

ESET Endpoint Encryption Quick-Start Guide

User guide

[Click here to display the online version of this document](#)

Copyright ©2024 by ESET, spol. s r.o.

ESET Endpoint Encryption Quick-Start Guide was developed by ESET, spol. s r.o.

For more information visit <https://www.eset.com>.

All rights reserved. No part of this documentation may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without permission in writing from the author.

ESET, spol. s r.o. reserves the right to change any of the described application software without prior notice.

Technical Support: <https://support.eset.com>

REV. 2/13/2024

1 Introduction	1
1.1 Changelog	1
1.2 Supported operating systems	1
1.3 File size limitations	2
2 Install ESET Endpoint Encryption Client	3
3 Activate ESET Endpoint Encryption Client	6
3.1 Activate ESET Endpoint Encryption via email	6
4 Initiate Full Disk Encryption	7
4.1 Single Sign-on	11
4.2 TPM PIN	12
4.3 Change encryption password	14
4.4 Recover encryption password	16
5 Encryption features	17
5.1 Removable Media Encryption	18
5.2 Email Encryption	25
5.2 ESET Endpoint Encryption Reader	30
5.2 ESET Endpoint Encryption Reader for Windows	30
5.2 ESET Endpoint Encryption Reader for macOS	35
5.3 File/Folder Encryption	41
5.4 Text Encryption	46
5.5 Virtual Disks	49
5.6 Encrypted Archives	57
6 Key-File	62
6.1 Encryption Key Manager	63
6.2 Log in and out of the Key-File	64
7 Pre-boot screen shortcuts	65
8 Troubleshooting	66
8.1 Single Sign-On (SSO) does not log in to Windows	66
8.2 Single Sign-On (SSO) and network password	67
8.3 Single Sign-On (SSO) synchronization	67
9 Glossary	68
10 End User License Agreement	70
11 Privacy Policy	76


Introduction

ESET Endpoint Encryption is a comprehensive security application designed to protect your data at rest and in transit.

All editions of ESET Endpoint Encryption encrypt files, folders and emails. They also create encrypted virtual disks, compress archives and include a desktop shredder for secure file deletion. A patented encryption key sharing system means seamless sharing of encrypted files, email and media. There are also fewer passwords to remember and an exceptionally intuitive user experience.

An administrator remotely manages user installation using the ESET Endpoint Encryption Server. ESET Endpoint Encryption Server communicates changes made by an administrator so that systems used or kept off-site are always up to date.

A managed installation has a small number of user-accessible settings but benefits from a wide range of software and enforced security policy settings, controlled from the ESET Endpoint Encryption Server.

 Managed users are not required to back up recovery passwords or encryption keys.


Changelog

Supported operating systems

You can install ESET Endpoint Encryption Client on the following operating systems:

Windows version	X86	X64
Windows 11	N/A	✓
Windows 10	✓	✓

Windows Server version	X86	X64
Windows Server 2022	✓	✓
Windows Server 2019	✓	✓
Windows Server 2016	✓	✓
Windows Server 2012 R2	✓	✓
Windows Server 2012	✓	✓

 ESET Endpoint Encryption Client version 5.1 is the last to support Windows 7 and Windows 8.1. [More information.](#)

macOS version	
macOS Sonoma (14.0)	✓
macOS Ventura (13.0)	✓

macOS version	
macOS Monterey (12.0)	✓
macOS Big Sur (11.0)	✓
macOS Catalina (10.15)	✓
macOS Mojave (10.14)	✓
macOS High Sierra (10.13)	✓

Compatibility:

- ESET Endpoint Encryption supports Apple M1 Mac natively. You
- ESET Endpoint Encryption does not support ARM processors on Windows.
- Dual-boot or software RAID systems do not support full disk encryption.
- Full disk encryption is not compatible with Apple Mac systems using Apple Boot Camp.
- Microsoft Storage Spaces and Dynamic Disks are not supported.
- Use Windows Insider Previews for testing, as data may be at risk.
- You can use ESET Endpoint Encryption in a virtual machine environment on a PC or Mac. The successfully tested hypervisors include VMWare Workstation, Parallels Desktop for Mac and VMWare Fusion for Mac OS X.
- Windows Server Core environments are not supported.

 You cannot install ESET Endpoint Encryption at the same time as ESET Full Disk Encryption.

Hardware:

- Full Disk Encryption of system disks supports only 512-byte size sectors.
- Removable media encryption supports 512-byte and 4k-size sectors for file mode encryption but only 512-byte for full disk encryption.

File size limitations

The following table details the maximum file sizes of the various encryption features of the ESET Endpoint Encryption.

Feature	Maximum size
Full Disk Encryption	No ESET Endpoint Encryption limit; operating system, and hardware limits still apply.
Removable Media Encryption	No ESET Endpoint Encryption limit; operating system, and hardware limits still apply.
ESET Endpoint Encryption Go	Maximum size of 4GB per file by Microsoft WebDAV services.
File Encryption (.dlp files - file encryption, email attachments, ESET Endpoint Encryption Reader)	Maximum size of 3.99 GB.

Feature	Maximum size
Text and Clipboard Encryption	Maximum size of 3.99 GB, additional limits by text container.
Archives (.dpk files)	Maximum size of 4 GB, the maximum size of individual files within archive is 2 GB.
Virtual Disks (.mnt, .dlpvdisk)	Maximum size of 2 TB on NTFS/exFAT drives, 4GB on FAT32.
Folder Encryption	No ESET Endpoint Encryption limit; operating system, and hardware limits still apply.

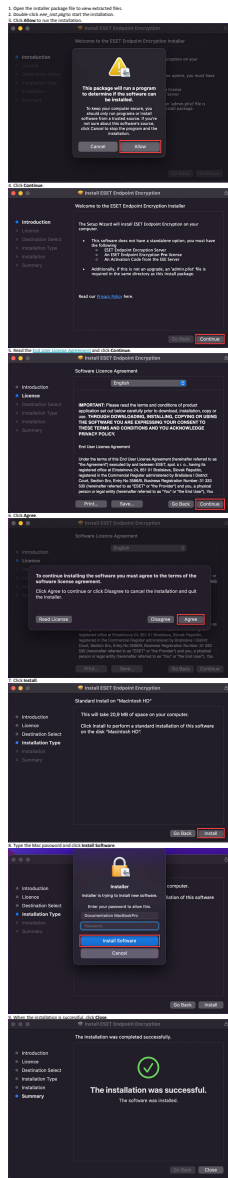
Install ESET Endpoint Encryption Client

Typically, your administrator has already installed ESET Endpoint Encryption Client for you. If not, they will provide you with an install package generated from your organization and give you sufficient privileges to install the software.



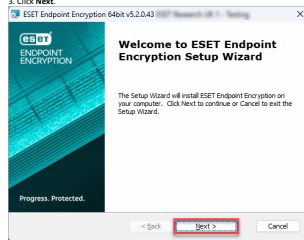
- You need administrative rights on your computer to complete installation.
- Restart the system after you complete installation.

 [Installation on macOS](#)

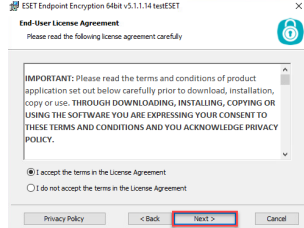


Installation on Windows

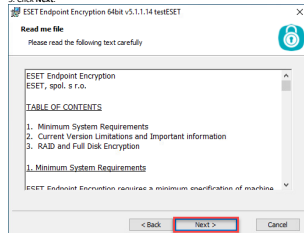
1. Locate the install package from your administrator.
2. Double-click the install package to run the installation.
3. Click Next.



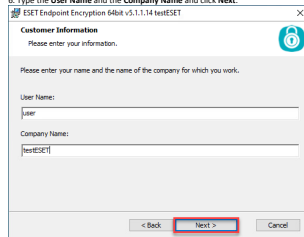
4. Read the [End User License Agreement](#), select **I accept the terms in the License Agreement** and click Next.



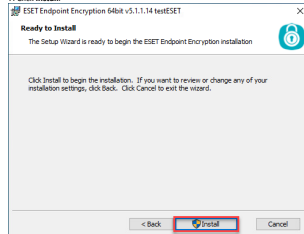
5. Click Next.



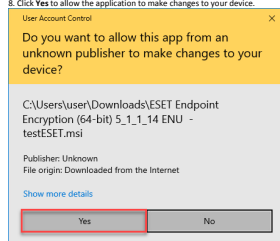
6. Type the User Name and the Company Name and click Next.



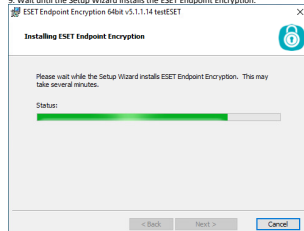
7. Click Install.



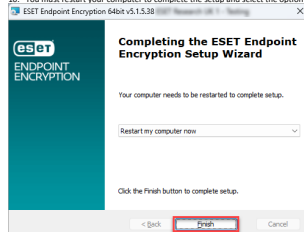
8. Click Yes to allow the application to make changes to your device.



9. Wait until the Setup Wizard installs the ESET Endpoint Encryption.



10. You must restart your computer to complete the setup and select the option when to restart the computer. Click Finish.

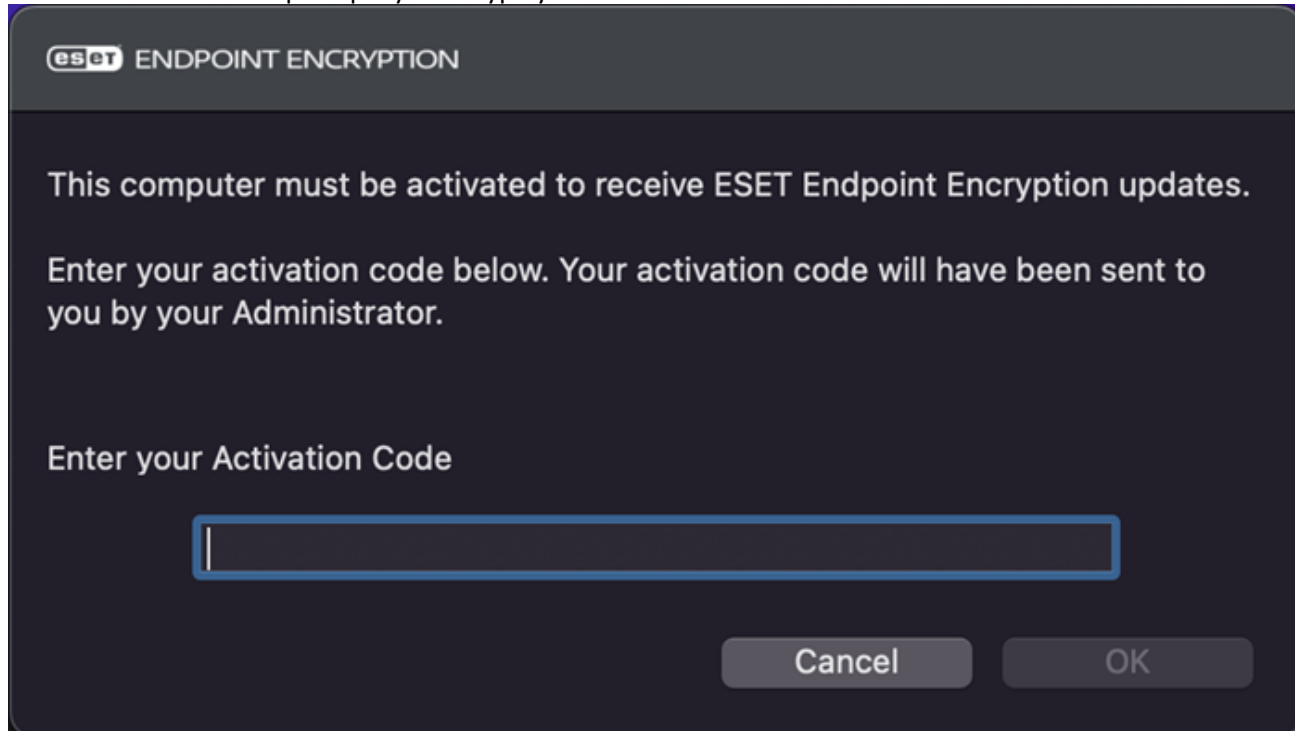


Activate ESET Endpoint Encryption Client

 You need an activation code from the administrator to activate ESET Endpoint Encryption Client.

[Activation on macOS](#)

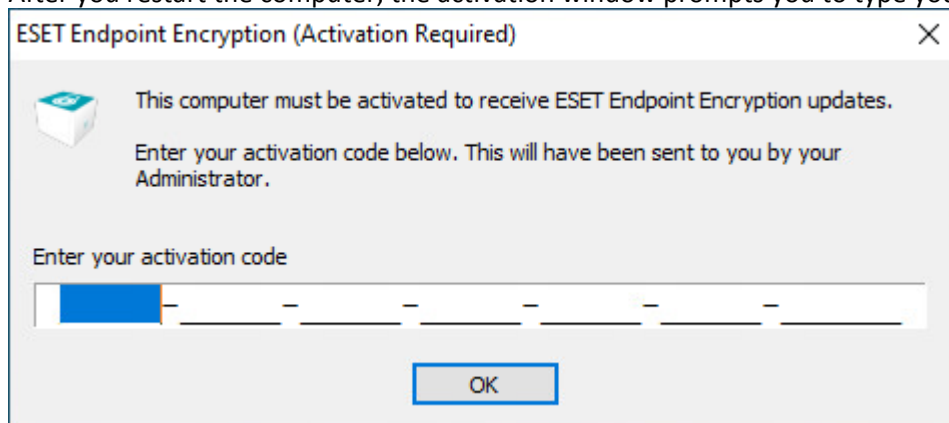
The activation window prompts you to type your activation code when the installation is successful.



Type or copy the activation code you received from the administrator and click **OK**.

[Activation on Windows](#)

After you restart the computer, the activation window prompts you to type your activation code.



Type or copy the activation code you received from the administrator and click **OK**.

Activate ESET Endpoint Encryption via email

In the email you received from your administrator:

Click **Activate ESET Endpoint Encryption**.

Product Activation



ESET Endpoint Encryption Pro

Your Systems Administrator has sent this activation for your PC.

Activate ESET Endpoint Encryption

Click on the button to activate ESET Endpoint Encryption on your systems.



Problems activating?

If your Email client has blocked the activation button, open the attached activation file.

Alternatively you can enter the activation code into the ESET Endpoint Encryption activation window:

66C9R- [REDACTED] 1QNPPD

Don't have ESET Endpoint Encryption installed?

Please ask your Administrator for a copy of ESET Endpoint Encryption.

i Alternatively, type the activation code into the activation window.

Initiate Full Disk Encryption

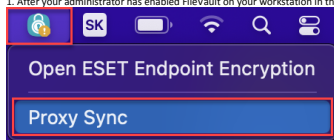
ESET Endpoint Encryption Full Disk Encryption enables encrypting an entire disk, disks, or selected partitions using 256-bit AES encryption. Pre-Boot authentication is required to gain access to the machine.



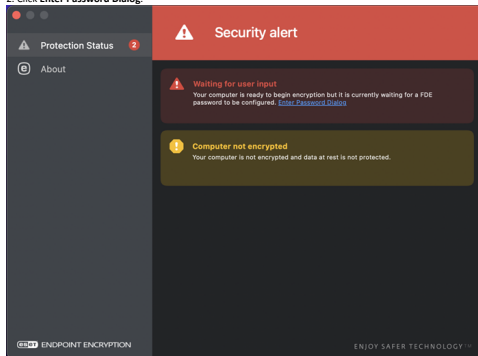
Managed users (you) are under administrative control. By default, the ESET Endpoint Encryption Server administrator sets Full Disk Encryption to run in a managed administrative mode. The administrator can specify settings for individual machines, including default passwords, and securely delegate the encryption process to the users if required.

[Initiation on macOS](#)

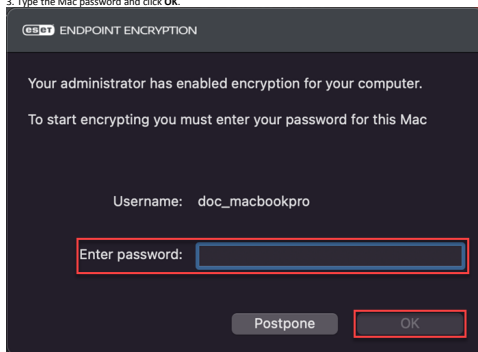
1. After your administrator has enabled FileVault on your workstation in the ESET Endpoint Encryption Server, click the ESET Endpoint Encryption icon and click **Proxy Sync**.



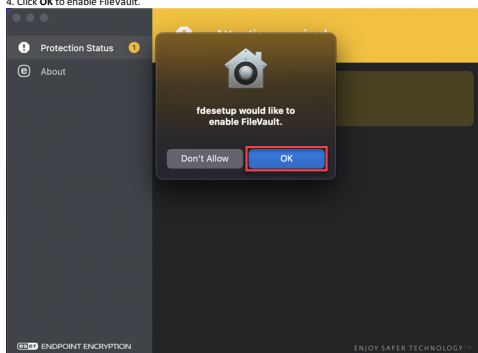
2. Click **Enter Password Dialog**.



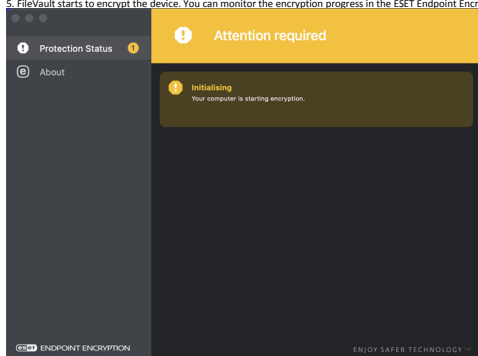
3. Type the Mac password and click **OK**.



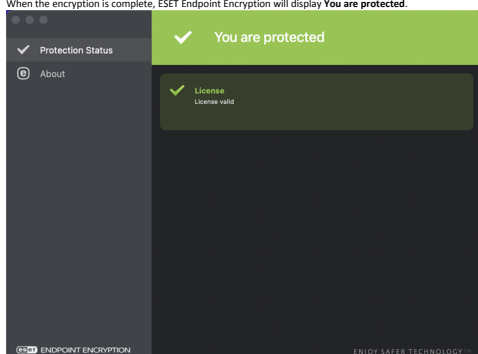
4. Click **OK** to enable FileVault.



5. FileVault starts to encrypt the device. You can monitor the encryption progress in the ESET Endpoint Encryption window.




When the encryption is complete, ESET Endpoint Encryption will display **You are protected**.



Initiation on Windows


1. Type and confirm a pre-boot password.


ESET Endpoint Encryption Deployment Client - Set pre-boot password

 **IMPORTANT: This workstation is changing to use pre-boot users.**

Once changed, you will be required to enter a user name and password whenever you start the computer.

You should note the user name below and then choose your own password. The user name can be changed later by asking your systems administrator.

 **Without the correct user name and password you will be unable to start your computer.**

 New pre-boot user name being added is: **user**

Please create your pre-boot password now


••••••••


Confirm Password:

••••••••

Keyboard United States-International Show typing ☐

Password Policy - hover for details



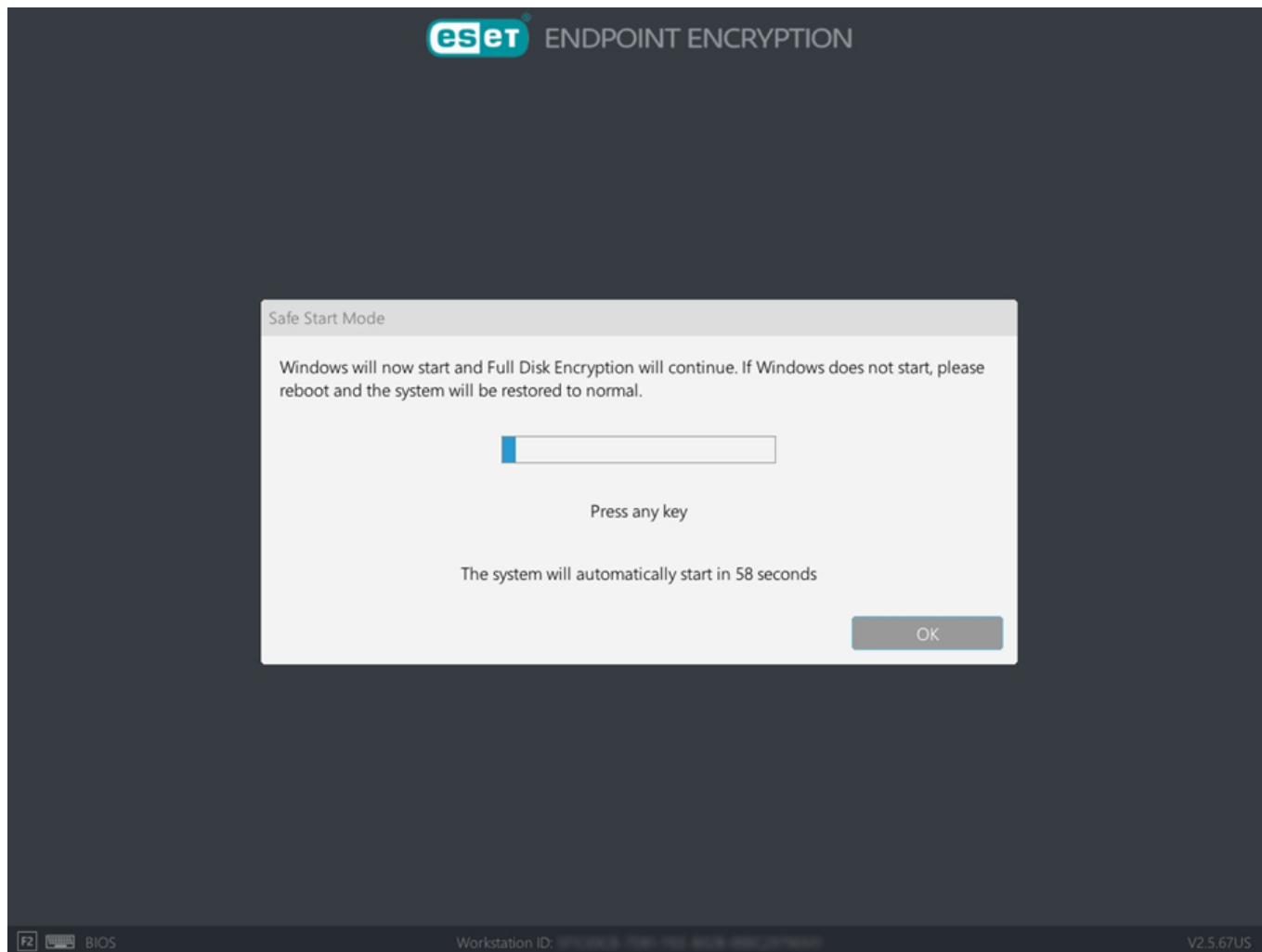
 The password logs you in to ESET Endpoint Encryption Client and encrypts your [Key File](#). The password you create must conform to the password policy defined by your administrator.

2. Click **OK**.

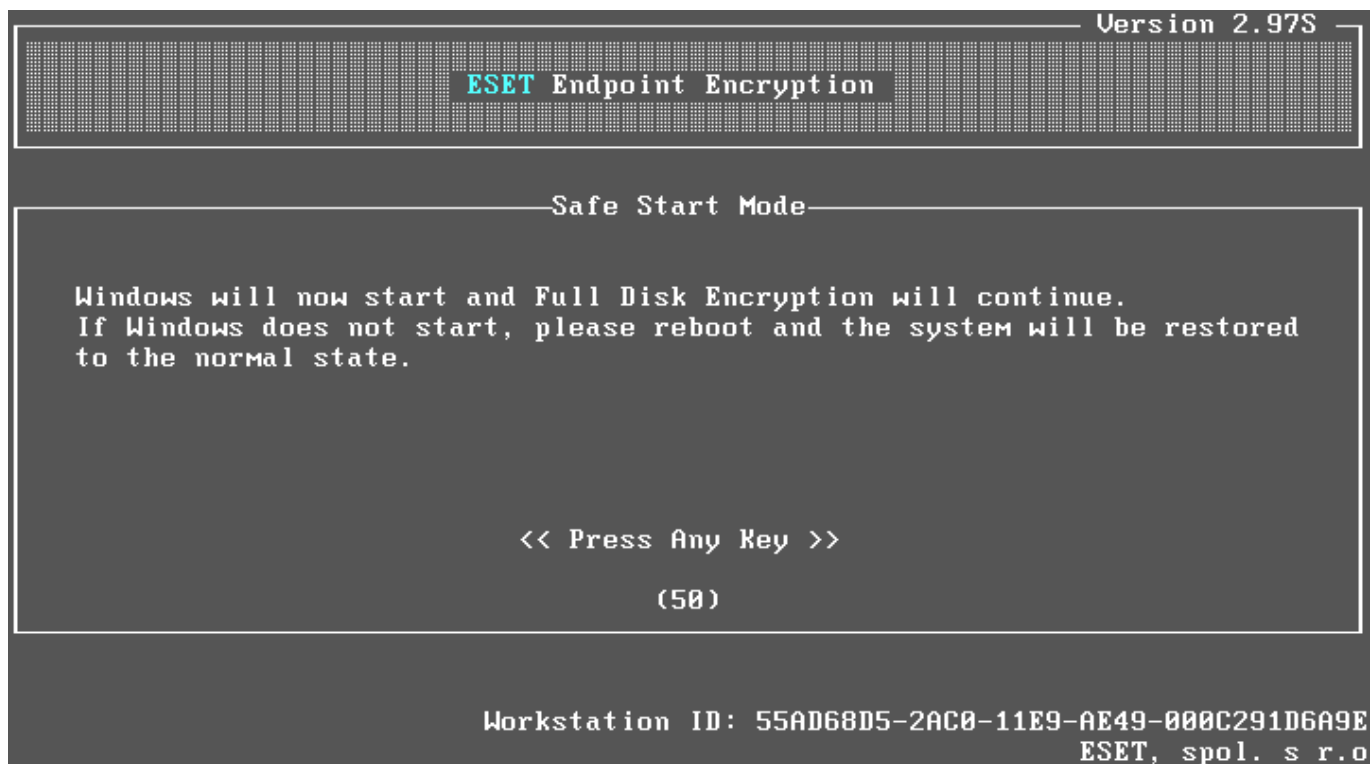
A message appears above the ESET Endpoint Encryption icon to confirm that the software is now licensed and all software features and encryption security policies are fully configured.

Safe Start

Safe Start is a pre-encryption test to ensure your machine successfully starts when encrypted. ESET Endpoint Encryption will install the Full Disk Encryption MBR bootloader and use it to start Windows before any disk encryption occurs. Under normal circumstances, Safe Start initiates, and your PC will restart, displaying the following screen:



Alternatively, on a workstation using a Legacy BIOS, Safe Start may appear as below:




Safe Start ensures the machine is fully supported and enables encryption with ESET Endpoint Encryption Full Disk Encryption. A machine may be incompatible with Full Disk Encryption utilities for several reasons, including

different disk controller types, such as RAID, or any third-party drivers that may be installed.

If the machine is incompatible and fails to start, Safe Start will attempt to repair the problem and log back in to Windows automatically. If Safe Start cannot automatically repair the problem, system repair can restore the machine because it is not encrypted.

The actual encryption operation will only proceed if Safe Start detects no issues. Safe Start guarantees the safety of your machine and any data on it because Full Disk Encryption only occurs when Safe Start has determined that your machine can start safely with the ESET Endpoint Encryption bootloader.

Single Sign-on

 The following feature is only available in Windows.

Single Sign-on (SSO) enables the Full Disk Encryption pre-start login to log the user directly in to their Windows profile.




The encryption password automatically re-synchronizes with the Windows password when the Windows password is changed.

The workstation must be joined to a Windows domain to use SSO. However, the actual account used can either be a domain account or a local machine account.

You receive the request to enable SSO:

1. A notification displays to confirm the user's Windows login password.
2. Type the Windows password and click **Verify**.

Single Sign On Settings ✕

 Your administrator has enabled single sign on for this pre-boot user. Please provide your Windows network logon details.

Pre-Boot Username:

Domain:


Network Username:


Network Password:

Keyboard: United Kingdom

3. When the verification is successful, click **OK** to configure the login to use SSO.

TPM PIN


 The following feature is only available in Windows.


 TPM PIN mode provides a single method of authentication—a numeric PIN. You can only start the computer when you know the PIN. However, you can change the PIN.

After [Safe Start](#), create your pre-boot PIN:

1. Type and confirm the pre-boot PIN, and click **OK**.

ESET Endpoint Encryption Full Disk Encryption

 **IMPORTANT: Full disk encryption for this workstation is being remotely started by your administrator.**
Once started, you will be required to enter a PIN code whenever you start the computer.
The PIN code must be at least 4 digits long.

 **Without the correct PIN you will be unable to start your computer.**

Please create your pre-boot PIN now

••••

Confirm PIN

••••|

Keyboard US Show typing ☐

2. The disk encryption process starts.

Disk Encryption Status

Disk Number	Status
Disk 0	Encrypted 740MB of 40311MB. 1% complete.

A disk encryption operation is currently in progress.
Encrypted 740MB of 40311MB. 1% complete.

Estimated completion time: 7:03:25 AM (11 minutes)

3. After restarting, type the PIN code and press **Enter** to confirm the **OK** button.

PIN

Enter your PIN to start the system.

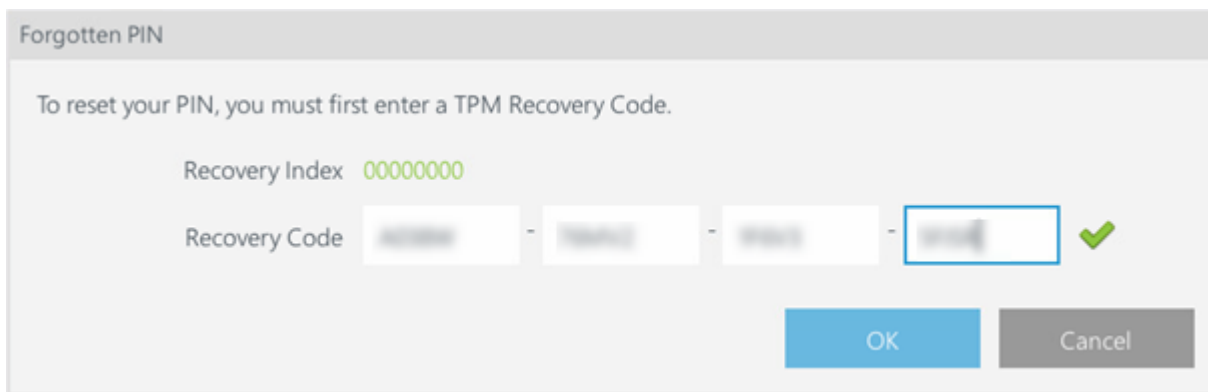
* * * * |

If you have forgotten your PIN press F1 or choose Forgot PIN

PIN Reset

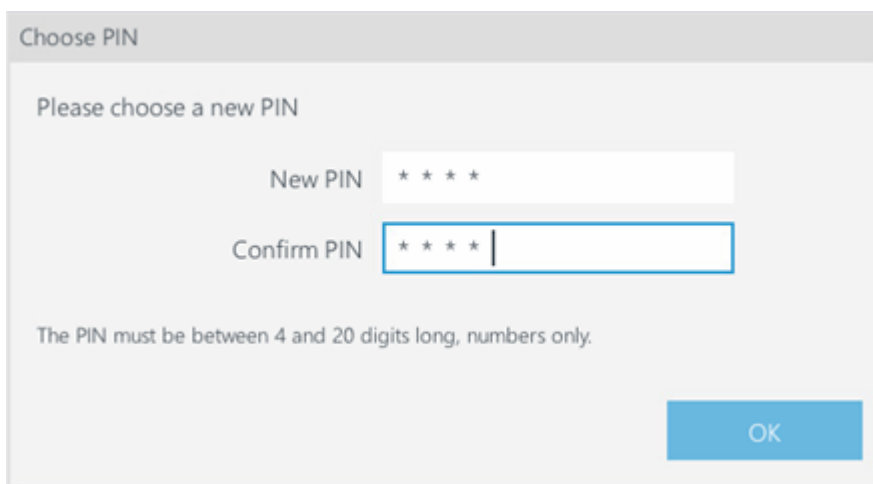
You must reset the PIN if you forget or incorrectly type Full Disk Encryption PIN too many times.

1. Press the **F1** key on the keyboard at the pre-boot login to access the recovery section.
2. Type the **Recovery Code** you received from your administrator.



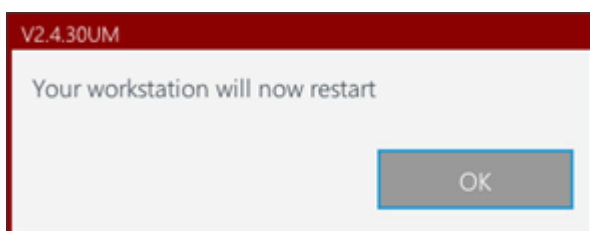
A dialog box titled "Forgotten PIN". It contains the text "To reset your PIN, you must first enter a TPM Recovery Code." Below this, there is a "Recovery Index" field showing "00000000". The "Recovery Code" field is divided into four boxes, each containing a digit (0, 0, 0, 0), with a green checkmark to the right. At the bottom right, there are "OK" and "Cancel" buttons.

3. Type and confirm the **New PIN** and click **OK**.



A dialog box titled "Choose PIN". It contains the text "Please choose a new PIN". Below this, there are two input fields: "New PIN" and "Confirm PIN". Both fields contain four asterisks. At the bottom right, there is an "OK" button.

