ESET Mobile Security

Uživatelská příručka

Klikněte sem pro zobrazení online verze tohoto dokumentu

Copyright ©2023 ESET, spol. s r.o.

ESET Mobile Security 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. 2023-03-19

1 Představení 1
1.1 Co je nového? 1
1.2 Minimální systémové požadavky 1
2 Instalace 2
3 Průvodce prvotním spuštěním 3
4 Verze produktové licence 5
5 Aktivace 6
6 Odinstalace 7
7 Připojení k ESET HOME 7
8 Antivirus 10
8.1 Protokoly kontrol 11
8.2 Rozšířená nastavení 12
8.3 Adware Detector 13
9 Bezpečnostní přehled 13
10 Protokol aktivity 15
11 Anti-Theft 15
11.1 Nastavení Anti-Theft 17
11.2 SMS příkazy 18
11.3 Optimalizace 18
11.4 Webový portál 19
11.5 Důvěryhodné kontakty 19
11.6 Heslo k ESET HOME 20
12 Anti-Phishing 21
13 Zámek aplikace 22
13.1 Zapomenutý PIN k Zámku aplikace 23
14 Ochrana plateb 24
15 Filtr hovorů 25
15.1 Přidání nového pravidla 25
16 Strážce sítě 26
17 Bezpečnostní audit 27
17.1 Monitorování zařízení 27
17.2 Audit aplikací 28
18 Nastavení 28
19 Technická podpora 29
20 Licenční ujednání s koncovým uživatelem 29
21 Zásady ochrany osobních údajů 37

Představení

ESET Mobile Security je komplexní bezpečnostní řešení, které chrání mobilní zařízení před novými hrozbami a podvodnými stránkami, a také umožňuje vzdáleně převzít kontrolu nad zařízením v případě ztráty nebo odcizení.

Mezi hlavní přednosti patří:

- Antivirus
- Anti-Theft
- Anti-Phishing
- Integrace s portálem ESET HOME
- Filtr hovorů
- Bezpečnostní audit
- Bezpečnostní přehled
- Strážce sítě
- Zámek aplikace
- Ochrana plateb

Co je nového?

Nové funkce v ESET Mobile Security verze 7:

Vylepšení

- Nový design domovské obrazovky
- Nový design hlavního menu

Minimální systémové požadavky

Pro instalaci aplikace ESET Mobile Security musí zařízení s operačním systémem Android splňovat níže uvedené minimální systémové požadavky.

- Operační systém: Android 6 (Marshmallow) nebo novější
- Rozlišení dotykového displeje: minimálně 240x320 px
- CPU: 500+ MHz ARM s instrukční sadou ARMv7+
- RAM: 512+ MB

- Připojení k internetu

Podpora specifických zařízení

- Dual SIM zařízení a zařízení s rootem nejsou podporována. Funkce Anti-Theft a Filtr hovorů nejsou k dispozici u tabletů nepodporujících volání a zasílání zpráv.
- Android Go není podporován.
- Pro správnou funkci ESET Mobile Security je třeba využívat služeb Google Play. Na zařízeních Huawei bez služeb Google Play není ESET Mobile Security podporovaný.
- Funkce Anti-Theft (důvěryhodné SIM karty a SMS příkazy) nejsou dostupné na zařízeních CDMA a zařízeních, které nepodporují zasílání SMS zpráv.
- Dostupnost některých funkcí závisí na verzi OS.

Instalace

Pro stažení ESET Mobile Security z webových stránek společnosti ESET ťukněte na uvedený odkaz:

Alternativou pro stažení je kliknutí na odkaz nebo oskenování zobrazeného QR kódu:

Případně využijte našeho průvodce instalací (článek nemusí být dostupný ve všech jazycích).

Ruční instalace produktu prostřednictvím .APK balíčku bude vyžadovat povolení pro instalaci aplikací z neznámých zdrojů. Více informací naleznete v článku Databáze znalostí Instalace .APK souboru ESET Mobile Security pro Android (článek nemusí být dostupný ve všech jazycích).

Po stažení .APK balíčku aplikace ESET Mobile Security na něj ťukněte a vyberte možnost Instalovat. Po dokončení instalace produktu ESET Mobile Security a jeho spuštění se zobrazí průvodce prvotním spuštěním.

Pro ochranu vašich osobních dat uložených v Android zařízení potřebuje aplikace ESET Mobile Security přístup k mnoha funkcím systému, aby mohla v některých případech převzít kontrolu nad zařízením. Přehled všech

oprávnění, která aplikace vyžaduje společně s vysvětlením, k čemu je potřebuje, naleznete v naší databázi znalostí ESET Mobile Security for Android FAQ (článek nemusí být dostupný ve všech jazycích).

Průvodce prvotním spuštěním

Po dokončení instalace postupujte podle pokynů zobrazených v Průvodci prvotním spuštěním:

Udělení požadovaných oprávnění pro ESET Mobile Security

Tento průvodce zmiňuje postup pro běžná zařízení s operačním systémem Android. Nastavení mohou být různá v závislosti na výrobci zařízení.

1. Ťuknutím do nabídky vyberte **zemi**, ve které se převážně nacházíte.

2. Ťuknutím do nabídky vyberte **jazyk**, ve kterém chcete aplikaci používat. Jazyk můžete kdykoli změnit v nastavení aplikace.

3. Abyste mohli pokračovat, ťuknutím na tlačítko **Další** udělte souhlas s Licenčním ujednáním s koncovým uživatelem a Zásadami ochrany osobních údajů.

4. Pokud souhlasíte s následujícími možnostmi, zaškrtněte je a ťukněte na **Další**:

- Systém zpětné vazby **ESET LiveGrid©** Více informací o **ESET LiveGrid©** naleznete v kapitole Rozšířená nastavení.
- **Chci dostávat informace o slevách a nových produktech ESET**.

5. Pro připojení svého mobilního zařízení a aktivaci ESET Mobile Security se přihlaste se ke svému účtu ESET HOME.

Přihlášení pomocí Google

a.Přihlaste se ke svému účtu Google nebo jej vyberte ze seznamu nabídnutých účtů.

b.Pokud se účtem Google připojujete k již existujícímu účtu ESET HOME poprvé, budete za účelem ověření vyzváni k zadání hesla ke svému účtu ESET HOME. Ťukněte poté na **Potvrdit heslo**.

Přihlášení pomocí Apple ID

a.Zadejte e-mailovou adresu a heslo ke svému Apple ID.

b.Ťukněte na **Přihlásit se**.

c.Zadejte kód zaslaný na vaše zařízení Apple.

d.Ťukněte na **Pokračovat**.

e.Pokud důvěřujete zařízení, na kterém operaci provádíte, klikněte na **Důvěřovat**.

f.Pro přístup do ESET HOME prostřednictvím Apple ID klikněte na **Pokračovat**.

g.Ťukněte v levém horním rohu na ikonu **X** pro návrat do ESET Mobile Security.

Naskenovat QR kód

Tato možnost vyžaduje k přihlášení druhé zařízení s nainstalovanou aplikací ESET HOME.

a.Na druhém zařízení si otevřete aplikaci ESET HOME.

b.Ťukněte na tlačítko menu .

c.Tap **Scan a QR code**.

d.Ťukněte na **Naskenujte QR kód**. Aplikace vás může vyzvat, abyste ESET HOME povolili přístup k fotografiím a nahrávání videí. Ťukněte na **Při používání aplikace** nebo **Pouze tentokrát**.

e.Pomocí svého zařízení naskenujte QR kód.

f.Ťukněte na **Připojit zařízení**.

Přihlášení pomocí e-mailové adresy

Zadejte svůj e-mail a heslo.

Ťukněte na **Přihlásit se**.

Pokud jste se přihlásili ke svému účtu ESET HOME, pojmenujte si své zařízení. Tím jej snadněji identifikujete na portále ESET HOME. Zadejte název a ťukněte na tlačítko **Další**.

Pokud nemáte založený účet ESET HOME nebo k němu aktuálně nechcete zařízení připojit, ťukněte na tlačítko **Přeskočit**. Zařízení můžete k účtu připojit kdykoli později pomocí aplikace ESET Mobile Security.

Pokud se rozhodnete přeskočit tento krok, požádáme vás a uvedení e-mailové adresy, kterou chcete použít pro registraci licence ESET a komunikaci s technickou podporu. Ťukněte na nabídku pro výběr e-mailové adresy a cílovou adresu vyberte nebo ťukněte na **Přidat účet**. Ze seznamu vyberte požadovaný účet nebo ťukněte na **Přidat účet** a přidejte si do zařízení další e-mailový účet. Pro pokračování ťukněte na **OK**. Pokud chcete použít e-mailový účet bez toho, aniž byste jej přidali do svého zařízení, ťukněte na tlačítko **Další** > **Zrušit**. Tuto akci opakujte dvakrát. Zadejte svůj e-mail a pokračujte ťuknutím na **Vybrat**.

6. Poslední krok průvodce prvotním spuštěním je rozdílný v závislosti na verzi operačního systému Android nainstalovaném na vašem zařízení.

Android 6-10

a.Chcete-li povolit kontrolu svého zařízení, je třeba aplikaci ESET Mobile Security udělit několik oprávnění. V dalším kroku vás informujeme, jaká oprávnění potřebuje aplikace ESET Mobile Security ke svému běhu. Pro postup dále ťukněte na **Pokračovat**.

b.Ťukněte na **Povolit** pro udělení přístupu. Pokud ťuknete na **Odmítnout**, ESET Mobile Security nebude kontrolovat zařízení na možný výskyt hrozeb do té doby, než oprávnění povolíte, a bude zobrazovat oznámení o bezpečnostním riziku.

Android 11 a novější

a.Ťukněte na **Pokračovat**.

b.Vyberte ESET Mobile Security.

c.Ťukněte na přepínač vedle ESET Mobile Security.

d.Průvodce prvotním spuštěním je kompletní. Ťukněte na **Spustit prvotní kontrolu**.

