ESET Endpoint Antivirus for Linux

Podręcznik użytkownika

Kliknij tutaj aby wyświetlić ten dokument jako Pomoc.

Digital Security
Progress. Protected.

Prawa autorskie ©2024 ESET, spol. s r.o.

Produkt ESET Endpoint Antivirus for Linux został opracowany przez ESET, spol. s r.o.

Aby uzyskać więcej informacji, odwiedź stronę https://www.eset.com.

Wszelkie prawa zastrzeżone. Żadna część tej dokumentacji nie może być powielana, przechowywana w systemie wyszukiwania lub przesyłana w jakiejkolwiek formie lub za pomocą jakichkolwiek środków elektronicznych, mechanicznych, fotokopiowania, nagrywania, skanowania lub w inny sposób bez pisemnej zgody autora.

Firma ESET, spol. s r.o. zastrzega sobie prawo do zmiany dowolnej z opisanych aplikacji bez uprzedniego powiadomienia.

Pomoc techniczna: https://support.eset.com

WER. 12.04.2024

1 Wprowadzenie ... 1
1.1 Główne funkcje systemu ... 1
2 Wymagania systemowe ... 1
2.1 Bezpieczny rozruch ... 3
3 Instalacja ... 5
3.1 Odinstalowywanie ... 6
3.2 Wdrożenie masowe ... 6
4 Aktualizowanie, uaktualnianie ... 11
4.1 Kopia dystrybucyjna aktualizacji ... 14
5 Aktywacja usługi ESET Endpoint Antivirus for Linux ... 14
5.1 Gdzie znajduje się licencja? ... 15
5.2 Stan aktywacji ... 16
6 Używanie programu ESET Endpoint Antivirus for Linux ... 16
6.1 Interfejs użytkownika ... 16
6.2 Skanowanie ... 18
6.2 Wyłączenia ... 20
6.3 Kwarantanna ... 22
6.4 Zdarzenia ... 24
6.5 Powiadomienia ... 25
7 Konfiguracja ... 25
7.1 Silnik detekcji ... 26
7.1 Wyłączenia ... 27
7.1 Ochrona systemu plików w czasie rzeczywistym ... 28
7.1 Parametry technologii ThreatSense ... 30
7.1 Dodatkowe parametry ThreatSense ... 32
7.1 Ochrona oparta na chmurze ... 32
7.1 Skanowania w poszukiwaniu szkodliwego oprogramowania ... 35
7.1 Udostępniona lokalna pamięć podręczna ... 35
7.2 Aktualizacja ... 36
7.3 Kontrola dostępu do urządzeń ... 37
7.3 Edytor reguł kontroli dostępu do urządzeń ... 38
7.3 Grupy urządzeń ... 39
7.3 Dodawanie reguł kontroli dostępu do urządzeń ... 39
7.4 Narzędzia ... 41
7.4 Serwer proxy ... 41
7.4 Pliki dziennika ... 42
7.5 Interfejs użytkownika ... 43
7.5 Stan aplikacji ... 43
8 Zdalne zarządzanie ... 44
9 Przykłady praktycznego zastosowania ... 44
9.1 Pobieranie informacji o modułach ... 44
9.2 Planowanie skanowania ... 44
10 Struktura plików i folderów ... 45
11 Rozwiązywanie problemów ... 48
11.1 Zbieranie dzienników ... 48
11.2 Korzystanie z flagi noexec ... 49
11.3 Nie można uruchomić ochrony w czasie rzeczywistym ... 50
12 Słowniczek ... 51
13 Umowa licencyjna użytkownika końcowego ... 51

14 Zasady ochrony prywatności 59

Wprowadzenie

Nowoczesny silnik skanowania firmy ESET charakteryzuje się niedoścignioną szybkością skanowania i szerokim zakresem wykrywania, co w połączeniu z niewielkim rozmiarem sprawia, że program ESET Endpoint Antivirus for Linux (EEAU) stanowi idealny wybór dla każdego urządzenia z systemem Linux, o ile spełnione zostaną wymagania systemowe.

Skaner na żądanie i skaner podczas dostępu obejmują główne funkcje.

Skaner na żądanie może uruchamiać użytkownik uprzywilejowany (zazwyczaj będzie to administrator systemu) za pośrednictwem interfejsu wiersza polecenia, ESET PROTECT lub narzędzia systemu operacyjnego do planowania automatycznych operacji (np. `cron`). Termin na żądanie odnosi się do skanowania obiektów w systemie plików na podstawie żądania użytkownika lub samego systemu.

Skaner podczas dostępu jest wywoływany przy każdej próbie uzyskania dostępu do obiektów w systemie plików.

Główne funkcje systemu

- Skanowanie podczas dostępu z użyciem niewielkiego modułu firmy ESET na poziomie jądra systemu
- Kompleksowe dzienniki skanowania
- Nowa, łatwa konfiguracja
- Kwarantanna
- Powiadomienia na pulpicie
- Możliwość zarządzania za pośrednictwem konsoli ESET PROTECT
- Ochrona oparta na chmurze

Wymagania systemowe

Wymagania sprzętowe

Minimalne wymagania sprzętowe, które należy spełnić przed zainstalowaniem programu ESET Endpoint Antivirus for Linux w celu zapewnienia jego prawidłowego działania:

- procesor Intel/AMD x64
- 700 MB dostępnego miejsca na dysku

Wymagania dotyczące oprogramowania

Oficjalnie obsługiwane i testowane są następujące systemy operacyjne o architekturze 64-bitowej:

- Ubuntu Desktop 18.04 LTS 64-bit
- Ubuntu Desktop 20.04 LTS
- Red Hat Enterprise Linux 7, 8 z zainstalowanym obsługiwanym środowiskiem pulpitu.
- SUSE Linux Enterprise Desktop 15

> **AWS kernel**
> Dystrybucje Linuksa z AWS kernel nie są obsługiwane.

Obsługiwane serwery interfejsu graficznego:

- X11
- Wayland

Obsługiwane środowiska pulpitu:

- GNOME 3.28.2 i nowsze
- KDE
- XFCE

Dowolny region z kodowaniem UTF-8.

Interfejs użytkownika i lista poleceń w oknie Terminal są dostępne w następujących językach:

- Angielski
- Niemiecki
- Hiszpański
- Hiszpański (Ameryka Łacińska)
- Francuski
- Polski
- Japoński

Jeśli system operacyjny hosta używa nieobsługiwanego języka, domyślnie używany jest język angielski.

Zdalne zarządzanie za pomocą konsoli ESET PROTECT

Program ESET Endpoint Antivirus for Linux jest również kompatybilny z ESET PROTECT w wersji 7.1 lub nowszej.

Bezpieczny rozruch

Aby korzystać z ochrony systemu plików w czasie rzeczywistym na komputerze z włączonym bezpiecznym rozruchem, moduł jądra produktu ESET Endpoint Antivirus for Linux (EEAU) musi być podpisany przy użyciu klucza prywatnego. Odpowiedni klucz publiczny musi zostać zaimportowany do UEFI. Program EEAU w wersji 8.1 jest wyposażony we wbudowany skrypt podpisywania, który działa w trybie interaktywnym lub nieinteraktywnym.

Użyj narzędzia `mokutil`, aby sprawdzić, czy na urządzeniu włączony jest bezpieczny rozruch. Wykonaj następujące polecenie z okna terminala jako użytkownik uprzywilejowany:

```
mokutil --sb-state
```

Tryb interaktywny

Jeśli nie posiadasz klucza publicznego lub prywatnego do podpisania modułu jądra, tryb interaktywny może generować nowe klucze i podpisywać moduł jądra. Tryb ten pomaga również w rejestracji wygenerowanych kluczy w UEFI.

1. Wykonaj następujące polecenie z okna terminala jako użytkownik uprzywilejowany:

```
/opt/eset/eea/lib/install_scripts/sign_modules.sh
```

2. Gdy skrypt wyświetli monit o naciśnięcie klawiszy, wpisz **n**, a następnie naciśnij klawisz **Enter**.

3. Po wyświetleniu monitu o wygenerowanie nowych kluczy wpisz **y**, a następnie naciśnij klawisz **Enter**. Skrypt podpisuje moduł jądra za pomocą wygenerowanego klucza prywatnego.

4. Aby zarejestrować wygenerowany klucz publiczny do UEFI w sposób półautomatyczny, wpisz **y**, a następnie naciśnij klawisz **Enter**. Aby ukończyć rejestrację ręcznie, wpisz **n**, naciśnij klawisz **Enter** i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

5. Po wyświetleniu monitu wprowadź wybrane hasło. Zapamiętaj je, ponieważ będzie potrzebne do ukończenia rejestracji (zatwierdzenie Machine Owner Key [MOK]) w UEFI.

6. Aby zapisać wygenerowane klucze na dysku twardym w celu ich późniejszego użycia, wpisz **y**, wprowadź ścieżkę do katalogu i naciśnij klawisz **Enter**.

7. Aby ponownie uruchomić komputer i uzyskać dostęp do UEFI, wpisz **y** po wyświetleniu monitu, a następnie naciśnij klawisz **Enter**.

8. Naciśnij dowolny klawisz w ciągu 10 sekund od wyświetlenia monitu o dostęp do UEFI.

9. Wybierz pozycję **Zarejestruj MOK** i naciśnij klawisz **Enter**.

10. Naciśnij przycisk **Kontynuuj**, a następnie naciśnij klawisz **Enter**.

11. Wybierz pozycję **Tak** i naciśnij klawisz **Enter**.

12. Aby ukończyć rejestrację i ponownie uruchomić komputer, wpisz hasło z kroku 5 i naciśnij klawisz **Enter**.

Tryb nieinteraktywny

Użyj tego trybu, jeśli na komputerze docelowym jest dostępny klucz prywatny i publiczny.

Syntax: `/opt/eset/eea/lib/install_scripts/sign_modules.sh [OPTIONS]`

Opcje — forma skrócona	Opcje — forma długa	Opis
`-d`	`--public-key`	Ustawianie ścieżki do klucza publicznego w formacie DER używanego do podpisywania
`-p`	`--private-key`	Ustawianie ścieżki do klucza prywatnego używanego do podpisywania
`-k`	`--kernel`	Ustawianie nazwy jądra, którego moduły muszą być podpisane. Jeśli go nie podasz, bieżące jądro zostanie ustawione jako domyślnie
`-a`	`--kernel-all`	Podpisywanie (i tworzenie) modułów jądra na wszystkich istniejących jądrach zawierających nagłówki
`-h`	`--help`	Pokaż pomoc

1. Wykonaj następujące polecenie z okna terminala jako użytkownik uprzywilejowany:

```
/opt/eset/eea/lib/install_scripts/sign_modules.sh -p <path_to_private_key> -
d <path_to_public_key>
```

Zastąp `<path_to_private_key>` i `<path_to_public_key>` ścieżką prowadzącą odpowiednio do klucza prywatnego i klucza publicznego.

2. Jeśli podany klucz publiczny nie jest jeszcze zarejestrowany w UEFI, wykonaj następujące polecenie jako użytkownik uprzywilejowany:

```
mokutil --import <path_to_public_key>
```

`<path_to_public_key>` represents the provided public key.

3. Uruchom ponownie komputer, uzyskaj dostęp do UEFI, wybierz pozycję **Zarejestruj MOK** > **Kontynuuj** > **Tak**.

Zarządzanie kilkoma urządzeniami

Załóżmy, że zarządzasz kilkoma komputerami, które używają tego samego jądra Linuksa i mają ten sam klucz publiczny zarejestrowany w UEFI. W takim przypadku można podpisać moduł jądra produktu EEAU na jednej z maszyn zawierających klucz prywatny, a następnie przenieść podpisany moduł jądra na inne komputery. Po zakończeniu podpisywania wykonaj poniższe czynności:

1. Kopiuj i wklej podpisany moduł jądra z `/lib/modules/<kernel-version>/eset/eea/eset_rtp` do tej samej ścieżki na komputerach docelowych.

2. Wywołaj `depmod <kernel-version>` na komputerach docelowych.

3. Uruchom ponownie produkt ESET Endpoint Antivirus for Linux na komputerze docelowym, aby zaktualizować tabelę modułów. Wykonaj następujące polecenie jako użytkownik uprzywilejowany:

```
systemctl restart eea
```

We wszystkich przypadkach należy zastąpić `<kernel-version>` odpowiednią wersją jądra.

Instalacja

Program ESET Endpoint Antivirus for Linux jest rozpowszechniany w formie pliku binarnego (`.bin`).

> **Aktualizacja systemu operacyjnego**
> Przed instalacją programu ESET Endpoint Antivirus for Linux należy upewnić się, że w systemie operacyjnym zainstalowano najnowsze aktualizacje.

Instalacja za pośrednictwem terminalu

Aby zainstalować lub uaktualnić produkt, należy uruchomić skrypt dystrybucyjny firmy ESET dla używanej dystrybucji systemu operacyjnego z uprawnieniami użytkownika root:

- `./eeau.x86_64.bin`
- `sh ./eeau.x86_64.bin`

Aby wyświetlić dostępne parametry (argumenty) pliku binarnego programu ESET Endpoint Antivirus for Linux, należy uruchomić następujące polecenie w oknie terminalu:
`./eeau.x86_64.bin -h`

Dostępne parametry

Forma skrócona	Forma długa	Opis
`-h`	`--help`	Wyświetl argumenty wiersza polecenia
`-n`	`--no-install`	Nie przeprowadzaj instalacji po rozpakowaniu
`-y`	`--accept-license`	Nie pokazuj licencji, licencja została zaakceptowana
`-f`	`--force-install`	Wymuś instalację za pośrednictwem menedżera pakietów bez monitowania
`-u`	`--unpack-ertp-sources`	Rozpakuj źródła "ESET Ochrona systemu plików w czasie rzeczywistym", jednak nie przeprowadzaj instalacji

> **Uzyskanie pakietu instalacyjnego w formacie .deb**
> Aby uzyskać pakiet instalacyjny w formacie `.deb` odpowiedni dla używanego systemu operacyjnego, uruchom skrypt dystrybucyjny firmy ESET z argumentem wiersza polecenia „`-n`”:
> `sudo ./eeau.x86_64.bin -n`
> lub
> `sudo sh ./eeau.x86_64.bin -n`

Aby wyświetlić informacje na temat zależności pakietu instalacyjnego, uruchom jedno z następujących poleceń:

- `dpkg -I <deb package>`
- `rpm -qRp <rpm package>`

Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie. Zaakceptuj umowę licencyjną produktu, aby zakończyć instalację.

W przypadku problemów dotyczących zależności w instalatorze zostanie wyświetlony odpowiedni komunikat.

Instalacja za pomocą konsoli ESET PROTECT

Aby zdalnie wdrożyć program ESET Endpoint Antivirus for Linux na komputerach, należy zapoznać się z sekcją pomocy online Instalacja oprogramowania za pomocą konsoli ESET PROTECT.

Aby włączyć regularną aktualizację modułów wykrywania, należy aktywować program ESET Endpoint Antivirus for Linux.

> **Aplikacje innych firm**
> Podsumowanie dotyczące aplikacji innych firm używanych przez program ESET Endpoint Antivirus for Linux znajduje się w pliku `NOTICE_mode` zapisanym w lokalizacji `/opt/eset/eea/doc/modules_notice/`.

Odinstalowywanie

Aby odinstalować produkt firmy ESET, należy użyć okna terminalu jako administrator i wykonać polecenie usunięcia pakietów odpowiadających danej dystrybucji systemu Linux.

Dystrybucje oparte na systemie Ubuntu/Debian:

- `apt remove eea`

Dystrybucje oparte na systemie Red Hat:

- `yum remove eea`
- `rpm -e eea`

Wdrożenie masowe

Ten temat zawiera przegląd wysokiego poziomu wdrożenia masowego programu ESET Endpoint Antivirus for Linux za pomocą narzędzi Puppet, Chef i Ansible. Przedstawione poniżej bloki kodu obejmują tylko podstawowe przykłady metod instalacji pakietów. Mogą one różnić się w zależności od dystrybucji systemu Linux.

Wybór pakietu

Przed rozpoczęciem masowego wdrożenia programu ESET Endpoint Antivirus for Linux należy wybrać pakiet do zastosowania. Program ESET Endpoint Antivirus for Linux jest rozpowszechniany jako pakiet w formacie `.bin`. Można również uzyskać pakiet w formacie deb/rpm, uruchamiając skrypt dystrybucyjny firmy ESET z użyciem argumentu wiersza polecenia „`-n`”.

Puppet

Warunki wstępne

- pakiet w formacie bin lub deb/rpm dostępny na serwerze puppet-master
- agent puppet-agent połączony z serwerem puppet-master

Pakiet w formacie bin

Kroki wdrożenia:

- skopiowanie pakietu instalacyjnego w formacie bin na odpowiednie komputery
- uruchomienie pakietu instalacyjnego w formacie bin

Przykładowy manifest narzędzia Puppet

```
node default {
    file {"/tmp/eea-8.0.1081.0.x86_64.bin":
           mode => "0700",
           owner => "root",
           group => "root",
           source => "puppet:///modules/eea/eea-8.0.1081.0.x86_64.bin"
         }
    exec {"Execute bin package installation":
           command => '/tmp/eea-8.0.1081.0.x86_64.bin -y -f'
         }
}
```

Pakiet w formacie deb/rpm

Kroki wdrożenia:

- skopiowanie pakietu instalacyjnego w formacie deb/rpm zgodnie z rodziną dystrybucji na odpowiednie komputery
- uruchomienie pakietu instalacyjnego w formacie deb/rpm

Zależności

Problemy z zależnościami należy rozwiązać przed rozpoczęciem instalacji

Przykładowy manifest narzędzia Puppet

```
node default {
if $osfamily == 'Debian' {
        file {"/tmp/eea-8.0.1081.0.x86_64.deb":
               mode => "0700",
               owner => "root",
               group => "root",
               source => "puppet:///modules/eea/eea-8.0.1081.0.x86_64.deb"
             }
        package {"eea":
               ensure => "installed",
               provider => 'dpkg',
               source => "/tmp/eea-8.0.1081.0.x86_64.deb"
             }
}
if $osfamily == 'RedHat' {
        file {"/tmp/eea-8.0.1081.0.x86_64.rpm":
               mode => "0700",
               owner => "root",
               group => "root",
               source => "puppet:///modules/eea/eea-8.0.1081.0.x86_64.rpm"
             }
        package {"eea":
               ensure => "installed",
               provider => 'rpm',
               source => "/tmp/eea-8.0.1081.0.x86_64.rpm"
             }
 }
}
```

Chef

Warunki wstępne

- pakiet w formacie bin lub deb/rpm dostępny na serwerze Chef
- klient narzędzia Chef połączony z serwerem Chef

Pakiet w formacie bin

Kroki wdrożenia:

- skopiowanie pakietu instalacyjnego w formacie bin na odpowiednie komputery
- uruchomienie pakietu instalacyjnego w formacie bin

Przykładowy przepis narzędzia Chef

```
cookbook_file '/tmp/eea-8.0.1084.0.x86_64.bin' do
        source 'eea-8.0.1084.0.x86_64.bin'
        owner 'root'
        group 'root'
        mode '0700'
        action :create
end

execute 'package_install' do
        command '/tmp/eea-8.0.1084.0.x86_64.bin -y -f'
end
```

Pakiet w formacie deb/rpm

Kroki wdrożenia:

- skopiowanie pakietu instalacyjnego w formacie deb/rpm zgodnie z rodziną dystrybucji na odpowiednie komputery
- uruchomienie pakietu instalacyjnego w formacie deb/rpm

Zależności

Problemy z zależnościami należy rozwiązać przed rozpoczęciem instalacji

Przykładowy przepis narzędzia Chef

```
cookbook_file '/tmp/eea-8.0.1084.0.x86_64.deb' do
        source 'eea-8.0.1084.0.x86_64.deb'
        owner 'root'
        group 'root'
        mode '0700'
        action :create
        only_if { node['platform_family'] == 'debian'}
end

cookbook_file '/tmp/eea-8.0.1084.0.x86_64.rpm' do
                source 'eea-8.0.1084.0.x86_64.rpm'
                owner 'root'
                group 'root'
                mode '0700'
                action :create
                only_if { node['platform_family'] == 'rhel'}

dpkg_package 'eea' do
        source '/tmp/eea-8.0.1084.0.x86_64.deb'
        action :install
        only_if { node['platform_family'] == 'debian'}
end

rpm_package 'eea' do
        source '/tmp/eea-8.0.1084.0.x86_64.rpm'
        action :install
        only_if { node['platform_family'] == 'rhel'}
end
```

Ansible

Warunki wstępne

- pakiet w formacie bin lub deb/rpm dostępny na serwerze Ansible
- dostęp ssh do komputerów docelowych

Pakiet w formacie bin

Kroki wdrożenia:

- skopiowanie pakietu instalacyjnego w formacie bin na odpowiednie komputery
- uruchomienie pakietu instalacyjnego w formacie bin

Przykładowe zadanie Playbook

```
....
- name: "INSTALL: Copy configuration json files"
  copy:
    src: eea-8.0.1084.0.x86_64.bin
    dest: /home/ansible/

- name : "Install product bin package"
  shell: bash ./eea-8.0.1084.0.x86_64.bin -y -f -g
.....
```

Pakiet w formacie deb/rpm

Kroki wdrożenia:

- skopiowanie pakietu instalacyjnego w formacie deb/rpm zgodnie z rodziną dystrybucji na odpowiednie komputery
- uruchomienie pakietu instalacyjnego w formacie deb/rpm

Przykładowe zadanie Playbook

```
....
      - name: "Copy deb package to VM"
        copy:
          src: ./eea-8.0.1085.0.x86_64.deb
          dest: /home/ansible/eea-8.0.1085.0.x86_64.deb
          owner: ansible
          mode: a+r
        when:
          - ansible_os_family == "Debian"

      - name: "Copy rom package to VM"
        copy:
          src: ./eea-8.0.1085.0.x86_64.rpm
          dest: /home/ansible/eea-8.0.1085.0.x86_64.rpm
          owner: ansible
          mode: a+r
        when:
          - ansible_os_family == "RedHat"

      - name: "Install deb package"
        apt:
          deb: /home/ansible/eea-8.0.1085.0.x86_64.deb
          state: present
        when:
          - ansible_os_family == "Debian"

      - name: "Install rpm package"
        apt:
          deb: /home/ansible/eea-8.0.1085.0.x86_64.rpm
          state: present
        when:
          - ansible_os_family == "RedHat"
....
```

Aktualizowanie, uaktualnianie

Szybkie przechodzenie do uaktualnienia

Aktualizowanie modułów

Moduły produktu, włącznie z modułami wykrywania, są aktualizowane automatycznie.

