ESET Endpoint Security for macOS

Uživatelská příručka

Klikněte sem pro zobrazení online verze tohoto dokumentu

Digital Security
Progress. Protected.

ESET Endpoint Security for macOS byl vyvinut společností ESET, spol. s r.o.

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

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

REV. 2023-03-19

ESET Endpoint Security for macOS

ESET Endpoint Security for macOS představuje nový přístup k plně integrované počítačové bezpečnosti. Nejnovější verze skenovacího jádra ThreatSensespolečně s firewallem přináší vyšší rychlost a přesnější detekci a udržuje váš počítač v bezpečí. Výsledkem je inteligentní systém, který neustále kontroluje veškeré dění na počítači na přítomnost škodlivého kódu.

ESET Endpoint Security for macOS 6 je komplexní bezpečnostní řešení, které kombinuje maximální ochranu s minimálním dopadem na operační systém. Pokročilé technologie založené na umělé inteligenci jsou schopny proaktivně eliminovat viry, spyware, trojské koně, červy, adware, rootkity a další internetové hrozby, bez znatelného dopadu na výkon počítače nebo funkčnost operačního systému.

Produkt je navržen pro ochranu pracovních stanic v SMB i enterprise prostředí. Pomocí nástroje ESET PROTECT (dříve známý jako ESET Security Management Center) můžete snadno spravovat libovolné množství klientských stanic – aplikovat na ně politiky, sledovat zachycené útoky a vzdáleně je konfigurovat z jakéhokoli počítače v síti.

Co je nového ve verzi 6?

Uživatelské rozhraní ESET Endpoint Security for macOS bylo po grafické stránce kompletně přepracováno a poskytuje více informací při zachování intuitivního ovládání. Verze 6 nabízí následující vylepšení:

- Podpora ESET Enterprise Inspector – ESET Endpoint Security for macOS může být od verze 6.9 připojen k ESET Enterprise Inspector (EEI). EEI je komplexní EDR (Endpoint Detection and Response) systém, který nabízí následující funkce: detekce incidentů, správu incidentu a reakce na ně, sběr dat, indikaci na kompromitaci systémů, detekci anomálií, detekci chování a poručení firemní politiky. Pro více informací o ESET Enterprise Inspector, jeho instalaci a možnostech se podívejte do uživatelské příručky.

- **Podpora 64-bitové architektury**

- **Firewall** – pravidla firewallu můžete nově vytvářet přímo z protokolu nebo upozornění modulu IDS (Intrusion detection system) a přiřazovat je konkrétním síťovým adaptérům,

- **Filtrování obsahu webu** – umožňuje blokovat webové stránky s nevhodným obsahem,

- **Ochrana přístupu na web** – monitoruje HTTP komunikaci mezi webových prohlížečem a vzdálenými servery

- **Ochrana poštovních klientů** – zajišťuje kontrolu e-mailové komunikace probíhající na protokolech POP3 a IMAP,

- **Anti-Phishingová ochrana** – chrání vás před pokusy o získání hesla a dalších citlivých informací zablokováním přístupu na podvodné webové stránky, které se vydávají za legitimní,

- **Správa zařízení** – zajišťuje kontrolu výměnných médií a umožňuje zablokovat přístup k externím zařízením jednotlivým uživatelům nebo celým skupinám. Tato funkce je dostupná od verze 6.1.

- **Prezentační režim** – potlačí všechna oznamovací okna ESET Endpoint Security for macOS a zabrání spuštění naplánovaných úloh,

- **Sdílená lokální cache** – zvyšuje rychlost kontroly ve virtuálních prostředích.

Systémové požadavky

Pro plynulý běh ESET Endpoint Security for macOS by měl váš systém splňovat následující hardwarové a softwarové požadavky:

	Systémové požadavky:
Architektura procesoru	Intel 64-bit, Apple ARM 64-bit
Operační systém	macOS 10.12 a novější
Operační paměť	300 MB
Volné místo na pevném disku	200 MB

Kromě procesorů Intel podporuje ESET Endpoint Security for macOS od verze 6.10.900.0 také Apple ARM čip (prostřednictvím emulátoru Rosetta 2).

Představení ESET PROTECT

ESET PROTECT je aplikace, prostřednictvím které můžete spravovat bezpečnostní produkty ESET na stanicích, serverech i mobilních zařízeních z jednoho centrálního místa v síti.

Prostřednictvím ESET PROTECT Web Console můžete vzdáleně instalovat bezpečnostní řešení ESET na zařízení, spravovat jejich konfiguraci a rychle reagovat na nové problémy a detekce v síti. Seznamte se s ESET PROTECT architekturou a jednotlivými prvky infrastruktury, podporovanými Desktop Provisioning prostředími a následně přejděte do kapitoly Začínáme s ESET PROTECT Web Console.

ESET PROTECT se skládá z následujících komponent:

- ESET PROTECT Server – výkonná část, která zajišťuje komunikaci mezi klientskými stanice (ESET Management Agenty). ESET PROTECT Server můžete nainstalovat na Windows, Linux nebo jej do virtuální prostředí nasadit jako virtuální appliance.

- ESET PROTECT Web Console – ESET PROTECT Web Console představuje primární rozhraní pro správu zařízení ve vaší síti. Jedná se o webové rozhraní, které poskytuje informace o zařízeních ve vaší síti, bezpečnostních incidentech a umožňuje instalaci i konfiguraci produktů ESET. Pokud máte webový server dostupný z internetu, můžete ESET PROTECT spravovat prakticky odkudkoli z libovolného zařízení s internetovým prohlížečem.

- ESET Management Agent – komponenta, která zajišťuje komunikaci mezi klientskou stanicí a ESET PROTECT Serverem. ESET Management Agenta musíte nainstalovat na každé zařízení, které chcete vzdáleně spravovat prostřednictvím ESET PROTECT Web Console. Instalaci můžete provést lokálně nebo vzdáleně. Díky agentovi jste schopni ze stanici získat mnohem větší množství dat, a protože si agent pamatuje veškeré politiky, odpovídající nastavení aplikuje v případě detekce okamžitě bez nutnosti přímé viditelnosti ESET PROTECT Serveru. Agenta můžete prostřednictvím ESET Management Web Console nasadit na nespravované stanice, jejichž seznam jste získali synchronizací s Active Directory, případně je detekoval ESET RD Sensor. Agenta také můžete na stanice instalovat ručně.

- Rogue Detection Sensor – ESET Rogue Detection Sensor (RD Sensor) je nástroj, který vyhledává zařízení v síti a představuje pohodlný způsob pro přidání nových počítačů do ESET PROTECT bez nutnosti jejich ručního

zadávání. RD Sensor si pamatuje počítače, které již objevil, a neodesílá duplicitní informace.

- Apache HTTP Proxy – je služba, kterou v kombinaci s ESET PROTECT můžete použít:
  - Jako cache, ze které se budou klientům distribuovat aktualizace detekčních modulů a ESET Management Agentovi instalační balíčky.
  - Pro přesměrování komunikace ESET Management Agentů na ESET PROTECT Server.
- Mobile Device Connector – komponenta, která zajišťuje komunikaci mezi ESET PROTECT a mobilními zařízení s OS Android (a aplikací ESET Endpoint Security pro Android) případně operačním systémem iOS.
- ESET PROTECT Virtuální appliance – připravený virtuální stroj založený na operačním systému CentOS 7 s ESET PROTECT (ESET PROTECT) určený pro provoz ve virtuálním prostředí.
- ESET PROTECT Virtual Agent Host – komponenta ESET PROTECT, která virtualizuje agenty chráněných virtuálních strojů ve VMware prostředí prostřednictvím produktu ESET Virtualization Security. Toto řešení vám přináší do agent-less prostředí stejné možnosti automatizace, využití dynamických skupin a správy úloh jako v případě fyzických stanic, na kterých je nainstalován ESET Management Agent. Zároveň v ESET PROTECT máte k dispozici informace o z těchto virtuálních stanic.
- Mirror Tool – představuje řešení pro sítě bez přístupu k internetu. Prostřednictvím tohoto nástroje vytvoříte lokální kopii aktualizačních serverů i online repozitáře s instalačními balíčky.
- Deployment Tool – prostřednictvím tohoto nástroje můžete vzdáleně nasadit all-in-one instalační balíček vytvořený v <%PRODUCT%> Web Console. Jedná se o pohodlný způsob, jak na stanice můžete vzdáleně nasadit ESET Management Agenta společně s bezpečnostním produktem ESET.
- ESET Business Account – nový licenční portál, prostřednictvím kterého můžete spravovat všechny své licence. Pro více informací o aktivaci bezpečnostních produktů přejděte do kapitoly ESET Business Account v této příručce, případně se podívejte do uživatelské příručky k samotnému portálu. Pokud máte k dispozici pouze uživatelské jméno a heslo, na tomto portále si je můžete převést na licenční klíč.
- ESET Enterprise Inspector – je komplexní EDR (Endpoint Detection and Response) systém, který nabízí následující funkce: detekce incidentů, správu incidentu a reakce na ně, sběr dat, indikaci na kompromitaci systémů, detekci anomálií, detekci chování a poručení firemní politiky.

Prostřednictvím ESET PROTECT Web Console můžete vzdáleně nasazovat ESET produkty, spouštět úlohy, vynutit bezpečnostní politiky, monitorovat stav produktu a rychle reagovat na nově vniklé problémy nebo hrozby.

Pro více informací se podívejte do online nápovědy ESET PROTECT.

Představení ESET PROTECT Cloud

Prostřednictvím ESET PROTECT CLOUD můžete spravovat bezpečnostní produkty ESET na stanicích a serverech z jednoho centrálního místa, kdy k jeho provozu nepotřebujete fyzický ani virtuální server jako v případě ESET PROTECT nebo ESET Security Management Center. Přímo z ESET PROTECT CLOUD Web Console můžete vzdáleně instalovat bezpečnostní řešení ESET na zařízení, spravovat jejich konfiguraci a rychle reagovat na nové problémy a hrozby na spravovaných počítačích.

- Pro více informací přejděte do uživatelské příručky ESET PROTECT CLOUD.

Vzdálená instalace

Předtím, než začnete

macOS 10.15 a starší

Předtím, než začnete ESET Endpoint Security for macOS instalovat na macOS 10.13 a novější, povolte načtení ESET rozšíření jádra. Na cílových stanicích s macOS 10.14 a novějším navíc povolte úplný přístup k disku. Pokud výše uvedené požadavky povolíte až po dokončení instalace, uživatelům se do té doby v hlavním okně produktu objeví hlášení, že je **blokováno systémové rozšíření** a **Váš počítač není plně chráněn**.

Pro vzdálené povolení načtení ESET rozšíření jádra a úplného přístupu k disku musí být počítače registrovány k MDM (Mobile Device Management) serveru, jako je například Jamf.

Povolení ESET systémových rozšíření

Pro vzdálené povolení načtení rozšíření jádra:

- Pokud jako MDM používáte Jamf, postupujte podle kroků uvedených v naší Databázi znalostí.
- Pokud používáte odlišné MDM, stáhněte .plist konfigurační profil. Vygenerujte si dvě UUID v libovolném generátoru UUID. Pomocí textového editoru nahraďte ve staženém konfiguračním profilu řetězce `insert your UUID 1 here` a `insert your UUID 1 here` vámi vygenerovanými UUID. Nasaďte .plist konfigurační profil prostřednictvím svého MDM serveru. Aby si počítače převzali konfiguraci, musí být registrovány k MDM serveru.

Povolení úplného přístupu k disku

Na macOS 10.14 se po dokončení instalace produktu ESET Endpoint Security for macOS zobrazí hlášení **Váš počítač není plně chráněn**. Pro zajištění úplné funkčnosti programu ESET Endpoint Security for macOS a potlačení zobrazování hlášení musíte aplikaci povolit **Úplný přístup k disku** ještě před zahájením instalace. Pro vzdálené povolení **úplného přístupu k disku**:

- Pokud jako MDM používáte Jamf, postupujte podle kroků uvedených v naší Databázi znalostí.
- Pro vzdálené přidělení **úplného přístupu k disku** si stáhněte .plist konfigurační soubor. Vygenerujte si dvě UUID v libovolném generátoru UUID. Pomocí textového editoru nahraďte ve staženém konfiguračním profilu řetězce `insert your UUID 1 here` a `insert your UUID 1 here` vámi vygenerovanými UUID. Nasaďte .plist konfigurační profil prostřednictvím svého MDM serveru. Aby si počítače převzali konfiguraci, musí být registrovány k MDM serveru.

macOS Big Sur (11)

Předtím, než začnete ESET Endpoint Security for macOS instalovat na macOS BigSur, je nutné povolit načtení ESET systémového rozšíření a povolit úplný přístup k disku. Pokud výše uvedené požadavky povolíte až po dokončení instalace, uživatelům se do té doby v hlavním okně produktu objeví hlášení, že je **blokováno systémové rozšíření** a **Váš počítač není plně chráněn**. Rozšíření systému je možné povolit vzdáleně pouze před zahájením instalace ESET Endpoint Security for macOS.

Pro vzdálené povolení načtení ESET systémového rozšíření a úplného přístupu k disku musí být počítače

registrovány k MDM (Mobile Device Management) serveru, jako je například Jamf.

Povolení ESET systémových rozšíření

Pro vzdálené povolení načtení systémových rozšíření:

- Pokud jako MDM používáte Jamf, postupujte podle kroků uvedených v naší Databázi znalostí.
- Pokud používáte jiné MDM, stáhněte .plist konfigurační profil. Nasaďte .plist konfigurační profil prostřednictvím svého MDM serveru. Aby si počítače převzali konfiguraci, musí být registrovány k MDM serveru. Při tvorbě vlastního konfiguračního profilu použijte níže uvedená nastavení:

Identifikátor týmu (TeamID)	P8DQRXPVLP
Identifikátor balíku (BundleID)	com.eset.endpoint com.eset.network com.eset.firewall com.eset.devices

Povolení úplného přístupu k disku

Pro vzdálené povolení **úplného přístup k disku**:

- Pokud jako MDM používáte Jamf, postupujte podle kroků uvedených v naší Databázi znalostí.
- Pro vzdálené přidělení **úplného přístupu k disku** si stáhněte .plist konfigurační soubor. Nasaďte .plist konfigurační profil prostřednictvím svého MDM serveru. Aby si počítače převzali konfiguraci, musí být registrovány k MDM serveru. Při tvorbě vlastního konfiguračního profilu použijte níže uvedená nastavení:

ESET Endpoint Security	
Identifikátor	com.eset.ees.6
Typ identifikátoru	bundleID
Code Requirement	identifier "com.eset.ees.6" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
Aplikace nebo Služba	SystemPolicyAllFiles
Přístup	Allow

ESET Endpoint Antivirus a ESET Endpoint Security	
Identifikátor	com.eset.devices
Typ identifikátoru	bundleID
Code Requirement	identifier "com.eset.devices" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
Aplikace nebo Služba	SystemPolicyAllFiles
Přístup	Allow

ESET Endpoint Antivirus a ESET Endpoint Security

Identifikátor	`com.eset.endpoint`
Typ identifikátoru	`bundleID`
Code Requirement	`identifier "com.eset.endpoint" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP`
Aplikace nebo Služba	`SystemPolicyAllFiles`
Přístup	`Allow`

Instalace

Před zahájením instalace si můžete vytvořit balíček pro vzdálenou instalaci produktu ESET Endpoint Security for macOS v požadované konfiguraci, který následně můžete nasadit prostřednictvím ESET PROTECT nebo vámi preferovaného MDM.

- Vytvoření balíčku pro vzdálenou instalaci

Instalace ESET Endpoint Security for macOS prostřednictvím **klientské úlohy** vytvořené v ESET konzoli pro vzdálenou správu:

- Klientská úloha pro instalaci aplikace v ESET PROTECT
- Klientská úloha pro instalaci aplikace v ESET Security Management Center

Po dokončení instalace

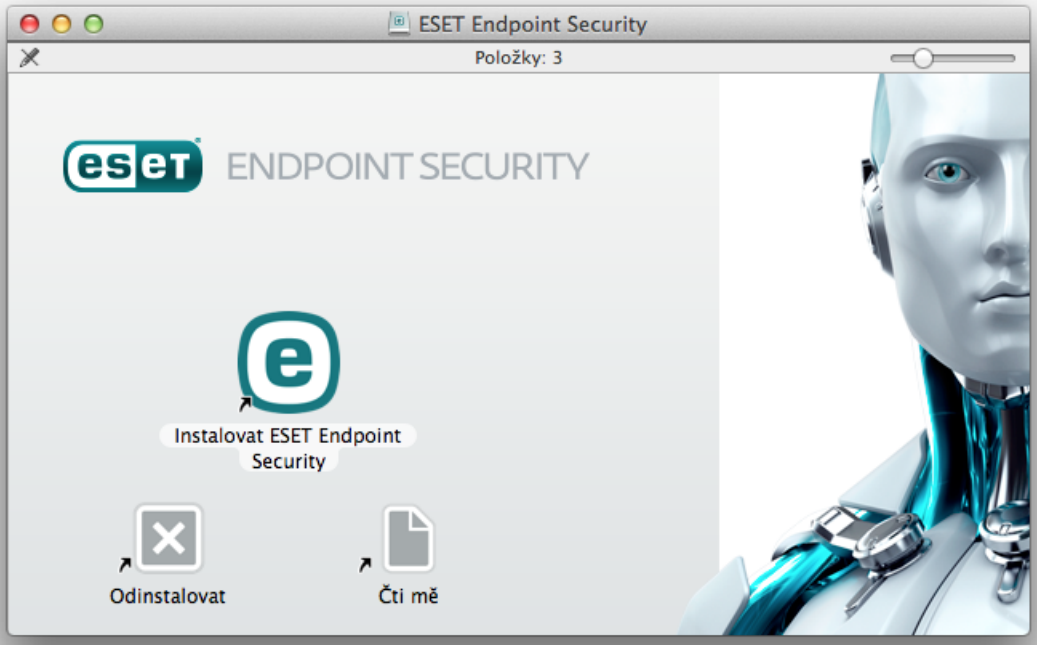
Uživatelům se zobrazí následující upozornění: **"**ESET Endpoint Security for macOS**" by rád filtroval síťovou komunikaci**. Jakmile obdrží toto oznámení, musí kliknout na **Povolit**. Při vybrání možnosti **Nepovolit** nebude ochrana přístupu na web fungovat.

Vytvoření balíčku pro vzdálenou instalaci

Vytvoření instalačního balíčku pro nasazení prostřednictvím Apple Remote Desktop

1. Z webových stránek společnosti ESET si stáhněte běžný instalační balíček:
ESET Endpoint Security for macOS

2. Instalační balíček ESET Endpoint Security for macOS spusťte dvojklikem na stažený soubor.



1. Klikněte **Instalovat** ESET Endpoint Security for macOS.

2. Po zobrazení výzvy klikněte na tlačítko **Povolit**, čímž instalační balíček ověří, zda je možné produkt nainstalovat.

3. Kliknutím na tlačítko **Pokračovat**. Při vytváření balíčku pro vzdálenou instalaci se ESET Endpoint Security for macOS na váš stroj nenainstaluje.

4. Ověřte, zda splňujete systémové požadavky a klikněte na tlačítko **Pokračovat**.

5. Přečtěte si licenční ujednání, a pokud s ním souhlasíte, klikněte na tlačítko **Pokračovat** > **Souhlasím**.

6. V kroku **Režim instalace** vyberte možnost **Vzdálená**.

7. Vyberte si komponenty, které chcete nainstalovat. Standardně se nainstalují všechny komponenty. Klikněte na tlačítko **Pokračovat**.

8. V kroku **Proxy server** vyberte možnost, která vystihuje způsob připojení k internetu. Pokud si nejste jisti, použijte možnost pro převzetí nastavení ze systému. Pokračujte kliknutím na tlačítko **Další**. V případě, že používáte proxy server, v dalším kroku budete vyzváni k zadání adresy proxy serveru a případně přístupových údajů (uživatelského jména a hesla).

9. Vyberte uživatele, kteří budou schopni modifikovat konfiguraci produktu. Oprávněni jsou k tomu privilegovaní uživatelé a skupiny. Standardně je předvybrána administrátorská skupina. Pomocí možnosti **Zobrazit všechny uživatele**, případně **Zobrazit všechny skupiny** si zobrazíte všechny virtuální uživatele a skupiny jako jsou programy a procesy.

10. Dále se rozhodněte, zda chcete na cílovém počítači aktivovat ESET LiveGrid.

11. Dále se rozhodněte, zda chcete na cílovém počítači aktivovat detekci potenciálně nechtěných aplikací.

12. Vyberte režim firewallu:
Automatický režim s výjimkami – výchozí režim. Tento režim je vhodný pro uživatele, kteří si nepotřebují nastavovat vlastní pravidla pro firewall. Automatický režim automaticky povoluje odchozí komunikaci a blokuje příchozí komunikaci, která nebyla vyžádána. Navíc si však můžete v případě potřeby nastavit i vlastní pravidla.

Interaktivní režim – umožňuje vytvořit si vlastní konfiguraci firewallu. Pokud je zjištěna komunikace a není k dispozici odpovídající pravidlo, zobrazí se dialogové okno s výběrem možnosti. V dialogovém okně se můžete rozhodnout, zda komunikaci chcete povolit nebo zakázat. Akce se provede jednou nebo si produkt může rozhodnutí zapamatovat a vytvořit z něj nové pravidlo firewallu. Pokud vyberte možnost pro vytvoření nového pravidla, na identickou komunikaci v budoucnu se použije vytvořené pravidlo.