Ochrana před vybitím

Mnoho výrobců mobilních telefonů nabízí v operačním systému Android 6 a vyšším Ochranu před vybitím. Tato funkce vypíná Anti-Phishing ESET Mobile Security při nízkém stavu baterie, pokud byl zapnut. Tato funkce vypíná Anti-Phishing při nízkém stavu baterie, pokud byl zapnutý. Aby zůstal Anti-Phishing zapnutý, vytvořte pro tuto funkci ESET Mobile Security výjimku. K vytvoření výjimky se, prosíme, podívejte do návodu k použití vašeho zařízení.

Verze produktové licence

ESET Mobile Security můžete používat ve třech verzích:

- Bezplatná verze – máte na neomezenou dobu přístup ke všem bezplatným funkcím.
- Zkušební verze – máte na omezenou dobu (standardně 30 dní) přístup ke všem prémiovým funkcím. Zkušební licence se aktivuje automaticky při prvotním nainstalování aplikace na váš Google Play účet.
- Premium verze – máte přístup ke všem prémiovým funkcím po celou dobu platnosti své licence

Níže uvádíme srovnání funkcí, které jsou dostupné v bezplatné a zkušební/premium verzi aplikace:

	Bezplatná	Zkušební a Premium
Antivirus	✔	✔
Antivirus – automatické kontroly		✔
Automatická aktualizace detekčních modulů		✔
Zámek aplikace		✔
Anti-Theft – SMS příkazy		✔
Anti-Theft – webový portál		✔
Anti-Theft – ochrana SIM karty		✔
Strážce sítě		✔
Anti-Phishing		✔
Filtr hovorů		⍰ (dostupné na OS Android 6 a novějším)
Ochrana plateb		✔
Bezpečnostní audit		✔
Bezpečnostní přehled	✔	✔

Pro aktivaci aplikace ESET Mobile Security ťukněte v hlavním okně na ikonu menu  (případně stiskněte tlačítko

MENU na svém zařízení) a vyberte možnost **Licence**.

ESET Mobile Security můžete aktivovat několika způsoby.

- **Přejít na Premium** – tuto možnost vyberte, pokud si chcete zakoupit licenci prostřednictvím Google Play.

- **Zadat licenční klíč** – tuto možnost vyberte, pokud již máte zakoupenou licenci. Licenční klíč je unikátní řetězec znaků ve formátu XXXX-XXXX-XXXX-XXXX-XXXX, který slouží pro identifikaci vlastníka licence a aktivaci programu. Licenční klíč jste obdrželi na e-mail, který jste zadali během online nákupu. V případě krabicové verze jej naleznete na licenčním štítku.

- **Mám uživatelské jméno a heslo. Co mám dělat?** – pokud máte pouze uživatelské jméno a heslo, získáte licenční klíč zadáním údajů na stránce https://home.eset.com/convert

Aktivace

Abyste mohli využívat prémiové funkce ESET Mobile Security, je nutné aplikaci aktivovat pomocí licenčního klíče.

Zatím nemám licenci

1. Ťukněte na tlačítko menu ☰ pro zobrazení hlavního menu.

2. Na hlavní obrazovce ESET Mobile Security ťukněte na tlačítko **Přejít na premium** (případně akční slevu) a **Zakoupit licenci**.

3. Následně budete přesměrováni na webové stránky společnosti ESET.

4. Zakupte si licenci šitou na míru svým potřebám v našem e-store ESET.

5. Na e-mailovou adresu uvedenou v objednávce obdržíte licenční klíč. Poté pokračujte podle níže uvedených kroků.

Již mám licenci

Připojte své zařízení k ESET HOME a aktivujte ESET Mobile Security licencí spárovanou s ESET HOME.

Pro připojení svého zařízení k ESET HOME a aktivaci ESET Mobile Security si přečtěte kapitolu Připojení k ESET HOME.

Aktivace ESET Mobile Security bez ESET HOME

1. V hlavním menu aplikace ESET Mobile Security ťukněte na možnost **Přejít na premium** a **Již mám licenci**.

2. Ťukněte na **Vložit licenční klíč**.

3. Do zobrazeného pole zadejte licenční klíč a ťukněte na tlačítko **Aktivovat**.

4. Po ověření licence se zobrazí informace: **Aktivace byla úspěšná**. Ťukněte na **Dokončit**.

Odinstalace

Pro odinstalování ESET Mobile Security použijte **Průvodce odinstalací**.

1.Ťukněte na ikonu menu .

2.Ťukněte na **Nastavení**.

3.Ťukněte na **Odinstalovat**.

4.Pokud je ochrana Anti-Theft zapnutá, budete požádáni o zadání bezpečnostního PINu/vzoru do ESET Mobile Security nebo o otisk prstu.

5.Ťukněte na **Odinstalovat**.

V případě, že se vám aplikace nedaří standardní cestou odinstalovat, postupujte podle následujících kroků:

Android 6 a starší:

1.Ťukněte na ikonu Launcheru (nebo přejděte na **Domů** > **Menu**), vyberte **Nastavení** a přejděte do sekce **Zabezpečení** > **Správce zařízení**. V seznamu najděte **ESET Mobile Security** a odeberte mu oprávnění pomocí možnosti **Deaktivovat**. Ťukněte na **Odemknout** a zadejte bezpečnostní heslo. Pokud nemá aplikace PRODUCTNAME oprávnění správce pokračujte dalším krokem.

2.V **Nastavení** přejděte do sekce **Aplikace**, najděte **ESET Mobile Security** a vyberte možnost **Odinstalovat**.

Android 7 a novější:

1.Přejděte na nastavení OS Android a ťukněte na **Správa aplikací**. Vyberte **ESET Mobile Security** a ťukněte na **Odinstalovat**. Pokud je aktivní ochrana Anti-Theft, před odinstalováním ESET Mobile Security můžete být vyzváni k odebrání oprávnění Správce zařízení.

nebo

1.Ťukněte na k zobrazení hlavního menu.

2.V seznamu vyberte **Nastavení**.

3.Ťukněte na **Odinstalovat**.

4.Ťukněte znovu na **Odinstalovat** pro potvrzení výběru.

Připojení k ESET HOME

Abyste mohli využívat tuto funkci, je třeba aktualizovat ESET Mobile Security na verzi 6.3 a novější.

Aktivace ESET Mobile Security prostřednictvím ESET HOME

Jestliže chcete aktivovat stejné zařízení prostřednictvím ESET HOME po opětovné instalaci ESET Mobile Security, je třeba původní zařízení v účtu ESET HOME odpojit od licence. V opačném případě toto zařízení nebudete moci prostřednictvím ESET HOME aktivovat.

Jak připojit své zařízení k existujícímu účtu ESET HOME?

1. Ťukněte na tlačítko menu ☰.
2. Ťukněte na položku **Účet ESET HOME**.

Přihlášení pomocí Google

a.Přihlaste se ke svému účtu Google nebo jej vyberte ze seznamu nabídnutých účtů.

b.Pokud se účtem Google připojujete k již existujícímu účtu ESET HOME poprvé, budete za účelem ověření vyzváni k zadání hesla ke svému účtu ESET HOME. Ťukněte poté na **Potvrdit heslo**.

Přihlášení pomocí Apple ID

a.Zadejte e-mailovou adresu a heslo ke svému Apple ID.

b.Ťukněte na **Přihlásit se**.

c.Zadejte kód zaslaný na vaše zařízení Apple.

d.Ťukněte na **Pokračovat**.

e.Pokud důvěřujete zařízení, na kterém operaci provádíte, klikněte na **Důvěřovat**.

f.Pro přístup do ESET HOME prostřednictvím Apple ID klikněte na **Pokračovat**.

g.Ťukněte v levém horním rohu na ikonu **X** pro návrat do ESET Mobile Security.

Naskenovat QR kód

Tato možnost vyžaduje k přihlášení druhé zařízení s nainstalovanou aplikací ESET HOME.

a.Na druhém zařízení si otevřete aplikaci ESET HOME.

b.Ťukněte na tlačítko menu ☰.

c.Tap **Scan a QR code**.

d.Ťukněte na **Naskenujte QR kód**. Aplikace vás může vyzvat, abyste ESET HOME povolili přístup k fotografiím a nahrávání videí. Ťukněte na **Při používání aplikace** nebo **Pouze tentokrát**.

e.Pomocí svého zařízení naskenujte QR kód.

f.Ťukněte na **Připojit zařízení**.

Přihlášení pomocí e-mailové adresy

a.Zadejte svou e-mailovou adresu a heslo.

b.Ťukněte na **Přihlásit se**.

3. Pokud se s tímto zařízením přihlašujete ke svému účtu ESET HOME poprvé, pro jeho snadnější identifikaci v ESET HOME si jej pojmenujte. Ťukněte na tlačítko **Další**.

4. Pokud používáte bezplatnou nebo zkušební licenci a máte v ESET HOME dostupnou licenci k ESET Mobile Security, bude vám nabídnuta aktivace pomocí této licence.

a.Vyberte využitelnou licenci.

b.Ťukněte na tlačítko **Aktivovat**.

5. Ťukněte na **Dokončit**.

Jak vytvořit účet ESET HOME a připojit k němu zařízení?

1. Ťukněte na tlačítko menu ☰.

2. Ťukněte na položku **Účet ESET HOME**.

3. Ťukněte na **Vytvořit účet**.

4. Zadejte e-mailovou adresu a heslo.

> **Požadavky na heslo**
> Heslo by mělo mít alespoň deset znaků, mělo by obsahovat alespoň jedno malé písmeno, jedno velké písmeno a číslo.

5. Ťukněte na **Vytvořit účet**, čím se odešle do vaší e-mailové schránky zpráva s odkazem pro potvrzení.

6. Zadejte název zařízení pro jeho snadnější identifikaci a ťukněte na tlačítko **Další**.

7. Ťukněte na **Dokončit**.

8. Pro dokončení registrace si otevřete e-mailovou zprávu o vytvoření účtu a ťukněte na odkaz pro potvrzení.

Jak odpojit své zařízení od ESET HOME?

1. Ťukněte na tlačítko menu ☰.

2. Ťukněte na položku **Účet ESET HOME**.

