ESET Full Disk Encryption

Uživatelská příručka

Klikněte sem pro zobrazení online verze tohoto dokumentu

Digital Security
Progress. Protected.

Copyright ©2024 ESET, spol. s r.o.

ESET Full Disk Encryption byl vyvinut společností ESET, spol. s r.o.

Pro více informací navštivte https://www.eset.cz.

Všechna práva vyhrazena. Žádná část této publikace nesmí být reprodukována žádným prostředkem, ani distribuována jakýmkoliv způsobem bez předchozího písemného povolení společnosti ESET, spol. s r.o.

ESET, spol. s r.o. si vyhrazuje právo změny programových produktů popsaných v této publikaci bez předchozího upozornění.

Technická podpora: https://servis.eset.cz

REV. 2024-03-18

1 O této nápovědě 1
2 Seznam změn 1
3 Představení produktu 2
3.1 Systémové požadavky 2
3.2 EFDE pro MAC 3
4 Zakoupení licence 3
5 Používání ESET Full Disk Encryption 4
6 Zapnutí a konfigurace ESET Full Disk Encryption 4
6.1 Možnosti šifrování 6
6.2 Politika hesla 7
6.3 Uživatelské rozhraní 9
6.4 Nástroje 9
6.5 Nasazení EFDE klienta 10
6.5 EFDE all-in-one instalační balíček 10
6.5 Klientská úloha pro instalaci EFDE 11
6.5 Průvodce zapnutím šifrování 12
6.6 Nasazení ESET Full Disk Encryption prostřednictvím příkazového řádku 14
6.6 Nasazení instalačního balíčku s předdefinovaným heslem 14
6.6 Zneplatnění hesla prostřednictvím příkazového řádku 15
6.6 Pozastavení/obnovení FDE autentifikace prostřednictvím příkazového řádku 16
6.6 Přidání/odebrání rozložení klávesnice prostřednictvím příkazového řádku 17
7 Proces šifrování na straně EFDE klienta 18
8 Správa šifrování 20
8.1 Pozastavit FDE autentifikaci 21
9 Pre-boot přihlašovací obrazovka 24
9.1 Zkratky pro použití na pre-boot obrazovce 25
10 Obnovení šifrování 26
10.1 Heslo pro obnovení 26
10.2 Data pro obnovení 29
11 Dešifrování/odinstalace 33
12 Nejčastější dotazy 35
13 Řešení problémů 36
14 Ochrana soukromí 38
15 Licenční ujednání s koncovým uživatelem 41

O této nápovědě

V této nápovědě vás seznámíme se správou a použitím ESET Full Disk Encryption. Detailně vám rovněž představíme komunikaci mezi ESET Full Disk Encryption a bezpečnostními produkty ESET.

Stránky nápovědy jsou pro lepší orientaci logicky uspořádány do jednotlivých kapitol a podkapitol. Související informace tak naleznete jednoduchým procházením této struktury stránek. Využít můžete rovněž vyhledávání v horší části stránky.

Primárním zdrojem této příručky je online nápověda. Aktuální verze příručky se otevře v případě, kdy jste připojeni k internetu.

- V Databázi znalostí naleznete odpovědi na nejčastější dotazy stejně jako doporučené řešení mnoha situací. Články pravidelně aktualizujeme a připravujeme návody na řešení aktuálních situací.

- ESET forum představuje jednoduchý způsob, jak ESET uživatelé mohou požádat o radu a pomoci ostatním. Můžete sem umístit váš problém nebo dotaz týkající se produktu ESET.

- Ohodnotit příručku a poskytnout nám zpětnou vazbu na konkrétní kapitolu můžete kliknutím na možnost **Byla pro vás tato informace užitečná?**

Zvláštní sdělení:

Poznámka poskytuje cenné informace k dané funkci nebo odkaz na související kapitoly.

Tato akce vyžaduje vaši pozornost a neměli byste ji ignorovat. Obvykle obsahuje nekritické, ale však důležité informace.

Kritická informace, které byste měli věnovat pozornost. Upozornění jsou umístěna tak, aby vás včas varovala a zároveň vám pomohla vyvarovat se chybám, které by mohly mít negativní následky. Prosím, důkladně si přečtěte text ohraničený tímto označením, protože se týká velmi citlivých systémových nastavení nebo upozorňuje na možná rizika.

Praktický příklad použití. Příklady používáme pro vysvětlení složitějších témat.

Seznam změn

ESET Full Disk Encryption pro Windows

ESET Full Disk Encryption pro macOS

Představení produktu

ESET Full Disk Encryption (EFDE) je doplňková funkce, kterou nativně disponují ESET konzole určené pro vzdálenou správu – ESET PROTECT On-Prem a ESET PROTECT. Hlavním účelem EFDE je zajištění full disk encryption na spravovaných pracovních stanicích s operačním systémem Windows a macOS tím, že přidává další bezpečnostní vrstvu v podobě pre-boot autentifikace. EFDE je plně kompatibilní s funkcemi (skupiny, politiky, úlohy a přehledy), které znáte z ESET PROTECT On-Prem a ESET PROTECT.

Systémové požadavky

Podporované OS ze strany aplikace EFDE klienta:

ESET Full Disk Encryption pro Windows	32-bit	64-bit
Windows 11	N/A	✔
Windows 10	✔	✔

ESET Full Disk Encryption pro macOS	Podporováno
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	✔

Neinstalujte aplikaci EFDE klienta na stejné zařízení, na kterém vám běží ESET PROTECT Server databáze.

Kompatibilita:

- Firmware staršího typu/BIOS není podporován. ESET Full Disk Encryption vyžaduje systém s rozhraním UEFI.
- ESET Full Disk Encryption nepodporuje disky ve formátu MBR. Podporovány jsou pouze disky se schématem oddílů GPT.
- ESET Full Disk Encryption podporuje Apple M1 Mac zařízení, pokud máte nainstalován emulátor Rosetta.
- ESET Full Disk Encryption nepodporuje Windows zařízení s ARM procesory.
- ESET Full Disk Encryption nepodporuje zařízení současné používající více operačních systémů (tzv. dual-boot) ani softwarový RAID.
- ESET Full Disk Encryption není kompatibilní s Apple Mac systémy využívající Apple Boot Camp.
- ESET Full Disk Encryption nepodporuje funkci Prostory úložiště společnosti Microsoft ani dynamické disky.
- Produkt na Windows Insider sestaveních používejte výhradně pro testování, může dojít ke ztrátě dat.
- Grafický čip s DirectX 9 a WDDM 1.0 ovladačem nebo novějším.

ESET Full Disk Encryption můžete použít v prostředí virtuálního počítače na následujících PC nebo Mac hypervisorech:

- VMware Workstation 16.2.3
- VMware ESXi 7.0 / vSphere 7.0.3.00300
- VMware Fusion 12.2.3
- Parallels
- Microsoft Hyper-V (Secure boot není podporován)

Stejná pravidla kompatibility platí pro hostovaný operační systém. Například ESET Full Disk Encryption pro Windows není podporován na ARM zařízeních a nelze jej použít v systému Windows virtualizovaném na procesorech Apple ARM.

Požadavky na konzoli pro správu:

- **ESET PROTECT** nebo **ESET PROTECT On-Prem 8.0+**
- **ESET Management Agent ve verzi 7.1 a novější** pro Windows
- **ESET Management Agent ve verzi 8.0 a novější** pro macOS

EFDE pro MAC

ESET Full Disk Encryption pro macOS využívá pro šifrování spravovaných stanic nativní aplikaci Apple pro šifrování disku nazvanou FileVault2, která uživatelům i administrátorům poskytuje efektivní proces šifrování. ESET Full Disk Encryption pro macOS reportuje stav šifrování do konzole pro vzdálenou správu a umožňuje vzdáleně šifrovat a dešifrovat spravované stanice – díky čemuž vám pomůže dodržet mnoho nařízení týkajících se zabezpečení dat.

Zakoupení licence

Pro aktivaci produktu ESET Full Disk Encryption je vyžadována samostatná licence. ESET Full Disk Encryption je rozšíření konzole pro vzdálenou správu, které je možné zakoupit k novým i stávajícím ESET licencím určeným pro firemní uživatele. Zákazník si může zakoupit nejvýše počet licencí, který odpovídá velikosti jeho licence pro ochranu koncových stanic. Licenci pro ESET Full Disk Encryption si zakupte u lokálního distributora ESET. Po obdržení licence ji nahrajte do svého účtu na portále ESET Business Account. Následně se vám v konzoli pro vzdálenou správu odemknou funkce související s produktem ESET Full Disk Encryption.

Kontaktujte nás

S dotazy týkající se licencování produktu a jeho nákupu se obraťte na lokální obchodní oddělení společnosti ESET. Podporu ESET můžete kontaktovat e-mailem, prostřednictvím chatu nebo telefonicky. Všechny kontakty naleznete na webových stránkách.

Používání ESET Full Disk Encryption

Po úspěšném importování ESET Full Disk Encryption licence následující níže uvedené kroky:

1. Vytvoření EFDE politiky.

2. Nasazení EFDE klienta na pracovní stanice.

3. Uživatel každé stanici si vytvoří pre-boot heslo.

4. Po úspěšném dokončení procesu šifrování budou disky v pracovních stanicích zašifrovány a chráněny před neoprávněným přístupem.



Zapnutí a konfigurace ESET Full Disk Encryption

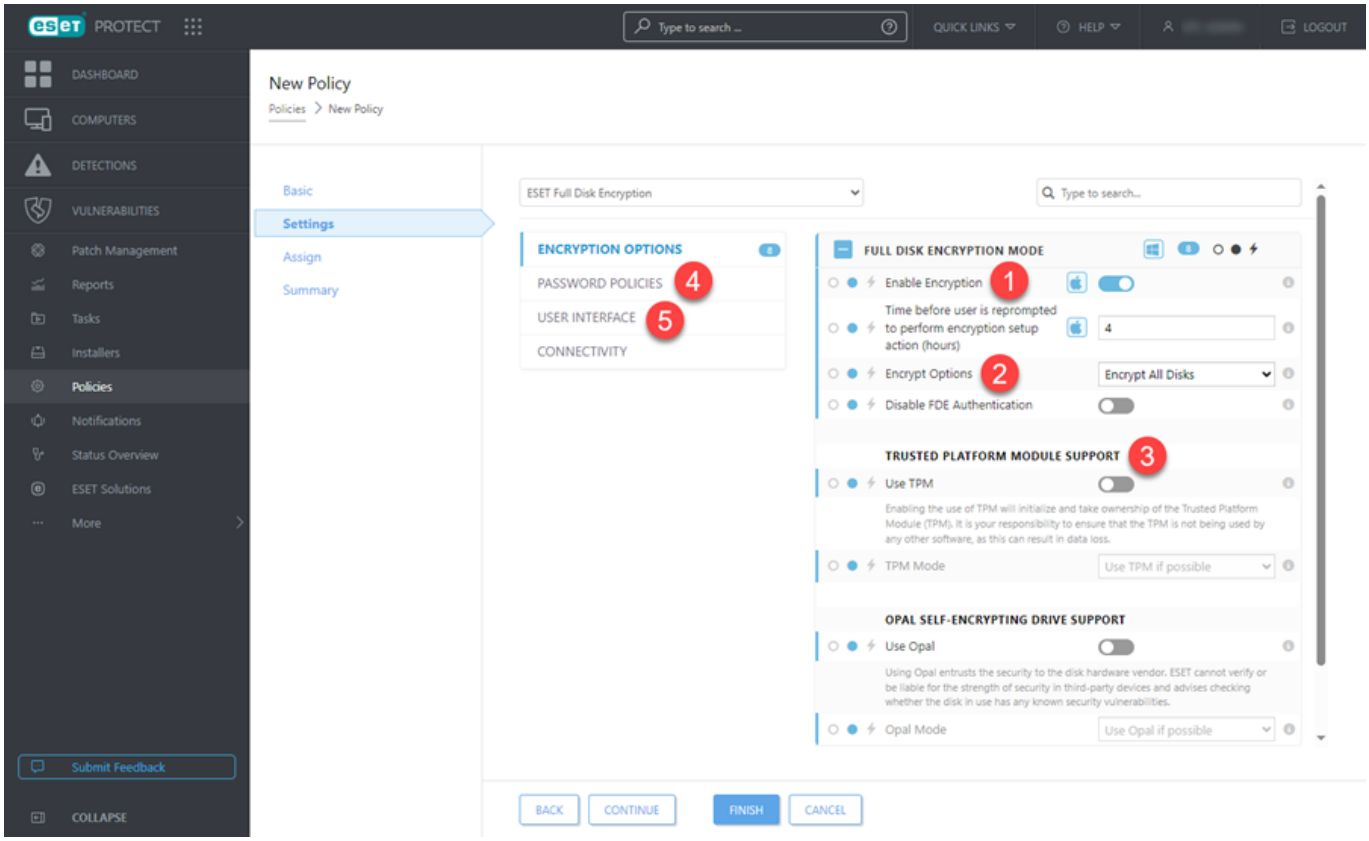
Pokud dojde k chybě: **Váš počítač není zašifrován a data v něm uložená nejsou chráněna**, podle následujících kroků nastavte šifrování počítače a chybu vyřešte.

ESET Full Disk Encryption Můžete konfigurovat prostřednictvím ESET Security Management Center, ESET PROTECT On-Prem nebo ESET PROTECT politiky: pro její vytvoření klikněte v hlavním menu na záložku **Politiky**, následně tlačítko **Nová politika** a v **průvodci pro vytvořením politiky** si jako produkt z rozbalovacího menu vyberte **ESET Full Disk Encryption**.

Konfigurovat můžete:

Možnosti konfigurace platné pro macOS mají štítek .

1. V sekci **Možnosti šifrování** > **Režim Full Disk Encryption** aktivujte pomocí přepínače možnost **Zapnout šifrování**. Prostřednictvím této možnosti aktivujete/deaktivujete šifrování na spravované stanici.



2. Dále se **rozhodněte**, zda chcete **Zašifrovat všechny disky** nebo **Zašifrovat pouze bootovací disk**.

3. Na základě toho, zda je spravovaná stanice vybavena potřebným hardwarem definujte možnosti v části **Podpora Trusted Platform Modulu** (TPM) nebo **Podpora Opal samošifrovacích disků**.

4. V sekci **Politika hesla** definujte **Požadavky na uživatelské heslo**, které bude uživatel zadávat na pre-boot obrazovce pro přihlášení ke své stanici.

5. V poslední řadě můžete v sekci **Uživatelské rozhraní** > **Prvky uživatelského rozhraní** ovlivnit chování EFDE a jeho míru interakce s uživatelem.

6. Vytvoření politiky potvrdí kliknutím na tlačítko **Dokončit**. Politiku zatím nepřiřazujte. Můžete ji aplikovat až po nasazení EFDE klienta na stanici.

7. Před zahájením šifrování nasaďte EFDE klienta na pracovní stanice.

Detailní popis jednotlivých možností konfigurace ESET Full Disk Encryption naleznete v níže uvedených kapitolách:

- Politika hesla
- Možnosti šifrování
- Uživatelské rozhraní
- Nástroje

Možnosti šifrování

Režim Full Disk Encryption

- **Zapnout šifrování** – prostřednictvím této možnosti aktivujete/deaktivujete šifrování na spravované stanici. Pokud na stanici aplikujete politiku, ve které bude toto nastavení deaktivováno, dojde k jejímu **dešifrování**.

- **Doba, po jejímž uplynutí bude uživatel opět vyzván ke konfiguraci šifrování (v hodinách)** – nejvyšší povolená hodnota je 24 hodin. Pomocí této možnosti definujte interval, ve kterém bude uživateli zobrazována výzva k nastavení hesla pro zašifrování jeho stanice.

- **Možnosti šifrování**:

  - **Zašifrovat všechny disky** – aktivováním této možnosti zašifrujete všechny fyzické disky ve stanici. Tato možnost nemá vliv na externí HDD a USB jednotky.

  - **Zašifrovat pouze bootovací disk** – aktivováním této možnosti se zašifruje pouze fyzický disk, z něhož je spuštěna aktuální instance Windows.

- **Deaktivovat FDE autentifikaci** – pomocí této možnosti vynutíte/zrušíte požadavek na zadání pre-boot hesla.

Podpora Trusted Platform Modulu

Nastavení politiky	Podporované OS	Popis
Použít TPM		Aktivováním této možnosti se inicializuje TPM a převezme se vlastnictví Trusted Platform Modulu (TPM). Vaší odpovědností je ujistit se, že TPM není používáno jinou aplikací. V opačném případě může dojít ke ztrátě dat.
Režim TPM		• **Použít TPM, pokud je dostupný** – v průběhu procesu šifrování se produkt pokusí použít TPM. Pokud verze TPM není podporována nebo TPM není dostupný, šifrovat se začne bez použití TPM. • **Vyžadovat TPM** – pomocí této možnosti vynutíte použití TPM. Vybráním této možnosti na stanicích s nedostupným nebo nepodporovanou verzí TPM povede k neúspěšnému zahájení šifrování.

Od verze 1.2.4 nedochází před použitím ESET Full Disk Encryption k vymazání TPM.

Podpora Opal samošifrovacích disků

Nastavení politiky	Podporované OS	Popis
Použít Opal		Po aktivování této možnosti se šifrování zahájí s využitím samošifrovací funkce OPAL disků. Mějte na paměti, že se jedná o hardwarovou funkci disku.
Opal režim		• **Použít Opal, pokud je dostupný** – v průběhu procesu šifrování se produkt pokusí použít hardwarové šifrování Opal. Pokud verze Opal není podporována nebo podpora Opal není dostupná, šifrovat se začne bez použití Opal. • **Vyžadovat Opal** – pomocí této možnosti vynutíte použití Opal šifrování. Vybráním této možnosti na stanicích s nedostupnou podporou nebo nepodporovanou verzí Opal povede k neúspěšnému zahájení šifrování.

Politika hesla

Požadavky na uživatelské heslo

- **Uživatel si může změnit heslo** – pokud tuto možnost deaktivujete, heslo bude možné změnit pouze na podnět inicializovaným administrátorem z konzole pro vzdálenou správu.

Síla hesla

Nastavení politiky	Podporované OS	Popis
Vyžadovat malá písmena		Heslo musí obsahovat alespoň jedno malé písmeno. (a-z)
Vyžadovat velká písmena		Heslo musí obsahovat alespoň jedno velké písmeno. (A-Z)
Vyžadovat čísla		Heslo musí obsahovat alespoň jedno číslo. (0-9)
Je nutné použít symboly		Heslo musí obsahovat alespoň jeden speciální znak. (!@#$%)
Minimální délka hesla		Definujte minimální délku hesla (1-127 znaků).

Počet pokusů

Nastavení politiky	Podporované OS	Popis
Omezit nesprávné zadání hesla		Pokud tuto možnost deaktivujete, počet pokusů nebude omezen. Z bezpečnostních důvodů tuto možnost nedoporučujeme mít trvale vypnutou.
Maximální počet neúspěšných zadání hesla		Maximální hodnota: 254. Maximální počet po sobě jdoucích pokusů o zadání hesla před zamčením účtu. Následně bude vyžadováno heslo pro obnovení.

Platnost hesla

Nastavení politiky	Podporované OS	Popis
Heslo má omezenou platnost		Pokud tuto možnost deaktivujete, uživatelské heslo bude stále platné.
Maximální stáří hesla (ve dnech)		Zadávejte hodnotu mezi 1 a 999 dny. Doporučujeme definovat platnost v rozmezí 30 až 90 dní.
Upozornit uživatele na blížící se konec platnosti hesla		Pokud tuto možnost deaktivujete, uživatel nebude upozorněn na blížící se konec platnosti hesla.
Upozornit uživatele, pokud do konce zbývá méně než (dny)		Zadávejte hodnotu mezi 1 a 999 dny. Pomocí této možnosti definujte počet dní, odkdy začne produkt uživatele upozorňovat na blížící se konec platnost hesla.