4. Click **OK**. The workstation will restart and you can use your new PIN code.

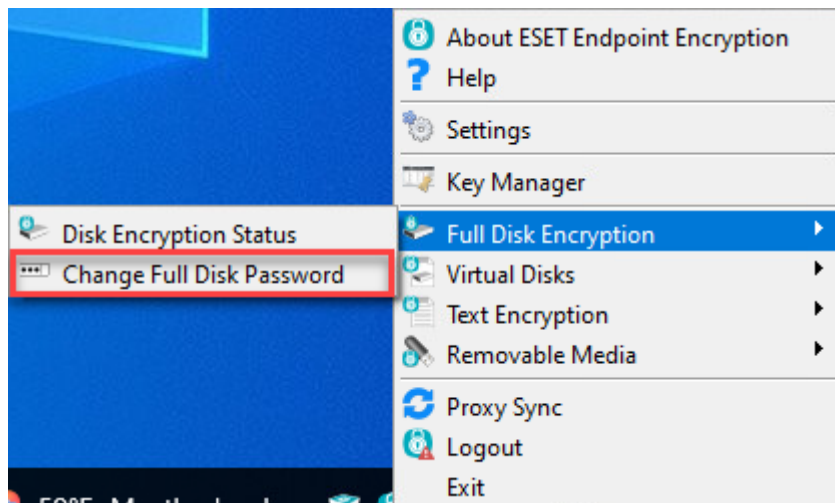


A message box with a red border. It contains the text "V2.4.30UM" in the top left corner and "Your workstation will now restart" in the center. At the bottom right, there is an "OK" button.

Change encryption password

i The following feature is only available in Windows.

1. Right-click the icon ESET Endpoint Encryption, select **Full Disk Encryption** and click **Change Full Disk Password**.



2. Type your original password, new password and retype your new password to confirm it.

Password policy

As you type, the progress bar turns from red to green, indicating the progress toward meeting the password requirements. The password meets the password policy when the progress bar is completed and green.

When you hover the mouse pointer over the Password Policy bar, a tooltip dialog shows the details of the policy requirements and which of those requirements have been reached by the current entry (it displays **OK** below the requirements that have been met).

3. Click **Change**.

4. Restart your computer and type your new password.



Single Sign-On requires your Windows password to be updated on your computer. See [Single Sign-On synchronization](#).

Recover encryption password



The following feature is only available in Windows.

1. Select **Reset Password (Lost details on Legacy systems)** from the menu.
2. Type the Full Disk Encryption username and click **OK**.

3. Provide the **Recovery Index** number displayed on the screen to your administrator.
4. You will receive a **Recovery Password** from your administrator. Type the **Recovery Password** and click **OK**.

Reset Password

A recovery password is required to continue, this will enable you to reset your login password.

Recovery Index 00000000

Recovery Password

OK Cancel

5. If you are not configured for [Single Sign-On](#), type the new FDE password for future use.

Password policy



The password policy affects the quality of generated recovery login passwords used when you forget your FDE password. You can see the password quality bar at the bottom of the **Password** field.

Reset Password

Please choose a new login password. You will not be able to start this workstation until a new password has been set that meets the password policy set out by your system administrator.

User bob

Password

Confirm Password

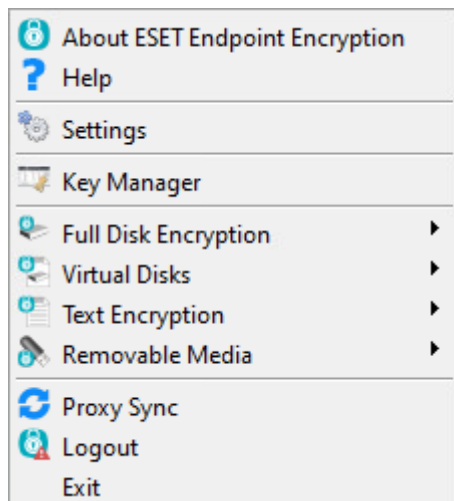
OK

You do not have to change the password if you are configured for [Single Sign-On](#). At the Windows login screen, type your domain password. When you log in successfully, ESET Endpoint Encryption automatically synchronizes with FDE and Windows passwords.

Encryption features

In managed installations, the list of available features in the context menu is controlled by the user's Group Policy as set by the ESET Endpoint Encryption Server Administrator.

Right-click the icon in the Windows notification area to access the notification menu. Depending on the installed version, a variation of the following menu appears:



Removable Media Encryption

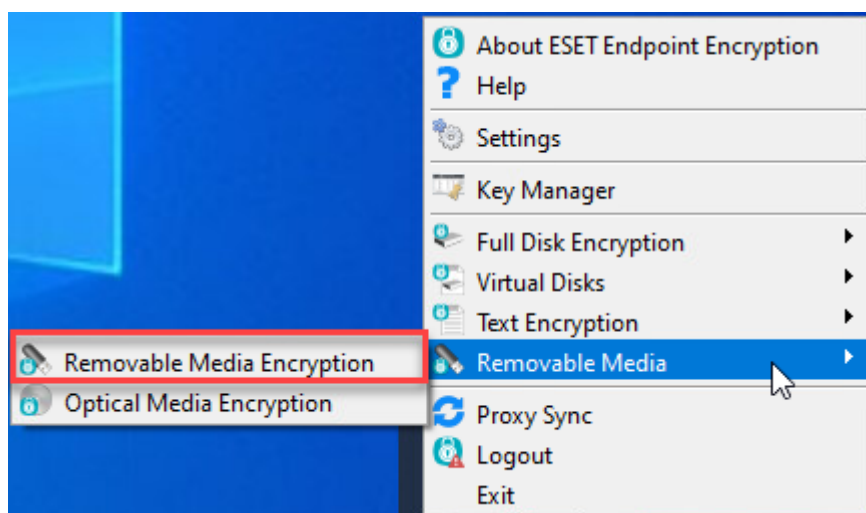
i The following feature is only available in Windows.

You can fully encrypt removable media (USB, HDD, USB memory sticks) or encrypt files on removable media.

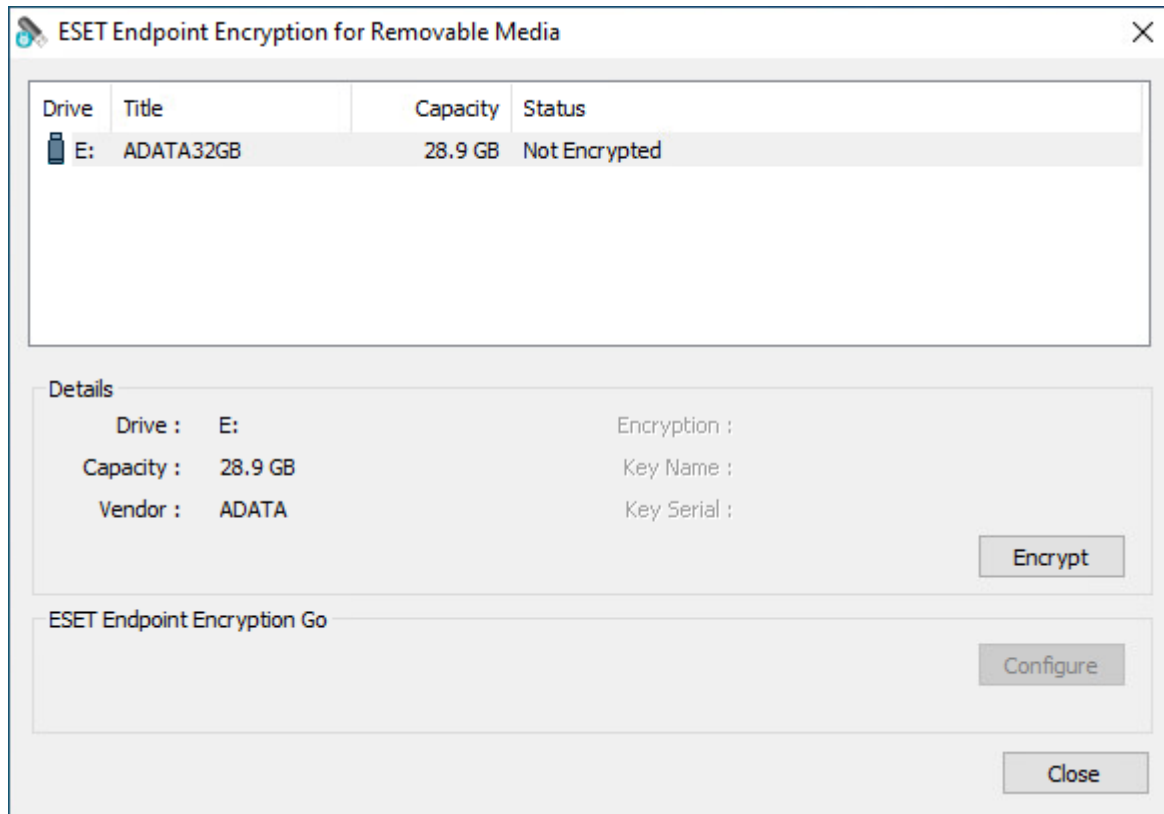
! Removable media can only be read or written if the workstation (managed in ESET Endpoint Encryption Server) **Removable Media machine policy** is set to **Open**.

Removable Media Encryption

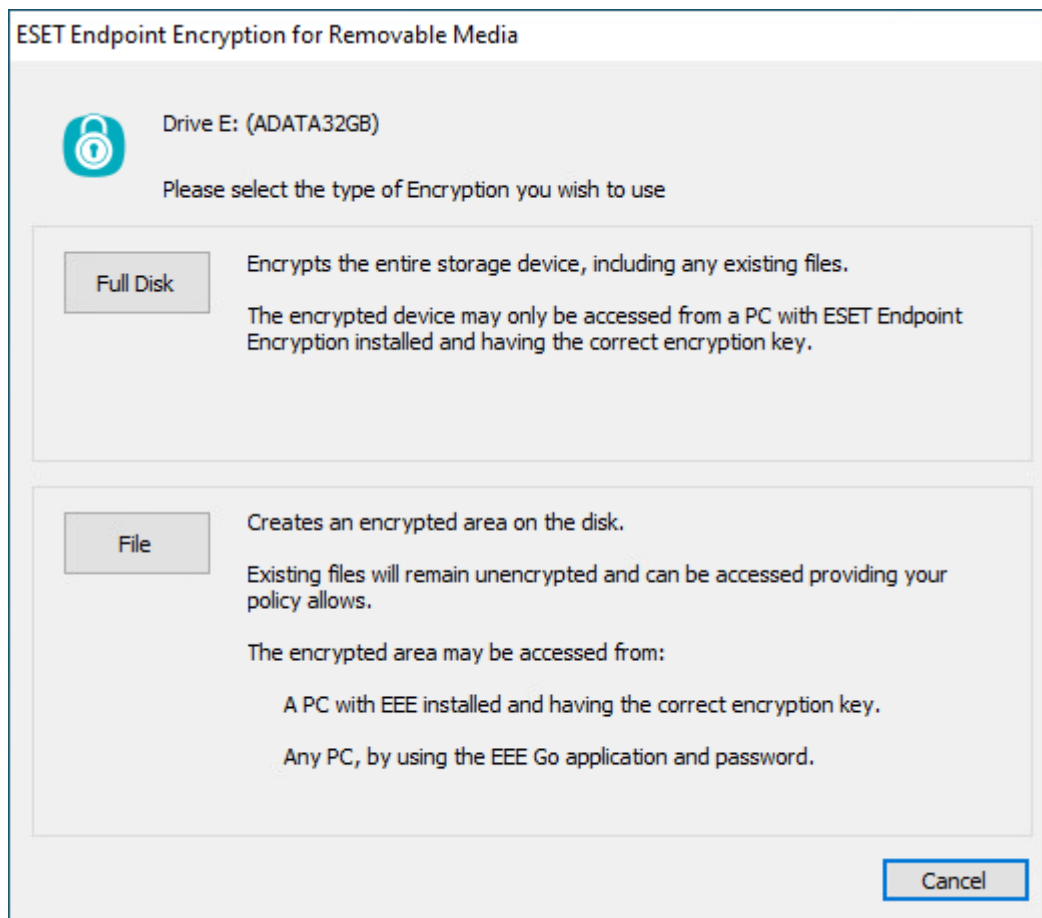
1. In the Windows notification area, right-click the icon ESET Endpoint Encryption icon, select **Removable Media** and click **Removable Media Encryption**.



2. Select the device to encrypt and click **Encrypt**.



3. Select the type of encryption: **Full Disk** or **File**.



4. Select an encryption key and click **OK**.

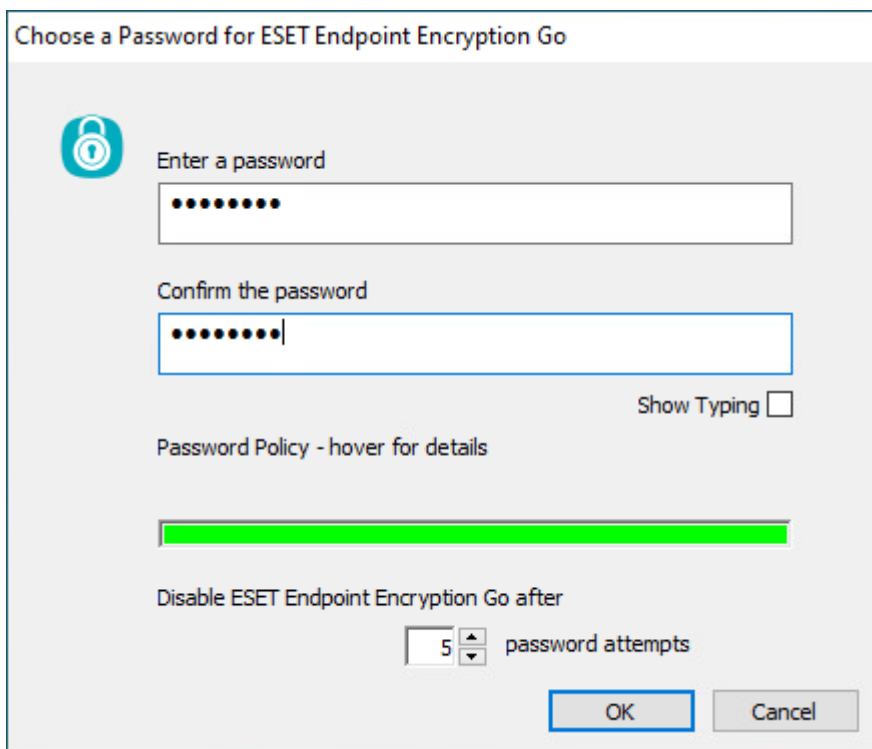
! If only one encryption key exists, it is selected by default.

5. Based on your encryption type selection:

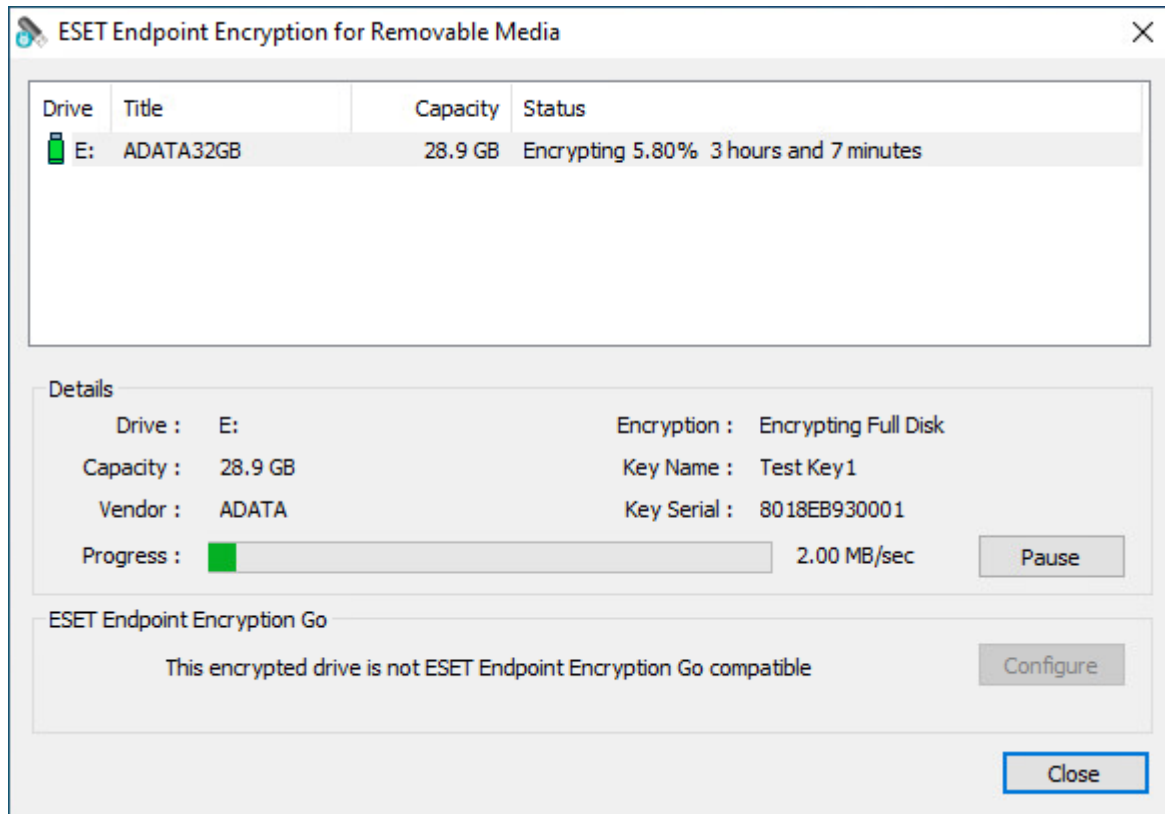
- If you selected **File**, click **Yes** to enable the **ESET Endpoint Encryption Go** feature.



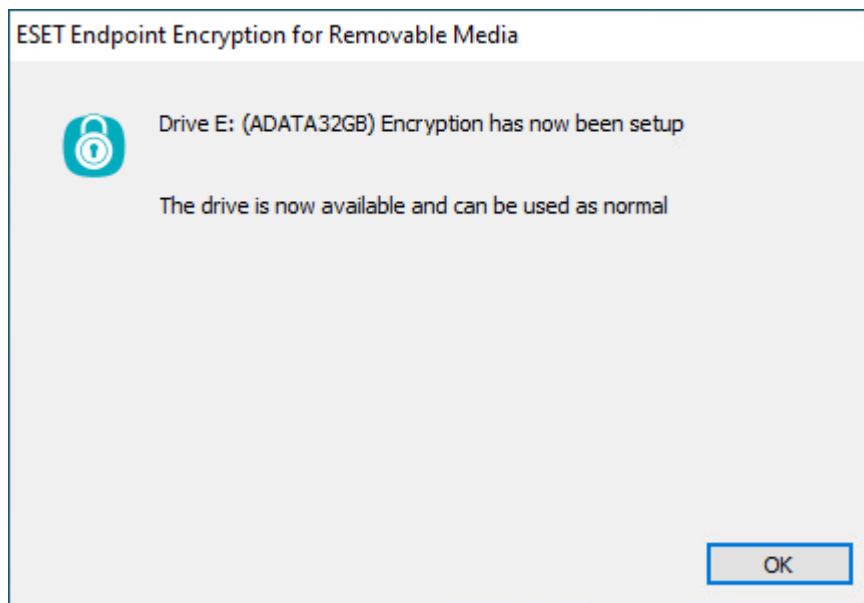
➤ If you selected to enable **ESET Endpoint Encryption Go**, type and confirm a password and click **OK**.



- If you selected **Full Disk**, click **Yes**. The window displays the encryption progress.

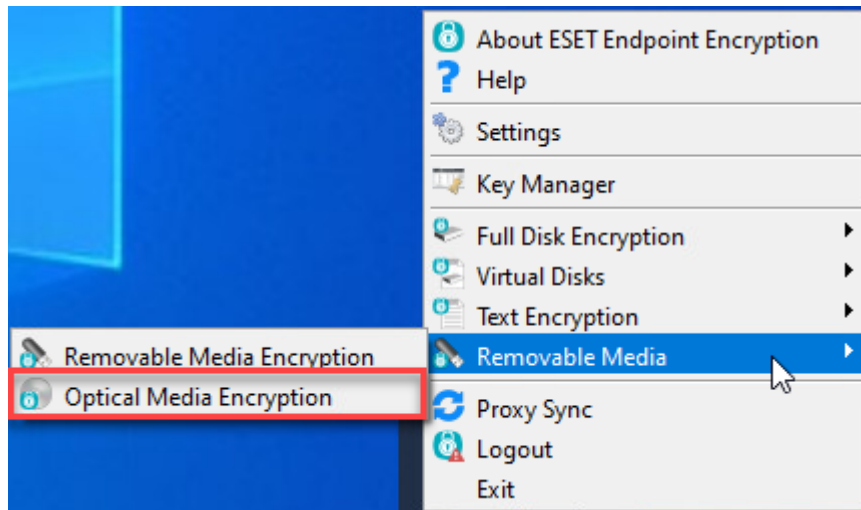


6. When the operation is complete, click **OK**.



Optical Media Encryption

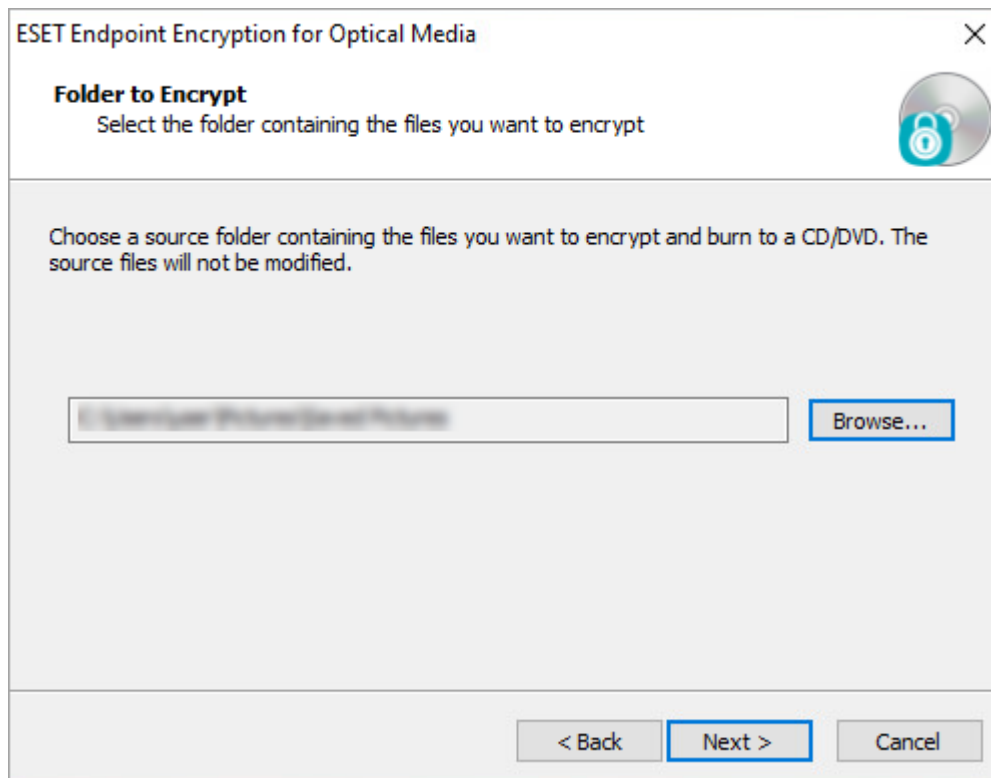
1. Right-click the ESET Endpoint Encryption icon, select **Removable Media** and click **Optical Media Encryption**.



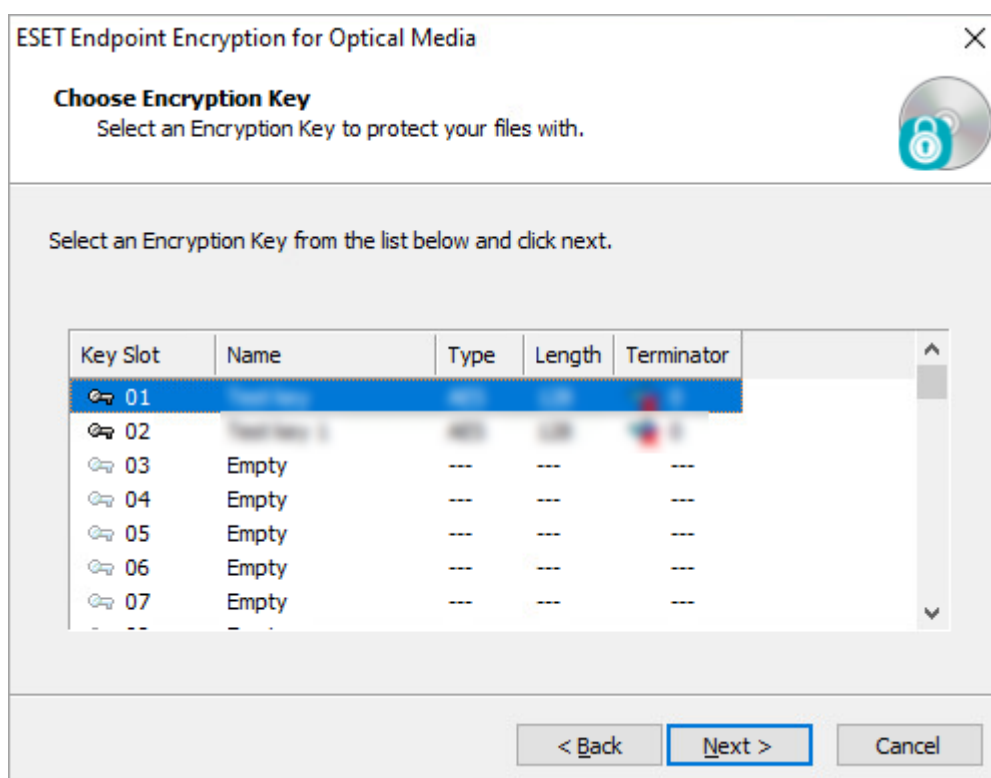
2. Click **Next**.



3. Click **Browse** to select the folder containing the files you want to encrypt and click **Next**.



4. Select an encryption key from the list and click **Next**.



5. If you want to enable **ESET Endpoint Encryption Go**, select **Enable ESET Endpoint Encryption Go** and create a password. Click **Next**.

ESET Endpoint Encryption for Optical Media

ESET Endpoint Encryption Go
Would you like to enable ESET Endpoint Encryption Go?

ESET Endpoint Encryption Go allows users without ESET Endpoint Encryption to access your encrypted data through the use of a password.

☒ Enable ESET Endpoint Encryption Go

●●●●●●●●

●●●●●●●●

Show Typing ☐

Password Policy - hover for details

< Back Next > Cancel

6. Click **Next** without selecting **Enable ESET Endpoint Encryption Go**.

ESET Endpoint Encryption for Optical Media

ESET Endpoint Encryption Go
Would you like to enable ESET Endpoint Encryption Go?

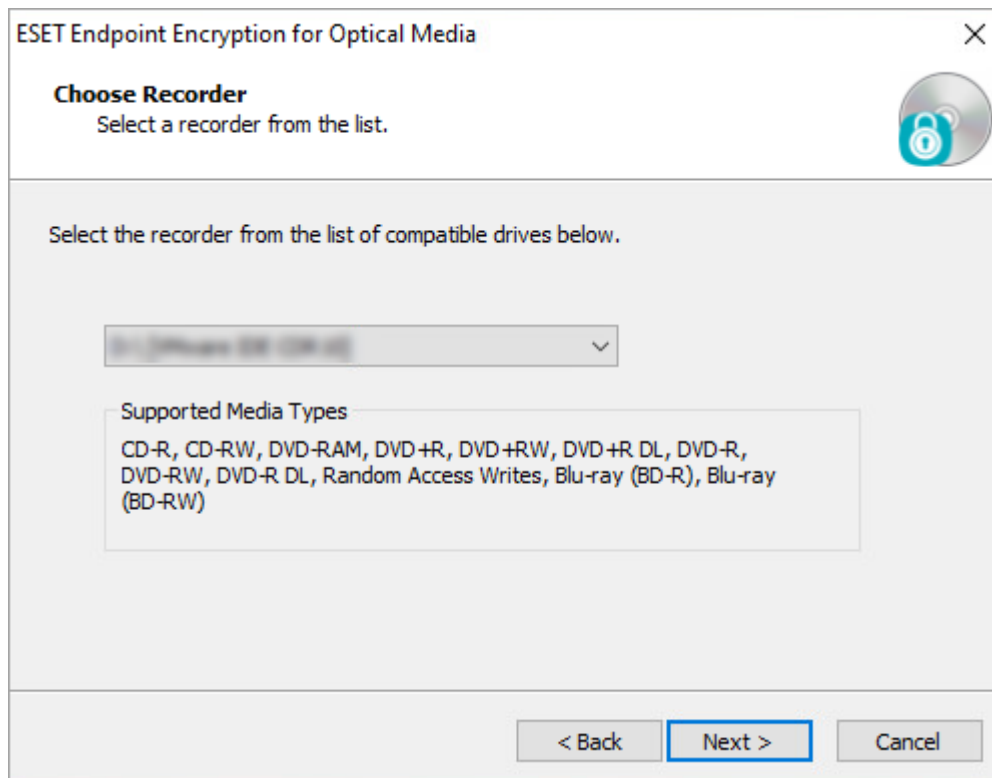
ESET Endpoint Encryption Go allows users without ESET Endpoint Encryption to access your encrypted data through the use of a password.

☐ Enable ESET Endpoint Encryption Go

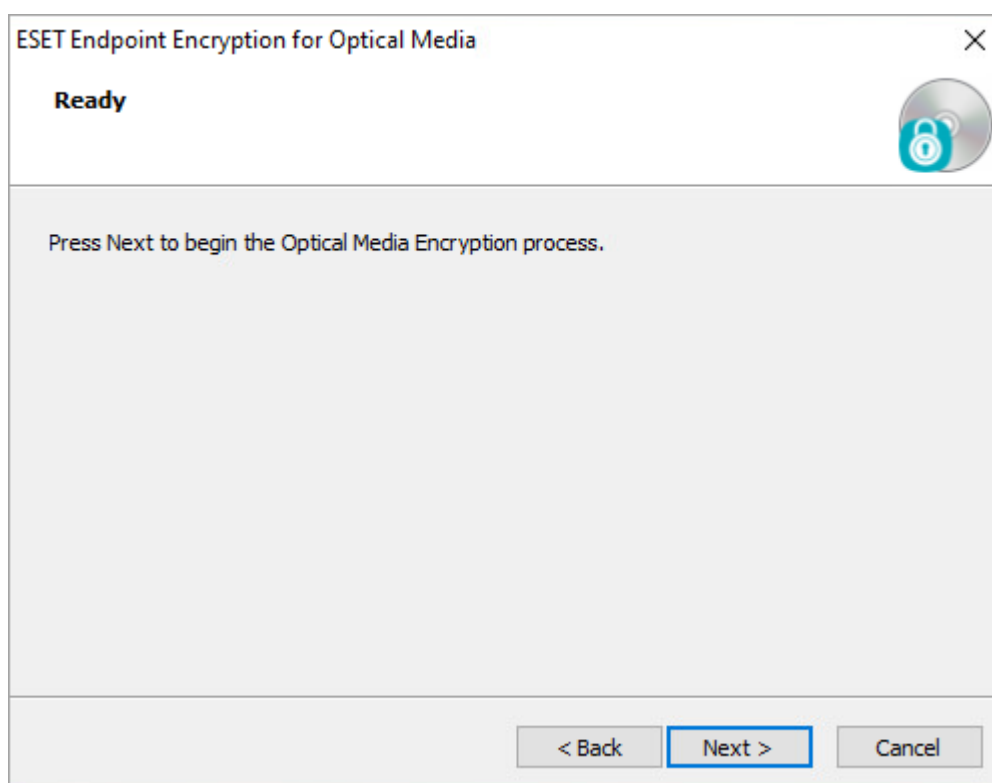
Show Typing ☐

< Back Next > Cancel

7. Select the recorder of compatible drives from the list and click **Next**.



8. Click **Next** to start the **Optical Media Encryption** process.



9. If necessary, insert a CD into the drive. The **Burning Disc** process begins.

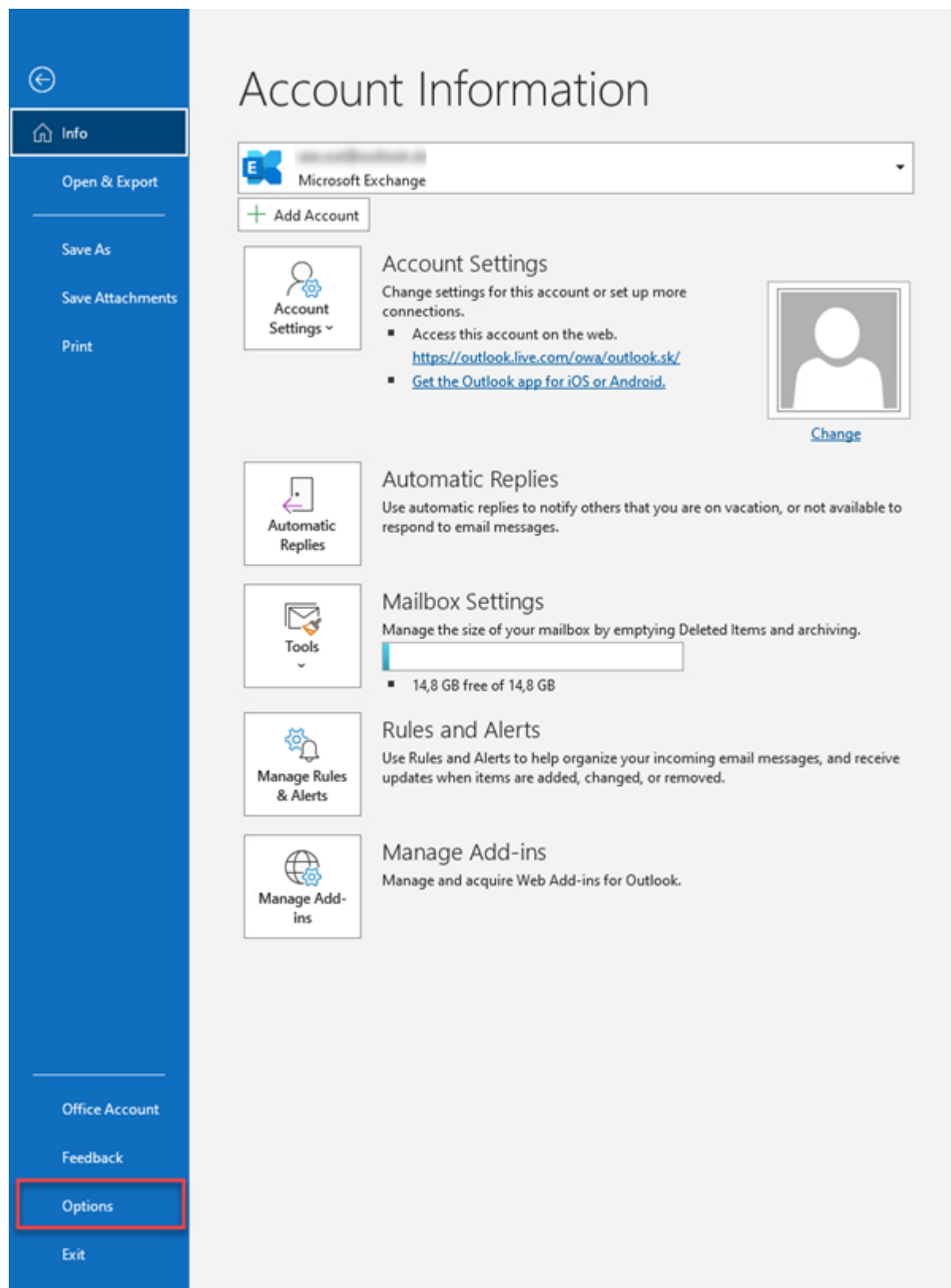
Email Encryption

i The following feature is only available in Windows.