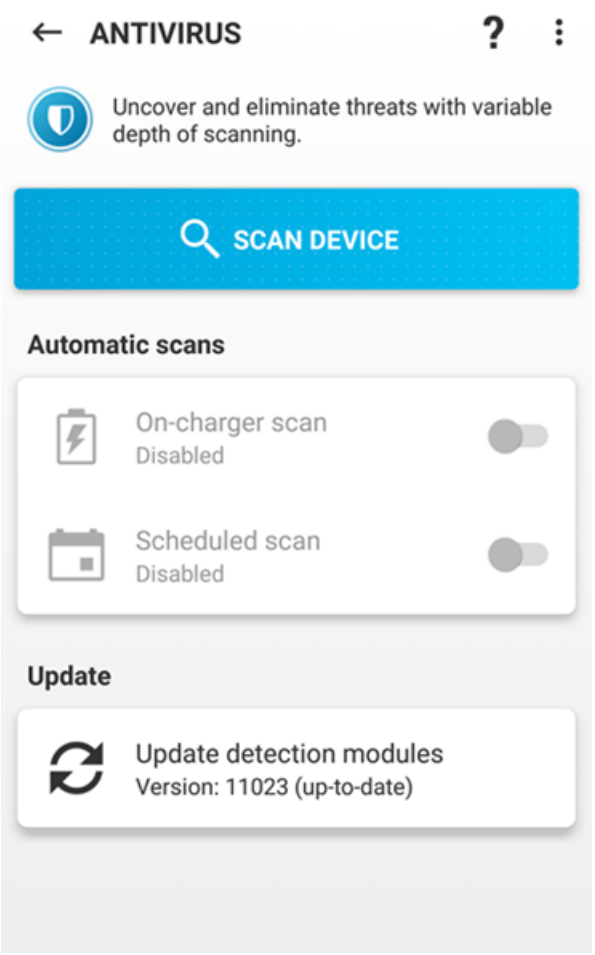
3. Ťukněte na odkaz **Odpojit zařízení**. Tato možnost není dostupná v případě, kdy zařízení není připojené k účtu ESET HOME.

4. Použijte otisk prstu nebo zadejte PIN.

5. Ťukněte na tlačítko **Dokončit**.

Antivirus

Modul antivirové ochrany chrání zařízení před škodlivým kódem tím, že hrozby blokuje a léčí.



Rezidentní ochrana

Rezidentní ochrana souborového systému skenuje všechny soubory ve složkách pro stažené soubory na možný výskyt škodlivého kódu, jakmile dojde k jejich spuštění, otevření nebo vytvoření.

Rezidentní ochrana souborového systému poskytuje nepřetržitou ochranu a spouští se standardně při startu systému. Rozhodně vám nedoporučujeme zapnutou Rezidentní ochranu souborového systému v části **Antivirus** vypínat.

Kontrola zařízení

Standardně se kontrolují předdefinované typy souborů. Při spuštění úplné kontroly zařízení se zkontrolují spuštěné procesy, paměť, dynamické knihovny procesů a soubory umístěné na vnitřním i vyměnitelném úložišti. Souhrn kontroly se uloží do protokolu, který je přístupný ze sekce **Protokoly kontrol**. Pokud chcete přerušit běžící kontrolu, ťukněte na tlačítko **Zrušit** v pravém dolním rohu obrazovky. Výsledek kontroly a statistiky během kontroly si zobrazíte po ťuknutí na dlaždici **Antivirus**.



Kontrola paměťových karet

ESET Mobile Security nepodporuje kontrolu paměťových karet na zařízeních s operačním systémem Android 5 a starším.

Nevyřešené hrozby

Tato možnost se v produktu zobrazí, pokud ESET Mobile Security detekuje ve vašem zařízení hrozbu, a zůstane aktivní do doby, než na ni zareagujete. Seznam dostupných akcí: odebrat hrozbu nebo ignorovat.

Ignorování hrozby

Při použití možnosti **ignorovat hrozbu** se v produktu zobrazí tato sekce. Stále bude schopni případnou hrozbu odstranit nebo ji nadále ignorovat.

Kontrola při nabíjení

Pokud aktivujete tuto možnost, kontrola zařízení se spustí automaticky, pokud je zařízení nečinné, zapojené na nabíječce a plně nabité.

Naplánovaná kontrola

Prostřednictvím této možnosti si můžete nastavit automatické spuštění kontroly v předem definovaném čase. Pro naplánování kontroly ťukněte na ikonu vedle možnosti **Naplánovaná kontrola** a nastavte datum a čas, kdy se má kontrola provést. Standardně je vybráno pondělí a čas nastaven na 4:00.

Aktualizovat detekční moduly

ESET Mobile Security Pravidelně kontroluje a stahuje aktualizace. Pokud chcete spustit aktualizaci ručně, ťukněte na **Aktualizovat detekční moduly**.



Poplatky za přenos dat

Pro zabránění zbytečnému stahování dat jsou aktualizace vydávány v případě výskytu nové hrozby. Zatímco aktualizace jsou bezplatné, může vám být účtován poplatek za přenos dat podle tarifu mobilního operátora.

Další informace o možnostech kontroly naleznete v těchto kapitolách:

- Protokoly kontrol
- Rozšířená nastavení

Protokoly kontrol

Protokoly kontrol se automaticky vytváří po každé naplánované či ručně spuštěné kontrole zařízení.

Každý protokol obsahuje:

- Datum a čas kontroly,
- Informace o typu kontroly včetně její nastavení úrovně (smart nebo hloubková),
- Dobu kontroly,
- Počet zkontrolovaných souborů
- Provedené akce nebo chyby, které se vyskytly během kontroly.
- Počet nalezených hrozeb a jejich seznam.

Rozšířená nastavení

Úroveň kontroly

K dispozici jsou dvě úrovně kontroly:

- **Smart** – zkontroluje všechny nainstalované aplikace, DEX soubory (spustitelné soubory Android OS), SO soubory (knihovny), archivy do maximálně třetí úrovně zanoření a obsah SD karty.
- **Hloubková** — zkontroluje všechny typy souborů bez ohledu na příponu, a to jak v interní paměti zařízení, tak na SD kartě.

Rezidentní ochrana

Rezidentní ochrana se spouští automaticky při startu systému/zařízení a kontroluje soubory s nimiž manipulujete. Kontroluje také složku Stažené soubory (Download) a nainstalované a aktualizované aplikace.

Reputační systém ESET LiveGrid©

ESET LiveGrid© je preventivní systém navržený pro poskytnutí další úrovně ochrany zařízení. Neustále monitoruje běžící programy a procesy na zařízení a porovnává je s nejnovějšími informacemi získanými od milionů uživatelů ESET po celém světě. Díky tomu dokážeme všem uživatelům poskytnout účinnější proaktivní ochranu a vyšší rychlost kontroly. Tuto funkci doporučujeme zapnout.

Systém zpětné vazby ESET LiveGrid©

Prostřednictvím tohoto systému sbíráme anonymní statistická data, informace o pádech a diagnostická data o podezřelých objektech, které v cloudu zpracováváme a vytváříme z nich detekční signatury.

Výměnná média

ESET Mobile Security kontroluje všechna výměnná média připojená k vašemu zařízení – USB flash disky, externí pevné disky…

Detekovat potenciálně nechtěné aplikace

Potenciálně nechtěná aplikace je program, který obsahuje adware, a instaluje rozšíření, které zobrazuje reklamu,

skenuje výsledky vyhledávání nebo vykazuje jiné nežádoucí chování. V některých případech můžete mít pocit, že přínosy převáží rizika nechtěné aplikace. Z tohoto důvodu ESET řadí tyto aplikace do kategorie s nižším rizikem než jiný škodlivý software.

Detekovat potenciálně zneužitelné aplikace

Existuje řada aplikací, jejichž úkolem je zjednodušit správu síťových zařízení. Tato klasifikace zahrnuje programy pro vzdálený přístup k zařízení, nástroje pro dešifrování hesel a programy zaznamenávající stisky kláves a další. Potenciálně zneužitelné aplikace je označení pro komerční a legitimní software. Nicméně v nesprávných rukou mohou být snadno zneužity ke škodlivým účelům. Po aktivování možnosti **Detekovat potenciálně zneužitelné aplikace** vás na tyto aplikace ve vašem zařízení upozorníme.

Aktualizační server

Pomocí této možnosti můžete získat přístup k **testovacím aktualizacím**. Tyto aktualizace jsou otestované vývojové aktualizace, které budou později dostupné jako standardní. Výhodou těchto aktualizací je, že nabízejí rychlý přístup k nejnovějším metodám detekce a různým opravám. Testovací aktualizace však představují riziko nestabilního chování zařízení. Seznam aktuálně používaných modulů naleznete v sekci **O programu: ťukněte na ikonu menu** ⋮ a ťukněte na O programu > **ESET Mobile Security**. Doporučujeme ponechat předdefinovanou hodnotu (**Standardní aktualizace**). Tuto volbu by měli měnit pouze zkušení uživatelé.

Adware Detector

Adware Detector představuje řešení pro boj s adwarovými aplikacemi. Aplikace tohoto typu mohou být legitimní nebo se za legitimní mohou vydávat (například Kalkulačka nebo Svítilna). Adware zobrazuje reklamy přes celou obrazovku, ačkoli samotná aplikace není používaná. Uživatel proto nemůže zjistit, která aplikace reklamy zobrazuje.

Adware Detector vám pomůže tyto adwarové aplikace identifikovat. Po zobrazení reklamy proto postupujte dle následujících kroků:

1. Otevřete si ESET Mobile Security.
2. V hlavním okně aplikace ESET Mobile Security ťukněte na dlaždici **Antivirus**.
3. Ťukněte vpravo nahoře na ⋮ pro zobrazení menu.
4. Ťukněte na položku **Adware Detector**.
5. Po zobrazení instrukcí k používání Adware Detector ťukněte na tlačítko **Pokračovat**.

Adware Detector zobrazí seznam aplikací, které se na vašem zařízení otevřely v posledních pěti minutách. Identifikujte podezřelé aplikace a ťuknutím na možnost **Odstranit** konkrétní aplikaci případně odeberte ze zařízení. Podezřelá aplikace je obvykle ta, o které víte, že jste ji s určitostí v daný moment nespustili.

