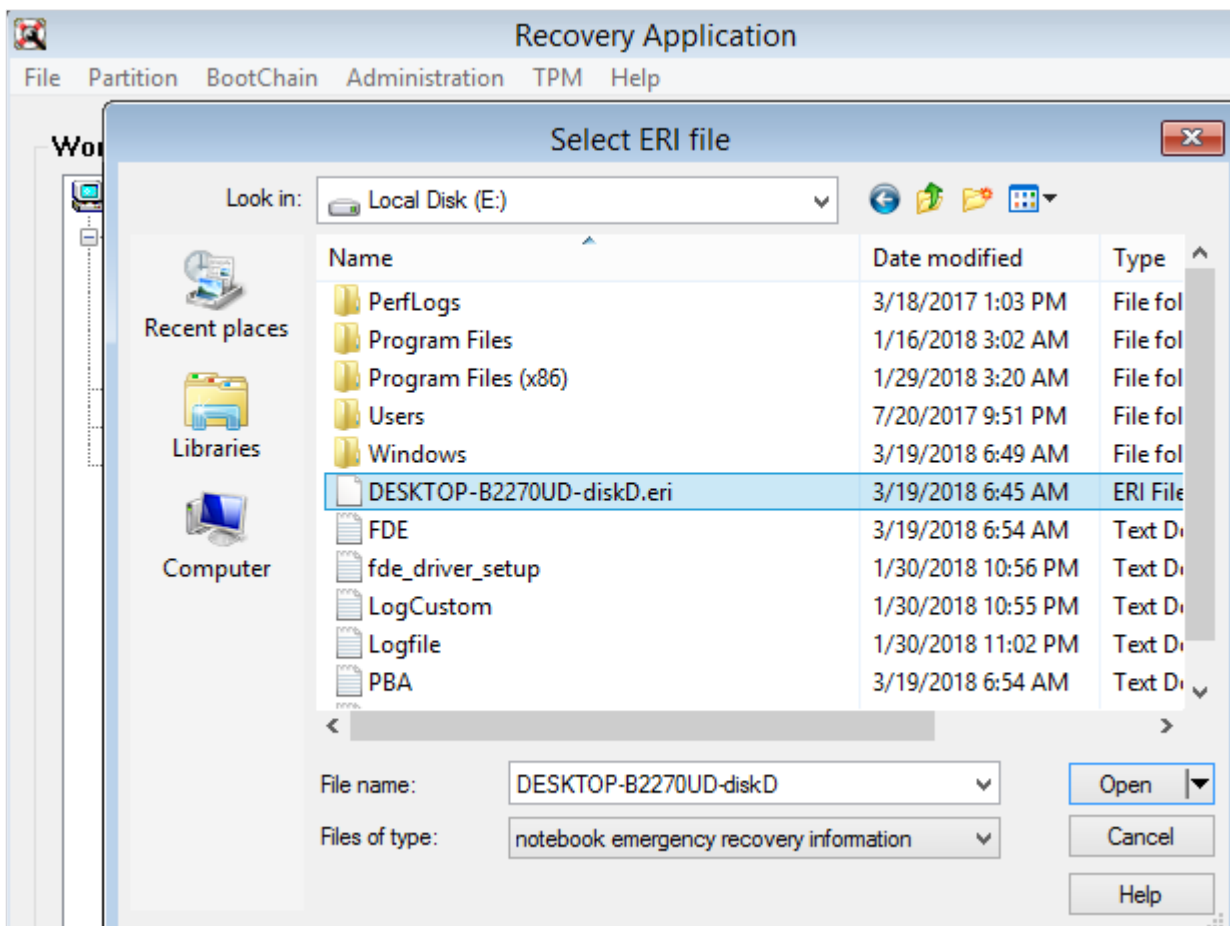
INFO

**Loading ERI file from computer**

1. Start the emergency recovery CD as stated in [Start the emergency recovery application \(GUI\)](#).

Select the menu command **File | Open ERI file**.

→ The **Select ERI file** dialog appears:



→ The file explorer should automatically open the directory in which the relevant ERI file(s) are stored – providing that the creation of the ERD was performed according to [Creating a WinPE emergency recovery boot CD or USB flash drive](#). If not, then use the following path:

<ERD>\Programs\FIS\ERI\

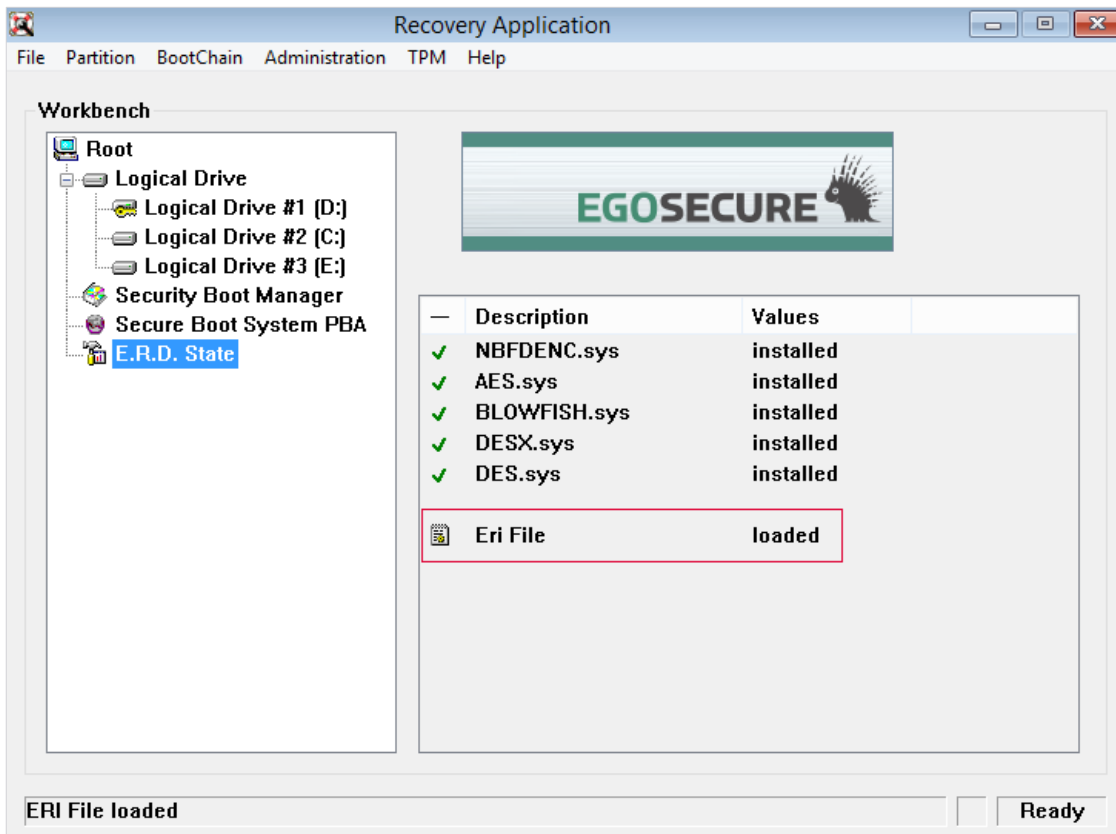
Select the correct ERI file and click **Open**. If you have stored the ERI file(s) on removable storage media (i.e. USB stick), then locate them there.

→ If you protected the ERI file with a password during its creation, then you would now be prompted to enter the password.

2. Once the password is entered, click **OK**.

→ If the password is valid, the ERI file is loaded into the emergency recovery application.

The main window reappears, confirming that the ERI file has been loaded:



## Loading ERI from cache

ERI can be loaded from cache if the **Cache emergency recovery information on disk** option was checked before disk encryption. ERI file password is required.

1. Start the emergency recovery CD as stated in [Start the emergency recovery application \(GUI\)](#).

Select the menu command **File | Load ERI from Cache**.

→ The **Enter ERI Password** dialog appears.

2. Enter the password defined for the ERI file.

! Only the English keyboard layout is supported.

3. Click **OK**.

## Further tasks

Now that the ERI file is loaded you can continue to repair/recover the computer using the following methods:

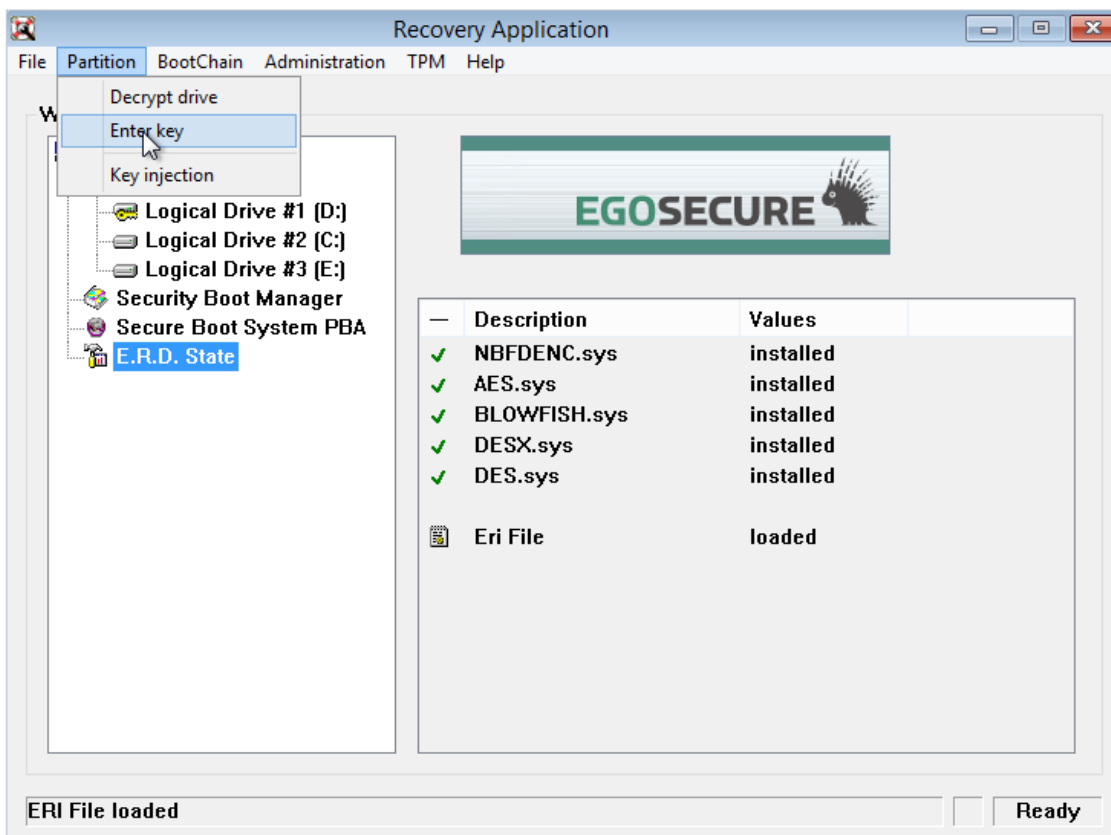
- Decrypt a drive. For details, see [Decrypt a drive](#).
- Update the master boot record (MBR). For details, see [Repair MBR](#).
- Replace the Original MBR. For details, see [Restore original MBR](#).
- Set the administration password. For details, see [Set the administration password](#).

## Entering the encryption key manually

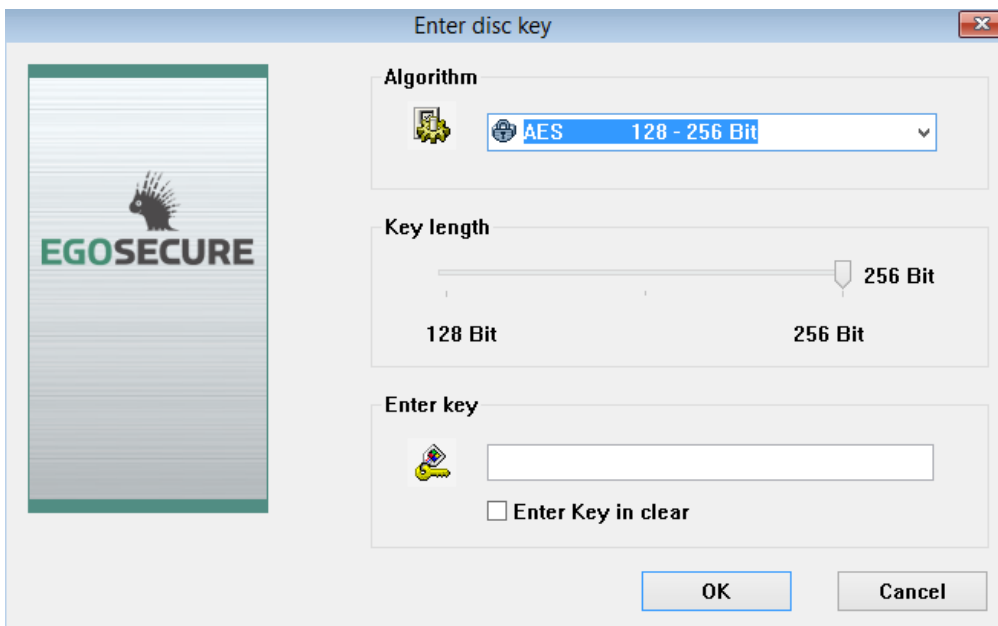
If there is no ERI file available for the damaged computer, you have the option to enter the encryption keys manually. The keys used to encrypt each partition of the hard disk must be entered before you can use the emergency recovery application to decrypt any drive. Follow these steps to enter the encryption key(s):

1. To activate all the recovery options in the recovery application, open an arbitrary ERI file via the Menu option *File > Open ERI file* (refer to [Load ERI](#)). It does not matter which ERI file is used – it can belong to any computer. If prompted, enter the password for the ERI file.

Select the partition to decrypt from the **Logical drives** node in the left-hand pane of the main window. Subsequently, select the option **Enter Key** from the **Partition** menu:



→ The **Enter disk key** dialog appears.



This dialog allows you to enter the encryption parameters set for the drive/partition in question.

The following options are available:

GUI element	Details
Algorithm	Here you have to select the algorithm that was used to encrypt the drive.
Key length	Some encryption algorithms support different key lengths. Use the slider to define the correct key length for the selected algorithm and partition.
Key input	Enter the encryption key password used for the partition into this field. Check Enter key in clear to make the password entry visible.

2. Once the information is entered, click **OK**. If the information is correct, it is loaded into the emergency recovery application.

- The ERD main window reappears. Repeat steps 2 and 3 for every encrypted partition you need to decrypt.
- Drive decryption can now be performed (see next section).

### Decrypting a drive

This procedure can be used when you have either not decrypted the hard disk(s) before removing *EgoSecure Full Disk Encryption* or if the decryption of a hard disk was interrupted (due to power failure) and needs to be continued.



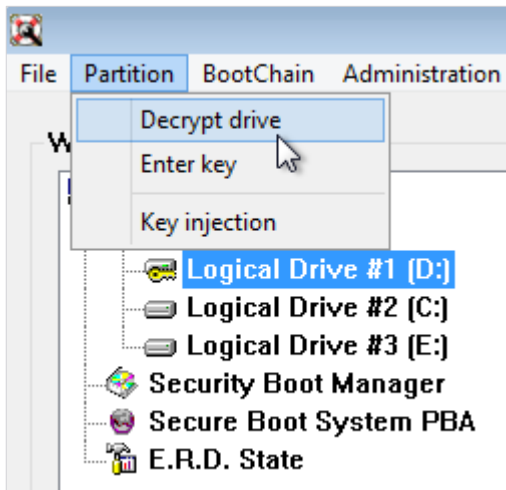
#### ATTENTION

#### Valid ERI file or encryption key required

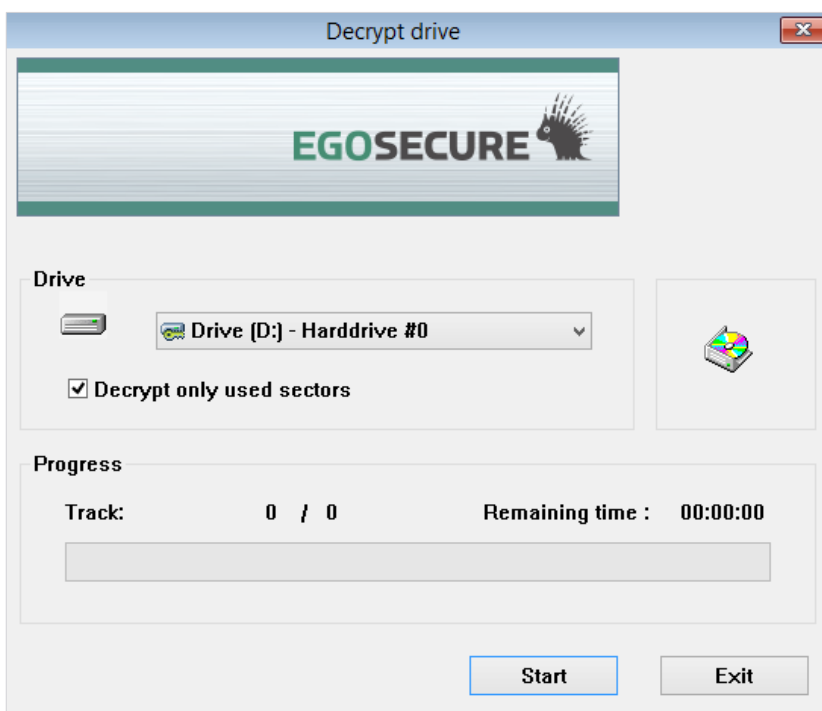
This procedure assumes that either a valid ERI file has been loaded or that the encryption key has been entered manually, and that the drive node has been selected.

Follow these steps to decrypt a partition/hard disk via the ERD:

1. Make sure that you have loaded the correct ERI file via the Menu option *File > Open ERI file* (see [Load ERI](#)).
2. Select the respective drive from the tree in the left-hand pane.
3. Select the **Decrypt drive** option from the **Partition** menu.



→ The **Decrypt drive** dialog appears.



4. From the **Drive** combo box, select a drive for decryption.
5. Check the **Decrypt only used sectors** option to decrypt only those sectors of the selected drive that contain data. Leave this option unchecked to decrypt every sector (this will take longer).
6. Click **OK** to begin the decryption.



- ! Any loss of power during the decryption process may cause data corruption. The decryption of a hard disk may take some considerable time depending on the size of the disk and the speed of the computer.

## Entering the encryption key from ERI file

Inject the encryption keys from an ERI file, the automatic comparison takes place to add only the keys of the any partition that has been encrypted by a previous FDE installation but is unavailable in the new one.



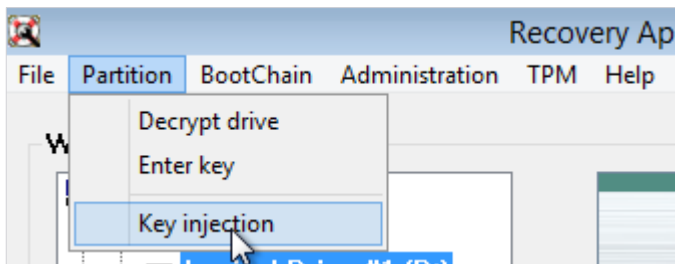
### ATTENTION

#### Valid ERI file or encryption key required

This procedure assumes that either a valid ERI file has been loaded or that the encryption key has been entered manually, and that the drive node has been selected.

1. Make sure that you have loaded the correct ERI file via the Menu option *File > Open ERI file* (see [Load ERI](#)).

Select the **Key Injection** option from the **Partition** menu.



→ The success message appears if encryption keys are encrypted.

Click **OK** to close the message.

## Decrypting a drive in a silent mode

To enable the decryption of a partition without using a graphical user interface you can use the emergency recovery console (`pe_erd_console.exe`) from within the *WinPE 2.x* boot CDs. This section details the console and the commands/options open to you.

Follow these steps to decrypt a drive from the ERD:

1. Once you have booted the target computer using the WinPE ERD, open a command prompt window.

Use the following commands to decrypt drives/partitions (case insensitive):

```
pe_erd_console.exe eripath=<?> eripwd=<?> partition=<?>
```

The following options are available:

Option	Details
ERIPATH	The path to the ERI file

ERIPWD	The password for the ERI file
PARTITION	The letter of the partition/hard disk to be decrypted
/H	Help – information about each option available in the console
/L	Load keys to memory

For example:

- `pe_erd_console.exe eripwd=87654321 eripath=f:\fde.eri partition=d`
- `pe_erd_console.exe eripwd=87654321 eripath=f:\fde.eri /L`

During and until the decryption process is finished, a series of dots will appear in the command prompt. Depending on how large the partition is, the number of dots may scroll the command prompt – this is normal!

If the decryption is finished successfully, the message `'Hard disk was successfully decrypted'` appears. If the decryption is unsuccessful an error message will appear.

### Repairing MBR

It may be necessary to update the MBR if your computer does not start after the installation of a third-party application. The most likely cause is that the installer has modified the MBR. Follow these steps to update the MBR:

1. Make sure that you have loaded the correct ERI file via the Menu option *File > Open ERI file* (see [Load ERI](#)).

In the main window select the Menu option *BootChain > Repair MBR*. The **Repair MBR** dialog appears:



2. Click **OK** to start the procedure.
  - Once complete, the dialog will close automatically with no further prompting or interaction.

## Restoring original MBR

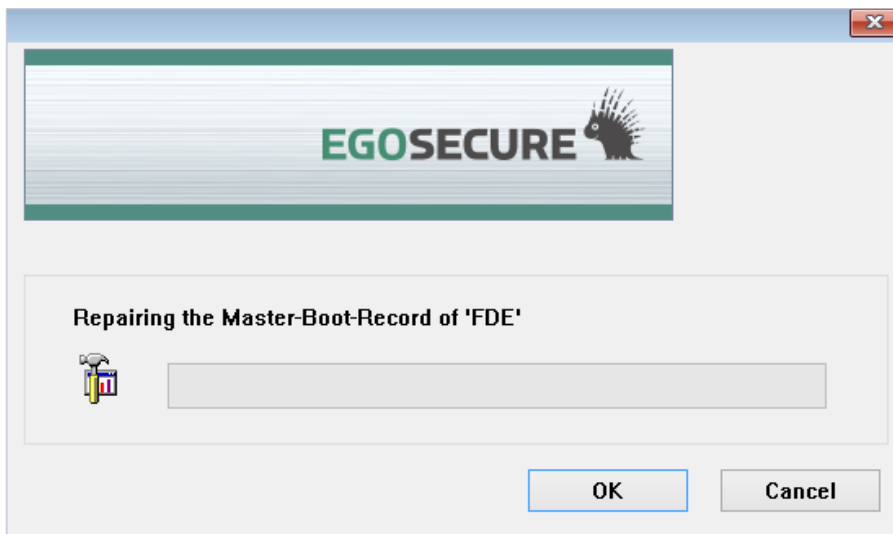
This option replaces the EgoSecure MBR with the original MBR archived by EgoSecure during installation.

Follow these steps to replace the EgoSecure MBR:

1. Make sure that you have loaded the correct ERI file via the Menu option *File > Open ERI file* (see [Load ERI](#)).

In the main window select the Menu option *BootChain > Restore Original MBR*.

→ The MBR repair dialog appears:



→ Once complete, the dialog will close automatically with no further prompting or interaction.

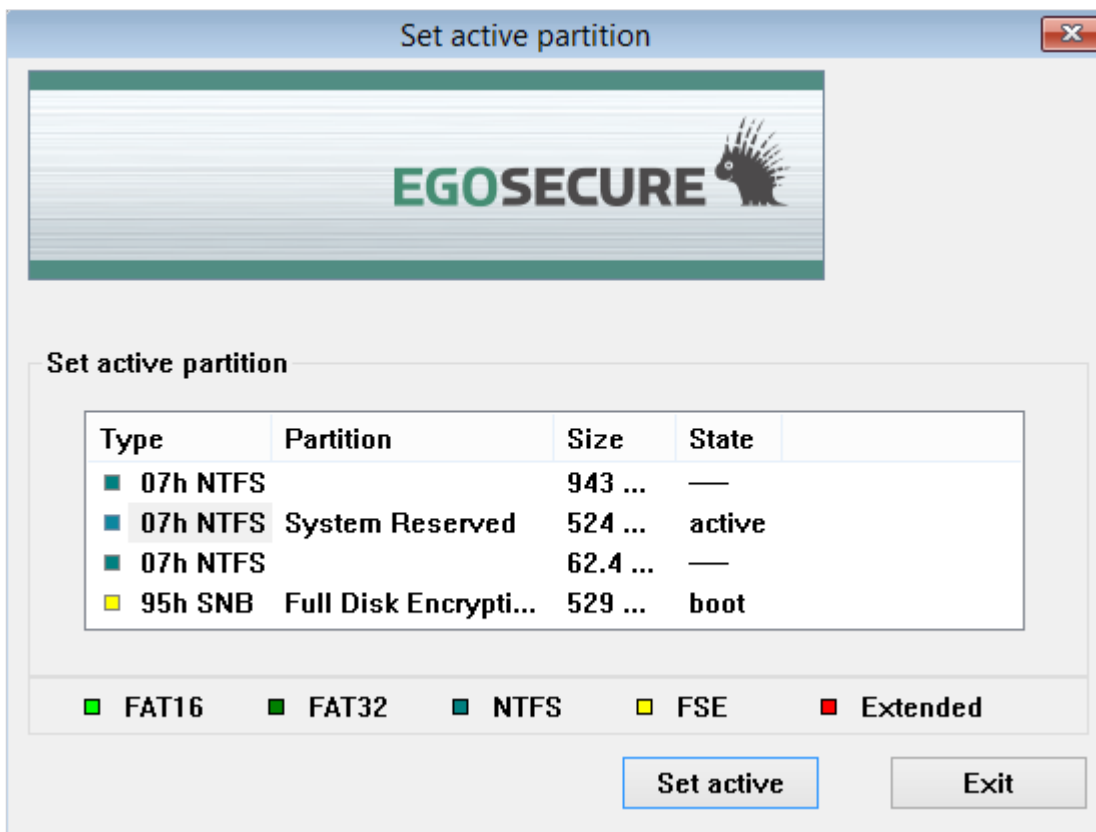
## Setting active partition

This option allows the user to set active partition for the MBR. The active partition becomes the boot sector for the MBR to load the boot program.

Follow these steps to set active partition:

1. Make sure that you have loaded the correct ERI file via the Menu option *File > Open ERI file* (see [Load ERI](#)).

In the main window select the Menu option *BootChain > Set active partition*. The **Set active partition** dialog appears:



2. Select the partition and click **Set active**.

→ The selected partition becomes the active partition for the MBR.

### Setting the administration password

Use this feature to set the Control Center administration password.

1. In the main window select the menu option *Administration > Set admin password*.

→ The **Set admin password** dialog appears.

2. Enter and confirm a new password.

3. Click **OK**.

4. Once the password has been changed close the emergency recovery application (*File > Exit*).

5. Click *GO > Shut down > Restart* to end this procedure and to restart the computer. Windows should boot as normal.

## 1.14. Remote Administration

Deploying a policy locally may be useful for a uniform installation of EgoSecure Full Disk Encryption on a small number of computers or on an ad-hoc basis. But what about a large number of computers scattered throughout a company that need to be installed or updated as soon as they are connected to the network?

This section details how to install, and configure EgoSecure Full Disk Encryption remotely via the use of policy files. For details about unattended installation, the [EgoSecure FDE – Installation and Troubleshooting Guide](#), chapter 2.4, subchapter “Unattended installation”.

## Policy files

A *policy file* is a file that contains all the required EgoSecure Full Disk Encryption configuration settings for the target computer. These policy files can be created using the Policy Builder (for details, see section [2](#)).

There are two types of policy files:

- **Full Disk Encryption policies** to configure the Full Disk Encryption mechanism as well as boot security settings and external media control.
- **Pre-Boot Authentication policies** for the PBA component.

## Administration tasks

The following tasks can be performed using policy files:

*FDE policy files* can be used to:

- Install, remove, and configure FDE boot security settings.
- Install, remove, and configure FDE external mass storage media encryption.
- Encrypt and decrypt hard disk partitions.
- Create ERI and configure ERI password restrictions.
- Change Administration password.
- Configure Logging, TPM, Branding or HelpDesk text updates.
- Remove the whole product or deinitialize FDE.

*PBA policy files* can be used to:

- Install and configure PBA smart card reader and PKCS#11 settings.
- Install and configure PBA settings for encryption mechanisms and certificate labels.
- Configure authentication options to PBA.
- Change Administration password.
- Configure Pre-boot appearance
- Update the branding or HelpDesk text files.
- Configure Logfile settings.
- Add/Remove HelpDesk key to PBA.
- De-initialize PBA or remove PBA

## Deploying Full Disk Encryption policies

To remotely administrate *EgoSecure Full Disk Encryption* the following tasks are required:

1. Create a *Full Disk Encryption* policy that contains all the required settings for the target computers (for details, see [Creating an initialization policy](#)).

Save this policy under the filename 'Autoconf.nbs'.

Copy the Autoconf.nbs policy to each target computer, in the FDE installation directory.

Usually the FDE installation directory is: C:\WINDOWS\NAC.

There are now two different ways to start processing the policy:

- Restart the computer to automatically process the Autoconf.nbs file when the target computer boots. After successfully processing the FDE policy, the Autoconf.nbs will be deleted on the target computer.
- Restart the **pbaservice** service (can be performed via services.msc).

For details about creating FDE policies, see section [2.1](#).

## Deploying Pre-Boot Authentication policies

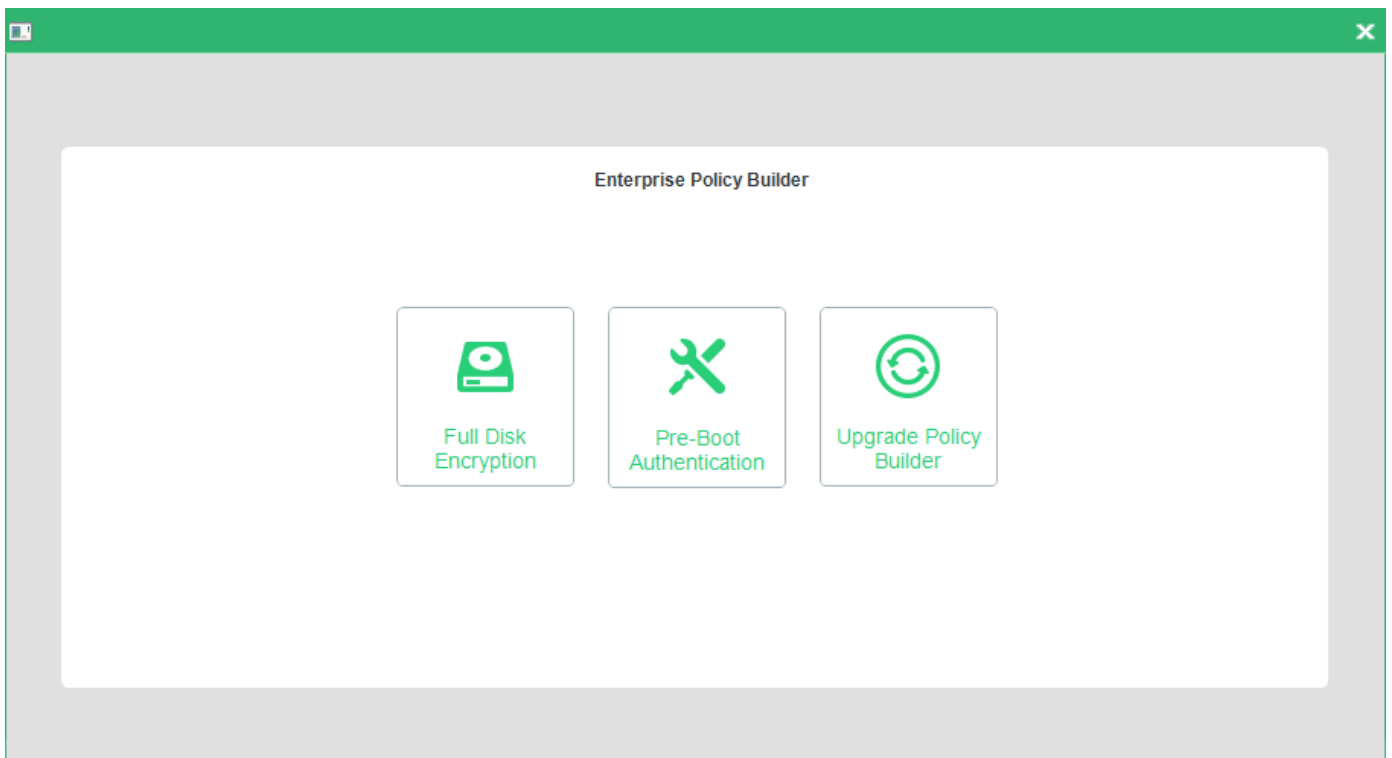
Follow these steps to perform remote PBA administrative tasks:

1. Create a PBA policy that contains all the settings required for the target computers and save this policy under the filename Autoconf.PBA. For further information refer to chapter [2.2](#).
2. Copy autoconf.PBA to the PBA installation directory on each target computer. Usually the PBA installation directory is: C:WINDOWS\NAC\SBS.
3. There are now two different ways to start processing the policy:
  - Restart the computer to automatically process the Autoconf.pba file when the target computer boots. After successfully processing the PBA policy, the Autoconf.pba will be deleted on the target computer.
  - Restart the **fdeservice** service (can be performed via services.msc).

## 2. BUILDING POLICY FOR DEPLOYMENT

EgoSecure Full Disk Encryption offers administrators the possibility to remotely manage EgoSecure Full Disk Encryption installations with a minimum of effort. This has been realized via the use of policy that can be deployed to either each computer, or to a central server. To this end, Policy Builder has been developed to give administrators full control over every aspect of EgoSecure Full Disk Encryption security:

- The **Policy Builder** is a tool to create and edit policies for the purpose of configuration, initialization, and de-initialization of FDE and PBA components. The purpose of these policies is to allow for an administrator to remotely control and ensure the consistent, central deployment, and configuration of FDE and PBA with no need for user interaction.



- The **Full Disk Encryption policy builder** creates policies to configure the Full Disk Encryption component.
- The **Pre-Boot Authentication policy builder** creates policies to configure the PBA component.
- The **Upgrade policy builder** allows you to create an upgrade policy to prevent the FDE administration password from being entered in the commandline in plain text for the purpose of silently upgrading or removing EgoSecure Full Disk Encryption.

### CONTENTS

- ◆ [The Full Disk Encryption Policy Builder](#)
- ◆ [The Pre-Boot Authentication Policy Builder](#)
- ◆ [Creating an upgrade policy](#)

## 2.1. The Full Disk Encryption Policy Builder

The Full Disk Encryption Policy Builder is used to create and edit policies for the purpose of configuration, initialization, and de-initialization. The purpose of these policies is to allow for an administrator to remotely control and ensure the consistent, central deployment, and configuration of FDE with no need for user interaction.

### ■ Initialization Policy

These policies allow you to initialize and configure computers that already have EgoSecure Full Disk Encryption installed but not yet initialized.

### ■ Configuration Policy

These policies allow you to either perform a new installation of FDE to another networked computer (remote installation), or to remotely configure FDE after it has been installed.

### ■ De-initialization Policy

These policies allow you to decrypt drives or remove boot security on a client machine, or remove the whole product (for details, see [Creating deinitialization policy](#)).

A policy is usually created on a different computer from the computer to which the policy will be deployed. FDE has to be installed on the computer that generates the policy, but boot security and drive encryption do not.

### CONTENTS

- ◆ [Creating an initialization policy](#)
- ◆ [Creating a configuration policy](#)
- ◆ [Creating a de-initialization policy](#)
- ◆ [Editing policies](#)
- ◆ [Deploying Full Disk Encryption policies](#)



#### Storing policy

It is recommended that the policy is stored in the shared network for future reference. Make sure you have the access to the network in case you need to use the policy at a later date.

**INFO**

### Creating an initialization policy

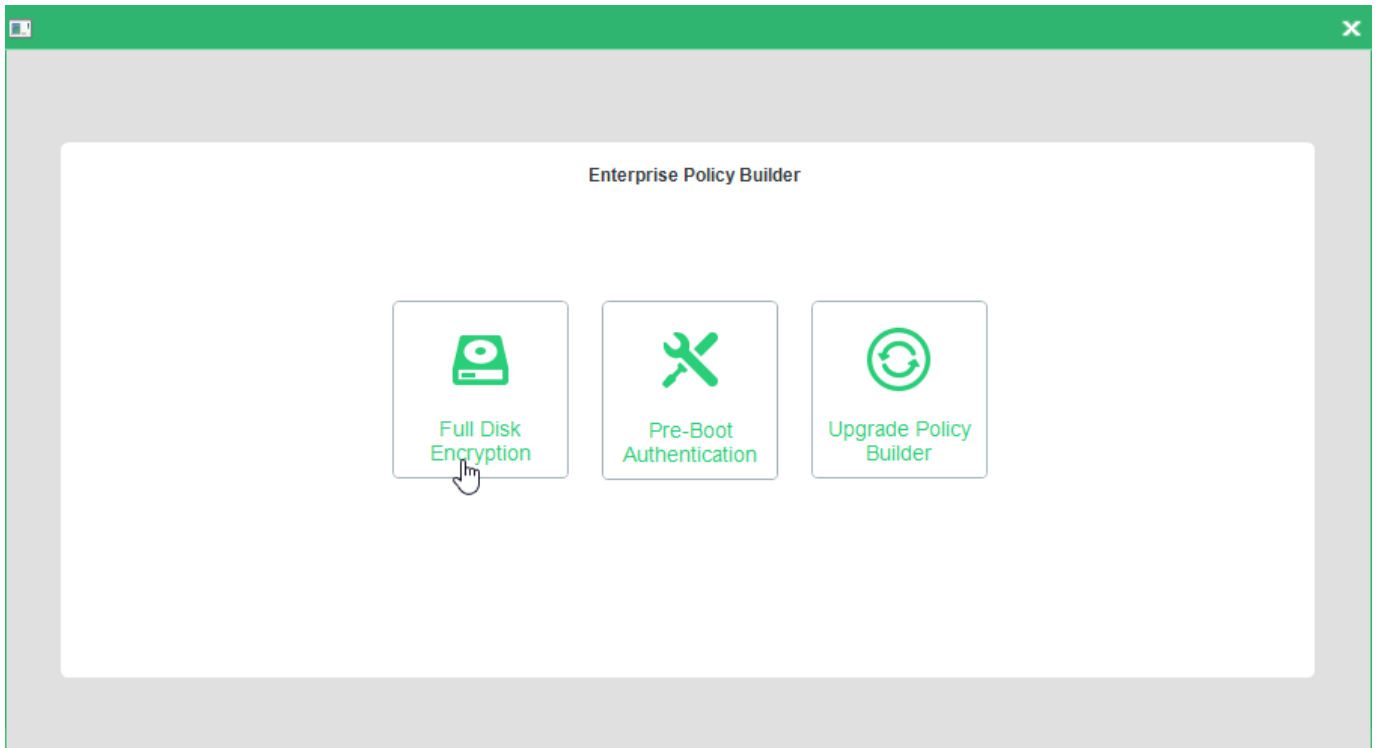
This section details how to create an initialization policy for the FDE component only. You need to have knowledge about the target computer for deployment. Details such as number of partitions, drive letters, whether encrypted, and so on are necessary for the successful deployment of EgoSecure Full Disk Encryption. Once the policy is created, deploy it, for details see [Deploying FDE policies](#).

Follow the steps below to create a FDE initialization policy:

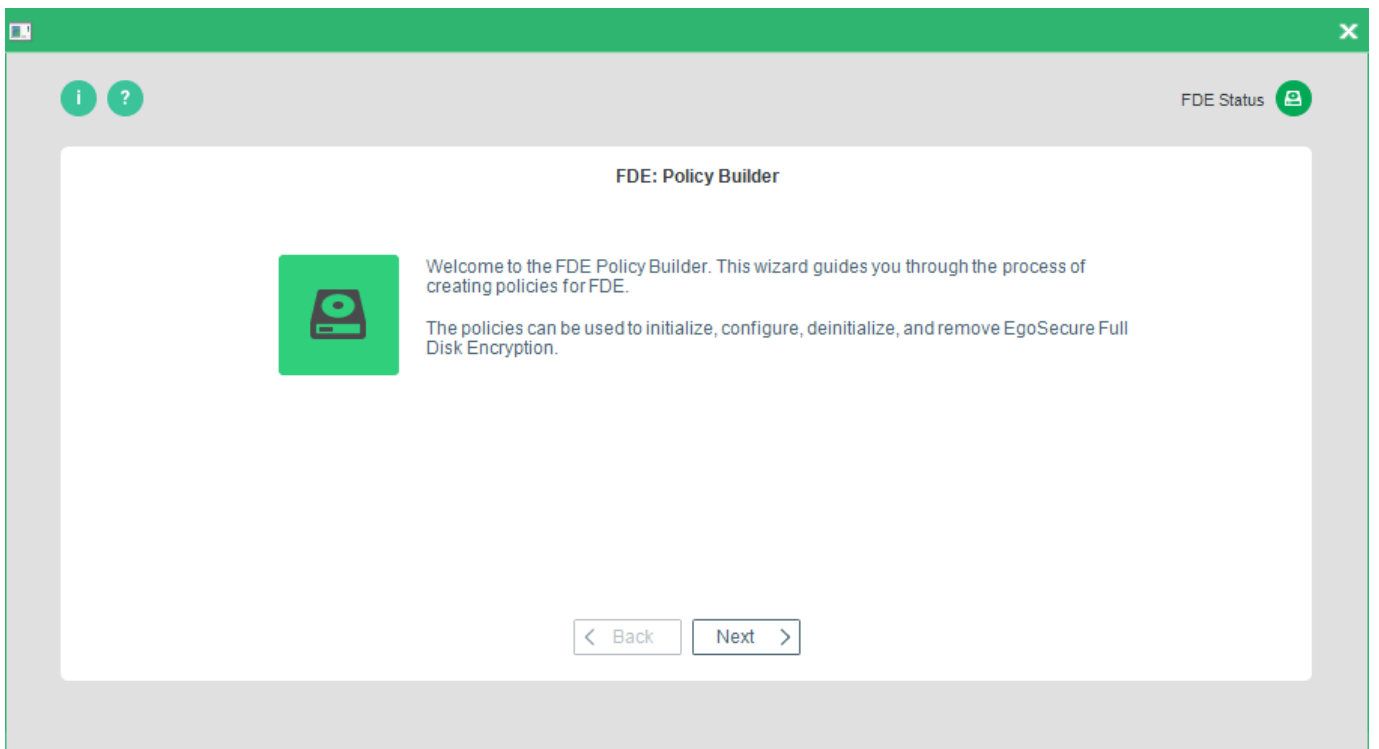
1. Open the **Control Center** (as described in section [1.5](#)).



2. Double-click the Policy Builder icon.
3. Select Full Disk Encryption policy builder.

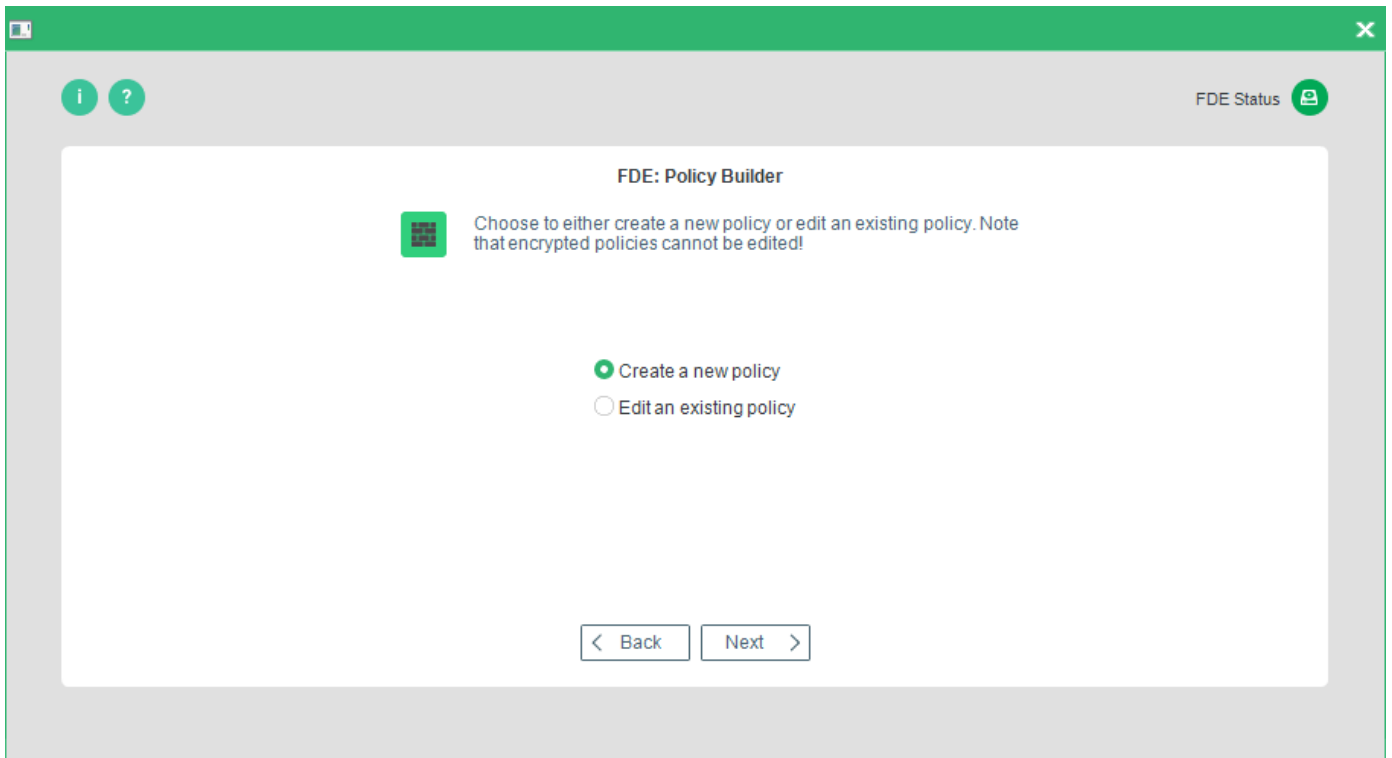


→ The FDE Policy Builder **Welcome** dialog appears.



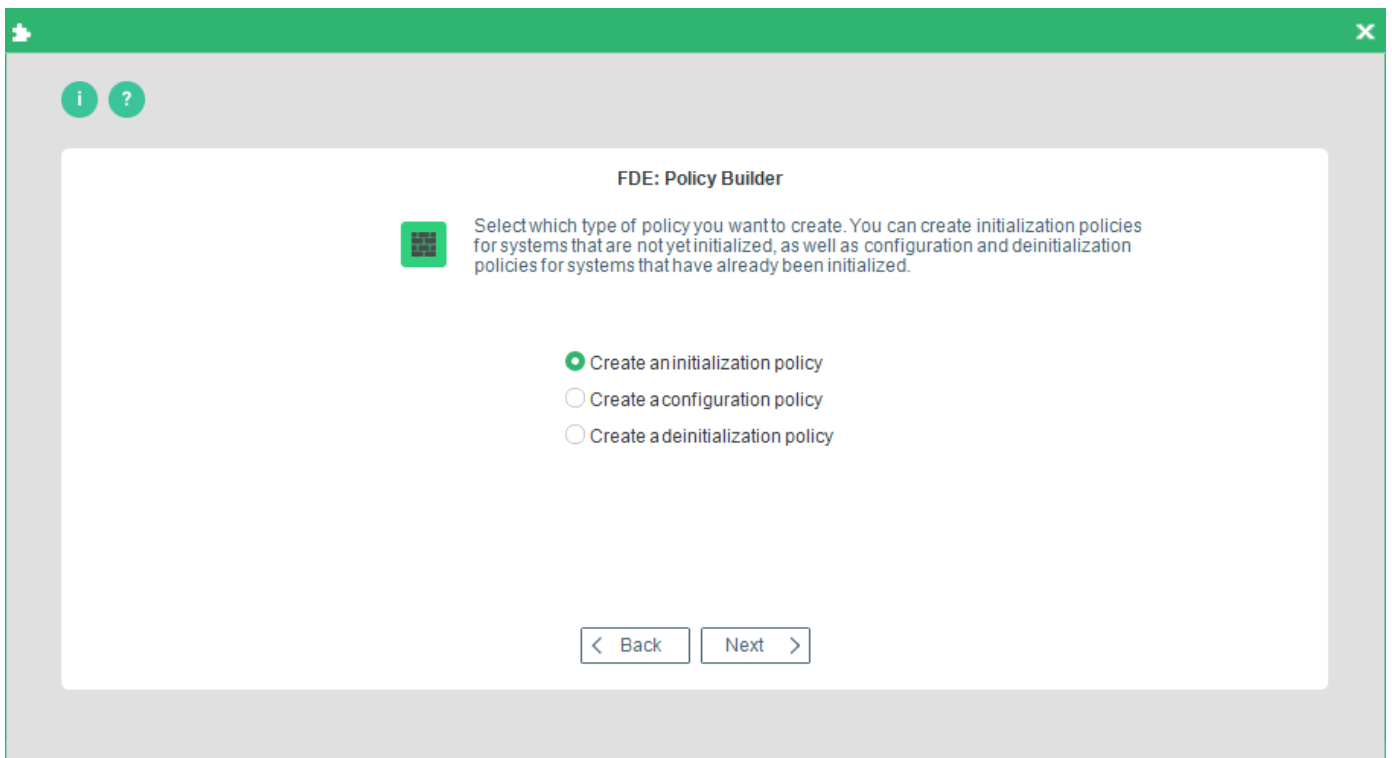
4. Click **Next**.

→ The **Policy selection** dialog appears.



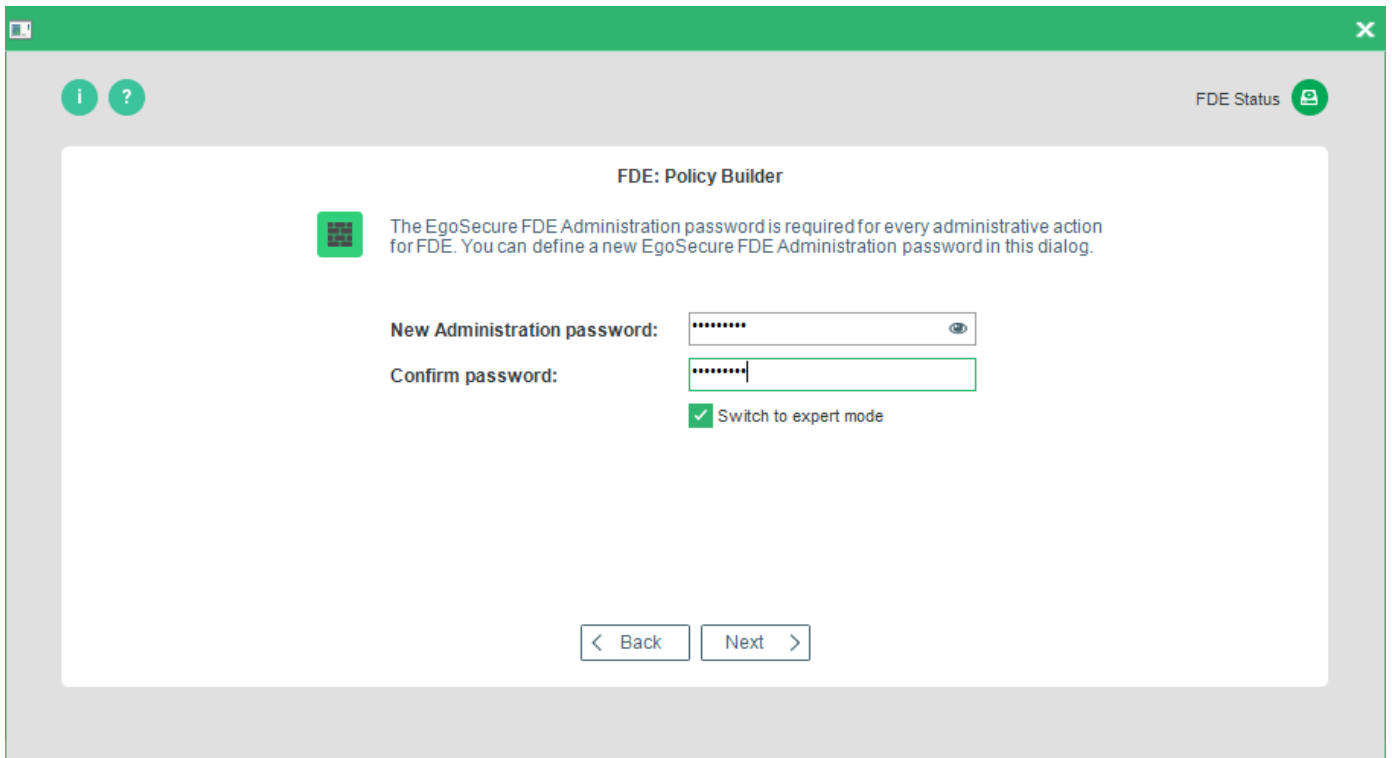
5. Select **Create a new policy**.

→ The **Policy type** dialog appears.

