

ESET Full Disk Encryption

Benutzerhandbuch

[Klicken Sie hier um die Hilfe-Version dieses Dokuments anzuzeigen](#)

Copyright ©2024 by ESET, spol. s r.o.

ESET Full Disk Encryption wurde entwickelt von ESET, spol. s r.o.

Weitere Informationen finden Sie unter <https://www.eset.com>.

Alle Rechte vorbehalten. Kein Teil dieser Dokumentation darf ohne schriftliche Einwilligung des Verfassers reproduziert, in einem Abrufsystem gespeichert oder in irgendeiner Form oder auf irgendeine Weise weitergegeben werden, sei es elektronisch, mechanisch, durch Fotokopien, Aufnahmen, Scannen oder auf andere Art.

ESET, spol. s r.o. behält sich das Recht vor, ohne vorherige Ankündigung Änderungen an allen hier beschriebenen Software-Anwendungen vorzunehmen.

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

REV. 18.03.2024

1 Über die Hilfe	1
2 Änderungslog	1
3 Produktübersicht	1
3.1 Systemanforderungen	2
3.2 EFDE für Mac	3
4 So erwerben Sie den Dienst	3
5 Verwenden ESET Full Disk Encryption	4
6 ESET Full Disk Encryption Aktivieren und konfigurieren	4
6.1 Verschlüsselungsoptionen	6
6.2 Passwort-Policies	7
6.3 Benutzeroberfläche	9
6.4 Tools	10
6.5 EFDE-Client-Bereitstellung	10
6.5 EFDE-All-in-One-Installationsprogramm	10
6.5 Task „EFDE-Software-Installation“	11
6.5 Assistent „Verschlüsselung aktivieren“	13
6.6 ESET Full Disk Encryption über die Kommandozeile bereitstellen	15
6.6 Installationsprogramm mit einem vordefinierten Passwort bereitstellen	15
6.6 Passwort über Befehlszeile ungültig machen	17
6.6 FDE-Authentifizierung über die Befehlszeile aussetzen/fortsetzen	17
6.6 Tastaturlayouts über Befehlszeile hinzufügen/entfernen	18
7 Clientseitiger EFDE-Verschlüsselungsprozess	19
8 Verschlüsselungsverwaltung	21
8.1 FDE-Authentifizierung anhalten	22
9 Pre-Boot-Anmeldung	25
9.1 Verknüpfungen für den Pre-Boot-Bildschirm	26
10 Wiederherstellen der Verschlüsselung	27
10.1 Wiederherstellungspasswort	27
10.2 Wiederherstellungsdaten	30
11 Entschlüsselung/Deinstallation	35
12 Häufige Fragen	37
13 Fehlerbehebung	38
14 Datenschutzerklärung	40
15 Endbenutzer-Lizenzvereinbarung	44

Über die Hilfe

Diese Hilfe beschreibt die Verwendung und Verwaltung von ESET Full Disk Encryption. Zudem gibt es Ihnen detaillierte Informationen zur Verbindung zwischen ESET Full Disk Encryption und anderen ESET-Geschäftsprodukten.

Wir verwenden einen einheitlichen Satz von Symbolen, um besonders interessante oder wichtige Themen hervorzuheben. Die Themen sind in Kapitel und Unterkapitel eingeteilt. Verwenden Sie das Suchfeld im oberen Bereich, um nach relevanten Informationen zu suchen.

Die [Onlinehilfe](#) ist die primäre Quelle für Hilfeinhalte. Bei funktionierender Internetverbindung wird automatisch die neueste Version der Onlinehilfe angezeigt.

- Die [ESET-Knowledgebase](#) enthält Antworten auf häufig gestellte Fragen sowie Lösungsvorschläge für zahlreiche Probleme. Die Knowledgebase wird regelmäßig von den ESET-Supportmitarbeitern aktualisiert und eignet sich daher hervorragend für die Lösung verschiedenster Probleme.
- Im [ESET-Forum](#) erhalten ESET-Benutzer schnell und einfach Hilfe und können anderen Benutzern helfen. Dort können Sie Themen zu beliebigen Fragen oder Problemen mit Ihren ESET-Produkten erstellen.

Textfelder:



Hinweise können wichtige Informationen wie bestimmte Features oder einen Link zu einem verwandten Thema enthalten.



Auf diese Weise gekennzeichnete Informationen sind wichtig und sollten nicht übersprungen werden. Normalerweise handelt es sich um nicht-kritische, jedoch wichtige Informationen.



Kritische Informationen, die besondere Vorsicht erfordern. Warnungen haben den Zweck, Sie vor potenziell schädlichen Fehlern zu schützen. Der Text in Warnhinweisen weist auf besonders empfindliche Systemeinstellungen oder riskante Vorgänge hin und muss daher unbedingt gelesen und verstanden werden.



Beispiel mit einem relevanten Anwendungsfall für das jeweilige Thema. Beispiele werden eingesetzt, um komplexere Themen zu erklären.

Änderungslog

ESET Full Disk Encryption für Windows

ESET Full Disk Encryption für MacOS

Produktübersicht

ESET Full Disk Encryption (EFDE) ist ein systemeigenes Feature der ESET Remote-Management-Konsolen ESET PROTECT On-Prem und ESET PROTECT. Mit EFDE können Sie die Laufwerksverschlüsselung auf verwalteten

Windows- und [macOS](#)-Workstations mit der Pre-Boot-Anmeldung als zusätzliche Sicherheitsebene verwalten. EFDE ist vollständig kompatibel mit ESET PROTECT On-Prem und ESET PROTECT-Funktionen wie Gruppen, Policies, Tasks und Berichten.

Systemanforderungen

Unterstützte Betriebssysteme für die EFDE-Clientanwendung:

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

ESET Full Disk Encryption für MacOS	Unterstützt
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	✓



Installieren Sie die EFDE-Clientanwendung nicht auf derselben Workstation wie Ihre ESET PROTECT Server Datenbank.

Kompatibilität:

- Veraltete/BIOS-Firmware wird nicht unterstützt. ESET Full Disk Encryption benötigt ein UEFI-fähiges System.
- ESET Full Disk Encryption unterstützt keine Datenträger mit MBR-Partitionsschema. Nur Datenträger mit GPT-Partitionsschema werden unterstützt.
- ESET Full Disk Encryption unterstützt Apple M1 Macs, sofern [Rosetta installiert](#) ist.
- ESET Full Disk Encryption unterstützt keine ARM-Prozessoren unter Windows.
- ESET Full Disk Encryption unterstützt keine Dual-Boot- oder Software-RAID-Systeme.
- ESET Full Disk Encryption unterstützt keine Apple Mac-Systeme mit Apple Boot Camp.
- ESET Full Disk Encryption unterstützt keine Microsoft Storage Spaces oder dynamische Datenträger.
- Verwenden Sie Software mit Windows Insider Preview nur zu Testzwecken, da andernfalls Datenverluste auftreten können.
- DirectX 9-Grafikkarte mit WDDM 1.0 oder einem höheren Treiber.

Sie können ESET Full Disk Encryption in Umgebungen mit virtuellen Computern auf PC- oder Mac-Hypervisoren einsetzen:

- VMware Workstation 16.2.3
- VMware ESXi 7.0 / vSphere 7.0.3.00300
- VMware Fusion 12.2.3
- Parallels
- Microsoft Hyper-V (Sicherer Start wird nicht unterstützt)



Für das Gastbetriebssystem gelten die gleichen Kompatibilitätsregeln. ESET Full Disk Encryption für Windows wird beispielsweise nicht auf ARM unterstützt und kann nicht in virtualisierten Windows-Umgebungen auf Apple ARM-CPU's verwendet werden.

Anforderungen an die Management-Konsole:

- **ESET PROTECT** oder **ESET PROTECT On-Prem 8.0+**
- **ESET Management Agent Version 7.1 oder höher** für Windows.
- **ESET Management Agent Version 8.0+** für macOS.

EFDE für Mac

ESET Full Disk Encryption für macOS verwendet Apples systemeigene Verschlüsselungsanwendung mit dem Namen FileVault2, um die verwaltete Workstation zu verschlüsseln und die Verschlüsselung für Benutzer und Administratoren zu vereinfachen. ESET Full Disk Encryption für macOS bietet nicht nur Remote-Verschlüsselung und -Entschlüsselung für verwaltete Workstations, sondern auch Berichte für den Verschlüsselungsstatus in der Management-Konsole, um verschiedene Datenschutz-Compliancebestimmungen zu erfüllen.

So erwerben Sie den Dienst

ESET Full Disk Encryption erfordert eine separate Lizenz für die Produktaktivierung. ESET Full Disk Encryption ist eine Add-On-Funktion der Management-Konsole und kann nur als Ergänzung zu einer neuen oder vorhandenen ESET-Unternehmenslizenz erworben werden. Unsere Kunden können nur die maximale Anzahl an Plätzen kaufen, die mit der Anzahl der Endgerätelizenzen übereinstimmen. Sie können eine ESET Full Disk Encryption-Lizenz bei Ihrem örtlichen ESET-Vertriebspartner erwerben. Nachdem Sie Ihre Lizenz erhalten haben, können Sie diesen in Ihren [ESET Business-Account](#) importieren. Dabei werden alle ESET Full Disk Encryption-Funktionen in der Verwaltungskonsole freigeschaltet.

Kontaktieren Sie uns

Wenden Sie sich an Ihren [ESET-Partner](#), um Antworten auf Fragen bezüglich Lizenzierung und Erwerb des Dienstes zu erhalten. Sie können den ESET-Support via E-Mail, Chat oder Telefon kontaktieren. Um detaillierte Informationen zu erhalten, lesen Sie bitte die [Kontaktinformationen auf unserer Webseite](#).

Verwenden ESET Full Disk Encryption

Nachdem Sie die ESET Full Disk Encryption-Lizenz erfolgreich importiert haben, führen Sie die folgenden Schritte aus:

1. [Erstellen Sie eine EFDE-Konfigurations-Policy](#).
2. [Stellen Sie den EFDE-Client auf den Workstations bereit](#).
3. Die Benutzer sämtlicher Workstations müssen ihre [Pre-Boot-Anmeldepasswörter](#) erstellen.
4. Nach der erfolgreichen Verschlüsselung sind die ausgewählten Datenträger auf der Arbeitsstation verschlüsselt und geschützt.



ESET Full Disk Encryption Aktivieren und konfigurieren

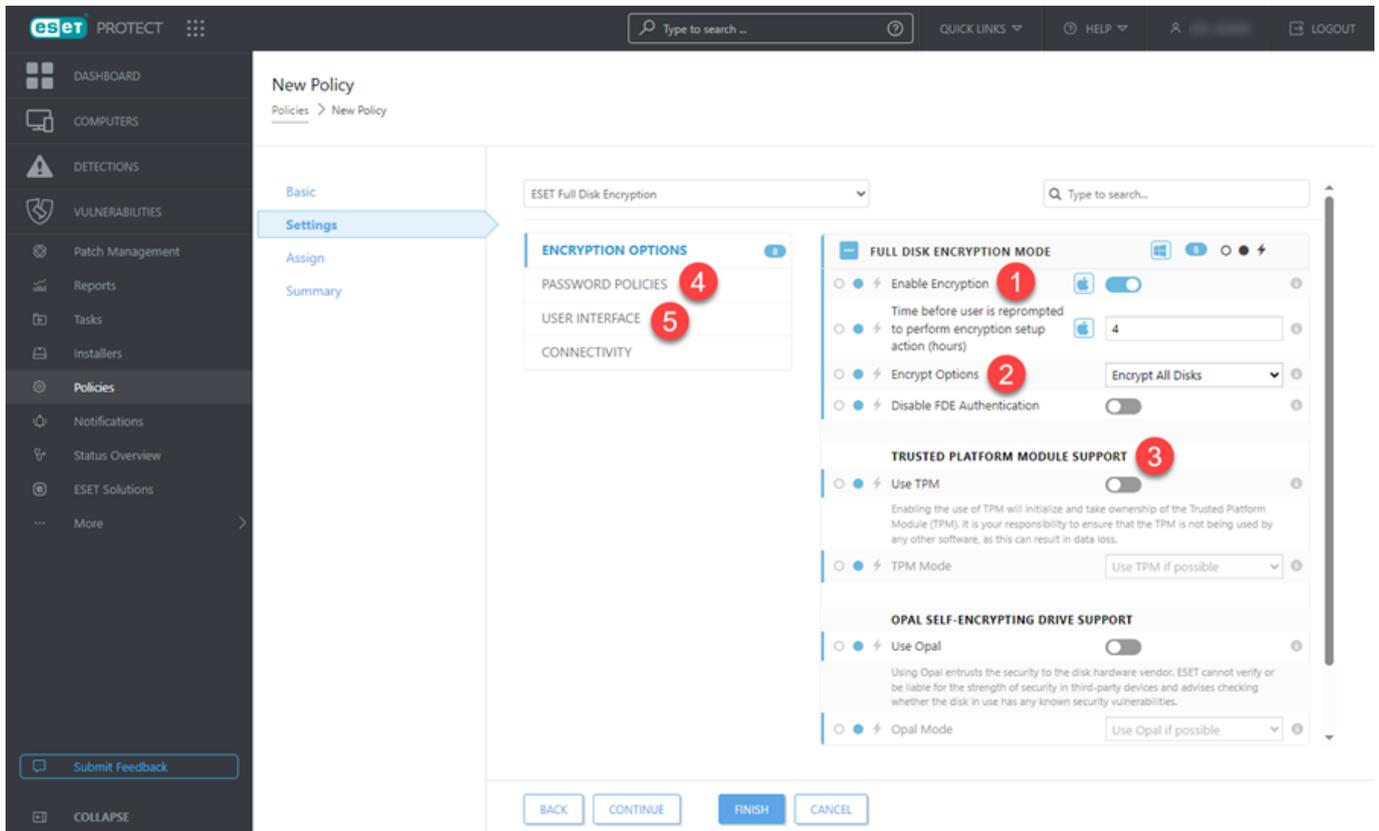
! Falls der Fehler **Ihr Computer ist nicht verschlüsselt und die gespeicherten Daten sind nicht geschützt** angezeigt wird, gehen Sie wie folgt vor, um die Computerverschlüsselung einzurichten und den Fehler zu beheben.

Sie können die ESET Full Disk Encryption-Einstellungen mit einer Policy in ESET Security Management Center, ESET PROTECT On-Prem oder ESET PROTECT konfigurieren: Wählen Sie **Policies > Neue Policy > Einstellungen** aus und wählen Sie das Produkt **ESET Full Disk Encryption** im Dropdownmenü aus.

Hier können Sie die gewünschte EFDE-Konfiguration erstellen:

i Die für macOS verfügbaren Policy-Optionen sind mit  markiert.

1. Öffnen Sie **Verschlüsselungsoptionen** -> **Modus für Laufwerksverschlüsselung** und aktivieren Sie die Einstellung **Verschlüsselung aktivieren**. Diese Einstellung aktiviert/deaktiviert die Verschlüsselung auf der verwalteten Workstation.



2. Wählen Sie unter **Verschlüsselungsoptionen** zwischen **Alle Laufwerke verschlüsseln** und **Nur Boot-Datenträger verschlüsseln**.

3. Um die **Unterstützung für Trusted Platform Module (TPM)** oder die **Unterstützung für selbstverschlüsselnde Opal-Laufwerke (OPAL)** für Ihre Verschlüsselung zu verwenden, wählen Sie die entsprechende Option für die verfügbare Hardware auf den verwalteten Workstations aus.

4. Legen Sie unter **Password-Policies** -> **Anforderungen an das Benutzerpasswort** fest, welche Anforderungen für das Pre-Boot-Passwort gelten sollen, mit dem sich der Benutzer bei der Workstation anmeldet.

5. Zuletzt können Sie unter **Benutzeroberfläche** -> **Elemente der Benutzeroberfläche** das Verhalten des EFDE-Clients festlegen, der auf den Workstations ausgeführt wird.

6. Klicken Sie auf **Fertig stellen**, um die Policy zu speichern. Weisen Sie die Policy noch nicht zu. Sie können die Policy anwenden, nachdem EFDE auf der Client-Workstation bereitgestellt wurde.

7. Bevor Sie die Verschlüsselung starten, [stellen Sie den EFDE Client auf den Workstations bereit](#).

Vollständige Beschreibung der Konfigurationsoptionen für ESET Full Disk Encryption:

- [Passwort-Policies](#)
- [Verschlüsselungsoptionen](#)
- [Benutzeroberfläche](#)
- [Tools](#)

Verschlüsselungsoptionen

Modus für Laufwerksverschlüsselung

-  **Verschlüsselung aktivieren** - Diese Einstellung aktiviert/deaktiviert die Verschlüsselung auf dem Gerät. Wenn Sie eine **Deaktivieren**-Policy auf eine verschlüsselte Workstation anwenden, wird die Workstation entschlüsselt.
-  **Legt fest, nach wie vielen Stunden der Benutzer aufgefordert wird, das Verschlüsselungssetup auszuführen** - Der maximale Wert ist 24 Stunden. Legt fest, in welchen Abständen (in Stunden) der Benutzer aufgefordert wird, das Verschlüsselungspasswort auf der Workstation einzurichten.
-  **Verschlüsselungsoptionen:**
 - **Alle Laufwerke verschlüsseln** - Verschlüsselt alle physischen Datenträger auf der Workstation. Externe Festplatten und USB-Laufwerke sind nicht betroffen.
 - **Nur Boot-Datenträger verschlüsseln** - Verschlüsselt nur den physischen Datenträger, den Windows momentan als Boot-Laufwerk verwendet.
-  **FDE-Authentifizierung deaktivieren** – Diese Einstellung aktiviert/deaktiviert die Pre-Boot-Passwortauthentifizierungsanforderung für die Workstation.

Unterstützung für Trusted Platform Module

Policy-Einstellung	Unterstützte Betriebssysteme	Beschreibung
TPM verwenden		Aktivieren Sie TPM, um das Trusted Platform Module (TPM) zu initialisieren und in Betrieb zu nehmen. Stellen Sie unbedingt sicher, dass TPM von keiner anderen Software verwendet wird, da andernfalls Datenverluste auftreten können.
TPM-Modus		<ul style="list-style-type: none">• TPM verwenden, wenn möglich - Der Verschlüsselungsprozess versucht, TPM für die Verschlüsselung zu verwenden. Wenn die TPM-Version nicht unterstützt wird oder kein TPM vorhanden ist, wird die Verschlüsselung ohne TPM fortgesetzt.• Muss TPM verwenden - Die Verschlüsselung muss TPM verwenden. Wenn TPM nicht vorhanden ist oder in einer nicht unterstützten Version ausgeführt wird, kann die Verschlüsselung nicht gestartet werden.

 Ab Version 1.2.4 von ESET Full Disk Encryption wird das TPM vor der Verwendung nicht gelöscht.