13. Uložte si instalační balíček do svého počítače. Pokud jste již dříve ve výchozím umístění vytvořili instalační balíček, vyberte jiné cílové umístění nebo před pokračováním dané soubory odstraňte. Tím máte dokončenou první fázi vzdálené instalace. Lokálně spuštěný instalační balíček se ukončí a následně vytvoří ve vámi definované složce soubory pro vzdálenou instalaci.

Soubory pro vzdálenou instalaci jsou následující:

- *esets_setup.dat* – data, která jste definovali při vytváření balíčku v sekci Nastavení.

- *program_components.dat* – informace o komponentách, které se mají nainstalovat. (Tento soubor je volitelný a vytvoří se pouze v případě, kdy nechcete nainstalovat některé komponenty produktu ESET Endpoint Security for macOS.)

- *esets_remote_install.pkg* – balíček pro vzdálenou instalaci

- *esets_remote_uninstall.sh* – skript pro vzdálenou odinstalaci

Nainstalujte si Apple Remote Desktop

1. Spusťte aplikaci Apple Remote Desktop a připojte se k cílovému počítači. Pro více informací se podívejte do uživatelské příručky společnosti Apple.

2. Pomocí funkce **Kopírovat soubor nebo složku** v aplikaci Apple Remote Desktop zkopírujte níže uvedené soubory do složky */tmp* na cílovém počítači:

Pokud chcete nainstalovat všechny komponenty, zkopírujte soubor:
- *esets_setup.dat*

Pokud nechcete nainstalovat všechny komponenty, zkopírujte soubor:
- *esets_setup.dat*
- *product_components.dat*

3. Pro nainstalování balíčku *esets_remote_install.pkg* na cílový počítač použijte příkaz **Nainstalovat balíčky**.

Vzdálené odinstalování prostřednictvím Apple Remote Desktop

1. Spusťte aplikaci Apple Remote Desktop a připojte se k cílovému počítači. Pro více informací se podívejte do uživatelské příručky společnosti Apple.

2. Pomocí funkce **Kopírovat soubor nebo složku** v aplikaci Apple Remote Desktop zkopírujte skript *esets_remote_uninstall.sh* do složky */tmp* na cílovém počítači:

3. V aplikaci Apple Remote Desktop spusťte na cílovém počítači pomocí funkce **Send a UNIX shell command** níže uvedený příkaz:

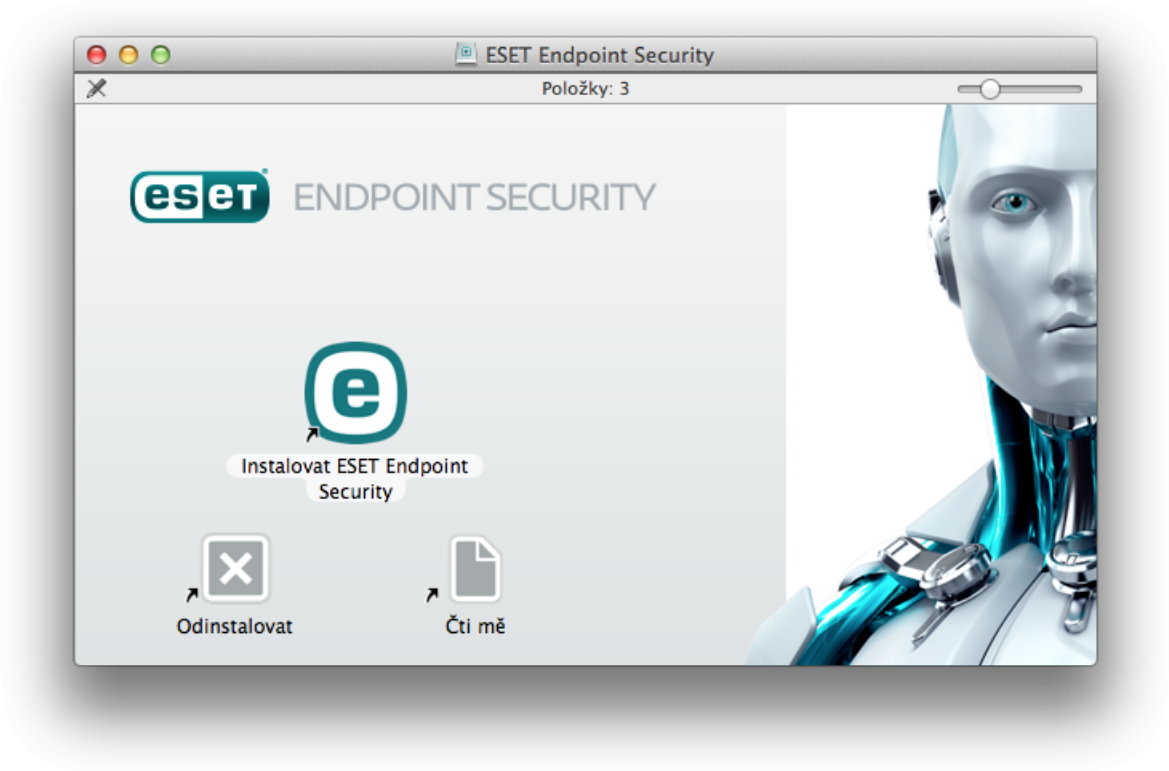
```
/tmp/esets_remote_uninstall.sh
```

Po dokončení procesu odinstalace se na cílovém počítači zobrazí výstup konzole Apple Remote Desktop.

Instalace

Průvodce instalací vás provede základní konfigurací. Detailní návod naleznete v naší Databázi znalostí.

1. Instalační balíček ESET Endpoint Security for macOS spusťte dvojklikem na stažený soubor.



1. Pro zahájení instalace klikněte na tlačítko **Nainstalovat** ESET Endpoint Security for macOS.

> **Instalace z .pkg balíčku**
> V průběhu instalace a prvního spuštění produktu ESET pro macOS je vyžadován přístup k internetu, aby systém mohl ověřit důvěryhodnosti ESET systémových rozšíření.

2. Po zobrazení výzvy klikněte na tlačítko **Povolit**, čímž instalační balíček ověří, zda je možné produkt nainstalovat.

3. V případě, že jste tak dosud neučinili, odstraňte ze systému jiné bezpečnostní aplikace jako je antivirus, antispyware nebo firewall. Pokud v počítači žádný takový software nemáte, klikněte na tlačítko **Pokračovat**.

4. Ověřte, zda splňujete systémové požadavky a klikněte na tlačítko **Pokračovat**.

5. Přečtěte si licenční ujednání, a pokud s ním souhlasíte, klikněte na tlačítko **Pokračovat** > **Souhlasím**.

6. Vyberte typ instalace, který vám vyhovuje.

- Typická instalace
- Pokročilá instalace
- Vzdálená instalace

> **Kontrola verze**
> V počáteční fázi instalace dojde k automatickému ověření, zda není dostupná novější verze produktu. Pokud ano, před pokračováním instalace bude nabídnuto její stažení.

Typická instalace

Typická instalace nainstaluje produkt s doporučeným nastavením, které je vhodné pro většinu uživatelů. Toto nastavení zajišťuje maximální zabezpečení počítače v kombinaci s nízkými nároky na systémové prostředky. Tento typ instalace je předvybrán jako výchozí a je doporučen pro uživatele, kteří nevyžadují specifické nastavení.

1. V okně **ESET LiveGrid** vyberte požadovanou možnost a klikněte na **Pokračovat**. Pokud se později rozhodnete, že chcete nastavení změnit, přejdete do **Nastavení LiveGrid**. Více informací o technologii ESET Live Grid najdete v našem glosáři.
2. V okně **Potenciálně nechtěné aplikace** vyberte požadovanou možnost (viz potenciálně nechtěná aplikace?) a klikněte na **Pokračovat**. Pokud se později rozhodnete, že chcete toto nastavení změnit, použijte **Rozšířeného nastavení**.

3. Klikněte na možnost **Instalovat**. Pokud vás k tomu systém vyzve, zadejte administrátorské heslo do macOS, potvrďte jej a klikněte na tlačítko **Instalovat aplikaci**.

Pro dokončení instalace ESET Endpoint Security for macOS:

macOS Big Sur (11)

1. Povolte systémová rozšíření.

2. Povolte úplný přístup k disku.

3. Umožněte programu ESET přidat do systému konfiguraci proxy. V této souvislosti obdržíte následující upozornění: "ESET Endpoint Security for macOS" **by rád filtroval síťovou komunikaci**. Po obdržení tohoto oznámení klikněte na **Povolit**. Pokud kliknete na **Nepovolit**, nebude ochrana přístupu na web fungovat.

macOS 10.15 a starší

1. Na macOS 10.13 a novější zobrazí operační systém upozornění, že je **blokováno systémové rozšíření**, a v hlavním okně produktu ESET Endpoint Security for macOS se objeví hlášení **Váš počítač není chráněn**. Aby mohl program ESET Endpoint Security for macOS plně fungovat, musíte ručně povolit načítání rozšíření jádra systému. To provedete v **Předvolbách systému** v sekci **Zabezpečení a soukromí**, kde povolte aplikacím vydaným společností **ESET, spol. s.r.o.** načítat rozšíření kliknutím na tlačítko **Povolit.** Další

informace naleznete v Databázi znalostí.

2. Na macOS 10.14 a novějších se v hlavním okně produktu ESET Endpoint Security for macOS objeví hlášení **Váš počítač není plně chráněn**. Aby mohl program ESET Endpoint Security for macOS plně fungovat, musíte aplikaci povolit **Úplný přístup k disku**. Klikněte na **Otevřít předvolby systému** > **Zabezpečení a soukromí**. Přejděte na záložku **Soukromí** a vyberte možnost **Úplný přístup k disku**. Pro povolení změn klikněte na ikonu zámku. Klikněte na ikonu + a ze seznamu vyberte aplikaci ESET Endpoint Security for macOS. Zobrazí se výzva k restartování počítače. Klikněte na tlačítko **Později**. Počítač zatím nerestartujte. V oznámení produktu ESET Endpoint Security for macOS klikněte na tlačítko **Spustit znovu** nebo restartujte počítač. Další informace naleznete v Databázi znalostí.

Po dokončení instalace ESET Endpoint Security for macOS doporučujeme provést kontrolu počítače na přítomnost škodlivého kódu. Pro spuštění kontroly klikněte v hlavním okně programu na záložku **Kontrola počítače** a vyberte možnost **Smart kontrola**. Pro více informací o volitelné kontrole počítače přejděte do kapitoly volitelná kontrola počítače.

Pokročilá instalace

Pokročilá instalace je vhodná pro zkušené uživatele, kteří si chtějí upravit nastavení programu již v průběhu instalace.

- **Programové komponenty**
Vyberte programové komponenty ESET Endpoint Security for macOS, které chcete nainstalovat. Dále pomocí zaškrtávacích polí označte komponenty, které nechcete instalovat.

- **Proxy server**
Pokud pro připojení k internetu používáte proxy server, pro jeho konfiguraci vyberte možnost **Používám proxy server**. Následně do pole **Adresa** zadejte IP adresu nebo URL adresu proxy serveru. Dále zadejte **port**, na kterém proxy naslouchá (standardně 3128). Pokud proxy vyžaduje autentifikaci, zadejte **uživatelské jméno** a **heslo**. Pokud proxy server nepoužíváte, vyberte **Nepoužívám proxy server**. Pokud nevíte, zda pro připojení k internetu používáte proxy server, vyberte možnost **Převzít nastavení ze systému**.

- **Oprávnění**
Můžete definovat seznam privilegovaných uživatelů a skupin, které budou mít oprávnění k úpravě konfigurace programu. Ze seznamu na levé straně vyberte uživatele nebo skupinu a následně klikněte na tlačítko **Přidat** pro přidání uživatele do seznamu **Privilegovaných uživatelů**. Pro zobrazení všech uživatelů dostupných v systému vyberte možnost **Zobrazit všechny uživatele**. Pokud ponecháte seznam prázdný, všichni uživatelé budou privilegovaní.

- **ESET LiveGrid®**
Pro více informací o ESET LiveGrid přejděte do Slovníku pojmů.

- **Potenciálně nechtěné aplikace**
Pro více informací o potenciálně nechtěných aplikacích přejděte do Slovníku pojmů.

- **Firewall**
V posledním kroku můžete vybrat režim filtrování firewallu.

Pro dokončení instalace ESET Endpoint Security for macOS:

macOS Big Sur (11)

1. Povolte systémová rozšíření.

2. Povolte úplný přístup k disku.

3. Umožněte programu ESET přidat do systému konfiguraci proxy. V této souvislosti obdržíte následující upozornění: "ESET Endpoint Security for macOS" **by rád filtroval síťovou komunikaci**. Po obdržení tohoto oznámení klikněte na **Povolit**. Pokud kliknete na **Nepovolit**, nebude ochrana přístupu na web fungovat.

macOS 10.15 a starší

1. Na macOS 10.13 a novější zobrazí operační systém upozornění, že je **blokováno systémové rozšíření**, a v hlavním okně produktu ESET Endpoint Security for macOS se objeví hlášení **Váš počítač není chráněn**. Aby mohl program ESET Endpoint Security for macOS plně fungovat, musíte ručně povolit načítání rozšíření jádra systému. To provedete v **Předvolbách systému** v sekci **Zabezpečení a soukromí**, kde povolte aplikacím vydaným společností **ESET, spol. s.r.o.** načítat rozšíření kliknutím na tlačítko **Povolit**. Další informace naleznete v Databázi znalostí.

2. Na macOS 10.14 a novějších se v hlavním okně produktu ESET Endpoint Security for macOS objeví hlášení **Váš počítač není plně chráněn**. Aby mohl program ESET Endpoint Security for macOS plně fungovat, musíte aplikaci povolit **Úplný přístup k disku**. Klikněte na **Otevřít předvolby systému** > **Zabezpečení a soukromí**. Přejděte na záložku **Soukromí** a vyberte možnost **Úplný přístup k disku**. Pro povolení změn klikněte na ikonu zámku. Klikněte na ikonu + a ze seznamu vyberte aplikaci ESET Endpoint Security for macOS. Zobrazí se výzva k restartování počítače. Klikněte na tlačítko **Později**. Počítač zatím nerestartujte. V oznámení produktu ESET Endpoint Security for macOS klikněte na tlačítko **Spustit znovu** nebo restartujte počítač. Další informace naleznete v Databázi znalostí.

Po dokončení instalace ESET Endpoint Security for macOS doporučujeme provést kontrolu počítače na přítomnost škodlivého kódu. Pro spuštění kontroly klikněte v hlavním okně programu na záložku **Kontrola počítače** a vyberte možnost **Smart kontrola**. Pro více informací o volitelné kontrole počítače přejděte do kapitoly volitelná kontrola počítače.

Lokální povolení systémových rozšíření

V macOS 11 (Big Sur) bylo rozšíření jádra nahrazeno systémovými rozšířeními. Pro načtení nových systémových rozšíření třetích stran je nutný souhlas uživatele.

Na macOS 11 a novější zobrazí operační systém upozornění, že je blokováno systémové rozšíření, a v hlavním okně produktu ESET Endpoint Security for macOS se objeví hlášení **Váš počítač není chráněn**. Aby mohl program ESET Endpoint Security for macOS plně fungovat, musíte ručně povolit načítání rozšíření jádra systému.

Aktualizace z předchozí verze macOS na Big Sur.
Pokud máte nainstalovaný ESET Endpoint Security for macOS a chcete provést aktualizaci na macOS Big Sur, povolte po aktualizaci ručně rozšíření jádra ESET. Je vyžadován fyzický přístup ke klientskému počítači – při vzdáleném přístupu je tlačítko **Povolit** zakázáno.

Pokud máte nainstalovaný ESET Endpoint Security for macOS na macOS Big Sur a novějším, povolte ručně systémová rozšíření ESET. Je vyžadován fyzický přístup ke klientskému počítači – při vzdáleném přístupu je tato vypnutá.

Ruční povolení systémových rozšíření

1. Klikněte na **Otevřít předvolby systému** nebo **Otevřít předvolby zabezpečení**.

2. Pro povolení změn klikněte na ikonu zámku vlevo dole.

3. Využijte funkci Touch ID nebo klikněte na **Použít heslo** a zadejte své uživatelské jméno a heslo a poté klikněte na možnost **Odemknout**.

4. Klikněte na tlačítko **Detaily**.

5. Vyberte všechny položky ESET Endpoint Security for macOS**.app**.

6. Klikněte na tlačítko **OK**.

Pro podrobný návod si prostudujte článek v Databázi znalostí. (Obsah nemusí být dostupný ve všech jazycích.)

Lokální povolení úplného přístupu k disku

Na macOS 10.14 se v hlavním okně produktu ESET Endpoint Security for macOS objeví hlášení **Váš počítač není plně chráněn**. Aby mohl program ESET Endpoint Security for macOS plně fungovat, udělte aplikaci **Úplný přístup k disku**:

1. Klikněte na **Otevřít předvolby systému**.

2. Pro povolení změn klikněte na ikonu zámku vlevo dole.

3. Využijte funkci Touch ID nebo klikněte na **Použít heslo** a zadejte své uživatelské jméno a heslo a poté klikněte na možnost **Odemknout**.

4. Vyberte ze seznamu ESET Endpoint Security for macOS**.app** .

5. Tím se zobrazí oznámení o restartu ESET Endpoint Security for macOS. Klikněte na tlačítko **Později**.

6. Vyberte ze seznamu možnost **ESET rezidentní ochrana souborového systému**.

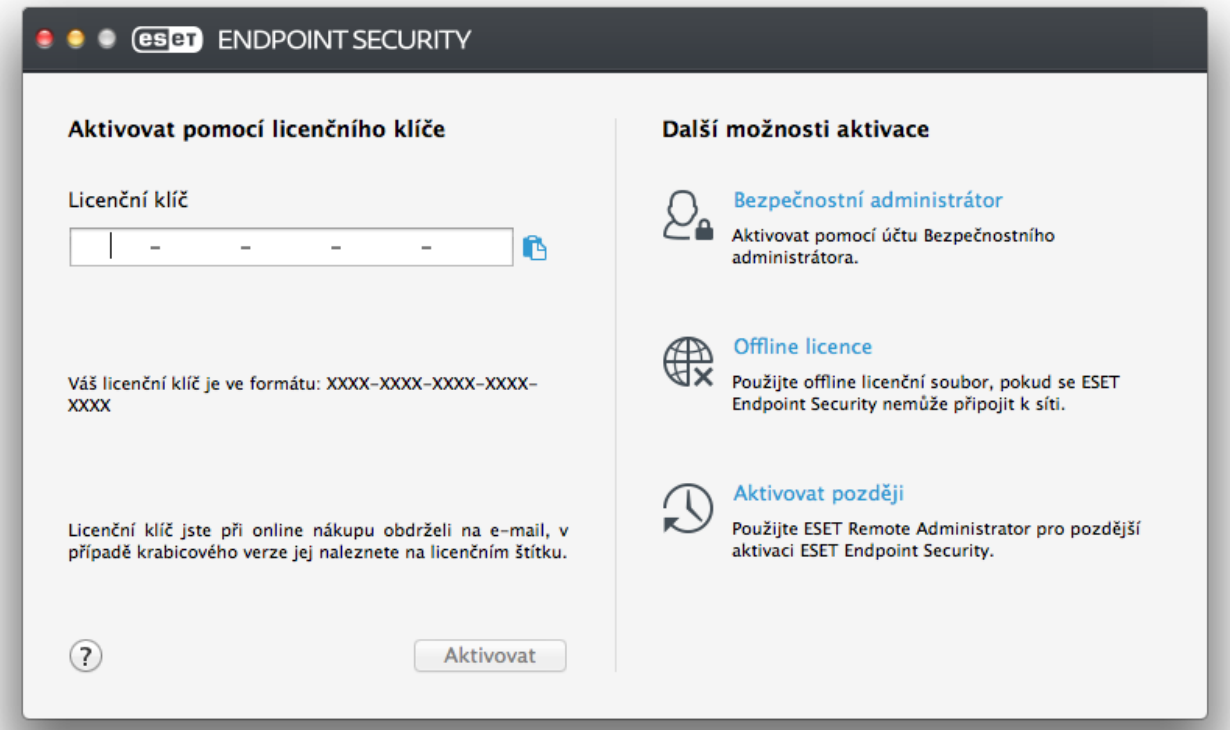
> **Nedostupná ESET rezidentní ochrana souborového systému**
> Pokud v seznamu není možnost **Rezidentní ochrana souborového systému** uvedena povolte pro produkt ESET systémová rozšíření.

7. V oznámení produktu ESET Endpoint Security for macOS klikněte na tlačítko Spustit znovu nebo restartujte počítač. Více si přečtete v databázi znalostí. (Obsah nemusí být dostupný ve všech jazycích.)

Aktivace produktu

Po dokončení instalace budete vyzváni k aktivaci produktu. Produkt můžete aktivovat několika způsoby. Dostupnost jednotlivých metod závisí na zemi a způsobu distribuce (CD/DVD, webové stránky společnosti ESET, apod.).

Pro aktivaci ESET Endpoint Security for macOS klikněte na ikonu na hlavním panelu macOS a vyberte možnost **Aktivovat produkt**. Produkt můžete aktivovat také v hlavním okně po kliknutí na záložku **Nápověda a podpora** > **Aktivovat licenci** nebo **Stav ochrany** > **Aktivovat licenci**.



ESET Endpoint Security for macOS můžete aktivovat níže uvedenými způsoby:

- **Licenční klíč** – unikátní řetězec znaků ve formátu XXXX-XXXX-XXXX-XXXX-XXXX, který slouží pro identifikaci vlastníka licence a aktivaci. Licenční klíč jste obdrželi na e-mail po nákupu licence nebo jej naleznete na licenčním štítku.
- **Účet Bezpečnostního administrátora** – prostřednictvím účtu vytvořeného na licenčním portále ESET License Administrator můžete spravovat více licencí pohodlně z jednoho místa.
- **Offline licenční soubor** – automaticky generovaný soubor obsahující informace o licenci. Offline licenční soubor si můžete vygenerovat na licenčním portále použít jej pro aktivaci stanic, které nejsou připojeny k internetu a není možné je aktivovat jiným způsobem.