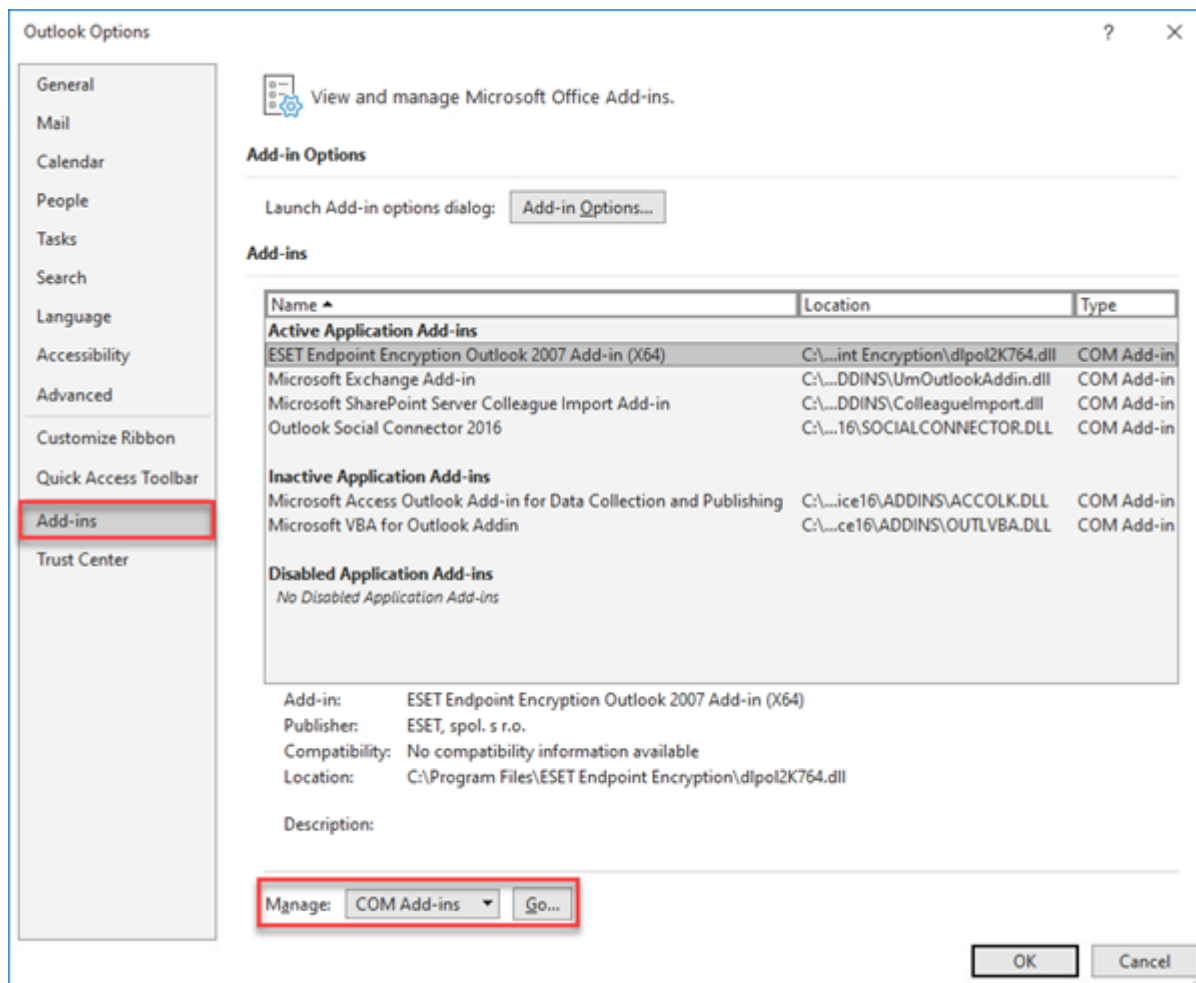
Within Microsoft Outlook, the ESET Endpoint Encryption tab allows users to send encrypted emails.

Verify that the ESET Endpoint Encryption Outlook is enabled:

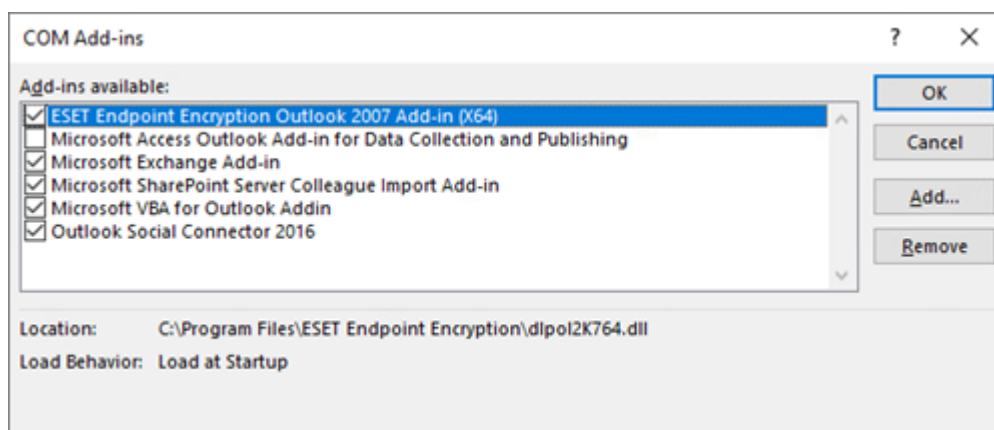
1. Open the Microsoft Outlook.
2. Click **File**.
3. Click **Options**.



4. Click **Add-ins**, select **COM Add-ins** from the drop-down menu and click **Go**.



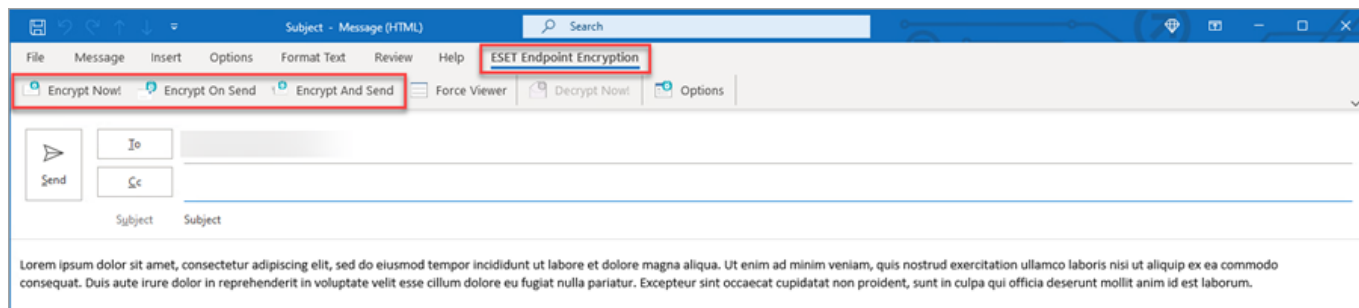
5. Select **ESET Endpoint Encryption Outlook Add-in** to enable the add-in and click **OK**. Optionally, click **Add** to view the available add-in options.



Emails can be completely encrypted or have either an encrypted body and plain text attachment or vice versa. Emails can be encrypted using an encryption key or password.

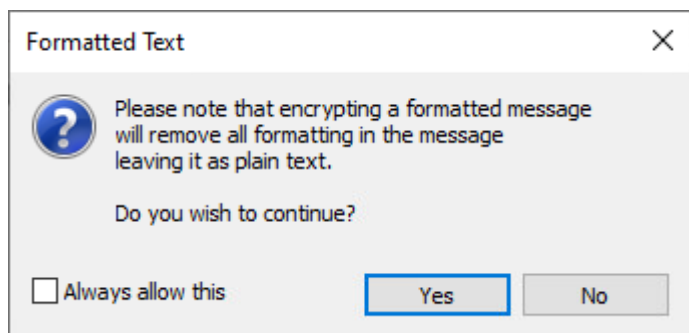
1. Open Microsoft Outlook and click **New Email**.

2. Type your email and click the **ESET Endpoint Encryption** tab. Select one of the three encryption options:



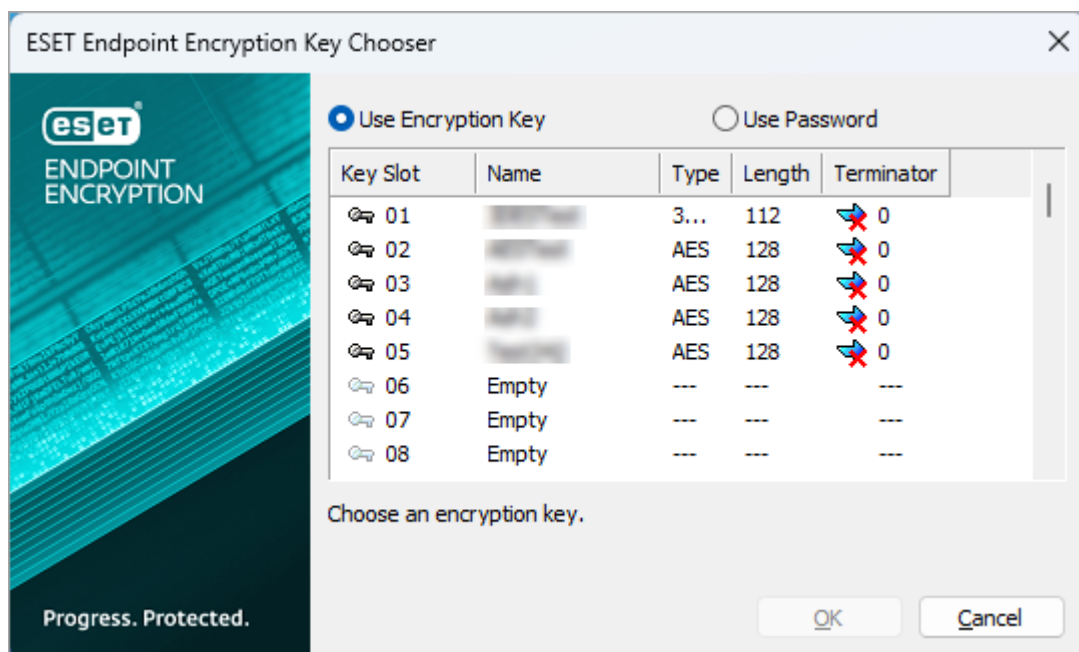
- Click **Encrypt Now!** to encrypt the email as is. For example, after you add an attachment, it will encrypt the attachment but any text typed afterward remains unencrypted.
- Click **Encrypt On Send** to enable sending the message as encrypted after you click **Send**.
- Click **Encrypt And Send** to combine the functionality of **Encrypt Now** and **Encrypt on Send**.

3. Click **Yes**.



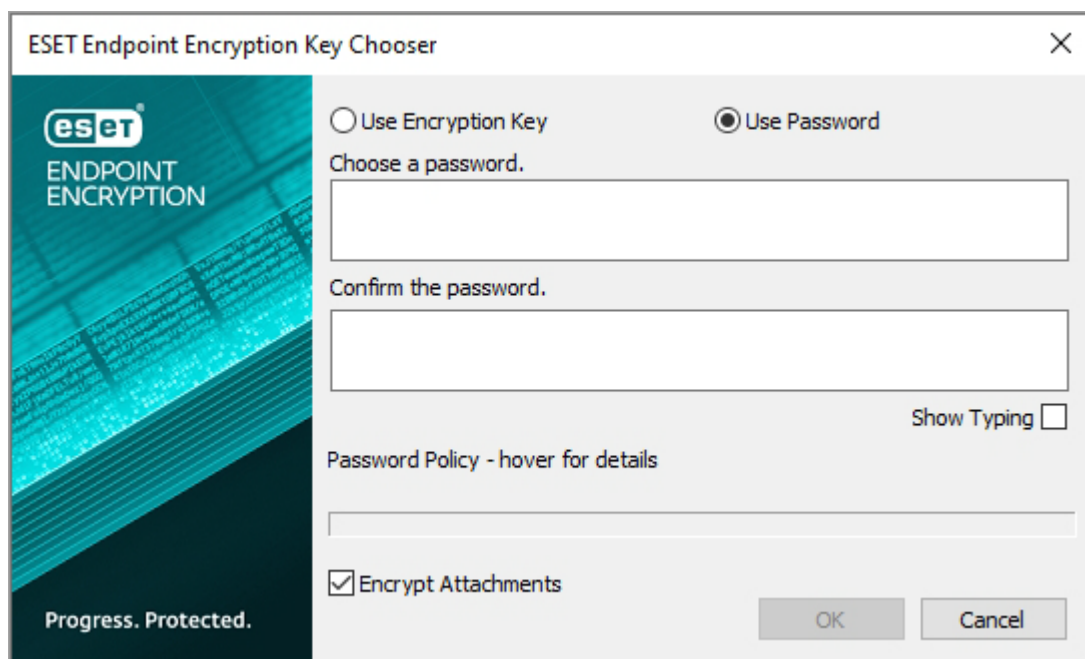
4. Select either **Use Encryption Key** or **Use Password** in the **ESET Endpoint Encryption Key Chooser** window.

- Select the **Use Encryption Key** option for email recipients with ESET Endpoint Encryption installed on their machine.



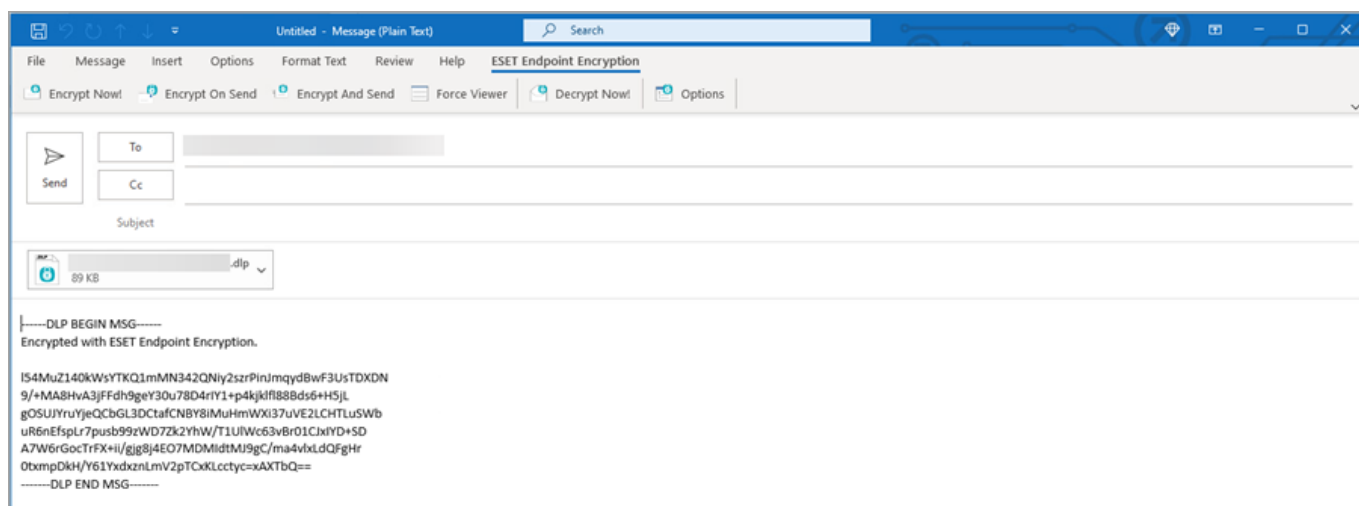
- Select the **Use Password** option for email recipients without ESET Endpoint Encryption installed on their machine. Type and confirm the password and click **OK**. We recommend sharing the password with the

recipient using an alternative communication method (other than email).



The dialog box is titled "ESET Endpoint Encryption Key Chooser". It features the ESET logo and "ENDPOINT ENCRYPTION" text on the left. On the right, there are two radio buttons: "Use Encryption Key" (unselected) and "Use Password" (selected). Below these are two text input fields labeled "Choose a password." and "Confirm the password.". A "Show Typing" checkbox is to the right of the second field. Below the fields is a "Password Policy - hover for details" label and another text input field. At the bottom left is a checked checkbox for "Encrypt Attachments". At the bottom right are "OK" and "Cancel" buttons.

5. Click **Send**.



The screenshot shows the Microsoft Outlook "Compose" window. The "ESET Endpoint Encryption" ribbon is active, showing buttons for "Encrypt Now!", "Encrypt On Send", "Encrypt And Send", "Force Viewer", "Decrypt Now!", and "Options". The "To" field is empty. Below the "To" field is a "Send" button. The "Subject" field is empty. Below the "Subject" field is a file attachment icon and the text "89 KB .dip". The body of the email contains a DLP BEGIN MSG header, followed by "Encrypted with ESET Endpoint Encryption.", and a large block of base64-encoded text. The body ends with a DLP END MSG footer.

The recipient can [decrypt](#) the email if they are within the same organization as the sender and share the an encryption key. You can set up Microsoft Outlook to automatically decrypt all received emails provided the recipient has access to the encryption key.

If the recipient of the encrypted email is not an ESET Endpoint Encryption customer, they can decrypt the email with the free [ESET Endpoint Encryption Reader](#).

To automatically decrypt email:

1. Click **ESET Endpoint Encryption** tab and select **Options**.
2. In the **Decrypting** section, select the checkbox next to **Automatically decrypt message text** and select preferred decryption option.
3. Click **Apply** and then **OK** to save changes.

ESET Endpoint Encryption Reader

The ESET Endpoint Encryption Reader utility is available for Windows and macOS and enables decryption of files or text encrypted using a password.

[ESET Endpoint Encryption Reader for Windows](#)

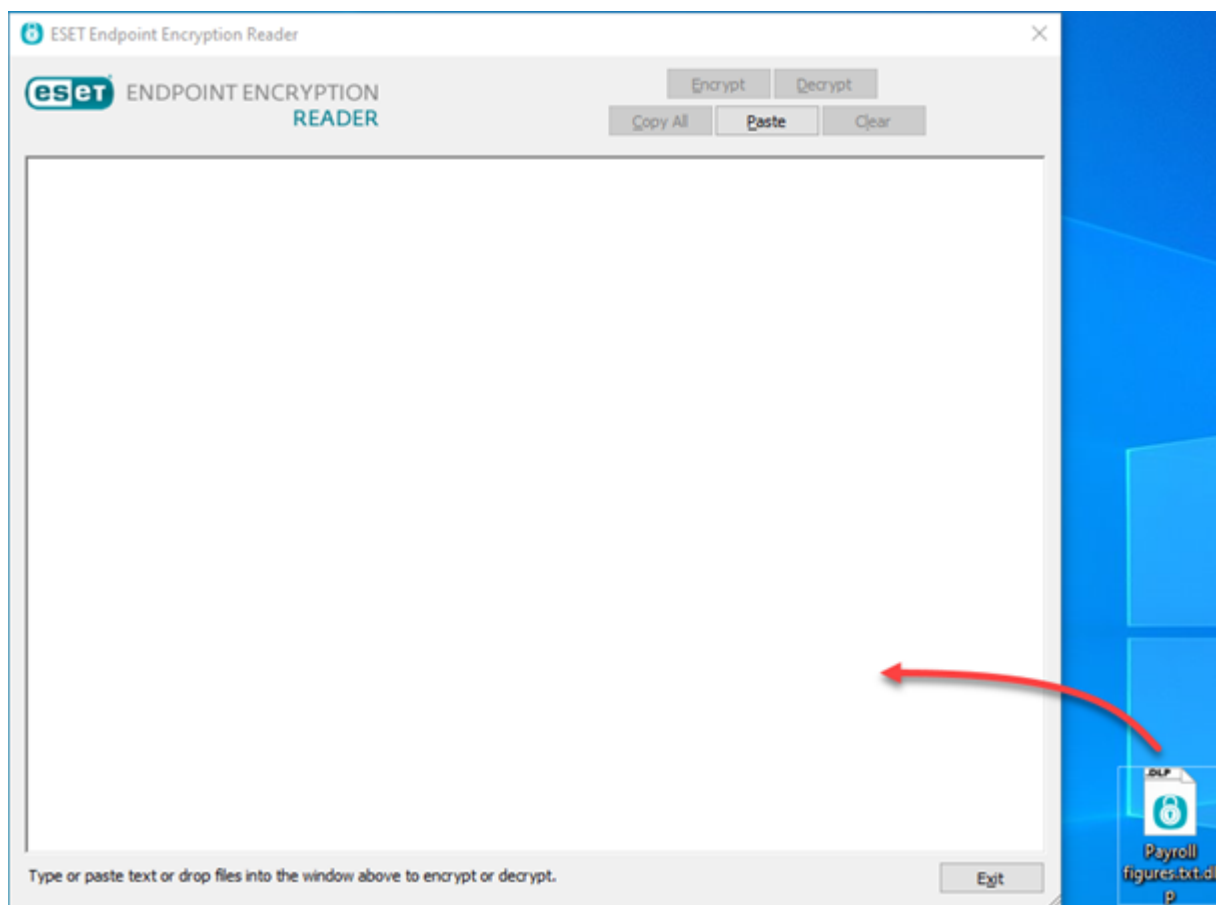
[ESET Endpoint Encryption Reader for macOS](#)

ESET Endpoint Encryption Reader for Windows

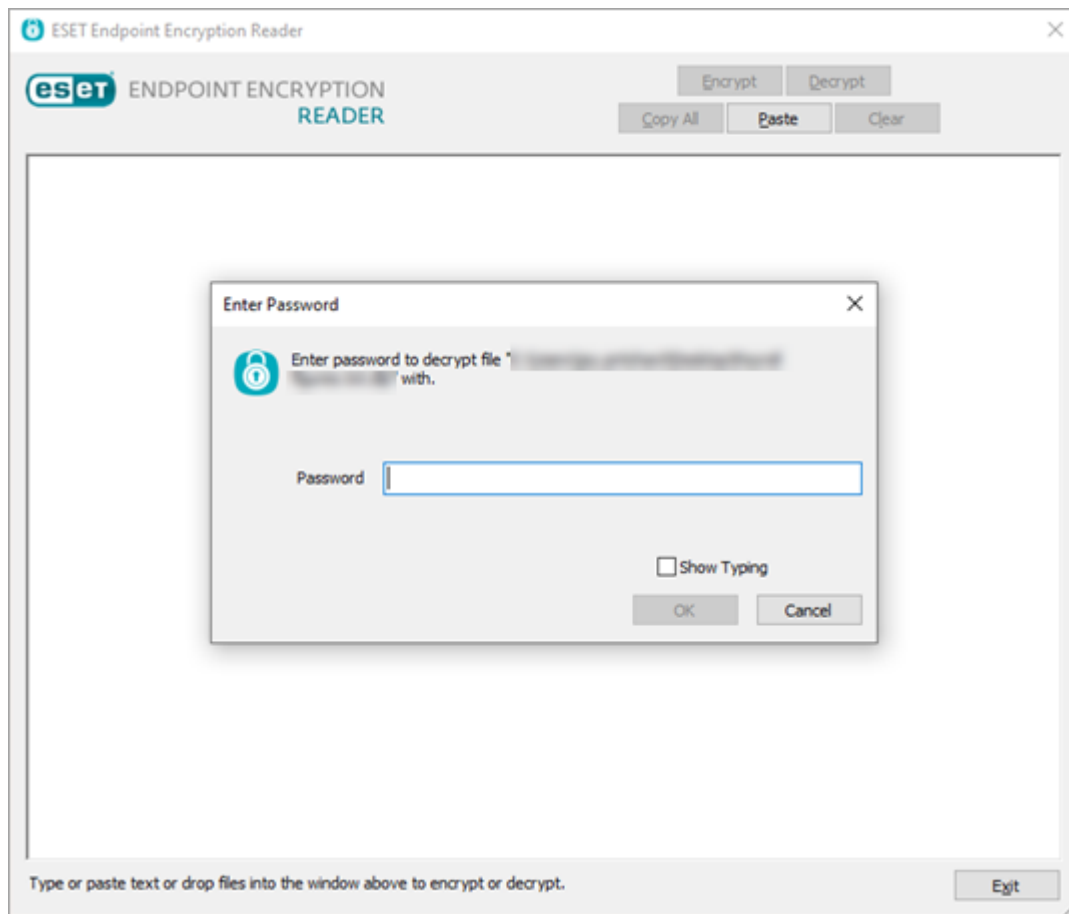
1. Download and install the [ESET Endpoint Encryption Reader](#).
2. Save it to your desktop.
3. Open the **ESET Endpoint Encryption Reader** to use the app.

Decrypt files

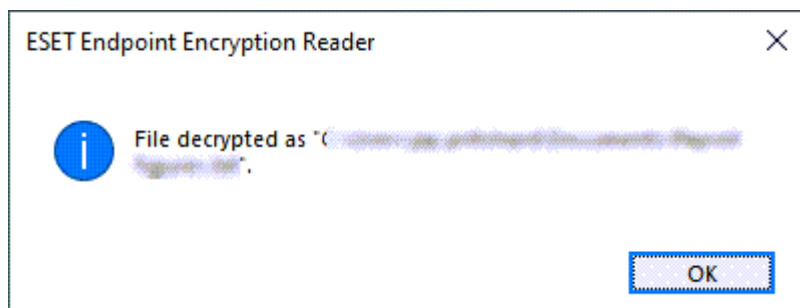
1. Drag-and-drop an encrypted file (.dlp file extension) to the **ESET Endpoint Encryption Reader**.



2. Click **Decrypt**.



3. Type the required password and click **OK** to complete the decryption.

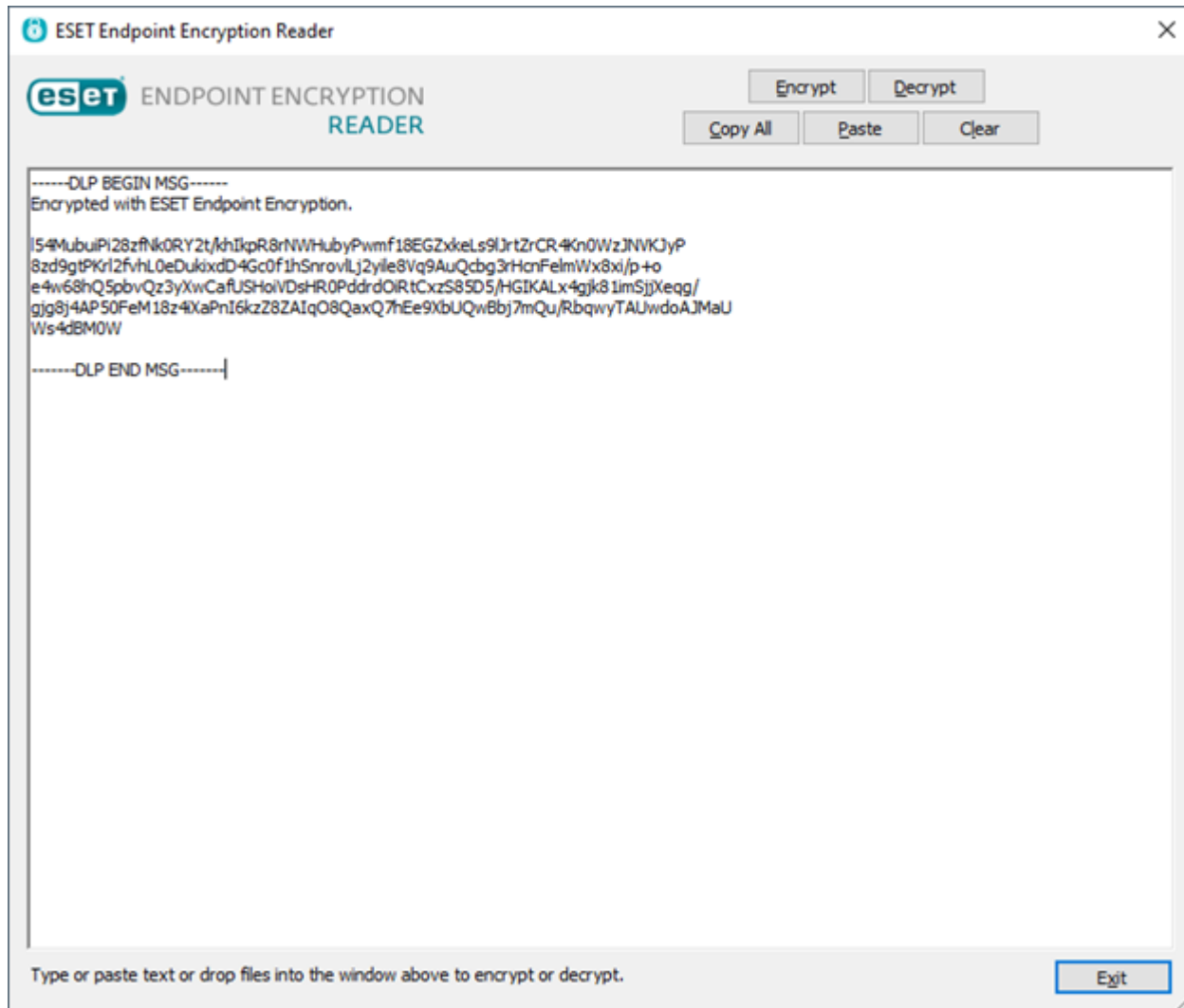


The decrypted file is saved in the same directory as the provided encrypted file.

Decrypt text

1. Copy/paste an encrypted message into the **ESET Endpoint Encryption Reader**.

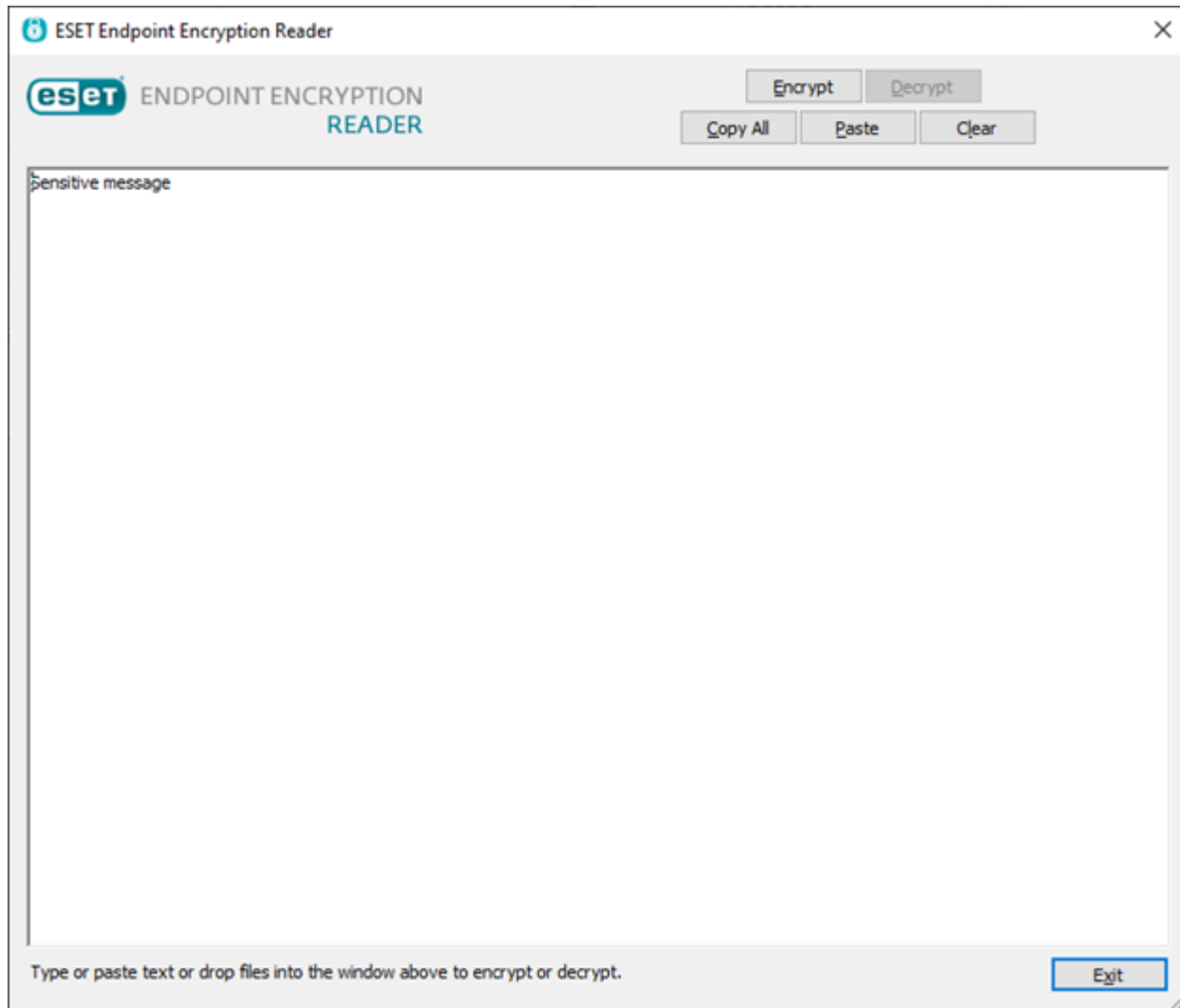
! Ensure you include **---DLP BEGIN MSG---** and **---DLP END MSG---** for the text to be recognized correctly.