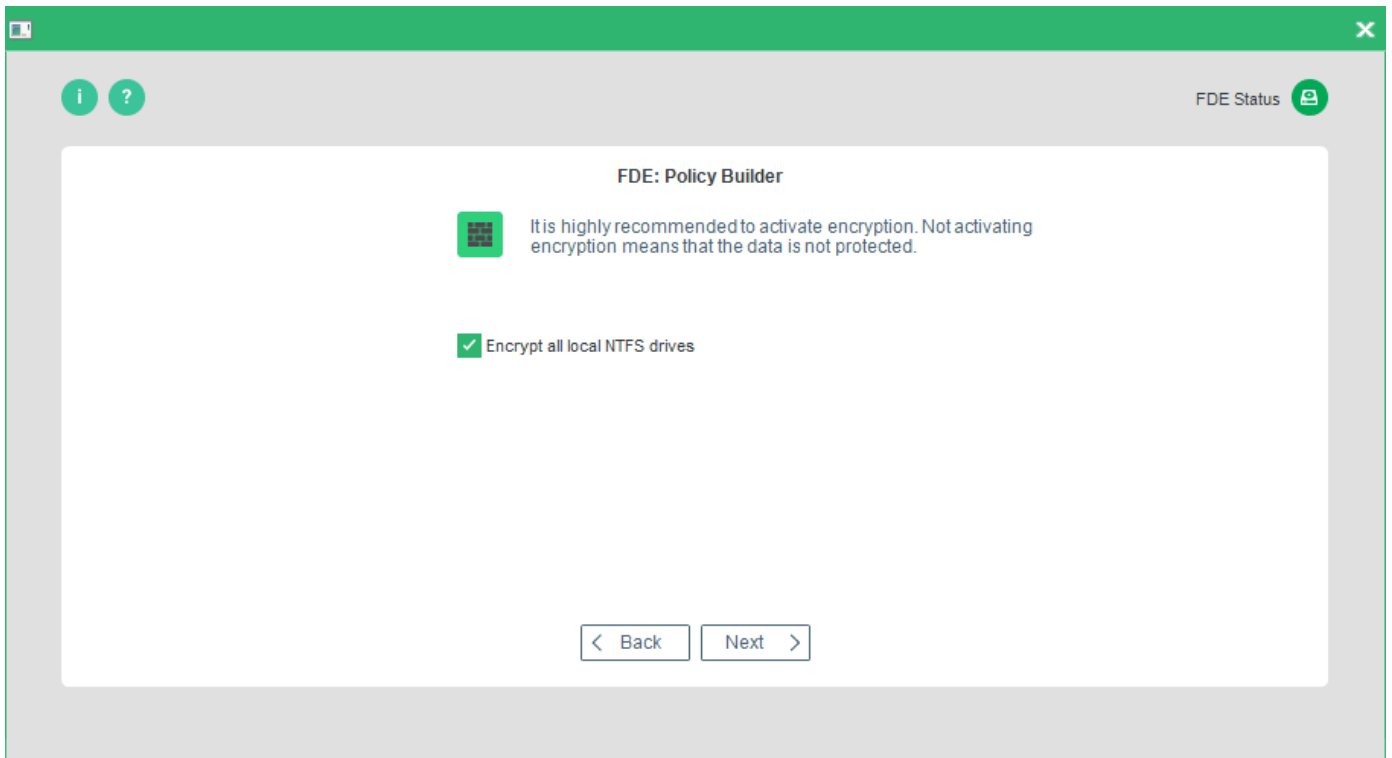


6. Select **Create an initialization policy** and click **Next** to continue.

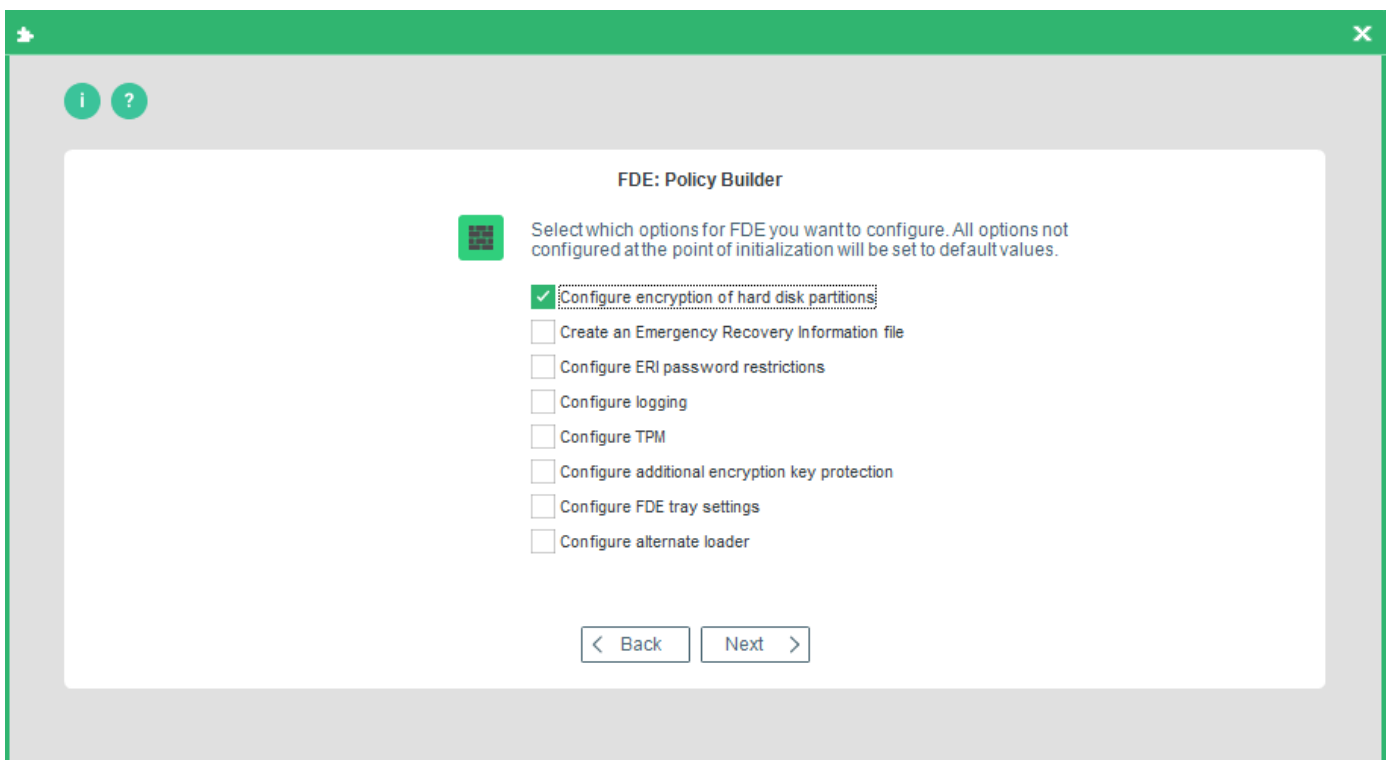
→ The **Administration Password** dialog appears:



7. Enter the administration password defined during installation/initialization. Set the **Switch to expert mode** checkbox to configure every aspect of initialization instead of leaving the defaults active. If you do not check **Switch to expert mode** then you need only refer to steps [9](#), [12](#), [13](#) and [18](#).
8. Once you have made your selection click **Next**.
  - If you DID NOT check **Switch to expert mode** in the previous step then, the **Drive encryption** dialog appears (skip the following step if you did check **Switch to expert mode**).
9. Check **Encrypt all local NTFS drives**. This will encrypt all the local hard disk partitions using the AES encryption algorithm (256 bits). Click **Next** to continue.




→ The **Configuration options** dialog appears.



This dialog allows you to configure the following:

Option	Details	Steps
Configure encryption of hard disk partitions	Check this option to configure how each partition is encrypted.	<a href="#">11</a>
Create an Emergency Recovery Information file	Check this option to create new ERI for the target computer.	<a href="#">12</a> , <a href="#">13</a>
Configure ERI password restrictions	Check this option to configure how the ERI password is handled.	<a href="#">11 (part 2)</a>
Configure Logging	Check this option to configure the FDE log file location, filename, and maximum size.	<a href="#">14</a>
Configure TPM	Check this option to enable the TPM for <i>EgoSecure Full Disk Encryption</i> . <b>NOTE:</b> <i>This feature is for the FDE component only! You cannot install the PBA if this is enabled.</i>	<a href="#">15</a>
Configure FDE tray settings	Check this option to define whether to hide or to show the encryption tray icon.	<a href="#">16</a>
Configure additional encryption key protection	Check this option to configure the additional key for the disk encryption key.	<a href="#">17</a>

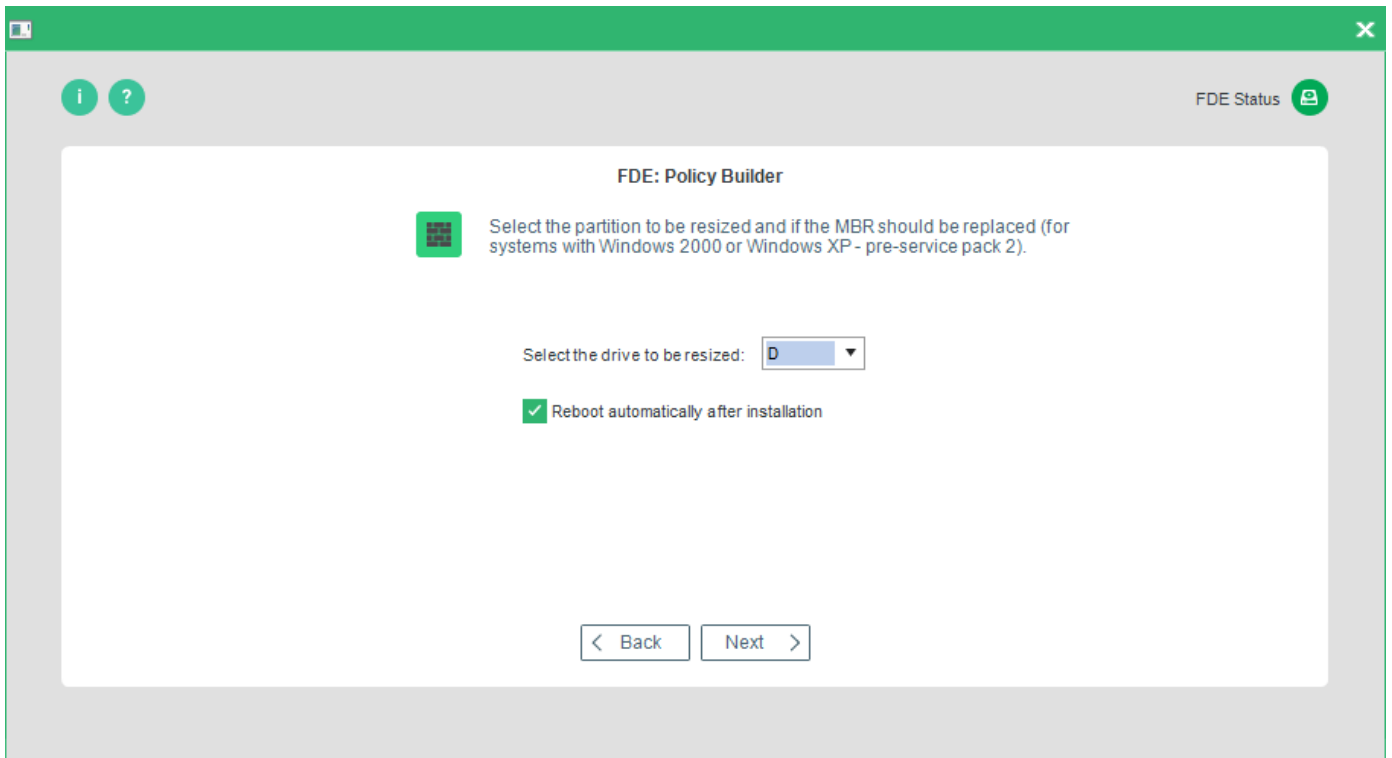
10. Once you have made your selection, press **Next** to continue.



**INFO**

Checking the options in this dialog will affect the dialogs that appear hereafter. The following steps assume that you have checked every option to configure every detail. If you have not checked every option and have reached one of the steps here that does not match that on your monitor then skip the step(s) until you reach the correct dialog.

→ The PBA partition options dialog appears:

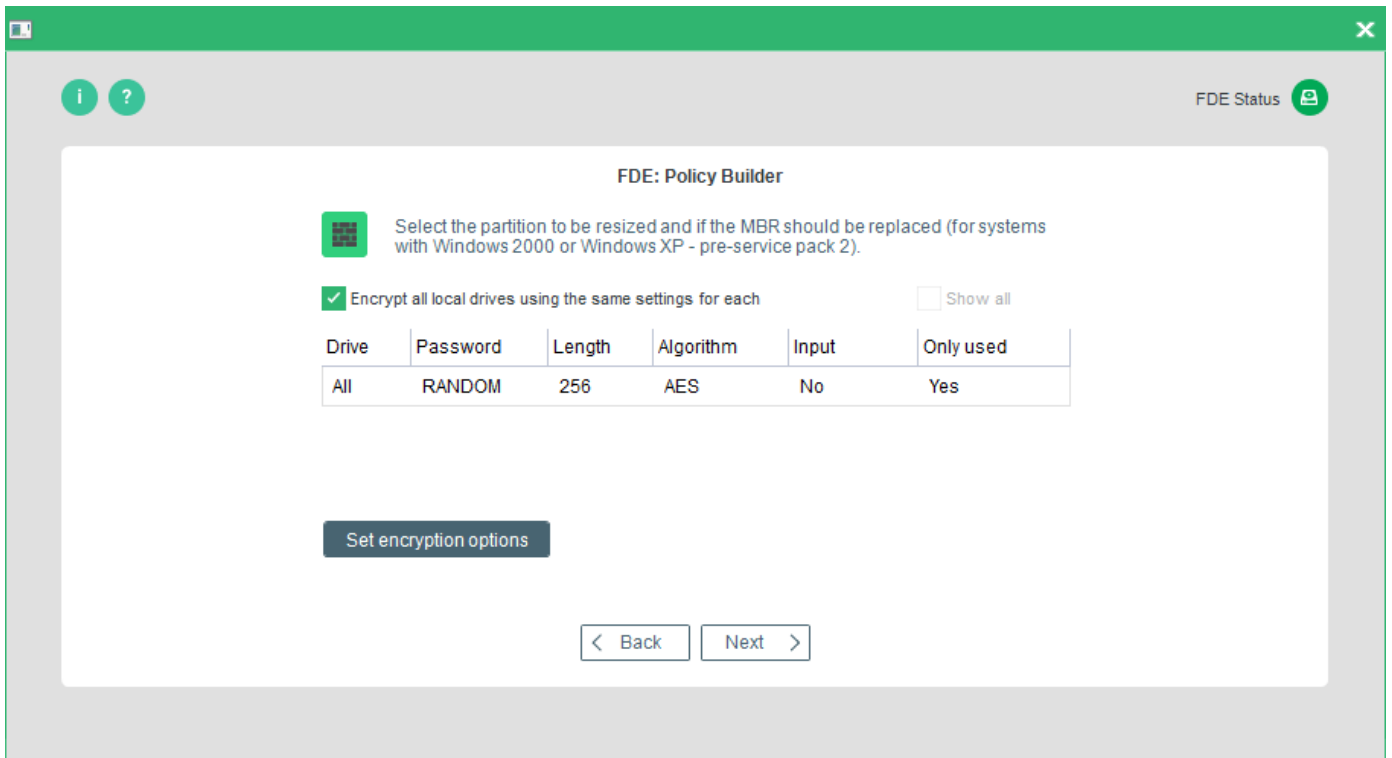


The following options are available:

Option	Details
Select drive to be resized	The drive to be resized to accommodate the PBA partition.
Reboot automatically after installation	Reboot the target computer automatically to initialize PBA directly. If you do not check this option <i>EgoSecure Full Disk Encryption</i> will be initialized upon the next reboot.

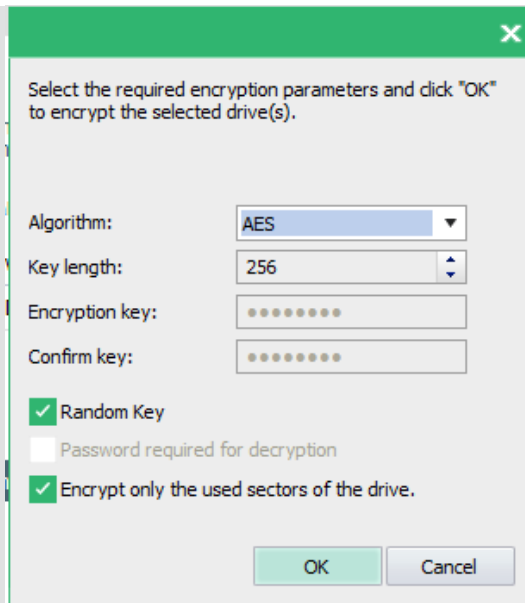
11. Once you have made your selection, click **Next** to continue.

→ The Hard Disk Encryption Options dialog appears.



The following options are available:

Option	Details
Encrypt all local drives using the same settings for each	This option enables the encryption for every partition/hard disk on the target computer with the same settings. If you uncheck this option, all the available drives in the hard disk will be displayed in the list. To display every drive letter, click <b>Show all</b> .
Show all	Display every drive letter in the drive list.
Set encryption options	Set the encryption options for every partition or the selected drive in the list. The following dialog will appear:



The dialog has the following options:

- Algorithm

Select which algorithm will be used for the encryption of the selected drive.

- Key length

Some encryption algorithms support different key lengths. Click the up/down arrows to define the preferred key length for the selected algorithm. The key that will be generated out of the Password will be of this length.

- Encryption Key (Password), Confirm key (Confirmation Password)

The encryption key will be generated out of the password you enter (and confirm) here.

- Random key

With this option you do not have to enter an encryption password. The encryption key will be generated randomly when encryption takes place.

- Password required for decryption

This option is only active if the option Random key is unchecked.

- Encrypt only the used sectors of the drive

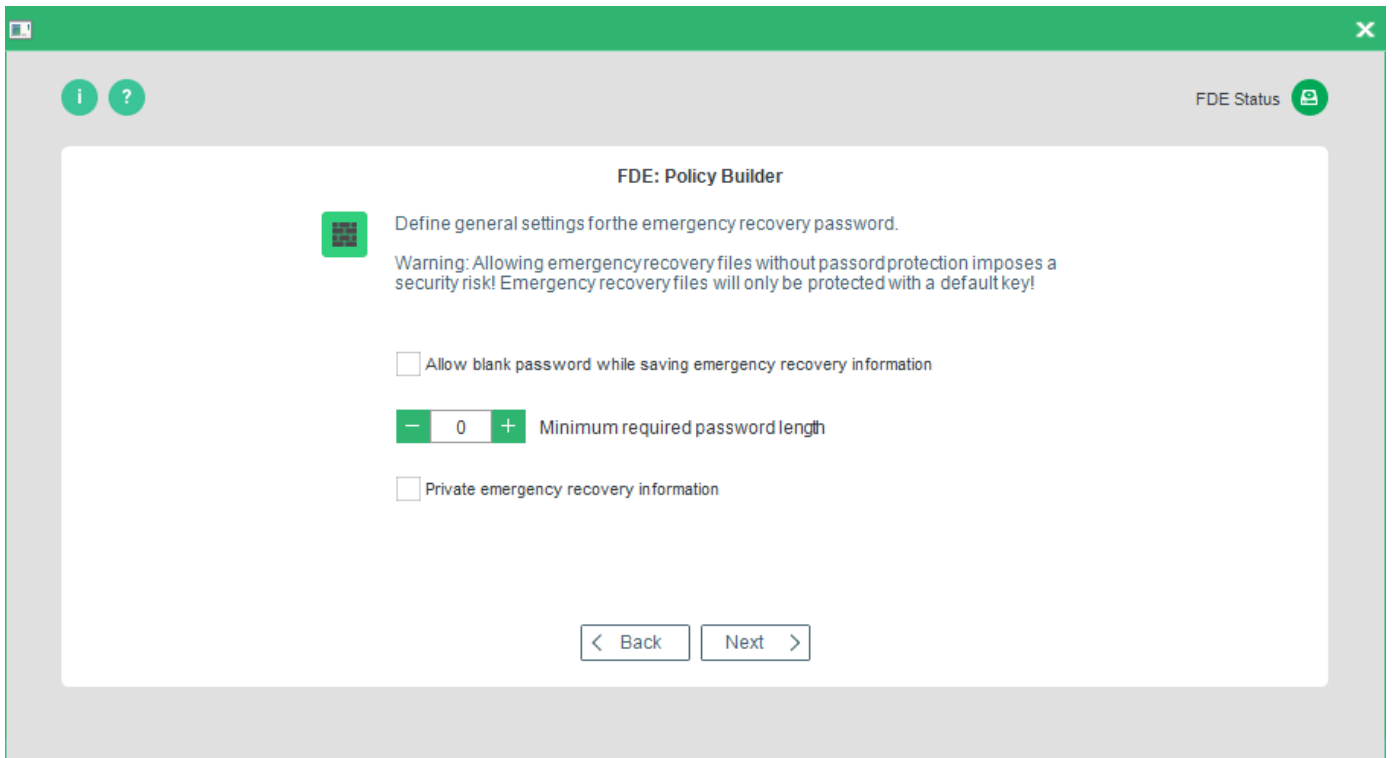
When a drive is initially encrypted, either all the sectors (regardless of whether they contain data or not), or only those sectors that contain data, can be encrypted. Encrypting only those portions of the drive that are used is much faster in most of the cases. Select this option, if you want to encrypt only the used sectors of the drive.

Clear

Clear any incorrect settings made to a drive.

→ The Emergency Recovery Information Password dialog appears.





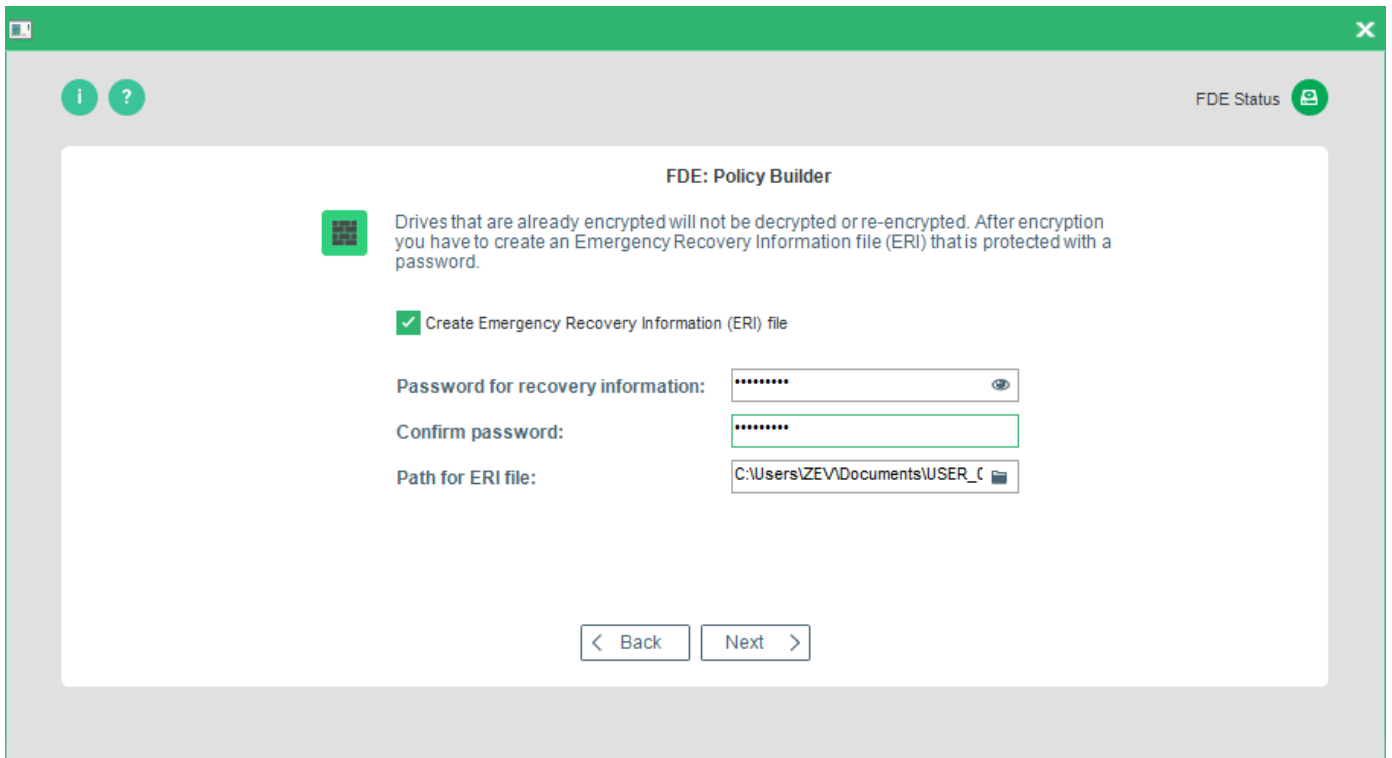
The following options are available:

Option	Details
Allow blank password while saving emergency recovery password	Check this option if you do not want to protect the ERI file a password ( <b>not recommended!</b> ).
Minimum required password length	Set a minimum password length for the ERI file ( <b>recommended!</b> ).
Private emergency recovery information	This option should be used if you do NOT intend to define a single ERI file for company-wide use. This disables the recovery of all notebooks through one ERI file.

! Allowing the storage of ERI files without a password imposes a security risk! It is recommended to ALWAYS use a password to protect ERI files.

12. Once you have made your selection, press **Next** to continue.

→ The first Emergency Recovery Information options dialog appears.

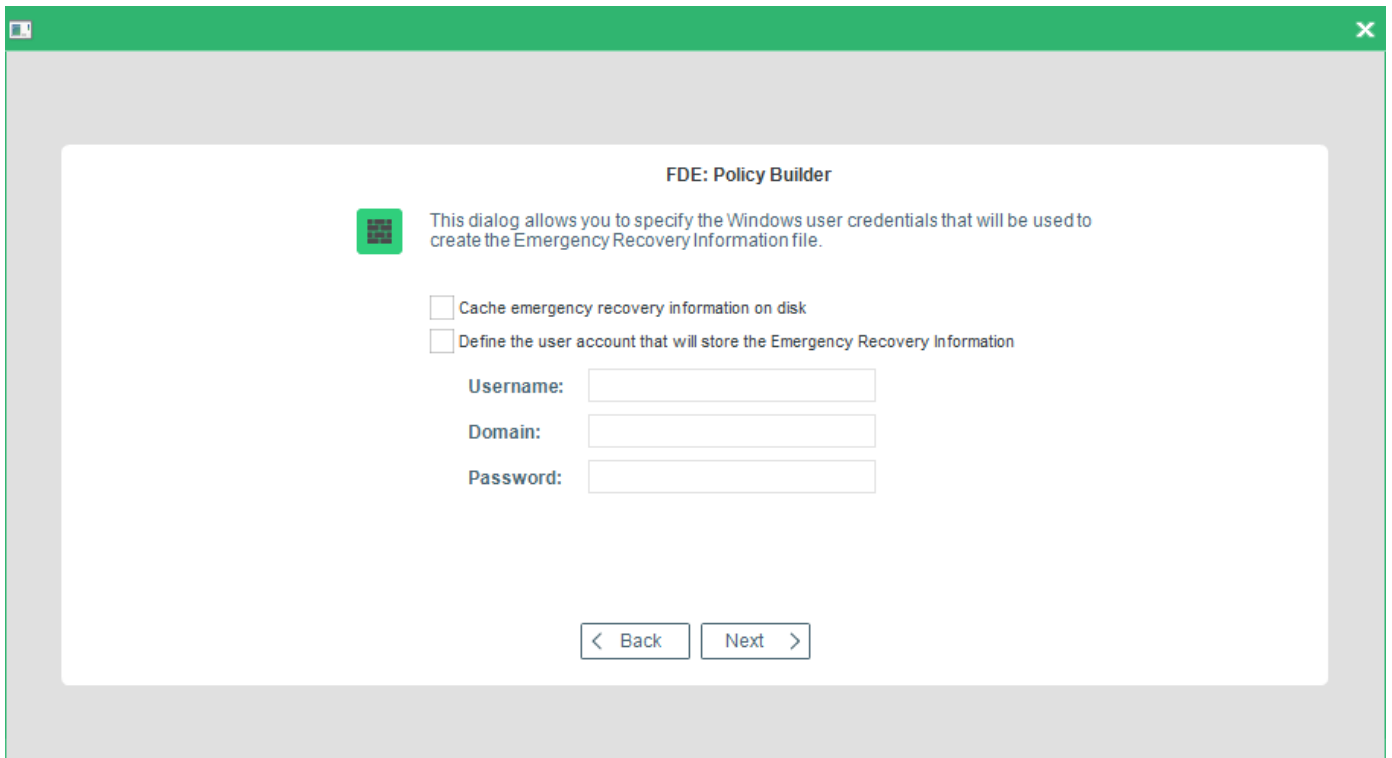


The options available are in the table below:

Option	Details
Create emergency recovery information	Check this option to create ERI (highly recommended!).
Emergency recovery password	The password used to access the ERI file in an emergency. Only the English keyboard layout is supported in the recovery application, that is why please enter the password, which contains no symbols from other languages.
Confirm password	Confirm the password for the ERI file.
Path for ERI file	The location to which the ERI file is saved. Either enter the path for the ERI file manually or click "... " to browse for a location. <b>Remember that this location must be accessible from the target computer!</b> For details about ERI copies, see <a href="#">Creating an ERI file</a> .

13. Make your selection and click **Next**.

→ The second Emergency Recovery Information options dialog appears.



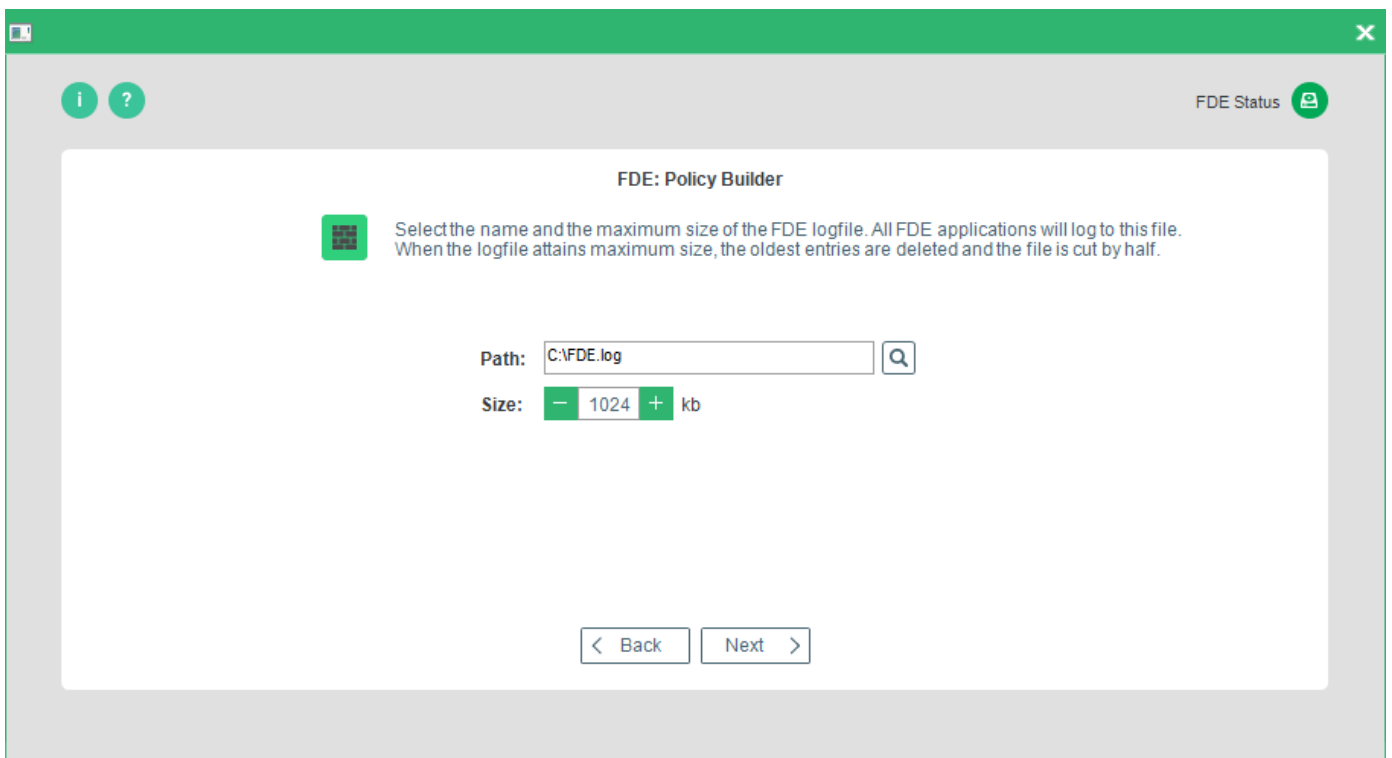
The following options are available:

Option	Details
Cache Emergency Recovery Information on hard disk	Check this to store the ERI on the hard disk.
Define the user account that will store the Emergency Recovery Information	Check this if you want a specific user to be able to store ERI to a network drive that requires specific access.
Username	The <i>Windows</i> credentials username required for network access.
Domain	The <i>Windows</i> credentials domain required for network access.
Password	The <i>Windows</i> credentials password required for network access.

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

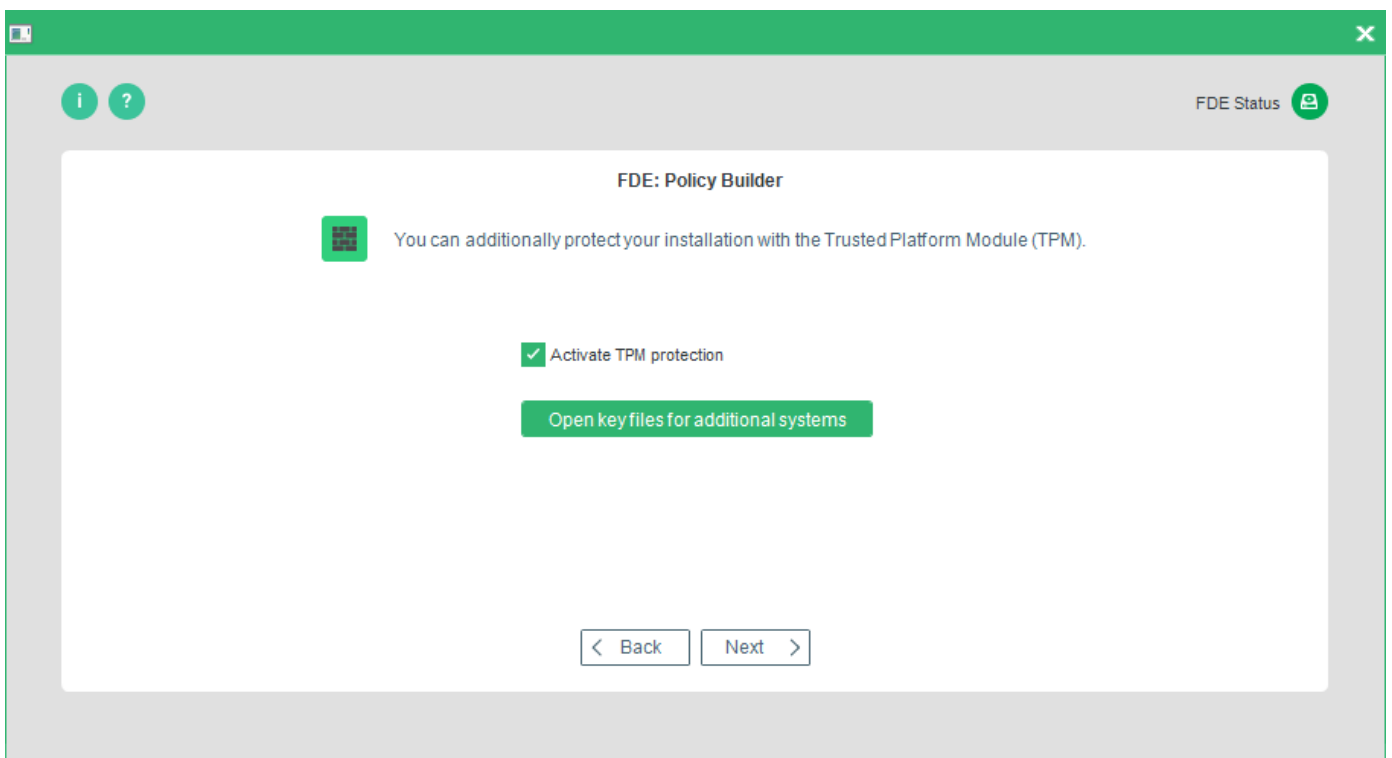
→ The **Logging** dialog appears. The options available are in the table below.

Option	Details
Path	Enter a full path for the FDE log file either directly into the field Path or click "...". Remember to enter the log file name and *.log extension.
Size	Set the maximum log file size.



15. Once you have made your selection, press **Next** to continue.

→ The **TMP** dialog appears.



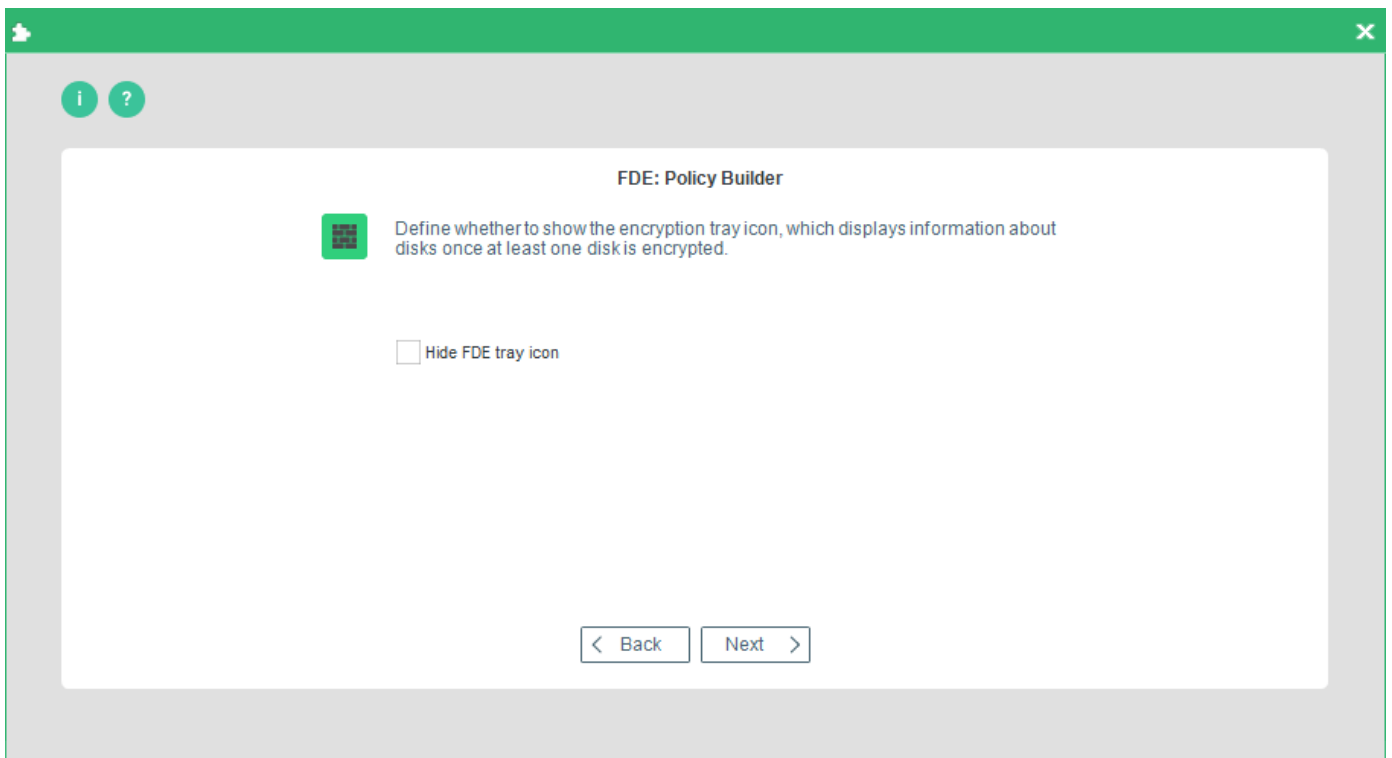
The following options are available:

Option	Details
Activate TPM protection	Check this option to enable the TPM feature for <i>EgoSecure Full Disk Encryption</i> on your computer.
Open key files for additional systems	Check this option to import TPM keys from another <i>EgoSecure Full Disk Encryption</i> installation.

16. Make your selection and click **Next**.

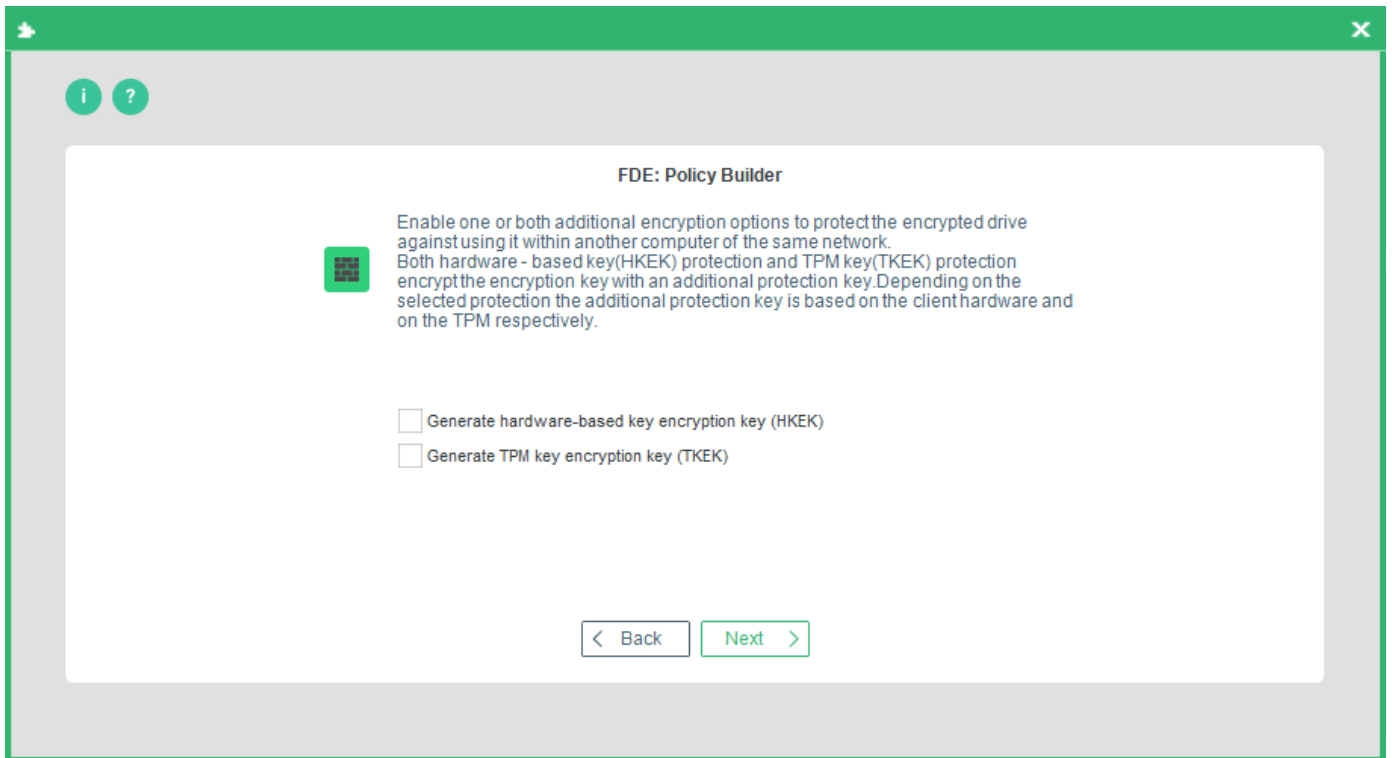
→ The step for hiding an encryption tray icon appears.

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.



17. To hide the icon, check the **Hide encryption 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.

### 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.



## ATTENTION

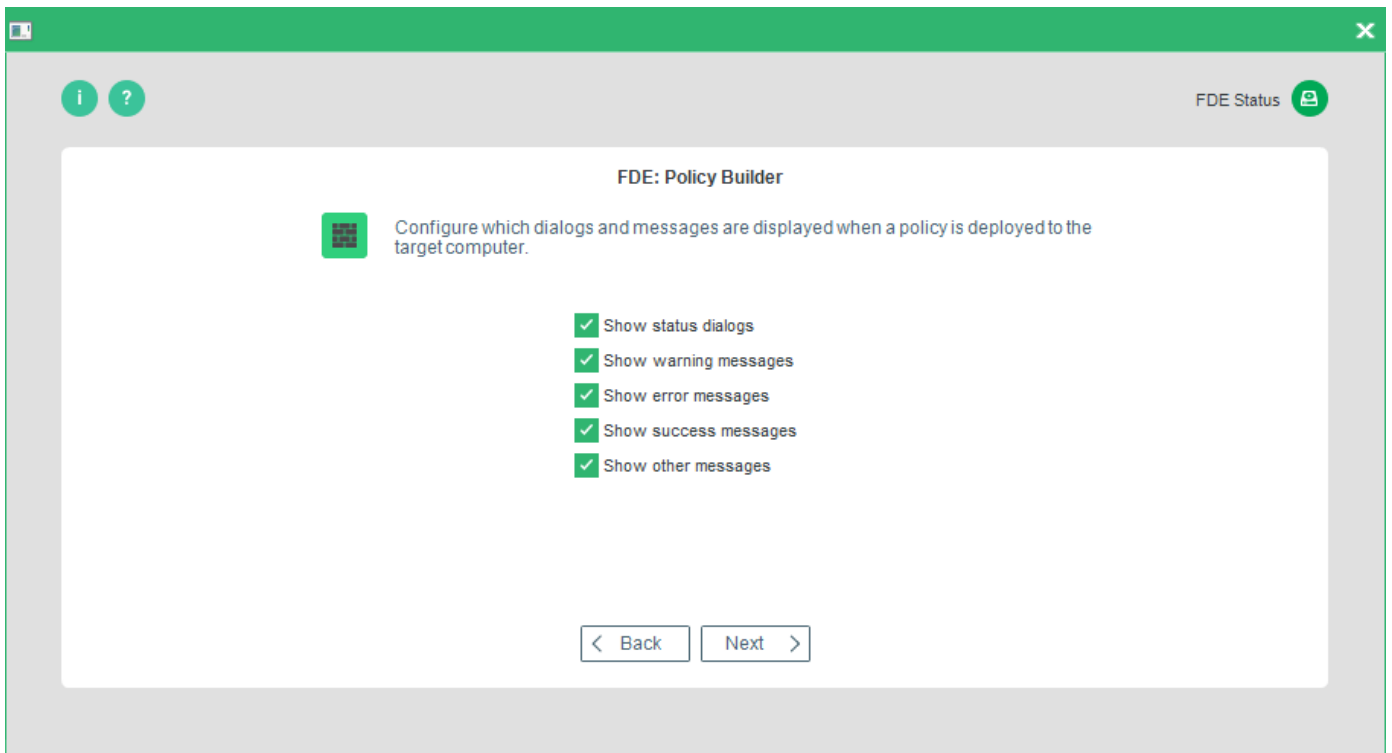
### Before updating BIOS or replacing hardware

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.

18. Check the **Generate hardware-based key encryption key (HKEK)** box and/or **Generate TPM-based key encryption key (TKEK)**, and then click **Next**.

→ The **Boot messages options** dialog appears. The messages below are shown only on computers with Windows versions below Windows 10.



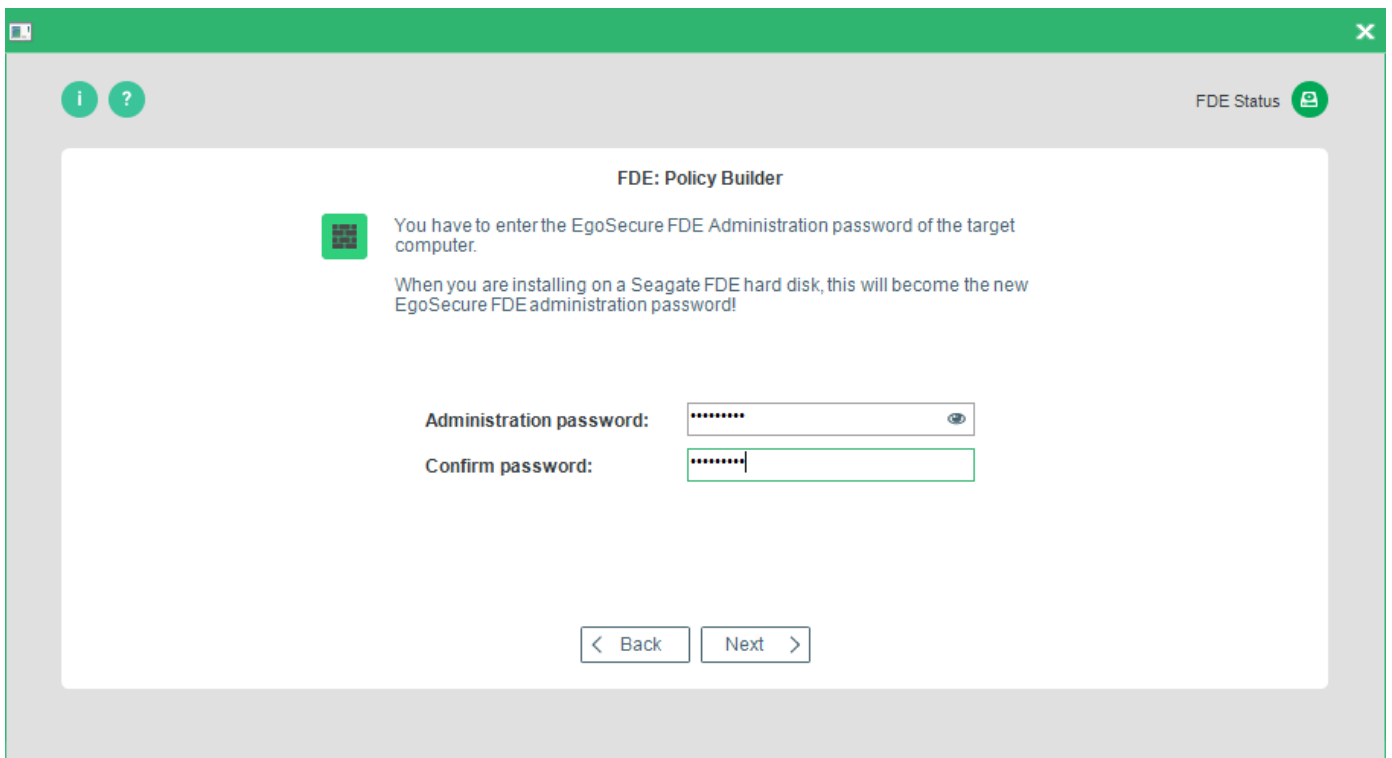
This dialog allows you to define the following installation messages:

Option	This option determines if...
Show status dialogs	... status dialogs should be displayed on the target computer during policy deployment.
Show warning messages	... warning messages should be displayed on the target computer during policy deployment. If you do not select this option, warning messages are suppressed.
Show error messages	... error messages should be displayed on the target computer during policy deployment. If you do not select this option, error messages are suppressed.
Show success messages	... success messages should be displayed on the target computer that relate to individual policy tasks during deployment.
Show other messages	... information messages should be displayed on the target computer during and after policy deployment. If you do not select this option, information messages are suppressed.

19. Make your selection, and press **Next** to continue.

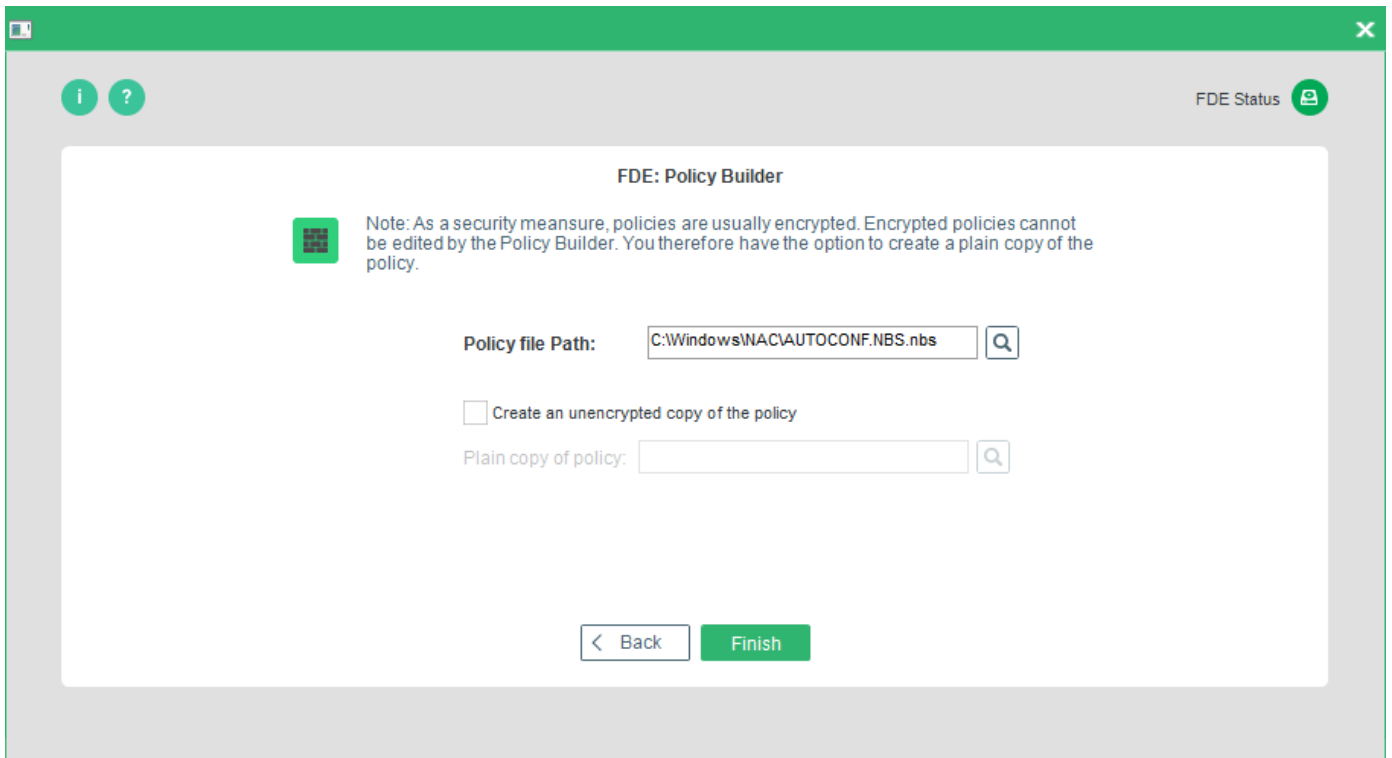
→ The **Administration password** (target computer) dialog appears.

20. Enter and confirm the EgoSecure Full Disk Encryption administration password already set on the target computer. Click **Next** to continue.



→ The **Policy location** dialog appears.





The following options are available:

Option	Details
Policy file path	Enter the path for the policy in this field by clicking `...` and selecting a location and filename for the file in the file browser.
Create an unencrypted copy of the policy	Check this option to create an unencrypted copy of the policy (recommended for reconfiguration). If you want to reconfigure a computer that has already been configured using a policy, then check this option - the Policy Builder can only open an unencrypted policy to edit the settings.
Plain copy of policy	Enter the path for the plain copy of the policy in this field by clicking `...` and selecting a location and filename for the file in the file browser.

21. Enter the paths for your policy, and click **Finish** to complete the procedure.

- ! It is recommended to always store plain copies in a safe place. Use the plain copies to create new policies for future changes in configuration.
- ! For security reasons encrypted policies cannot be edited with the FDE Policy Builder.

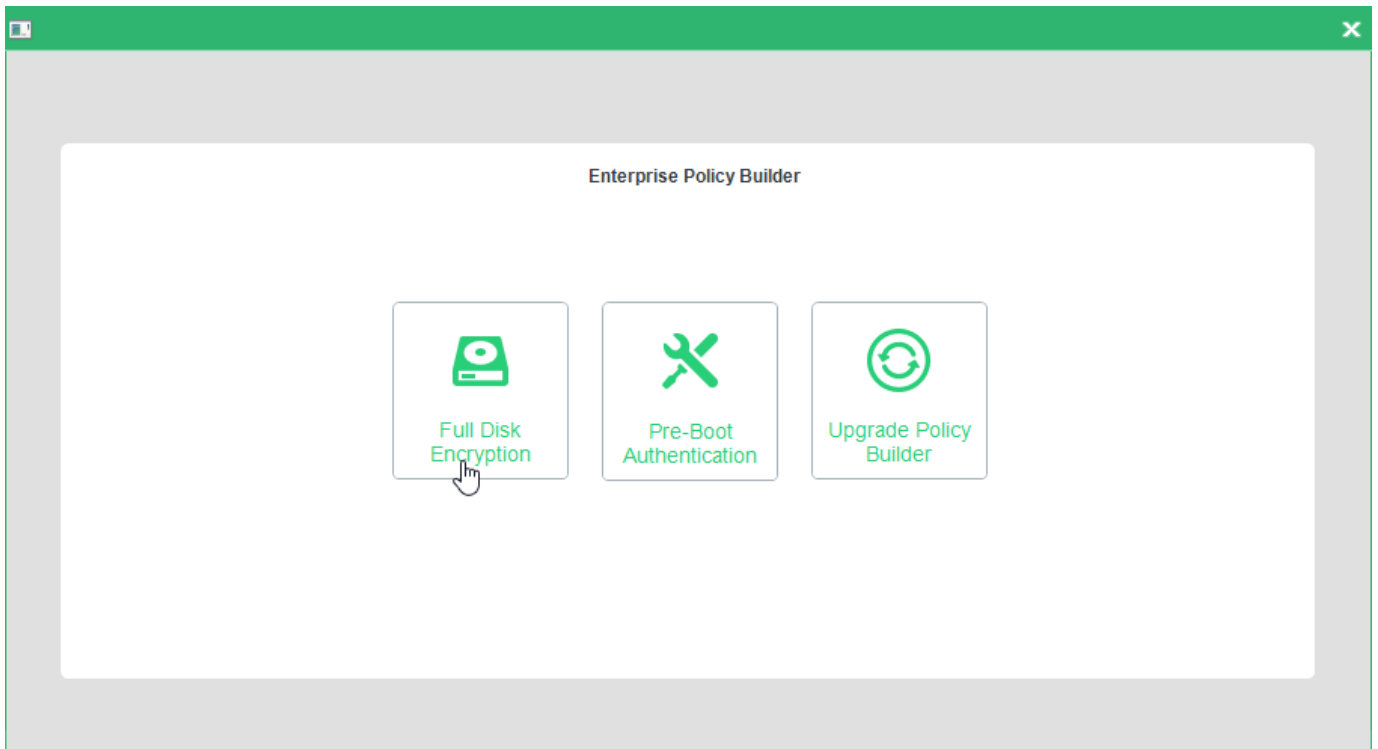
## Creating a configuration policy

This section details how to create a configuration policy for the FDE component only.