Možnost **Aktivovat později** použijte v případě, že je počítač připojen k internetu a vzdáleně spravován prostřednictvím ESET Remote Administrator. Tuto možnost můžete použít také v případě, kdy chcete klienta

aktivovat později jiným způsobem.

> **Tichá aktivace**
> Prostřednictvím ESET Remote Administrator můžete aktivovat produkt vzdáleně a plně automaticky.

ESET Endpoint Security for macOS od verze 6.3.85.0 můžete aktivovat přímo z Terminálu pomocí níže uvedeného příkazu:

```
sudo ./esets_daemon --wait-respond --activate key=XXXX-XXXX-XXXX-XXXX-XXXX
```

Pouze nahraďte `XXXX-XXXX-XXXX-XXXX-XXXX` vaším platným licenčním klíčem, který používáte pro aktivaci ESET Endpoint Security for macOS a registrovali jste jej na portále ESET License Administrator. Při úspěšné aktivaci příkaz vrátí "OK", v opačném případě kód chyby.

Odinstalace

Odinstalaci ESET Endpoint Security for macOS můžete provést třemi způsoby:

- otevřete instalační (*.dmg*) balíček produktu ESET Endpoint Security for macOS a odinstalaci spusťte dvojklikem na tlačítko **Odinstalovat**,

- Spusťte **Finder**, otevřete složku **Aplikace**, stiskněte klávesu CTRL a klikněte na ikonu **ESET Endpoint Security for macOS**. Z nabídky vyberte možnost **Zobrazit obsah balíčku**, otevřete složku **Contents** > **Helpers** a dvakrát klikněte na **Uninstaller**.

> **Odinstalace**
> Aby bylo možné ESET Endpoint Security for macOS komletně odstranit, v průběhu odinstalace bude nutné zadat několikrát heslo administrátora.

Základní přehled

Hlavní okno produktu ESET Endpoint Security for macOS je rozděleno na dvě hlavní části. Pravá část slouží k zobrazování informací, přičemž její obsah závisí na vybrané možnosti v levém menu.

Následuje popis jednotlivých záložek hlavního menu v levé části okna:

- **Stav ochrany** – v přehledné formě poskytuje informace o stavu ochrany počítače, přístupu na web, poštovních klientů a firewallu.

- **Kontrola počítače** – umožňuje nastavit a spustit tzv. Smart nebo volitelnou kontrolu počítače a kontrolu výměnných médií,

- **Aktualizace** – zobrazuje informace o aktualizacích detekčních modulů,

- **Nastavení** – obsahuje možnosti nastavení ochrany počítače.

- **Nástroje** – zajišťují přístup k Protokolům, Plánovači, Karanténě, Běžícím procesům a dalším funkcím programu.

- **Nápověda a podpora** – poskytuje přístup k nápovědě, ESET Databázi znalostí a webové stránce společnosti ESET. Dále zde můžete přímo vytvořit dotaz na technickou podporu a v dolní části okna naleznete informace o aktivaci produktu.

Klávesové zkratky

Klávesové zkratky, které můžete používat při práci s programem ESET Endpoint Security for macOS:

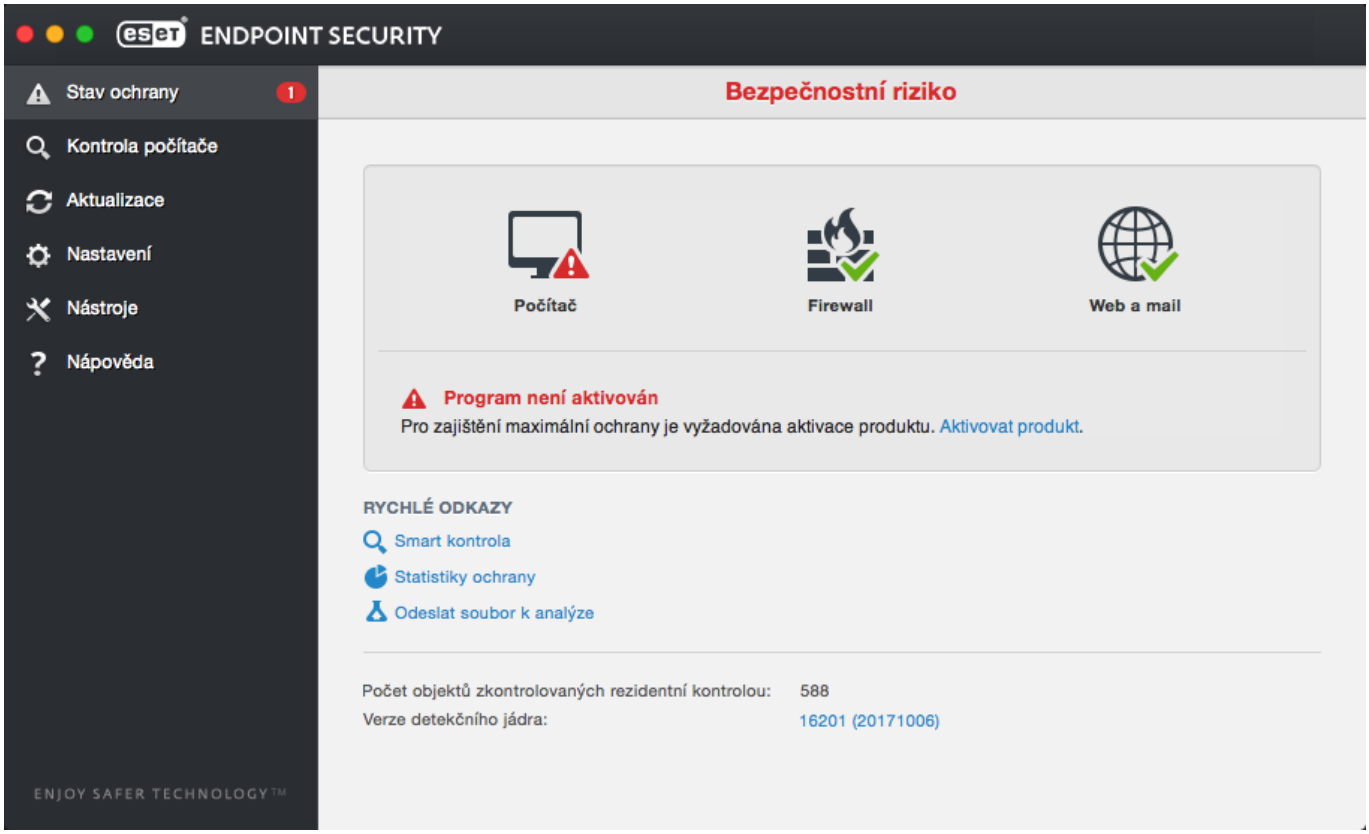
- *cmd+,* – zobrazí Rozšířená nastavení produktu ESET Endpoint Security for macOS
- *cmd+O* – obnoví výchozí pozici a velikost hlavního okna ESET Endpoint Security for macOS,
- *cmd+Q* – obnoví výchozí pozici a velikost hlavního okna ESET Endpoint Security for macOS, Znovu otevřít jej můžete kliknutím na ikonu produktu ESET Endpoint Security for macOS v menu baru macOS,
- *cmd+W* – zavře hlavní okno ESET Endpoint Security for macOS.

Následující klávesové zkratky můžete použít pouze v případě, že máte aktivovanou možnost **Použít standardní menu**, jejíž nastavení naleznete po kliknutí v hlavním okně programu v **Nastavení** > **Otevřít rozšířená nastavení programu...** (nebo po stisknutí klávesy *cmd+,*) > **Rozhraní**:

- *cmd+alt+L* – otevře **Protokoly**
- *cmd+alt+S*– otevře **Plánovač**
- *cmd+alt+Q* – otevře **Karanténu**

Zjištění stavu ochrany

Pro zjištění aktuálního stavu programu a ochrany operačního systému přejděte v hlavním menu na záložku **Stav ochrany**. V pravé části ESET Endpoint Security for macOS se zobrazí stav jednotlivých modulů ochrany.



Co dělat, pokud program nepracuje správně

Při plné funkčnosti ochrany má ikona stavu ochrany zelenou barvu. V opačném případě je barva červená nebo žlutá a není zajištěna maximální ochrana. Zároveň jsou na záložce Stav ochrany v hlavním okně programu zobrazeny bližší informace o stavu jednotlivých modulů a návrh na možné řešení problému pro obnovení maximální ochrany. Pro změnu stavu jednotlivých modulů klikněte na odkaz v zobrazeném oznámení.

Pokud uvedený návrh na řešení problému nezabral, zkuste prohledat ESET Databázi znalostí nebo kontaktujte technickou podporu ESET. Technická podpora Vám odpoví na Vaše otázky ohledně ESET Endpoint Security for macOS co nejdříve.

Ochrana počítače

Jednotlivé moduly ochrany počítače naleznete v hlavním okně programu na záložce **Nastavení** > **Počítač**. Zjistíte zde například stav **rezidentní ochrany souborového systému**. Pomocí přepínače **ZAPNUTO/VYPNUTO** můžete daný modul deaktivovat. Mějte na paměti, že deaktivováním ochrany dojde ke snížení úrovně zabezpečení počítače. Pro konfiguraci jednotlivého modulu ochrany klikněte na tlačítko **Nastavit...**

Antivirová a antispywarová ochrana

Antivirová ochrana chrání systém před útoky a manipulací se soubory, které představují potenciální hrozbu. Při detekci dokáže modul antivirové ochrany škodlivý kód zablokovat, vyléčit případně vymazat nebo umístit do karantény.

Obecné

V **rozšířeném nastavení** (dostupném po stisknutí kláves cmd + , v hlavním okně programu nebo po kliknutí na **Nastavení** > **Otevřít rozšířená nastavení programu…**) můžete v sekci **Obecné** nastavit detekci těchto druhů aplikací:

- **Potenciálně nechtěné aplikace** – sice nemusí představovat bezpečnostní riziko, ale mohou mít negativní dopad na výkon počítače. Tyto aplikace se obvykle do systému nainstalují až po souhlasu uživatele. Jejich instalací dojde k určitým změnám v chování systému (ve srovnání se stavem jejich přítomnosti). Nejčastěji se jedná o zobrazování oken (popup, reklamy), aktivaci a spouštění skrytých procesů, způsobují zvýšenou spotřebu systémových prostředků, ovlivňují výsledky vyhledávání a komunikují se servery výrobce aplikace.

- **Potenciálně zneužitelné aplikace** – Existuje řada legitimních programů, které za běžných podmínek zjednodušují například správu počítačových sítí. V nesprávných rukách však mohou být zneužity k nekalým účelům bez vědomí uživatele. Například se jedná o aplikace pro zobrazení vzdálené plochy a standardně je tato možnost vypnuta.

- **Podezřelé aplikace** – Jedná se o aplikace, které jsou komprimovány pomocí packerů nebo protektorů. Ty často zneužívají autoři malware, aby se vyhnuli detekci. Packery jsou runtime samorozbalovací spustitelné soubory, které spojují několik druhů škodlivého kódu do jednoho balíčku. Nejběžnějšími packery jsou UPX, PE_Compact, PKLite a ASPack. Stejný malware může být detekován odlišně, pokud je komprimován pomocí rozdílných metod. Packery navíc dokáží v průběhu času měnit své "podpisy" ve snaze vyhnout se detekci ze strany antivirových programů.

Pro vytvoření výjimky v rezidentní a internetové ochraně klikněte na tlačítko **Nastavit**.

Výjimky

V sekci Výjimky můžete vyloučit konkrétní soubory/složky, aplikace nebo adresy IP/IPv6 ze skenování.

Soubory a složky definované na záložce **Souborový systém** budou vyloučeny z kontroly souborů zaváděných při startu počítače, rezidentní ochrany souborového systému i volitelné kontroly počítače.

- **Cesta** – cesta k souboru nebo složce.

- **Hrozba** – pokud je vedle vyloučeného souboru zobrazen název hrozby, pak to znamená, že daný soubor je vyloučen ze skenování této konkrétní infiltrace. V případě, že je nakažen jiným druhem infiltrace, detekce proběhne.

-  – vytvoří novou výjimku. Při definování cesty k objektu můžete použít zástupné znaky (*a ?), případně konkrétní soubor nebo složku vybrat ze stromové struktury.

-  – odstraní vybranou výjimku.

- **Výchozí** – vrátí seznam výjimek do posledního uloženého stavu.

Na záložce **Web a mail** můžete vyloučit **aplikace** nebo **IPv4/IPv6 adresy** z filtrování protokolů.

Kontrola po startu

Tato kontrola analyzuje soubory, které se automaticky zavádějí při startu počítače do operační paměti. Ve výchozím nastavení se tato kontrola spouštění jako naplánovaná úloha při přihlášení uživatele a po úspěšné aktualizaci modulů. Pro změnu nastavení parametrů skenovacího jádra ThreatSense klikněte na tlačítko **Nastavení...**. Více informací o nastavení skenovacího jádra ThreatSense naleznete v této kapitole.

Rezidentní ochrana souborového systému

Rezidentní ochrana souborového systému kontroluje všechny typy médií a spouští se při mnoha typech událostí. Využívá metody detekce technologie ThreatSense (blíže popsáno v kapitole Nastavení parametrů skenovacího jádra ThreatSense), a může se lišit pro nově vytvořené a již existující soubory. Na vytvořené soubory se může použít hlubší úroveň kontroly.

Ve výchozím nastavení jsou kontrolovány soubory při jejich **otevření**, **vytvoření** nebo **spuštění**. Doporučujeme ponechat standardní nastavení, které poskytuje maximální možnou ochranu vašeho počítače. Standardně se rezidentní ochrana spouští ihned po startu a běží nepřetržitě na pozadí. V některých speciálních případech (například při konfliktu s jiných rezidentním štítem) ji můžete vypnout kliknutím na ikonu ⓔ produktu ESET Endpoint Security for macOS umístěnou v menu baru a vybráním možnosti **Vypnout rezidentní ochranu souborového systému**. Rezidentní ochranu také vypnete v hlavním okně na záložce **Nastavení** > **Počítač** pomocí přepínače **ZAPNUTO/VYPNUTO** u možnosti **Rezidentní ochrana souborového systému**).

Rezidentní kontrola může kontrolovat tyto typy médií:

- **Lokální disky** – systémové pevné disky;
- **Výměnná média** – CD, DVD, USB, Bluetooth atd.;
- **Síťové jednotky** – namapované síťové jednotky.

Nastavení doporučujeme měnit pouze v ojedinělých případech, například když pozorujete zpomalení při práci s daným typem média.

Konfigurovat nastavení rezidentní ochrany můžete v **Rozšířeném nastavení** (dostupném po stisknutí kláves *cmd + ,* v hlavním okně programu) v sekci **Rezidentní ochrana** po kliknutí na tlačítko **Nastavit** u možnosti **Rozšířená nastavení** (blíže popsáno v kapitole Rozšířená nastavení kontroly).

Rozšířená nastavení

V tomto okně můžete definovat typy objektů kontrolované skenovacím jádrem ThreatSense. Pro více informací o kontrole **samorozbalovacích archivů**, **runtime archivů** a **rozšířené heuristice** přejděte do kapitoly Nastavení parametrů skenovacího jádra ThreatSense.

Nedoporučujeme měnit hodnoty v sekci **Standardní nastavení archivů**. Změnu byste měli provádět pouze v případě, kdy řešíte konkrétní problém, například zpomalení počítače při kontrole vnořených archivů.

Parametry skenovacího jádra ThreatSense – standardně jsou spouštěné soubory kontrolovány za pomoci **Rozšířené heuristika**. Pro snížení dopadu na výkon systému doporučujeme ponechat aktivní **Smart optimalizaci** a

také technologii **ESET LiveGrid**.

Zvýšit kompatibilitu se síťovými jednotkami – po aktivování této možnosti zvýšíte rychlost při přístupu k souborům umístěním na síťové jednotce. Doporučujeme ji aktivovat, pokud pozorujete zpomalení při práci se síťovými soubory. Tato funkce využívá systémový file coordinator, který je dostupný od macOS 10.10. Mějte na paměti, že file coordinator nepodporují všechny aplikace. Například Microsoft Word 2011 jej nepodporuje, zatímco Word 2016 jej podporuje.

Konfigurace rezidentní ochrany

Rezidentní ochrana patří mezi nejdůležitější součástí, pomocí kterých ESET Endpoint Security for macOS pomáhá udržovat počítač zabezpečený. K úpravě parametrů rezidentní ochrany přistupujte vždy s opatrností. Tato nastavení doporučujeme upravovat pouze ve speciálních případech. Například v situaci, kdy nastane konflikt mezi produktem ESET a specifickou aplikací.

Po instalaci ESET Endpoint Security for macOS, jsou všechna nastavení optimalizována pro maximální ochranu počítače. Pro obnovení nastavení na standardní hodnoty klikněte na tlačítko **Standardní** v levé části okna **Rezidentní ochrana** (dostupném po kliknutím v hlavním okně na **Nastavení** > **Otevřít rozšířená nastavení programu…** > **Ochrana** > **Rezidentní ochrana**).

Ověření stavu rezidentní ochrany

Pro ověření funkčnosti rezidentní ochrany použijte testovací soubor eicar.com. Tento soubor je speciální neškodný objekt, který detekují všechny antivirové programy. Soubor vyvinula společnost EICAR (European Institute for Computer Antivirus Research) za účelem testování antivirových programů.

Pro ověření stavu rezidentní ochrany bez použití ESET Security Management Center, se připojte na klientský počítač a v **Terminálu** spusťte následující příkaz:

```
/Applications/.esets/Contents/MacOS/esets_daemon --status
```

Stav rezidentního skeneru se zobrazí jako `RTPStatus=Enabled` nebo `RTPStatus=Disabled`.

Výstup Terminálu bude obsahovat následující informace:

- verze nainstalovaného produktu ESET Endpoint Security for macOS na klientském počítači
- datum a verze aktualizace detekčního jádra
- cesta k aktualizačnímu serveru

> **Používání Terminálu**
> Použití Terminálu doporučujeme pouze pokročilým uživatelům.

Co dělat, když nefunguje rezidentní ochrana?

V této kapitole jsou popsány problémové stavy, které mohou nastat při běhu rezidentní ochrany.

Rezidentní ochrana je vypnutá

Pokud byla rezidentní ochrana nedopatřením vypnuta uživatelem, je potřeba ji znovu aktivovat. Pro opětovné zapnutí rezidentní ochrany přejděte v hlavním menu programu na záložku **Nastavení** > **Počítač** a přepínač u položky **Rezidentní ochrana souborového systému** přepněte do polohy **ZAPNUTO**. Opětovné zapnutí je možné v hlavním okně programu na záložce **Nastavení** pomocí přepínače **ZAPNUTO/VYPNUTO** u možnosti **Rezidentní ochrana souborového systému**.

Rezidentní ochrana nedetekuje a neléčí infiltrace

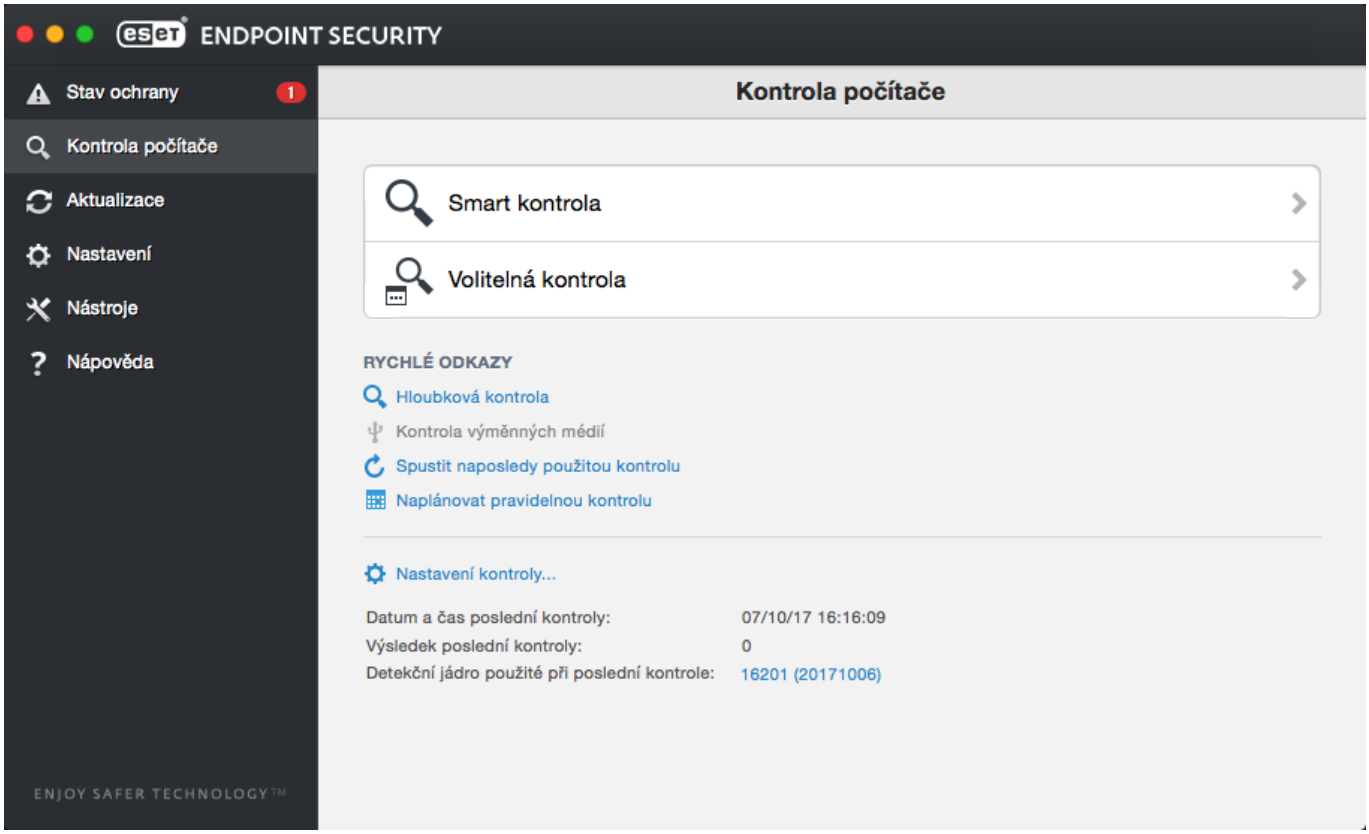
Ujistěte se, zda nemáte nainstalován další antivirový program. Mezi dvěma rezidentními ochranami může docházet ke konfliktu. Proto doporučujeme všechny ostatní antivirové programy odinstalovat, před instalací produktu ESET.