Možnosti hesla pro obnovení

Počet pokusů

Nastavení politiky	Podporované OS	Popis
Omezit nesprávné zadání hesla		Pokud tuto možnost deaktivujete, počet pokusů o obnovení hesla nebude nijak omezen. Z bezpečnostních důvodů tuto možnost nedoporučujeme mít trvale vypnutou.
Maximální počet neúspěšných zadání hesla		Maximální hodnota: 254. Maximální počet po sobě jdoucích pokusů o zadání hesla před zamčením účtu. Následně bude vyžadováno heslo pro obnovení.

Použití hesla pro obnovení

- Žádné nastavení v této sekci není ve výchozí konfiguraci zapnuté. Ujistěte se, že jste je zapnuli ručně.
- Všechna nastavení v této sekci se aplikují po dešifrování počítače a jeho opětovném zašifrování.

Nastavení politiky	Podporované OS	Popis
Omezit použití hesla pro obnovení		Pokud tuto možnost deaktivujete, stejné heslo nebude možné opakovaně použít, a bude nutné vygenerovat nové.
Maximální počet použití		Maximální hodnota: 254.
Upozornit uživatele, když se blíží k limitu hesla pro obnovení		Pokud je tato možnost aktivní, uživatel bude upozorněn na blížící se konec platnosti hesla pro obnovení.
Upozornit, když zbývá (použití)		Maximální hodnota: 255.
Automaticky generovat nové heslo pro obnovení		Pokud je tato možnost aktivní, nové heslo pro obnovení se automaticky vygeneruje po dosažení maximálního počtu použití.
Generovat, když (zbývá použití)		Maximální hodnota: 255.

Uživatelské rozhraní

Prvky uživatelského rozhraní

- **Režim spuštění**:
  - **Úplný** – bude k dispozici úplné hlavní okno programu.
  - **Minimální** – hlavní okno programu se spustí, ale uživateli se zobrazí pouze oznámení.

Stavy aplikace

- **Stavy aplikace**: V této části se můžete rozhodnout, které stavy aplikace chcete zobrazit uživateli v hlavním okně programu, a které chcete odesílat do konzole.

Prezentační režim

Nastavení politiky	Podporované OS	Popis
Automaticky vypínat Prezentační režim		Aktivujte tuto možnost, pokud chcete automaticky vypínat prezentační režim.
Vypnout za (minut)		Pomocí této možnosti definujte interval v minutách (maximální hodnota je 2000), po jehož uplynutí se prezentační režim ukončí.

Nástroje

V sekci Nástroje můžete definovat parametry proxy serveru, které má EFDE použít v průběhu aktivace.

Proxy server

Nastavení politiky	Podporované OS	Popis
Používat proxy server		Pomocí této možnosti povolíte použití proxy v průběhu aktivace produktu.
Proxy server		Zadejte adresu proxy serveru.
Port		Zadejte port proxy serveru.
Proxy server vyžaduje autentifikaci		Tuto možnost aktivujte v případě, kdy je pro připojení k proxy serveru vyžadováno ověření.
Uživatelské jméno		Zadejte uživatelské jméno.
Heslo		Zadejte heslo.
Použít přímé spojení, pokud není dostupný proxy server		Pokud aktivujete tuto možnost, v případě kdy nebude proxy server dostupný, se produkt pokusí s aktivačními servery spojit přímo.

Nasazení EFDE klienta

Pro zašifrování disků je nutné na spravované stanice nainstalovat EFDE klienta.

> ⚠ Z důvodu známého problému není možné v ESET PROTECT vytvořit Live Installer pro EFDE pro macOS. Doporučený postup je nejprve nasadit ESET Management Agenta. Následně prostřednictvím klientské úlohy na instalaci aplikace, případně pomocí průvodce pro aktivaci šifrování dostupného v detailech počítače, nasadit EFDE pro macOS.

EFDE klienta můžete nasadit třemi různými způsoby:

- Vytvořením all-in-one instalačního balíčku
- Pomocí úlohy pro instalaci aplikace
- Pomocí Průvodce zapnutím šifrování

EFDE all-in-one instalační balíček

> ⚠ Z důvodu známého problému není možné v ESET PROTECT vytvořit Live Installer pro EFDE pro macOS. Doporučený postup je nejprve nasadit ESET Management Agenta. Následně prostřednictvím klientské úlohy na instalaci aplikace, případně pomocí průvodce pro aktivaci šifrování dostupného v detailech počítače, nasadit EFDE pro macOS.

Prostřednictvím all-in-one instalačního balíčku můžete na stanici nasadit ESET Management Agent společně s EFDE klientem.

1. V hlavním menu konzole přejděte do sekce **Instalační balíčky** a klikněte na **Vytvořit instalační balíček** > **All-in-one instalační balíček**.

2. V sekci **Obecné** zaškrtněte možnost **Full Disk Encryption** (tím do balíčku přidáte EFDE klienta) a klikněte na tlačítko **Pokračovat**.

3. Dále vyberte EFDE licenci, kterou chcete používat pro aktivaci.

4. Dále si vyberte **Produkt/Verzi**, který chcete zahrnout do instalačního balíčku. Automaticky se předvybere nejnovější verze. Změnu provádějte pouze ve specifických případech.

5. Vyberte si **Jazyk**, ve kterém chcete produkt nainstalovat.

6. Pokud jste si již vytvořili vlastní **politiku**, vyberte ji. Standardně se vyberte jedna z předdefinovaných politik.

7. Odsouhlaste licenční ujednání s koncovým uživatelem a zásady ochrany osobních údajů.

8. V sekci **Rozšířené** si můžete balíček **pojmenovat** a volitelně mu přidat **popis**.

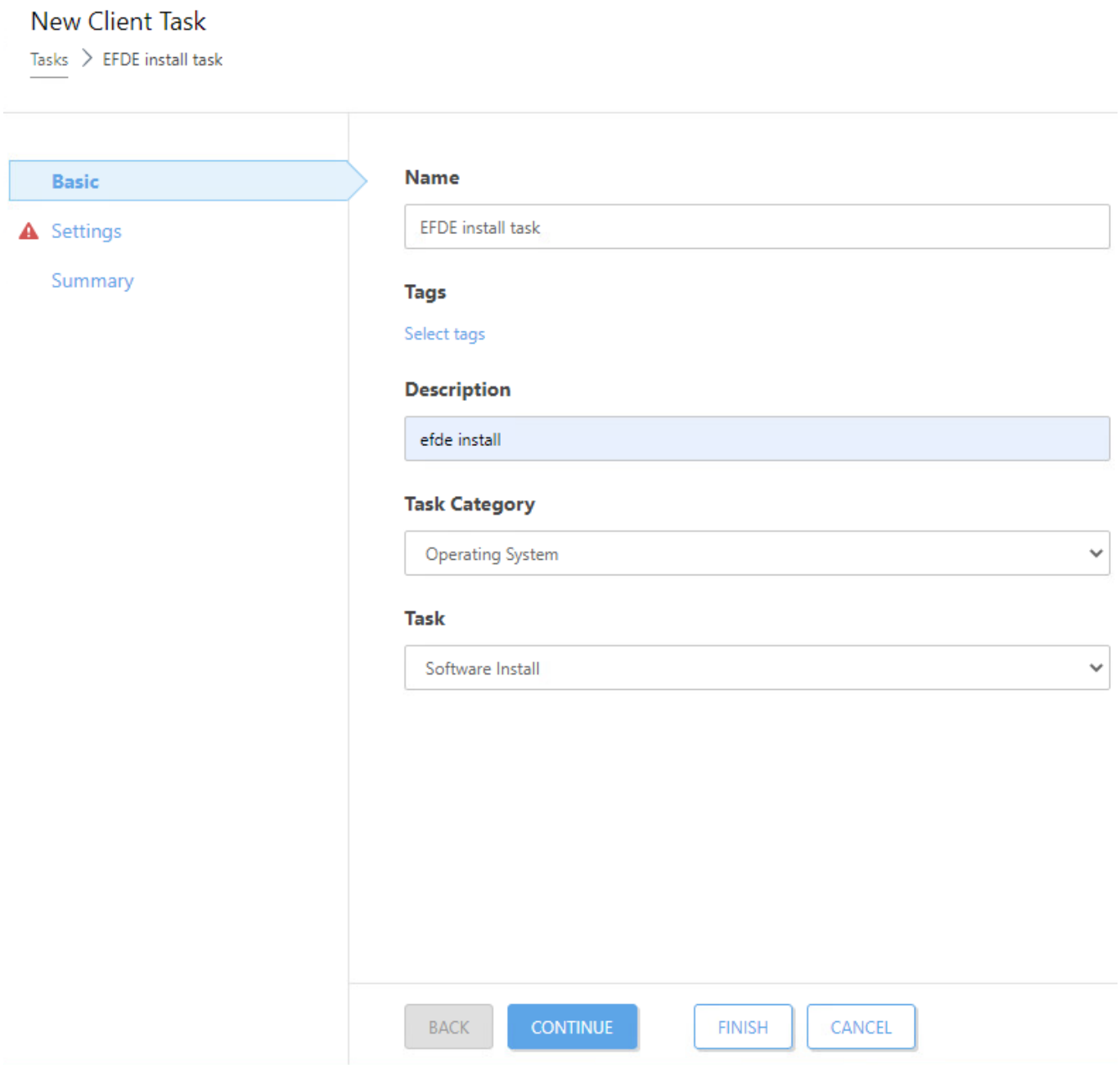
9. Po kliknutí na tlačítko **Dokončit** si balíček stáhněte, a můžete jej nasadit.

Klientská úloha pro instalaci EFDE

Na Apple M1 Mac zařízeních se ujistěte, že máte nainstalován emulátor Rosetta.

Na již spravované stanice můžete EFDE klienta nasadit prostřednictvím klientské úlohy na instalaci aplikace.

1. V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.
2. Zadejte **název**, volitelně **popis**, nově vytvářené úlohy.
3. Z rozbalovacího menu **Kategorie úlohy** vyberte možnost **Operační systém**.
4. Jako typ **Úlohy** vyberte z rozbalovacího menu možnost **Instalace aplikace**.

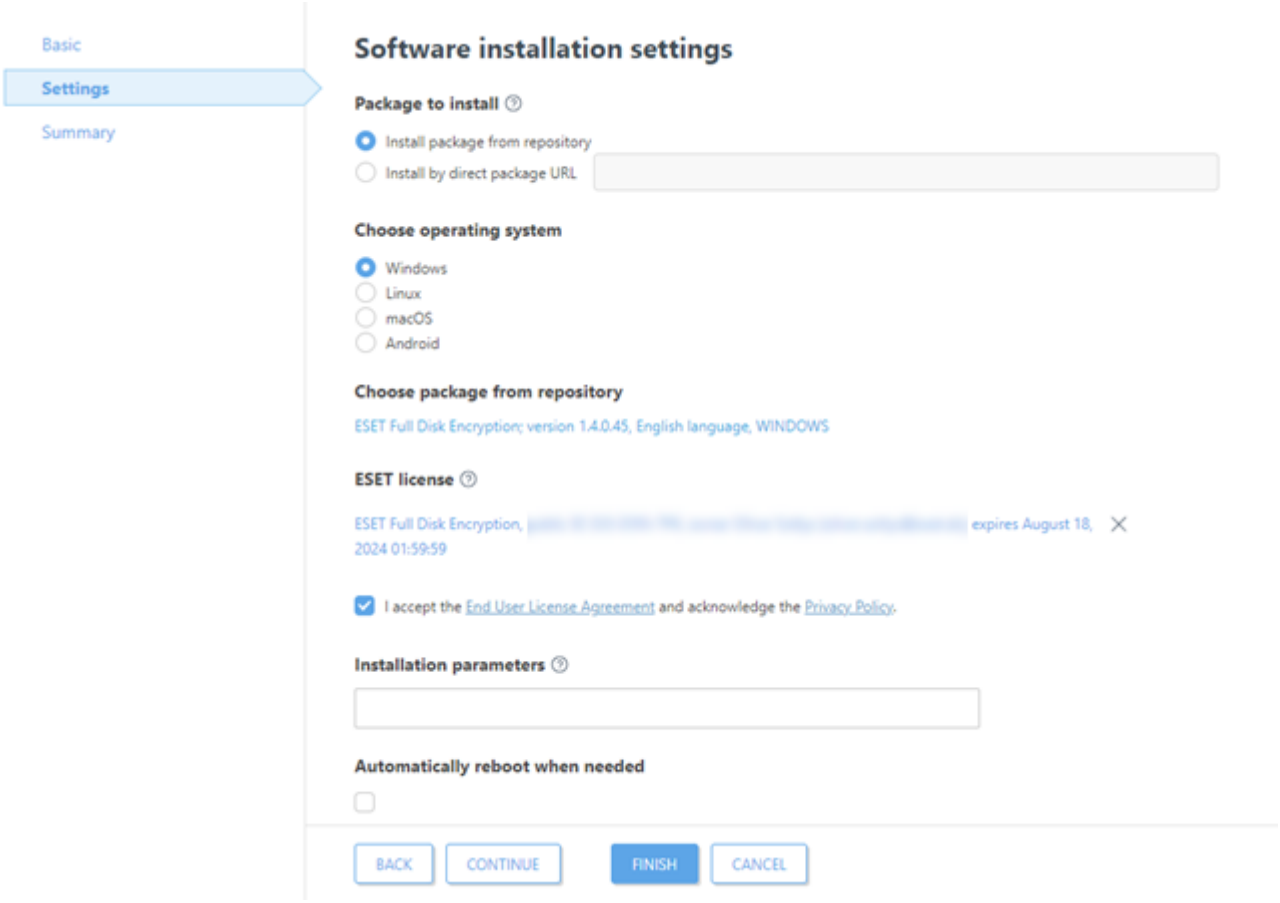


5. Klikněte na tlačítko **Pokračovat**.

6. Klikněte na možnost **Vybrat balíček** a jako produkt v repozitáři najděte **ESET Full Disk Encryption** (pro Windows) nebo **ESET Full Disk Encryption for macOS** (pro macOS).

7. Dále vyberte EFDE licenci, kterou chcete používat pro aktivaci.

8. Odsouhlaste licenční ujednání s koncovým uživatelem a zásady ochrany osobních údajů.



9. Pokračujte kliknutím na tlačítko **Dokončit** a v zobrazeném oznámení klikněte na tlačítko **Vytvořit podmínku spuštění**.

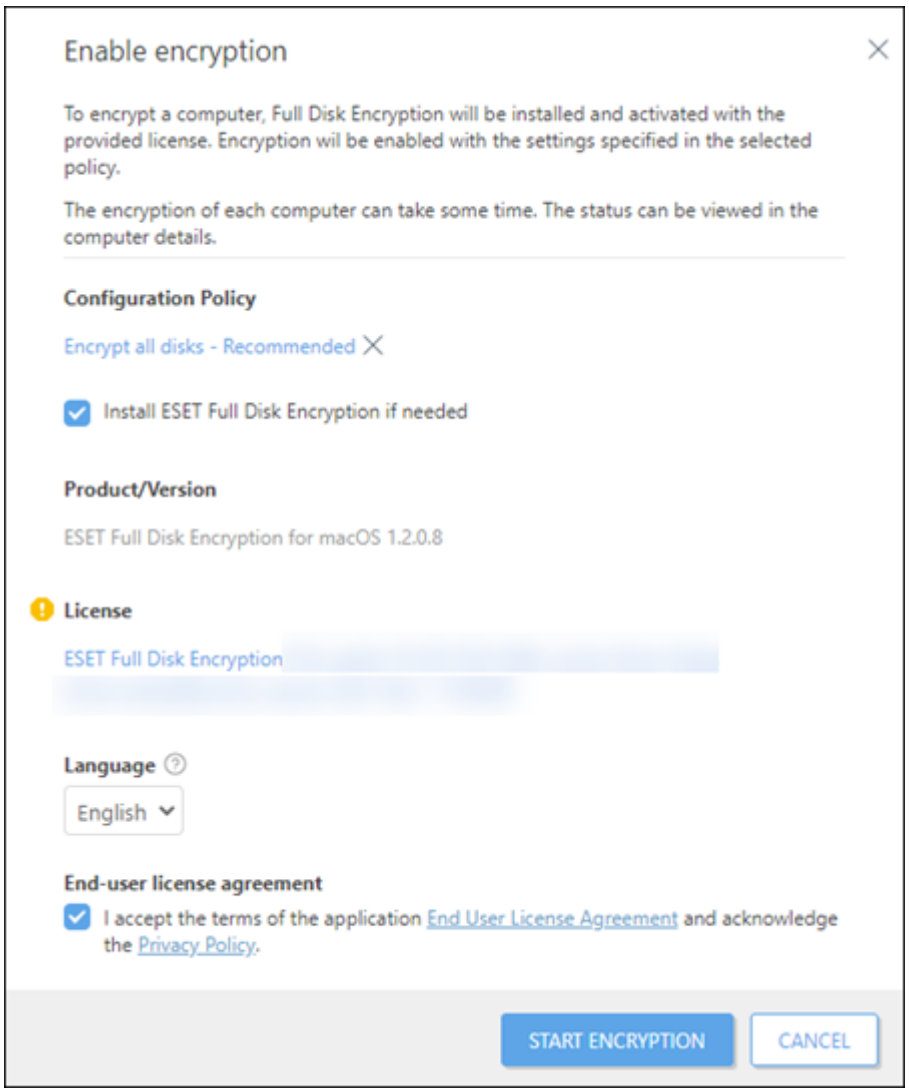
10. V sekci **Cíl** klikněte na tlačítko **Přidat počítače** a vyberte stanice, na které chcete produkt nainstalovat.

11. Vyberte si **Podmínku spuštění** a provedení úlohy naplánujte kliknutím na tlačítko **Dokončit**.

Po úspěšném spuštění úlohy můžete na cílové stanici aktivovat šifrování.

Průvodce zapnutím šifrování

Možnost pro zahájení šifrování na konkrétní spravované stanici naleznete v hlavním menu konzole v sekci **Počítače**. Klikněte v seznamu na požadovanou stanici a v jejím kontextovém menu vyberte možnost **Zapnout šifrování**, případně vyberte možnost **Zobrazit detaily** a následně v **detailech počítače** na dlaždici **Šifrování** klikněte na tlačítko **Zašifrovat počítač**.



Po zobrazení průvodce pro **Zapnutí šifrování**:

1. Vyberte EFDE **politiku**, kterou chcete na stanici aplikovat.
2. Zaškrtněte možnost **Nainstalovat EFDE klienta, pokud je to potřeba**.
3. **Produkt/Verze** se vyberte automaticky na základě OS pracovní stanice.

> Pokud používáte ESET Security Management Center, bude nutné ručně vybrat **Produkt/Verzi**, který chcete zahrnout do instalačního balíčku. Automaticky se předvybere nejnovější verze. Změnu provádějte pouze ve specifických případech.

4. Dále vyberte EFDE licenci, kterou chcete používat pro aktivaci.
5. Vyberte si **Jazyk**, ve kterém chcete produkt nainstalovat.
6. Odsouhlaste licenční ujednání s koncovým uživatelem a zásady ochrany osobních údajů.
7. Pro zahájení procesu šifrování klikněte na tlačítko **Zahájit šifrování**.

Nasazení ESET Full Disk Encryption prostřednictvím příkazového řádku

- Nasazení instalačního balíčku s předdefinovaným heslem
- Zneplatnění hesla prostřednictvím příkazového řádku
- Pozastavení/obnovení FDE autentifikace prostřednictvím příkazového řádku
- Přidání/odebrání rozložení klávesnice prostřednictvím příkazového řádku

Nasazení instalačního balíčku s předdefinovaným heslem

Při nasazování ESET Full Disk Encryption můžete prostřednictvím parametrů definovat heslo, které se použije pro šifrování, stejně tak rozložení klávesnice. Tyto instalační parametry využijete v případě, kdy pokud chcete nasadit nový systém s předdefinovaným heslem tak, aby MSP nebo administrátor pouze nastavil nový počítač, nasadil na něj ESET Full Disk Encryption a automaticky došlo k zašifrování systému tím, že je na něj aplikována šifrovací politika.