Unterstützung für selbstverschlüsselnde Opal-Laufwerke

Policy-Einstellung	Unterstützte Betriebssysteme	Beschreibung
Opal verwenden		Wenn aktiviert, muss die Verschlüsselung mit Opal-Verschlüsselungsunterstützung ausgeführt werden. Dies ist eine Hardwarefunktion von Laufwerken.
Opal-Modus		<ul style="list-style-type: none"> • Opal verwenden, wenn möglich - Der Verschlüsselungsprozess versucht, die Opal-Hardwareverschlüsselung zu verwenden. Wenn die Opal-Version nicht unterstützt wird oder die Opal-Verschlüsselungsoption nicht vorhanden ist, wird die Verschlüsselung ohne Opal fortgesetzt. • Muss Opal verwenden - Verschlüsselung muss Opal verwenden. Wenn Opal nicht vorhanden ist oder in einer nicht unterstützten Version ausgeführt wird, kann die Verschlüsselung nicht gestartet werden.

Passwort-Policies

Anforderungen an das Benutzerpasswort

- **Benutzer kann Passwort ändern** - Wenn Sie diese Option deaktivieren, können Passwortänderungen nur vom Administrator in der Remoteverwaltungskonsole ausgelöst werden.

Passwortzeichen

Policy-Einstellung	Unterstützte Betriebssysteme	Beschreibung
Muss Kleinbuchstaben verwenden		Das Passwort muss mindestens einen Kleinbuchstaben enthalten (a-z).
Muss Großbuchstaben verwenden		Das Passwort muss mindestens einen Großbuchstaben enthalten (A-Z).
Muss Ziffern verwenden		Das Passwort muss mindestens eine Ziffer enthalten (0-9).
Muss Sonderzeichen verwenden		Das Passwort muss mindestens ein Sonderzeichen enthalten (!@#\$%).
Passwort-Mindestlänge		Definiert die erforderliche Mindestlänge des Passworts (1-127 Zeichen).

Passwortversuche

Policy-Einstellung	Unterstützte Betriebssysteme	Beschreibung
Limit für ungültige Passwortversuche		Wenn diese Option deaktiviert ist, gilt kein Limit für falsche Passwordeingaben. Deaktivieren Sie diese Einstellung aus Sicherheitsgründen nie für längere Zeit.

Policy-Einstellung	Unterstützte Betriebssysteme	Beschreibung
Maximale Anzahl für ungültige Passwortversuche		Der Höchstwert ist 254. Die maximale Anzahl ungültiger Passwortversuche, bevor das Konto gesperrt wird und ein neues Passwort mit einem Wiederherstellungspasswort eingerichtet werden muss.

Passwortablauf

Policy-Einstellung	Unterstützte Betriebssysteme	Beschreibung
Passwort läuft ab		Wenn diese Option deaktiviert ist, läuft das Benutzerpasswort nicht ab.
Maximales Passwortalter (Tage)		Ein Wert zwischen 1 und 999 Tagen. Der empfohlene Bereich liegt zwischen 30 und 90.
Warnen, wenn ein Passwort bald abläuft		Wenn diese Option deaktiviert ist, wird der Benutzer vom Produkt nicht gewarnt, wenn sein Passwort demnächst abläuft.
Warnen, wenn der Zeitraum kürzer ist als (Tage)		Ein Wert zwischen 1 und 999 Tagen. Legen Sie fest, wie viele Tage vor Ablauf des Passworts der Benutzer gewarnt werden soll.

Optionen für das Wiederherstellungspasswort

Passwortversuche

Policy-Einstellung	Unterstützte Betriebssysteme	Beschreibung
Limit für ungültige Passwortversuche		Wenn diese Option deaktiviert ist, gilt keine Einschränkung für falsche Eingaben des Wiederherstellungspassworts. Deaktivieren Sie diese Einstellung aus Sicherheitsgründen nie für längere Zeit.
Maximale Anzahl für ungültige Passwortversuche		Der Höchstwert ist 254. Die maximale Anzahl ungültiger Passwortversuche, bevor das Konto gesperrt wird und ein neues Passwort mit einem Wiederherstellungspasswort eingerichtet werden muss.

Verwendung des Wiederherstellungspassworts



- Alle Einstellungen in diesem Bereich sind standardmäßig deaktiviert. Aktivieren Sie sie daher manuell.
- Die Einstellungen in diesem Bereich werden übernommen und treten in Kraft, nachdem der Computer entschlüsselt und anschließend erneut verschlüsselt wurde.

Policy-Einstellung	Unterstützte Betriebssysteme	Beschreibung
Verwendung des Wiederherstellungspassworts einschränken		Wenn diese Option deaktiviert ist, kann das gleiche Wiederherstellungspasswort wiederholt verwendet werden, bis ein neues Passwort erstellt wurde.
Maximale Verwendungen		Der Höchstwert ist 254.
Benutzer warnen, wenn das Limit für das Wiederherstellungspasswort fast erreicht ist		Wenn diese Option aktiviert ist, wird der Benutzer gewarnt, wenn das Wiederherstellungspasswort demnächst abläuft.
Warnen bei verbleibenden Verwendungen		Der Höchstwert ist 255.
Neues Wiederherstellungspasswort automatisch generieren		Wenn diese Option aktiviert ist, wird automatisch ein neues Wiederherstellungspasswort generiert, wenn die festgelegte verbleibende Anzahl an Passwortnutzungen erreicht wird.
Generieren bei (verbleibende Verwendungen)		Der Höchstwert ist 255.

Benutzeroberfläche

Elemente der Benutzeroberfläche

-   **Startmodus:**

oVollständig – Das komplette Hauptprogrammfenster wird angezeigt.

oMinimal – Die grafische Benutzeroberfläche wird ausgeführt, aber nur Benachrichtigungen werden angezeigt.

Status

-   **Anzuzeigende Hinweise:** Legen Sie fest, welche Anwendungsstatusmeldungen in der Desktopanwendung angezeigt und welche Statusmeldungen gesendet werden sollen.

Präsentationsmodus

Policy-Einstellung	Unterstützte Betriebssysteme	Beschreibung
Präsentationsmodus automatisch deaktivieren nach		Aktivieren Sie diese Option, um festzulegen, nach welchem Zeitraum der Präsentationsmodus deaktiviert werden soll.
Deaktivieren nach (Minuten)		Legen Sie den Zeitraum (in Minuten, maximal 2000) fest, nach dessen Ablauf der Präsentationsmodus deaktiviert werden soll.

Tools

Im Abschnitt „Tools“ können Sie eine Proxyverbindung für die Aktivierung von EFDE angeben.

Proxyserver

Policy-Einstellung	Unterstützte Betriebssysteme	Beschreibung
Proxyserver verwenden	 	Aktiviert die Nutzung der Proxyverbindung für die Produktaktivierung.
Proxyserver	 	Geben Sie die Adresse des Proxyservers an.
Port	 	Geben Sie den Port des Proxyservers an.
Proxyserver erfordert Authentifizierung	 	Diese Einstellung muss aktiviert werden, wenn für die Proxyverbindung Authentifizierung erforderlich ist.
Benutzername	 	Geben Sie den Benutzernamen für die Proxyauthentifizierung an.
Passwort	 	Geben Sie das Passwort für die Proxyauthentifizierung an.
Direktverbindung verwenden, wenn der Proxy nicht verfügbar ist	 	Wenn diese Option aktiviert ist, kann die direkte Verbindung als Fallback verwendet werden.

EFDE-Client-Bereitstellung

Der EFDE-Client muss installiert werden, um Laufwerke auf verwalteten Workstations verschlüsseln zu können.

Aufgrund eines bekannten Problems ist es nicht möglich, ein Live-Installationsprogramm in ESET PROTECT für EFDE für macOS zu erstellen.

 Daher empfehlen wir, zunächst den ESET Management Agent auf der Ziel-Workstation bereitzustellen und anschließend EFDE für macOS mit dem [Task „Software-Installation“](#) oder dem [Verschlüsselungsassistenten für die Computerdetails](#) zu installieren.

Sie können den EFDE Client auf drei verschiedene Arten bereitstellen:

- [All-in-One-Installer erstellen](#)
- [Task „Software-Installation“](#)
- [Assistent „Verschlüsselung aktivieren“](#)

EFDE-All-in-One-Installationsprogramm

Aufgrund eines bekannten Problems ist es nicht möglich, ein Live-Installationsprogramm in ESET PROTECT für EFDE für macOS zu erstellen.

 Daher empfehlen wir, zunächst den ESET Management Agent auf der Ziel-Workstation bereitzustellen und anschließend EFDE für macOS mit dem [Task „Software-Installation“](#) oder dem [Verschlüsselungsassistenten für die Computerdetails](#) zu installieren.

Das EFDE-All-in-One-Installationsprogramm stellt den ESET Management Agent und den EFDE-Client mit einer ausführbaren Installationsdatei bereit.

1. Klicken Sie auf **Installationsprogramme > Installationsprogramm erstellen > All-in-One-Installationsprogramm**.
2. Klicken Sie im Abschnitt **Einfach** auf das Kontrollkästchen neben **Festplattenverschlüsselung**, um den EFDE-Client zum Installationsprogramm hinzuzufügen, und klicken Sie auf **Weiter**.
3. Wählen Sie die EFDE-Lizenz aus, die Sie verwenden möchten.
4. Wählen Sie **Produkt und Version** aus, die Sie zum Installationsprogramm hinzufügen möchten. Mit Ausnahme bestimmter Fälle sollten Sie immer die neueste verfügbare Version des Produkts verwenden.
5. Wählen Sie die **Sprache** für das Installationsprogramm und das zu installierende Produkt aus.
6. Wählen Sie die **Konfigurations-Policy** aus, die Sie zuvor erstellt haben, oder wählen Sie eine der standardmäßig verfügbaren vorkonfigurierten Policies aus.
7. Aktivieren Sie das Kontrollkästchen, um die EULA und die Datenschutzerklärung zu akzeptieren.
8. Im Abschnitt **Erweitert** können Sie einen **Namen** und eine **Beschreibung** für das Installationsprogramm eingeben, um die Identifikation zu erleichtern und zu beschleunigen.
9. Wenn Sie auf **Fertig stellen** klicken, können Sie das Installationspaket herunterladen und bereitstellen.

Task „EFDE-Software-Installation“

 Falls Sie einen Apple M1 Mac verwenden, stellen Sie sicher, dass Sie [Rosetta installiert](#) haben.

Sie können den EFDE-Client auf einer bereits verwalteten Workstation oder auf einer Gruppe von Workstations bereitstellen, indem Sie den Task „Software-Installation“ ausführen.

1. Klicken Sie auf **Tasks > Neu > Client-Task**.
2. Geben Sie einen **Namen** und eine **Beschreibung** für den Task ein, um die Identifikation zu erleichtern und zu beschleunigen.
3. Wählen Sie das **Betriebssystem** im Dropdownmenü **Taskkategorie** aus.
4. Wählen Sie die Option **Software-Installation** im Dropdownmenü **Task** aus.

New Client Task

Tasks > EFDE install task

Basic

Settings

Summary

Name

Tags

Select tags

Description

Task Category

Task

BACK CONTINUE FINISH CANCEL

5. Klicken Sie auf **Weiter**.

6. Klicken Sie auf **Paket auswählen** und wählen Sie das Produkt **ESET Full Disk Encryption** (für Windows) oder **ESET Full Disk Encryption für macOS** (für MacOS) aus.

7. Wählen Sie die EFDE-Lizenz aus, die Sie verwenden möchten.

8. Aktivieren Sie das Kontrollkästchen, um die EULA und die Datenschutzerklärung zu akzeptieren.

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, [REDACTED] 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. Klicken Sie auf **Fertig stellen** und wählen Sie **Trigger erstellen** im Benachrichtigungsfenster aus.

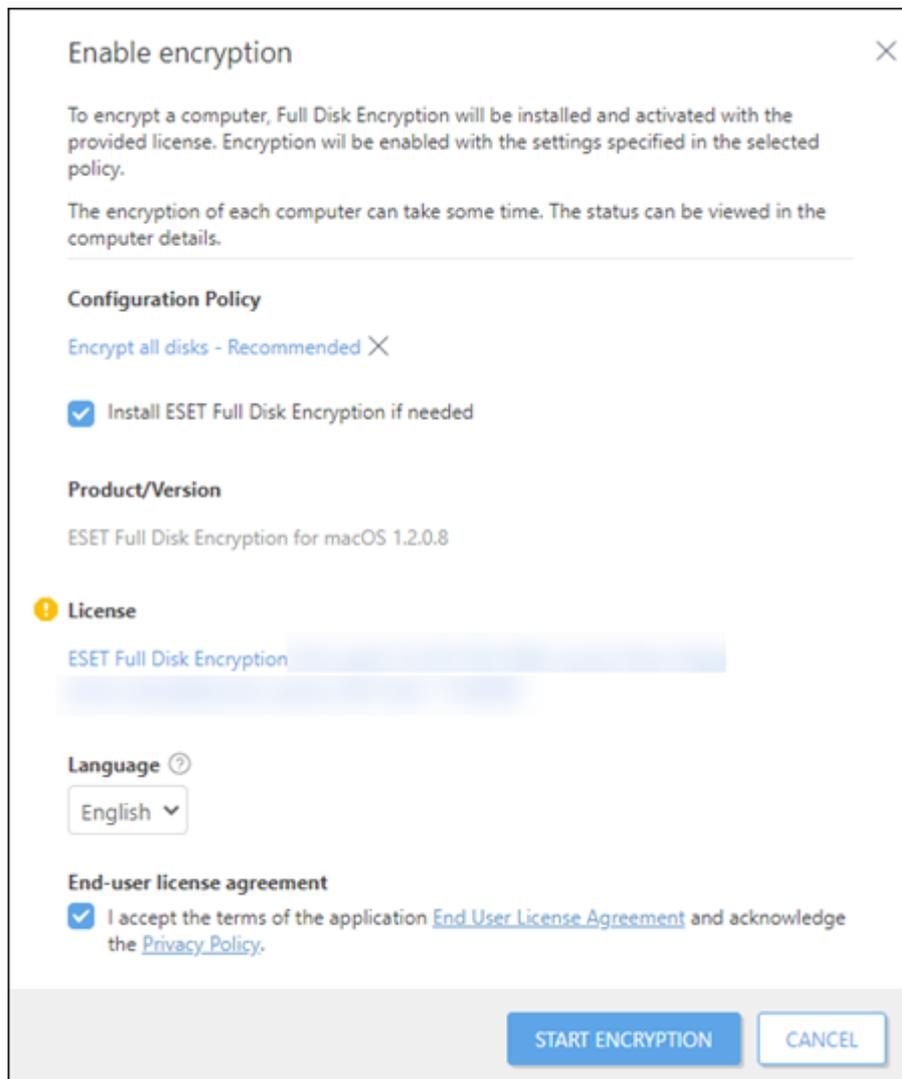
10. Wählen Sie im Abschnitt **Ziel** die Option **Computer hinzufügen** aus, um einzelne Workstations auszuwählen, auf denen Sie das Produkt installieren möchten.

11. Legen Sie den **Trigger** fest, der den Task ausführen soll, und klicken Sie auf **Fertig stellen**, um mit der Taskausführung fortzufahren.

Nachdem der Task erfolgreich ausgeführt wurde, müssen Sie im nächsten Schritt auf der Ziel-Workstation die [Verschlüsselung aktivieren](#).

Assistent „Verschlüsselung aktivieren“

Sie können die Verschlüsselung auf einer verwalteten Workstation im Bildschirm **Computer** starten, indem Sie im **Kontextmenü** die Option **Verschlüsselung aktivieren** auswählen, oder in den Computerdetails der ausgewählten Workstation unter **Details anzeigen** -> **Übersicht** > Kachel „Verschlüsselung“ -> **Computer verschlüsseln**.



Gehen Sie im Assistent **Verschlüsselung aktivieren** wie folgt vor:

1. Wählen Sie die **EFDE-Konfigurations-Policy** aus, die Sie verwenden möchten.
2. Wählen Sie das Kontrollkästchen neben **ESET Full Disk Encryption bei Bedarf installieren** aus, wenn der EFDE-Client nicht bereits auf der Workstation installiert ist.
3. **Produkt und Version** werden anhand des BS auf der Workstation ausgewählt.

i Falls Sie ESET Security Management Center verwenden, müssen Sie **Produkt und Version** auswählen, die Sie zum Installationsprogramm hinzufügen möchten. Mit Ausnahme bestimmter Fälle sollten Sie immer die neueste verfügbare Version des Produkts verwenden.

4. Wählen Sie die EFDE-Lizenz aus, die Sie verwenden möchten.
5. Wählen Sie die **Sprache** für das Installationsprogramm und das zu installierende Produkt aus.
6. Aktivieren Sie das Kontrollkästchen, um die EULA und die Datenschutzerklärung zu akzeptieren.
7. Anschließend können Sie auf **Verschlüsselung starten** klicken, um den Verschlüsselungsprozess auf der Workstation zu starten.

ESET Full Disk Encryption über die Kommandozeile bereitstellen

- [Installationsprogramm mit einem vordefinierten Passwort bereitstellen](#)
- [Passwort über Befehlszeile ungültig machen](#)
- [FDE-Authentifizierung über die Befehlszeile aussetzen/fortsetzen](#)
- [Tastaturlayouts über Befehlszeile hinzufügen/entfernen](#)

Installationsprogramm mit einem vordefinierten Passwort bereitstellen

Bei der Bereitstellung von ESET Full Disk Encryption können Sie Installationsparameter verwenden um ein Passwort für den Start der Verschlüsselung und ein Tastaturlayout festzulegen. Sie können Installationsparameter verwenden, um ein System mit einem vordefinierten Passwort bereitzustellen, damit ein MSP oder ein Administrator einen neuen Computer einrichten, ESET Full Disk Encryption bereitstellen und das System automatisch verschlüsseln kann, wenn eine Verschlüsselungs-Policy festgelegt wurde.

Voraussetzungen:

- Die Parameter `STARTUPPASSWORD` und `STARTUPPASSWORDKLID` müssen bei der Installation von ESET Full Disk Encryption angegeben werden.
- ESET Full Disk Encryption Version 1.3.0.x
- Die Installation von ESET Full Disk Encryption muss aktiviert sein.
- Das System muss über den ESET Management Agent mit der ESET PROTECT On-Prem Konsole verbunden sein.