You need to have knowledge about the target computer for deployment. Details such as number of partitions, drive letters, whether encrypted, and so on are necessary for the successful deployment of EgoSecure Full Disk Encryption. Once the policy is created, deploy it, for details see [Deploying FDE policies](#).

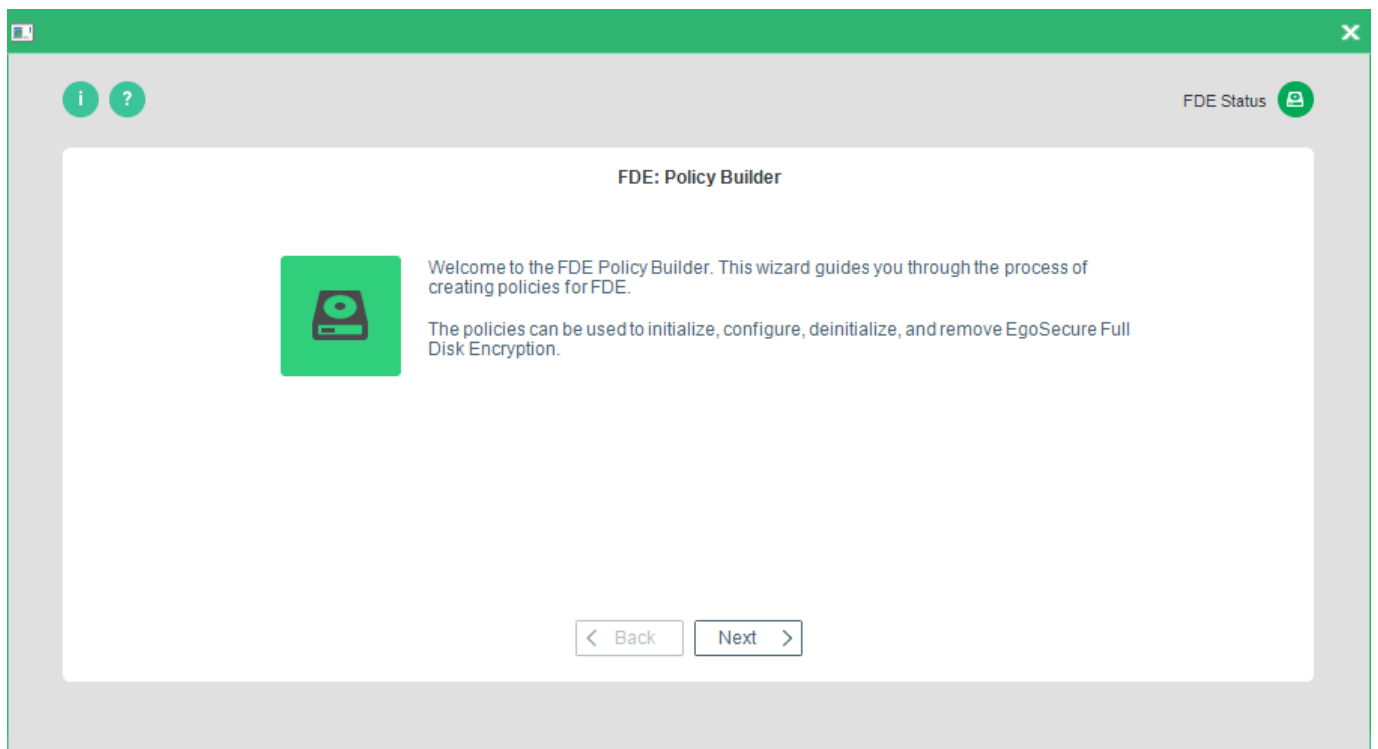
Follow these steps to create a FDE configuration policy:

1. Open the **Control Center** (as described in section [1.5](#)).
2. Double-click the Policy Builder icon.
3. Select Full Disk Encryption policy builder.



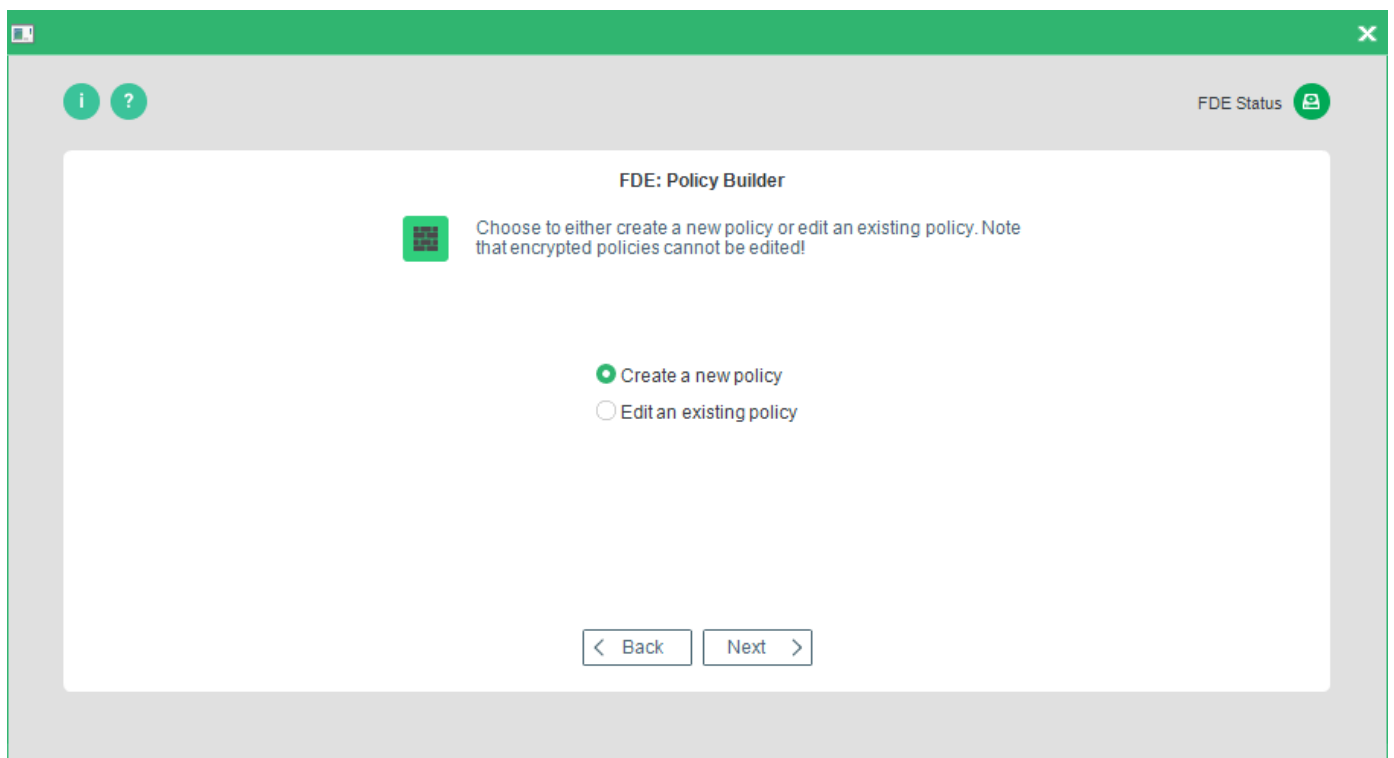
→ The FDE Policy Builder **Welcome** dialog appears.

4. Click **Next**.



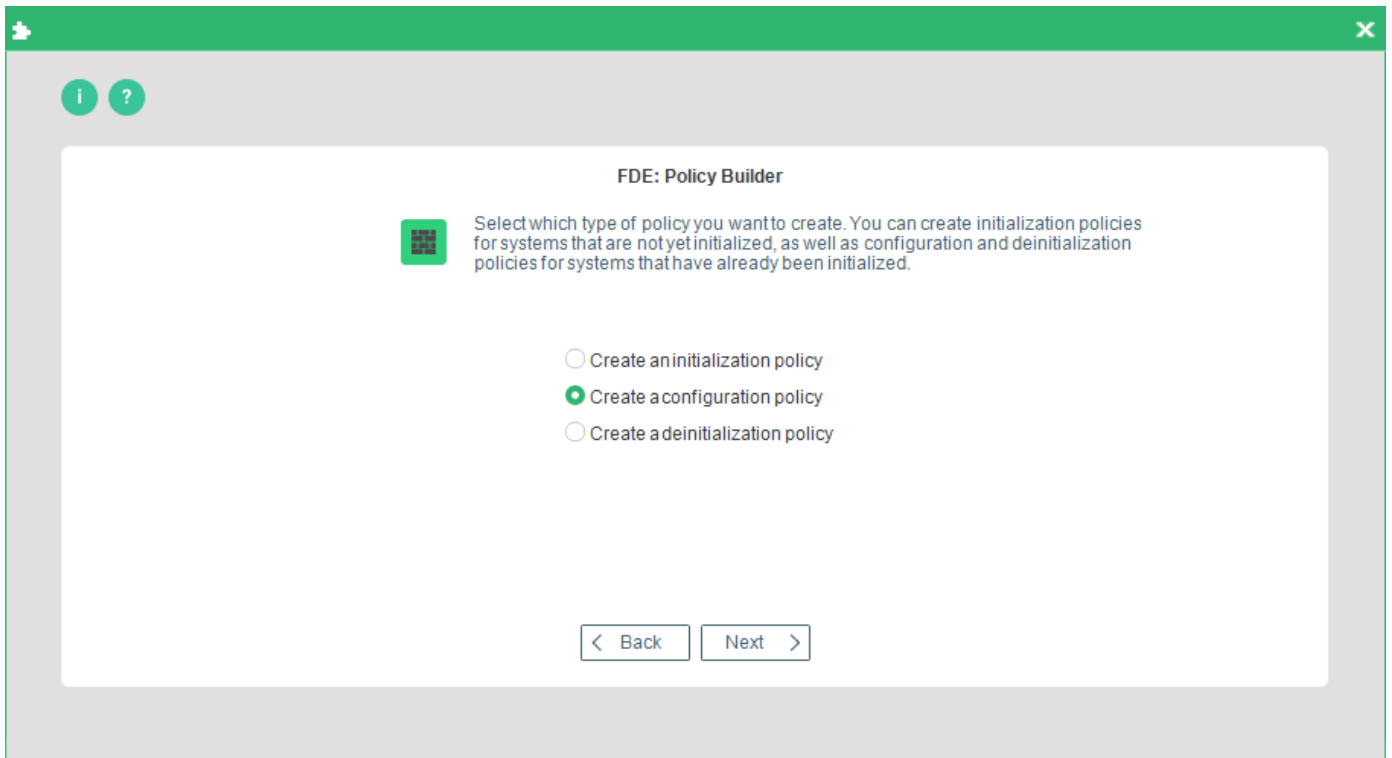
→ The **Policy selection** dialog appears.

5. Select Create a new policy.

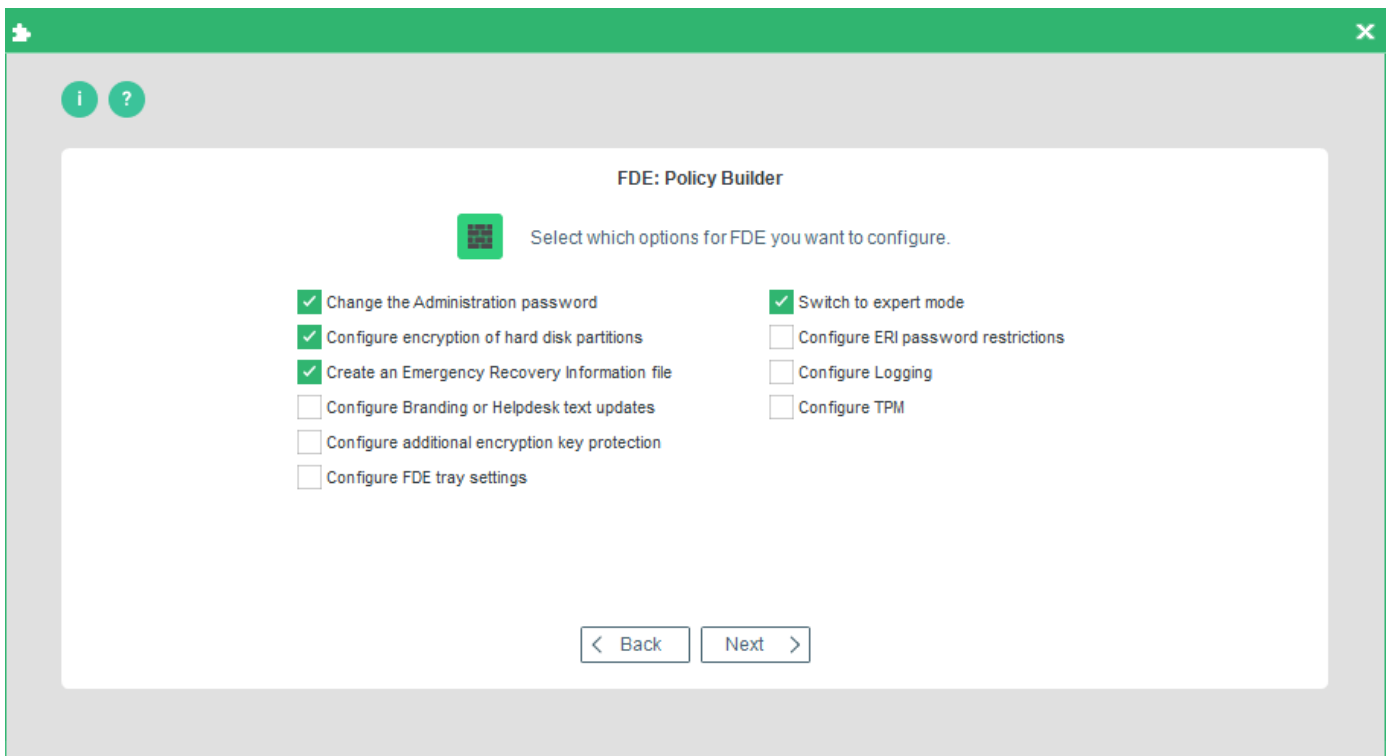


→ The **Policy type** dialog appears.

6. Select Create a configuration policy and click **Next** to continue.



→ The configuration options dialog appears:



! Any option you check in this dialog will affect the dialogs that appear hereafter! These steps assume that you have checked every option to detail every dialog! If you have not checked every option and have reached one of the steps here that

does not match that on your monitor, then skip the step(s) until you come to the correct dialog!

The following options are available:

Option	Description
Change the Administration password	Check this option to change the administration password on the target computer.
Perform encryption of hard drive partitions	Check this option to encrypt the partitions on the target computer.
Create an Emergency Recovery Information file	Check this option to create new ERI for the target computer.
Configure ERI password restrictions	Check this option to configure ERI password restrictions.
Configure Logging	Check this option to configure logging.
Configure TPM	Check this option to enable the TPM for EgoSecure Full Disk Encryption.
Configure Branding or Helpdesk text updates	Check this option to configure Branding or Helpdesk text updates
Switch to expert mode	Check this option to configure each option in detail.

7. Make your selection and click **Next**.

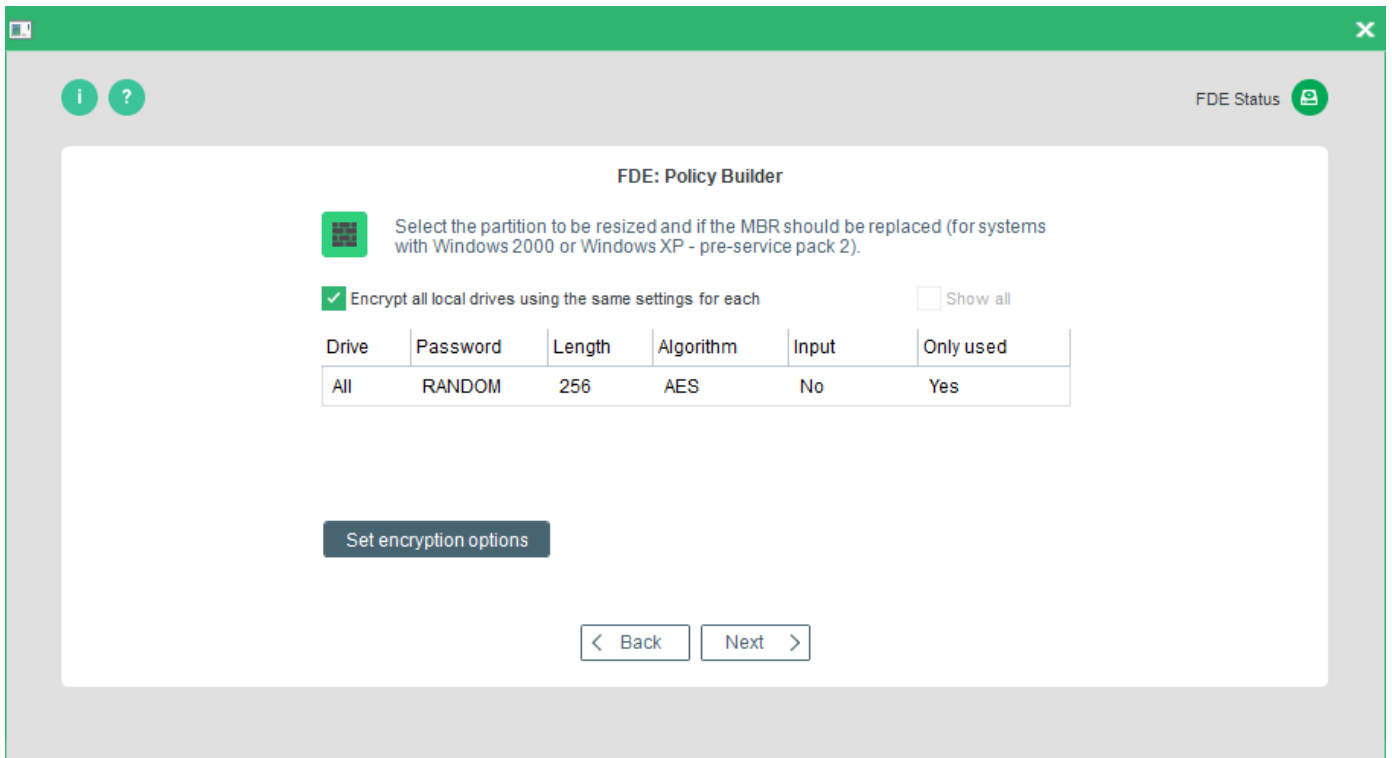
→ The Administration Password dialog appears.

The screenshot shows a window titled "FDE: Policy Builder" with a green header bar. The main content area contains the following text and controls:

- Information icon (i) and Help icon (?) in the top left.
- FDE Status icon in the top right.
- Title: FDE: Policy Builder
- Message: The EgoSecure FDE Administration password is required for every administrative action for FDE. You can define a new EgoSecure FDE Administration password in this dialog.
- Form fields:
  - New Administration password: [password field]
  - Confirm password: [password field]
  - Switch to expert mode:
- Navigation buttons: < Back and Next >

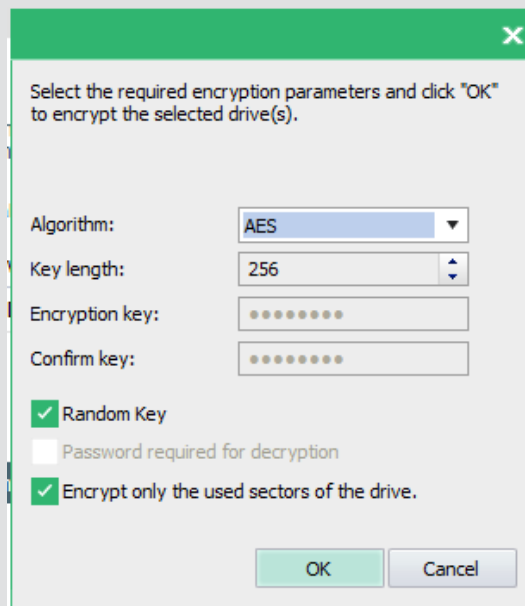
8. Enter the new administration password and confirm it. Click **Next**.

→ The Hard Disk Encryption Options dialog appears.



The following options are available:

Option	Details
Encrypt all local drives using the same settings for each	This option enables the encryption for every partition/hard disk on the target computer with the same settings. If you uncheck this option, all the available drives in the hard disk will be displayed in the list. To display every drive letter, click Show all.
Show all	Display every drive letter in the drive list.
Set encryption options	Set the encryption options for every partition or the selected drive in the list. The following dialog will appear:



The dialog has the following options:

- Algorithm

Select which algorithm will be used for the encryption of the selected drive.

- Key length

Some encryption algorithms support different key lengths. Click the up/down arrows to define the preferred key length for the selected algorithm. The key that will be generated out of the Password will be of this length.

- Encryption Key (Password), Confirm key (Confirmation Password)

The encryption key will be generated out of the password you enter (and confirm) here.

- Random key

With this option you do not have to enter an encryption password. The encryption key will be generated randomly when encryption takes place.

- Password required for decryption

This option is only active if the option Random key is unchecked.

- Encrypt only the used sectors of the drive

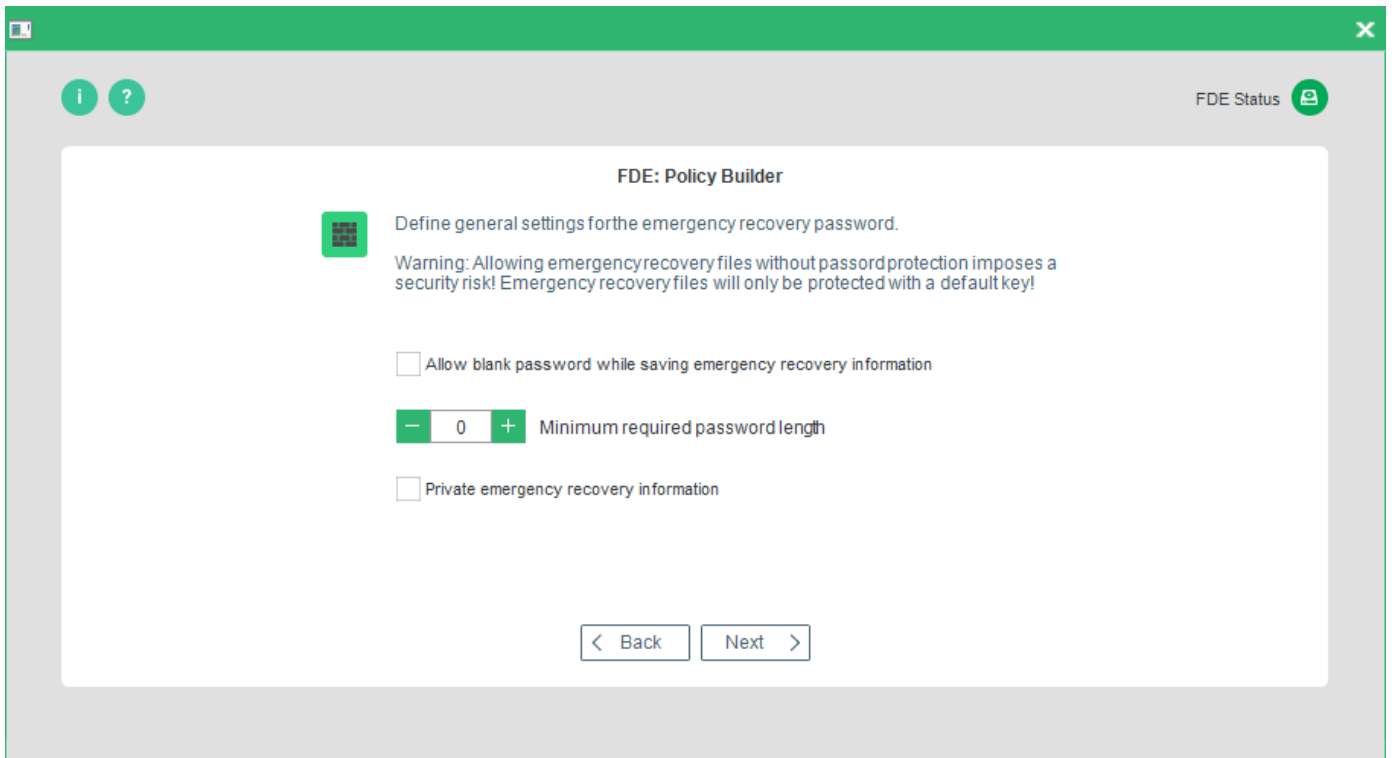
When a drive is initially encrypted, either all the sectors (regardless of whether they contain data or not), or only those sectors that contain data, can be encrypted. Encrypting only those portions of the drive that are used is much faster in most of the cases. Select this option, if you want to encrypt only the used sectors of the drive.

Clear

Clear any incorrect settings made to a drive.

9. Select the encryption settings for either all drives or independently for each one and click **Next** to continue.

→ The Emergency Recovery Password dialog appears.



The following options are available:

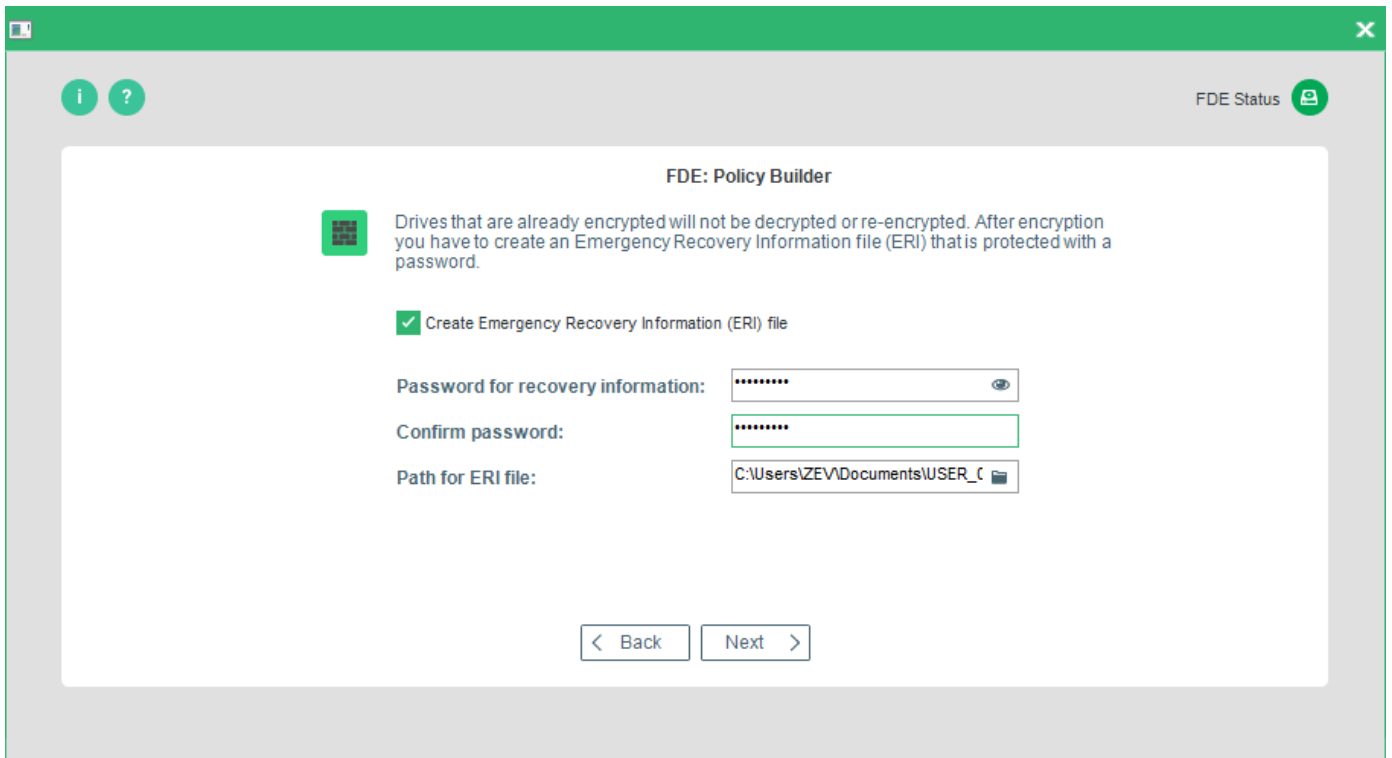
Option	Details
Allow blank password while saving emergency recovery password	Check this option if you do not want to protect the ERI file a password ( <b>not recommended!</b> ).
Minimum required password length	Set a minimum password length for the ERI file ( <b>recommended!</b> ).
Private emergency recovery information	This option should be used if you do NOT intend to define a single ERI file for company-wide use. This disables the recovery of all notebooks through one ERI file.

! Allowing the storage of ERI files without a password imposes a security risk! It is recommended to ALWAYS use a password to protect ERI files.

10. Once you have made your selection, press **Next** to continue.

→ The first Emergency Recovery Information options dialog appears.



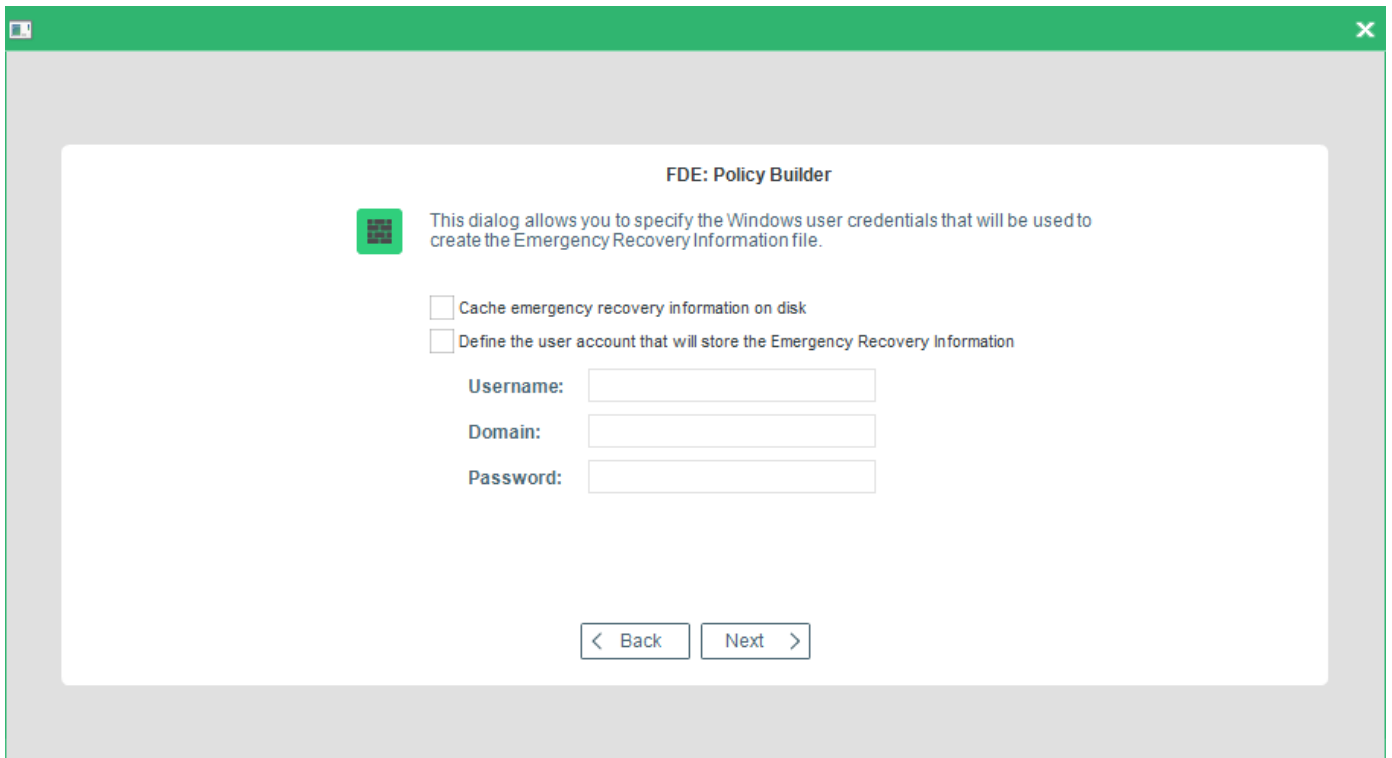


The options available are in the table below:

Option	Details
Create emergency recovery information	Check this option to create ERI (highly recommended!).
Emergency recovery password	The password used to access the ERI file in an emergency. Only the English keyboard layout is supported in the recovery application, that is why please enter the password, which contains no symbols from other languages.
Confirm password	Confirm the password for the ERI file.
Path for ERI file	The location to which the ERI file is saved. Either enter the path for the ERI file manually or click "..." to browse for a location. <b>Remember that this location must be accessible from the target computer!</b> For details about ERI copies, see <a href="#">Creating an ERI file</a> .

11. Make your selection and click **Next**.

→ The second Emergency Recovery Information options dialog appears.

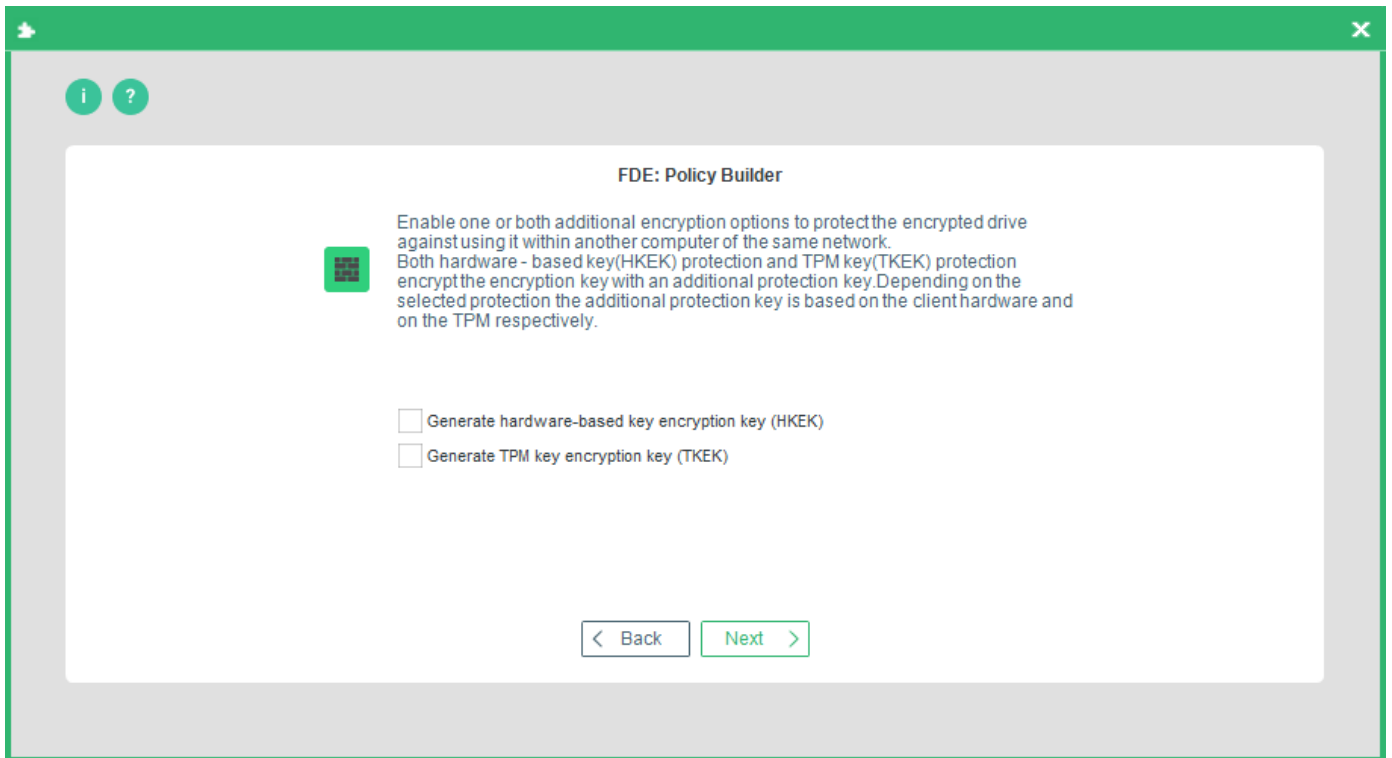


The following options are available:

Option	Details
Cache Emergency Recovery Information on hard disk	Check this to store the ERI on the hard disk.
Define the user account that will store the Emergency Recovery Information	Check this if you want a specific user to be able to store ERI to a network drive that requires specific access.
Username	The <i>Windows</i> credentials username required for network access.
Domain	The <i>Windows</i> credentials domain required for network access.
Password	The <i>Windows</i> credentials password required for network access.

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

→ 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.

### 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.



**ATTENTION**

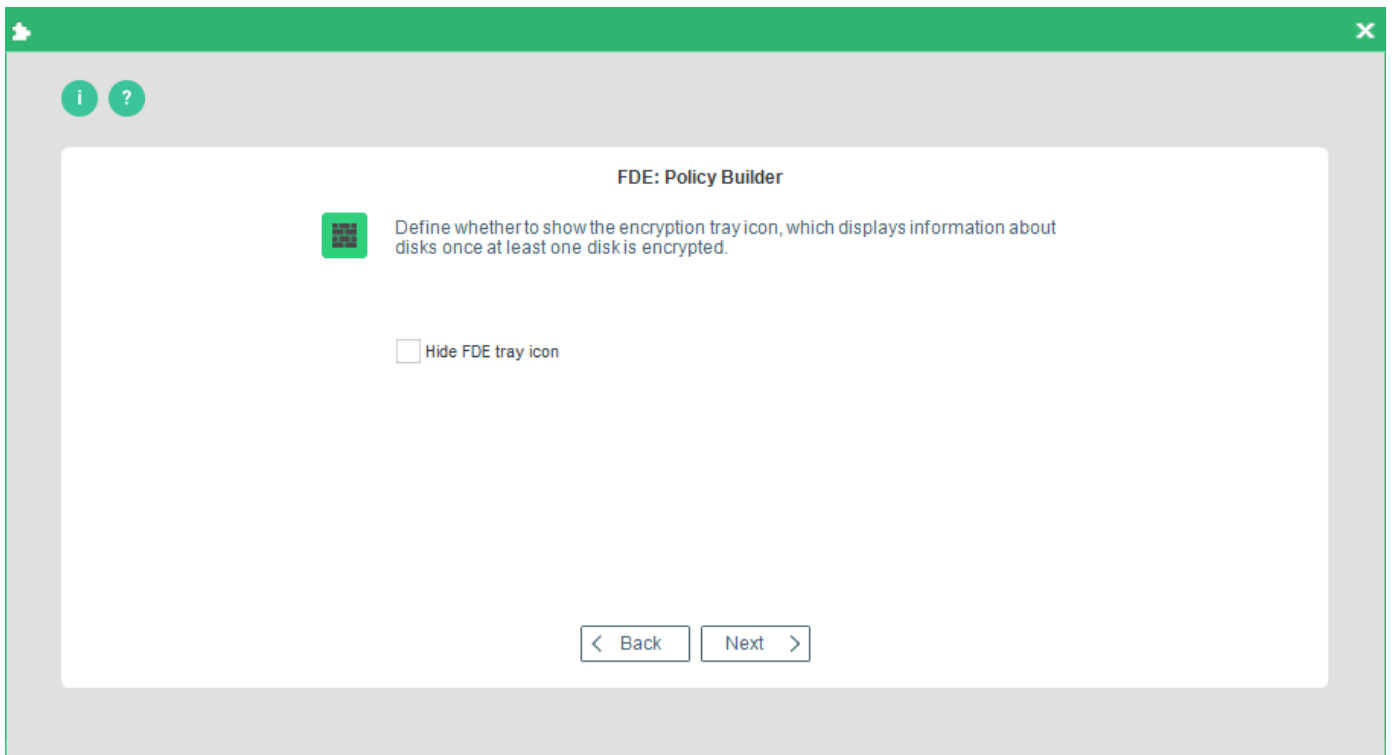
**Before updating BIOS or replacing hardware**

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.

13. Enable the **Generate hardware-based key encryption key (HKEK)** option and/or **Generate TPM-based key encryption key (TKEK)** option, and then click **Next**.

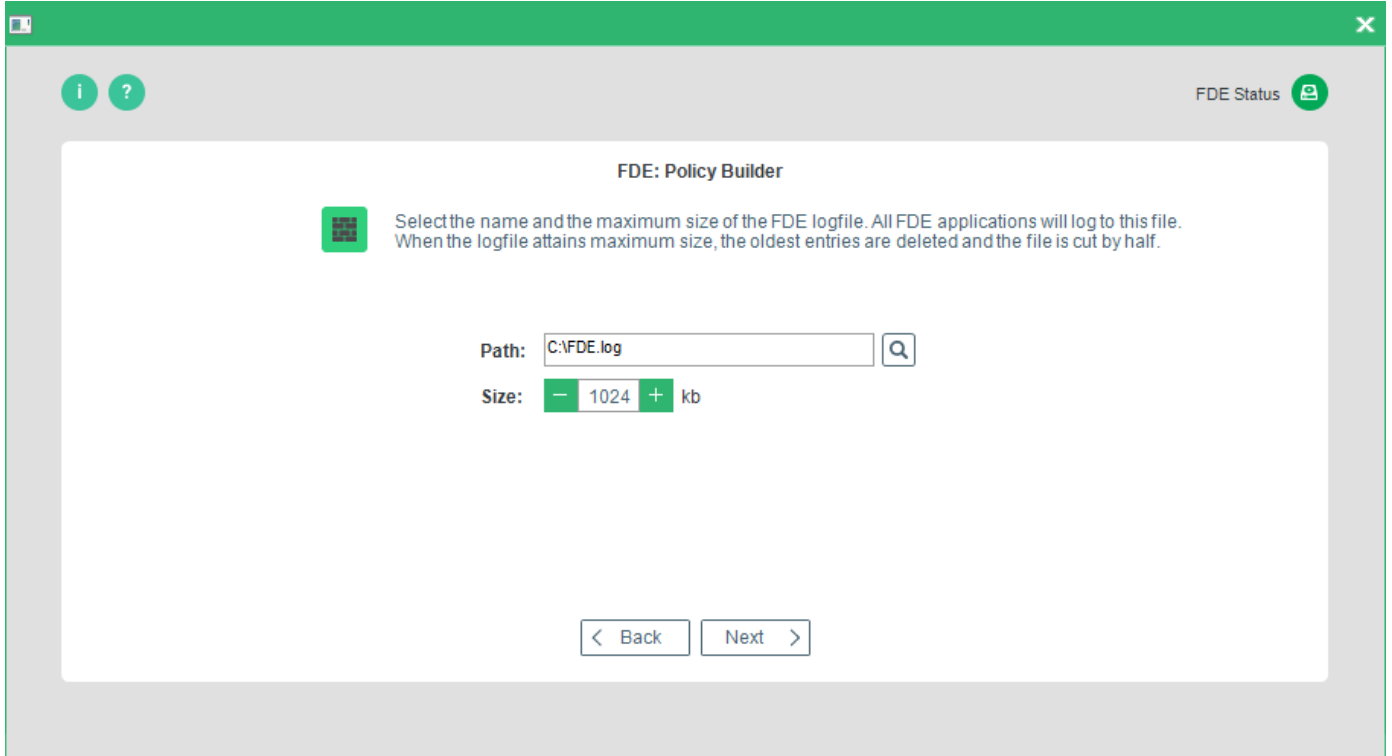
→ The step for configuring FDE tray settings appears.



14. By default, the encryption tray appears on the Windows taskbar once a disk is encrypted. To hide the icon, check the **Hide FDE tray icon** box and click **Next**.

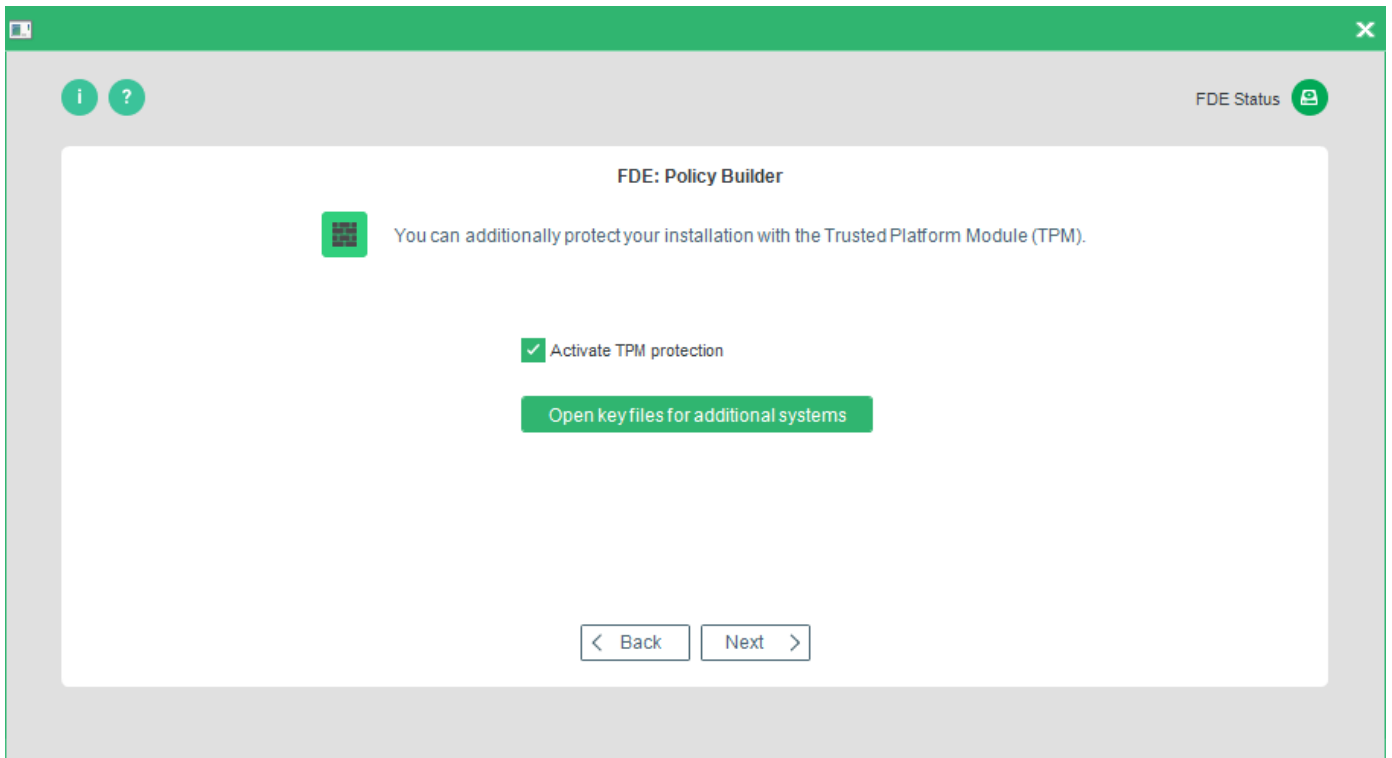
→ The **Logging** dialog appears. The available options are in the table below.

Option	Details
Path	Enter a full path for the FDE log file either directly into the field Path or click "..." to open a file explorer. Remember to enter the log file name and *.log extension.
Size	Set the maximum log file size.



15. Once you have made your selection, press **Next** to continue.

→ The **TMP** dialog appears.

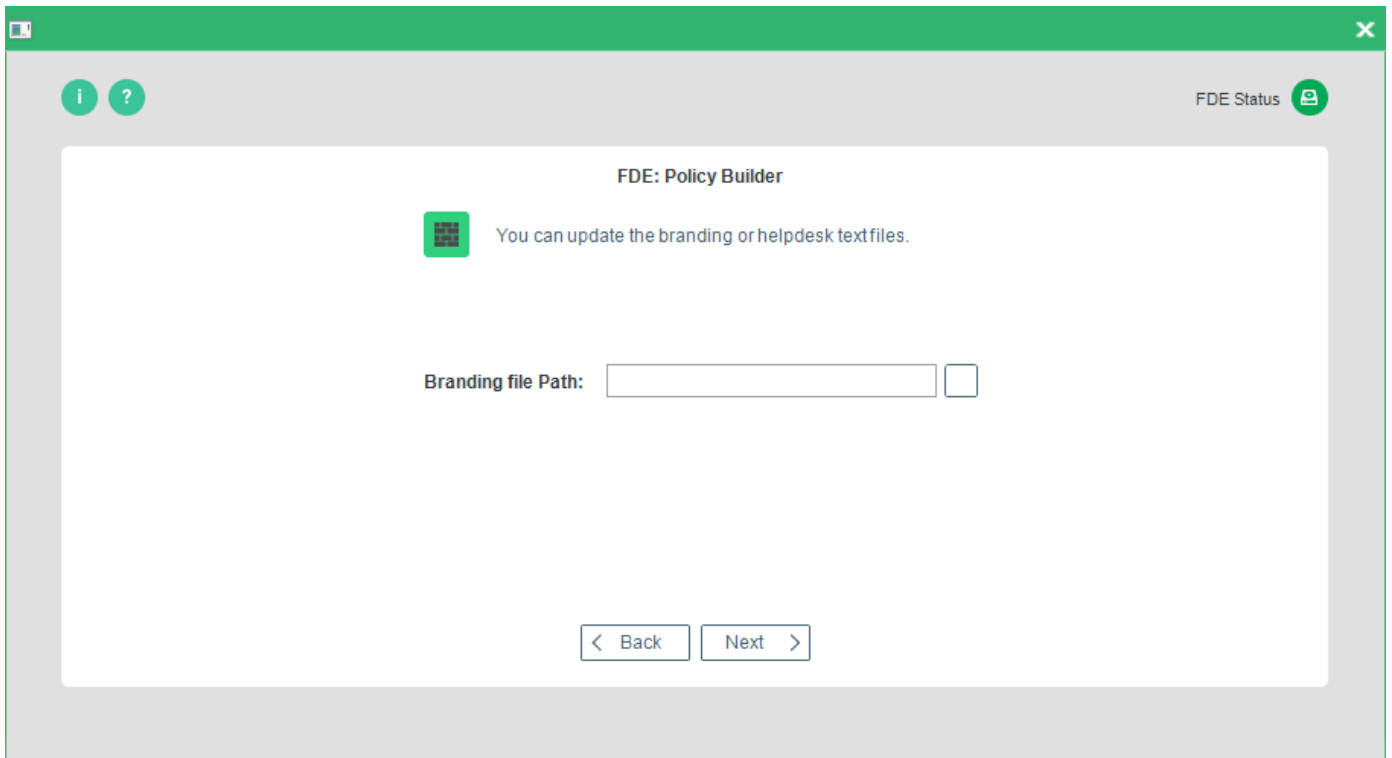


The following options are available:

Option	Details
Activate TPM protection	Check this option to enable the TPM feature for <i>EgoSecure Full Disk Encryption</i> on your computer.
Open key files for additional systems	Check this option to import TPM keys from another <i>EgoSecure Full Disk Encryption</i> installation.

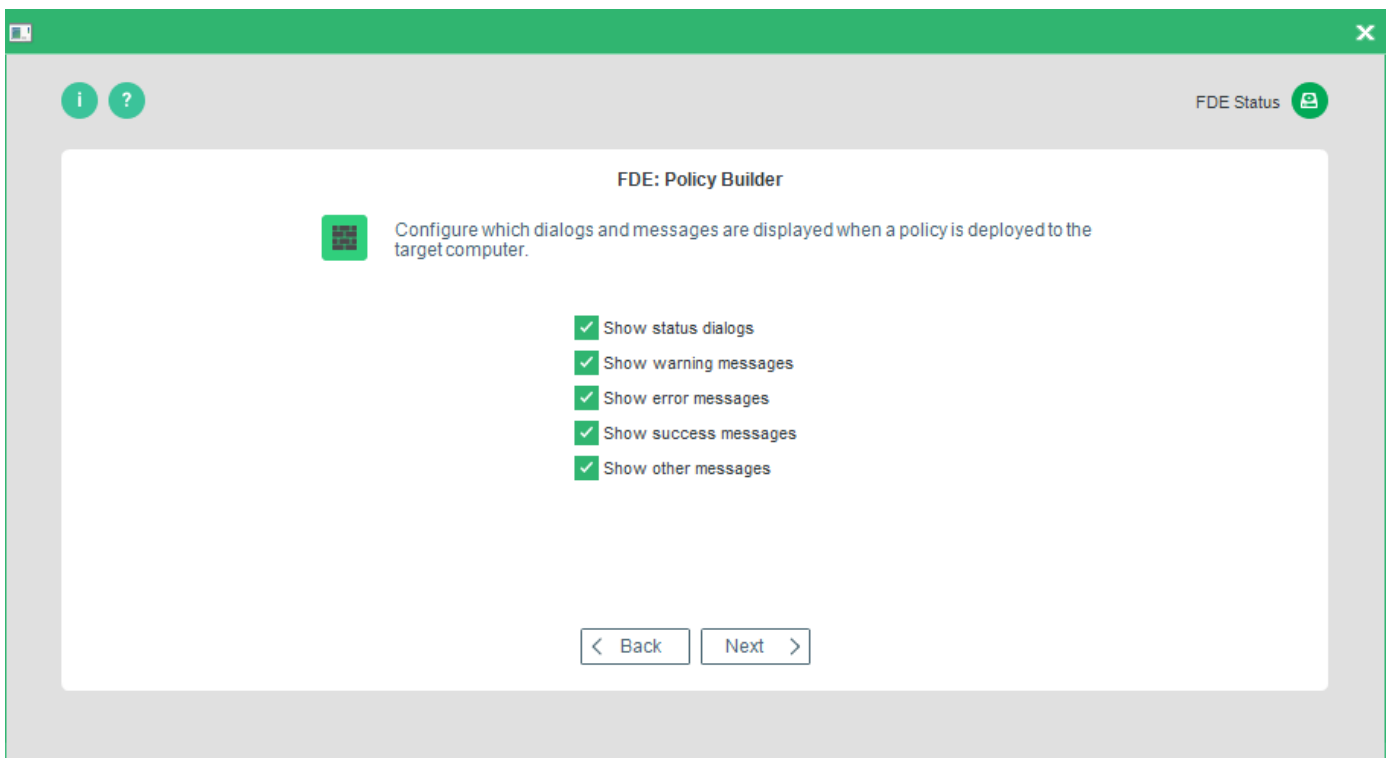
16. Make your selection and click **Next**.

→ The **Branding Update** dialog appears.



17. Select the branding or helpdesk text file, and click **Next** to continue.

→ The **Boot messages options** dialog appears. The messages below are shown only on computers with Windows versions below Windows 10.



This dialog allows you to define the following installation messages:

Option	This option determines if...
Show status dialogs	... status dialogs should be displayed on the target computer during policy deployment.
Show warning messages	... warning messages should be displayed on the target computer during policy deployment. If you do not select this option, warning messages are suppressed.
Show error messages	... error messages should be displayed on the target computer during policy deployment. If you do not select this option, error messages are suppressed.
Show success messages	... success messages should be displayed on the target computer that relate to individual policy tasks during deployment.
Show other messages	... information messages should be displayed on the target computer during and after policy deployment. If you do not select this option, information messages are suppressed.