Bezpečnostní přehled

Tento přehled vám poskytuje souhrnné informace o stavu a funkčnosti aplikace . Pokud máte některé součásti programu vypnuté, můžete je přímo v tomto **přehledu** aktivovat. Přehled je rozdělen do jednotlivých sekcí podle

jednotlivých součástí programu a k dispozici jsou tyto informace.

Antivirus

- Nainstalované aplikace
- Aktualizované aplikace
- Zkontrolované aplikace
- Nalezeno hrozeb
- Aktualizace detekčního jádra

Zámek aplikace

- Počet chráněných aplikací
- Počet úspěšně odemčených aplikací
- Počet neúspěšných pokusů o odemčení

Anti-Phishing

- Zkontrolováno stránek
- Nalezeno hrozeb

Filtr hovorů

- Příchozí hovory
- Zablokované hovory

Bezpečnostní audit

- Roamingová upozornění
- Upozornění na nezabezpečené Wi-Fi

Ochrana plateb

- Počet chráněných aplikací
- Počet kontrol chráněných aplikací

ESET Mobile Security zobrazí měsíční zprávu ve stavové liště systému Android každý měsíc. Pokud nechcete dostávat toto upozornění, povolte možnost **Neupozorňovat na měsíční přehled**.

Protokol aktivity

Přehled o provedených akcí máte k dispozici přímo na úvodní stránce programu ESET Mobile Security. V protokolu aktivit ESET Mobile Security naleznete informace o počtu zkontrolovaných stránek, provedených aktualizacích, přehled zkontrolovaných aplikací, provedených kontrol a mnohem více.

Ťuknutím na **Úplný přehled** zobrazíte historii Protokolu aktivity. Klepnutím na Úplný přehled zobrazíte historii Protokolu aktivity. Ve výpisu použijte **filtry** k třídění činností dle stavu nebo ESET Mobile Security funkce, Příklad: Varování, Riziko, Anti-Theft, Licence. Činnosti můžete rovněž třídit dle data výskytu od novějších po starší.

Chcete vymazat historii Protokolu aktivity?

1.Otevřete si ESET Mobile Security.

2.Přejeďte prstem po obrazovce vzhůru.

3.Ťukněte na **Zobrazit vše**.

4.Ťukněte na ikonu menu ⋮.

5.A ťukněte na **Vymazat vše**.

Pro smazání konkrétních záznamů z historie Protokolu aktivity:

1.Otevřete si ESET Mobile Security.

2.Přejeďte prstem po obrazovce vzhůru.

3.Ťukněte na **Zobrazit vše**.

4.Přejeďte prstem vlevo přes příslušný záznam.

5.Ťukněte na tlačítko **Odstranit**.

Anti-Theft

Technologie ESET Anti-Theft chrání mobilní zařízení před neoprávněným přístupem, umožňuje sledovat cizí aktivitu a monitorovat polohu zařízení. Pokud zařízení ztratíte, oceníte možnost zobrazení zprávy nálezci zařízení.

Ztracené zařízení spravujte prostřednictvím portálu ESET Anti-Theft. Zařízení můžete rovněž ovládat pomocí speciálních SMS příkazů zaslaných z důvěryhodných kontaktů. Abyste mohli funkci SMS příkazů používat, je třeba ji předem nastavit. Do seznamu důvěryhodných kontaktů vložte ta telefonní čísla, ze kterých bude možno případně příkazy zasílat. Podrobnější návod získáte v článku databáze znalostí (v angl.) Set up Anti-Theft protection in ESET Mobile Security. (článek nemusí být dostupný ve všech jazycích.)

Technologie ESET Anti-Theft vyžaduje ke svému fungování přístup k informacím o poloze zařízení a k fotoaparátu. Pro zobrazení varování a uzamčení zařízení vyžaduje aplikace ESET Mobile Security oprávnění pro překrytí obrazovky.

Aplikace ESET Mobile Security při podezřelých aktivitách automaticky odesílá na My ESET portál informaci o poloze, IP adrese a snímky pořízené fotoaparátem. V této části můžete konfigurovat nastavení:

Automatický zámek zařízení

Nastavte si v ESET Mobile Security automatický zámek zařízení pro případ:

- **Když je vyjmuta důvěryhodná SIM karta** – V případě vyjmutí se zařízení uzamkne. Pozor! Pokud chcete důvěryhodnou SIM kartu vyjmout, ťukněte na **Spravovat důvěryhodné SIM karty** > ťukněte na SIM kartu určenou k vyjmutí a poté na ikonu koše . Pro přidání důvěryhodné SIM karty ji nejprve vložte. Pokud je Automatický zámek zařízení zapnutý, bude třeba zařízení odemknout. Poté se vás ESET Mobile Security dotáže na přidání SIM karty jako důvěryhodné. Pro aktivaci této funkce vytvoříme na vaší SIM kartě a ve vašich kontaktech jedinečný identifikátor ESET ####. Tento unikátní identifikátor nesmíte smazat. Pokud identifikátor smažete, vaše zařízení se uzamkne.



Podpora Automatického zámku zařízení při vyjmutí SIM karty

- Tato funkce není podporována u CDMA, WCDMA a WiFi-only zařízeních.

- **Jakmile dojde k [X] neúspěšným pokusům o odemknutí zařízení** – Pokud je funkce zapnuta, zařízení se automaticky uzamkne při konkrétním počtu neúspěšných pokusů. Určete si v nastavení Anti-Theft počet neúspěšných pokusů, které je povoleno zadat před uzamknutím zařízení. Pokud dojde k neúspěšnému pokusu omylem, lze pokus opravit do 30 sekund. Tím nebude počítán pokus jako neúspěšný. V nastavení Anti-Theft je možno **Čas pro opravu zadání** změnit. Možnost nastavení času na opravu zadání lze i vypnout. V tomto případě se zařízení uzamkne po vámi určeném počtu neúspěšných pokusů.

Pokud je zařízení uzamčeno, budou se zobrazovat informace pro kontaktování vlastníka zařízení. Rovněž lze povolit funkci pořizování fotografií oběma fotoaparáty pro identifikaci osoby, která se snažila odemknout vaše zařízení.

Po uzamčení zařízení

Pro případ uzamčení zařízení lze nastavit následující akce:

- **Zobrazit kontaktní informace** – Jakmile je zadáno nesprávné přístupové heslo (kód) k zařízení, zobrazí se možnost **Kontaktovat vlastníka** zařízení.

- **Pořídit fotografii** – V případě, že se kdokoli pokusí neúspěšně odemknout vaše zařízení nebo vyjme ze zařízení důvěryhodnou SIM kartu, pořídí přední i zadní fotoaparát zařízení fotografie okolí a uloží je do Galerie zařízení a portálu Anti-Theft.

SMS příkazy

Pokud tuto funkci zapnete, využijte SMS příkazy k akcím jako zamknutí zařízení na dálku, nalezení polohy zařízení nebo kompletní vymazání obsahu telefonu. Tyto příkazy lze zasílat pouze ze zařízení, jejichž telefonní číslo jste v části Anti-Theft uložili do svých důvěryhodných kontaktů.

Spravovat důvěryhodné kontakty

Pro přidání telefonních čísel ťukněte na odkaz **Spravovat důvěryhodné kontakty** a další obrazovce na ikonu **plus**

v pravém dolním rohu. Vyberte, které příkazy může důvěryhodný kontakt zasílat. Váš kontakt zároveň obdrží oznámení v případě, kdy je vyjmuta důvěryhodná SIM karta.

> **SMS funkce**
> Funkce Anti-Theft (důvěryhodné SIM karty a SMS příkazy) nejsou dostupné na zařízeních CDMA a zařízeních, které nepodporují zasílání SMS zpráv.

Nastavení Anti-Theft

Uzamknout po neúspěšných pokusech

Zvolte počet povolených neúspěšných pokusů o přístup do zařízení před tím, než se zařízení uzamkne. Počet neúspěšných pokusů nastavíte ťuknutím na ⋮ na obrazovce Anti-Theft, poté ťukněte na **Nastavení**, dále na **Uzamknout po neúspěšných pokusech** a vyberte počet neúspěšných pokusů.

Čas na opravu zadání

Pokud zapnete funkci Uzamknout po neúspěšných pokusech, vaše zařízení se po dosaženém počtu pokusů uzamkne. Pro okamžité uzamčení zařízení nastavte možnost Vypnuto. Uzamknutí zařízení můžete oddálit výběrem konkrétní časové hodnoty, po kterou lze ještě zařízení úspěšně odemknout.

> **Příklad**
> Funkce **Uzamknout po neúspěšných pokusech** je zapnuta a počet neúspěšných pokusů je nastaven na 3.
> **Čas na opravu zadání** je nastaven na 15 sekund.
> Pokud zadáte třikrát nesprávný vzor (PIN) pro odemknutí, máte 15 sekund na zadání správného vzoru, než ESET Mobile Security zařízení uzamkne.

Změnit kontaktní informace

Pokud je zařízení na portále ESET Anti-Theft označeno jako ztracené nebo pokud dojde k dosažení daného počtu neúspěšných pokusů o odemknutí, na obrazovce zamčeného zařízení se zobrazí **Kontaktní informace**. Díky těmto informacím vás nálezce zařízení bude schopen kontaktovat, a zařízení tak můžete získat zpět.

Tyto informace mohou obsahovat:

- Jméno (nepovinné),
- Záložní telefonní číslo, případně kontakt na někoho blízkého (přátele nebo rodinného příslušníka),
- Popis zařízení (nepovinné),
- E-mailovou adresu (nepovinné).

Správa důvěryhodných SIM karet

Tato funkce umožňuje odebrat nebo přejmenovat vložené SIM karty. Pokud je ochrana SIM karty aktivní, pro přidání nové důvěryhodné SIM karty ji nejprve do zařízení vložte. Zařízení se uzamkne. Odemkněte zařízení zadáním přístupového hesla k účtu ESET HOME. Po úspěšném zadání hesla vás ESET Mobile Security vyzve k přidání nově vložené SIM karty na seznam důvěryhodných SIM karet. Pokud SIM kartu do seznamu nepřidáte, ochrana SIM karty zůstane vypnuta.

Změnit typ zámku

Zvolte si možnost odemknutí ESET Anti-Theft. Ve výchozím nastavení je předvolena možnost odemykání pomocí PIN. Místo zadávání kódu můžete k odemknutí zařízení využít i vzor.

Použití otisku prstu

Pokud je tato možnost zapnuta, k odemknutí ESET Anti-Theft poslouží otisk prstu uložený v zařízení.

SMS příkazy

Používat můžete tyto SMS příkazy:

Uzamknout
`eset lock`
Zařízení se uzamkne a bude možné jej odblokovat pouze heslem do ESET HOME.

Siréna
`eset siren`
Na zařízení se spustí siréna, i pokud je hlasitost ztlumena.

Najít
`eset find`
Obdržíte GPS souřadnice ztraceného zařízení s odkazem na dané místo v mapách Google. Pokud bude získána přesnější pozice, po 10 minutách odešle zařízení další informaci o své pozici.

Vymazat
`eset wipe`
Všechny kontakty, zprávy, e-maily, účty, obsah SD karty, hudba, obrázky a videa uložená v systémových složkách budou nenávratně odstraněna ze zařízení.

Po odeslání SMS příkazu obdržíte SMS s bezpečnostním kódem. Pro potvrzení SMS příkazu odpovězte příkazem s bezpečnostním kódem podle pokynů v přijaté SMS.

Optimalizace

Optimalizace ESET Anti-Theft je technická funkce, která kontroluje bezpečností stav vašeho zařízení. ESET Anti-Theft ochrana detekuje následující problémy:

U každého bezpečnostního problému se ťuknutím na tlačítko **Změnit nastavení** dostanete na obrazovku s

návodem, jak daný problém vyřešit. Pokud nechcete, aby vás aplikace ESET Mobile Security upozorňovala na daný problém, ťukněte na tlačítko **Ignorovat tento problém**.

• **Služby určování polohy jsou vypnuty** – pro zapnutí přejděte do nastavení OS Android > **Přístup k poloze** a vyberte možnost **Použít Wi-Fi a mobilní sítě**

• **GPS satelity nejsou používány** – pro zapnutí přejděte do nastavení OS Android > **Přístup k poloze** a **režim** nastavte na **Vysoká přesnost**

• **Zamykací obrazovka není zabezpečena** – pro zabezpečení zamykací obrazovky (vzorem, PINem nebo heslem) přejděte do nastavení OS Android; **Zámek obrazovky a hesla.** Většina zařízení s OS Android podporuje odemčení heslem, gestem, PINem, případně hlasem nebo rozpoznáním tváře. Pokud se kdokoli pokusí několikrát neúspěšně odemknout vaše zařízení, technologie ESET Anti-Theft vás na tuto akci upozorní prostřednictvím portálu ESET HOME.

• **Mobilní data nejsou zapnuta** – pro zapnutí přejděte do nastavení OS Android > **Bezdrátová připojení a sítě** > **Mobilní sítě** > **Data**.

• **Služby Google Play nejsou dostupné** – technologie ESET Anti-Theft používá Služby Google Play k doručování příkazů na zařízení a zobrazování push notifikací. Pokud nejsou v zařízení tyto služby nainstalovány nebo jsou vypnuté, možnost správy zařízení prostřednictvím portálu ESET Anti-Theft > ESET HOME budou velmi omezené. V takovém případě doporučujeme používat SMS příkazy zveřejněné na portálu ESET HOME.

Webový portál

Technologie ESET Anti-Theft v aplikaci ESET Mobile Security verze 7 nabízí kompletní integraci s portálem ESET HOME. Prostřednictvím tohoto portálu můžete v části ESET Anti-Theft vzdáleně sledovat aktivitu zařízení, zjistit jeho polohu, uzamknout jej, odeslat uživatelskou zprávu nálezci zařízení, spustit sirénu a smazat data v zařízení uložená.

Pokud zatím nemáte ESET HOME účet, ťukněte na tlačítko **Vytvořit nový účet** a vyplňte registrační formulář. Následně zkontrolujte svou e-mailovou schránku a klikněte v e-mailu na odkaz pro aktivaci účtu. Od té chvíle můžete spravovat bezpečnostní funkci Anti-Theft vzdáleně prostřednictvím portálu ESET HOME. Pokud již máte účet ESET HOME, ťukněte na **Přihlásit se** a zadejte svou e-mailovou adresu a heslo. Po dokončení těchto kroků propojte své zařízení s účtem ESET HOME.

Více informací o tom, jak používat funkce ESET Anti-Theft naleznete v uživatelské příručce Anti-Theft, případně v pravém horním rohu portálu ťukněte na ikonu "**?**".

Důvěryhodné kontakty

Do seznamu **Důvěryhodných kontaktů** můžete přidávat nebo z něj odebírat telefonní čísla přátel a rodinných příslušníků. To má následující výhody:

- Na tato čísla se zašle SMS upozornění při neautorizované změně důvěryhodné SIM karty ve vašem zařízení
- Z těchto čísel bude možno zasílat SMS příkazy

Pro přidání nového Důvěryhodného kontaktu ťukněte na ikonu **+** . Zadejte jméno kontaktu a telefonní číslo, případně ťukněte na ikonu siluety  a kontakt vyberte ze svého telefonního seznamu. Pro odebrání kontaktu na něj ťukněte a následující obrazovce ťukněte na ikonu odpadkového koše .

V případě, že u Důvěryhodného kontaktu máte definováno více telefonních čísel, SMS s upozorněním se zašle na všechna čísla tohoto kontaktu. Více informací naleznete v článku databáze znalostí **Přidání důvěryhodného kontaktu v ESET Mobile Security pro Android** . (článek nemusí být dostupný ve všech jazycích).

> **Dostupnost služeb ze zahraničí**
> Pokud jste v zahraničí, všechna telefonní čísla zadaná v seznamu musí obsahovat mezinárodní předvolbu (např. +420777123456).

Heslo k ESET HOME

Pro změnu zapomenutého hesla:

1.Navštivte odkaz https://login.eset.com/LostPassword.

2.Zadejte e-mailovou adresu, kterou jste použili při registraci účtu ESET HOME, a klikněte na tlačítko **Odeslat**.

3.Přihlaste se do své e-mailové schránky, otevřete si **e-mail pro reset hesla do účtu ESET HOME** a klikněte na odkaz v e-mailu.

4.Zadejte a potvrďte nové heslo, poté klikněte/ťukněte na **Potvrdit změnu**.

5.Potvrďte kliknutím/ťuknutím na **OK**.

6.Na zařízení zadejte nové heslo a ťukněte na tlačítko **Odemknout**.

Změna hesla prostřednictvím portálu ESET HOME:

1.Přejděte do aplikace ESET HOME nebo na stránku ESET HOME.

2.Přihlaste na počítači pomocí e-mailové adresy a příslušným heslem.
3.Ťukněte na e-mailovou adresu vedle symbolu šipky dolů (nebo u tabletů na ikonu profilu) v pravém horním rohu. U telefonů ťukněte na ikonu menu v levém horním rohu. Následně zvolte **Můj účet**.
4.Klikněte na tlačítko **Změnit heslo**.

5.Zadejte své aktuální heslo.

6.Zadejte své nové heslo a potvrďte jej.

7.Klikněte na tlačítko **Odeslat**.

Anti-Phishing

Pojem *phishing* definuje kriminální činnost, jejímž cílem je donutit uživatele k vyplnění důvěrných informací na webových stránkách, které se na první pohled tváří legitimně. Tomuto způsobu manipulace se říká sociální inženýrství. Phishing se často používá k získání přístupu k citlivým údajům, jako jsou čísla bankovních účtů, čísla platebních karet, PIN kódy nebo uživatelská jména a hesla.

Anti-Phishing v ESET Mobile Security chrání také před přístupem na webové stránky, které se nacházejí na seznamu škodlivých nebo nebezpečných webů.

Proto doporučujeme ponechat funkci **Anti-Phishing** zapnutou. Všechny potenciální phishingové útoky přicházející z webových stránek či domén uvedených v databázích ESET budou zablokovány a zobrazí se varovné upozornění informující o útoku.

Anti-Phishing podporuje nejrozšířenější webové prohlížeče na platformě Android – Chrome a výchozí webový prohlížeč, který je na zařízení předinstalován (zpravidla pojmenovaný jako *Internet* nebo *Prohlížeč*). Ostatní nepodporované prohlížeče budou označeny jako nechráněné. V rámci zajištění maximální bezpečnosti nedoporučujeme tyto prohlížeče používat.



Důležité

Abychom ve webových prohlížečích zajistili bezproblémovou funkci Anti-Phishingové ochrany, doporučujeme vám používat operační systém verze Android 6 (Marshmallow) nebo novější.

Vylepšit funkčnost – tato možnost se zobrazí, pokud technologie Anti-Phishing vyžaduje dodatečná systémová oprávnění. Ťuknutím na tlačítko **Povolit** se zobrazí nastavení operačního systému, kde v sekci Usnadnění přidělte aplikaci potřebná oprávnění. Tímto krokem aktivujete technologii Anti-Phishing v dosud nechráněných prohlížečích a tato funkce bude dostupná také v privátních režimech prohlížečů. Pokud nechcete vylepšit funkčnost technologie Anti-Phishing a chcete skrýt tuto oznámení, vyberte možnost **Ignorovat tento problém (nedoporučujeme)**.

Pro deaktivování funkce Anti-Phishing ťukněte na ikonu menu ⋮ a vyberte možnost **Vypnout**.



Anti-Phishing na Samsung DeX

Anti-Phishing není podporován na zařízeních připojených k dokovací stanici Samsung DeX.

Chráněné prohlížeče

- Chrome
- Chrome Beta
- Firefox
- Firefox Beta
- Opera
- Opera Beta

- Opera Mini
- Opera Mini Beta
- Opera TV browser
- Samsung Internet
- Mint
- Yandex browser
- DuckDuckGo (ESET Mobile Security ve verzi 6.1 a novější)
- Kiwi browser
- Edge
- Silk na Amazon zařízeních
- Mi browser
- Xiaomi Mi browser
- Vewd v Android TV

Chráněné aplikace sociálních sítí

- Facebook
- Facebook Lite
- Messenger
- Messenger Lite
- Instagram
- Aplikace sociálních sítí, které pro webové zobrazení využívají součásti chráněných prohlížečů, jsou rovněž chráněné.