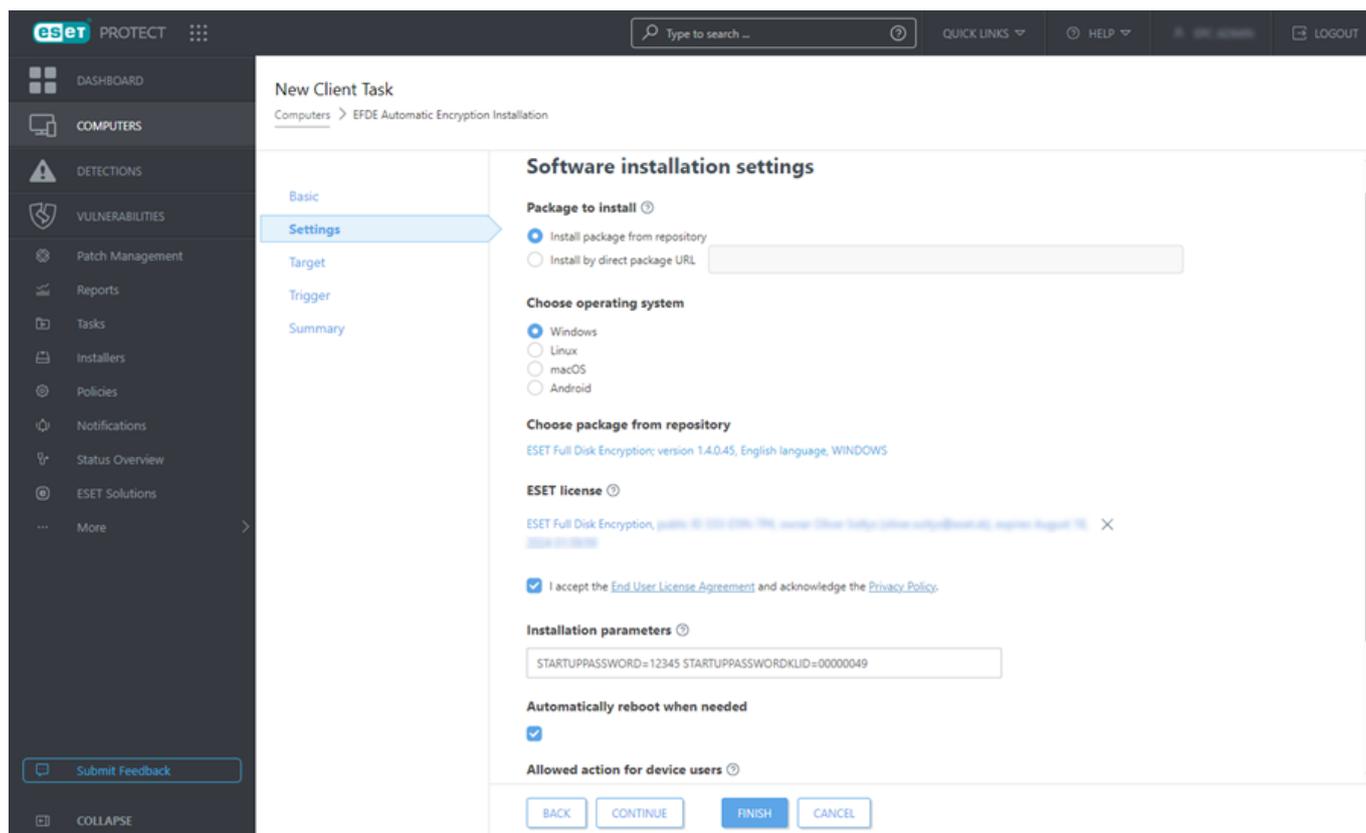
1. Klicken Sie in der ESET PROTECT On-Prem Konsole auf **Computer**.
2. Klicken Sie auf den Computer und dann auf **Tasks > Neuer Task**.
3. Geben Sie den Tasknamen ein (z. B. EFDE-Installation mit automatischer Verschlüsselung) und wählen Sie **Softwareinstallation** im Dropdownmenü **Task** aus.
4. Klicken Sie auf **Weiter**.
5. Klicken Sie auf **<Choose package>** und wählen Sie das Installationspaket aus dem Repository aus.
6. Geben Sie `STARTUPPASSWORD` und `STARTUPPASSWORDKLID` unter **Installationsparameter** ein.

STARTUPPASSWORD legt das ursprüngliche FDE-Passwort fest. Wenn Sie beispielsweise den Parameter STARTUPPASSWORD=12345 angeben, wird das Verschlüsselungspasswort 12345 festgelegt.

STARTUPPASSWORDKLID legt das Tastaturlayout fest. Wenn Sie den Parameter STARTUPPASSWORDKLID=00000409 angeben, wird eine englische US-Tastatur auf dem System installiert. Der Parameter verwendet Tastatur-KLIDs, um das Tastaturlayout zu identifizieren und zum System hinzuzufügen. Siehe [Liste der Tastaturlayouts](#).

Diese Parameter müssen gemeinsam verwendet werden, um die Verschlüsselung automatisch zu starten, wenn eine Verschlüsselungs-Policy auf dem System angewendet wird.

7. Wählen Sie **Bei Bedarf automatisch neu starten** aus. Der automatische Neustart ist nicht erforderlich, aber für die Installation von ESET Full Disk Encryption ist ein Neustart erforderlich. Ohne Neustart wird die Verschlüsselung nicht ausgeführt.



8. Nach der Installation von ESET Full Disk Encryption müssen Sie das Produkt aktivieren, um die Verschlüsselung zu starten. Sie müssen eine Verschlüsselungs-Policy erstellen und auf dem Gerät anwenden, um die Verschlüsselung im passenden Modus für die Kundenanforderungen zu starten.

Nachdem sie diese Schritte abgeschlossen haben, fordert das Gerät den Benutzer auf, den **Sicheren Start** auszuführen. Wenn der **Sichere Start** erfolgreich abgeschlossen wurde, beginnt das Gerät den Verschlüsselungsprozess, ohne dass der Benutzer ein Passwort eingeben muss.

Wenn der Kunde das Gerät neu startet, muss das im Installationsparameter STARTUPPASSWORD festgelegte Passwort eingegeben werden.

Der ESET PROTECT On-Prem Administrator kann den Task **FDE-Anmeldepasswort ungültig machen** senden, wenn ein Gerät neu zugeteilt wird. Auf diese Weise muss der Benutzer ein eigenes Passwort erstellen.

Passwort über Befehlszeile ungültig machen

Sie können das [FDE-Anmeldepasswort über die Befehlszeile auf dem Clientgerät ungültig machen](#).

Voraussetzungen:

- ESET Full Disk Encryption Version 1.3.0.x
- Die Installation von ESET Full Disk Encryption muss aktiviert sein.
- Das System muss über den ESET Management Agent mit der ESET PROTECT On-Prem Konsole verbunden sein.
- Das System muss gerade verschlüsselt werden oder bereits verschlüsselt sein.

1. Öffnen Sie eine Eingabeaufforderung als Administrator.

2. Navigieren Sie zu `C:\Program Files\ESET\ESET Full Disk Encryption` und führen Sie den Befehl `efdeais /command=invalidate_password` aus. Alternativ können Sie einen Befehl für den Speicherort und den Befehl verwenden: `C:\Program Files\ESET\ESET Full Disk Encryption efdeais /command=invalidate_password`.

3. Wenn der Befehl erfolgreich war, wird **Befehl erfolgreich** in der Befehlszeile angezeigt.

Die Benutzeroberfläche von ESET Full Disk Encryption informiert Sie über das abgelaufene Passwort und fordert die Benutzer auf, das Passwort zu ändern.

FDE-Authentifizierung über die Befehlszeile aussetzen/fortsetzen

Jedes Mal, wenn ein Benutzer versucht, das Gerät mit Full Disk Encryption zu starten, wird ein Pre-Boot-Authentifizierungsbildschirm angezeigt. Die Benutzer können den Pre-Boot-Authentifizierungsbildschirm aussetzen, beispielsweise wenn ein Neustart für Windows-Updates notwendig ist.

Voraussetzungen:

- ESET Full Disk Encryption Version 1.3.0.x
- Die Installation von ESET Full Disk Encryption muss aktiviert sein.
- Das System muss über den ESET Management Agent mit der ESET PROTECT On-Prem Konsole verbunden sein.
- Das System muss gerade verschlüsselt werden oder bereits verschlüsselt sein.

1. Öffnen Sie eine Eingabeaufforderung als Administrator.

2. Navigieren Sie zu `C:\Program Files\ESET\ESET Full Disk Encryption` und führen Sie den Befehl `efdeais /command=` mit einem der folgenden Parameter aus: `pause_authentication` oder `resume_authentication`. Alternativ können Sie einen Befehl für den Speicherort und den Befehl verwenden: `C:\Program Files\ESET\ESET Full Disk Encryption efdeais /command=pause_authentication`.

Wenn Sie den Befehl `pause_authentication` verwenden, müssen Sie eine Bedingung angeben, um die FDE-Authentifizierung für eine bestimmte Anzahl von Neustarts, einen bestimmten Zeitraum oder bis zu einem bestimmten Zeitpunkt auszusetzen. Beispiele:

```
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
```

Verwenden Sie einen [Unix-Zeitstempel](#), um einen Zeitpunkt anzugeben.

Für den Befehl `resume_authentication` müssen Sie keine zusätzlichen Parameter angeben. Wenn Sie die Authentifizierung fortsetzen, wird die FDE-Authentifizierung beim nächsten Systemstart angezeigt.

3. Wenn der Befehl erfolgreich war, wird **Befehl erfolgreich** in der Befehlszeile angezeigt, und ESET Full Disk Encryption zeigt an, dass die FDE-Authentifizierung deaktiviert ist.

Tastaturlayouts über Befehlszeile hinzufügen/entfernen

Mit Tastaturlayouts können Benutzer ihr Passwort bei der Pre-Boot-Authentifizierung eingeben und in der grafischen Benutzeroberfläche von ESET Full Disk Encryption ändern. Nicht alle Tastaturlayouts sind identisch, und Sie sollten sich mit den Unterschieden vertraut machen. Es gibt Befehlszeilenparameter, mit denen Benutzer Tastaturlayouts auf dem System hinzufügen, entfernen und auflisten können. Dies ist hilfreich, wenn ein Benutzer nach dem Start der Verschlüsselung ein Tastaturlayout zu Windows hinzufügen will. Wenn die Tastaturzuordnung nicht hinzugefügt wird, können die Benutzer ihr FDE-Passwort in Windows möglicherweise nicht ändern. Wenn eine andere physische Tastatur angeschlossen wurde, werden im Pre-Boot-Authentifizierungsbildschirm unter Umständen unerwartete Tasten angezeigt.

Voraussetzungen:

- ESET Full Disk Encryption Version 1.3.0.x
- Die Installation von ESET Full Disk Encryption muss aktiviert sein.
- Das System muss über den ESET Management Agent mit der ESET PROTECT On-Prem Konsole verbunden sein.
- Das System muss gerade verschlüsselt werden oder bereits verschlüsselt sein.

1. Öffnen Sie eine Eingabeaufforderung als Administrator.

2. Navigieren Sie zu `C:\Program Files\ESET\ESET Full Disk Encryption` und führen Sie den Befehl `efdeais /command=` mit einem der folgenden Parameter aus: `add_keyboard`, `remove_keyboard` oder `list_keyboards`. Alternativ können Sie einen Befehl für den Speicherort und den Befehl verwenden:
`C:\Program Files\ESET\ESET Full Disk Encryption efdeais /command=add_keyboard.`

Wenn Sie den Befehl `add_keyboard` verwenden, müssen Sie das Tastaturlayout, das Sie hinzufügen möchten, als Tastatur-KLID an den Befehl anhängen. Zum Beispiel „`efdeais /command=add_keyboard.00000809`“. Dieser Befehl fügt das GB-Tastaturlayout zum System hinzu.

Wenn Sie den Befehl `remove_keyboard` verwenden, müssen Sie das Tastaturlayout, das Sie entfernen möchten, als Tastatur-KLID an den Befehl anhängen. Zum Beispiel „`efdeais /command=remove_keyboard.00000809`“. Dieser Befehl entfernt das GB-Tastaturlayout aus dem System.

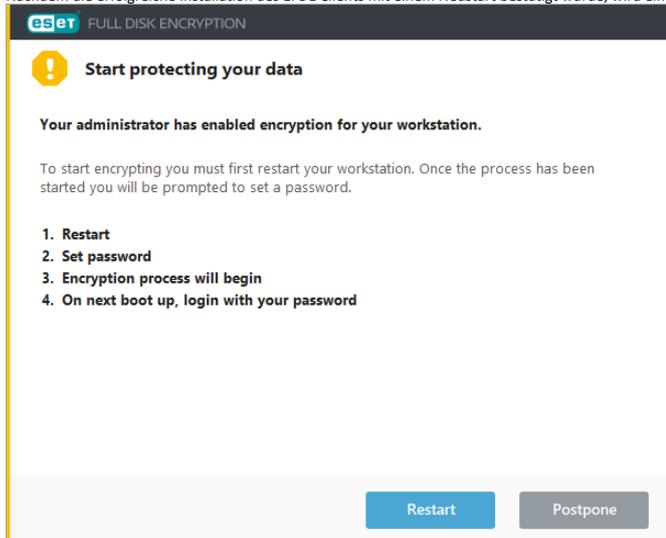
Für den Befehl `list_keyboard` müssen Sie keine zusätzlichen Parameter angeben. Zum Beispiel „`efdeais /command=list_keyboards`“. Dieser Befehl zeigt eine Nur-Text-Ansicht der aktuell im System installierten Tastaturlayouts an. Alternativ können Sie `.json` am Ende des Befehls anhängen, um das Tastaturlayout im JSON-Format anzuzeigen.

Clientseitiger EFDE-Verschlüsselungsprozess

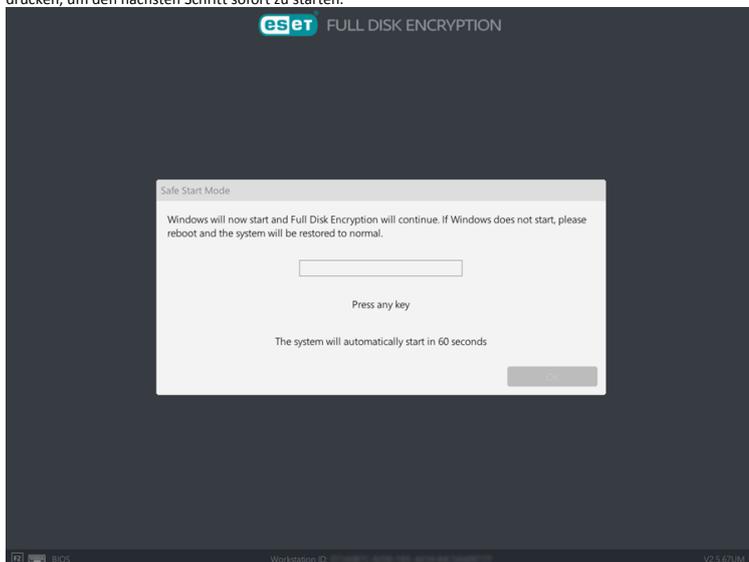
Nachdem Sie die Verschlüsselung in der Verwaltungskonsole initialisiert haben oder das All-in-One-Installationsprogramm erfolgreich abgeschlossen wurde, wird die Workstation neu gestartet, um den Verschlüsselungsprozess zu starten.

 [Windows](#)

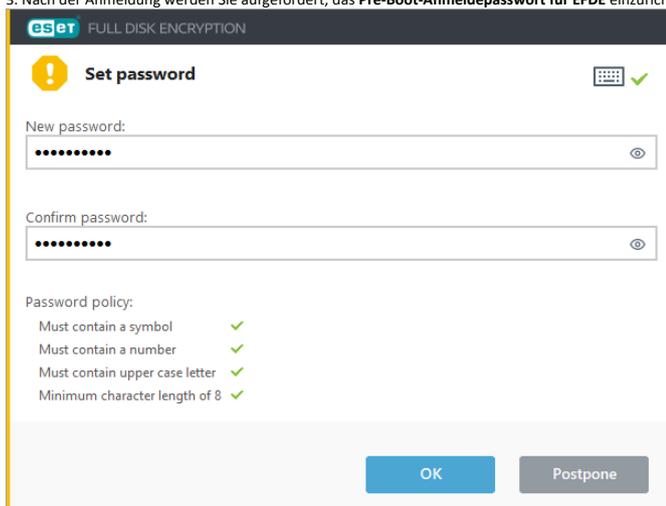
Nachdem die erfolgreiche Installation des EFDE Clients mit einem Neustart bestätigt wurde, wird ein Fenster mit den nächsten Verschlüsselungsschritten angezeigt.



1. Klicken Sie auf **Neu starten**, um die Verschlüsselung sofort zu starten, oder auf **Verschieben**, um die Verschlüsselung zu verschieben.
2. Nach dem Neustart wird der Bildschirm **EFDE Sicherer Startmodus** mit einem Timer von einer Minute angezeigt, und nach Ablauf des Timers wird der Vorgang gestartet. Sie können eine beliebige Taste drücken, um den nächsten Schritt sofort zu starten.



3. Nach der Anmeldung werden Sie aufgefordert, das **Pre-Boot-Anmeldepasswort für EFDE** einzurichten.



4. Der Benutzer kann das Passwort sofort festlegen (das Passwort muss die in der EFDE-Konfigurations-Policy festgelegten Anforderungen erfüllen) oder diesen Schritt auf später verschieben. Ohne diesen Schritt wird die Verschlüsselung nicht fortgesetzt.

i Wenn die Benutzer ihre Passwörter nicht eingerichtet haben und das System neu gestartet wird, wird der Verschlüsselungsprozess verschoben. Um den sicheren Start erneut auszuführen, muss der Administrator den EFDE-Client deinstallieren und anschließend den EFDE-Client erneut installieren.

5. Nachdem das Passwort erstellt wurde, wird die Verschlüsselung der Datenträger gestartet. Der Verschlüsselungsstatus wird in der EFDE Clientanwendung und in den Computerdetails der Workstation in der Management-Konsole angezeigt.
6. Wenn die Verschlüsselung erfolgreich abgeschlossen wurde und der Benutzer die Workstation neu startet, wird der EFDE-Pre-Boot-Anmeldebildschirm angezeigt, und der Benutzer muss das EFDE-Pre-Boot-Anmeldepasswort eingeben, um sich bei der Workstation anzumelden.

! Falls Sie einen Apple M1 Mac verwenden, stellen Sie sicher, dass Sie [Rosetta installiert](#) haben.

1. Nach der erfolgreichen Installation fordert die Clientanwendung Sie zur Eingabe der Anmeldeinformationen auf, um den Verschlüsselungsprozess zu starten.



2. Geben Sie Ihre Anmeldedaten im Fenster ein.



3. Nachdem Sie die korrekten Anmeldedaten eingegeben haben, wird der Verschlüsselungsprozess gestartet. Der Verschlüsselungsstatus wird in der EFDE Clientanwendung und in den **Computerdetails** der Workstation in der Management-Konsole angezeigt.

4. Nach Abschluss des Verschlüsselungsprozesses können Sie das Gerät weiterhin verwenden, aber das Laufwerk ist jetzt verschlüsselt.

Verschlüsselungsverwaltung

Zur Verwaltung verschlüsselter Arbeitsstationen gehört auch die Verwaltung der Pre-Boot-Anmeldung.

Sie erreichen diese Optionen unter **Computerdetails** -> **Übersicht** -> Kachel „Verschlüsselung“ -> **Verwalten**:

Sie können auch die  [Wartungsmodus](#)-Tasks und Policy-Optionen ausführen.

Alle EFDE-Tasks werden nur ausgeführt, wenn der ESET Management Agent den Task bei der Agenten-Replikation empfängt (normalerweise, wenn sich der Agent nach der Taskausführung wieder mit dem Management Server verbindet). Windows muss auf dem Computer gestartet werden, damit der Agent die Informationen zum Task empfangen kann. Der Pre-Boot-Anmeldesbildschirm reicht nicht aus, um diese Tasks auszuführen.