Rezidentní ochrana se nespouští při startu

Pokud se rezidentní ochrana nespouští při startu systému, zřejmě dochází ke konfliktu s jiným programem. V takovém případě doporučujeme kontaktovat technickou podporu společnosti ESET.

Volitelná kontrola počítače

Pokud máte podezření, že je váš počítač napaden škodlivým kódem, spusťte antivirovou kontrolu počítače v hlavním okně na záložce **Kontrola počítače**. Jedním z předpokladů pro udržení co nejvyšší úrovně ochrany jsou pravidelné antivirové kontroly počítače. Pravidelné kontroly mohou detekovat také infiltrace, které nebyly při ukládání na pevný disk identifikovány modulem rezidentní ochrany. Uvedená situace může nastat v případě, pokud byla během ukládání souboru vypnuta rezidentní ochrana, nebo nebyly aktuální detekční moduly.



Doporučujeme provádět kontrolu počítače alespoň jednou měsíčně. Pro pravidelnou kontrolu počítače můžete využít naplánované úlohy, jejichž konfiguraci naleznete v sekci **Nástroje** > **Plánovač**.

Soubory nebo složky, které chcete zkontrolovat můžete též uchopit myší a upustit do hlavního okna ESET Endpoint Security for macOS nebo na ikonu aplikace v menu baru, docku nebo seznamu aplikací (ve **Finder**u složka */Aplikace*).

Typ kontroly

K dispozici jsou dva druhy antivirové kontroly počítače. **Smart kontrola** rychle zkontroluje celý počítač s doporučeným nastavením kontroly. **Volitelná kontrola** umožňuje měnit parametry kontroly a také vybrat vlastní cíle (soubory, složky, média), které budou kontrolovány.

Smart kontrola

Smart kontrola je rychlá kontrola počítače, která léčí infikované soubory bez potřeby zásahu uživatele. Hlavní výhodou tohoto typu kontroly je její snadné použití bez nutnosti podrobného nastavování parametrů kontroly. Smart kontrola zkontroluje všechny soubory a složky a automaticky vyléčí nebo odstraní nalezené hrozby. Úroveň léčení je automaticky nastavena na standardní hodnotu. Pro podrobnější informace týkající se možností léčení si prostudujte kapitolu Léčení.

Volitelná kontrola

Volitelná kontrola je vhodným řešením, pokud chcete upravit parametry kontroly jako jsou cíle a metody kontroly. Výhodou volitelné kontroly je možnost podrobně specifikovat její parametry. Různé konfigurace můžete ukládat jako profily definované uživatelem, které jsou užitečné zejména pokud je potřeba periodicky opakovat

kontrolu se stejnými parametry.

V menu **Kontrola počítače** > **Volitelná kontrola** vyberte profil a **Cíle kontroly** ze stromové struktury. Cíl kontroly můžete blíže specifikovat i zadáním cesty ke složkám nebo souborům, které chcete zařadit do kontroly. Pokud chcete zkontrolovat systém bez provedení dostupných akcí léčení, vyberte možnost **Kontrolovat bez léčení**. Celkově si můžete vybrat ze tří úrovní léčení po kliknutí na **Nastavit...** > **Léčení**.

> **Volitelná kontrola**
> Volitelnou kontrolu počítače doporučujeme zejména pokročilým uživatelům, kteří již mají předchozí zkušenost s používáním antivirových programů.

Cíle kontroly

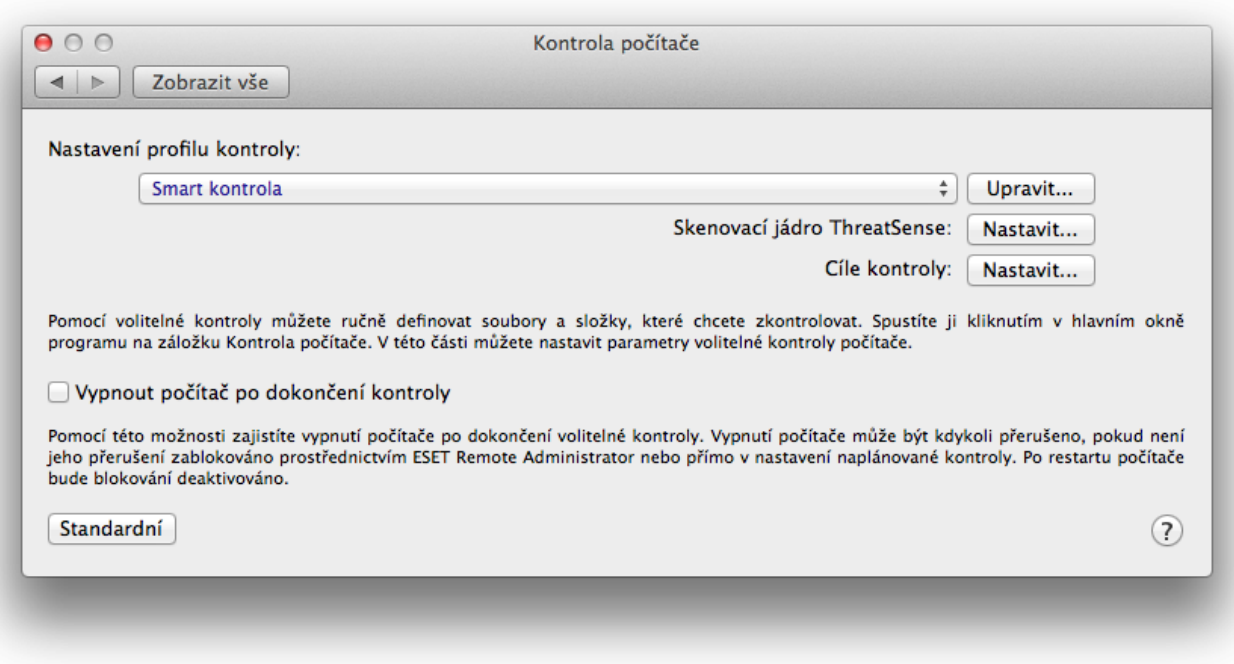
Stromová struktura cílů kontroly slouží k výběru souborů a složek, které budou zkontrolovány. Další složky mohou být automaticky vybrány z nastavení definovaném v profilu kontroly.

Cíl kontroly můžete blíže specifikovat také zadáním cesty ke složkám nebo souborům, které chcete zahrnout do kontroly. Cíle kontroly si vyberte ze stromové struktury, která obsahuje všechny složky ve vašem počítači.

Profily kontroly

Požadované nastavení kontroly si můžete uložit do profilu pro pozdější použití. Doporučujeme vytvořit nový profil (s různými cíli kontroly, metodami a dalšími parametry) pro každou pravidelně používanou kontrolu počítače.

Nový profil si můžete vytvořit v **rozšířeném nastavení** (dostupném po stisknutí kláves *cmd + ,* v hlavním okně programu) v sekci **Ochrana** > **Kontrola počítače** a kliknutím **Upravit...** vedle aktuálně vybraného profilu.



V kapitole parametry skenovacího jádra ThreatSense naleznete popis jednotlivých parametrů pro nastavení kontroly počítače.

Příklad

Předpokládejme, že chcete vytvořit vlastní profil kontroly a částečně vám pro tento účel vyhovuje konfigurace Smart kontroly, ale nechcete, aby byly kontrolovány runtime archivy a navíc chcete aplikovat metodu přísného léčení. V okně **Seznam profilů kontroly počítače** zadejte název pro svůj profil, klikněte na tlačítko **Přidat** a potvrďte stisknutím na tlačítko **OK**. Poté upravte parametry **skenovacího jádra ThreatSense** a definujte **cíle kontroly**, tak aby kontrola odpovídala vašim potřebám.

Pokud chcete po dokončení kontroly vypnout počítač, zaškrtněte možnost **Vypnout počítač po dokončení kontroly**.

Nastavení parametrů skenovací jádra ThreatSense

ThreatSense je název technologie, kterou tvoří soubor komplexních metod detekce infiltrace. Tato technologie je proaktivní, poskytuje ochranu i během prvních hodin šíření nové hrozby. K odhalení hrozeb využívá kombinaci několika metod (analýza kódu, emulace kódu, generické signatury, ...), které efektivně kombinuje a zvyšuje tím bezpečnost systému. Skenovací jádro je schopné kontrolovat několik datových toků paralelně a tak maximalizovat svůj výkon a účinnost detekce. Technologie ThreatSense dokáže účinně odstraňovat i rootkity.

Technologie ThreatSense umožňuje nastavit tyto parametry kontroly:

- Typy souborů a přípony, které se mají kontrolovat,
- Kombinace různých detekčních metod,
- Úrovně léčení.

Pro otevření okna s nastavením parametrů ThreatSense klikněte v hlavním okně programu na **Nastavení** > **Otevřít rozšířená nastavení programu...** (případně stiskněte klávesy *cmd+,*)a následně klikněte na tlačítko **Nastavit...** a to v sekci **Ochrana systému**, **Rezidentní ochrana** a **Kontrola počítače**, které používají ThreatSense technologii. Odlišné bezpečnostní scénáře vyžadují rozdílné konfigurace. V rámci technologie ThreatSense můžete konfigurovat následující moduly:

- **Ochrana po spuštění** – kontrola souborů spouštěných po startu,
- **Rezidentní ochrana** – ochrana počítače v reálném čase
- **Kontrola počítače** – kontrola složek a souborů
- **Ochrana přístupu na web**
- **Poštovní ochrana**

Parametry ThreatSense jsou speciálně optimalizovány pro každý modul a jejich změna může podstatně ovlivnit práci systému. Příkladem může být změna nastavení tak, aby byla vždy provedena kontrola runtime archivů, nebo zapnutí rozšířené heuristiky pro modul rezidentní ochrany souborů. Takové změny způsobí celkové zpomalení systému. Proto doporučujeme ponechat původní nastavení ThreatSense parametrů. Určitou volnost v konfiguraci

ponechává modul **Kontrola počítače**.

Objekty

V sekci **Objekty** můžete definovat typy souborů, které se budou kontrolovat na přítomnost infiltrace.

- **Symbolické odkazy** – (dostupné pouze pro volitelnou kontrolu počítače) kontroluje speciální typy souborů, které obsahují řetězec textu definovaný operačním systémem jako cesta k jinému souboru či složce,
- **Soubory e-mailů** – (není dostupné v rezidentní ochraně) kontrola souborů, které obsahují e-mailové zprávy.
- **Poštovní schránky** – (není dostupné v rezidentní ochraně) kontrola uživatelských poštovních účtů. Nesprávné použití může vést ke konfliktu s vaším e-mailovým klientem. Pro více informací o výhodách a nevýhodách si přečtěte tento článek.
- **Archivy** – (není dostupné v rezidentní ochraně) kontrola souborů v archivech (.rar, .zip, .arj, .tar, apod.).
- **Samorozbalovací archivy** – (není dostupné v rezidentní ochraně) kontrola souborů v samorozbalovacích archivech.
- **Runtime archivy** – runtime archivy se na rozdíl od klasických archivů dekomprimují v paměti počítače po spuštění souboru (typicky UPX, ASPack, yoda, FGS, apod.).

Možnosti

V části **Možnosti** můžete vybrat metody, které se použijí při kontrole počítače. Dostupné jsou následující možnosti:

- **Heuristika** – heuristika používá algoritmus pro analýzu (škodlivé) aktivity programů. Hlavní výhodou heuristické detekce je její schopnost identifikovat škodlivý software, který předtím neexistoval.
- **Rozšířená heuristika** – rozšířená heuristika používá jedinečný heuristický algoritmus vyvinutý společností ESET, který dokáže detekovat červy a trojské koně napsané ve vyšších programovacích jazycích. Schopnost detekce je tak značně vyšší právě díky rozšířené heuristice.

Léčení

Nastavení léčení určuje způsob jakým kontrola vyléčí infikované soubory. K dispozici jsou tři úrovně léčení:

- **Neléčit** –- infikované soubory se automaticky nevyléčí. Program zobrazí okno s varováním a možností výběru akce
- **Standardní úroveň léčení** – program se pokusí automaticky vyléčit, nebo vymazat infikovaný soubor. Pokud není možné provést akci automaticky, program nabídne možnost výběru akce
- **Přísné léčení** – program vyléčí, nebo vymaže všechny infikované soubory (včetně archivů). Jedinou výjimku tvoří systémové soubory. Pokud je nelze vyléčit, program zobrazí okno s varováním s možností výběru akce

Standardní režim léčení – léčení archivů

V přednastaveném režimu standardní úrovně léčení je vymazán celý archiv, pouze pokud jsou všechny soubory v archivu infikované. Pokud tedy archiv obsahuje i legitimní soubory (nenapadené), nebude vymazán. Pokud je archiv detekován v režimu přísného léčení, bude tento archiv vymazán pokud obsahuje alespoň jeden soubor s infiltrací, bez ohledu na stav ostatních souborů.

Výjimky

Přípona je část názvu souboru oddělená tečkou. Přípona určuje typ a obsah souboru (například dokument.txt označuje textový dokument). V této části nastavení parametrů ThreatSense můžete definovat typy souborů, které budou kontrolovány.

Standardně se kontrolují všechny soubory bez ohledu na příponu. Do seznamu souborů vyloučených z kontroly může být přidána jakákoli přípona. Pomocí tlačítek + a − můžete povolit nebo zakázat kontrolu požadovaných souborů podle jejich přípon.

Vyloučení přípon je někdy nutné, pokud probíhající kontrola narušuje činnost specifického programu, který k daným typům souborů bude přistupovat. V některých případech může být vhodné vyloučit z kontroly soubory s příponou *log*, *cfg* a *tmp*. Níže uvádíme správný formát zápisu (každá přípona je na samostatném řádku):

log

cfg

tmp

Omezení

V sekci **Omezení** nastavíte maximální velikost kontrolovaných objektů a maximální hloubku skenování v archivech (počet vnořených archivů do něhož je prováděna kontrola):

- **Maximální velikost:** Definuje největší možnou velikost souborů, které budou zkontrolovány. Modul antivirové ochrany bude kontrolovat pouze objekty s menší velikostí než je definovaná hodnota. Nedoporučujeme měnit přednastavenou hodnotu, protože většinou není pro tuto změnu důvod. Doporučujeme, aby tuto hodnotu měnili jen pokročilí uživatelé, kteří mají důvod vyloučení větších objektů z kontroly.

- **Maximální doba kontroly:** Definuje maximální čas věnovaný kontrole jednoho objektu. Pokud uživatel nastaví hodnotu, antivirový modul přestane kontrolovat objekt po uplynutí nastavené doby, bez ohledu na to, zda byla kontrola objektu dokončena či nikoli.

- **Maximální úroveň vnoření**: upravuje maximální hloubku vnoření při kontrole archivů. Pokud nejste zkušený uživatel, nedoporučujeme vám měnit přednastavenou hodnotu 10. Za běžných okolností není důvod toto nastavení měnit. Pokud se kontrola ukončí kvůli překročení počtu úrovní vnoření archivů, celý archiv zůstane nezkontrolován.

- **Maximální velikost souboru**: umožňuje nastavit maximální reálnou velikost souborů v archivech, které budou zkontrolovány. Pokud se kontrola ukončí kvůli tomuto omezení, celý archiv zůstane nezkontrolován.

Ostatní

Používat Smart optimalizaci

Se zapnutou Smart optimalizací se automaticky nastaví nejvýhodnější poměr mezi efektivitou a rychlostí skenování. který spočívá v inteligentním použití různých skenovacích metod pro různé typy souborů v rámci jednotlivých ochranných modulů. Nastavení Smart optimalizace nejsou v produktu definována napevno. Vývojový tým společnosti ESET má možnost dle uvážení měnit moduly prostřednictvím pravidelné automatické aktualizace produktu ESET Endpoint Security for macOS. Pokud je Smart optimalizace vypnuta, aplikuje se při kontrole souborů výhradně nastavení definované uživatelem v nastaveních skenovacího jádra ThreatSense jednotlivých ochranných modulů.

Kontrolovat alternativní datové proudy (platí pro Kontrolu počítače)

Alternativní datové proudy (resource/data forks) používané systémem NTFS jsou běžným způsobem neviditelné asociace k souborům a adresářům. Mnoho virů je proto využívá na své maskování před případným odhalením.

Nalezena infiltrace

Infiltrace se do systému mohou dostat mnoha způsoby: z internetových stránek, sdílených složek, pošty, výměnných médií (USB, externí disky, CD, DVD, diskety atd.).

Pokud váš počítač vykazuje znaky napadení škodlivým kódem, např. je pomalejší, často "mrzne" apod., doporučujeme provést následující kroky:

1. Otevřete ESET Endpoint Security for macOS a klikněte na záložku **Kontrola počítače**.

2. Vyberte **Smart kontrola** (více informací v kapitole Smart kontrola).

3. Po ukončení kontroly si prohlédněte protokol, který obsahuje počet zkontrolovaných, infikovaných a vyléčených souborů.

Pokud chcete zkontrolovat pouze určitou část disku, klikněte na **Volitelná kontrola** a vyberte cíl kontroly.

Obecným příkladem postupu při řešení problému s infiltrací je situace, kdy rezidentní ochrana souborového systému s nastavenou standardní úrovní léčení najde hrozbu a pokusí se o vyléčení nebo vymazání souboru. Pokud modul rezidentní ochrany nemá nastavenou akci, která se má provést, ESET Endpoint Security for macOS vás vyzve prostřednictvím okna s upozorněním k výběru akce. Obvykle jsou k dispozici možnosti **Léčit**, **Smazat** a **Ponechat**. Pokud vyberte **Ponechat**, s infikovaným souborem se neprovede žádná akce, což nedoporučujeme. Výjimkou může být situace, kdy máte jistotu, že soubor je neškodný a byl chybně detekován.

Léčení a mazání
Použijte léčení, pokud byl soubor napaden virem, který k němu přidal škodlivý kód. Infikovaný soubor se tak může v některých případech obnovit do původního stavu. Pokud však soubor obsahuje výhradně škodlivý kód, bude vymazán.

Mazání souborů v archivech
Ve výchozím režimu léčení bude celý archiv vymazán pouze tehdy, pokud obsahuje výhradně infikované a žádné "čisté" soubory. Jinými slovy, archivy se nevymazávají, pokud obsahují i neškodné (nenapadené) soubory.

Opatrnost je však nutná, pokud spustíte kontrolu s nastavením **Přísné léčení** - v režimu Přísné léčení bude totiž archiv obsahující alespoň jeden soubor s infiltrací, bez ohledu na stav ostatních souborů v archivu smazán.

Webová a poštovní ochrana

Nastavení webové a mailové ochrany najdete po kliknutí v hlavním okně programu na **Nastavení** > **Web a Mail**. Upravit podrobné nastavení jednotlivých modulů ochrany můžete po kliknutí na tlačítko **Nastavit...**.

> **Výjimky**
> ESET Endpoint Security for macOS nekontroluje komunikaci přenášenou šifrovanými protokoly HTTPS, POP3S a IMAPS.

- **Ochrana přístupu na web** – monitoruje HTTP komunikaci mezi webových prohlížečem a vzdálenými servery.
- **Ochrana poštovních klientů** – zajišťuje kontrolu e-mailové komunikace přijímané prostřednictvím POP3 a IMAP protokolu.
- **Anti-Phishingová ochrana** – blokuje potenciální útoky přicházející z webových stránek a domén.
- **Filtrování obsahu webu** – blokuje webové stránky s potenciálně nevhodným a škodlivým obsahem.

Ochrana přístupu na web

Ochrana přístupu na web monitoruje veškerou komunikaci mezi webovými prohlížeči a vzdálenými servery pomocí protokolu HTTP (Hypertext Transfer Protocol) a zajišťuje aplikování definovaných pravidel pro filtrování obsahu.

Ve výchozím nastavení je kontrolována komunikace na standardních portech. V případě potřeby můžete definovat další porty a případně využít seznamy URL adres.

Porty

Na záložce **Porty** můžete definovat čísla portů, které jsou používány pro HTTP komunikaci. Standardně jsou přednastaveny porty 80, 8080 a 3128.

Seznam URL adres

Správa seznamů **URL adres** umožňuje definovat seznamy adres webových stránek, které budou blokovány, povoleny, nebo vyloučeny z kontroly. Webové stránky zařazené na seznamu blokovaných stránek nebudou dostupné, zatímco stránky vyloučené z kontroly nebudou kontrolovány na přítomnost škodlivého kódu.