Předpoklady:
- Parametry `STARTUPPASSWORD` a `STARTUPPASSWORDKLID` musí být součástí instalačního balíčku ESET Full Disk Encryption
- ESET Full Disk Encryption ve verzi 1.3.0.x
- Nainstalovaný ESET Full Disk Encryption musí být aktivován
- V systému musí být nainstalován ESET Management Agent připojený k ESET PROTECT On-Prem

1. V hlavním menu ESET PROTECT On-Prem Web Console přejděte na záložku **Počítače**.

2. Klikněte na požadovaný počítač > **Úloha** > **Nová úloha**.

3. Zadejte název úlohy (například Instalace EFDE a automatické zašifrování) a v rozbalovacím nabídce jako typ **Úlohy** vyberte možnost **Instalace aplikace**.

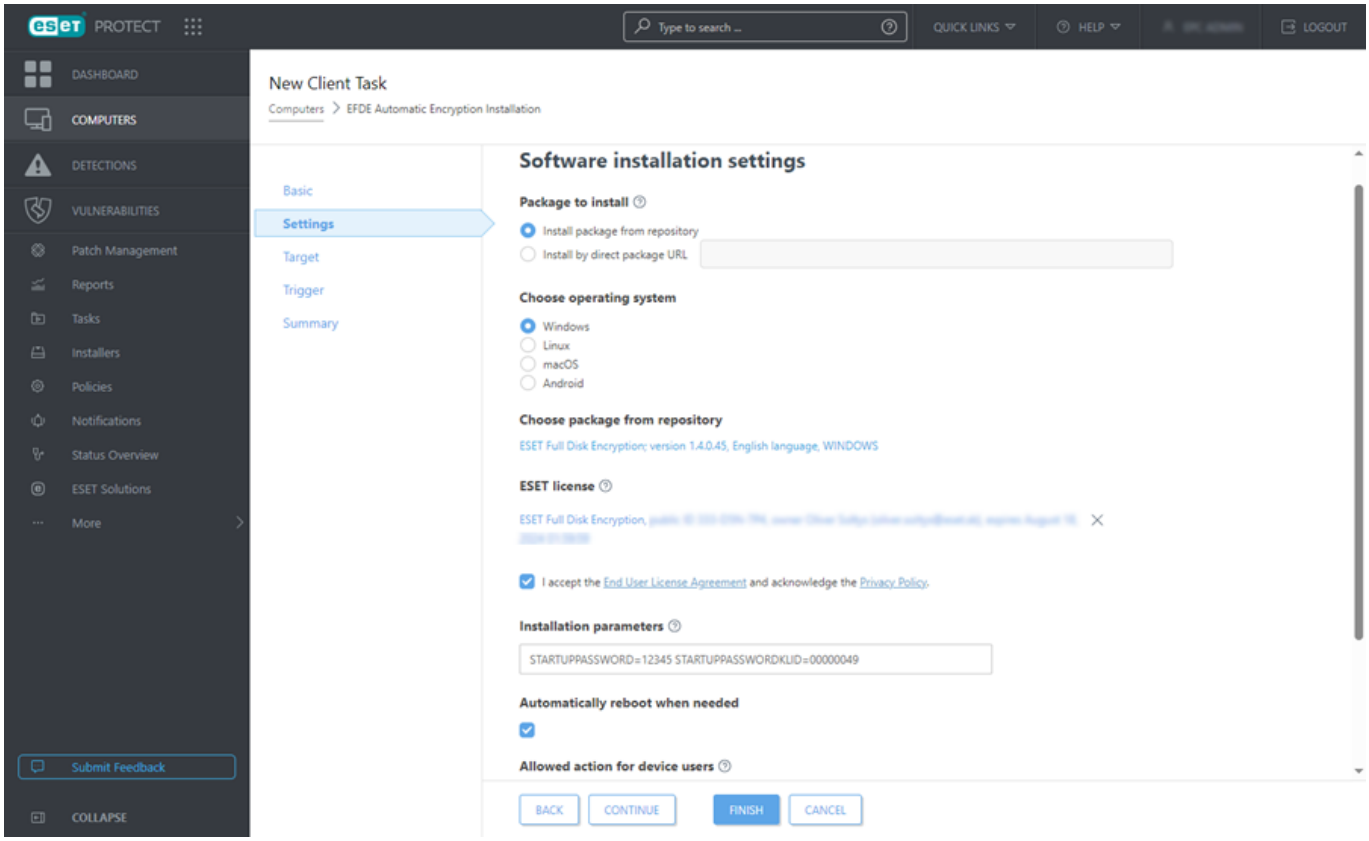
4. Klikněte na tlačítko **Pokračovat**.

5. Klikněte na **<Choose package>** a z repozitáře vyberte odpovídající instalační balíček.

6. Do pole **Parametry instalace** zadejte `STARTUPPASSWORD` a `STARTUPPASSWORDKLID`.

Parametrem `STARTUPPASSWORD` definujete počáteční heslo FDE. Příklad: pokud zadáte `STARTUPPASSWORD=12345`, heslo pro šifrování bude 12345.
Parametrem `STARTUPPASSWORDKLID` nastavíte rozložení klávesnice. Příklad: pokud zadáte `STARTUPPASSWORDKLID=00000405`, do systému se nainstaluje česká klávesnice. Parametr používá klávesové identifikátory KLID klávesnice pro identifikaci a přidání správné klávesnice do systému. Viz seznam rozložení klávesnic.
Tyto parametry je nutné použít současně, aby při aplikování šifrovací politiky mohlo dojít k zahájení automatického šifrování.

7. Pokud je to vyžadováno, vyberte možnost **Automaticky restartovat, když je potřeba**. Automatické restartování není vyžadováno, přesto ESET Full Disk Encryption vyžaduje restart zařízení. Bez restartování nedojde k zahájení šifrování.



8. Po dokončení instalace ESET Full Disk Encryption je nutné produkt aktivovat, aby mohlo dojít k zahájení šifrování. Vytvořte šifrovací politiku obsahující parametry vyhovující vašim požadavkům a aplikujte ji na zařízení, aby mohlo dojít k zahájení šifrování.

Po dokončení všech výše uvedených kroků zařízení bude uživatel produktem vyzván k inicializaci tzv. **Bezpečného spuštění**. Po úspěšném dokončení **Bezpečného spuštění** se zahájí samotný proces šifrování, aniž by uživatel musel zadávat heslo.

Pokud uživatel zařízení restartuje, bude muset použít heslo, které bylo definováno prostřednictvím parametru `STARTUPPASSWORD`.

Administrátor ESET PROTECT On-Prem může z konzole na zařízení odeslat úlohu **Zneplatnit FDE heslo**. Následně se uživateli zobrazí výzva pro vytvoření nového hesla.

Zneplatnění hesla prostřednictvím příkazového řádku

Zneplatnit FDE heslo je možné na klientské stanici prostřednictvím příkazového řádku.

Předpoklady:

- ESET Full Disk Encryption ve verzi 1.3.0.x
- Nainstalovaný ESET Full Disk Encryption musí být aktivován
- V systému musí být nainstalován ESET Management Agent připojený k ESET PROTECT On-Prem
- Systém musí být zašifrován nebo dešifrován

1. Otevřete si příkazový řádek se zvýšenými oprávněními.

2. Přejděte do složky *C:\Program Files\ESET\ESET Full Disk Encryption* a spusťte příkaz `efdeais /command=invalidate_password`. Případně můžete v rámci jednoho příkazu definovat cestu a samotný příkaz: `C:\Program Files\ESET\ESET Full Disk Encryption efdeais /command=invalidate_password`.

3. Při úspěšném provedení příkazu se v příkazovém řádku zobrazí informace **Command successful**.

V uživatelském rozhraní ESET Full Disk Encryption se zobrazí informace, že platnost hesla vypršela, a uživatel bude vyzván k nastavení nového.

Pozastavení/obnovení FDE autentifikace prostřednictvím příkazového řádku

Při každém spuštění zašifrovaného zařízení se zobrazí pre-boot přihlašovací obrazovka. Uživatelé mohou uživatelé dočasně pozastavit autentifikaci před spuštěním systému – například v případech, kdy instalace aktualizací Windows vyžaduje restart.

Předpoklady:

- ESET Full Disk Encryption ve verzi 1.3.0.x
- Nainstalovaný ESET Full Disk Encryption musí být aktivován
- V systému musí být nainstalován ESET Management Agent připojený k ESET PROTECT On-Prem
- Systém musí být zašifrován nebo dešifrován

1. Otevřete si příkazový řádek se zvýšenými oprávněními.

2. Přejděte do složky *C:\Program Files\ESET\ESET Full Disk Encryption* a spusťte příkaz `efdeais / command=` společně s jedním z následujících příkazů: `pause_authentication` nebo `resume_authentication`. Případně můžete v rámci jednoho příkazu definovat cestu a samotný příkaz: `C:\Program Files\ESET\ESET Full Disk Encryption efdeais / command=pause_authentication`.

Při použití příkazu `pause_authentication` je nutné zadat podmínku pro pozastavení FDE autentifikace: počtem restartů, v sekundách, minutách, hodinách nebo do konkrétního času. Příklady:

```
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
```

Čas definujte v unixovém formátu.

Při použití příkazu `resume_authentication` není nutné zadávat žádné další parametry. Tím dojde k obnovení autentifikace a při příštím spuštění zařízení se zobrazí pre-boot obrazovka.

3. Při úspěšném provedení příkazu se v příkazovém řádku zobrazí informace **Command successful**. Zároveň se změní stav produktu ESET Full Disk Encryption a upozorní uživatele, že je FDE autentifikace je vypnutá.

Přidání/odebrání rozložení klávesnice prostřednictvím příkazového řádku

Definované rozložení klávesnice se využívá při zadávání hesla na pre-boot obrazovce, stejně tak ve chvíli, kdy si uživatel mění heslo prostřednictvím grafického uživatelského rozhraní produktu ESET Full Disk Encryption. Ne všechny klávesnice mají stejné rozložení, proto je nutné je rozlišovat. Prostřednictvím parametrů příkazového řádku si uživatelé mohou zobrazit seznam nainstalovaných rozložení klávesnic v systému, stejně tak další přidávat, případně odebírat. To využije v případě, kdy se uživatel rozhodne přidat další rozložení klávesnice poté, co již zahájil šifrování Windows zařízení. Pokud si uživatelé nepřidají odpovídající rozložení klávesnice, po změně fyzické klávesnice nemusí být schopni ve Windows změnit své FDE heslo, stejně tak může docházet ke stisknu jiných kláves na pre-boot ověřovací obrazovce, než očekávají.

Předpoklady:

- ESET Full Disk Encryption ve verzi 1.3.0.x
- Nainstalovaný ESET Full Disk Encryption musí být aktivován
- V systému musí být nainstalován ESET Management Agent připojený k ESET PROTECT On-Prem
- Systém musí být zašifrován nebo dešifrován

1. Otevřete si příkazový řádek se zvýšenými oprávněními.

2. Přejděte do složky *C:\Program Files\ESET\ESET Full Disk Encryption* a spusťte příkaz `efdeais /command=` společně s jedním z následujících příkazů: `add_keyboard`, `remove_keyboard`, nebo `list_keyboards`. Případně můžete v rámci jednoho příkazu definovat cestu a samotný příkaz: `C:\Program Files\ESET\ESET Full Disk Encryption efdeais /command=add_keyboard`.

Při použití příkazu `add_keyboard` je nutné následně definovat rozložení klávesnice, které chcete do systému přidat, a to prostřednictvím identifikátoru KLID. Příklad: `efdeais /command=add_keyboard.00000809`. Tím se do systému přidá české rozložení klávesnice.

Při použití příkazu `remove_keyboard` je nutné následně definovat rozložení klávesnice, které chcete ze systému odebrat, a to prostřednictvím identifikátoru KLID. Příklad: `efdeais /command=remove_keyboard.00000809`. Tím se ze systému odebere české rozložení klávesnice.

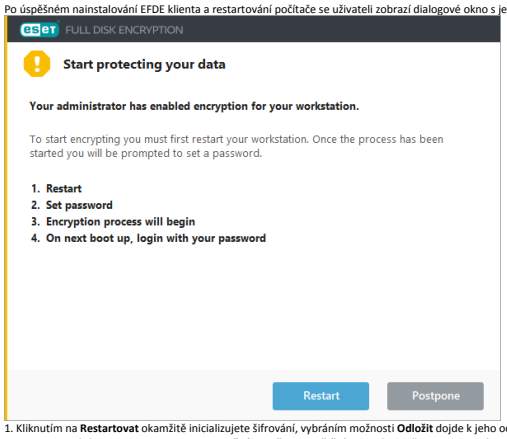
Při použití příkazu `list_keyboard` není nutné zadávat žádné další parametry. Příklad: `efdeais /command=list_keyboards`. Po jeho provedení se vrátí textový seznam rozložení klávesnic aktuálně nainstalovaných v systému. Přidáním argumentu `.json` na konec příkazu si zobrazíte rozložení klávesnice v JSON formátu.

Proces šifrování na straně EFDE klienta

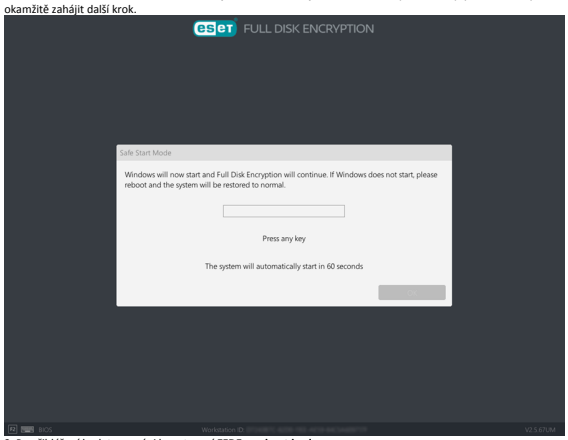
Po inicializaci procesu šifrování z konzole pro vzdálenou správu nebo úspěšném nasazení all-in-one instalačního balíčku je nutné pro zahájení šifrování stanici restartovat.

Windows

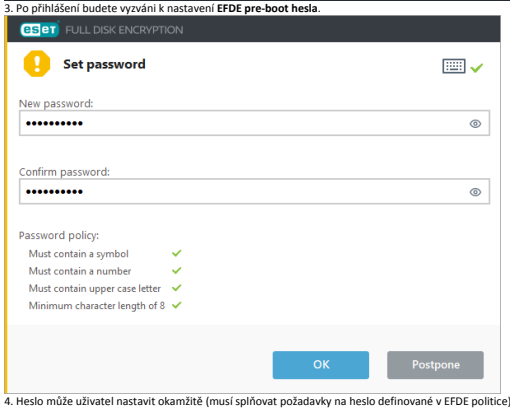
Po úspěšném nainstalování EFDE klienta a restartování počítače se uživateli zobrazí dialogové okno s jednotlivými kroky, které povedou k zašifrování stanice.



1. Kliknutím na **Restartovat** okamžitě inicializujete šifrování, vybráním možnosti **Odložit** dojde k jeho odložení.
2. Po restartování se na obrazovce **EFDE Bezpečného režimu spuštění** zobrazí odpočet. Po uplynutí 1 minuty bude automaticky pokračovat další krok. Stisknutím libovolné klávesy můžete okamžitě zahájit další krok.



3. Po přihlášení budete vyzváni k nastavení **EFDE pre-boot hesla**.



4. Heslo může uživatel nastavit okamžitě (musí splňovat požadavky na heslo definované v EFDE politice) nebo jeho nastavení odložit na později. Do doby, než si uživatel nastaví heslo, nebude šifrování pokračovat.

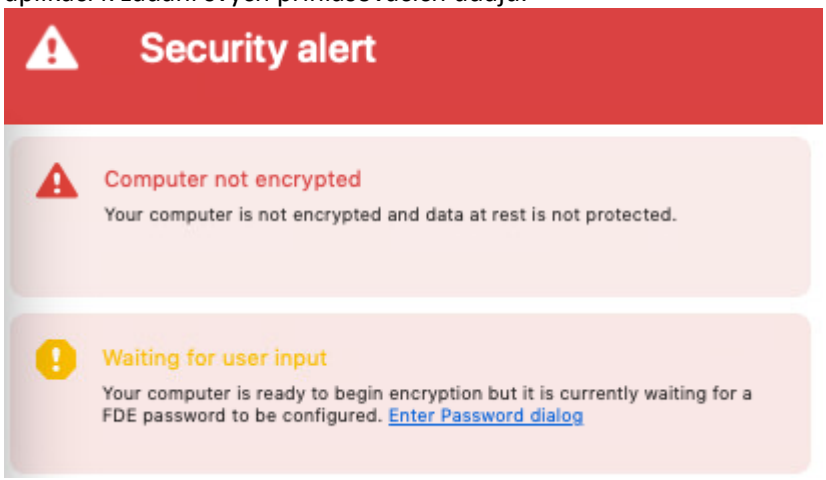
> Pokud si uživatel nenastaví heslo a restartuje počítače, šifrování se odloží. Pro opětovné inicializování bezpečného spuštění bude nutné EFDE klienta odinstalovat a znovu nainstalovat.

5. Po vytvoření se zahájí proces šifrování disků. Stav šifrování se zobrazí v hlavním okně EFDE klienta, a zároveň se přenese do konzole pro vzdálenou správu, kde jej naleznete v **Detailech počítače**.
6. Po úspěšné zašifrování se uživateli při dalším spuštění počítače zobrazí EFDE pre-boot přihlašovací obrazovka, na které bude vyzván k zadání hesla.

macOS

Na Apple M1 Mac zařízeních se ujistěte, že máte nainstalován emulátor Rosetta.

1. Po dokončení instalace bude pro zahájení šifrování uživatel vyzván klientskou aplikací k zadání svých přihlašovacích údajů.



2. Následně se zobrazí dialogové okno pro zadání přihlašovacích údajů.



3. Po zadání platných přihlašovacích údajů se zahájí šifrování. Stav šifrování se zobrazí v hlavním okně EFDE klienta, a zároveň se přenese do konzole pro vzdálenou správu, kde jej naleznete v **Detailech počítače**.

4. Po dokončení šifrování může uživatel pokračovat v používání zařízení jako dosud, nicméně disk je již nyní zašifrován.

Správa šifrování

Správa šifrování stanic spočívá ve správě pre-boot přihlašovacích údajů.

Tyto možnosti naleznete v konzoli pro vzdálenou správu v **Detailech počítače**, kdy na dlaždici **Šifrování** klikněte na tlačítko **Spravovat**:

Případně využijte úlohu pro aktivaci režimu údržby nebo možnosti, které jsou dostupné v politice.

Všechny EFDE úlohy se provedou až ve chvíli, kdy informaci o ní obdrží ESET Management Agent v průběhu procesu replikace dat (obvykle při dalším připojení agenta k serveru). Aby mohl agent informaci o úloze přijmout, musí být stanice nabootována do Windows. Agent informaci o úloze neobdrží, pokud je na stanici zobrazena pouze pre-boot obrazovka.

- **Zneplatnit FDE heslo** – po provedení této úlohy dojde k okamžitému zneplatnění aktuálně používaného hesla pro přihlášení a uživatel bude prostřednictvím EFDE klienta vyzván k nastavení nového hesla. Pokud uživatel neprovede změnu v hlavním okně EFDE klienta a vypne počítač, bude ke změně hesla vyzván na pre-boot obrazovce při dalším spuštění počítače.

- **Vygenerovat nové heslo pro obnovení FDE** – pomocí této úlohy okamžitě zneplatníte stávající heslo pro přihlášení a vygeneruje se nové, které může administrátor poskytnout uživateli.

- **Obnovení přístupu**

  - **Heslo pro obnovení** – pomocí této úlohy vygenerujete heslo pro obnovení, které uživatel použije při nastavení nového hesla.

  - **Data pro obnovení** – pomocí této úlohy vygenerujete soubor, který je vyžadován v průběhu procesu obnovení šifrování.

- **Zablokování přístupu**

  - **Zablokovat FDE heslo** – prostřednictvím této úlohy vynutíte při příštím spuštění počítače použití hesla pro obnovení. Pro vytvoření nového pre-boot hesla bude vyžadováno **Heslo pro obnovení**. V opačném případě se nebude schopen uživatel přihlásit. Po provedení této úlohy nebude uživatel schopen si heslo změnit na pre-boot obrazovce (ani v případě, kdy je tato možnost povolena v EFDE politice).

  - **Vymazat FDE heslo** – po spuštění této úlohy se na zařízení vyvolá BSOD (modrá obrazovka smrti). Ze zařízení se odstraní FDE heslo a uživatel nebude schopen se přihlásit. V tomto stavu není umožněno přihlášení, změna hesla ani jeho obnovení. Jedinou možností pro získání přístupu k zařízení je použití média pro obnovení šifrování.

Pozastavit FDE autentifikaci

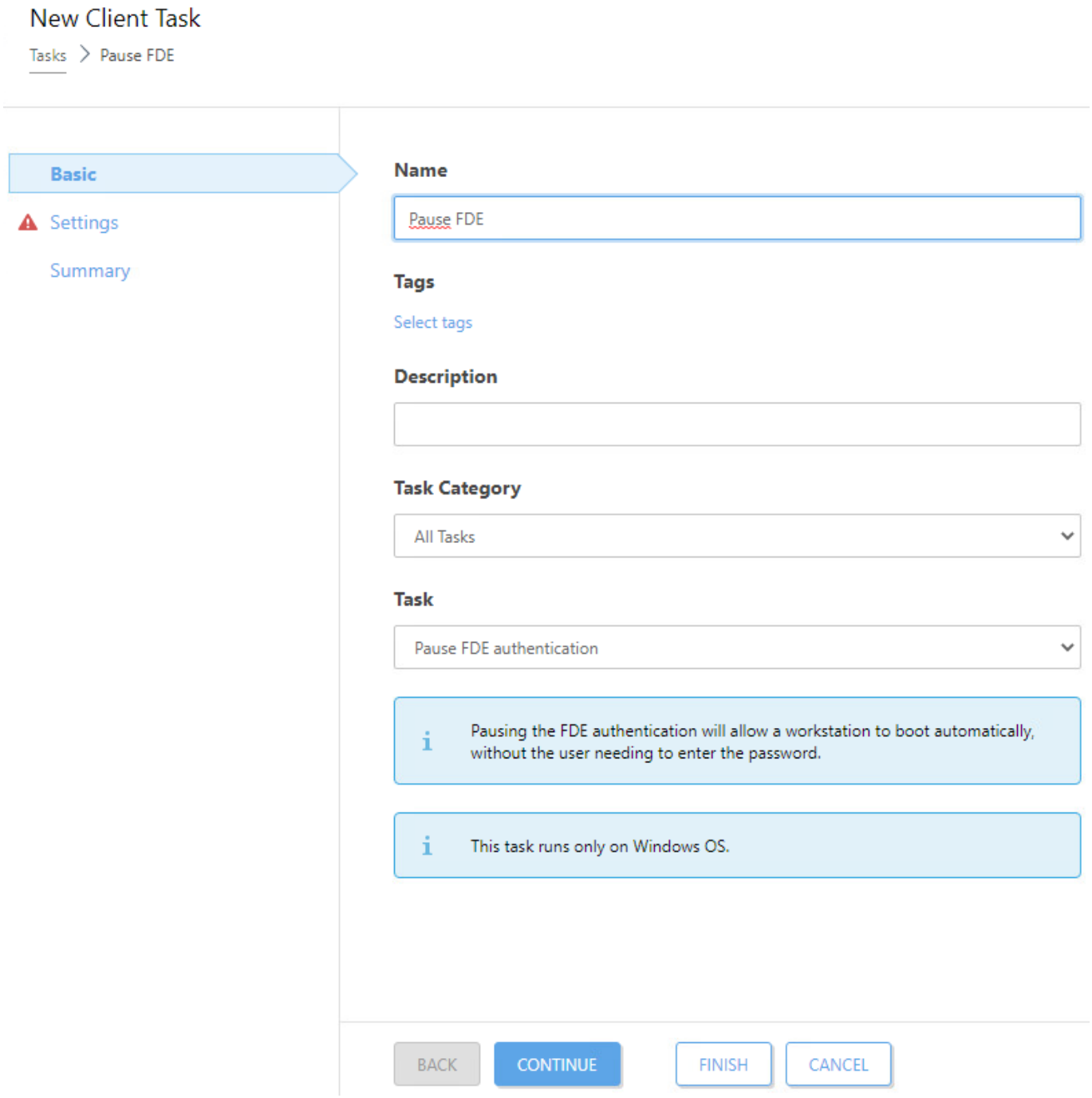
Tato možnost není dostupná v případě spravovaného EFDE pro macOS.

Pokud je na stanici zapnutá možnost **Pozastavit FDE autentifikaci**, při startu systému není ověřování vyžadované a není zajištěna jeho ochrana před útočníky.

Prostřednictvím možnosti **Pozastavit FDE autentifikaci** můžete požadavek na FDE autentifikaci v EFDE zapnout/vypnout nebo dočasně pozastavit.

Jako administrátor můžete použít klientskou úlohu na **pozastavení FDE autentifikace** při příštím restartování počítače.

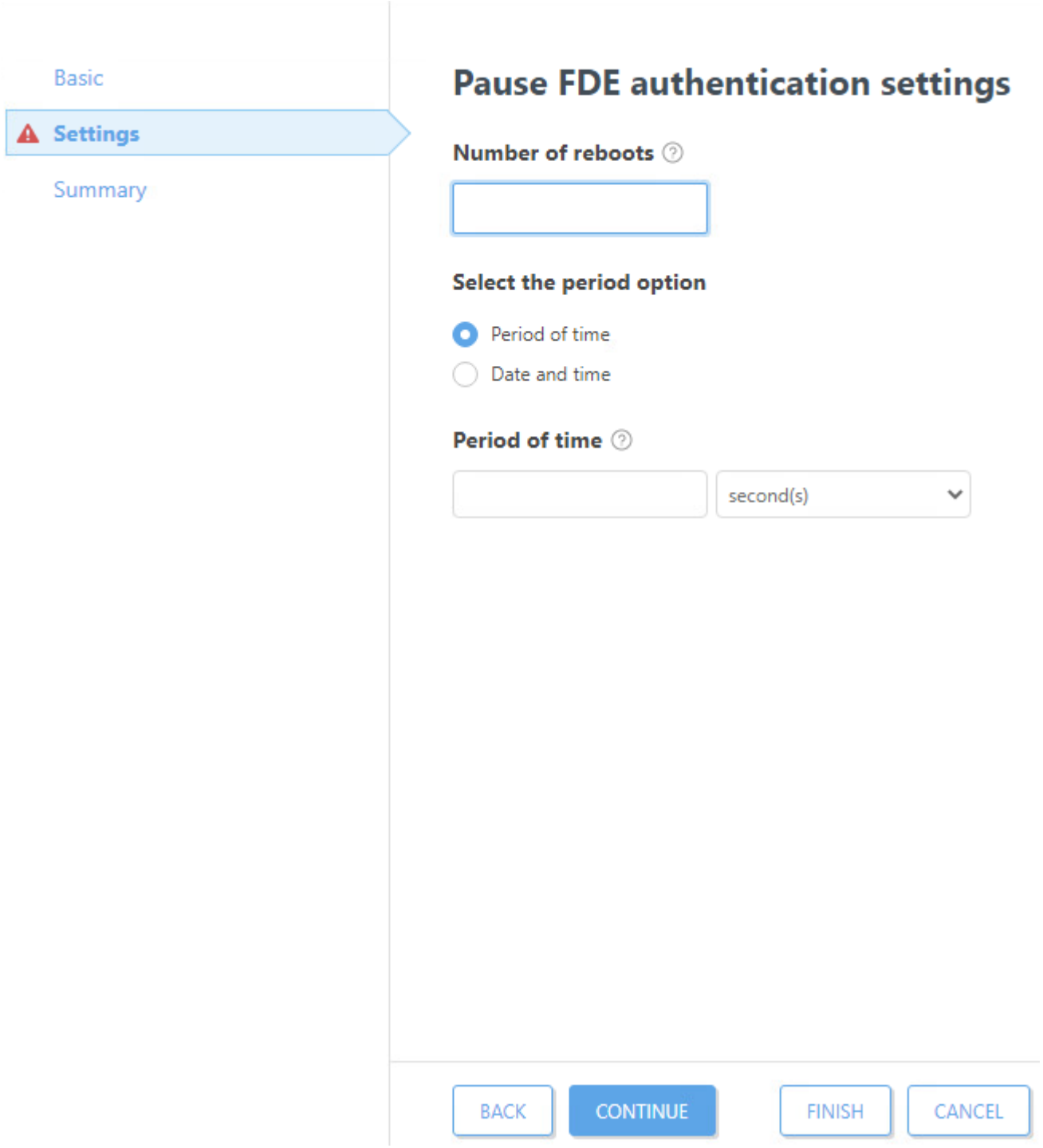
V **konzoli** pro vzdálenou správu ji naleznete v hlavním menu v sekci **Úlohy**, kdy klikněte na tlačítko **Nová** > **Klientská úloha** a jako **typ úlohy** vyberte z rozbalovacího menu **Pozastavit FDE autentifikaci**.



- **Nastavení**:

  o**Počet restartování** – zadejte počet povolených restartování, při kterých uživatel nebude nucen zadat FDE heslo.

  o**Vyberte dobu: Časové období** – definujte časové období (v sekundách, minutách, hodinách nebo dnech) nebo zadejte konkrétní **datum a čas**, po které nebude při restartování vyžadována FDE autentifikace.



Pokud dojde k dosažení jednoho z výše definovaných limitů, FDE autentifikace se opět aktivuje.

Pro obnovení FDE autentifikace před dosažením definovaných limitů/ můžete jako administrátor využít klientskou úlohu **Obnovit FDE autentifikaci**.

Pro trvalé deaktivování FDE autentifikace aplikujte prostřednictvím EFDE politiky možnost **Vypnout FDE autentifikaci**.

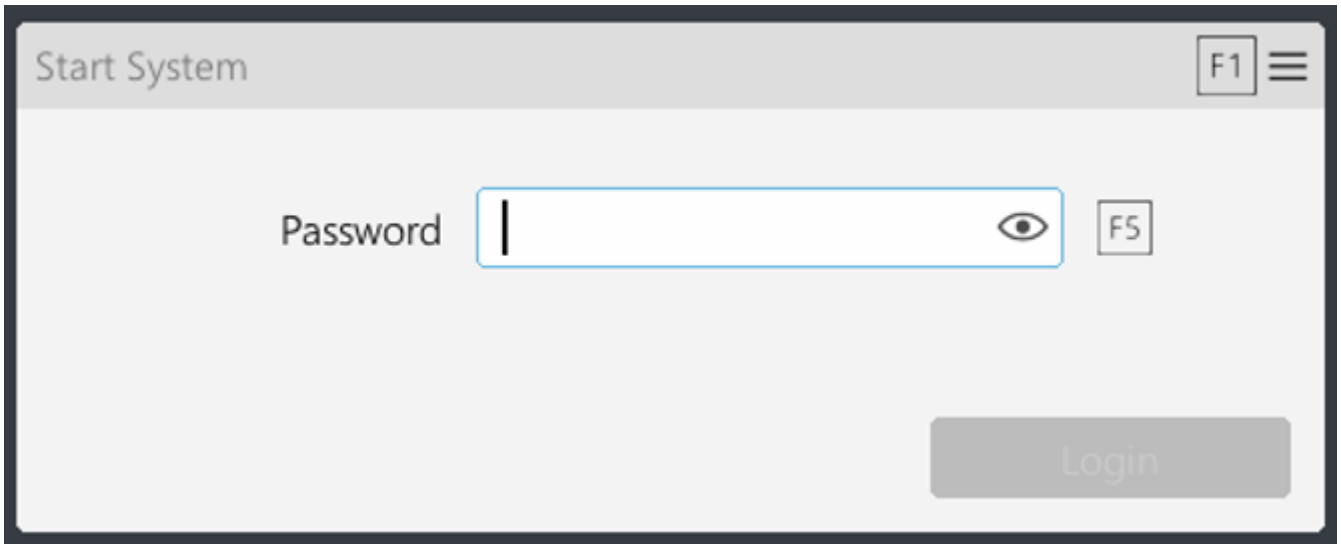
Tuto možnost (**Vypnout FDE autentifikaci**) naleznete v konfigurační šabloně pro EFDE v sekci **Možnosti šifrování** > **Režim Full Disk Encryption**.

Po **deaktivování FDE autentifikace** prostřednictvím EFDE politiky bude vypnutá po celou dobu, kdy bude politika aplikována na stanici. V tomto případě **není možné FDE autentifikaci obnovit** spuštěním klientské úlohy na **Obnovení FDE autentifikace**.

Pre-boot přihlašovací obrazovka

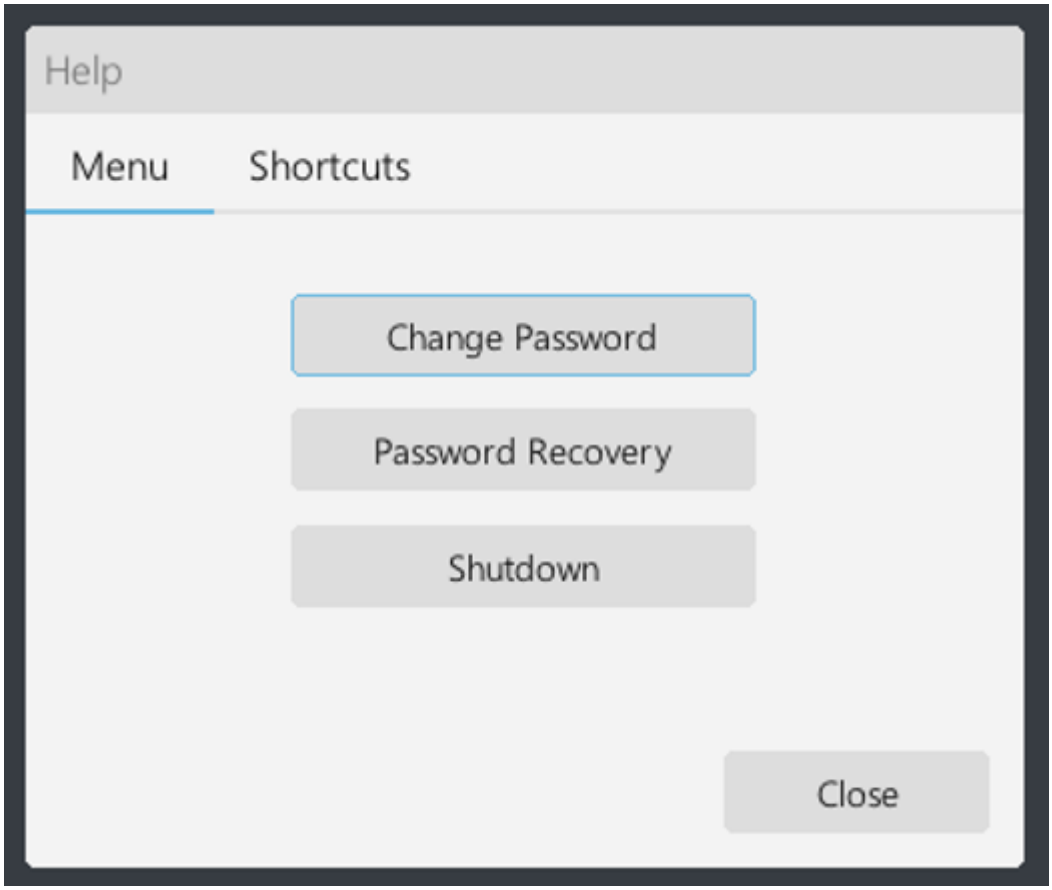
Pokud je produkt aktivován platnou licencí a stanice je zašifrována, při každém jejím spuštění se zobrazí pre-boot přihlašovací obrazovka.

EFDE pre-boot přihlašovací obrazovka představuje bezpečnostní vrstvu, která brání neoprávněnému přístupu k datům uloženým na pracovní stanici.

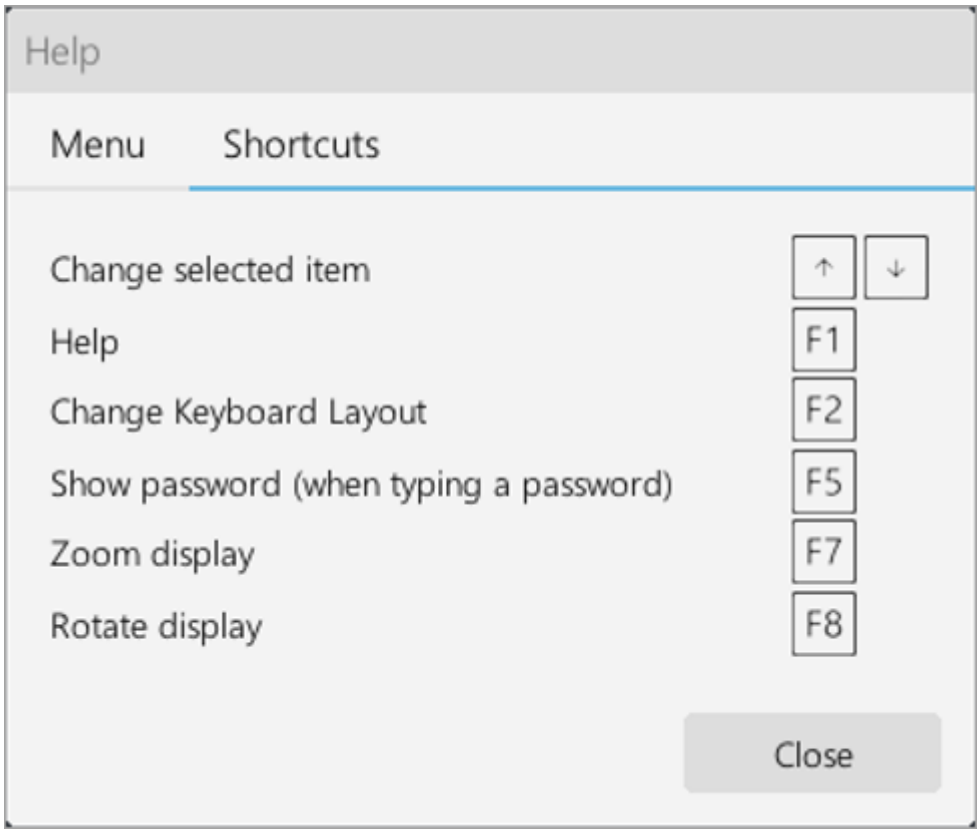


Pro zobrazení menu na pre-boot obrazovce stiskněte klávesu **F1**. Následně získáte možnost pro **Změnu hesla**, inicializaci procesu na obnovení hesla, **vypnutí** počítače a **ukončení** menu.

Pro **zobrazení hesla** můžete na pre-boot obrazovce stisknout klávesu **F5**, případně obrazovku **otočit** pomocí klávesy **F8** (pokud není zobrazena správně).