-  **FDE-Anmeldepasswort ungültig machen** – Dieser Task macht das aktuelle Anmeldepasswort sofort ungültig und fordert den Benutzer auf, sein Anmeldepasswort im Hauptprogrammfenster des EFDE Clients zu ändern. Wenn der Benutzer sein Passwort nicht im Hauptprogrammfenster des EFDE Clients ändert und das Gerät herunterfährt, wird er beim nächsten Start des Geräts aufgefordert, das Passwort im Pre-Boot-Anmeldebildschirm zu ändern.
-  **Neues FDE-Wiederherstellungspasswort generieren** – Dieser Task macht das aktuelle Anmeldepasswort sofort ungültig und generiert ein neues Passwort, das dem Benutzer vom Administrator bereitgestellt werden kann.
-   **Zugriff wiederherstellen**
 - o   **Wiederherstellungspasswort** – Generiert das Wiederherstellungspasswort des Benutzers, um ein neues Anmeldepasswort einzurichten.
 - o   **Wiederherstellungsdaten** - Generiert die für die Wiederherstellen der Verschlüsselung erforderliche Entschlüsselungsdatei.
-  **Zugriff blockieren**
 - o  **FDE-Anmeldepasswort blockieren** – Dieser Task erzwingt, dass der Benutzer ein Wiederherstellungspasswort benötigt, um den Computer zu starten. Der Benutzer braucht das **Wiederherstellungspasswort**, um ein neues Pre-Boot-Anmeldepasswort festlegen und sich wieder beim Gerät anmelden zu können. Der Benutzer kann sein Anmeldepasswort in diesem Zustand im Pre-Boot-Anmeldebildschirm nicht ändern, selbst wenn dies per EFDE-Konfigurations-Policy erlaubt ist.
 - o  **FDE-Anmeldepasswort löschen** – Dieser Task setzt das Gerät, auf dem er ausgeführt wird, sofort außer Betrieb. Die FDE-Anmeldung wird auf dem Gerät gelöscht, und der Benutzer kann sich nicht mehr anmelden. Benutzeranmeldung, Passwortänderung und Passwortwiederherstellung sind in diesem Zustand deaktiviert. Die einzige Option ist das Wiederherstellen der Verschlüsselung mit einem Wiederherstellungslaufwerk.

FDE-Authentifizierung anhalten

 Diese Option ist für EFDE für macOS nicht verfügbar.

 Wenn **FDE-Authentifizierung anhalten** auf einer Workstation aktiviert ist, kann das System ohne Authentifizierung gestartet werden und ist daher nicht vor Bedrohungen geschützt.

Mit der Option **FDE-Authentifizierung anhalten** können Sie die EFDE FDE-Authentifizierungsanforderung aktivieren, deaktivieren oder aufschieben.

Der Administrator kann den Clienttask **FDE-Authentifizierung anhalten** verwenden, um die FDE-Authentifizierung

nach dem Starten des Computers vorübergehend zu deaktivieren.

Sie können den Client-Task **FDE-Authentifizierung anhalten** über Ihre Management-Konsole aufrufen, indem Sie zu **Tasks** -> **Neu** -> **Clienttask** navigieren und im Dropdownmenü **Task FDE-Authentifizierung anhalten** auswählen:

New Client Task

Tasks > Pause FDE

Basic

Settings

Summary

Name

Tags

Select tags

Description

Task Category

Task

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

- **Einstellungen:**

0Anzahl der Neustarts – Hier können Sie die Anzahl der Neustarts für die Workstation festlegen, die ohne Aufforderung zur FDE-Authentifizierung erfolgen dürfen.

0Zeitraumoption auswählen: Zeitintervall – Geben Sie ein Zeitintervall (in Sekunden, Minuten, Stunden oder Tagen) oder ein **Datum und eine Uhrzeit** an, in dem die Workstation ohne die FDE-Authentifizierung neugestartet werden kann.

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

 Wenn der Task mindestens einen der festgelegten Werte erreicht, wird die FDE-Authentifizierung wieder aktiviert.

Um die FDE-Authentifizierung fortzusetzen, bevor der Task das festgelegte Limit erreicht, kann der Administrator den Client-Task **FDE-Authentifizierung fortsetzen** verwenden.

Um die FDE-Authentifizierung für längere Zeit dauerhaft zu deaktivieren, kann der Administrator die Option **FDE-Authentifizierung deaktivieren** in der EFDE-Policy verwenden.

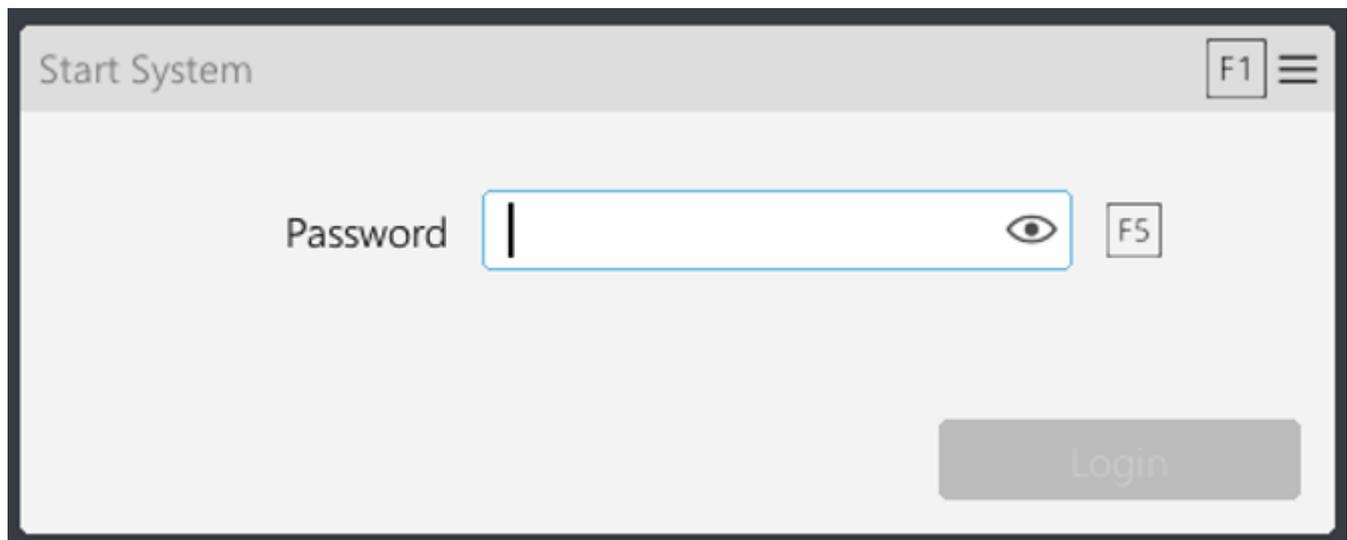
Die Einstellung  **FDE-Authentifizierung deaktivieren** befindet sich in der EFDE-Policy unter **Verschlüsselungsoptionen - > Modus für vollständige Laufwerksverschlüsselung**.

Wenn die FDE-Authentifizierung mit der Option **FDE-Authentifizierung deaktivieren** in der EFDE-Policy deaktiviert wurde, bleibt die FDE-Authentifizierung solange deaktiviert, bis diese Einstellung deaktiviert und auf eine bestimmte Workstation angewendet wurde. Der Clienttask **FDE-Authentifizierung fortsetzen** kann die FDE-Authentifizierung nicht fortsetzen, wenn die Policy-Einstellung **FDE-Authentifizierung deaktivieren** angewendet ist.

Pre-Boot-Anmeldung

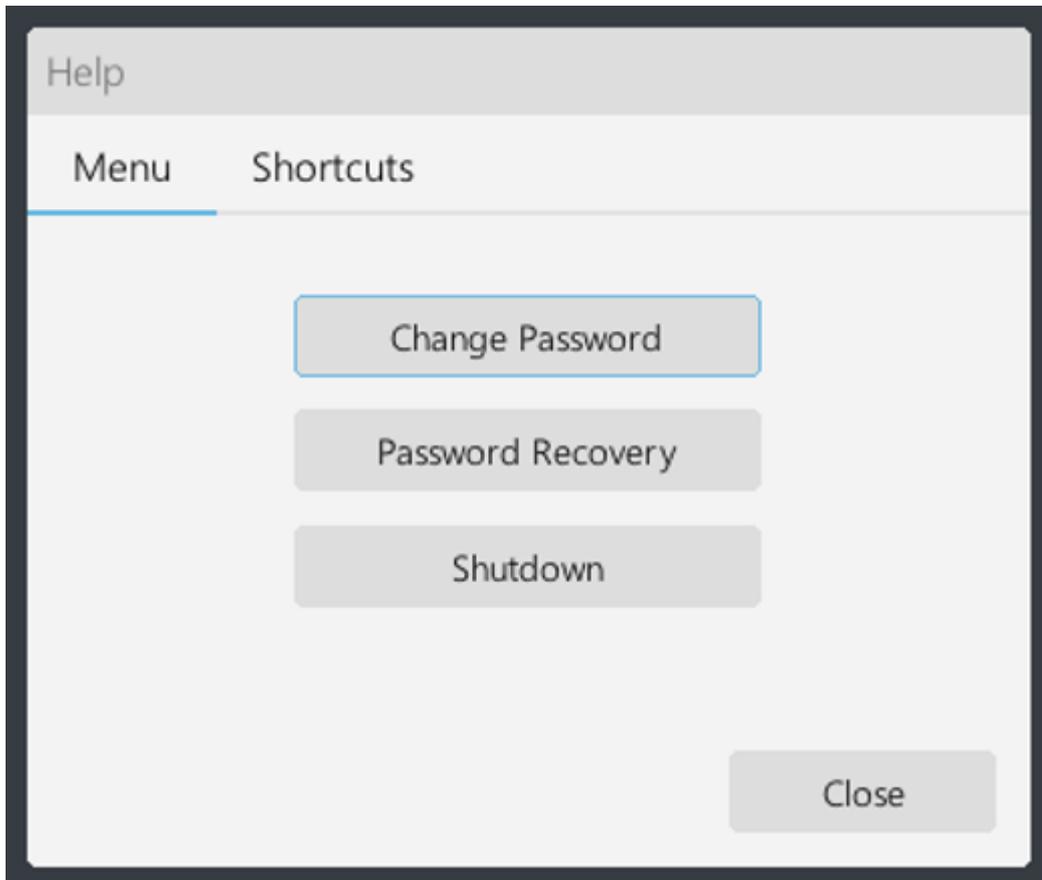
Wenn die Verschlüsselung auf einer Workstation aktiv ist und das Produkt eine gültige Lizenz hat, wird der Pre-Boot-Anmeldebildschirm beim Starten der Workstation angezeigt.

Die Pre-Boot-Anmeldung ist eine zusätzliche Sicherheitsebene des EFDE-Produkts, die den Zugriff auf die Daten der Workstation schützt.

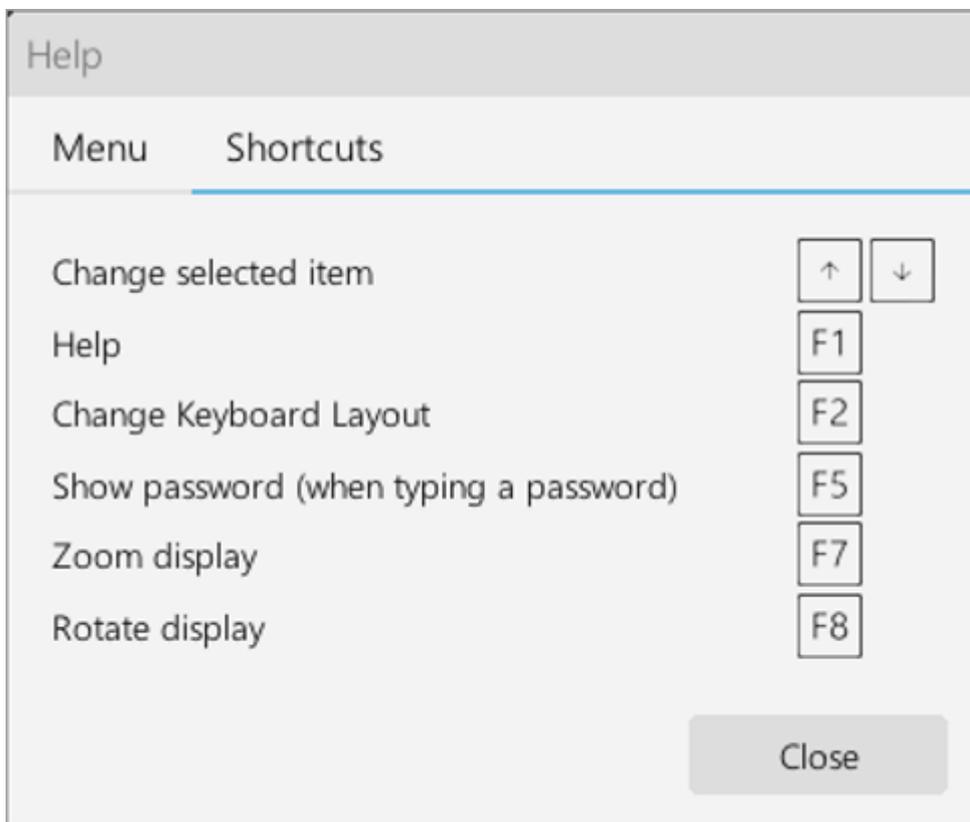


Im Pre-Boot-Anmeldebildschirm können Sie das Menü öffnen, indem Sie **F1** drücken. Dort können Sie das **Passwort ändern**, die [Passwort-Wiederherstellung](#) starten, die Workstation **herunterfahren** oder das Menü für die Pre-Boot-Anmeldung **schließen**.

Drücken Sie im Pre-Boot-Anmeldebildschirm auf **F5** für die Funktion **Passwort anzeigen** oder **F8**, um den **Bildschirm zu drehen**, falls der Bildschirm nicht korrekt angezeigt wird.



Verknüpfungen für den Pre-Boot-Bildschirm



Tastaturbefehl	
F1	Drücken Sie F1, um das Menü zu öffnen.

Tastaturbefehl	
F2	Drücken Sie F2, um das Tastaturlayout für FDE Pre-Boot zu ändern. Das ausgewählte Layout wird unten links angezeigt.
F5	Drücken Sie während der Eingabe Ihres Pre-Boot-Passworts F5, um es im Klartext anzuzeigen.
F7	Drücken Sie F7, um den Zoom anzupassen.
F8	Drücken Sie F8, um den Bildschirm zu drehen.
F10	Drücken Sie F10, um den Computer herunterzufahren.

Wiederherstellen der Verschlüsselung

Beim Wiederherstellen der Verschlüsselung kann ein Administrator die Wiederherstellung starten, falls sich der Benutzer mit seinem Passwort nicht anmelden kann oder die verschlüsselten Daten auf der Workstation aufgrund eines technischen Problems nicht verfügbar sind.

- [Passwort-Wiederherstellung](#) - Mit diesem Prozess kann ein Administrator ein Wiederherstellungspasswort für den Benutzer generieren.
- [Daten wiederherstellen](#) - Mit diesem Prozess kann ein Administrator ein Wiederherstellungslaufwerk für den Fall generieren, dass die Daten auf der Workstation mit normalen Methoden nicht mehr verfügbar sind.

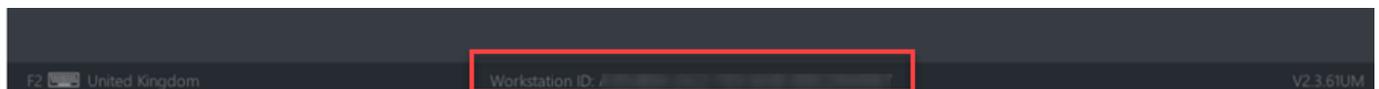
Wiederherstellungspasswort

Eine Passwortwiederherstellung ist erforderlich, wenn der Benutzer das Limit für falsche Passworteingaben im Pre-Boot-Anmeldebildschirm überschreitet oder wenn der Task „**FDE-Anmeldepasswort blockieren**“ ausgeführt wurde.



Falls keine Wiederherstellungsversuche mehr möglich sind, müssen Sie eine manuelle [Entschlüsselung](#) durchführen.

Sie benötigen eine **Workstation-ID** für den Wiederherstellungsprozess. Die **Workstation-ID** unterscheidet zwischen Groß- und Kleinbuchstaben. Sie finden die **Workstation-ID** am unteren Rand des Pre-Boot-Anmeldebildschirms:



 [Windows](#)

In diesem Zustand wird im Pre-Boot-Anmeldebildschirm die Warnung „Benutzer ist deaktiviert“ angezeigt. Der Benutzer muss **F1** drücken, um das Pre-Boot-Anmeldemenü zu öffnen, und dort **Passwort-Wiederherstellung** auswählen. An dieser Stelle muss sich der Benutzer an einen Administrator wenden, um ein Wiederherstellungspasswort zu erhalten.

Ein Administrator kann diesen Task auf zwei verschiedene Arten ausführen:

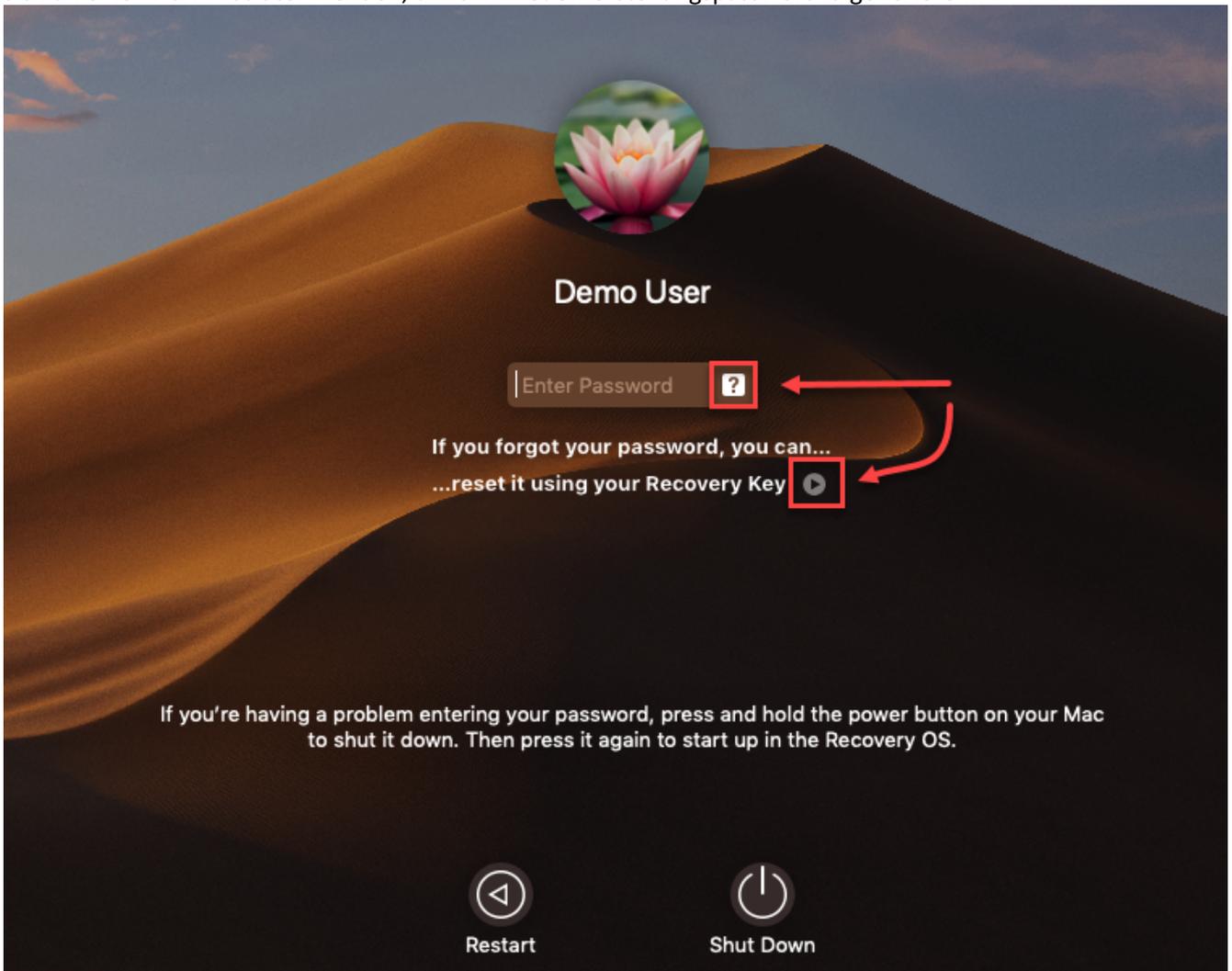
Wenn die betroffene Workstation in der Verwaltungskonsole identifiziert werden kann:

1. Klicken Sie auf die **Computerdetails** der Workstation in der Management-Konsole.
2. Klicken Sie auf **Übersicht** -> Kachel „Verschlüsselung“ -> **Verwalten** -> **Zugriff wiederherstellen** -> **Wiederherstellungspasswort**.
3. Mit dem Wiederherstellungsindex, der auf dem Bildschirm des Benutzers angezeigt wird, kann der Administrator dem Benutzer das korrekte Wiederherstellungspasswort zur Verfügung stellen.
4. Die Benutzer können ihr FDE-Anmeldepasswort ändern, nachdem sie ihr Passwort eingegeben haben.