Aby ręcznie uruchomić aktualizację modułu wykrywania, uruchom polecenie aktualizacji w oknie terminala lub zaktualizuj moduł za pomocą programu ESET PROTECT.

Jeśli aktualizacja programu ESET Endpoint Antivirus for Linux okazała się niestabilna, można wycofać aktualizację modułów, przywracając poprzedni stan. Uruchom odpowiednie polecenie w oknie terminala lub wycofaj aktualizację za pomocą programu ESET PROTECT.

Aby zaktualizować wszystkie moduły produktu z okna terminalu, wykonaj następujące polecenie:

```
/opt/eset/eea/bin/upd -u
```

Aktualizowanie i wycofywanie za pośrednictwem terminalu

Opcje — forma skrócona	Opcje — forma długa	Opis
`-u`	`--update`	Aktualizuj moduły
`-c`	`--cancel`	Anuluj pobieranie modułów
`-e`	`--resume`	Odblokuj aktualizacje
`-l`	`--list-modules`	Pokaż wersję używanych modułów
`-r`	`--rollback=VALUE`	Wycofuje najstarszą migawkę modułu skanera i blokuje wszystkie aktualizacje przez liczbę godzin określoną parametrem `WARTOŚĆ`

Nie można wprowadzać zmian w konfiguracji produktu za pomocą narzędzia `upd`.

PRZYKŁAD

Aby zatrzymać aktualizacje na 48 godzin i wycofać najstarszą migawkę modułu skanera, wykonaj następujące polecenie jako użytkownik uprzywilejowany:

```
sudo /opt/eset/eea/bin/upd --update --rollback=48
```

Aby wznowić automatyczne aktualizacje modułu skanera, wykonaj następujące polecenie jako użytkownik uprzywilejowany:

```
sudo /opt/eset/eea/bin/upd --update --cancel
```

Aby przeprowadzić aktualizację z serwera kopii dystrybucyjnych dostępnego pod adresem IP „192.168.1.2” i portem „2221”, wykonaj następujące polecenie jako użytkownik uprzywilejowany:

```
sudo /opt/eset/eea/bin/upd --update --server=192.168.1.2:2221
```

Uaktualnienie ESET Endpoint Antivirus do nowszej wersji dla systemu Linux (EEAU)

Nowsze wersje programu EEAU publikuje się w celu wprowadzania w nim poprawek lub udoskonaleń, których nie można wdrożyć w ramach automatycznych aktualizacji poszczególnych modułów.

Która wersja produktu jest obecnie zainstalowana?

Są dostępne dwie opcje sprawdzania wersji produktu programu EEAU:

1. Wykonaj polecenie /opt/eset/eea/lib/egui -v w oknie terminalu.
2. Sprawdź w programie ESET PROTECT (wcześniej ESET PROTECT) w sekcji Komputery.

Uaktualnianie?

Aby uaktualnić program do nowszej wersji, uruchom pakiet instalacyjny dla danego systemu operacyjnego w sposób opisany w sekcji Instalacja.

W przypadku zarządzania programem ESET Endpoint Antivirus for Linux za pomocą konsoli ESET PROTECT można zainicjować uaktualnienie za pośrednictwem zadania Instalacja oprogramowania lub przechodząc do obszaru **Panel kontrolny** > **Aplikacje firmy ESET** > kliknij prawym przyciskiem pozycję ESET Endpoint Antivirus for Linux > **Zaktualizuj zainstalowane produkty firmy ESET**.

> **Bezpośrednia aktualizacja z ESET NOD32 Antivirus 4 Business Edition for Linux Desktop nie jest możliwa**
> ESET Endpoint Antivirus for Linux jest całkowicie nowym produktem, a jego konfiguracja nie jest kompatybilna z konfiguracją ESET NOD32 Antivirus 4 Business Edition for Linux Desktop.

Aby uaktualnić ESET NOD32 Antivirus 4 Business Edition for Linux Desktop do ESET Endpoint Antivirus for Linux, postępuj zgodnie z poniższymi instrukcjami.

Zdalnie zarządzane środowisko (ESET PROTECT)

Jeśli zarządzasz produktem ESET NOD32 Antivirus 4 Business Edition for Linux Desktop zdalnie, ESET PROTECT nie powiadomi o dostępnym uaktualnieniu.

1. Wykonaj zadanie Dezinstalacja oprogramowania dla istniejących instalacji programu ESET NOD32 Antivirus 4 Business Edition for Linux Desktop.

2. Wdróż zdalnie produkt ESET Endpoint Antivirus for Linux na komputerach przy użyciu zadania Instalacja oprogramowania.

Środowisko zarządzane osobiście

Jeśli spróbujesz zainstalować produkt ESET Endpoint Antivirus for Linux przed usunięciem produktu ESET NOD32 Antivirus 4 Business Edition for Linux Desktop, instalacja zakończy się niepowodzeniem i wyświetlony zostanie następujący komunikat:

"Błąd: Poprzedni produkt ESET Security musi zostać najpierw odinstalowany. Pakiet nie zostanie zainstalowany."

1. Odinstaluj produkt ESET NOD32 Antivirus 4 Business Edition for Linux Desktop za pomocą pobranego instalatora.

    i. Kliknij prawym przyciskiem myszy pobrany plik instalatora `eset_nod32av_64bit_<languge_code>.linux`, kliknij kartę **Właściwości** > **Uprawnienia**, zaznacz opcję **Zezwalaj na wykonanie pliku jako programu** i zamknij okno.

    ii. Kliknij dwukrotnie instalator, aby uruchomić **instalatora produktu ESET NOD32 Antivirus**.

    iii. Kliknij przycisk **Dalej**, wybierz pozycję **Odinstaluj program ESET NOD32 Antivirus z komputera** i kliknij przycisk **Dalej**.

    iv. Z listy rozwijanej **Wybierz jedną z opcji** wybierz pozycję **Żadna z wymienionych**.

v. Wprowadź "*Uaktualnij do ESET Endpoint Antivirus for Linux*" w polu **Inne dodatkowe dane**, kliknij przycisk **Dalej**, a następnie **Odinstaluj**.

vi. Po zakończeniu kliknij przycisk **Zakończ**, a następnie przycisk **Tak**, aby ponownie uruchomić komputer.

2. Zainstaluj program ESET Endpoint Antivirus for Linux.

Kopia dystrybucyjna aktualizacji

Wiele produktów zabezpieczających firmy ESET (ESET PROTECT, ESET Endpoint Antivirus itp.) umożliwia tworzenie kopii plików aktualizacji, których można używać do aktualizowania innych stacji roboczych w sieci. Korzystanie z kopii dystrybucyjnej, czyli kopii plików aktualizacji, w środowisku sieci LAN jest wygodne, ponieważ eliminuje potrzebę pobierania tych plików przez każdą stację roboczą bezpośrednio z serwera aktualizacji dostawcy. Aktualizacje są pobierane na lokalny serwer kopii dystrybucyjnych, a następnie rozpowszechniane do wszystkich stacji roboczych, aby uniknąć ryzyka generowania nadmiernego ruchu sieciowego. Aktualizowanie klienckich stacji roboczych przy użyciu kopii dystrybucyjnej pozwala na oszczędne korzystanie z przepustowości połączenia internetowego.

Skonfiguruj ESET Endpoint Antivirus for Linux, aby korzystać z kopii dystrybucyjnej aktualizacji

1. W ESET PROTECT kliknij kolejno **Polityki** > **Nowa polityka** i wpisz nazwę nowej polityki.

2. Kliknij przycisk **Ustawienia** i wybierz z menu rozwijanego pozycję**ESET Endpoint for Linux (V7+)**.

3. Kliknij kolejno **Aktualizuj** > **Główny serwer**.

4. W sekcji **Podstawowe** dezaktywuj przełącznik obok pozycji **Wybierz automatycznie**.

5. W polu **Serwer aktualizacji** wpisz adres URL serwera kopii dystrybucyjnych w jednym z poniższych formatów:

   - `http://<IP>:<port>`
   - `http://<hostname>:<port>`

6. Wprowadź odpowiednią nazwę użytkownika i hasło.

7. Kliknij **Kontynuuj** > **Przypisz**, a następnie wybierz grupę komputerów, wobec których polityka będzie miała zastosowanie.

8. Kliknij przycisk **OK**, a następnie przycisk **Zakończ**.

Jeśli w sieci znajduje się więcej serwerów kopii dystrybucyjnych, powtórz powyższe kroki, aby skonfigurować pomocnicze serwery aktualizacji.

Aktywacja usługi ESET Endpoint Antivirus for Linux

Program ESET Endpoint Antivirus for Linux należy aktywować za pomocą licencji uzyskanej od lokalnego dystrybutora firmy ESET.

Aktywacja za pomocą terminalu

Można użyć narzędzia `/opt/eset/eea/sbin/lic` jako użytkownik uprzywilejowany, aby aktywować program ESET Endpoint Antivirus for Linux z okna terminalu.

Składnia: `/opt/eset/eea/sbin/lic [OPTIONS]`

PRZYKŁADY:

Poniższe polecenia należy wykonać jako użytkownik uprzywilejowany

Aktywacja za pomocą klucza licencyjnego

```
/opt/eset/eea/sbin/lic -k XXXX-XXXX-XXXX-XXXX-XXXX
```

lub

```
/opt/eset/eea/sbin/lic --key XXXX-XXXX-XXXX-XXXX-XXXX
```

gdzie ciąg XXXX-XXXX-XXXX-XXXX-XXXX oznacza klucz licencyjny programu ESET Endpoint Antivirus for Linux.

Aktywacja za pomocą nazwy użytkownika i hasła

Poniższe polecenia należy wykonać jako użytkownik uprzywilejowany:

```
/opt/eset/eea/sbin/lic -u <username> -p <public_id>
```

użytkownik zostanie poproszony o wprowadzenie hasła. `public_id` to identyfikator licencji publicznej. Jeśli nazwa użytkownika, hasło i identyfikator licencji publicznej są przechowywane w pliku `password.txt`, wykonaj następujące czynności jako uprzywilejowany użytkownik:

```
cat password.txt | /opt/eset/eea/sbin/lic -u <username> -p <public_id> --stdin-pass
```

Aktywacja za pomocą pliku licencji offline

```
/opt/eset/eea/sbin/lic -f offline_license.lf
```

lub

```
/opt/eset/eea/sbin/lic -FILE=offline_license.lf
```

Aktywuj za pomocą ESET PROTECT

Zaloguj się do interfejsu webowego konsoli ESET PROTECT, przejdź do obszaru **Zadania klienta** > **Aktywacja produktu**, a następnie postępuj według instrukcji dotyczących aktywacji produktu.

Gdzie znajduje się licencja?

Jeśli zakupiono licencję, powinny nadejść dwie wiadomości e-mail z firmy ESET. W pierwszej wiadomości znajdują się informacje dotyczące portalu konta ESET Business Account. Druga wiadomość zawiera klucz licencyjny (XXXXX-XXXXX-XXXXX-XXXXX-XXXXX) lub nazwę użytkownika (EAV-xxxxxxxxxx) i hasło (w przypadku określonych produktów), identyfikator licencji publicznej (xxx-xxx-xxx), nazwę produktu lub listę produktów oraz ich ilość.

Jest dostępna nazwa użytkownika i hasło

Jeśli jest dostępna nazwa użytkownika i hasło, można skonwertować te poświadczenia na klucz licencyjny na stronie konwersji licencji na koncie ESET Business Account:

https://eba.eset.com/LicenseConverter

Sprawdź stan aktywacji

Aby wyświetlić stan aktywacji i ważność licencji, użyj narzędzia `lic`. Wykonaj następujące polecenia jako uprzywilejowany użytkownik:

Składnia: `/opt/eset/eea/sbin/lic [OPTIONS]`

Poniższe polecenia należy wykonać jako użytkownik uprzywilejowany:
`/opt/eset/eea/sbin/lic -s`
lub
`/opt/eset/eea/sbin/lic --status`

Przykładowy rezultat w przypadku aktywacji produktu:
```
Status: Aktywowany
Identyfikator publiczny: ABC-123-DEF
Ważność licencji: 2020-03-29
```

Rezultat w przypadku braku aktywacji produktu:
```
Stan: Nie aktywowano
```

Jeśli rozwiązanie ESET Dynamic Threat Defense jest aktywowane dla określonego wystąpienia ESET Endpoint Antivirus for Linux, wyświetlane są szczegóły powiązanej licencji.

W przypadku wersji 8.1 lub nowszej, aby wyświetlić identyfikator stanowiska na żądanie działu obsługi klienta firmy ESET, wykonaj polecenie:

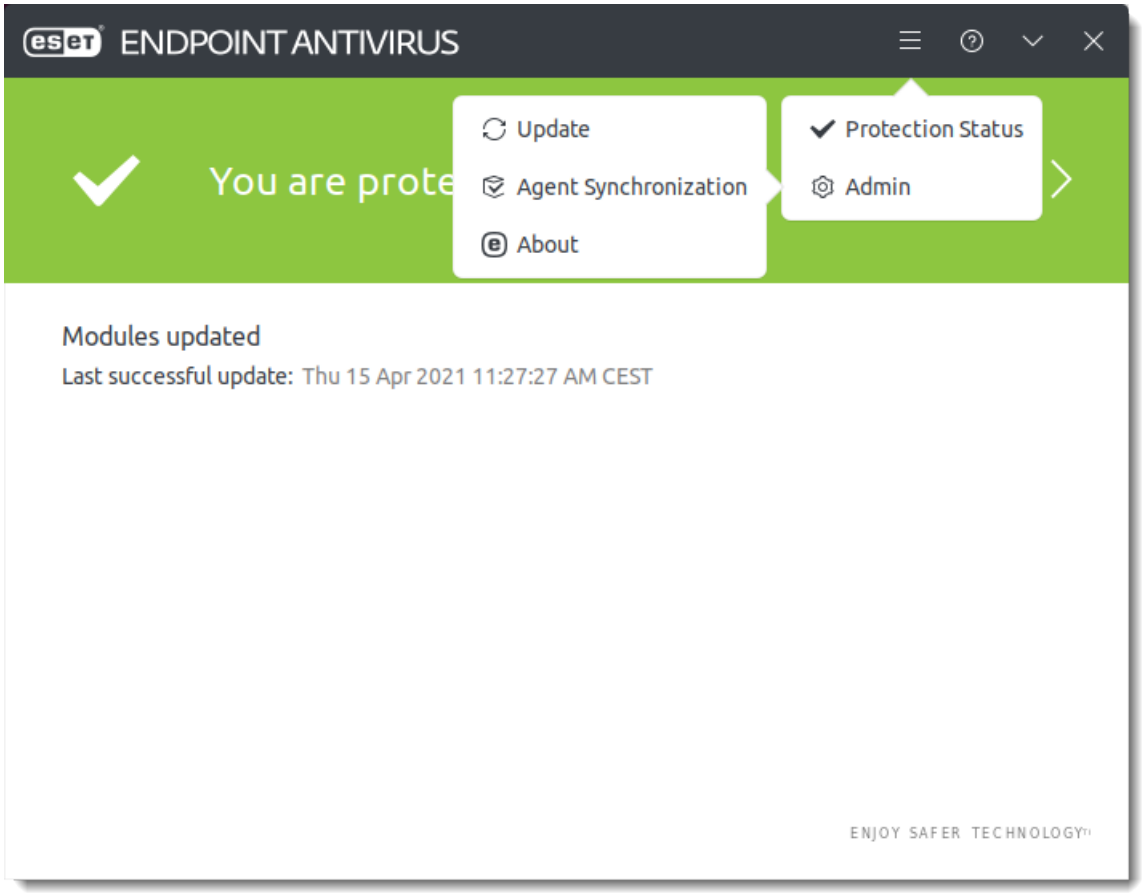
```
/opt/eset/efs/sbin/lic -s --with-details
```

Używanie programu ESET Endpoint Antivirus for Linux

Jeżeli instalacja została zakończona, użyj okna terminala lub programu ESET PROTECT do obsługi programu ESET Endpoint Antivirus for Linux.

Interfejs użytkownika

Program ESET Endpoint Antivirus for Linux wprowadza minimalistyczny graficzny interfejs użytkownika.



Ekran główny zawiera przegląd stanu ochrony, alertów i powiadomień.

Jeśli przejdziesz do dowolnego ekranu w menu , kliknij przycisk Wstecz , aby wrócić do ekranu głównego.

Stan ochrony

Jeśli wszystko działa bez problemów, ogólny stan ochrony (na ekranie głównym) jest oznaczony na zielono. Jeśli są dostępne opcje zwiększenia poziomu stanu ochrony systemu lub wykryto niewystarczający poziom stanu ochrony, kolor zmieni się na czerwony.

Aby uzyskać więcej informacji na temat stanu ochrony, kliknij ikonę menu > **Stan ochrony**.

Aktualizacja

Aby ręcznie uruchomić aktualizacje modułów, kliknij ikonę menu > **Administrator** > **Aktualizuj**. Na ekranie wyświetlana jest ostatnia pomyślna aktualizacja i ostatnie sprawdzenie dostępności aktualizacji.

Zainstalowane moduły

Listę zainstalowanych modułów można wyświetlić na dwa sposoby:

1. Kliknij ikonę menu > **Administrator** > **Aktualizuj** > **Pokaż wszystkie moduły**.
2. Kliknij ikonę menu > **Administrator** > **Informacje** > **Pokaż wszystko**.

Synchronizacja agentów

Jeśli zarządzasz produktem ESET Endpoint Antivirus for Linux zdalnie, możesz zobaczyć niektóre szczegóły agenta

zarządzania w menu ☰ > **Administrator** > **Synchronizacja z Agentem**.

Szczegóły obejmują informacje takie jak:

- Bieżąca wersja — wersja aktualnie zainstalowanego agenta zdalnego zarządzania
- Ostatnia replikacja — ostatnia próba synchronizacji między agentem zdalnego zarządzania, a ESET PROTECT
- Ostatnia pomyślna replikacja
- Ostatni wygenerowany dziennik stanu — ostatni dziennik stanu wygenerowany przez agenta zarządzania. Plik dziennika znajduje się pod adresem `/var/log/eset/RemoteAdministrator/Agent/status.html`

informacje

W oknie **Informacje** można znaleźć szczegółowe informacje na temat zainstalowanej wersji programu ESET Endpoint Antivirus for Linux, systemu operacyjnego oraz zasobów systemowych.

Kliknij pozycję **Pokaż wszystko**, aby wyświetlić informacje dotyczące zainstalowanych modułów programów.

Skanowanie

Szybkie łącza: Profile skanowania

Uruchamianie skanowania na żądanie z okna terminalu

Składnia: `/opt/eset/eea/bin/odscan [OPTIONS]`

Opcje — forma skrócona	Opcje — forma długa	Opis
`-l`	`--list`	Pokaż aktualnie uruchomione skanowania
	`--list-profiles`	Pokaż wszystkie dostępne profile skanowania
	`--all`	Pokaż również skanowania wykonywane przez innych użytkowników (wymaga uprawnień użytkownika root)
`-r`	`--resume=session_id`	Wznów wstrzymane skanowanie identyfikowane parametrem `session_id`
`-p`	`--pause=session_id`	Wstrzymaj skanowanie identyfikowane parametrem `session_id`
`-t`	`--stop=session_id`	Zatrzymaj skanowanie identyfikowane parametrem `session_id`
`-s`	`--scan`	Start scan
	`--profile=PROFILE`	Skanuj za pomocą wybranego PROFILU
	`--profile-priority=PRIORITY`	Zadanie zostanie uruchomione z określonym priorytetem. Dostępne ustawienia priorytetu: `normalny`, `niższy`, `najniższy`, `bezczynność`
	`--readonly`	Skanuj bez leczenia
	`--local`	Skanuj dyski lokalne

Opcje — forma skrócona	Opcje — forma długa	Opis
	`--network`	Skanuj dyski sieciowe
	`--removable`	Skanuj nośniki wymienne
	`--boot-local`	Skanuj sektory rozruchowe dysku lokalnego
	`--boot-removable`	Skanuj sektory rozruchowe nośników wymiennych
	`--boot-main`	Skanuj główny sektor rozruchowy
	`--exclude=FILE`	Pomiń wybrany plik lub katalog
	`--ignore-exclusions`	Skanuj również wyłączone ścieżki i rozszerzenia

PRZYKŁAD

Uruchomienie skanowania na żądanie katalogu */root/* rekursywnie z użyciem profilu skanowania „@Skanowanie inteligentne” jako procesu w tle:

```
/opt/eset/eea/bin/odscan --scan --profile="@Smart scan" /root/* &
```

Uruchomienie skanowania z użyciem profilu skanowania „@Skanowanie inteligentne” rekursywnie w odniesieniu do wielu lokalizacji docelowych:

```
/opt/eset/eea/bin/odscan --scan --profile="@Smart scan" /root/* /tmp/* /home/*
```

Wyświetlenie listy wszystkich uruchomionych skanowań:

```
/opt/eset/eea/bin/odscan -l
```

Wstrzymanie skanowania o parametrze session-id „15”. Każde skanowanie ma unikatowy parametr session-id generowany podczas jego uruchomienia.

```
/opt/eset/eea/bin/odscan -p 15
```

Zatrzymanie skanowania o parametrze session-id „15”. Każde skanowanie ma unikatowy parametr session-id generowany podczas jego uruchomienia.

```
/opt/eset/eea/bin/odscan -t 15
```

Uruchomienie skanowania na żądanie wyłączonego katalogu */root/exc_dir* i wyłączonego pliku */root/eicar.com*:

```
/opt/eset/eea/bin/odscan --scan --profile="@In-depth scan" --
exclude=/root/exc_dir/ --exclude=/root/eicar.com /
```

Skanowanie sektora rozruchowego nośników wymiennych. Należy wykonać poniższe polecenie jako użytkownik uprzywilejowany:

```
sudo /opt/eset/eea/bin/odscan --scan --profile="@In-depth scan" --boot-removable
```

Kody zakończenia

Narzędzie `odscan` kończy się kodem zakończenia po zakończeniu skanowania. Wykonaj `echo $?` w oknie Terminal po zakończeniu skanowania, aby wyświetlić kod zakończenia.

Kody zakończenia	Znaczenie
0	Nie znaleziono zagrożenia.
1	Zagrożenie zostało wykryte i usunięte
10	Niektórych plików nie można przeskanować (mogą stanowić zagrożenia).
50	Znaleziono zagrożenie
100	Błąd

Profile skanowania

Preferowane parameters (Threatsense parameters) skanowania mogą zostać zapisane i użyte w przyszłości. Zaleca się utworzenie osobnego profilu (z ustawionymi różnymi obiektami i metodami skanowania oraz innymi parametrami) dla każdego regularnie używanego skanowania.

Tworzenie nowego profilu za pomocą ESET PROTECT

1. W ESET PROTECT kliknij kolejno **Polityki** > **Nowa polityka** i wpisz nazwę nowej polityki.

2. Kliknij przycisk **Ustawienia** i wybierz z menu rozwijanego pozycję**ESET Endpoint for Linux (V7+)**.

3. Kliknij **Skanowania w poszukiwaniu szkodliwego oprogramowania > Skanowanie na żądanie**, a następnie kliknij opcję **Edytuj** obok pozycji **Lista profili**.

4. Wpisz nazwę nowego profilu, kliknij przycisk **Dodaj**, a następnie kliknij **Zapisz**.

5. Wybierz nowo utworzony profil z menu rozwijanego **Wybrany profil** i dostosuj ustawienia dotyczące skanowania w sekcji **Skanowania w poszukiwaniu szkodliwego oprogramowania**.

6. Przejdź do opcji **Przypisz**, kliknij **Przypisz** i wybierz grupę komputerów, wobec których polityka będzie miała zastosowanie.

7. Kliknij przycisk **OK**, a następnie przycisk **Zakończ**.

Wyłączenia

Wykluczenia wydajności

Czas potrzebny na przeskanowania systemu plików w poszukiwaniu złośliwego oprogramowania można znacznie skrócić, wyłączając niektóre ścieżki (foldery) z procesu skanowania.

1. W ESET PROTECT kliknij kolejno **Polityki** > **Nowa polityka** i wpisz nazwę nowej polityki.

2. Kliknij przycisk **Ustawienia** i wybierz z menu rozwijanego pozycję**ESET Endpoint for Linux (V7+)**.

3. Przejdź do opcji **Silnik detekcji** > **Podstawowe** i kliknij opcję **Edytuj** obok pozycji **Pliki i foldery wyłączone ze skanowania**.

4. Kliknij przycisk **Dodaj** i określ **ścieżkę**, którą skaner ma pominąć. Możesz też dodać komentarz pomocniczy.

5. Kliknij przycisk **OK**, a następnie kliknij przycisk **Zapisz**, aby zamknąć okno dialogowe.

6. Kliknij **Kontynuuj** > **Przypisz**, a następnie wybierz grupę komputerów, wobec których polityka będzie miała zastosowanie.

7. Kliknij przycisk **OK**, a następnie przycisk **Zakończ**.

Ścieżka &wyłączenia

*/root/** , — katalog „*root*„ oraz jego wszystkie podkatalogi z zawartością.

/root — Tylko plik „*root*”.

/root/file.txt — Tylko plik file.txt w katalogu „*root*”.

> Symbole wieloznaczności w środku ścieżki
> Zdecydowanie zalecamy, aby nie używać symboli wieloznaczności w środku ścieżki (na przykład */home/user/*/data/file.dat*), chyba że wymaga tego infrastruktura systemowa. Aby uzyskać więcej informacji, zobacz następujący artykuł bazy wiedzy.

Wyłączenia rozszerzeń plików

Ten typ wyłączenia można skonfigurować w przypadku funkcji **Ochrona systemu plików w czasie rzeczywistym**, **Skanowanie na żądanie**.

1. W ESET PROTECT kliknij kolejno **Polityki** > **Nowa polityka** i wpisz nazwę nowej polityki.

2. Kliknij przycisk **Ustawienia** i wybierz z menu rozwijanego pozycję**ESET Endpoint for Linux (V7+)**.

1. Przejdź do pliku:

• **Ochrona systemu plików w czasie rzeczywistym** > **Parametry technologii Threatsense**

• **Skanowania w poszukiwaniu szkodliwego oprogramowania** > **Skanowanie na żądanie** > **Parametry technologii Threatsense**

2. Kliknij przycisk **Edytuj** obok pozycji **Lista rozszerzeń plików wyłączonych ze skanowania**.

3. Kliknij przycisk **Dodaj** i wpisz rozszerzenie do wyłączenia. Aby równocześnie zdefiniować wiele rozszerzeń,

kliknij opcję **Wprowadź wiele wartości**, a następnie wpisz odpowiednie rozszerzenia, umieszczając je w nowych wierszach lub używając innego wybranego separatora.

4. Kliknij przycisk **OK**, a następnie kliknij przycisk **Zapisz**, aby zamknąć okno dialogowe.

5. Kliknij **Kontynuuj** > **Przypisz**, a następnie wybierz grupę komputerów, wobec których polityka będzie miała zastosowanie.

6. Kliknij przycisk **OK**, a następnie przycisk **Zakończ**.

Kwarantanna

Główną funkcją kwarantanny jest bezpieczne przechowywanie zainfekowanych plików. Pliki należy poddawać kwarantannie w przypadku, gdy nie można ich wyleczyć, ich usunięcie nie jest bezpieczne lub zalecane oraz gdy są one nieprawidłowo wykrywane przez program ESET Endpoint Antivirus for Linux. Kwarantanną można objąć dowolny plik, szczególnie, jeśli plik zachowuje się w podejrzany sposób, ale nie jest wykrywany przez skaner antywirusowy.

Ścieżka do katalogu kwarantanny: */var/opt/eset/eea/cache/quarantine/*

Katalog kwarantanny jest tworzony po wykryciu pierwszego elementu, który musi zostać poddany kwarantannie.

Zarządzanie elementami poddanymi kwarantannie za pośrednictwem terminalu

Składnia: `/opt/eset/eea/bin/quar [OPTIONS]`

Opcje — forma skrócona	Opcje — forma długa	Opis
`-i`	`--import`	Importuj plik do kwarantanny
`-l`	`--list`	Wyświetl listę plików poddanych kwarantannie
`-r`	`--restore=id`	Przywróć element poddany kwarantannie według identyfikatora do ścieżki zdefiniowanej przez `--restore-path`
`-e`	`--restore-exclude=id`	Przywróć element poddany kwarantannie według identyfikatora i oznaczony symbolem „x” w kolumnie podlega wyłączeniu
`-d`	`--delete=id`	Usuń element poddany kwarantannie według `id`
`-f`	`--follow`	Zaczekaj na nowe elementy i dodaj je do danych wyjściowych
	`--restore-path=path`	Ścieżka do przywrócenia elementów poddanych kwarantannie
`-h`	`--help`	Pokaż pomoc i zakończ.
`-v`	`--version`	Pokaż informacje o wersji i zakończ.

> **Przywróć**
> Przywracanie nie jest dostępne, jeśli polecenie nie jest wykonywane przez użytkownika uprzywilejowanego.

PRZYKŁAD

Usunięcie elementu poddanego kwarantannie o identyfikatorze „0123456789”:

```
/opt/eset/eea/bin/quar -d 0123456789
```

lub

```
/opt/eset/eea/bin/quar --delete=0123456789
```

Przywrócenie elementu poddanego kwarantannie o identyfikatorze „9876543210” do folderu *Download* zalogowanego użytkownika i zmiana jego nazwy na *restoredFile.test*:

```
/opt/eset/eea/bin/quar -r 9876543210 --restore-
path=/home/$USER/Download/restoredFile.test
```

lub

```
/opt/eset/eea/bin/quar --restore=9876543210 --restore-
path=/home/$USER/Download/restoredFile.test
```

Przywrócenie elementu poddanego kwarantannie o identyfikatorze „123456789” oznaczonego symbolem „**x**” w kolumnie **podlega wyłączeniu** do folderu *Download*:

```
/opt/eset/eea/bin/quar -e 9876543210 --restore-path=/home/$USER/Download/
```

lub

```
/opt/eset/eea/bin/quar --restore-exclude=9876543210 --restore-
path=/home/$USER/Download/
```

Przywracanie pliku z kwarantanny za pośrednictwem terminalu

1. Wyświetl listę elementów poddanych kwarantannie.
   `/opt/eset/eea/bin/quar -l`

2. Wyszukaj identyfikator i nazwę obiektu poddanego kwarantannie, który chcesz przywrócić, a następnie uruchom następujące polecenie:
   `/opt/eset/eea/bin/quar --restore=ID_OF_OBJECT_TO_RESTORE --restore-path=/final/path/of/restored/file`

Zdarzenia

W programie ESET Endpoint Antivirus for Linux (EEAU) polecenia wykonane za pośrednictwem terminala i inne informacje są rejestrowane przez EEAU.

Każdy wpis zarejestrowanej czynności obejmuje następujące informacje: godzina wystąpienia zdarzenia, komponent (jeśli dane są dostępne), zdarzenie i użytkownik

Wyświetlanie zdarzeń za pośrednictwem terminalu

Aby wyświetlić zarejestrowane **Zdarzenia** za pośrednictwem okna terminala, użyj narzędzia wiersza polecenia `lslog` jako użytkownik uprzywilejowany.

Składnia: `/opt/eset/eea/sbin/lslog [OPTIONS]`

Opcje — forma skrócona	Opcje — forma długa	Opis
`-f`	`--follow`	Zaczekaj na nowe dzienniki i dodaj je do danych wyjściowych
`-o`	`--optimize`	Zoptymalizuj dzienniki
`-c`	`--csv`	Wyświetl dzienniki w formacie CSV
`-e`	`--events`	Wyświetl listę dzienników zdarzeń
`-l`	`--device-control`	Lista dzienników kontroli dostępu do urządzeń
`-n`	`--sent-files`	Wyświetl listę plików przesłanych do analizy
`-s`	`--scans`	Wyświetl listę dzienników skanowania na żądanie
	`--with-log-name`	Wyświetl wraz z kolumną Nazwa dziennika
	`--ods-details=log-name`	Wyświetl szczegóły skanowania na żądanie według nazwy dziennika
	`--ods-detections=log-name`	Wyświetl wykrycia skanowania na żądanie według nazwy dziennika
	`--ods-notscanned=log-name`	Wyświetl nieskanowane elementy skanowania na żądanie według nazwy dziennika
`-d`	`--detections`	Wyświetl rekordy dzienników wykrywania

PRZYKŁADY

Wyświetlanie wszystkich dzienników zdarzeń:

```
/opt/eset/eea/sbin/lslog -e
```

Zapisywanie wszystkich dzienników zdarzeń w formacie CSV do pliku w katalogu *Documents* bieżącego użytkownika:

```
/opt/eset/eea/sbin/lslog -ec > /home/$USER/Documents/eventlogs.csv
```

Wyświetlaj wszystkie wykryte zagrożenia i czynności podjęto przeciwko:

```
/opt/eset/eea/sbin/lslog -d
```

Powiadomienia

EEAU wyświetla różne powiadomienia informujące o aktywności lub wymaganym działaniu. Niektóre powiadomienia można włączać i wyłączać.

Powiadomienia dotyczą:

- Skanowania na żądanie — na przykład rozpoczęto lub ukończono skanowanie urządzenia wymiennego.
- Sterowania urządzeniem — urządzenie zostało zablokowane lub zapisywanie danych na urządzeniu jest niedozwolone.
- Wykryć — na przykład zagrożenie zostało znalezione lub usunięte lub plik został wyczyszczony.
- Systemu operacyjnego — wymagane jest ponowne uruchomienie lub jest zaplanowane zamknięcie systemu.
- EDTD od EEAU w wersji 8.1 — na przykład plik jest analizowany i dlatego nie może być tymczasowo otwarty.

Konfiguracja

Aby zmienić konfigurację programu ESET Endpoint Antivirus for Linux:

1. W ESET PROTECT kliknij kolejno **Polityki** > **Nowa polityka** i wpisz nazwę nowej polityki.
2. Kliknij przycisk **Ustawienia** i wybierz z menu rozwijanego pozycję**ESET Endpoint for Linux (V7+)**.
3. Dostosuj ustawienia.
4. Kliknij **Kontynuuj** > **Przypisz**, a następnie wybierz grupę komputerów, wobec których polityka będzie miała zastosowanie.
5. Kliknij przycisk **OK**, a następnie przycisk **Zakończ**.

> **Dostosowywanie istniejących ustawień polityki**
> Aby dostosować istniejące ustawienia polityki dla ESET Endpoint Antivirus for Linux, kliknij politykę, którą chcesz zmienić, na liście polityk, a następnie kliknij przycisk **Edytuj**.

Można dostosować czynności wykrywania, aktualizacje produktu i ustawienia połączeń.

Jeśli program ESET Endpoint Antivirus for Linux skonfigurowano zgodnie z wymaganiami i użytkownik chce zapisać konfigurację do późniejszego użycia (lub zastosowania w przypadku innego wystąpienia programu ESET Endpoint Antivirus for Linux), można wyeksportować ją do pliku `.XML`.

Uruchom następujące polecenia z okna terminalu z uprawnieniami użytkownika root.

Eksportowanie konfiguracji

```
/opt/eset/eea/lib/cfg --export-xml=/tmp/export.xml
```

Importowanie konfiguracji

```
/opt/eset/eea/lib/cfg --import-xml=/tmp/export.xml
```

Dostępne opcje

Forma skrócona	Forma długa	Opis
`-i`	`--json-rpc`	list of json-rpc files
	`--import-xml`	import settings
	`--export-xml`	export settings
`-h`	`--help`	show help
`-v`	`--version`	show version information

Silnik detekcji

Konfiguracja domyślna czynności wykrywania zapewnia konieczny poziom ochrony obejmujący następujące funkcje:

- Ochrona systemu plików w czasie rzeczywistym
- Inteligentna optymalizacja (najbardziej wydajne połączenie ochrony systemu i szybkości skanowania)
- System reputacji ESET LiveGrid

Aby włączyć dodatkowe funkcje ochrony, użyj ESET PROTECT

Aby zmienić konfigurację programu ESET Endpoint Antivirus for Linux:

1. W ESET PROTECT kliknij kolejno **Polityki** > **Nowa polityka** i wpisz nazwę nowej polityki.
2. Kliknij przycisk **Ustawienia** i wybierz z menu rozwijanego pozycję**ESET Endpoint for Linux (V7+)**.
3. Dostosuj ustawienia.
4. Kliknij **Kontynuuj** > **Przypisz**, a następnie wybierz grupę komputerów, wobec których polityka będzie miała zastosowanie.
5. Kliknij przycisk **OK**, a następnie przycisk **Zakończ**.

> **Dostosowywanie istniejących ustawień polityki**
> Aby dostosować istniejące ustawienia polityki dla ESET Endpoint Antivirus for Linux, kliknij politykę, którą chcesz zmienić, na liście polityk, a następnie kliknij przycisk **Edytuj**.

- Wykrywanie potencjalnie niepożądanych aplikacji
- Wykrywanie potencjalnie niebezpiecznych aplikacji (np. programów rejestrujących znaki wprowadzane przez użytkownika, narzędzi do łamania haseł)
- Włączanie funkcji przesyłania próbek podejrzanych lub zainfekowanych plików
- Konfigurowanie wyłączeń (plików i katalogów wyłączonych ze skanowania) w celu przyspieszenia skanowania
- Włączanie udostępnionej lokalnej pamięci podręcznej

Aby wyświetlić wszystkie wykryte zagrożenia i podjęte czynności, użyj narzędzia lslog z parametrem --detections.

Wyłączenia

Wykluczenia wydajności

Czas potrzebny na przeskanowania systemu plików w poszukiwaniu złośliwego oprogramowania można znacznie skrócić, wyłączając niektóre ścieżki (foldery) z procesu skanowania.

1. W ESET PROTECT kliknij kolejno **Polityki** > **Nowa polityka** i wpisz nazwę nowej polityki.
2. Kliknij przycisk **Ustawienia** i wybierz z menu rozwijanego pozycję**ESET Endpoint for Linux (V7+)**.
3. Przejdź do opcji **Silnik detekcji** > **Podstawowe** i kliknij opcję **Edytuj** obok pozycji **Pliki i foldery wyłączone ze skanowania**.
4. Kliknij przycisk **Dodaj** i określ **ścieżkę**, którą skaner ma pominąć. Możesz też dodać komentarz pomocniczy.
5. Kliknij przycisk **OK**, a następnie kliknij przycisk **Zapisz**, aby zamknąć okno dialogowe.
6. Kliknij **Kontynuuj** > **Przypisz**, a następnie wybierz grupę komputerów, wobec których polityka będzie miała zastosowanie.
7. Kliknij przycisk **OK**, a następnie przycisk **Zakończ**.

Ścieżka &wyłączenia

*/root/** , — katalog „*root*„ oraz jego wszystkie podkatalogi z zawartością.

/root — Tylko plik „*root*”.

/root/file.txt — Tylko plik file.txt w katalogu „*root*”.

> **Symbole wieloznaczności w środku ścieżki**
> Zdecydowanie zalecamy, aby nie używać symboli wieloznaczności w środku ścieżki (na przykład */home/user/*/data/file.dat*), chyba że wymaga tego infrastruktura systemowa. Aby uzyskać więcej informacji, zobacz następujący artykuł bazy wiedzy.

Wyłączenia rozszerzeń plików

Ten typ wyłączenia można skonfigurować w przypadku funkcji **Ochrona systemu plików w czasie rzeczywistym**, **Skanowanie na żądanie**.

1. W ESET PROTECT kliknij kolejno **Polityki** > **Nowa polityka** i wpisz nazwę nowej polityki.

2. Kliknij przycisk **Ustawienia** i wybierz z menu rozwijanego pozycję**ESET Endpoint for Linux (V7+)**.

1. Przejdź do pliku:

• **Ochrona systemu plików w czasie rzeczywistym** > **Parametry technologii Threatsense**

• **Skanowania w poszukiwaniu szkodliwego oprogramowania** > **Skanowanie na żądanie** > **Parametry technologii Threatsense**

2. Kliknij przycisk **Edytuj** obok pozycji **Lista rozszerzeń plików wyłączonych ze skanowania**.

3. Kliknij przycisk **Dodaj** i wpisz rozszerzenie do wyłączenia. Aby równocześnie zdefiniować wiele rozszerzeń, kliknij opcję **Wprowadź wiele wartości**, a następnie wpisz odpowiednie rozszerzenia, umieszczając je w nowych wierszach lub używając innego wybranego separatora.

4. Kliknij przycisk **OK**, a następnie kliknij przycisk **Zapisz**, aby zamknąć okno dialogowe.

5. Kliknij **Kontynuuj** > **Przypisz**, a następnie wybierz grupę komputerów, wobec których polityka będzie miała zastosowanie.

6. Kliknij przycisk **OK**, a następnie przycisk **Zakończ**.

Ochrona systemu plików w czasie rzeczywistym

Ochrona systemu plików w czasie rzeczywistym sprawdza wszystkie zdarzenia związane z ochroną antywirusową systemu. Wszystkie pliki w momencie otwarcia, utworzenia lub uruchomienia na komputerze są skanowane w poszukiwaniu szkodliwego kodu. Domyślnie ochrona systemu plików w czasie rzeczywistym jest włączana przy uruchamianiu systemu i zapewnia nieprzerwane skanowanie.

> Ochrona systemu plików w czasie rzeczywistym nie skanuje zawartości plików w archiwach. Skanuje zawartość niektórych samorozpakowujących się archiwów po pobraniu ich na dysk twardy.

W wyjątkowych przypadkach (na przykład w przypadku konfliktu z innym skanerem w czasie rzeczywistym) można wyłączyć ochronę w czasie rzeczywistym:

1. W ESET PROTECT kliknij kolejno **Polityki** > **Nowa polityka** i wpisz nazwę nowej polityki.

2. Kliknij przycisk **Ustawienia** i wybierz z menu rozwijanego pozycję**ESET Endpoint for Linux (V7+)**.

3. Kolejno wybierz **Konfiguracja > Silnik detekcji > Ochrona systemu plików w czasie rzeczywistym > Podstawowa**.

4. Wyłącz opcję **Uruchom ochronę systemu plików w czasie rzeczywistym**.

5. Kliknij **Kontynuuj** > **Przypisz**, a następnie wybierz grupę komputerów, wobec których polityka będzie miała zastosowanie.

6. Kliknij przycisk **OK**, a następnie przycisk **Zakończ**.

Skanowane nośniki

Domyślnie wszystkie typy nośników są skanowane w celu wykrycia potencjalnych zagrożeń:

- **Dyski lokalne**— sprawdzane są wszystkie dyski twarde w komputerze.
- **Nośniki wymienne** — sprawdzane są płyty CD i DVD, urządzenia pamięci masowej USB, urządzenia Bluetooth itp.
- **Dyski sieciowe**— skanowane są wszystkie dyski mapowane.

Zalecane jest zachowanie ustawień domyślnych i modyfikowanie ich wyłącznie w szczególnych przypadkach, jeśli na przykład sprawdzanie pewnych nośników znacznie spowalnia przesyłanie danych.

Skanuj podczas

Domyślnie wszystkie pliki są skanowane podczas otwierania, tworzenia i wykonywania. Zalecane jest zachowanie ustawień domyślnych, ponieważ zapewniają one maksymalny poziom ochrony komputera w czasie rzeczywistym:

- **Otwierania pliku** — włącza lub wyłącza skanowanie plików przy ich otwieraniu.
- **Tworzenia pliku** — włącza lub wyłącza skanowanie plików przy ich tworzeniu.
- **Dostęp do nośników wymiennych** — włącza lub wyłącza automatyczne skanowanie nośników wymiennych podłączanych do komputera.

Moduł ochrony systemu plików w czasie rzeczywistym sprawdza wszystkie typy nośników. Sprawdzanie jest wywoływane wystąpieniem różnych zdarzeń systemowych, na przykład uzyskaniem dostępu do pliku. Korzystając z metod wykrywania zastosowanych w ramach technologii ThreatSense (opisanych w sekcji Parametry technologii ThreatSense), funkcja ochrony systemu plików w czasie rzeczywistym może działać inaczej w przypadku plików nowo tworzonych, a inaczej w przypadku już istniejących. Na przykład funkcję ochrony systemu plików w czasie rzeczywistym można skonfigurować tak, by umożliwić dokładniejsze monitorowanie nowo utworzonych plików.

Aby zminimalizować obciążenie systemu podczas korzystania z ochrony w czasie rzeczywistym, przeskanowane pliki nie są skanowane ponownie (dopóki nie zostaną zmodyfikowane). Pliki są niezwłocznie skanowane ponownie po każdej aktualizacji bazy silnika detekcji. Taki sposób postępowania jest kontrolowany za pomocą funkcji **Inteligentna optymalizacja**. Po jej wyłączeniu wszystkie pliki są skanowane za każdym razem, gdy uzyskiwany jest do nich dostęp. Aby zmodyfikować to ustawienie, skorzystaj z ESET PROTECT:

1. W ESET PROTECT kliknij kolejno **Polityki** > **Nowa polityka** i wpisz nazwę nowej polityki.
2. Kliknij przycisk **Ustawienia** i wybierz z menu rozwijanego pozycję**ESET Endpoint for Linux (V7+)**.
3. Kliknij **Silnik detekcji > Ochrona systemu plików w czasie rzeczywistym** > **Parametry ThreatSense**.
4. Włącz lub wyłącz opcję **Włącz inteligentną optymalizację**.
5. Kliknij **Kontynuuj** > **Przypisz**, a następnie wybierz grupę komputerów, wobec których polityka będzie miała zastosowanie.
6. Kliknij przycisk **OK**, a następnie przycisk **Zakończ**.

Parametry technologii ThreatSense

Technologia ThreatSense obejmuje wiele zaawansowanych metod wykrywania zagrożeń. Jest ona proaktywna, co oznacza, że zapewnia ochronę już od pierwszych godzin rozprzestrzeniania się nowego zagrożenia. Stosowana jest w niej kombinacja kilku metod (analiza kodu, emulacja kodu, sygnatury rodzajowe, sygnatury wirusów), które razem znacznie zwiększają bezpieczeństwo systemu. Aparat skanowania może kontrolować kilka strumieni danych jednocześnie, co zwiększa do maksimum skuteczność i wskaźnik wykrywalności. Ponadto technologia ThreatSense skutecznie eliminuje programy typu rootkit.

Za pomocą opcji ustawień parametrów technologii ThreatSense można określić kilka parametrów skanowania:

- Typy i rozszerzenia plików, które mają być skanowane;
- kombinacje różnych metod wykrywania;
- Poziomy leczenia itp.

Aby zmienić konfigurację, należy użyć programu ESET PROTECT. Po wybraniu jednego z wymienionych poniżej modułów należy kliknąć opcję **parametry technologii ThreatSense**. Różne scenariusze zabezpieczeń mogą wymagać różnych konfiguracji. Mając to na uwadze, technologię ThreatSense można konfigurować indywidualnie dla następujących modułów ochrony:

- **Ochrona systemu plików w czasie rzeczywistym**
- **Skanowania w poszukiwaniu szkodliwego oprogramowania**
- **Skanowanie zdalne**

Parametry technologii ThreatSense są w wysokim stopniu zoptymalizowane pod kątem poszczególnych modułów, a ich modyfikacja może znacząco wpływać na działanie systemu. Na przykład ustawienie opcji skanowania spakowanych programów za każdym razem lub włączenie zaawansowanej heurystyki w module ochrony systemu plików w czasie rzeczywistym może spowodować spowolnienie działania systemu (normalnie tymi metodami skanowane są tylko nowo utworzone pliki).

Skanowane obiekty

W sekcji Obiekty można określić, które pliki i składniki komputera będą skanowane w poszukiwaniu infekcji.

- **Sektory startowe/UEFI**— umożliwia skanowanie sektorów startowych w poszukiwaniu wirusów w głównym rekordzie rozruchowym
- **Pliki poczty**— program obsługuje następujące rozszerzenia: DBX (Outlook Express) oraz EML
- **Archiwa**— program obsługuje następujące rozszerzenia: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE i wiele innych
- **Archiwa samorozpakowujące**— archiwa samorozpakowujące (SFX) to archiwa, które rozpakowują się same.
- **Programy spakowane**— po uruchomieniu — w odróżnieniu od archiwów standardowych — dekompresują swoją zawartość do pamięci. Poza standardowymi statycznymi programami spakowanymi (UPX, yoda, ASPack, FSG itd.) skaner umożliwia również rozpoznawanie innych typów programów spakowanych, dzięki emulowaniu ich kodu

Ochrona systemu plików w czasie rzeczywistym nie skanuje zawartości plików w archiwach. Skanuje zawartość niektórych samorozpakowujących się archiwów po pobraniu ich na dysk twardy.

Opcje skanowania

Tu można wybrać metody stosowane podczas skanowania systemu w poszukiwaniu infekcji. Dostępne są następujące opcje:

- **Heurystyka** — heurystyka jest metodą analizy pozwalającą wykrywać działanie szkodliwych programów. Główną zaletą tej technologii jest to, że umożliwia wykrywanie szkodliwego oprogramowania, które w chwili pobierania ostatniej aktualizacji bazy danych sygnatur wirusów jeszcze nie istniało lub nie było w niej ujęte. Wadą może być ryzyko (niewielkie) wystąpienia tzw. fałszywych alarmów

- **Zaawansowana heurystyka/sygnatury DNA**— zaawansowana heurystyka jest oparta na unikatowym algorytmie heurystycznym opracowanym przez firmę ESET. Został on napisany w językach programowania wysokiego poziomu i zoptymalizowany pod kątem wykrywania robaków i koni trojańskich. Zastosowanie zaawansowanej heurystyki znacząco usprawnia wykrywanie zagrożeń w produktach ESET. Sygnatury pozwalają niezawodnie wykrywać i identyfikować wirusy. Dzięki systemowi automatycznej aktualizacji nowe sygnatury są udostępniane w ciągu kilku godzin od stwierdzenia zagrożenia. Wadą sygnatur jest to, że pozwalają wykrywać tylko znane wirusy (lub ich nieznacznie zmodyfikowane wersje)

Wyłączenia

Rozszerzenie jest częścią nazwy pliku oddzieloną kropką. Określa ono typ i zawartość pliku. Ta część ustawień parametrów technologii ThreatSense umożliwia określanie typów plików, które mają zostać wyłączone ze skanowania.

Inne

Podczas konfigurowania ustawień parametrów technologii ThreatSense dotyczących skanowania komputera na żądanie w sekcji **Inne** dostępne są również następujące opcje:

- **Skanuj alternatywne strumienie danych (ADS)** — alternatywne strumienie danych używane w systemie plików NTFS to skojarzenia plików i folderów, których nie można sprawdzić za pomocą standardowych technik skanowania. Wiele wirusów stara się uniknąć wykrycia, maskując się jako alternatywne strumienie danych

- **Uruchom skanowanie w tle z niskim priorytetem** — każde skanowanie wymaga użycia pewnej ilości zasobów systemowych. W przypadku używania programów, które wymagają dużej ilości zasobów systemowych, można uruchomić skanowanie w tle z niskim priorytetem, oszczędzając zasoby dla innych aplikacji

- **Włącz inteligentną optymalizację** — po włączeniu funkcji Inteligentna optymalizacja używane są optymalne ustawienia, które zapewniają połączenie maksymalnej skuteczności z największą szybkością skanowania. Poszczególne moduły ochrony działają w sposób inteligentny, stosując różne metody skanowania w przypadku różnych typów plików. Jeśli funkcja inteligentnej optymalizacji jest wyłączona, podczas skanowania są stosowane jedynie określone przez użytkownika dla poszczególnych modułów ustawienia technologii ThreatSense.

- **Zachowaj znacznik czasowy ostatniego dostępu**— wybranie tej opcji pozwala zachować oryginalny znacznik czasowy dostępu do plików zamiast przeprowadzania ich aktualizacji (na przykład na potrzeby

systemów wykonywania kopii zapasowych danych)

Limity

W części **Limity** można określić maksymalny rozmiar obiektów i poziomy zagnieżdżenia archiwów, które mają być skanowane.

Ustawienia obiektów

Aby zmodyfikować ustawienia obiektu, wyłącz **Domyślne ustawienia obiektów**.

- **Maksymalny rozmiar obiektu**— określa maksymalny rozmiar obiektów do skanowania. Dany moduł antywirusowy będzie skanować tylko obiekty o rozmiarze mniejszym niż określony. Ta opcja powinna być modyfikowana tylko przez zaawansowanych użytkowników, którzy mają określone powody do wyłączenia większych obiektów ze skanowania. Wartość domyślna: bez limitu

- **Maksymalny czas skanowania dla obiektu (s)** — określa maksymalny czas skanowania obiektu. W przypadku wprowadzenia wartości zdefiniowanej przez użytkownika moduł antywirusowy zatrzyma skanowanie obiektu po upływie danego czasu, niezależnie od tego, czy skanowanie zostało ukończone. Wartość domyślna: bez limitu

Ustawienia skanowania archiwów

Aby zmodyfikować ustawienia skanowania archiwów, wyłącz **Domyślne ustawienia skanowania archiwów**.

- **Poziom zagnieżdżania archiwów** — określa maksymalną głębokość skanowania archiwów. Wartość domyślna: 10

- **Maksymalny rozmiar pliku w archiwum**— ta opcja pozwala określić maksymalny rozmiar plików, które mają być skanowane w rozpakowywanych archiwach. Wartość domyślna: bez limitu

> **Wartości domyślne**
> Nie zalecamy modyfikowania wartości domyślnych. W zwykłych warunkach nie ma potrzeby ich zmieniać.

Dodatkowe parametry ThreatSense

Prawdopodobieństwo występowania infekcji w nowo utworzonych lub zmodyfikowanych plikach jest stosunkowo większe niż w przypadku istniejących już plików. Dlatego program sprawdza takie pliki z zastosowaniem dodatkowych parametrów skanowania. Zaawansowana heurystyka, która wykrywa nowe zagrożenia jeszcze przed opublikowaniem aktualizacji modułu. Poza nowo utworzonymi plikami skanowanie obejmuje też archiwa samorozpakowujące (SFX) i programy spakowane (skompresowane wewnętrznie pliki wykonywalne). Domyślnie archiwa są skanowane do dziesiątego poziomu zagnieżdżenia i są sprawdzane niezależnie od ich rozmiaru. Aby zmienić ustawienia skanowania archiwów, należy wyłączyć opcję **Domyślne ustawienia skanowania archiwów**.

Ochrona oparta na chmurze

Szybkie łącza: Ochrona oparta na chmurze, Przesyłanie próbek,, ESET Dynamic Threat Defense

ESET LiveGrid® to zaawansowany system wczesnego ostrzegania, składający się z kilku technologii opartych na

chmurze. Pomaga wykrywać pojawiające się zagrożenia na podstawie reputacji i poprawia wydajność skanowania z wykorzystaniem białej listy.

Wdrażając program ESET Endpoint Antivirus for Linux zdalnie za pomocą programu ESET PROTECT, można skonfigurować jedną z poniższych opcji dotyczących ochrony opartej na chmurze:

- Można nie włączać systemu ESET LiveGrid®. Nie spowoduje to utraty żadnych funkcji oprogramowania, jednak w niektórych przypadkach program ESET Endpoint Antivirus for Linux może reagować na nowe zagrożenia wolniej niż przy aktualizacji bazy danych silnika detekcji.
- W systemie ESET LiveGrid® można skonfigurować przesyłanie anonimowych informacji o nowych zagrożeniach i lokalizacjach nowego niebezpiecznego kodu, który został wykryty. Ten plik może być przesyłany do firmy ESET w celu szczegółowej analizy. Zbadanie zagrożeń pomoże firmie ESET ulepszać metody ich wykrywania.

Domyślnie program ESET Endpoint Antivirus for Linux jest skonfigurowany do przesyłania podejrzanych plików do analizy w laboratorium firmy ESET. Pliki z określonymi rozszerzeniami, takimi jak *doc* lub *xls*, są zawsze wyłączane z procesu przesyłania. Można również dodać inne rozszerzenia, jeśli istnieją pliki, które użytkownik lub jego firma życzy sobie wyłączyć z procesu przesyłania.

Ochrona oparta na chmurze

Włącz system reputacji ESET LiveGrid® (zalecane)

System reputacji ESET LiveGrid® poprawia wydajność rozwiązań firmy ESET do ochrony przed szkodliwym oprogramowaniem, porównując skanowane pliki z białą i czarną listą obiektów w chmurze.

Włącz system informacji zwrotnych ESET LiveGrid®

Próbka zostanie przesłana do laboratorium antywirusowego firmy ESET w celu przeprowadzenia dalszej analizy.

Wysyłaj raporty o awariach i dane diagnostyczne

Umożliwia wysyłanie danych, takich jak raporty o awariach, moduły lub zrzuty pamięci.

Pomóż ulepszyć produkt, przesyłając anonimowe statystyki użytkowania

Umożliwienie firmie ESET zbierania informacji o nowo wykrytych zagrożeniach, takich jak nazwa zagrożenia, data i godzina jego wykrycia, metoda wykrycia i skojarzone metadane, przeskanowanych plikach (skrót, nazwa pliku, pochodzenie pliku i telemetria), zablokowanych i podejrzanych adresach URL, wersji i konfiguracji produktu. Uwzględnione są także informacje o systemie użytkownika.

Kontaktowy adres e-mail (opcjonalnie)

Wraz z podejrzanymi plikami można wysyłać adres e-mail, który będzie używany do kontaktowania się z użytkownikiem, gdy przeprowadzenie analizy będzie wymagało dodatkowych informacji. Należy pamiętać, że specjaliści z firmy ESET kontaktują się z użytkownikiem tylko w szczególnych przypadkach, gdy wymagane są dodatkowe informacje.

Przesyłanie próbek

Automatyczne przesyłanie wykrytych próbek

W zależności od wybranej opcji pozwala przesyłać zainfekowane próbki do firmy ESET w celu analizy i poprawy wykrywania w przyszłości.

- Wszystkie zainfekowane próbki
- Wszystkie próbki oprócz dokumentów
- Nie przesyłaj

Automatyczne przesyłanie podejrzanych próbek

Podejrzane próbki przypominające zagrożenia i/lub pliki, których zawartość lub działanie jest nietypowe, są przesyłane do firmy ESET w celu wykonania analizy.

- Pliki wykonywalne — obejmuje pliki wykonywalne: *.exe*, *.dll*, *.sys*
- Archiwa — obejmuje typy plików archiwum: *.zip*, *.rar*, *.7z*, *.arch*, *.arj*, *.bzip2*, *.gzip*, *.ace*, *.arc*, *.cab*
- Skrypty — obejmuje typy plików skryptów: *.bat*, *.cmd*, *.hta*, *.js*, *.vbs*, *.ps1*
- Inne — obejmuje typy plików: *.jar*, *.reg*, *.msi*, *.swf*, *.lnk*
- Dokumenty — obejmuje dokumenty utworzone w programach pakietu Microsoft Office, Libre Office lub innego pakietu biurowego oraz pliki PDF z treścią aktywną.

Wyłączenia

Kliknij opcję **Edytuj** obok pozycji **Wyłączenia**, aby skonfigurować sposób przesyłania zagrożeń do laboratorium firmy ESET w celu przeprowadzenia analizy.

Maksymalny rozmiar próbek (MB)

Określanie maksymalnego rozmiaru próbek do skanowania.

ESET Dynamic Threat Defense

ESET Dynamic Threat Defense (EDTD) jest płatną usługą świadczoną przez ESET. Jej celem jest dodanie warstwy ochrony zaprojektowanej specjalnie w celu unikania najnowszych zagrożeń.

> **Dostępność**
> Usługa jest dostępna tylko wtedy, gdy produkt ESET Endpoint Antivirus for Linux w wersji 8.1 lub nowszej jest zarządzany zdalnie.
> W zależności od ustawień proaktywnej ochrony EDTD, uruchomienie pliku przesłanego do analizy może zostać zablokowane do momentu otrzymania wyniku. Takiemu zablokowaniu towarzyszy komunikat „Operacja niedozwolona” lub podobny.

Aby wyświetlić stan usługi EDTD w danej kopii EEAU, wykonaj jedno z następujących poleceń w oknie terminala jako użytkownik uprzywilejowany:

```
/opt/eset/eea/lib/cloud -e
lub

/opt/eset/eea/lib/cloud --edtd-status
```

Aby włączyć usługę w EEAU:

1. W ESET PROTECT kliknij kolejno **Polityki** > **Nowa polityka** i wpisz nazwę nowej polityki.

2. Kliknij przycisk **Ustawienia** i wybierz z menu rozwijanego pozycję**ESET Endpoint for Linux (V7+)**.

3. **Silnik detekcji** > **Ochrona oparta na chmurze**.

4. Aktywuj opcje: **Włącz system informacji zwrotnych ESET LiveGrid®**, **Włącz system informacji zwrotnych ESET LiveGrid®** i **Włącz ESET Dynamic Threat Defense**.

5. Aby zmodyfikować domyślne ustawienia EDTD, kliknij ESET Dynamic Threat Defense i dostosuj dostępne opcje. Aby uzyskać więcej informacji na temat tych ustawień EDTD, zobacz tabelę z nagłówkiem „Sekcja: ESET Dynamic Threat Defense” w dokumentacji EDTD.

6. Kliknij **Kontynuuj** > **Przypisz** i wybierz żądaną grupę komputerów, do których zasada ma mieć zastosowanie.

7. Kliknij przycisk **OK**, a następnie przycisk **Zakończ**.

Skanowania w poszukiwaniu szkodliwego oprogramowania

W tej sekcji znajdują się opcje służące do wybierania parametrów skanowania funkcji **Skanowanie na żądanie**.

Wybrany profil

Określony zestaw parametrów stosowanych przez skaner na żądanie. Można użyć jednego z wstępnie zdefiniowanych profili skanowania lub utworzyć nowy profil. Profile skanowania korzystają z różnych parametrów technologii ThreatSense.

Lista profili

Aby utworzyć nowy profil, kliknij opcję **Edytuj**. Wprowadź nazwę profilu i kliknij przycisk **Dodaj**. Nowy profil zostanie wyświetlony w menu rozwijanym **Wybrany profil** zawierającym istniejące profile skanowania.

Udostępniona lokalna pamięć podręczna

Udostępniona lokalna pamięć podręczna ESET zwiększa wydajność w środowiskach zwirtualizowanych dzięki wyeliminowaniu skanowania duplikatów w sieci. Daje to pewność, że każdy plik zostanie przeskanowany tylko raz i będzie przechowywany w udostępnionej pamięci podręcznej. By zapisywać w lokalnej pamięci podręcznej informacje dotyczące skanowania plików i folderów w sieci, należy włączyć przełącznik Opcja pamięci podręcznej. Wykonanie nowego skanu spowoduje, że program ESET Endpoint Antivirus for Linux wyszuka skanowane pliki w

pamięci podręcznej. Jeśli pliki będą zgodne, zostaną wyłączone ze skanowania.

W ustawieniach Serwer pamięci podręcznej znajdują się następujące pozycje:

- Nazwa hosta— nazwa lub adres IP komputera, na którym umiejscowiona jest pamięć podręczna.
- Port— liczba portów używanych do komunikacji (taka sama, jak w ustawieniu Udostępniona lokalna pamięć podręczna).
- Hasło— ustawienie hasła do udostępnionej lokalnej pamięci podręcznej, jeśli jest wymagane.

Aktualizacja

Domyślnie w polu **Typ aktualizacji** jest wybrane ustawienie **Regularna aktualizacja**. Zapewnia to codzienną, automatyczną aktualizację bazy danych sygnatur wykrywania i modułów produktu bezpośrednio z serwerów aktualizacji firmy ESET.

Aktualizacje w wersji wstępnej zawierają większość ostatnich poprawek błędów i/lub metody wykrywania, które wkrótce zostaną udostępnione do ogólnego użytku. Aktualizacje takie może jednak cechować niestabilność, dlatego nie zalecamy ich używania w środowisku produkcyjnym.

Umożliwia dokonywanie aktualizacji ze specjalnych serwerów aktualizacji, zapewniających dostęp do nowych wersji baz wirusów z opóźnieniem co najmniej X godzin, czyli baz przetestowanych w prawdziwym środowisku i z tego powodu uważanych za stabilne.

Jeśli aktualizacja programu ESET Endpoint Antivirus for Linux okazała się niestabilna, można wycofać aktualizację modułów, przywracając poprzedni stan. Uruchom odpowiednie polecenie w oknie terminala lub wycofaj aktualizację za pomocą programu ESET PROTECT.

Można zdefiniować do dwóch zastępczych źródeł aktualizacji — serwer główny i alternatywny.

Domyślnie tylko jedna migawka modułów jest przechowywana lokalnie. Aby przechowywać więcej migawek, zwiększ liczbę w polu **Liczba kopii przechowywanych lokalnie**.

Aktualizacja produktu

Domyślnie program ESET Endpoint Antivirus for Linux (EEAU) nie aktualizuje komponentów produktu automatycznie.

Aktywacja automatycznych aktualizacji:

1. W ESET PROTECT kliknij kolejno **Polityki** > **Nowa polityka** i wpisz nazwę nowej polityki.
2. Kliknij przycisk **Ustawienia** i wybierz z menu rozwijanego pozycję**ESET Endpoint for Linux (V7+)**.
3. Wybierz **Aktualizuj automatycznie** z pola listy **Tryb aktualizacji**.
4. Kliknij **Kontynuuj** > **Przypisz**, a następnie wybierz grupę komputerów, wobec których polityka będzie miała zastosowanie.
5. Kliknij przycisk **OK**, a następnie przycisk **Zakończ**.

Tryb aktualizacji

Aktualizuj automatycznie — nowe pakiety są pobierane i instalowane przy następnym uruchomieniu systemu. W przypadku zmian w dokumencie Umowa licencyjna użytkownika końcowego użytkownik musi zaakceptować zaktualizowaną wersję dokumentu Umowa licencyjna użytkownika końcowego przed pobraniem nowego pakietu.

Nigdy nie aktualizuj — nowe pakiety nie są pobierane, ale produkt informuje o ich dostępności w **panelu kontrolnym**.

Serwer niestandardowy, Nazwa użytkownika, Hasło

Jeśli zarządzasz kilkoma instancjami EEAU i wolisz przeprowadzać aktualizację z lokalizacji niestandardowej, zdefiniuj adres i odpowiednie poświadczenia dostępu do serwera HTTP(S), dysku lokalnego lub dysku wymiennego.

Kontrola dostępu do urządzeń

ESET Endpoint Antivirus for Linux udostępnia funkcje automatycznej kontroli korzystania z urządzeń (CD, DVD, USB/...). Przy użyciu tego modułu można blokować i dostosowywać rozszerzone filtry i uprawnienia oraz określać uprawnienia dostępu użytkowników do danego urządzenia i pracy z nim. Jest to przydatne w sytuacji, gdy administrator komputera zamierza uniemożliwić korzystanie z urządzeń z niepożądaną zawartością.

> **Możliwe uszkodzenie systemu plików**
> Stosowanie zasad z działaniem blokady/tylko do odczytu na już podłączonych urządzeniach podczas zapisywania/odczytywania danych może uszkodzić ich system plików, ponieważ są one siłą odinstalowane.

> **Zastępowanie polityki**
> Jeśli w instancji programu EEAU stosowane są różne reguły w zakresie kontroli dostępu do urządzeń, to ostatnio zastosowana polityka zastąpi poprzednie reguły polityk.

Obsługiwane urządzenia zewnętrzne:

- Urządzenia pamięci masowej podłączone przez USB
- Wewnętrzne napędy CD/DVD

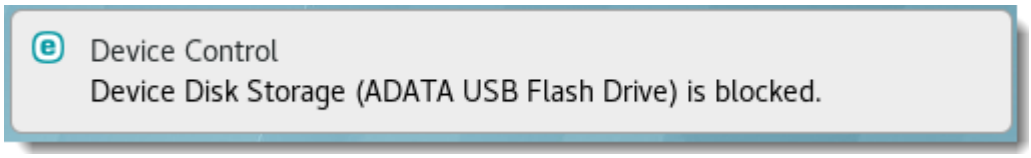
Kontrolę dostępu do urządzeń można włączyć i skonfigurować w rozwiązaniu ESET PROTECT w sekcji Zasady.

1. W ESET PROTECT kliknij kolejno **Polityki** > **Nowa polityka** i wpisz nazwę nowej polityki.
2. Kliknij przycisk **Ustawienia** i wybierz z menu rozwijanego pozycję**ESET Endpoint for Linux (V7+)**.
3. Przejdź do pozycji **Kontrola dostępu do urządzeń**.
4. Kliknij przełącznik obok pozycji **Zintegruj z systemem**.
5. Aby skonfigurować reguły i grupy, kliknij pozycję **Edytuj** obok odpowiedniego elementu.
6. Przejdź do pozycji **Przypisz**, kliknij przycisk **Przypisz** i wybierz żądaną grupę komputerów.

7. Kliknij przycisk **OK**, a następnie **Zakończ**.

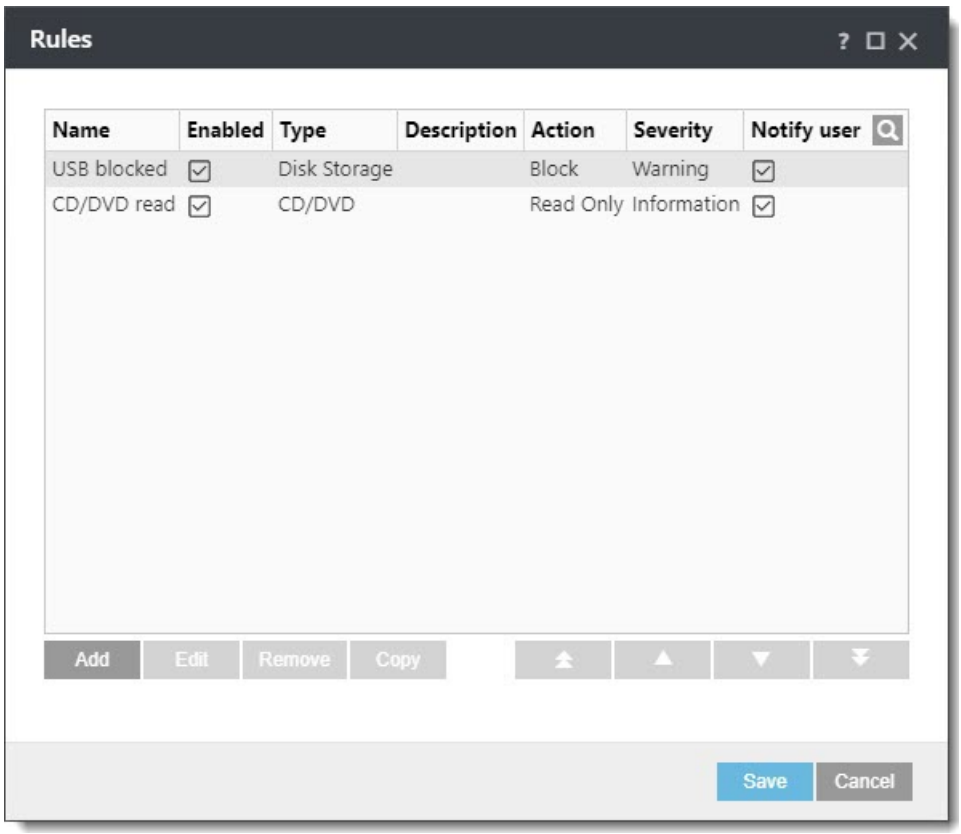
Zobacz więcej informacji na temat zarządzania produktami zabezpieczającymi punkty końcowe ESET PROTECT.

W przypadku podłączenia/wstawienia urządzenia blokowanego przez istniejącą regułę zostanie wyświetlone okno powiadomienia i dostęp do urządzenia nie będzie możliwy.



Edytor reguł kontroli dostępu do urządzeń

W oknie **Edytor reguł kontroli dostępu do urządzeń** w ESET PROTECT wyświetlane są istniejące reguły. Umożliwia ono również dokładną kontrolę obsługiwanych urządzeń zewnętrznych podłączanych przez użytkowników do komputera.



Można dopuszczać lub blokować określone urządzenia w oparciu o parametry określane w konfiguracji reguł. Lista reguł zawiera pewne informacje o regułach, takie jak nazwa, typ urządzenia zewnętrznego oraz czynność wykonywana po jego podłączeniu do komputera.

Kliknięcie przycisku **Dodaj** lub **Edytuj** umożliwia zarządzanie regułą. Odznaczenie pola wyboru **Włączona** obok reguły powoduje jej wyłączenie do momentu jej ponownego użycia w przyszłości. Można zaznaczyć jedną lub większą liczbę reguł i kliknąć opcję **Usuń**, aby trwale usunąć reguły.

Kliknij przycisk **Kopiuj**, aby utworzyć kopię zaznaczonej reguły.

Reguły są wyświetlane według priorytetów, przy czym reguły o wyższych priorytetach znajdują się wyżej na liście.

Przenoś reguły pojedynczo lub grupami, klikając opcje Na początek/W górę/W dół/Na koniec.

W dzienniku kontroli dostępu do urządzeń rejestrowane są wszystkie zdarzenia, w przypadku których uruchamiana jest funkcja kontroli dostępu do urządzeń.

Atrybuty podłączonych urządzeń

Aby wyświetlić listę atrybutów urządzeń podłączonych do komputera, na którym zainstalowany jest produkt ESET Endpoint Antivirus for Linux, użyj narzędzia `lsdev` z okna terminala lub uruchom je z poziomu ESET PROTECT.

Składnia: `/opt/eset/eea/bin/lsdev [OPTIONS]`

Opcje — forma skrócona	Opcje — forma długa	Opis
`-l`	`--list`	Wyświetlanie listy podłączonych urządzeń
`-c`	`--csv`	Wyświetlanie listy podłączonych urządzeń w formacie csv
`-h`	`--help`	Pokaż pomoc i zakończ.
`-v`	`--version`	Pokaż informacje o wersji i zakończ.

Grupy urządzeń

Okno Grupy urządzeń jest podzielone na dwie części. W prawej części okna znajduje się lista urządzeń należących do danej grupy, a w części lewej znajdują się utworzone grupy. Grupę, która ma zostać wyświetlona w prawym okienku należy wybrać z listy urządzeń.

Po otwarciu okna **Grupy urządzeń** i wybraniu grupy można dodawać lub usuwać urządzenia z listy. Innym sposobem dodawania urządzeń do grup jest zaimportowanie ich z pliku.

Elementy sterujące

Dodaj — dodaj grupę, wprowadzając jej nazwę, lub dodaj urządzenie do istniejącej grupy (opcjonalnie można wprowadzić szczegóły, takie jak nazwa dostawcy, model oraz numer seryjny).

Edytuj — zmień nazwę wybranej grupy lub parametry urządzenia (dostawcę, model, numer seryjny).

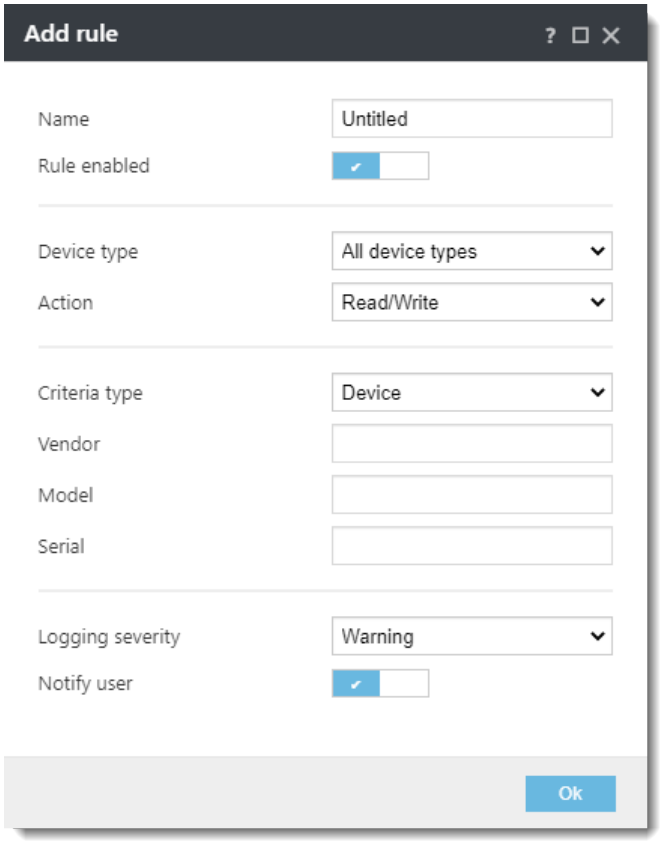
Usuń — usuń wybraną grupę lub urządzenie.

Import — importuj listę urządzeń z pliku.

Po zakończeniu dostosowywania należy kliknąć przycisk **OK**. Opuszczenie okna **Grupy urządzeń** bez zapisywania zmian umożliwia przycisk **Anuluj**.

Dodawanie reguł kontroli dostępu do urządzeń

Reguła kontroli dostępu do urządzeń definiuje czynność, która zostanie podjęta w chwili, gdy urządzenie spełniające kryteria reguły zostanie podłączone do komputera.



W celu łatwiejszego rozpoznawania reguł należy wprowadzać ich krótkie opisy w polu **Nazwa**. Kliknięcie przełącznika obok pozycji **Reguła włączona** pozwala wyłączać i włączać regułę. Jest to przydatne, gdy użytkownik nie chce trwale usuwać danej reguły.

Typ urządzenia

Wybierz typ urządzenia zewnętrznego z menu rozwijanego:

- **Pamięć masowa** — dotyczy każdej pamięci dyskowej podłączonej przez USB, w tym zewnętrznych napędów CD/DVD i konwencjonalnych czytników kart pamięci
- **CD/DVD** – dotyczy wewnętrznego napędu CD/DVD podłączonego przez IDE lub SATA
- **Wszystkie urządzenia** – obejmuje wszystkie powyższe typy

Informacje o typie urządzenia są zbierane z systemu operacyjnego. Użyj narzędzia lsdev, aby wyświetlić listę podłączonych urządzeń i ich atrybuty.

Ponieważ te urządzenia udostępniają wyłącznie informacje dotyczące realizowanych przez nie czynności, nie dostarczając informacji dotyczących użytkowników, można je tylko zablokować globalnie.

Czynność

Można zezwalać na dostęp do urządzeń innych niż urządzenia pamięci masowej lub go blokować. Reguły dotyczące urządzeń pamięci masowej umożliwiają natomiast wybranie jednego z poniższych ustawień:

- **Odczyt/zapis**— pełny dostęp do urządzenia
- **Blokuj**— dostęp do urządzenia jest zablokowany

- **Tylko do odczytu**— dostęp do urządzenia wyłącznie w trybie do odczytu

W polu **Typ kryteriów** należy wybrać pozycję **Urządzenie** lub **Grupa urządzeń**.

Poniżej przedstawiono dodatkowe parametry, które można wykorzystać do uszczegółowienia reguł i dopasowania ich do urządzeń. W parametrach nie jest rozróżniana wielkość liter:

- **Dostawca** — filtrowanie według nazwy lub identyfikatora dostawcy.
- **Model** — podana nazwa urządzenia.
- **Numer seryjny**— urządzenia zewnętrzne mają zwykle numery seryjne. W przypadku dysków CD i DVD jest to numer seryjny danego nośnika, a nie napędu.

> **Niezdefiniowane parametry**
> Jeśli te parametry nie zostaną zdefiniowane, te pola zostaną pominięte przez regułę podczas dopasowywania. W odniesieniu do parametrów filtrowania we wszystkich polach testowych rozróżniana jest wielkość liter i nie są obsługiwane symbole wieloznaczne (*, ?).

> **Dzienniki kontroli dostępu do urządzeń**
> W celu wyświetlenia informacji na temat urządzenia należy utworzyć regułę dla urządzeń tego typu, podłączyć urządzenie do komputera, a następnie zapoznać się ze szczegółami urządzenia, używając narzędzia wiersza polecenia lslog z parametrem `-l` lub `--device-control`.

Stopień szczegółowości zapisywania w dzienniku

- **Informacje** — rejestrowanie komunikatów informacyjnych, w tym powiadomień o pomyślnych aktualizacjach, oraz wszystkich rekordów wyższych kategorii.
- **Ostrzeżenie** — rejestrowanie błędów krytycznych oraz komunikatów ostrzegawczych i wysyłanie ich na serwer ESET PROTECT.

Narzędzia

W sekcji **Narzędzia** w konfiguracji programu ESET Endpoint Antivirus for Linux przez ESET PROTECT można modyfikować konfigurację ogólną programu ESET Endpoint Antivirus for Linux.

- Definiowanie informacji o serwerze proxy służących do nawiązywania połączeń z Internetem
- Konfigurowanie sposobu obsługi plików dziennika

Serwer proxy

Można skonfigurować program ESET Endpoint Antivirus for Linux w celu korzystania z serwera proxy do nawiązywania połączeń z Internetem lub ze zdefiniowanymi serwerami aktualizacji (kopii dystrybucyjnych). Aby dostosować parametry, kliknij kolejno opcje **Ustawienia > Narzędzia > Serwer proxy**.

Pliki dziennika

Można modyfikować konfigurację funkcji zapisywania w dzienniku programu ESET Endpoint Antivirus for Linux.

Minimalna szczegółowość zapisów w dzienniku

Szczegółowość zapisów w dzienniku definiuje poziom szczegółów danych w plikach dziennika dotyczących programu ESET Endpoint Antivirus for Linux.

- **Ostrzeżenia krytyczne** — tylko błędy krytyczne (np. niepowodzenie uruchomienia ochrony antywirusowej).
- **Błędy** — rejestrowanie błędów takich jak „Błąd podczas pobierania pliku” i **ostrzeżeń krytycznych**.
- **Ostrzeżenia** — rejestrowanie błędów krytycznych i komunikatów ostrzeżeń oraz **błędów**.
- **Rekordy informacyjne** — rejestrowanie komunikatów informacyjnych, w tym powiadomień o pomyślnych aktualizacjach, oraz wszystkich rekordów powyższych kategorii.
- **Rekordy diagnostyczne** — dołączanie informacji potrzebnych do ulepszenia konfiguracji programu oraz wszystkich rekordów powyższych kategorii.

Automatycznie usuwaj rekordy starsze niż (dni)

Aby ukryć wpisy dziennika starsze niż określona liczba dni na ekranie Zdarzenia lub liście dzienników (`lslog`):

1. W ESET PROTECT kliknij kolejno **Polityki** > **Nowa polityka** i wpisz nazwę nowej polityki.
2. Kliknij przycisk **Ustawienia** i wybierz z menu rozwijanego pozycję**ESET Endpoint for Linux (V7+)**.
3. Kliknij **Narzędzia** > **Pliki dziennika**.
4. Włącz **Automatycznie usuwaj rekordy starsze niż (dni)**.
5. Określ liczbę dni, po których pliki będą ukrywane.
6. Kliknij **Kontynuuj** > **Przypisz**, a następnie wybierz grupę komputerów, wobec których polityka będzie miała zastosowanie.
7. Kliknij przycisk **OK**, a następnie przycisk **Zakończ**.

Ukrytych dzienników nie można wyświetlić ponownie. Wpisy dzienników funkcji Skanowanie na żądanie są usuwane natychmiast. Aby zapobiec gromadzeniu się ukrytych dzienników, włącz opcję automatycznej optymalizacji plików dzienników.

Automatycznie optymalizuj pliki dzienników

Włączenie tej opcji powoduje automatyczną defragmentację plików dziennika po przekroczeniu stopnia fragmentacji określonego w polu **Jeśli liczba nieużywanych rekordów przekracza (%)**. Nieużywane rekordy odzwierciedlają ukryte dzienniki. Kliknij przycisk **Optymalizuj**, aby rozpocząć defragmentację plików dziennika. Wszystkie puste wpisy dzienników są usuwane w celu zwiększenia wydajności i szybkości przetwarzania dzienników. Poprawę można zaobserwować zwłaszcza w przypadku dzienników zawierających dużą liczbę

wpisów.

Funkcja programu syslog

Funkcja programu syslog to parametr polecenia syslog powiązany z zapisywaniem w dzienniku, który służy do grupowania podobnych wiadomości w dzienniku. Na przykład dzienniki demonów (gromadzone za pośrednictwem funkcji programu syslog daemon) można zapisywać w pliku */var/log/daemon.log*, używając odpowiedniej konfiguracji. Ze względu na niedawne zaadaptowanie polecenia systemd i jego dziennika ważność funkcji programu syslog obniżyła się, jednak nadal można korzystać z nich w celu filtrowania dzienników.

Interfejs użytkownika

W tej sekcji konfiguracji produktu ESET Endpoint Antivirus for Linux za pośrednictwem ESET PROTECT można włączyć/wyłączyć powiadomienia na pulpicie oraz wybrać, dla jakich czynności i stanów aplikacji będą wysyłane powiadomienia.

Powiadomienia na pulpicie

Można włączyć lub wyłączyć powiadomienia na pulpicie, używając przełącznika obok pozycji **Wyświetlaj powiadomienia na pulpicie**. Powiadomienia te są domyślnie włączone i informują o zdarzeniach, które nie wymagają interwencji użytkownika.

Włącz powiadomienia dla wybranych czynności:

1. Kliknij pozycję **Edytuj** obok **Powiadomienia aplikacji**.
2. Zaznacz/usuń zaznaczenie wybranych czynności.
3. Kliknij przycisk **OK**.

Stan ochrony

Skonfiguruj, które stany aplikacji będą zgłaszane do ESET Endpoint Antivirus for Linux.

1. Kliknij pozycję **Edytuj** obok pozycji Stan aplikacji.
2. Aby włączyć powiadomienia dla wybranych stanów aplikacji, w obszarze **Pokaż w punkcie końcowym** zaznacz interesujące cię stany.
3. Kliknij przycisk **OK**.

Stan aplikacji

Każdy stan wybrany w **Stan aplikacji** > **Edytuj** > **Pokaż w punkcie końcowym** wyświetli powiadomienie na ekranie początkowym programu ESET Endpoint Antivirus for Linux i w menu ☰ > **Stan ochrony**.

Zdalne zarządzanie

Aby zdalnie zarządzać programem ESET Endpoint Antivirus for Linux, połącz komputer hosta produktu zabezpieczającego ESET z konsolą ESET PROTECT.

1. Wdróż agenta ESET Management Agent.

2. Dodaj komputer do konsoli ESET PROTECT.

Od teraz można uruchamiać odpowiednie zadania klienta powiązane z programem ESET Endpoint Antivirus for Linux.

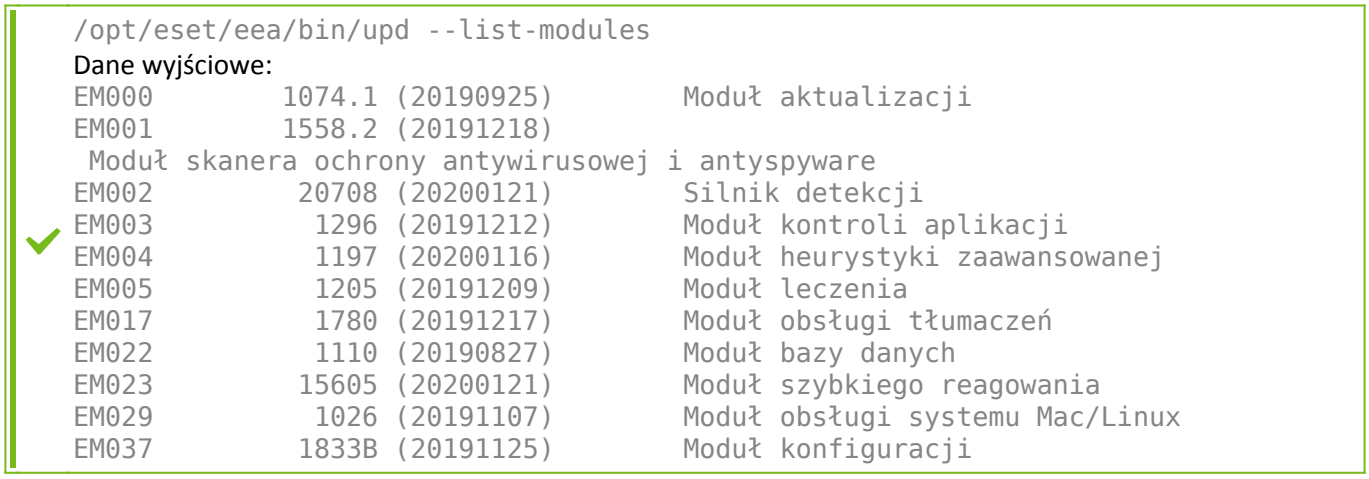
Przykłady praktycznego zastosowania

W tym rozdziale opisano typowe zastosowania programu ESET Endpoint Antivirus for Linux.

Pobieranie informacji o modułach

Aby zobaczyć listę wszystkich modułów programu ESET Endpoint Antivirus for Linux wraz z ich wersjami, uruchom następujące polecenie w oknie terminalu:

```
/opt/eset/eea/bin/upd --list-modules
```



Planowanie skanowania

W systemach opartych na systemie Unix można korzystać z narzędzia cron w celu planowania skanowania na żądanie w niestandardowym okresie.

Aby skonfigurować zaplanowane zadanie, należy edytować tabelę narzędzia cron (crontab) za pośrednictwem okna terminalu.

Jeśli tabela narzędzia cron jest edytowana po raz pierwszy, zostanie wyświetlony monit o wybranie edytora przez naciśnięcie odpowiedniego klawisza z cyfrą. Należy wybrać edytor znany użytkownikowi — poniższe instrukcje odwołują się do poleceń zapisywania zmian w edytorze Nano.

Zaplanuj dogłębne, pełne skanowanie dysku w każdą niedzielę o 2:00

1. Aby edytować tabelę narzędzia cron, wykonaj następujące polecenie z okna terminalu jako użytkownik uprzywilejowany z dostępem do folderów podlegających skanowaniu:

```
sudo crontab -e
```

2. Użyj klawiszy strzałek, aby przejść do odpowiedniego wiersza tabeli crontab, i wpisz następujące polecenie:

```
0 2 * * 0 /opt/eset/eea/bin/odscan --scan --profile="@In-depth scan" / &>/dev/null
```

3. Aby zapisać zmiany, naciśnij klawisze CTRL + X, wpisz literę Y i naciśnij klawisz **Enter**.

Zaplanowanie skanowania inteligentnego określonego folderu co wieczór o 23:00

W tym przykładzie zostanie zaplanowane skanowanie folderu */var/www/download/* co wieczór.

1. Aby edytować tabelę narzędzia cron, wykonaj następujące polecenie z okna terminalu jako użytkownik uprzywilejowany z dostępem do folderów podlegających skanowaniu:

```
sudo crontab -e
```

2. Użyj klawiszy strzałek, aby przejść do odpowiedniego wiersza w tabeli crontab, i wpisz następujące polecenie:

```
0 23 * * 0 /opt/eset/eea/bin/odscan --scan --
profile="@Smart scan" /var/www/download/ &>/dev/null
```

3. Aby zapisać zmiany, naciśnij klawisze CTRL + X, wpisz literę Y i naciśnij klawisz **Enter**.

Struktura plików i folderów

Ten temat zawiera szczegółowe informacje dotyczące struktury plików i folderów programu ESET Endpoint Antivirus for Linux przydatne w przypadku, kiedy personel działu pomocy technicznej firmy ESET wymaga dostępu do plików w celu rozwiązywania problemów. Lista demonów i narzędzi wiersza polecenia jest dostępna w dalszej części rozdziału.

Katalog bazowy

Katalog, w którym znajdują się moduły programu ESET Endpoint Antivirus for Linux możliwe do ładowania zawierające bazę danych sygnatur wirusów.

```
/var/opt/eset/eea/lib
```

Katalog pamięci podręcznej

Katalog, w którym znajdują się pliki pamięci podręcznej i pliki tymczasowe (takie jak pliki kwarantanny lub raporty) programu ESET Endpoint Antivirus for Linux.

`/var/opt/eset/eea/cache`

Katalog plików binarnych

Katalog, w którym znajdują się powiązane pliki binarne programu ESET Endpoint Antivirus for Linux.

`/opt/eset/eea/bin`

W tej lokalizacji znajdują się następujące narzędzia:

- odscan — służy do uruchamiania skanowania na żądanie za pośrednictwem okna terminalu
- quar — służy do zarządzania elementami poddanymi kwarantannie
- upd — służy do zarządzania aktualizacjami modułów i zmieniania ustawień aktualizacji

Katalog systemowych plików binarnych

Katalog, w którym znajdują się powiązane systemowe pliki binarne programu ESET Endpoint Antivirus for Linux.

`/opt/eset/eea/sbin`

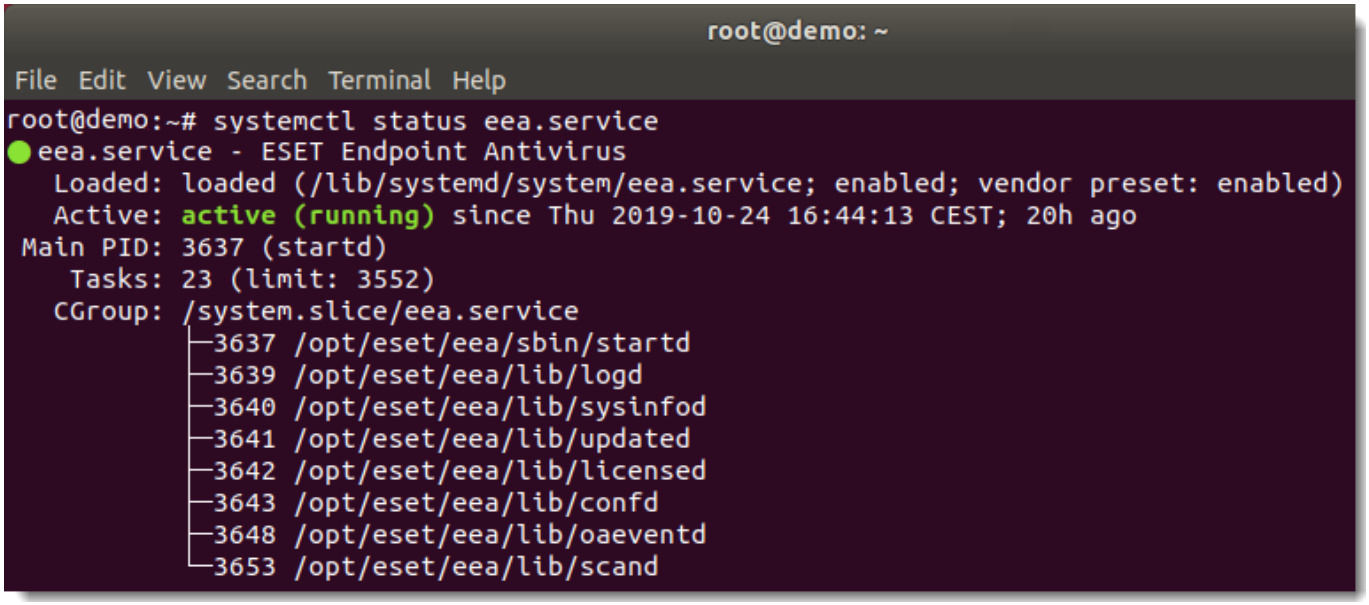
W tej lokalizacji znajdują się następujące narzędzia:

- collect_logs.sh — służy do generowania wszystkich niezbędnych dzienników jako pliku archiwum w folderze głównym zalogowanego użytkownika
- ecp_logging.sh — służy do generowania dzienników związanych z aktywacjami produktów
- lic — służy do aktywacji programu ESET Endpoint Antivirus for Linux przy użyciu zakupionego klucza licencyjnego lub do sprawdzenia stanu aktywacji i ważności licencji
- lslog — służy do wyświetlania dzienników zebranych przez program ESET Endpoint Antivirus for Linux
- startd — służy do ręcznego uruchamiania demona programu ESET Endpoint Antivirus for Linux, jeśli został on zatrzymany.

Aby sprawdzić, czy usługa programu ESET Endpoint Antivirus for Linux jest aktywna, uruchom następujące polecenie z okna terminalu z uprawnieniami użytkownika root:

```
systemctl status eea.service
```

Przykładowe dane wyjściowe po użyciu polecenia `systemctl`:



Demony

- sbin/startd — demon główny umożliwiający uruchamianie innych demonów i zarządzanie nimi
- lib/scand — demon skanowania
- lib/oaeventd — usługa przechwytywania zdarzeń przy dostępie (za pomocą modułu jądra eset_rtp)
- lib/confd — usługa zarządzania konfiguracją
- lib/logd — usługa zarządzania dziennikami
- lib/licensed — usługa aktywacji i licencjonowania
- lib/updated — usługa aktualizacji modułów
- lib/execd + lib/odfeeder — pomocnicy skanowania na żądanie
- lib/utild – usługa pomocnicza
- lib/sysinfod — usługa wykrywania systemu operacyjnego i nośników

Narzędzia wiersza polecenia

- sbin/lslog — Narzędzie do wyświetlania listy dzienników
- bin/odscan — skaner na żądanie
- lib/cfg — Narzędzie do konfigurowania
- sbin/lic — narzędzie do licencjonowania
- bin/upd — narzędzie do aktualizacji modułów

- bin/quar — narzędzie do zarządzania kwarantanną
- lib/cloud – umożliwia przesłanie próbki do ESET LiveGrid® lub ESET Dynamic Threat Defense za pośrednictwem wiersza poleceń (wymaga EEAU w wersji 8.1 lub nowszej)

Rozwiązywanie problemów

W tej sekcji opisano sposoby rozwiązywania poniższych problemów.

- Problemy z aktywacją (tylko w języku angielskim)
- Korzystanie z flagi noexec
- Nie można uruchomić demona ochrony w czasie rzeczywistym
- Zbieranie dzienników

Zbieranie dzienników

Jeśli dział pomocy technicznej firmy ESET poprosi o dzienniki z programu ESET Endpoint Antivirus for Linux, należy użyć skryptu *collect_logs.sh* dostępnego w lokalizacji */opt/eset/eea/sbin/*, aby je wygenerować.

Uruchom skrypt z okna terminalu z uprawnieniami użytkownika root. Na przykład w systemie Ubuntu uruchom następujące polecenie:

```
sudo /opt/eset/eea/sbin/collect_logs.sh
```

Skrypt generuje wszystkie niezbędne dzienniki jako plik archiwum w folderze głównym zalogowanego użytkownika, a następnie wyświetla do niego ścieżkę. Gromadzone są w nim również wszystkie dostępne dzienniki aktywacji. Wyślij ten plik do działu pomocy technicznej firmy ESET pocztą e-mail.

Dzienniki aktywacji

Dział pomocy technicznej firmy ESET może prosić o udostępnienie odpowiednich dzienników, aby ułatwić rozwiązywanie problemów z aktywacją produktu.

1. Włącz usługę dziennika aktywacji, uruchamiając jako użytkownik z odpowiednimi uprawnieniami polecenie:

```
sudo /opt/eset/eea/sbin/ecp_logging.sh -e
```

lub

```
sudo /opt/eset/eea/sbin/ecp_logging.sh -e -f
```

, aby bez żadnego monitu ponownie uruchomić produkt, jeśli jest to konieczne.

2. Przejdź ponownie przez proces aktywacji. Jeśli to nie rozwiąże problemu, uruchom skrypt zbierania

dzienników jako użytkownik z odpowiednimi uprawnieniami:

```
sudo /opt/eset/eea/sbin/collect_logs.sh
```

3. Wyślij zebrane dzienniki do działu pomocy technicznej firmy ESET.

4. Wyłącz dzienniki aktywacji, uruchamiając jako użytkownik z odpowiednimi uprawnieniami polecenie:

```
sudo /opt/eset/eea/sbin/ecp_logging.sh -d
```

lub

```
sudo /opt/eset/eea/sbin/ecp_logging.sh -d -f
```

, aby bez żadnego monitu ponownie uruchomić produkt, jeśli jest to konieczne.

Korzystanie z flagi noexec

Jeśli zamontowano ścieżki `/var` i `/tmp` z flagą `noexec`, instalacja programu ESET Endpoint Antivirus for Linux zakończy się niepowodzeniem z następującym komunikatem o błędzie:

```
Invalid value of environment variable MODMAPDIR. Modules cannot be loaded.
```

Obejście

Poniższe polecenia należy wykonać w oknie terminalu.

1. Utwórz folder z włączoną flagą `exec` oraz z poniższym właścicielem i zestawem uprawnień:

```
/usr/lib/eea drwxrwxr-x. root eset-eea-daemons
```

2. Wykonaj następujące polecenie:

```
# mkdir /usr/lib/eea
# chgrp eset-eea-daemons /usr/lib/eea
# chmod g+w /usr/lib/eea/
```

a.Jeśli włączono moduł SELinux, ustaw kontekst następującego folderu:

```
# semanage fcontext -a -t tmp_t /usr/lib/eea
# restorecon -v /usr/lib/eea
```

3. Skompiluj wymagane moduły:

```
# MODMAPDIR=/usr/lib/eea /opt/eset/eea/bin/upd --compile-nups
```

4. Ustaw parametr `MODMAPDIR` w pliku `/usr/lib/systemd/system/eea.service`, dodając wiersz do bloku `[Service]`:

```
Environment=MODMAPDIR=/usr/lib/eea
```

5. Załaduj ponownie konfigurację usługi systemd:

```
# systemctl daemon-reload
```

6. Uruchom ponownie usługę eea:

```
# systemctl restart eea
```

Nie można uruchomić ochrony w czasie rzeczywistym

Poniżej znajduje się przykładowy problem i jego rozwiązanie w systemie Ubuntu.

Problem

Nie można uruchomić ochrony w czasie rzeczywistym ze względu na brakujące pliki jądra.

W lokalizacji */var/log/messages* jest wyświetlany komunikat o błędzie dotyczący programu ESET Endpoint Antivirus for Linux:

Paź 15 15:42:30 localhost eea: ESET Endpoint Antivirus błąd: nie można znaleźć katalogu źródeł jądra dla wersji jądra 3.10.0-957.el7.x86_64

Paź 15 15:42:30 localhost eea: ESET Endpoint Antivirus błąd: sprawdź, czy wersja pakietu kernel-drive (lub linux-headers) jest zgodna z aktualną wersją jądra

Paź 15 15:42:30 localhost oaeventd[31471]: ESET Endpoint Antivirus Błąd: Nie można otworzyć pliku /lib/modules/3.10.0-957.el7.x86_64/eset/eea/eset_rtp.ko: Brak takiego pliku lub katalogu

Rozwiązanie

Metoda 1 — wymaga ponownego uruchomienia systemu operacyjnego

1. Uaktualnij pakiety systemu operacyjnego do najnowszej wersji. W systemie Ubuntu uruchom następujące polecenie z okna terminalu jako użytkownik uprzywilejowany:

```
apt-get update
```

```
apt-get upgrade
```

2. Uruchom ponownie system operacyjny.

Metoda 2

1. Zainstaluj moduły kernel-header (w przypadku dystrybucji systemu Linux opartej na pakietach DEB). W systemie Ubuntu uruchom następujące polecenia w oknie terminalu jako użytkownik uprzywilejowany:

```
apt update
apt install linux-headers-$(uname -r)
```

2. Uruchom ponownie usługę EEA:

```
systemctl restart eea
```

Słowniczek

- **Demon**: Rodzaj programu dla systemu operacyjnego z rodziny Unix, który działa dyskretnie w tle. Jest aktywowany na wskutek wystąpienia określonego zdarzenia lub spełnienia warunku.

Umowa licencyjna użytkownika końcowego

WAŻNE: Przed pobraniem, zainstalowaniem, skopiowaniem lub użyciem Oprogramowania należy się dokładnie zapoznać z poniższymi warunkami korzystania z produktu. **POBRANIE, ZAINSTALOWANIE, SKOPIOWANIE LUB UŻYCIE OPROGRAMOWANIA OZNACZA WYRAŻENIE ZGODY NA NINIEJSZE WARUNKI I AKCEPTACJĘ DOKUMENTU POLITYKA PRYWATNOŚCI.**

Umowę Licencyjną Użytkownika Końcowego

Niniejsza Umowa licencyjna użytkownika końcowego (w dalszej części nazywana „Umową”), zawierana między spółką ESET, spol. s r. o., z siedzibą w Słowacji pod adresem Einsteinova 24, 851 01 Bratislava, Slovak Republic, zarejestrowaną w Rejestrze Handlowym Sądu Rejonowego dla okręgu Bratislava I, w sekcji Sro pod numerem 3586/B, numer w rejestrze przedsiębiorców: 31333532 (w dalszej części nazywaną „firmą ESET” lub „Dostawcą”), a licencjobiorcą, który jest osobą fizyczną lub prawną (w dalszej części nazywanym „Licencjobiorcą” lub „Użytkownikiem końcowym”), uprawnia Licencjobiorcę do korzystania z Oprogramowania określonego w punkcie 1 niniejszej Umowy. Oprogramowanie określone w punkcie 1 niniejszej Umowy może znajdować się na nośniku danych albo zostać przesłane pocztą elektroniczną, pobrane z Internetu, pobrane z serwerów Dostawcy lub uzyskane z innych źródeł na warunkach wyszczególnionych poniżej.

NINIEJSZA UMOWA DOTYCZY WYŁĄCZNIE OKREŚLENIA PRAW UŻYTKOWNIKA KOŃCOWEGO I NIE STANOWI UMOWY SPRZEDAŻY. Dostawca pozostaje właścicielem kopii Oprogramowania i nośnika fizycznego zawartego w opakowaniu z produktem, a także wszystkich innych kopii Oprogramowania, które Użytkownik końcowy może wykonać zgodnie z niniejszą Umową.

Kliknięcie opcji „Akceptuję” lub „Akceptuję...” w trakcie instalowania, pobierania, kopiowania lub używania

Oprogramowania oznacza, że Licencjobiorca wyraża zgodę na warunki określone w niniejszej Umowie. Jeśli Licencjobiorca nie wyraża zgody na którykolwiek warunek określony w niniejszej Umowie, powinien niezwłocznie kliknąć opcję anulowania i przerwać instalację lub pobieranie albo zniszczyć Oprogramowanie, nośnik instalacyjny, dokumentację towarzyszącą Oprogramowaniu i dowód sprzedaży Oprogramowania bądź zwrócić je Dostawcy lub w miejscu zakupu Oprogramowania.

LICENCJOBIORCA PRZYJMUJE DO WIADOMOŚCI, ŻE KORZYSTANIE Z OPROGRAMOWANIA OZNACZA ZAPOZNANIE SIĘ Z NINIEJSZĄ UMOWĄ, ZROZUMIENIE WARUNKÓW W NIEJ OKREŚLONYCH ORAZ ZOBOWIĄZANIE DO ICH PRZESTRZEGANIA.

1. **Oprogramowanie.** W niniejszej Umowie termin „Oprogramowanie" oznacza: (i) program komputerowy, do którego dołączono niniejszą Umowę, i wszystkie jego składniki; (ii) całą zawartość dysków, płyt CD-ROM i płyt DVD, wiadomości e-mail wraz z ich załącznikami oraz innych nośników, do których jest dołączona niniejsza Umowa, w tym Oprogramowanie w formie kodu obiektowego dostarczone na nośniku danych albo za pośrednictwem poczty elektronicznej lub Internetu; (iii) wszelkie powiązane drukowane materiały instruktażowe oraz wszelką inną dokumentację powiązaną z Oprogramowaniem, w tym przede wszystkim wszelkie opisy Oprogramowania, jego dane techniczne, wszelkie opisy jego właściwości lub działania, wszelkie opisy środowiska operacyjnego, w którym Oprogramowanie jest używane, instrukcje obsługi lub instalacji Oprogramowania oraz wszelkie opisy sposobu korzystania z Oprogramowania (w dalszej części nazywane „Dokumentacją"); (iv) wszelkie ewentualne kopie Oprogramowania, poprawki możliwych błędów Oprogramowania, dodatki do Oprogramowania, rozszerzenia Oprogramowania, zmodyfikowane wersje Oprogramowania oraz aktualizacje składników Oprogramowania, na które Dostawca udziela Licencjobiorcy licencji zgodnie z zapisami w punkcie 3 niniejszej Umowy. Oprogramowanie będzie dostarczane wyłącznie w postaci wykonywalnego kodu obiektowego.

2. **Instalacja, komputer i klucz licencyjny**. Oprogramowanie dostarczone na nośniku danych, otrzymane za pośrednictwem poczty elektronicznej, pobrane z Internetu, pobrane z serwerów Dostawcy lub uzyskane z innych źródeł musi zostać zainstalowane. Oprogramowanie należy zainstalować na prawidłowo skonfigurowanym komputerze, który spełnia minimalne wymagania określone w Dokumentacji. Procedurę instalacji również opisano w Dokumentacji. Na komputerze, na którym zostanie zainstalowane Oprogramowanie, nie można instalować sprzętu komputerowego ani programów komputerowych, które mogłyby niekorzystnie wpłynąć na Oprogramowanie. Komputer oznacza sprzęt, w tym między innymi komputery osobiste, laptopy, stacje robocze, palmtopy, smartfony, przenośne urządzenia elektroniczne lub inne urządzenia elektroniczne, dla których przeznaczone jest Oprogramowanie, na których zostanie zainstalowane i/lub będzie używane. Klucz licencyjny oznacza niepowtarzalny ciąg symboli, liter, cyfr i znaków specjalnych, dostarczony Użytkownikowi końcowemu w celu umożliwienia mu legalnego korzystania z Oprogramowania, jego określonych wersji lub rozszerzenia warunków Licencji zgodnie z niniejszą Umową.

3 **Licencja**. Dostawca udziela Licencjobiorcy praw określonych poniżej (w dalszej części nazywanych zbiorczo „Licencją"), jeśli Licencjobiorca zobowiązał się przestrzegać i przestrzega wszelkich warunków określonych w niniejszej Umowie:

a) **Instalacja i użycie.** Licencjobiorcy przysługują niewyłączne, nieprzenoszalne prawa do zainstalowania Oprogramowania na dysku twardym komputera lub na innym nośniku do trwałego przechowywania danych, do zainstalowania i przechowywania Oprogramowania w pamięci systemu komputerowego oraz do zaimplementowania, przechowywania i wyświetlania Oprogramowania.

b) **Postanowienia w sprawie liczby Licencji.** Prawo do korzystania z Oprogramowania w ramach jednej Licencji jest ograniczone do jednego Użytkownika końcowego. Jeden Użytkownik końcowy oznacza: (i) instalację Oprogramowania na jednym systemie komputerowym lub, jeśli liczba Licencji zależy od liczby skrzynek pocztowych, (ii) użytkownika komputera, który odbiera pocztę elektroniczną za pośrednictwem klienta poczty elektronicznej. Jeśli do klienta poczty elektronicznej dociera poczta elektroniczna, która jest następnie automatycznie dystrybuowana do innych użytkowników, liczbę Użytkowników końcowych stanowi liczba

wszystkich użytkowników, do których jest dostarczana poczta. Jeśli serwer poczty pełni funkcję bramy pocztowej, liczba Użytkowników końcowych jest równa liczbie użytkowników serwera poczty, którzy są obsługiwani przez tę bramę. Jeśli jeden użytkownik odbiera pocztę przesyłaną na różne adresy e-mail (np. za pośrednictwem usługi aliasów), a liczba tych adresów jest nieokreślona i wiadomości nie są automatycznie dystrybuowane przez klienta poczty elektronicznej do większej liczby użytkowników, wymagana jest Licencja na jednego użytkownika komputera. Z jednej Licencji można korzystać każdorazowo tylko na jednym komputerze. Użytkownik końcowy może wprowadzić klucz licencyjny do Oprogramowania tylko w zakresie, w jakim przysługuje mu prawo do korzystania z Oprogramowania zgodnie z ograniczeniami wynikającymi z liczby Licencji przyznanych przez Dostawcę. Klucz licencyjny ma charakter poufny, Licencjobiorca nie może udostępniać Licencji stronom trzecim ani pozwalać im na używanie klucza licencyjnego, o ile nie dopuszcza tego niniejsza Umowa lub Dostawca. W przypadku naruszenia klucza licencyjnego należy bezzwłocznie powiadomić Dostawcę.

c) **Wersja Business Edition.** W przypadku zamiaru zainstalowania i użycia Oprogramowania na serwerze poczty, w systemie przekazywania wiadomości e-mail lub w połączeniu z bramą pocztową bądź internetową wymagane jest nabycie wersji Business Edition Oprogramowania.

d) **Okres obowiązywania Licencji.** Prawo do korzystania z Oprogramowania jest ograniczone w czasie.

e) **Oprogramowanie dostarczone przez producenta urządzenia (OEM).** Prawo do korzystania z Oprogramowania, które zostało dostarczone przez producenta zakupionego urządzenia (OEM, Original Equipment Manufacturer), jest ograniczone do tego urządzenia. Prawa tego nie można przenosić na inne urządzenia.

f) **Oprogramowanie w wersji próbnej lub nieprzeznaczonej do obrotu handlowego.** Nie można pobierać opłat za korzystanie z Oprogramowania, które jest oznaczone napisem „Not for resale" lub „NFR" (Nie do sprzedaży) albo „TRIAL" (Wersja próbna). Oprogramowanie takie jest przeznaczone wyłącznie do prezentacji lub testowania jego funkcji.

g) **Wygaśnięcie Licencji.** Licencja wygasa automatycznie po upływie okresu jej obowiązywania. Jeśli Licencjobiorca naruszył którekolwiek z postanowień niniejszej Umowy, Dostawca jest uprawniony do rozwiązania niniejszej Umowy oraz do wykonania wszelkich innych praw i zastosowania wszelkich innych środków prawnych przysługujących mu w takiej sytuacji. W razie anulowania Licencji Licencjobiorca musi natychmiast usunąć lub zniszczyć Oprogramowanie i wszystkie jego kopie zapasowe lub zwrócić je na własny koszt do firmy ESET bądź w miejscu zakupu Oprogramowania. Po wygaśnięciu Licencji Dostawca jest też uprawniony do anulowania prawa Użytkownika końcowego do używania funkcji Oprogramowania, które wymagają połączenia z serwerami Dostawcy lub serwerami innych firm.

4. **Wymagania dotyczące funkcji gromadzących dane i połączenia z Internetem.** Aby Oprogramowanie działało poprawnie, wymagane jest stałe połączenie z Internetem oraz regularne połączenia z serwerami Dostawcy lub z serwerami innych firm, a gromadzenie potrzebnych danych powinno odbywać się zgodnie z obowiązującą Polityką prywatności. Połączenie z Internetem oraz gromadzenie potrzebnych danych są wymagane w przypadku następujących funkcji Oprogramowania:

a) **Aktualizacje Oprogramowania.** Dostawca jest uprawniony do wprowadzania w Oprogramowaniu zmian w formie aktualizacji (w dalszej części nazywanych „Aktualizacjami"), przy czym nie jest on ograniczony żadnymi terminami wprowadzenia takich zmian ani nie jest zobowiązany do ich wprowadzenia. Funkcja Aktualizacji jest domyślnie włączona w ustawieniach standardowych Oprogramowania, dlatego Aktualizacje są instalowane automatycznie, o ile Użytkownik końcowy nie zmienił ustawienia automatycznego instalowania Aktualizacji. W celu przeprowadzania aktualizacji wymagana jest weryfikacja autentyczności Licencji, w tym informacji dotyczących komputera i/lub platformy, na której zostało zainstalowane Oprogramowanie zgodnie z Polityką prywatności.

b) **Przekazywanie szkodliwego oprogramowania i informacji o komputerze do Dostawcy**. Oprogramowanie

obejmuje funkcje, które gromadzą przykłady nowych wirusów komputerowych, innych szkodliwych programów komputerowych oraz podejrzanych, problematycznych, potencjalnie niepożądanych lub niebezpiecznych obiektów, takich jak pliki, adresy URL, pakiety IP oraz ramki Ethernet (odtąd ogólnie „Szkodliwe oprogramowanie"), po czym wysyłają je do Dostawcy. Wysyłane dane obejmują m.in. informacje o procesie instalacji, komputerze lub platformie, na której zainstalowano Oprogramowanie, w tym informacje o działaniu i funkcjonalności Oprogramowania (odtąd ogólnie „Informacje"). Informacje oraz Szkodliwe oprogramowanie mogą obejmować dane Użytkownika końcowego (w tym jego dane osobowe pobrane losowo lub przypadkowo) lub dane innych użytkowników komputera, na którym zainstalowano Oprogramowanie, a także pliki uszkodzone przez Szkodliwe oprogramowanie wraz z powiązanymi z nimi metadanymi.

Informacje oraz Szkodliwe oprogramowanie mogą być gromadzone przy użyciu następujących funkcji Oprogramowania:

i. Funkcja systemu reputacji LiveGrid służy do gromadzenia i wysyłania do Dostawcy jednokierunkowych skrótów związanych ze Szkodliwym oprogramowaniem. Funkcję tę można włączyć w ustawieniach standardowych Oprogramowania.

ii. System informacji zwrotnych LiveGrid służy do gromadzenia i wysyłania do Dostawcy Szkodliwego oprogramowania wraz z powiązanymi metadanymi, a także Informacji. Funkcję tę może włączyć Użytkownik końcowy podczas procesu instalacji Oprogramowania.

Dostawca może wykorzystać otrzymane Informacje oraz Szkodliwe oprogramowanie tylko w celu analizy Szkodliwego oprogramowania, usprawnienia Oprogramowania i zweryfikowania autentyczności Licencji i jest zobowiązany do podjęcia stosownych środków gwarantujących zachowanie poufności Szkodliwego oprogramowania i Informacji. Włączenie tej funkcji Oprogramowania oznacza, że Dostawca może gromadzić i przetwarzać Szkodliwe oprogramowanie i Informacje zgodnie z Polityką prywatności i obowiązującymi przepisami prawa. Użytkownik może wyłączyć te funkcje w każdej chwili.

Na potrzeby niniejszej Umowy konieczne jest gromadzenie, przetwarzanie i przechowywanie danych umożliwiających Dostawcy identyfikację Licencjobiorcy zgodnie z Polityką prywatności. Licencjobiorca niniejszym zgadza się, aby Dostawca, korzystając z własnych środków, mógł sprawdzić, czy Licencjobiorca używa Oprogramowania zgodnie z postanowieniami niniejszej Umowy. Licencjobiorca zgadza się, że na potrzeby niniejszej Umowy konieczne jest przekazywanie jego danych podczas komunikacji pomiędzy Oprogramowaniem a systemami komputerowymi Dostawcy lub jego partnerów handlowych w ramach sieci dystrybucyjnej i wsparcia Dostawcy w celu zapewnienia funkcjonalności Oprogramowania i upoważnienia do używania Oprogramowania oraz ochrony praw Dostawcy.

Po zawarciu niniejszej Umowy Dostawca i każdy z jego partnerów handlowych, w ramach sieci dystrybucyjnej i wsparcia Dostawcy, będzie uprawniony do przekazywania, przetwarzania i przechowywania istotnych danych identyfikujących Licencjobiorcę w celach związanych z rozliczaniem opłat, wykonywaniem niniejszej Umowy i przekazywaniem powiadomień na komputerze Licencjobiorcy. Licencjobiorca niniejszym wyraża zgodę na otrzymywanie powiadomień i wiadomości, w tym między innymi informacji marketingowych.

Szczegółowe informacje na temat ochrony prywatności, danych osobowych i praw Licencjobiorcy jako podmiotu danych dostępne są w Polityce prywatności w witrynie Dostawcy, bezpośrednio podczas procesu instalacji. Można do niej przejść także z poziomu sekcji pomocy w Oprogramowaniu.

5. Okno **Wykonywanie praw Użytkownika końcowego**. Licencjobiorca może wykonywać swoje prawa wyłącznie osobiście lub za pośrednictwem swoich pracowników. Licencjobiorca może korzystać z Oprogramowania wyłącznie w celu zapewnienia ciągłości swojej działalności gospodarczej i w celu zabezpieczenia komputerów lub systemów komputerowych, na które uzyskał Licencję.

6. **Ograniczenie praw.** Licencjobiorca nie może kopiować, rozpowszechniać ani wyodrębniać składników

Oprogramowania, jak również nie może tworzyć produktów na podstawie Oprogramowania (nie może wykonywać dzieł pochodnych). Korzystając z Oprogramowania, Licencjobiorca musi przestrzegać następujących ograniczeń:

a) Licencjobiorca może wykonać jedną kopię Oprogramowania na nośniku przeznaczonym do trwałego przechowywania danych i przechowywać tę kopię w charakterze archiwalnej kopii zapasowej, tj. nie może zainstalować ani użyć takiej kopii na żadnym komputerze. Wszelkie inne kopie Oprogramowania wykonane przez Licencjobiorcę stanowią naruszenie warunków określonych w niniejszej Umowie.

b) Licencjobiorca nie może używać, modyfikować, tłumaczyć ani odtwarzać Oprogramowania ani jego kopii w sposób inny niż wyszczególniony w niniejszej Umowie.

c) Licencjobiorca nie może sprzedawać Oprogramowania, udzielać na nie podlicencji, oddawać go w użytkowanie, wypożyczać go innym osobom ani pożyczać go od innych osób, a także nie może używać Oprogramowania w celu świadczenia usług o charakterze dochodowym.

d) Licencjobiorca nie może podejmować prób odtworzenia kodu źródłowego Oprogramowania na drodze dekompilacji lub dezasemblacji ani w żaden inny sposób, chyba że pozwalają mu na to przepisy, które w stosownym zakresie wyraźnie znoszą niniejsze postanowienie.

e) Licencjobiorca zobowiązuje się używać Oprogramowania w sposób zgodny z wszelkimi przepisami, które mają zastosowanie do Oprogramowania ze względu na właściwość terytorialną Licencjobiorcy, w tym między innymi ze stosownymi ograniczeniami dotyczącymi prawa autorskiego i innych praw własności intelektualnej.

f) Licencjobiorca zgadza się korzystać z Oprogramowania i jego funkcji w sposób, który nie ograniczy dostępu do tych usług innym Użytkownikom końcowym. Dostawca zastrzega sobie prawo do ograniczenia zakresu usług udostępnianych konkretnym Użytkownikom końcowym w celu zapewnienia możliwości korzystania z nich jak największej liczbie Użytkowników końcowych. Ograniczenie zakresu usług może również oznaczać całkowitą blokadę funkcji Oprogramowania oraz usunięcie Danych i informacji przechowywanych na serwerach Dostawcy lub zewnętrznego podmiotu związanych z wybranymi funkcjami Oprogramowania.

g) Licencjobiorca zobowiązuje się nie podejmować działań obejmujących korzystanie z klucza licencyjnego, niezgodnych z postanowieniami niniejszej Umowy lub prowadzących do przekazania klucza licencyjnego osobie nieuprawnionej do korzystania z Oprogramowania, takich jak przekazanie wykorzystanego lub niewykorzystanego klucza licencyjnego w dowolnej formie, a także nieautoryzowana reprodukcja lub dystrybucja zduplikowanych lub wygenerowanych kluczy licencyjnych albo korzystanie z Oprogramowania w wyniku wykorzystania klucza licencyjnego uzyskanego z innego źródła niż Dostawca.

7. **Prawo autorskie**. Oprogramowanie i wszystkie prawa z nim związane, w tym między innymi prawa własności i prawa własności intelektualnej do Oprogramowania, należą do firmy ESET i/lub jej licencjodawców. Prawa te gwarantują zapisy traktatów międzynarodowych oraz wszelkie właściwe przepisy ustawowe obowiązujące w kraju, w którym jest używane Oprogramowanie. Struktura Oprogramowania, sposób jego zorganizowania i kod w nim zawarty są cennymi tajemnicami handlowymi oraz informacjami poufnymi firmy ESET i/lub jej licencjodawców. Licencjobiorca nie może kopiować Oprogramowania poza okolicznościami opisanymi w punkcie 6(a). Wszelkie kopie utworzone przez Licencjobiorcę zgodnie z niniejszą Umową muszą zawierać te same informacje o prawie autorskim i innych prawach własności, które znajdują się w Oprogramowaniu. Licencjobiorca niniejszym przyjmuje do wiadomości, że w razie naruszenia postanowień niniejszej Umowy przez podjęcie próby odtworzenia kodu źródłowego Oprogramowania na drodze dekompilacji lub dezasemblacji albo w inny sposób prawa do wszelkich informacji uzyskanych przez Licencjobiorcę w wyniku podjęcia takiej próby zostaną uznane za automatycznie i nieodwołalnie przeniesione w całości na Dostawcę już w momencie powstania takich informacji i to niezależnie od praw przysługujących Dostawcy w związku z naruszeniem przez Licencjobiorcę warunków określonych w niniejszej Umowie.

8. **Zastrzeżenie praw**. Dostawca niniejszym zastrzega sobie wszelkie prawa do Oprogramowania, z wyjątkiem praw wyraźnie udzielonych Licencjobiorcy, występującemu w charakterze Użytkownika końcowego, na podstawie niniejszej Umowy.

9. **Różne wersje językowe, Oprogramowanie obsługujące wiele urządzeń i wiele kopii Oprogramowania**. Jeśli Oprogramowanie może obsługiwać wiele platform lub języków bądź jeśli Licencjobiorca uzyskał wiele kopii Oprogramowania, Oprogramowania można używać tylko na tych systemach komputerowych i w tych wersjach, na które Licencjobiorca uzyskał Licencje. Licencjobiorca nie może sprzedawać wersji ani kopii Oprogramowania, których nie używa, jak również nie może ich oddawać w użytkowanie, udzielać na nie podlicencji, wypożyczać ich ani przenosić do nich praw na inne osoby.

10. **Rozpoczęcie i zakończenie obowiązywania Umowy**. Niniejsza Umowa wchodzi w życie z datą wyrażenia przez Licencjobiorcę zgody na warunki określone w tej Umowie. Licencjobiorca może rozwiązać niniejszą Umowę w dowolnej chwili przez trwałe odinstalowanie i zniszczenie Oprogramowania, wszystkich jego kopii zapasowych i wszelkich powiązanych materiałów dostarczonych przez Dostawcę lub jego partnerów handlowych bądź przez zwrócenie tych produktów na własny koszt. Bez względu na powód rozwiązania niniejszej Umowy po zakończeniu jej obowiązywania nadal obowiązują postanowienia zawarte w punktach 7, 8, 11, 13, 19 i 21.

11. **OŚWIADCZENIA UŻYTKOWNIKA KOŃCOWEGO**. LICENCJOBIORCA (WYSTĘPUJĄCY W CHARAKTERZE UŻYTKOWNIKA KOŃCOWEGO) PRZYJMUJE OPROGRAMOWANIE W STANIE TAKIM, W JAKIM ZOSTAŁO MU ONO DOSTARCZONE, BEZ JAKICHKOLWIEK WYRAŹNYCH LUB DOROZUMIANYCH GWARANCJI, O ILE PRAWO WŁAŚCIWE TEGO NIE ZABRANIA. ANI WŁAŚCICIELE STOSOWNYCH PRAW AUTORSKICH NIE UDZIELAJĄ ŻADNYCH WYRAŹNYCH ANI DOROZUMIANYCH GWARANCJI, W TYM MIĘDZY INNYMI GWARANCJI PRZYDATNOŚCI HANDLOWEJ LUB PRZYDATNOŚCI DO OKREŚLONEGO CELU, JAK RÓWNIEŻ NIE GWARANTUJĄ, ŻE OPROGRAMOWANIE NIE BĘDZIE NARUSZAĆ PRAW PATENTOWYCH, PRAW AUTORSKICH, PRAW DO ZNAKÓW TOWAROWYCH ANI INNYCH PRAW OSÓB TRZECICH. ANI DOSTAWCA, ANI ŻADNA INNA OSOBA NIE GWARANTUJE, ŻE FUNKCJE OPROGRAMOWANIA SPEŁNIAJĄ WYMAGANIA LICENCJOBIORCY LUB ŻE DZIAŁANIE OPROGRAMOWANIA BĘDZIE NIEZAKŁÓCONE I POZBAWIONE BŁĘDÓW. LICENCJOBIORCA BIERZE NA SIEBIE WSZELKĄ ODPOWIEDZIALNOŚĆ I RYZYKO ZA DOBÓR OPROGRAMOWANIA ODPOWIEDNIEGO DO OSIĄGNIĘCIA CELÓW LICENCJOBIORCY ORAZ ZA PRZEPROWADZENIE INSTALACJI OPROGRAMOWANIA, ZA JEGO UŻYCIE I ZA WYNIKI TEGO UŻYCIA.

12. **Brak innych zobowiązań**. W niniejszej Umowie określono wszystkie zobowiązania Dostawcy i jego licencjodawców.

13. **OGRANICZENIE ODPOWIEDZIALNOŚCI**. O ILE PRAWO WŁAŚCIWE TEGO NIE ZABRANIA, ANI DOSTAWCA, ANI JEGO PRACOWNICY CZY LICENCJODAWCY NIE PONOSZĄ ŻADNEJ ODPOWIEDZIALNOŚCI ZA JAKIEKOLWIEK UTRATY ZYSKÓW, PRZYCHODÓW, ŹRÓDEŁ PRZYCHODÓW LUB DANYCH, SZKODY MAJĄTKOWE LUB OBRAŻENIA CIAŁA, ZAKŁÓCENIA DZIAŁALNOŚCI PRZEDSIĘBIORSTWA, UTRATY DANYCH HANDLOWYCH CZY JAKIEKOLWIEK SZKODY SZCZEGÓLNE, BEZPOŚREDNIE, POŚREDNIE, UBOCZNE, GOSPODARCZE, MORALNE LUB WYNIKOWE, JAK RÓWNIEŻ NIE BĘDĄ PONOSIĆ KOSZTÓW NABYCIA ZASTĘPCZYCH TOWARÓW LUB USŁUG ANI POKRYWAĆ RÓŻNIC MIĘDZY CENAMI KONTRAKTOWYMI A CENAMI TRANSAKCJI. ZASTRZEŻENIE OKREŚLONE W POWYŻSZYM ZDANIU MA ZASTOSOWANIE BEZ WZGLĘDU NA PRZYCZYNĘ POWSTANIA SZKODY I NA TO, CZY EWENTUALNE ROSZCZENIE ZOSTAŁO ZGŁOSZONE NA PODSTAWIE UMOWY, PRZEPISÓW O CZYNACH NIEDOZWOLONYCH, PRZEPISÓW DOTYCZĄCYCH ZANIEDBAŃ CZY NA JAKIEJKOLWIEK INNEJ PODSTAWIE ORAZ CZY ZOSTAŁO ONO ZGŁOSZONE W ZWIĄZKU Z UŻYCIEM, CZY Z NIEMOŻNOŚCIĄ UŻYCIA OPROGRAMOWANIA. ZASTRZEŻENIE TO MA ZASTOSOWANIE TAKŻE WÓWCZAS, GDY DOSTAWCA LUB JEGO LICENCJODAWCY BĄDŹ PODMIOTY STOWARZYSZONE ZOSTALI POWIADOMIENI O MOŻLIWOŚCI WYSTĄPIENIA DANEJ SZKODY. W PRZYPADKU JURYSDYKCJI, KTÓRE NIE ZEZWALAJĄ NA WYŁĄCZENIE ODPOWIEDZIALNOŚCI ODSZKODOWAWCZEJ, LECZ DOPUSZCZAJĄ JEJ OGRANICZENIE, ODPOWIEDZIALNOŚĆ DOSTAWCY, JEGO PRACOWNIKÓW, LICENCJODAWCÓW LUB PODMIOTÓW STOWARZYSZONYCH JEST OGRANICZONA DO KWOTY ZAPŁACONEJ PRZEZ LICENCJOBIORCĘ ZA LICENCJE.

14. Jeśli którekolwiek postanowienie niniejszej Umowy jest sprzeczne z ustawowymi prawami konsumenckimi jakiejkolwiek osoby, postanowienie to nie może być interpretowane w sposób naruszający te prawa.

15. **Pomoc techniczna**. Usługi pomocy technicznej świadczą wedle własnego uznania i bez udzielania jakichkolwiek gwarancji firma ESET lub inne firmy, którym firma ESET zleca świadczenie takich usług. Przed skorzystaniem z usługi pomocy technicznej Użytkownik końcowy musi utworzyć kopię zapasową wszystkich istniejących danych, programów i aplikacji. Ani firma ESET, ani inne firmy, którym firma ESET zleca świadczenie usług pomocy technicznej, nie mogą wziąć na siebie odpowiedzialności za uszkodzenie lub utratę danych, własności, oprogramowania lub urządzeń, jak również nie mogą odpowiadać za utratę zysków spowodowaną świadczeniem usług pomocy technicznej. Firma ESET i/lub inne firmy, którym firma ESET zleca świadczenie usług pomocy technicznej, zastrzegają sobie prawo do odmowy wykonania usługi, jeśli uznają, że nie mieści się ona w zakresie oferowanych usług pomocy technicznej. Firma ESET zastrzega sobie prawo do odmowy, wstrzymania lub zaprzestania świadczenia usług pomocy technicznej, jeśli uzna to za stosowne. Informacje dotyczące licencji, Informacje i inne dane zgodne z Polityką prywatności mogą być wymagane na potrzeby świadczenia pomocy technicznej.

16. **Przeniesienie Licencji**. Jeśli odpowiednie postanowienia niniejszej Umowy tego nie zabraniają, Oprogramowanie można przenosić między poszczególnymi systemami komputerowymi. O ile nie jest to sprzeczne z warunkami określonymi w niniejszej Umowie, za zgodą Dostawcy Użytkownik końcowy może trwale przenieść Licencję i wszelkie prawa przysługujące mu na podstawie niniejszej Umowy na innego Użytkownika końcowego, pod warunkiem że (i) nie zachowa dla siebie żadnych kopii Oprogramowania; (ii) przeniesienie praw będzie bezpośrednie, tj. prawa zostaną przeniesione bezpośrednio na nowego Użytkownika końcowego; (iii) nowy Użytkownik końcowy przejmie na siebie wszystkie prawa i obowiązki wynikające z niniejszej Umowy, które miały dotąd zastosowanie do Użytkownika końcowego przenoszącego Licencję; (iv) nowy Użytkownik końcowy otrzyma od Użytkownika końcowego przenoszącego Licencję dokumentację, która umożliwi mu stwierdzenie zgodnie z zapisami w punkcie 17, czy Oprogramowanie jest oryginalne.

17. **Weryfikowanie oryginalności Oprogramowania**. Użytkownik końcowy może wykazać swoje uprawnienia do korzystania z Oprogramowania w jeden z poniższych sposobów: (i) na podstawie certyfikatu licencyjnego wystawionego przez Dostawcę lub inną firmę wskazaną przez Dostawcę; (ii) na podstawie pisemnej umowy licencyjnej, jeśli została ona zawarta; (iii) na podstawie wiadomości e-mail od Dostawcy z danymi dotyczącymi licencji (nazwą użytkownika i hasłem). Informacje dotyczące licencji oraz dane identyfikujące Użytkownika końcowego zgodne z Polityką prywatności mogą być wymagane w celu weryfikacji oryginalności Oprogramowania.

18. **Udzielanie Licencji organom władzy publicznej i rządowi USA**. Organy władzy publicznej, w tym rząd Stanów Zjednoczonych Ameryki Północnej, otrzymują Licencje na Oprogramowanie zgodnie z postanowieniami niniejszej Umowy, tj. z uwzględnieniem wszystkich praw i obowiązków określonych w niniejszej Umowie.

19. **Zgodność z przepisami o kontroli handlu**.

a) Licencjobiorca nie będzie, bezpośrednio ani pośrednio, eksportować, reeksportować, przekazywać lub w inny sposób udostępniać Oprogramowania jakiejkolwiek osobie, nie będzie używać go w jakikolwiek sposób, ani też nie będzie uczestniczyć w jakichkolwiek działaniach, które mogłyby spowodować, że firma ESET lub jej spółki holdingowe, spółki zależne oraz spółki zależne dowolnych z jej spółek holdingowych, jak również podmioty kontrolowane przez jej spółki holdingowe (zwane dalej „Podmiotami stowarzyszonymi”), naruszyłyby przepisy o kontroli handlu, obejmujące:

i. wszelkie przepisy prawne, które kontrolują, ograniczają lub nakładają wymogi licencyjne na eksport, reeksport lub transfer towarów, oprogramowania, technologii lub usług, wydane lub przyjęte przez jakikolwiek rząd, stan lub organ regulacyjny Stanów Zjednoczonych, Singapuru, Wielkiej Brytanii, Unii Europejskiej lub dowolnego z jej państw członkowskich, albo jakikolwiek kraj, w którym mają być wykonywane zobowiązania wynikające z Umowy

lub w którym firma ESET lub dowolny z jej Podmiotów stowarzyszonych są zarejestrowane lub prowadzą działalność (zwane dalej „Przepisami o kontroli eksportu”);

ii. wszelkie gospodarcze, finansowe (handlowe lub inne) sankcje, ograniczenia, embarga, zakazy importu lub eksportu, zakazy przekazywania funduszy lub aktywów bądź świadczenia usług, lub też równoważne środki nałożone przez jakikolwiek rząd, stan lub organ regulacyjny Stanów Zjednoczonych, Singapuru, Wielkiej Brytanii, Unii Europejskiej lub dowolnego z jej państw członkowskich, albo jakikolwiek kraj, w którym mają być wykonywane zobowiązania wynikające z Umowy lub w którym firma ESET lub dowolny z jej Podmiotów stowarzyszonych są zarejestrowane lub prowadzą działalność (zwane dalej „Przepisami o sankcjach”).

b) Firma ESET ma prawo zawiesić swoje zobowiązania wynikające z niniejszych warunków lub wypowiedzieć je ze skutkiem natychmiastowym w następujących przypadkach:

i. Gdy firma ESET stwierdzi na podstawie stosownego uzasadnienia, że Użytkownik naruszył lub może naruszyć postanowienia punktu 19.a Umowy.

ii. Gdy Użytkownik końcowy i/lub Oprogramowanie podlegają przepisom o kontroli handlu i w związku z tym firma ESET stwierdzi na podstawie stosownego uzasadnienia, że dalsze wykonywanie zobowiązań wynikających z Umowy mogłoby spowodować, że firma ESET lub jej Podmioty stowarzyszone naruszyłyby przepisy o kontroli handlu lub byłyby narażone na negatywne konsekwencje wynikające z tych przepisów.

c) Żadne z postanowień Umowy nie ma na celu ani nie powinno być interpretowane lub odczytywane jako nakłanianie bądź wymaganie od którejkolwiek ze stron działania lub powstrzymania się od działania (albo wyrażenia zgody na działanie lub powstrzymanie się od działania) w sposób niezgodny z obowiązującymi przepisami o kontroli handlu, zabroniony przez te przepisy lub podlegający karze w związku z tymi przepisami.

20. **Zawiadomienia**. Wszystkie zawiadomienia oraz zwroty Oprogramowania i Dokumentacji należy kierować na adres: ESET, spol. s r. o., Einsteinova 24, 851 01 Bratislava, Slovak Republic.

21. **Prawo właściwe**. Niniejsza Umowa podlega przepisom prawnym obowiązującym w Słowacji i powinna być interpretowana zgodnie z tymi przepisami. Użytkownik końcowy i Dostawca niniejszym stwierdzają, że do niniejszej Umowy nie mają zastosowania przepisy dotyczące konfliktu praw ani Konwencja Organizacji Narodów Zjednoczonych o umowach międzynarodowej sprzedaży towarów. Licencjobiorca wyraźnie stwierdza, że wszelkie spory lub roszczenia względem Dostawcy wynikające z zawarcia niniejszej Umowy, jak również wszelkie spory lub roszczenia związane z użyciem Oprogramowania będą rozstrzygane przez Sąd Rejonowy dla okręgu Bratislava I. Licencjobiorca wyraźnie poddaje się jurysdykcji tego sądu.

22. **Postanowienia ogólne**. Uznanie któregokolwiek z postanowień niniejszej Umowy za nieważne lub niewykonalne nie wpływa na ważność innych postanowień niniejszej Umowy, które pozostają wówczas w mocy zgodnie z warunkami określonymi w niniejszej Umowie. W przypadku rozbieżności pomiędzy wersjami językowymi niniejszej Umowy pierwszeństwo ma wersja angielska. Zmiana niniejszej Umowy musi mieć formę pisemną i musi zostać zatwierdzona podpisem złożonym przez upoważnionego przedstawiciela Dostawcy lub przez osobę wyraźnie upoważnioną do reprezentowania Dostawcy na zasadzie pełnomocnictwa.

Niniejsza Umowa stanowi całość porozumienia między Dostawcą a Licencjobiorcą w sprawie Oprogramowania i zastępuje wszelkie wcześniejsze oświadczenia, negocjacje, zobowiązania, wymiany zdań lub reklamy związane z Oprogramowaniem.

EULA ID: BUS-STANDARD-20-01

Zasady ochrony prywatności

Firma ESET, spol. s r. o. z siedzibą pod adresem Einsteinova 24, 85101 Bratislava, Slovak Republic, wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Bratysławy I w sekcji Sro, pozycja nr 3586/B, numer w rejestrze gospodarczym: 31333532 jako administrator danych (dalej "ESET" lub "my") pragnie zachować przejrzystość w odniesieniu do danych osobowych oraz poufności informacji swoich klientów. W związku z tym publikujemy niniejsze Zasady ochrony prywatności wyłącznie w celu przekazania klientowi (dalej "Użytkownik" lub "Ty") informacji na następujące tematy: W związku z tym publikujemy niniejsze Zasady ochrony prywatności wyłącznie w celu przekazania klientowi (dalej „Użytkownik końcowy” lub „Ty”) informacji na następujące tematy:

- przetwarzanie danych osobowych,
- poufność danych,
- prawa osób, których dane dotyczą.

Przetwarzanie danych osobowych

Usługi zaimplementowane w produkcie firmy ESET są przez nas świadczone zgodnie z postanowieniami Umowy licencyjnej użytkownika końcowego („Umowa EULA”), ale niektóre z nich mogą wymagać szczególnej uwagi. Chcemy przekazać szczegółowe informacje na temat gromadzenia danych związanych ze świadczonymi przez nas usługami. Oferujemy szereg usług przedstawionych w umowie EULA i dokumentacji produktu, takich jak aktualizacja/uaktualnianie, ESET LiveGrid®, ochrona przed niewłaściwym użyciem danych, pomoc techniczna itp. Abyśmy mogli dostarczać nasze usługi, musimy gromadzić następujące informacje:

- Statystyki (dotyczące aktualizacji i inne) obejmujące informacje na temat procesu instalacji oraz komputera użytkownika końcowego (np. platformy, na której jest zainstalowany nasz produkt), a także informacje o działaniu i funkcjach naszych produktów, takie jak system operacyjny, dane dotyczące sprzętu, identyfikatory instalacji, identyfikatory licencji, adres IP, adres MAC oraz ustawienia konfiguracji produktu.
- Skróty jednokierunkowe związane z infekcjami używane przez system reputacji ESET LiveGrid®, które poprawiają wydajność naszych rozwiązań do ochrony przed szkodliwym oprogramowaniem, porównując skanowane pliki z białą i czarną listą obiektów w chmurze.
- Próbki podejrzanego kodu i metadanych używane przez system reputacji ESET LiveGrid®, które pozwalają produktom ESET reagować natychmiast na potrzeby użytkowników końcowych i zapewnić ochronę przed najnowszymi zagrożeniami. Korzystamy następujących danych otrzymanych od użytkowników końcowych
  - dane dotyczące infekcji, takie jak próbki potencjalnych wirusów i innych szkodliwych programów, a także podejrzane, potencjalnie niepożądane i potencjalnie niebezpieczne obiekty (np. pliki wykonywalne i wiadomości e-mail zgłoszone jako spam lub oznaczone przez nasz produkt);
  - informacje o urządzeniach w sieci lokalnej, takie jak typ, producent, model i/lub nazwa urządzenia;
  - informacje dotyczące korzystania z Internetu, takie jak adres IP, informacje geograficzne, pakiety IP, adresy URL i ramki sieci Ethernet;
  - pliki zrzutu awaryjnego i informacje w nich zawarte.

Nie mamy zamiaru gromadzić danych spoza tego zakresu, jednak czasami nie da się tego uniknąć. Przypadkowo zebrane dane mogą być zawarte w samym szkodliwym oprogramowaniu (i zebrane bez wiedzy i zgody użytkownika końcowego) lub mogą stanowić część nazwy pliku lub adresu URL. Nie zamierzamy wykorzystywać tych danych w naszych systemach ani przetwarzać ich w celu określonym w tej Polityce prywatności.

• Informacje dotyczące licencji, takie jak identyfikator licencji oraz dane osobowe, takie jak imię, nazwisko, adres oraz adres e-mail, są wymagane do celów związanych z rozliczeniami, weryfikacją autentyczności licencji oraz świadczeniem przez nas usług.

• Aby zapewnić możliwość świadczenia pomocy technicznej lub pomocy innego rodzaju mogą być wymagane informacje kontaktowe i dane zawarte w zgłoszeniach do działu pomocy. W zależności od wybranego przez Użytkownika końcowego sposobu komunikacji możemy gromadzić następujące dane: adres e-mail, numer telefonu, informacje o licencji, szczegółowe informacje o produkcie oraz opis zgłoszenia do pomocy technicznej. Możemy poprosić o podanie innych informacji, aby ułatwić świadczenie usługi pomocy technicznej.

Poufność danych

ESET jest firmą działającą na całym świecie za pośrednictwem swoich spółek stowarzyszonych oraz partnerów będących częścią sieci dystrybucji, usług i pomocy technicznej. Przetwarzane przez nas informacje mogą być przesyłane między nami a naszymi partnerami oraz spółkami stowarzyszonymi z tytułu realizacji Umowy EULA, na przykład świadczenia usług lub udzielania pomocy technicznej albo w celach rozliczeniowych. W zależności od lokalizacji Użytkownika końcowego i wybranych przez niego usług możemy być zmuszeni do wysyłania jego danych do kraju, który nie uzyskał decyzji Komisji Europejskiej stwierdzającej odpowiedni poziom ochrony. Każdorazowo proces ten przebiega zgodnie z przepisami o ochronie danych i odbywa się wyłącznie w razie konieczności. W każdym przypadku, bez wyjątków, muszą być ustanowione standardowe klauzule umowne, wiążące reguły korporacyjne lub inne odpowiednie zabezpieczenia.

Dokładamy wszelkich starań, aby nie dopuścić do przechowywania danych dłużej, niż jest to konieczne w związku ze sprzedażą usług na mocy umowy EULA. Okres przechowywania przez nas danych może być dłuższy niż okres ważność licencji użytkownika. Ma to umożliwić użytkownikowi łatwe i wygodne odnowienie licencji. Statystyki i inne dane zgromadzone przez usługę ESET LiveGrid® (w postaci zminimalizowanej i pseudonimizowanej) mogą być nadal przetwarzane w celach statystycznych.

Firma ESET stosuje odpowiednie środki techniczne i organizacyjne w celu zapewnienia poziomu zabezpieczeń odpowiedniego do zagrożeń. Dokładamy wszelkich starań, aby zapewnić ciągłą poufność, integralność, dostępność i odporność przetwarzanych systemów i usług. W przypadku naruszenia ochrony danych zagrażającego prawom i wolnościom Użytkownika końcowego jesteśmy jednak gotowi do powiadomienia o tym fakcie organów nadzorczych oraz właścicieli danych. Jako osoba, której dane dotyczą, użytkownik ma prawo do wniesienia skargi do organu nadzorczego.

Prawa osób, których dane dotyczą

Firma ESET podlega prawu słowackiemu i obowiązują ją przepisy Unii Europejskiej o ochronie danych. Zgodnie z warunkami zapisanymi w obowiązujących przepisach dotyczących ochrony danych osobowych, każdemu właścicielowi danych przysługują następujące prawa:

• prawo do uzyskania wglądu w swoje dane osobowe gromadzone przez firmę ESET;

• prawo do wprowadzenia zmian w swoich danych osobowych, jeśli są nieprawidłowe (Użytkownik końcowy ma także prawo do uzupełnienia niekompletnych danych osobowych);

• prawo do usunięcia swoich danych osobowych;

• prawo do ograniczenia zakresu przetwarzania swoich danych osobowych;

• prawo do niewyrażenia zgody na przetwarzanie danych;

• prawo do wniesienia skargi;

• prawo do przeniesienia danych.

Jeżeli użytkownik chce skorzystać z prawa przysługującego mu jako osobie, której dane dotyczą, a także w przypadku pytań lub wątpliwości, użytkownik może przesłać do nas wiadomość na adres:

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