Zkratky pro použití na pre-boot obrazovce



Klávesové zkratky	
F1	Stisknutím klávesy F1 otevřete nabídku.

Klávesové zkratky	
F2	Stisknutím klávesy F2 změníte rozložení klávesnice používané při pre-bootu FDE. Vybrané rozložení se zobrazí v levém dolním rohu.
F5	Stisknutím klávesy F5 odhalíte zadávané pre-boot heslo.
F7	Stisknutím klávesy F7 upravíte přiblížení.
F8	Stisknutím klávesy F8 otočíte obrazovku.
F10	Stisknutím klávesy F10 vypněte zařízení.

Obnovení šifrování

Proces na obnovení šifrování využije administrátor v případech, kdy se uživatel není schopen přihlásit svým heslem nebo pro dešifrování dat, k nimž není z technických důvodů umožněn přístup.

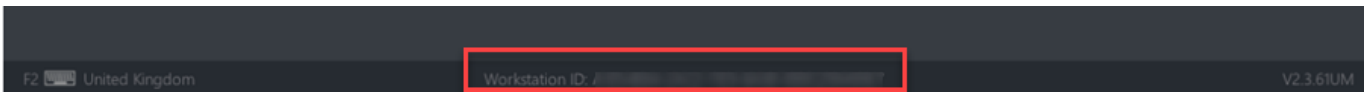
- Obnovení hesla – prostřednictvím tohoto procesu vygeneruje administrátor heslo pro obnovení.
- Obnovení dat – prostřednictvím tohoto procesu vygeneruje administrátor záchranné médium, které použije v případech, kdy není možné získat standardním způsobem přístup k datům uloženým na stanici.

Heslo pro obnovení

Proces na obnovení hesla je nutné inicializovat v případě, kdy uživatel překročil počet pokusů na neúspěšné zadání hesla na pre-boot přihlašovací obrazovce nebo došlo ke spuštění úlohy pro **zablokování FDE hesla**.

> Pokud již nemáte k dispozici další pokusy pro obnovení, proveďte dešifrování ručně.

Pro obnovení je vyžadováno **Workstation ID**. U **ID pracovní stanice** se rozlišují malá a velká písmena. **Workstation ID** je zobrazeno v dolní části pre-boot přihlašovací obrazovky:



Windows

V takovém případě se uživateli na pre-boot obrazovce zobrazí upozornění "Uživatel je deaktivován". Uživatel následně na pre-boot obrazovce musí stisknout klávesu **F1** a z menu vybrat možnost **Obnovení hesla**. V této chvíli uživatel musí kontaktovat administrátora, který mu dokáže vygenerovat heslo pro obnovení. Administrátor může tuto akci provést dvěma způsoby:

Administrátor dokáže identifikovat stanici v konzoli pro vzdálenou správu:

1. V konzoli pro vzdálenou správu si otevřete **Detaily počítače** požadované stanice.
2. Na dlaždici **Šifrování** klikněte na tlačítko **Spravovat** a v kontextovém menu vyberte možnost **Obnovení přístupu** > **Obnovení hesla**.
3. Platné heslo můžete administrátor vygenerovat na základě recovery indexu, který se uživateli zobrazil na obrazovce.
4. Poté, co uživatel použije heslo pro obnovení, bude schopen si změnit své FDE heslo.

Administrátor nedokáže identifikovat stanici v konzoli pro vzdálenou správu:

1. V pravém horním rohu konzole pro vzdálenou správu klikněte na **Nápověda** > **Obnovení šifrování**.
2. V zobrazeném dialogovém okně vyberte možnost **Obnovení hesla**.
3. V tomto bodě nyní administrátor potřebuje od uživatele získat Workstation ID. Workstation ID je zobrazeno v dolní části EFDE pre-boot přihlašovací obrazovky.
4. Po zadání Workstation ID se zobrazí okno pro obnovení hesla.
5. Platné heslo můžete administrátor vygenerovat na základě recovery indexu, který se uživateli zobrazil na obrazovce.
6. Poté, co uživatel použije heslo pro obnovení, bude schopen si změnit své FDE heslo.

macOS

V takovém případě musí uživatel kliknout na ikonu otazníku na přihlašovací obrazovce a následně kliknout na ikonu šipky vedle možnost ".. resetovat, pokud používáte klíč pro obnovení". V této chvíli uživatel musí kontaktovat administrátora, který mu dokáže vygenerovat heslo pro obnovení.



Administrátor může tuto akci provést dvěma způsoby:

Administrátor dokáže identifikovat stanici v konzoli pro vzdálenou správu:

1. V konzoli pro vzdálenou správu si otevřete **Detaily počítače** požadované stanice.
2. Na dlaždici **Šifrování** klikněte na tlačítko **Spravovat** a v kontextovém menu vyberte možnost **Obnovení přístupu** > **Obnovení hesla**.
3. Platné heslo můžete administrátor vygenerovat na základě recovery indexu, který se uživateli zobrazil na obrazovce.
4. Poté, co uživatel použije heslo pro obnovení, bude schopen si změnit své heslo.

Administrátor nedokáže identifikovat stanici v konzoli pro vzdálenou správu:

1. V pravém horním rohu konzole pro vzdálenou správu klikněte na **Nápověda** > **Obnovení šifrování**.
2. V zobrazeném dialogovém okně vyberte možnost **Obnovení hesla**.
3. V tomto bodě nyní administrátor potřebuje od uživatele získat Workstation ID. Workstation ID je zobrazeno v dolní části přihlašovací obrazovky.
4. Po zadání Workstation ID se zobrazí okno pro obnovení hesla.
5. Platné heslo můžete administrátor vygenerovat na základě recovery indexu, který se uživateli zobrazil na obrazovce.
6. Poté, co uživatel použije heslo pro obnovení, bude schopen si změnit své heslo.

Data pro obnovení

Proces pro obnovení šifrování je nutné provést v případě, kdy na stanici spuštěna úloha pro **zneplatnění FDE hesla**, vyskytl se problém se šifrováním nebo EFDE pre-boot přihlášením, případně se nepodařilo obnovit heslo. Tímto procesem dešifrujete disk na pracovní stanici a deaktivujete EFDE pre-boot přihlašovací obrazovku.

Pro obnovení je vyžadováno **Workstation ID**. U **ID pracovní stanice** se rozlišují malá a velká písmena. **Workstation ID** je zobrazeno v dolní části pre-boot přihlašovací obrazovky:

- Všichni uživatelé, kteří mají oprávnění **pro čtení** nad statickou skupinou **Všechna zařízení** (přístup ke všem zařízením) mají také přístup k datům pro obnovení odebraných zařízení.
- Z bezpečnostních důvodů jsou data pro obnovení k dispozici pouze uživatelům s přístupem ke statické skupině **Všechna zařízení**, například pouze globálním správcům.

Administrátor může tuto akci provést dvěma způsoby:

Administrátor dokáže identifikovat stanici v konzoli pro vzdálenou správu:

1. V konzoli pro vzdálenou správu si otevřete **Detaily počítače** požadované stanice.

2. Na dlaždici **Šifrování** klikněte na tlačítko **Spravovat** a v kontextovém menu vyberte možnost **Obnovení přístupu** > **Data pro obnovení**.

Administrátor nedokáže identifikovat stanici v konzoli pro vzdálenou správu:

1. V pravém horním rohu konzole pro vzdálenou správu klikněte na **Nápověda** > **Obnovení šifrování**.

2. V zobrazeném dialogovém okně vyberte možnost **Data pro obnovení**.

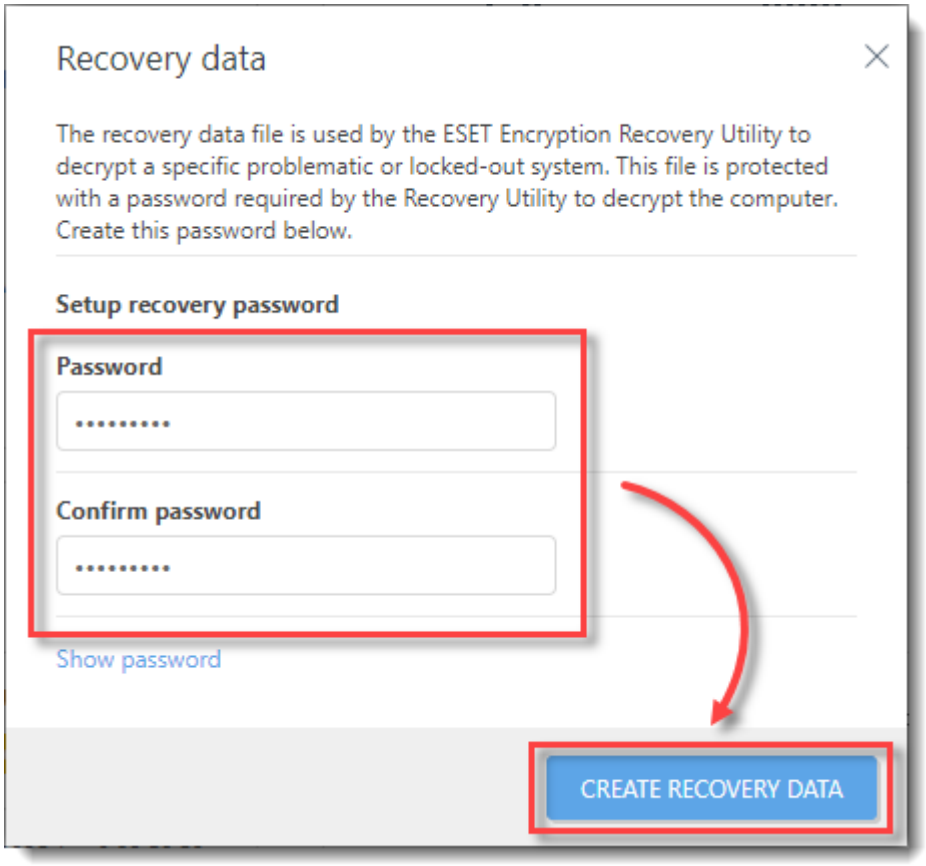
3. V tomto bodě nyní administrátor potřebuje od uživatele získat Workstation ID. Workstation ID je zobrazeno v dolní části EFDE pre-boot přihlašovací obrazovky.

Od tohoto kroku je proces obnovení stejný pro obě výše uvedené možnosti.

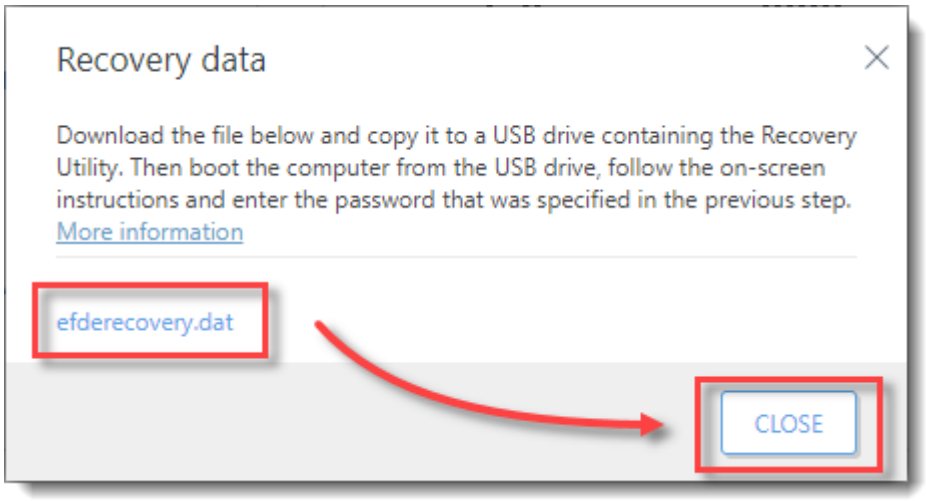
Stažení souboru s daty pro obnovení:

1. V zobrazeném dialogovém okně si vytvořte jednorázové heslo (toto heslo bude platné pouze pro tento konkrétní proces dešifrování).

2. Klikněte na **Vytvořit data pro obnovení** přejděte na další krok.



3. V dalším okně klikněte na `efderecovery.dat` > Stáhnout a uložit soubor. Po dokončení tohoto kroku klikněte na tlačítko **Zavřít**.



Soubor "efderecovery.dat" je unikátní pro každou pracovní stanici a každý proces šifrování. To znamená, že soubor nebude stejný, pokud jste stanici zašifrovali, dešifrovali a znovu zašifrovali.

Windows

ESET Recovery Media Creator

1. Do počítače vložte prvotně USB médium.

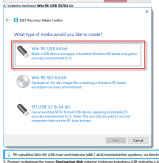
Upozornění na 32-USB jednotky je nadmístnostním se 16/32. (Doklad) vždělí je vyžadování pro nastavení ESET Recovery Media Creator.
Při použití režimu EFI je maximální limit 32 GB. Pokud limit překročíte, ESET Recovery Media Creator vrátí **Chybu vždělí je příliš velký (maximální 32 GB)**.

2. Spusťte ESET Recovery Media Creator.

3. Klikněte nevalže a ověřovacím tlačítkem na tlačítko **Další**.

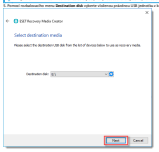


4. Vyberte možnost **Win RE USB 64 bit**

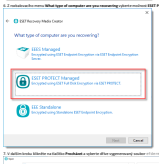


Při vytváření Win RE USB musí uživatelskému účtu v AD existovat lokální účet systému, na kterém jste zahájili vytvoření, odpovídající architektuře obnovovaného systému.

5. Formát médiaotevřete menu **Destination disk** vyberte vloženou jednotku USB jednotku v kroku 1.



6. Z nabídnutého menu **What type of computer are you recovering** vyberte možnost **ESET PROTECT Managed**.

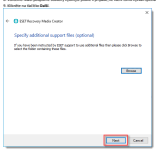


7. V dalším kroku klikněte na tlačítko **Prozkoumat** a vyberte dříve uppercreasovaný soubor

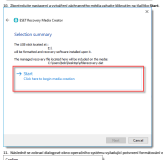


8. Volitelně: Další podpůrné soubory vyžadován pouze v případě, že vám k tomu vyzval specialista technické podpory ESET.

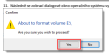
9. Klikněte na tlačítko **Další**.



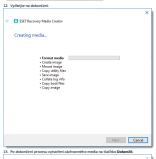
10. Zkontrolujte nastavení a vytvoření záchranného média zahájíte kliknutím na tlačítko **Start**.



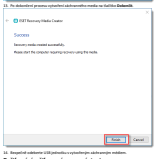
11. Následně se vám otevře dialogové okno operačního systému vyžadující potvrzení formátování vybrané jednotky. Pokračujte kliknutím na tlačítko **Ano**.



12. Vyčkejte na dokončení.



13. Po dokončení procesu vytvoření záchranného média se tlačítko **Dokončit**.



14. Bezpečně odstraňte USB jednotku a vytvořený/ne záchranného zařízení.

Dešifrování zašifrovaná pracovní stanice.

1. Zapněte počítač a spusťte z vytvořeného záchranného systému.
2. Na cílové pracovní stanici je vložte boot manager a jeden smart zařízení vytvořené USB.
3. Vyberte možnost **Decrypt all encrypted disks (EPCE managed recovery file)**



4. Následně se zobrazí upozornění. Přečtěte si zobrazené informace a pokračujte kliknutím na tlačítko **Ano**.



5. Do vzdálenosti pro zadání hesla pro obnovení dříve zašifrované pracovní stanice pro validaci.





Upozornění na dokončení procesu: **NEVYPÍNEJTE ani restartujte/jste použitel ani vám**



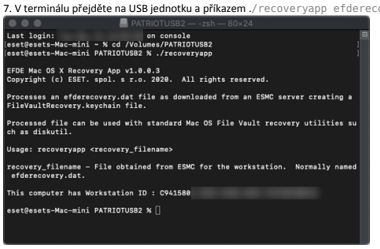
8. Při příštím spuštění pracovní stanice se vyvolá ESET pre-boot obrazovka a systém Windows by se měl spustit normálně.

Na systémech macOS 10.x – 11.x postupujte podle postupu uvedeném v Databázi znalostí v článku Decrypt an Apple computer encrypted with ESET Full Disk Encryption.

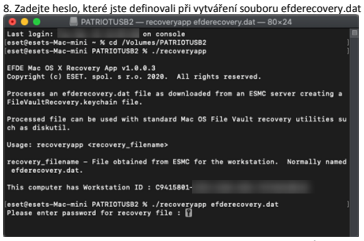
1. Do počítače vložte prázdné USB médium.
2. Stáhněte si Encryption recovery tool pro macOS.
3. Rozbalte obsah souboru staženého v předchozím kroku na USB jednotku.
4. Na USB jednotku dále zkopírujte soubor `efderecovery.dat`.

Pro úspěšné dokončení procesu je vyžadováno uživatelské heslo cílového počítače s operačním systémem macOS. Bez zadaní hesla nebude možné proces dokončit.

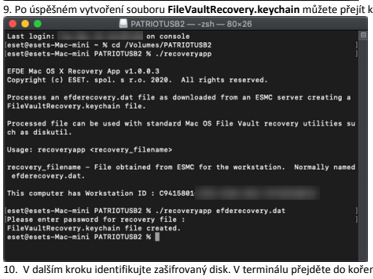
5. Vložte USB jednotku do obnovovaného macOS počítače a při startu počítače přejděte pomocí klávesové zkratky CMD+R do systému **Zotavení macOS**.
6. Zadejte uživatelské heslo a dále klikněte **Nástroje macOS** > **Utility** > **Terminál**.
7. V terminálu přejděte na USB jednotku a příkazem `./recoveryapp efderecovery.dat` vygenerujte soubor **FileVaultRecovery.keychain**.



8. Zadejte heslo, které jste definovali při vytváření souboru efderecovery.dat prostřednictvím konzole pro vzdálenou správu.



9. Po úspěšném vytvoření souboru **FileVaultRecovery.keychain** můžete přejít k dešifrování disku.



10. V dalším kroku identifikujte zašifrovaný disk. V terminálu přejděte do kořenového adresáře a spusťte příkaz `diskutil apfs list`. Tím si zobrazíte seznam APFS svazků.
11. V zobrazeném seznamu najděte svazek s názvem "**Macintosh HD**", u které je uvedeno **Filevault: Yes (Locked)**.

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

12. Poznamenejte si **ID svazku** (například **disk2s1**).
13. Dále níže uvedeným příkazem odemkněte soubor **FileVaultRecovery.keychain**:

```
security unlock-keychain /path/to/FileVaultRecovery.keychain
```

příklad: `security unlock-keychain /Volumes/PatriotUSB/FileVaultRecovery.keychain`

14. Před zahájením dešifrování je nutné dále odemknout svazek. To provedete následujícím příkazem:

```
diskutil apfs unlockVolume /dev/disk2s1
```

, kde nahradíte "**disk2s1**" skutečným ID svazku získaného dříve. Pro pokračování je vyžadováno zadání uživatelského hesla.

15. Od této chvíle je jednotka odemčena a můžete pokračovat v dešifrování disku pomocí klíče pro obnovení vygenerovaného prostřednictvím recoveryapp.

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

16. Pro pokračování v dešifrování spusťte následující příkaz:

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

příklad: `diskutil apfs decryptVolume /dev/disk2s1 –recoverykeychain /Volumes/PatriotUSB/FileVaultRecovery.keychain`

17. Stav dešifrování můžete kdykoli zkontrolovat pomocí příkazu: `diskutil apfs list`

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

18. Po úspěšném dešifrování ukončete terminál a restartujte počítač.

Dešifrování/odinstalace

Před odinstalováním EFDE klienta z klientské stanice je nutné dešifrovat všechny zašifrované jednotky.