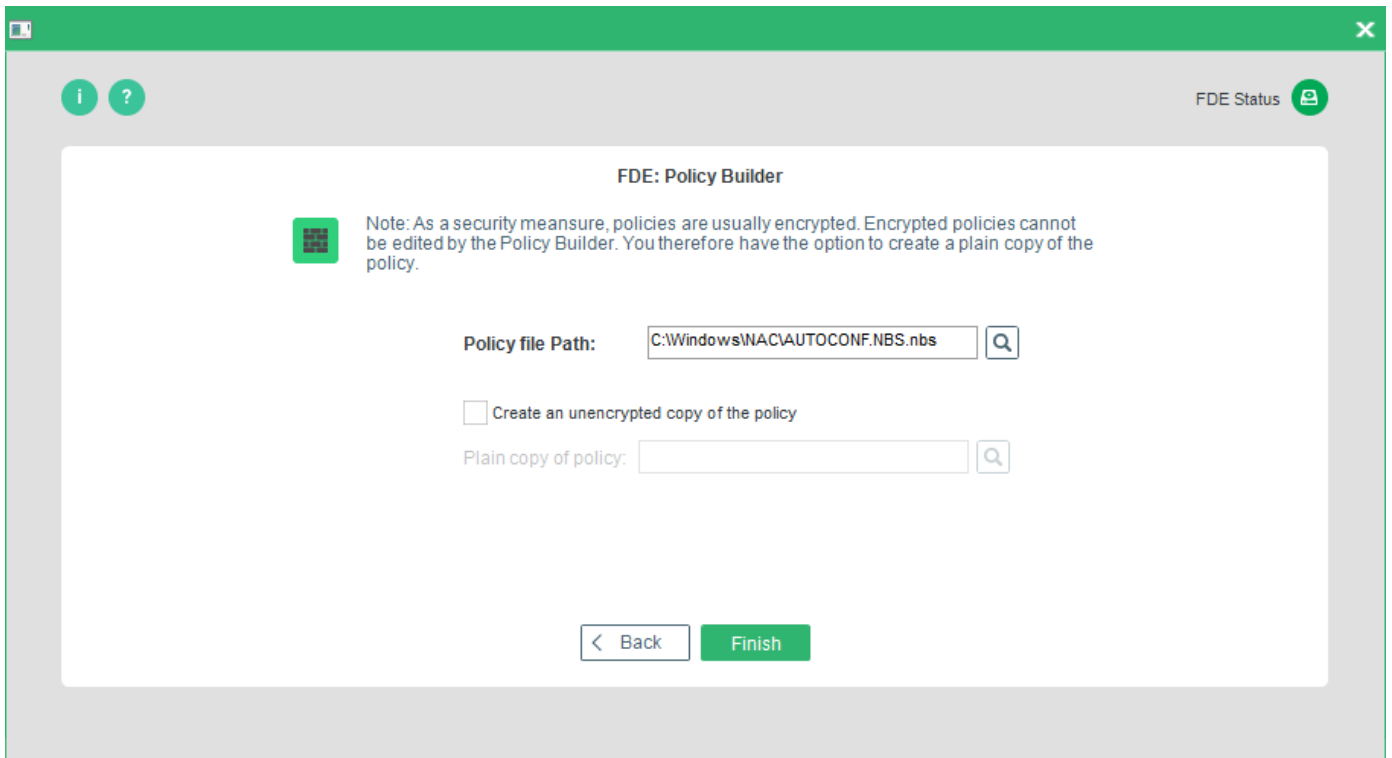
18. Make your selection and click **Next** to continue.

→ The **Administration password** (target computer) dialog appears.

19. Enter and confirm the EgoSecure Full Disk Encryption administration password already set on the target computer. Click **Next** to continue.

→ The **Policy location** dialog appears.





The following options are available:

Option	Details
Policy file path	Enter the path for the policy in this field by clicking `...` and selecting a location and filename for the file in the file browser.
Create an unencrypted copy of the policy	Check this option to create an unencrypted copy of the policy (recommended for reconfiguration). If you want to reconfigure a computer that has already been configured using a policy, then check this option - the Policy Builder can only open an unencrypted policy to edit the settings.
Plain copy of policy	Enter the path for the plain copy of the policy in this field by clicking `...` and selecting a location and filename for the file in the file browser.

20. Enter the paths for your policy, and click **Finish** to complete the procedure.

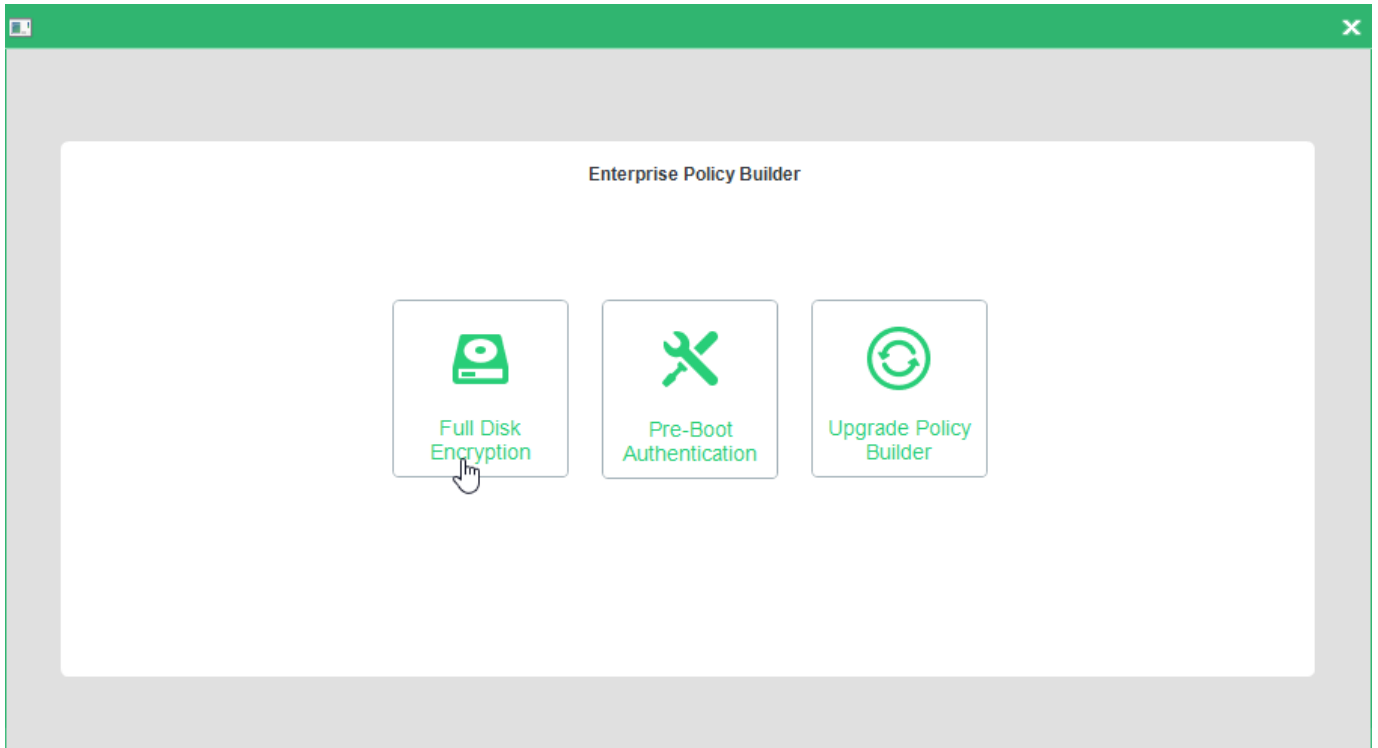
- ! It is recommended to always store plain copies in a safe place. Use the plain copies to create new policies for future changes in configuration.
- ! For security reasons encrypted policies cannot be edited with the FDE Policy Builder.

## Creating a de-initialization policy

This section details how to create an initialization policy for the FDE component only. You need to have knowledge about the target computer for deployment. Details such as number of partitions, drive letters, whether encrypted, and so on are necessary for the successful deployment of EgoSecure Full Disk Encryption. Once the policy is created, deploy it, for details see [Deploying FDE policies](#).

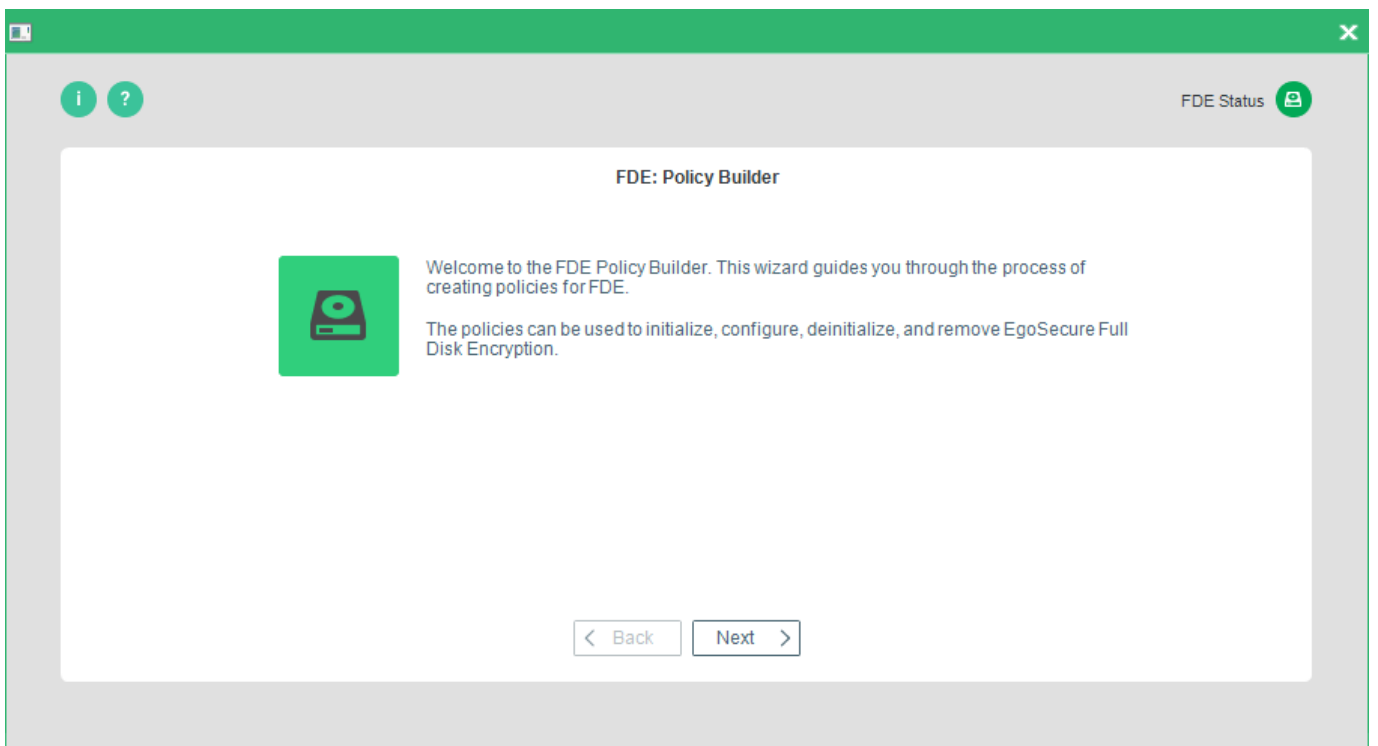
Follow the steps below to create a FDE initialization policy:

1. Open the **Control Center** (as described in section [1.5](#)).
2. Double-click the Policy Builder icon.
3. Select Full Disk Encryption policy builder.



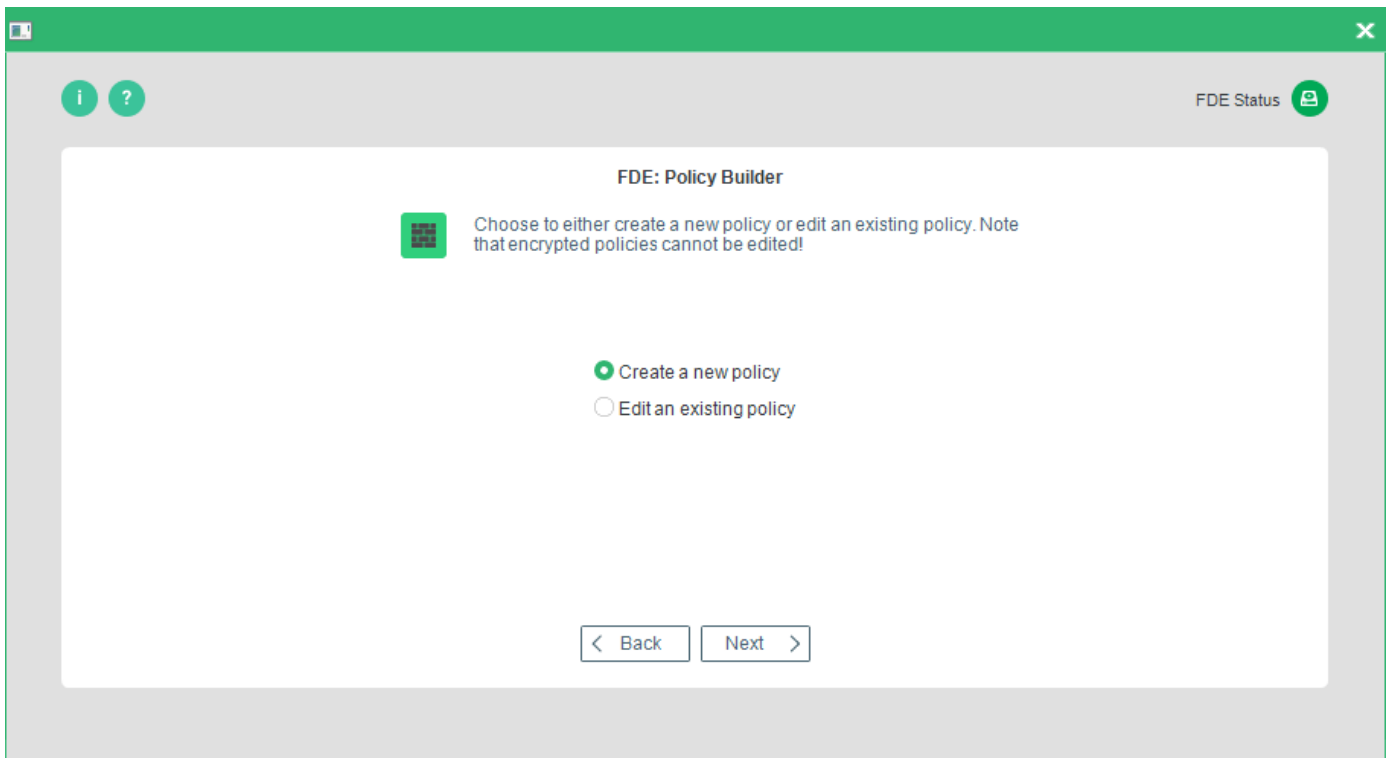
→ The FDE Policy Builder Welcome dialog appears.

4. Click **Next**.



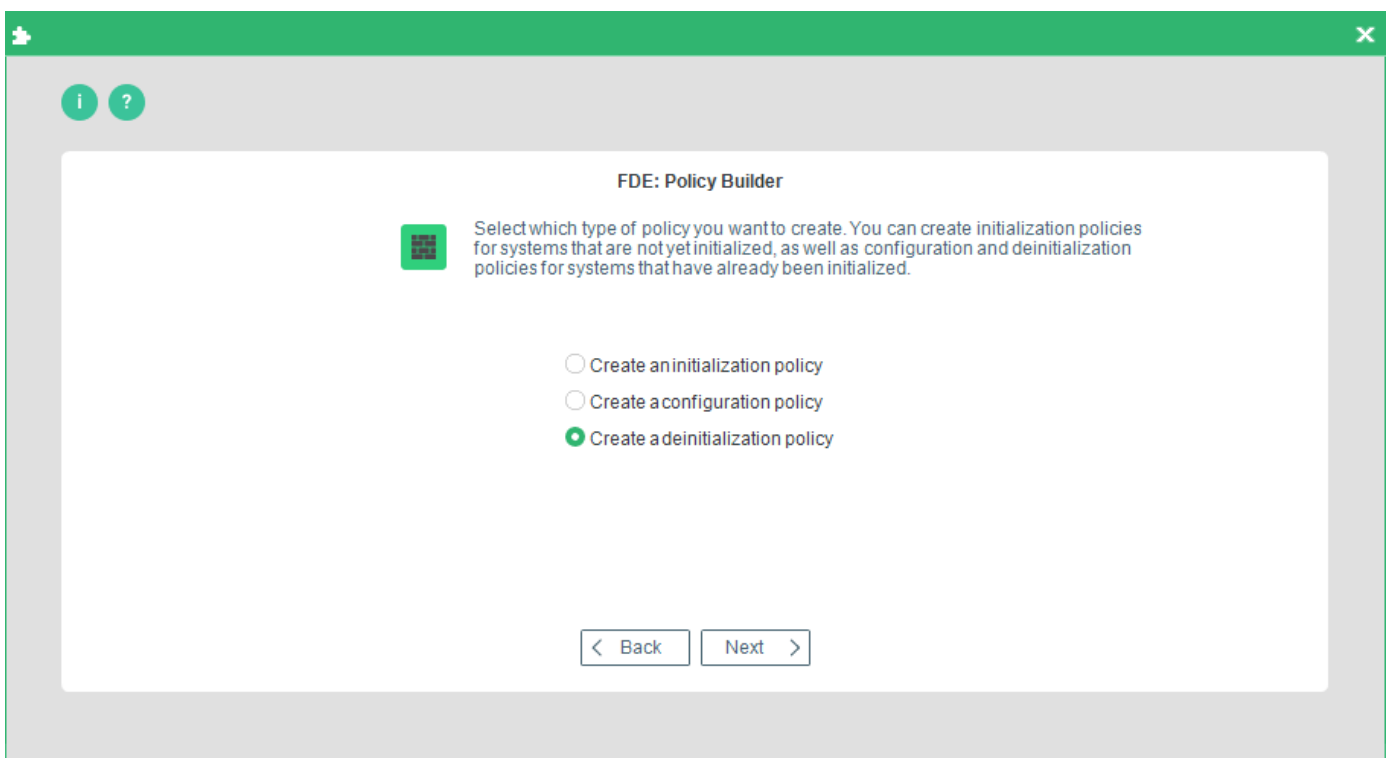
→ The **Policy selection** dialog appears.

5. Select Create a new policy.

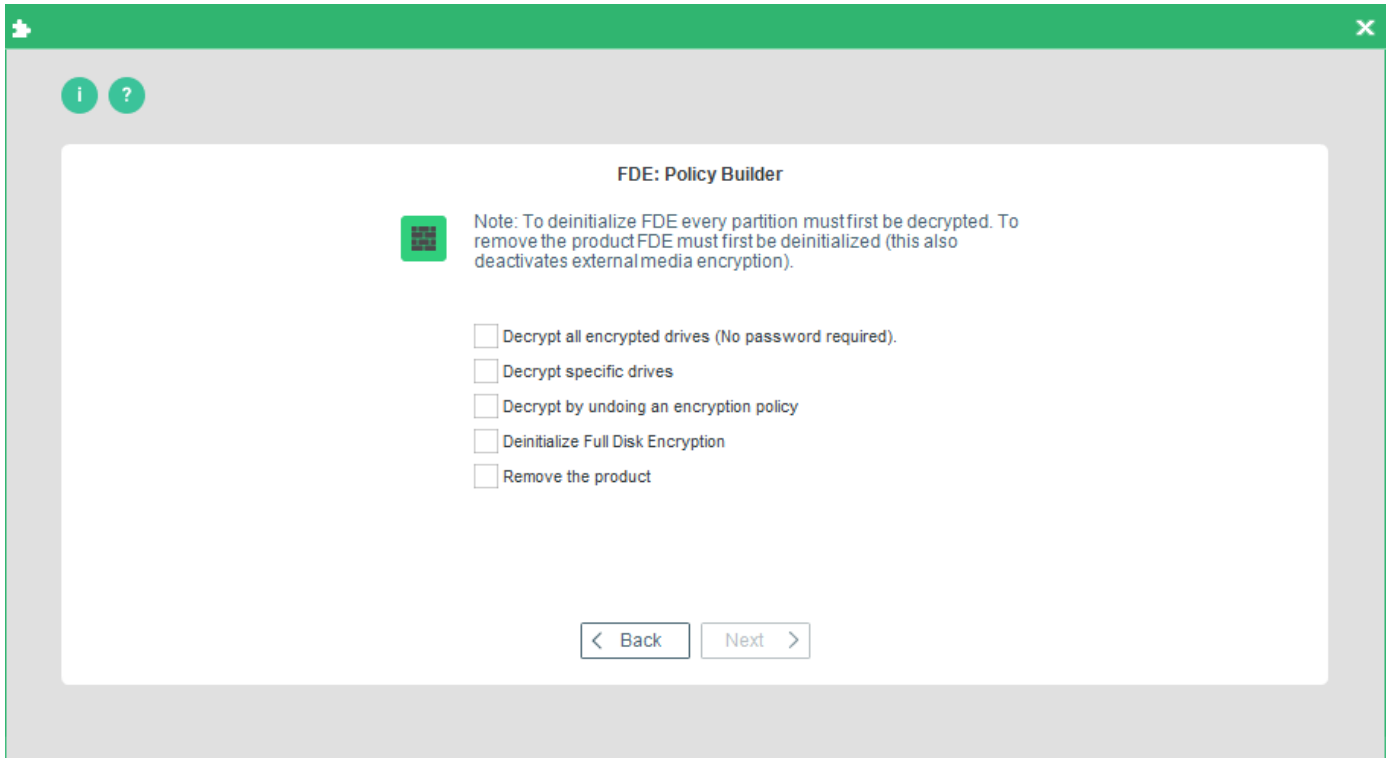


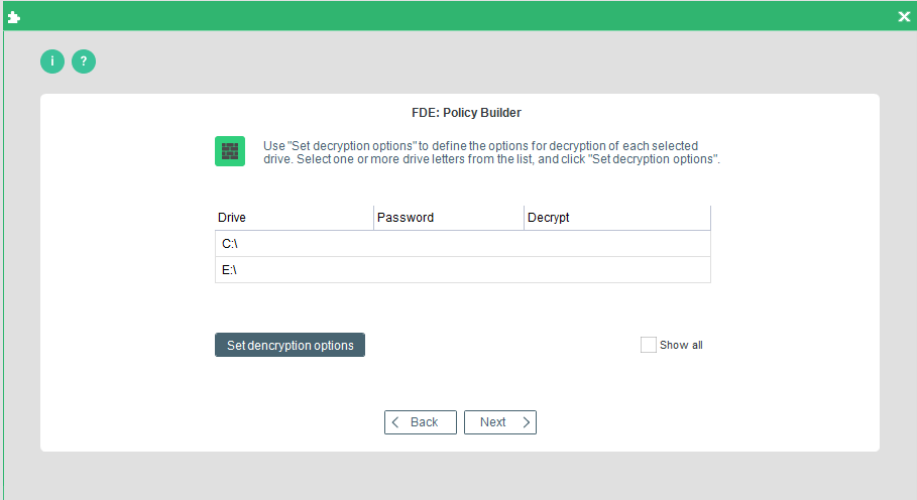
→ The **Policy type** dialog appears.

6. Select Create a deinitialization policy, and click Next.

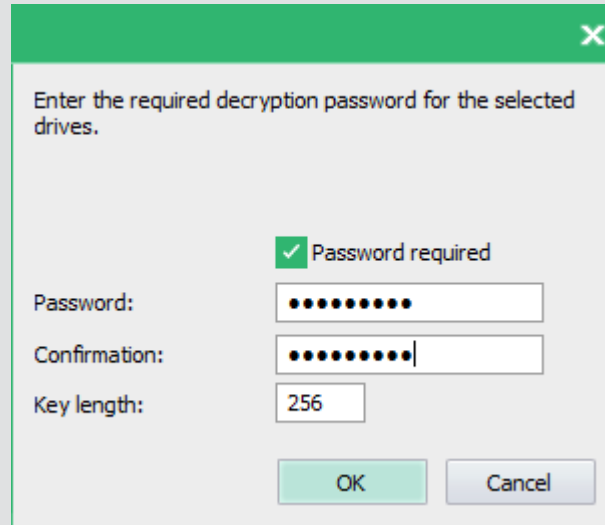


→ The Deinitialization options dialog appears.



Option	Details
<p>Decrypt all encrypted drives (No password required)</p>	<p>Check this option to decrypt all partitions encrypted by <i>EgoSecure Full Disk Encryption</i>. This option is only valid if none of the decrypted drives requires key input for decryption. Partitions that require key input for decryption can only be decrypted with the <b>Decrypt specific drives</b> or <b>Decrypt by undoing an encryption policy</b> options.</p>
<p>Decrypt specific drives</p>	<p>Check this option to decrypt specific partitions encrypted by <i>EgoSecure Full Disk Encryption</i>. If you select this option, you will be prompted to select the drive to be decrypted:</p>  <p>Click <b>Set decryption options</b> to enter the decryption specifics:</p>

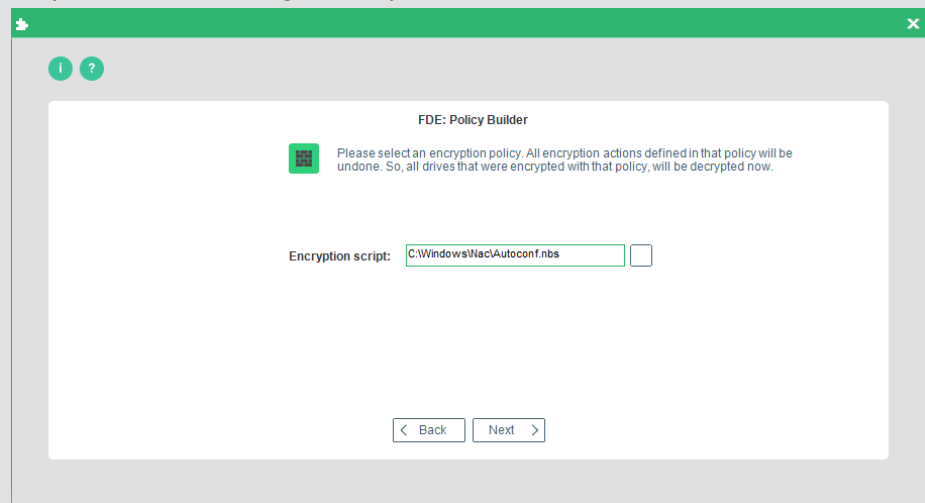
If a decryption password is required, enter and confirm the password as well as the key length, and click **OK**.



A dialog box with a green header bar and a close button (X) in the top right corner. The text inside reads: "Enter the required decryption password for the selected drives." Below this text, there is a checkbox labeled "Password required" which is checked with a green checkmark. Underneath the checkbox are three input fields: "Password:" with a masked password of ten dots, "Confirmation:" with a masked password of ten dots and a cursor at the end, and "Key length:" with the value "256". At the bottom of the dialog are two buttons: "OK" and "Cancel".

Check this option to decrypt any partition (except the partitions encrypted with a random key) encrypted via a configuration or initialization policy. If you select this option, you will be prompted to locate the encryption policy used on the target computer:

Decrypt by undoing an encryption policy



A dialog box titled "FDE: Policy Builder" with a green header bar and a close button (X) in the top right corner. It contains an information icon (i) and a help icon (?). The main text says: "Please select an encryption policy. All encryption actions defined in that policy will be undone. So, all drives that were encrypted with that policy, will be decrypted now." Below this is an "Encryption script:" label followed by a text box containing "C:\Windows\Wac\Autoconf.nbs" and a file browser icon (...). At the bottom are two buttons: "< Back" and "Next >".

Click `...` to open the file browser, locate the policy, and press **Next** to continue with the steps below. The policy content will automatically be displayed in each dialog.

Deinitialize Full Disk Encryption

Check this option to temporarily deactivate (not remove) the full disk encryption component.

Remove the product

Check this option to remove *EgoSecure Full Disk Encryption* from the target computer. This will automatically include the **Deinitialize Full Disk Encryption** option.  
While removing the product please ensure that PBA is not initialized and that there are no encrypted drives on the target computer(s). If PBA (initialized) or an encrypted drive exists an error will occur during policy processing. It is therefore recommended to also check the PBA status and select the option Decrypt all encrypted drives if you want to access your data after EgoSecure Full Disk Encryption has been removed.

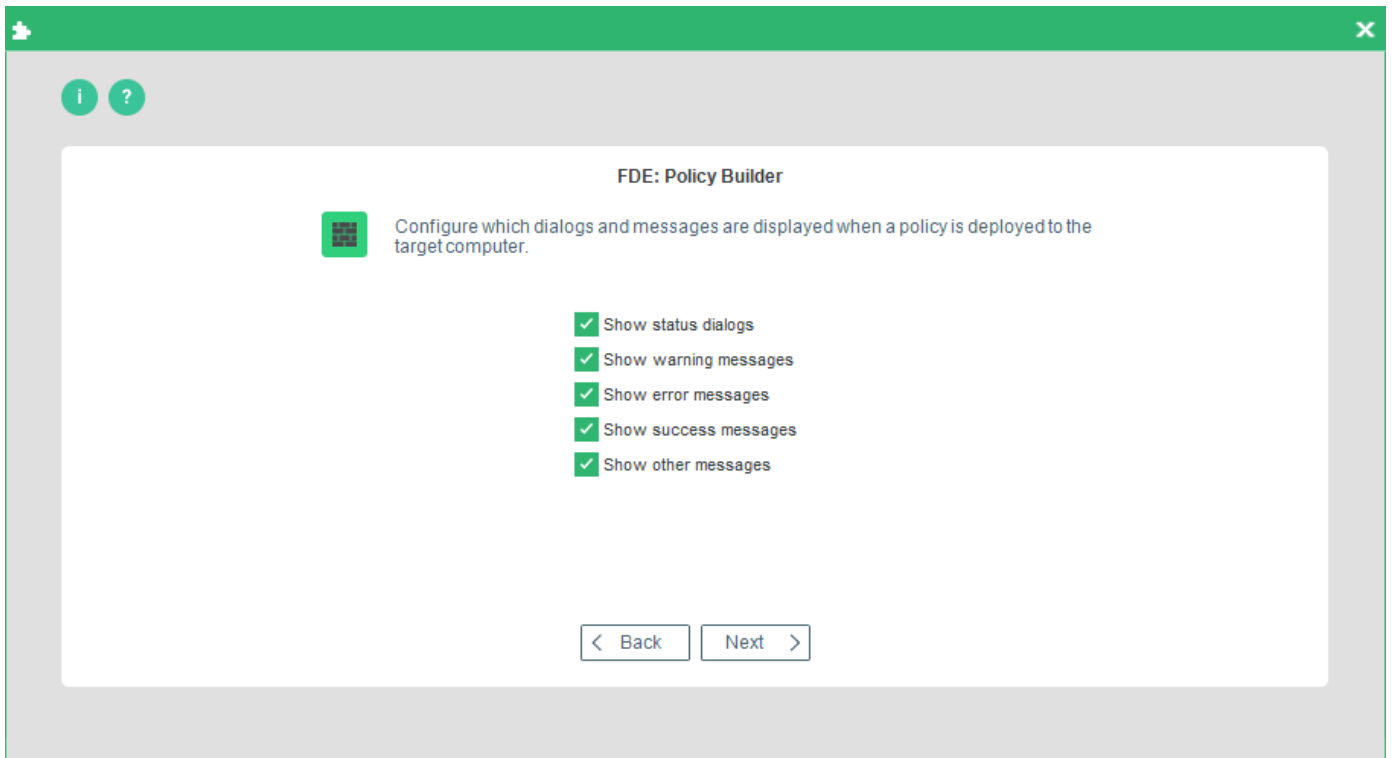
7. Once you have made your selection, click **Next** to continue.

! Any option you check in this dialog will affect the dialogs that appear hereafter! The following steps assume that you have checked every option to configure every detail! If you have not checked some options and have reached one of the steps here that does not match that on your monitor, then skip the step(s) until you come to the correct dialog!

→ The **Policy messages options** dialog appears. The messages below are shown only on computers with Windows versions below Windows 10.

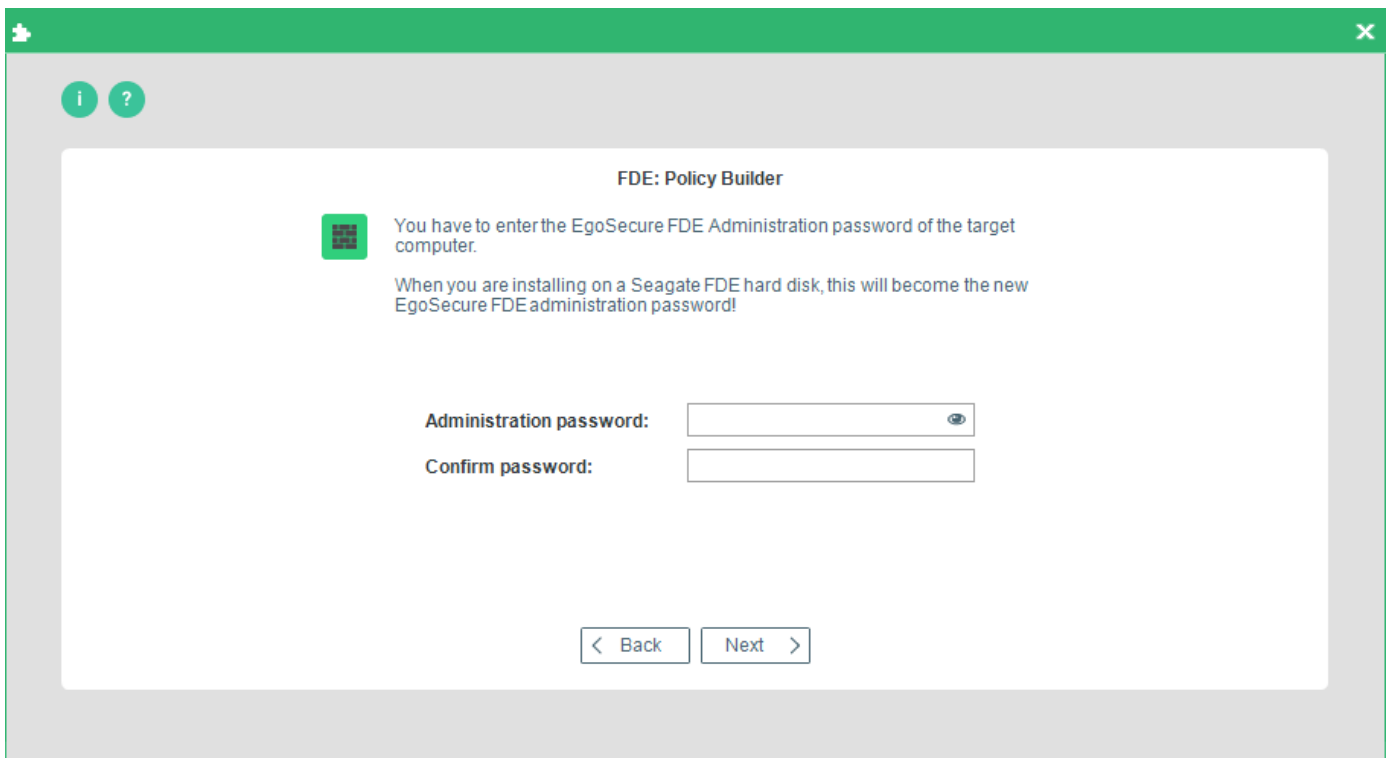
→ This dialog allows you to define the following installation messages:

Option	This option determines if...
Show status dialogs	... status dialogs should be displayed on the target computer during policy deployment.
Show warning messages	... warning messages should be displayed on the target computer during policy deployment. If you do not select this option, warning messages are suppressed.
Show error messages	... error messages should be displayed on the target computer during policy deployment. If you do not select this option, error messages are suppressed.
Show success messages	... success messages should be displayed on the target computer that relate to individual policy tasks during deployment.
Show other messages	... information messages should be displayed on the target computer during and after policy deployment. If you do not select this option, information messages are suppressed.



8. Make your selection and click **Next** to continue.

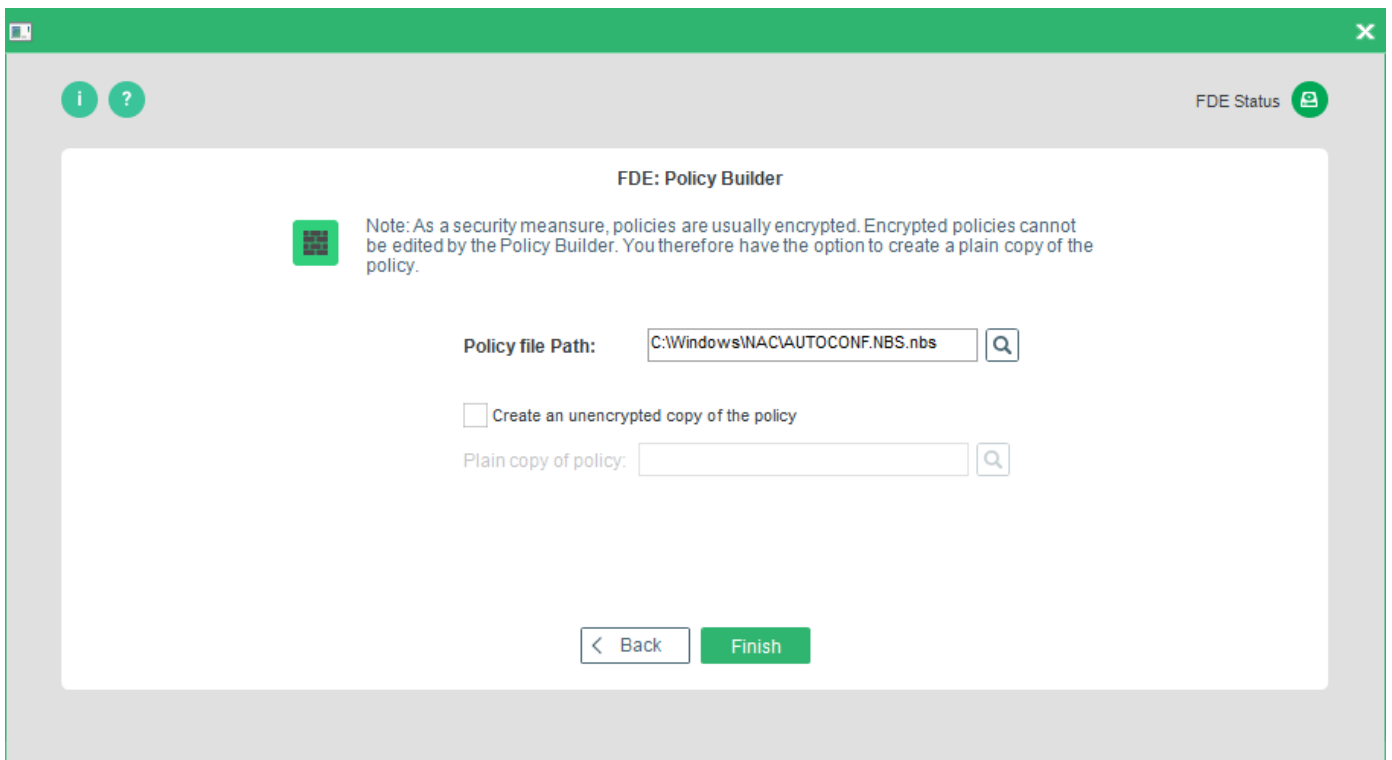
→ The **Administration password** (target computer) dialog appears:



9. Enter and confirm the EgoSecure Full Disk Encryption administration password already set on the target computer. Click **Next** to continue.

→ The **Policy location** dialog appears. The following options are available:

Option	Details
Policy file path	Enter the path for the policy in this field by clicking `...` and selecting a location and filename for the file in the file browser.
Create an unencrypted copy of the policy	Check this option to create an unencrypted copy of the policy (recommended for reconfiguration). If you want to reconfigure a computer that has already been configured using a policy, then check this option - the Policy Builder can only open an unencrypted policy to edit the settings.
Plain copy of policy	Enter the path for the plain copy of the policy in this field by clicking `...` and selecting a location and filename for the file in the file browser.



10. Enter the paths for your policy and click **Finish** to complete the procedure.

- ! It is recommended to always store plain copies in a safe place. Use the plain copies to create new policies for future changes in configuration.
- ! For security reasons, encrypted policies cannot be edited with the FDE Policy Builder.

### Editing policies

Policy Builder offers an editing function when you need to change or tweak a policy.





## ATTENTION

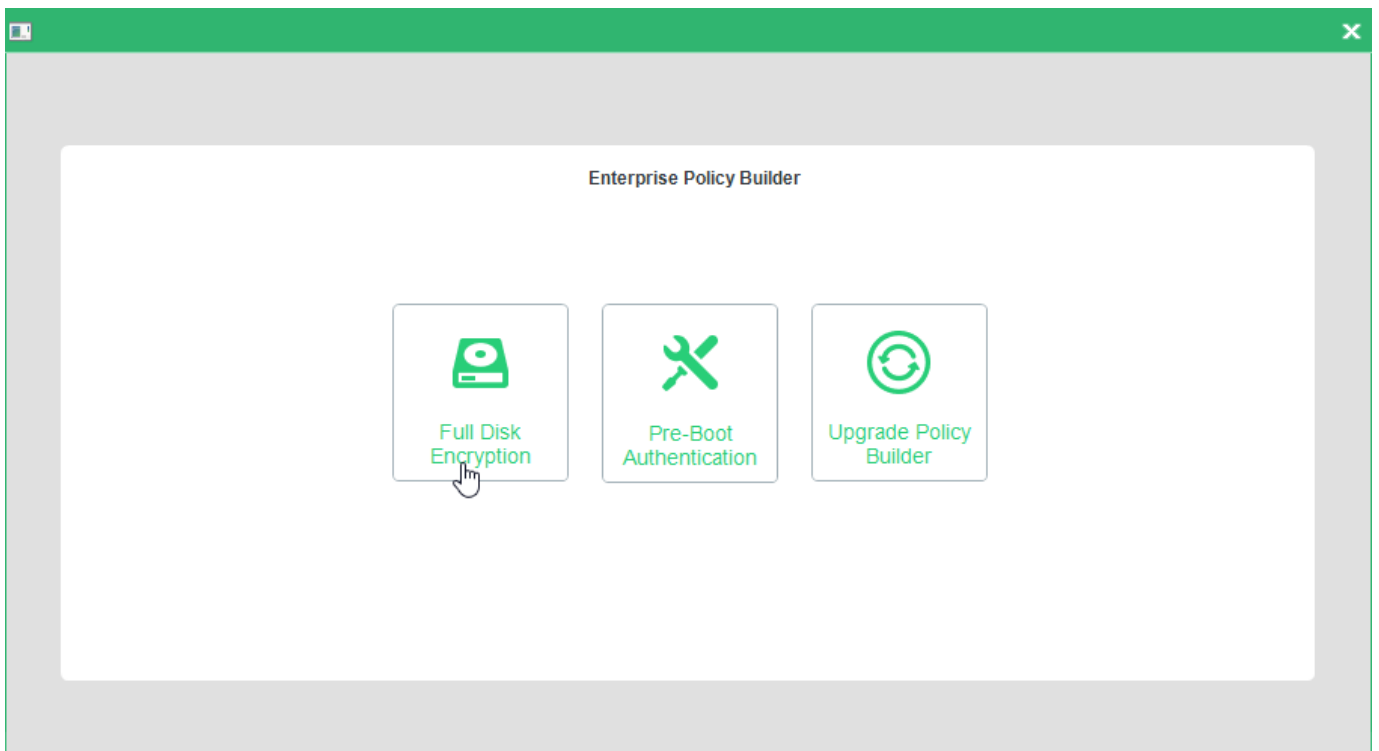
### Selecting policies for editing in Policy Builder

Only plain (unencrypted) policies can be selected to be edited in Policy Builder.

For details about saving an unencrypted copy of a policy during the policy creation process, see [creating initialization policy](#) (step 18), [creating configuration policy](#) (step 19), and [creating de-initialization policy](#) (step 9).

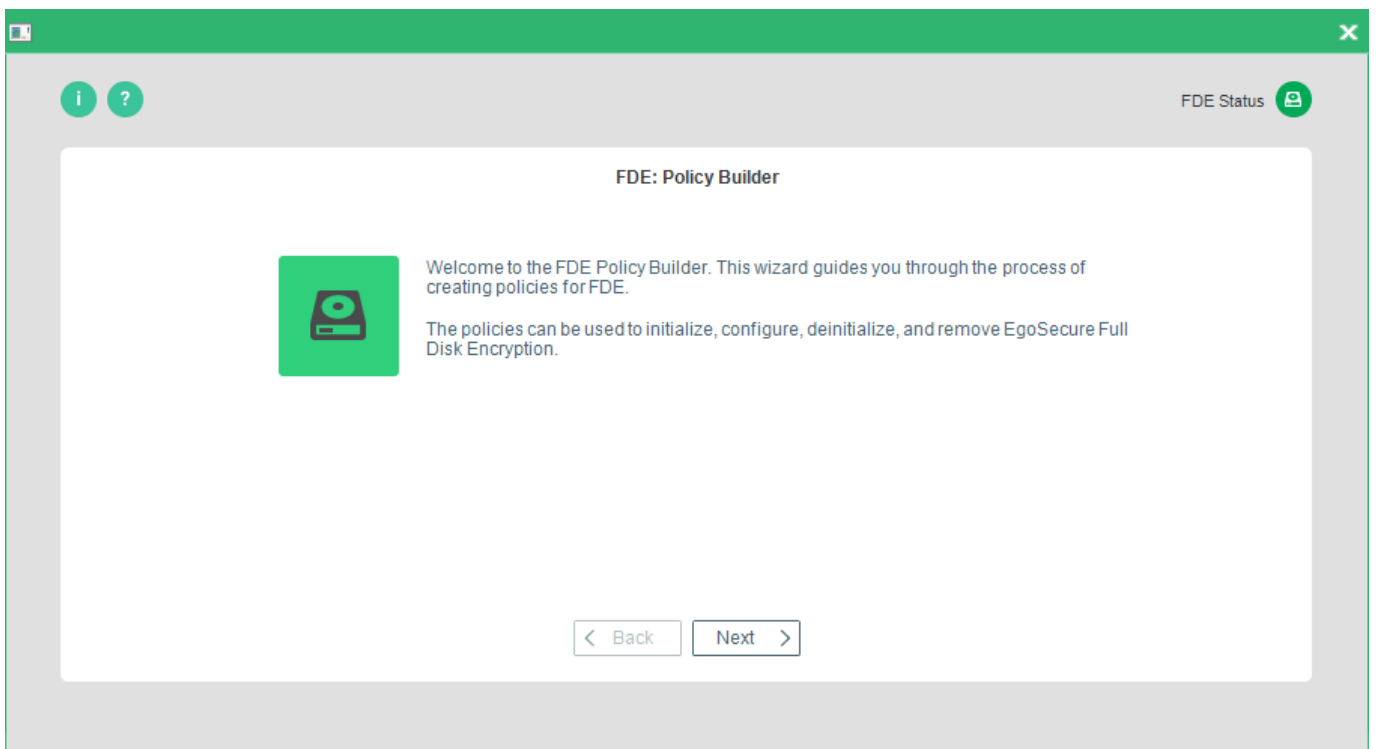
Follow these steps to edit a policy:

1. Open the **Control Center** (as described in section [1.5](#)).
2. Double-click the Policy Builder icon.
3. Select Full Disk Encryption policy builder.

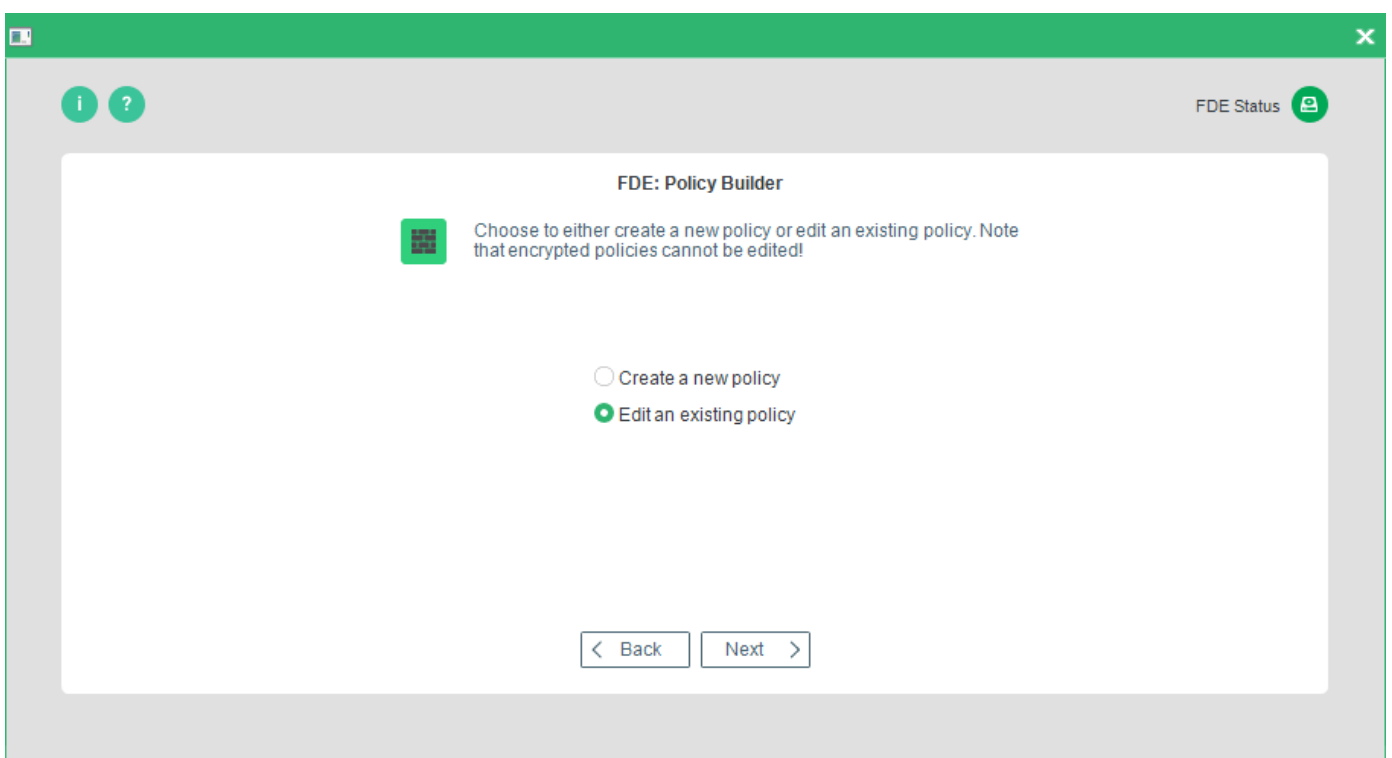


→ The FDE Policy Builder **Welcome** dialog appears.

4. Press **Next**.

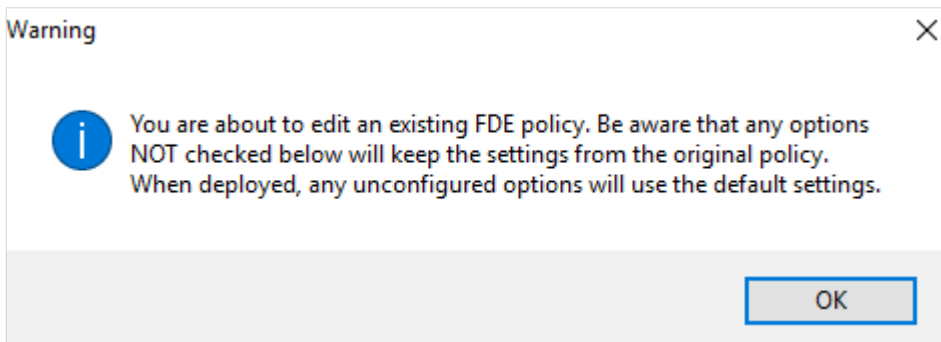


→ The **Policy selection** dialog appears.



5. Click **Edit existing policy**, and select a plain policy from the file browser.

→ The following warning message appears:



6. Click **OK**.

→ Depending on which type of policy you have selected, the editing process is the same as the policy creation process. For further steps, please refer to...

Option	Details
Initialization policy	Step <a href="#">6</a> .
Configuration policy	Step <a href="#">6</a> .
De-initialization policy	Step <a href="#">6</a> .

➤ Now you are ready to deploy the policy.

## 2.2. The Pre-Boot Authentication Policy Builder

The PBA Policy Builder is a tool to create and edit policies for the purpose of configuration, initialization, and de-initialization. The purpose of these policies is to allow for an administrator to remotely control and ensure the consistent, central deployment and configuration of PBA with no need for user interaction.

### ■ Initialization Policies

These policies allow you to initialize and configure computers that already have EgoSecure Full Disk Encryption PBA installed but not yet initialized.

### ■ Configuration Policies

These policies allow you to either perform a new installation of PBA to another networked computer, or to remotely configure FDE after it has been installed.

### ■ De-initialization policies

These policies allow you to decrypt drives, remove boot security on a client machine, or even to remove the whole product.

A policy is usually created on a different computer from the computer to which the policy will be deployed. FDE has to be installed on the computer that generates the policy, but boot security and drive encryption do not.

## CONTENTS

- ◆ [Creating an initialization or configuration policy](#)

- ◆ [Creating a de-initialization policy](#)
- ◆ [Editing an existing PBA policy](#)
- ◆ [Deploying Pre-Boot Authentication policies](#)

**INFO****Storing policy**

It is recommended that the policy is stored in the shared network for future reference. Make sure you have the access to the network in case you need to use the policy at a later date.

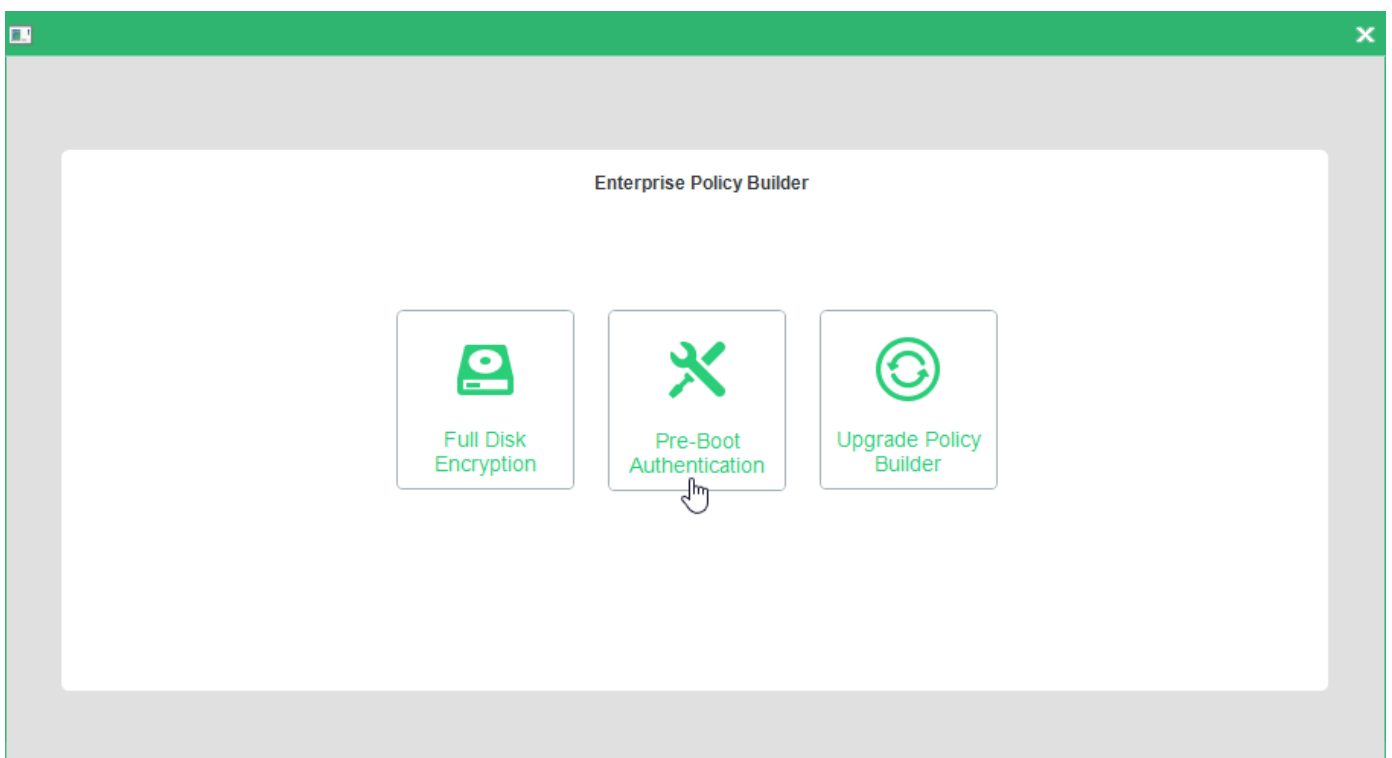
## Creating an initialization or configuration policy

This section details how to create an initialization or configuration policy for the PBA component only.