Zámek aplikace

Prostřednictvím zámku aplikace můžete zabezpečit přístup k vybraným aplikacím (pro čtení e-mailů, SMS, kalendáři atp.) pomocí PINu nebo otisku prstu. Tím zabráníte neautorizovanému přístupu k vybraným aplikacím ve chvíli, kdy máte zařízení odemknuté.



Doporučení

Přidělte aplikaci ESET Mobile Security oprávnění **Překrytí** (**Aplikace, které se mohou vykreslit navrchu**), abyste zajistili lepší chod funkce.

Aktivování zámku aplikace

1. V hlavním okně aplikace ESET Mobile Security ťukněte na dlaždici **Zámek aplikace**.
2. Ťukněte na tlačítko **Zapnout**.
3. Type your PIN, which unlocks applications.
4. Confirm your PIN by typing it again.
5. Ťukněte na aplikaci, kterou chcete zámkem ochránit nebo naopak odemknout.

Nastavení zámku aplikace

Pro přístup do nastavení Zámku aplikace ťukněte vpravo nahoře na menu ⋮ > **Nastavení**:

- **Uzamknout nové aplikace** – pokud je možnost zapnutá, po nainstalování nové aplikace se zobrazí výzva, zda chcete aplikaci zámkem ochránit.
- **Uzamknout aplikaci** – ťuknutím na položku vyberte interval, po jehož uplynutí se Zámek aplikace automaticky uzamkne. Dostupné možnosti: okamžitě, po zamknutí obrazovky, za 1 minutu.
- **Typ zámku** – ťuknutím na položku rozhodněte, zda chcete přístup k aplikaci chránit pomocí PIN nebo vzorem.
- **Odemknout otiskem prstu** – tato možnost je dostupná pouze v případě, kdy máte ve svém zařízení uložen otisk prstu. Pokud možnost zapnete, můžete aplikace otiskem prstu odemknout. Nadále zůstává možnost odemykání aplikací zadáním PIN. V takovém případě na obrazovce pro odemčení ťukněte na **Použít PIN**.
- **Detekce pokusu o vniknutí** – po několika neúspěšných pokusech o odemčení pořídí aplikace ESET Mobile Security fotografii narušitele, která se následně zobrazí při dalším úspěšném odemčení aplikace.

Vypnutí zámku aplikace:

1. V ESET Mobile Security ťukněte na dlaždici Zámek aplikace.
2. Zadejte PIN pro přístup.
3. Ťukněte vpravo nahoře na menu ⋮.
4. Ťukněte na **Vypnout**.

Zapnutí nočního režimu

Noční režim slouží pro úlevu vašim očím. Na obrazovce zámku jej aktivujete ťuknutím na ikonu v pravém horním rohu.

Zapomenutý PIN k Zámku aplikace

Pokud jste zapomněli PIN k zámku aplikace a nemáte ve svém zařízení uložen otisk prstu, v závislosti na nastavení bezpečnostního hesla existují dvě možnosti pro obnovení přístupu k aplikacím.

- Pokud jste si v ESET Mobile Security aktivovali technologii Anti-Theft:

  1.Otevřete si ESET Mobile Security.

  2.Ťukněte na dlaždici Zámek aplikace.

  3.Zadejte svůj PIN **ťukněte na odkaz Zapomněli jste PIN?**

  4.Do prázdného pole zadejte své **heslo** pro přístup do účtu ESET HOME a ťukněte na tlačítko **Potvrdit**.

  5.Zadejte svůj nový PIN a ťukněte na symbol .

  6.Pro potvrzení zadejte znovu svůj nový PIN a ťukněte na symbol .

- V případě, že jste si neaktivovali Anti-Theft, odinstalujte ESET Mobile Security a znovu si jej nainstalujte.

Ochrana plateb

Ochrana plateb představuje další bezpečnostní vrstvu, která byla navržená za účelem ochrany vašich finančních dat proti sofistikovanému phishingu a dalším hrozbám v zařízeních Android. Ochrana plateb zamezuje ostatním aplikacím zaznamenat spuštění chráněných aplikací a zároveň u chráněných aplikací znemožňuje zaměňování nebo čtení informací zobrazených na obrazovce. Ochrana plateb kontroluje každou aplikaci, která je v seznamu chráněných aplikací. Po aktivaci ochrany plateb se některé bankovní a platební aplikace automaticky do seznamu chráněných aplikací přidají.

Přidání nové aplikace do seznamu chráněných aplikací

1. V menu aplikace ESET Mobile Security ťukněte na položku Ochrana plateb.
2. Ťukněte na **Spravovat**.
3. Ťuknutím vyberte aplikace, které chcete chránit Ochranou plateb.
4. Pro potvrzení ťukněte na **OK**.

Otevřete si aplikaci pro ochranu bankovnictví a on-line plateb ťuknutím na ikonu Ochrana plateb

Chcete-li zajistit nejvyšší ochranu pro své bankovní a platební aplikace, otevírejte je prostřednictvím bezpečného spouštěče Ochrany plateb. Tento způsob spuštění poskytuje aplikacím další vrstvu ochrany oproti standardnímu otevírání aplikací mimo bezpečný spouštěč.
Bezpečný spouštěč Ochrany plateb se vytvoří automaticky, jakmile zapnete funkci Ochrany plateb. Spouštěč zahrnuje všechny aplikace, které jsou do ochrany přidané.

Co je bezpečný spouštěč a jak jej spustím?

Bezpečný spouštěč otevřete ťuknutím na ikonu Ochrana plateb. Ikonu najdete na obrazovce mezi ostatními instalovanými aplikacemi nebo v ESET Mobile Security > Ochrana plateb.

Rychlý přístup k bezpečnému spouštěči

Pro rychlejší a snadnější přístup k bankovním a platebním aplikacím si přidejte Bezpečný spouštěč na svou domovskou obrazovku. Abyste tak učinili, podržte dlouze prst na ikoně Ochrana plateb a přesuňte ji na svou domovskou obrazovku.

Filtr hovorů

Filtr hovorů blokuje příchozí a odchozí hovory v závislosti na pravidlech, která jste nastavili.

Upozornění na volání se nebudou zobrazovat, pokud je příchozí hovor zablokován. Při ťuknutí na položku**Historie** si můžete ověřit, zda některý ze svých kontaktů nemáte blokován omylem.

Pokud chcete zablokovat hovory z naposledy přijatého telefonního čísla, ťukněte na **Blokovat posledního volajícího**. Tím se vytvoří nové pravidlo filtru hovorů a zpráv.

Pravidla

Pro vytvoření nového pravidla ťukněte na ikonu +. Více informací o vytváření pravidel naleznete v této kapitole.

Pro úpravu existujícího pravidla na něj ťukněte v seznamu. Pro odebrání **pravidla** ťukněte na možnost **Odstranit** .

Protokol hovorů

V sekci **Protokol hovorů** naleznete přehled všech zablokovaných hovorů. Každý záznam obsahuje název události, odpovídající telefonní číslo, datum a čas, kdy se událost vyskytla.

Zařízení bez SIM karty

Filtr hovorů není dostupný na zařízeních, které nepodporují příjem hovorů a zpráv.

Odchozí hovory

Filtr hovorů neblokuje odchozí hovory v ESET Mobile Security staženém na Google Play.

Podpora Android

Filtr hovorů je dostupný pouze v zařízeních s OS Android 6 a novějším.

Přidání nového pravidla

Pro vytvoření nového pravidla ťukněte na ikonu **+**.

1.Pro přidání nového pravidla ťukněte na ikonu **+** v pravém horním rohu. Vyberte možnost **povolit** nebo **blokovat** v závislosti na tom, kterou chcete použít. V sekci Co vyberte akci (povolit nebo blokovat), kterou chcete použít. Zároveň definujte směr hovoru (standardně jsou vybrány příchozí hovory).

2.V sekci **Kdo** vyberte telefonní čísla, pro která bude pravidlo platné.

- **Osoba** – vyberte ze seznamu kontaktů nebo jméno a telefonní číslo zadejte ručně. Více telefonních čísel k jednomu jménu přiřadíte ťuknutím na ikonu **+** v sekci **Telefonní číslo**.
- **Skupina** – ESET Mobile Security rozpoznává používané skupiny ve vašem seznamu kontaktů (například Rodina, Přátelé, Práce).
- **All unknown numbers** will include all phone numbers not saved in your contact list. Tuto možnost můžete použít pro blokování nežádoucích hovorů (např. "marketingové hovory") nebo zabránění dětem ve vytáčení neznámých čísel.
- **Všechna známá čísla** – tento seznam obsahuje všechna telefonní čísla z vašeho seznamu kontaktů.
- **Všechna čísla** – blokovány budou všechny příchozí hovory.
- **Skrytá čísla** – volající, kteří mají své telefonní číslo záměrně skryto pomocí Call Line Identification Restriction (CLIR).

3.Pokud chcete uplatnit pravidlo pouze v určitou dobu, v sekci **Kdy** ťukněte na **Vždy** a vyberte možnost **Vlastní**. Poté ve spodní části obrazovky zadejte den a čas, ve kterém chcete pravidlo použít. Standardně je vybrána sobota a neděle a čas od 22:00 do 6:00. Tato funkce může přijít vhod, pokud nechcete být rušeni v noci během víkendu.

Podrobnější informace včetně obrázků naleznete v Databázi znalostí.

Filtr v zahraničí

Pokud jste v zahraničí, všechna telefonní čísla zadaná v seznamu musí obsahovat mezinárodní předvolbu (např. +420777123456).

Strážce sítě

Funkce Strážce sítě umožňuje zjistit, jaká zařízení jsou připojena k vašemu routeru včetně jejich možné zranitelnosti. Kontrola sítě probíhá ve dvou krocích.