Pokud chcete povolit přístup pouze na adresy uvedené v **Seznamu povolených adres**, aktivujte možnost **Povolit přístup pouze na URL adresy zařazené do seznamu povolených adres**.

Pro aktivování daného seznamu aktivujte možnost **Seznam je aktivní**. Pokud chcete zobrazit upozornění při přístupu na webovou stránku umístěnou na seznamu, zaškrtněte možnost **Upozornit při aplikování adresy ze seznamu**.

V seznamech můžete používat speciální znaky *a ?. Přičemž hvězdička nahrazuje libovolný řetězec a otazník nahrazuje libovolný znak. Vyloučené adresy se nekontrolují proti hrozbám a proto by měl seznam výjimek obsahovat pouze ověřené a důvěryhodné adresy. Rovněž je potřeba dbát opatrnosti při používání speciálních znaků v tomto seznamu.

Poštovní ochrana

Poštovní ochrana zabezpečuje kontrolu poštovní komunikace přijímané prostřednictvím protokolu POP3 a IMAP. Při kontrole přijímaných zpráv jsou použity všechny pokročilé metody obsažené ve skenovacím jádru ThreatSense produktu ESET Endpoint Security for macOS. Kontrola POP3 a IMAP protokolu je nezávislá na použitém poštovním klientovi.

Jádro ThreatSense – pokročilé nastavení kontroly poštovních klientů jako jsou cíle kontroly, metody detekce atd. Pro zobrazení nastavení klikněte na tlačítko **Nastavit…**.

Přidávat upozornění do poznámky pod čarou – po aktivování této možnosti se bude výsledek kontroly zpráv přidávat na konec zprávy. Tato informace je užitečná, ale není spolehlivá a nemůže být použita pro finální rozhodnutí o škodlivosti zprávy, jelikož některé zprávy mohou být škodlivým kódem pozměněny, případně se nemusí vložit do problematických HTML zpráv. Dostupné jsou následující možnosti:

- **Nikdy** – podpisy nebudou přidávány do žádných kontrolovaných zpráv,
- **Pouze do infikovaných zpráv** – podpisy budou přidávány pouze do infikovaných zpráv,
- **Do všech kontrolovaných zpráv** – ESET Endpoint Security for macOS bude podpisy přidávat do všech kontrolovaných zpráv.

Přidávat do předmětu příchozích a čtených infikovaných zpráv – tuto možnost vyberte, pokud chcete do předmětu zpráv přidat informaci o tom, že je infikována. Pomocí této funkce můžete snadno filtrovat zprávy s nákazou. Dále zvyšuje tato informace důvěryhodnost pro příjemce zprávy. Pokud zpráva obsahuje hrozbu, poskytne tato možnost hodnotné informace o úrovni hrozby.

Šablona přidávaná do předmětu infikovaných zpráv – prefix, který bude přidán do předmětu infikovaných zpráv.

- %avstatus% – přidá informace o stavu infiltrace (příklad: čisté, infikováno, …)
- %virus% – přidá název hrozby
- %product% – přidá název ESET produktu, který provedl kontrolu (v tomto případě ESET Endpoint Security for macOS)
- %product_url% – přidá odkaz na webové stránky společnosti ESET (www.eset.com)

V dolní části tohoto okna se můžete rozhodnout, zda chcete, aby byly kontrolovány zprávy při jejich příjmu prostřednictvím POP3 a IMAP protokolu. Více informací naleznete v následujících kapitolách:

- Kontrola protokolu POP3
- Kontrola protokolu IMAP

Kontrola protokolu POP3

POP3 protokol je nejrozšířenější protokol pro příjem e-mailové komunikace prostřednictvím poštovního klienta. ESET Endpoint Security for macOS zabezpečuje ochranu tohoto protokolu nezávisle na používaném poštovním klientovi.

Modul zabezpečující kontrolu se zavádí při startu operačního systému a po celou dobu je zaveden v paměti. Pro správné fungování stačí ověřit, zda je modul zapnutý. Kontrola POP3 protokolu je prováděna automaticky bez nutnosti konfigurace poštovního klienta. Standardně je kontrolována komunikace na portu 110. V případě potřeby můžete přidat také další používané porty, kdy čísla portů oddělujte čárkou.

Po aktivování možnosti **Zapnout kontrolu protokolu POP3** bude veškerá POP3 komunikace kontrolována na přítomnost hrozeb.

Kontrola protokolu IMAP

(IMAP) (Internet Message Access Protocol) je další internetový protokol pro přijímání e-mailových zpráv. IMAP má v porovnání s protokolem POP3 několik výhod. Umožňuje například připojení více klientů na stejný účet a zachovávání informace stavu zprávy (zda zpráva byla či nebyla přečtena, bylo na ni odpovězeno nebo byla vymazána). ESET Endpoint Security for macOS zabezpečuje ochranu tohoto protokolu nezávisle na používaném poštovním klientovi.

Modul zabezpečující kontrolu se zavádí při startu operačního systému a po celou dobu je zaveden v paměti. Pro správné fungování stačí ověřit, zda je modul zapnutý. Kontrola IMAP protokolu je prováděna automaticky bez nutnosti konfigurace poštovního klienta. Standardně je kontrolována komunikace na portu 143. V případě potřeby můžete přidat také další používané porty, kdy čísla portů oddělujte čárkou.

Aktivovat kontrolu protokolu IMAP – zapne kontrolu poštovní komunikace přes IMAP na přítomnost škodlivého kódu.

Anti-Phishing

Termín phishing definuje kriminální činnost, která využívá sociální inženýrství (manipulace uživatelů za účelem získání citlivých dat). Cílem je získat citlivé údaje, jako například hesla k bankovním účtům, PIN kódy a jiné detaily.

Důrazně doporučujeme tuto ochranu aktivovat v **rozšířeném nastavení** (dostupném po stisknutí kláves cmd + , v hlavním okně programu) v sekci **Anti-Phishingová ochrana** > vybráním možnosti **Zapnout Anti-Phishingovou ochranu**. Poté zablokuje a zobrazí upozornění při detekování všech potenciálních phishingových útoků pocházejících z podezřelých webových stránek a domén.

Firewall

Firewall sleduje veškerý síťový provoz (odchozí i příchozí) a umožňuje konkrétní komunikaci na základě pravidel povolit nebo zakázat. Poskytuje ochranu proti útokům ze vzdálených počítačů a dokáže blokovat některé služby. Dále také poskytuje antivirovou ochranu aplikačních protokolů HTTP, POP3 a IMAP.

> **Výjimky**
> ESET Endpoint Security for macOS nekontroluje komunikaci přenášenou šifrovanými protokoly HTTPS, POP3S a IMAPS.

Nastavení firewallu naleznete v hlavním okně v sekci **Nastavení** > **Firewall**. Změnit můžete režim filtrování, pravidla a další nastavení. Dále zde naleznete přístup k detailnějším nastavením programu.

Pokud přepnete položku **Blokovat veškerou komunikaci** na **ZAPNUTO**, veškerá odchozí a příchozí komunikace bude firewallem blokována. Tuto možnost použijte v případě podezření na kritickou nákazu, při které je nutné odpojit počítač od sítě.

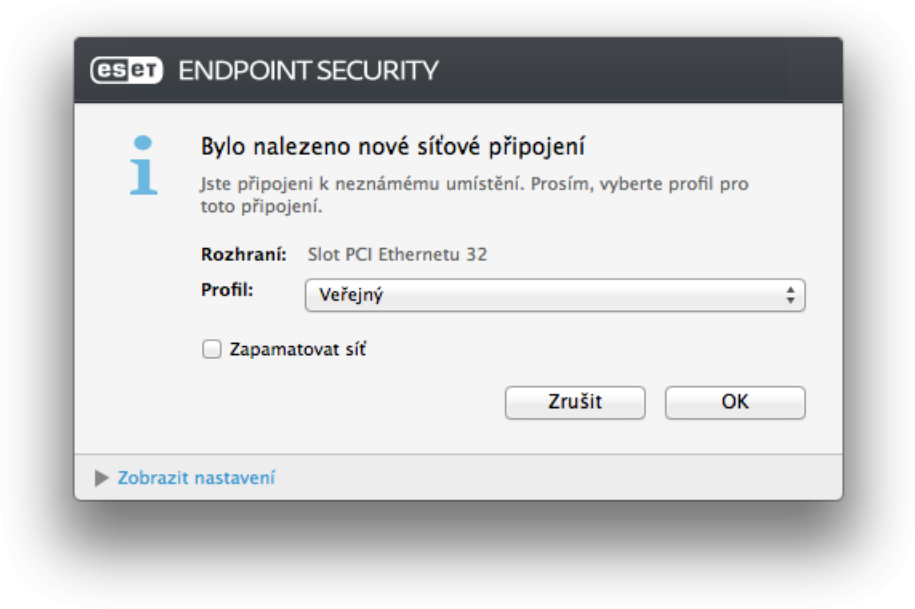
Režimy filtrování

Firewall ESET Endpoint Security for macOS nabízí tři režimy filtrování. Nastavení režimu filtrování naleznete v **rozšířeném nastavení** produktu (dostupném po stisknutí kláves *cmd+,* v hlavním okně programu) v sekci **Firewall**. Chování firewallu se mění s použitým režimem filtrování. Zároveň ovlivňuje míru interakce s uživatelem.

Veškerá komunikace zablokována – všechna příchozí a odchozí spojení budou blokována.

Automatický režim s výjimkami – výchozí režim. Tento režim je vhodný pro uživatele, kteří si nepotřebují nastavovat vlastní pravidla pro firewall. Automatický režim automaticky povoluje odchozí komunikaci a blokuje příchozí komunikaci, která nebyla vyžádána. Navíc si však můžete v případě potřeby nastavit i vlastní pravidla.

Interaktivní režim – umožňuje vytvořit si vlastní konfiguraci firewallu. Pokud je zjištěna komunikace a není k dispozici odpovídající pravidlo, zobrazí se dialogové okno s výběrem možnosti. V dialogovém okně se můžete rozhodnout, zda komunikaci chcete povolit nebo zakázat. Akce se provede jednou nebo si produkt může rozhodnutí zapamatovat a vytvořit z něj nové pravidlo firewallu. Pokud vyberte možnost pro vytvoření nového pravidla, na identickou komunikaci v budoucnu se použije vytvořené pravidlo.



Pokud chcete zaznamenat detailní informace o blokovaných připojeních do protokolu, zaškrtněte možnost **Zapisovat všechna zablokovaná spojení**. Pro prohlížení protokolů pak přejděte v hlavním okně ESET Endpoint Security for macOS na záložku **Nástroje** > **Protokoly** a z rozbalovacího menu **Protokol** vyberte **Firewall**.

Pravidla firewallu

Pravidla firewallu představují soubor podmínek a akcí přiřazených k určitým typům komunikace. V nastavení firewallu můžete určit, jaká akce se má provést při zjištění určité síťové komunikace.

Příchozí spojení jsou ta, která jsou inicializována vzdáleným počítačem. Odchozí spojení fungují opačně, v tomto případě místní systém kontaktuje vzdálený počítač.

Pokud je rozpoznána neznámá komunikace (komunikace, pro kterou neexistuje pravidlo), je třeba zvážit, zda ji povolit či zakázat. Nevyžádaná, nezabezpečená a neznámá spojení představují bezpečnostní riziko pro počítač. Pokud je takové připojení navázáno, doporučujeme věnovat pozornost tomu, jaká aplikace a vzdálený počítač se pokouší připojit na váš počítač. Mnoho infiltrací se pokouší získat a odesílat soukromá data nebo naopak stahovat škodlivý obsah do počítače. Firewall umožňuje detekci a blokování těchto připojení.

Aplikacím podepsaným společností Apple povolit automaticky přístup k síti – standardně mají k síti přístup všechny aplikace podepsané společností Apple. Aby mohly aplikace komunikovat s Apple službami nebo je bylo možné na zařízení nainstalovat, musí být podepsány certifikátem vydaným společností Apple. Pokud chcete toto chování změnit, deaktivujte tuto možnost. Následně aplikace, které nejsou podepsány certifikátem společnosti Apple, budou při pokusu o přístup k síti vyžadovat schválení ze strany uživatele nebo pro ně bude muset existovat pravidlo.

Po deaktivování této možnosti bude jakákoli síťová komunikace se službami podepsanými společností Apple vyžadovat schválení ze strany uživatele, pokud pro ni neexistuje povolovací pravidlo.

Toto chování se ve srovnání s předchozími verzemi změnilo. V ESET Endpoint Security for macOS 6.8 a starších docházelo k blokování příchozí komunikace do služeb podepsaným certifikátem společnosti Apple. V aktuální verzi dokáže produkt ESET Endpoint Security for macOS identifikovat lokálního příjemce příchozí komunikace. To znamená, že pokud je tato možnost zapnutá, dojde k povolení příchozí komunikace.

Vytvoření nového pravidla

Záložka **Pravidla** obsahuje seznam všech pravidel, kterými se řídí komunikace aplikací. Pravidla se přidávají automaticky v závislosti na reakci uživatele na novou komunikaci (interaktivní režim) nebo můžete ručně přidat vlastní pravidla.

1. Pro vytvoření nového pravidla klikněte na **Přidat...**, zadejte jméno pravidla a přetáhněte ikonu aplikace do prázdného pole nebo kliknutím na **Prohledat...** vyhledejte program ve složce */Aplikace*. Pokud chcete aplikovat pravidlo na všechny aplikace v počítači, vyberte možnost **Všechny aplikace**.

2. V dalším kroku specifikujte v poli **Akce**, zda komunikace bude povolena či zakázána a vyberte **Směr** komunikace (příchozí, odchozí, oba). Pokud chcete zaznamenat komunikaci související s konkrétním pravidlem, vyberte možnost **Protokol pravidla**. Pro zobrazení protokolů firewallu přejděte v hlavním okně produktu ESET Endpoint Security for macOS na záložku **Nástroje** > **Protokoly** a z rozbalovacího menu **Protokol** vyberte možnost **Firewall**.

3. V sekci **Protokol/Porty** vyberte protokol, který aplikace používá ke komunikaci a čísla portů (pokud je vybrán TCP nebo UDP protokol). Transportní vrstva představuje bezpečný a efektivní přenos dat.

4. V posledním kroku vyberte **Cíl** (IP adresu, rozsah IP adres, podsíť, ethernet nebo Internet).

Zóny firewallu

Zóna představuje skupinu síťových adres, které dohromady tvoří logickou skupinu. Každá adresa ve skupině má daná práva, která jsou platná pro celou skupinu.

Vlastní zóny můžete vytvořit kliknutím na tlačítko **Přidat...**. V zobrazeném dialogu zadejte **Název** a volitelně **Popis** zóny, vyberte profil a přidejte IP adresy, jejich rozsah, podsíť, Wi-Fi síť nebo jiné síťové rozhraní, které definuje novou zónu.

Profily firewallu

Profily umožňují kontrolovat chování firewallu ESET Endpoint Security for macOS. Při vytváření nebo úpravě pravidel firewallu je můžete přiřadit konkrétnímu profilu. Po vybrání profilu se budou na síťovou komunikaci aplikovat pouze globální pravidla a pravidla přiřazená danému profilu. Můžete také vytvořit více profilů s různými pravidly pro snazší úpravu chování firewallu.

Protokoly firewallu

Firewall ESET Endpoint Security for macOS ukládá důležité události do protokolu. Pro zobrazení protokolů firewallu přejděte v hlavním okně produktu na záložku **Nástroje** > **Protokoly** a z rozbalovacího menu **Protokol** vyberte možnost **Firewall**.

Protokoly jsou cenným nástrojem pro zjišťování chyb a odhalování průniků do systému. Protokol firewallu obsahuje následující informace:

- Datum a čas události,
- Jméno události
- Zdroj
- Síťovou adresu cíle
- Síťový komunikační protokol
- Název použitého pravidla
- Název aplikace
- Jméno uživatele.

Důkladná analýza těchto dat pomáhá odhalovat pokusy o průnik do systému. I další faktory však umožňují rozpoznat nebezpečí a snížit dopad na systém: časté připojování z neznámých lokalit, vícenásobné pokusy o navázání připojení, neznámé aplikace, které komunikují do internetu, nebo použití neobvyklých portů.

Správa zařízení

ESET Endpoint Security for macOS dokáže kontrolovat i blokovat přístup k externím zařízením - stejně tak nabízí možnosti pro přizpůsobení filtrů a uživatelských oprávnění pro přístup a používání paměťových zařízením. To může být užitečné v případě, kdy například administrátor chcete zabránit používaní zařízení s nežádoucím obsahem.

> **Správa zařízení na macOS 11 a novějším**
> ESET Endpoint Security for macOS nainstalovaný na macOS 11 a novějším kontroluje pouze paměťová zařízení (jako jsou USB jednotky, CD/DVD, aj.).

Podporovaná externí zařízení na macOS 10.15 a starším

- Datové úložiště (HDD, výměnné USB jednotky),
- CD/DVD,
- USB tiskárna,
- Obrazové zařízení,
- Sériový port,

- Síť
- Přenosné zařízení

Pokud do počítače vložíte externí zařízení, na které se použije pravidlo o blokování, zobrazí se informační okno a přístup k zařízení bude odepřen.

Zároveň se související informace zaznamenají do protokolu Správy zařízení. Protokoly z fungování tohoto modulu naleznete v hlavním okně programu ESET Endpoint Security for macOS na záložce **Nástroje** > **Protokoly**.

Editor pravidel

Pro zobrazení konfigurace správy zařízení přejděte v hlavním okně programu na záložku **Nastavení**, klikněte na možnost **Otevřít rozšířená nastavení...** a vyberte možnost **Správa zařízení**.

Pro aktivování této funkce v produktu ESET Endpoint Security for macOS zaškrtněte možnost **Zapnout správu zařízení**. Pokud již máte tuto funkci aktivní můžete vytvářet nová a upravovat existující pravidla. Pomocí zaškrtávacího pole vedle názvu pravidla můžete pravidla pohodlně vypínat a zapínat.

Pomocí tlačítek + nebo − přidáte nebo odstraníte pravidlo. Pravidla jsou seřazena dle priority, tedy pravidlo s nejvyšší prioritou je umístěno nahoře. Pro změnu pořadí jednoduše pravidlo přetáhněte na požadovanou pozici (drag&drop) nebo klikněte na ⚙ a vyberte jednu z možností.

ESET Endpoint Security for macOS automaticky detekuje připojená zařízení a jejich parametry (typ zařízení, výrobce, model atp.). Nemusíte pravidlo vytvářet ručně, ale stačí kliknout na tlačítko **Načíst**, vybrat požadované zařízení a dále kliknout na **Pokračovat** pro vytvoření pravidla.

Konkrétní zařízení můžete povolit nebo zakázat pro vybraného uživatele nebo skupinu uživatelů na základě parametrů zařízení, které definujete v konfiguraci pravidla. Seznam pravidel obsahuje popis, tedy název pravidla, typ externích zařízení, akci, která se má provést po připojení k počítači a úroveň protokolování.

Název
Pro snadnější identifikaci do pole **Název** zadejte jméno pravidla. Zaškrtnutím možnosti **Pravidlo je aktivní** dané pravidlo povolíte. Pokud ponecháte tuto možnost neaktivní, pravidlo se nebude uplatňovat a můžete jej použít v budoucnu.

Typ zařízení
Z rozbalovacího menu vyberte typ zařízení. Typy zařízení se přebírají ze systému. Možnost Optická média představuje data uložená na optických médiích jako jsou CD nebo DVD. Úložná média zahrnuje externí disky nebo čtečky paměťových karet připojených pomocí USB nebo FireWire. Příkladem zobrazovacích zařízení jsou fotoaparáty a kamery. Tato zařízení neposkytují informace o uživateli, pouze vyvolávají akce. To znamená, že tato zařízení mohou být blokována pouze globálně.

Akce

Přístup na zařízení, která neslouží pro ukládání dat, může být pouze povolen nebo zakázán. Oproti tomu úložným zařízením můžete nastavit následující práva:

Čtení/Zápis – plný přístup k zařízení,

Pouze pro čtení – uživatel může pouze číst soubory na daném zařízení,

Blokovat – přístup k zařízení bude zakázán.

Typ kritéria

Vyberte, zda chcete pravidlo vytvořit pro jednotlivé **zařízení** nebo **skupinu zařízení.** Pro přizpůsobení pravidel vztažených pouze na konkrétní zařízení můžete použít další parametry:

Výrobce – filtruje podle názvu výrobce nebo ID,

Model – filtruje podle názvu zařízení,

Sériové číslo – filtruje podle sériového čísla, které zpravidla externí zařízení mají. V případě CD/DVD se jedná o sériové číslo média, nikoli mechaniky.

> **Nedefinování parametrů**
>
> Pokud ponecháte výše uvedené údaje prázdné, pravidlo bude tyto hodnoty ignorovat. Filtrování parametrů rozlišuje velikost písmen a nepodporuje zástupné znaky (*, ?). Data musí být zadána tak, jak je poskytuje výrobce.

> **TIP**
>
> Pro získání parametrů zařízení, pro které chcete vytvořit pravidlo, připojte zařízení k počítači a ověřte detaily zařízení v protokolu správy zařízení.

Zaznamenávat do protokolu

Vše – do protokolu se zapíší všechny události

Diagnostické – do protokolu se zapíší informace důležité pro diagnostiku problému

Informační – do protokolu se zapíší informativní zprávy a všechny níže uvedené informace

Varování – do protokolu se zapíší chybové a varovné hlášky

Nikdy – do protokolu se nezapíší žádné informace

Seznam uživatelů

Pravidla můžete přiřadit konkrétnímu uživateli nebo celé skupině uživatelů pomocí dialogového okna Seznam uživatelů

Změnit... – po kliknutí se otevře **Editor identity**, ve kterém můžete vybrat požadovaného uživatele nebo skupinu. Pro sestavení seznamu vyberte v levé části **Uživatele** a klikněte na **Přidat**. Pro odebrání vyberte uživatele v pravé části (**Vybraní uživatelé**) a klikněte na **Odebrat**. Pro zobrazení všech uživatelů dostupných v systému vyberte možnost **Zobrazit všechny uživatele**. Pokud ponecháte seznam prázdný, přístup k zařízení bude povolen/blokován všem uživatelům.