2. Click **Decrypt**.

3. Type the required password and click **OK** to complete the decryption.

The decrypted text shows in the window.



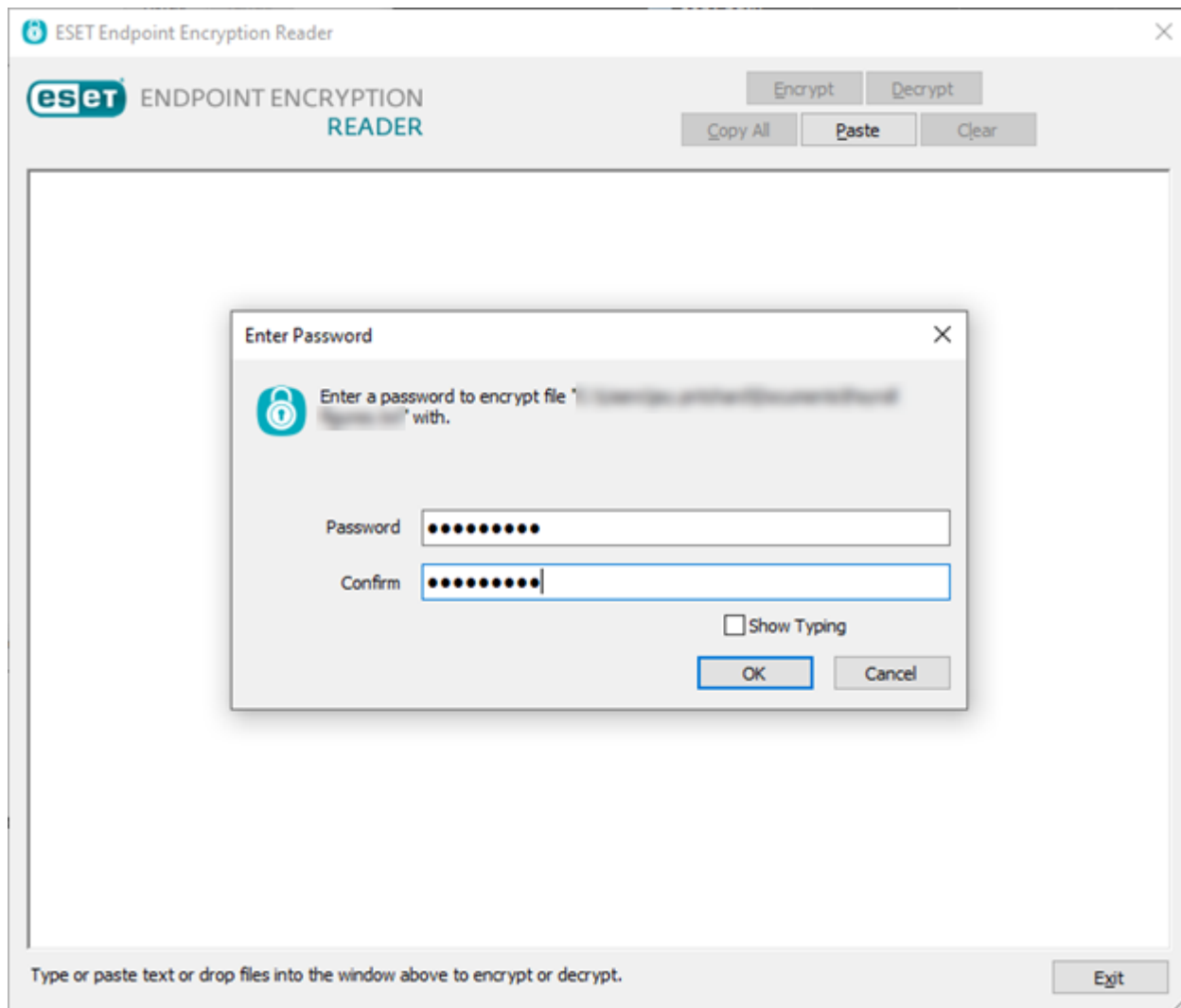
Troubleshooting



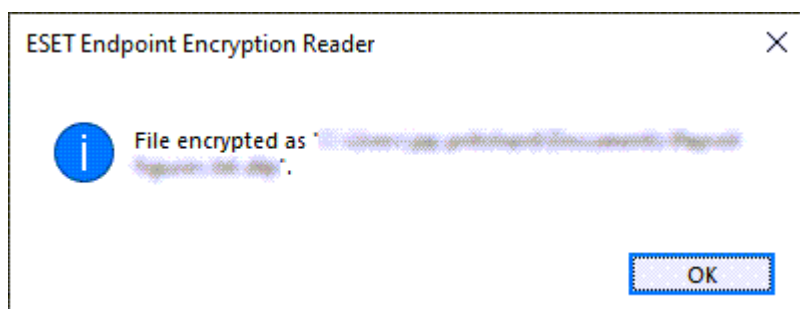
When you receive the error **The text could not be decrypted because it is not a supported or valid format**, [disable mobile device compatibility](#).

Encrypt files

1. Drag-and-drop a file to the **ESET Endpoint Encryption Reader**.
2. Click **Encrypt**.
3. Type the required password and click **OK** to complete the decryption.



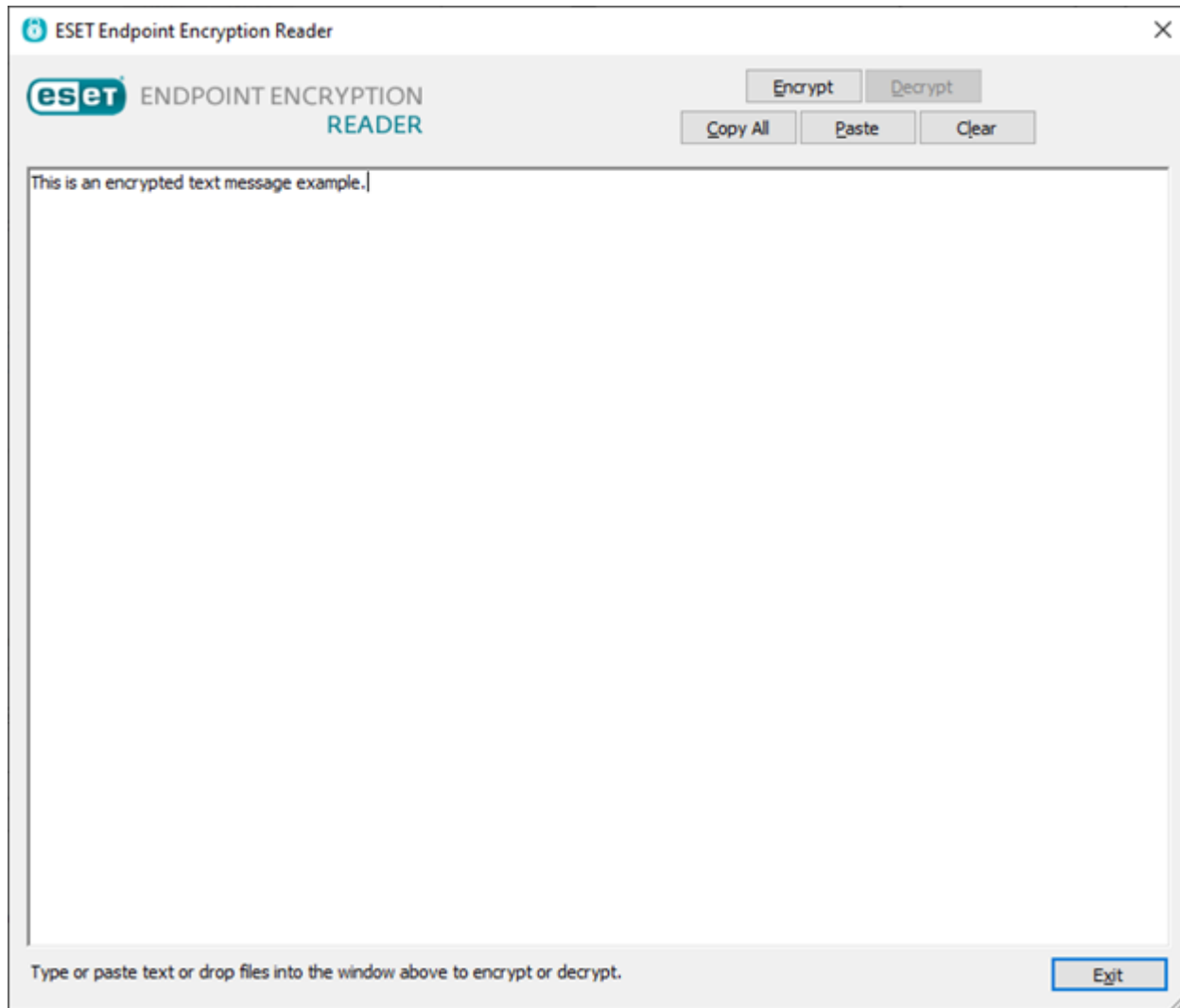
The encrypted version of the file is created in the same directory as the original file.



! The original file remains unchanged.

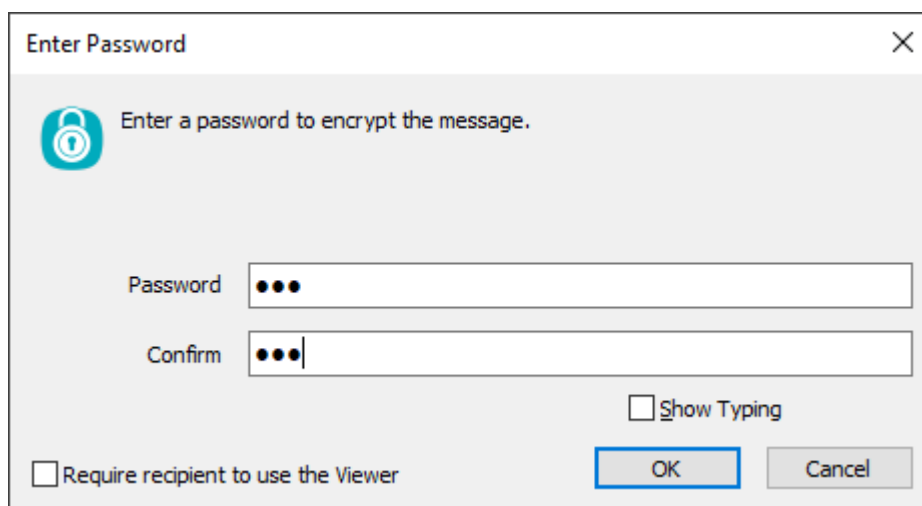
Encrypt text

1. Type or copy/paste a message into the **ESET Endpoint Encryption Reader**.



2. Click **Encrypt**.

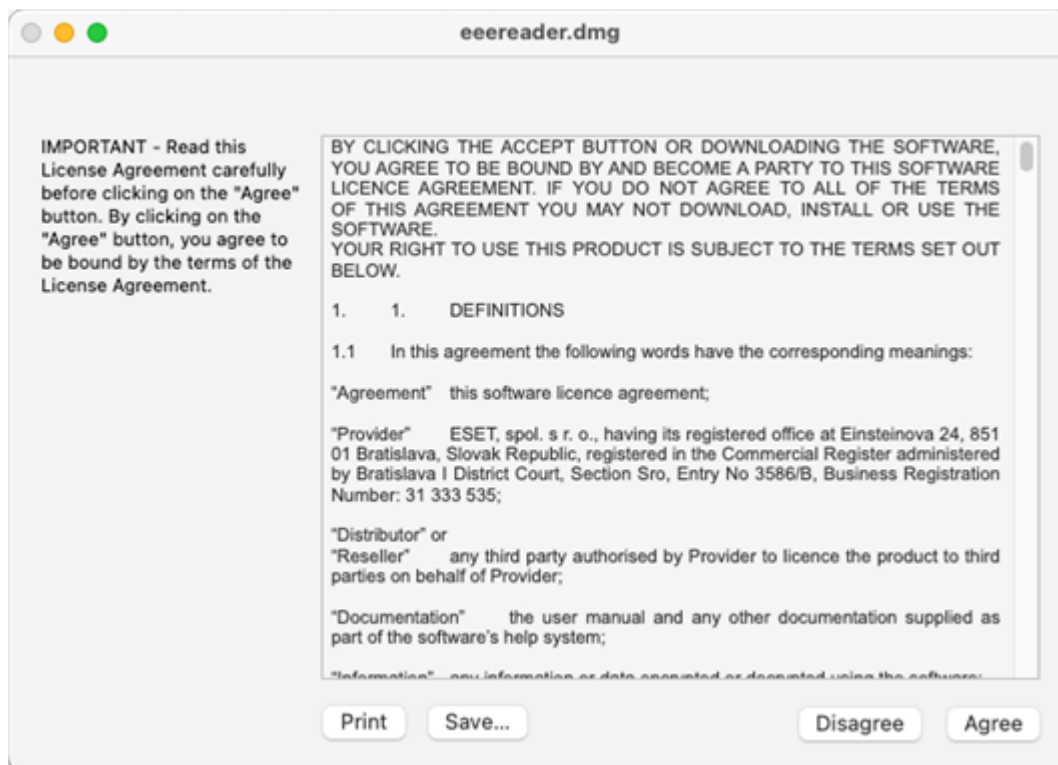
3. Type the required password and click **OK**.



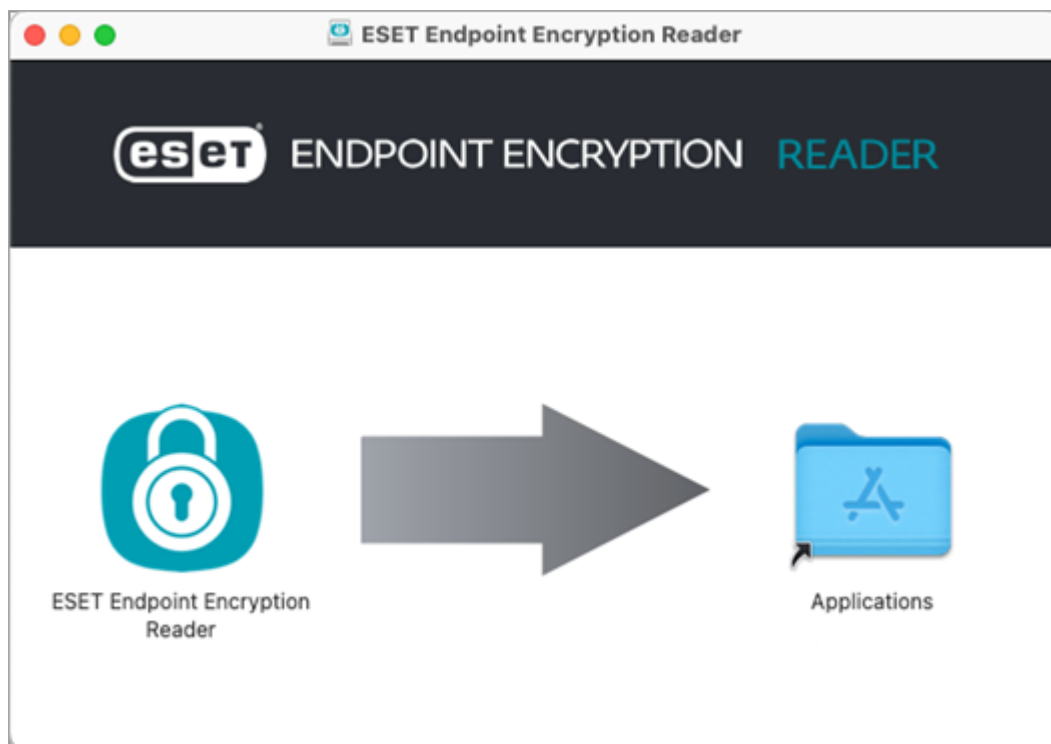
ESET Endpoint Encryption Reader for macOS

1. Download the ESET Endpoint Encryption Reader.

2. Run the package and follow the steps.



3. Drag the ESET Endpoint Encryption Reader icon to Applications to install the package.



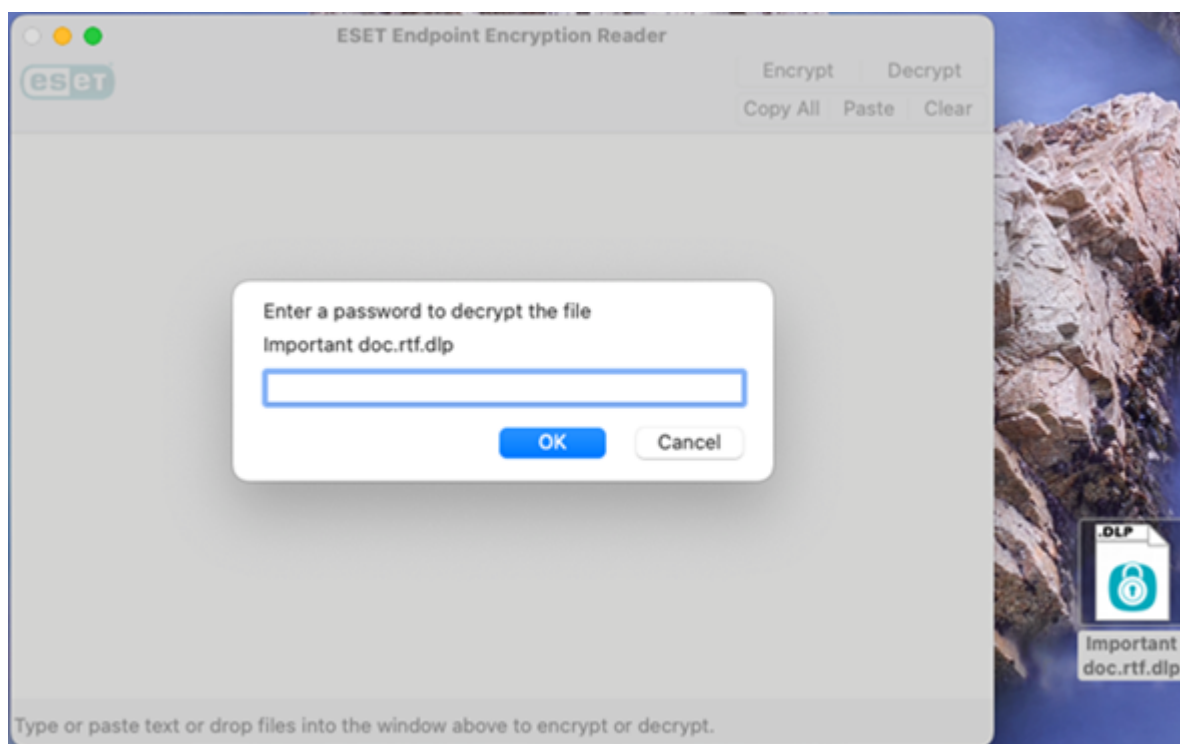
Decrypt files

1. Drag-and-drop an encrypted file (.dlp file extension) to the **ESET Endpoint Encryption Reader**.



2. Click **Decrypt**.

3. Type the required password and click **OK** to complete the decryption.

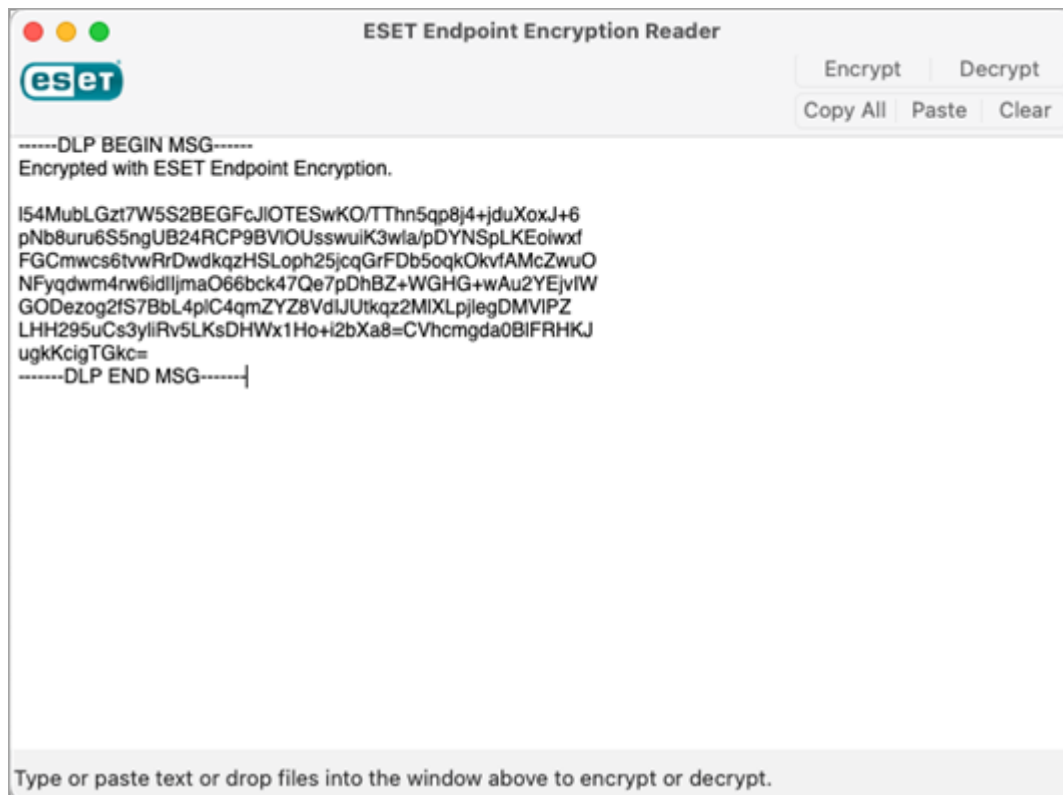


The decrypted file is saved in the same directory as the provided encrypted file.

Decrypt text

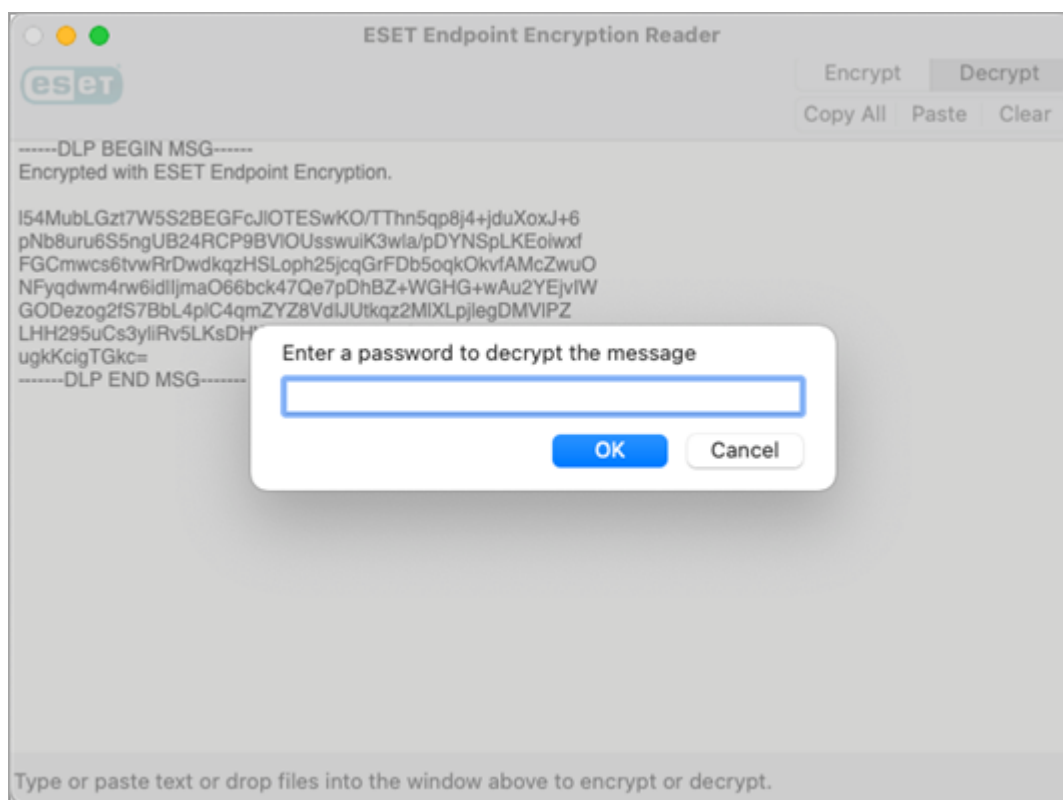
1. Copy/paste an encrypted message into the **ESET Endpoint Encryption Reader**.

⚠ Ensure you include **---DLP BEGIN MSG---** and **---DLP END MSG---** for the text to be recognized correctly.



2. Click **Decrypt**.

3. Type the required password and click **OK** to complete the decryption.

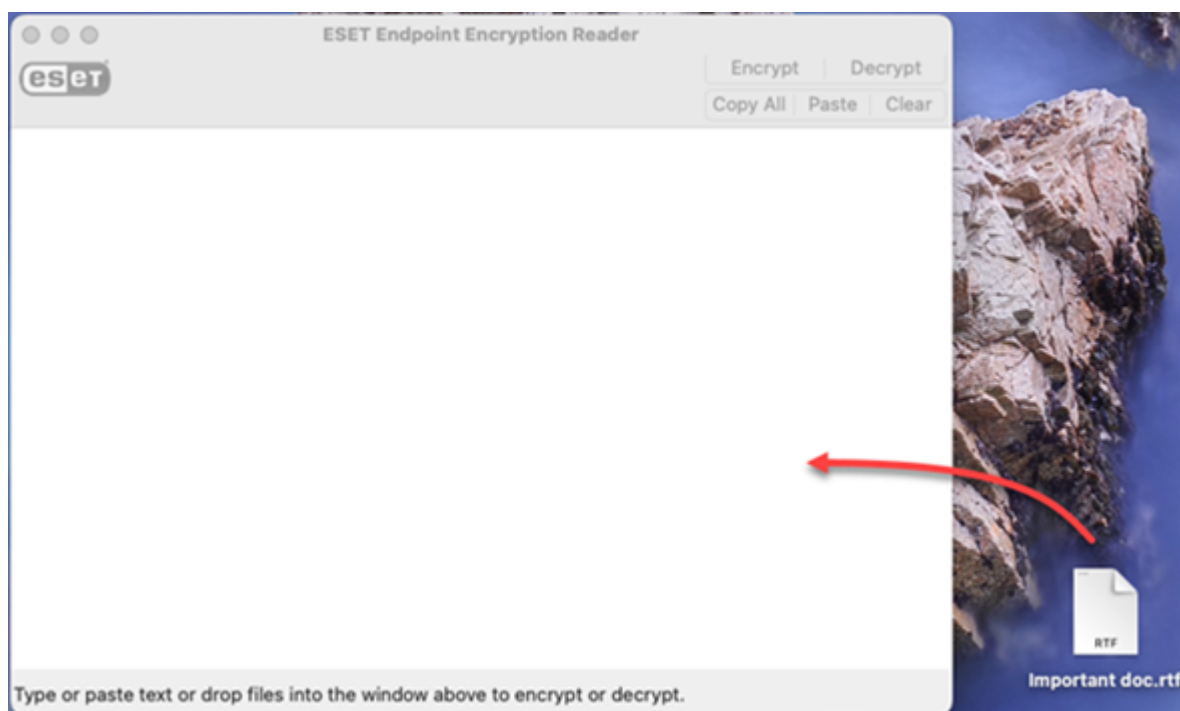


The decrypted text shows in the window.

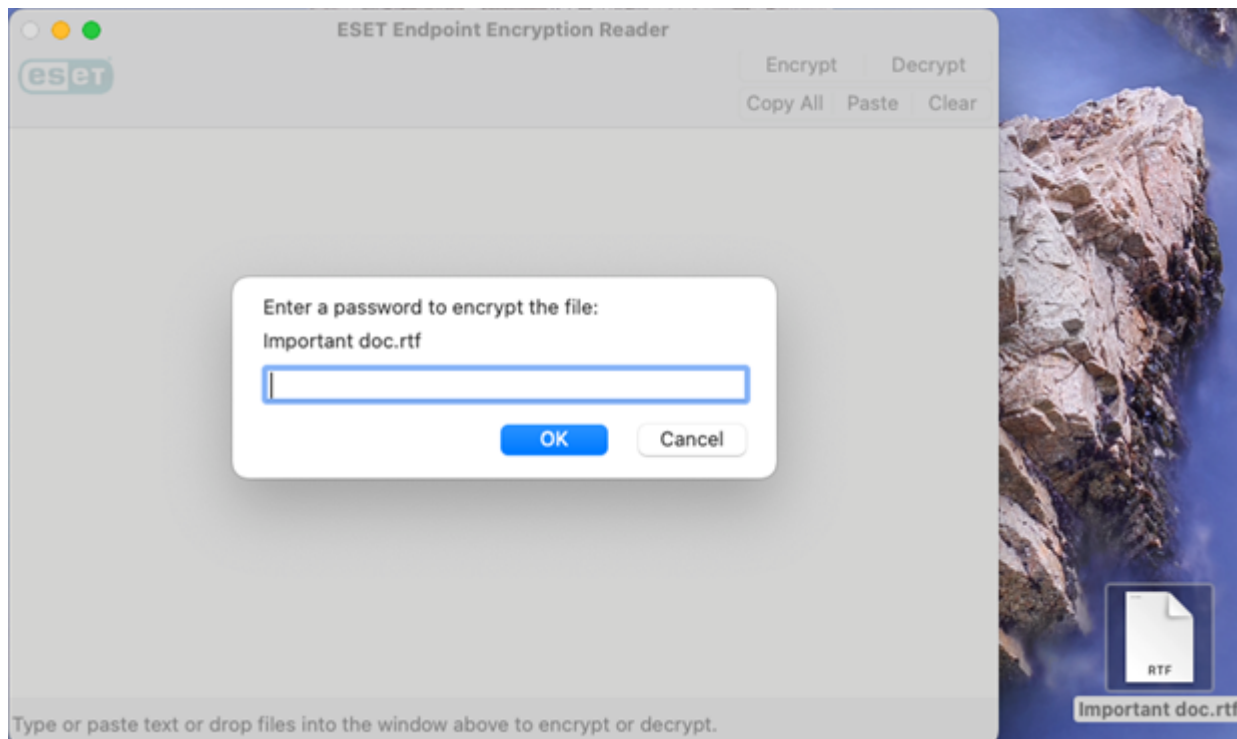


Encrypt files

1. Drag-and-drop a file to the **ESET Endpoint Encryption Reader**.



2. Click **Encrypt**.
3. Type the required password and click **OK** to complete the decryption.

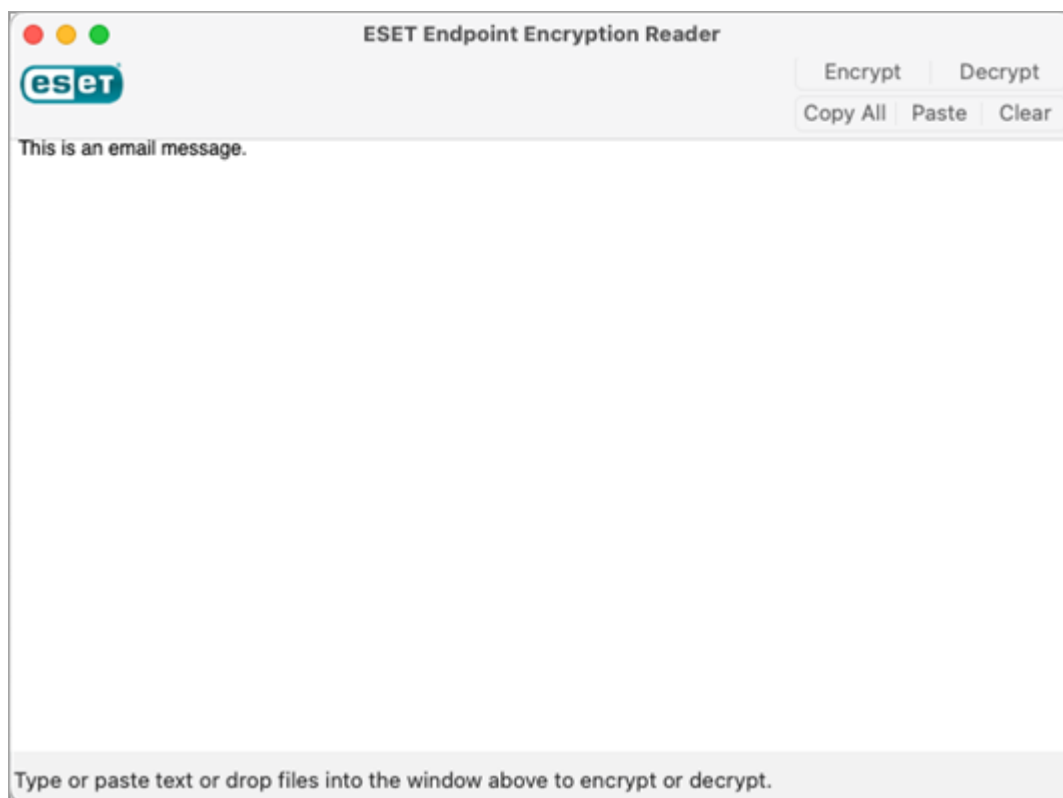


The encrypted version of the file is created in the same directory as the original file.

! The original file remains unchanged.