You need to have knowledge about the target computer for deployment. Details such as the number of partitions, drive letters, whether the drive is already encrypted, and so on are necessary for the successful deployment of EgoSecure Full Disk Encryption. Once the policy is created, deploy it, for details see [Deploying PBA policies](#).

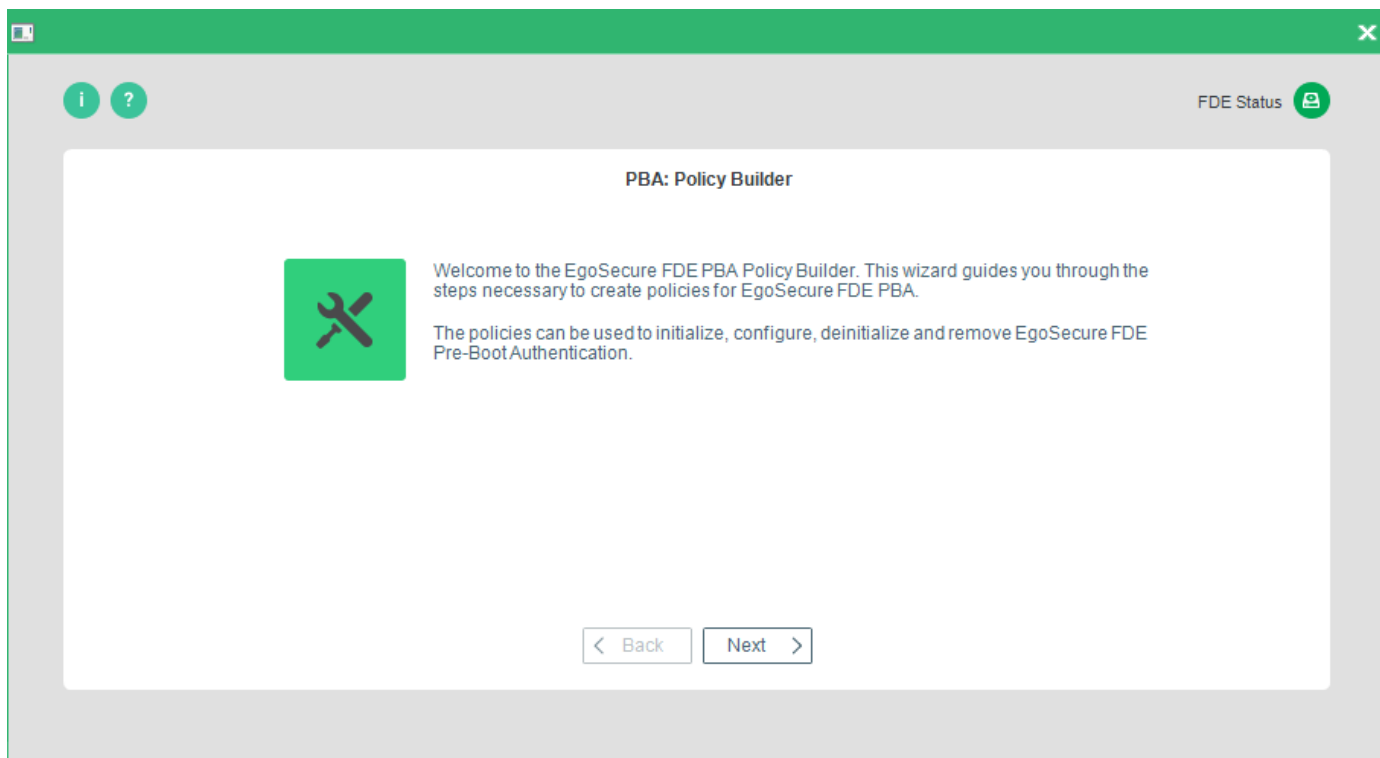
Follow these steps to create a new policy in PBA Policy Builder:

1. Open the **Control Center** (as described in section [1.5](#)).
2. Double-click the Policy Builder icon.
3. Select **Pre-Boot Authentication**.



→ The PBA Policy Builder Welcome dialog appears.

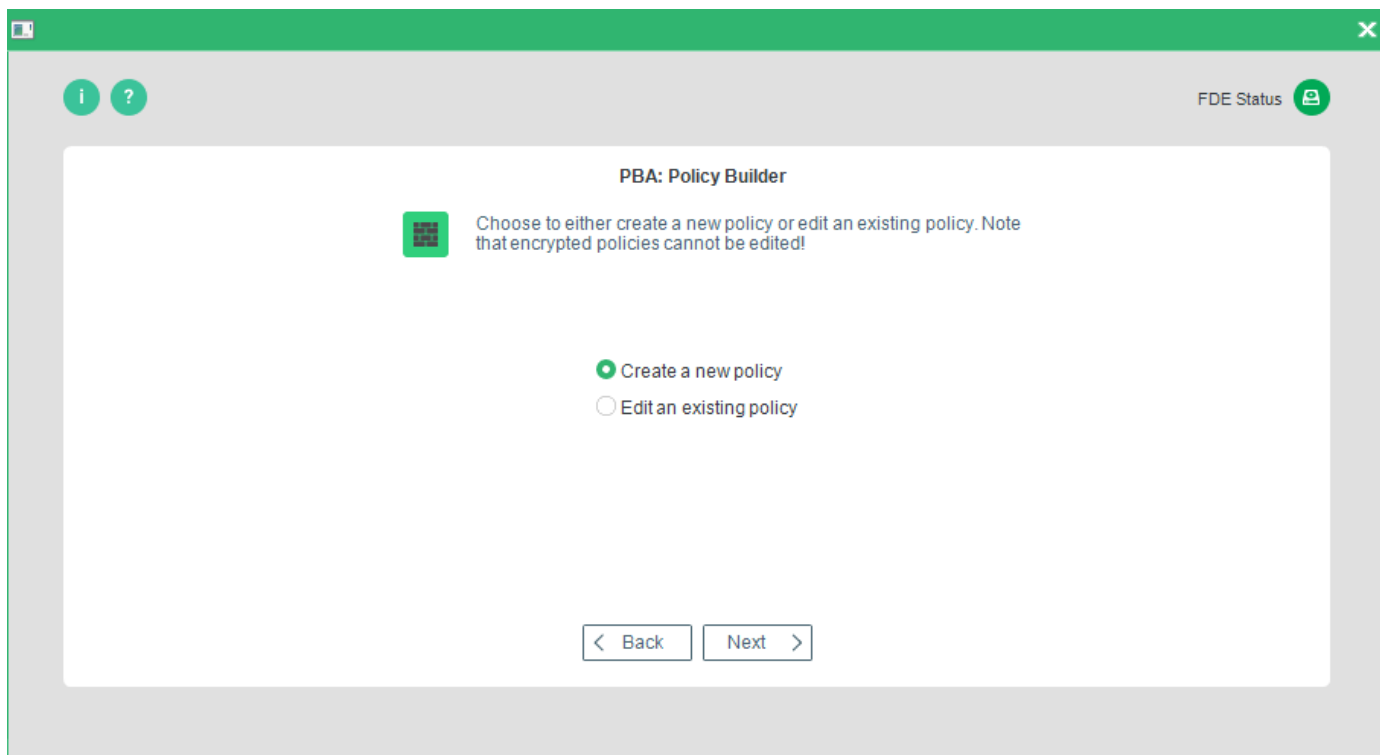
4. Click **Next** to continue.



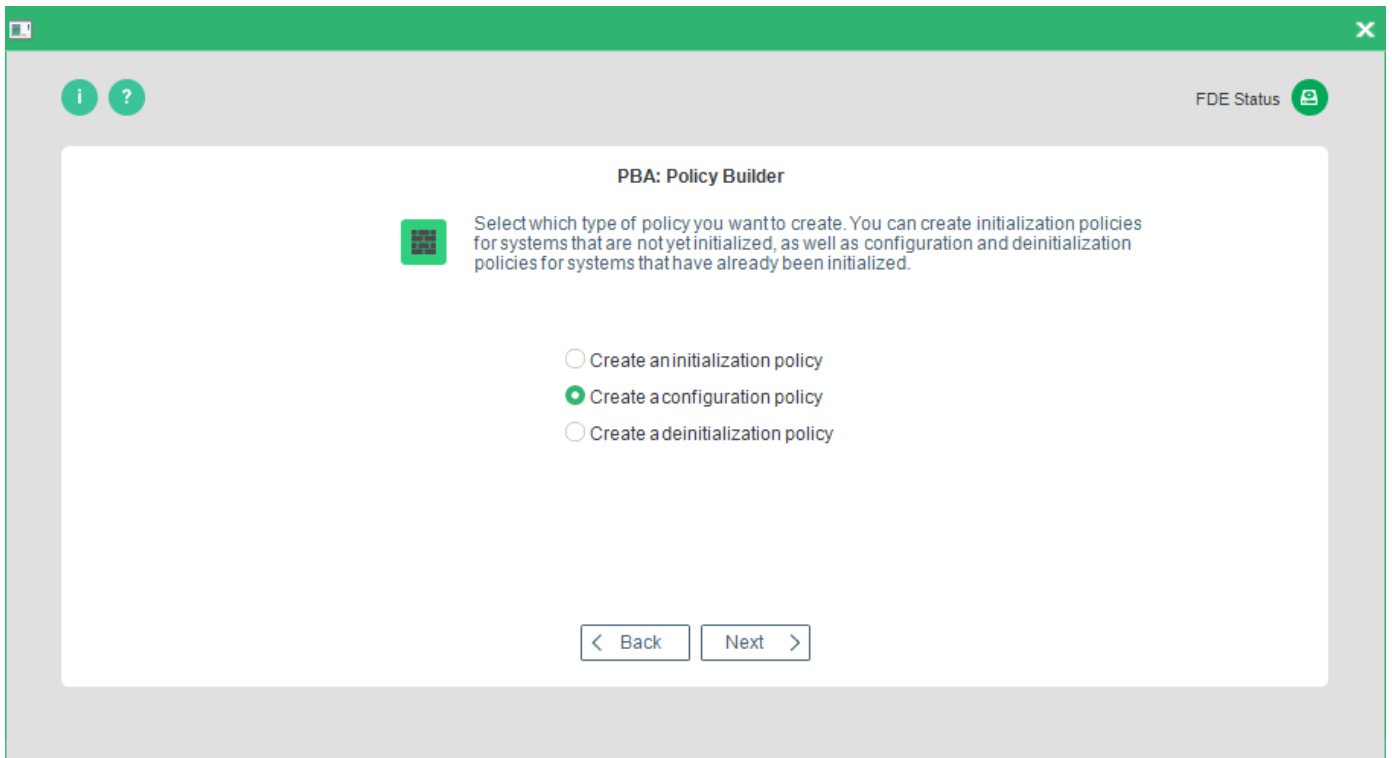
→ The **Policy selection** dialog appears.

5. Select the **Create a new policy** radio button.

Click **Next** to continue.

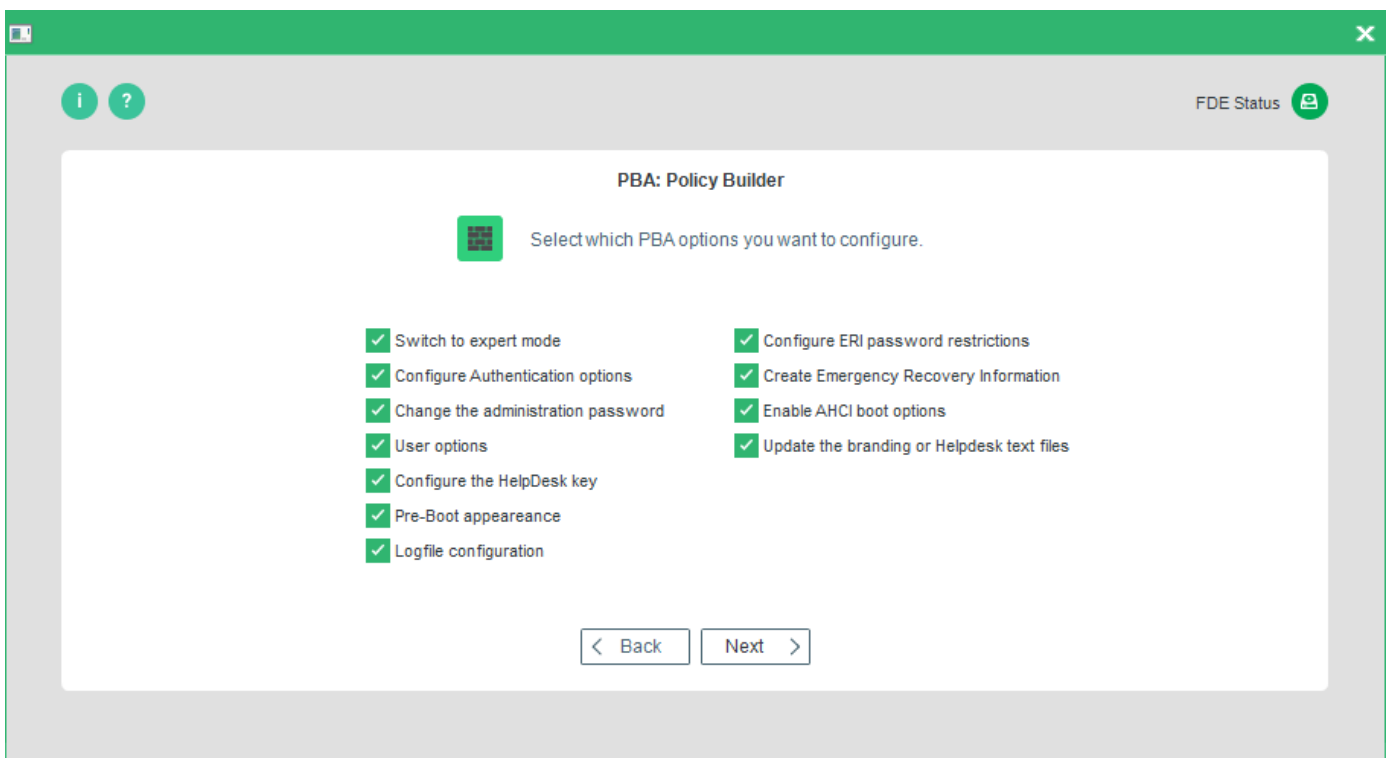


→ The **Policy type** dialog appears.



6. Select either **Create an initialization policy** or **Create a configuration policy**, and click **Next** to continue.

→ The **Initialization** dialog appears.



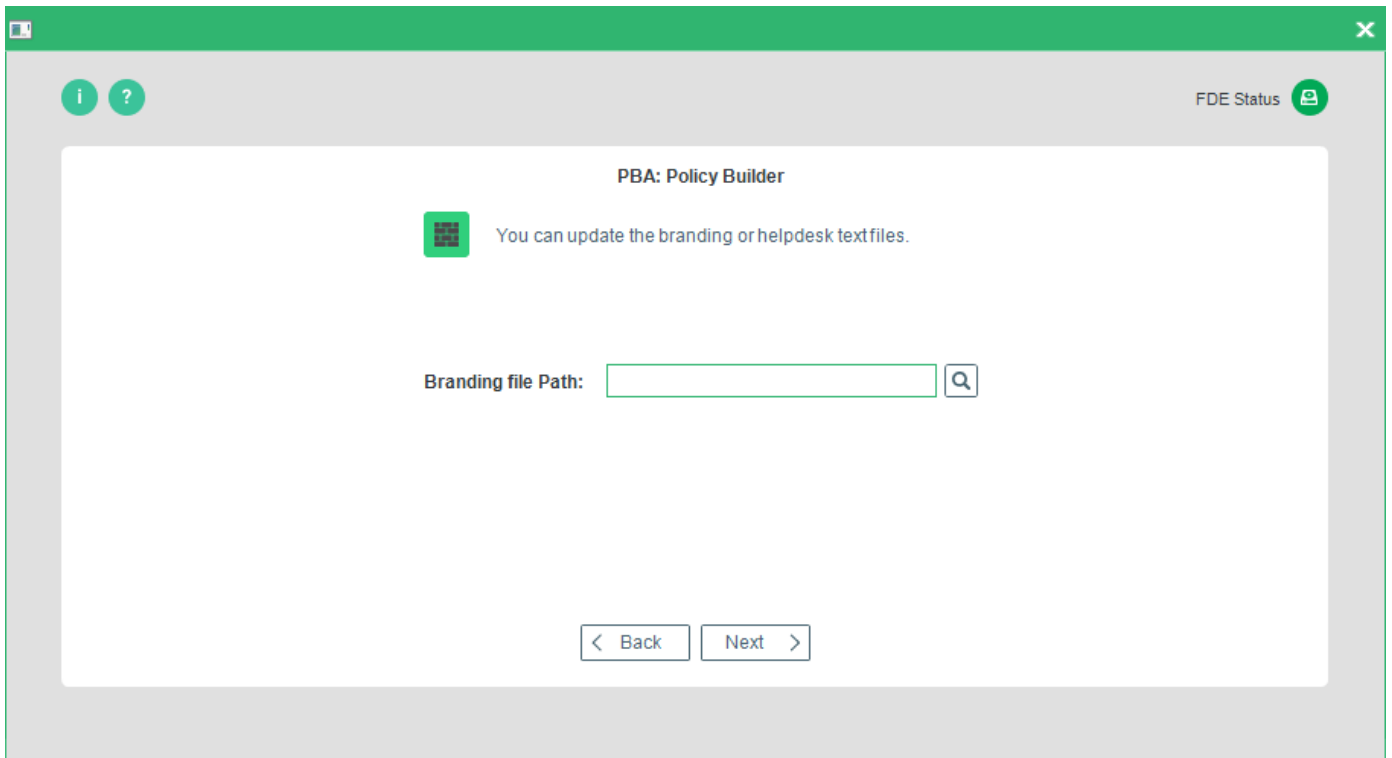
7. Check the **Switch to expert mode** option to display all of the initialization/configuration options available for this type of policy:

The following steps detail all of the available dialogs that you can configure. According to whether you are creating an initialization or configuration policy, some options – and therefore dialogs - will not be available (the screenshot above shows all of the available options if you create a configuration policy). If you reach a dialog in the steps below that you do not see on your screen please move on to the next step.

Option	Details
Switch to expert mode	Configure every aspect of initialization (activating this option will also display further options – see below).
Configure Authentication options	Configure Windows credentials and smart card logon details (not available for an initialization policy).
Pre-Boot appearance	Configure a custom PBA background as well as the PBA integrity checking/advanced options.
Configure the HelpDesk key	Define a HelpDesk key for the HelpDesk challenge-response scenario in case of emergency. Once the HelpDesk is configured, you can activate Friendly Network.
User options	Configure Windows credentials and smart card logon details, as well as error message options.
Logfile configuration	Configure the location, name and file size of the PBA and notification DLL log files.
Configure ERI password restrictions	Define if the ERI file should have password restrictions.
Create Emergency Recovery Information	Define general settings for ERI.
Enable ACHI boot Options	This option enables 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 resolves all hardware compatibility issues or the PBA boots up after that. The mechanism used here is Dmiconfig. With this option it is available to create a dmi.ini for the current hardware platform with the configuration stated above.

8. Once you have made your selection click **Next** and go to step 9 or continue with the below dialog if configuration policy is selected.

→ The **Branding file** dialog appears.



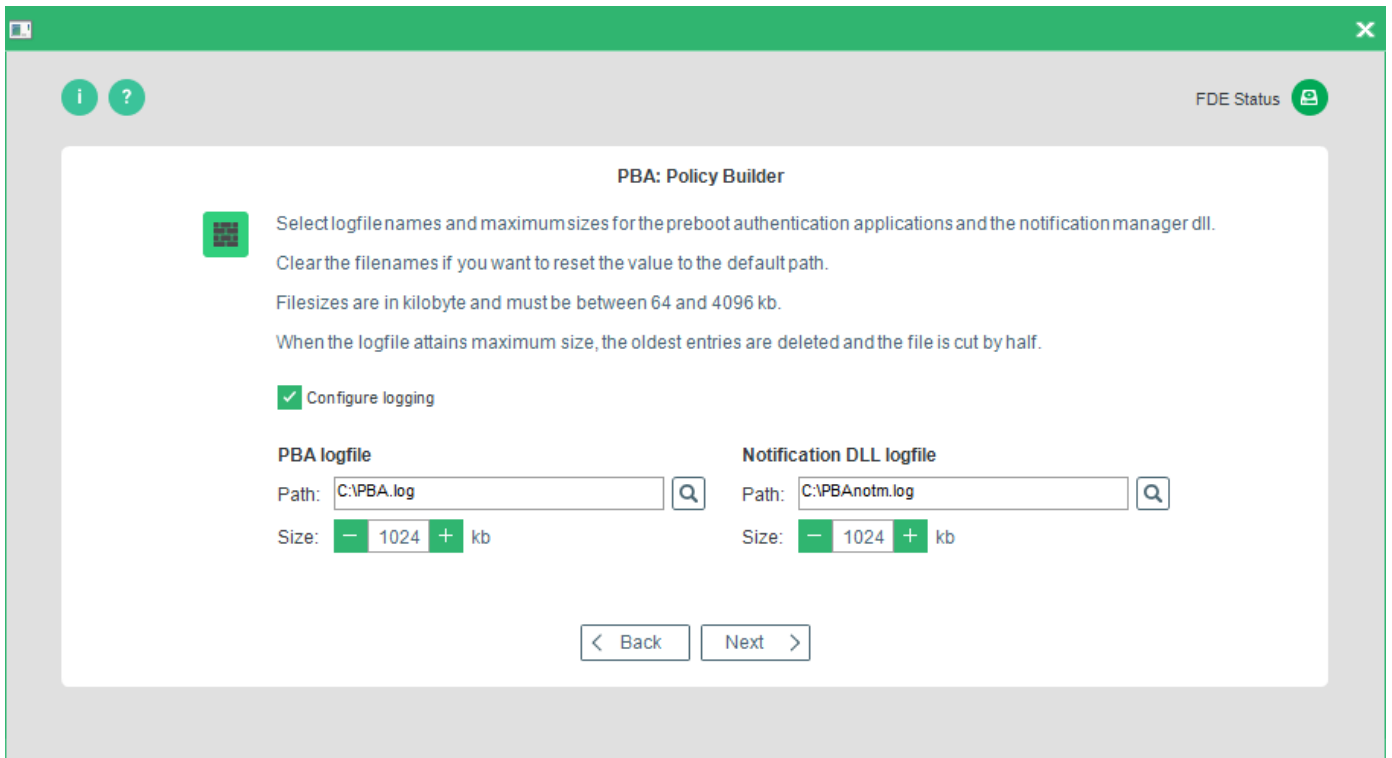
9. Browse and select a new branding file. Click **Next** to continue.

→ The **Logging** dialog appears.

10. Check **Configure logging** to set a specific location, filename, and maximum size for the log files generated by the PBA component. Clear **Configure logging** to use the default settings. The following options are available:

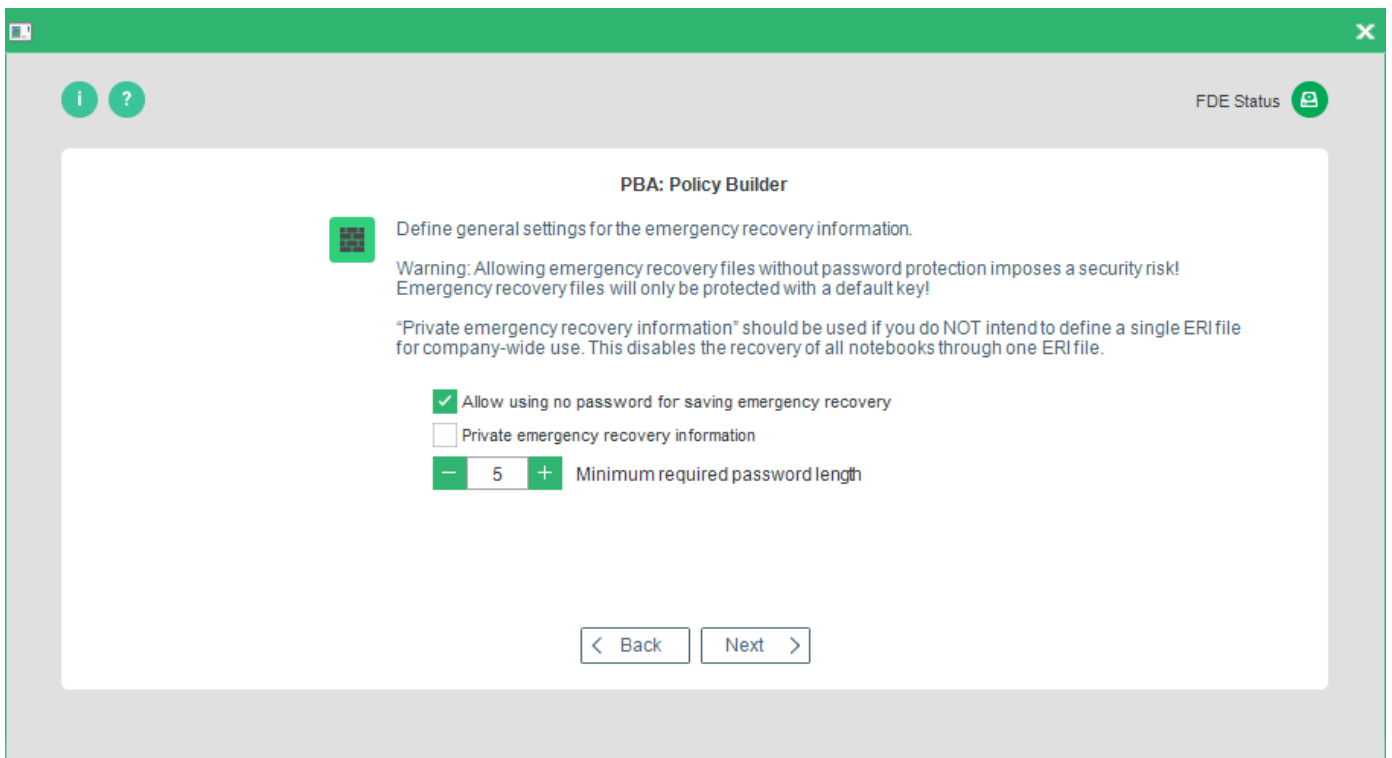
Option	Details
Path	Enter a full custom path for the PBA and notification DLL log files either directly into the <b>Path</b> field or click "..." to open a file explorer. Remember to enter the log file name and *.log extension.
Size	Set the maximum log file size.





11. Once you have made your selection, press **Next** to continue.

→ The first of three **Emergency Recovery Information** dialogs appears:



The following options are available:

Option	Details
--------	---------

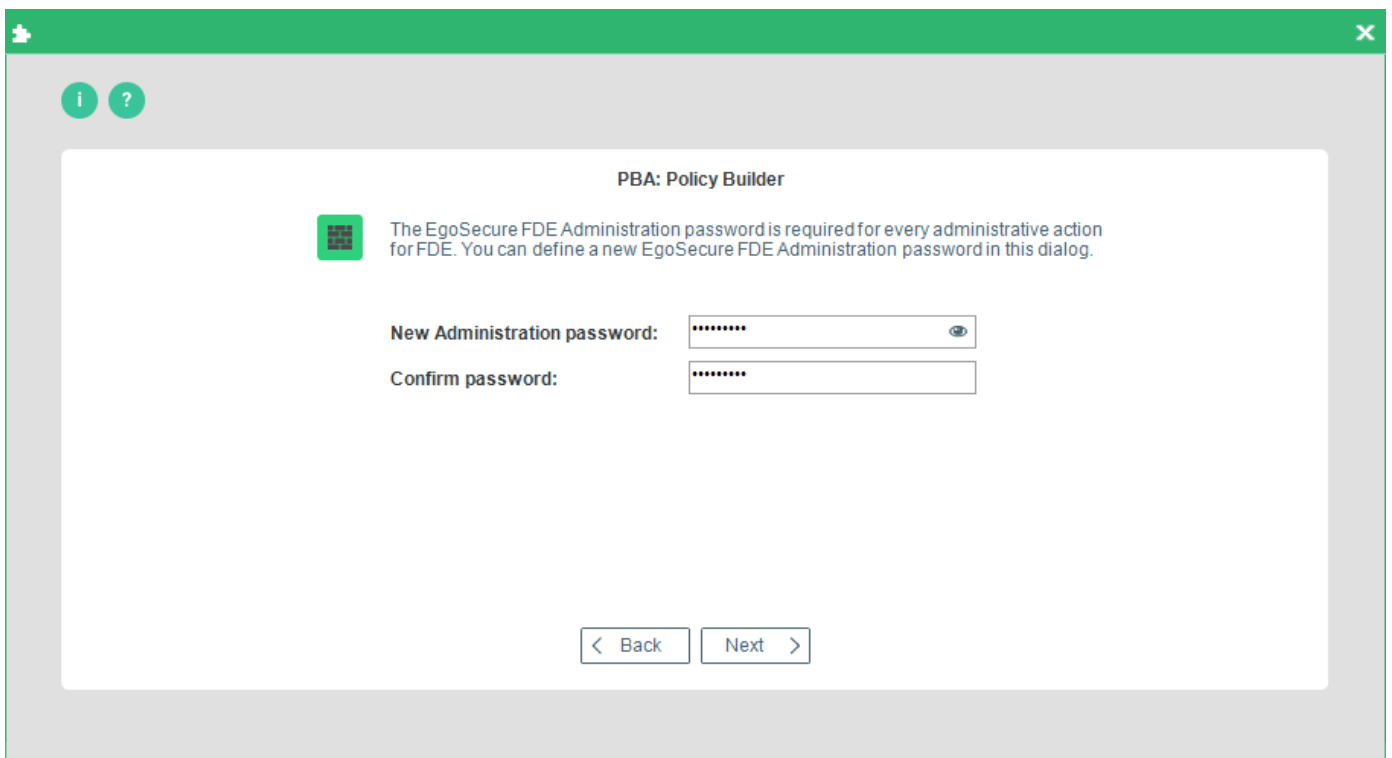
Configure emergency recovery file settings	Check this option if you want to either allow the use of unprotected ERI files, or set a minimum password length for the ERI file (up to 63 characters). <i>NOTE: Leaving the option unchecked will automatically use the default of an 8-character minimum password and generating a private ERI specifically for this computer.</i>
Allow using no password for saving emergency recovery information	Check this option to generate a password-free ERI file ( <b>not recommended</b> ).
Minimum required password length	Enter minimum length of the password.
Private emergency recovery information	Check this option if you want only ERI files generated on this computer to be able to recover this computer (recommended). If you leave this option unchecked, an administrator can access this computer using an ERI file generated on a similar system.

12. Once you have made a selection, click **Next** and go to step 13 or continue with the dialog below if configuration policy is selected.

→ The **Administration password setting** dialog appears.

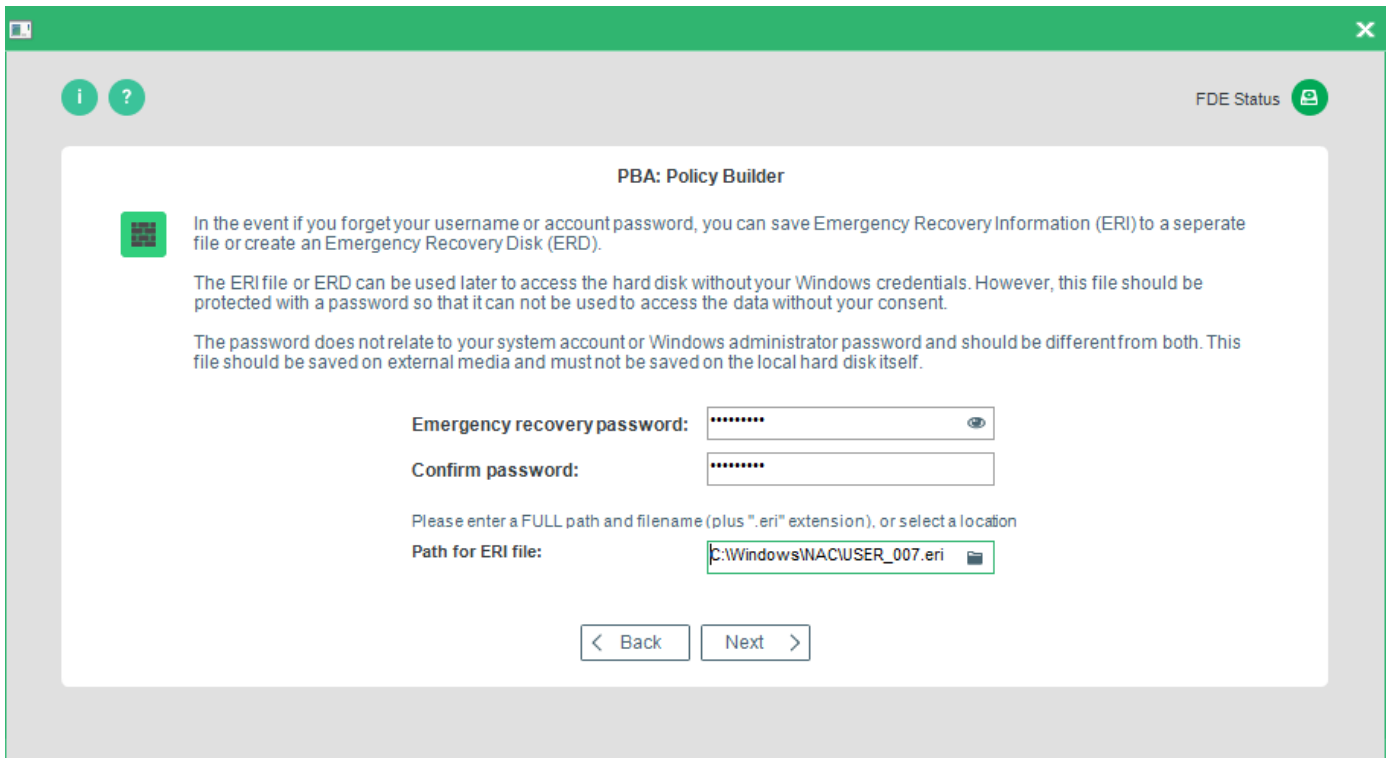
13. Select **Set the administration password** check box to specify the administration password.

14. Enter administration password and confirm it in respective text boxes.



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

→ The second **Emergency Recovery Information** options dialog appears:



The following options are available:

Option	Details
Emergency recovery password	The password used to access the ERI file in an emergency. Remember to enter the minimum number of characters as defined in step 10 (if you are using the default then enter a password between 8 to 63 characters).
Confirm password	Confirm the password for the ERI file.
Path for ERI file	The location to which the ERI file is saved. Either enter the path for the ERI file manually or click '...' to browse for a location. <i>Remember that this location must be accessible from the target computer!</i> For details about ERI copies, see <a href="#">Creating an ERI file</a> .

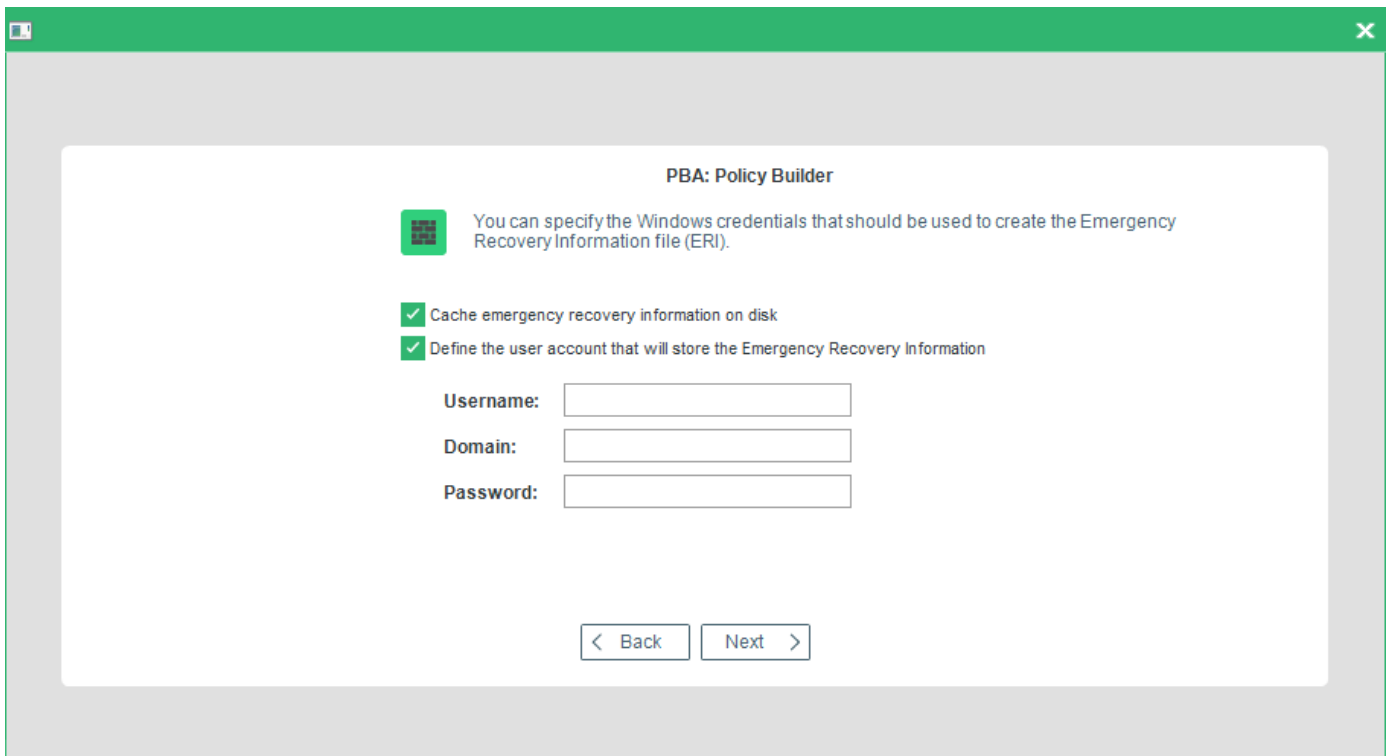
16. Make your selection and click **Next**.

- ! If you choose to save the ERI file to the local hard disk, and your hard disk is already encrypted, then a dialog will appear to remind you that saving the ERI file to encrypted location is not a good idea. If you do save the ERI file to the local drive then please transfer it to an unencrypted network, or external drive (USB stick recommended), as soon as possible so that it is accessible in an emergency.

→ The last Emergency Recovery Information options dialog appears:

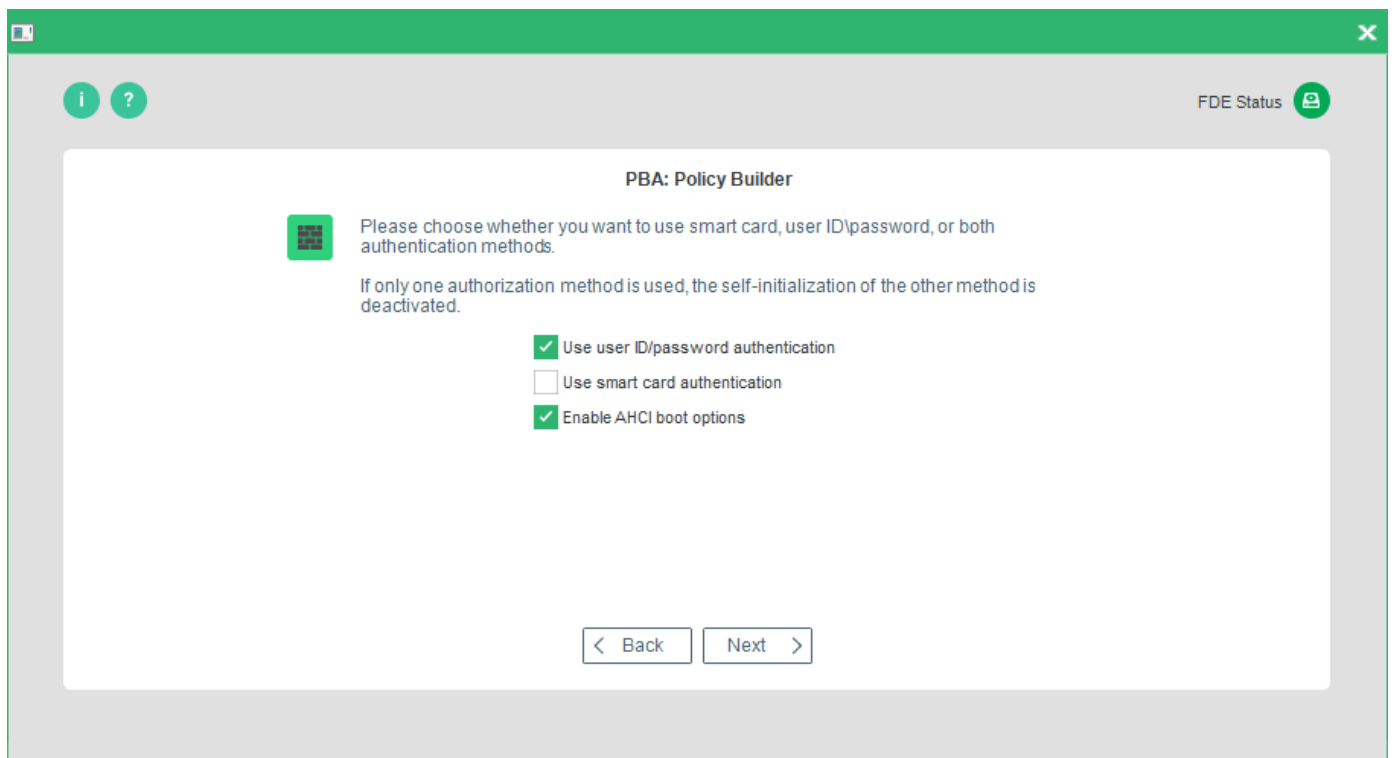
The following options are available:

Option	Details
Cache Emergency Recovery Information on disk	Check this to store the ERI on the hard disk.
Define the user account that will store the Emergency Recovery Information	Check this option if you want a specific user to be able to store ERI
Username	The <i>Windows</i> credentials username.
Domain	The <i>Windows</i> credentials domain.
Account Password	The <i>Windows</i> credentials password.



17. Make your selection, and click **Next** to continue.

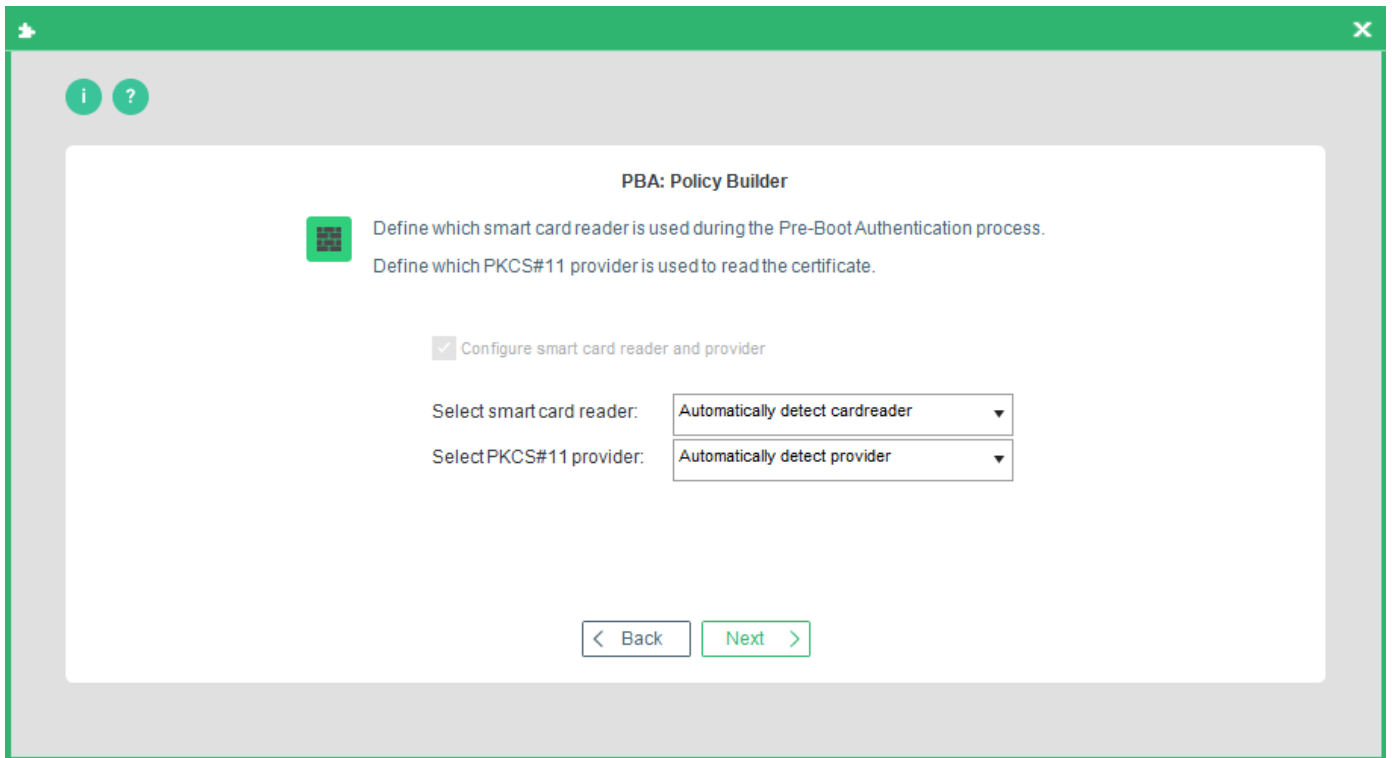
→ The **Authentication Options** dialog appears:



18. Enable the method of authentication you want to implement on the target computer (this will affect which dialogs are displayed hereafter). You can implement both **user ID/password** (Windows credentials) and **smart card authentication**. Select **Enable AHCI boot options** (this option enables only if the BIOS is set to AHCI-mode) and if a dmi.ini file already exist, the user will be asked to overwrite it or not.

19. Make your selection and click **Next** to continue.

→ The Smart card reader/PKCS#11 provider dialog appears:

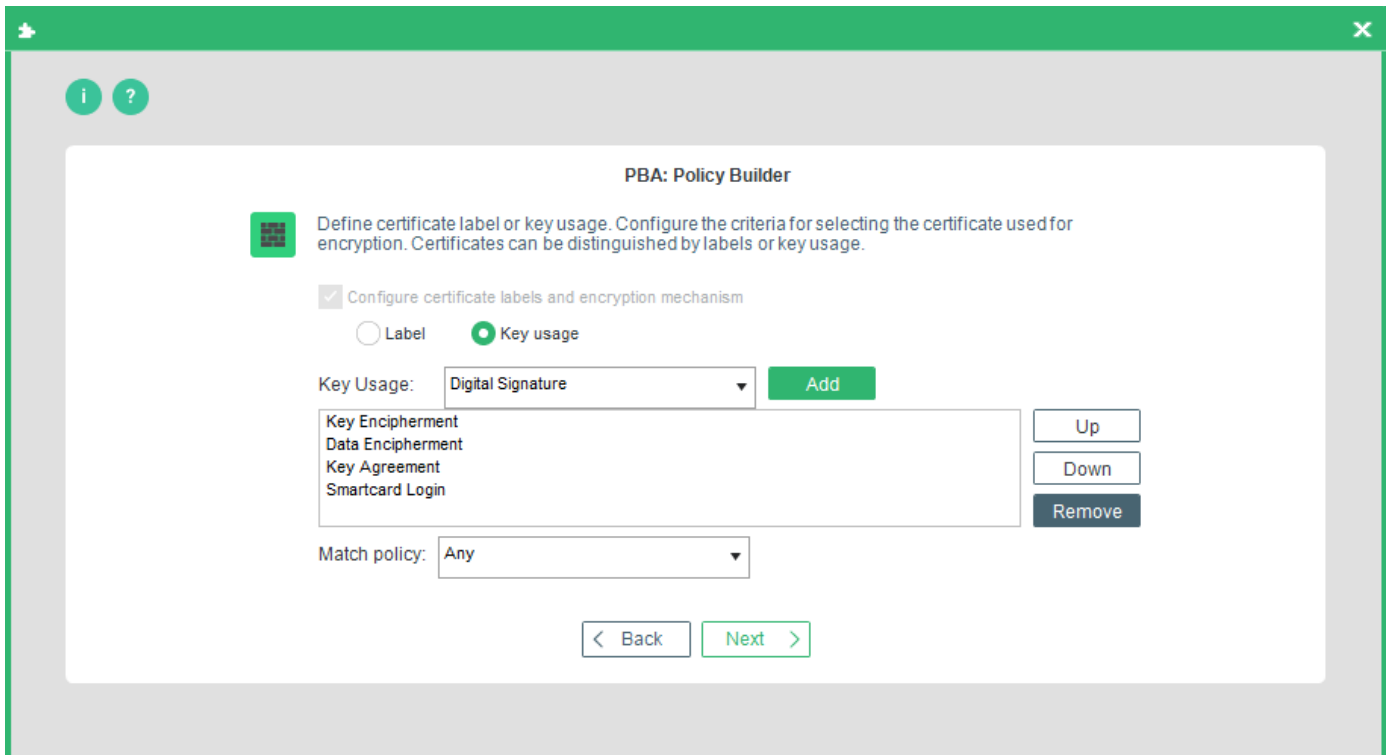


Use the following options to determine the smart card reader and provider:

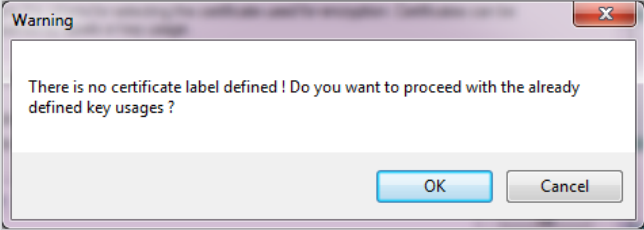
Option	Details
Choose a smart reader	Set <b>Configure the smart card reader and provider</b> check box to choose a reader and provider. Select the card reader you want to use for PBA from the drop-down list (choosing a specific card reader vendor will decrease the amount of time it takes the computer to start; choosing <b>Automatically detect card reader</b> will mean that all the smart card-reader vendors will be checked upon startup, therefore increasing the startup time).
Use PKCS#11 provider	Select the <b>PKCS#11 provider</b> mechanism on the smart card by selecting it from the combo box. (Selecting <b>Automatically detect provider</b> will mean that all the providers will be checked upon startup - this setting does not work with several smart cards).

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

→ The **Certificates** dialog appears:



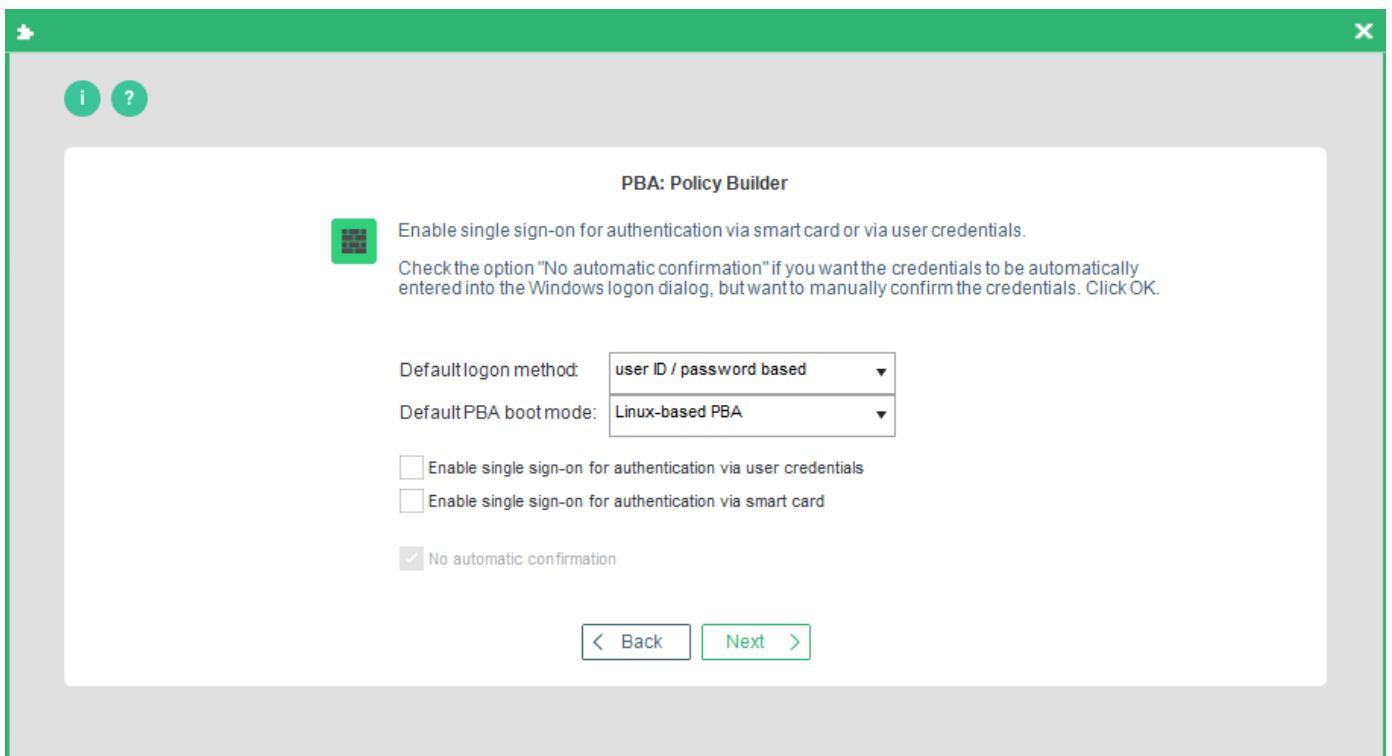
This dialog enables you to define the criteria for selecting the certificate used for encryption. Certificates can be distinguished by labels or key usage.