Dešifrování:

1. Odeberte všechny EFDE politiky aktuálně přiřazené počítači.
2. Vytvořte novou politiku pro EFDE.
3. V sekci **Možnosti šifrování** > **Režim Full Disk Encryption** deaktivujte pomocí přepínače možnost **Zapnout šifrování**.
4. Uložte politiku a přiřaďte ji stanici, kterou chcete dešifrovat.

5. Po dokončení dešifrování se v **Detailech počítače** změní stav na **Šifrování: neaktivní**.

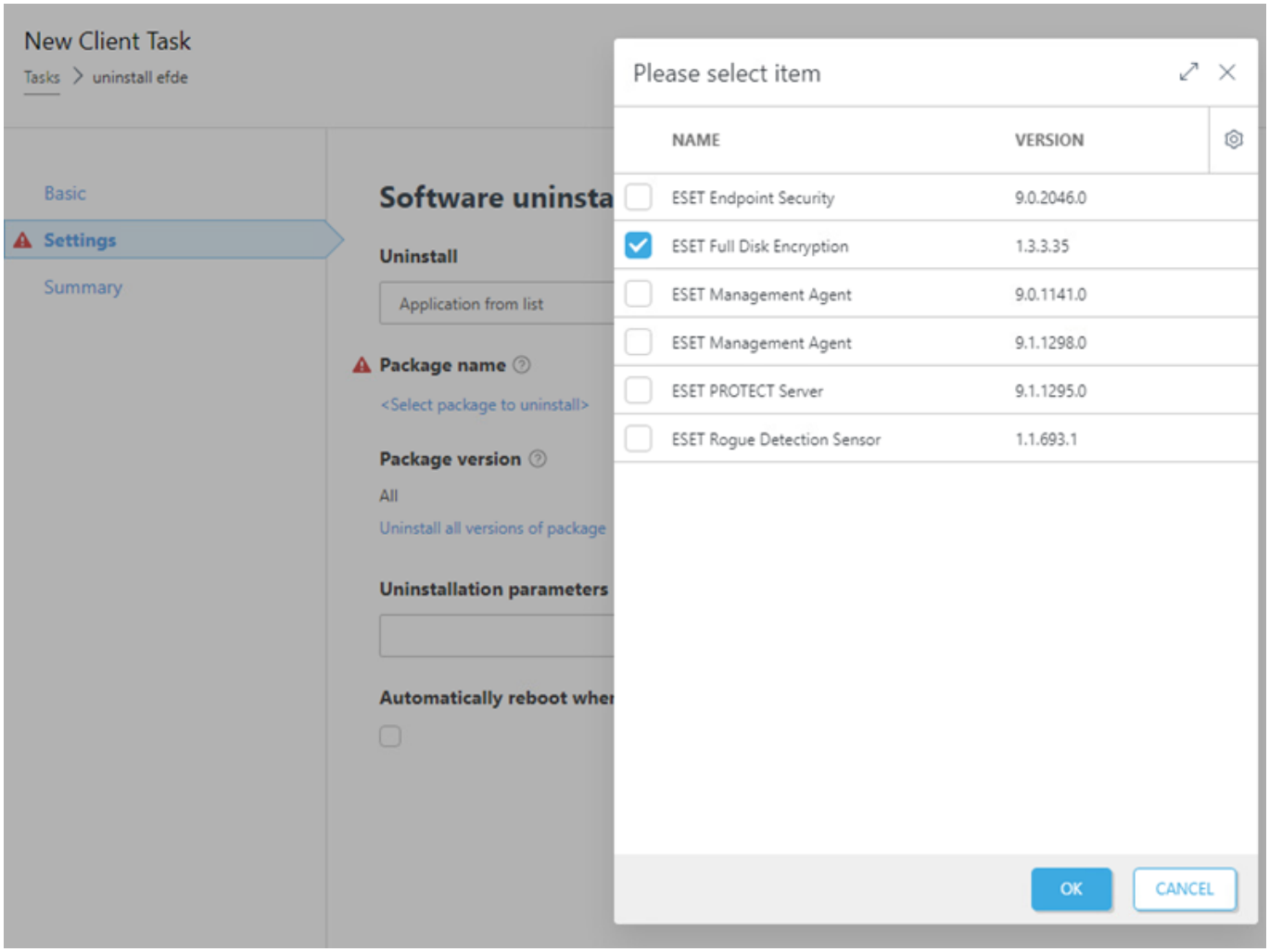
Odinstalace:

Po dešifrování všech jednotek můžete přejít k odinstalaci EFDE klienta.

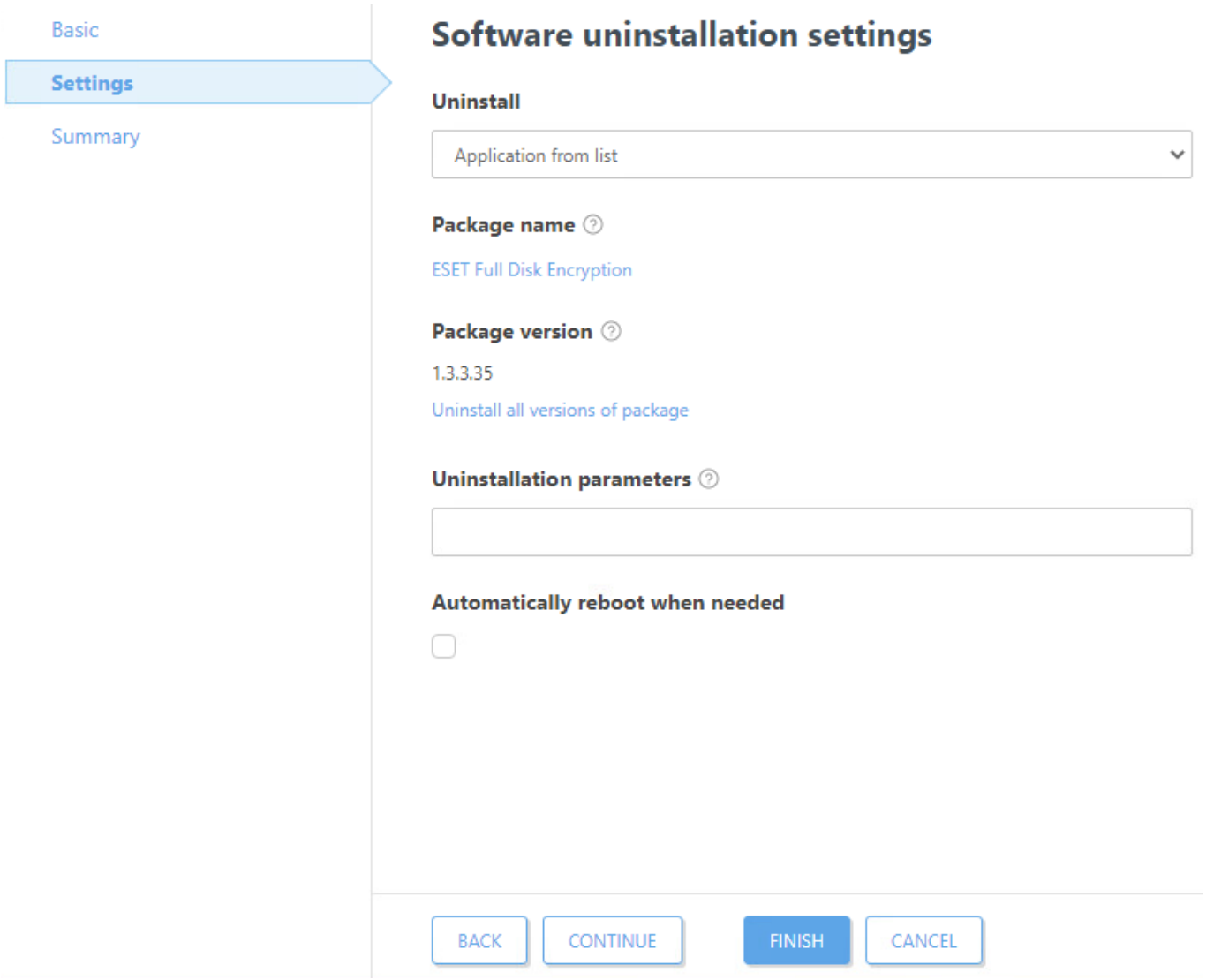
1. Vytvořte novou **klientskou úlohu** na **odinstalaci aplikace**.

2. V sekci **Nastavení** vyberte z rozbalovacího menu možnost **Aplikace ze seznamu**.

3. Klikněte na možnost **Vybrat balíček k odinstalaci** a vyberte **ESET Full Disk Encryption**.



4. Úlohu vytvořte kliknutím na tlačítko **Dokončit** a následně ji spusťte na požadované stanici.



Nejčastější dotazy

Proč jsou stanice, na kterých není nainstalován EFDE, členy dynamických skupin souvisejících s bezpečnostními produkty?

EFDE není považován za bezpečnostní produkt.

Mohu migrovat mezi EFDE a ESET Endpoint Encryption?

Ne. Není možné provést migraci EFDE na ESET Endpoint Encryption a opačně.

Jaké bude pořadí přihlašovacích obrazovek, pokud mám na stanici aktivováno UEFI pre-boot přihlašování?

Nejprve se zobrazí UEFI pre-boot, následně EFDE pre-boot obrazovka.

Mohu ESET Remote Deployment Tool využít pro nasazení EFDE, který je součástí vytvořeného all-in-one

instalačního balíčku?

Ano All-in-one instalační balíček obsahující EFDE je možné nasadit prostřednictvím nástroje pro nasazení.

Existuje v EFDE režim údržby podobně jako v ESET Endpoint Encryption?

Ano. EFDE klient ve verzi 1.2.0.5 a novější podporuje režim údržby.

Pokud při chcete IT oddělení provést údržbu, ale uživatel nechce poskytnout své EFDE heslo, je jedinou možností pro přístup do počítače heslo pro obnovení?

Nikoli. Klient od verze 1.2.0.5 podporuje režim údržby, prostřednictvím kterého můžete dočasně vypnout FDE autentifikaci.

Mohu obnovit data z naformátovaného pevného disku, který byl zašifrován pomocí EFDE?

Ne. Nelze obnovit data naformátovaného pevného disku zašifrovaného pomocí EFDE.

Existuje k EFDE backdoor?

Ne. EFDE lze bootovat pouze za pomocí EFDE hesla.

Řešení problémů

EFDE chyba/upozornění	Vysvětlení
V politice je definováno, že pro zašifrování vašeho počítače musí být použit TPM. Nicméně nemáte žádný vhodný TPM. Vyžadován je TPM 2.0.	V EFDE politice je vynuceno šifrování prostřednictvím TPM. Pokud stanice TPM 2.0 nepodporuje, aplikujte na ni EFDE politiku, ve které nebude vynuceno šifrování s podporou TPM. Pokud stanice TPM 2.0 podporuje a přesto se hlášení stále zobrazuje, pro více informací se podívejte do protokolu produktu.
V politice je definováno, že pro zašifrování vašeho počítače musí být použit Opal, ale jeden nebo více disků nepodporuje Opal 2 protokol.	V EFDE politice je vynuceno šifrování prostřednictvím OPAL. Pokud stanice OPAL nepodporuje, aplikujte na ni EFDE politiku, ve které nebude vynuceno šifrování s podporou OPAL. Pokud stanice Opal podporuje a přesto se hlášení stále zobrazuje, pro více informací se podívejte do protokolu produktu.

EFDE chyba/upozornění	Vysvětlení
Platnost vaší licence vyprší za několik dní a počítač již nebude chráněn. Následně již nebude při spuštění počítače vyžadováno pre-boot heslo a kdokoli bude schopen spustit počítač bez nutnosti se autentifikovat. Prodlužte si platnost licence, zajistěte si aktivní pre-boot autentifikaci a zůstaňte chráněni. Pokud jste si zakoupili novou licenci, aktivujte bezpečnostní produkt ESET novým licenčním klíčem.	Po vypršení platnosti licence se již nezobrazí EFDE pre-boot přihlašovací obrazovka, nicméně data zůstanou stále zašifrována. Stávající licenci si můžete prodloužit nebo stanici dešifrovat prostřednictvím politiky pro dešifrování.
Platnost licence vypršela nebo je neplatná, proto byla pre-boot autentifikace deaktivována.	Bez platné licence zůstanou data ve stanici zašifrována, ale nezobrazí se před přihlášením do Windows EFDE pre-boot přihlašovací obrazovka. Aktivujte produkt platnou EFDE licencí nebo stanici dešifrovat a aplikaci EFDE klienta odinstalujte.
Váš počítač není zašifrován a data v něm uložená nejsou chráněna.	Jedná se o obecné upozornění, které poukazuje na stav, kdy aplikace EFDE klienta na stanici běží, ale data v ní uložená nejsou zašifrována. Pro vyřešení této chyby zapněte a nakonfigurujte EFDE.
Šifrování vašeho počítače se nepodařilo zahájit z důvodu výskytu chyby. Pro více informací se podívejte do systémového protokolu.	Šifrování se nepodařilo zahájit. Další informace naleznete v protokolech aplikace.
Váš počítač je připraven na zahájení šifrování, ale čeká se na konfiguraci pre-boot hesla.	Toto upozornění poukazuje na stav, kdy je vyžadována interakce uživatele. Aby bylo možné pokračovat v procesu šifrování, důrazně doporučujeme nastavit pre-boot hesla před tím, než dojde k dalšímu restartování stanice.
Pro inicializaci bezpečného spuštění k ověření kompatibility hardwaru a firmwaru je vyžadován restart počítače.	Po úspěšném nainstalování EFDE klienta poukazuje toto upozornění na stav, kdy je vyžadován restart stanice pro inicializaci režimu bezpečného spuštění. V průběhu tohoto jednorázového procesu dojde k ověření kompatibility pracovní stanice a zjištění, zda je možné ji prostřednictvím EFDE zašifrovat.
Váš počítač byl restartován a bezpečně spuštěn, ale před dalším restartem nedošlo ke korektnímu spuštění procesu šifrování. K zahájení šifrování tedy nedojde. Pro více informací se podívejte do systémového protokolu.	Navzdory tomu, že v průběhu procesu bezpečného spuštění došlo k ověření, že je hardware a firmware splňuje podmínky pro šifrování, nebude šifrování pokračovat, neboť došlo k restartování stanice před nastavením EFDE pre-boot hesla. V protokolu naleznete uvedenou chybu ve znění: "Předchozí bezpečné spuštění bylo úspěšné, nicméně výsledek je zastaralý, a je nutné znovu spustit režim bezpečného spuštění." Inicializovat bezpečné spuštění můžete třemi způsoby: • V **ESET PROTECT** klikněte u počítače na **Detaily** > **Upozornění** > klikněte na položku **Šifrování se nepodařilo zahájit** > vyberte možnost **Zkusit znovu zašifrovat**. • V **ESET PROTECT** klikněte na položku **Politiky** > změňte **nastavení** politiky: 1.Pro odstranění aktuální politiky spusťte Zapnout šifrování. 2.Pro přidání nové politiky vypněte Zapnout šifrování. 3.Pro obnovení stavu bezpečného spuštění vyčkejte na zpracování požadavku na **EFDE klientovi**. 4.Pro nové přidání původní politiky spusťte Zapnout šifrování. • Odinstalujte a znovu nainstalujte aplikaci **EFDE klienta**.

EFDE chyba/upozornění	Vysvětlení
Produkt byl nainstalován nebo aktualizován na novou verzi, a pro zajištění funkčnosti je vyžadován restart počítače.	Tato chyba se zobrazí po dokončení čerstvé instalace, přeinstalaci nebo aktualizaci produktu. Pro zajištění jeho funkčnosti je vyžadován restart. Po restartování stanice by měla chyba zmizet.
Prezentační režim je zapnutý	Aktivace prezentačního režimu prostřednictvím EFDE politiky představuje potenciální bezpečnostní riziko. Při zapnutém Prezentačním režimu se může stát, že uživatel nebude schopen přistoupit na problematickou nebo nebezpečnou webovou stránku, případně použít takovou aplikaci. Uživateli se nezobrazí žádné vysvětlení nebo varování, protože jsou vypnuté všechny akce vyžadující zásah uživatele.

Protokoly aplikace EFDE klienta naleznete na stanici v níže uvedeném umístění:

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

K vygenerování protokolů pro technickou podporu použijte ESET Encryption Diagnostics tool.

Zásady ochrany osobních údajů

Ochrana osobních údajů je pro společnost ESET, spol. s r. o., se sídlem na adrese Einsteinova 24, 851 01 Bratislava, Slovak Republic, která je zapsaná v Obchodním registru vedeném Okresním soudem Bratislava I, oddíl Sro, vložka číslo 3586/B, IČO: 31333532, jako pro správce údajů („ESET“ nebo „My“) obzvlášť důležitá. Snažíme se dodržovat požadavky na transparentnost, které jsou právně standardizovány v rámci Obecného nařízení EU o ochraně osobních údajů („GDPR“). Abychom dosáhli tohoto cíle, zveřejňujeme tyto Zásady ochrany osobních údajů výhradně za účelem informování našich zákazníků („Koncový uživatel“ nebo „Vy“) jako subjektů údajů o následujících tématech týkajících se ochrany osobních údajů:

- Právní základ pro zpracování osobních údajů
- Sdílení a důvěrnost dat
- Zabezpečení dat
- Vaše práva jako subjektu údajů
- Zpracování vašich osobních údajů
- Kontaktní informace.

Právní základ pro zpracování osobních údajů

Při zpracování dat používáme v souladu s příslušným legislativním rámcem v souvislosti s ochranou osobních údajů jen několik právních základů. Zpracování osobních údajů ve společnosti ESET je potřebné zejména za účelem plnění dokumentu Licenční ujednání s koncovým uživatelem („EULA“) odsouhlaseného s koncovým uživatelem (dle článku 6 (1) (b) nařízení GDPR), který je platný pro poskytování produktů nebo služeb společnosti ESET, pokud není výslovně uvedeno jinak, například:

- Oprávněný zájem: Právní základ (dle článku 6 (1) (f) nařízení GDPR), který nám umožňuje zpracovávat údaje o tom, jak naši zákazníci využívají naše služby a jak jsou s nimi spokojeni, abychom jim mohli poskytnout nejlepší možnou ochranu, podporu a služby. Podle platných právních předpisů je za oprávněný zájem považován i marketing, proto se při marketingové komunikaci s našimi zákazníky obvykle spoléháme na tento koncept.

- Souhlas (dle článku 6 (1) (a) nařízení GDPR): Můžeme jej od vás vyžadovat v konkrétních situacích, kdy považujeme tento právní základ za nejvhodnější, nebo pokud to vyžaduje zákon.
- Splnění zákonné povinnosti (dle článku 6 (1) (c) nařízení GDPR): Například specifikace požadavků na elektronickou komunikaci nebo uchovávání dokumentů souvisejících s fakturací.

Sdílení a důvěrnost dat

Vaše data nesdílíme se třetími stranami. ESET je ale společnost s celosvětovou působností a v rámci naší prodejní, servisní a podpůrné sítě využíváme přidružené firmy a partnery. Informace o licencování, fakturaci a technické podpoře, které společnost ESET zpracovává, mohou být přenášeny k přidruženým firmám nebo partnerům a zpět za účelem plnění smlouvy EULA, jako je poskytování služeb nebo podpora.

Společnost ESET upřednostňuje zpracování svých dat v Evropské unii (EU). V závislosti na vaší poloze (používání našich produktů a/nebo služeb mimo EU) a/nebo službě, kterou jste si zvolili, ovšem může být nutné přenést vaše data do země mimo EU. Služby třetích stran využíváme například ve spojení s cloudovým computingem. V těchto případech si naše poskytovatele služeb pečlivě vybíráme a zajišťujeme příslušnou úroveň ochrany dat prostřednictvím smluvních, ale i technických a organizačních opatření. Je pravidlem, že uzavíráme standardní smluvní klauzule pro EU, ke kterým v případě potřeby přijímáme doplňková smluvní omezení.

U některých zemí mimo EU, jako jsou Spojené království nebo Švýcarsko, již EU uznala srovnatelnou úroveň ochrany dat. Vzhledem ke srovnatelné úrovni ochrany dat nevyžaduje přenos dat do těchto zemí žádnou speciální autorizaci nebo smluvní dohodu.

Zabezpečení dat

Společnost ESET implementuje příslušná technická a organizační opatření k zajištění úrovně bezpečnosti, která odpovídá potenciálním rizikům. Děláme vše, co je v našich silách, abychom zajistili nepřetržitou důvěrnost, integritu, dostupnost a odolnost zpracovatelských systémů a služeb. Pokud však dojde k narušení ochrany údajů, které ohrožuje vaše práva a svobody, jsme připraveni informovat příslušné dozorčí orgány i ohrožené koncové uživatele jakožto subjekty údajů.

Práva subjektu údajů

Práva každého koncového uživatele jsou důležitá a rádi bychom vás informovali, že všichni koncoví uživatelé (z libovolné země v EU nebo mimo ni) mají společností ESET garantována následující práva. Pokud chcete uplatnit svá práva subjektu údajů, můžete nás kontaktovat prostřednictvím formuláře podpory nebo e-mailem na adrese dpo@eset.sk. Za účelem identifikace po vás budeme požadovat následující údaje: Jméno, e-mailová adresa a – pokud jsou k dispozici – licenční klíč nebo číslo zákazníka a afilace společnosti. Neposílejte nám prosím žádné jiné osobní údaje, jako je datum narození. Rádi bychom vás upozornili, že v zájmu zpracování vaší žádosti a za účelem identifikace budeme zpracovávat vaše osobní údaje.

Právo odvolat souhlas. Právo odvolat souhlas lze uplatnit pouze v případě zpracování založeného výhradně na souhlasu. Pokud zpracováváme vaše osobní údaje na základě vašeho souhlasu, máte právo svůj souhlas kdykoli odvolat i bez uvedení důvodu. Vaše odvolání souhlasu bude platné pouze do budoucna a nebude mít vliv na legálnost údajů zpracovaných před odvoláním.

Právo vznést námitku. Právo vznést námitku proti zpracování lze uplatnit v případě zpracování založeného na oprávněném zájmu společnosti ESET nebo třetí strany. Pokud zpracováváme vaše osobní údaje v zájmu ochrany oprávněného zájmu, máte jako subjekt údajů právo kdykoli vznést námitku vůči námi uvedenému oprávněnému zájmu a vůči zpracování vašich osobních údajů. Vaše námitka bude platná pouze do budoucna a nebude mít vliv na zákonnost údajů zpracovaných před vznesením námitky. Pokud vaše osobní údaje zpracováváme pro účely

přímého marketingu, není nutné u námitky uvádět důvody. Platí to rovněž pro profilování, pokud je spojeno s přímým marketingem. Ve všech ostatních případech vás žádáme, abyste nás stručně informovali o svých stížnostech vůči oprávněnému zájmu společnosti ESET na zpracování vašich osobních údajů.

Upozorňujeme vás, že v některých případech jsme i přes odvolání vašeho souhlasu oprávněni dále zpracovávat vaše osobní údaje na jiném právním základě, například za účelem plnění smlouvy.

Právo na přístup. Jako subjekt údajů máte právo kdykoli bezplatně získat informace o vašich údajích, které má společnost ESET uloženy.

Právo na opravu. Pokud si o vás omylem uložíme nesprávné osobní údaje, máte právo na jejich opravu.

Právo na výmaz a právo na omezení zpracování. Jako subjekt údajů máte právo požádat o výmaz nebo o omezení zpracování vašich osobních údajů. Pokud například zpracováváme vaše osobní údaje s vaším souhlasem a vy tento souhlas odvoláte, přičemž neexistuje žádný jiný právní základ (například smlouva), vymažeme vaše osobní údaje okamžitě. Vaše osobní údaje budou rovněž vymazány, jakmile nebudou dále vyžadovány pro uvedené účely na konci období uchovávání.

Pokud vaše údaje využíváme pouze za účelem přímého marketingu a vy odvoláte svůj souhlas nebo vznesete námitku vůči uvedenému oprávněnému zájmu společnosti ESET, omezíme zpracování vašich osobních údajů do té míry, že vaše kontaktní údaje přidáme na naši interní černou listinu, abychom předešli nevyžádanému kontaktování. V ostatních případech budou vaše osobní údaje vymazány.

Upozorňujeme, že může být potřebné, abychom vaše údaje měly uloženy do konce platnosti povinností na uchovávání a období stanovených legislativou nebo dozorčími úřady. Povinnosti na uchovávání a příslušná období mohou také vyplývat ze zákonů Slovenské republiky. Po uplynutí daných lhůt budou příslušné údaje rutinně vymazány.

Právo na přenositelnost dat. Jako subjektu dat vám rádi poskytneme osobní údaje, které o vás společnost ESET zpracovává, ve formátu xls.

Právo podat stížnost. Jako subjekt údajů máte právo kdykoli podat stížnost u dozorčího orgánu. Společnost ESET podléhá regulaci zákonů Slovenské republiky a je vázána právními předpisy o ochraně údajů Evropské unie. Příslušným dozorčím orgánem pro ochranu osobních údajů je Úrad na ochranu osobných údajov Slovenskej republiky, který sídlí na adrese Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Zpracování vašich osobních údajů

Služby poskytované společností ESET implementované v našem produktu jsou poskytovány za podmínek uvedených v dokumentu Licenční ujednání s koncovým uživatelem, ale některé z nich mohou vyžadovat zvláštní pozornost. Rádi bychom vám poskytli další informace o sběru dat spojených s poskytováním našich služeb. Poskytujeme různé služby popsané v Licenčním ujednání s koncovým uživatelem („EULA“) a v produktové dokumentaci. Aby všechny tyto služby fungovaly, potřebujeme shromažďovat následující informace:

Licenční a fakturační údaje. Jméno, e-mailová adresa, licenční klíč a (v některých případech) adresa, afilace společnosti a platební údaje jsou společností ESET shromažďovány a zpracovávány za účely aktivace licence, doručení licenčního klíče, připomenutí konce platnosti, požadavků na podporu, ověření pravosti licence, poskytování našich služeb a dalších oznámení, včetně marketingových zpráv v souladu s příslušnými zákony nebo vaším souhlasem. Společnost ESET má zákonnou povinnost uchovávat fakturační údaje po dobu 10 let, ovšem informace o licencích jsou anonymizovány nejpozději 12 měsíců po skončení platnosti licence.

Aktualizace a další statistiky. Mezi zpracovávané informace patří informace o procesu instalace a vašem počítači,

včetně platformy, na které je náš produkt nainstalován, a údaje o činnostech a funkčnosti našich produktů, jako je operační systém, údaje o hardwaru, ID instalace, ID licencí, IP adresa, adresa MAC a nastavení konfigurace produktu. Tyto informace jsou zpracovávány za účelem poskytování služeb aktualizace a upgradu a za účelem údržby, zabezpečení a vylepšování naší backendové infrastruktury.

Technická podpora. Za účelem poskytování podpory mohou být vyžadovány kontaktní a licenční informace a údaje obsažené ve vašich požadavcích na podporu. V závislosti na kanálu, kterým se nás rozhodnete kontaktovat, můžeme shromáždit vaši e-mailovou adresu, telefonní číslo, informace o licenci, podrobnosti o produktu a popis vašeho případu podpory. Můžete být vyzváni k poskytnutí dalších informací, které usnadní poskytnutí podpory. Údaje zpracovávané za účelem poskytování technické podpory jsou ukládány na dobu 4 let.

Upozorňujeme, že pokud osoba používající naše produkty a služby není koncový uživatel, který si zakoupil produkt nebo službu a uzavřel s námi smlouvu EULA (například zaměstnanec koncového uživatele, člen rodiny nebo osoba, která od koncového uživatele jiným způsobem dostala oprávnění používat produkt nebo službu v souladu se smlouvou EULA), je zpracování údajů prováděno na základě oprávněného zájmu společnosti ESET, jak je definován v článku 6 (1) f) nařízení GDPR, abychom mohli uživateli autorizovanému koncovým uživatelem umožnit používání námi poskytovaných produktů a služeb v souladu se smlouvou EULA.

Kontaktní informace

Pokud byste chtěli uplatnit svá práva jako subjekt údajů nebo máte nějakou otázku či obavy, pošlete nám zprávu na adresu:

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

Licenční ujednání s koncovým uživatelem

Platné od 19. října 2021.

DŮLEŽITÉ UPOZORNĚNÍ: Před stáhnutím, instalací, kopírováním anebo použitím si pozorně přečtěte níže uvedené podmínky používání produktu. **INSTALACÍ, STÁHNUTÍM, KOPÍROVÁNÍM ANEBO POUŽITÍM SOFTWARU VYJADŘUJETE SVŮJ SOUHLAS S TĚMITO PODMÍNKAMI A BERETE NA VĚDOMÍ ZÁSADY OCHRANY OSOBNÍCH ÚDAJŮ.**

Licenční ujednání s koncovým uživatelem

Tato Licenční smlouva s koncovým uživatelem („Smlouva“) uzavřená mezi společností ESET, spol. s r. o., se sídlem Einsteinova 24, 851 01 Bratislava, Slovenská republika, zapsanou v Obchodním rejstříku vedeném Okresním soudem Bratislava I v oddílu Sro, vložka 3586/B, s obchodním registračním číslem 31333532 („ESET“ nebo „Poskytovatel“) a Vámi, fyzickou anebo právnickou osobou („Vy“ anebo „Koncový uživatel”) Vás opravňuje k používání Softwaru definovaného v článku 1 této Smlouvy. Software definovaný v článku 1 této Smlouvy může být uložen na fyzickém datovém nosiči, zaslán elektronickou poštou, stažen z internetu, stažen ze serverů Poskytovatele nebo získán z jiných zdrojů za podmínek a ujednání uvedených níže.

TOTO NENÍ KUPNÍ SMLOUVA, ALE DOHODA O PRÁVECH KONCOVÉHO UŽIVATELE. Poskytovatel zůstává vlastníkem kopie Software a případného fyzického média na kterém se Software dodává v obchodním balení jako

i všech kopií Software na které má Koncový uživatel právo podle této Dohody.

Kliknutím na tlačítko „Přijímám“ nebo „Přijímám...“ při instalaci, stahování, kopírování nebo používání Softwaru vyjadřujete souhlas s podmínkami této Smlouvy a berete na vědomí Zásady ochrany osobních údajů. V případě, že s některými podmínkami této Smlouvy nebo ustanoveními Zásad ochrany osobních údajů nesouhlasíte, ihned klikněte na možnost pro zrušení, zrušte instalaci nebo stahování nebo zlikvidujte, případně vraťte Software, instalační média, průvodní dokumentaci a doklad o nákupu Poskytovateli nebo pracovníkům prodejny, kde jste Software pořídili.

SOUHLASÍTE S TÍM, ŽE VAŠE POUŽÍVÁNÍ SOFTWARE JE ZNAKEM TOHO, ŽE JSTE SI PŘEČETLI TUTO DOHODU, ROZUMÍTE JÍ, A SOUHLASÍTE S TÍM, ŽE JSTE VÁZANÍ JEJÍMI USTANOVENÍMI.

1. **Software**. Pojem „Software“ v této Smlouvě znamená: (i) počítačový program doprovázený touto Smlouvou včetně všech jeho součástí; (ii) obsah disků, médií CD-ROM, médií DVD, e-mailů a jejich všech případných příloh, anebo jiných médií ke kterým je přiložená tato Smlouva včetně Softwaru dodaného ve formě objektového kódu na hmotném nosiči dat, elektronickou poštou nebo staženého prostřednictvím internetu, (iii) se Softwarem související vysvětlující materiály a jakoukoliv dokumentaci, zejména jakýkoliv popis Software, jeho specifikaci, popis vlastností, popis ovládání, popis operačního prostředí ve kterém se Software používá, návod na použití anebo instalaci Softwaru anebo jakýkoliv popis správného používání Software („Dokumentace“), (iv) kopie Softwaru, opravy případných chyb Softwaru, dodatky k Softwaru, rozšíření Softwaru, modifikované verze Softwaru a aktualizace součástí Softwaru, jak jsou dodané, na které Vám Poskytovatel uděluje Licenci ve smyslu článku 3. této Smlouvy. Software se dodává výlučně ve formě objektového spustitelného kódu.

2. **Instalace, počítač a licenční klíč**. Software dodaný na datovém nosiči, zaslaný elektronickou poštou, stažený z internetu, stažený ze serverů Poskytovatele nebo získaný z jiných zdrojů vyžaduje instalaci. Software musíte nainstalovat na správně nakonfigurovaný počítač splňující minimální požadavky uvedené v Dokumentaci. Způsob instalace je popsaný v Dokumentaci. Na počítači, na který Software instalujete, nesmí být nainstalované žádné počítačové programy anebo technické vybavení, které by mohlo Software nepříznivě ovlivnit. Počítačem se rozumí hardware, mimo jiné včetně osobních počítačů, notebooků, pracovních stanic, palmtopů, smartphonů, ručních elektronických zařízení nebo jiných elektronických zařízení, pro který je Software navržen, na který je nainstalován anebo používán. Licenčním klíčem se rozumí jedinečná sekvence symbolů, písmen, čísel nebo zvláštních znaků poskytnutých Koncovému uživateli, aby bylo možné legálně využívat Software, jeho konkrétní verzi nebo prodloužit dobu trvání Licence v souladu s touto Smlouvou.

3. **Licence**. Za předpokladu, že jste souhlasili s podmínkami této Smlouvy a splníte všechna pravidla a ujednání stanovená v těchto podmínkách, Vám Poskytovatel udělí následující práva („Licence“):

a) **Instalace a používání**. Máte nevýhradní a nepřevoditelné, časově omezené právo instalovat Software na pevný disk počítače anebo na jiné podobné médium sloužící na trvalé ukládání dat, instalaci a na ukládání Software do paměti počítačového systému, na vykonávání, na ukládání a na zobrazování Software.

b) **Stanovení počtu licencí**. Právo na použití Software se váže na počet Koncových uživatelů. Jedním Koncovým uživatelem se přitom rozumí: (i) instalace Software na jednom počítačovém systému, anebo (ii) pokud se rozsah licence váže na počet poštovních schránek, potom se rozumí jedním Koncovým uživatelem uživatel počítače, který si pomocí Mail User Agent („MUA“) přebírá elektronickou poštu. Pokud MUA přebírá elektronickou poštu a následně ji automaticky rozděluje vícerým uživatelům potom se počet Koncových uživatelů stanovuje podle skutečného počtu uživatelů, pro které je elektronická pošta rozdělovaná. V případě, že poštovní server vykonává funkci poštovní brány, je počet Koncových uživatelů shodný s počtem uživatelů poštovních serverů, pro které poskytuje tato brána služby. Pokud je jednomu uživateli směřovaný libovolný počet adres elektronické pošty (například pomocí aliasů) a přebírá si je jeden uživatel, a zprávy nejsou automaticky na straně klienta rozdělované pro více uživatelů je potřebná licence pro jeden počítač. Jednu licenci nesmíte současně používat na vícerých počítačích. Koncový uživatel je oprávněn zadávat Licenční klíč do Softwaru pouze v rozsahu, v němž je oprávněn

používat Software v souladu s omezením vyplývajícím z počtu Licencí poskytnutých Poskytovatelem. Licenční klíč je považován za důvěrný. Licenci nesmíte sdílet s třetími stranami nebo povolit třetím stranám používat Licenční klíč, pokud to nepovoluje tato Smlouva nebo Poskytovatel. Pokud je Licenční klíč zneužit, okamžitě informujte Poskytovatele.

c) **Home/Business Edition.** Verzi Home Edition tohoto Softwaru lze používat výlučně v soukromém a/nebo nekomerčním prostředí pouze pro domácí a rodinné použití. Pro použití Softwaru v komerčním prostředí a na mailových serverech, mail relay serverech, mailových branách anebo internetových branách musíte získat Software ve verzi Business Edition.

d) **Trvání Licence**. Vaše právo používat Software je časově omezené.

e) **OEM Software**. Software označovaný jako „OEM“ je vázán na počítač, se kterým jste ho získali. Není ho možné přenést na jiný počítač.

f) **NFR, TRIAL Software.** Software označený jako "Not-for -resale", NFR anebo TRIAL nemůžete převést za protihodnotu anebo používat na jiný účel, jako na předvádění, testování jeho vlastností anebo vyzkoušení.

g) **Zánik licence**. Licence zaniká automaticky uplynutím období na které byla udělená. Pokud nedodržíte kterékoliv ustanovení této Dohody má Poskytovatel právo odstoupit od Dohody bez toho, aby byl dotknutý jakýkoliv nárok anebo prostředek, který má Poskytovatel pro takovýto případ k dispozici. V případě zrušení Licence musíte neprodleně na vlastní náklady Software včetně všech záložních kopií odstranit, zničit nebo vrátit společnosti ESET nebo prodejně či obchodu, od kterých jste Software získali. Po ukončení Licence je Poskytovatel rovněž oprávněn zrušit nárok Koncového uživatele na používání funkcí Softwaru, které vyžadují připojení k serverům Poskytovatele nebo třetích stran.

4. **Funkce sběru dat a požadavky na připojení k internetu.** Software vyžaduje pro správné fungování připojení k internetu a v pravidelných intervalech se připojuje k serverům Poskytovatele anebo serverům třetích stran a provádí související sběr dat v souladu se Zásadami ochrany osobních údajů. Připojení k internetu a související sběr dat jsou potřebné pro fungování Softwaru a pro jeho aktualizaci a upgrade. Poskytovatel je oprávněn vydávat aktualizace nebo upgrade Softwaru („Aktualizace“), avšak není povinen Aktualizace poskytovat. Tato funkce je při standardním nastavení Softwaru zapnutá, proto se Aktualizace nainstalují automaticky, kromě případů, kdy Koncový uživatel automatickou instalaci Aktualizací zakázal. Pro poskytování aktualizací je vyžadováno ověření pravosti Licence včetně informací o počítači anebo platformě, na které je Software nainstalován, v souladu se Zásadami ochrany osobních údajů.

Poskytování jakýchkoli aktualizací může podléhat „Zásadám konce životnosti“, které jsou k dispozici na webu https://go.eset.com/eol_business. Poté, co Software nebo některé z jeho funkcí dosáhnou data konce životnosti definovaného v Zásadách konce životnosti, nebudou poskytovány žádné aktualizace.

Pro účely této Smlouvy je nutné shromažďovat, zpracovávat a ukládat data, která Vás umožňují Poskytovateli identifikovat v souladu se Zásadami ochrany osobních údajů. Tímto berete na vědomí, že Poskytovatel smí kontrolovat pomocí vlastních prostředků, zda Software používáte v souladu s ustanoveními této Smlouvy. Tímto berete na vědomí, že pro účely této Smlouvy je nutné, aby byla vaše data přenášena při komunikaci mezi Softwarem a počítačovými systémy Poskytovatele nebo jeho obchodních partnerů za účelem zajištění funkčnosti Softwaru, ověření oprávnění k používání Softwaru a ochrany práv Poskytovatele.

V souvislosti s uzavřením této Smlouvy jsou Poskytovatel nebo obchodní partneři, kteří jsou součástí jeho distribuční a podpůrné sítě, oprávnění pro účely fakturace a plnění této Dohody přenášet, zpracovávat a uchovávat údaje, které Vás umožní identifikovat v nevyhnutelném rozsahu.

Podrobnosti o ochraně soukromí, ochraně osobních údajů a Vašich práv týkajících se údajů naleznete v Zásadách ochrany osobních údajů, které jsou k dispozici na webu Poskytovatele. Můžete si je také zobrazit z

nabídky nápovědy v Softwaru.