Nejprve Strážce sítě zkontroluje veškerá zařízení připojená do sítě. Jestliže bylo nějaké zařízení detekováno, na obrazovce uvidíte oznámení a zařízení bude označeno symbolem hvězdičky. Zobrazení připojených zařízení manuálně docílíte ťuknutím na **Zkontrolovat síť**. Rovněž můžete nechat zařízení vyhledat automaticky. Pro použití této možnosti ťukněte na ikonu menu ⋮ > **Nastavení** a vyberte možnost **Vyhledávat zařízení automaticky**.

Ve druhém kroku kontroluje funkce Strážce sítě zranitelnosti připojených zařízení tím, že se k nim připojí a ověřuje otevřené porty, slabé uživatelské jméno a heslo k routeru, problémy s firmwarem routeru apod. Chyby v zabezpečení mohou hackeři využít, aby získali kontrolu nad routerem a dalším zařízením k němu připojeným. Routery a zařízení ovládaná hackery mohou být využita ke sběru informací o vás nebo mohou být využita jako součást DDoS útoků aj.

Funkce Strážce sítě vám také poskytuje komplexní seznam zařízení připojených k vaší síti. Na základě získané informace z webového rozhraní routeru můžete spravovat případně zamezit zařízením přístupu k síti. Do webového rozhraní routeru se dostanete přímo z funkce Strážce sítě po ťuknutí na ikonu routeru a následně ťuknutím na možnost **Otevřít webové rozhraní**.

Připojená zařízení můžete zobrazit jako seznam nebo jako sonarové zobrazení:

- Seznam – připojená zařízení zobrazíte ve formě seznamu, ve kterém je router na prvním místě, následují aktuálně připojená zařízení a nejníže naleznete zařízení, která byla připojena k síti v minulosti.

- Sonarové zobrazení – zařízení jsou zobrazena v půlkruhu okolo routeru umístěném uprostřed první vrstvy. Ve druhé vrstvě od středu jsou zobrazena zařízení, která jsou momentálně připojena síti. Ve třetí vrstvě jsou připojena zařízení připojená k síti v minulosti. Mezi zařízeními se můžete pohybovat ťuknutím na tlačítka šipek nebo posunutím po směru kruhu.

Pro snadnější správu přiřaďte zařízením kategorie, jako jsou chytré telefony, TV, herní konzole, počítače atd. Zařízení lze i přejmenovat z továrních názvů či jejich IP adres na rozpoznatelná jména (například: SM-G955F přejmenujte na "Honzíkův telefon", 192.168.1.52 na "Taťkův komp" atd.).

Pro přejmenování zařízení ve Strážci sítě ťukněte na ikonu zařízení > dále pak na ikonu tužky v pravém horním rohu, vyberte kategorii zařízení, zadejte název zařízení a následně potvrďte volbou **OK**.

Bezpečnostní audit

Díky bezpečnostnímu auditu budete mít přehled o důležitých nastaveních vašeho zařízení. Tak máte pod kontrolou oprávnění každé aplikace nainstalované ve vašem zařízení jako ochranu před případnými bezpečnostními riziky.

To enable or disable Security Audit and its specific components, tap the menu button and tap **Disable Device Monitoring** or **Disable Application Audit**.

- Monitorování zařízení
- Audit aplikací

Monitorování zařízení

V této části můžete nastavit, která nastavení operačního systému bude aplikace ESET Mobile Security monitorovat.

Ťuknutím na každou možnost se zobrazí podrobný popis nastavení a aktuální stav (zda je daná funkce zapnutá nebo vypnutá). Některé možnosti, jako jsou **Neznámé zdroje** a **Režim ladění**, můžete změnit ťuknutím na tlačítko **Otevřít nastavení**. Poté budete přesměrováni do Nastavení systému Android.

Tímto způsobem můžete vypnout každou komponentu.

1. Ťukněte na komponentu, kterou chcete vypnout.
2. Ťukněte na ikonu menu .
3. Ťukněte na **Vypnout**.

Audit aplikací

Některé aplikace nainstalované na zařízení mohou mít přístup ke službám, které jsou zpoplatněny, sledovat vaši polohu, získávat informace o vaší identitě, kontaktech nebo textových zprávách. ESET Mobile Security vás na tyto aplikace upozorní. V Bezpečnostním auditu v části Audit aplikací máte k dispozici seznam aplikací seřazený podle kategorií. Ťuknutím na jednotlivé kategorie zobrazíte jejich podrobný popis. Detaily oprávnění každé aplikace si zobrazíte ťuknutím na název dané aplikace.

Nastavení

Pro přístup do nastavení aplikace ESET Mobile Security ťukněte na hlavní obrazovce na ikonu menu ☰ (případně stiskněte tlačítko Menu na svém zařízení) a vyberte možnost **Nastavení**.

Zálohovat a obnovit

ESET Mobile Security dokáže vytvořit soubor se zálohou nastavení aplikace. Tento soubor si můžete stáhnout, uložit na externí úložiště a použít v budoucnu pro obnovení nastavení ESET Mobile Security.

Jazyk

By default, ESET Mobile Security is installed in the language set as the system default on your device (in Android OS Language and keyboard settings). Pokud chcete změnit jazyk uživatelského rozhraní aplikace, ťukněte na možnost **Jazyk** a vyberte si jiný.

Trvalé upozornění

(Tato možnost je dostupná na OS Android 7 a starším)

Oznámení produktu ESET Mobile Security se standardně zobrazují v dolní části oznamovací oblasti OS Android. Pokud oznámení nechcete zobrazovat, vypněte možnost Trvalé upozornění.

Program zvyšování spokojenosti zákazníků

Aktivováním této možnosti se z produktu ESET Mobile Security budou zasílat anonymní informace (o výkonu a statistiky běhu), které nám pomohou v dalším vylepšování produktu a našich služeb.

Speciální nabídky

Pokud aktivujete tuto možnost, do aplikace vám budeme zasílat informace o novinkách a výhodných akcích na produkty ESET.

Aktualizace

Pro zajištění maximální ochrany je důležité používat nejnovější verzi ESET Mobile Security. Ťuknutím na položku **Aktualizace** zjistíte, zda je k dispozici ke stažení novější verze programu. Tato možnost není dostupná, pokud jste si ESET Mobile Security stáhli a nainstalovali prostřednictvím Google Play – v tomto případě se produkt aktualizuje automaticky z Google Play.

Odinstalovat

Running the Uninstall wizard will permanently remove ESET Mobile Security from the device. Pokud je aktivní ochrana Anti-Theft, budete požádáni o zadání bezpečnostního PINu/vzoru do ESET Mobile Security nebo o otisk prstu. Ruční odinstalaci aplikace máme popsanou v této kapitole.



Ochrana proti odinstalování
Ochrana proti odinstalování není dostupná na OS Android 7 a novějším.

Technická podpora

Specialisté technické podpory ESET jsou vám k dispozici a poskytnou vám administrativní nebo technickou podporu související s programem ESET Mobile Security nebo dalšími produkty ESET.

Kontaktujte technickou podporu ESET

Pro odeslání žádosti na technickou podporu ze svého zařízení:

1. Ťukněte na hlavní obrazovce ESET Mobile Security na ikonu menu ☰ (případně stiskněte tlačítko menu na svém zařízení).

2. Ťukněte na **Technická podpora**.

3. Opět na **Technická podpora** pro vytvoření požadavku.

4. Vyplňte všechna povinná pole. ESET Mobile Security obsahuje rozšířené protokolování, které je užitečné při diagnostice technických problémů.

5. Aby došlo k odeslání diagnostických dat z aplikace, ujistěte se, že je zaškrtnuta možnost **Odeslat protokol aplikace** (standardně zapnuta).

6. Dotaz odešlete ťuknutím na tlačítko **Odeslat**.

7. Specialisté technické podpory ESET vás kontaktují na zadané e-mailové adrese, resp. adrese uvedené u licence.



Aplikaci není možno otevřít nebo neodpovídá
Chcete-li odeslat společnosti ESET žádost o podporu v případě, že ESET Mobile Security neodpovídá nebo jej nelze otevřít, přejděte ve svém zařízení s Android do **Nastavení** > **Aplikace** > > **Úložiště** > **Správa paměti**. Ťukněte na **Technická podpora** a vyplňte všechna povinná pole.

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 následující funkce Softwaru:

a) **Aktualizace Software**. 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_home. Poté, co Software nebo některé z jeho funkcí dosáhnou data konce životnosti definovaného v Zásadách konce životnosti, nebudou poskytovány žádné aktualizace.

b) **Zasílání infiltrací a informací Poskytovateli.** Software obsahuje funkce, které slouží ke shromažďování vzorků počítačových virů a jiných škodlivých počítačových programů a podezřelých, problematických nebo potenciálně nežádoucích nebo nebezpečných objektů, jako jsou soubory, adresy URL, IP pakety a ethernetové rámce (dále jen "Infiltrace") a jejich následnému odeslání Poskytovateli, mimo jiné včetně informací o procesu instalace, počítači a/nebo platformě, kde je Software nainstalován, a informací o operacích a funkcích Softwaru ("Informace"). Informace a Infiltrace mohou zahrnovat údaje (včetně náhodně nebo nezáměrně získaných osobních údajů) o Koncovém uživateli a/nebo jiných uživatelích počítače, na kterém je Software nainstalován, a soubory postižené Infiltracemi, včetně přidružených metadat.

Informace a Infiltrace mohou být shromažďovány následujícími funkcemi Softwaru:

i. Funkce Reputační systém LiveGrid zahrnuje shromažďování a odesílání jednosměrných hodnot hash, které souvisejí s Infiltracemi, Poskytovateli. Tato funkce je povolena v rámci standardního nastavení Softwaru.

ii. Funkce Systém zpětné vazby LiveGrid zahrnuje shromažďování a odesílání Infiltrací s příslušnými metadaty a Informacemi Poskytovateli. Tuto funkci aktivuje Koncový uživatel během procesu instalace Softwaru.