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> <ol style="list-style-type: none"> <li>1. Select <b>Configure labels and encryption mechanism</b> check box to enable the label and key settings.</li> <li>2. Select <b>Label</b> (the GUI will change).</li> <li>3. Enter the label into the field <b>Label</b>, and click <b>Add</b>. If the smart card contains more than one certificate (multi-user access) then you should add the labels for those as well.</li> <li>4. If you have mistakenly entered a false label, select it from the list, and click the <b>Remove</b> button to remove it from the list.</li> <li>5. To sort label preference, select a label in the list and click either <b>Up</b> or <b>Down</b> - the certificate that will be used for authentication is the first one in the list that matches the label criteria.</li> </ol> <p>The following warning messages appears if there is no certificate Label defined:</p> 

<p><b>Key usage</b></p>	<p>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.</p> <p>For example, if you have a key used only for signing, enable the <b>Digital Signature</b> and/or <b>Non-repudiation</b> extensions. Alternatively, if a key is used only for key management, enable <b>Key Encipherment</b>.</p> <p>Follow these steps to add a certificate based on Key usage:</p> <ol style="list-style-type: none"> <li>1. Select <b>Key usage</b>.</li> <li>2. Choose a standardized form of key usage from the <b>Key usage</b> combo box, for example <b>Data Encipherment</b>, and click <b>Add</b>. To give preference to a specific key usage, select it from the list and click either <b>Up</b> or <b>Down</b>. 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).</li> <li>3. If you have mistakenly entered a false certificate label, select it from the list and click <b>Remove</b>.</li> </ol>
<p><b>Match policy</b></p>	<p>Select one of the following policies:</p> <ul style="list-style-type: none"> <li>■ <b>Any</b>: The first certificate that contains any key usage from the list will be used.</li> <li>■ <b>All</b>: The certificate must fulfill all the key usages in the list.</li> <li>■ <b>None</b>: No certificate may contain any of the key usages from the list.</li> </ul>

21. Click **Next** to continue.

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



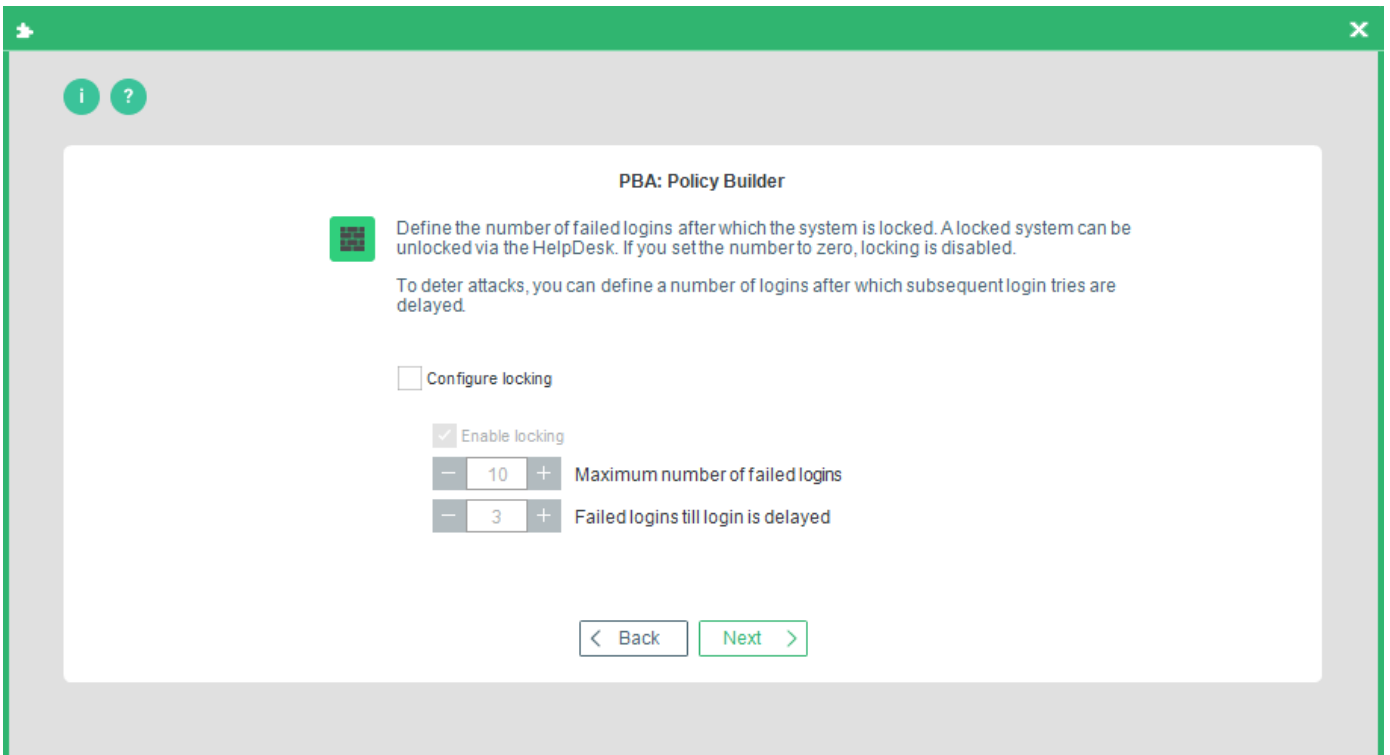


Option	Details
Default logon method	Select the default logon method from the combo box. Choose between Windows credentials (user ID/password based) or smart card-based logon. Both logon methods can be available at boot time.
Default PBA boot mode	Select the default PBA boot method. <ul style="list-style-type: none"> <li>■ <b>Linux-based PBA:</b> usual pre-boot authentication with its graphical user interface.</li> <li>■ <b>Text-based Simple PBA:</b> simple pre-boot authentication without a graphical user interface. Not available for smart card authentication.</li> <li>■ <b>Graphical Simple PBA:</b> simple pre-boot authentication with a graphical user interface. Available only for UEFI systems. Authentication via user credentials and via smart cards is supported.</li> </ul> For details, see "Boot mechanisms" in the <a href="#">EgoSecure FDE – Installation and Troubleshooting Guide</a>
Enable single sign-on for authentication user credentials	Check this option if you want PBA to take care of the traditional username/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.).
Enable single sign-on for authentication via smart card	Check this option if you already use a smart card (with X.509 certificates) to logon to the Windows domain.

22. Click **Next** to continue.

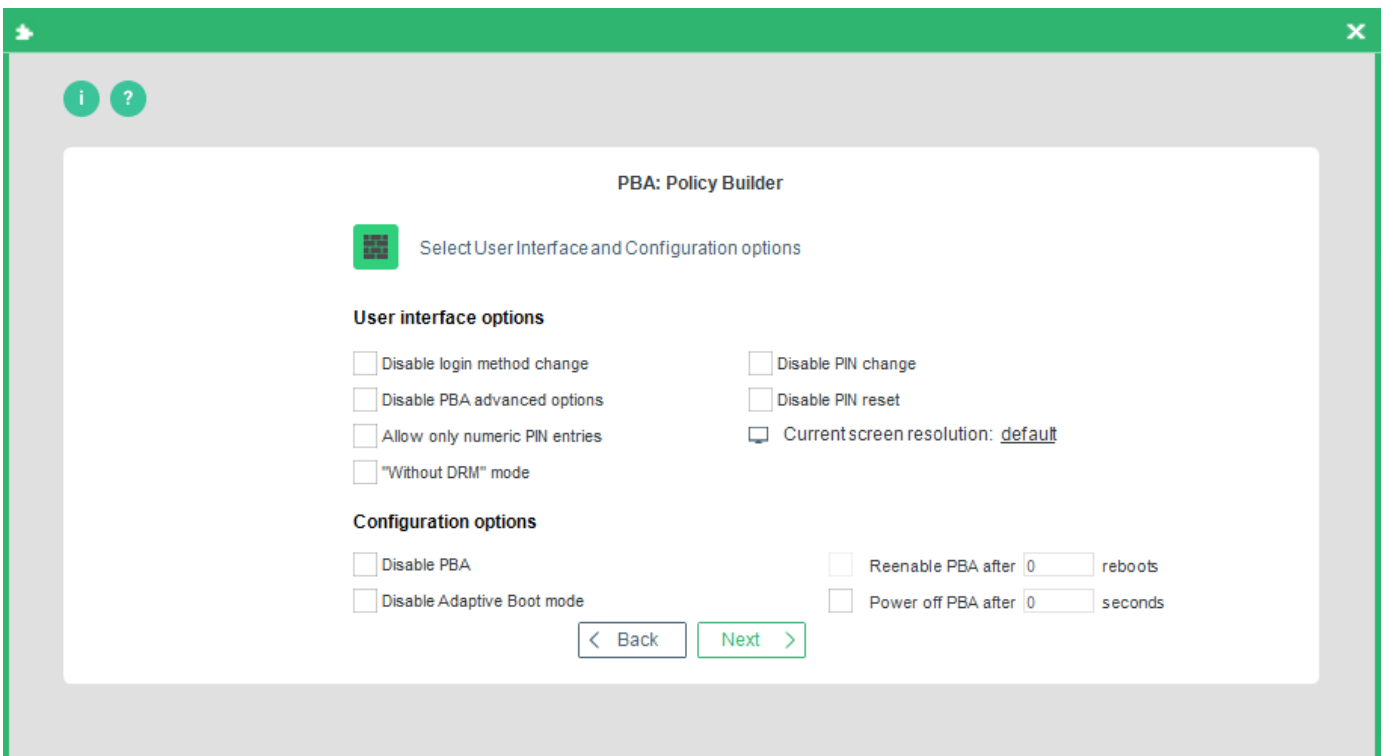
→ The **Locking** dialog appear. This page allows to set the PBA login behavior. The following options are available:

Option	Details
Configure locking	Use this option to enable the authentication locking mechanism where you can define the number of login tries before PBA locking.
Maximum number of failed logins	This option limits the total number of attempts a user needs to successfully login to the EgoSecure Full Disk Encryption Pre-Boot Authentication component.
Failed logins till login is delayed	This option penalizes the user after entering their credentials incorrectly. This value must be lower or equal than the maximum number of failed logins.



23. Select the options and click **Next**.

→ The first **Pre-boot options** dialog appears.



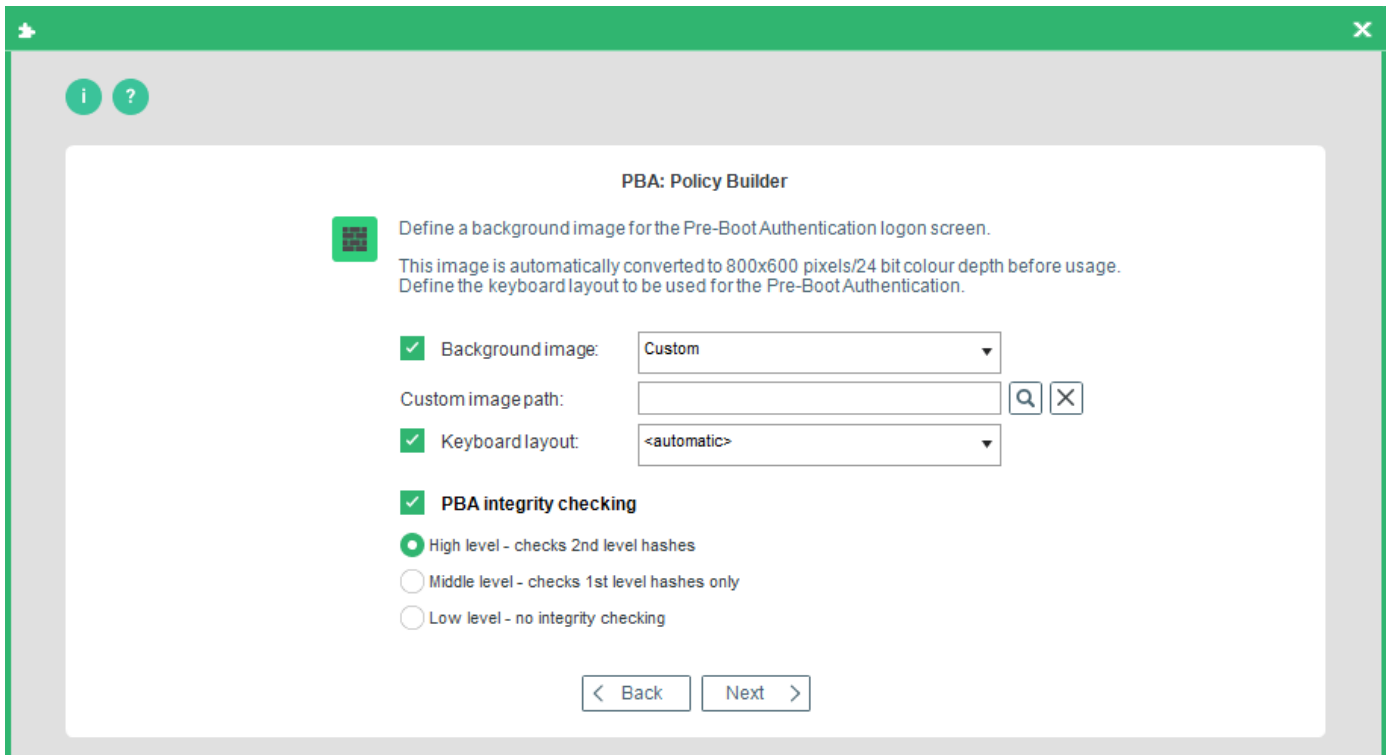
Use this dialog to determine, which pre-boot options will be available to the end user in the PBA component:

- **Disable login method change:** Check this option to disable switching between authentication methods in the PBA component.
- **Disable PBA advanced options:** Check this option to disable access to the PBA log options as well as the PBA advanced options.
- **Allow only numeric PIN entries:** This option allows only numeric smart card PIN entries.
- **Disable PIN change** (in HelpDesk): Check this option to prevent smart card users from changing their PIN during the PBA HelpDesk procedure.
- **Disable PIN reset** (in HelpDesk): Check this option to prevent smart card users from resetting their PIN during the PBA-HelpDesk procedure.
- **Select screen resolution:** change screen resolution if the default one doesn't fit.
- **"Without DRM" mode:** select this boot mode option if there are problems with graphic card and PBA loading.
- **Disable PBA:** temporarily deactivate PBA so that the computer can be rebooted without the need for authentication in the PBA. This can be permanent or configurable for 'n' reboots.
- **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](#).
- **Re-enable PBA after 'n' reboots:** Use this option to allow the user/admin to reboot the computer a specific number of times before the PBA is automatically re-enabled.
- **Power off PBA after 'n' seconds:** Set whether the PBA should turn the computer off if the PBA is left unattended for a configurable number of seconds.

For further information, refer to [EgoSecure FDE – Installation and Troubleshooting Guide](#).

24. Click **Next** to continue.

- The second **Pre-boot Options** dialog appear. This dialog allows you to customize the PBA background and keyboard layout.



Select one of the **Background image** options for the PBA logon dialog:

- **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 in the **Custom image path** field. The image is automatically resized to the correct resolution and color depth for the PBA screen: 800x600 pixels, 24-bit.

Take into account that the custom background image path must be accurate and valid. If you intend to use a specific background image to many target computers, then the image must either be located locally on each target computers, or on a network drive that uses local system access.

If you choose to copy the image to each target computer, then copy it per software distribution to the C:\WINDOWS\NAC\ directory. EgoSecure recommends copying the image to each target computer.

*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.

**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.

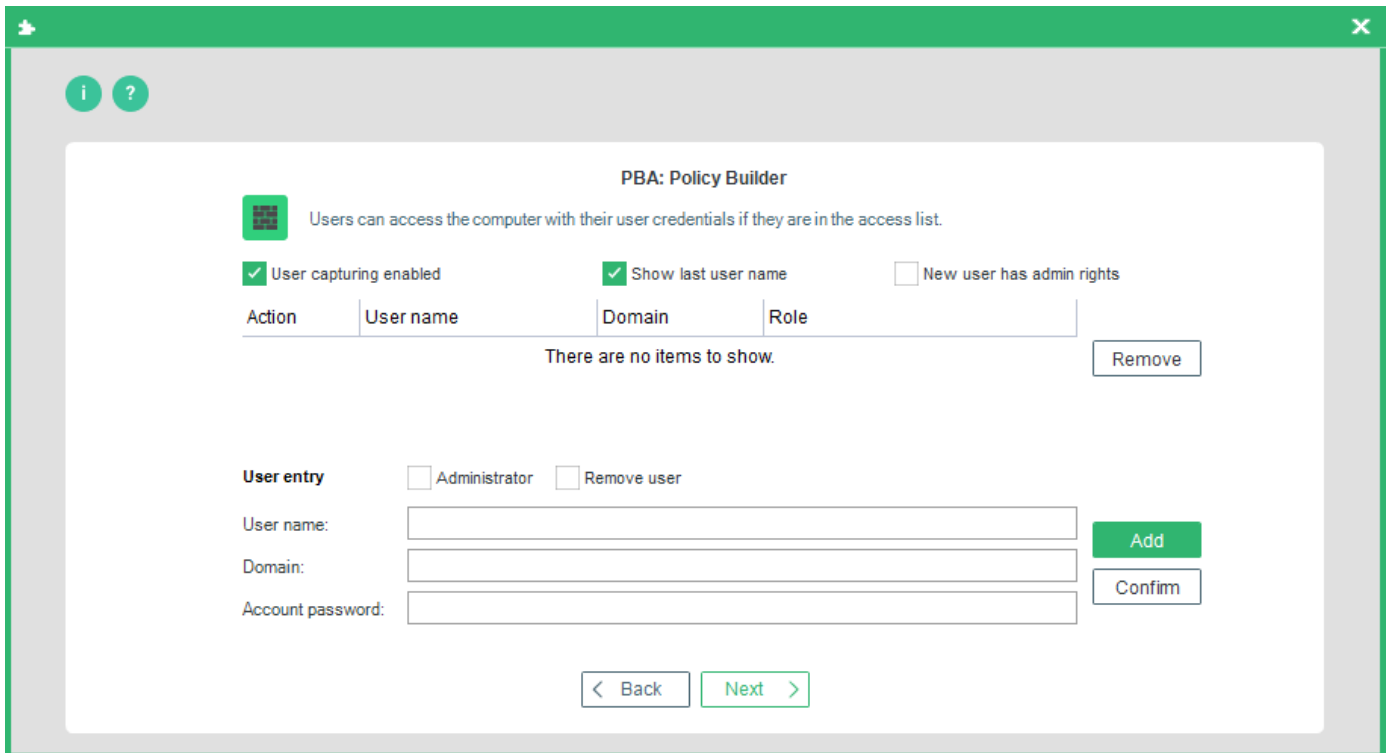
25. Press **Next** to continue.

- The **HelpDesk keys and Friendly Network** dialog appears. This dialog allows you to configure the HelpDesk keys for use in an emergency. Once the HelpDesk is configured, you can activate Friendly Network. For further information, refer to [EgoSecure FDE – Installation and Troubleshooting Guide](#).

The screenshot shows a Windows-style dialog box titled "PBA: Policy Builder". At the top left, there are two circular icons: one with an 'i' and one with a question mark. The main content area has a green icon on the left and text on the right: "The HelpDesk key is needed for the challenge-response scenario with the HelpDesk. Friendly Network is used to simplify the authentication if the network is known." Below this, there is a checkbox labeled "Activate self-initialization via helpdesk" followed by a dropdown menu currently set to "Strong". There are two buttons: a green "Insert HelpDesk key" and a grey "Delete HelpDesk key". Below these is another checkbox labeled "Activate Friendly Network". Underneath, there are input fields for "IP:" and "Port:", with an "Add" button below them. To the right of these fields is a table with two columns, "IP" and "Port", and a single row containing the text "There are no items to show." and a "Remove" button. At the bottom of the dialog, there are two buttons: "< Back" and "Next >".

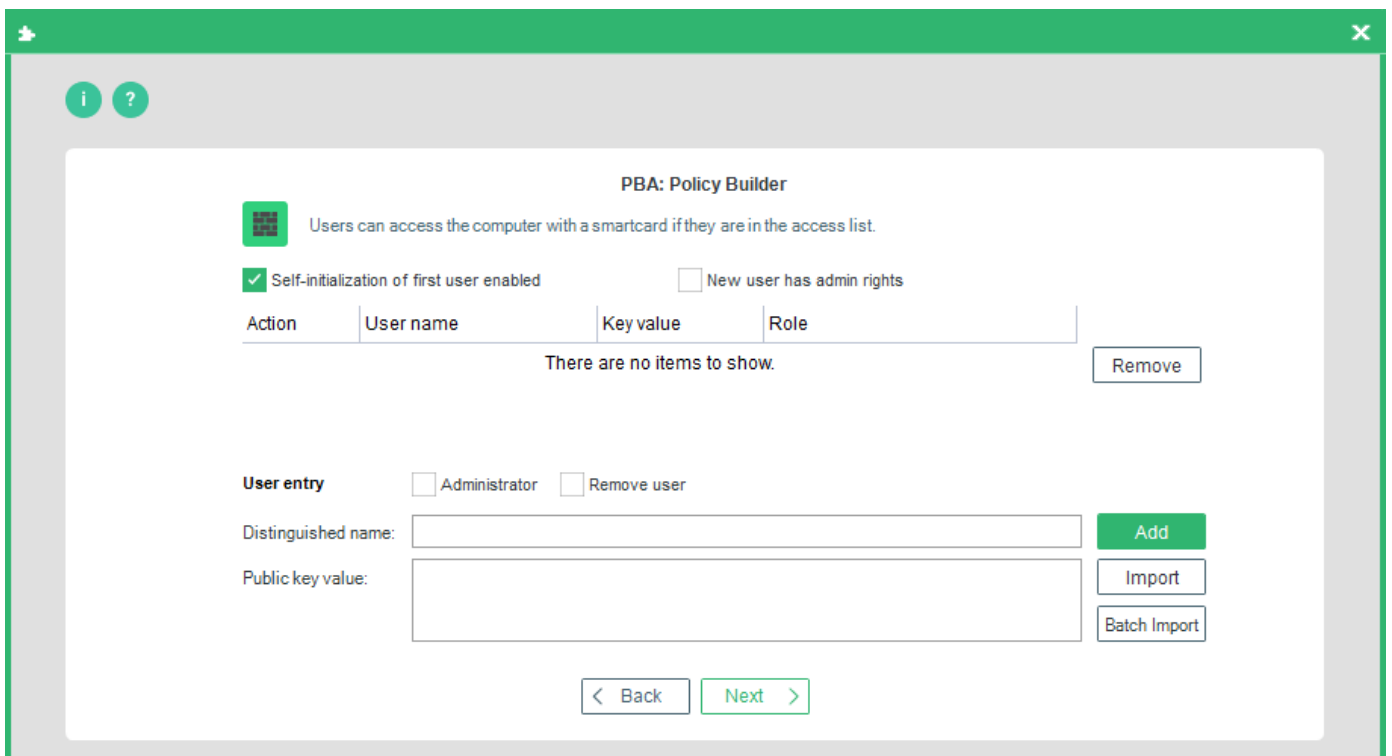
26. Click **Next** to continue.

- The **Windows credentials** user dialog appears. This dialog helps you to define the users to be authenticated to the system via their Windows user account details. For further information, refer to [EgoSecure FDE – Installation and Troubleshooting Guide](#).



27. Click **Next** to continue.

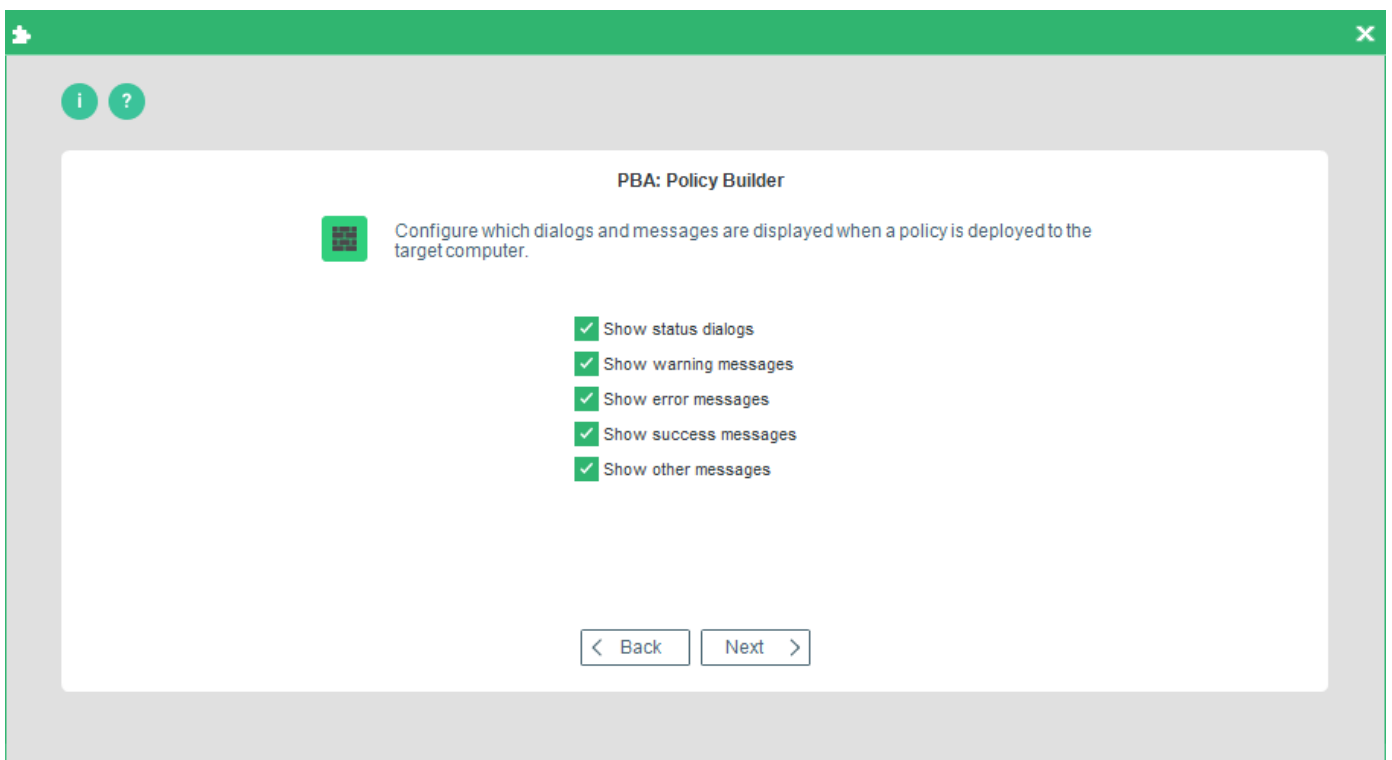
→ The **Smart card** user dialog appears. This dialog helps you to define the users to be authenticated to the system via their smart card details. For further information, refer to the [EgoSecure FDE – Installation and Troubleshooting Guide](#).



28. Click **Next** to continue.

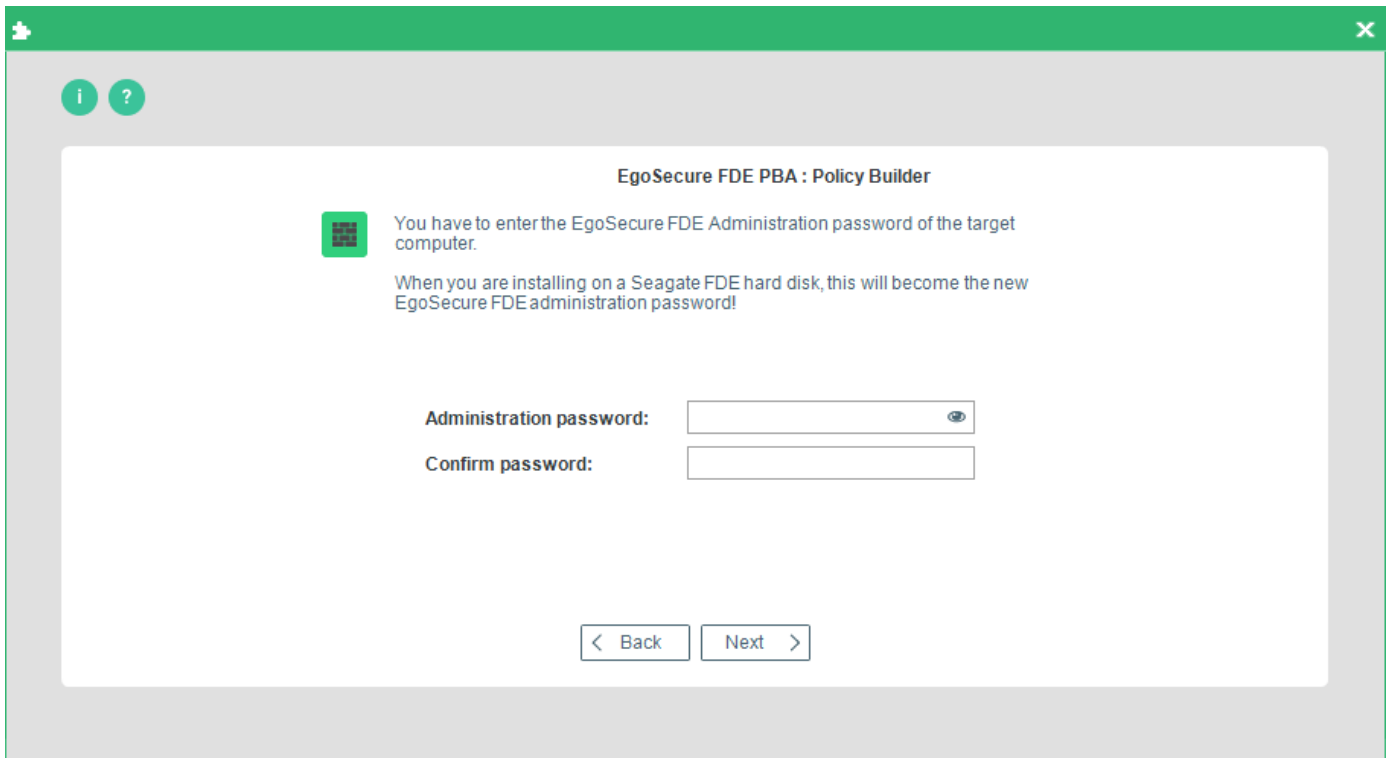
→ The **Messages options** dialog appears. The messages below are shown only on computers with Windows versions below Windows 10.

Option	This option determines if...
Show status dialogs	... status dialogs should be displayed on the target computer during policy deployment.
Show warning messages	... warning messages should be displayed on the target computer during policy deployment. If you do not select this option, warning messages are suppressed.
Show error messages	... error messages should be displayed on the target computer during policy deployment. If you do not select this option, error messages are suppressed.
Show success messages	... success messages should be displayed on the target computer that relate to individual policy tasks during deployment.
Show other messages	... information messages should be displayed on the target computer during and after policy deployment. If you do not select this option, information messages are suppressed.



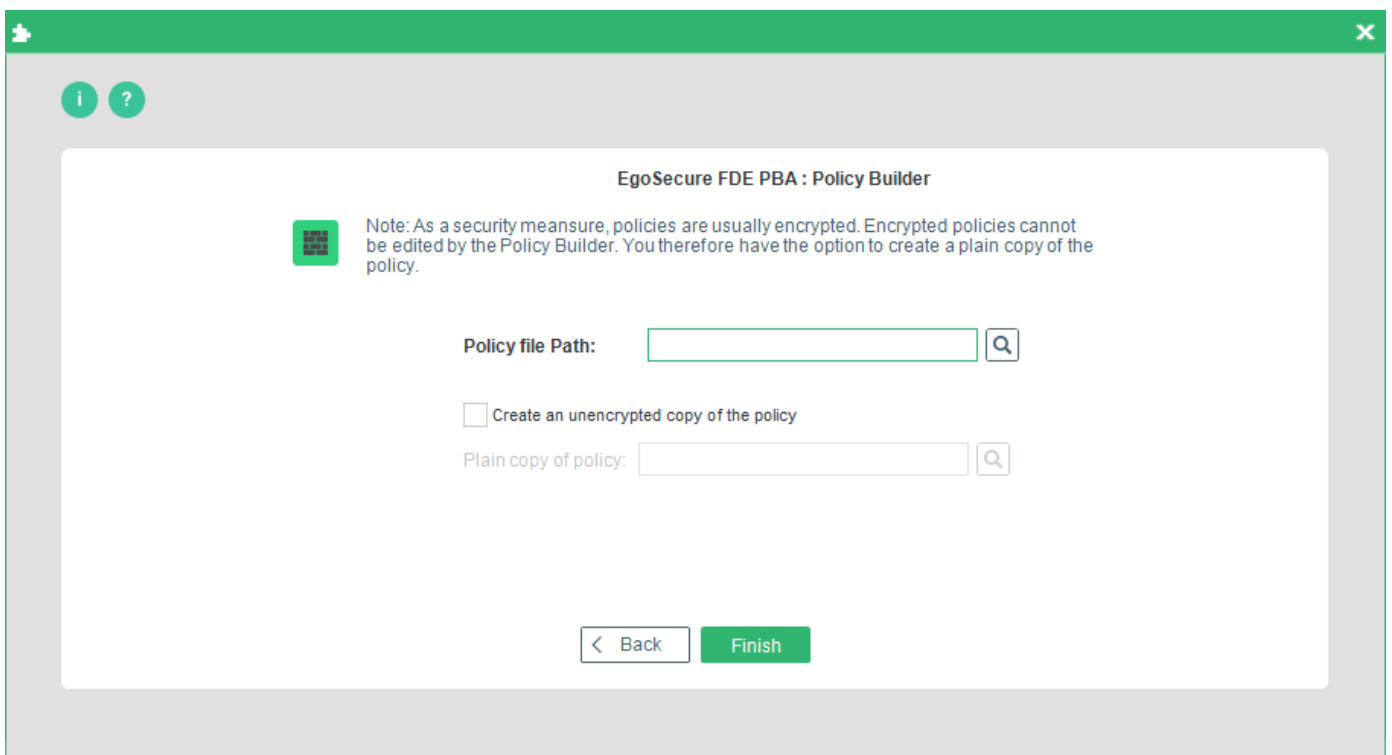
29. Make option selection and click **Next**.

→ The Administration password options dialog appears.



30. Enter and confirm the administration password to be used on the target computer. Click **Next** to continue.

→ The **Policy location** dialog appears:





Option	Details
Policy file Path	Enter the path for the policy in this field by clicking `...` and selecting a location and filename for the file in the file browser.
Create an unencrypted copy of the policy	Check this option to create an unencrypted copy of the policy (recommended for reconfiguration). If you want to reconfigure a computer that has already been configured using a policy, then check this option - the Policy Builder can only open an unencrypted policy to edit the settings.
Plain copy of policy	Enter the path for the plain copy of the policy in this field by clicking `...` and selecting a location and filename for the file in the file browser.

- If you want to use your configuration policy for remote deployment, then name the encrypted file Autoconf.PBA (the policy will not be recognized by the target computer as a deployment policy if it has any other name).
- Use the plain copies to create new policies for future changes in configuration.

31. Enter the path for your policy and click **Finish** to complete the procedure.

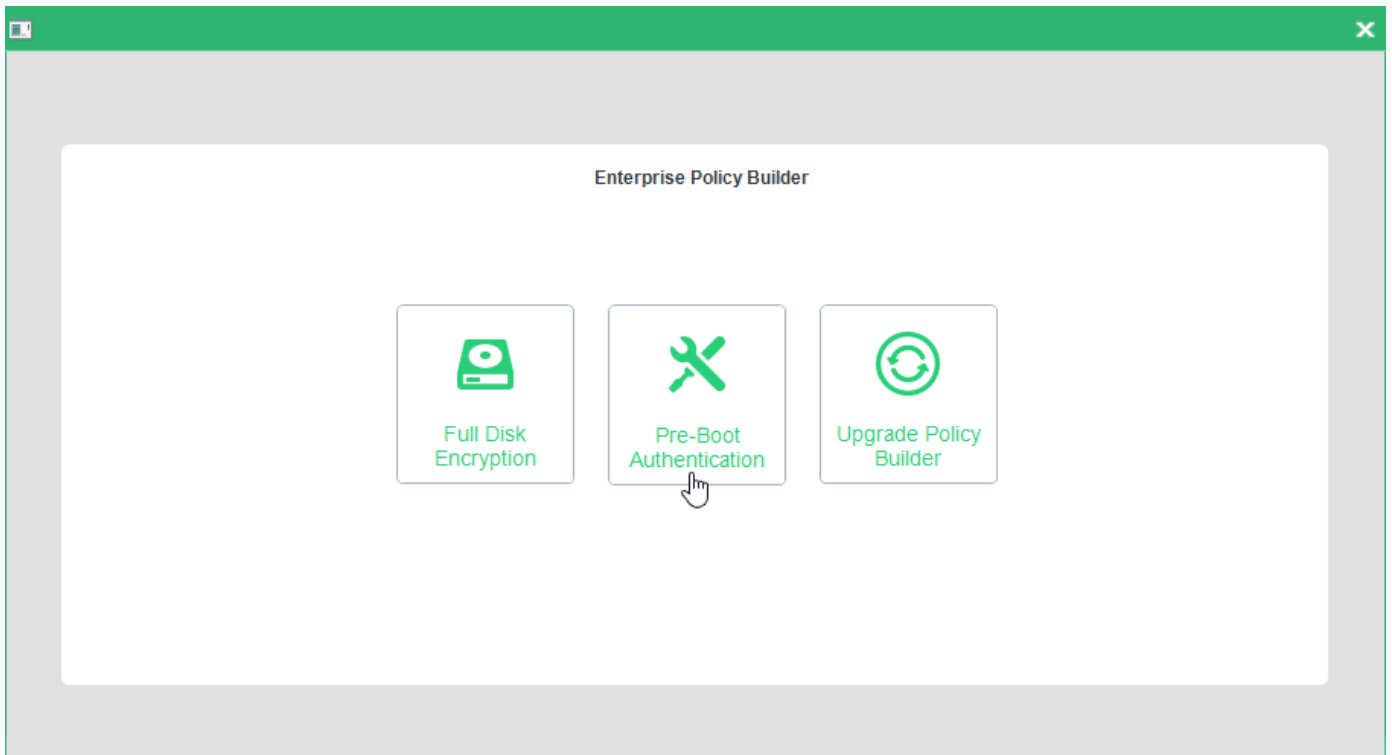
! For security reasons, encrypted policies cannot be edited with the FDE Policy Builder.

## Creating a de-initialization policy

This section details how to create a de-initialization policy for the PBA component only. You need to have knowledge about the target computer for deployment. Details such as number of partitions, drive letters, is it already encrypted etc... are necessary for the successful deployment of EgoSecure Full Disk Encryption. Once the policy is created, deploy it, for details see [Deploying PBA policies](#).

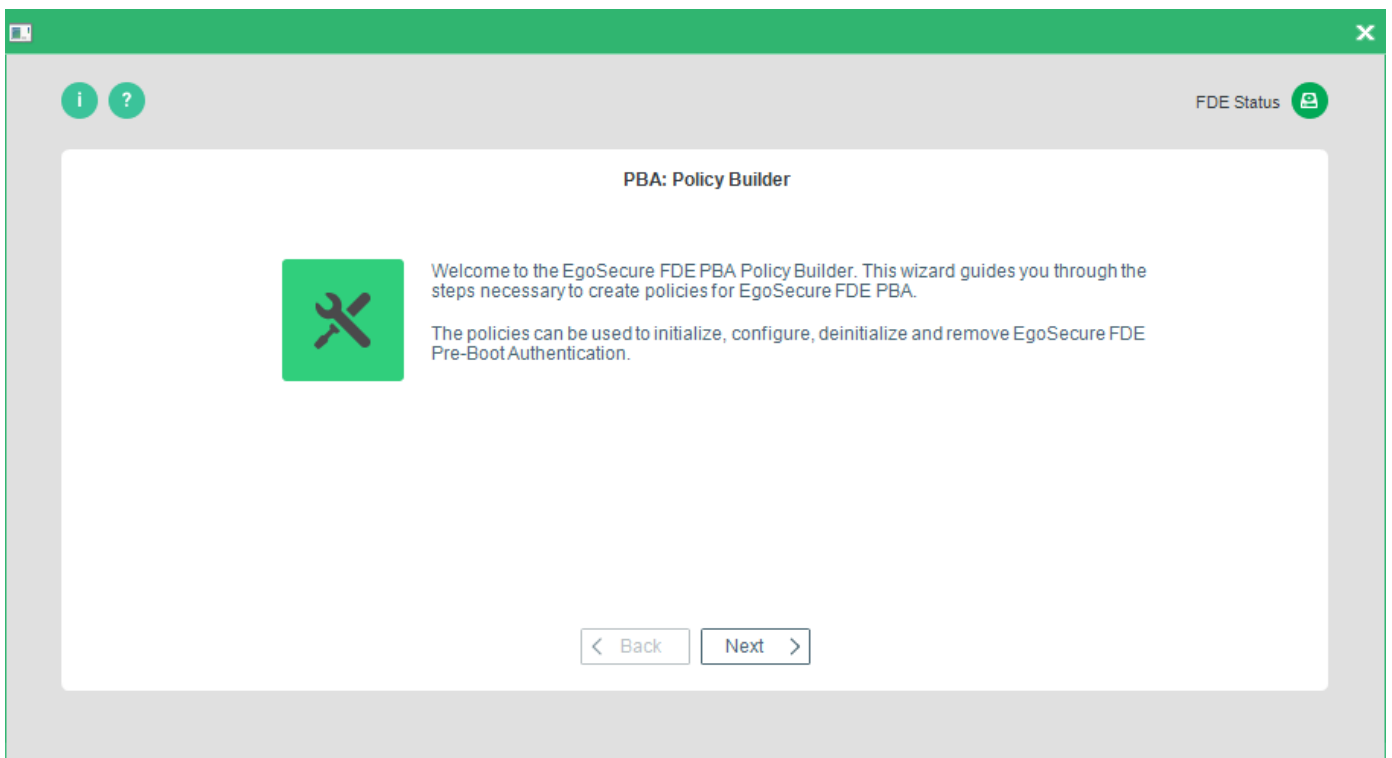
Follow the step below to create a new policy in PBA Policy Builder:

1. Open the Control Center (as described in section 1.5).
2. Double-click the Policy Builder icon.
3. Select **Pre-Boot Authentication** policy builder.



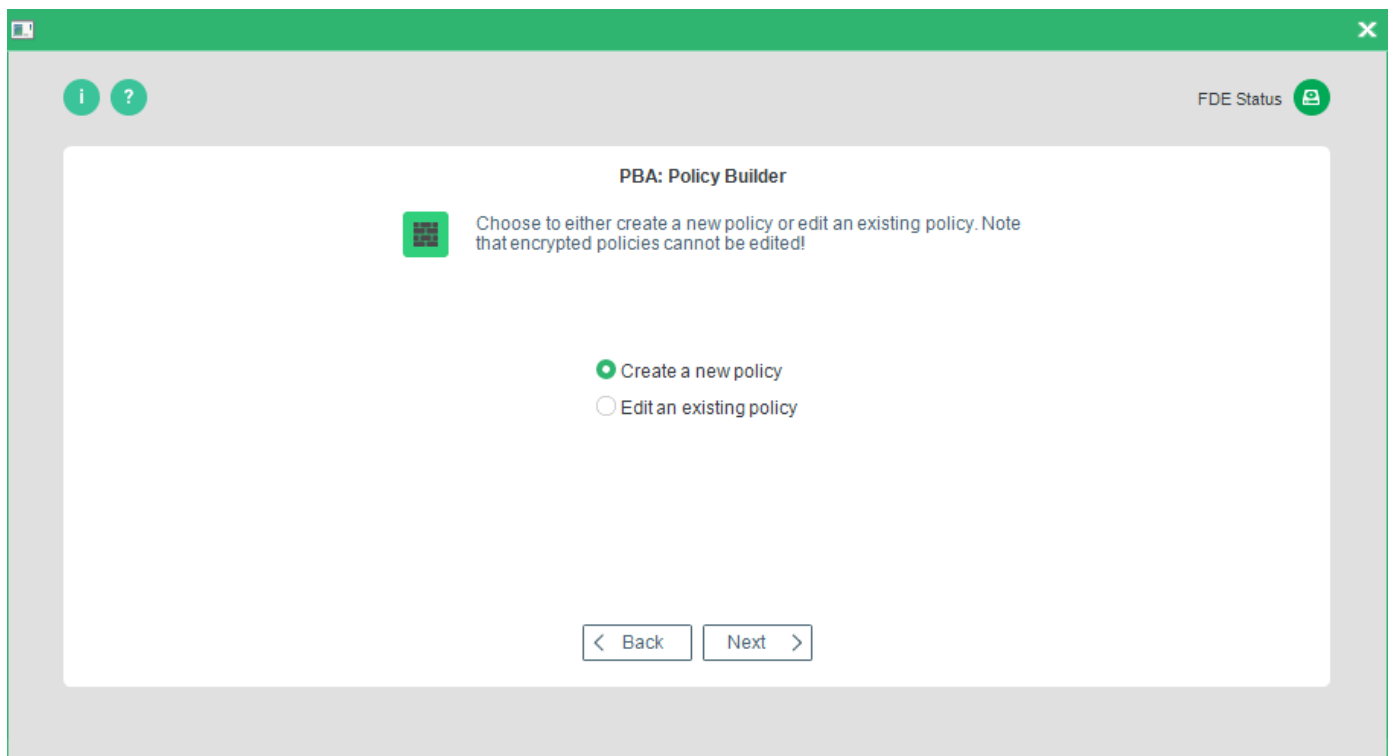
→ The PBA Policy Builder Welcome dialog appears.

4. Click **Next** to continue.



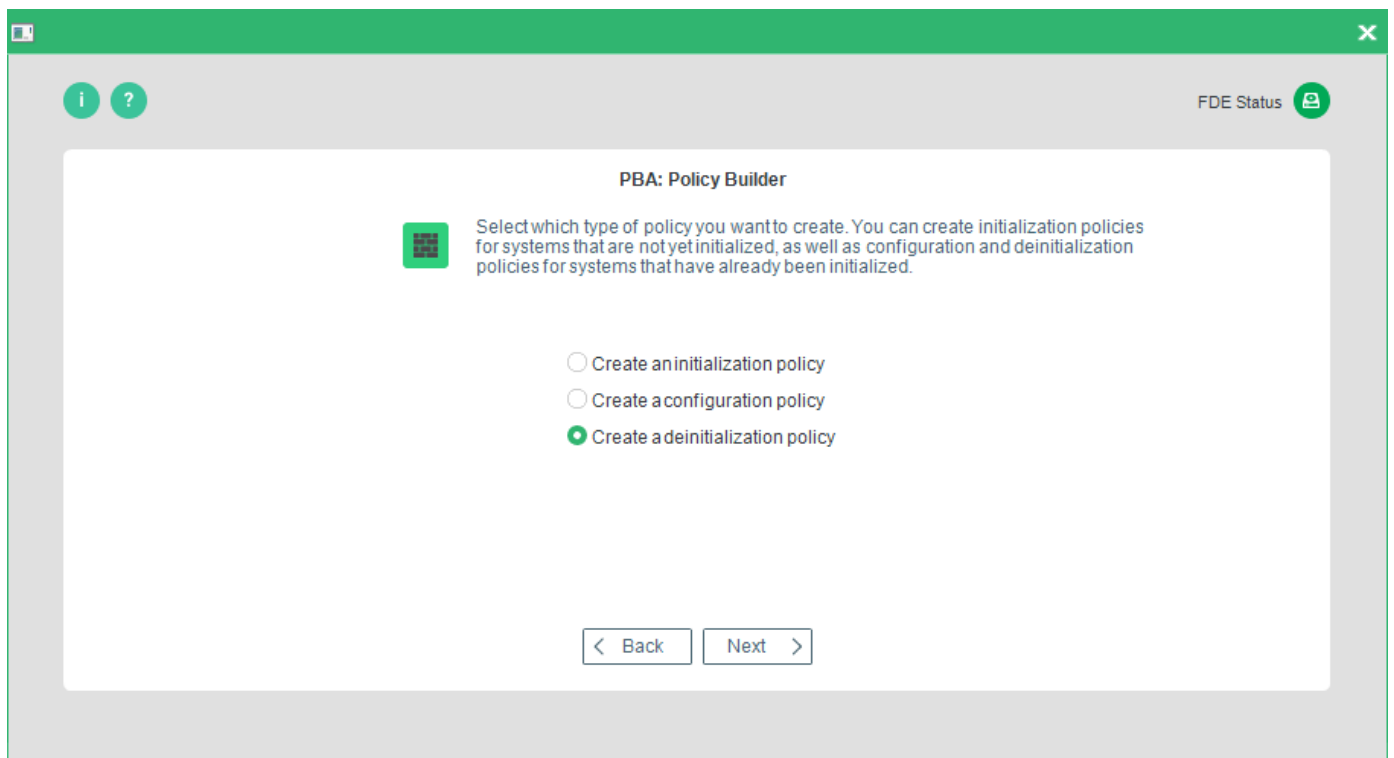
→ The **Policy selection** dialog appears.

5. Select the **Create a new policy** radio button. Click **Next** to continue.

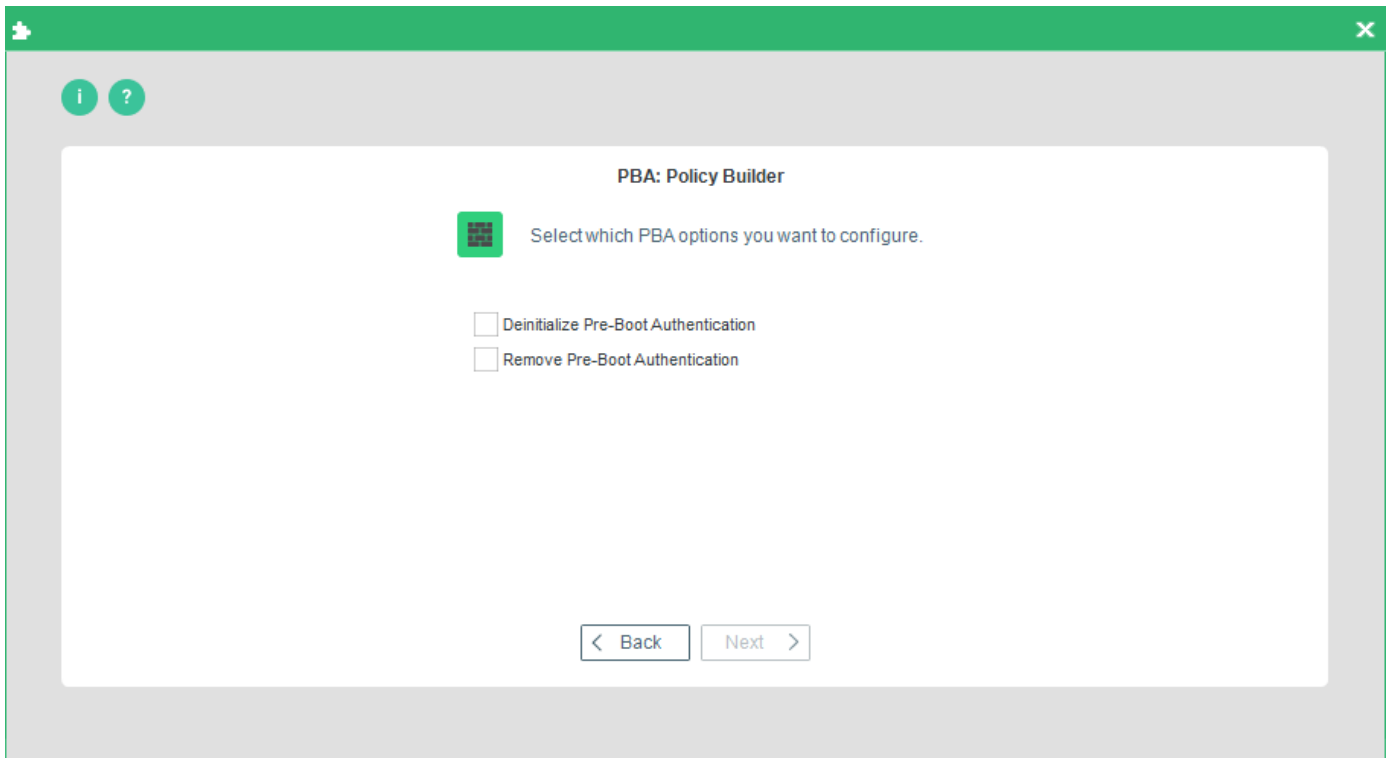


→ The **Policy type** dialog appears.

6. Select **Create a deinitialization policy**. Click **Next** to continue.



→ The Deinitialization Options dialog appears.

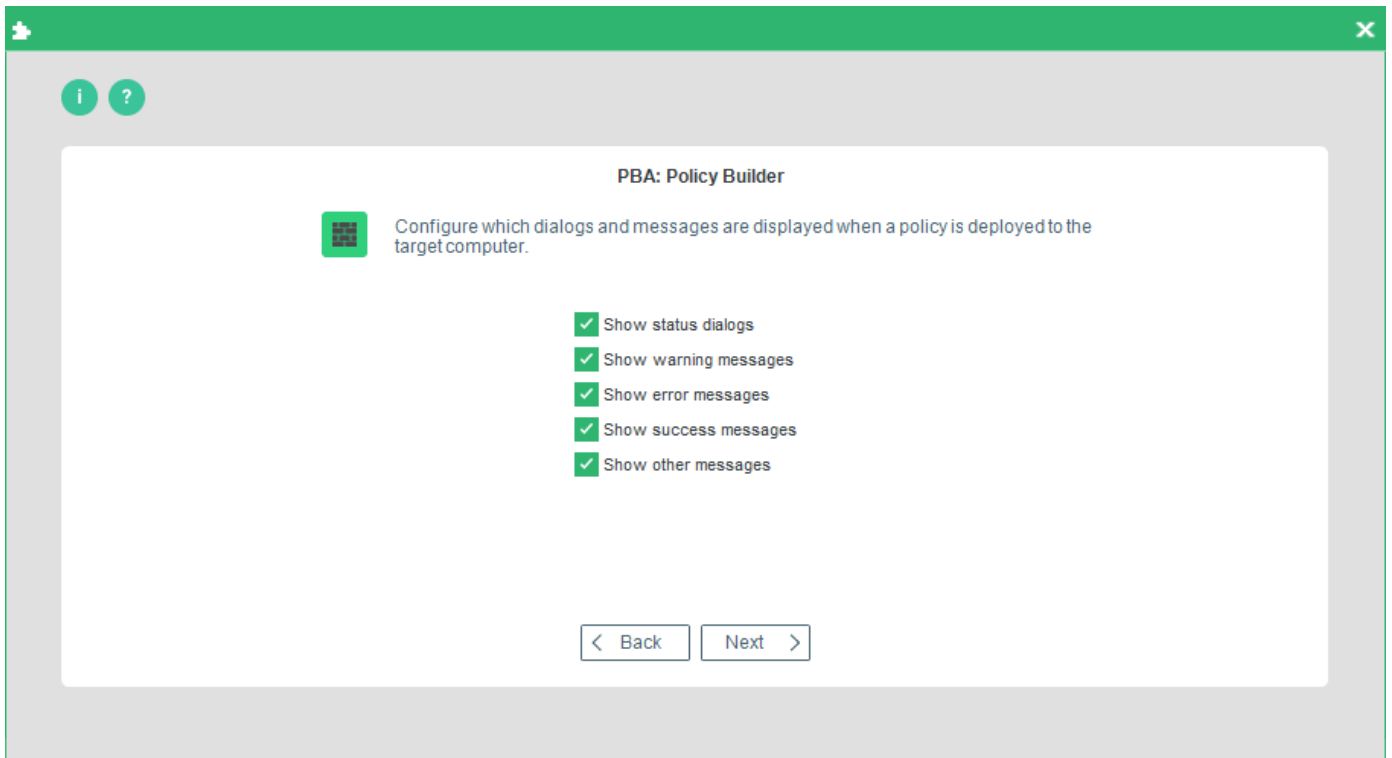


This dialog allows you to define the following options:

Option	Details
Deinitialize Pre-Boot Authentication	Deactivate <i>EgoSecure Full Disk Encryption</i> PBA only. <i>EgoSecure Full Disk Encryption</i> can be re-activated remotely via a second policy, or manually via the Control Center.
Remove Pre-Boot Authentication	Remove <i>EgoSecure Full Disk Encryption</i> PBA completely.

7. Once you have made you selection click **Next**.

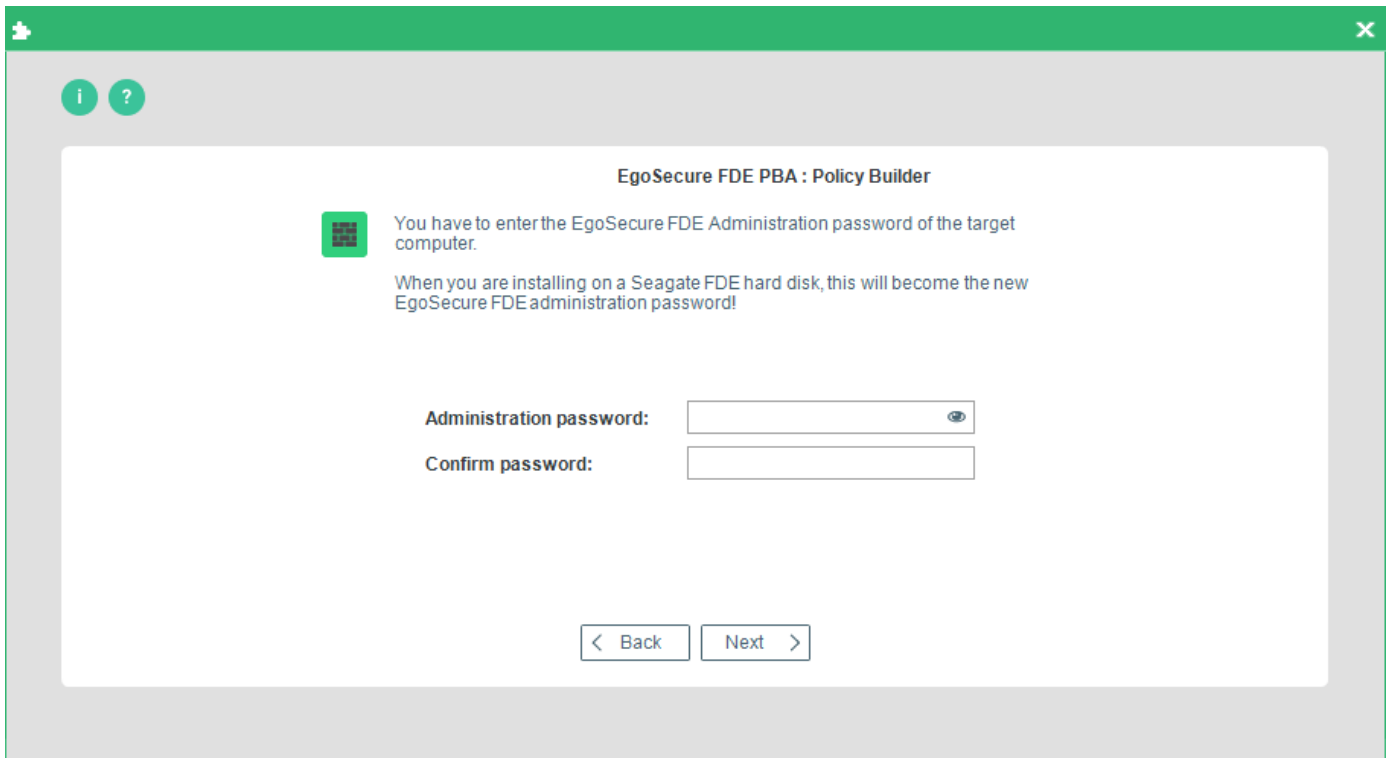
- The **Message** options dialog appears. The messages below are shown only on computers with Windows versions below Windows 10.