5. **Výkon práv Koncového uživatele.** Práva Koncového uživatele musíte vykonávat osobně anebo prostřednictvím svých případných zaměstnanců. Software můžete použít výlučně jen na zabezpečení své činnosti a na ochranu výlučně těch počítačových systémů, pro které jste získali Licenci.

6. **Omezení práv**. Nesmíte Software kopírovat, šířit, oddělovat jeho části anebo vytvářet od Software odvozená díla. Při používání Software jste povinný dodržovat následovné omezení:

a) Můžete pro sebe vytvořit jedinou kopii Software na médiu určeném na trvalé ukládání dat jako záložní kopii, za předpokladu, že vaše archivní záložní kopie se nebude instalovat anebo používat na jiném počítači. Vytvoření jakékoliv další kopie Software je porušením této Dohody.

b) Software nesmíte používat, upravovat, překládat, reprodukovat, anebo převádět práva na používání Software anebo kopií Software jinak, než je výslovně uvedené v této Dohodě.

c) Software nesmíte prodat, sublicencovat, pronajmout ani zapůjčit a nesmíte jej ani používat k poskytování komerčních služeb.

d) Nesmíte Software zpětně analyzovat, dekompilovat, převádět do zdrojového kódu anebo se jiným způsobem pokoušet získat zdrojový kód Softwaru s výjimkou rozsahu, ve kterém je takovéto omezení výslovně zakázané zákonem.

e) Souhlasíte s tím, že budete používat Software jen způsobem, který je v souladu se všemi platnými právními předpisy v právním systému, ve kterém Software používáte, zejména v souladu s platnými omezeními vyplývajícími z autorského práva a dalších práv duševního vlastnictví.

f) Souhlasíte s tím, že budete Software a jeho funkce používat pouze způsobem, který neomezuje přístup k těmto službám pro ostatní Koncové uživatele. Poskytovatel si vyhrazuje právo omezit rozsah poskytovaných služeb jednotlivým Koncovým uživatelů, aby mohl služby využívat nejvyšší možný počet Koncových uživatelů. Omezením rozsahu služeb se rozumí též úplné ukončení možnosti využívat některé z funkcí Softwaru a odstranění dat a informací o serverech Poskytovatele nebo třetích stran vztahujících se na konkrétní funkce Softwaru.

g) Souhlasíte s tím, že nebudete provádět žádné činnosti zahrnující používání Licenčního klíče, které jsou v rozporu s podmínkami této Smlouvy nebo by vedly k poskytnutí Licenčního klíče jakékoli osobě, která není oprávněna používat tento Software, jako je například převod použitého nebo nepoužitého Licenčního klíče v jakékoliv formě, stejně jako neoprávněná reprodukce nebo distribuce duplikovaných nebo generovaných Licenčních klíčů nebo používání Softwaru v důsledku použití Licenčního klíče získaného z jiného zdroje než od Poskytovatele.

7. **Autorská práva**. Software a všechna práva, zejména vlastnická práva a práva duševního vlastnictví k němu, jsou vlastnictvím společnosti ESET a/anebo jejích poskytovatelů licencí. Tato jsou chráněná ustanoveními mezinárodních dohod a všemi dalšími aplikovatelnými zákony krajiny, ve které se Software používá. Struktura, organizace a kód Software jsou obchodními tajemstvími a důvěrnými informacemi společnosti ESET a/anebo jejích poskytovatelů licencí. Software nesmíte kopírovat, s výjimkou uvedenou v ustanovení článku 6 písmeno a). Jakékoliv kopie, které smíte vytvořit podle této Dohody, musí obsahovat stejná upozornění na autorská a vlastnická práva, jaká jsou uvedená na Software. V případě, že v rozporu s ustanoveními této Dohody budete zpětně analyzovat, dekompilovat, převádět do zdrojového kódu anebo se jiným způsobem pokusíte získat zdrojový kód, souhlasíte s tím, že takto získané informace se budou automaticky a neodvolatelně považovat za převedené na Poskytovatele a vlastněné v plném rozsahu Poskytovatelem od okamžiku jejich vzniku, tím nejsou dotčená práva Poskytovatele spojená s porušením této Dohody.

8. **Výhrada práv**. Všechna práva k Software, kromě práv které Vám jako Koncovému uživateli Software byly

výslovně udělená v této Dohodě, si Poskytovatel vyhrazuje pro sebe.

9. **Víceré jazykové verze, verze pro více operačních systémů, víceré kopie**. V případě jestliže Software podporuje víceré platformy anebo jazyky, anebo jestliže jste získali více kopií Software, můžete Software používat jen na takovém počtu počítačových systémů a v takových verzích, na které jste získali Licenci. Verze anebo kopie Software, které nepoužíváte nesmíte prodat, pronajmout, sublicencovat, zapůjčit anebo převést na jiné osoby.

10. **Začátek a trvání Dohody.** Tato Dohoda je platná a účinná ode dne, kdy jste odsouhlasili tuto Dohodu. Dohodu můžete kdykoliv ukončit tak, že natrvalo odinstalujete zničíte anebo na své vlastní náklady vrátíte Software, všechny případné záložní kopie a všechen související materiál, který jste získali od Poskytovatele anebo jeho obchodních partnerů. Vaše právo používat Software a všechny jeho funkce mohou podléhat Zásadám konce životnosti. Poté, co Software nebo některé z jeho funkcí dosáhnou data konce životnosti definovaného v Zásadách konce životnosti, vaše právo používat Software zanikne. Bez ohledu na způsob zániku této Dohody, ustanovení jejích článků 7, 8, 11, 13, 19 a 21 zůstávají v platnosti bez časového omezení.

11. **PROHLÁŠENÍ KONCOVÉHO UŽIVATELE**. JAKO KONCOVÝ UŽIVATEL UZNÁVÁTE, ŽE SOFTWARE JE POSKYTOVANÝ "JAK STOJÍ A LEŽÍ", BEZ VÝSLOVNÉ ANEBO IMPLIKOVANÉ ZÁRUKY JAKÉHOKOLIV DRUHU A V MAXIMÁLNÍ MÍŘE DOVOLENÉ APLIKOVATELNÝMI ZÁKONY. ANI POSKYTOVATEL, ANI JEHO POSKYTOVATELÉ LICENCÍ, ANI DRŽITELÉ AUTORSKÝCH PRÁV NEPOSKYTUJÍ JAKÉKOLIV VÝSLOVNÉ ANEBO IMPLIKOVANÉ PROHLÁŠENÍ ANEBO ZÁRUKY, ZEJMÉNA NE ZÁRUKY PRODEJNOSTI ANEBO VHODNOSTI PRO KONKRÉTNÍ ÚČEL ANEBO ZÁRUKY, ŽE SOFTWARE NEPORUŠUJE ŽÁDNÉ PATENTY, AUTORSKÁ PRÁVA, OCHRANNÉ ZNÁMKY ANEBO JINÁ PRÁVA TŘETÍCH STRAN. NEEXISTUJE ŽÁDNÁ ZÁRUKA ZE STRANY POSKYTOVATELE ANI ŽÁDNÉ DALŠÍ STRANY, ŽE FUNKCE, KTERÉ OBSAHUJE SOFTWARE, BUDOU VYHOVOVAT VAŠÍM POŽADAVKŮM, ANEBO ŽE PROVOZ SOFTWARE BUDE NERUŠENÝ A BEZCHYBNÝ. PŘEBÍRÁTE ÚPLNOU ZODPOVĚDNOST A RIZIKO ZA VÝBĚR SOFTWARE PRO DOSÁHNUTÍ VÁMI ZAMÝŠLENÝCH VÝSLEDKŮ A ZA INSTALACI, POUŽÍVÁNÍ A VÝSLEDKY, KTERÉ SE SOFTWARE DOSÁHNETE.

12. **Žádné další závazky**. Tato Dohoda nezakládá na straně Poskytovatele a jeho případných poskytovatelů licencí kromě závazků konkrétně uvedených v této Dohodě žádné jiné závazky.

13. **OMEZENÍ ODPOVĚDNOSTI**. V MAXIMÁLNÍ MÍŘE, JAKOU DOVOLUJÍ PLATNÉ PRÁVNÍ PŘEDPISY, V ŽÁDNÉM PŘÍPADĚ NEBUDE POSKYTOVATEL, JEHO ZAMĚSTNANCI ANEBO JEHO POSKYTOVATELÉ LICENCÍ ZODPOVÍDAT ZA JAKÝKOLIV UŠLÝ ZISK, PŘÍJEM ANEBO PRODEJ, ANEBO ZA JAKOUKOLIV ZTRÁTU DAT, ANEBO ZA NÁKLADY VYNALOŽENÉ NA OBSTARÁNÍ NÁHRADNÍHO ZBOŽÍ ANEBO SLUŽEB, ZA MAJETKOVÉ ŠKODY, ZA OSOBNÍ ÚJMU, ZA PŘERUŠENÍ PODNIKÁNÍ, ZA ZTRÁTU OBCHODNÍCH INFORMACÍ, ANI ZA JAKÉKOLIV SPECIÁLNÍ, PŘÍMÉ, NEPŘÍMÉ, NÁHODNÉ, EKONOMICKÉ, KRYCÍ, TRESTNÉ, SPECIÁLNÍ ANEBO NÁSLEDNÉ ŠKODY, JAKKOLIV ZAPŘÍČINĚNÉ, ČI UŽ VYPLYNULY ZE SMLOUVY, ÚMYSLNÉHO JEDNÁNÍ, NEDBALOSTI ANEBO JINÉ SKUTEČNOSTI, ZAKLÁDAJÍCÍ VZNIK ZODPOVĚDNOSTI, VZNIKLÉ INSTALACÍ, POUŽÍVÁNÍM ANEBO NEMOŽNOSTÍ POUŽÍVAT SOFTWARE, A TO I V PŘÍPADĚ, ŽE POSKYTOVATEL ANEBO JEHO POSKYTOVATELÉ LICENCÍ BYLI UVĚDOMĚNÍ O MOŽNOSTI TAKOVÝCHTO ŠKOD. POKUD NĚKTERÉ STÁTY A NĚKTERÉ PRÁVNÍ SYSTÉMY NEDOVOLUJÍ VYLOUČENÍ ZODPOVĚDNOSTI, ALE MOHOU DOVOLOVAT OMEZENÍ ZODPOVĚDNOSTI, JE ZODPOVĚDNOST POSKYTOVATELE, JEHO ZAMĚSTNANCŮ ANEBO POSKYTOVATELŮ LICENCÍ OMEZENÁ DO VÝŠE CENY, KTEROU JSTE ZAPLATILI ZA LICENCI.

14. Žádné ustanovení této Dohody se nedotýká práv strany, které zákon přiznává práva a postavení spotřebitele, pokud je s nimi v rozporu.

15. **Technická podpora**. Technickou podporu poskytuje ESET anebo ním pověřená třetí strana na základě vlastního uvážení bez jakýchkoliv záruk anebo prohlášení. Poté, co Software nebo některé z jeho funkcí dosáhnou data konce životnosti definovaného v Zásadách konce životnosti, nebude poskytována žádná technická podpora. Koncový uživatel je povinný před poskytnutím technické podpory zálohovat všechny jeho existující data, software a programové vybavení. ESET a/anebo ním pověřená třetí strana nepřebírají zodpovědnost za poškození anebo

ztrátu dat, majetku, software anebo hardware anebo ušlý zisk při poskytování technické podpory. ESET a/anebo ním pověřená třetí strana si vyhrazuje právo na rozhodnutí, že řešený problém přesahuje rozsah technické podpory. ESET si vyhrazuje právo odmítnout, pozastavit anebo ukončit poskytování technické podpory na základě vlastního uvážení. Za účelem poskytování technické podpory mohou být vyžadovány informace o licenci, Informace a další údaje v souladu se Zásadami ochrany osobních údajů.

16. **Převod Licence**. Software můžete přenést z jednoho počítačového systému na jiný počítačový systém, pokud to není v rozporu s Dohodou. Pokud to není v rozporu s Dohodou, Koncový uživatel může jednorázově trvale převést Licenci a všechna práva z této Dohody na jiného Koncového uživatele jen se souhlasem Poskytovatele za podmínky, že (i) původní Koncový uživatel si neponechá žádnou kopii Software, (ii) převod práv musí být přímý, tedy z původního Koncového uživatele na nového Koncového uživatele, (iii) nový Koncový uživatel musí přebrat všechna práva a povinnosti, které má podle této Dohody původní Koncový uživatel (iv) původní Koncový uživatel musí odevzdat novému Koncovému uživateli doklady umožňující ověření legality Software jako je uvedené v článku 17.

17. **Ověření pravosti Softwaru.** Koncový uživatel může prokázat nárok na užívání Softwaru jedním z následujících způsobů: (i) na základě certifikátu licence vydaného Poskytovatelem nebo třetí stranou jmenovanou Poskytovatelem, (ii) prostřednictvím písemné licenční smlouvy, byla-li taková smlouva uzavřena, (iii) předložením e-mailu zaslaného Poskytovatelem obsahujícího licenční údaje (uživatelské jméno a heslo). Za účelem ověření pravosti Softwaru mohou být v souladu se Zásadami ochrany osobních údajů vyžadovány Informace o licenci a identifikační údaje Koncového uživatele.

18. **Licencování pro státní orgány a vládu USA**. Software se poskytuje státním orgánům včetně vlády Spojených států amerických s licenčními právy a omezeními popsanými v této Dohodě.

19. **Soulad se zákony o kontrole obchodu**.

a) Nebudete přímo ani nepřímo exportovat, reexportovat, převádět nebo jinak zpřístupňovat Software žádné osobě, používat jej jakýmkoli způsobem nebo se podílet na jakémkoli jednání, které by mohlo mít za následek, že by společnost ESET nebo její holdingové společnosti, její dceřiné společnosti a dceřiné společnosti kterékoli z jejích holdingových společností, jakož i subjekty ovládané jejími holdingovými společnostmi („přidružené společnosti“), porušily nebo podléhaly negativním důsledkům zákonů o kontrole obchodu, které zahrnují

i. zákony, které kontrolují, omezují nebo ukládají licenční požadavky na export, reexport nebo převod zboží, softwaru, technologie nebo služeb, vydané nebo přijaté jakoukoli vládou, státem nebo regulačním orgánem Spojených států amerických, Singapuru, Spojeného království, Evropské unie nebo kteréhokoli z jejích členských států, nebo libovolné země, ve které mají být plněny povinnosti vyplývající z této Dohody, nebo v níž má společnost ESET nebo kterákoli z jejích přidružených společností sídlo nebo je v ní provozována a

ii. jakékoli hospodářské, finanční, obchodní nebo jiné sankce, omezení, embargo, zákaz importu nebo exportu, zákaz převodu finančních prostředků nebo aktiv nebo poskytování služeb nebo rovnocenné opatření uložené jakoukoli vládou, státem nebo regulačním orgánem Spojených států amerických, Singapuru, Spojeného království, Evropské unie nebo kteréhokoli z jejích členských států, nebo libovolné země, ve které mají být plněny povinnosti vyplývající z této Dohody, nebo v níž má společnost ESET nebo kterákoli z jejích přidružených společností sídlo nebo je v ní provozována.

(právní akty uvedené v bodech i. a ii. výše společně jako „zákony o kontrole obchodu“).

b) Společnost ESET má právo pozastavit své závazky podle těchto Podmínek nebo je ukončit s okamžitou platností v případě, že:

i. Společnost ESET rozhodne, že podle jejího opodstatněného názoru Uživatel porušil nebo pravděpodobně poruší ustanovení článku 19 a) Dohody; nebo

ii. Koncový uživatel a/nebo Software podléhají zákonům o kontrole obchodu a v důsledku toho společnost ESET stanoví, že podle jejího opodstatněného názoru by pokračující plnění jejích závazků vyplývajících z Dohody mohlo vést k tomu, že by společnost ESET nebo její přidružené společnosti porušily zákony o kontrole obchodu nebo podléhaly jejich negativním důsledkům.

c) Nic v této Dohodě není zamýšleno a nic by nemělo být interpretováno ani vykládáno tak, aby přimělo nebo nutilo některou ze stran jednat nebo zdržet se jednání (nebo souhlasit s jednáním nebo zdržet se jednání) jakýmkoli způsobem, který je v rozporu s platnými zákony o kontrole obchodu nebo je jimi penalizován či zakázán.

20. **Oznámení**. Veškerá oznámení a vrácení Softwaru a Dokumentace je nutné doručit na adresu ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic. Tím není dotčeno právo společnosti ESET sdělovat Vám jakékoli změny této Dohody, Zásad ochrany osobních údajů, Zásad konce životnosti a Dokumentace v souladu s čl. 22 této Dohody. Společnost ESET Vám může posílat e-maily, oznámení v aplikaci prostřednictvím Softwaru nebo zveřejňovat komunikaci na našich webových stránkách. Souhlasíte s tím, že od společnosti ESET obdržíte právní sdělení v elektronické podobě, včetně jakýchkoli sdělení o změně podmínek, zvláštních podmínek nebo zásad ochrany osobních údajů, jakéhokoli návrhu/přijetí smlouvy nebo pozvánek k jednáním, oznámení nebo jiných právních sdělení. Tato elektronická komunikace se považuje za přijatou písemně, pokud platné právní předpisy výslovně nevyžadují jinou formu komunikace.

21. **Rozhodující právo**. Táto Dohoda se řídí a musí být vykládána v souladu se zákony Slovenské republiky s vyloučením ustanovení o kolizi právních norem. Koncový uživatel a Poskytovatel se dohodli, že kolizní ustanovení rozhodujícího právního řádu a Dohod OSN o smlouvách při mezinárodní koupi zboží se nepoužijí. Výslovně souhlasíte, že řešení jakýchkoliv sporů anebo nároků z této Dohody vůči Poskytovateli anebo spory a nároky související s používáním software je příslušný Okresní soud Bratislava V a výslovně souhlasíte s výkonem jurisdikce tímto soudem.

22. **Všeobecná ustanovení**. V případě, že jakékoliv ustanovení této Dohody je neplatné anebo nevykonatelné, neovlivní to platnost ostatních ustanovení Dohody. Ta zůstanou platná a vykonatelná podle podmínek v ní stanovených. Tato Dohoda byla uzavřena v angličtině. V případě, že je pro pohodlí uživatelů nebo pro jiný účel vyhotoven překlad této Dohody, nebo v případě rozporů mezi jazykovými verzemi této Dohody je rozhodující anglická verze.

Společnost ESET si vyhrazuje právo kdykoli provést změny Softwaru a úpravy této Dohody, jejích příloh, dodatků, Zásad ochrany osobních údajů, Zásad konce životnosti a Dokumentace nebo jakýchkoli jejich částí, a to aktualizací příslušného dokumentu (i) tak, aby se do něj promítly změny týkající se Softwaru nebo změny způsobu podnikání společnosti ESET, (ii) z právních, regulačních nebo bezpečnostních důvodů nebo (iii) s cílem zabránit zneužití nebo poškození. O jakékoli změně Dohody budete informováni e-mailem, oznámením v aplikaci nebo jinými elektronickými prostředky. Pokud nesouhlasíte s navrhovanými změnami Dohody, můžete ji vypovědět v souladu s čl. 10 do 30 dnů od obdržení oznámení o změně. Pokud Dohodu v této lhůtě nevypovíte, budou navrhované změny považovány za přijaté a vstoupí vůči Vám v platnost ode dne, kdy jste obdrželi oznámení o změně.

Tato Dohoda mezi Vámi a Poskytovatelem představuje jedinou a úplnou Dohodu vztahující se na Software, a plně nahrazuje jakékoliv předcházející prohlášení, jednání, závazky, zprávy anebo reklamní informace, týkající se Software.

EULAID: EULA-PRODUCT; 3537.0