Wenn die betroffene Workstation in der Verwaltungskonsole nicht identifiziert werden kann:

1. Navigieren Sie in oberen Leiste in der Management-Konsole zu **Hilfe** -> **Wiederherstellen der Verschlüsselung**.
2. Wählen Sie die Option **Wiederherstellungspasswort** aus.
3. An dieser Stelle muss der Benutzer dem Administrator die Workstation-ID übermitteln. Die Workstation-ID wird am unteren Rand des EFDE Pre-Boot-Anmeldebildschirms angezeigt.
4. Nachdem die korrekte Workstation-ID eingegeben wurde, wird eine Tabelle mit Wiederherstellungspasswörtern angezeigt.
5. Mit dem Wiederherstellungsindex, der auf dem Bildschirm des Benutzers angezeigt wird, kann der Administrator dem Benutzer das korrekte Wiederherstellungspasswort zur Verfügung stellen.
6. Die Benutzer können ihr FDE-Anmeldepasswort ändern, nachdem sie ihr Passwort eingegeben haben.

In diesem Fall muss der Benutzer auf das Fragezeichen  auf dem Anmeldebildschirm und anschließend auf das Pfeilsymbol  neben „Zurücksetzen mit Ihrem Wiederherstellungsschlüssel“ klicken. Die Benutzer müssen sich an einen Administrator wenden, um ein Wiederherstellungspasswort zu generieren.



Ein Administrator kann diesen Task auf zwei verschiedene Arten ausführen:

Wenn die betroffene Workstation in der Verwaltungskonsole identifiziert werden kann:

1. Klicken Sie auf die **Computerdetails** der Workstation in der Management-Konsole.
2. Klicken Sie auf **Übersicht** -> Kachel „Verschlüsselung“ -> **Verwalten** -> **Zugriff wiederherstellen** -> **Wiederherstellungspasswort**.
3. Mit dem Wiederherstellungsindex, der auf dem Bildschirm des Benutzers angezeigt wird, kann der Administrator dem Benutzer das korrekte Wiederherstellungspasswort zur Verfügung stellen.
4. Die Benutzer können ihr Anmeldepasswort ändern, nachdem sie ihr Passwort eingegeben haben.

Wenn die betroffene Workstation in der Verwaltungskonsole nicht identifiziert werden kann:

1. Navigieren Sie in oberen Leiste in der Management-Konsole zu **Hilfe** -> **Wiederherstellen der Verschlüsselung**.
2. Wählen Sie die Option **Wiederherstellungspasswort** aus.
3. An dieser Stelle muss der Benutzer dem Administrator die Workstation-ID übermitteln. Die Workstation-ID wird am unteren Rand des Anmeldebildschirms angezeigt.
4. Nachdem die korrekte Workstation-ID eingegeben wurde, wird eine Tabelle mit Wiederherstellungspasswörtern angezeigt.
5. Mit dem Wiederherstellungsindex, der auf dem Bildschirm des Benutzers angezeigt wird, kann der Administrator dem Benutzer das korrekte Wiederherstellungspasswort zur Verfügung stellen.
6. Die Benutzer können ihr Anmeldepasswort ändern, nachdem sie ihr Passwort eingegeben haben.

Wiederherstellungsdaten

Das Wiederherstellen der Verschlüsselung ist erforderlich, wenn der Task **FDE-Anmeldepaswort löschen** ausgeführt wurde oder falls ein Problem mit der Verschlüsselung oder im EFDE-Pre-Boot-Anmeldebildschirm auftritt und die Passwort-Wiederherstellung nicht möglich ist. Dieser Prozess entschlüsselt das Laufwerk auf der Workstation und deaktiviert die EFDE-Pre-Boot-Anmeldung.

Sie benötigen eine **Workstation-ID** für den Wiederherstellungsprozess. Die **Workstation-ID** unterscheidet zwischen Groß- und Kleinbuchstaben. Sie finden die **Workstation-ID** am unteren Rand des Pre-Boot-Anmeldebildschirms:

- Alle Benutzer mit **Lesezugriff** auf die statische Gruppe **Alle** (Zugriff auf alle Geräte) haben auch Zugriff auf die Wiederherstellungsdaten der entfernten Geräte.
- Wiederherstellungsdaten sind aus Sicherheitsgründen nur für Benutzer mit Zugriff auf die statische Gruppe **Alle** (Zugriff auf alle Geräte) verfügbar, zum Beispiel nur für globale Administratoren.

Ein Administrator kann diesen Task auf zwei verschiedene Arten ausführen:

Wenn die betroffene Workstation in der Verwaltungskonsole identifiziert werden kann:

1. Klicken Sie auf die **Computerdetails** der Workstation in der Management-Konsole.
2. Wählen Sie **Übersicht** -> Kachel „Verschlüsselung“ -> **Verwalten** -> **Zugriff wiederherstellen** -> **Wiederherstellungsdaten** aus.

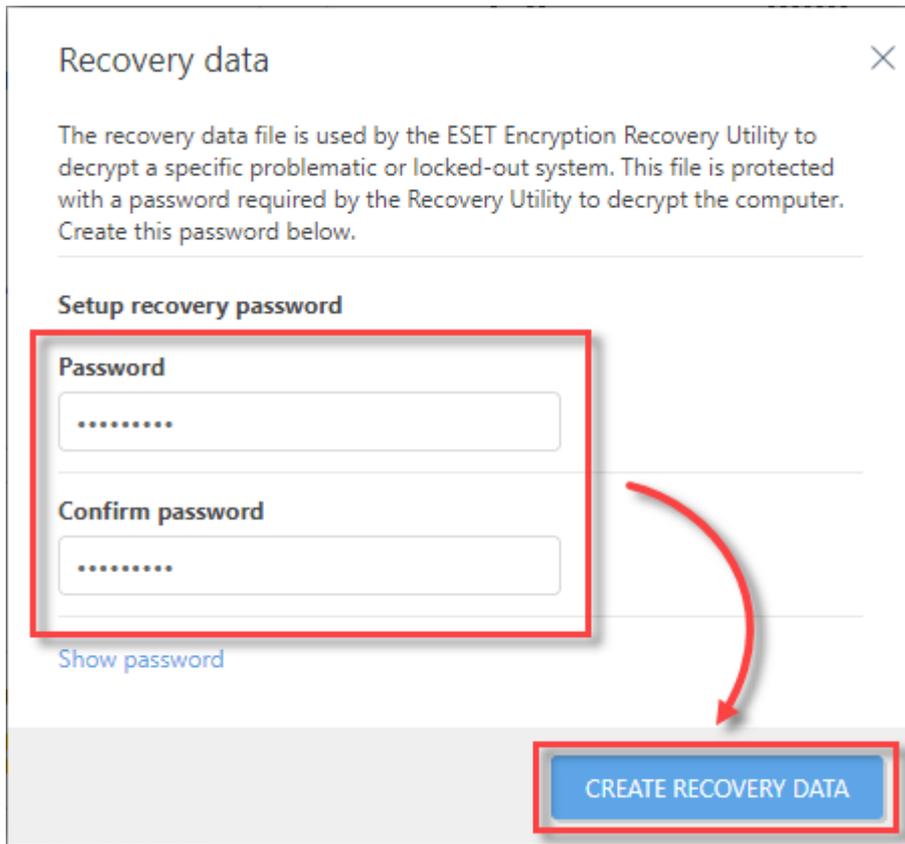
Wenn die betroffene Workstation in der Verwaltungskonsole nicht identifiziert werden kann:

1. Navigieren Sie zur oberen Leiste in der Verwaltungskonsole -> **Hilfe** -> **Wiederherstellen der Verschlüsselung**.
2. Wählen Sie die Option **Wiederherstellungsdaten** aus.
3. An dieser Stelle muss der Benutzer dem Administrator die Workstation-ID übermitteln. Die Workstation-ID wird im EFDE-Pre-Boot-Anmeldebildschirm am unteren Rand angezeigt.

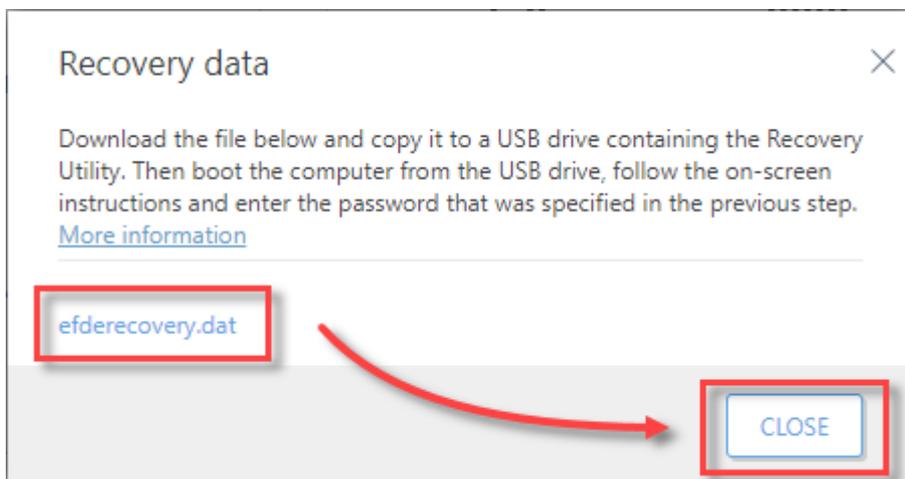
Ab diesem Moment ist der Wiederherstellungsprozess für beide Optionen gleich.

Laden Sie die Wiederherstellungsdatendatei herunter:

1. Erstellen Sie auf dem Bildschirm ein Einmal-Wiederherstellungspasswort (dieses Passwort ist nur für eine bestimmte Verschlüsselungswiederherstellung gültig).
2. Klicken Sie auf **Wiederherstellungsdaten erstellen**, um mit dem nächsten Schritt fortzufahren.



3. Klicken Sie im nächsten Fenster auf `efderecovery.dat`, laden Sie die Datei herunter und speichern Sie sie. Klicken Sie nach Abschluss dieses Schritts auf **Schließen**.



i Die Datei „efderecovery. dat“ ist einzigartig für jede Workstation und jede Verschlüsselung der Workstation. Wenn die Workstation verschlüsselt, entschlüsselt und anschließend erneut verschlüsselt wurde, ist die Entschlüsselungsdatei nicht mehr gültig.

 [Windows](#)

CDT Recovery Media Creator

1. Wählen Sie die Sprache für die Recovery Media Creator (Standard: Englisch).
2. Wählen Sie die Sprache für die Recovery Media Creator (Standard: Englisch).



3. Wählen Sie die Sprache für die Recovery Media Creator (Standard: Englisch).



4. Wählen Sie die Sprache für die Recovery Media Creator (Standard: Englisch).



5. Wählen Sie die Sprache für die Recovery Media Creator (Standard: Englisch).



6. Wählen Sie die Sprache für die Recovery Media Creator (Standard: Englisch).



7. Wählen Sie die Sprache für die Recovery Media Creator (Standard: Englisch).



8. Wählen Sie die Sprache für die Recovery Media Creator (Standard: Englisch).



9. Wählen Sie die Sprache für die Recovery Media Creator (Standard: Englisch).



10. Wählen Sie die Sprache für die Recovery Media Creator (Standard: Englisch).



11. Wählen Sie die Sprache für die Recovery Media Creator (Standard: Englisch).



12. Wählen Sie die Sprache für die Recovery Media Creator (Standard: Englisch).



13. Wählen Sie die Sprache für die Recovery Media Creator (Standard: Englisch).



14. Wählen Sie die Sprache für die Recovery Media Creator (Standard: Englisch).



15. Wählen Sie die Sprache für die Recovery Media Creator (Standard: Englisch).



16. Wählen Sie die Sprache für die Recovery Media Creator (Standard: Englisch).

Führen Sie für macOS 10.x - 11.x die unter [Einen mit ESET Full Disk Encryption verschlüsselten Apple-Computer entschlüsseln](#) beschriebene Prozedur aus.

- Schließen Sie ein leeres USB-Laufwerk an Ihren Computer an.
- Laden Sie das [Verschlüsselungs-Wiederherstellungstool für macOS herunter](#).
- Entpacken Sie den Inhalt der Datei, die Sie im vorherigen Schritt heruntergeladen haben, auf das USB-Laufwerk.
- Kopieren Sie die Datei `efderecovery.dat` auf das USB-Laufwerk.

Um diesen Prozess abschließen zu können, benötigen Sie ein Benutzerpasswort für den entsprechenden macOS-Computer. Ohne das Passwort kann der Prozess nicht abgeschlossen werden.

- Schließen Sie das USB-Laufwerk an den macOS-Computer an, den Sie wiederherstellen möchten, und starten Sie den **macOS-Wiederherstellungsmodus (CMD+R)**.
- Sie benötigen das Benutzerpasswort für den Zugriff auf die **macOS-Hilfsprogramme**. Klicken Sie auf **Hilfsprogramme > Terminal**.
- Navigieren Sie in der Konsole zum USB-Laufwerk und generieren Sie die Datei `FileVaultRecovery.keychain` mit dem Befehl `./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 %
```

- Geben Sie das Passwort ein, das Sie bei der Erstellung der Datei `efderecovery.dat` in Ihrer Management-Konsole festgelegt haben.

```
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 :
```

- Nachdem Sie die Datei `FileVaultRecovery.keychain` erstellt haben, können Sie mit der Laufwerksentschlüsselung fortfahren.

```
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 %
```

- Als Nächstes müssen Sie das verschlüsselte Laufwerk identifizieren. Navigieren Sie dazu zum Stammverzeichnis und führen Sie den Befehl `diskutil apfs list` im Terminal aus, um eine Liste der APFS-Volumes anzuzeigen.

- Suchen Sie in der angezeigten Liste nach dem Volume mit „**Macintosh HD**“ und vergewissern Sie sich, dass unter **Filevault: Ja (gesperrt)** angezeigt wird.

```
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)
```

- Notieren Sie sich den **Volume-ID-Namen** (z. B.: `disk2s1`).

- Entsperren Sie `FileVaultRecovery.keychain` mit dem folgenden Befehl:
`security unlock-keychain /path/to/FileVaultRecovery.keychain`
beispiel: `security unlock-keychain /Volumes/PatriotUSB/FileVaultRecovery.keychain`

- Anschließend müssen Sie das Volume entsperren, bevor Sie mit der Entschlüsselung fortfahren. Führen Sie dazu den folgenden Befehl aus:
`diskutil apfs unlockVolume /dev/disk2s1`. Ersetzen Sie dabei „`disk2s1`“ durch den Volume-ID-Namen aus dem vorherigen Schritt. Sie benötigen die Benutzer-Passphrase, um den Prozess fortsetzen zu können.

- An dieser Stelle ist das Laufwerk entsperrt und Sie können den Datenträger mit dem Wiederherstellungsschlüssel entschlüsseln, den Sie mit `recoveryapp` generiert haben.