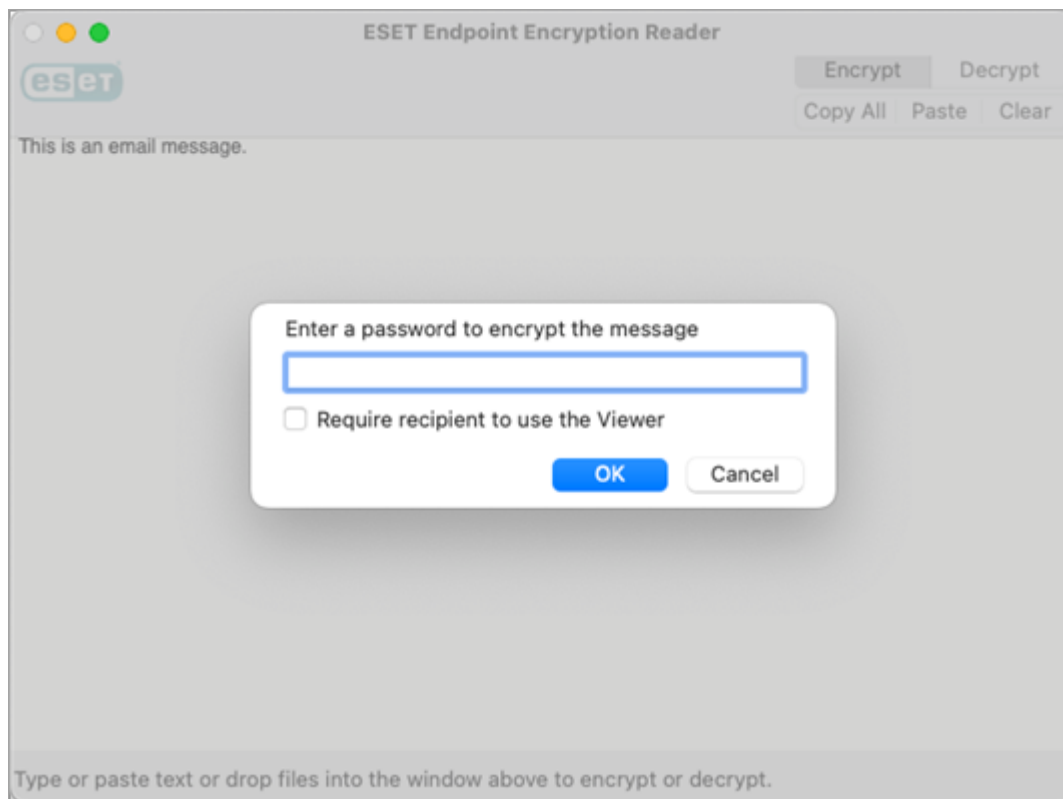
Encrypt text

1. Type or copy/paste a message into the **ESET Endpoint Encryption Reader**.



2. Click **Encrypt**.

3. Type the required password and click **OK**.



The text is encrypted, and you can copy it.

File and Folder Encryption

i The following feature is only available in Windows.

You can encrypt files and entire folders. Any files in a folder and also files placed in it later are encrypted. Subfolders are also encrypted. The decryption/encryption process is transparent because files are opened normally (by their application).

ESET Endpoint Encryption can encrypt all folders, excluding the following folders:

- C:\Windows
- C:\Program Files
- C:\Program Files (x86) (64-bit systems only)
- C:\Documents and Settings (Windows XP)
- C:\Users (Windows Vista or later)

Avoid encrypting redirected folders



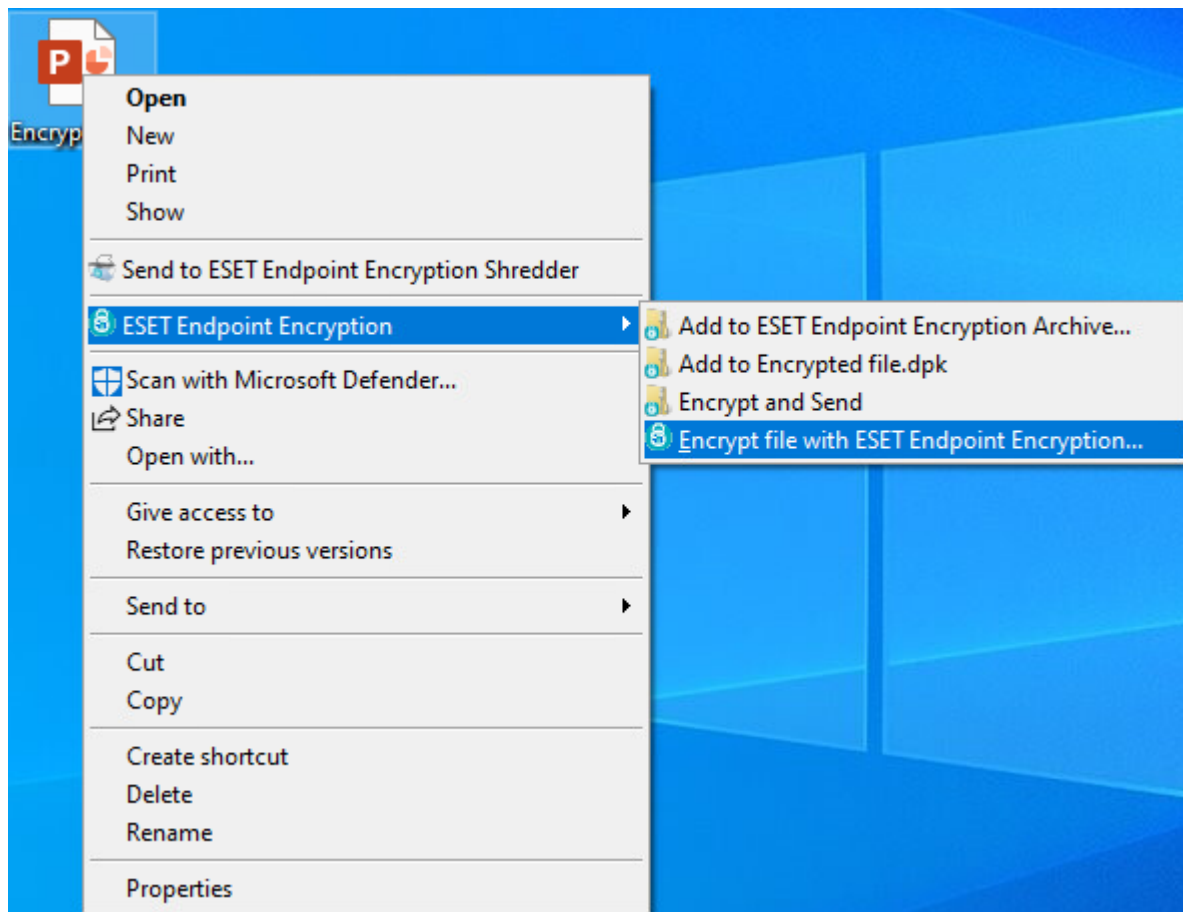
Do not encrypt redirected folders located with the User profile to prevent Windows from loading your profile correctly or to cause problems accessing the application when ESET Endpoint Encryption is not logged in to your Key-File.

There are few exclusions to the the excluded folders list:

- Folders with C:\Users or C:\Documents and Settings can be encrypted.
- Sub-folders on the Desktop can be encrypted; however, the Desktop itself cannot be encrypted.
- Sub-folders in My Documents/Documents can be encrypted.

Encrypt a file

1. Right-click the file and select **ESET Endpoint Encryption > Encrypt file with ESET Endpoint Encryption**.

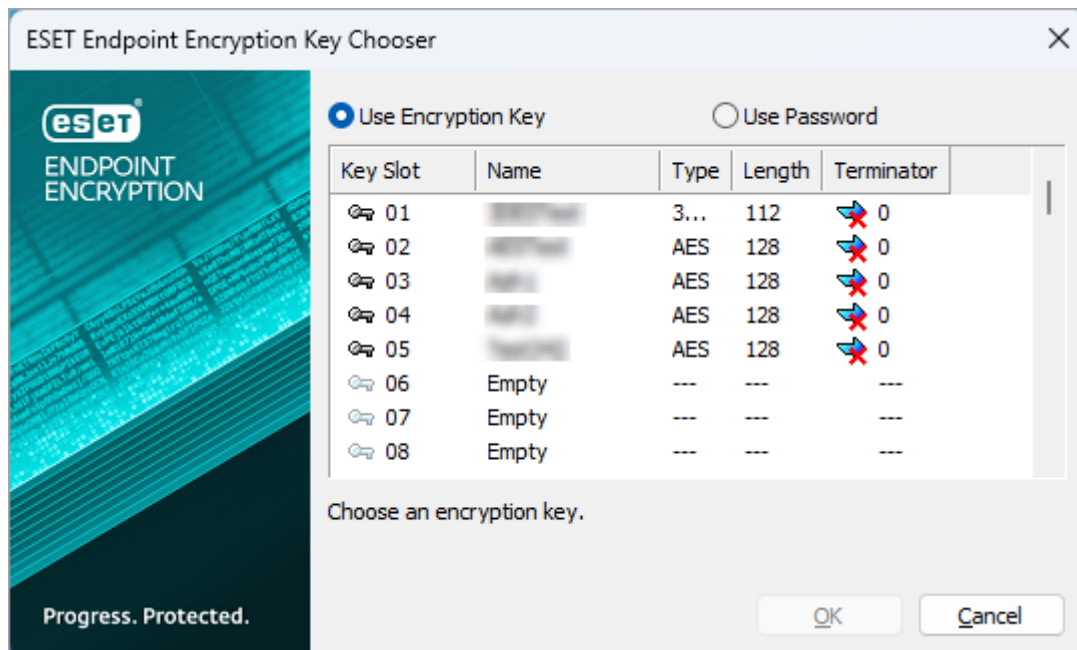


2. Select a file encryption option: **Use Encryption Key** or **Use Password**.

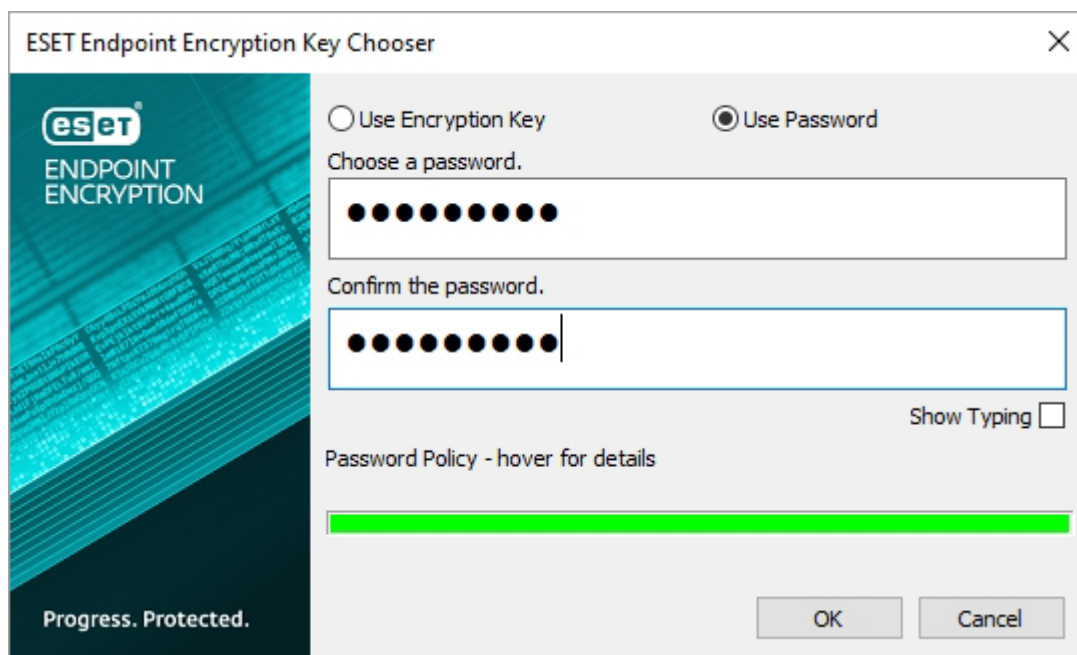


You can see the **Use Password** option only if the administrator enabled the **Enable Password Encryption group** policy option.

3. If you selected **Use Encryption Key**, select the **Encryption Key** and go to step 5.



4. If you selected **Use Password**, type and confirm your password and go to step 5.

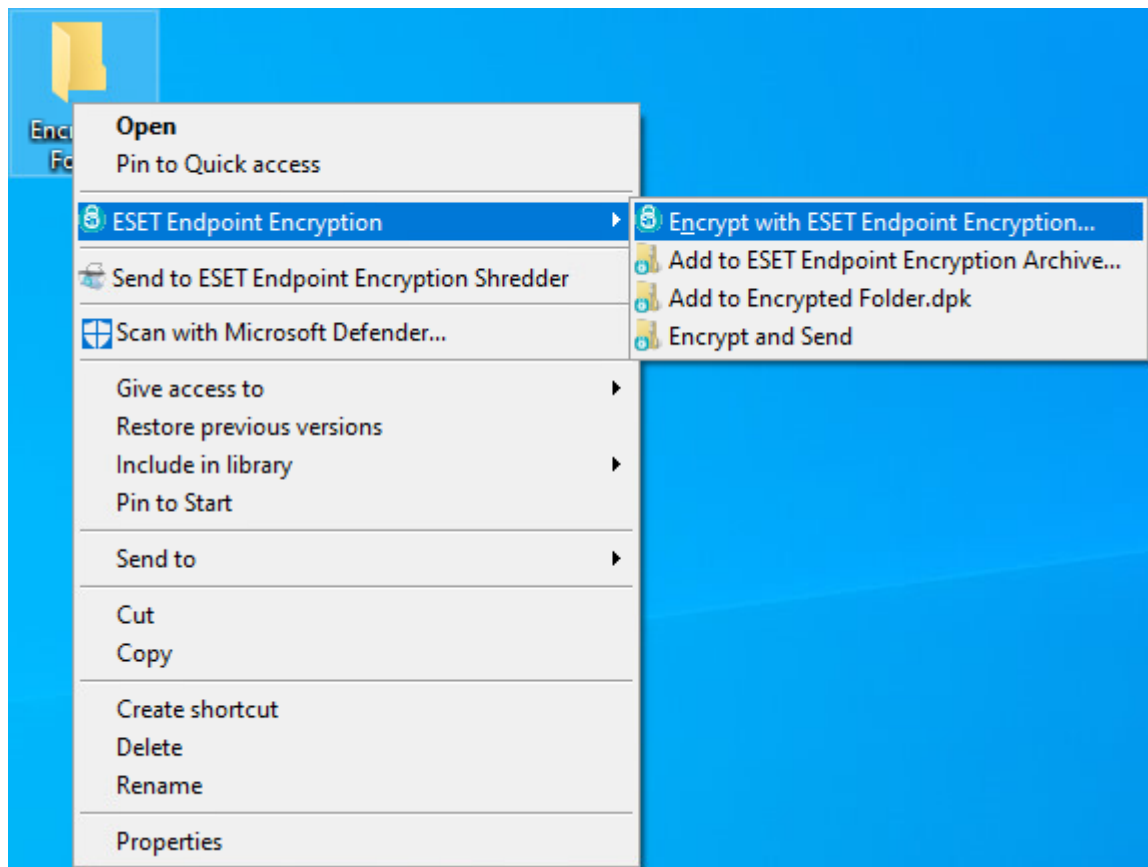


5. Click **OK**.

When the file is encrypted, the file icon changes to indicate encryption, and the *.dlp* suffix is added to the filename. The encrypted file copy is created in the original folder.

Encrypt a folder

1. Right-click the folder you want to encrypt and select **ESET Endpoint Encryption > Encrypt with ESET Endpoint Encryption**.

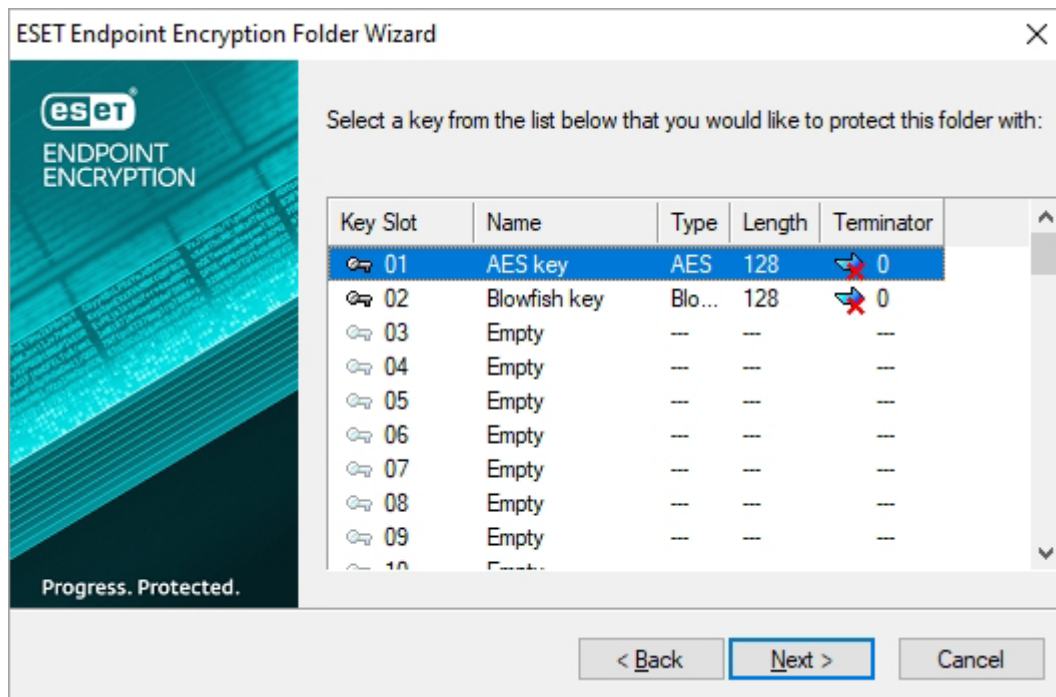


⚠ Ensure you have backed up all data before encrypting.

2. Select **I have backed up my data and wish to continue** and click **Next**.

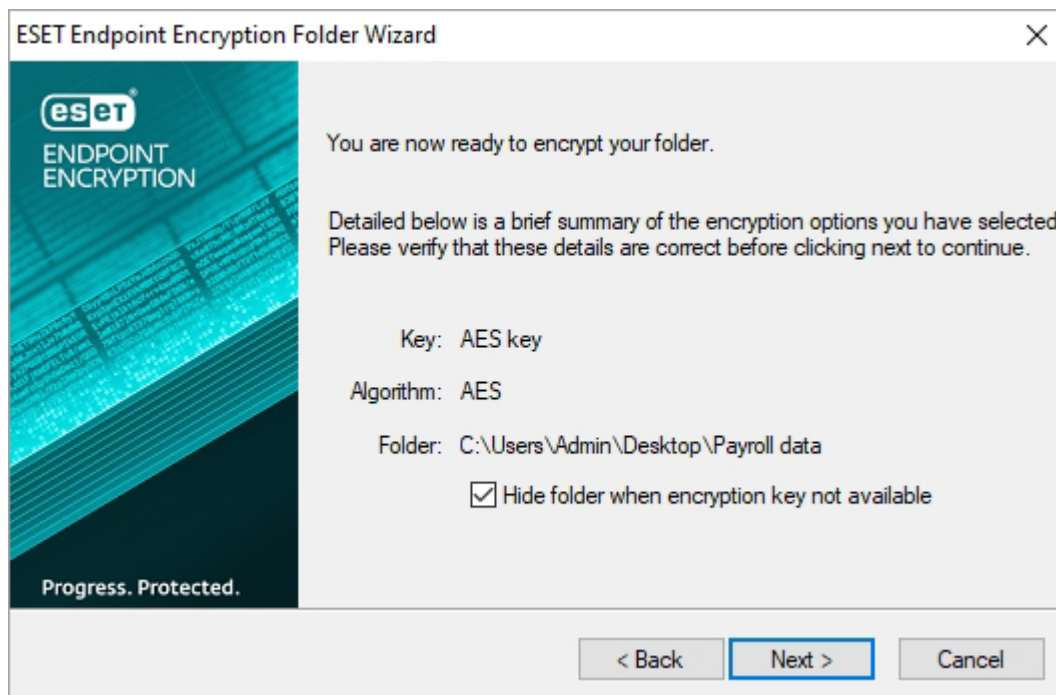


3. Select the Encryption Key for folder encryption and click **Next**.

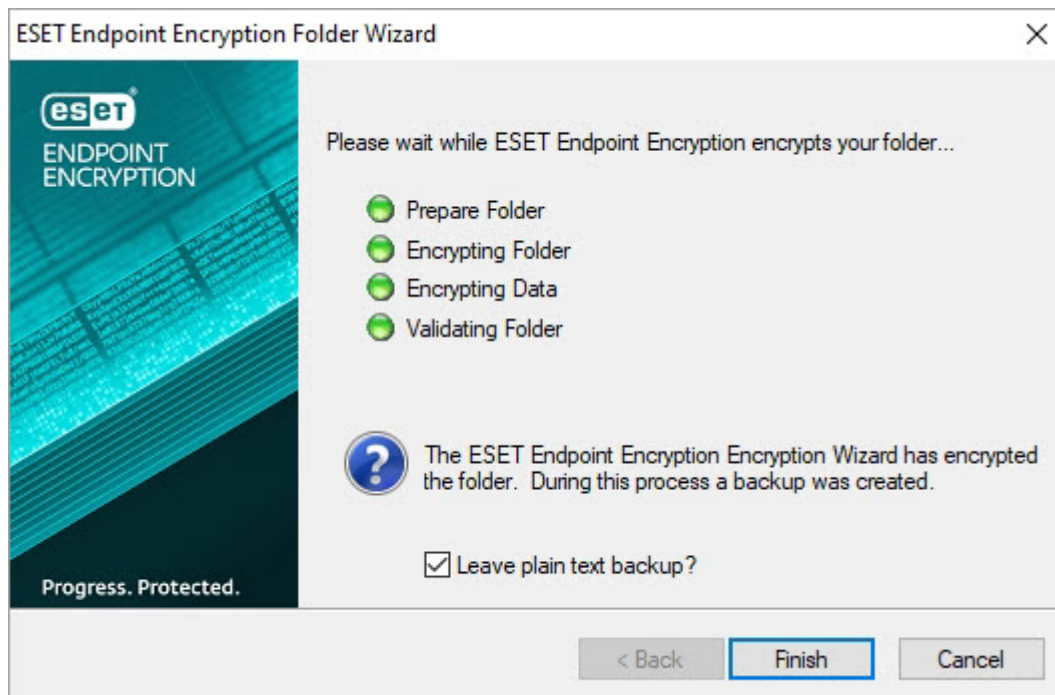


! If only one encryption key exists, it is selected by default.

4. Optionally, select **Hide folder when encryption key not available** to hide the encrypted folder while you are logged out of ESET Endpoint Encryption and click **Next**.



5. Optionally, select **Leave plain text backup?** to leave a plain text (unencrypted) backup of the folder and click **Finish**.



When the folder is encrypted, all data stored inside the folder is automatically encrypted and protected.

Network drives

- ! You cannot encrypt folders on a network drive or copy encrypted folders to a network drive. However, you can create a virtual encrypted drive on a network drive.

- ! If the recipient of a encrypted document is not an ESET Endpoint Encryption customer, they can decrypt the document with the free [ESET Endpoint Encryption Reader](#).

To encrypt multiple files:

- !
 - create a .zip file and encrypt the file
 - create an [encrypted archive](#)

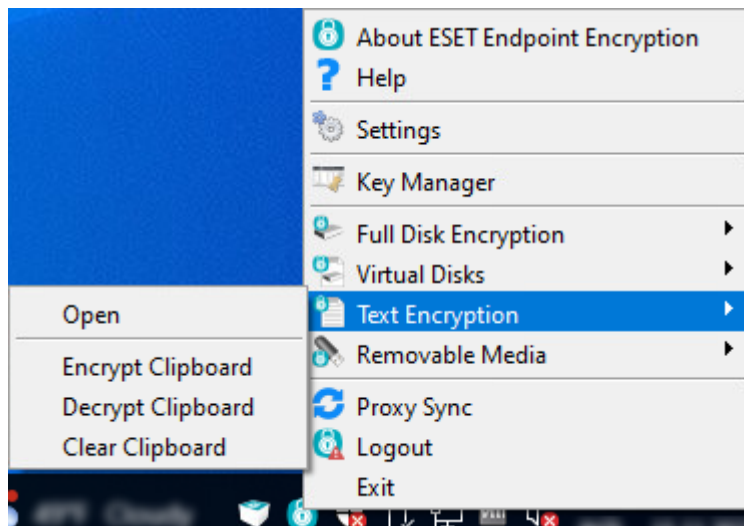
Text Encryption

i The following feature is only available in Windows.

You can encrypt or decrypt selected text or a whole document manually with ESET Endpoint Encryption Text Encryption tools.

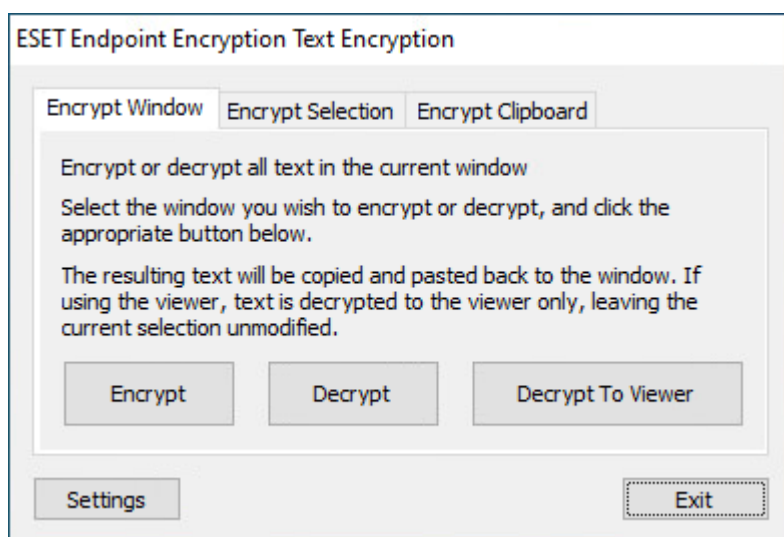
Encrypt a text

1. Right-click the ESET Endpoint Encryption icon, select **Text Encryption** and click **Open**.

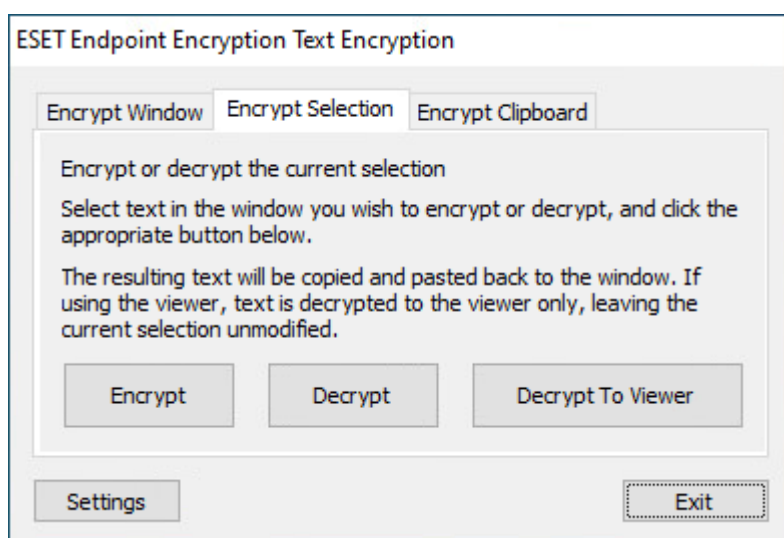


2. Select one of the encryption options:

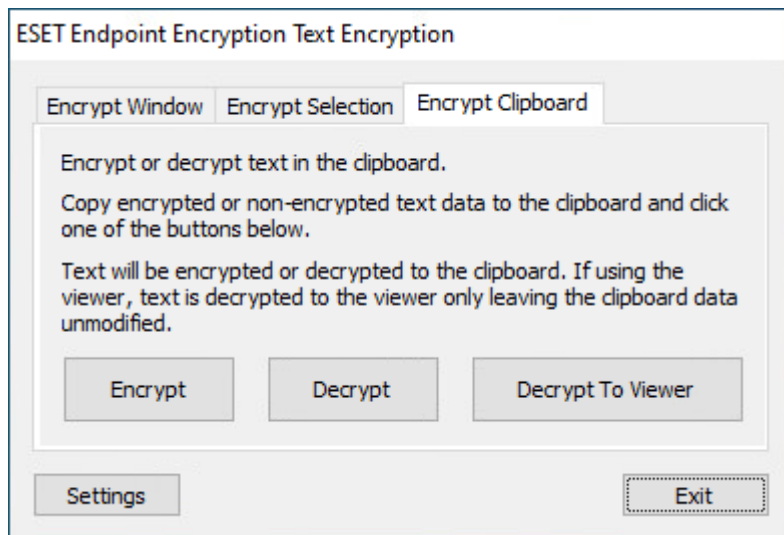
- Select the **Encrypt Window** tab to encrypt all the text in the window.



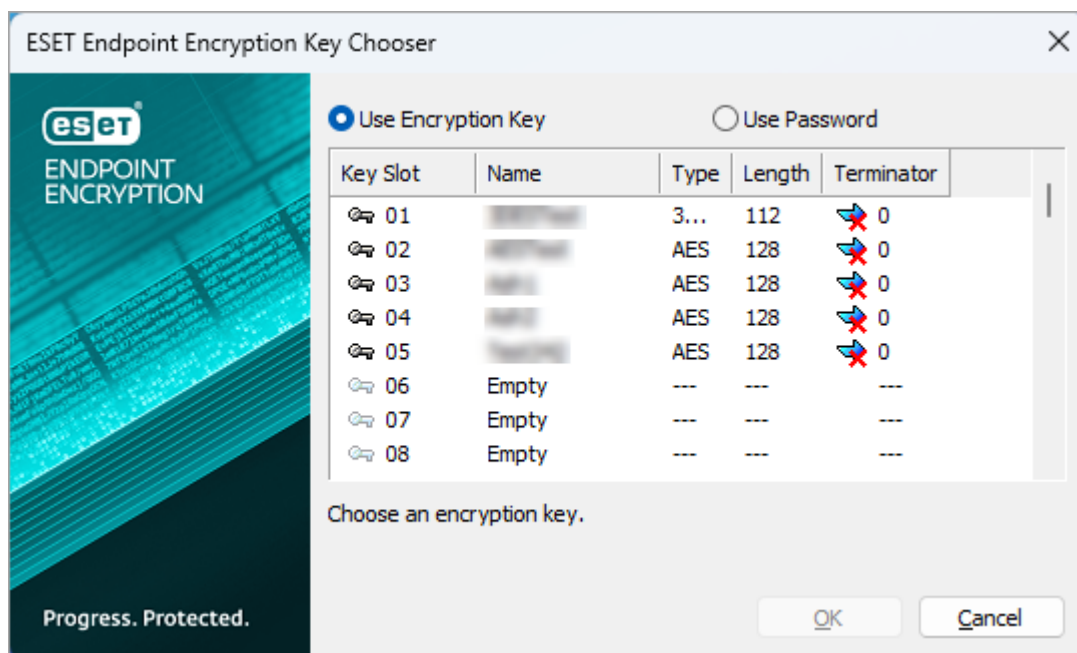
- Select the **Encrypt Selection** tab to encrypt the selected text in the window.



- Select the **Encrypt Clipboard** tab to encrypt text in the clipboard.



3. Click **Encrypt**.
4. Select a text encryption option: **Use Encryption Key** or **Use Password**.
5. Select the encryption method:
 - If you selected **Use Encryption Key**, select the **Encryption Key**.



- If you selected **Use Password**, type and confirm your password.



6. Click **OK**.

Decrypt a text

1. Right-click the ESET Endpoint Encryption icon, select **Text Encryption** and click **Open**.
2. Select one of the decryption options:
 - Select **Encrypt Window** tab to decrypt full text in the current window.
 - Select **Encrypt Selection** tab to decrypt the selected text in the window.
 - Select **Encrypt Clipboard** tab to decrypt text in the clipboard.
3. Click **Decrypt** or click **Decrypt to Viewer**.
 - The **Decrypt to Viewer** option will only decrypt the text to the viewer; selected or clipboard data remain unmodified.

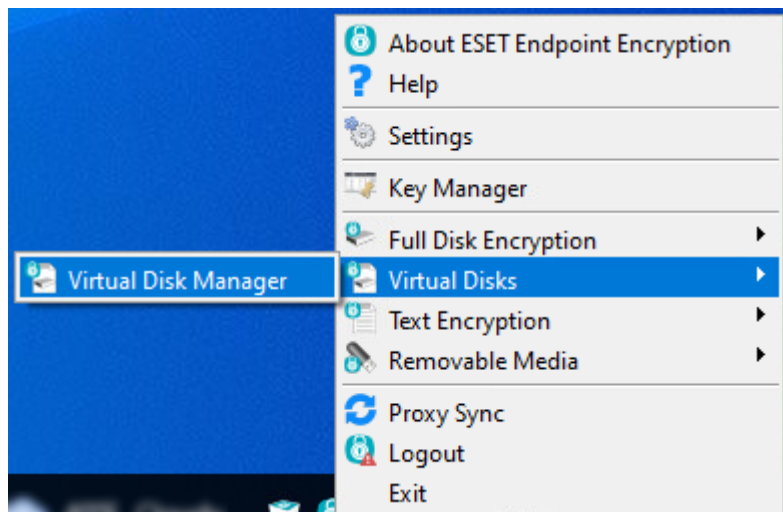
Virtual Disks

i The following feature is only available in Windows.