Poskytovatel bude obdržené Informace a Infiltrace používat pouze pro účely analýzy a zkoumání Infiltrací, zlepšování ověřování pravosti Softwaru a Licence a přijme veškerá vhodná opatření, aby zajistil, že obdržené Infiltrace a Informace zůstanou v bezpečí. Po aktivaci této funkce Softwaru mohou být Infiltrace a Informace shromažďovány a zpracovávány Poskytovatelem, jak je uvedeno v Zásadách ochrany osobních údajů a v příslušných právních předpisech. Tyto funkce můžete kdykoliv deaktivovat.

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.

DODATEK K DOHODĚ

Posouzení zabezpečení zařízení připojených k síti. Na posouzení zabezpečení zařízení připojených k síti se vztahují následující dodatečná ustanovení:

Software je vybaven funkcí určenou pro ověření zabezpečení lokální sítě Koncového uživatele a zařízení v lokální síti, k čemuž potřebuje získat název sítě a informace o zařízeních připojených do lokální sítě jako je jejich přítomnost, typ, název, IP adresa a MAC adresa zařízení v lokální síti společně s informací o licenci. V případě routeru tyto informace dále zahrnují způsob zabezpečení bezdrátové sítě a typ použitého šifrování bezdrátové sítě. Tato funkce může dále nabízet informace týkající se dostupnosti bezpečnostního software určeného pro zabezpečení zařízení v lokální síti.

Ochrana proti zneužití dat Na ochranu proti zneužití dat se vztahují následující dodatečná ustanovení:

Software obsahuje funkci, která zabraňuje ztrátě nebo zneužití důležitých dat v přímé souvislosti s odcizením počítače. Tato funkce je ve výchozím nastavení Softwaru vypnutá. Aby bylo možné tuto funkci aktivovat, je nutné si vytvořit účet ESET HOME, přes který funkce aktivuje sběr dat v případě odcizení počítače. Pokud tuto funkci Softwaru aktivujete, budou data o odcizeném počítači shromažďovány a odesílány Poskytovateli (může se jednat o údaje o umístění počítače v síti, údaje o obsahu zobrazovaném na obrazovce počítače, údaje o konfiguraci počítače nebo o data zaznamenaná kamerou připojenou k počítači (dále jen "Data"). Koncový uživatel je oprávněn

používat Data získaná touto funkcí a poskytnutá prostřednictvím účtu ESET HOME výhradně k nápravě nepříznivé situace způsobené odcizením počítače. Výhradně pro účely této funkce Poskytovatel zpracuje Data v souladu se Zásadami ochrany osobních údajů a příslušnými právními předpisy. Poskytovatel umožní Koncovému uživateli přístup k Datům po dobu nezbytně nutnou k dosažení účelu, pro který byla data získána. Tato doba nesmí překročit dobu uchovávání stanovenou v Zásadách ochrany osobních údajů. Ochrana proti zneužití dat se bude používat výlučně u počítačů a účtů, ke kterým má Koncový uživatel oprávněný přístup. Jakékoli nezákonné používání bude oznámeno příslušným orgánům. Poskytovatel bude v případě zneužití postupovat v souladu s příslušnými zákony a pomáhat orgánům činným v trestním řízení. Souhlasíte a potvrzujete, že je Vaší zodpovědností zabezpečit heslo pro přístup k účtu ESET HOME, a souhlasíte s tím, že nesmíte předat své heslo žádné třetí straně. Koncový uživatel je odpovědný za jakoukoli aktivitu, při které se používá funkce ochrany proti zneužití dat a účet ESET HOME, bez ohledu na to, zda k provádění takovýchto aktivit měl nebo neměl povolení. Pokud zjistíte, že je zabezpečení účtu ESET HOME ohroženo, neprodleně tuto skutečnost Poskytovateli oznamte.

Kódy. Na kódy se vztahují následující dodatečná ustanovení:

Společnost ESET může dle vlastního uvážení vytvořit odkazující kód anebo jiný kód pro propagační nebo marketingové účely (dále jen „Kód“). Kód můžete použít k prodloužení doby platnosti licence v souladu s touto Smlouvou. Společnost ESET si vyhrazuje právo Kód kdykoli deaktivovat, pokud je Kód získán nebo používán způsobem, který není v souladu s touto Smlouvou, anebo v případě důvodného přesvědčení, že došlo k chybě, podvodu nebo nezákonnému jednání. Musíte dodržet následující omezení:

i. Kód nesmíte uplatnit více než jednou.

ii. Kód nesmíte prodat, zapůjčit ani pronajmout anebo ho používat k poskytování komerčních služeb.

iii. Souhlasíte s tím, že společnost ESET může kdykoli zakázat poskytování anebo používání Kódu bez implikování jakéhokoli závazku vůči společnosti ESET.

iv. Souhlasíte s tím, že Kód nelze vyměnit za hotovost nebo jakoukoli jinou náhradu.

v. Souhlasíte s tím, že Kód anebo jeho používání může podléhat zvláštním podmínkám společnosti ESET pro konkrétní odkazující, propagační anebo marketingovou kampaň.

EULAID: EULA-PRODUCT-LG-EMS; 3537.0

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.

Tyto informace jsou uchovávány odděleně od identifikačních údajů potřebných pro účely licencování a fakturace, protože nevyžadují identifikaci koncového uživatele. Doba uchovávání je maximálně 4 roky.

Reputační systém **ESET LiveGrid®.** Jednosměrné hodnoty hash, které souvisejí s infiltracemi, jsou zpracovávány pro účely reputačního systému ESET LiveGrid®, který zlepšuje účinnost našich řešení proti malwaru tím, že porovnává kontrolované soubory s databází povolených a zakázaných položek v cloudu. Koncový uživatel během tohoto procesu není identifikován.

Systém zpětné vazby **ESET LiveGrid®.** Podezřelé vzorky a metadata jako součást systému zpětné vazby ESET LiveGrid®, který umožňuje společnosti ESET okamžitě reagovat na potřeby našich koncových uživatelů a udržet akceschopnost tváří v tvář nejnovějším hrozbám. Jsme závislí na tom, že nám zasíláte:

- Infiltrace, jako jsou potenciální vzorky virů a jiných škodlivých programů, a podezřelé; problematické, potenciálně nežádoucí nebo nebezpečné objekty, jako jsou spustitelné soubory nebo e-mailové zprávy, které jsou nahlášeny koncovým uživatelem jako nevyžádané nebo označené naším produktem; údaje o zařízeních v místní síti, jako je typ, dodavatel, model a/nebo název zařízení;
- Údaje týkající se používání internetu, jako jsou IP adresa a informace o zeměpisné poloze, IP pakety, adresy URL a ethernetové rámce;
- Soubory výpisu chyb a v nich obsažené informace.

Nechceme shromažďovat data mimo uvedený rozsah, někdy je však nemožné tomu zabránit. Kontaktní informace a údaje obsažené ve vašich požadavcích na podporu mohou být vyžadovány za účelem poskytování podpory. 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.

Veškeré informace získané a zpracovávané prostřednictvím systému zpětné vazby ESET LiveGrid® jsou určeny k použití bez identifikace koncového uživatele.

Posouzení zabezpečení zařízení připojených k síti. Abychom mohli poskytovat funkci posouzení zabezpečení, zpracováváme název lokální sítě a informace o zařízeních v lokální síti, jako jsou přítomnost, typ, název, IP adresa a adresa MAC zařízení v lokální síti společně s informacemi o licencích. V případě routeru tyto informace dále zahrnují způsob zabezpečení bezdrátové sítě a typ použitého šifrování bezdrátové sítě. Informace o licencích identifikující koncové uživatele jsou anonymizovány nejpozději 12 měsíců po skončení platnosti licence.

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.

Ochrana proti zneužití dat. Pokud si vytvoříte účet ESET HOME na webu https://home.eset.com a prostřednictvím funkce Anti-Theft označíte své zařízení jako ztracené, budou shromažďovány a zpracovávány následující informace: údaje o poloze, snímky obrazovky, data o konfiguraci počítače a data zaznamenaná kamerou počítače. Shromážděné údaje jsou uloženy na našich serverech nebo na serverech našich poskytovatelů služeb a jsou uchovávány po dobu 3 měsíců.

Analýza využití a pádů produktu. Na základě vašeho souhlasu s používáním budeme shromažďovat a analyzovat údaje týkající se používání našich produktů, abychom mohli testovat jejich výkon a zlepšovat je pro naše uživatele. Shromážděné údaje mohou zahrnovat různé akce uživatele a události, ke kterým dochází v produktu (například spuštění aplikace, aktualizace aplikace, doba trvání relace, nákup v aplikaci), informace o použitém zařízení, platformě nebo operačním systému, jakož i údaje týkající se vašeho věku, pohlaví, polohy a zájmů, které mohou být spojeny s různými identifikátory (například ID instalace). Dále budeme shromažďovat a zpracovávat technická data související s pády aplikace (například informace o zařízení, identifikátor instalace, trasování pádu, minivýpis chyb při pádu), abychom mohli získat přehled o pádech, zjistit jejich příčiny a zajistit úplnou funkčnost našeho produktu. Ke shromažďování a analýze těchto údajů používáme náš Program zvyšování spokojenosti zákazníků (kde se zpracovávají pouze anonymní telemetrická data) a služby Google, abychom získali podrobnější přehled. Další informace o zpracování vašich údajů společností Google naleznete v příslušných zásadách ochrany osobních údajů společnosti Google.

Zpracování pro marketingové účely. Pokud se rozhodnete udělit nám svůj souhlas pro marketingové účely, my a naši marketingoví partneři použijeme údaje o vašem používání našeho produktu k vyhodnocení výkonu našich online marketingových aktivit, lepšímu pochopení vašich zájmů a zobrazování relevantnějších online reklam. Shromážděné údaje mohou zahrnovat různé akce uživatele a události, ke kterým dochází v produktu (například spuštění aplikace, aktualizace aplikace, doba trvání relace, nákup v aplikaci), informace o použitém zařízení, platformě nebo operačním systému, jakož i údaje týkající se vašeho věku, pohlaví, polohy a zájmů, které mohou být spojeny s různými identifikátory (ID instalace, ID mobilní reklamy). Tato data pro nás shromažďuje a analyzuje společnost Google. Další informace o zpracování vašich údajů společností Google naleznete v příslušných zásadách ochrany osobních údajů společnosti Google.

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