```
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)
```

- Führen Sie den folgenden Befehl aus, um die Laufwerksentschlüsselung fortzusetzen:
`diskutil apfs decryptVolume /dev/volume id -recoverykeychain /path/to/filename.keychain`
beispiel: `diskutil apfs decryptVolume /dev/disk2s1 -recoverykeychain /Volumes/PatriotUSB/FileVaultRecovery.keychain`

- Mit dem folgenden Befehl können Sie den Status des Entschlüsselungsvorgangs überprüfen: `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)

- Nachdem der Prozess erfolgreich abgeschlossen wurde, beenden Sie das Terminal und starten Sie den Computer neu.

Entschlüsselung/Deinstallation

Bevor Sie den EFDE Client von der Workstation deinstallieren, müssen Sie alle verschlüsselten Laufwerke entschlüsseln.

Entschlüsselung:

1. Entfernen Sie alle aktuell auf den Computer angewendeten EFDE-Policies.
2. [Erstellen einer neuen EFDE Policy](#).
3. Klicken Sie auf **Verschlüsselungsoptionen** -> **Modus für Laufwerksverschlüsselung** und deaktivieren Sie die Einstellung **Verschlüsselung aktivieren**.
4. Speichern Sie diese Policy und weisen Sie Sie der Workstation zu, die Sie entschlüsseln möchten.
5. Sobald die Entschlüsselung auf der Workstation abgeschlossen wurde, wird die Workstation im Abschnitt **Computerdetails** als **Verschlüsselung nicht aktiv** angezeigt.

Deinstallation:

Sobald alle Laufwerke an der Workstation entschlüsselt wurden, können Sie den EFDE-Client deinstallieren.

1. Erstellen Sie einen neuen **Client-Task** -> **Software-Deinstallation**.
2. Klicken Sie auf **Einstellungen** und wählen Sie **Anwendung aus Liste** im Dropdownmenü aus.
3. **Zu deinstallierendes Paket auswählen: ESET Full Disk Encryption**.

New Client Task
Tasks > uninstall efde

Basic
Settings
Summary

Software uninsta

Uninstall
Application from list

Package name ⓘ
<Select package to uninstall>

Package version ⓘ
All
Uninstall all versions of package

Uninstallation parameters
[Empty text box]

Automatically reboot when

Please select item

NAME	VERSION	
<input type="checkbox"/> ESET Endpoint Security	9.0.2046.0	
<input checked="" type="checkbox"/> ESET Full Disk Encryption	1.3.3.35	
<input type="checkbox"/> ESET Management Agent	9.0.1141.0	
<input type="checkbox"/> ESET Management Agent	9.1.1298.0	
<input type="checkbox"/> ESET PROTECT Server	9.1.1295.0	
<input type="checkbox"/> ESET Rogue Detection Sensor	1.1.693.1	

OK CANCEL

4. Klicken Sie auf **Fertig stellen** und weisen Sie den Task zur Workstation zu.

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

Häufige Fragen

Warum werden Workstations mit EFDE als Teil der dynamischen Gruppen für das Sicherheitsprodukt installiert?

EFDE fällt nicht in die Kategorie der Sicherheitsprodukte.

Kann ich zwischen EFDE und ESET Endpoint Encryption migrieren?

Nein. Sie können nicht zwischen EFDE und ESET Endpoint Encryption migrieren.

In welcher Reihenfolge werden die UEFI-Pre-Boot-Anmeldebildschirme angezeigt, wenn die Pre-Boot-Anmeldung auf der Workstation aktiviert ist?

Die EFDE-Pre-Boot-Anmeldung wird nach der UEFI-Pre-Boot-Anmeldung angezeigt.

Kann ich das ESET Deployment Tool verwenden, um das All-in-One-Installationsprogramm mit EFDE bereitzustellen?

Ja Sie können das Deployment Tool verwenden, um das All-in-One-Installationsprogramm mit EFDE bereitzustellen.

Ist eine ähnliche Funktion wie der Wartungsmodus von ESET Endpoint Encryption in EFDE verfügbar?

Ja. Die Client-Version 1.2.0.5 und neuere Versionen von EFDE unterstützen den [Wartungsmodus](#).

Wenn die IT-Abteilung Wartungsarbeiten durchführen möchte und ein Benutzer sein Passwort für EFDE nicht verraten möchte, ist ein Wiederherstellungspasswort die einzige Option?

Nein. Die Clientversion 1.2.0.5 und neuere Versionen können den [Wartungsmodus](#) verwenden, um die FDE-Authentifizierungsanforderung auszusetzen.

Kann ich Daten von der formatierten Festplatte wiederherstellen, die ich mit EFDE verschlüsselt habe?

Nein. Sie können keine Daten von formatierten Festplatten wiederherstellen, die mit EFDE verschlüsselt wurden.

Gibt es einen Backdoor-Zugang für EFDE?

Nein. EFDE kann nur mit dem EFDE Passwort gestartet werden.

Fehlerbehebung

EFDE-Fehler/Warnung	Erklärung
Laut Policy muss ein TPM für die Verschlüsselung Ihres Computers verwendet werden, aber es ist kein passendes TPM vorhanden. TPM 2.0 ist erforderlich.	TPM wird in der EFDE-Konfigurations-Policy für die Verschlüsselung vorgeschrieben. Wenn die Workstation TPM 2.0 nicht unterstützt, wenden Sie die EFDE-Konfigurations-Policy ohne verbindliche TPM-Verschlüsselungsunterstützung an. Falls TPM 2.0 auf der Arbeitsstation unterstützt wird, der Fehler jedoch weiterhin angezeigt wird, finden Sie weitere Informationen in den Produkt-Logs.
Laut einer Policy muss Ihr Computer mit Opal verschlüsselt werden, aber mindestens ein Laufwerk unterstützt das Opal 2-Protokoll nicht.	OPAL wird in der EFDE-Konfigurations-Policy für die Verschlüsselung vorgeschrieben. Wenn die Workstation OPAL nicht unterstützt, wenden Sie die EFDE-Konfigurations-Policy ohne verbindliche OPAL-Verschlüsselungsunterstützung an. Wenn Opal auf der Arbeitsstation unterstützt wird, der Fehler jedoch weiterhin angezeigt wird, finden Sie weitere Informationen unter den Produkt-Logs.

EFDE-Fehler/Warnung	Erklärung
<p>In wenigen Tagen läuft Ihre Lizenz ab, und Ihr Computer verliert seinen Schutz. Dabei wird das Pre-Boot-Passwort entfernt, und Ihr Computer wird ohne jegliche Authentifizierung gestartet. Verlängern Sie Ihre Lizenz, um sich weiterhin zu schützen, oder aktivieren Sie das ESET Sicherheitsprodukt, falls Sie bereits einen Verlängerungsschlüssel oder eine neue Lizenz besitzen.</p>	<p>In diesem Zustand ist keine EFDE-Pre-Boot-Anmeldung erforderlich, aber die Daten auf der Workstation sind weiterhin verschlüsselt. Sie können entweder Ihre vorhandene Lizenz verlängern oder die Workstation mit einer Entschlüsselungs-Policy entschlüsseln.</p>
<p>Die Lizenz ist abgelaufen oder ungültig und die Pre-Boot-Authentifizierung wurde deaktiviert.</p>	<p>Ohne gültige Lizenz ist die Workstation weiterhin verschlüsselt, aber die EFDE-Pre-Boot-Anmeldung ist auf der Workstation nicht mehr erforderlich, bevor der Windows-Anmeldebildschirm angezeigt wird. Aktivieren Sie das Produkt mit einer gültigen EFDE Lizenz oder entschlüsseln Sie die Workstation und deinstallieren Sie die EFDE Clientanwendung.</p>
<p>Ihr Computer ist nicht verschlüsselt und die gespeicherten Daten sind nicht geschützt.</p>	<p>Diese allgemeine Warnung deutet darauf hin, dass die EFDE-Clientanwendung zwar ausgeführt wird, aber die Daten auf der Workstation nicht verschlüsselt sind. Um den Fehler zu beheben, aktivieren und konfigurieren Sie EFDE.</p>
<p>Die Verschlüsselung Ihres Computers konnte aufgrund eines Fehlers nicht gestartet werden. Weitere Informationen finden Sie in den System-Logs.</p>	<p>Der Verschlüsselungsprozess konnte nicht gestartet werden. Weitere Details zur Fehlerbehebung finden Sie in den Anwendungs-Logs.</p>
<p>Ihr Computer ist bereit für die Verschlüsselung, wartet jedoch darauf, dass ein Pre-Boot-Passwort konfiguriert wird.</p>	<p>Dieser Fehler deutet darauf hin, dass ein Benutzereingriff auf der Arbeitsstation erforderlich ist. Es wird dringend empfohlen, das Pre-Boot-Passwort vor dem nächsten Neustart festzulegen, um den Verschlüsselungsprozess fortzusetzen.</p>
<p>Ein Neustart des Computers ist erforderlich, um den sicheren Start zur Überprüfung der Hardware- und Firmware-Kompatibilität zu überprüfen und die Initialisierung auszuführen.</p>	<p>Nachdem das Produkt erfolgreich installiert wurde, deutet diese Fehlermeldung darauf hin, dass die Workstation als nächster erforderlicher Schritt neu gestartet werden muss, um den SafeStart-Modus von EFDE zu aktivieren. Dabei wird zum ersten Mal überprüft, ob die Workstation mit EFDE kompatibel ist und verschlüsselt werden kann.</p>

EFDE-Fehler/Warnung	Erklärung
Ihr Computer wurde neu gestartet und der sichere Start war erfolgreich, aber die Verschlüsselung wurde vor dem erneuten Neustart nicht korrekt gestartet. Daher wird die Verschlüsselung nicht gestartet. Weitere Informationen finden Sie in den System-Logs.	<p>Wenn der SafeStart-Prozess zwar überprüft hat, ob Hardware und Firmware der Workstation mit der Verschlüsselung kompatibel sind, aber die Workstation neu gestartet wurde, bevor das EFDE-Pre-Boot-Anmeldepasswort festgelegt wurde, wird der Verschlüsselungsprozess beendet. Dies wird in den Workstation-Logs wie folgt angegeben: „Der sichere Start war zwar erfolgreich, aber das Ergebnis ist veraltet, und der sichere Start muss erneut ausgeführt werden.“</p> <p>Sie können den Auswertungsprozess für den sicheren Start auf drei verschiedene Arten starten:</p> <ul style="list-style-type: none"> • Klicken Sie in ESET PROTECT für den Computer auf Details > Warnungen, klicken Sie auf Fehler beim Starten der Verschlüsselung und wählen Sie Fehlgeschlagene Verschlüsselung wiederholen aus. • Klicken Sie in ESET PROTECT auf Policies und ändern Sie die Einstellungen der Policy: <ol style="list-style-type: none"> 1. Aktivieren Sie die Option „Verschlüsselung aktivieren“, um die aktuelle Policy zu entfernen. 2. Deaktivieren Sie die Option „Verschlüsselung aktivieren“, um eine neue Policy hinzuzufügen. 3. Warten Sie die Verarbeitung auf dem EFDE Client ab, um den Status „Sicherer Start“ zurückzusetzen. 4. Aktivieren Sie die Option „Verschlüsselung aktivieren“, um die ursprüngliche Policy erneut hinzuzufügen. • Deinstallieren Sie die EFDE Client-App, und installieren Sie sie erneut.
Das Produkt wurde installiert oder aktualisiert. Starten Sie Ihren Computer neu, um die Software verwenden zu können.	Dieser Fehler wird angezeigt, nachdem das Produkt frisch installiert, erneut installiert oder aktualisiert wurde, und der Computer muss neu gestartet werden, bevor das Produkt seine Funktion wieder aufnehmen kann. Der Fehler sollte nach dem Neustart der Workstation verschwinden.
Präsentationsmodus ist aktiviert	Es ist ein potenzielles Sicherheitsrisiko, den Präsentationsmodus mit einer EFDE-Konfigurations-Policy zu aktivieren. Wenn der Präsentationsmodus aktiviert ist und jemand eine problematische oder unsichere Webseite oder Anwendung aufruft, kann dies blockiert werden. Für die Benutzer wird jedoch keine Erklärung oder Warnung angezeigt, da die Benutzerinteraktion deaktiviert ist.

Auf der Workstation finden Sie die EFDE Clientanwendungs-Logs an diesem Speicherort:

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

Um Logs für das Supportteam zu generieren, brauchen Sie das [ESET Encryption Diagnostics Tool](#).

Datenschutzerklärung

Der Schutz personenbezogener Daten genießt absolute Priorität bei ESET, spol. s r. o. mit eingetragenem Firmensitz in Einsteinova 24, 851 01 Bratislava, Slovak Republic, dem Handelsregistereintrag 3586/B vor dem Bezirksgericht Bratislava I, Rubrik Sro und der eingetragenen Unternehmensnummer 31333532 als Datenverantwortlicher („ESET“ oder „wir“). Wir möchten die Transparenzanforderungen erfüllen, die in der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union gesetzlich festgelegt sind. Aus diesem Grund veröffentlichen wir diese Datenschutzerklärung mit dem ausschließlichen Ziel, unsere Kunden („Endbenutzer“

oder „Sie“) als betroffene Person über die folgenden Themen im Hinblick auf den Schutz personenbezogener Daten zu informieren:

- Rechtliche Grundlage der Verarbeitung personenbezogener Daten
- Datenweitergabe und Vertraulichkeit
- Datensicherheit
- Ihre Rechte als betroffene Person
- Verarbeitung personenbezogener Daten
- Kontaktinformationen.

Rechtliche Grundlage der Verarbeitung personenbezogener Daten

Es gibt nur wenige rechtliche Grundlagen für die Datenverarbeitung, die wir gemäß dem geltenden rechtlichen Rahmen für den Schutz personenbezogener Daten verwenden. Die Verarbeitung personenbezogener Daten bei ESET dient hauptsächlich der Erfüllung der [Endbenutzer-Lizenzvereinbarung](#) („EULA“) im Hinblick auf den Endbenutzer (Art. 6 (1) (b) der DSGVO, die für die Bereitstellung von ESET-Produkten oder -Diensten gilt, sofern nicht ausdrücklich anders angegeben. Beispiele für rechtliche Grundlagen sind:

- Rechtliche Grundlage aufgrund legitimer Interessen (Art. 6 (1) (f) der DSGVO), mit der wir Daten zur Nutzung unserer Dienste und zur Zufriedenheit von Kunden verarbeiten, um Benutzer bestmöglich schützen, unterstützen und bedienen zu können. Sogar Marketing ist im geltenden Recht ebenfalls als legitimes Interesse anerkannt, daher verwenden wir es in Bezug auf die Marketingkommunikation mit unseren Kunden.
- Zustimmung (Art. 6 (1) (a) der DSGVO), die wir ggf. in bestimmten Situationen von Ihnen erbitten, wenn wir diese Rechtsgrundlage für besonders geeignet halten oder wenn dies gesetzlich erforderlich ist.
- Einhaltung einer gesetzlichen Verpflichtung (Art. 6 (1) (c) der DSGVO), z. B. die Anforderungen bei elektronischer Kommunikation, Rechnungsstellung oder Abrechnungsdokumenten.

Datenweitergabe und Vertraulichkeit

Wir geben Ihre Daten nicht an Dritte weiter. Allerdings ist ESET ein internationales Unternehmen, das weltweit durch angeschlossene Unternehmen oder Partner im Rahmen unseres Vertriebs-, Dienstleistungs- und Supportnetzwerks vertreten ist. Die von ESET verarbeiteten Informationen zu Lizenzierung, Abrechnung und technischem Support können zur Einhaltung der EULA an angeschlossene Unternehmen oder Partner übertragen und von diesen weitergeleitet werden, beispielsweise zur Bereitstellung von Diensten und zur Erbringung von Supportleistungen.

ESET bevorzugt die Verarbeitung seiner Daten in der Europäischen Union (EU). Je nach Ihrem Standort (Nutzung unserer Produkte und/oder Dienste außerhalb der EU) und/oder der von Ihnen ausgewählten Dienste kann es jedoch erforderlich sein, die Daten in ein Land außerhalb der EU zu übertragen. Im Zusammenhang mit Cloud-Computing nehmen wir beispielsweise Dienste von Drittanbietern in Anspruch. In diesen Fällen wählen wir unsere Dienstleister sorgfältig aus und gewährleisten durch vertragliche sowie technische und organisatorische Maßnahmen einen angemessenen Datenschutz. In der Regel werden EU-Standardvertragsklauseln vereinbart, bei Bedarf ergänzt durch vertragliche Bestimmungen.

In einigen Ländern außerhalb der EU, z. B. dem Vereinigten Königreich und der Schweiz, hat die EU bereits ein vergleichbares Datenschutzniveau beschlossen. Aufgrund dieses vergleichbaren Datenschutzstandards bedarf es zur Übertragung von Daten in diese Länder keiner besonderen Genehmigung oder Vereinbarung.

Datensicherheit

ESET implementiert angemessene technische und organisatorische Maßnahmen, um einen angemessenen Schutz vor potenziellen Risiken zu bieten. Wir bemühen uns nach Kräften, die fortlaufende Vertraulichkeit, Integrität, Verfügbarkeit und Ausfallsicherheit der Verarbeitungssysteme und Dienste zu gewährleisten. Sollten Ihre Rechte und Freiheiten durch einen Datenangriff gefährdet sein, informieren wir die Aufsichtsbehörden sowie die Endbenutzer als die betroffenen Personen.

Rechte betroffener Personen

Die Rechte aller Endbenutzer liegen uns am Herzen, und wir möchten Ihnen versichern, dass ESET allen Endbenutzern (aus einem EU-Land oder anderen Nicht-EU-Ländern) die nachstehenden Rechte garantiert. Zur Ausübung Ihrer Rechte als betroffene Person kontaktieren Sie uns mithilfe des Supportformulars, oder schreiben Sie eine E-Mail an dpo@eset.sk. Zu Identifizierungszwecken bitten wir Sie um die folgenden Informationen: Name, E-Mail-Adresse und, sofern vorhanden, Lizenzschlüssel oder Kundennummer sowie Firmenmitgliedschaft. Bitte senden Sie uns keine anderen personenbezogenen Daten wie beispielweise Ihr Geburtsdatum. Wir weisen zudem darauf hin, dass wir zur Abwicklung Ihrer Anfrage sowie zu Identifizierungszwecken Ihre personenbezogenen Daten verarbeiten.

Recht auf Widerruf der Zustimmung: Das Recht auf Widerruf der Zustimmung gilt nur im Falle einer Verarbeitung auf Grundlage einer Zustimmung. Wenn wir Ihre personenbezogenen Daten auf Grundlage Ihrer Zustimmung verarbeiten, können Sie Ihre Zustimmung jederzeit und ohne Angabe von Gründen widerrufen. Der Widerruf der Zustimmung gilt nur für die Zukunft und hat keinen Einfluss auf die Rechtmäßigkeit der vor dem Widerruf verarbeiteten Daten.

Recht auf Einspruch: Das Recht auf Einspruch gilt im Falle einer Verarbeitung auf Grundlage eines berechtigten Interesses von ESET oder eines Dritten. Wenn wir Ihre personenbezogenen Daten verarbeiten, um ein legitimes Interesse zu schützen, haben Sie als betroffene Person jederzeit das Recht, dem von uns angegebenen legitimen Interesse und der Verarbeitung Ihrer personenbezogenen Daten zu widersprechen. Ihr Einspruch gilt nur für die Zukunft und hat keinen Einfluss auf die Rechtmäßigkeit der vor dem Einspruch verarbeiteten Daten. Sofern wir Ihre personenbezogenen Daten zu Direktwerbungszwecken verarbeiten, müssen Sie Ihren Einspruch nicht begründen. Dies gilt auch für die Profilerstellung, insofern diese mit einer solchen Direktvermarktung in Zusammenhang steht. In allen anderen Fällen bitten wir Sie, uns die Beschwerde bezüglich des legitimen Interesses von ESET an der Verarbeitung Ihrer personenbezogenen Daten unverzüglich zukommen zu lassen.

Beachten Sie, dass wir in manchen Fällen trotz des Widerrufs Ihrer Zustimmung berechtigt sind, Ihre personenbezogenen Daten auf einer anderen rechtlichen Grundlage weiter zu verarbeiten, z. B. zur Erfüllung eines Vertrags.