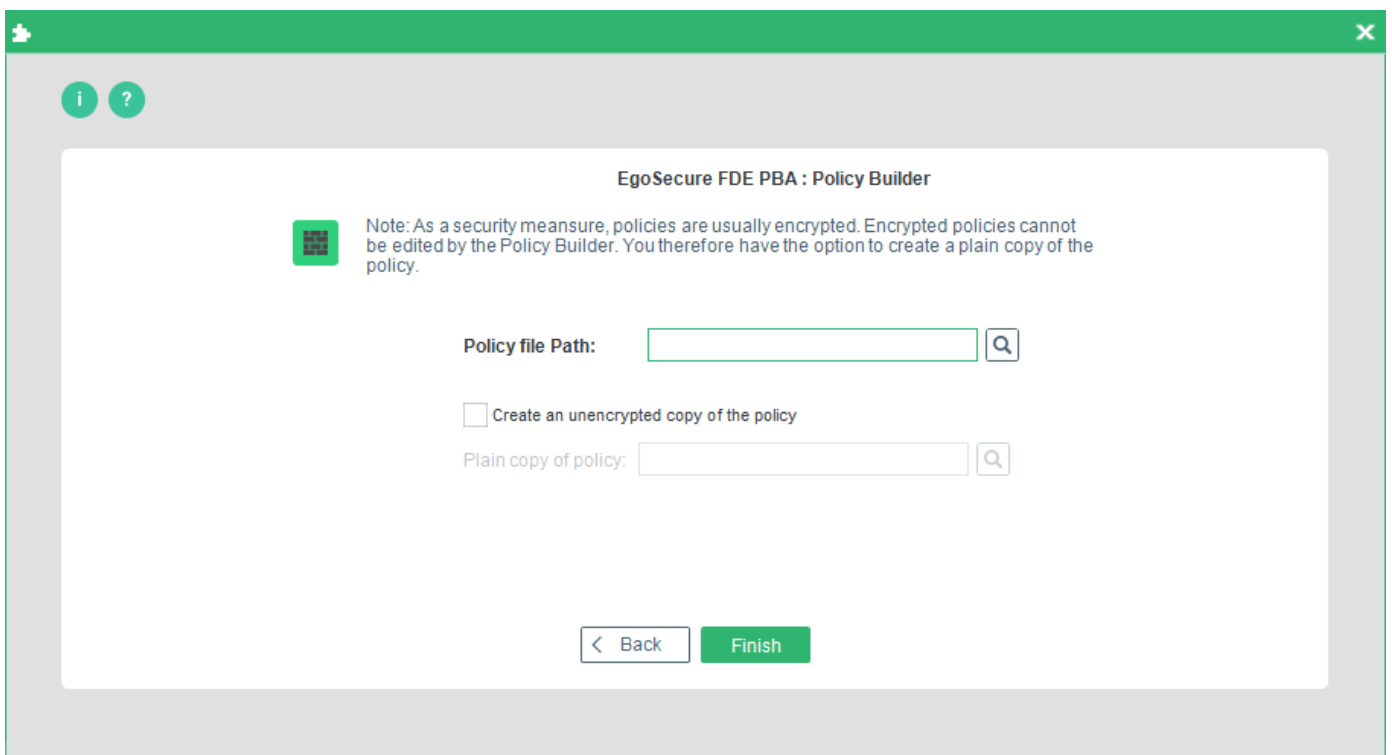
Option	This option determines whether...
Show status dialogs	... status dialogs should be displayed on the target computer during policy deployment.
Show warning messages	... warning messages should be displayed on the target computer during policy deployment. If you do not select this option, warning messages are suppressed.
Show error messages	... error messages should be displayed on the target computer during policy deployment. If you do not select this option, error messages are suppressed.
Show success messages	... success messages should be displayed on the target computer that relate to individual policy tasks during deployment.
Show other messages	... information messages should be displayed on the target computer during and after policy deployment. If you do not select this option, information messages are suppressed.

8. Make your selection and click **Next** to continue.

→ The **Administration password** (target computer) dialog appears:



9. Enter and confirm the EgoSecure Full Disk Encryption administration password, which you already set on the target computer. Click **Next** to continue.  
→ The **policy location** dialog appears.




Option	Details
Policy file Path	Enter the path for the policy in this field by clicking `...` and selecting a location and filename for the file in the file browser.
Create an unencrypted copy of the policy	Check this option to create an unencrypted copy of the policy (recommended for reconfiguration). If you want to reconfigure a computer that has already been configured using a policy, then check this option - the Policy Builder can only open an unencrypted policy to edit the settings.
Plain copy of policy	Enter the path for the plain copy of the policy in this field by clicking `...` and selecting a location and filename for the file in the file browser.

10. Enter the paths for your policy, and click **Finish** to complete the procedure.

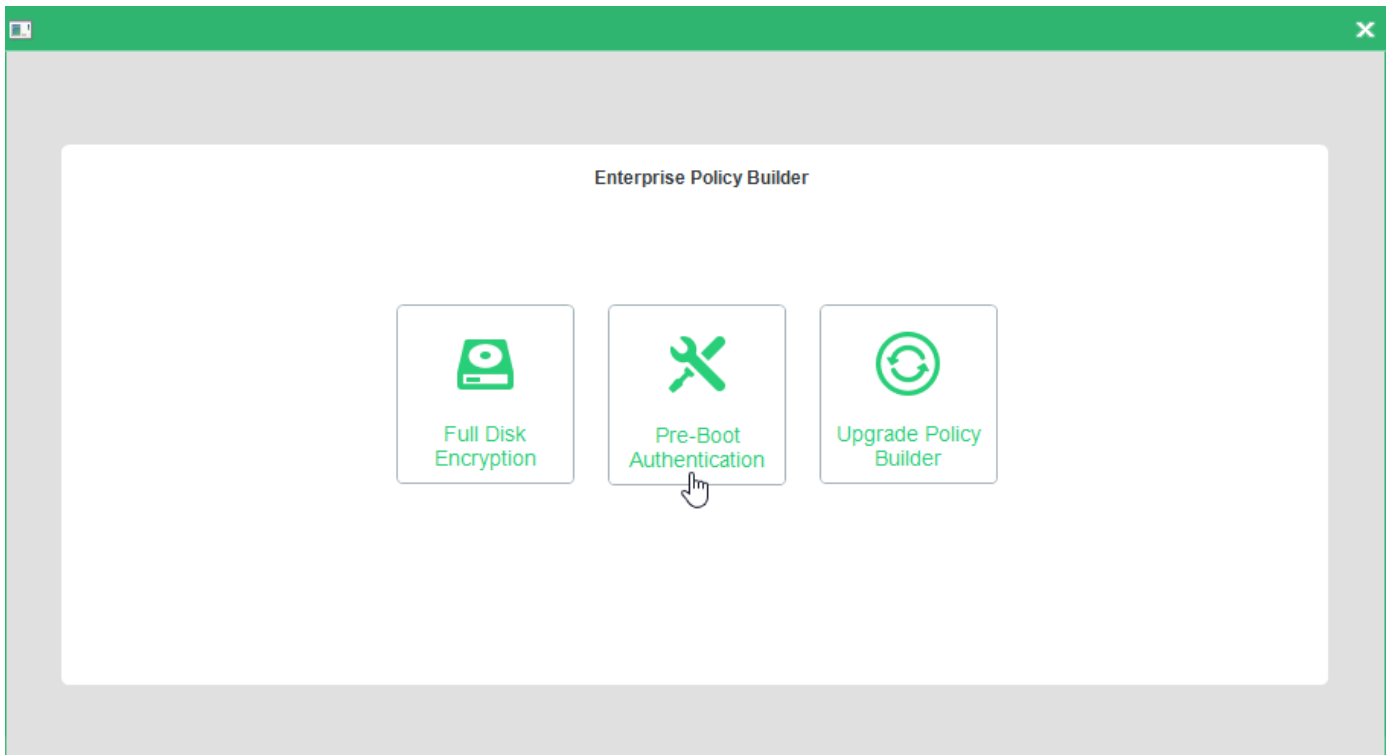
## Editing an existing PBA policy

Policy Builder offers an editing function when you need to change or tweak a policy.

	<p><b>Selecting policies for editing in Policy Builder</b></p> <p>Only plain (unencrypted) policies can be selected to be edited in Policy Builder.</p> <p><b>ATTENTION</b> For details about saving an unencrypted copy of a policy during the policy creation process, see <a href="#">Creating an initialization or configuration policy</a>, step <a href="#">30</a>.</p>
---	---

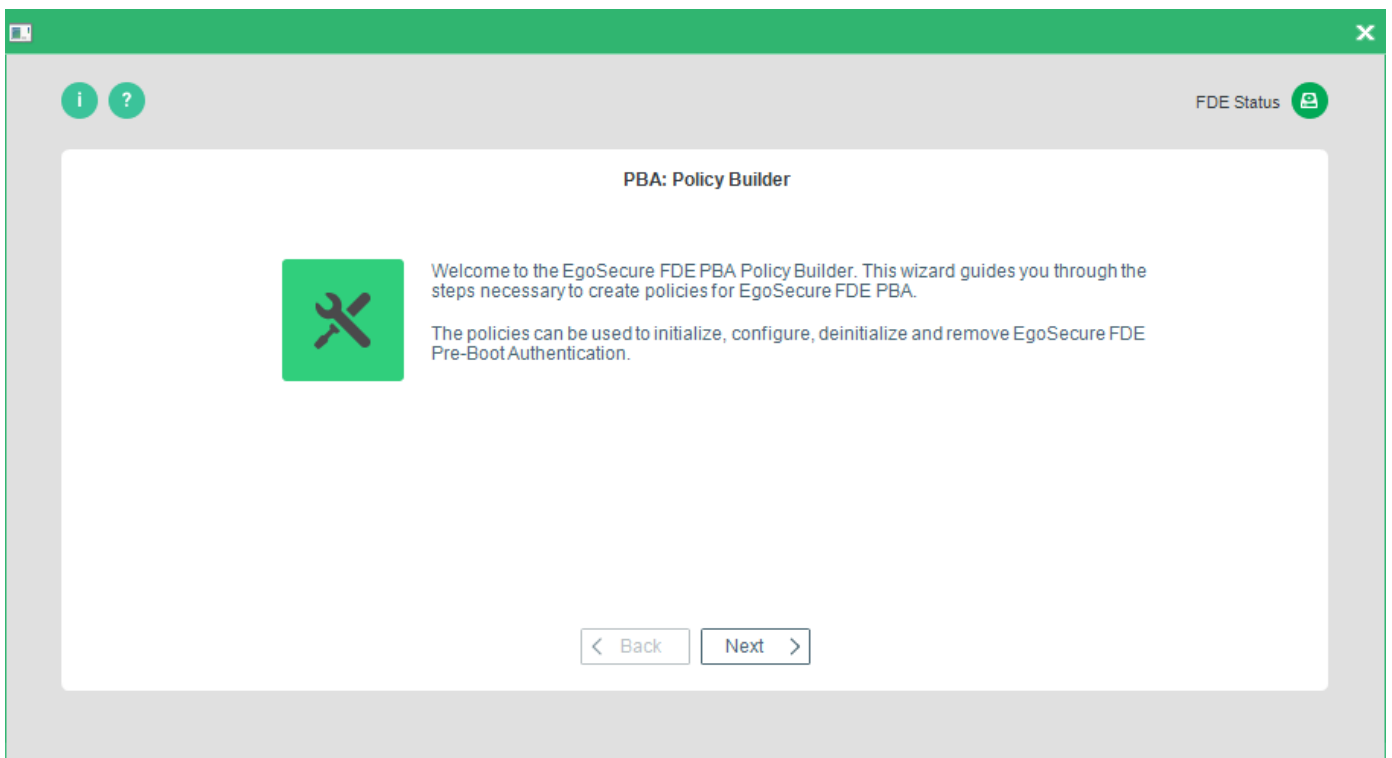
Follow the steps below to edit a policy:

1. Open the **Control Center** (as described in section [1.5](#)).
2. Double-click the Policy Builder icon.
3. Click Pre-Boot Authentication policy builder.



→ The PBA Policy Builder Welcome dialog appears.

4. Click **Next** to continue.

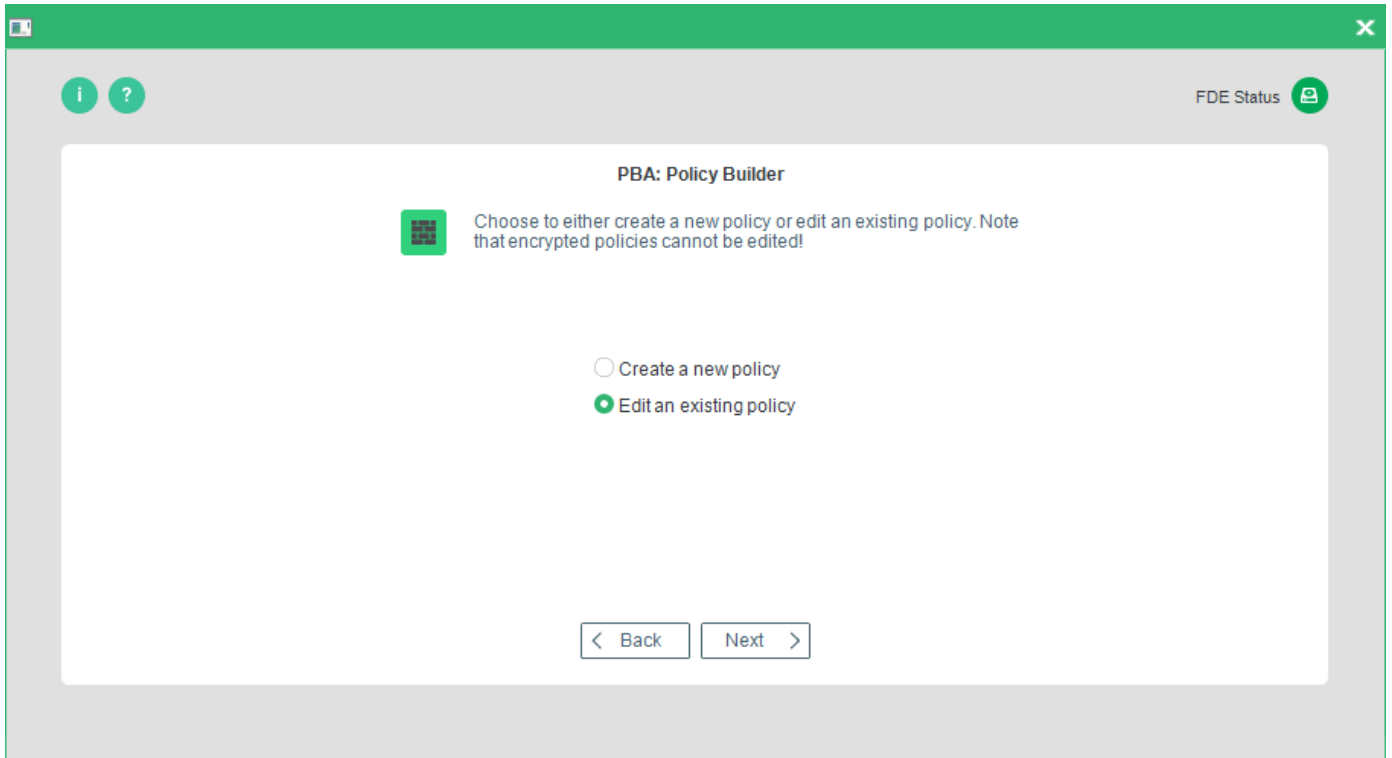


→ The **Policy selection** dialog appears.

5. Select the **Edit an existing policy** radio button.



6. Click **Next**, and select the created policy from the file browser.



According to the type of policy you have selected the editing process is the same as the policy creation process:

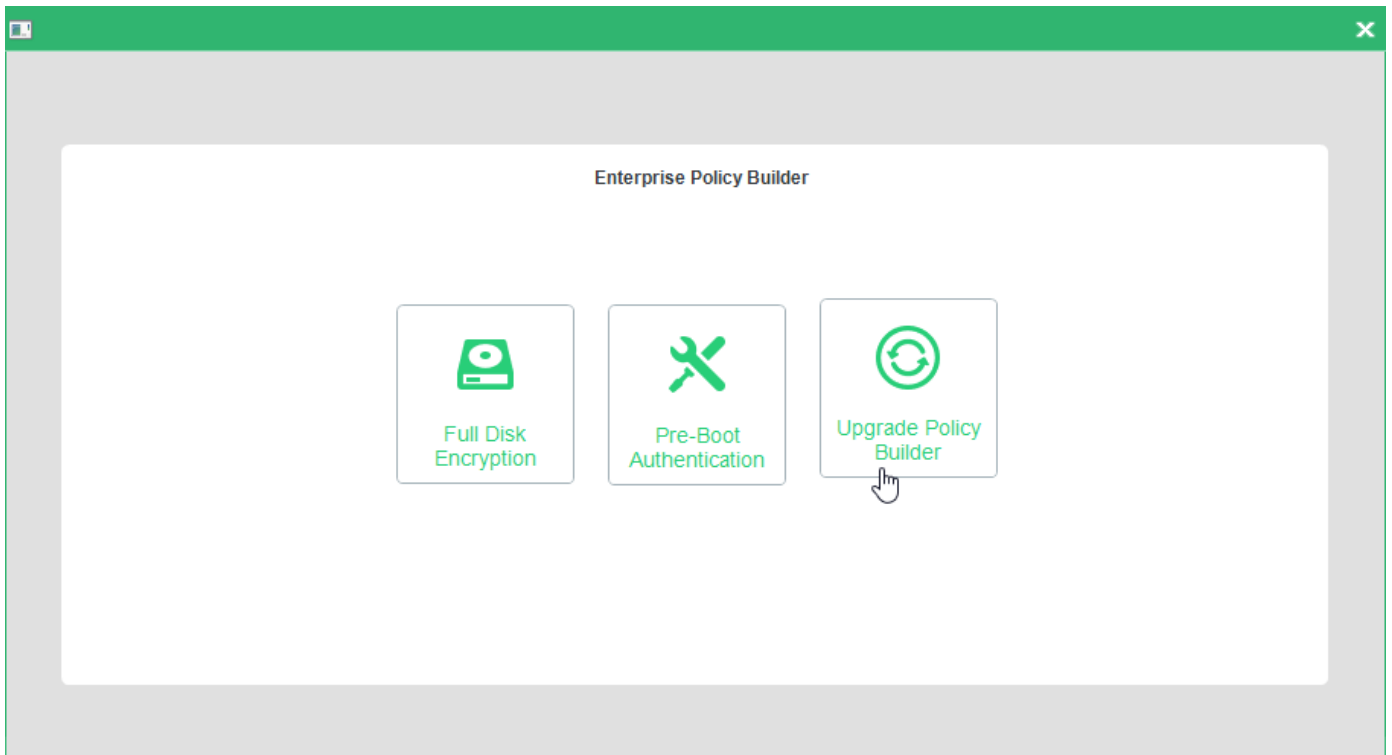
Option	Details
Initialization policy	Step <a href="#">0</a> .
Configuration policy	Step <a href="#">0</a> .
De-initialization policy	Step <a href="#">6</a> .

## 2.3. Creating an upgrade policy

The **Upgrade policy builder** allows you to create an upgrade policy to prevent the EgoSecure FDE administration password from being entered in the commandline in plain text for the purpose of silently upgrading or removing EgoSecure Full Disk Encryption. Information about the commandline version of this module can be found in section 5.2 "[GUS](#)".

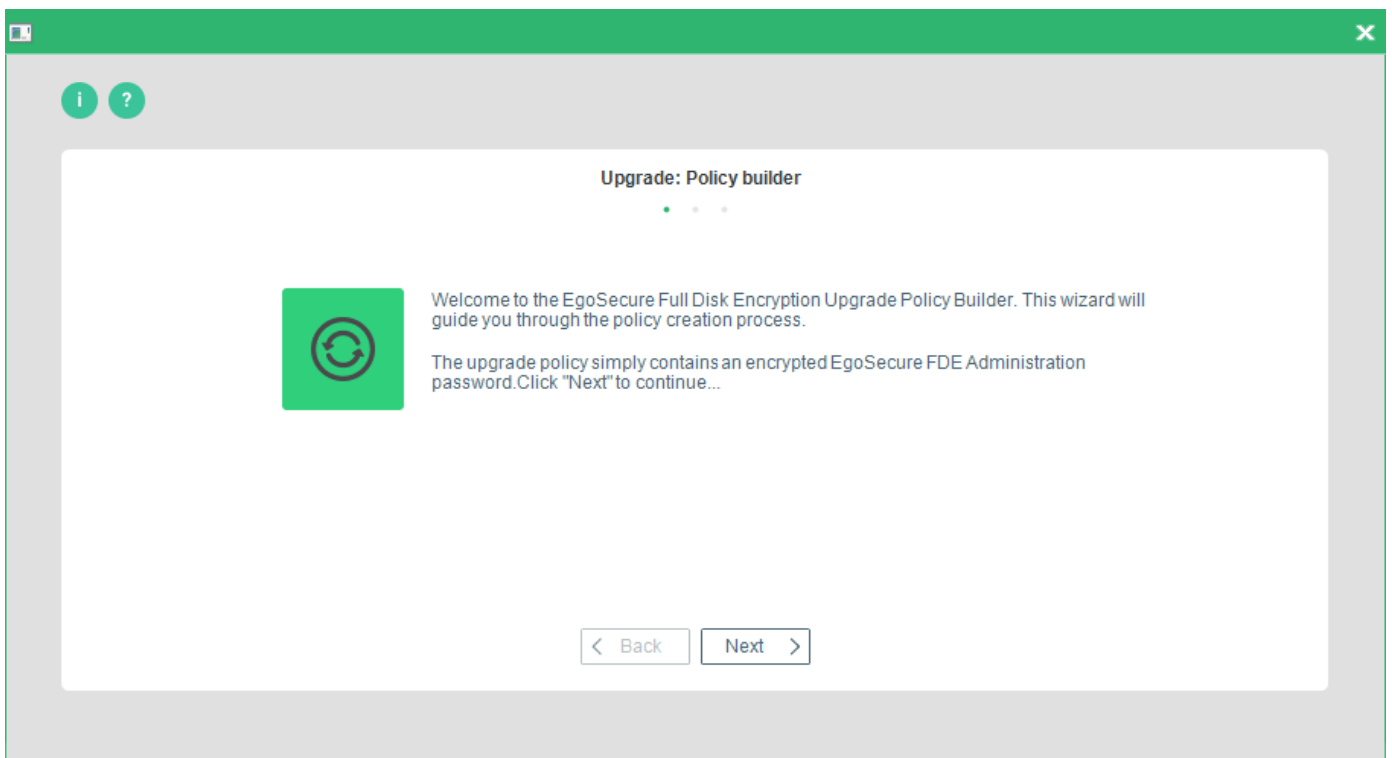
Follow the steps below to create an upgrade policy:

1. Open the **Control Center** (as described in section [1.5](#)).
2. Double-click the Policy Builder icon.
3. Select Upgrade policy builder.



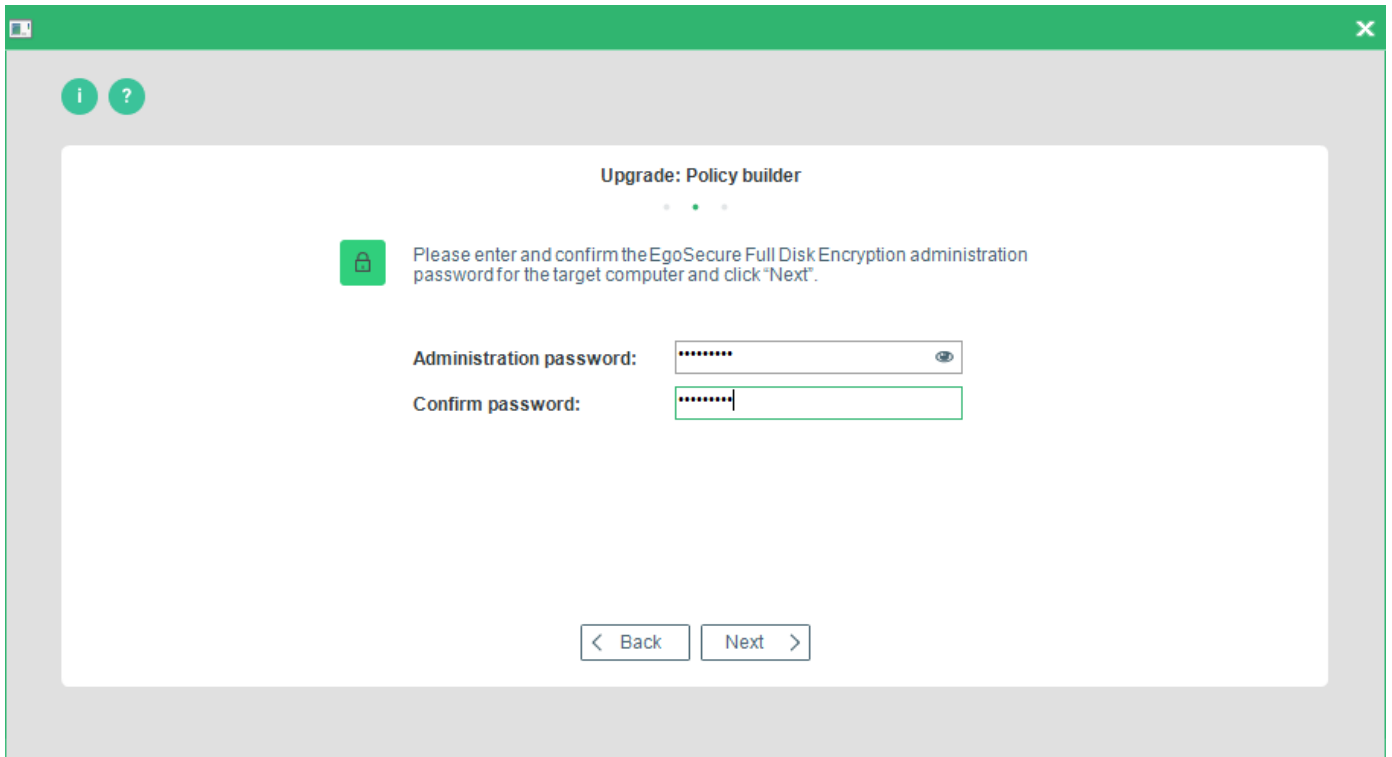
→ The Upgrade Policy Builder Welcome dialog appears.

4. Click **Next** to continue.



→ The Administration password dialog appears.

5. Enter and confirm the administration password you intend to use for the target machine(s) and click **Next**.



Upgrade: Policy builder

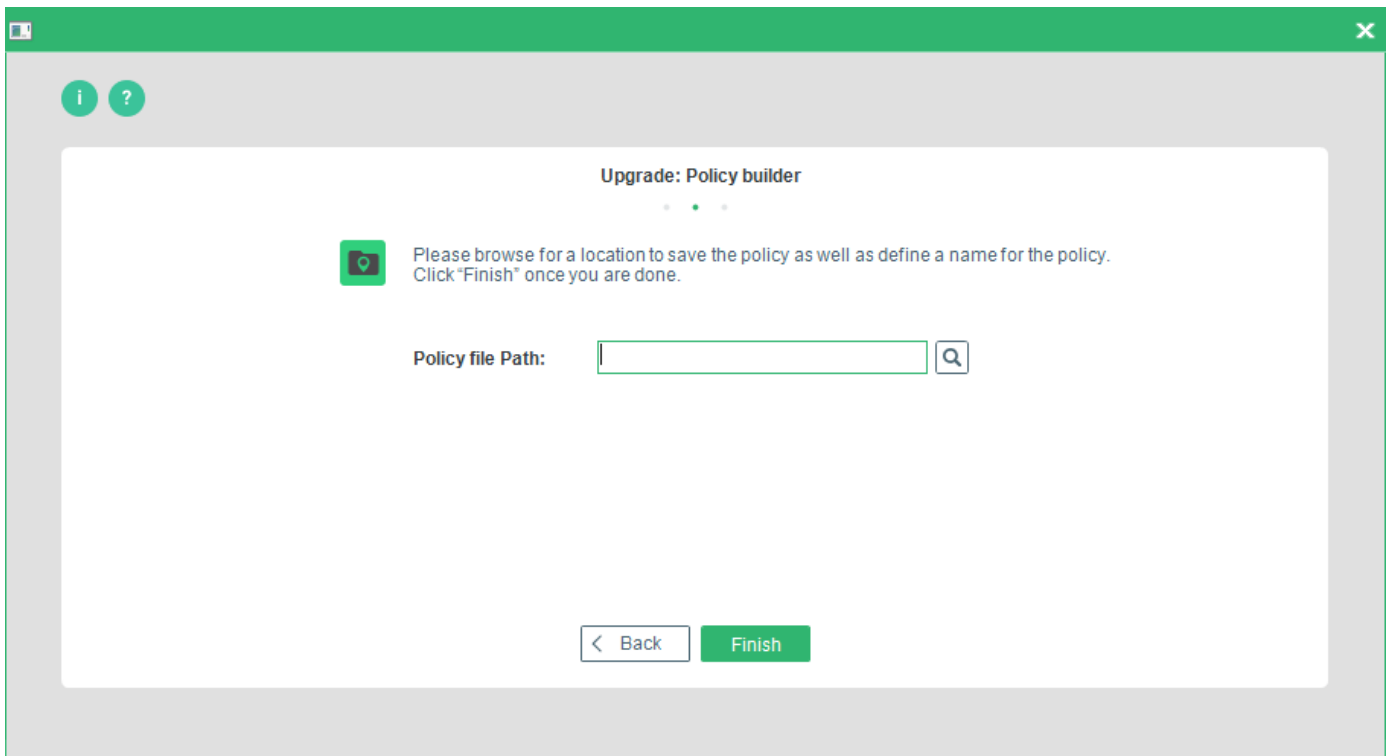
Please enter and confirm the EgoSecure Full Disk Encryption administration password for the target computer and click "Next".

Administration password:

Confirm password:

< Back    Next >

→ The **Policy Path** dialog appears.



Upgrade: Policy builder

Please browse for a location to save the policy as well as define a name for the policy. Click "Finish" once you are done.

Policy file Path:

< Back    Finish

6. Click '...' to open a file browser and select a directory to save the policy as well as a name for the policy. Click **Finish** to complete the process.

## 3. TRUSTED PLATFORM MODULE (OBSOLETE)



### ATTENTION

#### TPM without PBA

TPM support is currently limited to the FDE component only. This means that that if you want to use this feature you cannot install the PBA. Doing so will result in a fatal error (blue screen).

TPM support can only be used if the computer vendor fully supports on-board TPM chips in the BIOS. Please check this before proceeding with any installation.

### Introduction

*EgoSecure* security can be taken to a new level via the use of a TPM chip found on most business-oriented computers. *EgoSecure Full Disk Encryption* offers the following advantages when using the TPM chip:

- The hard disk Key Encryption Key (KEK) is encrypted through the TPM using an RSA key. This means that the hard disk cannot be removed and placed in another computer because the encryption used for the KEK is unique to the original TPM chip.
- 'Disk Roaming' can be achieved in an emergency scenario via the BartPE plug-in by temporarily deactivating the TPM. As an alternative you can add TPM key files from other computers to *EgoSecure Full Disk Encryption* so that a hard disk can be easily transported and used on a backup computer.

### Contents

- Overview
- TPM installation
- Removal
- TPM usage
- TPM utilities
- Boot Code Errors
- Creating policy for TPM (Full Disk Encryption Policy Builder)

## 3.1. Overview

### Introduction

TPM support in *EgoSecure Full Disk Encryption* is based on encrypting the KEK using a unique TPM-based RSA key. With this key we encrypt the *TPM secret*. Both the RSA key and the encrypted *TPM secret* are stored in the *EgoSecure* partition – not in the TPM itself. The *TPM secret* protects the KEK wherever it is stored in the partition.

The TPM functionality can be tested during the TPM activation under *Windows*, but this test does not ensure that TPM access also functions correctly in the boot code or the PBA. To

ensure that *EgoSecure* is robust, the activation under *Windows* only activates a self-initialization mode in which the KEK has yet to be encrypted and the real KEK-TPM protection is performed in the next boot process - after the TPM functions have been successfully called.

## Requirements

For successful TPM operation, several requirements must be met before trying to enable TPM support in *EgoSecure Full Disk Encryption*:

- The TPM must be turned on and activated in the computer BIOS.
- The TPM must have an owner.
- The SRK protection for generating and loading a key must be the well-known secret.
- The TCG Software Stack (TSS) must be installed in *Windows*. *EgoSecure Full Disk Encryption* expects to find the TSS in one of the following:
  - tsp.dll
  - tsp1.dll
  - as a COM object

## Limitations

TPM support is currently limited to the FDE component only. This means that that if you want to use this feature you cannot install the PBA. Doing so will result in a fatal error (blue screen).

## Tested systems

TPM support has been successfully tested on the following systems/TPM chip combinations:

System	TPM Vendor	BIOS Access	Windows TSS
<i>Toshiba Portege M400</i> (Notebook)	<i>Infineon</i>	Failed	COM
<i>Fujitsu-Siemens Esprimo E 5616</i> (desktop)	<i>Infineon</i>	Successful	COM
<i>DELL Latitute D620</i> (notebook)	<i>Broadcom</i>	Successful	TSP.DLL
<i>DELL Optiplex</i> (desktop)	<i>STMicroElectronics</i>	Successful	TSP1

If your system does not appear in the list, it only means that such a combination has not yet been tested.

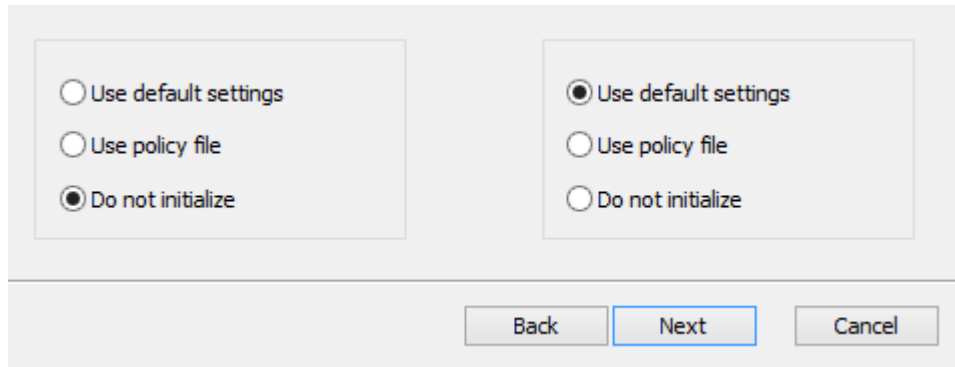
## 3.2. TPM installation

- [Attended installation](#)
- [Unattended installation](#)

## Attended installation

This section details the TPM-specific part of the installation process for the preview version of *EgoSecure TPM*.

Please begin by following the standard installation as detailed [EgoSecure FDE – Installation and Troubleshooting Guide](#). **Remember to only install/initialize the FDE component!** When the *Select initialization type* dialog appears, choose *NOT* to initialize the PBA component:



Click **Next**.

The Initialization Wizard should start automatically. Follow the wizard dialogs to complete the initialization and reboot the computer when prompted. This completes the initial setup. Go to chapter [3.4](#) to find out how to enable the TPM component.

## Unattended installation

Unattended installation is the same as already detailed in [EgoSecure FDE – Installation and Troubleshooting Guide](#). As with attended installation, remember to only install/initialize the FDE component!

Go to chapter [3.4](#) to find out how to enable the TPM component.

## 3.3. Removal

'TPM removal', as such, never occurs. You can either disable the TPM as detailed in the next section, or simply remove *EgoSecure Full Disk Encryption* as detailed in [EgoSecure FDE – Installation and Troubleshooting Guide](#).

## 3.4. TPM usage

This section details how to enable, disable, and enhance TPM support for *EgoSecure Full Disk Encryption*.

- [TPM administration module \(attended mode\)](#)
- [Remote TPM functionality \(unattended mode\)](#)

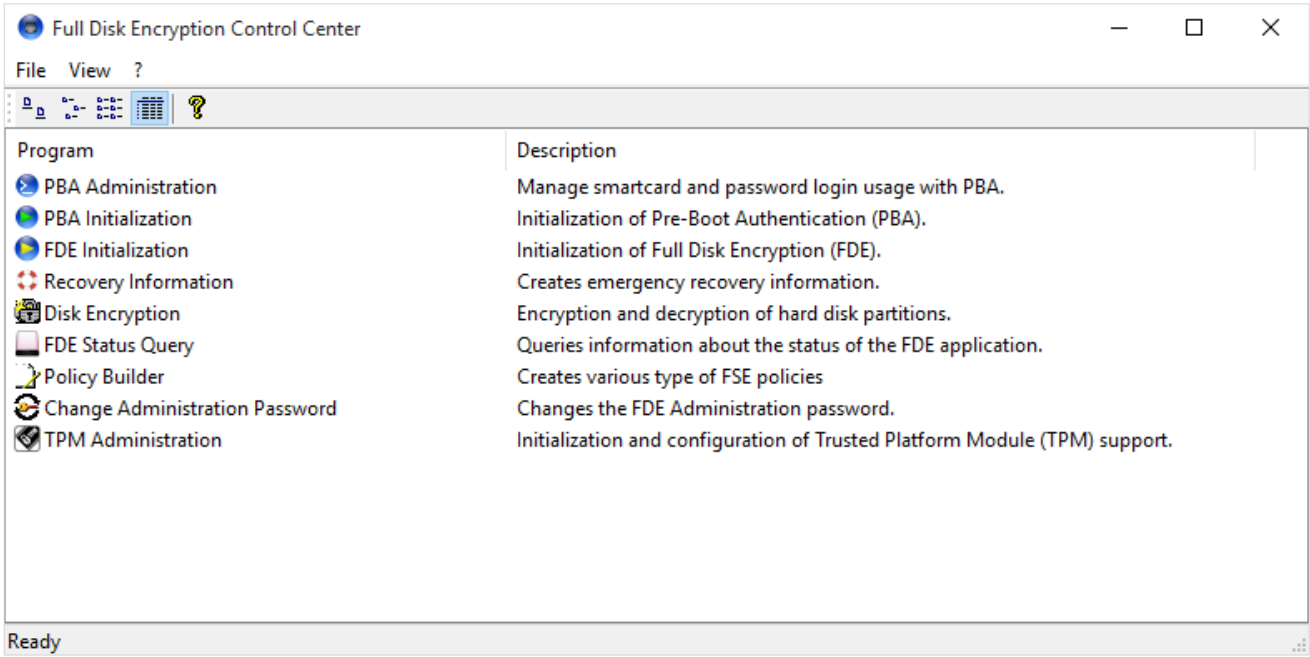
## TPM administration module (attended mode)

This section details how to manually perform TPM-related tasks on an EgoSecure Full Disk Encryption installation.

Follow these steps to perform manual TPM-related tasks in EgoSecure FDE:

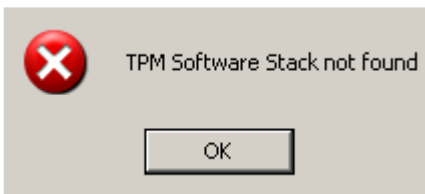
1. Open the Windows Control Panel and double-click the EgoSecure Full Disk Encryption icon.

→ The Full Disk Encryption Control Center appears:



2. Double-click the *TPM Administration* module, enter the *EgoSecure FDE* administration password when prompted, and click **OK**.

→ If the TPM chip is not ready for EgoSecure FDE, the following dialog appears. Please make sure that you have fulfilled the requirements as stated in [chapter 3.1](#). Restart the TPM installation once the TPM chip is correctly initialized.



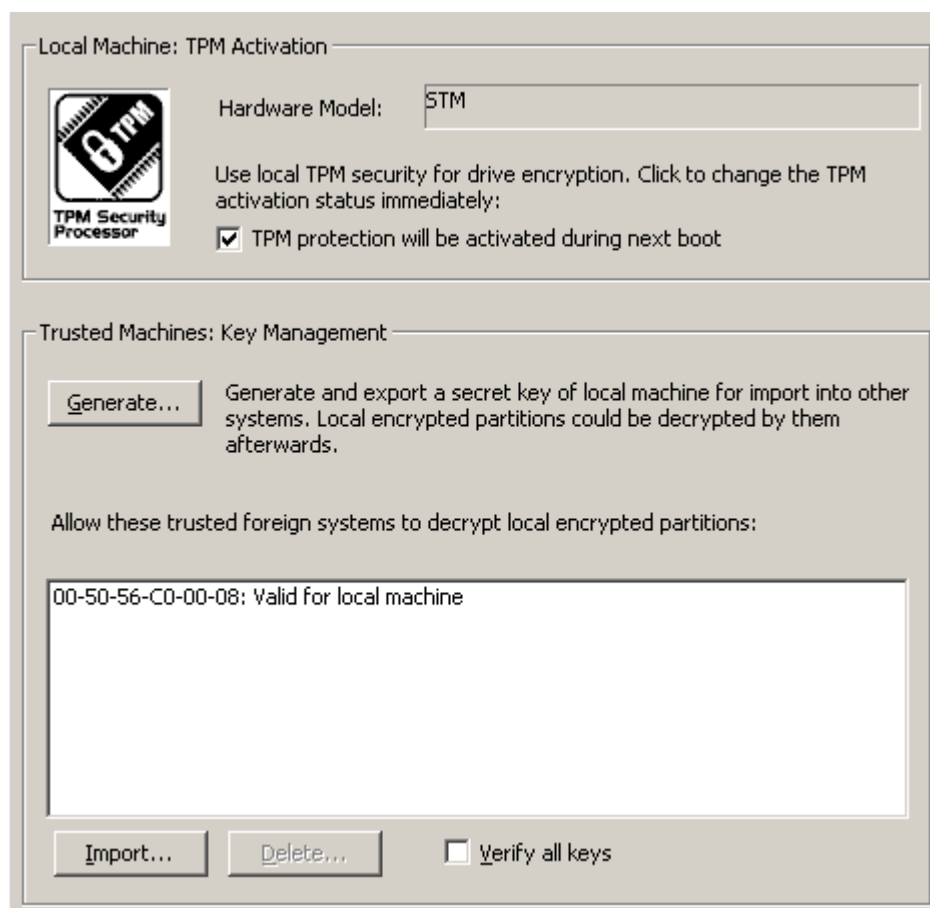
→ The **TPM Administration** dialog appears. The TPM vendor is displayed in the **Hardware Model** field at the top of the dialog. The following options are available:

Option	Description
TPM protection will be activated during next boot	Check this option to enable/disable TPM support.

Generate...	Generate a TPM key file for emergency recovery purposes and safe storage. This key file will allow the data on a hard disk transferred from one computer to another to be authenticated by the new TPM (see Import below). NOTE: A filename extension is optional (it has no effect on the functionality).
Import...	Import a TPM key file so that a hard disk (previously encrypted by another TPM) can be recognized by this TPM chip.
Delete...	Delete a selected key from the list.
Verify all keys	Verify that keys loaded onto this computer can be used by this TPM chip. This should prevent an administrator from deleting keys that apply to the local installation.

3. Click **OK** to close the **TPMAdmin** dialog.

→ Once the TPM is activated, the TPM administration dialog should look like this:



### Remote TPM functionality (unattended mode)

Follow these steps to silently enable TPM support in *EgoSecure Full Disk Encryption*:

1. Open a command prompt (administrator privileges are required for this task).
2. Navigate to the executable used for TPM tasks (`TPMAdmin.exe`) located under:



C:\Windows\NAC\

The following parameters are allowed:

```
TPMAdmin.exe [-password <admin Password>] [-generate <generated key file>]
[-import <import key file>] [-activate] [-deactivate] [-h]
```

The parameters have the following function:

Syntax	Mandatory/ Optional	Description
-h	O	Display the options listed here in the command prompt.
-password <FS administration password>	M (except for keyfile generation)	The EgoSecure FDE administration password set during installation/initialization.
-generate <generated key file>	O	Generate a TPM key file for emergency recovery purposes and safe storage. This will allow a hard disk to be transferred from one computer to another. <b>NOTE:</b> A filename extension is optional (it has no effect on the functionality). If a full path is not specified, then the key file will be saved to the same directory as the TPMAdmin module (C:\Windows\NAC\).
-import <import key file>	O	Import a TPM key file so that a hard disk can be recognized by this TPM chip. <b>NOTE:</b> This must include the full path to the key file.
-activate	O	Activate TPM functionality. <b>NOTE:</b> Remember, the activation requires a reboot for the full functionality to become active.
-deactivate	O	Disable TPM functionality.

## Examples

### ■ To enable the TPM:

```
TPMAdmin.exe -password 12345678 -activate
```

### ■ To disable the TPM:

```
TPMAdmin.exe -password 12345678 -deactivate
```

- To generate a TPM key file:

```
TPMAdmin.exe -generate EGOSECUREnotebook01TPM
```

Or...

```
TPMAdmin.exe -generate EGOSECUREnotebook01TPM.keyfile
```

Or...

```
TPMAdmin.exe -generate N:\TPMbackup\EGOSECUREnotebook01TPM
```

- To import a TPM key file:

```
TPMAdmin.exe -password 12345678 -import N:\TPMbackup\EGOSECUREnotebook01TPM
```

### 3.5. TPM utilities

This section details the utilities (helper applications) specific to TPM operation.




- [Obtain TPM status](#)
- [Test TPM compatibility](#)

#### Obtain TPM status

The current status of the TPM can be obtained via the *EgoSecure Full Disk Encryption* Control Center module **FDE status query** (otherwise known as `Nbstatus.exe`) or via the commandline (see [Start a status query via the commandline](#) for details).

#### Start TPM status query (GUI)

1. Double-click the **FDE status query** module in the Control Center.
  - The dialog appears (information may differ). For details about the non-TPM icons and information displayed in the dialog, see [The FDE status query GUI](#). The TPM icons have the following meaning:

Icon	Details
 (Active)	The TPM has been enabled for operation with <i>EgoSecure Full Disk Encryption</i> .
 (Not active)	The TPM has not yet been enabled for operation with <i>EgoSecure Full Disk Encryption</i> .
 (Activating or activation error)	This icon has one of the following meanings: The TPM has been enabled for operation with <i>EgoSecure Full Disk Encryption</i> but the computer must be restarted to complete the support. An error occurred during the TPM activation procedure.

2. Click **OK** to close the module.

## Log file interpretation

The `Nbstatus` application, via GUI or commandline, updates the log file each time it is executed. When opened, a typical log file entry appears as follows:

```
Error status = 0
Driver letter = C
Encrypt status = 0x1
Algorithm:
-----
Error status = 0
Driver letter = E
Encrypt status = 0x1
Algorithm:
-----
Computer name: MB-WINXP-02
Date: 20090923
Exit code = 9
FDE installed: Yes
Boot security installed: Yes
TPM protection: 2 (Active)
Unencrypted drivers = 2
Encrypted drivers = 0
Partly encrypted drivers = 0
Boot security errors = 0
Encrypted errors = 0
-----
MB-WINXP-02 20090429 9 1 1 2 0 0 0 0 2
```

Note that the details of TPM status (marked in **green**) are as follows:

State	Description
0 (Not active)	The TPM has not yet been enabled for operation with <i>EgoSecure Full Disk Encryption</i> .
1 (Activating)	The TPM has been enabled for operation with <i>EgoSecure Full Disk Encryption</i> but the computer must be restarted to complete the support.
2 (Active)	The TPM has been enabled for operation with <i>EgoSecure Full Disk Encryption</i> .
3 (Activation error)	An error occurred during the TPM activation procedure.

## Test TPM compatibility

A commandline utility is available in the Helper Applications directory called `TPM_test.exe`. This will allow you to test the availability and suitability of the TPM on your computer. For detailed information about this utility refer to Section 5.6 'TPM\_test'.

## 3.6. Boot Code Errors

At boot time, EgoSecure displays a message as to the status of the TPM-encrypted KEK. Usually this will be 'Unlock TPM successful'. However, should there be a problem; an error message will be displayed.

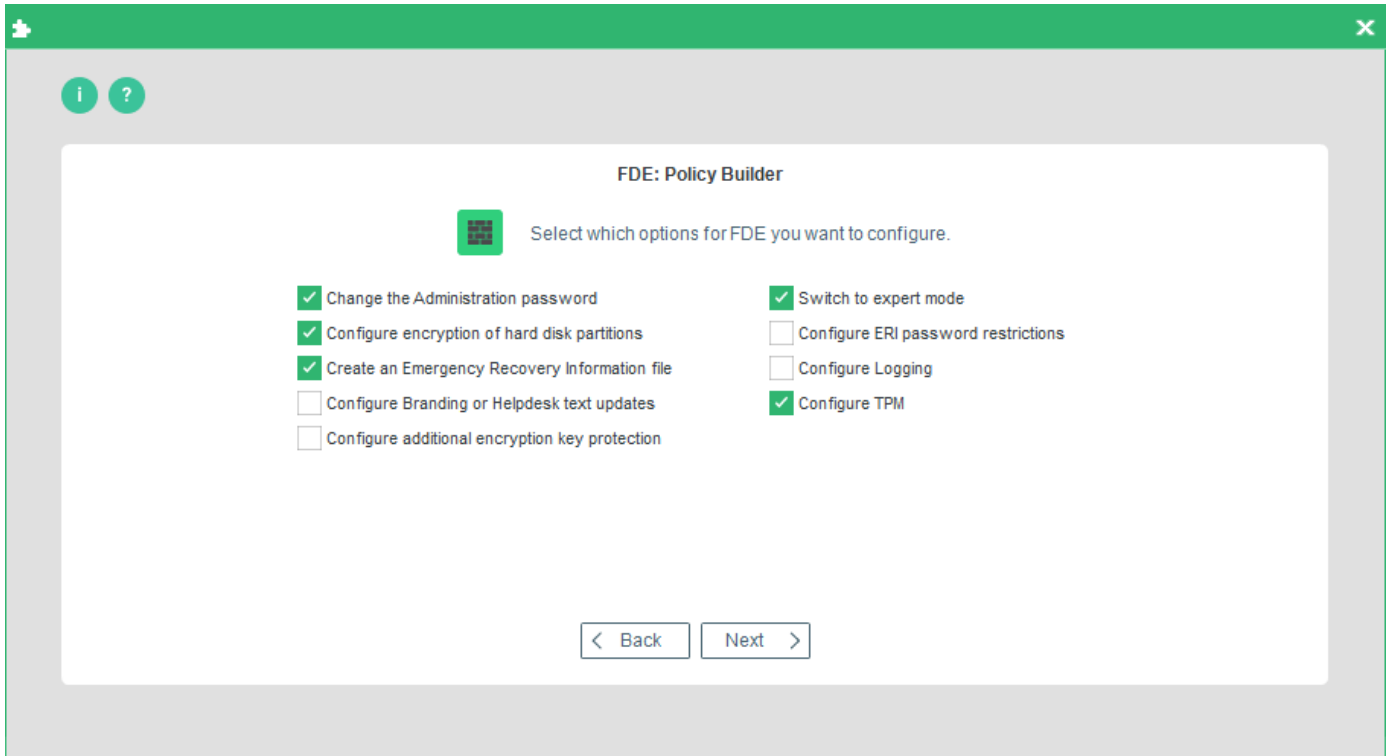
Here is a list of error messages that may appear:

Code Name	Value	Description
ERR_TPM_BIOS_CALL_FAILED	AA130000	BIOS call to access the TPM failed.
ERR_TPM_BAD_RESPONSE_SYNTAX	AA140000	Response of TPM function call (BIOS) has bad syntax.
ERR_TPM_BAD_RESPONSE_TOO_LONG	AA150000	Response of TPM function call (BIOS) is too long.
ERR_TPM_BAD_RESPONSE_TAG	AA160000	Response of TPM function call (BIOS) contains an unexpected tag.
ERR_TPM_BAD_RESPONSE_VERIFICATION	AA170000	Response of TPM function call (BIOS) has bad check sum.
ERR_TPM_MASK_BIOS_INIT_AUTH	AA910XXX	BIOS error: Error authenticating to TPM.
ERR_TPM_MASK_BIOS_UNSEAL	AA920XXX	BIOS error: Error in TPM decryption.
ERR_TPM_MASK_BIOS_LOAD_KEY	AA930XXX	BIOS error: Error loading key into TPM.
ERR_TPM_NAC_BAD_NAC_STRUCT	AA0A0000	Structure of NAC block inconsistent.
ERR_TPM_NAC_NO_TPM_INFO	AA1A0000	TPM info structure missing in NAC block.
ERR_TPM_NOT_ENOUGH_MEMORY_PROVIDED	AA040000	Not enough memory to store function result.

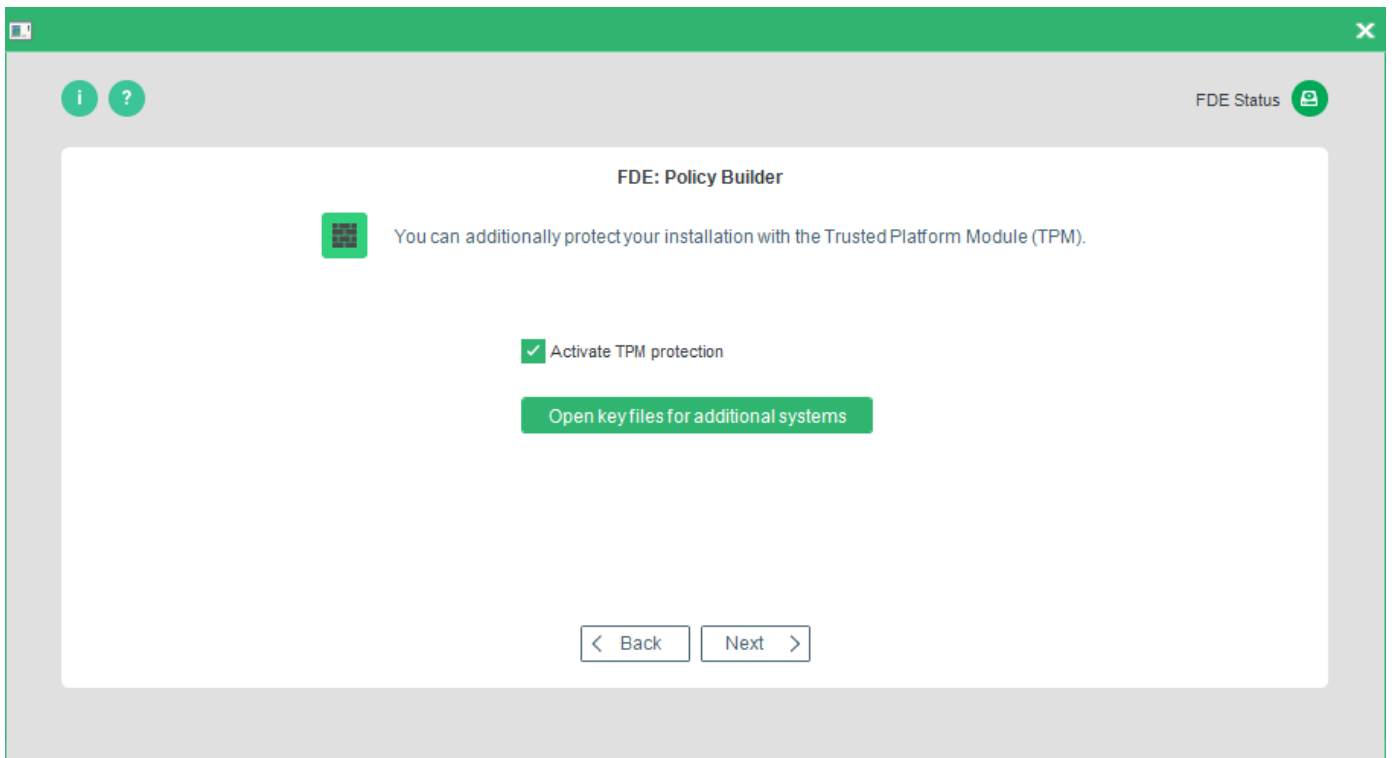
## 3.7. Creating policy for TPM (Full Disk Encryption Policy Builder)

This section details the TPM-specific dialogs in the Full Disk Encryption Policy Builder.