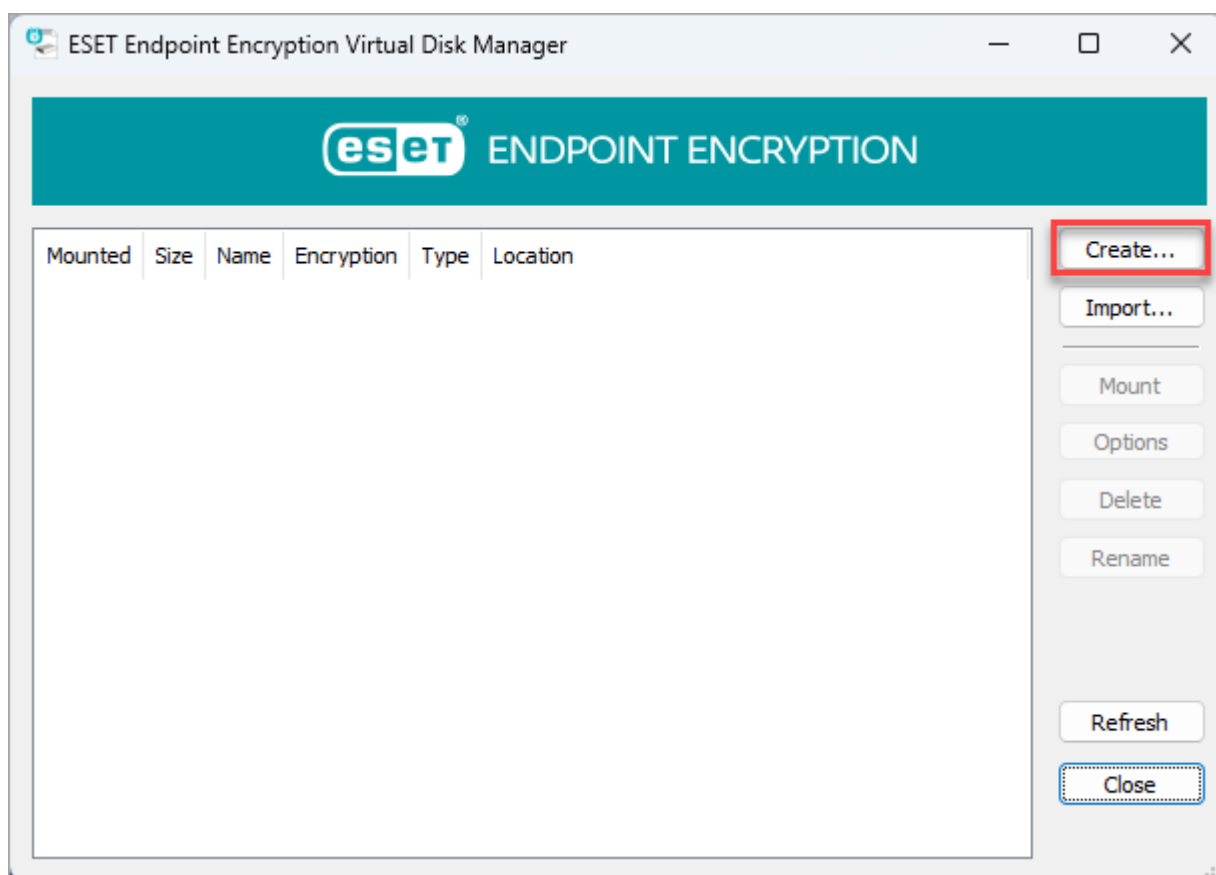
Virtual disks are encrypted containers that provide access through a mapped drive letter to the files within the virtual disks.

Create a new Virtual Disk

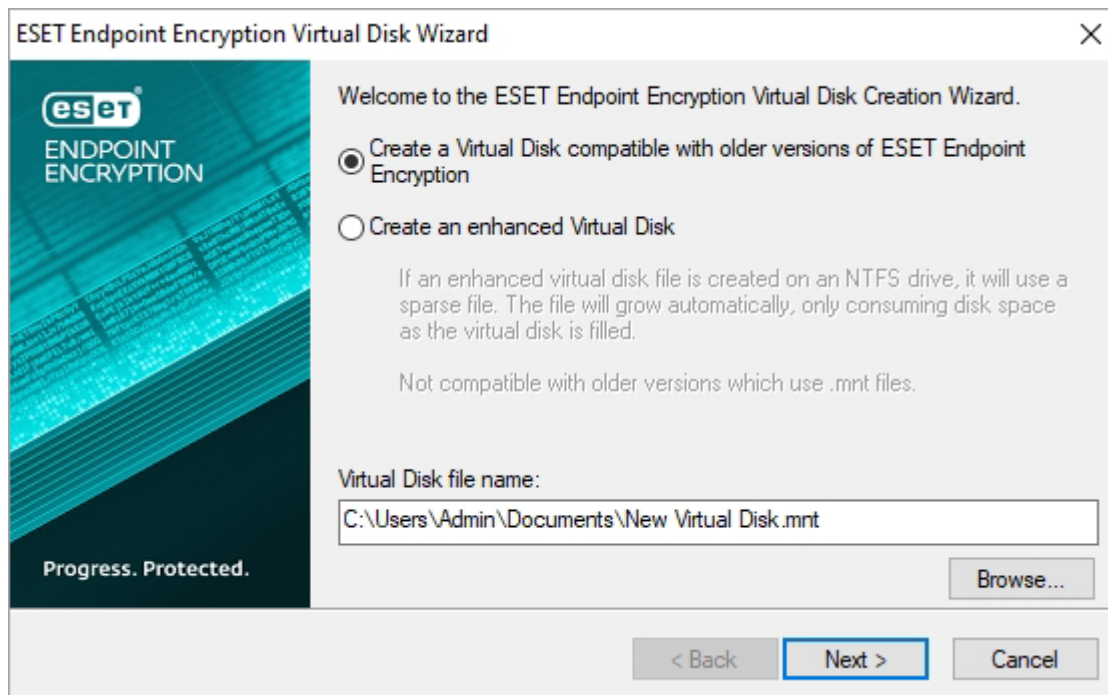
1. Right-click the ESET Endpoint Encryption icon, select **Virtual Disks** and click **Virtual Disk Manager**.



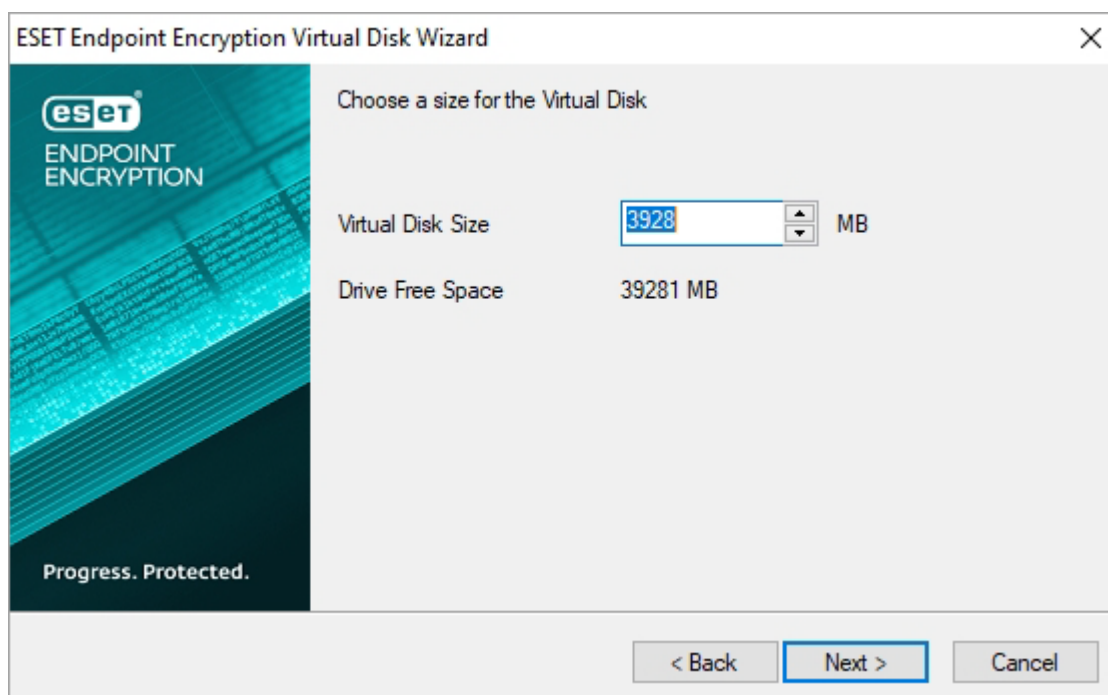
2. Click **Create**.



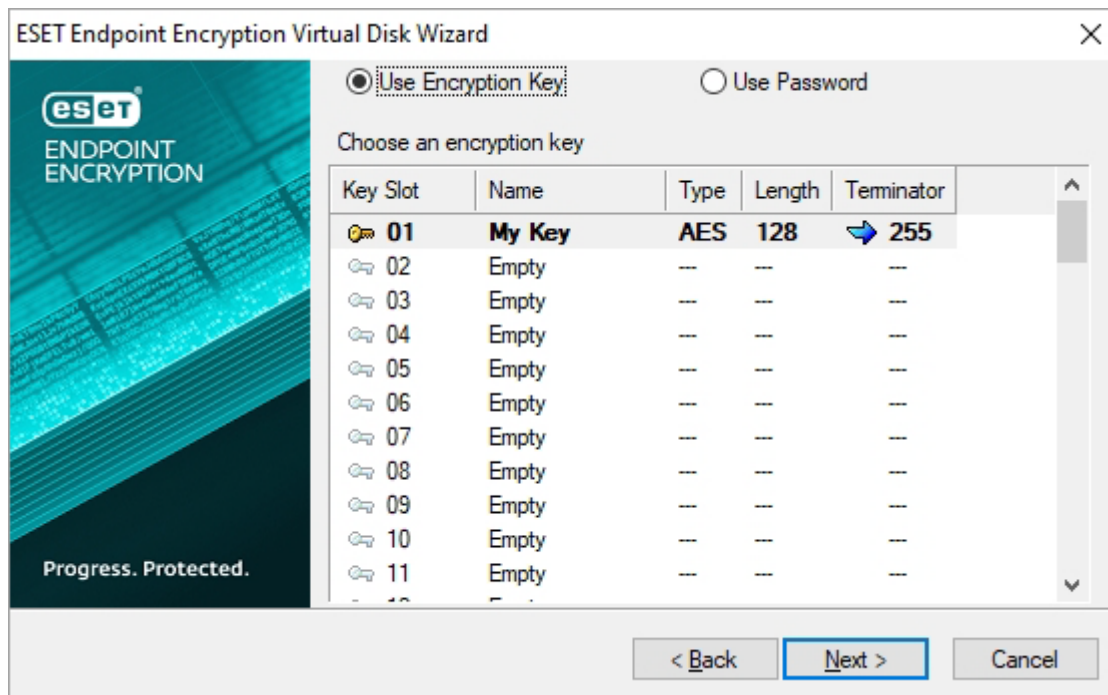
3. Select the Virtual Disk type.



4. Click **Browse** to select the destination path for the newly created Virtual Disk.
5. Click **Next**.
6. Set the size of the Virtual Disk and click **Next**.



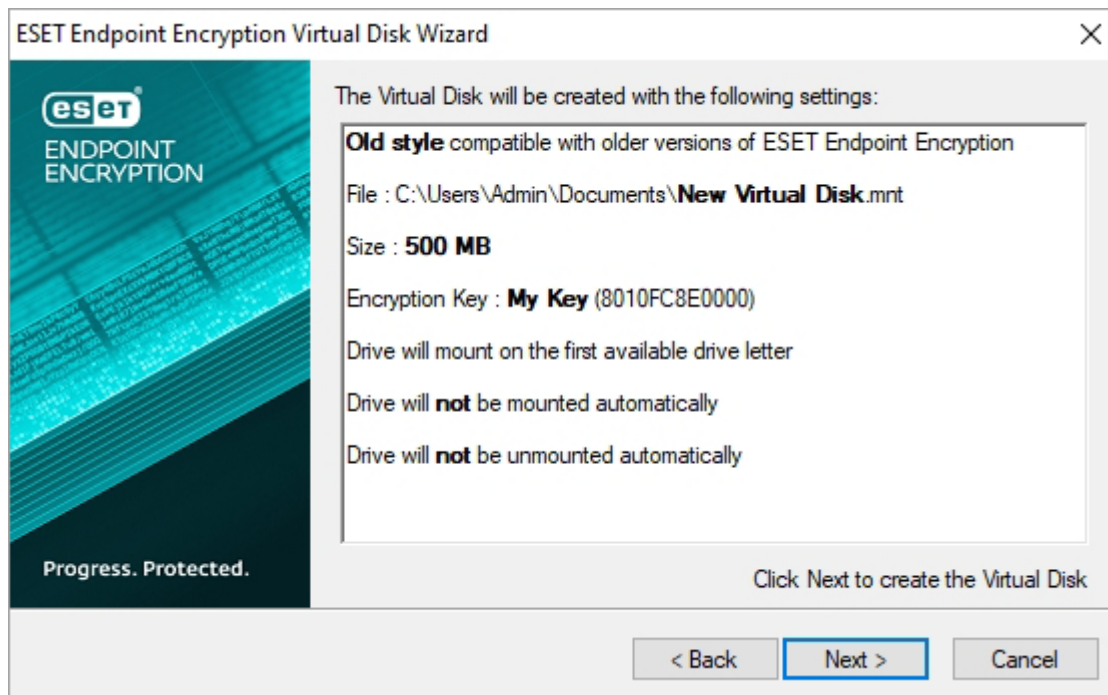
7. Select the encryption method and click **Next**.



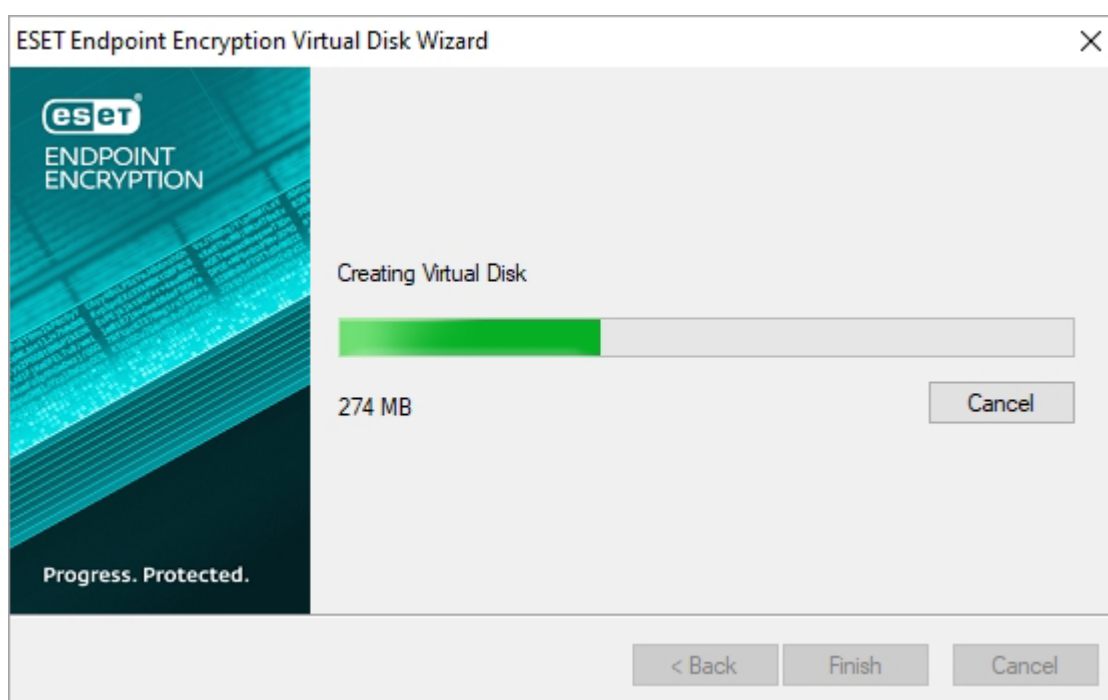
8. Set **Default Drive Assignment** and click **Next**.



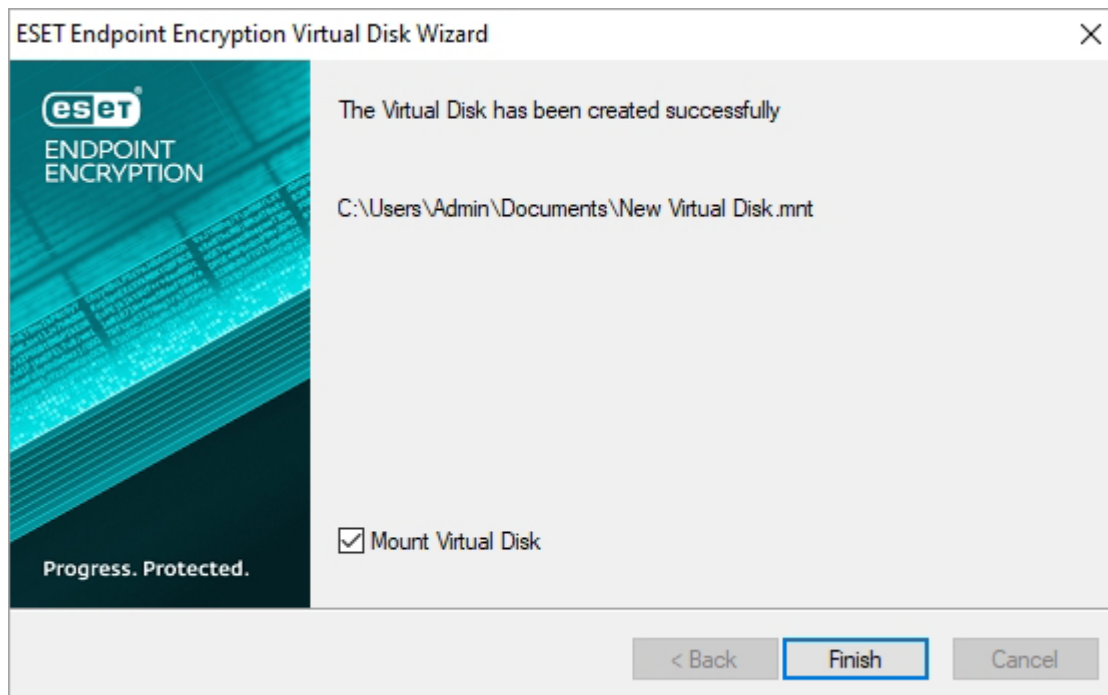
9. An overview of the selected settings displays. Click **Next** to create the Virtual Disk.



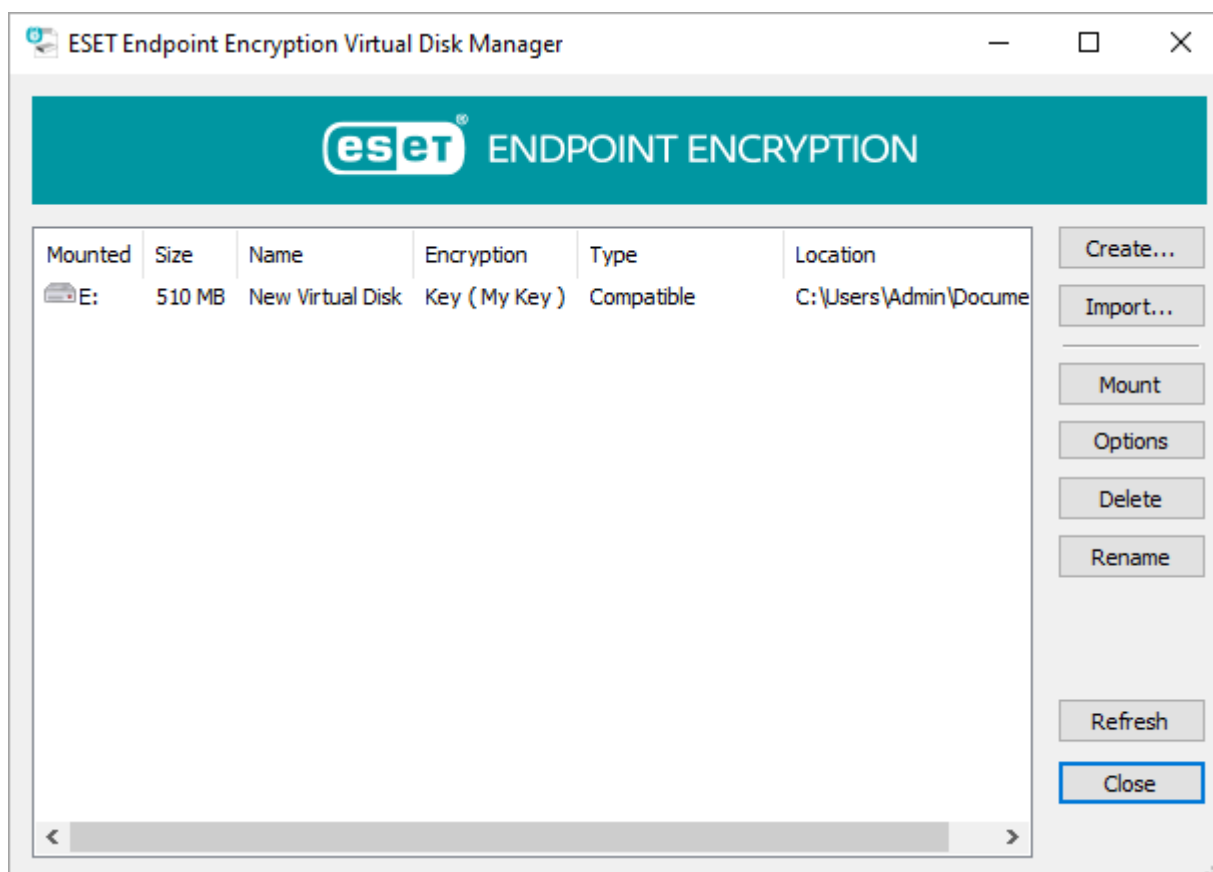
10. A progress bar of the Virtual Disk creation displays.



11. After the Virtual Disk has been created, select **Mount Virtual Disk** to access the new Virtual Disk and click **Finish**.



The drive letter used to access the container is displayed within the Virtual Disk Manager interface, and you can see the mapped drive letter with ESET Endpoint Encryption icon.



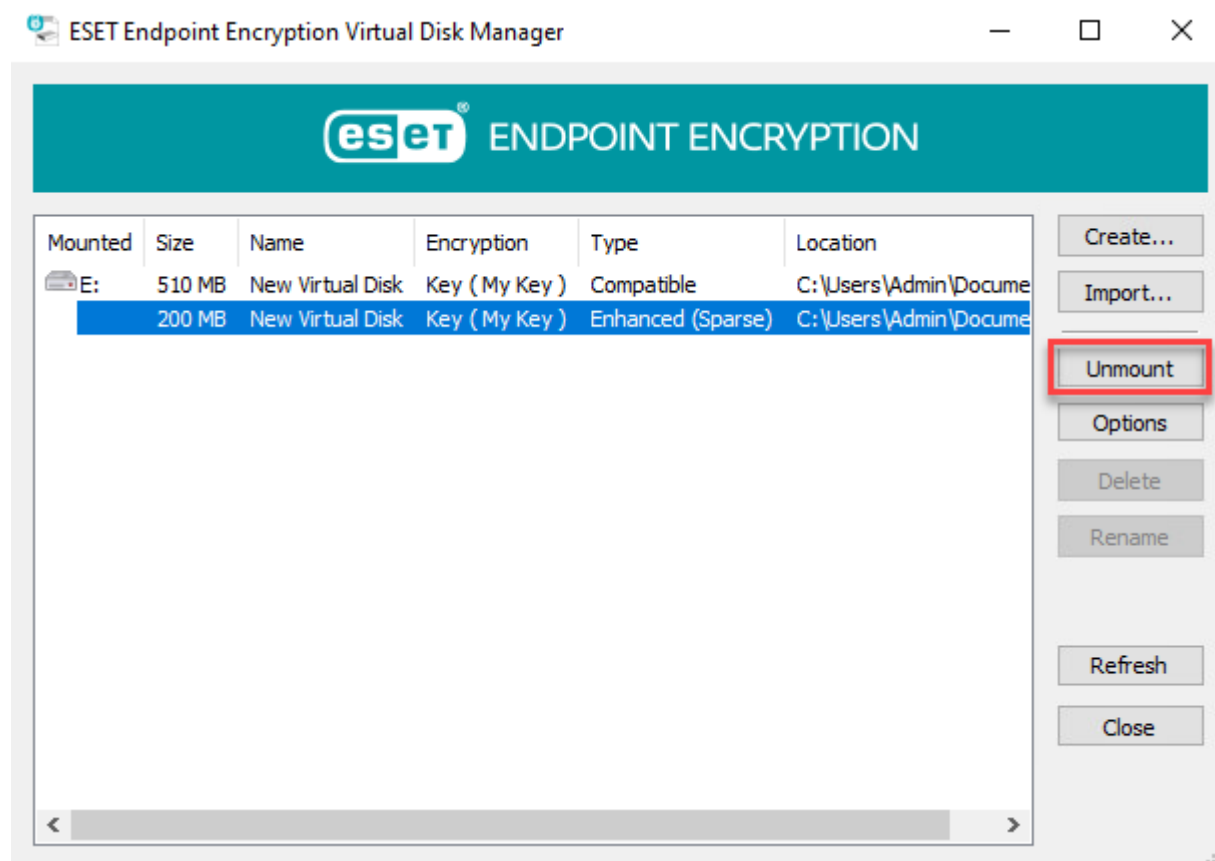
▼ Devices and drives (4)

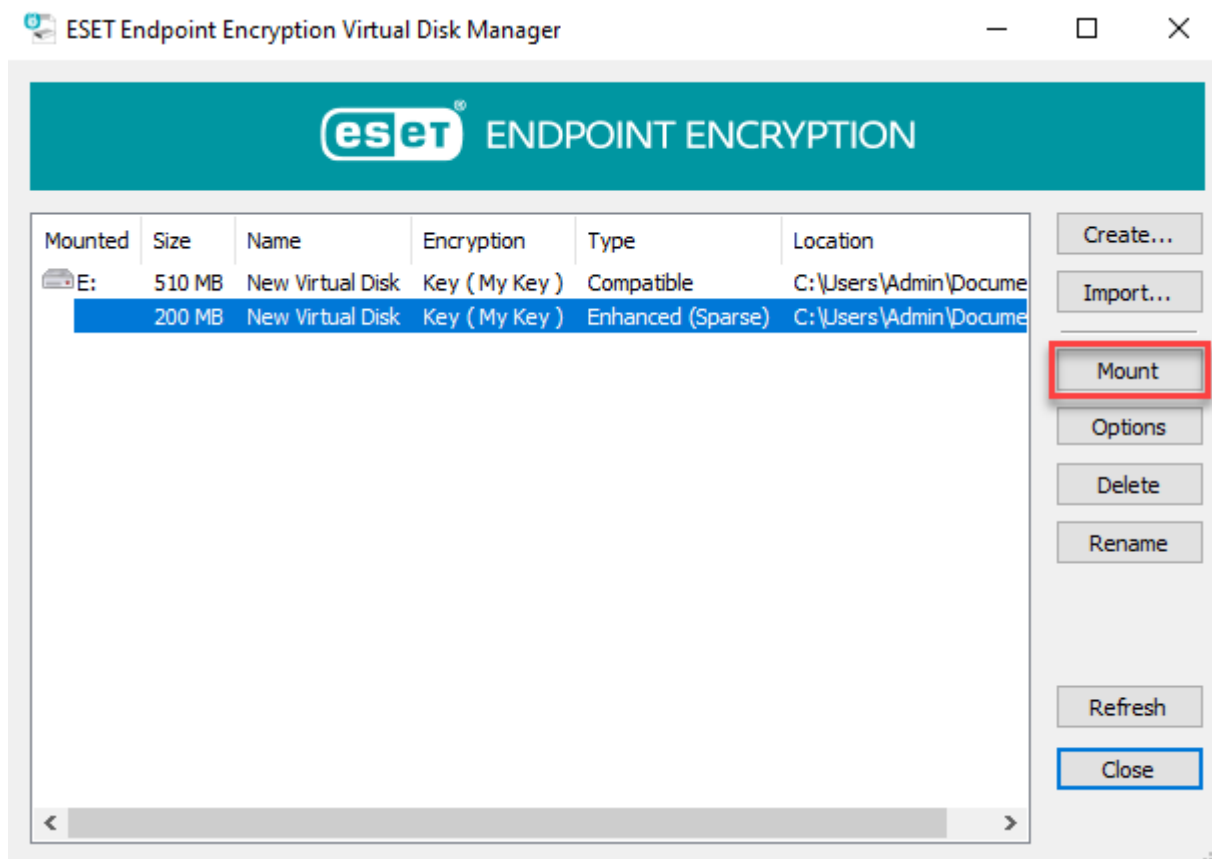


Unmount/Mount the Virtual Disk

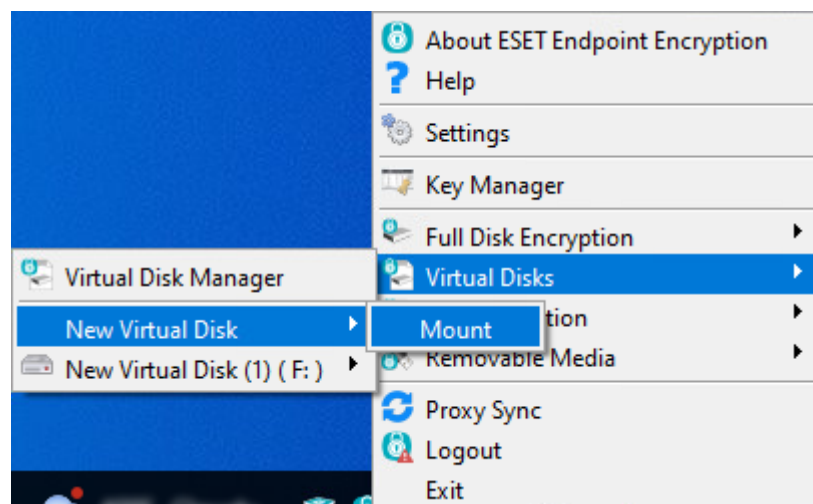
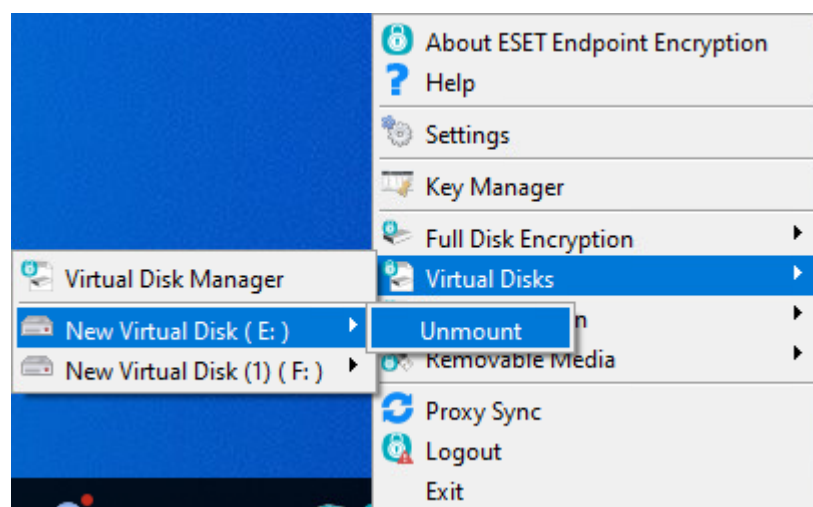
There are two methods to unmount/mount a virtual disk.

- Using the Virtual Disk Manager:





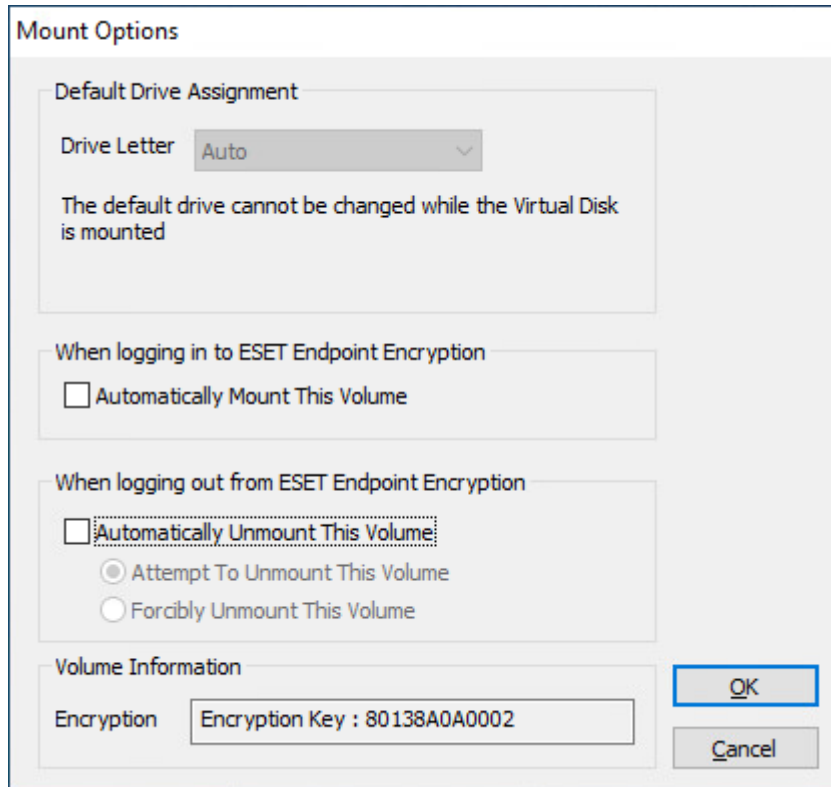
- Using the pop-out menu from ESET Endpoint Encryption icon in the notification area:



Options

The Virtual Disk has configurable options to mount to a preferred drive letter and automatically mount/unmount when you log in or out of ESET Endpoint Encryption.

In the Virtual Disk Manager, click **Options** to change the settings.



The image shows a 'Mount Options' dialog box with the following sections:

- Default Drive Assignment:** A 'Drive Letter' dropdown menu is set to 'Auto'. Below it, a note states: 'The default drive cannot be changed while the Virtual Disk is mounted'.
- When logging in to ESET Endpoint Encryption:** A checkbox for 'Automatically Mount This Volume' is present and unchecked.
- When logging out from ESET Endpoint Encryption:** A checkbox for 'Automatically Unmount This Volume' is present and unchecked. Below this checkbox are two radio buttons: 'Attempt To Unmount This Volume' (which is selected) and 'Forcibly Unmount This Volume'.
- Volume Information:** An 'Encryption' field displays the 'Encryption Key : 80138A0A0002'.