Recht auf Auskunft: Als betroffene Person haben Sie das Recht, jederzeit kostenlos Informationen über Ihre bei ESET gespeicherten Daten zu verlangen.

Recht auf Berichtigung: Sollten wir versehentlich falsche personenbezogene Daten über Sie verarbeiten, haben Sie das Recht, diese berichtigen zu lassen.

Recht auf Löschung und auf Einschränkung der Verarbeitung: Als betroffene Person haben Sie das Recht, die Löschung Ihrer personenbezogenen Daten oder die Einschränkung der Verarbeitung dieser zu verlangen. Wenn wir Ihre personenbezogenen Daten verarbeiten, z. B. mit Ihrer Zustimmung, Sie diese Zustimmung widerrufen und keine andere gesetzliche Grundlage wie beispielsweise ein Vertrag vorliegt, löschen wir Ihre personenbezogenen Daten umgehend. Ihre personenbezogenen Daten werden auch gelöscht, sobald sie zum Ende der Aufbewahrungsdauer zu den genannten Zwecken nicht mehr benötigt werden.

Wenn wir Ihre personenbezogenen Daten ausschließlich für Direktmarketing verwenden und Sie Ihre Zustimmung widerrufen oder Einspruch gegen das berechnigte Interesse von ESET erheben, schränken wir die Verarbeitung Ihrer personenbezogenen Daten soweit ein, dass wir Ihre Kontaktdaten in unsere interne Negativliste aufnehmen, um derartige unerwünschte Kontaktaufnahmen zu vermeiden. Andernfalls werden Ihre personenbezogenen Daten gelöscht.

Beachten Sie, dass wir unter Umständen verpflichtet sind, Ihre Daten bis zum Ablauf der von Gesetzgeber und Aufsichtsbehörden vorgegebenen Aufbewahrungsdauer zu speichern. Aufbewahrungspflichten und Aufbewahrungsdauer können sich auch aus der slowakischen Gesetzgebung ergeben. Anschließend werden die entsprechenden Daten routinemäßig gelöscht.

Das Recht auf Übertragbarkeit der Daten. Als betroffene Person stellen wir Ihnen gerne die von ESET verarbeiteten personenbezogenen Daten im XLS-Format zur Verfügung.

Recht auf Beschwerde: Betroffene Personen haben das Recht, jederzeit Beschwerde bei einer Aufsichtsbehörde einzulegen. ESET unterliegt slowakischem Recht und ist als Teil der Europäischen Union an die Datenschutzgesetze gebunden. Die zuständige Aufsichtsbehörde ist das Büro für den Schutz personenbezogener Daten der Slowakischen Republik mit Sitz in Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Verarbeitung personenbezogener Daten

Die von ESET angebotenen und in unserem Produkt implementierten Dienste werden gemäß den Bestimmungen der [Endbenutzer-Lizenzvereinbarung](#) angeboten, bedürfen jedoch mitunter zusätzlicher Maßnahmen. Wir möchten Ihnen weitere Details zur Datensammlung im Zusammenhang mit der Bereitstellung unserer Dienste liefern. Wir bieten verschiedene in der EULA und der [Dokumentation](#). Für die Erbringung dieser Dienste erfassen wir die folgenden Informationen:

Lizenzierungs- und Abrechnungsdaten: Der Name, die E-Mail-Adresse, der Lizenzschlüssel und ggf. die Adresse, die Mitgliedschaft in der Firma und die Zahlungsdaten werden von ESET erfasst und verarbeitet, um die Aktivierung der Lizenz, die Zustellung von Lizenzschlüsseln, Erinnerungen bei Ablauf, Supportanfragen, die Überprüfung der Echtheit der Lizenz, die Bereitstellung unserer Dienste sowie die Zustellung sonstiger Benachrichtigungen einschließlich Marketingnachrichten nach geltendem Gesetz oder gemäß Ihrer Zustimmung zu ermöglichen. ESET ist gesetzlich verpflichtet, die Abrechnungsdaten zehn Jahre lang aufzubewahren. Die Lizenzinformationen hingegen werden spätestens zwölf Monate nach Ablauf der Lizenz anonymisiert.

Update- und andere Statistiken: Zu den Informationen, die verarbeitet werden, gehören Informationen zu Installationsprozess und Computer, z. B. die Plattform, auf der unser Produkt installiert wird, sowie Informationen zum Betrieb und Funktionsumfang der Produkte, darunter Betriebssystem, Hardwareinformationen, Installations- und Lizenz-IDs, IP-Adresse, MAC-Adresse und Konfigurationseinstellungen des Produkts. Zweck der Verarbeitung dieser Informationen sind die Bereitstellung von Update- und Upgrade-Diensten, Wartung, Sicherheit und Verbesserung unserer Back-End-Struktur.

Technischer Support. Kontaktinformationen und andere Daten aus Ihren Supportanfragen werden unter Umständen für Supportleistungen benötigt. Je nachdem, über welchen Kanal Sie uns kontaktieren, speichern wir möglicherweise Ihre E-Mail-Adresse, Telefonnummer, Lizenzinformationen, Produktdetails und eine Beschreibung Ihres Supportfalls. Unter Umständen werden Sie nach weiteren Informationen gefragt, um die Erbringung der Supportleistung zu erleichtern. Die im Rahmen des technischen Supports verarbeiteten Daten werden vier Jahre lang aufbewahrt.

Hinweis: Ist die Person, die unsere Produkte und Dienste in Anspruch nimmt, nicht mit dem Endbenutzer identisch, der das Produkt oder den Dienst erworben und die EULA mit uns geschlossen hat (beispielsweise ein Mitarbeiter des Endbenutzers, ein Familienmitglied oder eine vom Endbenutzer bevollmächtigte und im Einklang

mit der EULA anderweitig zur Nutzung des Produkts oder Dienstes berechtigte Person), so erfolgt die Datenverarbeitung im legitimen Interesse von ESET gemäß Auslegung von Art. 6 (1) (f) der DSGVO, damit der vom Endbenutzer bevollmächtigte Benutzer die von uns bereitgestellten Produkte und Dienste im Einklang mit der EULA verwenden kann.

Kontaktinformationen

Falls Sie Ihre Rechte als betroffene Person in Anspruch nehmen möchten oder Fragen oder Bedenken haben, schicken Sie uns eine Nachricht an:

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

Endbenutzer-Lizenzvereinbarung

Gültig ab dem 19. Oktober 2021.

WICHTIG: Vor dem Herunterladen, Installieren, Kopieren oder Verwenden des Produkts lesen Sie bitte die folgenden Nutzungsbedingungen. **DURCH DAS HERUNTERLADEN, INSTALLIEREN, KOPIEREN ODER VERWENDEN DER SOFTWARE ERKLÄREN SIE SICH MIT DEN NUTZUNGSBEDINGUNGEN EINVERSTANDEN UND ERKENNEN DIE [DATENSCHUTZERKLÄRUNG AN.](#)**

Endbenutzer-Lizenzvereinbarung

Diese Endbenutzer-Lizenzvereinbarung (die "Vereinbarung") zwischen ESET, spol. s r. o., mit Sitz in Einsteinova 24, 85101 Bratislava, Slovak Republic, Handelsregistereintrag 3586/B in der Rubrik Sro beim Amtsgericht Bratislava I, Firmennummer 31333532, ("ESET" oder "Anbieter") und Ihnen, einer natürlichen oder juristischen Person ("Sie" oder der "Endbenutzer"), berechtigt Sie zur Nutzung der in Abschnitt 1 dieser Vereinbarung definierten Software. Die in Abschnitt 1 dieser Vereinbarung definierte Software darf unter den im Folgenden aufgeführten Bedingungen auf einem Datenträger gespeichert, per E-Mail versendet, aus dem Internet oder von Servern des Anbieters heruntergeladen oder auf andere Weise beschafft werden.

DIESES DOKUMENT IST KEIN KAUFVERTRAG, SONDERN EINE VEREINBARUNG ÜBER DIE RECHTE DES ENDBENUTZERS. Der Anbieter bleibt Eigentümer des Exemplars der Software und, soweit vorhanden, des physischen Mediums, auf dem die Software für den Verkauf vorliegt, sowie aller Kopien der Software, zu deren Erstellung der Endbenutzer unter den Bedingungen dieser Vereinbarung berechtigt ist.

Durch Klicken auf die Schaltfläche „Ich stimme zu“ oder „Ich stimme zu...“ beim Installieren, Herunterladen, Kopieren oder Verwenden der Software erklären Sie sich mit den Bestimmungen und Bedingungen dieser Vereinbarung einverstanden und akzeptieren die Datenschutzerklärung. Wenn Sie mit einer der Bestimmungen dieser Vereinbarung und/oder der Datenschutzerklärung nicht einverstanden sind, klicken Sie auf die Schaltfläche „Ablehnen“ oder „Ich stimme nicht zu“. Brechen Sie den Download oder die Installation der Software ab, vernichten oder geben Sie die Software, das Installationsmedium, die zugehörige Dokumentation und den Erwerbsnachweis an den Anbieter oder an dem Ort, an dem Sie die Software erworben haben, zurück.

MIT DER NUTZUNG DER SOFTWARE ZEIGEN SIE AN, DASS SIE DIESE VEREINBARUNG GELESEN UND VERSTANDEN HABEN UND DASS SIE DIESER VEREINBARUNG ZUGESTIMMT HABEN.

1. Software. Mit "Software" wird in dieser Vereinbarung bezeichnet: (i) das mit dieser Vereinbarung ausgelieferte Computerprogramm und all dessen Komponenten; (ii) alle Inhalte der Disks, CD-ROMs, DVDs, E-Mails und Anlagen oder sonstiger Medien, denen diese Vereinbarung beigelegt ist, einschließlich der Objektcodeform der Software, die auf einem Datenträger, in einer E-Mail oder durch Herunterladen im Internet bereitgestellt wurde; (iii) alle verwandten erklärenden Schriftdokumente und andere Dokumentationen in Bezug auf die Software, insbesondere Beschreibungen der Software und ihrer Spezifikationen, jede Beschreibung der Softwareeigenschaften oder -funktionen, Beschreibungen der Betriebsumgebung, in der die Software verwendet wird, Anweisungen zu Installation und zum Einsatz der Software ("Dokumentation"); (iv) Kopien der Software, Patches für mögliche Softwarefehler, Hinzufügungen zur Software, Erweiterungen der Software, geänderte Versionen und Aktualisierungen der Softwarebestandteile, sofern zutreffend, deren Nutzung der Anbieter gemäß Artikel 3 dieser Vereinbarung gewährt. Die Software wird ausschließlich in Form von ausführbarem Objektcode ausgeliefert.

2. Installation, Computer und ein Lizenzschlüssel. Die auf einem Datenträger bereitgestellte, per E-Mail verschickte, aus dem Internet oder von den Servern des Anbieters heruntergeladene oder auf anderem Weg beschaffte Software muss installiert werden. Sie müssen die Software auf einem korrekt konfigurierten Computer installieren, der die in der Dokumentation genannten Mindestvoraussetzungen erfüllt. Die Installationsmethode ist in der Dokumentation beschrieben. Auf dem Computer, auf dem Sie die Software installieren, darf kein Computerprogramm und keine Hardware vorhanden sein, die sich negativ auf die Software auswirken könnte. Die Bezeichnung "Computer" erstreckt sich auf Hardware inklusive, jedoch nicht ausschließlich, Personal Computer, Laptops, Arbeitsstationen, Palmtop-Computer, Smartphones, tragbare elektronische Geräte oder andere elektronische Geräte, für die die Software entwickelt wurde und auf denen die Software installiert und/oder eingesetzt wird. Der Begriff "Lizenzschlüssel" bezeichnet die eindeutige Abfolge von Symbolen, Buchstaben und Zahlen, die dem Endbenutzer bereitgestellt wird, um die legale Nutzung der Software in der jeweiligen Version bzw. die Verlängerung der Lizenz gemäß dieser Vereinbarung zu ermöglichen.

3. Lizenz. Unter der Voraussetzung, dass Sie sich mit dieser Vereinbarung einverstanden erklärt haben und sämtliche darin enthaltenen Bestimmungen einhalten, gewährt Ihnen der Anbieter die folgenden Rechte (die "Lizenz"):

a) Installation und Nutzung. Sie erhalten das nicht exklusive und nicht übertragbare Recht, die Software auf der Festplatte eines Computers oder einem ähnlichen Medium zur dauerhaften Datenspeicherung zu installieren, die Software im Arbeitsspeicher eines Computers zu speichern und die Software auf Computern zu implementieren, zu speichern und anzuzeigen.

b) Anzahl der Lizenzen. Das Nutzungsrecht für die Software ist durch die Anzahl der Endbenutzer beschränkt. Unter einem „Endbenutzer“ ist Folgendes zu verstehen: (i) die Installation der Software auf einem Computer; oder (ii) wenn sich der Umfang einer Lizenz nach der Anzahl von Postfächern richtet, ist ein Endbenutzer ein Computerbenutzer, der E-Mails über ein E-Mail-Programm empfängt. Wenn das E-Mail-Programm E-Mail empfängt und diese anschließend automatisch an mehrere Benutzer weiterleitet, richtet sich die Anzahl der Endbenutzer nach der tatsächlichen Anzahl von Benutzern, an die auf diesem Weg E-Mail-Nachrichten gesendet werden. Wenn ein Mailserver die Funktion eines E-Mail-Gateways ausführt, entspricht die Zahl der Endbenutzer der Anzahl von Mailservern, für die dieses Gateway Dienste bereitstellt. Wenn mehrere E-Mail-Adressen (z. B. durch Aliasnamen) von einem Benutzer verwendet werden und nur ein Benutzer über diese Adressen E-Mail empfängt, während auf Clientseite keine E-Mail-Nachrichten automatisch an mehrere Benutzer verteilt werden, ist nur eine Lizenz für einen Computer erforderlich. Die gleichzeitige Nutzung derselben Lizenz auf mehreren Computern ist untersagt. Der Endbenutzer darf den Lizenzschlüssel für die Software nur in dem Umfang eingeben, für den er die entsprechende Anzahl von Lizenzen zur Nutzung der Software vom Anbieter erworben hat. Der Lizenzschlüssel ist vertraulich, und die Lizenz darf nicht mit Drittparteien geteilt oder von Drittparteien genutzt werden, sofern dies nicht in dieser Vereinbarung oder vom Anbieter erlaubt wurde. Benachrichtigen Sie den Anbieter unverzüglich, falls Ihr Lizenzschlüssel kompromittiert wurde.

c) **Home/Business Edition.** Die Home Edition der Software darf ausschließlich in privaten und/oder nichtkommerziellen Umgebungen für den Haus- und Familiengebrauch eingesetzt werden. Für die Verwendung der Software in kommerziellen Umgebungen sowie auf E-Mail-Servern, E-Mail-Relays, E-Mail- oder Internet-Gateways ist die Business Edition der Software erforderlich.

d) **Laufzeit der Lizenz.** Ihr Nutzungsrecht für die Software ist zeitlich beschränkt.

e) **OEM-Software.** Als „OEM“ klassifizierte Software darf ausschließlich auf dem Computer genutzt werden, mit dem sie ausgeliefert wurde. Eine Übertragung auf einen anderen Computer ist nicht gestattet.

f) **Nicht für den Wiederverkauf bestimmte Software und Testversionen.** Nicht für den Wiederverkauf („not for resale“, NFR) oder als Testversion bereitgestellte Software darf nicht veräußert, sondern ausschließlich zum Vorführen oder Testen der Softwarefunktionen verwendet werden.

g) **Ablauf und Kündigung der Lizenz.** Die Lizenz läuft automatisch zum Ende des jeweiligen Lizenzzeitraums aus. Sollten Sie eine Ihrer Pflichten aus dieser Vereinbarung verletzen, ist der Anbieter berechtigt, diese außerordentlich zu kündigen und, ggf. auf dem Rechtsweg, etwaige weitere Ansprüche geltend zu machen. Bei Ablauf oder Kündigung der Lizenz müssen Sie die Software und ggf. alle Sicherungskopien sofort löschen, zerstören oder auf eigene Kosten an ESET oder das Geschäft zurückgeben, in dem Sie die Software erworben haben. Nach Ablauf oder Kündigung der Lizenz ist der Anbieter berechtigt, das Recht des Endbenutzers zur Nutzung der Softwarefunktionen zurückzuziehen, für die eine Verbindung zu Servern des Anbieters oder zu Servern von Drittanbietern erforderlich ist.

4. Funktionen mit Datenerfassung und Anforderungen an die Internetverbindung. Für den korrekten Betrieb benötigt die Software eine Internetverbindung und muss in der Lage sein, sich in regelmäßigen Abständen mit den Servern des Anbieters, Servern einer Drittpartei und entsprechenden Datenerfassungen gemäß der Datenschutzrichtlinie zu verbinden. Eine Internetverbindung und die entsprechende Datenerfassung ist für den Betrieb der Software sowie für deren Updates und Upgrades erforderlich. Der Anbieter hat das Recht, Aktualisierungen für die Software („Updates“) oder Upgrades bereitzustellen, ist dazu jedoch nicht verpflichtet. Diese Funktion ist in den Standardeinstellungen der Software aktiviert. Die Updates werden also automatisch installiert, sofern der Endbenutzer dies nicht deaktiviert hat. Zur Bereitstellung von Aktualisierungen muss die Echtheit der Lizenz überprüft werden. Dazu gehören Informationen über den Computer und/oder die Plattform, auf der die Software installiert wurde, in Übereinstimmung mit der Datenschutzerklärung.

Die Bereitstellung von Updates unterliegt möglicherweise der End-of-Life-Richtlinie („EOL-Richtlinie“), die auf https://go.eset.com/eol_business verfügbar ist. Nachdem die Software oder eine ihrer Funktionen das in der EOL-Policy festgelegte End-of-Life-Datum erreicht hat, werden keine Aktualisierungen mehr bereitgestellt.

Für die in dieser Vereinbarung festgelegten Zwecke werden Daten gesammelt, verarbeitet und gespeichert, mit denen der Anbieter Sie gemäß der Datenschutzrichtlinie identifizieren kann. Für die in dieser Vereinbarung festgelegten Zwecke werden Daten gesammelt, verarbeitet und gespeichert, mit denen der Anbieter Sie gemäß der Datenschutzrichtlinie identifizieren kann. Sie stimmen zu, dass der Anbieter mit eigenen Mitteln überprüfen darf, ob Sie die Software in Übereinstimmung mit den Bestimmungen dieser Vereinbarung nutzen. Sie erkennen an, dass es für die in dieser Vereinbarung festgelegten Zwecke erforderlich ist, dass Ihre Daten zwischen der Software und den Computersystemen des Anbieters bzw. denen seiner Geschäftspartner im Rahmen des Distributions- und Verteilungsnetzwerks des Anbieters übertragen werden, um die Funktionstüchtigkeit der Software und die Genehmigung zu deren Nutzung sowie die Rechte des Anbieters zu schützen.

Mit Abschluss dieser Vereinbarung willigen Sie zudem in die Übertragung, Verarbeitung und Speicherung Ihrer personenbezogenen Daten durch den Anbieter bzw. seine Geschäftspartner ein, soweit eine solche Nutzung zur Abrechnung und zur Erfüllung dieser Vereinbarung und zum Übertragen von Benachrichtigungen auf Ihren Computer erforderlich ist.

Details zur Privatsphäre, zum Schutz persönlicher Daten und zu Ihren Rechten als betroffene Person finden Sie in der Datenschutzrichtlinie auf der Webseite des Anbieters oder direkt beim Installationsprozess. Sie finden diese Informationen außerdem im Hilfebereich der Software.

5. Ausübung der Rechte des Endbenutzers. Sie müssen Ihre Rechte als Endbenutzer selbst oder gegebenenfalls über Ihre Angestellten ausüben. Sie dürfen die Software ausschließlich zur Gewährleistung der Arbeitsfähigkeit und zum Schutz der Computer verwenden, für die Sie eine Lizenz erworben haben.

6. Beschränkungen der Rechte. Es ist untersagt, die Software zu kopieren, zu verbreiten oder aufzuteilen. Außerdem dürfen keine abgeleiteten Versionen erstellt werden. Für die Nutzung der Software gelten die folgenden Einschränkungen:

a) Sie dürfen eine Kopie der Software auf einem Medium zur dauerhaften Speicherung als Sicherungskopie erstellen, vorausgesetzt die Sicherungskopien werden nicht auf einem anderen Computer installiert oder verwendet. Das Erstellen jeder weiteren Kopie der Software verstößt gegen diese Vereinbarung.

b) Jegliche von den Bestimmungen dieser Vereinbarung abweichende Nutzung, Modifikation, Übersetzung oder Reproduktion der Software sowie die Einräumung von Rechten zur Nutzung der Software oder von Kopien der Software ist untersagt.

c) Die Software darf nicht an andere Personen verkauft, sublizenziert oder vermietet werden. Ebenso darf die Software nicht von einer anderen Person gemietet, einer anderen Person ausgeliehen oder zur gewerbsmäßigen Erbringung von Dienstleistungen verwendet werden.

d) Der Quellcode der Software darf nicht durch Reverse-Engineering analysiert, dekompiert oder disassembliert oder auf andere Weise beschafft werden, soweit eine solche Beschränkung nicht ausdrücklich gesetzlichen Bestimmungen widerspricht.

e) Sie verpflichten sich, die Software nur in Übereinstimmung mit allen am Verwendungsort geltenden gesetzlichen Bestimmungen zu verwenden, insbesondere gemäß den Beschränkungen, die sich aus dem Urheberrecht und anderen Rechten an geistigem Eigentum ergeben.

f) Sie verpflichten sich, die Software und ihre Funktionen nur so zu nutzen, dass der Zugriff anderer Endbenutzer auf die betreffenden Dienste nicht eingeschränkt wird. Der Anbieter behält sich das Recht vor, den Leistungsumfang gegenüber einzelnen Endbenutzern einzuschränken, damit die Dienste von möglichst vielen Endbenutzern verwendet werden können. Dies kann auch bedeuten, dass die Nutzung beliebiger Softwarefunktionen vollständig gesperrt wird und dass Daten sowie Informationen im Zusammenhang mit bestimmten Funktionen der Software von den Servern des Anbieters bzw. Dritter gelöscht werden.

g) Sie verpflichten sich hiermit, keine Aktivitäten im Zusammenhang mit dem Lizenzschlüssel auszuführen, die den Bestimmungen dieser Vereinbarung widersprechen oder die dazu führen, dass der Lizenzschlüssel an unbefugte Personen weitergegeben wird, z. B. durch die Übertragung von benutzten oder nicht benutzten Lizenzschlüsseln in jeglicher Form oder die nicht autorisierte Verteilung von duplizierten oder generierten Lizenzschlüsseln oder die Nutzung der Software im Zusammenhang mit einem Lizenzschlüssel, der aus einer anderen Quelle als direkt vom Anbieter beschafft wurde.

7. Urheberrecht. Die Software und alle Rechte einschließlich des Rechtstitels und der geistigen Eigentumsrechte daran sind Eigentum von ESET und/oder seiner Lizenzgeber. Sie unterliegen dem Schutz der Bestimmungen internationaler Abkommen und aller sonstigen geltenden Gesetze des Landes, in dem die Software verwendet wird. Die Struktur, die Aufteilung und der Code der Software sind Geschäftsgeheimnisse und vertrauliche Informationen von ESET und/oder seiner Lizenzgeber. Die Software darf nicht kopiert werden, wobei lediglich die in Abschnitt 6(a) angegebene Ausnahme gilt. Alle gemäß dieser Vereinbarung zulässigen Kopien müssen dieselben Urheberrechts- und Eigentümerhinweise wie die ursprüngliche Software enthalten. Wenn Sie in Verstoß gegen

die Bestimmungen dieser Vereinbarung Quellcode durch Reverse-Engineering analysieren, dekompileieren oder disassemblieren oder versuchen, sich den Quellcode auf andere Weise zu beschaffen, gehen automatisch sämtliche dadurch gewonnenen Informationen unwiderruflich und unmittelbar in das Eigentum des Anbieters über. Weiterhin ist der Anbieter in diesem Fall berechtigt, etwaige weitere Ansprüche aus Ihrem Verstoß gegen diese Vereinbarung geltend zu machen.

8. Rechteevorbehalt. Mit Ausnahme der Rechte, die Ihnen als Endbenutzer der Software in dieser Vereinbarung ausdrücklich gewährt werden, behält sich der Anbieter alle Rechte an der Software vor.

9. Versionen in verschiedenen Sprachen/auf mehreren Datenträgern, mehrere Exemplare. Wenn die Software mehrere Plattformen oder Sprachen unterstützt, oder wenn Sie mehrere Exemplare der Software erhalten haben, darf die Software nur auf derjenigen Anzahl von Computern und nur in den Versionen verwendet werden, für die Sie eine Lizenz erworben haben. Es dürfen keine Versionen oder Kopien der Software, die von Ihnen nicht verwendet werden, an andere Personen verkauft, vermietet, sublizenziert, verliehen oder auf diese übertragen werden.

10. Beginn und Gültigkeitsdauer der Vereinbarung. Diese Vereinbarung tritt an dem Tag in Kraft, an dem Sie sich mit ihren Bestimmungen einverstanden erklären. Sie können diese Vereinbarung jederzeit kündigen, indem Sie die Software, alle Sicherungskopien und, falls vorhanden, alle vom Anbieter oder seinen Geschäftspartnern zur Verfügung gestellten zugehörigen Materialien dauerhaft löschen, sie zerstören bzw. auf eigene Kosten zurückgeben. Ihr Recht zur Nutzung der Software und deren Funktionen unterliegt möglicherweise einer EOL-Richtlinie. Wenn die Software oder deren Funktionen das in der EOL-Richtlinie definierte Ende des Lebenszyklus erreichen, erlischt Ihr Nutzungsrecht für die Software. Unabhängig von der Gültigkeitsdauer dieser Vereinbarung und der Art und Weise ihres Ablaufs bzw. ihrer Kündigung behalten die Bestimmungen der Abschnitte 7, 8, 11, 13, 19 und 21 auf unbegrenzte Zeit ihre Gültigkeit.

11. AUSDRÜCKLICHE ERKLÄRUNGEN DES ENDBENUTZERS. ALS ENDBENUTZER ERKENNEN SIE AN, DASS DIE SOFTWARE IM JEWEILIGEN IST-ZUSTAND UND OHNE JEDWEGE AUSDRÜCKLICHE ODER KONKLUDENTE GEWÄHRLEISTUNG BEREITGESTELLT WIRD, SOWEIT DIES IM RAHMEN DER GELTENDEN GESETZE ZULÄSSIG IST. WEDER DER ANBIETER NOCH SEINE LIZENZGEBER ODER DIE RECHTEINHABER GEWÄHREN AUSDRÜCKLICHE ODER KONKLUDENTE ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN, INSBESONDERE KEINE ZUSICHERUNGEN HINSICHTLICH DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER DER NICHTVERLETZUNG VON PATENTEN, URHEBER- UND MARKENRECHTEN ODER SONSTIGEN RECHTEN DRITTER. ES BESTEHT VON SEITEN DES ANBIETERS ODER DRITTER KEINERLEI GEWÄHRLEISTUNG, DASS DIE IN DER SOFTWARE ENTHALTENEN FUNKTIONEN IHREN ANFORDERUNGEN ENTSPRECHEN ODER DASS DIE SOFTWARE STÖRUNGS- UND FEHLERFREI AUSGEFÜHRT WIRD. SIE ÜBERNEHMEN DIE VOLLE VERANTWORTUNG UND DAS VOLLE RISIKO HINSICHTLICH DER AUSWAHL DER SOFTWARE ZUM ERREICHEN DER VON IHNEN BEABSICHTIGTEN ERGEBNISSE SOWIE FÜR INSTALLATION UND NUTZUNG DER SOFTWARE UND DEN MIT DIESER ERZIELTEN ERGEBNISSEN.

12. Keine weiteren Verpflichtungen. Aus dieser Vereinbarung ergeben sich für den Anbieter und seine Lizenzgeber keine weiteren Verpflichtungen außer den explizit aufgeführten.

13. HAFTUNGSAUSSCHLUSS. SOWEIT IM RAHMEN DER GELTENDEN GESETZE ZULÄSSIG, ÜBERNEHMEN DER ANBIETER, SEINE ANGESTELLTEN UND SEINE LIZENZGEBER KEINERLEI HAFTUNG FÜR ENTGANGENE GEWINNE, ERTRÄGE ODER VERKÄUFE. VON DER HAFTUNG AUSGESCHLOSSEN SIND AUSSERDEM DATENVERLUSTE, BESCHAFFUNGSKOSTEN FÜR ERSATZTEILE ODER DIENSTE, SACH- UND PERSONENSCHÄDEN, GESCHÄFTSUNTERBRECHUNGEN, DER VERLUST VON GESCHÄFTSINFORMATIONEN SOWIE JEDWEGE ANDERE NEBEN-, VERMÖGENS- ODER FOLGESCHÄDEN, DIE INFOLGE DER INSTALLATION, NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DER SOFTWARE ENTSTEHEN. DA IN BESTIMMTEN LÄNDERN UND UNTER BESTIMMTEN GESETZEN EIN HAFTUNGSAUSSCHLUSS NICHT ZULÄSSIG IST, EINE HAFTUNGSBESCHRÄNKUNG JEDOCH MÖGLICH, BESCHRÄNKT SICH DIE HAFTUNG DES ANBIETERS, SEINER ANGESTELLTEN UND LIZENZGEBER AUF DEN FÜR DIE LIZENZ ENTRICHTETEN PREIS.

14. Gesetzlich verankerte Verbraucherrechte haben im Konfliktfall Vorrang vor den Bestimmungen dieser Vereinbarung.

15. **Technischer Support.** ESET bzw. die von ESET beauftragten Dritten erbringen jeglichen technischen Support ausschließlich nach eigenem Ermessen und ohne diesbezügliche Zusicherungen oder Gewährleistungen. Nachdem die Software oder eine ihrer Funktionen das in der EOL-Policy festgelegte End-of-Life-Datum erreicht hat, wird kein technischer Support mehr bereitgestellt. Endbenutzer sind verpflichtet, vor der Inanspruchnahme von Supportleistungen eine Sicherungskopie aller vorhandenen Daten, Softwareanwendungen und sonstigen Programme zu erstellen. ESET bzw. die von ESET beauftragten Dritten übernehmen keinerlei Haftung für Datenverluste, Sach- und Vermögensschäden (insb. Schäden an Software und Hardware) oder entgangene Gewinne infolge der Erbringung von Supportleistungen. ESET bzw. die von ESET beauftragten Dritten sichern nicht zu, dass ein bestimmtes Problem auf dem Wege des technischen Support gelöst werden kann, und behalten sich das Recht vor, die Arbeit an einem Problem ggf. einzustellen. ESET behält sich das Recht vor, die Erbringung von Supportleistungen nach eigenem Ermessen vorübergehend auszusetzen, ganz einzustellen oder im konkreten Einzelfall abzulehnen. Für die Bereitstellung des technischen Supports sind unter Umständen Lizenzinformationen, Informationen und andere Daten gemäß der Datenschutzrichtlinie erforderlich.

16. **Übertragung der Lizenz.** Die Software darf von einem Computersystem auf ein anderes übertragen werden, sofern dabei nicht gegen Bestimmungen dieser Vereinbarung verstoßen wird. Sofern in dieser Vereinbarung nicht anderweitig geregelt, ist es dem Endbenutzer gestattet, die Lizenz und alle Rechte aus dieser Vereinbarung an einen anderen Endbenutzer zu übertragen, sofern der Anbieter dem zustimmt und die folgenden Voraussetzungen beachtet werden: (i) Der ursprüngliche Endbenutzer darf keine Kopien der Software zurückbehalten. (ii) Die Übertragung der Rechte muss direkt erfolgen, d. h. vom ursprünglichen Endbenutzer an den neuen Endbenutzer. (iii) Der neue Endbenutzer muss sämtliche Rechte und Pflichten des ursprünglichen Endbenutzers aus dieser Vereinbarung übernehmen. (iv) Der ursprüngliche Endbenutzer muss dem neuen Endbenutzer einen der in Abschnitt 17 genannten Nachweise für die Gültigkeit des Softwarelizenz übereignen.

17. **Gültigkeitsnachweis für die Softwarelizenz.** Der Endbenutzer kann seine Nutzungsrechte an der Software auf eine der folgenden Arten nachweisen: (i) über ein Lizenzzertifikat, das vom Anbieter oder einem von diesem beauftragten Dritten ausgestellt wurde; (ii) über eine schriftliche Lizenzvereinbarung, falls abgeschlossen; (iii) durch Vorlage einer E-Mail des Anbieters mit den Lizenzdaten (Benutzername und Passwort). Zur Überprüfung der Echtheit der Software sind unter Umständen Lizenzinformationen und Identifikationsdaten des Endbenutzers gemäß der Datenschutzrichtlinie erforderlich.

18. **Lizenzvergabe an Behörden und die US-Regierung.** Für die Lizenzvergabe an Behörden, insbesondere an Stellen der US-Regierung, gelten ausschließlich die in dieser Vereinbarung beschriebenen Lizenzrechte und Einschränkungen.

19. **Einhaltung von Handelskontrollen.**

(a) Sie werden die Software nicht direkt oder indirekt an andere Personen exportieren, reexportieren, übertragen oder auf andere Arten verfügbar machen, auf eine Art verwenden oder sich an Handlungen beteiligen, die zu einer Verletzung der Handelskontrollgesetze durch oder zu sonstigen negativen Folgen für ESET oder eines der übergeordneten Unternehmen, die Tochtergesellschaften von ESET oder die Tochtergesellschaften der übergeordneten Unternehmen sowie die Entitäten unter der Kontrolle der übergeordneten Unternehmen („angeschlossene Unternehmen“) führen könnten. Zu diesen Handelskontrollgesetzen zählen:

i. alle Gesetze, die Lizenzierungsanforderungen zum Export, Reexport oder zur Übertragung von Waren, Software, Technologie oder Dienstleistungen kontrollieren, einschränken oder auferlegen und die von Regierungen, Bundesstaaten/Bundesländern oder Regulierungsbehörden in den USA, in Singapur, in Großbritannien, der Europäischen Union oder ihren Mitgliedsstaaten oder in anderen Ländern eingeführt oder übernommen wurden, in denen die Verpflichtungen der Vereinbarung gelten, oder in denen ESET oder eines der angeschlossenen

Unternehmen sesshaft oder tätig ist

ii. alle sonstigen wirtschaftlichen, finanziellen oder handelsbezogenen Sanktionen, Einschränkungen, Embargos, Import- oder Exportbeschränkungen, Verbote von Vermögens- oder Assetübertragungen oder von Dienstleistungen sowie alle gleichwertigen Maßnahmen, die von Regierungen, Bundesstaaten/Bundesländern oder Regulierungsbehörden in den USA, in Singapur, in Großbritannien, der Europäischen Union oder ihren Mitgliedsstaaten oder in anderen Ländern eingeführt oder übernommen wurden, in denen die Verpflichtungen der Vereinbarung gelten, oder in denen ESET oder eines der angeschlossenen Unternehmen sesshaft oder tätig ist.

(die in den Punkten i und ii genannten Gesetze zusammengefasst als „Handelskontrollgesetze“).

b) ESET behält sich das Recht vor, die eigenen Verpflichtungen im Rahmen dieser Bestimmungen fristlos aufzuheben oder die Bestimmungen fristlos aufzukündigen, falls Folgendes eintritt:

i. ESET hat nach eigenem Ermessen festgestellt, dass ein Benutzer die Bestimmungen in Artikel 19 a) dieser Vereinbarung verletzt hat oder vermutlich verletzen wird; oder

ii. ein Endbenutzer und/oder die Software fällt unter die Handelskontrollgesetze, und ESET ist nach eigenem Ermessen der Ansicht, dass die weitere Erfüllung der Verpflichtungen aus der Vereinbarung dazu führen könnte, dass ESET oder ein angeschlossenes Unternehmen die Handelskontrollgesetze verletzt oder dass sonstige negative Folgen zu erwarten sind.

c) Die Vereinbarung ist nicht darauf ausgelegt und darf nicht so interpretiert oder ausgelegt werden, dass eine der Parteien dazu aufgefordert oder verpflichtet wird, auf irgendeine Weise zu handeln oder Handlungen zu unterlassen (oder Handlungen bzw. deren Unterlassung zuzustimmen), die geltende Handelskontrollgesetze verletzt oder gemäß dieser Gesetze unter Strafe steht oder verboten ist.

20. Kündigungen. Alle Kündigungen sowie zurückgegebene Software und Dokumentation sind an folgende Adresse zu senden: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic. ESET behält sich das Recht vor, Sie über alle Änderungen an dieser Vereinbarung, der Datenschutzerklärung, der EOL-Richtlinie und der Dokumentation gemäß Art. 22 der Vereinbarung zu informieren. ESET kann Ihnen E-Mails oder In-App-Benachrichtigungen über die Software schicken oder die Kommunikation auf unserer Website veröffentlichen. Sie stimmen zu, rechtliche Mitteilungen von ESET in elektronischer Form zu erhalten, inklusive Mitteilungen zu Änderungen an Bedingungen, Sonderbedingungen oder Datenschutzerklärungen, Benachrichtigungen oder Einladungen zu Vertragsverlängerungen, Kündigungen oder andere rechtliche Mitteilungen. Diese elektronische Kommunikation gilt als schriftlich empfangen, sofern nicht durch geltendes Recht eine andere Kommunikationsform vorgeschrieben ist.

21. Geltendes Recht, Gerichtsstand. Diese Vereinbarung unterliegt slowakischem Recht. Endbenutzer und Anbieter vereinbaren, dass gesetzliche Bestimmungen zur Konfliktlösung und UN-Kaufrecht nicht zur Anwendung kommen. Sie erklären sich ausdrücklich damit einverstanden, dass als Gerichtsstand für alle Streitfälle mit dem Anbieter oder bezüglich Ihrer Verwendung der Software das Amtsgericht Bratislava I, Slowakische Republik vereinbart wird.

22. Allgemeine Bestimmungen. Wenn eine der Bestimmungen dieser Vereinbarung ungültig oder uneinklagbar ist, beeinträchtigt dies nicht die Gültigkeit der übrigen Bestimmungen der Vereinbarung. Diese bleiben unter den hier festgelegten Bedingungen gültig und einklagbar. Diese Vereinbarung wird auf Englisch getroffen. Falls eine Übersetzung der Vereinbarung aus Gründen der Annehmlichkeit bereitgestellt wird, sind die Bestimmungen der englischen Version maßgeblich, falls Abweichungen bestehen.

ESET behält sich das Recht vor, Änderungen an der Software vorzunehmen und die Bestimmungen dieser Vereinbarung, deren Anhänge und Ergänzungen, die Datenschutzerklärung, die EOL-Richtlinie und die

Dokumentation ganz oder in Teilen jederzeit zu ändern, indem das entsprechende Dokument aktualisiert wird, (i) um Änderungen an der Software oder der Funktionsweise von ESET zu berücksichtigen, (ii) aus rechtlichen, regulatorischen oder Sicherheitsgründen oder (iii) um Missbrauch oder Schaden zu verhindern. Bei Änderungen an dieser Vereinbarung werden Sie per E-Mail, per In-App-Benachrichtigung oder über andere elektronische Kommunikationsformen informiert. Wenn Sie den Änderungen der Vereinbarung nicht zustimmen, können Sie diese gemäß Artikel 10 innerhalb von 30 Tagen nach Erhalt der Änderungsbenachrichtigung kündigen. Sofern Sie die Vereinbarung nicht innerhalb dieser Frist kündigen, gelten die Änderungen als von Ihnen akzeptiert und wirksam ab dem Tag, an dem Sie die Änderungsbenachrichtigung erhalten haben.

Dies ist die vollständige Vereinbarung zwischen dem Anbieter und Ihnen in Bezug auf die Software. Sie ersetzt alle vorigen Darstellungen, Diskussionen, Unternehmungen, Kommunikationen und Werbungen in Bezug auf die Software.

EULAID: EULA-PRODUCT; 3537.0