1. Double-click the Policy Builder module in the Control Center as described in section [2.1](#) and click **Full Disk Encryption Policy builder**.
2. Choose to create an initialization or configuration policy.
  - The options dialog appears:



3. Check, which options you want to configure and configure each one until the TPM dialog appears:



The following options are available:

<b>Option</b>	<b>Description</b>
Activate TPM protection	Enable/disable TPM protection. Once the policy is deployed, the target computer must be restarted to enable the TPM.
Open key files for additional systems	Open additional TPM key files so that the target drive may be installed on the computers from which the additional key files were obtained.

4. Complete the Full Disk Encryption Policy Builder wizard and deploy the policy.

## 4. THE INTEGRATED BOOT MANAGER

The integrated boot manager enables you to configure separate Windows hard disk partitions either for different versions of Windows or for a separate area of the drive that can be used for private, non-business use that does not compromise official security policies.

### 4.1. Overview



#### ATTENTION

#### Selecting a system

It is only necessary to use the boot manager functionality on systems that have more than one primary partition.

### Graphical interface

The boot manager has a similar graphical user interface to the Windows 2000/XP boot menu and should be used in the same way:

```
Select the operating system to boot from:

Windows XP Professional - C: + D: drive
Windows XP Professional - only C: drive
DOS FAT32 - Service Partition - X:

To mark an entry, scroll the cursor up and down.
Subsequently, press the ENTER button.
Time in seconds, until the marked selection will be started automatically: 19

Press F3 to unlock the keyboard lock.
```

The example above gives the user the option to either boot from C only, or to have an extra partition visible in Windows (C + D). This demonstrates that a boot partition, plus optional partitions, can be defined in the boot manager configuration file.

### Manual approach

To achieve this functionality, a hands-on, manual approach is necessary, for example, the boot menu entries specified in the boot manager configuration file are identified and entered into the configuration file per keyboard (there is no automated application that will achieve this for you). Do not worry about making a wrong entry here – you cannot go wrong provided you follow this guide accurately.

## 4.2. Step 1: Creating a configuration file

As a first step we will examine the configuration file to be created - `bootmgr.ini`.

### Notes

- A printed example of a configuration file can be found in Appendix, chapter [6.1](#), as well as a file in the `C:\WINDOWS\NAC` directory on a computer that has FDE installed.
- The boot menu screen consists of 25 lines of text with 80 characters per line (so-called '80 x 25'screen display). Therefore, a menu line may have no more than 80 characters!
- The boot menu is coded using the IBM-PC-ASCII-8-Bit character set. To create the boot menu, you need an ASCII editor, not editors that use the Windows ANSI character set which would result in umlauts being incorrectly represented - editors such as "Notepad" are not suitable. Use an ASCII editor to edit/create the configuration file.
- To open the ASCII editor either select **Start > Run** and enter `edit` into the **Open** field, or open the application `edit.com` directly in the `C:\WINDOWS\system32` directory.

### Understanding the bootmgr.ini

To create a `bootmgr.ini`, it is necessary to understand exactly what is to be performed. The following steps explain in detail each entry in the `bootmgr.ini` file.

Let us start by examining the code in the configuration file that we will adjust to our needs:

1. Open the `bootmgr.ini` file in the `C:\WINDOWS\NAC` directory on your computer.
2. The `bootmgr.ini` file contains the following key names in square brackets:

```
[Options]
[Menuetext]
[Entry1]
[Entry2]
[Entry3]
[Entry4]
```

3. Under each key name there are parameter names followed by '=' and the actual value.

For example:

```
[Options]
Timeout = 20
[Menuetext]
TextLine3 = Select the operating system to boot from:
.....
```

4. Now let us examine each key name and the values that follow them:

- `[Options]`

The key `[Options]` specifies the general options valid for the boot menu. It only includes the parameter `Timeout`. This parameter indicates after how many seconds the default configuration is started if no key is pressed in the boot menu (Up-and-Down cursor keys, Enter key).

In the following example the user has 20 seconds to select a boot entry and confirm his



selections before the computer starts with the first system in the list:

```
[Options]
Timeout = 20 ;
```

## ■ [Menuetext]

The key `[Menuetext]` specifies the text visible after the boot options in the boot menu. This key only includes the parameter `TextLine`. This parameter is followed by a number indicating the position at which the text will be displayed in the boot menu. For example, `TextLine3` indicates that the text will be displayed in line 3 out of 25, `TextLine9` will be displayed in line 9, and so on.

Here is an example of the key `[Menuetext]`:

```
[Menuetext]
TextLine3 = Select the operating system to boot from:
TextLine9 = To mark an entry, scroll the cursor up and
down.
TextLine10 = Subsequently, click the ENTER key.
TextLine12 = Time in seconds, until the marked selection
will be started automatically:
TextLine23 = Press F3 to unlock the keyboard lock.
```

## Partition table check

Before we move on to explain `[Entry1]` to `[Entry4]` we must first discover which partition entries are relevant:



### ATTENTION

Check the partition table of the system concerned before defining the keys `[Entry1]` to `[Entry4]` (see below). Be sure to enter the correct partition number and corresponding drive name for the values `BootPartition` and `Menuetext`, respectively! If the partition number and corresponding menu text do not match, you may boot to the wrong system.

Follow these steps to check the partition table:

1. Select **Start** > **Run** and enter `cmd` into the **Open** field to open a command box.
2. Enter `bootcfg` and press the **Enter/Return** key. The result should resemble the following example:

```
Boot Loader Settings
-----
timeout: 30
default: multi(0)disk(0)rdisk(0)partition(2)\WINDOWS

Boot Entries
-----
Boot entry ID: 1
Friendly Name: "Microsoft Windows XP Professional"
Path: multi(0)disk(0)rdisk(0)partition(2)\WINDOWS
OS Load Options: /noexecute=optin /fastdetect
```

3. The entry `'Boot entry ID: =1'` is what we are looking for. This identifies a primary partition with the ID `'1'`.

■ [Entry1] to [Entry4]

The key [Entry<number>] specifies the boot menu entries visible at the beginning of the boot menu. **ALL** four entries **MUST** remain in the boot configuration file (refer to [Unused boot menu entries](#) near the end of this section). You can define up to 4 boot menu entries, for different partitions, via the keys [Entry1] to [Entry4] respectively, as in the example below:

```
[Entry1]
MenuText      = Windows XP Professional - C: + D: drive
BootPartition = 1; Number of the boot partition (valid
values 1 - 4)
BlackList1 = 0
BlackList2 = 0
BlackList3 = 0
BlackList4 = 0
BlackList5 = 0
BlackList6 = 0
BlackList7 = 0
BlackList8 = 0
```

Where:

- The parameter `MenuText` determines the text displayed in the boot menu.
- The parameter `BootPartition` represents the number in the partition table of the partition to be booted from. The primary partition table has the values 1 to 4.
- The parameters `BlackList1` to `BlackList8` represent the numbers of the hidden partitions in the selected configuration. The partitions defined by the parameter(s) `Blacklist` apply only to the parameter `BootPartition` they follow.

`Blacklist` can be given the following values:

Blacklist<number>	Details
1-4	Corresponding primary partitions
5	First extended partition
6, 7, etc.	Further extended partitions
0	Entry is inactive

If the value 0 is found at a certain position, then any further `BlackList` values following it are ignored!

For example:

```
BlackList1 = 2
BlackList2 = 3
BlackList3 = 0
BlackList4 = 5
```

```
BlackList5 = 6
```

The values for `BlackList4` and `BlackList5` will be ignored because `BlackList3` has the value 0. Therefore the partitions defined by `BlackList4` and `BlackList5` will be visible.

Example of a correct configuration:

```
BlackList1 = 2
BlackList2 = 3
BlackList3 = 5
BlackList4 = 6
BlackList5 = 0
```

The following example details a hard disk with a primary partition (C) and an extended partition (D):

```
...
[Entry1]
MenuText = Windows XP Professional - C: + D: drive
BootPartition = 1
BlackList1 = 0
BlackList2 = 0
BlackList3 = 0
...
[Entry2]
MenuText = Windows XP Professional - only C: drive
BootPartition = 1
BlackList1 = 5
BlackList2 = 0
BlackList3 = 0
...
```

In the example above, we see under `Entry1` that the computer boots from boot partition 1 and there are no `BlackList` entries, therefore you can see all the hard disk partitions under Windows. Under `Entry2` we see that the computer boots from the same partition as in `Entry1` but the first extended partition (D) has been defined in the `BlackList`, therefore you can see only partition C under Windows.

### Unused boot menu entries

Boot menu entries that you have no need of, must contain an empty `MenuText` key and the values for the parameters `BootPartition`, and `BlackList1` to `BlackList8` must be set to 0.

Here is an example of an unused entry:

```
[Entry4]
MenuText =
BootPartition = 0
BlackList1 = 0
BlackList2 = 0
```

```
BlackList3 = 0  
BlackList4 = 0  
BlackList5 = 0  
BlackList6 = 0  
BlackList7 = 0  
BlackList8 = 0
```

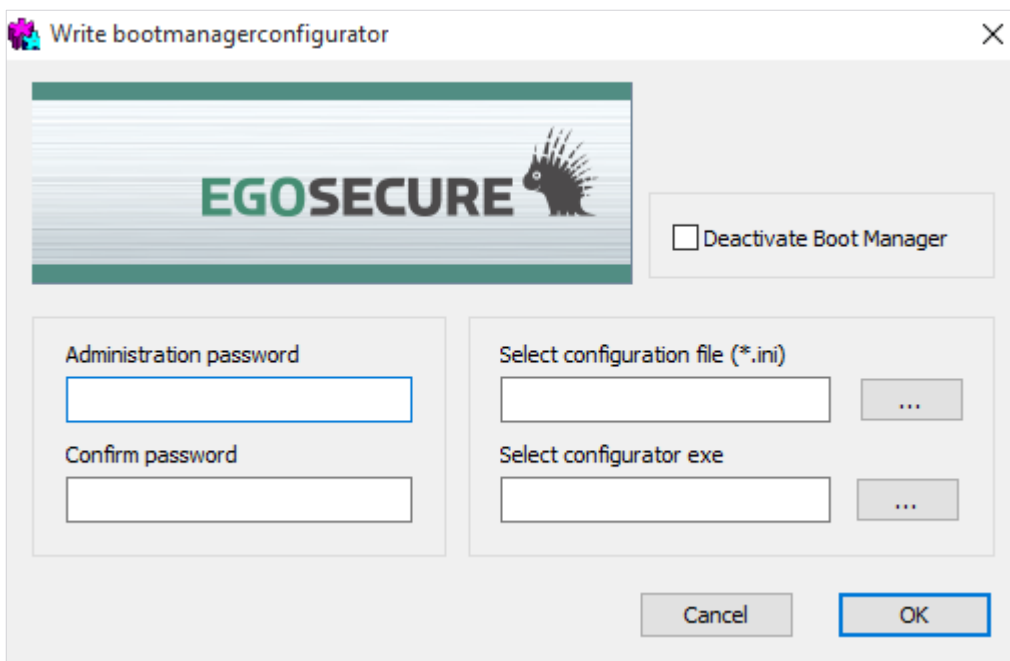
- Now you are ready to move onto the next step – creating the deployment application, see section [4.3](#).

### 4.3. Step 2: Create a configurator.exe file

The second step, after creating the `bootmgr.ini` configuration file, is to make a `configurator.exe` file out of `bootmgr.ini`. This is performed via the Boot Manager Configuration Writer (`bmcfgwriter.exe`). This application will encrypt the configuration file with an administrator password and make a `configurator.exe` file out of it. Unlike the manual approach in Section 4.2, this tool offers an easy-to-use interface. Follow these steps to create the deployment application `configurator.exe`:

1. Open the directory `C:\WINDOWS\NAC\`.
2. Double-click `bmcfgwriter.exe`.

→ The following dialog appears when the application is started:



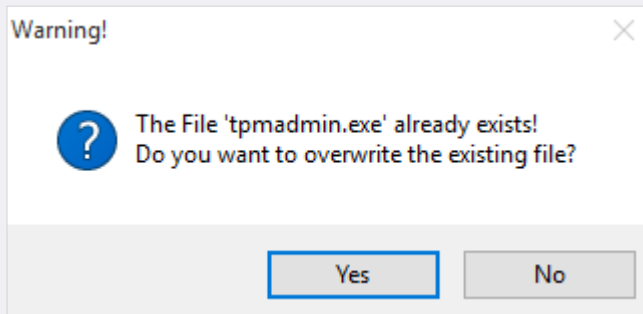
The dialog contains the following fields:

GUI element	Details
Deactivate Boot Manager	If you check this option, the boot manager will be deactivated (that is, a configurator.exe file will be created that deactivates the boot menu on the target computer).
Administration password, Confirm password	These fields are reserved for the administrator password defined during the FDE installation (see <a href="#">Installing boot security</a> for details).
Select configuration file (*.ini)	The bootmgr.ini file can be selected here via the '...' button.
Select configurator exe	Define the path and filename for the configurator.exe application field via the '...' button.

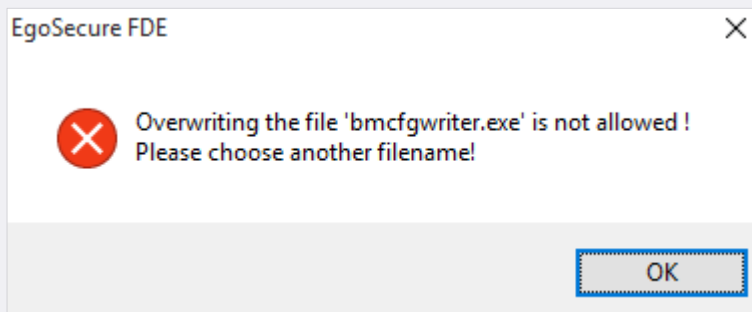


## ATTENTION

It is not necessary to name your application configurator.exe. You may choose any name you wish, but remember, do not choose the name of an application that already exists! If you should mistakenly choose the name of an application that already exists, a warning will appear asking you whether you really want to overwrite the existing file:



Some files cannot be overwritten and an error message will inform you of this if you try:



- Fill out the password fields, select your `bootmgr.ini` file, define a location for the `configurator.exe` application, and click **OK**.

➤ Now deploy your boot settings to the target computer. For details, see section [4.4](#).

## 4.4. Step 3: Executing the configurator.exe file on the target system

The third and final step is to deploy the configurator.exe application you created in section [4.3](#) to the target computer.

Follow these steps to deploy the new boot configuration:

1. Double-click configurator.exe.

→ The application will check whether the configuration file can be decrypted using the administrator password of the installation on the target computer. If successful, the boot configuration data will be encrypted and stored on the hard disk of the target machine, and the boot manager functionality will be activated.

! Configurator.exe has no dialog window and does not run as a console application, but rather runs in hidden mode.

2. To verify a successful deployment, you can refer to the FDE log file (C:\Notebook.log) for the following entries:

- The log entry below details the correct installation and activation of the boot manager:

```
"BMWRI: Writing of configfile successfully"
14:35:20, 15.08.2008 INFO BMCFG: execute configurator
14:35:20, 15.08.2008 INFO BMCFG: Activate Bootmanager
14:35:20, 15.08.2008 INFO BMCFG: Install BOOTMANAGER
14:35:20, 15.08.2008 INFO BMCFG: Config written
successfully to NAC
```

- The following log entry appears when a false administrator password has been used to decrypt the configuration file:

```
14:51:43, 15.08.2008 INFO BMCFG: execute configurator
14:51:43, 15.08.2008 INFO BMCFG: Sanity is wrong, stored
password doesn't match!
14:51:43, 15.08.2008 ERROR BMCFG: Password does not match
```

- If you checked the option **Deactivate bootmanager** in the previous step (Section [4.3](#)), then this is an example log entry for the correct removal and deactivation of the boot manager:

```
16:48:38, 15.08.2008 INFO BMCFG: execute configurator
16:48:38, 15.08.2008 INFO BMCFG: Deactivate Bootmanager
16:48:38, 15.08.2008 INFO BMCFG: Uninstall BOOTMANAGER
```

## 5. HELPER APPLICATIONS

### 5.1. Changeeripw

This utility allows you to change the password used to protect the contents of a single ERI file or batch convert multiple ERI files. This may be useful in an emergency in which you must give ERI files to a third party, for the purpose of data recovery, without compromising the original ERI password.



#### INFO

#### Keeping current ERI files

To keep your current ERI files, duplicate the files to a new directory in readiness for conversion. The ChangeERIPW utility does not duplicate the files for you – it simply changes the password used to access the same file.

Follow these steps to open the utility and change the password used to protect one or more ERI files:

1. Open the Helper Applications directory in the download package. The directory contains the helper application `Changeeripw.exe`.
2. Double-click the file.

→ The following dialog opens:

Full Disk Encryption Convert ERI File(s) Password

Convert password Activity Log

— Select a file or directory —

Select a single ERI file

Select multi ERI files

Warning: In batch conversion mode, make sure all the ERI files to be converted have the same "Old password" specified below. Otherwise those ERI file(s) can NOT be converted.

Browse

— Input password —

Old password

New password

Confirm password

Convert Close

The following options are available:

Option	Details
Select a single ERI files	Choose this option to convert a single ERI file.
Select multi ERI files	Choose this option to batch convert multiple ERI files.
Input password (area)	Password input fields for the old and new passwords.
Activity Log (tab)	This tab displays the progress of the ERI conversion.

3. Choose whether you want to convert a single or multiple ERI files by clicking the appropriate option.
4. Click **Browse**.
  - The file browser appears.
5. Select either a single file or the directory of files and click **Open**. The path should now be visible in the main window.
  - ! Only ERI files that have the same "old" password can be successfully batch converted. Don't forget that this utility tries to open each file using the same password.
6. Enter the current ERI password in the field **Old Password**, as well as the new password in **New password** and **Confirm password**.
 

Only the English keyboard layout is supported in the recovery application, that is why please enter the password, which contains no symbols from other languages.
7. Click **Convert**.
  - The window will automatically switch to the **Activity Log** tab and display the status of the conversion. The **Activity Log** area displays how many of the files have successfully been converted.
8. Click **Close** to close the application.

## 5.2. GUS

GUS is a commandline version of the GUI Upgrade Policy Builder detailed in section [2.3](#). Both the GUI and the commandline application allow you to generate an update policy to prevent the FDE administration password from being entered in the commandline in plain text for the purpose of silently upgrading or removing EgoSecure Full Disk Encryption.

### Usage

Follow these steps to create an update policy (encrypted *EgoSecure* FDE administration password):

1. Open a command prompt and navigate to the Helper Applications directory in the download package (or to wherever the Helper Applications directory is located).



2. Enter the following command to encrypt the *EgoSecure FDE* administration password and save it in policy form:

```
GUS <FDE admin password> <full path, file name, and extension>
```

For example:

```
GUS 12345678 C:\update.upd
```

### Example upgrade policy usage

The update policy can then be included in a batch file as follows:

```
msiexec.exe /i "<full MSI file path, name, and extension>"
UPGDPOLICY="<full policy path, name, and extension>" /l*
"<full log file path, name, and extension>" /passive
```

## 5.3. PSEnc

This commandline utility is used to batch-encrypt plain PBA policies to encrypted PBA policies and save them to a specific location.

### Usage

- Batch-decryption of encrypted PBA/FDE policies. The decrypt function requires the administrator password in the encrypted policies.
- Command line utility or GUI application.

```
PSEnc -f <source> -t <target> -p <password> [-d] [-s] [-b] [-h] [-n]
```

The following parameters are available:

Parameter	Details
-f	Indicator followed by source PBA policy file or directory to be encrypted.
<Source>	Name of the source policy file or directory to be encrypted.
-t	Indicator followed by target directory to store the encrypted policy/policies.
<Encrypted>	Name of the target directory to store the encrypted policy/policies.
-p	Indicator followed by encryption password.
<Password>	Encryption password.
[-d]	Indicates decryption of the encrypted PBA policy file. Supported only in Command line mode. If this option is provided: -f indicates encrypted PBA policy file; -t indicates directory to save encrypted/decrypted PBA policy file(s).
[-s]	Silent mode, without GUI.
[-b]	Batch processing indicator.

[-h]	Display the parameters listed here in the command prompt.
[-n]	Indicates switch to FDE policy mode (to encrypt/decrypt FDE policies). Supported only in Command line mode.

## Examples

- Example 1: Encrypt a plain PBA policy file located at C:\plain.pba and save it to D:\. The password is set to 12345678:

```
psenc -f c:\plain.pba -t D:\ -p 12345678
```

- Example 2: Perform the same as in example 1 in silent mode:

```
psenc -f c:\plain.pba -t D:\ -p 12345678 -s
```

- Example 3: Encrypt all the plain PBA policy files in directory C:\policies and save the encrypted files to the directory d:\policies. The password is set to 12345678:

```
psenc -f c:\policies -t D:\policies -p 12345678 -s -b
```

- Example 4: Decrypt encrypted PBA policy file c:\encrypt.pba and save it to D:\. The password is set to 12345678

```
Psync -d -f c:\ encrypt.pba -t D:\ -p 12345678
```

- Example 5: Decrypt the encrypted FDE policy file C:\encrypted.nbs and save it into D:\. The password is 12345678.

```
psenc -d -f C:\encrypted.nbs -t D:\ -p 12345678 -n
```

## Specific example

- Example 1: provide single file mode in source option, after processing copy it into target directory.

- Decrypt PBA Policy

```
psenc -d -s -f D:\encpolicies\PBA\t1.pba -t D:\target -p 12345678
```

- Decrypt FDE policy

```
psenc -n -d -s -f D:\encpolicies\FDE\fe1.nbs -t D:\target -p 12345678
```

- Example 2: Batch mode -provide files in source directory, after processing copy it into target directory.

- Decrypt PBA Policy

```
psenc -d -s -f D:\encpolicies\PBA1\ -t D:\target -b -p 12345678
```

- Decrypt FDE policy

```
psenc -n -d -s -f D:\encpolicies\FDE\ -t D:\target -b -p
12345678
```

## 5.4. Dmiconfig (hardware compatibility mode)

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, as with EgoSecure Full Disk Encryption.

A hardware compatibility mode has been introduced to allow for the support of older or unusual hardware configurations until they can be researched and fully supported in a future release. For example:

- Hardware does not function correctly under Windows after successful PBA authentication. This includes hardware that is no longer recognized. The cause of such a failure is that once successful authentication has taken place in the Linux PBA not all the BIOS settings can be correctly handled and set for Windows.
- Hardware support for newer systems as yet not natively supported by EgoSecure Full Disk Encryption.
- Poorly programmed BIOS.

### Mechanisms

It is now possible to use two mechanisms to change the boot method as well as select an alternative Linux kernel configuration that enables ACPI support:

- Boot mechanism;

Changes the method with which information is passed from the PBA to the FDE 16-bit code – known as **KICKSTART**.

- Alternative kernel with ACPI support.

	Boot method	Details
Boot mechanisms	<code>KICKSTART=[BIOS]</code>	Standard mechanism used by EgoSecure and should not be edited.
	<code>KICKSTART=[FAST]</code>	This mechanism has been implemented for systems that have unusual hardware configurations not supported by the KEXEC mechanism.
	<code>KICKSTART=[KEXEC]</code>	This mechanism is similar to <code>KICKSTART=BIOS</code> but does not need a reboot.
Alternative kernel	<code>KERNEL=/boot/bzImage-acpi</code>	This will automatically select an alternative Linux kernel configuration that enables ACPI kernel with DRM support. This is something found almost exclusively in desktop computers and is rarely needed.



**INFO**

**Using KEXEC and FAST**

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

**Screen parameters**

■ `PBA_RESOLUTION`

Defines the default or specific resolution of the display when loading PBA.

`PBA_RESOLUTION=DEFAULT` uses the resolution specified in the default settings of a device.

`PBA_RESOLUTION=800x600` (where 800 is width and 600 is height) uses the certain specified resolution.

**Kernel parameters**

■ `Irqpoll`

Alters the way that the kernel handles interrupts. This is useful if the PBA kernel log shows messages stating that an interrupt occurred.

■ `pci=snb -enable -ahci -to -legacy`

EgoSecure AHCI mode kernel option switches the chipset to ATA mode prior to performing the soft reset which boots the Windows. It fixes many instances where the chipset is in AHCI mode and the soft reset fails to boot Windows.

**Default computers**

Some computers have already been identified as ready for hardware compatibility mode and have already been included in the msi package (this can be edited). They are the following:

- Acer Veriton M665 (`KICKSTART=KEXEC`)
- Fujitsu-Siemens C1110D (`KICKSTART=BIOS` plus `KERNEL=/boot/bzImage-acpi`)
- Fujitsu S710 and E780 (`KICKSTART=KEXEC`)
- *LenovoS12* (`KICKSTART=BIOS`)
- *Panasonic ToughbookCF-19.3* (`KICKSTART=KEXEC`)
- *Panasonic ToughbookCF-52* (`KICKSTART=KEXEC`)
- *Toshiba TecraS4* (`KICKSTART=BIOS`)

**How to implement?**

A helper application is provided with the product package called `dmiconfig` (direct media interface configuration) that allows you to obtain the information necessary to create a new default configuration setup (whitelist) for deployment with the msi package. Systems defined per default in this file (`dmi.ini`) file will be automatically installed and booted accordingly.

## Dmiconfig tool

Open `dmiconfig` by starting a command prompt and entering `<path>dmiconfig` into the commandline. This will display the following options:

Command line parameter	Details
export	<p>Copy the default <code>*.ini</code> files from the PBA partition to the <i>Windows</i> partition under <code>c:\windows\nac\sbs</code>.</p> <p><b>NOTE:</b> If the files on the <i>Windows</i> partition are newer than the files on the PBA partition, the operation will fail.</p> <p>The following option is available:</p> <p><code>--force</code>: force the replacement of newer files.</p>
import	<p>This will copy the custom configuration file from the <i>Windows</i> partition to the PBA partition. If the file on the PBA partition is newer then the file on the <i>Windows</i> partition, the operation will fail.</p> <p>The following option is available:</p> <p><code>--force</code>: force the replacement of newer files.</p>
dump	<p>Dump the effective configuration for the machine on which <code>dmiconfig</code> is running. The result is displayed in the command line. For example:</p> <pre>[Acer,Veriton T/M/S661;461] DMI_SYS_VENDOR=Acer DMI_PRODUCT_NAME=Veriton T/M/S661;461</pre> <p>The following options are available:</p> <p><code>--short</code>: Perform the shortest possible configuration dump (recommended for broad rollouts).</p> <p><code>--long</code>: Perform the longest possible configuration dump (recommended for specific computers as this includes serial number information etc.).</p> <p><code>--pba</code>: View the current DMI configuration used by the PBA.</p> <p><code>--db</code>: Dump the content of the two configuration files on the PBA-Partition (must be used with <code>--pba</code>).</p>
set	<p>Replace settings for the machine on which <code>dmiconfig</code> is running.</p> <p>The following option is available:</p> <p><code>--pba</code>: If you do not use this parameter, you have to call <code>dmiconfig import</code> to activate the new configuration.</p>
stat	<p>Check if the files on the PBA-Partition are the same as the files on the <i>Windows</i> Partition. This will then inform you if the configuration needs updating or not:</p> <ul style="list-style-type: none"> <li>■ If the files are the same: Configuration is up-to-date.</li> <li>■ If the PBA files are newer: The configuration files on the PBA partition are newer! Call <code>'dmiconfig export'</code> to update the files in <code>C:\windows\nac\sbs</code></li> <li>■ If the PBA files are older: The configuration files on the <i>Windows</i> partition are newer. Call <code>'dmiconfig import'</code> to update the files in the on the PBA-partition.</li> </ul>

## Creating a dmi file to be included in the installation

1. Install, but do not initialize *EgoSecure Full Disk Encryption*.
2. Open a command shell (run as administrator) and start the `dmiconfig.exe` tool in the Helper Applications directory.
3. Enter the following command: `dmiconfig dump`. This will display the configuration of the computer.
4. Open the file `C:\WINDOWS\NAC\SBS\dmi.default.ini` in a text editor add the lines of configuration that were dumped in the previous step.
5. Under the configuration add the line `KICKSTART=BIOS` or `KICKSTART=KEXEC` depending on which mechanism that works on the target computer.
6. To boot the computer using the alternative *Linux* kernel (with ACPI support) add the following: `KERNEL=/boot/bzImage-acpi`.
  - The final entry should look something like this:

```
[Acer,Veriton T/M/S661;461]
DMI_SYS_VENDOR=Acer
DMI_PRODUCT_NAME=Veriton T/M/S661;461
KICKSTART=KEXEC
KERNEL=/boot/bzImage-acpi
```
7. Save the file as `dmi.ini` to a location of your choice. Place the file in the same installation directory as the msi package so that it will be automatically included in the rollout.

## Adding current configuration to the PBA

1. Install and initialize the FDE component, install, but do not initialize the PBA component.
2. Reboot as prompted after FDE initialization.
3. Follow steps 1 – 6 as stated above for dmi creation.
4. Save the file as `dmi.ini` under `C:\WINDOWS\NAC\SBS\`.
5. Initialize the PBA component.
6. Go back to the open command prompt and enter the following syntax: `dmiconfig.exe import`.
7. Reboot the computer.
  - The PBA will appear as normal. After successful authentication, a quick reboot will be performed in compatibility mode.

## 5.5. Systemcheck

The `systemcheck.exe` is a stand-alone application for checking information about the *EgoSecure Full Disk Encryption* installation on your computer.

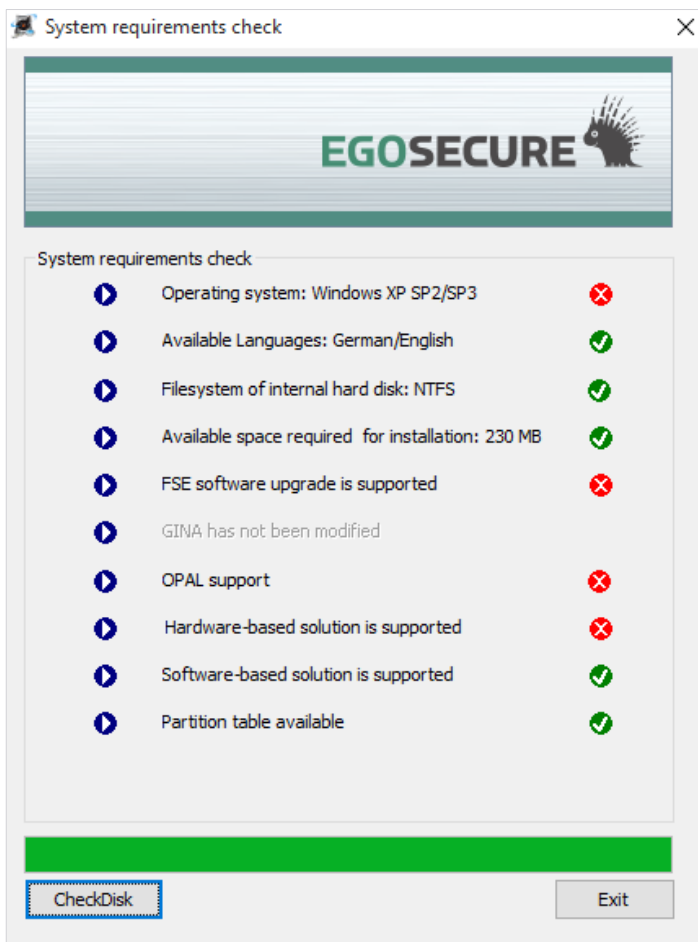
**Prerequisites.** Please execute the systemcheck.exe within its delivered directory or make sure the delivered libraries sdpseagate.dll and libeay32.dll are available in the same directory where the systemcheck.exe is executed.

Follow these steps to query the status of the EgoSecure Full Disk Encryption installation on your computer:

1. Double-click systemcheck.exe in the Helper Application directory (or whichever directory you have placed it).

→ The **System requirements check** dialog appears.

**Figure 12. System check**



→ The application will automatically gather and display information about the *EgoSecure Full Disk Encryption* installation on your computer. An icon will be displayed next to each of the entries allowing you to determine if *EgoSecure Full Disk Encryption* is suitable for your system or the simply give you the details of a current *EgoSecure Full Disk Encryption* installation. Click **CheckDisk** to start the Windows application `CHKDSK` (recommended before installation).

2. Click **Exit** to close the dialog.

## 5.6. TPM\_test

A commandline utility is available in the Helper Applications directory called TPM\_test.exe. This will allow you to test the availability and suitability of the TPM on your computer for use with *EgoSecure Full Disk Encryption*.

This utility will not work unless the TCG Software Stack (TSS) has been installed under Windows. EgoSecure FDE expects to find the TSS in one of the following:

- tsp.dll
- tsp1.dll
- as a COM object

Follow these steps to test the TPM using this utility:

1. Open a command prompt and navigate to the Helper Applications directory in the product package (or to wherever the Helper Applications directory is located).
2. Enter `TPM_test` to start the utility.

→ A successful scenario appears as follows:

```
C:\TPM-Tools>tpm_test.exe

Trusted Platform Module *** TPM Test Utility
Copyright (c) 2010 by SECUDE AG. All rights reserved.

*** This test may take a few minutes to complete ***

Getting TPM driver                ... OK
Connecting to TPM service         ... OK
Getting TPM infos                 ... OK
    owner                         ... existing
    manufacturer                   ... 49465800 (IFX )
Getting handle for Storage Root Key (SRK) ... OK
Creating policies for key secrets ... OK
Creating own key (may take some time) ... OK
Getting public key                 ... OK
Encrypting data with public key (TPM) ... OK
Decrypting data with private key   ... OK
Comparing data                     ... OK
Encrypting data with public key (RSA module) ... OK
Decrypting data with private key   ... OK
Comparing data                     ... OK

Finished. All tests passed successfully.

C:\TPM-Tools>
```

→ The application will automatically gather and display information about the EgoSecure Full Disk Encryption.

## 5.7. Tcosconfig

A commandline utility is available in the Helper Applications directory called tcosconfig.exe. This will allow you to scan TCOS smart cards via the PC/SC interface for the purpose of customizing the TCOS configuration in the PBA.



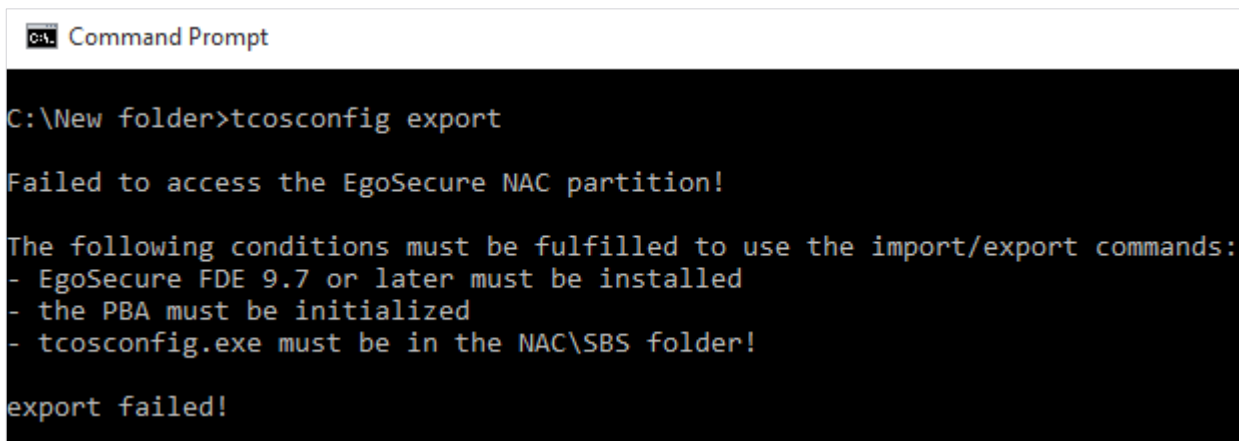
- Local Administrator privileges are required to start and use this utility.
- The following prerequisites must be met to successfully use `tcosconfig`:
  - The PBA must have undergone successful initialization
  - `Tcosconfig` must be copied to the `Windows\NAC\SBS` directory

Follow these steps to start `tcosconfig`:

1. Copy the `tcosconfig.exe` application from the *EgoSecure Full Disk Encryption* delivery package to the `Windows\NAC\SBS` directory on a client that has undergone successful PBA initialization.

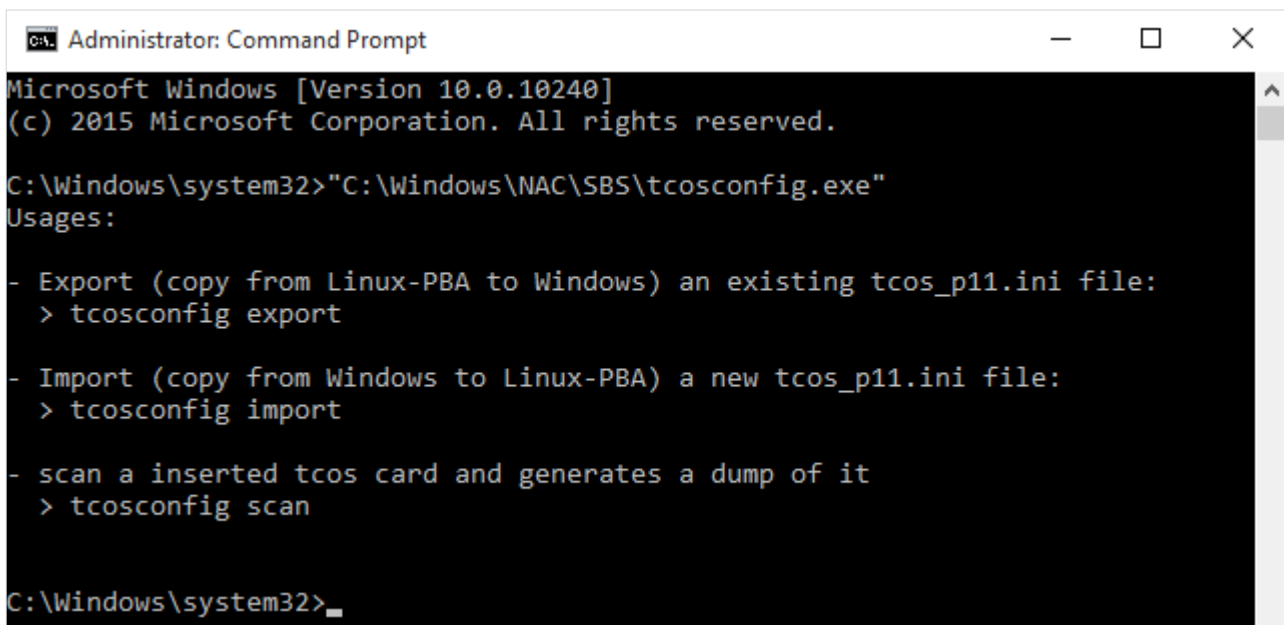
If you start `tcosconfig` from another directory, then the following error will be displayed if you try to perform any of the administration tasks:

**Figure 13. Error when starting from another directory**



```
Command Prompt
C:\New folder>tcosconfig export
Failed to access the EgoSecure NAC partition!
The following conditions must be fulfilled to use the import/export commands:
- EgoSecure FDE 9.7 or later must be installed
- the PBA must be initialized
- tcosconfig.exe must be in the NAC\SBS folder!
export failed!
```

2. Open a command prompt (with administrator privileges) and navigate to `Windows\NAC\SBS` directory).
3. Enter `tcosconfig` [Return] to start the utility and display the usage as follows:



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.
C:\Windows\system32>"C:\Windows\NAC\SBS\tcosconfig.exe"
Usages:
- Export (copy from Linux-PBA to Windows) an existing tcos_p11.ini file:
  > tcosconfig export
- Import (copy from Windows to Linux-PBA) a new tcos_p11.ini file:
  > tcosconfig import
- scan a inserted tcos card and generates a dump of it
  > tcosconfig scan
C:\Windows\system32>
```

The tcosconfig utility has the following usages:

Command line parameter	Details
export	Use this parameter to copy the existing tcos_p11.ini file from the PBA ( <i>Linux</i> ) to the Windows\NAC\SBS directory. Example: tcosconfig export
import	Use this parameter to copy a new custom tcos_p11.ini file from the Windows\NAC\SBS directory to the PBA ( <i>Linux</i> ). Example: tcosconfig import
scan	Generate a dump of a TCOS card inserted into the smart card reader. This is necessary if you want to check the smart card profile against that that is already supported in the tcos_p11.ini file, and edit the tcos_p11.ini file accordingly to support the smart card profile. Example: tcosconfig scan

### Exporting the tcos\_p11.ini file from the PBA

1. Enter `tcosconfig export` [Return] to export the `tcos_p11.ini` file and `tcos_p11_default.ini` file to the Windows\NAC\SBS directory.

```
C:\Windows\NAC\SBS>tcosconfig export
export of '/etc/tcos_p11_default.ini' to 'C:\Windows\NAC\SBS\tcos_p11_default.ini' succeeded
export of '/etc/tcos_p11.ini' to 'C:\Windows\NAC\SBS\tcos_p11.ini' succeeded
C:\Windows\NAC\SBS>
```

2. Once completed the command prompt can be closed.

### Importing the tcos\_p11.ini file into the PBA

1. Enter `tcosconfig import` [Return] to export the `tcos_p11.ini` file and `tcos_p11_default.ini` file from the Windows\NAC\SBS directory to the PBA.

```
C:\Windows\NAC\SBS>tcosconfig import
import of 'C:\Windows\NAC\SBS\tcos_p11.ini' to '/etc/tcos_p11.ini' succeeded
C:\Windows\NAC\SBS>
```

2. Once completed the command prompt can be closed.

### Scanning a TCOS smart card

1. Enter `tcosconfig scan` [Return] (without a smart card in the reader) to display the following sub-parameters:

**Figure 14. Scanning TCOS smart card**

```

C:\Users\user win10>cd C:\Users\user win10\Desktop\Helper Applications\x86-64
C:\Users\user win10\Desktop\Helper Applications\x86-64>tcosconfig.exe scan
Scanner for TCOS Smartcards using PC/SC interface.
Version 12.1.888.2 Copyright (c) 2004 - 2017 EgoSecure

Syntax: scantcos.exe [dfprt]

d: dump to screen
f: dump to files in current folder
r: raw, do not strip TeleSec ASN.1 prefix
a: dump all files (default: certificates only)
z: dump empty files (default: check for starting zero byte)

```

The subparameters have the following meaning:

Command line parameter	Details
d	Dump to screen
f	Dump information to the Windows\NAC\SBS directory as *.der files. This will also strip the TeleSec ASN.1 prefix
r	Dump raw files - do not strip TeleSec ASN.1 prefix
a	Dump all files (default: certificates only)
z	Dump empty files (default: check for starting zero byte)



**INFO**

The information displayed in the usage - scantos.exe – refers to an application with the tcosconfig construct for the purpose of reading TCOS cards. It CANNOT be addressed directly via the commandline but rather indirectly through tcosconfig.

Use one of the options detailed above to obtain the information you need from the smart card profile you want the PBA to support. If you enter tcosconfig scan [Return] with a TCOS smart card in the reader, then the smart card details will be automatically displayed on the screen. For example:

```

C:\Windows\NAC\SBS>tcosconfig scan
Broadcom Corp Contacted SmartCard 0
ATR is 3bbf96008131fe5d00640411030131c073f701d00090007d
/
/DF01/          name=D27600006601 name=A000000167455349474E

```

```

/DF01/D000      s=0008 ft=Trans
/DF01/5049      s=00C0 ft=LinVar t=DATA
                PIN 81 status: NULL-PIN
                PIN 83 status: FBZ: 0
                PIN 82 status: NULL-PIN
/DF01/5044      s=0042 ft=LinFix t=PIN
/DF01/5045      s=0016 ft=LinFix t=PIN
/DF01/5349      s=0069 ft=LinVar t=DATA
                A0(76)=[FID=84 94(25)=[alg=RSA-CRT len=128 record=01
                ... ] ] B6(25)=[7A(12)=[SigCntStart=1] ]
/DF01/5344      s=0288 ft=LinVar t=Key
/DF01/4531      s=0278 ft=LinVar
/DF01/B000      s=0200 ft=Trans
/DF01/C000      s=1000 ft=Trans
/DF01/C008      s=0C00 ft=Trans
/DF01/C00E      s=0C00 ft=Trans
/DF02/          name=D2760000030102
/DF02/5349      s=0250 ft=LinVar t=DATA
                A0(81)=[FID=80 94(38)=[alg=RSA-CRT len=128 fid=5344
                record=01 ... ] ] B6(8)=[
                A0(89)=[FID=81 94(38)=[alg=RSA-CRT len=128 fid=5344
                record=07 ... ] ]
                A0(89)=[FID=82 94(38)=[alg=RSA-CRT len=128 fid=5344
                record=0D ... ] ]
                A0(83)=[FID=83 94(32)=[alg=RSA-CRT len=96 fid=5344
                record=13 ... ] ]
                A0(15)=[FID=84 94(7)=[alg=DES3 len=96 fid=4480
                record=01 ... ] ]
                A0(32)=[FID=85 94(4)=[alg=DES3 len=0 ... ] ]
                A0(32)=[FID=86 94(4)=[alg=DES3 len=0 ... ] ]
/DF02/5344      s=0A20 ft=LinVar t=Key
/DF02/4480      s=0030 ft=LinVar t=Key
/DF02/5049      s=00F0 ft=LinVar t=DATA
                PIN 81 status: FBZ: 3
                PIN 83 status: FBZ: 3
                PIN 82 status: NULL-PIN
/DF02/5044      s=0058 ft=LinFix t=PIN
/DF02/5453      s=0800 ft=Trans
/DF02/C000      s=0800 ft=Trans
/DF02/C200      s=0800 ft=Trans
/DF02/C500      s=0800 ft=Trans
/DF02/C201      s=0800 ft=Trans
/DF02/4531      s=0208 ft=LinVar
/DF02/45B1      s=0108 ft=LinVar
/DF02/4571      s=0108 ft=LinVar
/DF02/45B2      s=0088 ft=LinVar
/DF02/B000      s=0288 ft=Trans
/DF02/5345      s=0066 ft=LinVar t=DATA
/DF02/544F      s=0048 ft=LinVar t=DATA
/DF02/43B1      s=06C5 ft=Trans
/DF02/4331      s=06A1 ft=Trans
/DF03/          name=D2760000030302
/DF03/5349      s=0100 ft=LinVar t=DATA
                A0(15)=[FID=81 94(7)=[alg=DES len=96 fid=5344 record=01... ] ]

```

```
A0(15)=[FID=82 94(7)=[alg=DES3 len=96 fid=5344
record=02 ... ] ]
/DF03/5344 s=0020 ft=LinVar t=Key
/DF03/5049 s=00F0 ft=LinVar t=DATA
PIN 81 status: FBZ: 3
PIN 83 status: NULL-PIN
/DF03/5044 s=0042 ft=LinFix t=PIN
/DF03/474F s=0008 ft=Trans
/DF03/5345 s=004A ft=LinVar t=DATA
/DF04/
name=D2760000030202
/DF04/5349 s=0080 ft=LinVar t=DATA
A0(15)=[FID=81 94(7)=[alg=DES len=96 fid=5344
record=01 ... ] ]
/DF04/5344 s=0008 ft=LinVar t=Key
/DF04/5049 s=0070 ft=LinVar t=DATA
/DF04/5044 s=002C ft=LinFix t=PIN
/DF04/474C s=0010 ft=Trans
/DF04/5345 s=0020 ft=LinVar t=DATA
/DF05/
name=4F564944
/DF05/5349 s=0080 ft=LinVar t=DATA
A0(42)=[FID=80 94(7)=[alg=DES3 len=96 fid=5344
record=01 ... ] ]
/DF05/5344 s=0018 ft=LinVar t=Key
/DF05/5049 s=0070 ft=LinVar t=DATA
PIN 80 status: FBZ: 3
/DF05/5044 s=0016 ft=LinFix t=PIN
/DF05/6E64 s=001E ft=Trans
/DF05/6570 s=0008 ft=Trans
/DF05/5345 s=0020 ft=LinVar t=DATA
/4101/
name=D2760001050002
/4101/5345 s=00F0 ft=LinVar t=DATA
/4101/5183 s=0250 ft=LinVar t=DATA
/4101/5283 s=0610 ft=LinVar t=Key
/4101/4E03 s=0210 ft=LinVar
/4101/4352 s=06A0 ft=Trans
/DF06/
name=4D534350
/DF06/5345 s=0080 ft=LinVar t=DATA
/DF06/80FE s=0020 ft=Trans
/DF06/8003 s=0015 ft=Trans
/DF06/8001 s=002F ft=Trans
/DF06/8002 s=000D ft=Trans
/DF06/8080 s=0005 ft=Trans
/DF06/80FF s=01E2 ft=Trans
/DF06/0002 s=050F ft=Trans
/DF06/1100 s=000E ft=Trans
/DF06/1201 s=000E ft=Trans
/DF06/1202 s=000E ft=Trans
/DF06/1103 s=000E ft=Trans
/DF06/1104 s=000E ft=Trans
/DF06/1105 s=000E ft=Trans
/DF06/80FD s=0066 ft=Trans
/2F02 s=000C ft=Trans t=DATA
/2F00 s=0320 ft=LinVar-STLV
/5049 s=00CD ft=LinVar t=DATA
PIN 00 status: FBZ: 3
```

```

PIN 01 status: FBZ: 3
PIN 02 status: FBZ: 3
/5044      s=0058 ft=LinFix t=PIN
/5349      s=0255 ft=LinVar t=DATA
A0(30)=[FID=74 94(7)=[alg=DES3 len=96 fid=4400
record=01 ... ] 90(1)=05 ]
A0(28)=[FID=01 94(20)=[alg=RSA-CRT len=32 record=01
... ] ]
A0(67)=[FID=73 name=3030 00 00 00 00 00 00 00 00 00 00 00 00 00
0000 00 94(13)=[alg=RSA-Pub len=128 fid=4500 record=03 ... ] ]
B6(7)=[]
A0(45)=[FID=77 94(13)=[alg=RSA-Pub len=128 fid=4500
record=05 ... ] ]
A0(41)=[FID=72 name= 94(4)=[alg=RSA-Pub len=0 ... ]
] B6(11)=[]
A0(45)=[FID=71 name=4445545343110106
94(13)=[alg=RSA-Pub len=128 fid=4500 record=01 ... ]
] B6(11)=[]
A0(25)=[FID=75 94(3)=[alg=DES3 len=138 fid=0105 ...
] ]
A0(25)=[FID=76 94(3)=[alg=DES3 len=138 fid=0105 ...
] ]
A0(27)=[FID=07 94(7)=[alg=DES3 len=96 fid=5007
record=01 ... ] ]
/5344      s=0144 ft=LinVar t=Key
/4400
/4500      s=018C ft=LinVar t=Key
/4349      s=009A ft=LinVar t=DATA
/2F03      s=00D1 ft=Trans
/4570      s=0088 ft=LinVar
/2F04      s=00D2 ft=Trans
/4401      s=0018 ft=LinVar
/2F01      s=0024 ft=LinVar t=DATA

```

```

~~~~~
Scanner for TCOS Smartcards using PC/SC interface.
Version 06.04.2017. Copyright (c) 2004-2017 by EgoSecure.

```

Syntax: scantcos.exe [dfprt]

```

d: dump to screen
f: dump to files in current folder
r: raw, do not strip TeleSec ASN.1 prefix
a: dump all files (default: certificates only)
z: dump empty files (default: check for starting zero
byte)

```

2. Once completed, the command prompt can be closed.

## 6. APPENDIX

### 6.1. Bootmgr.ini example

```
;
; Configuration file for the Boot-Manager of
; EgoSecure FDE 12.1.883.0
;
[Options]
Timeout = 20

[Menuetext]
TextLine3 = Select the operating system to boot from:
TextLine9 = To mark an entry, scroll the cursor up and down
TextLine10 = Subsequently, click the ENTER key.
TextLine12 = time in seconds, until the marked selection will
be started automatically ...
TextLine23 = Press F3 to unlock the keyboard lock.

[Entry1]
MenueText      = Windows XP Professional - C: + D: drive
BootPartition  = 1 ; Number of the boot partition
(valid values 1 - 4)
BlackList1     = 0
BlackList2     = 0
BlackList3     = 0
BlackList4     = 0
BlackList5     = 0
BlackList6     = 0
BlackList7     = 0
BlackList8     = 0

[Entry2]
MenueText      = Windows XP Professional - only C: drive
BootPartition  = 1
BlackList1     = 5 ; set partition D: hidden - the first
extended partition begins always with number 5
BlackList2     = 0 ; with the blacklist entries you can set up
to 8 partitions hidden (invisible)
BlackList3     = 0
BlackList4     = 0
BlackList5     = 0
BlackList6     = 0
BlackList7     = 0
BlackList8     = 0

[Entry3]
```

```
MenueText = DOS FAT32 - Service Partition - X:
BootPartition = 3
BlackList1 = 0
BlackList2 = 0
BlackList3 = 0
```

; A sample of an unused entry - Menuetext is empty, all other entries must be zero

```
[Entry4]
MenueText =
BootPartition = 0
BlackList1 = 0
BlackList2 = 0
BlackList3 = 0
BlackList4 = 0
BlackList5 = 0
BlackList6 = 0
BlackList7 = 0
BlackList8 = 0
```

## 6.2. Key usage

Here is a list of Key Usages supported by EgoSecure FDE smart card authentication:

Key usage	Details
Digital signature	Use when the public key is used with a digital signature mechanism to support security services other than non-repudiation, certificate signing, or CRL signing. A digital signature is often used for entity authentication and data origin authentication with integrity.
Non-repudiation	Use when the public key is used to verify digital signatures used to provide a non-repudiation service. Non-repudiation protects against the signing entity falsely denying some action (excluding certificate or CRL signing).
Key encipherment	Use when a certificate will be used with a protocol that encrypts keys. An example is S/MIME enveloping, where a fast (symmetric) key is encrypted with the public key from the certificate. SSL protocol also performs key encipherment.
Data encipherment	Use when the public key is used for encrypting user data, other than cryptographic keys.
Key agreement	Use when the sender and receiver of the public key need to derive the key without using encryption. This key can then be used to encrypt messages between the sender and receiver. Key agreement is typically used with Diffie-Hellman ciphers.
Encipher only	Use only when key agreement is also enabled. This enables the public key to be used only for enciphering data while performing key agreement.



---

Decipher only	Use only when key agreement is also enabled. This enables the public key to be used only for deciphering data while performing key agreement.
Client authentication	Enable for these key usage extensions: Digital signature and/or Key agreement
E-mail protection	Enable for these key usage extensions: Digital signature, Non-repudiation, and/or Key encipherment or Key agreement.
Encrypted filesystem	This key usage is defined by Microsoft. The certificate can be used to encrypt files by using the Encrypting File Systems. For further information, refer to: <a href="http://msdn.microsoft.com/en-gb/library/aa378132.aspx">http://msdn.microsoft.com/en-gb/library/aa378132.aspx</a>
Smart card login	This key usage is defined by Microsoft. The certificate enables an individual to log on to a computer via a smart card.