At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

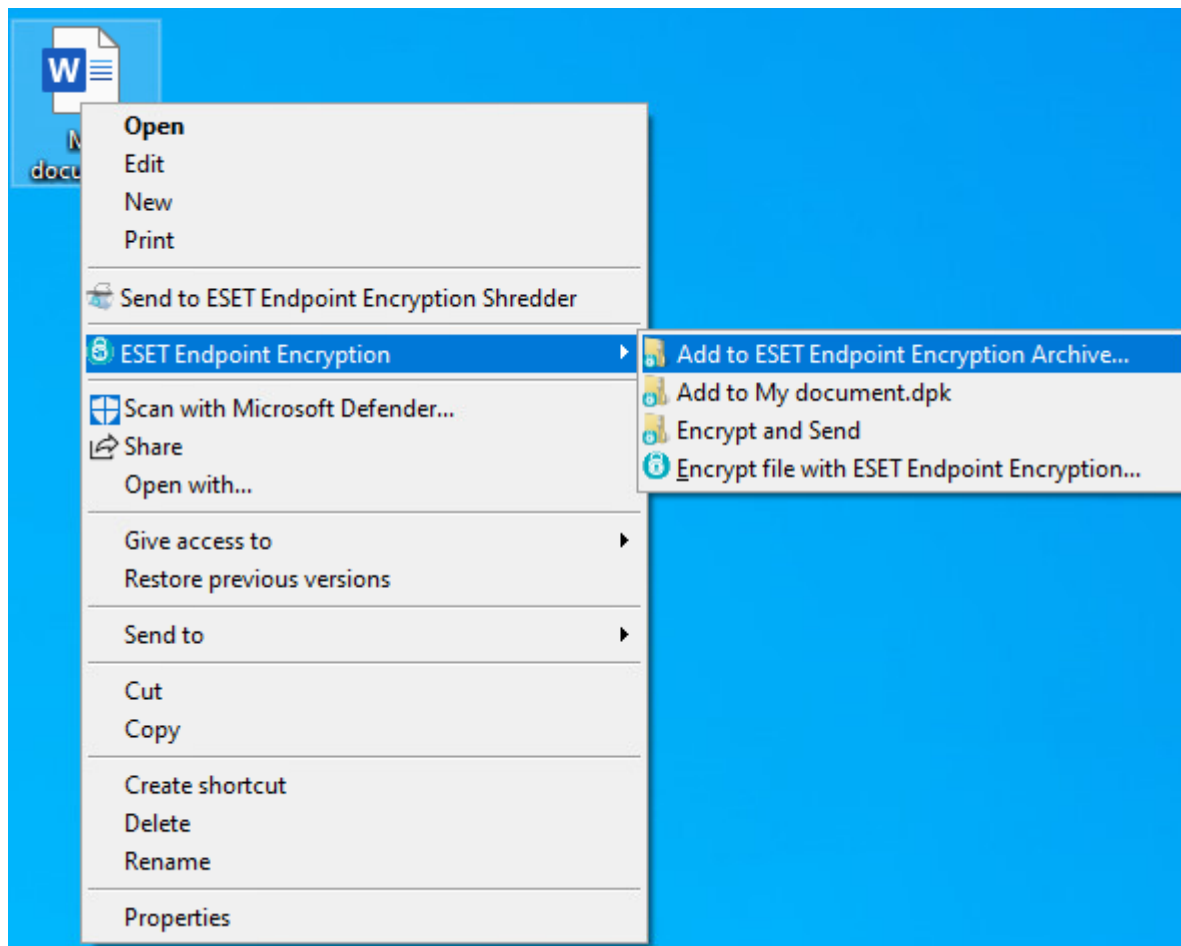
Encrypted Archives

i The following feature is only available in Windows.

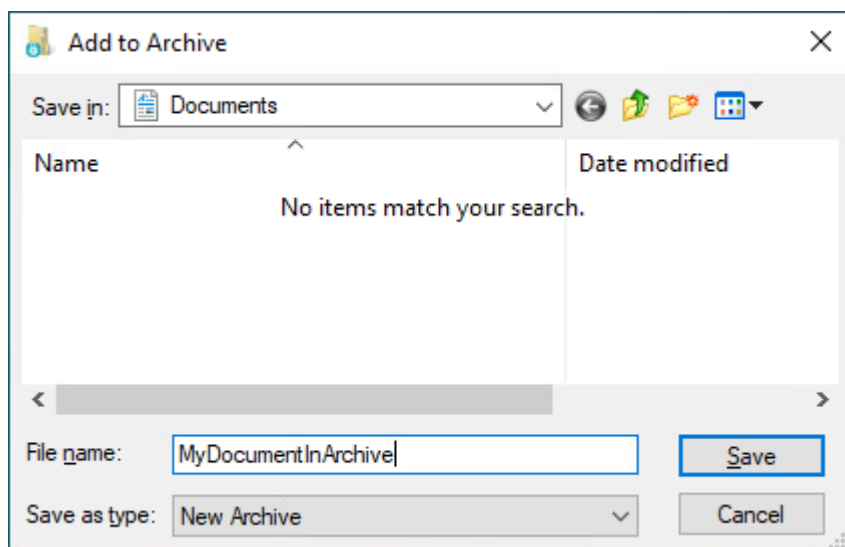
The ESET Endpoint Encryption Archive compresses and stores sensitive data and is similar to a ZIP folder. All data stored inside the ESET Endpoint Encryption Archive is encrypted.

Create the ESET Endpoint Encryption Archive

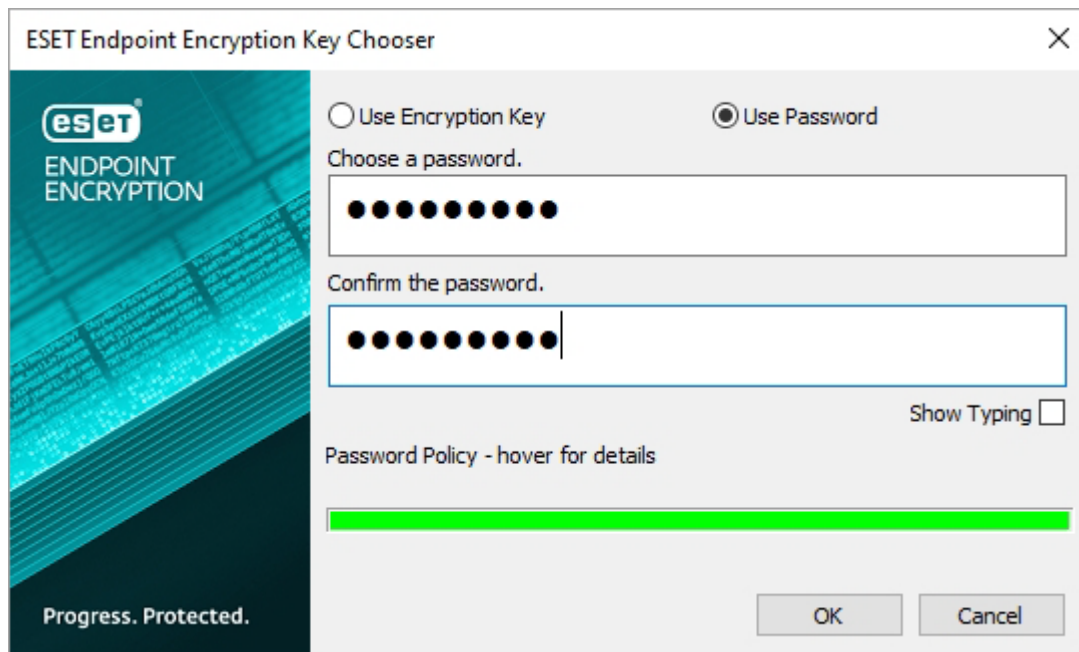
1. Right-click the file you want to store inside an Encrypted Archive; select **ESET Endpoint Encryption** and click **Add to ESET Endpoint Encryption Archive**.



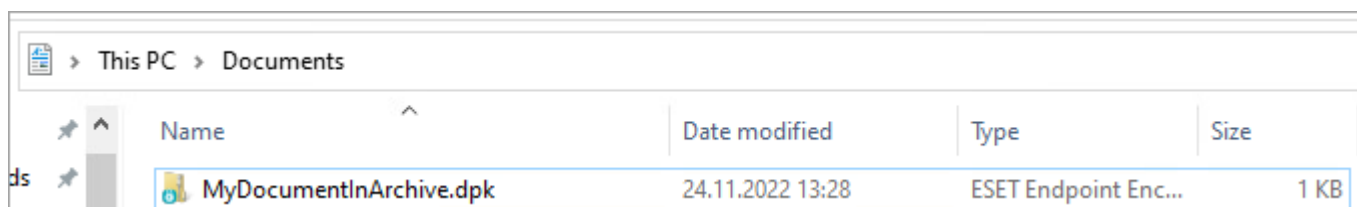
2. Select a destination folder for your ESET Endpoint Encryption Archive; type a name and click **Save**.



3. Select an encryption option: **Use Encryption Key** or **Use Password**. If you selected **Use Password**, type and confirm your password and click **OK**.



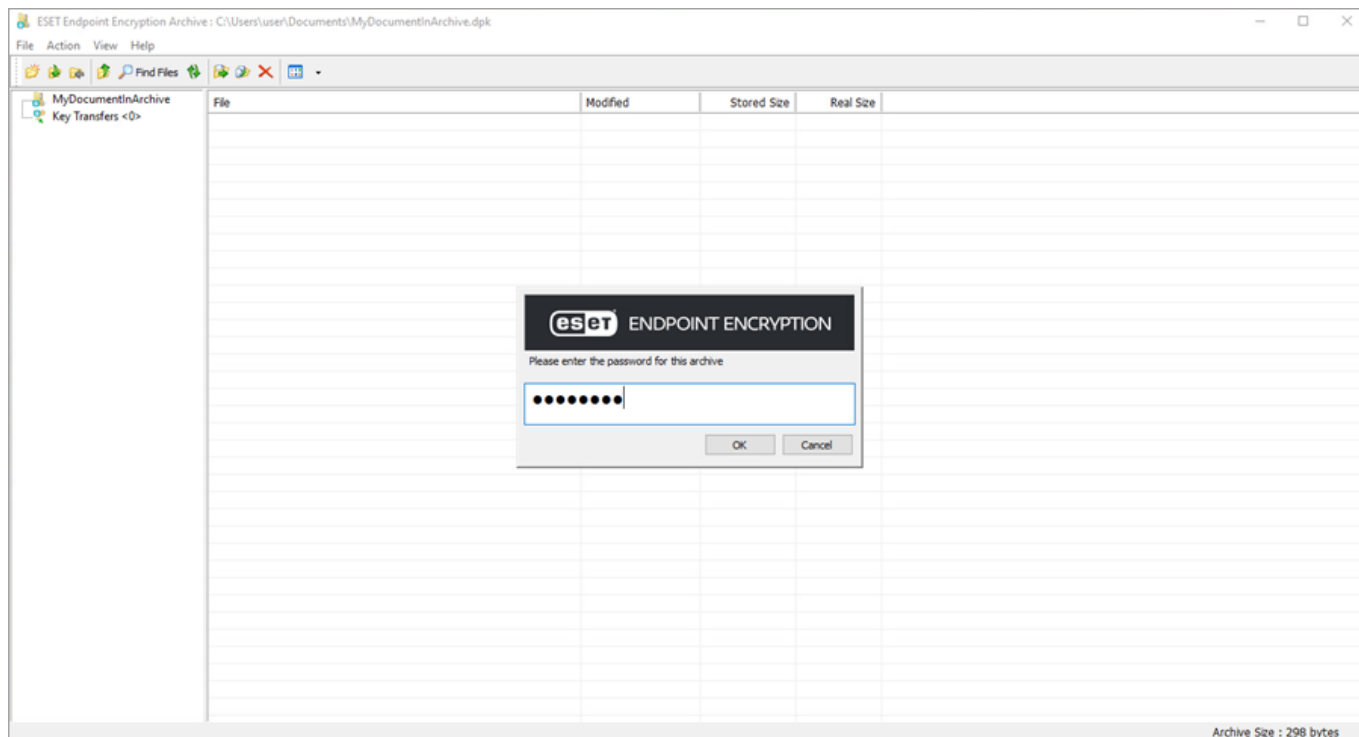
ESET Endpoint Encryption Archive is saved in the specified location and contains the selected file.



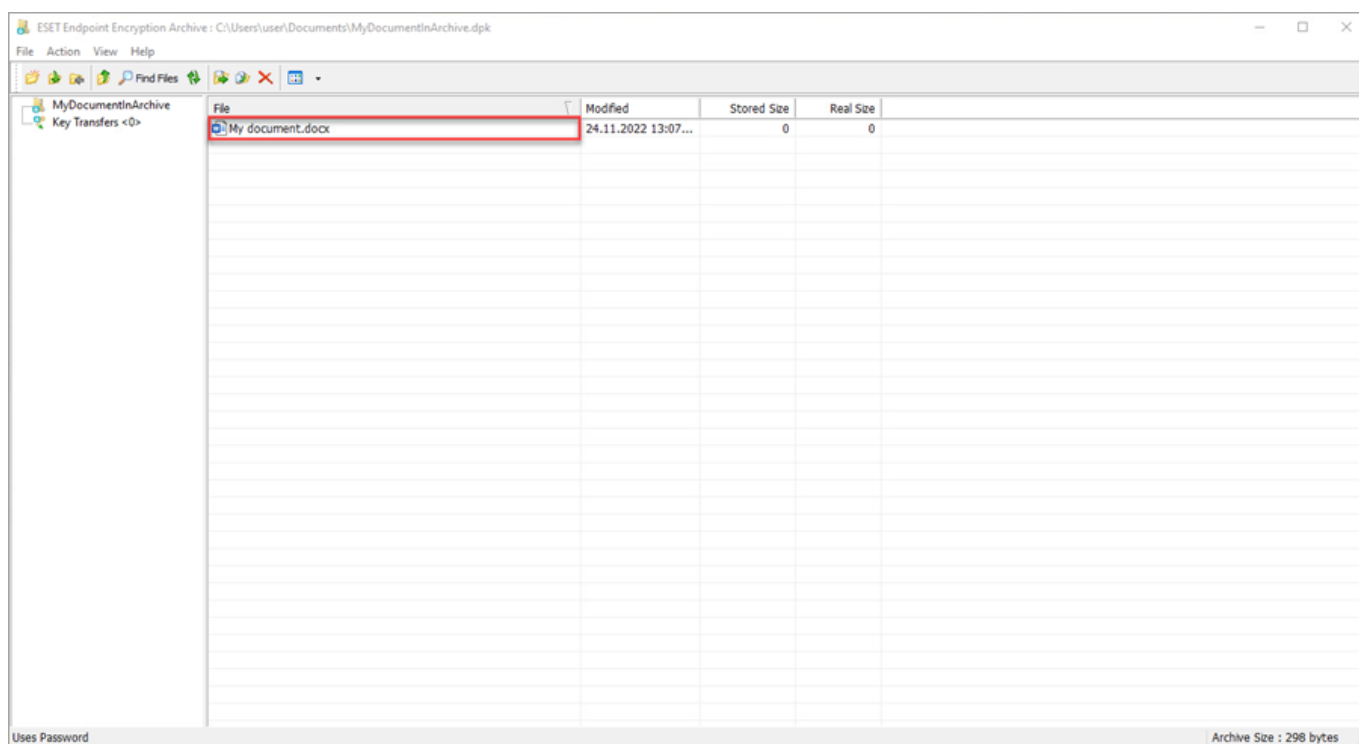
After you create the ESET Endpoint Encryption Archive, the original file still exists as a plain file (unencrypted).

Open files from the ESET Endpoint Encryption Archive

1. Double-click the ESET Endpoint Encryption Archive.
2. If your ESET Endpoint Encryption Archive is password-protected, type the password. If your ESET Endpoint Encryption Archive is protected by an Encryption Key, you must log in to ESET Endpoint Encryption and have access to the Encryption Key.



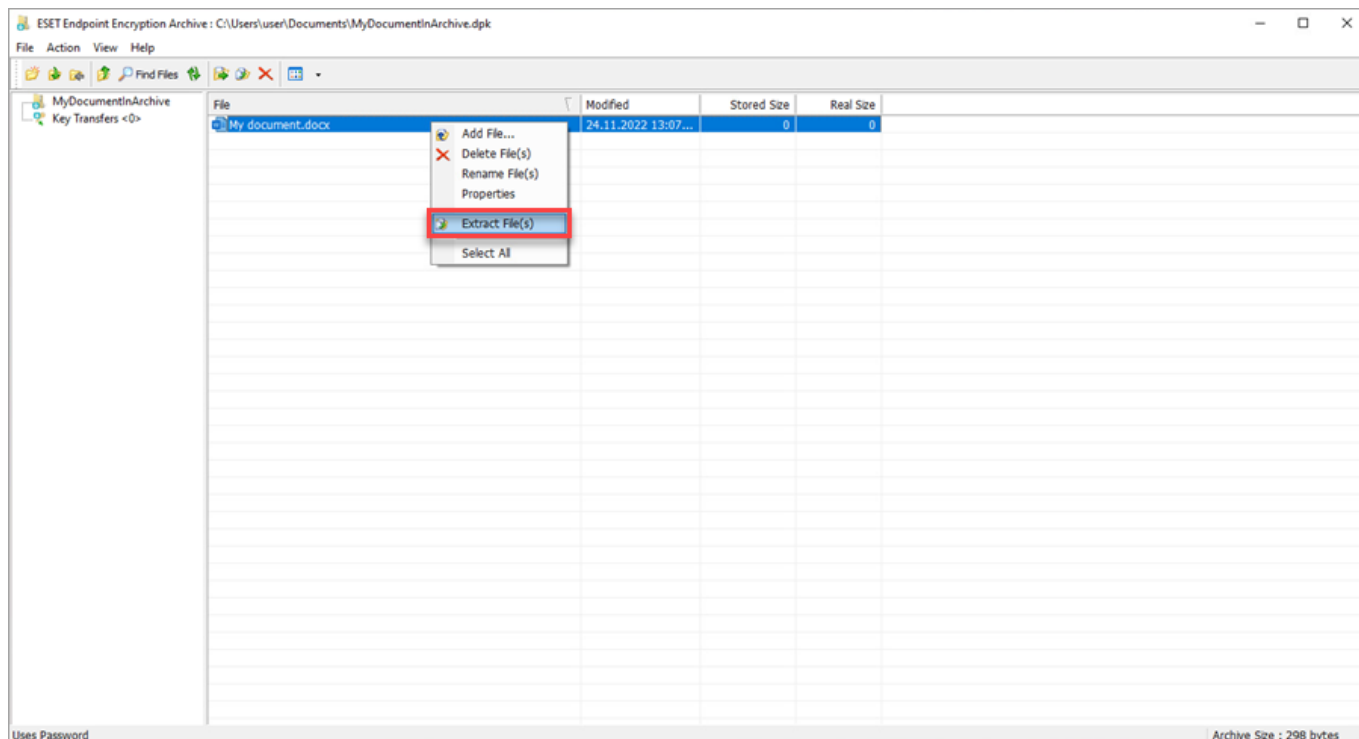
3. You can see Archive contents. To select a file to view, double-click the file.



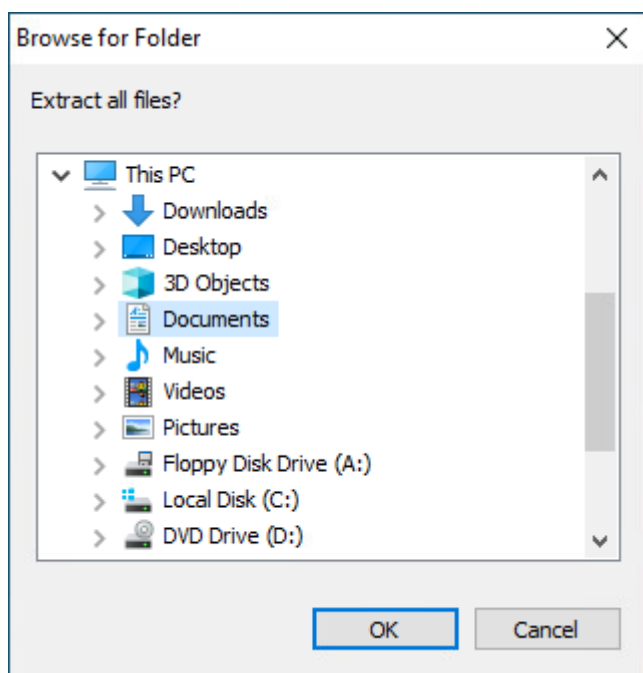
! To edit files, you must extract them first.

Extract files from the ESET Endpoint Encryption Archive

1. Open the ESET Endpoint Encryption Archive.
2. Right-click the file and click **Extract File(s)**.



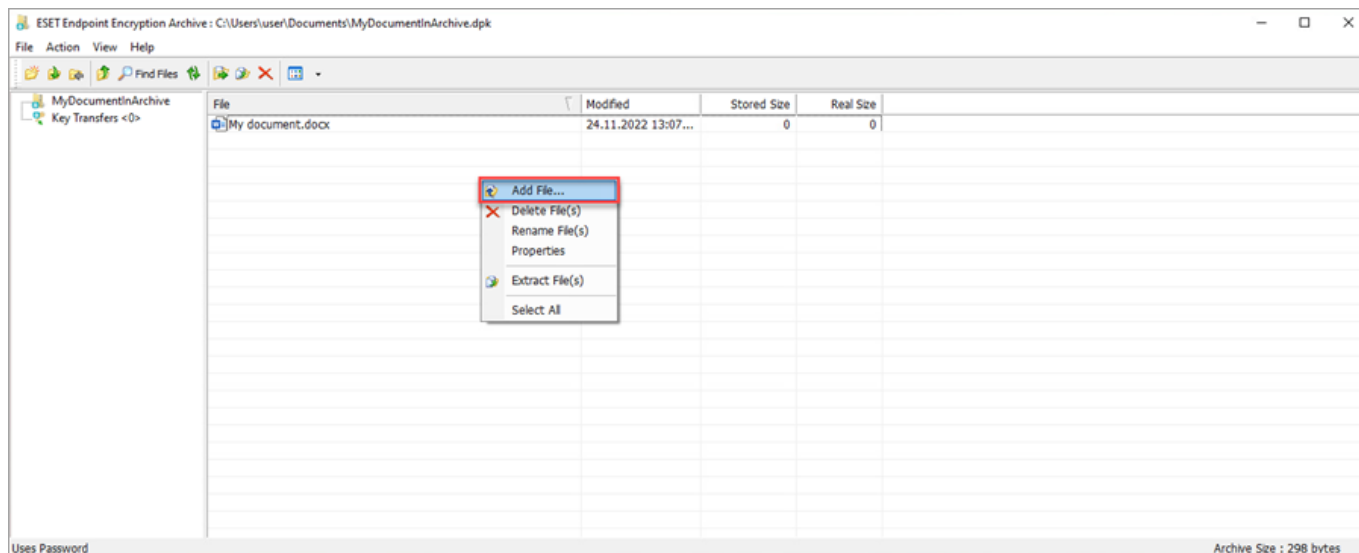
3. Select the extraction location for the decrypted file and click **OK**.



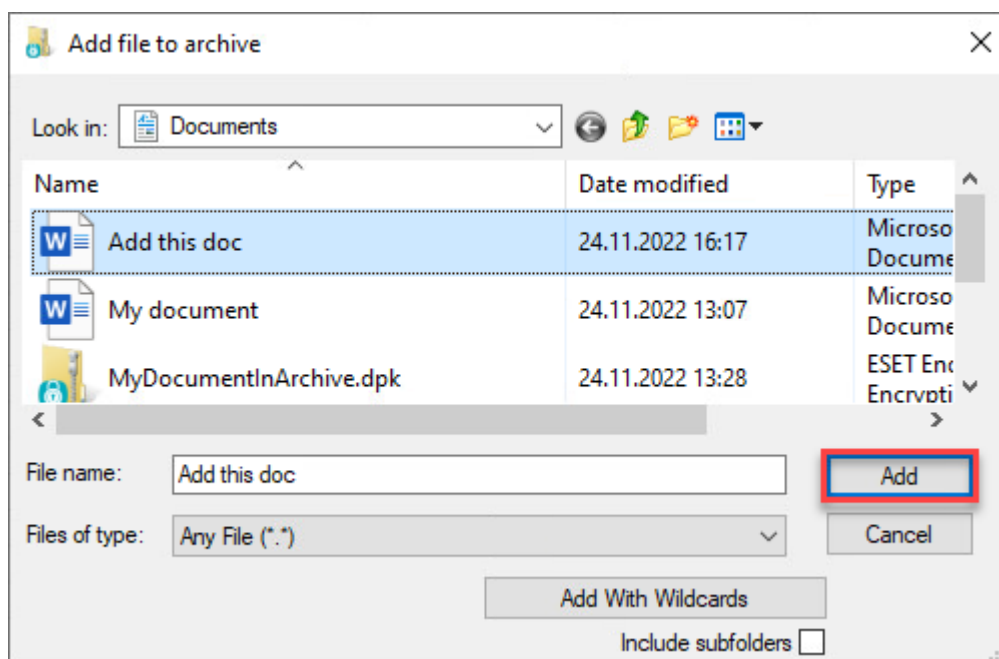
You can now edit the document from the specified location. After extraction, the file remains stored inside the ESET Endpoint Encryption Archive.

Add files to the ESET Endpoint Encryption Archive

1. Open the ESET Endpoint Encryption Archive.
2. Right-click in the blank space of the opened Archive and click **Add File**.



3. Locate the file and click **Add**.



4. The file is now displayed in the Archive window.

Key-File

The Key-File is an encryption key container that can hold up to 64 unique encryption keys.

These keys encrypt your computer, USB flash drive/hard drive, emails and files. The Key-File stores encryption keys, software settings, and organizational security policy.

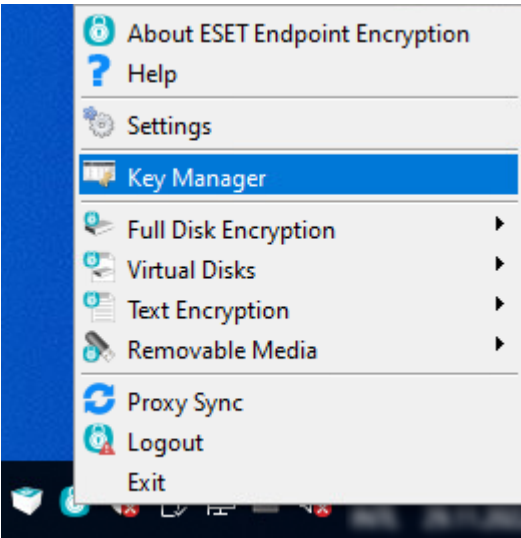
The Key-File is important because it is unique to your computer and organization; it acts as an identifier to allow communication between devices and parties via the same encryption key.

! Your ESET Endpoint Encryption Server administrator manages encryption key distribution for users.

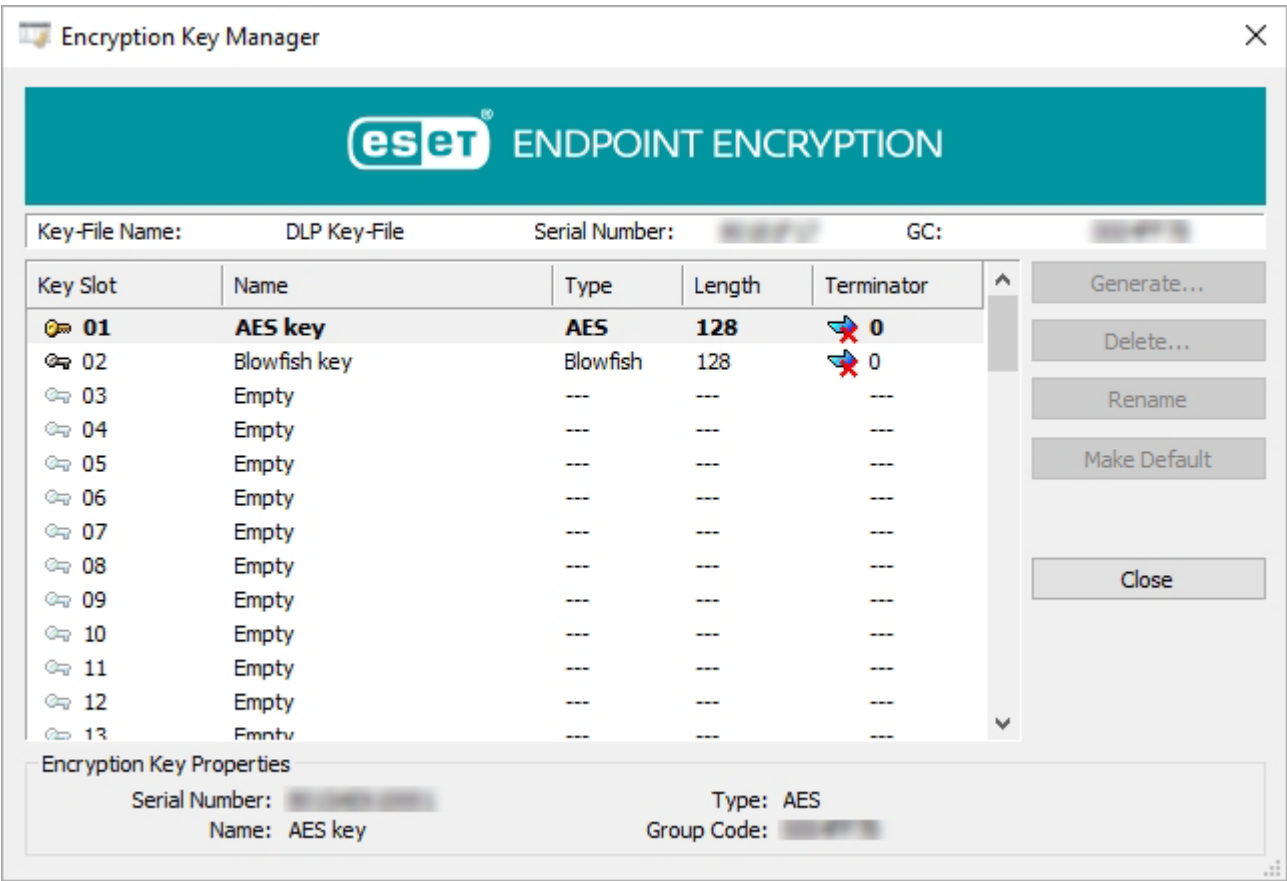
The Key-File is encrypted with your ESET Endpoint Encryption user password.

Encryption Key Manager

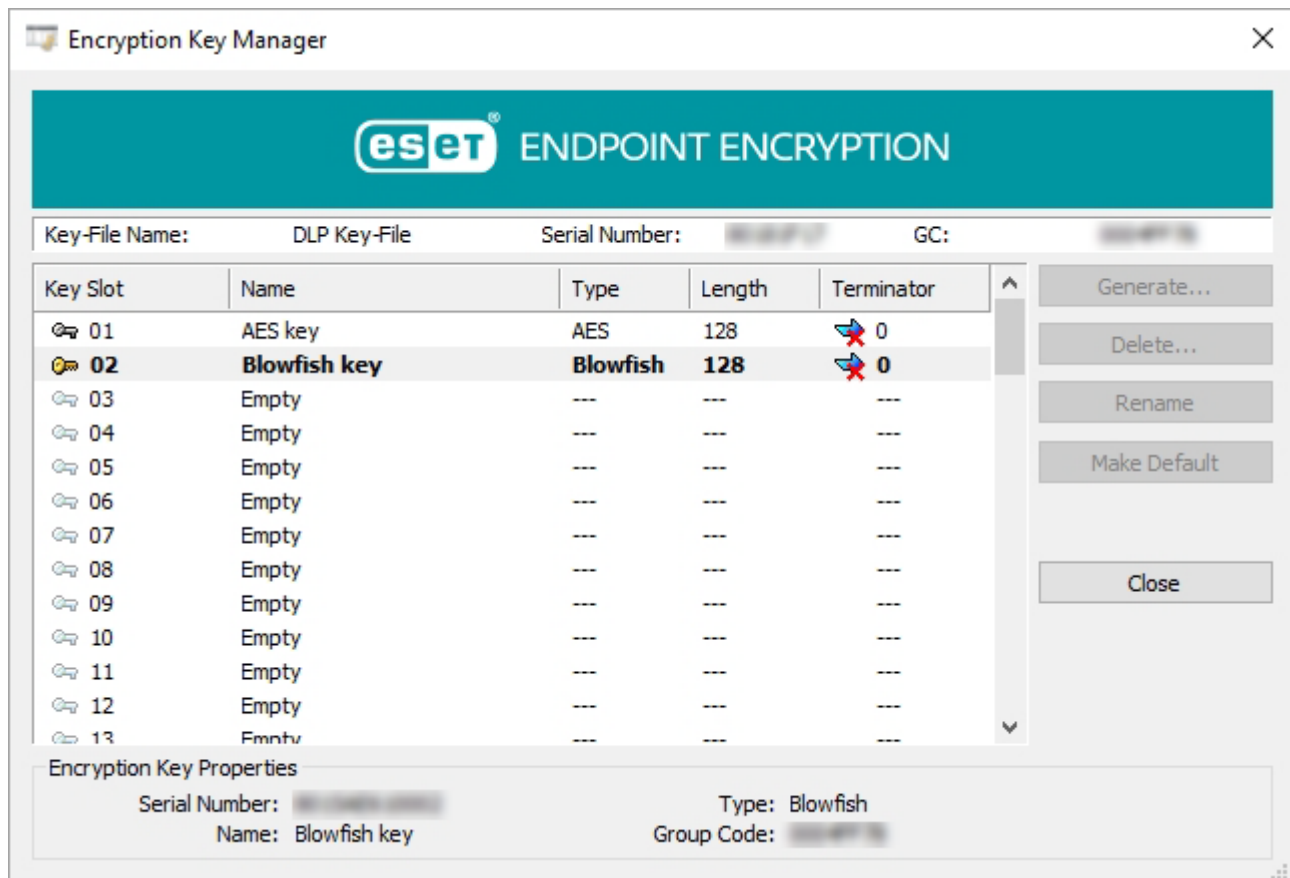
1. Right-click ESET Endpoint Encryption and click **Key Manager**.



2. The **Encryption Key Manager** window displays, and you can see the available encryption keys.



3. Select the Key and click **Make Default**. The **Key Slot** icon will change.



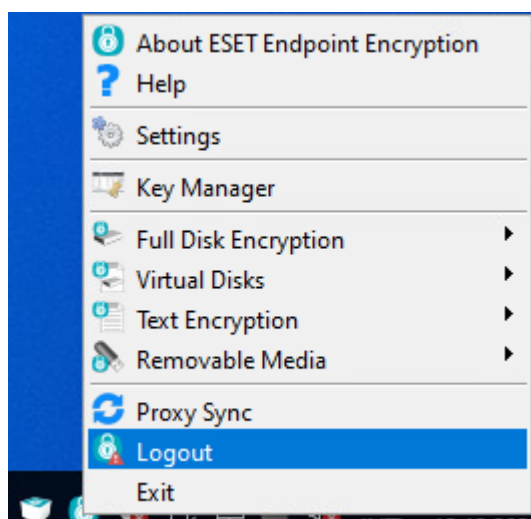
Managed users are not able to generate, delete or rename encryption keys.

Log in and out of the Key-File

Logging out of the Key-File protects all granular encrypted data, and the Workstation Policy settings resume. The group policy is only active while you are logged in to the Key-File. You cannot access the granular encrypted data, as the encryption key is only available when you log in again.

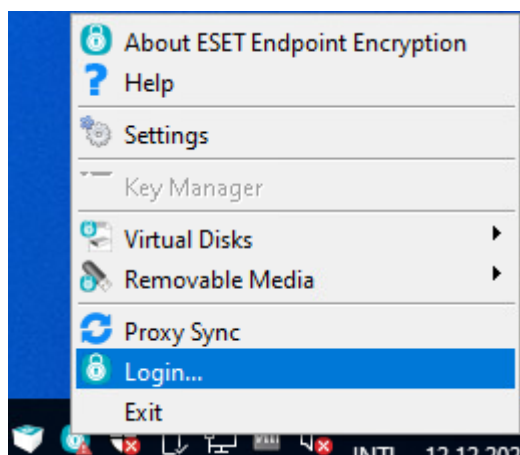
Logging out

Right-click the ESET Endpoint Encryption icon and click **Logout**.

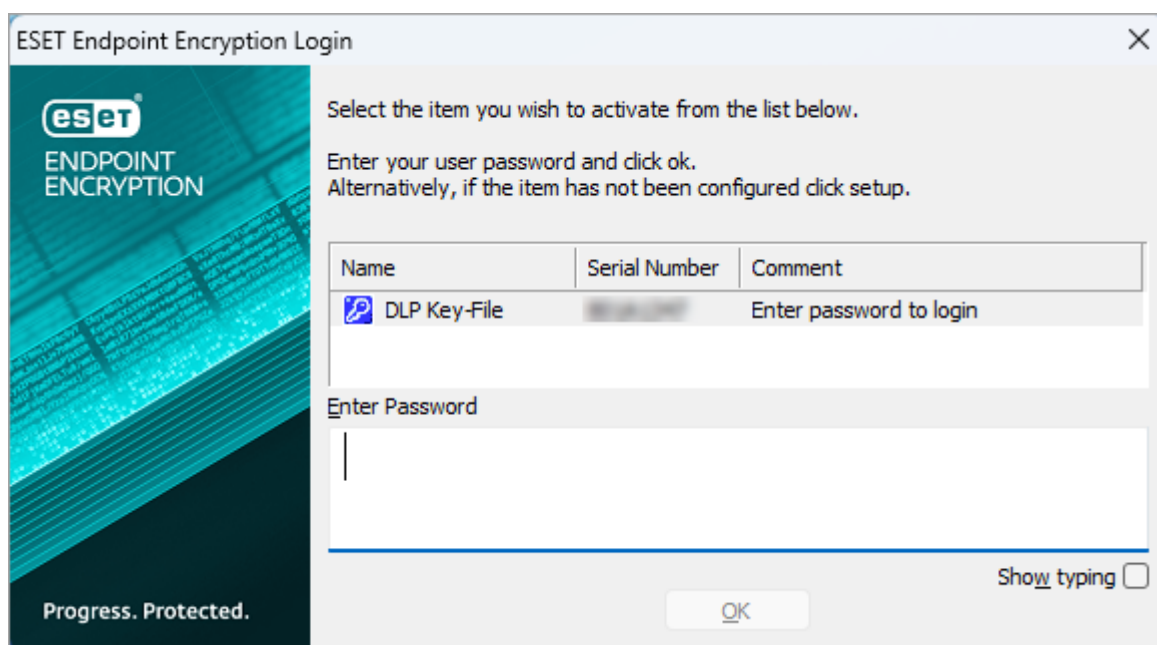


Logging in

1. Right-click the ESET Endpoint Encryption icon and click **Login**.



2. Type your Windows password and click **OK**.



In the default Group policy settings, the Key-File password is synchronized with your Windows password, so you must type your Windows password.

Pre-boot screen shortcuts

Keyboard shortcut	
F2	Press F2 to change the keyboard layout used by the FDE pre-boot. You can see the selected layout in the bottom left corner.
F5	Press F5 while entering your pre-boot password to reveal it in plain text.
F7	Press F7 to adjust the zoom.
F8	Press F8 to rotate the screen.
F10	Press F10 to shut down your machine.

Troubleshooting

[Single Sign-On \(SSO\) does not log in to Windows](#)

[Single Sign-On \(SSO\) and network passwords](#)

[Single Sign-ON \(SSO\) synchronization](#)

[Windows User context and ESET Endpoint Encryption](#)

[Encryption with network servers](#)

[Technical details for ESET Endpoint Encryption and Windows feature updates](#)

[Encrypt new removable or fixed disk in ESET Endpoint Encryption](#)

[Adjusting the graphical pre-boot FDE login screen in ESET Endpoint Encryption and ESET Full Disk Encryption](#)

Single Sign-On (SSO) does not log in to Windows

ESET Endpoint Encryption Full Disk Encryption configured for Single Sign-On is not logging in to Windows as expected.

Solution

Hibernate

When you hibernate your PC, the Full Disk Encryption Pre-boot authentication shows as expected. However, when Windows resumes, the login screen appears. This behavior is normal. When you return from Hibernate, Windows does not process its Automatic Logic feature. As a result, ESET Endpoint Encryption Single Sign-On is ignored.

Hard boot

If you shut down your PC and start it from a "cold" state, the Full Disk Encryption Pre-Boot authentication shows as expected. However, when Windows reaches the logic screen, nothing happens.

On Windows 8 and later, this behavior is caused by the **fast startup** feature. When **fast startup** is enabled, Windows uses Hibernate mode to speed up the loading process. This makes Windows behave as if you hibernate the PC instead of shutting it down.

In Windows 8, you can [disable fast startup](#), and Single Sign-On will work as expected.

To verify that fast startup is the issue, restart immediately after you set the Single Sign-On. If you are logged in to Windows automatically, fast startup is the issue. If you still experience the issue, [submit a support ticket](#).

Single Sign-On (SSO) and network password

And SSO-enabled user cannot log in after their network password has been changed. **Access Denied** appears on their pre-boot login screen.

If a Single Sign-On (SSO) enabled user cannot log in after their network password has been changed, the user's password has been changed on their Windows account externally. This can happen for several reasons:

- A user changed their password on another workstation.
- A user had their password changed on a server, such as when using Active Directory on the Domain server.
- A user attempted to change their password but has not been authenticated at the FDE login screen.

i The ESET Endpoint Encryption Full Disk Encryption login page is a pre-operating system and will not receive the change until the user has successfully logs in to their Windows account. When the user has successfully logged in to their Windows account, SSO will automatically re-sync during the Windows login process. The user changing their password must be successfully authenticated to start the workstation at the FDE login screen. The user must also have used their credentials to boot the machine.

Solution

At the pre-start login screen you should type your previous password. When you start Windows, you must log in to Windows manually, as SSO will not work. When you log into Windows, SSO will automatically re-sync, and you can use the new password on the next restart.

If you change your Windows account, the pre-boot login will be automatically updated, so SSO will still work.

Single Sign-On (SSO) synchronization

ESET Endpoint Encryption SSO synchronization is out of sync.

ESET Endpoint Encryption will automatically synchronize your Windows password with the ESET Endpoint Encryption Full Disk Encryption (FDE) pre-boot password when:

- you change your Windows password locally from your machine (using **CTRL + ALT + DEL - Change Password**)
- you sign into the Windows profile on your machine

The password can become out-of-sync when:


- you change your Windows password on another workstation
- an administrator changes your Windows password on a server (for example, using Active Directory on the Domain server)
- you attempt to change your Windows password, but the machine was booted using a different user's pre-boot credentials

Solution

You need to re-sync your machines individually, because SSO is controlled locally.

1. Go to the FDE pre-boot screen.
2. Type the old password and then the new password at the Windows screen (the sync will be performed when you log in to Windows).

Known SSO issue with ESET Endpoint Encryption version 4.9.4

 Following the Windows Feature update installation, you may find that SSO does not re-sync automatically after changing your Windows password. If you have been affected by this problem, [upgrade](#) to version 5.0.0 or later, follow the password recovery steps above, and log in to Windows manually to allow SSO to re-sync automatically.

Glossary

3DES (Triple DES)

3DES is a variant form of the DES (Data Encryption Standard) algorithm, originally developed by IBM in 1974. It uses 2 x 56-bit keys, giving an effective key length of 112 bits, and performs DES encryption three times using these keys.

AES

The Advanced Encryption Standard (AES) algorithm was developed under the name Rijndael by Joan Daemen and Vincent Rijmen, Belgian Ph.D. cryptographers from the computer security and industrial cryptography labs at Universiteit Leuven. Rijndael was accepted in October 2000 as the AES, which replaces the Data Encryption Standard (DES) algorithm. ESET Endpoint Encryption supports AES with a key length of up to 256 bits.

Blowfish

Blowfish was developed in 1993 by Bruce Schneier, a cryptographer, computer security specialist and author of several books on general security topics, computer security and cryptography. Blowfish is a 64-bit block cipher with a single 128-bit encryption key.

Complete security

ESET Endpoint Encryption Full Disk Encryption (FDE) provides security for unintended and unexpected events, such as theft or loss of a computer, laptop or USB flash drive.

When used on your computer, your hard drive, including the free space, is protected while the system is shut down. You must first enter pre-boot security before starting from this state.

All data remains encrypted if the drive is removed and read from another system.

ESET Endpoint Encryption for removable media also provides FDE for USB drives.

Data in transit versus Data at rest

Data in transit is information shared from one user to another via a trusted (private) network or an untrusted

(public) network, such as the internet, that can be protected with some form of granular encryption.

Data at rest is the information stored on your hard drive, backup drive or removable media when not in use.

ESET Endpoint Encryption Reader

The ESET Endpoint Encryption Reader is a free utility you can [download](#). ESET Endpoint Encryption Reader allows anyone, regardless of whether or not they are a ESET Endpoint Encryption customer, to decrypt any email, file or text that has been encrypted with ESET Endpoint Encryption using a password.

- The ESET Endpoint Encryption Reader utility is generally used on machines where ESET Endpoint Encryption is not installed.
- To decrypt an encrypted message, copy/paste the encrypted email body or text into the Reader and click the Decrypt button. Then, provide the password used to encrypt the text as decryption authentication.
- To decrypt an encrypted file, save the encrypted file to your machine. When saved, drag the encrypted file into the reader window, and you will be prompted for the password to decrypt it.
- The ESET Endpoint Encryption Reader is only for standalone files, and does not support archives.
- Files encrypted using a Key-File are not supported. Only files encrypted using the password are supported.
- See detailed information on how to [Encrypt or decrypt a document or email using the ESET Endpoint Encryption Reader](#).

Full Disk Encryption (FDE)

When using FDE to encrypt a computer disk, ESET Endpoint Encryption uses the Advanced Encryption Standard (AES) algorithm with a 256-bit key. This encryption is generated when FDE is started.

Granular encryption

Granular encryption refers to the protection of individual items like files, folders and emails.

File and email encryption allows users to share data and collaborate securely when data is in transit.

ESET Endpoint Encryption can encrypt folders on your hard drive or removable media. ESET Endpoint Encryption can also create encrypted virtual disks and compressed archives.

When you are logged in to ESET Endpoint Encryption, you can transparently access the files within encrypted folders and virtual disks.

Only encrypted data is protected if your computer hard drive is removed or removable media is read from another system.

Managed users

If you are a managed user, you can only view encryption keys that have been made available to you by your ESET Endpoint Encryption Server Administrator. Administrator can create new keys and allocate them via ESET Endpoint Encryption Server.

Password encryption

Password encryption uses a 192-bit AES key, not to be confused with **Removable Media Encryption (RME)**.

Removable Media Encryption (RME)

All data on removable media is encrypted by the AES algorithm with a 256-bit key, whether using Full Disk Encryption or File and Folder RME.

When you encrypt removable media, you select an encryption key from key-file using either AES, 3DES or Blowfish algorithms. An AES 256-bit key that will encrypt the data is then derived from the key you select. We recommend to use an encryption key to generate the AES 256-bit key. This method is more secure than a password or a pass-phrase as it and enables ESET Endpoint Encryption to provide seamless access to data on encrypted removable media when the end-use is logged into the key file.

End User License Agreement

Effective as of October 19, 2021.

IMPORTANT: Please read the terms and conditions of product application set out below carefully prior to download, installation, copy or use. **THROUGH DOWNLOADING, INSTALLING, COPYING OR USING THE SOFTWARE YOU ARE EXPRESSING YOUR CONSENT TO THESE TERMS AND CONDITIONS AND YOU ACKNOWLEDGE [PRIVACY POLICY](#).**

End User License Agreement

Under the terms of this End User License Agreement ("Agreement") executed by and between ESET, spol. s r. o., having its registered office at Einsteinova 24, 85101 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 ("ESET" or "Provider") and you, a physical person or legal entity ("You" or "End User"), You are entitled to use the Software defined in Article 1 of this Agreement. The Software defined in Article 1 of this Agreement can be stored on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources, subject to the terms and conditions specified below.

THIS IS AN AGREEMENT ON END USER RIGHTS AND NOT AN AGREEMENT FOR SALE. The Provider continues to own the copy of the Software and the physical media contained in the sales package and any other copies that the End User is authorized to make pursuant to this Agreement.

By clicking on "I Accept" or "I Accept..." while installing, downloading, copying or using the Software, You agree to the terms and conditions of this Agreement and acknowledge the Privacy Policy. If You do not agree to all of the terms and conditions of this Agreement and/or Privacy Policy, immediately click on the canceling option, cancel the installation or download, or destroy or return the Software, installation media, accompanying documentation and sales receipt to the Provider or the outlet from which You acquired the Software.

YOU AGREE THAT YOUR USE OF THE SOFTWARE ACKNOWLEDGES THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

1. Software. As used in this Agreement the term "Software" means: (i) computer program accompanied by this Agreement and all components thereof; (ii) all the contents of the disks, CD-ROMs, DVDs, e-mails and any attachments, or other media with which this Agreement is provided, including the object code form of the Software supplied on a data carrier, via electronic mail or downloaded via the Internet; (iii) any related

explanatory written materials and any other possible documentation related to the Software, above all any description of the Software, its specifications, any description of the Software properties or operation, any description of the operating environment in which the Software is used, instructions for use or installation of the Software or any description of how to use the Software ("Documentation"); (iv) copies of the Software, patches for possible errors in the Software, additions to the Software, extensions to the Software, modified versions of the Software and updates of Software components, if any, licensed to You by the Provider pursuant to Article 3 of this Agreement. The Software shall be provided exclusively in the form of executable object code.

2. Installation, Computer and a License key. Software supplied on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources requires installation. You must install the Software on a correctly configured Computer, complying at least with requirements set out in the Documentation. The installation methodology is described in the Documentation. No computer programs or hardware which could have an adverse effect on the Software may be installed on the Computer on which You install the Software. Computer means hardware, including but not limited to personal computers, laptops, workstations, palmtop computers, smartphones, hand-held electronic devices, or other electronic devices for which the Software is designed, on which it will be installed and/or used. License key means the unique sequence of symbols, letters, numbers or special signs provided to the End User in order to allow the legal use of the Software, its specific version or extension of the term of the License in compliance with this Agreement.

3. License. Subject to the condition that You have agreed to the terms of this Agreement and You comply with all the terms and conditions stipulated herein, the Provider shall grant You the following rights ("License"):

a) Installation and use. You shall have the non-exclusive, non-transferable right to install the Software on the hard disk of a Computer or other permanent medium for data storage, installation and storage of the Software in the memory of a computer system and to implement, store and display the Software.

b) Stipulation of the number of licenses. The right to use the Software shall be bound by the number of End Users. One End User shall be taken to refer to the following: (i) installation of the Software on one Computer; or (ii) if the extent of a license is bound to the number of mailboxes, then one End User shall be taken to refer to a Computer user who accepts electronic mail via a Mail User Agent ("MUA"). If MUA accepts electronic mail and subsequently distributes it automatically to several users, then the number of End Users shall be determined according to the actual number of users for whom the electronic mail is distributed. If a mail server performs the function of a mail gate, the number of End Users shall equal the number of mail server users for which the said gate provides services. If an unspecified number of electronic mail addresses are directed to and accepted by one user (e.g., through aliases) and messages are not automatically distributed by the client to a larger number of users, a License for one computer shall be required. You must not use the same License at the same time on more than one Computer. The End User is entitled to enter the License key to the Software only to the extent to which the End User has the right to use the Software in accordance with the limitation arising from the number of Licenses granted by Provider. The License key is deemed confidential, You must not share the License with third parties or allow third parties to use the License key unless permitted by this Agreement or Provider. If your License key is compromised, notify Provider immediately.

c) Home/Business Edition. A Home Edition version of the Software shall be used exclusively in private and/or non-commercial environments for home and family use only. A Business Edition version of the Software must be obtained for use in a commercial environment as well as to use the Software on mail servers, mail relays, mail gateways, or Internet gateways.

d) Term of the License. Your right to use the Software shall be time-limited.

e) OEM Software. Software classified as "OEM" shall be limited to the Computer You obtained it with. It cannot be transferred to a different Computer.

f) **NFR, TRIAL Software.** Software classified as "Not-for-resale", NFR or TRIAL cannot be assigned for payment and must only be used for demonstration or testing the Software's features.

g) **Termination of the License.** The License shall terminate automatically at the end of the period for which granted. If You fail to comply with any of the provisions of this Agreement, the Provider shall be entitled to withdraw from the Agreement, without prejudice to any entitlement or legal remedy open to the Provider in such eventualities. In the event of cancellation of the License, You must immediately delete, destroy or return at your own cost, the Software and all backup copies to ESET or to the outlet from which You obtained the Software. Upon termination of the License, the Provider shall also be entitled to cancel the End User's entitlement to use the functions of the Software, which require connection to the Provider's servers or third-party servers.

4. Functions with data collection and internet connection requirements. To operate correctly, the Software requires connection to the Internet and must connect at regular intervals to the Provider's servers or third-party servers and applicable data collection in compliance with Privacy Policy. Connection to the Internet and applicable data collection is necessary for functioning of the Software and for updating and upgrading the Software. The Provider shall be entitled to issue updates or upgrades to the Software ("Updates"), but shall not be obliged to provide Updates. This function is enabled under the Software's standard settings and Updates are therefore installed automatically, unless the End User has disabled the automatic installation of Updates. For provisioning of Updates, License authenticity verification is required, including information about Computer and/or the platform on which the Software is installed in compliance with Privacy Policy.

Provision of any Updates may be subject to End of Life Policy ("EOL Policy"), which is available on https://go.eset.com/eol_business. No Updates will be provided after the Software or any of its features reaches the End of Life date as defined in the EOL Policy.

For the purpose of this Agreement, it is necessary to collect, process and store data enabling the Provider to identify You in compliance with Privacy Policy. You hereby acknowledge that the Provider checks using its own means whether You are using the Software in accordance with the provisions of this Agreement. You hereby acknowledge that for the purpose of this Agreement it is necessary for your data to be transferred, during communication between the Software and the Provider's computer systems or those of its business partners as part of Provider's distribution and support network to ensure functionality of Software and authorization to use the Software and to protection of the Provider's rights.

Following conclusion of this Agreement, the Provider or any of its business partners as part of Provider's distribution and support network shall be entitled to transfer, process and store essential data identifying You for billing purposes, performance of this Agreement and transmitting notifications on your Computer.

Details about privacy, personal data protection and Your rights as a data subject can be found in Privacy Policy which is available on Provider's website and accessible directly from the installation process. You can also visit it from Software's help section.

5. Exercising End User rights. You must exercise End User rights in person or via your employees. You are only entitled to use the Software to safeguard your operations and protect those Computers or computers systems for which You have obtained a License.

6. Restrictions to rights. You may not copy, distribute, extract components or make derivative works of the Software. When using the Software, You are required to comply with the following restrictions:

a) You may make one copy of the Software on a permanent storage medium as an archival backup copy, provided your archival back-up copy is not installed or used on any Computer. Any other copies You make of the Software shall constitute a breach of this Agreement.

b) You may not use, modify, translate or reproduce the Software or transfer rights to use the Software or copies

of the Software in any manner other than as provided for in this Agreement.

c) You may not sell, sub-license, lease or rent or borrow the Software or use the Software for the provision of commercial services.

d) You may not reverse engineer, reverse compile or disassemble the Software or otherwise attempt to discover the source code of the Software, except to the extent that this restriction is expressly prohibited by law.

e) You agree that You will only use the Software in a manner that complies with all applicable laws in the jurisdiction in which You use the Software, including, but not limited to, applicable restrictions concerning copyright and other intellectual property rights.

f) You agree that You will only use the Software and its functions in a way which does not limit the possibilities of other End Users to access these services. The Provider reserves the right to limit the scope of services provided to individual End Users, to enable use of the services by the highest possible number of End Users. Limiting the scope of services shall also mean complete termination of the possibility to use any of the functions of the Software and deletion of Data and information on the Provider's servers or third-party servers relating to a specific function of the Software.

g) You agree not to exercise any activities involving use the License key, contrary to the terms of this Agreement or leading to provide License key to any person who is not entitled to use the Software, such as the transfer of used or unused License key in any form, as well as the unauthorized reproduction, or distribution of duplicated or generated License keys or using the Software as a result of the use of a License key obtained from the source other than the Provider.

7. Copyright. The Software and all rights, without limitation including proprietary rights and intellectual property rights thereto are owned by ESET and/or its licensors. They are protected by international treaty provisions and by all other applicable national laws of the country in which the Software is being used. The structure, organization and code of the Software are the valuable trade secrets and confidential information of ESET and/or its licensors. You must not copy the Software, except as set forth in Article 6(a). Any copies which You are permitted to make pursuant to this Agreement must contain the same copyright and other proprietary notices that appear on the Software. If You reverse engineer, reverse compile, disassemble or otherwise attempt to discover the source code of the Software, in breach of the provisions of this Agreement, You hereby agree that any information thereby obtained shall automatically and irrevocably be deemed to be transferred to and owned by the Provider in full, from the moment such information comes into being, notwithstanding the Provider's rights in relation to breach of this Agreement.

8. Reservation of rights. The Provider hereby reserves all rights to the Software, with the exception of rights expressly granted under the terms of this Agreement to You as the End User of the Software.

9. Multiple language versions, dual media software, multiple copies. In the event that the Software supports multiple platforms or languages, or if You receive multiple copies of the Software, You may only use the Software for the number of computer systems and for the versions for which You obtained a License. You may not sell, rent, lease, sub-license, lend or transfer versions or copies of the Software which You do not use.

10. Commencement and termination of the Agreement. This Agreement shall be effective from the date You agree to the terms of this Agreement. You may terminate this Agreement at any time by permanently uninstalling, destroying and returning, at your own cost, the Software, all backup copies and all related materials provided by the Provider or its business partners. Your right to use Software and any of its features may be subject to EOL Policy. After the Software or any of its features reaches the End of Life date defined in the EOL Policy, your right to use the Software will terminate. Irrespective of the manner of termination of this Agreement, the provisions of Articles 7, 8, 11, 13, 19 and 21 shall continue to apply for an unlimited time.

11. END USER DECLARATIONS. AS THE END USER YOU ACKNOWLEDGE THAT THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. NEITHER THE PROVIDER, ITS LICENSORS OR AFFILIATES, NOR THE COPYRIGHT HOLDERS MAKE ANY REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR THAT THE SOFTWARE WILL NOT INFRINGE ANY THIRD-PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. THERE IS NO WARRANTY BY THE PROVIDER OR BY ANY OTHER PARTY THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE. YOU ASSUME ALL RESPONSIBILITY AND RISK FOR THE SELECTION OF THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS AND FOR THE INSTALLATION, USE AND RESULTS OBTAINED FROM IT.

12. No other obligations. This Agreement creates no obligations on the part of the Provider and its licensors other than as specifically set forth herein.

13. LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE PROVIDER, ITS EMPLOYEES OR LICENSORS BE LIABLE FOR ANY LOST PROFITS, REVENUE, SALES, DATA OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, PROPERTY DAMAGE, PERSONAL INJURY, INTERRUPTION OF BUSINESS, LOSS OF BUSINESS INFORMATION OR FOR ANY SPECIAL, DIRECT, INDIRECT, INCIDENTAL, ECONOMIC, COVER, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND WHETHER ARISING UNDER CONTRACT, TORT, NEGLIGENCE OR OTHER THEORY OF LIABILITY, ARISING OUT OF THE INSTALLATION, THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF THE PROVIDER OR ITS LICENSORS OR AFFILIATES ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME COUNTRIES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF LIABILITY, BUT MAY ALLOW LIABILITY TO BE LIMITED, IN SUCH CASES, THE LIABILITY OF THE PROVIDER, ITS EMPLOYEES OR LICENSORS OR AFFILIATES SHALL BE LIMITED TO THE SUM THAT YOU PAID FOR THE LICENSE.

14. Nothing contained in this Agreement shall prejudice the statutory rights of any party dealing as a consumer if running contrary thereto.

15. Technical support. ESET or third parties commissioned by ESET shall provide technical support at their own discretion, without any guarantees or declarations. No technical support will be provided after the Software or any of its features reaches the End of Life date defined in the EOL Policy. The End User shall be required to back up all existing data, software and program facilities prior to the provision of technical support. ESET and/or third parties commissioned by ESET cannot accept liability for damage or loss of data, property, software or hardware or loss of profits due to the provision of technical support. ESET and/or third parties commissioned by ESET reserve the right to decide that resolving the problem is beyond the scope of technical support. ESET reserves the right to refuse, suspend or terminate the provision of technical support at its own discretion. License information, Information and other data in compliance with Privacy Policy may be required for the purpose of technical support provision.

16. Transfer of the License. The Software can be transferred from one Computer to another, unless contrary to the terms of the Agreement. If not contrary to the terms of the Agreement, the End User shall only be entitled to permanently transfer the License and all rights ensuing from this Agreement to another End User with the Provider's consent, subject to the condition that (i) the original End User does not retain any copies of the Software; (ii) the transfer of rights must be direct, i.e. from the original End User to the new End User; (iii) the new End User must assume all the rights and obligations incumbent on the original End User under the terms of this Agreement; (iv) the original End User has to provide the new End User with documentation enabling verification of the genuineness of the Software as specified under Article 17.

17. Verification of the genuineness of the Software. The End User may demonstrate entitlement to use the Software in one of the following ways: (i) through a license certificate issued by the Provider or a third party appointed by the Provider; (ii) through a written license agreement, if such an agreement was concluded; (iii)

through the submission of an e-mail sent by the Provider containing licensing details (user name and password). License information and End User identification data in compliance with Privacy Policy may be required for the purpose of Software genuineness verification.

18. Licensing for public authorities and the US Government. The Software shall be provided to public authorities, including the United States Government, with the license rights and restrictions described in this Agreement.

19. Trade control compliance.

a) You will not, directly or indirectly, export, re-export, transfer or otherwise make available the Software to any person, or use it in any manner, or be involved in any activity, that could result in ESET or its holding companies, its subsidiaries, and the subsidiaries of any of its holding companies, as well as entities controlled by its holding companies ("Affiliates") being in violation of, or being subject to, negative consequences under trade control laws which include:

i. any laws that control, restrict, or impose licensing requirements on export, re-export or transfer of goods, software, technology, or services, issued or adopted by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under the Agreement are to be performed, or in which ESET or any of its Affiliates are incorporated or operate, and

ii. any economic, financial, trade or other, sanction, restriction, embargo, import or export ban, prohibition on transfer of funds or assets or on performing services, or equivalent measure imposed by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under the Agreement are to be performed, or in which ESET or any of its Affiliates are incorporated or operate.

(legal acts referred to in points i, and ii. above together as "Trade Control Laws").

b) ESET shall have the right to suspend its obligations under, or terminate, these Terms with immediate effect in the event that:

i. ESET determines that, in its reasonable opinion, the User has breached or is likely to breach provision of Article 19 a) of the Agreement; or

ii. the End User and/or the Software become subject to Trade Control Laws and, as a result, ESET determines that, in its reasonable opinion, the continued performance of its obligations under the Agreement could result in ESET or its Affiliates being in violation of, or being subject to negative consequences under, Trade Control Laws.

c) Nothing in the Agreement is intended, and nothing should be interpreted or construed, to induce or require either party to act or refrain from acting (or to agree to act or refrain from acting) in any manner which is inconsistent with, penalized, or prohibited under any applicable Trade Control Laws.

20. Notices. All notices and returns of the Software and Documentation must be delivered to: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, without prejudice to ESET's right to communicate to You any changes to this Agreement, Privacy Policies, EOL Policy and Documentation in accordance with art. 22 of the Agreement. ESET may send You emails, in-app notifications via Software or post the communication on our website. You agree to receive legal communications from ESET in electronic form, including any communications on change in Terms, Special Terms or Privacy Policies, any contract proposal/acceptance or invitations to treat, notices or other legal communications. Such electronic communication shall be deemed as received in writing, unless applicable laws specifically require a different form of communication.

21. Applicable law. This Agreement shall be governed by and construed in accordance with the laws of the Slovak

Republic. The End User and the Provider hereby agree that the principles of the conflict of laws and the United Nations Convention on Contracts for the International Sale of Goods shall not apply. You expressly agree that any disputes or claims ensuing from this Agreement with respect to the Provider or any disputes or claims relating to use of the Software shall be settled by Bratislava I District Court and You expressly agree to the said court exercising jurisdiction.

22. General provisions. Should any of the provisions of this Agreement be invalid or unenforceable, this shall not affect the validity of the other provisions of the Agreement, which shall remain valid and enforceable under the conditions stipulated therein. This Agreement has been executed in English. In case any translation of the Agreement is prepared for the convenience or any other purpose or in any case of a discrepancy between language versions of this Agreement, the English version shall prevail.

ESET reserves the right to make changes to the Software as well as to revise terms of this Agreement, its Annexes, Addendums, Privacy Policy, EOL Policy and Documentation or any part thereof at any time by updating the relevant document (i) to reflect changes to the Software or to how ESET does business, (ii) for legal, regulatory or security reasons, or (iii) to prevent abuse or harm. You will be notified about any revision of the Agreement by email, in-app notification or by other electronic means. If You disagree with the proposed changes to the Agreement, You may terminate it in accordance with Art. 10 within 30 days after receiving a notice of the change. Unless You terminate the Agreement within this time limit, the proposed changes will be deemed accepted and become effective towards You as of the date You received a notice of the change.

This is the entire Agreement between the Provider and You relating to the Software and it supersedes any prior representations, discussions, undertakings, communications or advertising relating to the Software.

ADDENDUM TO THE AGREEMENT

Patents. Additional provisions apply to the Software as follows:

The Software contains and is protected by Patents GB 2378539, US 7099478, US 7471796, EU 1423765 (ES, FI, FR, UK, IE, IT, NL, DE, SE), RU 2273959, CN 02820752-1, IN 231403, IL 160709.

EULAID: EULA-PRODUCT-EEE; 3537.0

Privacy Policy

ESET, spol. s r. o., having its registered office at Einsteinova 24, 851 01 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 as a Data Controller ("ESET" or "We") would like to be transparent when it comes to processing of personal data and privacy of our customers. To achieve this goal, We are publishing this Privacy Policy with the sole purpose of informing our customer ("End User" or "You") about following topics:

- Processing of Personal Data,
- Data Confidentiality,
- Data Subject's Rights.

Processing of Personal Data

Services provided by ESET implemented in our product are provided under the terms of End User License Agreement ("EULA"), but some of them might require specific attention. We would like to provide You with more details on data collection connected with the provision of our services. We render various services described in

the EULA and product documentation such as update/upgrade service, ESET LiveGrid®, protection against misuse of data, support, etc. To make it all work, We need to collect the following information:

- Update and other statistics covering information concerning version of product and request for update.
- Licensing information such as license ID and personal data such as name, surname, address, email address is required for billing purposes, license genuineness verification and provision of our services.
- Contact information and data contained in your support requests may be required for service of support. Based on the channel You choose to contact us, We may collect your email address, phone number, license information, product details and description of your support case. You may be asked to provide us with other information to facilitate service of support.

Data Confidentiality

ESET is a company operating worldwide via affiliated entities or partners as part of our distribution, service and support network. Information processed by ESET may be transferred to and from affiliated entities or partners for performance of the EULA such as provision of services or support or billing. Based on your location and service You choose to use, We might be required to transfer your data to a country with absence of adequacy decision by the European Commission. Even in this case, every transfer of information is subject to regulation of data protection legislation and takes place only if required. Standard Contractual Clauses, Binding Corporate Rules or another appropriate safeguard must be established without any exception.

We are doing our best to prevent data from being stored longer than necessary while providing services under the EULA. Our retention period might be longer than the validity of your license just to give You time for easy and comfortable renewal. Minimized and pseudonymized statistics and other data from ESET LiveGrid® may be further processed for statistical purposes.

ESET implements appropriate technical and organizational measures to ensure a level of security which is appropriate to potential risks. We are doing our best to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and Services. However, in case of data breach resulting in a risk to your rights and freedoms, We are ready to notify supervisory authority as well as data subjects. As a data subject, You have a right to lodge a complaint with a supervisory authority.

Data Subject's Rights

ESET is subject to regulation of Slovak laws and We are bound by data protection legislation as part of European Union. Subject to conditions laid down by applicable data protection laws, You are entitled to following rights as a data subject:

- right to request access to your personal data from ESET,
- right to rectification of your personal data if inaccurate (You also have the right to have the incomplete personal data completed),
- right to request erasure of your personal data,
- right to request restriction of processing your personal data,
- right to object to processing,
- right to lodge a complaint as well as,
- right to data portability.

We believe that every information we process is valuable and necessary for the purpose of our legitimate interest which is provision of services and products to our customers.

If You would like to exercise your right as a data subject or You have a question or concern, send us a message at:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk