

ESET Full Disk Encryption

User guide

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

Copyright ©2024 by ESET, spol. s r.o.

ESET Full Disk Encryption 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. 3/18/2024

1 About help	1
2 Changelog	1
3 Product Overview	2
3.1 System requirements	2
3.2 EFDE for MAC	3
4 Purchase the service	3
5 Use ESET Full Disk Encryption	4
6 Enable and configure ESET Full Disk Encryption	4
6.1 Encryption options	6
6.2 Password policies	7
6.3 User interface	9
6.4 Tools	9
6.5 EFDE Client deployment	10
6.5 EFDE All-in-one Installer	10
6.5 EFDE Software Install task	11
6.5 Enable encryption wizard	12
6.6 Deploy ESET Full Disk Encryption via command line	14
6.6 Deploy an installer with a pre-defined password	14
6.6 Invalidate password via command line	15
6.6 Pause/Resume FDE authentication via command line	16
6.6 Add/Remove keyboard layouts via command line	17
7 EFDE client-side encryption process	17
8 Encryption management	19
8.1 Pause FDE authentication	20
9 Pre-boot login	23
9.1 Pre-boot screen shortcuts	24
10 Encryption recovery	25
10.1 Recovery password	25
10.2 Recovery data	28
11 Decryption/Uninstallation	33
12 Common questions	35
13 Troubleshooting	36
14 Privacy Policy	38
15 End User License Agreement	41

About help

This help explains how to use and manage ESET Full Disk Encryption. It also details the connection of ESET Full Disk Encryption to other ESET business products.

We use a uniform set of symbols to highlight topics of specific interest or significance. Topics are divided into several chapters and sub-chapters. You can find relevant information by using the Search field at the top.

[Online help](#) is the primary source of help content. The latest version of Online help will automatically be displayed when you have a working internet connection.

- The [ESET Knowledgebase](#) contains answers to the most frequently asked questions, as well as recommended solutions for various issues. Regularly updated by ESET technical specialists, the Knowledgebase is the most powerful tool for resolving various types of problems.
- The [ESET Forum](#) provides ESET users with an easy way to get help and to help others. You can post any problem or question related to your ESET products.
- You can post your rating and/or provide feedback on a specific topic in help, click **Was this information helpful?** to rate the article and add your comment.

Text boxes:



Notes can provide valuable information, such as specific features or a link to some related topic.



This requires your attention and it should not be skipped. Usually, it provides non-critical but significant information.



Critical information you should treat with increased caution. Warnings are placed specifically to deter you from committing potentially harmful mistakes. Please read and understand text placed in warning brackets, as it references highly sensitive system settings or something risky.



Example case which describes a user case relevant for the topic where it is included. Examples are used to explain more complicated topics.

Changelog

ESET Full Disk Encryption for Windows

ESET Full Disk Encryption for macOS

Product Overview


ESET Full Disk Encryption (EFDE) is an add-on feature native to ESET remote management consoles - ESET PROTECT On-Prem and ESET PROTECT. EFDE's main feature is the management of full disk encryption of managed Windows and [macOS](#) workstations with additional security layer in pre-boot login. EFDE is fully compatible with ESET PROTECT On-Prem, and ESET PROTECT functions like Groups, Policies, Tasks, and Reports.

System requirements

Supported OS for EFDE Client application:


ESET Full Disk Encryption for Windows	32-bit	64-bit
Windows 11	N/A	✓
Windows 10	✓	✓

ESET Full Disk Encryption for macOS	Supported
macOS 14.0 Sonoma	✓
macOS 13.0 Ventura	✓
macOS 12.0 Monterey	✓
macOS 11.0 Big Sur	✓
macOS 10.15 Catalina	✓
macOS 10.14 Mojave	✓

 Do not install EFDE Client application on the same workstation as your ESET PROTECT Server database.


Compatibility:

- Legacy/BIOS firmware is not supported. ESET Full Disk Encryption requires a UEFI-capable system.
- GPT Partition Schemed Disks, which are part of NTFS (New Technology Files System), are supported for BOOT Disks. MBR Partition Schemed Disks (also part of NTFS) are supported for any DATA (secondary) Disks.
- ESET Full Disk Encryption supports Apple M1 Mac with [Rosetta installed](#).
- ESET Full Disk Encryption does not support ARM processors on Windows.
- ESET Full Disk Encryption is not supported on dual-boot or software RAID systems.
- ESET Full Disk Encryption is not compatible with Apple Mac system using Apple Boot Camp.
- ESET Full Disk Encryption does not support Microsoft Storage Spaces and Dynamic Disks.
- Use software with Windows Insider Previews for testing purposes only, as data may be at risk.
- DirectX 9 graphics device with WDDM 1.0 or later driver.
- Full Disk Encryption of system disks supports only 512-byte size sectors.

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

You can use ESET Full Disk Encryption in a virtual machine environment on a PC or Mac Hypervisors:

- VMware Workstation 16.2.3
- VMware ESXi 7.0 / vSphere 7.0.3.00300
- VMware Fusion 12.2.3
- Parallels
- Microsoft Hyper-V (secure boot not supported)

 The same compatibility rules apply for the guest operating system; for example, ESET Full Disk Encryption for Windows is not supported on ARM and cannot be used in Windows virtualized on Apple ARM CPUs.

Management console requirements:

- **ESET PROTECT** or **ESET PROTECT On-Prem 8.0+**
- **ESET Management Agent version 7.1+** for Windows.
- **ESET Management Agent version 8.0+** for macOS.

EFDE for MAC

ESET Full Disk Encryption for macOS utilizes Apple's native full-disk encryption application called FileVault2 to encrypt the managed workstation, which provides the user and the administrator a streamlined encryption process. ESET Full Disk Encryption for macOS provides remote encryption or decryption of the managed workstation in addition to a reporting of the state of the encryption to the management console - helping to solve numerous data security compliance regulations.

Purchase the service

ESET Full Disk Encryption requires a separate license for product activation. ESET Full Disk Encryption is an add-on feature of the management console so that it can be purchased only as an addition to a new or existing ESET business solution license. The customer can only purchase the maximum number of seats that match their endpoint license seat count. An ESET Full Disk Encryption license can be purchased from your local ESET reseller. After you have received your license, import it to your [ESET Business Account](#). This will unlock all ESET Full Disk Encryption features of the management console.

Contact us

Locate your [ESET partner](#) for any questions related to licensing and buying the service. You can contact ESET support via email, chat, or phone; see our [contact information page](#) for details.

Use ESET Full Disk Encryption

After successfully importing the ESET Full Disk Encryption license, the next steps are:

1. [Create an EFDE configuration policy](#).
2. [Deploy EFDE client on the workstations](#).
3. The user of each workstation needs to create its [pre-boot login](#) password.
4. After a successful encryption process, the designated disks on the workstation are now encrypted and protected.



Enable and configure ESET Full Disk Encryption



If you encounter an error **Your computer is not encrypted, and data at rest is not protected** follow the steps below to set up computer encryption and resolve the error.




ESET Full Disk Encryption version 1.4 (and later) supports the [automatic updates](#) (configurable via a [Policy](#)).

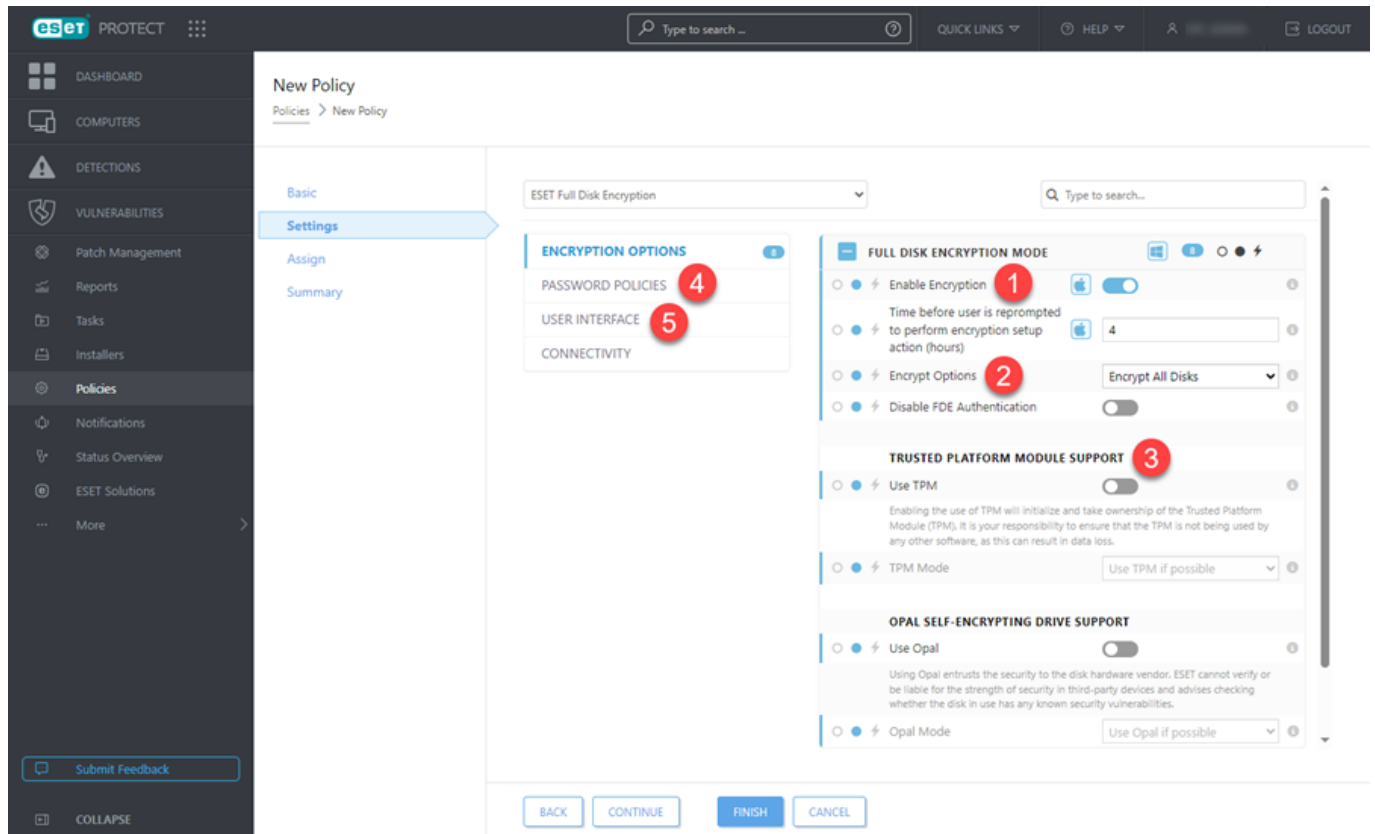
You can configure ESET Full Disk Encryption settings via policy in ESET Security Management Center, ESET PROTECT On-Prem or ESET PROTECT: select **Policies > New Policy > Settings** > select the product **ESET Full Disk Encryption** from the drop-down menu.

Here you can create your desired EFDE configuration:



Policy options available for macOS are marked with .

1. Under **Encryption options -> Full Disk Encryption Mode** enable the **Enable Encryption** setting. This setting enables/disables encryption on the managed workstation.



2. Under **Encryption Options**, decide if you want to **Encrypt All Disks** or **Encrypt Boot Disk Only**.

3. To use **Trusted Platform Module support (TPM)** or **OPAL Self-encrypting drive support (OPAL)** for your encryption, select the applicable option based on the hardware available on the managed workstations.

4. Under **Password Policies** -> **User Password Requirements**, specify the requirements for the pre-boot password the user will use to log in to their workstation.

5. Under **User Interface** -> **User Interface Elements**, you can specify the behavior of the EFDE client running on the workstations.

6. Click **Finish** to save the policy. Do not assign the policy yet; you can apply the policy after EFDE is deployed to the client workstation.





7. Before starting the encryption, [deploy the EFDE client](#) on the workstations.

See the full description of configuration options for ESET Full Disk Encryption:



- [Password Policies](#)
- [Encryption Options](#)
- [User Interface](#)
- [Tools](#)

Encryption options

Full Disk Encryption Mode


-  **Enable Encryption** - This setting enables/disables the encryption on the device. If a policy with the **Disabled** setting is applied to an encrypted workstation, it will be decrypted.
-  **Time before user is reprompted to perform encryption setup action (hours)** - The maximum value is 24 hours. Defines the interval in hours how often is user prompted to setup the encryption password on his workstation.
-  **Encrypt Options:**
 - o**Encrypt All Disks** - Encrypts all physical disks on the workstation. External HDD and USB drives are not affected.
 - o**Encrypt Boot Disk Only** - Encrypts only the physical disk that is used as a current Windows boot drive.
-  **Disable FDE Authentication** - This setting enables/ disables the pre-boot password authentication requirement for the workstation.


Trusted Platform Module Support

Policy setting	Supported on OS	Description
Use TPM		Enabling the use of TPM will initialize and take ownership of the Trusted Platform Module (TPM). It is your responsibility to ensure that the TPM is not being used by any other software, as this can result in data loss.
TPM Mode		<ul style="list-style-type: none">• Use TPM if possible - Encryption process will attempt to use TPM for the encryption. If the TPM version is not supported or TPM is not present, encryption will continue without TPM.• Must use TPM - Encryption requires TPM. If TPM is not present or it is running in an unsupported version, the encryption will fail to start.

 From version 1.2.4 ESET Full Disk Encryption does not clear the TPM before use.

OPAL Self-Encrypting Drive Support

Policy setting	Supported on OS	Description
Use Opal		If enabled, encryption will be performed with the use of OPAL encryption support. This is a hardware functionality of a disk.






Policy setting	Supported on OS	Description
Opal Mode		<ul style="list-style-type: none"> • Use Opal if possible - Encryption process will attempt to use OPAL hardware encryption support for the encryption. If OPAL version is not supported or OPAL encryption support is not present, encryption will continue without OPAL. • Must use Opal - Encryption requires OPAL. If OPAL is not present or it is running in an unsupported version, the encryption will fail to start.

Password policies



User Password Requirements

- **User can change password** - If disabled, a password change is possible only when initiated by the administrator from the remote management console.

Password Characters





Policy setting	Supported on OS	Description
Must use lowercase letters		Password must contain at least one lowercase character (a-z).
Must use uppercase letters		Password must contain at least one uppercase character (A-Z).
Must use numbers		Password must contain at least one numeric character (0-9).
Must use symbols		Password must contain at least one special character (!@#%\$%).
Minimum password length		Defines the minimum required length of the password (1-127 characters).

Password Retries

Policy setting	Supported on OS	Description
Limit incorrect password attempts		When disabled, incorrect password attempts are unlimited. It is not recommended to disable this setting for a long period due to security risk.
Maximum incorrect password attempts		The maximum value is 254. Maximum consecutive incorrect password attempts before the account is locked and a recovery password is required to set up a new password.



Password Expiry

Policy setting	Supported on OS	Description
----------------	-----------------	-------------

Policy setting	Supported on OS	Description
Password expires		When disabled, the user password does not have an expiration period.
Maximum password age (days)		A value between 1 and 999 days. The recommended range is between 30 and 90.
Warn user when password is due to expire		When disabled, the user is not warned by the product that their password is about to expire.
Warn when period less than (days)		A value between 1 and 999 days. Specify how many days before the password expiration is user warned.







Recovery Password Options

Password Retries

Policy setting	Supported on OS	Description
Limit incorrect password attempts		When disabled, there is no limit on incorrect recovery password attempts. It is not recommended to disable this setting for a long period of time due to security risk.
Maximum incorrect password attempts		The maximum value is 254. Maximum consecutive incorrect password attempts before the account is locked and a recovery password is required to set up a new password.

Recovery Password Uses

- All settings in this section are not enabled by default. Ensure you enable them manually.
- All settings in this section are applied and take effect after the computer is decrypted and then encrypted again.

Policy setting	Supported on OS	Description
Limit use of Recovery Password		When disabled, the same recovery password can be used repeatedly, until a new one is generated.
Maximum uses		The maximum value is 254.
Warn user when recovery password limit is near		When enabled, the user will be warned when the recovery password is near its expiration.
Warn with uses remaining		The maximum value is 255.
Automatically generate new recovery password		When enabled, a new recovery password will be generated automatically after the set remaining password uses are reached.
Generate when (uses remains)		The maximum value is 255.

User interface



User Interface Elements

-   **Start mode:**



o**Full** - the complete main program window will be displayed.

o**Minimal** - the main program window is running, but only notifications are displayed to the user.

Statuses

-   **Application statuses:** Define which application statuses will be displayed in the desktop application and which statuses will be sent.















Presentation Mode

Policy setting	Supported on OS	Description
Disable Presentation mode automatically after		Turn on to enable setting the time period after which the Presentation mode will be disabled.
Disable after (minutes)		Set the time period (in minutes, maximum 2000), after which the Presentation mode will be disabled.

Tools

Tools section allows you to specify a proxy connection used for the activation of EFDE.

Proxy server

Policy setting	Supported on OS	Description
Use proxy server	 	Enables the use of proxy connection for product activation.
Proxy server	 	Specify a proxy server address.
Port	 	Specify a proxy server port.
Proxy server required authentication	 	This setting needs to be enabled if the proxy connection requires authentication.
Username	 	Specify the username used for proxy authentication.
Password	 	Specify the password used for proxy authentication.
Use direct connection if proxy is not available	 	If enabled, it allows a fallback to direct connection.

EFDE Client deployment


To encrypt disks on the managed workstation, EFDE client must be installed.

 Due to a known issue, you cannot create a Live Installer from ESET PROTECT for EFDE for macOS. The recommended deployment process is to deploy ESET Management Agent on the target workstation and then deploy the EFDE for macOS via the [Software Install Task](#) or [Computers Details Encryption Wizard](#).

You can perform deployment of EFDE client in three different ways:

- [Create All-in-one Installer](#)
- [Software Install Task](#)
- [Enable Encryption Wizard](#)

EFDE All-in-one Installer

 Due to a known issue, you cannot create a Live Installer from ESET PROTECT for EFDE for macOS. The recommended deployment process is to deploy ESET Management Agent on the target workstation and then deploy the EFDE for macOS via the [Software Install Task](#) or [Computers Details Encryption Wizard](#).

EFDE All-in-one installer will deploy ESET Management Agent and EFDE client in one executable installer file.

1. Click **Installers** -> **Create installer** -> **All-in-one Installer**.
2. In the **Basic** section, select the check box next to **Full Disk Encryption** to include EFDE client in the installer and click **Continue**.
3. Select the EFDE license you want to use.
4. Select the **Product/Version** you want to include in the installer. Except for specific cases, always use the latest available version of the product.
5. Select the **Language** of the installer and product to install.
6. Select the **Configuration Policy** you created earlier, or you can choose one of the pre-configured policies available by default.
7. Select the check box to agree with the EULA and Privacy Policy.
8. In the **Advanced** section, you can specify the **Name** and **Description** of the installer for better and easier identification.
9. After you click **Finish**, you can now download the installer package and deploy it.

EFDE Software Install task

! If you work with Apple M1 Mac, ensure you [installed Rosetta](#).

EFDE Client can be deployed to a managed workstation or a group of workstations by execution Software Install task.

1. Click **Tasks** -> **New** -> **Client Task**.
2. Specify the **Name** and **Description** of the task for better and easier identification.
3. Select the **Operating System** from **Task Category** drop-down menu.
4. Select the **Software Install** from **Task** drop-down menu.

New Client Task

Tasks > EFDE install task

Basic

Settings

Summary

Name

EFDE install task

Tags

Select tags

Description

efde install

Task Category

Operating System

Task

Software Install

BACK

CONTINUE

FINISH

CANCEL

5. Click **Continue**.

6. Click **Choose Package** and select the **ESET Full Disk Encryption** product (for Windows) or **ESET Full Disk Encryption for macOS** (for macOS).
7. Select the EFDE license you want to use.
8. Select the check box to agree with the EULA and Privacy Policy.

Basic

Settings

Summary

Software installation settings

Package to install

☒ Install package from repository

☐ Install by direct package URL

Choose operating system

☒ Windows

☐ Linux

☐ macOS

☐ Android

Choose package from repository

ESET Full Disk Encryption; version 1.4.0.45, English language, WINDOWS

ESET license

ESET Full Disk Encryption, expires August 18, 2024 01:59:59

☒ I accept the [End User License Agreement](#) and acknowledge the [Privacy Policy](#).

Installation parameters

Automatically reboot when needed

☐

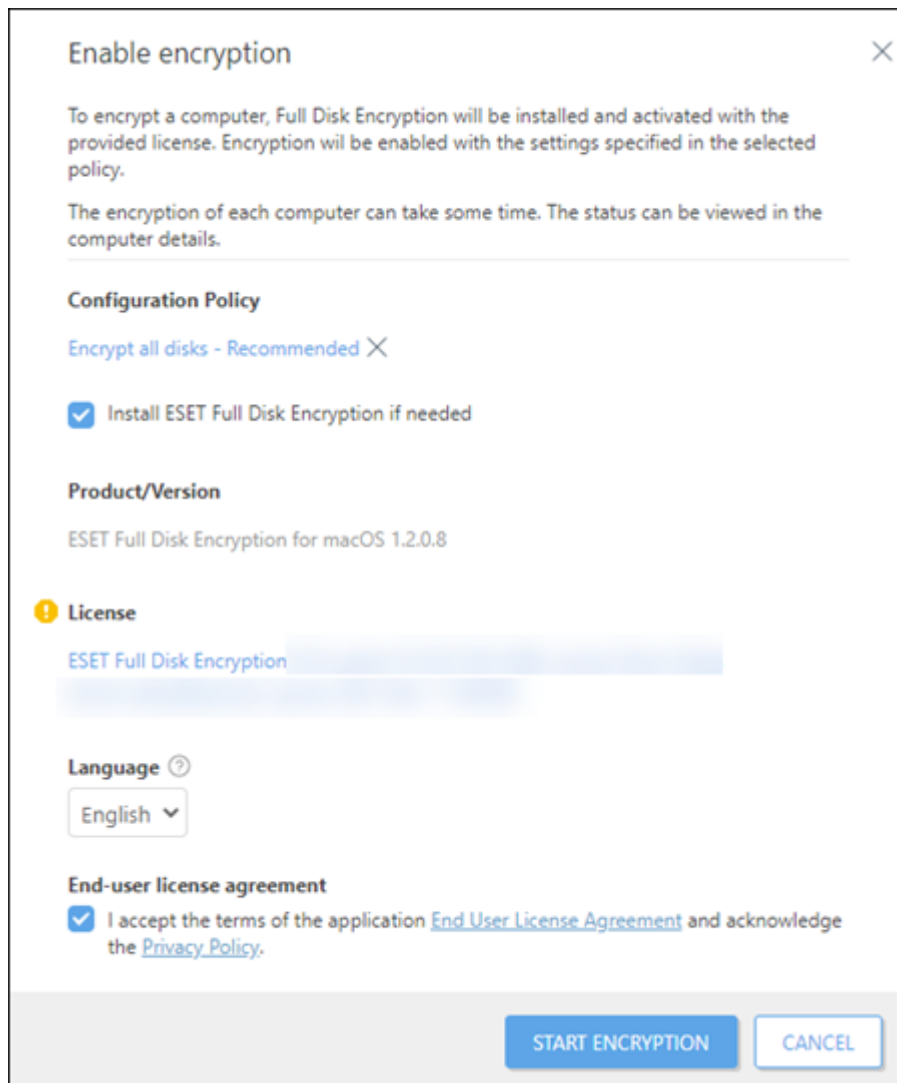
BACK CONTINUE FINISH CANCEL

9. Click **Finish**, and in the notification window, select **Create Trigger**.
10. Inside the **Target** section, select **Add Computers** to select individual workstations where the product will be installed.
11. Specify the **Trigger**, when the task will be executed and click **Finish** to proceed to the task execution.

After the task is successfully executed, in the next step, you will need to [Enable Encryption](#) on the target workstation.

Enable encryption wizard

You can start encryption on a specific managed workstation from the **Computers** screen from the **context menu** -> **Enable Encryption**, or from the Computers Details of the selected workstation -> **Show Details** -> **Overview** -> Encryption tile -> **Encrypt computer**.



Inside the **Enable Encryption** wizard:

1. Select the EFDE **Configuration Policy** you want to use.
2. Select the check box next to **Install ESET Full Disk Encryption if needed** if the EFDE client is not already installed on the workstation.
3. The **Product/Version** is selected based on the workstation OS.

i If you are using ESET Security Management Center, you must select the **Product/Version** you want to include in the installer. Except for specific cases, it is always recommended to use the latest available version of the product.

4. Select the EFDE license you want to use.
5. Select the **Language** of the installer and product that will be installed.
6. Select the check box to agree with the EULA and Privacy Policy.
7. Click **Start Encryption** to initialize the encryption process on the workstation.

Deploy ESET Full Disk Encryption via command line

- [Deploy an installer with a pre-defined password](#)
- [Invalidate password via command line](#)
- [Pause/Resume FDE authentication via command line](#)
- [Add/Remove keyboard layouts via command line](#)

Deploy an installer with a pre-defined password

When you deploy ESET Full Disk Encryption, you can set installation parameters to include a password to start encryption and a keyboard map. You can use installation parameters when you want to deploy a system with a pre-defined password so that an MSP or Administrator can set up a new computer, deploy ESET Full Disk Encryption and automatically encrypt the system when an encryption policy is set.

Prerequisites:

- **STARTUPPASSWORD** and **STARTUPPASSWORDKLID** parameters must be included in ESET Full Disk Encryption installation
- ESET Full Disk Encryption 1.3.0.x version
- ESET Full Disk Encryption installation must be activated
- The system must be connected to ESET PROTECT On-Prem console via the ESET Management Agent

1. In ESET PROTECT On-Prem console, click **Computers**.
2. Click the computer and click **Tasks > New Task**.
3. Type the task name (for example, EFDE Automatic Encryption Installation) and select **Software Install** from **Task** drop-down menu.
4. Click **Continue**.
5. Click **<Choose package>** and select the installation package from the repository.
6. Into **Installation parameters**, type **STARTUPPASSWORD** and **STARTUPPASSWORDKLID**.

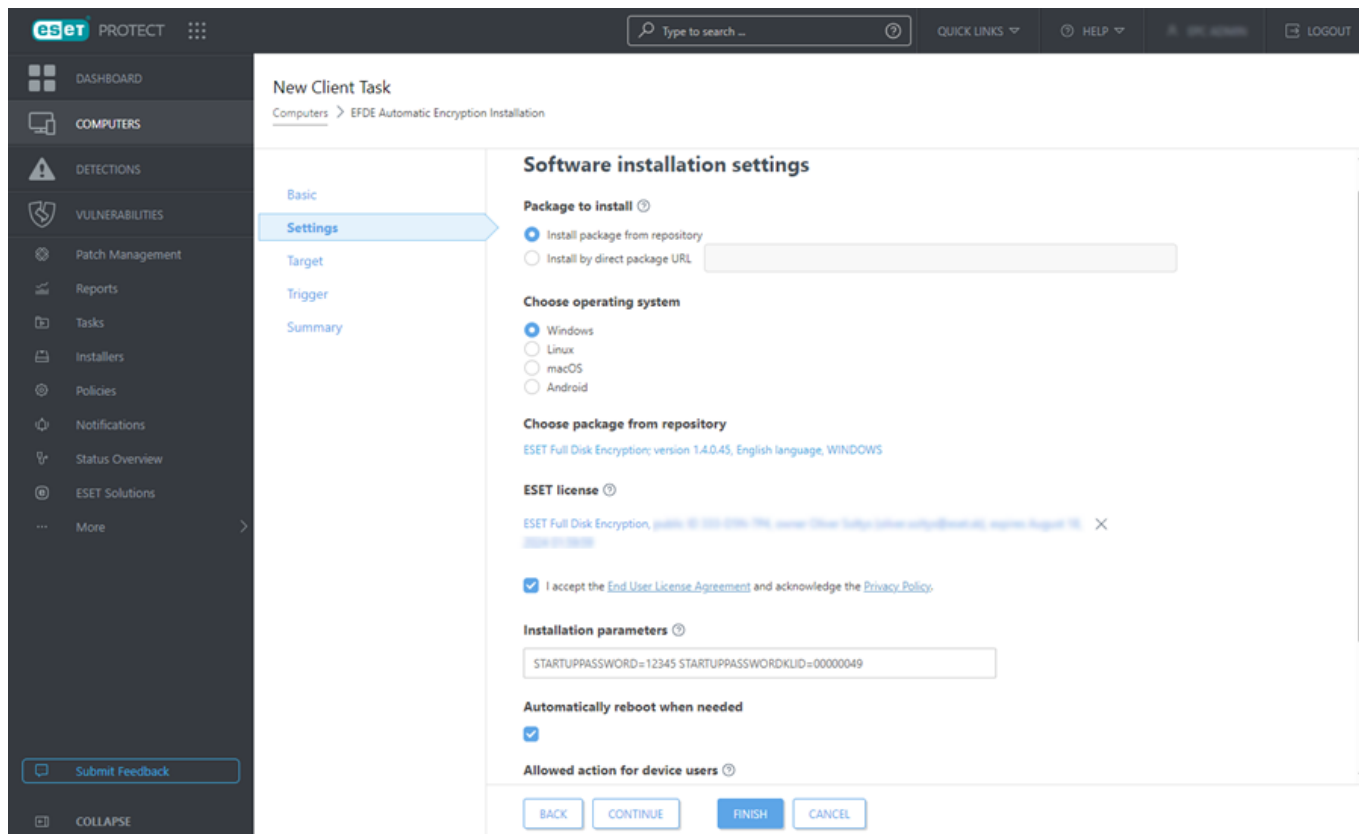
STARTUPPASSWORD sets the initial FDE password. For example, if the parameter is **STARTUPPASSWORD=12345**, the password for encryption will be 12345.

STARTUPPASSWORDKLID sets the keyboard layout. For example, if the parameter is

STARTUPPASSWORDKLID=00000409, an English US keyboard will be installed on the system. The parameter uses keyboard KLIDs to identify and add the right keyboard to the system. See [the list of keyboard layouts](#).

These parameters must be used simultaneously to start encryption automatically when an encryption policy is applied to the system.

7. If required, select **Automatically reboot when needed**. The automatic reboot is not needed, although ESET Full Disk Encryption needs a restart to install. No encryption will take place without a restart.



`/command=invalidate_password`. Alternatively, you can use one command for both the location and the command: `C:\Program Files\ESET\ESET Full Disk Encryption efdeais /command=invalidate_password`.

3. If the command is successful, **Command successful** appears in the command line.

ESET Full Disk Encryption user interface will inform you the password is expired and prompt the users to change the password.

Pause/Resume FDE authentication via command line

A pre-boot authentication screen appears every time the user attempts to boot the device with Full Disk Encryption. Users can pause the pre-boot authentication screen, usually when Windows updates require a reboot.

Prerequisites:



- ESET Full Disk Encryption 1.3.0.x version
- ESET Full Disk Encryption installation must be activated
- The system must be connected to ESET PROTECT On-Prem console via the ESET Management Agent
- The system must be encrypting or encrypted

1. Open an elevated command prompt.

2. Navigate to `C:\Program Files\ESET\ESET Full Disk Encryption`, then run the command `efdeais /command=` with one of the commands - `pause_authentication` or `resume_authentication`. Alternatively, you can use one command for both the location and the command: `C:\Program Files\ESET\ESET Full Disk Encryption efdeais /command=pause_authentication`.

When you use the `pause_authentication` command, you must specify the condition to pause the FDE authentication via a number of reboots, seconds, minutes, hours or a specific time. Examples:

```
efdeais /command=pause_authentication.boots.2
```

```
efdeais /command=pause_authentication.seconds.30
```

```
efdeais /command=pause_authentication.minutes.10
```

```
efdeais /command=pause_authentication.hours.1
```

```
efdeais /command=pause_authentication.time.1617147114
```

Use [unix time stamp](#) to specify the time mode.

When you use the `resume_authentication` command, you do not need to specify any additional parameters. Resuming the authentication will display the FDE authentication screen on the next boot.

3. If the command is successful, **Command successful** appears in the command line, and ESET Full Disk Encryption will state that FDE authentication is disabled.

Add/Remove keyboard layouts via command line

Keyboard maps are used for the user to type their password at the pre-boot authentication and when they change their password within ESET Full Disk Encryption Graphical User Interface. Not all keyboard maps are identical, so you need to distinguish between them. Command line parameters allow users to add, remove and list keyboard maps installed on the system. This is useful if the user decides to add a keyboard map to Windows after encryption has started. If users do not add the keyboard map, they may be unable to change their FDE password within Windows, and they will have unexpected keys in the pre-boot authentication screen if their physical keyboard has changed.

Prerequisites:



- ESET Full Disk Encryption 1.3.0.x version
- ESET Full Disk Encryption installation must be activated
- The system must be connected to ESET PROTECT On-Prem console via the ESET Management Agent
- The system must be encrypting or encrypted

1. Open an elevated command prompt.

2. Navigate to `C:\Program Files\ESET\ESET Full Disk Encryption`, then run the command `efdeais /command=` with one of the commands - `add_keyboard`, `remove_keyboard`, or `list_keyboards`. Alternatively, you can use one command for both the location and the command: `C:\Program Files\ESET\ESET Full Disk Encryption efdeais /command=add_keyboard`.

When you use the `add_keyboard` command, you must specify the keyboard map you want to add via keyboard KLID after the command. For example, `efdeais /command=add_keyboard.00000809`. This will add the UK keyboard layout to the system.

When you use the `remove_keyboard` command, you must specify the keyboard map you want to remove via keyboard KLID after the command. For example, `efdeais /command=remove_keyboard.00000809`. This will remove UK keyboard from the system.

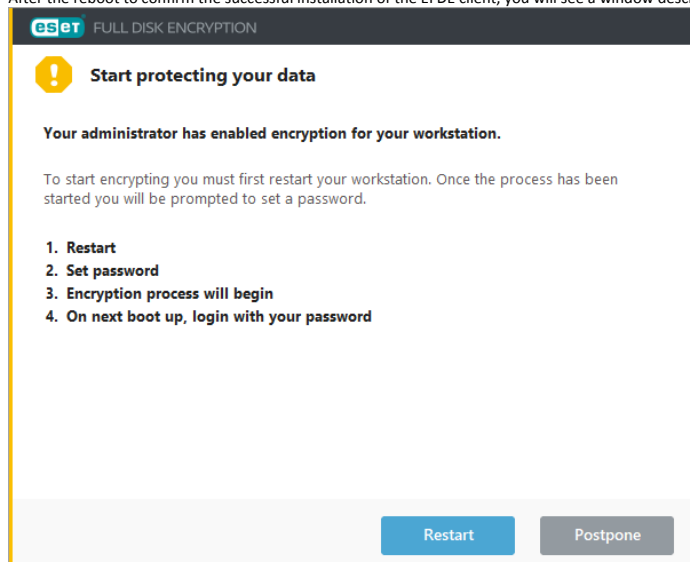
When you use the `list_keyboard` command, you do not need to specify any additional parameters. For example, `efdeais /command=list_keyboards`. This will return a plain text view of the current keyboard maps installed in the system. Alternatively, you can add `.json` to the end of the command to show the keyboard map in a JSON format.

EFDE client-side encryption process

After you initialize the encryption from the management console or after the All-in-one installer is successfully finished, the workstation will reboot to start the encryption process.

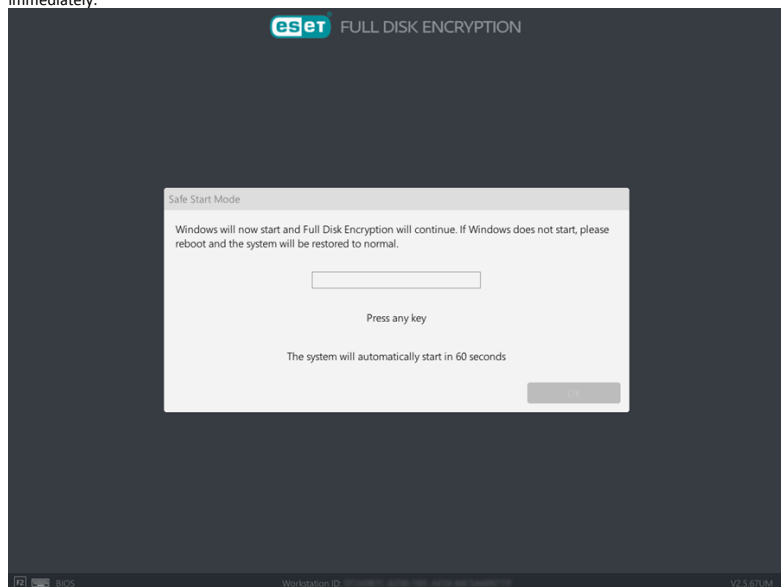
 [Windows](#)

After the reboot to confirm the successful installation of the EFDE client, you will see a window describing the following encryption steps.

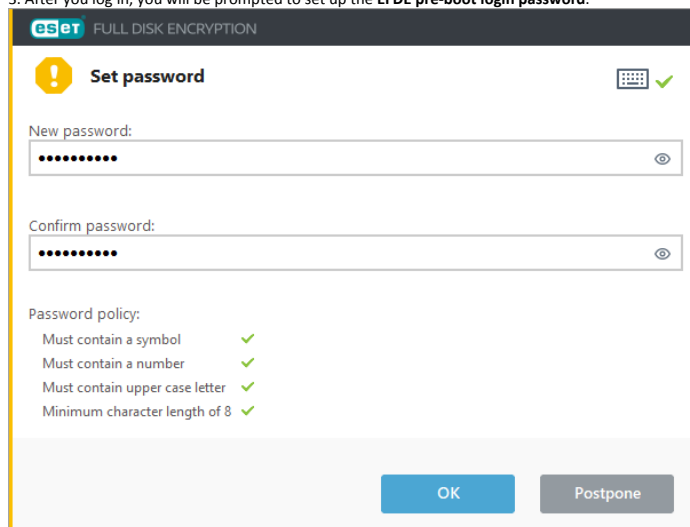


1. Click **Restart** to start the encryption immediately, or **Postpone** to postpone it.

2. After the reboot, the **EFDE Safe Start mode** screen will be displayed with a one-minute counter and automatically start after the timer reaches 0. You can press any key to initiate the next step immediately.



3. After you log in, you will be prompted to set up the **EFDE pre-boot login password**.



4. You can set up the password immediately (the password must meet the password requirements specified in the EFDE configuration policy) or postpone the step for later. Without completing this step, encryption will not continue.

i If users do not set up their passwords and the system is restarted, the encryption process will be postponed. To initiate the Safe Start again, the administrator needs to uninstall the EFDE client and reinstall the EFDE Client again.

5. When the password is created, the encryption of the disk(s) will be initiated. The encryption status is displayed in the EFDE client application and the workstation's Computer Details in the management console.

6. After the encryption process is successfully finished, when the workstation is rebooted, you will be prompted with the EFDE pre-boot login screen for the EFDE pre-boot login password to log in to the workstation.

! If you work with Apple M1 Mac, ensure you [installed Rosetta](#).

1. After the successful installation, the client application will prompt you to insert credentials to begin the encryption process.



2. In the window, fill in your login credentials.




3. After you fill in the correct credentials, the encryption process starts. You can view the encryption status in the EFDE client application and the **Computer Details** of the workstation in the management console.
4. When the encryption process completes, you can continue to use the device as before, but the device's drive is now encrypted.












Encryption management

Management of encrypted workstations consists of pre-boot log in management.


You can access these options from **Computer Details** -> **Overview** -> Encryption tile -> **Manage**:


Or execute the  [maintenance mode](#) tasks and policy options.

All EFDE tasks are executed only after the ESET Management Agent receives the task during the agent replication process (usually next time the agent connects to the management server after the task is executed). The computer requires to be booted into the windows for the agent to receive the information about the task. The pre-boot login screen is not sufficient enough state for the agent to execute these tasks.

-  **Invalidate FDE login password** - This task immediately invalidates the current login password and prompts users to change their login password in the EFDE client's main program window. If the user does not change their password in the EFDE client's main program window and shuts down the device, users are prompted to change the password on the pre-boot login screen the next time the device is booted.
-  **Generate new FDE recovery password** - This task immediately invalidates the current login password and generates a new one that the administrator can provide to the user.
-   **Restore Access**
 - o   **Recovery password** - generates the user's recovery password to set up a new login password.
 - o   **Recovery data** - generates the decryption file required for encryption recovery.
-  **Block Access**
 - o  **Block FDE login password** - This task forces the user to require a recovery password to boot the machine. The **Recovery password** is required to set a new pre-boot login password for the user to log in on the device. The user cannot change their login password (even if this is enabled by EFDE configuration policy) at the pre-boot login screen at this state.
 - o  **Wipe FDE login password** - This task initializes BSOD the device immediately after the execution on the device. The FDE login is wiped on the device, and the user is blocked from any login attempt. User login, password change, and password recovery are disabled in this state. The only option is encryption recovery with an encryption recovery drive.

Pause FDE authentication

 This option is not available for EFDE for macOS management.

 While **Pause FDE authentication** is enabled on a workstation, the system will boot with no authentication and therefore is not secure from threats.

Pause FDE authentication offers you an option to enable/ disable, or postpone EFDE FDE authentication requirement.

Administrator can use **Pause FDE authentication** Client Task to temporary disable the FDE authentication after the computer boots.

You can access **Pause FDE authentication** client task in your management console by navigating to **Tasks** -> **New** -> **Client Task** and in the **Task** drop-down menu select **Pause FDE authentication**:

New Client Task

Tasks > Pause FDE

Basic

Settings

Summary

Name

Pause FDE

Tags

Select tags

Description

Task Category

All Tasks

Task

Pause FDE authentication

i Pausing the FDE authentication will allow a workstation to boot automatically, without the user needing to enter the password.

i This task runs only on Windows OS.

BACK

CONTINUE

FINISH

CANCEL

- **Settings:**

Number of reboots - Here you can specify how many reboots are allowed for the workstation to allow user login to the workstation without being prompted to perform FDE authentication.


Select the period option: Period of time - you can specify a time period (in seconds, minutes, hours or days) or **Date and time** during which the workstation can be rebooted without the requirement to perform FDE authentication.

Basic

 **Settings**

Summary


Pause FDE authentication settings

Number of reboots 

Select the period option

☒ Period of time

☐ Date and time

Period of time 

second(s) 

BACK

CONTINUE

FINISH

CANCEL

 If the task reaches at least one of the specified values in the task, the FDE authentication will be renewed.

To resume the FDE authentication, before the task reaches its specified limit(s), the administrator can use the **Resume FDE authentication** Client task.

To permanently disable FDE authentication for a longer period of time, administrator can use the **Disable FDE Authentication** option in the EFDE policy.



Disable FDE Authentication setting can be found in the EFDE policy under **Encryption options** -> **Full Disk Encryption Mode**.

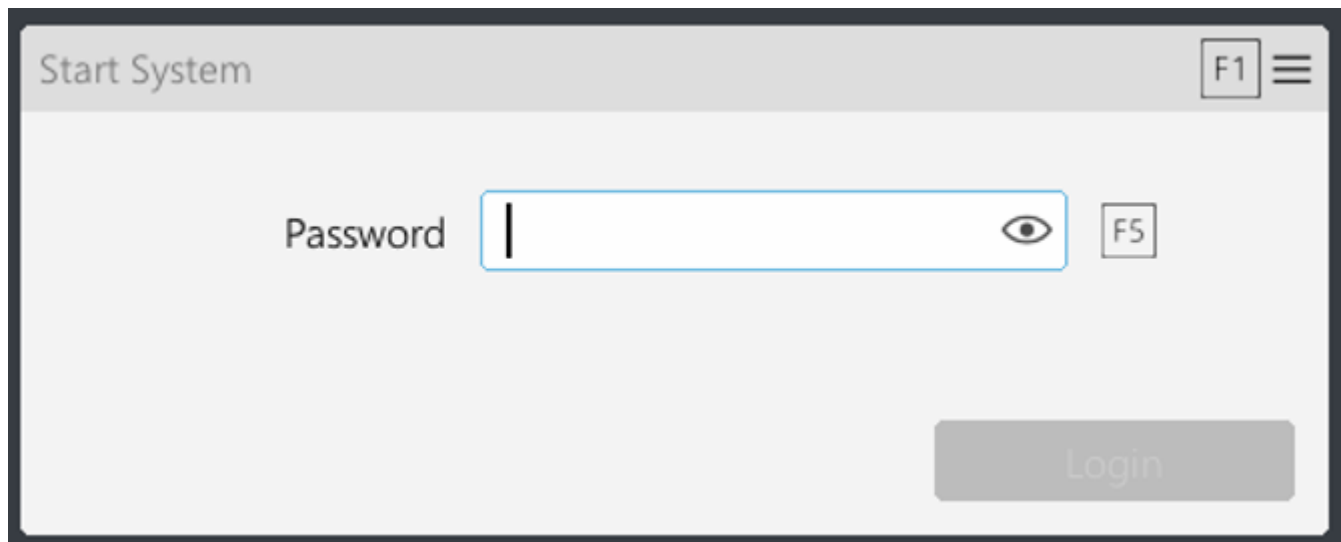


When the FDE authentication is disabled with **Disable FDE Authentication** setting in the EFDE policy, the FDE authentication will be disabled until this setting is disabled and applied to specific workstation. **Resume FDE authentication** client task is not able to resume the FDE authentication if the **Disable FDE Authentication** policy setting is applied.

Pre-boot login

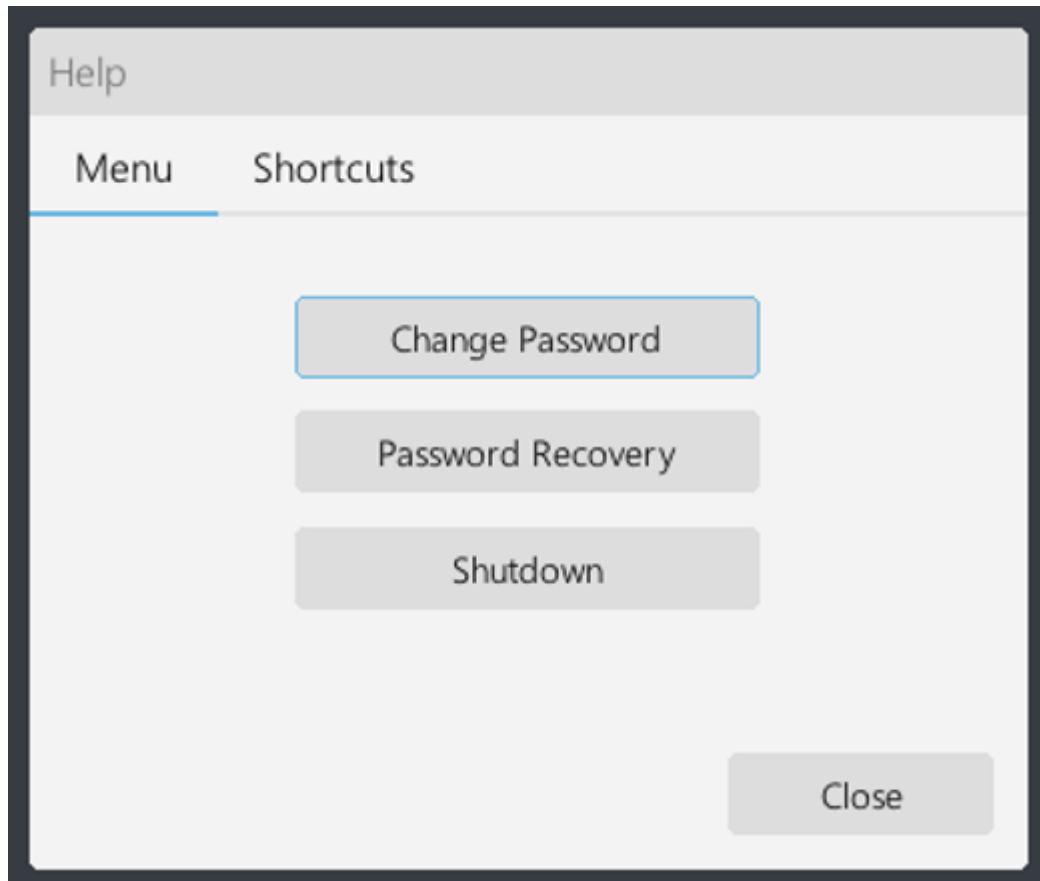
When the encryption is active on a workstation and the product has a valid license, the pre-boot login screen will be after the workstation's boot.

The pre-boot login is a security layer of the EFDE product that secures access to the data on the workstation.

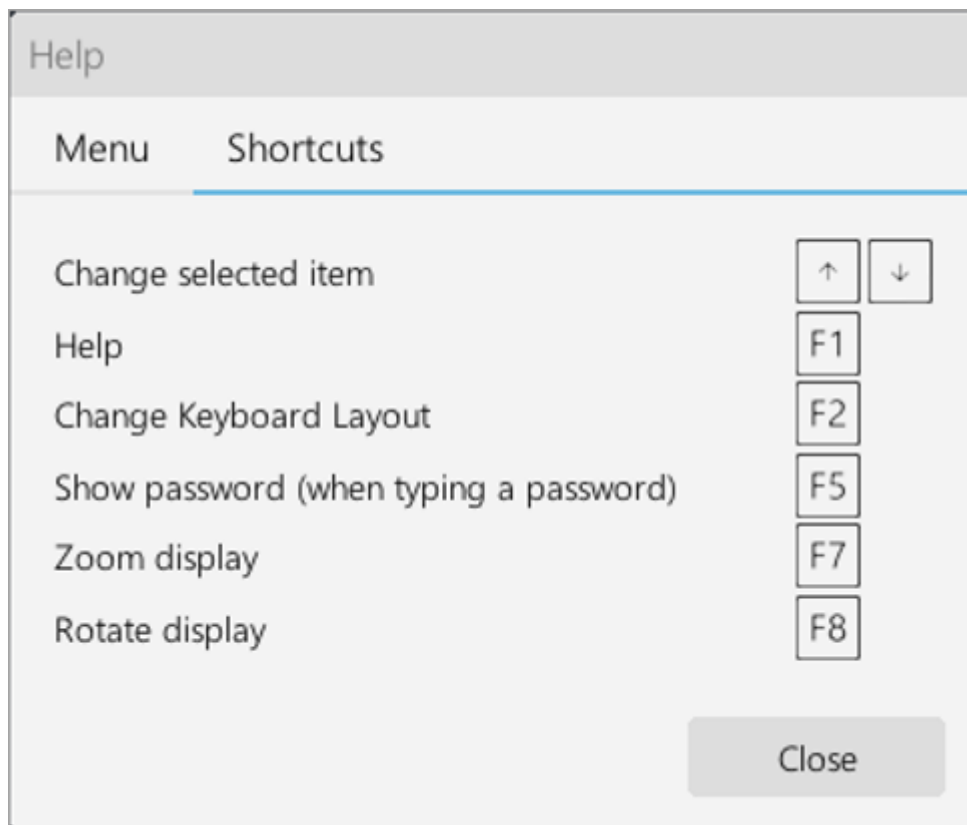


You can access the menu of the pre-boot login screen by pressing **F1**. It enables you to **Change password**, initiate the [Password recovery](#), **Shutdown** the workstation or **Close** the pre-boot login menu.

On the pre-boot login screen, press **F5** for **Show password** function or **F8** to **rotate the screen** if it is not displayed properly.



Pre-boot screen shortcuts



Keyboard shortcut	
F1	Press F1 to open Menu.

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.


Encryption recovery

Encryption recovery process allows the administrator to initiate the recovery process if the user cannot log in with their password or the encrypted data on the workstation is not accessible due to a technical problem.

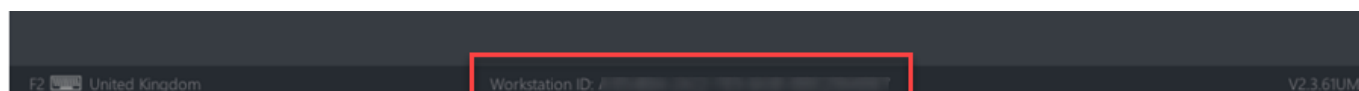
- [Password recovery](#) - This process allows the administrator to generate a recovery password for the user.
- [Data recovery](#) - This process allows the administrator to generate a recovery drive if the data on the workstation is not accessible by standard methods.

Recovery password

Password recovery is required if the user exceeds the incorrect password attempts limit on the pre-boot login screen or if the **Block FDE login password** task is initiated.

 If you have no recovery attempts remaining, you have to [decrypt](#) manually.

You need a **Workstation ID** for the recovery process. **Workstation ID** is case-sensitive. You can find **Workstation ID** at the bottom of the pre-boot login screen:



 [Windows](#)

In this state, the user will see on their pre-boot login screen a warning "User is disabled." The user needs to press **F1** to open the pre-boot login menu and select **Password recovery**. At this point, the user needs to contact the administrator who can generate a recovery password.

The administrator can perform this task in two ways:



If the administrator can identify the affected workstation in the management console:

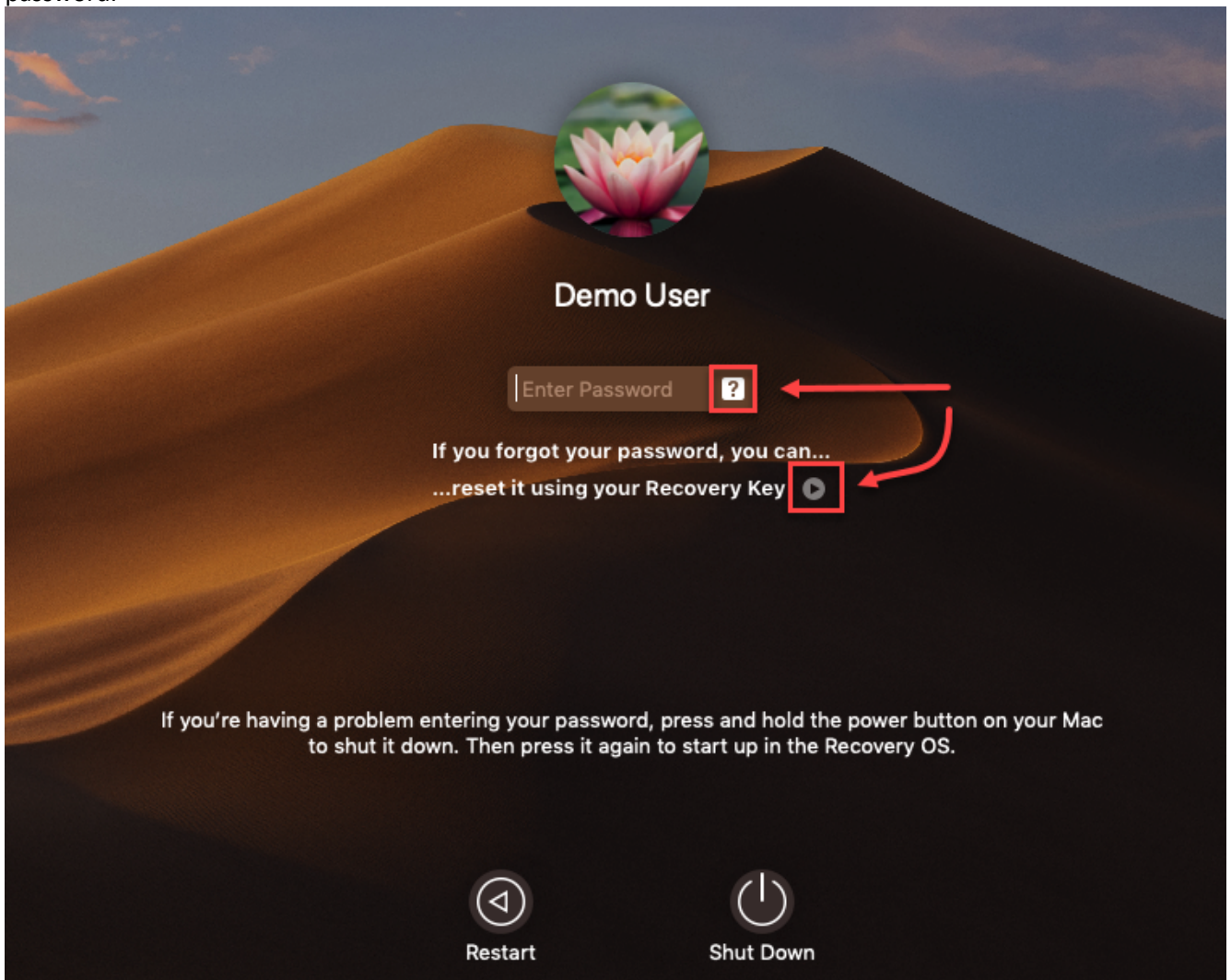
1. Click **Computer Details** of the workstation in the management console.
2. Click **Overview** -> Encryption tile select **Manage** -> **Restore Access** -> **Recovery Password**.
3. Based on the Recovery Index, which appears on the user's screen, the administrator can provide the correct recovery password for the user.
4. After the user inserts the password, they can change their FDE login password.

If the administrator can not identify the affected workstation in the management console:

1. Click **Help** -> **Encryption recovery** in the top bar of the management console.
2. Select the **Recovery password** option.
3. The user must provide the Workstation ID to the administrator. Workstation ID is displayed at the bottom of the EFDE pre-boot login screen.
4. After inserting the correct Workstation ID, a Recovery password table appears.
5. Based on the Recovery Index displayed on the user's screen, the administrator can provide the correct recovery password for the user.
6. After the user inserts the password, they can change their FDE login password.



The user needs to click the question mark icon  on their login screen and then click the arrow icon  next to the "...reset if using your Recovery Key." The user needs to contact the administrator to generate a recovery password.



The administrator can perform this task in two ways:

If the administrator can identify the affected workstation in the management console:

1. Click **Computer Details** of the workstation in the management console.
2. Click **Overview** -> Encryption tile select **Manage** -> **Restore Access** -> **Recovery Password**.
3. Based on the Recovery Index displayed on the user's screen, the administrator can provide the correct recovery password for the user.
4. After the user inserts the password, they can change their login password.

If the administrator can not identify the affected workstation in the management console:

1. Click **Help** -> **Encryption recovery** in the top bar of the management console.
2. Select the **Recovery password** option.
3. The user must provide the Workstation ID to the administrator. Workstation ID is displayed at the bottom of the login screen.
4. After inserting the correct Workstation ID, a Recovery password table appears.
5. Based on the Recovery Index displayed on the user's screen, the administrator can provide the correct recovery password for the user.
6. After the user inserts the password, they can change their login password.

Recovery data

The encryption recovery process is required if the **Wipe FDE Login password** task was executed or if there is a problem with the encryption or EFDE pre-boot login screen and Password recovery is not successful. This process will decrypt the drive on the workstation and disable the EFDE pre-boot login.

You need a **Workstation ID** for the recovery process. **Workstation ID** is case-sensitive. You can find **Workstation ID** at the bottom of the pre-boot login screen:



- All users with **Read** access to the **All** static group (access to all devices) also have access to recovery data of removed devices.
- Due to security reasons, recovery data is available only to users with access to the **All** static group (access to all devices), for example, only to global administrators.

The administrator can perform this task in two ways:

If the administrator can identify the affected workstation in the management console:

1. Click **Computer Details** of the workstation in the management console.
2. In the **Overview** -> Encryption tile select **Manage** -> **Restore Access** -> **Recovery data**.

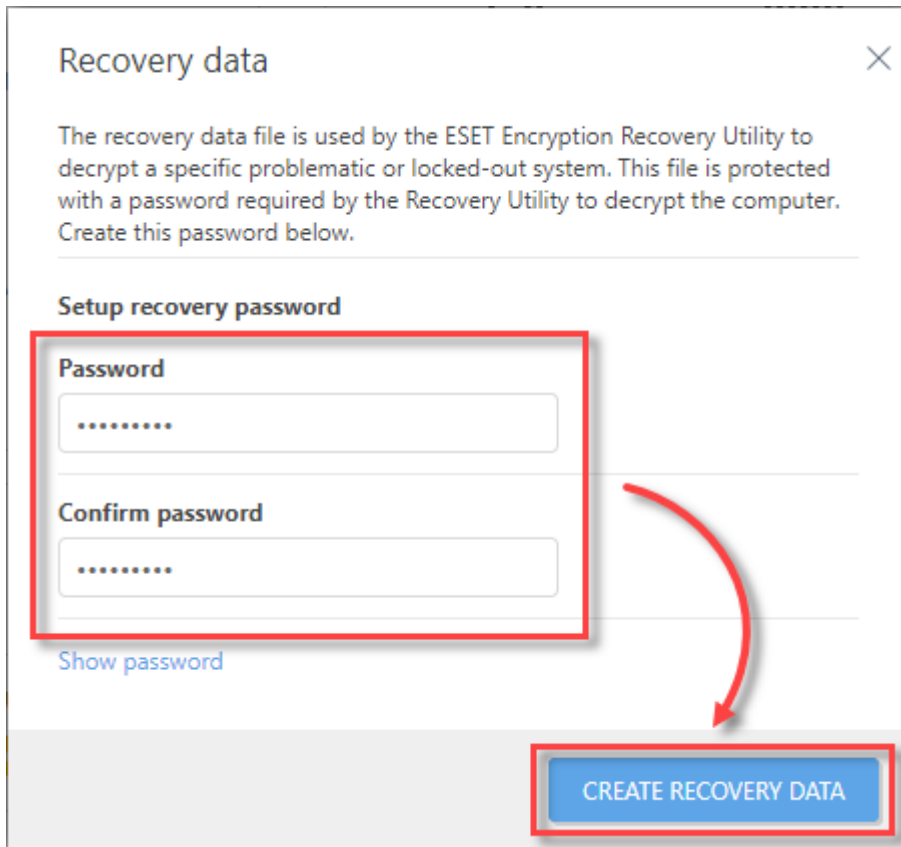
If the administrator can not identify the affected workstation in the management console:

1. In the top bar of the management console, click -> **Help** -> **Encryption recovery**.
2. Select the **Recovery data** option.
3. The user must provide the Workstation ID to the administrator. Workstation ID is displayed at the bottom on the EFDE pre-boot login screen.

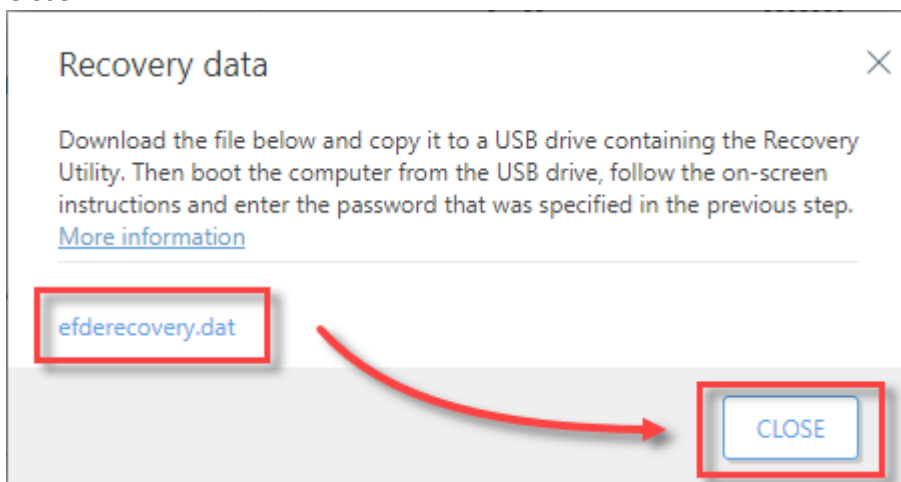
From this point, the recovery process is the same for both options.

Download the Recovery Data File:

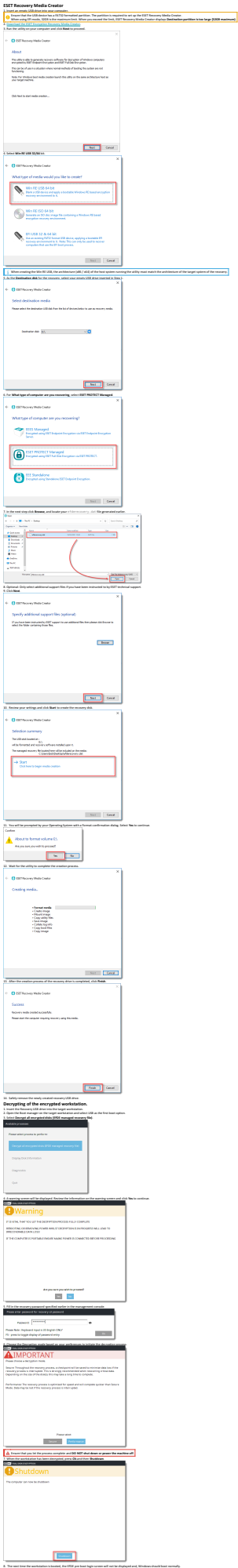
1. On the screen, create a one-time recovery Password (this password is valid only for this one specific encryption recovery).
2. Click **Create Recovery Data** to proceed to the next step.



3. In the next window, click `efderecovery.dat` and Download&Save the file. After this step is finished, click **Close**.



The "efderecovery.dat" file is unique for every workstation and every encryption of the workstation. e.g., the decryption file will not be the same if the workstation was encrypted, decrypted, and then encrypted again.



For macOS 10.x - 11.x, follow the procedure [Decrypt an Apple computer encrypted with ESET Full Disk Encryption](#).

1. Insert an empty USB drive into your computer.
 2. [Download the Encryption recovery tool for macOS](#).
 3. Unzip the content of the file downloaded in the previous step on the USB drive.
 4. Copy the `efderecovery.dat` file onto the USB drive.
- ⚠ User password of the targeted macOS computer is required for the process to complete successfully. Without the password, the process will be unable to finish.**
5. Insert the USB drive to the macOS computer that will be undergoing the recovery process and type the **macOS Recovery mode (CMD+R)**.
 6. You will need to type the user password to access the **macOS Utilities**, click **Utilities > Terminal**.
 7. In the console, navigate to the USB drive and generate the **FileVaultRecovery.keychain** file by running the following command `./recoveryapp efderecovery.dat`.

```
PATRIOTUSB2 -- zsh -- 80x24
Last login:          on console
eset@esets-Mac-mini ~ % cd /Volumes/PATRIOTUSB2
eset@esets-Mac-mini PATRIOTUSB2 % ./recoveryapp

EFDE Mac OS X Recovery App v1.0.0.3
Copyright (c) ESET. spol. s r.o. 2020. All rights reserved.

Processes an efderecovery.dat file as downloaded from an ESMC server creating a
FileVaultRecovery.keychain file.

Processed file can be used with standard Mac OS File Vault recovery utilities su
ch as diskutil.

Usage: recoveryapp <recovery_filename>

recovery_filename - File obtained from ESMC for the workstation. Normally named
efderecovery.dat.

This computer has Workstation ID : C941580

eset@esets-Mac-mini PATRIOTUSB2 %
```

8. Type the password that was set during the creation of the `efderecovery.dat` file in your management console.

```
PATRIOTUSB2 -- recoveryapp efderecovery.dat -- 80x24
Last login:          on console
eset@esets-Mac-mini ~ % cd /Volumes/PATRIOTUSB2
eset@esets-Mac-mini PATRIOTUSB2 % ./recoveryapp

EFDE Mac OS X Recovery App v1.0.0.3
Copyright (c) ESET. spol. s r.o. 2020. All rights reserved.

Processes an efderecovery.dat file as downloaded from an ESMC server creating a
FileVaultRecovery.keychain file.

Processed file can be used with standard Mac OS File Vault recovery utilities su
ch as diskutil.

Usage: recoveryapp <recovery_filename>

recovery_filename - File obtained from ESMC for the workstation. Normally named
efderecovery.dat.

This computer has Workstation ID : C9415801-

eset@esets-Mac-mini PATRIOTUSB2 % ./recoveryapp efderecovery.dat
Please enter password for recovery file : 
```

9. After successfully creating the **FileVaultRecovery.keychain**, you can continue to the disk decryption.

```
PATRIOTUSB2 -- zsh -- 80x26
Last login:          on console
eset@esets-Mac-mini ~ % cd /Volumes/PATRIOTUSB2
eset@esets-Mac-mini PATRIOTUSB2 % ./recoveryapp

EFDE Mac OS X Recovery App v1.0.0.3
Copyright (c) ESET. spol. s r.o. 2020. All rights reserved.

Processes an efderecovery.dat file as downloaded from an ESMC server creating a
FileVaultRecovery.keychain file.

Processed file can be used with standard Mac OS File Vault recovery utilities su
ch as diskutil.

Usage: recoveryapp <recovery_filename>

recovery_filename - File obtained from ESMC for the workstation. Normally named
efderecovery.dat.

This computer has Workstation ID : C9415801

eset@esets-Mac-mini PATRIOTUSB2 % ./recoveryapp efderecovery.dat
Please enter password for recovery file : 
FileVaultRecovery.keychain file created.
eset@esets-Mac-mini PATRIOTUSB2 %
```

10. Next you need to identify the encrypted disk. To do this, navigate to the root directory and execute the command `diskutil apfs list` in the terminal to see the list of the APFS volume disks.

11. In the displayed list, look for the volume with **"Macintosh HD"** and verify that under **Filevault: Yes (Locked)**.

```
APFS Volume Disk (Role):disk2s1 (Data)
Name:                macintosh HD - Data (Case-insensitive)
Mount point:         Not Mounted
Capacity Consumed:   5490372608 B (5.5 GB)
FileVault:           Yes (Locked)
```

12. Make a note of the **volume ID name** (for example: **disk2s1**).

13. You need to unlock the **FileVaultRecovery.keychain** with the following command:
`security unlock-keychain /path/to/FileVaultRecovery.keychain`

for example: `security unlock-keychain /Volumes/PatriotUSB/FileVaultRecovery.keychain`

14. Next you need to unlock the volume before you continue with the decryption process. To do so, execute the following command:
`diskutil apfs unlockVolume /dev/disk2s1` where you replace the **"disk2s1"** with the volume ID name from the previous step. User passphrase is required to continue with the process.

15. At this point, the drive has been unlocked, and you can continue with the decryption of the disk using the recovery key you generated with the `recoveryapp`.

```
APFS Volume Disk (Role):disk2s1 (Data)
Name:                macintosh HD - Data (Case-insensitive)
Mount point:         /Volumes/macintosh HD - Data
Capacity Consumed:   9967968256 B (10.0 GB)
FileVault:           Yes (Unlocked)
```

16. To continue the disk decryption, execute the following command:

```
diskutil apfs decryptVolume /dev/volume id -recoverykeychain /path/to/filename.keychain
```

for example: `diskutil apfs decryptVolume /dev/disk2s1 -recoverykeychain /Volumes/PatriotUSB/FileVaultRecovery.keychain`

17. You can check the status of the decryption process with the following command: `diskutil apfs list`

```
APFS Volume Disk (Role):disk2s1 (Data)
Name:                macintosh HD - Data (Case-insensitive)
Mount point:         /Volumes/macintosh HD - Data
Capacity Consumed:   9983823872 B (10.0 GB)
FileVault:           36.0% (Unlocked)
```

18. After the process is successfully finished, exit the terminal and reboot the computer.

Decryption/Uninstallation

Before you uninstall the EFDE client from the workstation, you must decrypt all encrypted drives.

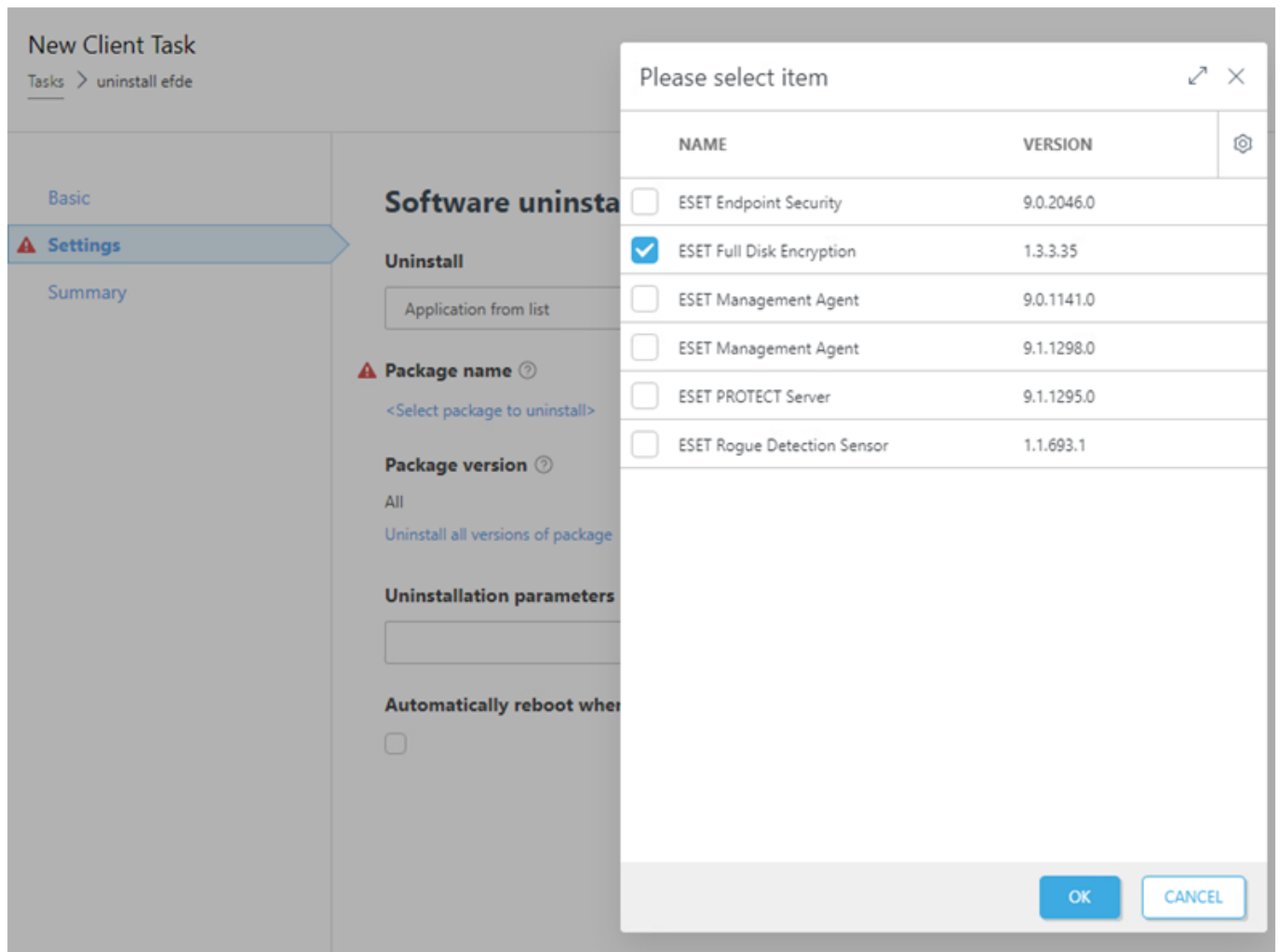
Decryption:

1. [Remove all EFDE policies](#) currently applied to the computer.
2. [Create a new EFDE policy](#).
3. Click **Encryption Options** -> **Full Disk Encryption Mode** and disable the **Enable Encryption** setting.
4. Save and assign this policy to the workstation you want to decrypt.
5. When the decryption process on the workstation completes, the workstation will report as **Encryption Inactive** in the **Computer Details** section.

Uninstallation:

When all drives on the workstation are decrypted, you can uninstall the EFDE client.

1. Create a new **Client task** -> **Software Uninstall**.
2. Click **Settings** and select **Application from list** from the drop-down menu.
3. **Select Package to uninstall: ESET Full Disk Encryption**.



4. Click **Finish** and assign the task to the workstation.

Basic

Settings

Summary

Software uninstallation settings

Uninstall

Application from list

Package name ?
ESET Full Disk Encryption

Package version ?
1.3.3.35
Uninstall all versions of package

Uninstallation parameters ?

Automatically reboot when needed

☐

BACK

CONTINUE

FINISH

CANCEL

Common questions

Why are workstations with EFDE not installed as part of Security Product Dynamic Groups?

EFDE is not considered a security product.

Can I migrate between EFDE and ESET Endpoint Encryption?

No. You cannot migrate between EFDE and ESET Endpoint Encryption.

What is the order of UEFI pre-boot login screens displayed if I have the UEFI pre-boot login enabled on the workstation?

EFDE pre-boot login is displayed after the UEFI pre-boot login.

Can I use the ESET Deployment tool to deploy All-in-one installer with EFDE?

Yes. You can use the Deployment tool to deploy All-in-one installer with EFDE.

Is there a similar thing like maintenance mode from ESET Endpoint Encryption available in EFDE?

Yes. EFDE client version 1.2.0.5 and later supports [Pause FDE authentication](#).

When the IT department wants to perform maintenance, and the user does not want to give their EFDE password, the only option is to use a recovery password?

No. Client version 1.2.0.5 and later can use [Pause FDE authentication](#) requirement.

Can I recover data from the formatted hard disk encrypted with EFDE?

No. You can not recover data from formatted hard disk encrypted with EFDE.

Is there backdoor for EFDE?

No. You can boot EFDE only using EFDE password.

Troubleshooting

EFDE Error/Alert	Explanation
Policy states a TPM must be used to encrypt your computer, but no suitable TPM is present. A TPM 2.0 is required.	TPM is specified as mandatory for encryption by the EFDE configuration policy. If the workstation does not support TPM 2.0, apply the EFDE configuration policy without the TPM encryption support set as mandatory. If the TPM 2.0 is supported on the workstation, but the error persists to display, investigate the product logs for more information.
Policy states Opal must be used to encrypt your computer, but one or more disks do not support the Opal 2 protocol.	Opal is specified as mandatory for encryption by the EFDE configuration policy. If the workstation does not support Opal, apply the EFDE configuration policy without the Opal encryption support set as mandatory. If Opal is supported on the workstation, but the error still displays, investigate the product logs for more information.
Your license expires in a few days, and your computer will lose protection. When this happens, the pre-boot password will be removed, and your computer will start without requiring any authentication. Renew your license to stay protected or activate ESET Security Product if you already have a renewal key or a new license.	In this state, the EFDE pre-boot login is not required, but the data on the workstation is still encrypted. You can renew your existing license or decrypt the workstation with a decryption policy .

EFDE Error/Alert	Explanation
The license has expired or is invalid, which has disabled pre-boot authentication.	Without a valid license, encryption on the workstation persists, but the EFDE pre-boot login is no longer required before the windows login screen. Activate the product with a valid EFDE license or decrypt the workstation and uninstall the EFDE Client application.
Your computer is not encrypted, and data at rest is not protected.	General alert indicating that the EFDE Client application is running, but the data on the workstation is not encrypted. To solve the error, enable and configure EFDE .
Encryption on your computer failed to start due to an error. Check system logs for more information.	The encryption process failed to start. You can find more details for troubleshooting in the application logs.
Your computer is ready to begin encryption, but it is currently waiting for a configured pre-boot password.	This error indicates that user interaction on the workstation is required. It is highly recommended to set the pre-boot password before the next restart to proceed in the encryption process.
A computer restart is required to initiate Safe Start to check hardware and firmware compatibility and perform initialization.	After the product is successfully installed, this error message will indicate that the next required step is to reboot the workstation to initiate the EFDE SafeStart mode. The first time, it will check if the workstation is compatible with EFDE and can be encrypted.
Your computer restarted, and Safe Start succeeded, but encryption did not start correctly before the system restarted again. Therefore encryption will not start. Check system logs for more information.	<p>After the Safe Start process confirmed that the hardware and firmware of the workstation are suitable for encryption, but the workstation was restarted before the EFDE pre-boot login password was set, the encryption process will be terminated. It is also indicated in the workstation logs as: "Safe Start was previously successful, but the result is now stale and Safe Start must be re-run."</p> <p>You can initiate the Safe Start evaluation process by three methods:</p> <ul style="list-style-type: none"> • In ESET PROTECT, click the computer's Details > Alerts > click the Encryption failed to start and select Retry failed encryption. • In ESET PROTECT, click Policies and change policy's Settings: <ol style="list-style-type: none"> 1.Enable Enable Encryption to remove the current policy. 2.Disable Enable Encryption to add a new policy. 3.Wait for processing at the EFDE client to reset the Safe Start state. 4.Enable Enable Encryption to re-add the original policy. • Uninstall and reinstall the EFDE client app.
The product has been installed or upgraded, and you must restart your computer before the software functions.	This error is displayed right after the product was freshly installed, reinstalled or upgraded, and the reboot of the workstation is required before the product can resume its function. The error should disappear after the workstation is rebooted.
Presentation mode is enabled	Enabling Presentation mode via the EFDE configuration policy is a potential security risk. If Presentation mode is enabled and a user goes to a web page or an application that might be problematic or unsafe, it may be blocked. However, the user will not see any explanation or warning because user interaction is disabled.

You can find EFDE Client application logs on the workstation at this location:

i	Windows	C:\ProgramData\ESET\ESET Full Disk Encryption\AIS\Logs\Status.html C:\ProgramData\ESET\ESET Full Disk Encryption\AIS\Logs\efde_ais_<date>.txt
	macOS	/library/application support/eset/ESET Full Disk Encryption/ais/logs/efde_ais_<date>.log /library/application support/eset/ESET Full Disk Encryption/ais/logs/status.html

To generate logs for the support team, you need [ESET Encryption Diagnostics tool](#).

Privacy Policy

The protection of personal data is of particular importance to 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"). We want to comply with the transparency requirement as legally standardized under the EU General Data Protection Regulation ("GDPR"). To achieve this goal, We are publishing this Privacy Policy with the sole purpose of informing our customer ("End User" or "You") as a data subject about following personal data protection topics:

- Legal Basis of Personal Data Processing,
- Data Sharing and Confidentiality,
- Data Security,
- Your Rights as a Data Subject,
- Processing of Your Personal Data
- Contact Information.

Legal Basis of Personal Data Processing

There are a few legal bases for data processing which We use according to the applicable legislative framework related to protection of personal data. The processing of personal data at ESET is mainly necessary for the performance of the [End User License Agreement](#) ("EULA") with End User (Art. 6 (1) (b) GDPR), which is applicable for the provision of ESET products or services, unless explicitly stated otherwise, e.g.:

- Legitimate interest legal basis (Art. 6 (1) (f) GDPR), that enables us to process data on how our customers use our Services and their satisfaction to provide our users with the best protection, support and experience We can offer. Even marketing is recognized by applicable legislation as a legitimate interest, therefore We usually rely on it for marketing communication with our customers.
- Consent (Art. 6 (1) (a) GDPR), which We may request from You in specific situations when we deem this legal basis as the most suitable one or if it is required by law.
- Compliance with a legal obligation (Art. 6 (1) (c) GDPR), e.g. stipulating requirements for electronic communication, retention for invoicing or billing documents.

Data Sharing and Confidentiality

We do not share your data with third parties. However, ESET is a company that operates globally through affiliated companies or partners as part of our sales, service and support network. Licensing, billing and technical support information processed by ESET may be transferred to and from affiliates or partners for the purpose of fulfilling the EULA, such as providing services or support.

ESET prefers to process its data in the European Union (EU). However, depending on your location (use of our products and/or services outside the EU) and/or the service you choose, it may be necessary to transfer your data to a country outside the EU. For example, we use third-party services in connection with cloud computing. In these cases, we carefully select our service providers and ensure an appropriate level of data protection through contractual as well as technical and organizational measures. As a rule, we agree on the EU standard contractual clauses, if necessary, with supplementary contractual regulations.

For some countries outside the EU, such as the United Kingdom and Switzerland, the EU has already determined a comparable level of data protection. Due to the comparable level of data protection, the transfer of data to these

countries does not require any special authorization or agreement.

Data Security

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 the relevant supervisory authority as well as affected End Users as data subjects.

Data Subject's Rights

The rights of every End User matter and We would like to inform you that all End Users (from any EU or any non-EU country) have the following rights guaranteed at ESET. To exercise your data subject's rights, you can contact us via support form or by e-mail at dpo@eset.sk. For identification purposes, we ask you for the following information: Name, e-mail address and - if available - license key or customer number and company affiliation. Please refrain from sending us any other personal data, such as the date of birth. We would like to point out that to be able to process your request, as well as for identification purposes, we will process your personal data.

Right to Withdraw the Consent. Right to withdraw the consent is applicable in case of processing based on consent only. If We process your personal data on the basis of your consent, you have the right to withdraw the consent at any time without giving reasons. The withdrawal of your consent is only effective for the future and does not affect the legality of the data processed before the withdrawal.

Right to Object. Right to object the processing is applicable in case of processing based on the legitimate interest of ESET or third party. If We process your personal data to protect a legitimate interest, You as the data subject have the right to object to the legitimate interest named by us and the processing of your personal data at any time. Your objection is only effective for the future and does not affect the lawfulness of the data processed before the objection. If we process your personal data for direct marketing purposes, it is not necessary to give reasons for your objection. This also applies to profiling, insofar as it is connected with such direct marketing. In all other cases, we ask you to briefly inform us about your complaints against the legitimate interest of ESET to process your personal data.

Please note that in some cases, despite your consent withdrawal or your objection processing, we are entitled to further process your personal data on the basis of another legal basis, for example, for the performance of a contract.

Right of Access. As a data subject, you have the right to obtain information about your data stored by ESET free of charge at any time.

Right to Rectification. If we inadvertently process incorrect personal data about you, you have the right to have this corrected.

Right to Erasure. As a data subject, you have the right to request the deletion or restriction of the processing of your personal data. If we process your personal data, for example, with your consent, you withdraw it and there is no other legal basis, for example, a contract, We delete your personal data immediately. Your personal data will also be deleted as soon as they are no longer required for the purposes stated for them at the end of our retention period.

Right to Restriction of Processing. If we use your personal data for the sole purpose of direct marketing and you have revoked your consent or objected to the underlying legitimate interest of ESET, We will restrict the processing of your personal data to the extent that we include your contact data in our internal black list in order

to avoid unsolicited contact. Otherwise, your personal data will be deleted.

Please note that We may be required to store your data until the expiry of the retention obligations and periods issued by the legislator or supervisory authorities. Retention obligations and periods may also result from the Slovak legislation. Thereafter, the corresponding data will be routinely deleted.

Right to Data Portability. We are happy to provide You, as a data subject, with the personal data processed by ESET in the xls format.

Right to Lodge a Complaint. As a data subject, You have a right to lodge a complaint with a supervisory authority at any time. ESET is subject to the regulation of Slovak laws and We are bound by data protection legislation as part of the European Union. The relevant data supervisory authority is The Office for Personal Data Protection of the Slovak Republic, located at Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Processing of Your Personal Data

Services provided by ESET implemented in our product are provided under the terms of [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 the product [documentation](#). To make it all work, We need to collect the following information:

Licensing and Billing Data. The name, e-mail address, license key and (if applicable) address, company affiliation and payment data are collected and processed by ESET in order to facilitate the activation of license, license key delivery, reminders on expiration, support requests, license genuineness verification, provision of our service and other notifications including marketing messages in line with applicable legislation or Your consent. ESET is legally obliged to keep the billing information for the period of 10 years, however the licensing information will be anonymized no later than 12 months after the expiration of license.

Update and Other Statistics. The processed information includes information concerning installation process and your computer including platform on which our product is installed and information about the operations and functionality of our products such as operation system, hardware information, installation IDs, license IDs, IP address, MAC address, configuration settings of product are processed for the purpose of provision update and upgrade services and for the purpose of maintenance, security and improvement of our backend infrastructure.

Technical Support. The contact and licensing 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. The data processed for technical support is stored for 4 years.

Please note that if the person using our products and services is not the End User who has purchased the product or service and concluded the EULA with Us, (e.g. an employee of the End User, a family member or a person otherwise authorized to use the product or service by the End User in compliance with EULA, the processing of the data is carried out in the legitimate interest of ESET within the meaning of Art. 6 (1) f) GDPR to enable the user authorized by End User to use the products and services provided by Us in accordance with EULA.

Contact Information

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

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.

EULAID: EULA-PRODUCT; 3537.0