> **Omezení uživatelských pravidel**
>
> Mějte na paměti, že není možné omezit všechna zařízení. Například zobrazovací zařízení neposkytují žádné informace o uživateli, pouze vyvolávají akci.

Filtrování obsahu webu

V sekci **Filtrování obsahu webu** můžete konfigurovat nastavení filtrování obsahu webu, které vám umožňuje chránit vaše zaměstnance a nastavit omezení pro používání zařízení a služeb. Cílem je zabránit zaměstnancům v přístupu na stránky s nevhodným nebo škodlivým obsahem. Filtrování obsahu webu umožňuje blokovat webové stránky, které mohou obsahovat nevhodný obsah. Kromě toho můžete jako zaměstnavatel/administrátor zakázat přístup na 27 předdefinovaných kategorií webových stránek, které jsou dále rozděleny na více než 140 podkategorií.

Standardně je Filtrování obsahu webu vypnuté. Pro zapnutí této funkce přejděte do **Rozšířeného nastavení** (dostupného po stisknutí klávesy **cmd + ,** v hlavním okně programu) a v sekci **Filtrování obsahu webu** a vyberte možnost **Zapnout Filtrování obsahu webu**.

Následně se zpřístupní editor pravidel, pomocí kterého můžete vytvořit pravidlo na konkrétní webovou stránku nebo celou kategorii stránek. V zobrazeném editoru uvidíte seznam pravidel, společně s detailními informacemi jako je prováděná akce, vyhovující URL či kategorie URL a také úroveň protokolování.

Pro vytvoření nového pravidla klikněte na tlačítko  . **Upravit** pravidlo můžete dvojklikem na danou položku.

Pokud nechcete pravidlo odstranit, ale ponechat si jej pro budoucí použití, můžete jej deaktivovat odškrtnutím pole ve sloupci **Zapnuto**.

Typ

Akce na základě URL – dvojklikem otevřete editor **URL/kategorií**, do kterého zadejte požadovanou URL.

V editoru URL nemůžete použít zástupné znaky (* a ?). Pokud je webová stránka dostupná na více národních doménách, je nutné specifikovat všechny případy (*domena.cz*, *domena.sk*, …). Po přidání domény do seznamu dojde k zablokování či povolení přístupu na veškerý obsah umístěný na této doméně včetně subdomén (například po zadání *domena.cz* bude povolen nebo zablokován přístup také na *sub.domena.cz*).

Akce na základě kategorie – dvojklikem otevřete editor **URL/kategorií**, ve kterém vyberte kategorie stránek

Identita

Vyberte uživatele, pro kterého má být pravidlo platné.

Přístupová oprávnění

Povolit – přístup k URL adrese/kategorii bude povolen

Blokovat – přístup k URL adrese/kategorii bude blokován

Zaznamenávat do protokolu (důležité pro filtrování protokolu)

Vše – do protokolu se zapíší všechny události

Diagnostické – do protokolu se zapíší informace důležité pro diagnostiku problému

Informační – do protokolu se zapíší informativní zprávy a všechny níže uvedené informace

Varování – do protokolu se zapíší kritické chyby a varovná hlášení.

Nikdy – do protokolu se nezapíší žádné informace

Nástroje

Na záložce **Nástroje** naleznete součásti, které usnadňují správu programu a nabízejí rozšířené možnosti pro pokročilé uživatele.

Protokoly

Protokoly zachycují všechny podstatné události programu a nabízejí přehled detekovaných hrozeb. Záznamy v protokolech představují důležitý nástroj pro systémové analýzy, detekci hrozeb a řešení problémů. Vytváření protokolů probíhá aktivně na pozadí bez jakékoli interakce s uživatelem. Informace se zaznamenávají podle aktuálních nastavení podrobnosti protokolů. Textové informace a protokoly si můžete prohlédnout i archivovat přímo v prostředí ESET Endpoint Security for macOS.

Protokoly jsou dostupné v hlavním menu ESET Endpoint Security for macOS na záložce **Nástroje** > **Protokoly**. Požadovaný typ protokolu vyberte z rozbalovacího menu **Protokol** v horní části okna. Dostupné jsou následující typy protokolů:

1. **Zachycené hrozby** – tento protokol je vhodné použít k prohlížení všech událostí týkajících se detekce infiltrací,

2. **Události** – všechny důležité akce, které provede ESET Endpoint Security for macOS jsou zaznamenány v tomto protokolu. Tento protokol je určen hlavně správcům systémů a uživatelům při řešení různých problémů,

3. **Kontrola počítače** – výsledky každé kontroly počítače se zobrazují v tomto protokolu. Kliknutím na položku v protokolu zobrazíte podrobnosti vybrané kontroly počítače

4. **Správa zařízení** – obsahuje záznamy o výměnných médiích nebo zařízeních připojených k počítači. V protokolu se zobrazí pouze zařízení, na která byla aplikována pravidla Správce zařízení. Pokud nebylo na zařízení aplikováno žádné pravidlo, záznam v protokolu se nevytvoří. Pro každé zařízení se zobrazí také informace o typu zařízení, sériové číslo, název výrobce a velikost média (pokud jsou dostupné).

5. **Firewall** – protokol obsahuje všechny vzdálené útoky zachycené firewallem. Protokol firewallu obsahuje informace o detekovaných útocích na váš systém. Ve sloupci **Událost** se zobrazuje seznam útoků, ve sloupci **Zdroj** se zobrazují podrobnější informace o útočníkovi a ve sloupci **Protokol** naleznete komunikační protokol použitý při útoku.

6. **Filtrování obsahu webu** – protokol zobrazuje webové stránky, které byly zablokovány nebo povoleny.

7. **Filtrované webové stránky** – tento seznam je užitečný v případě, že si chcete prohlédnout stránky blokované modulem Ochrana přístupu na web nebo Filtrování obsahu webuProtokol obsahuje informace o času, URL adrese, uživateli a aplikaci, která se chtěla na stránky připojit

Jednotlivé události v protokolech můžete kopírovat do schránky vybráním daného protokolu a kliknutím na tlačítko **Kopírovat**.

Údržba protokolů

Nastavení protokolů ESET Endpoint Security for macOS je dostupné z hlavního okna programu po kliknutí na záložku **Nastavení** > **Otevřít rozšířená nastavení programu...** > **Nástroje** > **Protokoly**. Zde můžete nastavit tyto

parametry: Pro protokoly můžete definovat následující možnosti:

- **Automaticky odstranit staré záznamy protokolů** – po vybrání této možnosti se budou automaticky odstraňovat protokoly starší než určený počet dnů.
- **Automaticky optimalizovat protokoly** – tato možnost zajišťuje defragmentaci databáze protokolů podle nastavení horního limitu množství nevyužitých záznamů v procentech.

Všechny související informace zobrazené v grafickém rozhraní, zprávy o nalezených hrozbách a událostech můžete ukládat do čitelné podoby jako plain text nebo CSV (hodnoty oddělené středníkem) soubor. Pokud si chcete tyto soubory následně prohlížet v nástrojích třetích stran vyberte možnost **Zaznamenávat do textových souborů.**

Pro definování cílové složky, do které chcete uložit protokoly, klikněte na tlačítko **Nastavit...** v **Rozšířeném nastavení**.

V závislosti na vybrané možnosti v **Textové protokoly: Upravit** můžete do protokolů ukládat tyto typy informací:

- Události typu *Moduly se nepodařilo aktualizovat*, *Neplatné uživatelské jméno a heslo*, apod. jsou zapsány do souboru *eventslog.txt*.
- Detekované hrozby skenerem po spuštění, rezidentní ochranou nebo kontrolou počítače se zapisují do souboru *threatslog.txt*.
- Výsledky všech dokončených kontrol jsou uloženy do souboru *scanlog.ČÍSLO.txt*.
- Zařízení zablokovaná modulem Správa zařízení jsou uvedeny v souboru devctllog.txt.
- Všechny události související s firewallem naleznete v souboru firewalllog.txt.
- Zablokované stránky modulem filtrování obsahu webu jsou zapisovány do souboru webctllog.txt.

Pro konfiguraci filtrů **Standardní záznamy protokolů kontroly počítače** klikněte na tlačítko **Upravit...** a vyberte/zrušte označení u požadovaných typů záznamů. Více podrobností o protokolech naleznete v této kapitole.

Filtrování protokolů

Protokoly obsahují různé druhy záznamů. Použitím filtru můžete zobrazit protokoly pouze zaznamenávající pouze záznamy specifické události.

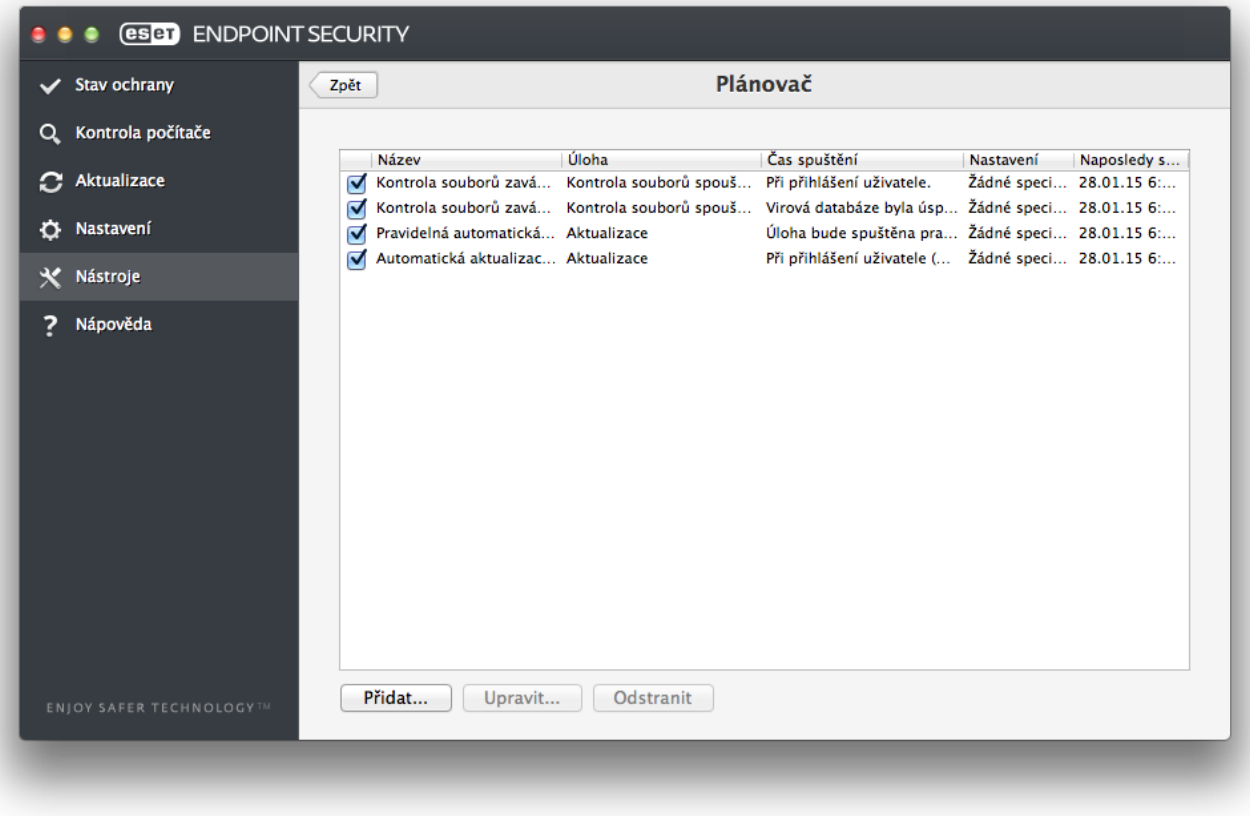
Vybírat můžete z následujících druhů protokolů:

- **Kritická varování** – zaznamenány budou pouze kritické chyby systému (např. nespuštění antivirové ochrany),
- **Chyby** – zaznamenány budou chyby typu "*Chyba při stahování souboru aktualizace"* a kritická upozornění,
- **Varování** – zaznamenány budou varovné zprávy a všechny výše uvedené záznamy,

- **Informační záznamy** – zaznamenány budou informační zprávy (např. o úspěšné aktualizaci) a všechny výše uvedené záznamy,
- **Diagnostické záznamy** – zaznamenány budou informace důležité pro ladění programu a všechny výše uvedené záznamy.

Plánovač

Plánovač najdete v hlavním okně ESET Endpoint Security for macOS na záložce **Nástroje**. **Plánovač** obsahuje seznam všech naplánovaných úloh a jejich nastavení, stejně jako je datum a čas provedením použitý profil kontroly atp.



Plánovač spravuje a spouští naplánované úlohy s nastavenými parametry a vlastnostmi. Parametry úlohy jsou datum, čas nebo jiné podmínky spuštění stejně jako profil kontroly.

Standardně se v plánovači zobrazují tyto naplánované úlohy:

- Údržba protokolů (po aktivování možnosti **Zobrazovat systémové úlohy** v nastavení Plánovače),
- Kontrola souborů spouštěných při startu počítače po přihlášení uživatele,
- Kontrola souborů spouštěných při startu počítače po úspěšné aktualizaci detekčních modulů,
- Pravidelná automatická aktualizace,
- Automatická aktualizace po přihlášení uživatele.

Pro úpravu existujících (a to jak předdefinovaných, tak vlastních) úloh podržte kláves CTRL a klepněte na úkol, který chcete upravit a vyberte možnost **Změnit**, případně po vybrání požadované úlohy klikněte na tlačítko **Změnit**.

Vytvoření nové úlohy

Pokud chcete vytvořit novou úlohu v Plánovači, klikněte na tlačítko **Přidat...** nebo klikněte pravým tlačítkem kamkoli do seznamu úloh a z kontextového menu vyberete **Přidat...**. Vytvořit můžete pět typů naplánovaných úloh:

- **Spuštění aplikace**
- **Aktualizace**
- **Volitelná kontrola počítače**
- **Kontrola souborů spouštěných po startu**

Uživatelem vytvořené úlohy

Po vybrání možnosti Spuštění aplikace můžete spouštět programy jako systémový uživatel "nobody." Oprávnění pro běh aplikací spouštěným pomocí plánovače je definováno v systému macOS. Pro změnu uživatele zadejte na začátek cesty k aplikaci jméno uživatele oddělené dvojtečkou (:). Pomocí této možnosti můžete spustit aplikaci pod uživatelem **root**.

Příklad: Spuštění úlohy jako uživatel

V tomto příkladu si ukážeme, jak spustit pod uživatelem **UserOne** v definovaný čas kalkulačku:
1. V **plánovači** klikněte na tlačítko **Přidat úlohu**.
2. Zadejte název úlohy. Jako **typ úlohy** vyberte možnost **Spustit aplikaci**. V sekci **Spuštění úlohy** vyberte možnost **Jednou** pro jednorázové spuštění úlohy. Pokračujte kliknutím na tlačítko **Další**.
3. Klikněte na tlačítko Procházet a vyberte aplikaci Kalkulačka.
4. Na začátek cesty zadejte **UserOne:** (UserOne:'/Applications/Calculator.app/Contents/MacOs/Calculator') a pokračujte kliknutím na tlačítko **Další**.
5. Vyberte čas, kdy chcete úlohu spustit, a pokračujte kliknutím na tlačítko **Další**.
6. Rozhodněte se, co se stane, pokud se úlohu nepodaří v daném čase spustit, a klikněte na tlačítko **Další**.
7. Klikněte na tlačítko **Dokončit**.
8. Plánovač v produktu ESET spustí v definovaný čas kalkulačku.

Omezení v názvech uživatelů

Mezery nebo bílé znaky nesmí být před jménem uživatele, a ani se v něm nemohou vyskytovat. Místo toho použijte znak reprezentující mezeru.

Kontrola jako vlastník složky

Kontrolu složek můžete spustit pod uživatelem, který je její vlastník:
root:for VOLUME in /Volumes/*; do sudo -u \#`stat -f %u "$VOLUME"` '/Applications/ESET Endpoint Security.app/Contents/MacOS/esets_scan' -f /tmp/scan_log "$VOLUME"; done

Jako aktuálně přihlášený uživatel můžete kontrolovat /tmp složku:
root:sudo -u \#`stat -f %u /dev/console` '/Applications/ESET Endpoint Security.app/Contents/MacOS/esets_scan' /tmp

Příklad: Aktualizační úloha

V tomto příkladu si ukážeme, jak vytvořit aktualizační úlohu, který se spustí v konkrétní čas.

1. Z rozbalovacího menu **Naplánovaná úloha** vyberte možnost **Aktualizace**.
2. Do pole **Název úlohy** zadejte název úlohy.
3. Z rozbalovacíhomenu **Provedení úlohy** vyberte interval, ve kterém chcete úlohu spustit. V závislosti na nastaveném intervalu budou dostupné další volby. Pokud jako interval vyberete **Definované uživatelem**, v dalším kroku je potřeba nastavit datum a čas ve formátu cron (pro více informací se podívejte se do kapitoly Vytvoření uživatelské úlohy).
4. V dalším kroku nastavte, jaká akce se provede v případě, že úlohu nebylo možné provést v naplánovaném čase.
5. Po nastavení všech parametrů se zobrazí souhrn vlastností naplánované úlohy a klikněte na tlačítko **Dokončit**.

Standardně ESET Endpoint Security for macOS obsahuje předdefinované úlohy, které jsou důležité pro správné fungování produktu. Tyto úlohy nemohou být změněny a jsou skryté. Pro zobrazení těchto úloh klikněte v hlavním okně programu na záložku **Nastavení** > **Otevřít rozšířené nastavení programu...**. Následně klikněte na **Nástroje** > **Plánovač** a zaškrtněte možnost **Zobrazovat systémové úlohy**.

Vytvoření uživatelské úlohy

Pokud jako typ naplánované úlohy vyberete uživatelem definovanou, je nutné použít několik speciálních parametrů.

Při tvorbě **uživatelem definované úlohy** zadávejte datum a čas v rozšířeném cron formátu (řetězec obsahující šest polí oddělených mezerou):

```
minuta(0-59) hodina(0-23) den v měsíci(1-31) měsíc(1-12) rok(1970-2099) den v týdnu(0-7)(neděle = 0 nebo 7)
```

Příklad:

```
30 6 22 3 2012 4
```

Speciální znaky podporované v cron formátu:

- hvězdička (`*`) – nahrazuje všechny hodnoty v poli, např. hvězdička ve třetím poli (den v měsíci) znamená každý den
- spojovník (`-`) – definuje rozsah; např. `3-9`
- čárka (`,`) – odděluje položky v seznamu; např. `1,3,7,8`
- lomítko (`/`) – definuje přírůstky v rozsahu; např. `3-28/5` ve třetím poli (den v měsíci) znamená třetí den v měsíci a pak každých 5 dní.

Názvy dnů (Monday-Sunday) a měsíců (January-December) nejsou podporovány.

Uživatelem vytvořené úlohy

Pokud definujete den v měsíci i den v týdnu, úloha se provede pouze v případě, že se obě hodnoty shodují.

ESET LiveGrid®

Systém včasného varování ESET LiveGrid® zajišťuje okamžité informování společnosti ESET v případě výskytu nových hrozeb. Obousměrný systém včasného varování LiveGrid má jediný účel – zlepšení ochrany, kterou vám můžeme poskytnout. Nejlepší způsob, jak zajistit, abychom věděli o nových hrozbách ihned po jejich vypuštění na internet, je spojením s našimi uživateli, a využití získaných informací k aktualizaci detekčních modulů. Vyberte si jednu z následujících možností:

1. Můžete se rozhodnout, že nechcete zapínat systém včasného varování ESET LiveGrid. Nepřijdete tím o žádnou funkci, ale v některých případech může ESET Endpoint Security for macOS reagovat na nové hrozby se zpožděním – dokud nedojde k aktualizaci detekčního jádra.

2. Můžete systém včasného varování ESET LiveGrid nakonfigurovat pro odesílání anonymních informací o nových hrozbách společně s informací, kde byl soubor detekován. Tyto informace mohou být odeslány do virových laboratoři ESET k bližší analýze. Jejich analýza nám pomůže vylepšovat detekční schopnosti programu a aktualizovat detekční moduly.

ESET LiveGrid® sbírá anonymní informace z vašeho počítače přímo související s novými hrozbami. Tyto informace mohou obsahovat vzorek nebo kopii souboru, ve kterém byla zjištěna hrozba, cestu k tomuto souboru, jeho název, datum a čas, jméno procesu, který k souboru přistoupil, a informace o vašem operačním systému.

Protože existuje šance, že po zapojení do systému LiveGrid se mohou do virové laboratoře společnosti ESET v některých případech odesílat soukromé informace o vašem počítači (jako uživatelské jména v cestě ke konkrétní složce apod.), zdůrazňujeme, že tyto informace nebudou NIKDY použity k jinému účelu, než pro okamžitou reakci na nové hrozby.

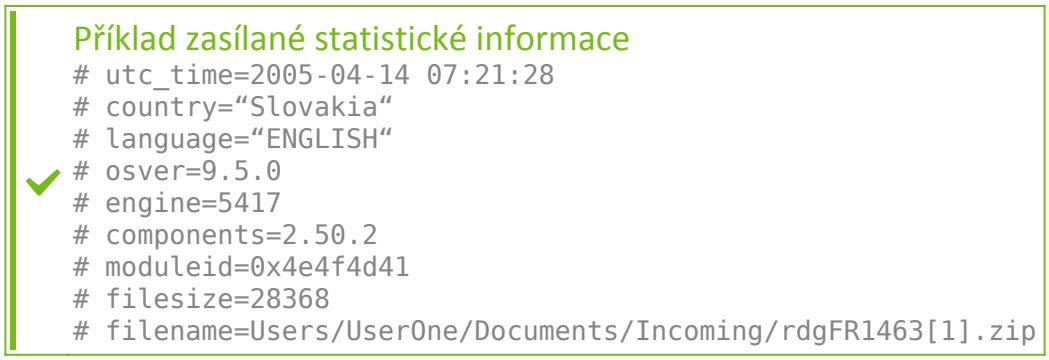
Pro nastavení technologie ESET LiveGrid® klikněte v hlavním okně programu na záložku **Nastavení** a klikněte na **Otevřít rozšířená nastavení programu...** (nebo stiskněte klávesy cmd+,). Dále přejděte do sekce **ESET LiveGrid®**, kde aktivujte možnost **Zapnout systém včasného varování**, a následně klikněte na tlačítko **Nastavit...** vedle možnosti **Rozšířená nastavení**.

Podezřelé soubory

Standardně ESET Endpoint Security for macOS **odesílá** podezřelé soubory do virové laboratoře ESET pro detailní analýzu. Pokud si nepřejete soubory posílat, odškrtněte možnost **Odeslat podezřelé soubory** (v **rozšířeném nastavení** dostupném po stisknutí kláves **cmd+**, v hlavním okně programu v sekci **LiveGrid**

Pokud naleznete podezřelý soubor, můžete jej okamžitě odeslat na analýzu do virové laboratoře ESET. To provedete kliknutím v hlavním okně programu na **Nástroje** > **Odeslat soubor k analýze**. V případě, že se jedná o škodlivou aplikaci, její detekce bude přidána do další aktualizace detekčního jádra.

Odesílat anonymní statistické informace – ESET LiveGrid® sbírá anonymní informace z vašeho počítače přímo související s novými hrozbami. Tyto informace obsahují jméno hrozby, datum a čas detekce, verzi produktu ESET, verzi operačního systému a vaši aktuální pozici. Statistické informace se většinou do laboratoře ESET odesílají dvakrát za den.



Vyloučit tyto soubory – pomocí této možnosti můžete vyloučit vybrané typy souborů, které nechcete odesílat do virové laboratoře ESET. To může být užitečné v případě souborů, které mohou obsahovat důvěryhodné informace, jako jsou dokumenty nebo tabulky. Standardně jsou vyloučeny nejrozšířenější typy souborů ((.doc, .rtf, …). Do seznamu výjimek můžete přidat vlastní typy souborů.

Kontaktní e-mail (nepovinný údaj) – na zadané e-mailové adrese vás mohou kontaktovat specialisté z virové laboratoře ESET za účelem získání dalších informací. Pokud nejsou vyžadovány další informace, standardně nebudete kontaktováni.

Karanténa

Hlavní funkcí karantény je bezpečně uschovat infikované soubory. Soubory jsou uloženy do karantény v případě, že nemohou být léčeny, pokud není bezpečné a doporučené jejich odstranění (systémové soubory) nebo pokud je ESET Endpoint Security for macOS detekoval nesprávně (tzv. falešný poplach).

Do karantény můžete ručně přidat jakýkoli soubor. To je vhodné v případě, kdy podezřelý soubor nebyl detekován antivirovým skenerem. Soubory z karantény můžete zaslat k analýze do virové laboratoře společnosti ESET.

Soubory uložené v karanténě můžete zobrazit v přehledné tabulce, která obsahuje datum a čas přidání souboru do karantény, cestu k původnímu umístění souboru, velikost souboru v bajtech, důvod přidání (např. přidaný uživatelem) a počet infiltrací (např. pokud se jedná o archiv obsahující více infikovaných souborů). Karanténa s uloženými soubory (*/Library/Application Support/Eset/esets/cache/quarantine*) zůstává na disku i po odinstalaci ESET Endpoint Security for macOS. Soubory jsou v karanténě uloženy v bezpečném šifrovaném formátu a můžete je obnovit například v případě nesprávné detekce. Dostupné budou i v případě přeinstalování produktu ESET Endpoint Security for macOS.

Vložení objektu do karantény

ESET Endpoint Security for macOS automaticky přesouvá do karantény soubory, které byly rezidentní ochranou vymazány (pokud jste tuto možnost nevypnuli v okně s upozorněním). V případě potřeby můžete kliknutím na tlačítko **Přesunout...** do karantény přesunout libovolný podezřelý soubor. K tomuto účelu můžete použít také kontextové menu karantény. Stiskněte klávesu CTRL, klikněte pravým tlačítkem do okna karantény a vyberte možnost **Přesunout...**. Následně najděte soubor, který chcete vložit do karantény, a klikněte na tlačítko **Otevřít**. Případně klikněte na soubor nebo složku pravým tlačítkem myši a z kontextového menu vyberte možnost **Služby** > ESET Endpoint Security for macOS - Přidat soubory do karantény.

Obnovení objektu z karantény

Soubory z karantény můžete obnovit do svého původního umístění kliknutím na tlačítko **Obnovit**. Obnovení souboru můžete provést v okně karantény kliknutím pravým tlačítkem myši na daný soubor (při stisknuté klávese CTRL) a vybráním možnosti **Obnovit**. Kontextové menu karantény nabízí také možnosti **Obnovit do...**, pomocí které můžete soubor obnovit do jiného než původního umístění.

Odesílání souborů z karantény k analýze

Pokud jste do karantény umístili podezřelý soubor, který nebyl detekován, nebo pokud byl soubor naopak nesprávně označen jako infikovaný a následně umístěn do karantény, pošlete ho prosím do virové laboratoře společnosti ESET. Stiskněte klávesu CTRL, klikněte pravým tlačítkem na soubor v karanténě a z kontextového menu vyberte možnost **Odeslat soubor k analýze**.

Oprávnění

Správné nastavení ESET Endpoint Security for macOS může být velmi důležité pro podnikovou bezpečnost. Neoprávněné změny mohou ohrozit stabilitu a stav ochrany systému. Můžete tedy nastavit, kteří uživatelé budou mít oprávnění měnit nastavení programu.

Pro definování privilegovaných uživatelů přejděte na záložku **Nastavení** , klikněte na **Otevřít rozšířená nastavení programu…** a následně přejděte do sekce **Uživatelé** > **Oprávnění**.

Pro zajištění maximálního zabezpečení systému je důležité, aby byl program správně nastaven. Neautorizovaná změna můžete vést k ztrátě důležitých dat. Pro nastavení seznamu oprávněných uživatelů vyberte daného uživatele ze seznamu **uživatelů** v levé části dialogového okna **Oprávnění** a klikněte na tlačítko **Přidat**. Všechny systémové účty zobrazíte po zaškrtnutí možnosti **Zobrazit všechny uživatele**. Pro zobrazení všech uživatelů dostupných v systému vyberte možnost **Zobrazit všechny uživatele**.

> **Prázdný seznam privilegovaných uživatelů**
> Pokud ponecháte seznam oprávněných uživatelů prázdný, všichni uživatelé budou automaticky považováni za oprávněné ke změně nastavení programu.

Prezentační režim

Prezentační režim je funkce uživatele softwaru, kteří nechtějí být nejen v režimu celé obrazovky rušeni vyskakujícími okny a chtějí minimalizovat veškeré nároky na zatížení procesoru. Prezentační režim oceníte v průběhu prezentací, kdy nechcete být rušeni aktivitami antiviru. Zapnutím této funkce zakážete zobrazování všech vyskakujících oken a všechny úlohy plánovače budou zastaveny. Samotná ochrana běží dál v pozadí, ale nevyžaduje žádné zásahy uživatele.

Prezentační režim můžete zapnout nebo vypnout v hlavním okně na záložce **Nastavení** > Počítač.

Dále můžete režim aktivovat v rozšířeném nastavení (dostupném po stisknutí kláves cmd + ,) v sekci vybráním možnosti **Aktivovat prezentační režim**. Vybráním možnosti **Automaticky zapnout Prezentační režim při běhu aplikací zobrazených na celou obrazovku** se Prezentační režim automaticky zapne po spuštění aplikace na celou obrazovku a po jejím ukončení se vypne. Tato možnost je užitečná pro okamžité aktivování Prezentačního režimu

po zahájení prezentace.

Můžete také aktivovat možnost **Automaticky vypínat Prezentační režim** a následně definovat interval, po jehož uplynutí se Prezentační režim automaticky vypne.

Aktivní prezentační režim představuje potenciální bezpečnostní riziko, proto se stav ochrany ESET Endpoint Security for macOS změní na oranžovou barvu a zobrazí se související upozornění.

> **Prezentační režim a interaktivní režim firewallu**
> Pokud je firewall v Interaktivním režimu a zapnete Prezentační režim, mohou se vyskytnout problémy s připojením do internetu. Toto může představovat problém, například pokud spouštíte aplikaci, která se připojuje do internetu. Je to způsobeno tím, že za normálních okolností by si firewall vyžádal potvrzení připojení (pokud nejsou definována žádná pravidla nebo výjimky pro spojení), ale v Prezentačním režimu jsou všechna vyskakovací okna vypnuta. Řešením je definovat pravidla nebo výjimky pro každou aplikaci, která by mohla mít konflikt s tímto chováním nebo použít jiný režim filtrování firewallu. Mějte také na paměti, že pokud při zapnutém Prezentačním režimu pracujete s aplikací nebo stránkou, která představuje potenciální riziko, pak bude tato stránka zablokována, ale nezobrazí se žádné vysvětlení nebo varování, protože jsou vypnuté všechny akce vyžadující zásah uživatele.

Spuštěné procesy

Nástroj **Spuštěné procesů**, který je součástí produktu ESET Endpoint Security for macOS, zobrazuje běžící procesy ve vašem počítači a poskytuje podrobné informace o běžících procesech díky technologii ESET LiveGrid.

- **Proces** – jméno běžícího procesu. Pro zobrazení všech běžících procesů v počítači můžete také použít nástroj Sledování aktivity, který najdete v systému macOS (*/Applications/Utilities*).

- **Úroveň rizika** – ve většině případů určí ESET Endpoint Security for macOS na základě technologie ESET LiveGrid® úroveň rizika jednotlivých objektů (souborů, procesů apod.). Úroveň rizika je vyhodnocena použitím několika heuristických metod, které zjistí charakteristiku každého objektu a váhu možné nebezpečné aktivity. Na základě těchto metod je objektu přiřazena úroveň rizika. Známé aplikace vyhodnocené jako čisté jsou označeny zeleně a jsou dále automaticky vyjmuty z kontroly počítače. Díky tomu dochází ke zrychlení rezidentní i uživatelsky spuštěné kontroly. Pokud je aplikace označena jako neznámá (žlutá), nemusí jít ještě o škodlivou aplikaci. Obvykle se jedná o novou verzi aplikace. V případě, že nedokážete sami rozhodnout, zda je aplikace škodlivá, odešlete ji na analýzu do virové laboratoře ESET. Pokud bude aplikace označena jako škodlivý kód, bude její detekce přidána do jedné z dalších aktualizací virové databáze.

- **Počet uživatelů** – množství uživatelů používající tuto aplikaci. Tato informace je poskytována technologií ESET LiveGrid®.

- **Datum nalezení** – doba, kdy byla aplikace poprvé zaznamenána technologií ESET LiveGrid®.

- **ID balíku aplikace** – jméno výrobce aplikace nebo procesu.

Pokud kliknete na některý proces, v dolní části okna se zobrazí následující informace:

- **Soubor** – umístění souboru v počítači,

- **Velikost souboru** – fyzická velikost souboru na disku,
- **Popis souboru** – popis souboru v operačním systému,
- **ID balíku aplikace** – jméno výrobce aplikace nebo procesu,
- **Verze souboru** – informace o verzi souboru od poskytovatele aplikace,
- **Název produktu** – jméno aplikace nebo její obchodní jméno.

Uživatelské rozhraní

Prostřednictvím možností pro konfiguraci uživatelského rozhraní si můžete přizpůsobit pracovního prostředí programu vašim potřebám. Pro jejich zobrazení klikněte v hlavním menu na **Nastavení** > **Otevřít rozšířená nastavení programu…** v sekci **Uživatel** > Rozhraní.

- Pro zobrazování úvodního obrázku produktu ESET Endpoint Security for macOS při spuštění systému zaškrtněte možnost **Zobrazit úvodní obrázek při startu**.
- Po vybrání možnosti **Ponechat aplikaci v Docku** se ikona produktu ESET Endpoint Security for macOS zobrazí v docku macOS a pro přepínání mezi ESET Endpoint Security for macOS a ostatními běžícími aplikacemi bude možné použít klávesy cmd+tab*cmd+tab*. Změna nastavení ESET Endpoint Security for macOS se projeví po restartu počítače.
- Pomocí možnosti **Použít standardní menu** aktivujete používání klávesových zkratek (viz kapitolu Klávesové zkratky). Dále se v menu baru macOS zobrazí standardní nabídky aplikace (Uživatelské rozhraní, Nastavení a Nástroje).
- Pokud chcete povolit zobrazování nápovědy pro některá tlačítka produktu ESET Endpoint Security for macOS, zaškrtnete možnost **Zobrazovat nápovědu tlačítek**.
- Pro zobrazení a možnost výběru skrytých souborů ke kontrole v části **Cíle kontroly** na záložce **Kontrola počítače** zaškrtněte možnost **Zobrazovat skryté soubory**.
- Standardně se ikona produktu ESET Endpoint Security for macOS zobrazuje v menu baru v pravém horním rohu obrazovky. Pokud nechcete tuto ikonu zobrazovat, deaktivujte možnost **Zobrazit ikonu v rozšířeném menu baru**. Změna tohoto nastavení se projeví po restartování produktu ESET Endpoint Security for macOS (případně počítače).

Upozornění a oznámení

Sekce **Upozornění a události** nabízí možnosti pro úpravu zobrazování upozornění týkajících se hrozeb, systémových zpráv a stavů ochrany ESET Endpoint Security for macOS.

Vypnutím možnosti **Zobrazovat výstražná upozornění** se přestanou zobrazovat všechna okna s upozorněními, a proto je vhodné tuto možnost vypnout pouze v určitých situacích. Většině uživatelů doporučujeme ponechat tuto

možnost zapnutou. Pokročilé možnosti máme popsané v samostatné kapitole.

Zaškrtnutím možnosti **Zobrazovat upozornění na pracovní ploše** zapnete zobrazování oken s upozorněními, které nepotřebují interakci uživatele (standardně se zobrazují v pravém horním rohu obrazovky). Pokud chcete nastavit dobu zobrazení tohoto upozornění upravte hodnotu v poli **Upozornění zavřít automaticky po X sekundách** (výchozí hodnota je 5 sekund). Pokud chcete při běhu aplikací v režimu celé obrazovky zobrazovat pouze upozornění vyžadující odezvu uživatele, zaškrtněte položku **Povolit režim celé obrazovky**. Tato možnost je vhodná během prezentací, při hraní her nebo při jiných činnostech s aplikacemi, které běží v režimu celé obrazovky.

Od verze ESET Endpoint Security for macOS 6.2 můžete **potlačit** zobrazování konkrétních **stavů ochrany** v hlavním okně programu. Více informací naleznete v kapitole stavy ochrany.

Zobrazení upozornění

ESET Endpoint Security for macOS zobrazuje dialogová okna s informacemi o nových aktualizacích programových komponent, aktualizacích operačního systému a také při vypnutí určitých částí programu, vymazání protokolů apod. Potlačit zobrazování každého upozornění můžete kliknutím na **Příště nezobrazovat**.

Seznam dialogových oken, které zobrazuje ESET Endpoint Security for macOS naleznete po kliknutí v hlavním okně na **Nastavení** > **Otevřít rozšířená nastavení programu…** > **Upozornění a události** > **Rozšířená nastavení: Nastavit…**. Pro zapnutí či potlačení každého oznámení použijte zaškrtávací pole vedle **jména dialogového okna**. Pokud je zaškrtávací pole vybrané, dané oznámení se vždy zobrazí a neuplatní se **Podmínky zobrazení**. Pokud nechcete zobrazovat konkrétní oznámení, v seznamu jej odškrtněte. Dále můžete definovat **Podmínky zobrazení** a ovlivnit, při jaké akci se oznámení může zobrazit.

Stavy ochrany

Informace o stavu ESET Endpoint Security for macOS se zobrazují v hlavním okně programu na záložce **Stav ochrany**. V případě potřeby můžete zobrazování konkrétních stavů ochrany potlačit. Konfiguraci jednotlivých stavů naleznete v **rozšířeném nastavení** (dostupném z hlavního okna po stisknutí kláves po *cmd+,*) v sekci **Upozornění a události**. Následně klikněte na tlačítko **Nastavit** u položky **Zobrazit v hlavním okně na záložce Stav ochrany**.

Potlačit můžete zobrazování stavů následujících komponent:

- Firewall
- Anti-Phishing
- Ochrana přístupu na web
- Ochrana poštovních klientů
- Prezentační režim
- Aktualizace operačního systému
- Platnost licence
- Vyžadován restart systému

Kontextové menu

Integraci kontextového menu produktu ESET Endpoint Security for macOS do systému můžete zapnout v **rozšířeném nastavení** (dostupném z hlavního okna po stisknutí kláves po *cmd+,*) v sekci **Uživatel** > **Kontextové menu** po zaškrtnutí možnosti **Používat kontextové menu**. Pro provedení změn je nutné provést odhlášení uživatele nebo restartovat počítač. Možnosti kontextového menu se zobrazí, když v okně **Finder** stiskněte klávesu CTRL a myší kliknete na jakýkoli soubor.

Aktualizace

Pravidelná aktualizace ESET Endpoint Security for macOS je základním předpokladem pro zajištění maximální bezpečnosti systému. Modul Aktualizace se stará o to, aby byl program stále aktuální pomocí aktualizace detekčních i programových modulů.

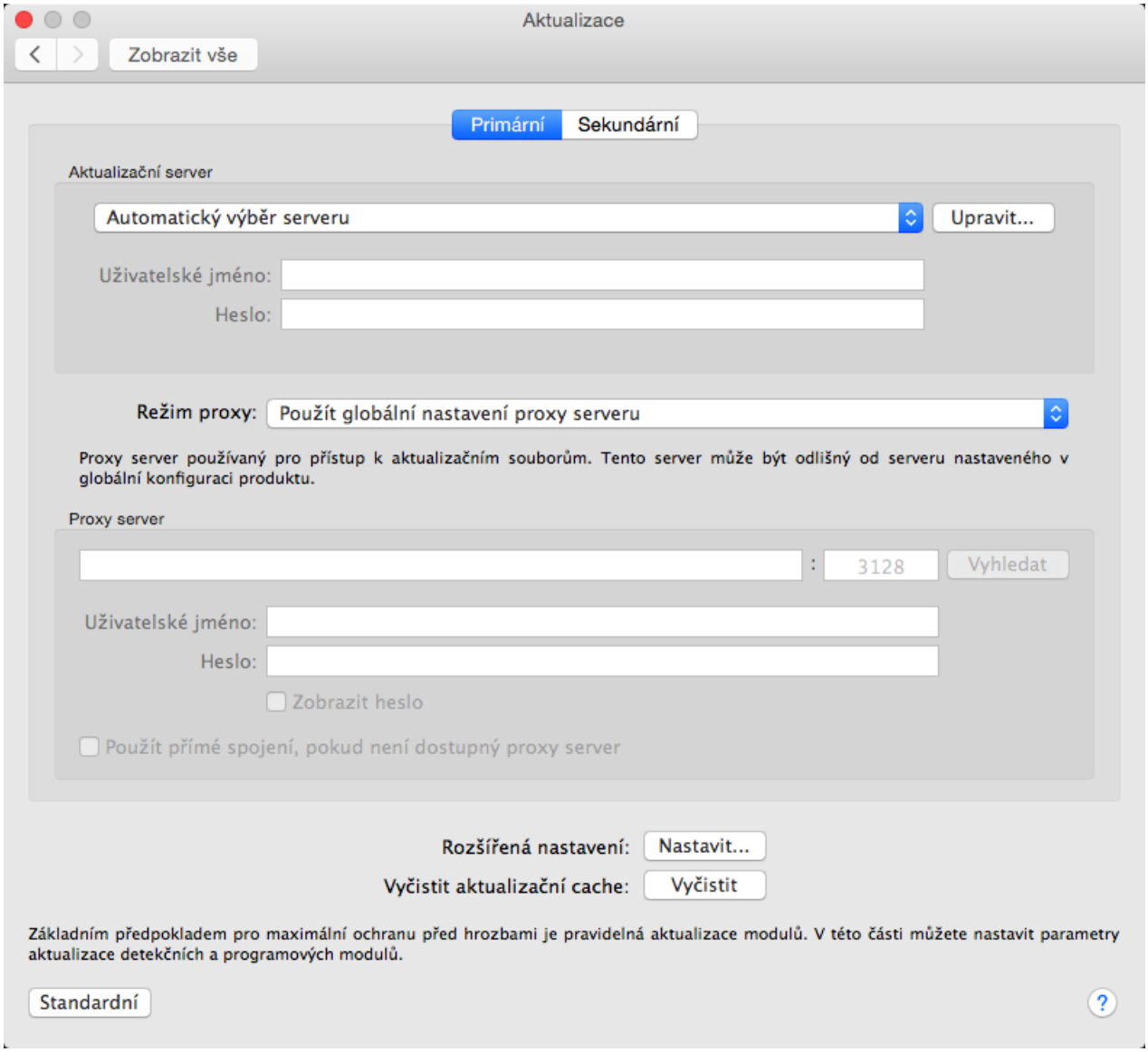
Informace o aktuálním stavu aktualizace se zobrazují na záložce **Aktualizace** v hlavním okně programu. Obsahují informaci o datu a čase poslední úspěšné aktualizace, zda jsou moduly aktuální, případně jestli není potřeba program aktualizovat. Kliknutím na **Aktualizovat moduly** spustíte aktualizaci ručně.

Pokud jsou moduly v pořádku staženy a aktuální, zobrazuje se informace *Aktualizace není potřeba - moduly jsou aktuální*. Pokud nelze program aktualizovat, zkontrolujte Nastavení aktualizace. Nejčastější příčinou selhání stahování aktualizací je neaktivovaný produkt, případně chybně nastavený proxy server.

Na záložce **Aktualizace** v hlavním okně programu naleznete také číselné označení detekčního jádra, které produkt aktuálně používá. Jedná se zároveň o funkční odkaz vedoucí na webové stránky společnosti ESET s podrobnými informacemi o nových vzorcích, které aktualizace zahrnuje.

Nastavení aktualizace

V sekci Aktualizace můžete konfigurovat aktualizační servery, ze kterých si klient bude stahovat detekční a programové moduly. Pokud server vyžaduje autentifikaci, máte možnost zadat uživatelské jméno a heslo. V rozbalovacím menu **Aktualizační server** je standardně vybrána položka **Automatický výběr serveru**. Tím je zajištěno, že aktualizace se budou stahovat z aktualizačního serveru ESET s nejmenším síťovým zatížením.



Seznam dostupných serverů naleznete v rozbalovacím menu **Aktualizační server**. Pro přidání nového aktualizačního serveru klikněte na tlačítko **Upravit**. Poté zadejte adresu nového serveru do pole **Aktualizační server** a klikněte na tlačítko **Přidat**

V produktu ESET Endpoint Security for macOS můžete mít definovány dva aktualizační servery. Jako **primární server** můžete mít nastaven například váš lokální mirror, a jako sekundární aktualizační servery ESET (tedy možnost **Automatický výběr serveru**). Při nedostupnosti například primárního serveru se aktualizace provede ze sekundárního serveru. Pokud nezadáte uživatelské jméno a heslo do alternativního aktualizačního profilu, aktualizace se při přepnutí na alternativní aktualizační server nezdaří. Vybráním možnosti Automatický výběr serveru a zadáním uživatelského jména a hesla do odpovídajících polí zajistíte, že si produkt ESET Endpoint Security for macOS vyberte vždy nejlepší server.

Nastavením **režimu proxy** může produkt detekční moduly stahovat prostřednictvím proxy serveru (například z lokálního HTTP Proxy serveru). Mějte na paměti, že proxy server pro stahování aktualizací může být odlišný od serveru definovaného v globálním nastavením proxy serveru, který se aplikuje na všechny moduly produktu vyžadující připojení k internetu. Globální nastavení proxy serveru je možné definovat již v průběhu instalace nebo kdykoli v rozšířeném nastavení.

Pro definování přístupu k aktualizacím prostřednictvím proxy:

1. Z rozbalovacího menu vyberte možnost **Připojovat se prostřednictvím proxy serveru**.

2. Po kliknutí na tlačítko **Vyhledat** se ESET Endpoint Security for macOS pokusí automaticky doplnit IP adresu proxy a port (standardně **3128**).

3. Pokud proxy server vyžaduje autentifikaci, zadejte do odpovídajících polí **uživatelské jméno** a **heslo**.

ESET Endpoint Security for macOS dokáže získat konfiguraci proxy z nastavení systému. V systému konfiguraci HTTP Proxy naleznete po kliknutí na ikonu > **Předvolby systému** > **Síť** > **Pokročilé** > **Proxy**.

Pokud aktivujete možnost **Použít přímé spojení, pokud není dostupný proxy server**, ESET Endpoint Security for macOS automaticky zkusí připojení k aktualizačním serverům ESET bez použití proxy. Tuto možnost je vhodné nastavit mobilním uživatelům.

Pro odstranění všech dočasně uložených aktualizačních souborů klikněte na tlačítko **Vyčistit** v dialogovém okně **Aktualizace**. Vymazat dočasné soubory doporučujeme provést v případě problémů s aktualizací.

Rozšířená nastavení

Pro deaktivaci zobrazování upozornění o provedené aktualizaci modulů aktivujte možnost **Nezobrazovat upozornění o úspěšné aktualizaci**.

Pokud chcete mít přístup k vývojářským aktualizacím, které mohou řešit váš problém, aktivujte si stahování předběžných aktualizací. Testovací aktualizace často obsahují opravy chyb programových modulů. Vyberete-li možnost **Opožděná aktualizace**, aktualizace se budou stahovat z aktualizačního severu, na který jsou aktualizace umisťovány se zpožděním (o několik hodin). Výhodou je stahování ověřených aktualizací, které nezpůsobují problémy, ale zároveň se tím snižuje úroveň zabezpečení.

ESET Endpoint Security for macOS zálohuje detekční a programové moduly pro případ **obnovení starší verze**. Aby produkt ESET Endpoint Security for macOS vytvářel tzv. snapshoty automaticky, ponechte možnost **Vytvářet zálohu aktualizačních souborů** zaškrtnutou. Pokud máte podezření, že nová verze modulů je nestabilní nebo poškozená, můžete se vrátit ke starší verzi modulů a na stanovený časový interval zakázat jejich aktualizaci. V případě, že jste již dočasně zakázali aktualizaci, můžete ji v této části znovu povolit. Při použití této funkce vyberte z rozbalovacího menu Časový interval, na jak dlouho chcete aktualizaci detekčních a programových modulů pozastavit. Možnost Do odvolání vyberte v případě, kdy chcete aktualizace modulů obnovit ručně. Protože tato možnost představuje potenciální bezpečnostní riziko, její výběr nedoporučujeme.

Nastavit automaticky maximální stáří detekčního jádra – pomocí této možnosti nastavíte maximální přístupné stáří detekčních modulů. Budou-li starší, zobrazí se informace, že moduly nejsou aktuální. Předdefinovaná doporučená hodnota je 7 dní.

Jak vytvořit aktualizační úlohu

Aktualizaci můžete spustit kdykoliv ručně kliknutím na **Aktualizovat moduly** na záložce **Aktualizace** v hlavním okně programu.

Aktualizaci můžete také spouštět jako naplánovanou úlohu. Pro vytvoření naplánované úlohy klikněte v hlavním okně programu na záložku **Nástroje** > **Plánovač**. Standardně jsou v ESET Endpoint Security for macOS již vytvořeny

tyto aktualizační úlohy:

- **Pravidelná automatická aktualizace**,
- **Automatická aktualizace po přihlášení uživatele.**

Každá z těchto úloh může být nastavena tak, aby odpovídala vašim potřebám. Kromě úpravy stávajících úloh aktualizace můžete vytvářet i nové úlohy s vlastní konfigurací. Pro bližší popis vytváření a nastavení úloh přejděte do kapitoly Plánovač.

Aktualizace operačního systému

Aktualizace systému macOS představují důležitou součást v ochraně proti škodlivému software. Pro maximální bezpečnost doporučujeme instalovat aktualizace co nejdříve po jejich vydání. ESET Endpoint Security for macOS vás může upozornit na chybějící aktualizace systému v závislosti na nastavené úrovni. Po kliknutím v hlavním okně na **Nastavení** > **Zobrazit rozšířené nastavení...** (nebo stisknutím kláves *cmd+,*) > **Upozornění a události > Nastavení...** můžete změnit následující **Podmínky upozornění** v sekci **Aktualizace operačního systému**:

- **Zobrazit všechny aktualizace** – budete upozorněni pouze na instalaci všech aktualizací operačního systému
- **Zobrazit pouze doporučené** – budete upozorněni pouze na instalaci důležitých aktualizací operačního systému.

Pokud nechcete být informováni o chybějících aktualizacích systému, odškrtněte možnost **Aktualizace operačního systému**.

Informace o dostupnosti aktualizací operačního systému macOS a souvisejících aplikací jsou poskytovány systémovým nástrojem Aktualizace systému. Aktualizaci můžete spustit přímo ze zobrazeného okna nebo kliknutím na záložku **Domů** (Stav ochrany) v hlavním okně ESET Endpoint Security for macOS na **Instalovat chybějící aktualizace**.

Okno s upozorněním obsahuje název aplikace, verzi, velikost aktualizace, vlastnosti (vlajky) a další informace o aktualizaci. Sloupec **Vlajky** může obsahovat následující informace:

- **[doporučeno]** – výrobce operačního systému doporučuje nainstalovat tuto aktualizaci pro zvýšení bezpečnosti a stability operačního systému,
- **[restart]** – po dokončení instalace je vyžadován restart,
- **[vypnutí]** – po dokončení instalace bude nutné vypnout a znovu zapnout počítač.

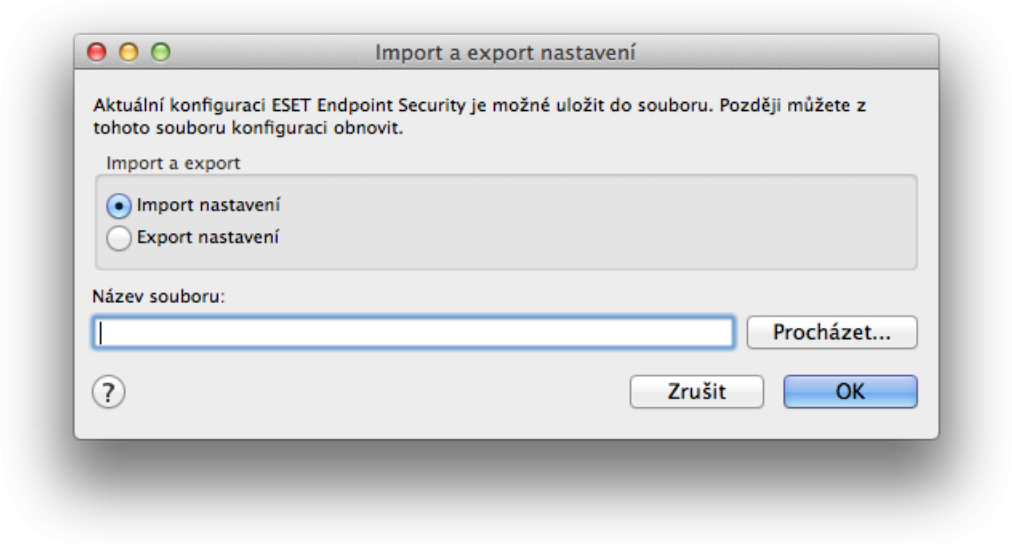
Okno s upozorněním zobrazuje aktualizace získané pomocí nástroje 'softwareupdate'. Aktualizace získané pomocí tohoto nástroje se mohou lišit od seznamu aktualizacích poskytovaných pomocí aplikace 'Aktualizace aplikací.' Pokud chcete nainstalovat aktualizace zobrazené v okně 'Chybějící aktualizace systému' a aplikace 'Aktualizace

aplikací' je nezobrazuje, je nutné použít nástroje 'softwareupdate' z příkazového řádku. Pro více informací o nástroji 'softwareupdate' se podívejte do manuálu po zadání `man softwareupdate` do okna **Terminál**. Toto doporučujeme pouze zkušeným uživatelům.

Import a export nastavení

Pro importování nebo exportování konfigurace produktu ESET Endpoint Security for macOS přejděte v hlavním okně na záložku **Nastavení** a klikněte na možnost **Import a export nastavení**.

Importování a exportování nastavení je užitečné například pokud si potřebujete zálohovat současné nastavení ESET Endpoint Security for macOS a chcete se k němu později vrátit. Export nastavení oceníte také v případě, že chcete stejné nastavení použít na více počítačích, kdy stačí pouze naimportovat daný .xml soubor.



Pro importování nastavení vyberte možnost **Import**, klikněte na tlačítko **Procházet...** vyberte soubor, který chcete importovat. Pro exportování nastavení vyberte možnost **Export**, zadejte název souboru a vyberte umístění pro uložení souboru.

Nastavení proxy serveru

Nastavení proxy serveru provedení v **rozšířeném nastavení** (dostupném z hlavního okna po stisknutí kláves po *cmd+,*) v sekci **Různé** > **Proxy server**. Tato nastavení specifikují globální nastavení proxy serveru a jsou platná pro všechny součástí produktu ESET Endpoint Security for macOS. Tyto parametry se použijí pro jakýkoliv modul produktu se snaží připojit k internetu. ESET Endpoint Security for macOS podporuje následující způsoby autentifikace: Basic Access a NTLM (NT LAN Manager).

Po zaškrtnutí možnosti **Použít proxy server** zadejte do pole **Proxy server** IP adresu nebo URL. Dále zadejte port, na kterém proxy naslouchá (standardně (3128). Případně můžete kliknout na tlačítko **Detekovat** a pokud máte v systému proxy nastavenou, údaje by se měly automaticky vyplnit.

Pokud proxy server vyžaduje autentifikaci, zadejte do odpovídajících polí **uživatelské jméno** a **heslo**.

Sdílená lokální cache

Pro zapnutí této funkce přejděte v hlavním menu na záložku Nastaveni a klikněte na Otevřít rozšířená nastavení programu. Dále vyberte možnost Sdílená lokální cache a pomocí zaškrtávací pole aktivujte tuto možnost. Sdílená lokální cache výrazně zrychluje kontrolu počítače ve virtuálních prostředích odstraněním duplicitní kontroly souborů v síti. Každý soubor je zkontrolován pouze jednou a výsledek je uložen do sdílené cache. Aktivováním této možnosti bude produkt ukládat informace o kontrolovaných souborech a složkách ve vaší síti do lokální cache. Pokud následně spustíte novou kontrolu, ESET Endpoint Security for macOS se nejprve podívá do cache. V případě, že byl již identický soubor jiným produktem v síti zkontrolován, vyloučí jej z aktuální kontroly.

Nastavení Cache serveru v produktu jsou následující:

- **Adresa serveru** – název počítače nebo IP adresa, na kterém se nachází lokální cache produktu ESET.
- **Port** – port, který při komunikaci využívá lokální cache produktu ESET (standardně (3537).
- **Heslo** – zadejte heslo pro přístup k ESET Shared Local Cache, pokud je vyžadováno.

> **Další informace**
> Pro více informací o instalaci a konfiguraci ESET Shared Local Cache si pročtěte uživatelskou příručku (pouze v angličtině).

Licenční ujednání s koncovým uživatelem

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 (dále jen „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 (dále jen "ESET" nebo "Poskytovatel") a Vámi, fyzickou anebo právnickou osobou (dále jen "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" "Přijímám..." nebo při instalaci, stahování, kopírování nebo používání Softwaru vyjadřujete souhlas s podmínkami této Smlouvy. V případě, že s některými podmínkami této Smlouvy 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 (dále jen „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 (dále jen „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 (dále jen „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) **Business Edition**. Pro použití Software 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**. OEM Software se váže 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 může čas od času vydat aktualizaci Software ("Update"), avšak není povinný poskytovat Update. Tato funkce je při standardním nastavení Software zapnutá, proto se Update nainstaluje automaticky, kromě případů, kdy Koncový uživatel automatickou instalaci Update zakázal. Pro účely 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.

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/nebo informací o operacích a funkcích Softwaru a informací o zařízeních v místní síti, jako je typ, dodavatel, model a/nebo název zařízení (dále jen "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. Tímto souhlasíte s přijímáním oznámení a zpráv, mimo jiné včetně marketingových informací.

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. 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 DOVOLUJE APLIKOVATELNÉ PRÁVO, 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 VYPLYNULI ZE SMLOUVY, ÚMYSLNÉHO JEDNÁNÍ, NEDBALOSTI ANEBO JINÉ SKUTEČNOSTI, ZAKLÁDAJÍCÍ VZNIK ZODPOVĚDNOSTI, VZNIKLÉ 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. 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 (dále jen „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 (dále jen „zákony o kontrole vývozu“) 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 (dále jen „sankční zákony“).

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**. Všechny oznámení, včetně Software a Dokumentací je potřebné doručit na adresu: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic.

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. V případě rozporů mezi jazykovými verzemi této Dohody má přednost anglická verze. Změny této Dohody jsou možné jen v písemné formě, přičemž za Poskytovatele musí takovouto změnu podepsat statutární zástupce anebo osoba k tomuto úkonu výslovně zplnomocněná.

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.

EULA ID: BUS-STANDARD-20-01

Privacy Policy

Společnost ESET spol. s r.o., se sídlem Einsteinova 24, 851 01 Bratislava, Slovenská republika, zapsaná v Obchodním rejstříku vedeném Okresním soudem Bratislava I v oddílu Sro, vložka 3586/B, s obchodním registračním číslem 31333532 jako „Správce údajů“ (dále jen „ESET“ nebo „My“) chce postupovat transparentně, pokud jde o zpracování osobních údajů a soukromí našich zákazníků. 31333532 jako „Správce údajů“ (dále jen „ESET“ nebo „My“) chce postupovat transparentně, pokud jde o zpracování osobních údajů a soukromí našich zákazníků. Abychom dosáhli tohoto cíle, zveřejňujeme zde tyto Zásady ochrany osobních údajů výhradně za účelem informování našich zákazníků ("Koncový uživatel" nebo "Vy") o následujících tématech:

- Zpracování osobních údajů
- Důvěrnost údajů,
- Práva subjektu údajů.

Zpracování osobních údajů

Služby poskytované společností ESET implementované v našem produktu jsou poskytovány za podmínek uvedených v Licenčním ujednáním s koncovým uživatelem ("EULA"), 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 ve smlouvě EULA a dokumentaci k produktu, například služby aktualizace/upgradu, ESET LiveGrid®, ochranu proti zneužití dat, podporu atd. Aby všechny tyto služby fungovaly, potřebujeme shromažďovat následující informace:

- Aktualizace a další statistiky zahrnující 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, MAC adresa a nastavení konfigurace produktu.
- Jednosměrné hodnoty hash, které souvisejí s infiltracemi, jako součást reputačního systému ESET LiveGrid®, který zlepšuje účinnost našich řešení proti malwaru tím, že porovnává kontrolované soubory s databází povolených a zakázaných položek v cloudu.
- 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:
  - Oinfiltrace, 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;
  - Oúdaje o zařízeních v místní síti, jako je typ, dodavatel, model a/nebo název zařízení;
  - Oúdaje týkající se používání internetu, jako jsou IP adresa a informace o zeměpisné poloze, IP pakety, adresy URL a ethernetové rámce;
  - ONemáme v úmyslu, aby byly součástí našich systémů nebo aby byly zpracovány pro účely uvedené v těchto Zásadách ochrany osobních údajů.

Informace o licencích, například ID licence, a osobní údaje, jako jsou jméno, příjmení, adresa, e-mailová adresa, jsou vyžadovány pro fakturační účely, ověření pravosti licencí a poskytování našich služeb. 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.

- Můžete být vyzváni k poskytnutí dalších informací, které usnadní poskytnutí podpory. Funkcí Ochrana proti zneužití dat mohou být shromažďovány a po dobu 3 měsíců uchovávány údaje o poloze, snímky obrazovky, data o konfiguraci vašeho počítače a data zaznamenaná kamerou počítače.
- Na webu https://my.eset.com je potřeba vytvořit účet, pomocí něhož tato funkce aktivuje sběr dat v případě odcizení počítače. Shromážděné údaje jsou uloženy na našich serverech nebo na serverech našich poskytovatelů služeb. 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.

Důvěrnost údajů

ESET je společnost s celosvětovou působností. Informace, které společnost ESET zpracovává, mohou být přenášeny k přidruženým subjektům nebo partnerům a zpět za účelem plnění smlouvy EULA, jako je poskytování služeb, podpora nebo fakturace. Na základě vaší polohy a služeb, které si zvolíte, může být potřeba přenést vaše údaje do země, kde neplatí rozhodnutí Evropské komise o odpovídající ochraně. I v takovém případě každý přenos informací podléhá právním předpisům o ochraně údajů a probíhá pouze v případě potřeby. Bez výjimky musí být stanoveny standardní smluvní doložky, závazná firemní pravidla nebo jiná vhodná ochrana.

Děláme vše pro to, aby nedocházelo k uchovávání dat delší dobu, než je nezbytné k poskytování služeb podle smlouvy EULA. Naše doba uchovávání může trvat déle než platnost vaší licence, a to z toho důvodu, abychom vám poskytli čas pro snadné a pohodlné obnovení. Minimalizované a pseudonymizované statistiky a další data ze služby ESET LiveGrid® mohou být dále zpracovávány pro statistické účely.

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 dozorčí orgány i subjekty údajů. Jako subjekt údajů máte právo podat stížnost u dozorčího orgánu.

Práva subjektu údajů

Společnost ESET podléhá regulaci zákonů Slovenské republiky a je vázána právními předpisy o ochraně údajů Evropské unie. Za podmínek stanovených příslušnými zákony o ochraně údajů máte jako subjekt údajů nárok na následující práva:

- právo požádat společnosti ESET o přístup k vašim osobním údajům,
- právo na opravu vašich osobních údajů, pokud jsou nepřesné (máte také právo na doplnění neúplných osobních údajů),
- právo požadovat vymazání vašich osobních údajů,
- právo požadovat omezení zpracování vašich osobních údajů,
- právo podat námitky proti zpracování,
- právo podat stížnost, stejně tak
- právo na přenositelnost dat.

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.
Vedoucí pracovník ochrany osobních údajů
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk