

# ESET Endpoint Antivirus for Linux

## Benutzerhandbuch

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

Copyright ©2023 by ESET, spol. s r.o.

ESET Endpoint Antivirus for Linux wurde entwickelt von ESET, spol. s r.o.

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

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

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

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

REV. 19.03.2023

1 Einführung .....	1
<b>1.1 Wichtige Systemfunktionen</b> .....	1
2 Systemanforderungen .....	1
3 Installation .....	2
<b>3.1 Deinstallation</b> .....	3
<b>3.2 Massenhafte Bereitstellung</b> .....	4
4 Update, Upgrade .....	10
<b>4.1 Update-Mirror</b> .....	13
5 ESET Endpoint Antivirus for Linux aktivieren .....	14
<b>5.1 Wo finde ich meine Lizenz?</b> .....	15
<b>5.2 Aktivierungsstatus</b> .....	15
6 Arbeiten mit ESET Endpoint Antivirus for Linux .....	16
<b>6.1 Scans</b> .....	16
6.1 Ausschlussfilter .....	19
<b>6.2 Quarantäne</b> .....	20
<b>6.3 Ereignisse</b> .....	22
7 Konfiguration .....	23
<b>7.1 Malware Scan Engine</b> .....	24
7.1 Ausschlussfilter .....	24
7.1 Echtzeit-Dateischutz .....	26
7.1 Cloudbasierter Schutz .....	27
7.1 Malware-Prüfungen .....	29
7.1 Shared local cache .....	29
7.1 ThreatSense-Parameter .....	29
7.1 Zusätzliche ThreatSense-Parameter .....	32
<b>7.2 Update</b> .....	32
<b>7.3 Medienkontrolle</b> .....	33
7.3 Regel-Editor für die Medienkontrolle .....	34
7.3 Gerätegruppen .....	35
7.3 Hinzufügen von Regeln für die Medienkontrolle .....	35
<b>7.4 Tools</b> .....	37
7.4 Proxyserver .....	37
7.4 Log-Dateien .....	38
<b>7.5 Benutzeroberfläche</b> .....	39
8 Remoteverwaltung .....	39
9 Beispielanwendungsfälle .....	39
<b>9.1 Modulinformationen abrufen</b> .....	39
<b>9.2 Scan planen</b> .....	40
10 Datei- und Ordnerstruktur .....	41
11 Fehlerbehebung .....	43
<b>11.1 Logs sammeln</b> .....	44
<b>11.2 Verwenden des noexec-Flags</b> .....	45
<b>11.3 Echtzeit-Schutz kann nicht gestartet werden</b> .....	46
12 Bekannte Probleme .....	47
13 Glossar .....	47
14 Endbenutzer-Lizenzvereinbarung .....	47
15 Datenschutzerklärung .....	54

# Einführung

Die leistungsstarke ESET-Erkennungsroutine bietet eine beispiellose Scangeschwindigkeit und herausragende Erkennungsraten in Kombination mit minimalem Ressourcenverbrauch. Damit ist ESET Endpoint Antivirus for Linux (EEAU) die ideale Wahl für alle Linux-Desktops, die die [Systemanforderungen](#) erfüllen.

Die Hauptfunktionen werden vom On-Demand-Scanner und vom Echtzeit-Scanner abgedeckt.

Der On-Demand-Scanner kann von privilegierten Benutzern (normalerweise ein Systemadministrator) in der Befehlszeile oder durch das Scheduling-Tool des Betriebssystems (z. B. cron) gestartet werden. Der Begriff On-Demand bezieht sich auf Dateisystemobjekte, die aufgrund von Benutzer- oder Systemanforderungen gescannt werden.

Der Echtzeit-Scanner wird aufgerufen, wenn ein Benutzer und/oder das Betriebssystem versucht, auf Dateisystemobjekte zuzugreifen. Daher auch der Name Echtzeit: Der Scan wird in Echtzeit ausgelöst, wenn auf Dateisystemobjekte zugegriffen wird.

## Wichtige Systemfunktionen

- Echtzeit-Scan mit dem ressourcenschonenden ESET-Kernelmodul
- Umfassende Scan-Logs
- Neu gestaltete, benutzerfreundliche Einrichtung
- Quarantäne
- Desktophinweise
- Verwaltbar mit [ESET Security Management Center](#)

## Systemanforderungen

Die folgenden Hardwareanforderungen müssen erfüllt sein, um die Installationsprozedur für ESET Endpoint Antivirus for Linux korrekt ausführen zu können:

- Prozessor: Intel/AMD x64
- 700 MB freier Speicherplatz auf der Festplatte

Die folgenden 64-Bit-Betriebssysteme wurden getestet und werden offiziell unterstützt:

- Ubuntu Desktop 18.04 LTS 64-bit
- Ubuntu Desktop 20.04 LTS 64-bit
- Red Hat Enterprise Linux 7, 8 64-bit mit installierter unterstützter Desktopumgebung.

- SUSE Linux Enterprise Desktop 15



### AWS- und ELREPO-Kernel

Linux-Distributionen mit AWS- oder [ELREPO](#)-Kernel werden nicht unterstützt.

Unterstützte Desktopumgebungen:

- GNOME
- KDE
- XFCE

Beliebiges Gebietsschema mit UTF-8-Encoding



### Secure Boot

Secure Boot wird nicht unterstützt.

[Remoteverwaltung mit ESET Security Management Center.](#)

ESET Endpoint Antivirus for Linux ist kompatibel mit ESET Security Management Center v7.1 und höher.

## Installation

ESET Endpoint Antivirus for Linux wird als Binärdatei verteilt (*.bin*).



### HINWEIS

Installieren Sie die aktuellsten Updates für Ihr Betriebssystem, bevor Sie ESET Endpoint Antivirus for Linux installieren.

## Terminal-Installation

Um Ihr Produkt zu installieren oder zu aktualisieren, führen Sie das ESET-Distributionskript mit root-Berechtigungen für Ihre jeweilige BS-Distribution aus:

- `./eea-<VERSION>.x86_64.bin`
- `sh ./eea-<VERSION>.x86_64.bin`

Führen Sie den folgenden Befehl in einem Terminalfenster aus, um die verfügbaren Parameters (Argumente) für die ESET Endpoint Antivirus for Linux-Binärdatei anzuzeigen:

```
bash ./eea-<VERSION>.x86_64.bin -h
```

## Verfügbare Parameter

Kurzform	Langform	Beschreibung
-h	--help	Befehlszeilenargumente anzeigen
-n	--no-install	Nach dem Entpacken keine Installation durchführen
-y	--accept-license	Lizenz nicht anzeigen, Lizenz wurde akzeptiert
-f	--force-install	Installation per Paket-Manager ohne Nachfrage erzwingen



### .deb-Installationspaket abrufen

Um das passende .deb-Installationspaket für Ihr BS abzurufen, führen Sie das ESET-Distributionskript mit dem Befehlszeilenargument „-n“ aus:

```
sudo ./eea-<VERSION>.x86_64.bin -n
```

oder

```
sudo sh ./eea-<VERSION>.x86_64.bin -n
```

Um die Abhängigkeiten des Installationspakets anzuzeigen, führen Sie einen der folgenden Befehle aus:

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

Folgen Sie den Anweisungen auf dem Bildschirm. Nachdem Sie die Produktlizenzvereinbarung akzeptiert haben, wird die Installation abgeschlossen.

Eventuelle Abhängigkeitsprobleme werden im Installationsprogramm angezeigt.

## Installation über ESET Security Management Center (ESMC)

Weitere Informationen zur Remotebereitstellung von ESET Endpoint Antivirus for Linux auf Ihren Computern finden Sie in der Onlinehilfe zur [ESMC-Software-Installation](#).

[Aktivieren Sie ESET Endpoint Antivirus for Linux](#), um reguläre Updates der Erkennungsmodule zu aktivieren.



### Apps von Drittanbietern

Sie finden eine Liste der von ESET Endpoint Antivirus for Linux verwendeten Apps von Drittanbietern in der Datei NOTICE\_mode unter `/opt/eset/eea/doc/modules_notice/`.

## Deinstallation

Um Ihr ESET-Produkt zu deinstallieren, führen Sie den Befehl zum Entfernen der Pakete für Ihre Linux-Distribution als Superuser in einem Terminalfenster aus.

Ubuntu/Debian-basierte Distributionen:

- `apt remove eea`

Red Hat-basierte Distributionen:

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

## Massenhafte Bereitstellung

Dieser Abschnitt enthält eine Übersicht über die massenhafte Bereitstellung von ESET Endpoint Antivirus for Linux mit [Puppet](#), [Chef](#) und [Ansible](#). Die folgenden Codeblocks enthalten lediglich einfache Beispiele für die Installation der Pakete und müssen je nach Linux-Distribution angepasst werden.

### Paketauswahl

Bevor Sie mit der massenhaften Bereitstellung von ESET Endpoint Antivirus for Linux beginnen, müssen Sie entscheiden, welches Paket Sie verwenden möchten. ESET Endpoint Antivirus for Linux wird als .bin-Paket verteilt. Sie können jedoch [das deb/rpm-Paket abrufen](#) indem Sie das ESET-Distributionskript mit dem Befehlszeilenargument „-n“ ausführen.

## Puppet

### Voraussetzungen

- bin- oder deb/rpm-Paket auf puppet-master verfügbar
- puppet-agent ist mit puppet-master verbunden

### Bin-Paket

Bereitstellungsschritte:

- Kopieren Sie das Installationspaket auf die gewünschten Computer.
- Führen Sie das bin-Installationspaket aus.



### Beispiel für Puppet-Manifest

```
node default {
  file {"/tmp/eea-7.0.1081.0.x86_64.bin":
    mode => "0700",
    owner => "root",
    group => "root",
    source => "puppet:///modules/eea/eea-7.0.1081.0.x86_64.bin"
  }
  exec {"Execute bin package installation":
    command => '/tmp/eea-7.0.1081.0.x86_64.bin -y -f'
  }
}
```

## Deb/rpm package

Bereitstellungsschritte:

- Kopieren Sie das deb/rpm-Installationspaket für die passende Distributionsfamilie auf die gewünschten Computer.
- Führen Sie das deb/rpm-Installationspaket aus.



### Abhängigkeiten

Abhängigkeiten müssen vor der Installation aufgelöst werden.



### Beispiel für Puppet-Manifest

```
node default {
  if $osfamily == 'Debian' {
    file {"/tmp/eea-7.0.1081.0.x86_64.deb":
      mode => "0700",
      owner => "root",
      group => "root",
      source => "puppet:///modules/eea/eea-7.0.1081.0.x86_64.deb"
    }
    package {"eea":
      ensure => "installed",
      provider => 'dpkg',
      source => "/tmp/eea-7.0.1081.0.x86_64.deb"
    }
  }
  if $osfamily == RedHat {
    file {"/tmp/eea-7.0.1081.0.x86_64.rpm":
      mode => "0700",
      owner => "root",
      group => "root",
      source => "puppet:///modules/eea/eea-7.0.1081.0.x86_64.rpm"
    }
    package {"eea":
      ensure => "installed",
      provider => 'rpm',
      source => "/tmp/eea-7.0.1081.0.x86_64.rpm"
    }
  }
}
```

## Chef

### Voraussetzungen

- bin- oder deb/rpm-Paket auf Chef-Server verfügbar
- Chef-Client ist mit Chef-Server verbunden

### Bin-Paket

Bereitstellungsschritte:

- Kopieren Sie das Installationspaket auf die gewünschten Computer.
- Führen Sie das bin-Installationspaket aus.



### Beispiel für Chef-Recipe

```
cookbook_file '/tmp/eea-7.0.1084.0.x86_64.bin' do
  source 'eea-7.0.1084.0.x86_64.bin'
  owner 'root'
  group 'root'
  mode '0700'
  action :create
end

execute 'package_install' do
  command '/tmp/eea-7.0.1084.0.x86_64.bin -y -f'
end
```

## Deb/rpm package

Bereitstellungsschritte:

- Kopieren Sie das deb/rpm-Installationspaket für die passende Distributionsfamilie auf die gewünschten Computer.
- Führen Sie das deb/rpm-Installationspaket aus.



### Abhängigkeiten

Abhängigkeiten müssen vor der Installation aufgelöst werden.



### Beispiel für Chef-Recipe

```
cookbook_file '/tmp/eea-7.0.1084.0.x86_64.deb' do
  source 'eea-7.0.1084.0.x86_64.deb'
  owner 'root'
  group 'root'
  mode '0700'
  action :create
  only_if { node['platform_family'] == 'debian'}
end

cookbook_file '/tmp/eea-7.0.1084.0.x86_64.rpm' do
  source 'eea-7.0.1084.0.x86_64.rpm'
  owner 'root'
  group 'root'
  mode '0700'
  action :create
  only_if { node['platform_family'] == 'rhel'}
end

dpkg_package 'eea' do
  source '/tmp/eea-7.0.1084.0.x86_64.deb'
  action :install
  only_if { node['platform_family'] == 'debian'}
end

rpm_package 'eea' do
  source '/tmp/eea-7.0.1084.0.x86_64.rpm'
  action :install
  only_if { node['platform_family'] == 'rhel'}
end
```

## Ansible

### Voraussetzungen

- bin- oder deb/rpm-Paket auf Ansible-Server verfügbar
- ssh-Zugriff auf Zielcomputer

### Bin-Paket

Bereitstellungsschritte:

- Kopieren Sie das Installationspaket auf die gewünschten Computer.
- Führen Sie das bin-Installationspaket aus.



### Beispiel für Playbook-Task

```
.....  
- name: "INSTALL: Copy configuration json files"  
  copy:  
    src: eea-7.0.1084.0.x86_64.bin  
    dest: /home/ansible/  
  
- name : "Install product bin package"  
  shell: bash ./eea-7.0.1084.0.x86_64.bin -y -f -g  
.....
```

## Deb/rpm package

Bereitstellungsschritte:

- Kopieren Sie das deb/rpm-Installationspaket für die passende Distributionsfamilie auf die gewünschten Computer.
- Führen Sie das deb/rpm-Installationspaket aus.



## Beispiel für Playbook-Task

```
.....  
- name: "Copy deb package to VM"  
  copy:  
    src: ./eea-7.0.1085.0.x86_64.deb  
    dest: /home/ansible/eea-7.0.1085.0.x86_64.deb  
    owner: ansible  
    mode: a+r  
  when:  
    - ansible_os_family == "Debian"  
  
- name: "Copy rpm package to VM"  
  copy:  
    src: ./eea-7.0.1085.0.x86_64.rpm  
    dest: /home/ansible/eea-7.0.1085.0.x86_64.rpm  
    owner: ansible  
    mode: a+r  
  when:  
    - ansible_os_family == "RedHat"  
  
- name: "Install deb package"  
  apt:  
    deb: /home/ansible/eea-7.0.1085.0.x86_64.deb  
    state: present  
  when:  
    - ansible_os_family == "Debian"  
  
- name: "Install rpm package"  
  apt:  
    deb: /home/ansible/eea-7.0.1085.0.x86_64.rpm  
    state: present  
  when:  
    - ansible_os_family == "RedHat"  
  
.....
```

## Update, Upgrade

[Abkürzung zum Upgrade](#)

### Modulupdate

Produktmodule, inklusive der Erkennungsmodule, werden automatisch aktualisiert.

Um das Update des Erkennungsmoduls manuell zu starten, führen Sie den Updatebefehl in einem Terminalfenster aus, oder führen Sie das [Update im ESET Security Management Center](#) aus.

Falls ein ESET Endpoint Antivirus for Linux-Update nicht stabil ist, können Sie das Modul-Update auf einen vorherigen Zustand zurücksetzen. Führen Sie den entsprechenden Befehl in einem Terminalfenster aus, oder führen Sie einen [Rollback mit ESET Security Management Center](#) aus.

Um alle Produktmodule in einem Terminalfenster zu aktualisieren, führen Sie den folgenden Befehl aus:

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

## Update und Rollback im Terminal

Optionen - Kurzform	Optionen - Langform	Beschreibung
-u	--update	Module aktualisieren
-c	--cancel	Download von Modulen abbrechen
-e	--resume	Updatesperre aufheben
-l	--list-modules	Version der verwendeten Module anzeigen
-r	--rollback=WERT	Rollback auf den ältesten Snapshot des Scanner-Moduls und sämtliche Updates für VALUE Stunden blockieren
	--server=ADRESSE	Adresse des Updateservers
	--username=BENUTZERNAME	Benutzername für die Authentifizierung des Update-Anrechts
	--password=PASSWORT	Passwort für die Authentifizierung des Update-Anrechts
	--proxy-addr=ADRESSE	Adresse des Proxyserver
	--proxy-port=PORT	Port des Proxyserver
	--proxy-username=BENUTZERNAME	Benutzername für den Proxyserver, falls dieser mit Benutzername/Passwort geschützt ist
	--proxy-password=PASSWORT	Passwort für den Proxyserver, falls dieser mit Benutzername/Passwort geschützt ist
	--update-server-type=UPDATE_TYP	Art des Updateservers
	--list-update-server-type	Arten von Updateservern auflisten



### Wichtig

Das upd-Hilfsprogramm kann nicht verwendet werden, um die Produktkonfiguration zu ändern.

## BEISPIEL

Um Updates für 48 Stunden auszusetzen und ein Rollback auf den ältesten Snapshot des Scanner-Moduls durchzuführen, führen Sie den folgenden Befehl als privilegierter Benutzer aus:

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

Um die automatischen Updates des Scanner-Moduls fortzusetzen, führen Sie den folgenden Befehl als privilegierter Benutzer aus:

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

Um ein Update von einem Mirror-Server unter der IP-Adresse „192.168.1.2“ und dem Port 2221 durchzuführen, führen Sie den folgenden Befehl als privilegierter Benutzer aus:

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

# ESET Endpoint Antivirus for Linux auf eine neuere Version aktualisieren

Neuere Versionen von ESET Endpoint Antivirus for Linux werden veröffentlicht, um Verbesserungen oder Patches durchzuführen, die ein automatisches Update der Programmmodule nicht leisten kann.

## Welche Produktversion ist aktuell installiert?

Um die Produktversion von ESET Endpoint Antivirus for Linux herauszufinden, haben Sie zwei Optionen:

1. Führen Sie `/opt/eset/eea/lib/egui -v` in einem Terminalfenster aus.
2. Sehen Sie in ESET Security Management Center (ESMC) im Bereich **Computer** nach.

## Durchführen des Upgrades?

Für ein Upgrade auf eine neuere Version führen Sie ein passendes Installationspaket für Ihr BS aus, wie im Abschnitt [Installation](#) beschrieben.

Wenn Sie ESET Endpoint Antivirus for Linux über ESET Security Management Center verwalten, können Sie das Upgrade mit dem Task [Software-Installation](#) oder unter **Dashboard > ESET-Anwendungen > Rechtsklick auf ESET Endpoint Antivirus for Linux > Installierte ESET-Produkte aktualisieren** starten.



Ein direktes Upgrade von ESET NOD32 Antivirus 4 for Linux Desktop ist nicht möglich.

ESET Endpoint Antivirus for Linux ist ein völlig neues Produkt, dessen Konfiguration nicht mit der Konfiguration von ESET NOD32 Antivirus 4 for Linux Desktop kompatibel ist.

Gehen Sie wie folgt vor, um ein Upgrade von ESET NOD32 Antivirus 4 for Linux Desktop auf ESET Endpoint Antivirus for Linux durchzuführen.

### Remote verwaltete Umgebung ([ESMC](#))

Falls Sie ESET NOD32 Antivirus 4 for Linux Desktop remote verwalten, zeigt ESMC keinen Hinweis für das verfügbare Upgrade an.

1. Führen Sie den Task [Software-Deinstallation](#) auf den vorhandenen Installationen von ESET NOD32 Antivirus 4 for Linux Desktop aus.
2. Stellen Sie ESET Endpoint Antivirus for Linux mit dem Task [Software-Installation](#) remote auf Ihren Computern bereit.

### Persönlich verwaltete Umgebung

Wenn Sie versuchen, ESET Endpoint Antivirus for Linux zu installieren, ohne ESET NOD32 Antivirus 4 for Linux Desktop zu entfernen, dann schlägt die Installation mit der folgenden Nachricht fehl:

„Fehler: das vorherige ESET Sicherheitsprodukt muss zuerst deinstalliert werden, das Paket wird nicht installiert.“

1. Deinstallieren Sie ESET NOD32 Antivirus 4 for Linux Desktop mit dem heruntergeladenen Installationsprogramm.

- i. Klicken Sie mit der rechten Maustaste auf die heruntergeladene Installationsdatei (*eset\_nod32av\_64bit\_<langue\_code>.linux*), klicken Sie auf die Registerkarte **Eigenschaften** > **Berechtigungen**, aktivieren Sie die Option **Ausführung von Datei als Programm zulassen** und schließen Sie das Fenster.
- ii. Doppelklicken Sie auf das Installationsprogramm, um das **Setup für ESET NOD32 Antivirus** zu starten.
- iii. Klicken Sie auf **Weiter**, wählen Sie **ESET NOD32 Antivirus von Ihrem Computer entfernen** aus und klicken Sie auf **weiter**.
- iv. Wählen Sie im Listenfeld **Wählen Sie eine der Optionen** die Option **Keiner der genannten Punkte** aus.
- v. Geben Sie „*Upgrade auf ESET Endpoint Antivirus for Linux*“ unter **Sonstige zusätzliche Daten** ein und klicken Sie auf **Weiter** und dann auf **Deinstallieren**.
- vi. Click Sie nach Abschluss der Deinstallation auf **Fertig stellen** und dann auf **Ja**, um den Computer neu zu starten.

2. [Installieren Sie ESET Endpoint Antivirus for Linux.](#)

## Update-Mirror

Mit verschiedenen ESET-Sicherheitsprodukten ([ESET Security Management Center](#), [ESET Endpoint Antivirus](#) usw.) haben Sie die Möglichkeit, Kopien der Update-Dateien zu erstellen. Diese können Sie dann zur Aktualisierung anderer Workstations im Netzwerk verwenden. Das Verwenden eines Update-Mirrors - das Vorhalten von Kopien der Update-Dateien im lokalen Netzwerk - kann vorteilhaft sein, da die Dateien dann nicht von allen Arbeitsplatzcomputern einzeln über das Internet heruntergeladen werden müssen. Updates werden auf den lokalen Mirror-Server heruntergeladen und von dort an die Arbeitsstationen verteilt. Die Internetverbindung wird erheblich entlastet. Das Aktualisieren der Clientcomputer von einem Update-Mirror optimiert die Lastenverteilung im Netzwerk und entlastet Internetverbindungen.

## ESET Endpoint Antivirus for Linux für die Verwendung eines Update-Mirrors konfigurieren

1. Klicken Sie in ESET Security Management Center auf **Policies** > **Neue Policy** und geben Sie einen Namen für die Policy ein.
2. Klicken Sie auf **Einstellungen**, und wählen Sie **ESET Endpoint for Linux (V7+)** im Dropdownmenü aus.
3. Klicken Sie auf **Update** > **Primärer Server**.
4. Deaktivieren Sie den Schalter neben **Automatisch auswählen** im Abschnitt **Einfach**.
5. Geben Sie im Feld **Updateserver** die URL-Adresse des Mirror-Servers in einem der folgenden Formate ein:

ohttp://<IP>:<port>

ohttp://<hostname>:<port>

6. Geben Sie den entsprechenden Benutzernamen und das Passwort ein.
7. Navigieren Sie zu **Zuweisen**, klicken Sie auf **Zuweisen**, und wählen Sie die Gruppe von Computern aus, auf die Sie die Policy anwenden möchten.
8. Klicken Sie auf **OK** und klicken Sie dann auf **Fertig**.

Falls in Ihrem Netzwerk mehrere Mirror-Server verfügbar sind, wiederholen Sie die genannten Schritte, um die sekundären Updateserver zu konfigurieren.

## ESET Endpoint Antivirus for Linux aktivieren

Aktivieren Sie Ihr Exemplar von ESET Endpoint Antivirus for Linux mit einer [Lizenz](#), die Sie von Ihrem ESET-Distributor erhalten haben.

### Mit Terminal aktivieren

Führen Sie das Hilfsprogramm `/opt/eset/eea/sbin/lic` als privilegierter Benutzer aus, um ESET Endpoint Antivirus for Linux in einem Terminalfenster zu aktivieren.

Syntax: `/opt/eset/eea/sbin/lic[OPTIONEN]`

#### BEISPIEL

Die folgenden Befehle müssen von einem privilegierten Benutzer ausgeführt werden.

#### Aktivierung mit Lizenzschlüssel

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

oder

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

wobei XXXX-XXXX-XXXX-XXXX-XXXX für Ihren ESET Endpoint Antivirus for Linux-Lizenzschlüssel steht.

#### Aktivierung mit Benutzername und Passwort

Die folgenden Befehle müssen von einem privilegierten Benutzer ausgeführt werden:

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

Der Benutzer wird zur Eingabe des Passworts aufgefordert. `public_id` enthält die öffentliche Lizenz-ID.

Wenn Sie Benutzername, Passwort und die öffentliche Lizenz-ID in einer `password.txt`-Datei gespeichert haben, führen Sie den folgenden Befehl als privilegierter Benutzer aus:

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

## Aktivierung mit Offline-Lizenzdatei

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

oder

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

## Mit ESET Security Management Center (ESMC) aktivieren

Melden Sie sich bei der ESMC-Web-Oberfläche an, navigieren Sie zu **Client-Tasks > Produktaktivierung** und folgen Sie den [Anweisungen zur Produktaktivierung](#).

## Wo finde ich meine Lizenz?

Beim Kauf Ihrer Lizenz sollten Sie zwei E-Mails von ESET erhalten haben. Die erste E-Mail enthält Informationen zum ESET Business Account-Portal. Die zweite E-Mail enthält Details zu Ihrem Lizenzschlüssel (XXXXX-XXXXX-XXXXX-XXXXX-XXXXX) oder Ihrem Benutzernamen (EAV-xxxxxxxxx) und Ihrem Passwort, soweit verfügbar, Ihre öffentliche Lizenz-ID (xxx-xxx-xxx), den Produktnamen (oder eine Liste der Produkte) und die entsprechenden Mengen.

## Ich habe einen Benutzernamen und ein Passwort

Falls Sie einen Benutzernamen und ein Passwort haben, können Sie sie auf der entsprechenden Konvertierungsseite im ESET Business Account zu einem Lizenzschlüssel konvertieren:

<https://eba.eset.com/LicenseConverter>

## Aktivierungsstatus überprüfen

Die unten beschriebene Funktion ist in ESET Endpoint Antivirus for Linux Version 7.1 und höher verfügbar. Mit dem Hilfsprogramm `lic` können Sie den Aktivierungsstatus und die Gültigkeit der Lizenz anzeigen. Führen Sie die folgenden Befehle als privilegierter Benutzer aus:

Syntax: `/opt/eset/eea/sbin/lic[OPTIONEN]`



### BEISPIEL

Die folgenden Befehle müssen von einem privilegierten Benutzer ausgeführt werden:

```
/opt/eset/eea/sbin/lic -s
```

oder

```
/opt/eset/eea/sbin/lic --status
```

Ausgabe, wenn das Produkt aktiviert ist:

```
Status: Activated
```

```
Public Id: ABC-123-DEF
```

```
License Validity: 2020-03-29
```

Ausgabe, wenn das Produkt nicht aktiviert ist:

```
Status: Not activated
```

## Arbeiten mit ESET Endpoint Antivirus for Linux

Nach Abschluss der Installation können Sie ein Terminalfenster oder [ESET Security Management Center](#) verwenden, um ESET Endpoint Antivirus for Linux zu steuern.

### Scans

Quicklinks: [Prüfprofile](#)

### On-Demand-Scan in einem Terminalfenster ausführen

Syntax: /opt/eset/eea/bin/odscan [OPTIONEN..]

Optionen - Kurzform	Optionen - Langform	Beschreibung
-l	--list	Aktuell laufende Scans anzeigen
	--list-profiles	Alle verfügbaren Scanprofile anzeigen
	--all	Von anderen Benutzern ausgeführte Scans ebenfalls anzeigen (root-Berechtigungen erforderlich)
-r	--resume=session_id	Zuvor pausierten Scan fortsetzen (identifiziert durch session_id)
-p	--pause=session_id	Scan pausieren (identifiziert durch session_id)
-t	--stop=session_id	Scan beenden (identifiziert durch session_id)
-s	--scan	Prüfung starten
	--profile=PROFIL	Mit ausgewähltem PROFIL scannen
	--profile-priority=PRIORITÄT	Task wird mit der angegebenen Priorität ausgeführt. Mögliche Prioritäten: normal, niedrig, minimal, Leerlauf
	--readonly	Prüfungsfortschritt anzeigen
	--local	Lokale Laufwerke scannen
	--network	Netzlaufwerke scannen
	--removable	Wechselmedien scannen
	--boot-local	Bootsektoren des lokalen Laufwerks scannen
	--boot-removable	Bootsektoren der Wechselmedien scannen
	--boot-main	Hauptsystembereich scannen
	--exclude=DATEI	Ausgewählte Datei oder ausgewähltes Verzeichnis überspringen
	--ignore-exclusions	<a href="#">Ausgeschlossene Pfade und Erweiterungen</a> ebenfalls scannen

## BEISPIEL

On-Demand-Scan für das Verzeichnis `/root/*` rekursiv mit dem Scanprofil „@Smart scan“ als Hintergrundprozess ausführen:

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

On-Demand-Scan mit dem Scan-Profil " @Smart Scan" für mehrere Ziele rekursiv ausführen:

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

Alle laufenden Scans auflisten

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

Scan mit der Session-ID „15“ pausieren. Jeder Scan hat eine eigene Session-ID, die beim Start generiert wird.

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

Scan mit der Session-ID „15“ beenden. Jeder Scan hat eine eigene Session-ID, die beim Start generiert wird.

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

On-Demand-Scan mit dem ausgeschlossenen Verzeichnis `/root/exc_dir/` und der ausgeschlossenen Datei `/root/eicar.com` ausführen:

```
/opt/eset/eea/bin/odscan --scan --exclude=/root/exc_dir/ --exclude=/root/eicar.com
```

Bootsektor der Wechselmedien scannen. Führen Sie den folgenden Befehl als privilegierter Benutzer aus.

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

## Exitcodes

Ab ESET Endpoint Antivirus for Linux Version 7.1 zeigt das Hilfsprogramm `odscan` nach abgeschlossenem Scan einen Exitcode an.

Exitcodes	Bedeutung
0	Keine Bedrohungen gefunden
1	Bedrohungen gefunden und entfernt
10	Einige Dateien konnten nicht geprüft werden (evtl. Bedrohungen)

50	Bedrohung gefunden
100	Fehler

## Scan-Profile

Ihre bevorzugten Scan-Parameter ([ThreatSense-Parameter](#)) können für zukünftige Prüfungen gespeichert werden. Wir empfehlen Ihnen, für jede regelmäßig durchgeführte Prüfung ein eigenes Profil zu erstellen (mit verschiedenen zu prüfenden Objekten, Prüfmethoden und anderen Parametern).

### Erstellen Sie ein neues Profil in ESET Security Management Center

1. Klicken Sie in ESET Security Management Center auf **Policies > Neue Policy** und geben Sie einen Namen für die Policy ein.
2. Klicken Sie auf **Einstellungen**, und wählen Sie **ESET Endpoint for Linux (V7+)** im Dropdownmenü aus.
3. Klicken Sie auf **Malware-Scans > On-Demand-Scan**, und klicken Sie auf **Bearbeiten** neben der **Profilliste**.
4. Geben Sie einen Namen für das neue Profil ein, klicken Sie auf **Hinzufügen** und dann auf **Speichern**.
5. Wählen Sie im Dropdownmenü **Ausgewähltes Profil** das neu erstellte Profil aus und passen Sie die Scan-Einstellungen im Bereich **Malware-Scans** an.
6. Navigieren Sie zu **Zuweisen**, klicken Sie auf **Zuweisen**, und wählen Sie die Gruppe von Computern aus, auf die Sie die Policy anwenden möchten.
7. Klicken Sie auf **OK** und dann auf **Fertig**.

## Ausschlussfilter

### Leistungsausschlüsse

Sie können Pfade (Ordner) vom Scannen ausschließen, um die Dauer der Dateisystem-Scans auf Malware erheblich zu verringern.

1. Klicken Sie in ESET Security Management Center auf **Policies > Neue Policy** und geben Sie einen Namen für die Policy ein.
2. Klicken Sie auf **Einstellungen**, und wählen Sie **ESET Endpoint for Linux (V7+)** im Dropdownmenü aus.
3. Navigieren Sie zu **Erkennungsroutine > Einfach**, und klicken Sie auf **Bearbeiten** neben **Leistungsausschlüsse**.
4. Klicken Sie auf **Hinzufügen**, und definieren Sie den **Pfad**, den der Scanner überspringen soll. Optional können Sie einen Kommentar zu Informationszwecken hinzufügen.
5. Klicken Sie auf **OK** und dann auf **Speichern**, um das Dialogfeld zu schließen.
6. Navigieren Sie zu **Zuweisen**, klicken Sie auf **Zuweisen**, und wählen Sie die Gruppe von Computern aus, auf die Sie die Policy anwenden möchten.
7. Klicken Sie auf **OK** und dann auf **Fertig stellen**.

## Ausschlusspfad

`/root/*` - Das Verzeichnis „root“ und sämtliche Unterverzeichnisse und deren Inhalte.

`/root` - Nur die Datei „root“.

`/root/file.txt` - Nur die Datei file.txt im Verzeichnis „root“.



### Platzhalter in Pfaden

Verwenden Sie Platzhalter in Pfaden (z. B. `/home/user/*/data/file.dat`) nur, wenn dies für Ihre Systeminfrastruktur erforderlich ist. Weitere Informationen finden Sie im folgenden [Knowledgebase-Artikel](#).

## Ausschlüsse von Dateieendungen

Diese Art von Ausschluss kann für den **Echtzeit-Dateischutz**, für **On-Demand-Scans** eingerichtet werden.

1. Klicken Sie in ESET Security Management Center auf **Policies > Neue Policy** und geben Sie einen Namen für die Policy ein.
2. Klicken Sie auf **Einstellungen**, und wählen Sie **ESET Endpoint for Linux (V7+)** im Dropdownmenü aus.
3. Navigieren Sie zu:
  - **Echtzeit-Dateischutz > Threatsense-Parameter**
  - **Malware-Scans > On-Demand-Scan > Threatsense-Parameter**
4. Klicken Sie auf **Bearbeiten** neben **Vom Scannen ausgeschlossene Dateieendungen**.
5. Klicken Sie auf **Hinzufügen** und geben Sie die auszuschließende Erweiterung ein. Um mehrere Erweiterungen gleichzeitig anzugeben, **geben Sie mehrere Werte ein** und trennen Sie die einzelnen Erweiterungen durch Zeilenumbrüche oder ein anderes von Ihnen festgelegtes Trennzeichen.
6. Klicken Sie auf **OK** und dann auf **Speichern**, um das Dialogfeld zu schließen.
7. Navigieren Sie zu **Zuweisen**, klicken Sie auf **Zuweisen**, und wählen Sie die Gruppe von Computern aus, auf die Sie die Policy anwenden möchten.
8. Klicken Sie auf **OK** und dann auf **Fertig stellen**.

## Quarantäne

Die Hauptfunktion der Quarantäne ist die sichere Verwahrung infizierter Dateien. Dateien sollten in die Quarantäne verschoben werden, wenn sie nicht gesäubert werden können, wenn es nicht sicher oder ratsam ist, sie zu löschen, oder wenn sie von ESET Endpoint Antivirus for Linux fälschlicherweise erkannt worden sind. Sie können beliebige Dateien gezielt in die Quarantäne verschieben. Dies macht Sinn für Dateien, die sich verdächtig verhalten, bei der Virenprüfung jedoch nicht erkannt werden. Dateien aus der Quarantäne können zur Analyse an

ESET eingereicht werden.

Pfad zum Quarantäne-Ordner: `/var/opt/eset/eea/cache/quarantine/`

Das Quarantäneverzeichnis wird erstellt, wenn Sie zum ersten Mal ein Element in die Quarantäne verschieben.

## Elemente in der Quarantäne im Terminal verwalten

Syntax: `/opt/eset/eea/bin/quar[OPTIONEN]`

Optionen - Kurzform	Optionen - Langform	Beschreibung
-i	--import	Datei in Quarantäne importieren
-l	--list	Liste der Dateien in der Quarantäne anzeigen
-r	--restore=id	Element aus Quarantäne wiederherstellen (mit angegebener ID) und in den unter --restore-path angegebenen Pfad
-e	--restore-exclude=id	Element aus Quarantäne wiederherstellen (mit angegebener ID und markiert durch „x“ in der Spalte <b>ausschließbar</b> )
-d	--delete=id	Element aus Quarantäne löschen (mit angegebener ID)
-f	--follow	Auf neue Elemente warten und an die Ausgabe anfügen
	--restore-path=pfad	Pfad, an dem das Element aus Quarantäne wiederhergestellt werden soll
-h	--help	Hilfe anzeigen und beenden.
-v	--version	Versionsinformationen anzeigen und beenden

## BEISPIEL

Element mit ID „0123456789“ aus Quarantäne löschen:

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

oder

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

Element mit ID „9876543210“ aus Quarantäne im Ordner *Download* des angemeldeten Benutzers wiederherstellen und umbenennen zu *restoredFile.test*:

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

oder

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

Element mit ID „123456789“ und mit Markierung „x“ in der Spalte **ausschließbar** aus Quarantäne in den Ordner *Download* wiederherstellen:

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

oder

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

## Dateien aus der Quarantäne im Terminal wiederherstellen

1. Listen Sie die Elemente in der Quarantäne auf.

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

2. Notieren Sie sich die ID und den Namen des Elements, das Sie wiederherstellen möchten, und führen Sie den folgenden Befehl aus:

```
/opt/eset/eea/bin/quar --restore=ID_DES_WIEDERHERZUSTELLENDEN_OBJEKTS --restore-path=/endgültiger/Pfad/der/wiederhergestellten/Datei
```

## Ereignisse

Im Terminal ausgeführte relevante ESET Endpoint Antivirus for Linux-Befehle und weitere Informationen werden im Bildschirm **Ereignisse** geloggt.

Jede erfasste Aktion enthält die folgenden Informationen: Zeitpunkt des Ereignisses, Komponente (falls verfügbar), Ereignis, Benutzer

## Ereignisse im Terminal anzeigen

Um den Inhalt des Bildschirms **Ereignisse** in einem Terminalfenster anzuzeigen, können Sie das Befehlszeilentool `lslog` verwenden.

Syntax: `/opt/eset/eea/sbin/lslog[OPTIONEN]`

Optionen - Kurzform	Optionen - Langform	Beschreibung
-f	--follow	Auf neue Logs warten und an die Ausgabe anfügen
-o	--optimize	Logs optimieren
-c	--csv	Logs im CSV-Format anzeigen.
-e	--events	Ereignis-Logs auflisten
-l	--device-control	Logs für die Medienkontrolle auflisten
-s	--scans	On-Demand-Scan-Logs auflisten
-d	--detections	Erkennungs-Log-Datensätze auflisten

## BEISPIELE

Alle Ereignis-Logs anzeigen:

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

Alle Ereignis-Logs im CSV-Format in einer Datei im Ordner *Documents* des aktuellen Benutzers speichern:

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

## Konfiguration

So ändern Sie die Konfiguration von ESET Endpoint Antivirus for Linux:

1. Klicken Sie in ESET Security Management Center auf **Policies > Neue Policy** und geben Sie einen Namen für die Policy ein.
2. Klicken Sie auf **Einstellungen**, und wählen Sie **ESET Endpoint for Linux (V7+)** im Dropdownmenü aus.
3. Speichern Sie die Einstellungen in den Dialogfeldern, falls Sie Änderungen vorgenommen haben.
4. Klicken Sie auf **Fertig**.

Sie können das [Erkennungsverhalten](#) anpassen und die Einstellungen für Produktupdates und die Verbindung ändern.

Wenn Sie ESET Endpoint Antivirus for Linux nach Ihren Anforderungen konfiguriert haben und die Konfiguration zum späteren Gebrauch speichern (oder für eine andere Instanz von ESET Endpoint Antivirus for Linux verwenden) möchten, können Sie sie in eine *.xml*-Datei exportieren.

Führen Sie die folgenden Befehle mit root-Berechtigungen in einem Terminalfenster aus.

### Konfiguration exportieren

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

### Konfiguration importieren

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

### Verfügbare Optionen

Kurzform	Langform	Beschreibung
-i	--json-rpc	list of json-rpc files

Kurzform	Langform	Beschreibung
	--import-xml	import settings
	--export-xml	export settings
-h	--help	show help
-v	--version	show version information

## Malware Scan Engine

Die Standardkonfiguration des Erkennungsverhaltens bietet grundlegende Sicherheitsfunktionen, inklusive:

- [Echtzeit-Dateischutz](#)
- Smart-Optimierung (effiziente Kombination aus Systemschutz und Scan-Geschwindigkeit)
- [ESET LiveGrid](#)-Reputationssystem

Um zusätzliche Schutzfunktionen zu aktivieren,  [verwenden ESET Security Management Center:](#)

So ändern Sie die Konfiguration von ESET Endpoint Antivirus for Linux:

1. Klicken Sie in ESET Security Management Center auf **Policies > Neue Policy** und geben Sie einen Namen für die Policy ein.
2. Klicken Sie auf **Einstellungen**, und wählen Sie **ESET Endpoint for Linux (V7+)** im Dropdownmenü aus.
3. Speichern Sie die Einstellungen in den Dialogfeldern, falls Sie Änderungen vorgenommen haben.
4. Klicken Sie auf **Fertig**.

- Ereignis auf [Potenziell unerwünschte Anwendungen](#)
- Erkennung [potenziell unsicherer Anwendungen](#) (zum Beispiel Keylogger, Passwort-Cracking-Tools)
- Übermittlung verdächtiger oder infizierter Samples aktivieren
- Konfigurieren von [Ausschlüssen](#) (Dateien oder Verzeichnisse, die nicht gescannt werden), um die Scans zu beschleunigen
- Aktivieren des [freigegebenen lokalen Cache](#)

## Ausschlussfilter

### Leistungsausschlüsse

Sie können Pfade (Ordner) vom Scannen ausschließen, um die Dauer der Dateisystem-Scans auf Malware erheblich zu verringern.

1. Klicken Sie in ESET Security Management Center auf **Policies > Neue Policy** und geben Sie einen Namen für die Policy ein.
2. Klicken Sie auf **Einstellungen**, und wählen Sie **ESET Endpoint for Linux (V7+)** im Dropdownmenü aus.
3. Navigieren Sie zu **Erkennungsroutine > Einfach**, und klicken Sie auf **Bearbeiten** neben **Leistungsausschlüsse**.
4. Klicken Sie auf **Hinzufügen**, und definieren Sie den **Pfad**, den der Scanner überspringen soll. Optional können Sie einen Kommentar zu Informationszwecken hinzufügen.
5. Klicken Sie auf **OK** und dann auf **Speichern**, um das Dialogfeld zu schließen.
6. Navigieren Sie zu **Zuweisen**, klicken Sie auf **Zuweisen**, und wählen Sie die Gruppe von Computern aus, auf die Sie die Policy anwenden möchten.
7. Klicken Sie auf **OK** und dann auf **Fertig stellen**.

## Ausschlusspfad

*/root/\** - Das Verzeichnis „root“ und sämtliche Unterverzeichnisse und deren Inhalte.

*/root* - Nur die Datei „root“.

*/root/file.txt* - Nur die Datei file.txt im Verzeichnis „root“.



### Platzhalter in Pfaden

Verwenden Sie Platzhalter in Pfaden (z. B. */home/user/\*/data/file.dat*) nur, wenn dies für Ihre Systeminfrastruktur erforderlich ist. Weitere Informationen finden Sie im folgenden [Knowledgebase-Artikel](#).

## Ausschlüsse von Dateiendungen

Diese Art von Ausschluss kann für den **Echtzeit-Dateischutz**, für **On-Demand-Scans** eingerichtet werden.

1. Klicken Sie in ESET Security Management Center auf **Policies > Neue Policy** und geben Sie einen Namen für die Policy ein.
2. Klicken Sie auf **Einstellungen**, und wählen Sie **ESET Endpoint for Linux (V7+)** im Dropdownmenü aus.
3. Navigieren Sie zu:
  - **Echtzeit-Dateischutz > Threatsense-Parameter**
  - **Malware-Scans > On-Demand-Scan > Threatsense-Parameter**
4. Klicken Sie auf **Bearbeiten** neben **Vom Scannen ausgeschlossene Dateiendungen**.
5. Klicken Sie auf **Hinzufügen** und geben Sie die auszuschließende Erweiterung ein. Um mehrere

Erweiterungen gleichzeitig anzugeben, **geben Sie mehrere Werte ein** und trennen Sie die einzelnen Erweiterungen durch Zeilenumbrüche oder ein anderes von Ihnen festgelegtes Trennzeichen.

6. Klicken Sie auf **OK** und dann auf **Speichern**, um das Dialogfeld zu schließen.

7. Navigieren Sie zu **Zuweisen**, klicken Sie auf **Zuweisen**, und wählen Sie die Gruppe von Computern aus, auf die Sie die Policy anwenden möchten.

8. Klicken Sie auf **OK** und dann auf **Fertig stellen**.

## Echtzeit-Dateischutz

Der Echtzeit-Dateischutz überwacht alle für den Virenschutz relevanten Systemereignisse. Alle Dateien werden beim Öffnen, Erstellen oder Ausführen auf Ihrem Computer auf Schadcode geprüft. Der Echtzeit-Dateischutz wird standardmäßig beim Systemstart gestartet und fortlaufend ausgeführt. In Ausnahmefällen (z. B. bei einem Konflikt mit einer anderen Echtzeitprüfung) kann der Echtzeit-Dateischutz deaktiviert werden. Deaktivieren Sie dazu die Option **Echtzeit-Dateischutz aktivieren** automatisch unter **Einstellungen > Erkennungsroutine > Echtzeit-Dateischutz > Einfach**.



Der Echtzeit-Dateischutz scannt den Inhalt von Archivdateien nicht. Beim Herunterladen auf die Festplatte wird der Inhalt bestimmter selbstentpackender Archive gescannt.

### Zu scannende Datenträger

In der Standardeinstellung werden alle Datenträger auf mögliche Bedrohungen geprüft:

- **Lokale Laufwerke** - Geprüft werden alle lokalen Laufwerke
- **Wechselmedien** - Geprüft werden CDs/DVDs, USB-Speichergeräte, Bluetooth-Geräte usw.
- **Netzlaufwerke** - Geprüft werden alle zugeordneten Netzlaufwerke

Es wird empfohlen, diese Einstellungen nur in Ausnahmefällen zu ändern, z. B. wenn die Prüfung bestimmter Datenträger die Datenübertragung deutlich verlangsamt.

### Prüfen beim

Standardmäßig werden alle Dateien beim Öffnen, Erstellen und Ausführen geprüft. Wir empfehlen Ihnen, die Standardeinstellungen beizubehalten. So bietet der Echtzeit-Dateischutz auf Ihrem Computer maximale Sicherheit:

- **Öffnen von Dateien** - Prüfen von Dateien beim Öffnen aktivieren/deaktivieren.
- **Erstellen von Dateien** - Prüfen von Dateien beim Erstellen aktivieren/deaktivieren.
- **Zugriff auf Wechselmedien** - Aktiviert oder deaktiviert die automatischen Scans von Wechselmedien, wenn diese an den Computer angeschlossen werden.

Der Echtzeit-Dateischutz überwacht alle Datenträger auf das Eintreten bestimmter Ereignisse wie den Zugriff auf eine Datei. Durch die Verwendung der ThreatSense-Erkennungsmethoden (siehe Abschnitt [Einstellungen](#) für [ThreatSense](#)) kann der Echtzeit-Dateischutz so konfiguriert werden, dass neu erstellte und vorhandene Dateien unterschiedlich behandelt werden. Sie können den Echtzeit-Dateischutz z. B. so konfigurieren, dass neuere Dateien genauer überwacht werden.

Bereits gescannte Dateien werden nicht erneut gescannt (sofern sie nicht geändert wurden), um die Systembelastung durch den Echtzeit-Dateischutz zu minimieren. Nach einem Update der Erkennungsroutine werden die Dateien sofort wieder gescannt. Dieses Verhalten wird mit der **Smart-Optimierung** gesteuert. Wenn die **Smart-Optimierung** deaktiviert ist, werden alle Dateien bei jedem Zugriff gescannt. Um diese Einstellung zu bearbeiten, [verwenden ESET Security Management Center](#)>

So ändern Sie die Konfiguration von ESET Endpoint Antivirus for Linux:

1. Klicken Sie in ESET Security Management Center auf **Policies > Neue Policy** und geben Sie einen Namen für die Policy ein.
2. Klicken Sie auf **Einstellungen**, und wählen Sie **ESET Endpoint for Linux (V7+)** im Dropdownmenü aus.
3. Speichern Sie die Einstellungen in den Dialogfeldern, falls Sie Änderungen vorgenommen haben.
4. Klicken Sie auf **Fertig**.

. Navigieren Sie dort zu **Erkennungsroutine > Echtzeit-Dateischutz**, klicken Sie auf **ThreatSense-Parameter > Sonstige** und aktivieren bzw. deaktivieren Sie die Option **Smart-Optimierung aktivieren**.

## Cloudbasierter Schutz

ESET LiveGrid® ist ein modernes Frühwarnsystem, das mehrere Cloud-basierte Technologien umfasst. Es unterstützt die Erkennung neuer Bedrohungen auf Grundlage einer Reputationstechnologie und verbessert durch die Verwendung von Positivlisten die Scan-Leistung. Neue Bedrohungsinformationen werden in Echtzeit zur Cloud gesendet, sodass das ESET-Virenlabor jederzeit einen schnellen und konsistenten Schutz vor Bedrohungen bieten kann. Benutzer können sich direkt im Programmfenster oder im jeweiligen Kontextmenü anzeigen lassen, wie ausgeführte Prozesse oder Dateien eingeschätzt werden. Zudem sind über ESET LiveGrid® weitere Informationen verfügbar.

Bei der [Remote-Bereitstellung von ESET Endpoint Antivirus for Linux über ESET Security Management Center](#) können Sie eine der folgenden Optionen für den cloudbasierten Schutz konfigurieren:

- Sie haben die Möglichkeit, ESET LiveGrid® nicht zu aktivieren. Die Funktionalität in der Software geht nicht verloren, in einigen Fällen reagiert ESET Endpoint Antivirus for Linux jedoch möglicherweise langsamer auf neue Bedrohungen als ein Update der Datenbank der Malware Scan Engine.
- Sie können ESET LiveGrid® so konfigurieren, dass Informationen über neue Bedrohungen und Fundstellen von gefährlichem Code übermittelt werden. Diese Datei kann zur detaillierten Analyse an ESET gesendet werden. Durch die Untersuchung dieser Bedrohungen kann ESET die Fähigkeit seiner Software zur Erkennung von Schadsoftware aktualisieren und verbessern.

ESET LiveGrid® sammelt Daten über neue Bedrohungen, die auf Ihrem Computer erkannt wurden. Dazu können auch Proben oder Kopien der Datei gehören, in der eine Bedrohung aufgetreten ist, der Pfad zu dieser Datei, der Dateiname, Datum und Uhrzeit, der Prozess, über den die Bedrohung auf Ihrem Computer in Erscheinung getreten ist, und Informationen zum Betriebssystem des Computers.

ESET Endpoint Antivirus for Linux ist standardmäßig so konfiguriert, dass verdächtige Dateien zur Analyse an ESET eingereicht werden. Dateien mit bestimmten Erweiterungen (z. B. *.doc* oder *.xls*) sind immer von der Übermittlung ausgeschlossen. Sie können andere Dateierweiterungen hinzufügen, wenn es bestimmte Dateitypen

gibt, die Sie oder Ihr Unternehmen nicht übermitteln möchten.

## ESET LiveGrid®-Reputationssystem aktivieren (empfohlen)

Das ESET LiveGrid®-Reputationssystem verbessert die Wirksamkeit der ESET-Sicherheitslösungen, indem es gescannte Dateien mit Positiv- und Negativlisten in einer Datenbank in der Cloud vergleicht.

## ESET LiveGrid®-Feedbacksystem aktivieren (empfohlen)

Die Daten werden zur weiteren Analyse an das ESET-Virenlabor übermittelt.

## Absturzberichte und Diagnosedaten senden

Reichen Sie Daten wie Absturzberichte, Module und Arbeitsspeicherdumps ein.

## Anonyme Nutzungsstatistiken senden

Ermöglicht ESET die Erfassung von Informationen über neu erkannte Bedrohungen wie Name, Datum und Uhrzeit der Erkennung, Erkennungsmethode und verknüpfte Metadaten, gescannte Dateien (Hash, Dateiname, Ursprung der Datei, Telemetrie), gesperrte oder verdächtige URLs und die Produktversion und -konfiguration, einschließlich Daten zum System.

## E-Mail-Adresse für Rückfragen (optional)

Sie können mit den verdächtigen Dateien eine E-Mail-Adresse für Rückfragen angeben, wenn zur Analyse weitere Informationen erforderlich sind. Beachten Sie, dass Sie nur dann eine Antwort von ESET erhalten, wenn weitere Informationen von Ihnen benötigt werden.

 [Samples einreichen](#)

## Infizierte Samples einreichen

Diese Option sendet alle infizierten Proben zur Analyse und Verbesserung der zukünftigen Erkennung an ESET.

- Alle infizierten Proben
- Alle Proben mit Ausnahme von Dokumenten
- Nicht übermitteln

## Verdächtige Samples einreichen

Verdächtige Dateien mit möglichen Bedrohungen und/oder Dateien mit ungewöhnlichen Eigenschaften oder Verhaltensweisen werden zur Analyse an ESET gesendet.

- **Ausführbar** - Ausführbare Dateien: *.exe, .dll, .sys*
- **Archive** - Archivdateien: *.zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab*
- **Skripts** - Skriptdateien: *.bat, .cmd, .hta, .js, .ps1*
- **Andere** - Andere Dateitypen: *.jar, .reg, .msi, .swf, .lnk*
- **Dokumente** - Dokumente, die in Microsoft Office, Libre Office oder anderen Office-Tools erstellt wurden, oder PDFs mit aktiven Inhalten.

## Ausschlussfilter

Klicken Sie auf Bearbeiten neben „Ausschlussfilter“ in ESET LiveGrid®, um festzulegen, wie Bedrohungen zur

Analyse an ESET gesendet werden.

## Maximalgröße für Proben (MB)

Definiert die maximale Größe der zu scannenden Proben.

# Malware-Prüfungen

Dieser Abschnitt enthält Optionen für die Auswahl von Scanparametern für den **On-Demand-Scan**.

## Ausgewähltes Profil

Diese Parameter werden vom On-Demand-Scanner und beim Scan des Systemstartbereichs verwendet. Sie können eines der vordefinierten Scanprofile verwenden oder ein neues Profil erstellen. Die Scanprofile verwenden jeweils unterschiedliche [Parameter für das ThreatSense-Modul](#).

## Profilliste

Klicken Sie auf **Bearbeiten**, um ein neues Profil zu erstellen. Geben Sie einen Namen für das Profil ein und klicken Sie auf **Hinzufügen**. Das neue Profil wird im Dropdownmenü **Ausgewähltes Profil** neben den vorhandenen Scanprofilen angezeigt.

# Shared local cache

Der freigegebene lokale ESET-Cache verbessert die Leistung in virtualisierten Umgebungen, indem er doppelte Prüfungen im Netzwerk vermeidet. Somit wird jede Datei nur einmal gescannt und im gemeinsamen Cache gespeichert. Durch Aktivieren der Caching-Option werden Informationen zu Scans von Dateien und Ordnern im Netzwerk im lokalen Cache gespeichert. Beim nächsten Scan sucht ESET Endpoint Antivirus for Linux nach gescannten Dateien im Cache. Übereinstimmende Dateien werden vom Scan ausgeschlossen.

Die Einstellungen für den Cache-Server umfassen Folgendes:

- Hostname - Name oder IP-Adresse des Computers, auf dem sich der Cache befindet.
- Port - Nummer des für die Kommunikation verwendeten Ports (mit der im gemeinsam genutzten lokalen Cache festgelegten identisch).
- Passwort - Bei Bedarf können Sie ein Passwort für den gemeinsamen lokalen Cache festlegen.

# ThreatSense-Parameter

ThreatSense ist eine Technologie, die verschiedene Methoden zur Erkennung von Bedrohungen verwendet. Die Technologie arbeitet proaktiv, d. h. sie schützt das System auch während der ersten Ausbreitung eines neuen Angriffs. Eingesetzt wird eine Kombination aus Code-Analyse, Code-Emulation, allgemeinen Signaturen und Virussignaturen verwendet, die zusammen die Systemsicherheit deutlich erhöhen. Die Prüffengine kann verschiedene Datenströme gleichzeitig kontrollieren und so die Effizienz und Erkennungsrate steigern. Die ThreatSense-Technologie entfernt auch erfolgreich Rootkits.

in den Einstellungen für ThreatSense können Sie verschiedene Prüfparameter festlegen:

- Dateitypen und -erweiterungen, die geprüft werden sollen
- Die Kombination verschiedener Erkennungsmethoden
- Säuberungsstufen usw.

[Verwenden Sie ESET Security Management Center](#), um die Konfiguration zu ändern. Wählen Sie eines der unten erwähnten Module aus, und klicken Sie auf **ThreatSense-Parameter**. Verschiedene Sicherheitsszenarien erfordern unterschiedliche Konfigurationen. Daher können Sie ThreatSense für die folgenden Schutzmodule individuell konfigurieren:

- Echtzeit-Dateischutz
- Malware-Scans
- Remote-Scans

ThreatSense-Parameter sind für jedes Modul optimal eingerichtet. Eine Veränderung der Einstellungen kann den Systembetrieb spürbar beeinträchtigen. Änderungen an den Einstellungen für das Prüfen laufzeitkomprimierter Dateien oder die Aktivierung der Advanced Heuristik im Modul „Echtzeit-Dateischutz“ können das System verlangsamen (normalerweise werden mit diesen Methoden nur neu erstellte Dateien geprüft).

## Zu prüfende Objekte

In diesem Bereich können Sie festlegen, welche Dateien und Komponenten Ihres Computers auf Schadcode gescannt werden sollen.

**Bootsektoren/UEFI** - Scan von Bootsektoren/UEFI auf Viren im Master Boot Record.

**E-Mail-Dateien** - Folgende Erweiterungen werden vom Programm unterstützt: DBX (Outlook Express) und EML.

**Archive** – Das Programm unterstützt die folgenden Erweiterungen: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE und viele andere.

**Selbstentpackende Archive** – Selbstentpackende Archive (SFX) sind Archivdateien, die sich selbst extrahieren können

**Laufzeitkomprimierte Dateien** - Im Unterschied zu Standardarchiven werden laufzeitkomprimierte Dateien nach dem Starten im Arbeitsspeicher dekomprimiert. Neben statischen laufzeitkomprimierten Dateiformaten (UPX, yoda, ASPack, FSG usw.) kann die Prüfung durch Code-Emulation viele weitere SFX-Typen erkennen



Der Echtzeit-Dateischutz scannt den Inhalt von Archivdateien nicht. Beim Herunterladen auf die Festplatte wird der Inhalt bestimmter selbstentpackender Archive gescannt.

## Prüfungseinstellungen

Wählen Sie die Methoden aus, mit denen das System auf Infiltrationen gescannt werden soll. Die folgenden Optionen stehen zur Verfügung:

**Heuristik** - Als heuristische Methoden werden Verfahren bezeichnet, die (böartige) Aktivitäten von Programmen analysieren. Auf diese Weise können auch böartige Programme erkannt werden, die noch nicht in der Erkennungsroutine verzeichnet sind. Nachteilig ist, dass es in Einzelfällen zu Fehlalarmen kommen kann

**Advanced Heuristik/DNA-Signaturen** - Advanced Heuristik sind besondere heuristische Verfahren, die von ESET entwickelt wurden, um Würmer, Trojaner und Schadprogramme besser zu erkennen, die in höheren Programmiersprachen geschrieben wurden. Mit Advanced Heuristik werden die Fähigkeiten von ESET-

Produkten zur Erkennung von Bedrohungen beträchtlich gesteigert. Mit Hilfe von Signaturen können Viren zuverlässig erkannt werden. Mit automatischen Updates sind Signaturen für neue Bedrohungen innerhalb weniger Stunden verfügbar. Nachteilig an Signaturen ist, dass mit ihrer Hilfe nur bekannte Viren und gering modifizierte Varianten bekannter Viren erkannt werden können

**Potenziell unerwünschte Anwendungen** - Siehe [potenziell unerwünschte Anwendungen](#) in unserem Glossar.

**Potenziell unsichere Anwendungen** - siehe [potenziell unsichere Anwendungen](#) in unserem Glossar.

## Ausschlussfilter

Die Erweiterung ist der Teil des Dateinamens nach dem Punkt. Die Erweiterung definiert den Typ und den Inhalt einer Datei. In diesem Teil der ThreatSense-Einstellungen können Sie die Dateitypen festlegen, die nicht gescannt werden sollen.

## Sonstige

Bei der Konfiguration der Einstellungen für ThreatSense für eine On-Demand-Prüfung des Computers sind folgende Optionen im Abschnitt **Sonstige** verfügbar:

**Alternative Datenströme (ADS) prüfen** - Bei den von NTFS-Dateisystemen verwendeten alternativen Datenströmen (ADS) handelt es sich um Datei- und Ordnerzuordnungen, die mit herkömmlichen Prüftechniken nicht erkannt werden können. Eindringene Schadsoftware tarnt sich häufig als alternativer Datenstrom, um nicht erkannt zu werden

**Hintergrundprüfungen mit geringer Priorität ausführen** - Jede Prüfung nimmt eine bestimmte Menge von Systemressourcen in Anspruch. Wenn Sie mit ressourcenintensiven Anwendungen arbeiten, können Sie eine Hintergrundprüfung mit geringer Priorität aktivieren, um Ressourcen für die Anwendungen zu sparen

**Alle Objekte in Log aufnehmen** - Wenn Sie diese Option aktivieren, werden alle geprüften Dateien im Log eingetragen, inklusive der Dateien, bei denen keine Bedrohung erkannt wurde. Wenn beispielsweise in einem Archiv Schadcode gefunden wird, enthält das Log auch die in diesem Archiv enthaltenen nicht infizierten Dateien.

**Smart-Optimierung aktivieren** - Wenn die Smart-Optimierung aktiviert ist, werden die optimalen Einstellungen verwendet, um die effizienteste Prüfung bei höchster Geschwindigkeit zu gewährleisten. Die verschiedenen Schutzmodule führen eine intelligente Prüfung durch. Dabei verwenden sie unterschiedliche Prüfmethode für die jeweiligen Dateitypen. Wenn die Smart-Optimierung deaktiviert ist, werden nur die benutzerdefinierten Einstellungen im ThreatSense-Kern der entsprechenden Module für die Prüfung verwendet.

**Datum für „Geändert am“ beibehalten** - Aktivieren Sie diese Option, um den Zeitpunkt des ursprünglichen Zugriffs auf geprüfte Dateien beizubehalten (z. B. für die Verwendung mit Datensicherungssystemen), anstatt ihn zu aktualisieren

## Grenzen

Im Bereich „Grenzen“ können Sie die Maximalgröße von Elementen und Stufen verschachtelter Archive festlegen, die geprüft werden sollen:

## Einstellungen für Objektprüfung

**Maximale Objektgröße** - Definiert die Maximalgröße der zu prüfenden Elemente. Der aktuelle Virenschutz prüft dann nur die Elemente, deren Größe unter der angegebenen Maximalgröße liegt. Diese Option sollte

nur von fortgeschrittenen Benutzern geändert werden, die bestimmte Gründe dafür haben, dass größere Elemente von der Prüfung ausgeschlossen werden. Der Standardwert ist unbegrenzt

**Maximale Scanzzeit pro Objekt (Sek.)** - Definiert die maximale Dauer für die Prüfung eines Elements. Wenn hier ein benutzerdefinierter Wert eingegeben wurde, beendet der Virenschutz die Prüfung eines Elements, sobald diese Zeit abgelaufen ist, und zwar ungeachtet dessen, ob die Prüfung abgeschlossen ist oder nicht. Der Standardwert ist unbegrenzt

## Einstellungen für Archivprüfung

**Verschachtelungstiefe bei Archiven** - Legt die maximale Tiefe der Virenprüfung von Archiven fest. Der Standardwert ist 10

**Maximalgröße von Dateien im Archiv** - Hier können Sie die maximale Dateigröße für Dateien in (extrahierten) Archiven festlegen, die geprüft werden sollen. Der Standardwert ist unbegrenzt



### Hinweis

Die Standardwerte sollten nicht geändert werden; unter normalen Umständen besteht dazu auch kein Grund.

## Zusätzliche ThreatSense-Parameter

Das Infektionsrisiko für neu erstellte oder geänderte Dateien ist vergleichsweise größer als für vorhandene Dateien. Daher prüft das Programm solche Dateien mit zusätzlichen Scanparametern. Zusätzlich zu den üblichen Prüfmethode auf Signaturbasis wird die Advanced Heuristik verwendet. Diese Methode erkennt neue Bedrohungen, bevor ein Update des Moduls veröffentlicht wird. Neben neu erstellten Dateien werden auch selbstentpackende Archive (.sfx) und Laufzeit-Packprogramme (intern komprimierte, ausführbare Dateien) gescannt. In den Standardeinstellungen werden Archive unabhängig von ihrer eigentlichen Größe bis zur 10. Verschachtelungstiefe geprüft. Deaktivieren Sie die Option **Standardeinstellungen Archivprüfung**, um die Archivprüfeinstellungen zu ändern.

## Update

Der **Updatetyp** ist standardmäßig auf **Reguläres Update**. Mit dieser Einstellung werden die Datenbank der Erkennungsroutine und die Produktmodule automatisch täglich von den [ESET-Updateservern](#) aktualisiert.

Pre-Release-Updates enthalten die aktuellsten Bugfixes und/oder Erkennungsmethoden, die demnächst für die allgemeine Öffentlichkeit bereitgestellt werden. Diese Updates sind jedoch nicht immer stabil und sollten daher nicht in Produktionsumgebungen eingesetzt werden.

Diese Option führt Updates über besondere Update-Server aus, die neue Versionen der Signaturdatenbank mit einer Verzögerung von mindestens X Stunden zur Verfügung stellen. Die Datenbanken wurden also bereits in einer Produktionsumgebung getestet und sind daher stabil.

Falls ein ESET Endpoint Antivirus for Linux-Update nicht stabil ist, können Sie das Modul-Update auf einen vorherigen Zustand zurücksetzen. Führen Sie den entsprechenden Befehl in einem Terminalfenster aus, oder führen Sie einen [Rollback mit ESET Security Management Center](#) aus.

Sie können zwei alternative Updatequellen definieren: einen primären und einen sekundären Server.

# Medienkontrolle

ESET Endpoint Antivirus for Linux (EEAU) bietet Methoden zur automatischen Prüfung von Geräten (CD/DVD/USB/...). Mit diesem Modul können Sie erweiterte Filter- und Berechtigungseinstellungen blockieren oder anpassen und definieren, wie ein Benutzer auf diese Geräte zugreifen und mit ihnen arbeiten kann. Dies ist sinnvoll, wenn ein Administrator verhindern möchte, dass die Benutzer Geräte mit unerwünschten Inhalten verwenden.



## Mögliche Schäden am Dateisystem

Wenn Sie eine Policy mit Blockieren/schreibgestützter Aktion auf bereits verbundene Geräte anwenden, während Daten geschrieben oder gelesen werden, können Schäden am Dateisystem auftreten, da Elemente zwangsweise entfernt werden.



## Policy ersetzen

Wenn mehrere Policies mit Regeln für die Medienkontrolle auf eine EEAU-Instanz angewendet werden, ersetzt die zuletzt angewendete Policy die Regeln der vorherigen Policies.

## Unterstützte externe Geräte:

- [Per USB verbundene Speichergeräte](#)
- Interne CD/DVD-Laufwerke

Sie können die Medienkontrolle in ESET Security Management Center (ESMC) im Abschnitt [Policies](#) aktivieren und konfigurieren.

1. Klicken Sie in ESET Security Management Center auf **Policies** > **Neue Policy** und geben Sie einen Namen für die Policy ein.
2. Klicken Sie auf **Einstellungen**, und wählen Sie **ESET Endpoint for Linux (V7+)** im Dropdownmenü aus.
3. Navigieren Sie zur **Medienkontrolle**.
4. Klicken Sie auf den Umschalter neben **Systemintegration**.
5. Klicken Sie auf **Bearbeiten** neben dem entsprechenden Element, um [Regeln](#) und [Gruppen](#) zu konfigurieren.
6. Navigieren Sie zu **Zuweisen**, klicken Sie auf **Zuweisen** und wählen Sie die gewünschte Gruppe von Computern aus.
7. Klicken Sie auf **OK** und dann auf **Fertig stellen**.

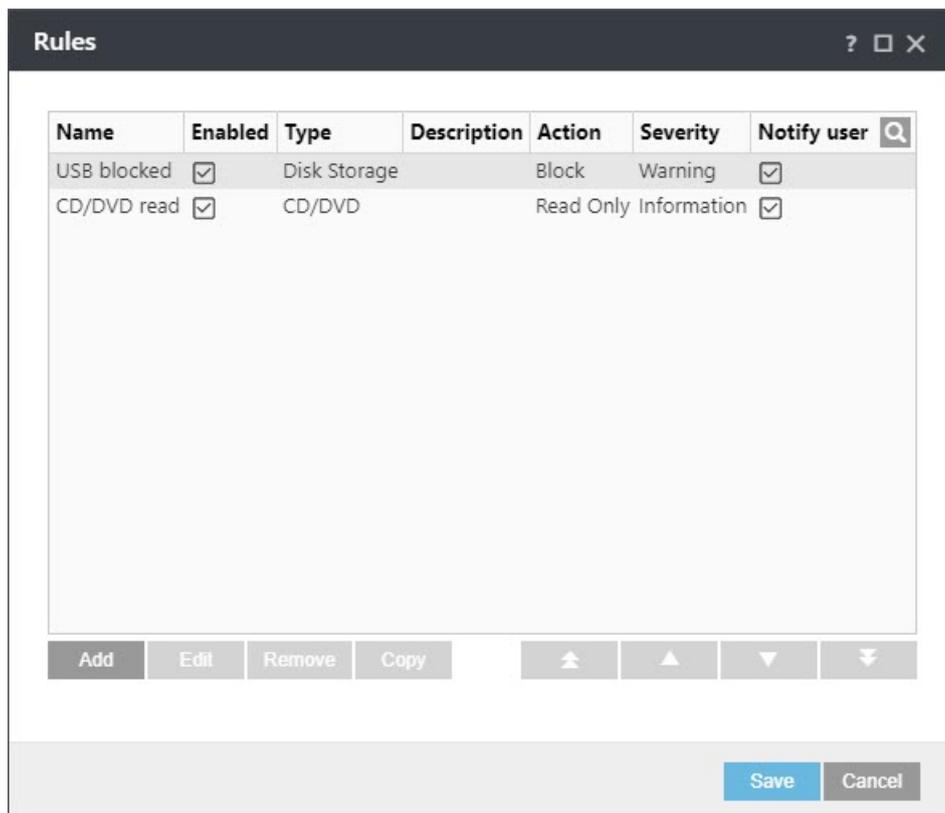
[Weitere Informationen zum Verwalten von Endpoint-Sicherheitsprodukten mit ESMC.](#)

Wenn ein von einer bestehenden Regel blockiertes Gerät angeschlossen oder eingefügt wird, wird ein Hinweisfenster angezeigt und der Zugriff auf das Gerät wird blockiert.

 Device Control  
Device Disk Storage (ADATA USB Flash Drive) is blocked.

## Regel-Editor für die Medienkontrolle

Im **Regel-Editor für die Medienkontrolle** in [ESMC](#) können Sie bestehende Regeln anzeigen und präzise Regeln für [unterstützte externe Geräte](#) erstellen, die Benutzer an den Computer anschließen.



Bestimmte Gerätetypen können auf Grundlage von Parametern in der Regelkonfiguration zugelassen oder gesperrt werden. Die Liste der Regeln enthält verschiedene Regelbeschreibungen wie Regelname, Art des externen Geräts und auszuführende Aktion beim Anschließen eines externen Geräts an Ihren Computer.

Klicken Sie zum Bearbeiten von Regeln auf **Hinzufügen** oder **Bearbeiten**. Deaktivieren Sie neben einer Regel das Kontrollkästchen **Aktiviert**, um die Regel zu deaktivieren, bis Sie sie später verwenden möchten. Wählen Sie eine oder mehrere Regeln aus und klicken Sie auf **Löschen**, um die Regel(n) dauerhaft zu löschen.

Klicken Sie auf **Kopieren**, um eine Kopie der ausgewählten Regel zu erstellen.

Die Regeln sind nach absteigender Priorität geordnet (Regeln mit höchster Priorität werden an oberster Stelle angezeigt). Sie können die Regeln durch Klicken auf     Anfang/Aufwärts/Abwärts/Ende einzeln oder in Gruppen verschieben.

Im Log der Medienkontrolle werden alle ausgelösten Vorkommnisse der Medienkontrolle aufgezeichnet.

### Attribute der verbundenen Geräte

Um die Attribute der Geräte aufzulisten, die mit dem Computer verbunden sind, auf dem ESET Endpoint Antivirus

for Linux installiert ist, [führen](#) Sie das Hilfsprogramm `lsdev` in einem Terminalfenster oder in [ESMC](#) aus.

Syntax: `/opt/eset/eea/bin/lsdev[OPTIONEN]`

Optionen - Kurzform	Optionen - Langform	Beschreibung
-l	--list	Liste der verbundenen Geräte anzeigen
-c	--csv	Liste der verbundenen Geräte im csv-Format anzeigen
-h	--help	Hilfe anzeigen und beenden
-v	--version	Versionsinformationen anzeigen und beenden

## Gerätegruppen

Das Fenster „Gerätegruppen“ ist in zwei Bereiche unterteilt. Im rechten Bereich des Fensters wird eine Liste der Geräte angezeigt, die zur jeweiligen Gruppe gehören. Links werden die erstellten Gruppen angezeigt. Wählen Sie eine Gruppe mit einer Liste von Geräten aus, die Sie rechts anzeigen möchten.

Wenn Sie das Fenster „**Gerätegruppen**“ öffnen und eine Gruppe auswählen, können Sie Geräte zur Liste hinzufügen oder daraus entfernen. Sie können Geräte auch über eine Datei importieren, um sie zur Gruppe hinzuzufügen.

### Steuerelemente

**Hinzufügen**– Sie können eine Gruppe durch Eingabe ihres Namens hinzufügen oder einer vorhandenen Gruppe ein Gerät hinzufügen (optional können Sie auch Details wie Herstellername, Modell und Seriennummer eingeben).

**Bearbeiten**– Bearbeiten Sie die ausgewählte Gruppe oder die Geräteparameter (Hersteller, Modell, Seriennummer).

**Löschen** – Löschen Sie eine ausgewählte Gruppe oder ein Gerät.

**Importieren**– Importieren Sie eine Geräteliste aus einer Datei.

Klicken Sie auf **OK**, wenn Sie die Bearbeitung abgeschlossen haben. Klicken Sie auf **Abbrechen**, wenn Sie das Fenster **Gerätegruppen** schließen möchten, ohne die Änderungen zu speichern.

## Hinzufügen von Regeln für die Medienkontrolle

Eine Regel für die Medienkontrolle definiert die auszuführende Aktion, wenn ein Gerät an den Computer angeschlossen wird, das die Regelkriterien erfüllt.

Geben Sie zur leichteren Identifizierung der Regel eine Beschreibung in das Feld **Name** ein. Mit dem Umschalter neben **Regel aktiviert** können Sie die Regel aktivieren bzw. deaktivieren. Dies ist beispielsweise nützlich, wenn Sie eine Regel deaktivieren, jedoch nicht dauerhaft löschen möchten.

## Gerätetyp

Wählen Sie den externen Gerätetyp im Dropdownmenü aus:

- **Datenträgerspeicher** – Gilt für alle per USBangeschlossenen Geräte, inklusive externe CD/DVD-Laufwerke und herkömmliche Speicherkartenleser
- **CD/DVD** – Gilt für interne CD/DVD-Laufwerke, die per IDE oder SATA angeschlossen sind
- **Alle Geräte** – Gilt für alle oben genannten Typen

Die Informationen zum Gerätetyp werden vom Betriebssystem erfasst. [Verwenden Sie das Hilfsprogramm „lsdev“, um die verbundenen Geräte und deren Attribute aufzulisten.](#)

Diese Geräte stellen nur Informationen zu den eigenen Aktionen bereit, keine Benutzerinformationen. Daher können sie nur global blockiert werden.

## Aktion

Der Zugriff auf andere Geräte als Speichergeräte kann entweder zugelassen oder gesperrt werden. Im Gegensatz dazu ist es für Speichergeräte möglich, eines der folgenden Rechte für die Regel auszuwählen:

- **Lese-/Schreibzugriff** - Vollständiger Zugriff auf das Gerät
- **Blockieren** - Zugriff auf das Gerät wird gesperrt
- **Nur Lesezugriff** - Nur Lesezugriff auf das Gerät

Wählen Sie unter **Kriterientyp** entweder **Gerät** oder **Gerätegruppe** aus.

Weitere Parameter zur Feinanpassung der Regeln und Anpassung an bestimmte Geräte. (die Groß-/Kleinschreibung muss nicht beachtet werden):

- **Hersteller**– Filtern Sie die Liste nach Herstellername oder -ID.
- **Modell**– Die Bezeichnung des Geräts.
- **Seriennummer** - Externe Geräte verfügen üblicherweise über eigene Seriennummern. Bei CDs/DVDs bezieht sich die Seriennummer auf das Exemplar, nicht auf das Laufwerk.



### Hinweis

Wenn diese Parameter nicht definiert werden, ignoriert die Regel diese Felder bei der Suche nach Übereinstimmungen. Bei Filterparametern mit Textfeldern wird die Groß-/Kleinschreibung nicht beachtet. Platzhalter (\*, ?) werden nicht unterstützt.



### Medienkontrollenlogs

Um Informationen zu einem Gerät anzuzeigen, erstellen Sie eine Regel für den entsprechenden Gerätetyp, schließen Sie das Gerät an den Computer an und überprüfen Sie dann die Gerätedetails mit dem Befehlszeilen-Hilfsprogramm [lslog](#) und dem Parameter `-l` oder `--device-control`.

## Logging-Schweregrad

- **Informationen**– Meldungen wie erfolgreiche Updates und alle Meldungen höherer Stufen werden protokolliert.
- **Warnungen**– Erfasst kritische Fehler und Warnungen und sendet sie an den ESET Security Management Center.

## Tools

Im Abschnitt **Tools** in der [ESET Endpoint Antivirus for Linux-Konfiguration in ESET Security Management Center](#) können Sie die allgemeine Konfiguration von ESET Endpoint Antivirus for Linux anpassen.

- Details eines [Proxyserver](#)s für die Verbindung zum Internet definieren
- Umgang mit [Log-Dateien](#) konfigurieren

## Proxyserver

ESET Endpoint Antivirus for Linux kann Ihren Proxyserver verwenden, um sich mit dem Internet oder den definierten Updateservern (Mirror) zu verbinden. Um die Parameter anzupassen, klicken Sie auf **Einstellungen > Tools > Proxyserver**.

# Log-Dateien

Bearbeiten Sie die Logging-Konfiguration von ESET Endpoint Antivirus for Linux.

## Mindestinformation in Logs

Der Informationsumfang in den Logs legt fest, welche Details in den Log-Dateien für ESET Endpoint Antivirus for Linux erfasst werden.

- **Kritische Warnungen** - Nur kritische Fehler (z. B. „Virenschutz konnte nicht gestartet werden“).
- **Fehler** - Fehler wie „Fehler beim Herunterladen der Datei“ und kritische Fehler werden aufgezeichnet.
- **Warnungen** - Kritische Fehler, Warnungen und Fehler werden protokolliert.
- **Informationen** - Meldungen wie erfolgreiche Updates und alle Meldungen höherer Stufen werden protokolliert.
- **Diagnosedaten** - Alle Meldungen höherer Stufen und alle sonstigen Informationen, die für das Beheben von Fehlern wichtig sein können, werden protokolliert.

## Einträge automatisch löschen, die älter sind als (Tage)

Um Log-Einträge, die älter als die ausgewählte Anzahl an Tagen sind, in der Log-Liste (`lslog`), auszublenden, aktivieren Sie den Schalter **Einträge automatisch löschen, die älter sind als (Tage)**. Passen Sie das Alter an, ab dem die Dateien ausgeblendet werden sollen, und klicken Sie auf **Speichern**.

Die ausgeblendeten Logs können nicht wieder angezeigt werden. Log-Einträge aus den On-Demand-Scans werden sofort gelöscht. Aktivieren Sie die automatische Optimierung von Log-Dateien, um zu vermeiden, dass sich ausgeblendete Logs ansammeln.

## Log-Dateien automatisch optimieren

Diese Option defragmentiert die Log-Dateien automatisch, wenn die Fragmentierung höher ist als der unter **Wenn ungenutzte Einträge größer als (%)** angegebene Wert. Ungenutzte Einträge beziehen sich auf ausgeblendete Logs. Klicken Sie zum Defragmentieren der Log-Dateien auf **Optimieren**. Bei diesem Prozess werden alle leeren Log-Einträge gelöscht, um Leistung und Log-Verarbeitung zu verbessern. Eine starke Verbesserung ist insbesondere dann erkennbar, wenn die Logs eine große Anzahl an Einträgen enthalten.

## Syslog Facility

[Syslog Facility](#) ist ein Syslog-Loggingparameter, mit dem Sie ähnliche Log-Nachrichten gruppieren können. Logs von Daemons (die Logs über die Syslog Facility daemon sammeln) können mit der entsprechenden Konfiguration nach `/var/log/daemon.log` geschrieben werden. Mit dem kürzlich erfolgten Wechsel zu systemd und dem entsprechenden Journal hat die Syslog Facility zwar an Bedeutung verloren, aber sie kann weiterhin zum Filtern von Logs verwendet werden.

# Benutzeroberfläche

In diesem Abschnitt de [ESET Endpoint Antivirus for Linux-Konfiguration in ESET Security Management Center](#) können Sie Desktopbenachrichtigungen mit dem Schalter neben **Benachrichtigungen auf dem Desktop anzeigen** ein- und ausschalten. Die Benachrichtigungen sind standardmäßig aktiviert. Diese Benachrichtigungen enthalten Informationen, die kein Eingreifen Ihrerseits erfordern.

## Remoteverwaltung

Um ESET Endpoint Antivirus for Linux remote zu verwalten, verbinden Sie sich vom Computer, auf dem Ihr ESET-Sicherheitsprodukt gehostet ist, mit [ESET Security Management Center](#) (ESMC).

1. [Stellen Sie den ESET Management Agent bereit.](#)
2. [Fügen Sie den Computer zu ESMC hinzu.](#)

Anschließend können Sie passende [Client-Tasks](#) mit ESET Endpoint Antivirus for Linux ausführen.

## Beispielanwendungsfälle

In diesem Kapitel besprechen wir die gängigsten Anwendungsfälle von ESET Endpoint Antivirus for Linux.

## Modulinformationen abrufen

Falls Sie aus irgendeinem Grund Informationen über ein bestimmtes Modul von ESET Endpoint Antivirus for Linux abrufen möchten, führen Sie den folgenden Befehl in einem Terminalfenster aus:

```
grep -asi -A3 "version" /var/opt/eset/eea/lib/Modulname
```



### BEISPIEL

```
grep -asi -A3 "version" /var/opt/eset/eea/lib/em000_64.dat
```

Ausgabe:

```
version: 1074.1 (20190925)  
build: 1133  
date (dd.mm.yyyy): 25.09.2019  
type: loader module
```

Führen Sie die folgenden Befehle in einem Terminalfenster aus, um eine Liste aller ESET Endpoint Antivirus for Linux-Module und deren Versionen anzuzeigen:

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



## BEISPIEL

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

Ausgabe:

EM000	1074.1	(20190925)	Updates
EM001	1558.2	(20191218)	Viren- und Spyware-Schutz
EM002	20708	(20200121)	Malware Scan Engine
EM003	1296	(20191212)	Archivunterstützung
EM004	1197	(20200116)	Advanced Heuristik-Modul
EM005	1205	(20191209)	Säuberungstechnologie
EM017	1780	(20191217)	Lokalisierungsunterstützung
EM022	1110	(20190827)	Datenbankmodul
EM023	15605	(20200121)	Soforteinsatz-Modul
EM029	1026	(20191107)	Modul für Mac/Linux-Unterstützung
EM037	1833B	(20191125)	Konfigurationsmodul

## Scan planen

In Unix-basierten Systemen können Sie cron verwenden, um einen On-Demand-Scan in benutzerdefinierten Intervallen zu planen.

Um einen geplanten Task einzurichten, bearbeiten Sie die cron-Tabelle (crontab) in einem Terminalfenster.

Falls Sie die cron-Tabelle zum ersten Mal bearbeiten, können Sie eine Zahl drücken, um einen Editor auszuwählen. Wählen Sie einen Editor aus, mit dem Sie sich auskennen. Die folgenden Beispiele beziehen sich beim Speichern von Änderungen auf den Editor Nano.

### Umfassenden kompletten Laufwerksscan jeden Sonntag um 2 Uhr morgens planen

1. Um die cron-Tabelle zu bearbeiten, führen Sie den folgenden Befehl in einem Terminalfenster als privilegierter Benutzer aus, der Zugriff auf die zu scannenden Verzeichnisse hat:

```
sudo crontab -e
```

2. Verwenden Sie die Pfeiltasten, um unter den Text in crontab zu navigieren, und geben Sie den folgenden Befehl ein:

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

3. Um die Änderungen zu speichern, drücken Sie CTRL+X, dann die Taste Y und zuletzt die **Eingabetaste**.

### Smart-Scan für einen bestimmten Ordner jeden Abend um 11 Uhr planen

In diesem Beispiel möchten wir den Ordner `/var/www/download/` jeden Abend scannen.

1. Um die cron-Tabelle zu bearbeiten, führen Sie den folgenden Befehl in einem Terminalfenster als privilegierter Benutzer aus, der Zugriff auf die zu scannenden Verzeichnisse hat:

```
sudo crontab -e
```

2. Verwenden Sie die Pfeiltasten, um unter den angezeigten Text in crontab zu navigieren, und geben Sie den folgenden Befehl ein:

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

3. Um die Änderungen zu speichern, drücken Sie CTRL+X, dann die Taste Y und zuletzt die **Eingabetaste**.

## Datei- und Ordnerstruktur

Dieser Abschnitt befasst sich mit der Datei- und Ordnerstruktur von ESET Endpoint Antivirus for Linux, falls Sie vom ESET-Support gebeten werden, Dateien zur Fehlerbehebung abzurufen. Weiter unten finden Sie eine [Liste der Daemons und Befehlszeilenhilfsprogramme](#).

### Basisverzeichnis

Dieses Verzeichnis enthält die Module, die von ESET Endpoint Antivirus for Linux geladen werden und die die Virensignaturdatenbanken enthalten.

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

### Cacheverzeichnis

In diesem Verzeichnis wird der Cache von ESET Endpoint Antivirus for Linux und temporäre Dateien (z. B. Quarantäne-Dateien oder Berichte) gespeichert.

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

### Verzeichnis der Binärdateien

Dieses Verzeichnis enthält die relevanten Binärdateien für ESET Endpoint Antivirus for Linux.

```
/opt/eset/eea/bin
```

Dort finden Sie die folgenden Hilfsprogramme:

- [odscan](#) — Um einen On-Demand-Scan in einem Terminalfenster auszuführen
- [quar](#) - Um die Elemente in der Quarantäne zu verwalten
- [upd](#) - Um Modul-Updates zu verwalten oder Update-Einstellungen zu verwalten

# Verzeichnis der Systembinärdateien

Dieses Verzeichnis enthält die relevanten Systembinärdateien für ESET Endpoint Antivirus for Linux.

`/opt/eset/eea/sbin`

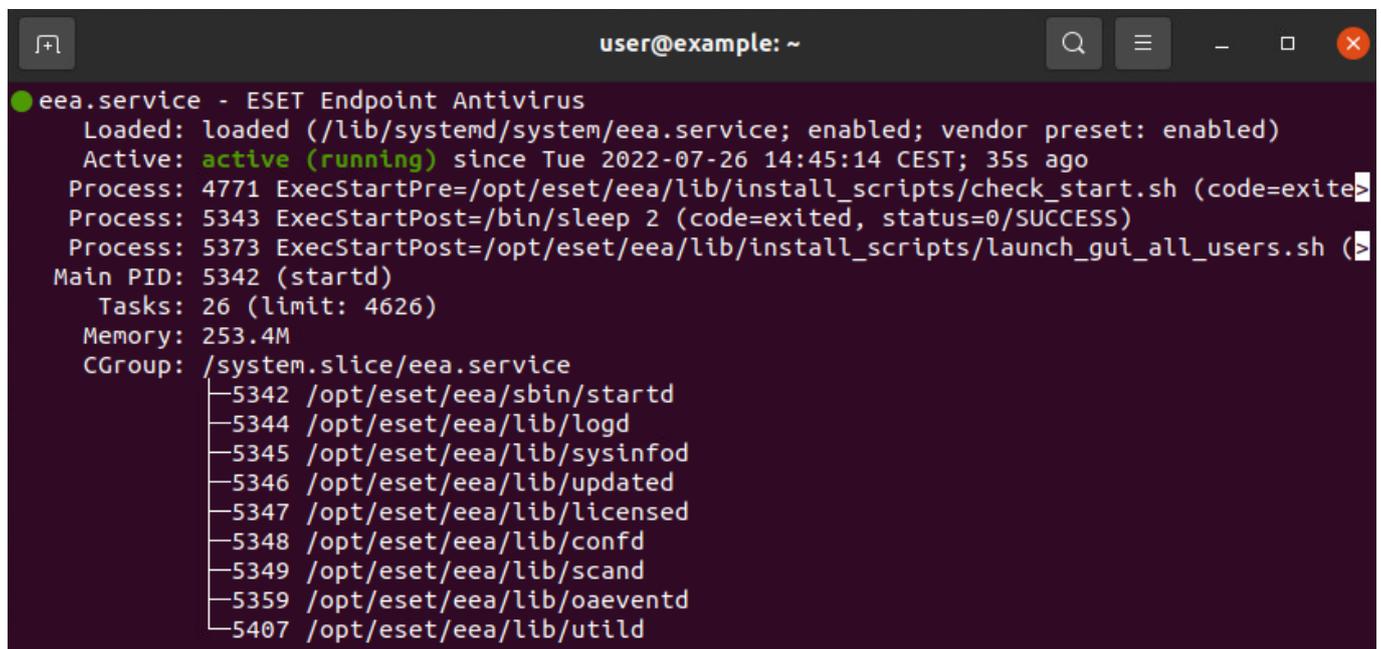
Dort finden Sie die folgenden Hilfsprogramme:

- [collect\\_logs.sh](#) - Um alle wichtigen Logs als Archivdatei im Stammordner des angemeldeten Benutzers zu generieren
- [ecp\\_logging.sh](#) - Um Logs im Zusammenhang mit der Produktaktivierung zu generieren.
- [lic](#) - Für die [Aktivierung von ESET Endpoint Antivirus for Linux](#) mit dem erworbenen Lizenzschlüssel oder um den Aktivierungsstatus und die Gültigkeit der Lizenz zu überprüfen
- [lslog](#) — Zum Anzeigen der von ESET Endpoint Antivirus for Linux gesammelten Logs
- `startd` — Um den ESET Endpoint Antivirus for Linux-daemon manuell zu starten, wenn dieser beendet wurde.

Führen Sie den folgenden Befehl aus mit root-Berechtigungen in einem Terminalfenster aus, um herauszufinden, ob der ESET Endpoint Antivirus for Linux-Dienst aktiv ist:

```
systemctl status eea.service
```

Beispielausgabe von `systemctl`:



```
user@example: ~
● eea.service - ESET Endpoint Antivirus
   Loaded: loaded (/lib/systemd/system/eea.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2022-07-26 14:45:14 CEST; 35s ago
     Process: 4771 ExecStartPre=/opt/eset/eea/lib/install_scripts/check_start.sh (code=exited, status=0/SUCCESS)
     Process: 5343 ExecStartPost=/bin/sleep 2 (code=exited, status=0/SUCCESS)
     Process: 5373 ExecStartPost=/opt/eset/eea/lib/install_scripts/launch_gui_all_users.sh (code=exited, status=0/SUCCESS)
   Main PID: 5342 (startd)
     Tasks: 26 (limit: 4626)
    Memory: 253.4M
    CGroup: /system.slice/eea.service
            └─5342 /opt/eset/eea/sbin/startd
              └─5344 /opt/eset/eea/lib/logd
                └─5345 /opt/eset/eea/lib/sysinfod
                  └─5346 /opt/eset/eea/lib/updated
                    └─5347 /opt/eset/eea/lib/licensed
                      └─5348 /opt/eset/eea/lib/confd
                        └─5349 /opt/eset/eea/lib/scand
                          └─5359 /opt/eset/eea/lib/oaeventd
                            └─5407 /opt/eset/eea/lib/utild
```

## Daemons

- sbin/startd – Haupt-Daemon, startet und verwaltet andere Daemons
- lib/scand – Scanning-Daemon
- lib/oaeventd – Dienst zum Abfangen von Ereignissen beim Zugriff (verwendet das Kernelmodul „eset\_rtp“)
- lib/confd – Konfigurationsverwaltungsdienst
- lib/logd – Logverwaltungsdienst
- lib/licensed – Aktivierungs- und Lizenzierungsdienst
- lib/updated – Modul-Update-Dienst
- lib/execd + lib/odfeeder – Helfer für On-Demand-Scans
- lib/utild – Helfer zum Wiederherstellen der Quarantäne
- lib/sysinfod – BS- und Medienerkennungsdienst

## Kommandozeilenhilfsprogramme

- sbin/[lslog](#) – Hilfsprogramm zum Auflisten von Logs
- bin/[odscan](#) – On-Demand-Scanner
- lib/[cfg](#) – Konfigurationshilfsprogramm
- sbin/[lic](#) – Lizenzierungshilfsprogramm
- bin/[upd](#) – Modul-Update-Hilfsprogramm
- bin/[quar](#) – Hilfsprogramm für die Quarantäneverwaltung

## Fehlerbehebung

Dieser Abschnitt enthält Lösungen für die unten genannten Probleme.

- [Aktivierungsprobleme \(nur auf Englisch\)](#)
- [Verwenden des noexec-Flags](#)
- [Daemon für Echtzeit-Schutz kann nicht gestartet werden](#)
- [Logs sammeln](#)

# Logs sammeln

Wenn der ESET-Support Logs von ESET Endpoint Antivirus for Linux anfordert, können Sie das Skript `collect_logs.sh` unter `/opt/eset/eea/sbin/` verwenden, um diese Logs zu generieren.

Starten Sie das Skript in einem Terminalfenster mit root-Berechtigungen. Führen Sie für Ubuntu beispielsweise den folgenden Befehl aus:

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

Das Skript generiert alle wichtigen Logs als Archivdatei im Stammordner des angemeldeten Benutzers und zeigt den entsprechenden Pfad an. Falls Aktivierungs-Logs verfügbar sind, werden diese ebenfalls gesammelt. Schicken Sie diese Datei per E-Mail an den ESET-Support.

## Aktivierungs-Logs

Für die Behebung von Problemen bei der Produktaktivierung kann der ESET-Support relevante Logs anfordern.

1. Aktivieren Sie den Aktivierungs-Log-Dienst, indem Sie den folgenden Befehl als privilegierter Benutzer ausführen:

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

Alternativ:

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

Mit dem zweiten Befehl können Sie das Produkt bei Bedarf ohne Aufforderung neu starten.

2. Wiederholen Sie den Aktivierungsprozess. Falls ein Fehler auftritt, führen Sie das Log-Sammlungs-Skript als privilegierter Benutzer aus:

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

3. Senden Sie die gesammelten Logs an den ESET-Support.
4. Deaktivieren Sie die Aktivierungs-Logs, indem Sie den folgenden Befehl als privilegierter Benutzer ausführen:

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

Alternativ:

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

Mit dem zweiten Befehl können Sie das Produkt bei Bedarf ohne Aufforderung neu starten.

## Verwenden des noexec-Flags

Falls Sie die Pfade */var* und */tmp* mit dem `noexec`-Flag eingehängt haben, wird die Installation von ESET Endpoint Antivirus for Linux mit der folgenden Fehlermeldung abgebrochen:

```
Invalid value of environment variable MODMAPDIR. Modules cannot be loaded. (Ungültiger Wert der Umgebungsvariable MODMAPDIR. Module können nicht geladen werden.)
```

## Behelfslösung

Die folgenden Befehle werden in einem Terminalfenster ausgeführt.

1. Erstellen Sie einen Ordner mit Ausführungsberechtigungen und dem folgenden Besitzer und Berechtigungssatz:

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

2. Führen Sie den folgenden Befehl aus:

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

- a. Falls SELinux aktiviert ist, legen Sie den Kontext für diesen Ordner fest:

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

3. Kompilieren Sie die wichtigsten Module:

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

4. Legen Sie `MODMAPDIR` in `/usr/lib/systemd/system/eea.service`, indem Sie eine Zeile zum Block `[Service]` hinzufügen:

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

5. Laden Sie die `systemd`-Dienstkonfiguration neu:

```
# systemctl daemon-reload
```

6. Starten Sie den `eea`-Dienst neu:

```
# systemctl restart eea
```

# Echtzeit-Schutz kann nicht gestartet werden

Hier finden Sie eine Demonstration für ein Beispielproblem und eine entsprechende Lösung unter Ubuntu.

## Problem

Der Echtzeit-Schutz kann aufgrund fehlender Kerneldateien nicht gestartet werden.

In `/var/log/messages` wird ein Fehler für ESET Endpoint Antivirus for Linux angezeigt:

```
Oct 15 15:42:30 localhost eea: ESET Endpoint Antivirus error: cannot find kernel sources directory for kernel version 3.10.0-957.el7.x86_64
```

```
Oct 15 15:42:30 localhost eea: ESET Endpoint Antivirus error: please check if kernel-devel (or linux-headers) package version matches the current kernel version
```

```
Oct 15 15:42:30 localhost oaeventd[31471]: ESET Endpoint Antivirus Error: Cannot open file /lib/modules/3.10.0-957.el7.x86_64/eset/eea/eset_rtp.ko: No such file or directory
```

## Lösung

### Methode 1: erfordert einen Neustart des Betriebssystems

1. Aktualisieren Sie die Pakete Ihres Betriebssystems auf die neueste Version. Führen Sie für Ubuntu den folgenden Befehl als privilegierter Benutzer in einem Terminalfenster aus:

```
apt-get update
```

```
apt-get upgrade
```

2. Starten Sie das Betriebssystem neu.

### Methode 2:

1. Installieren Sie die neuesten Kernel-Header für DEB-basierte Linux-Distributionen. Führen Sie unter Ubuntu die folgenden Befehle als privilegierter Benutzer in einem Terminalfenster aus:

```
apt update
```

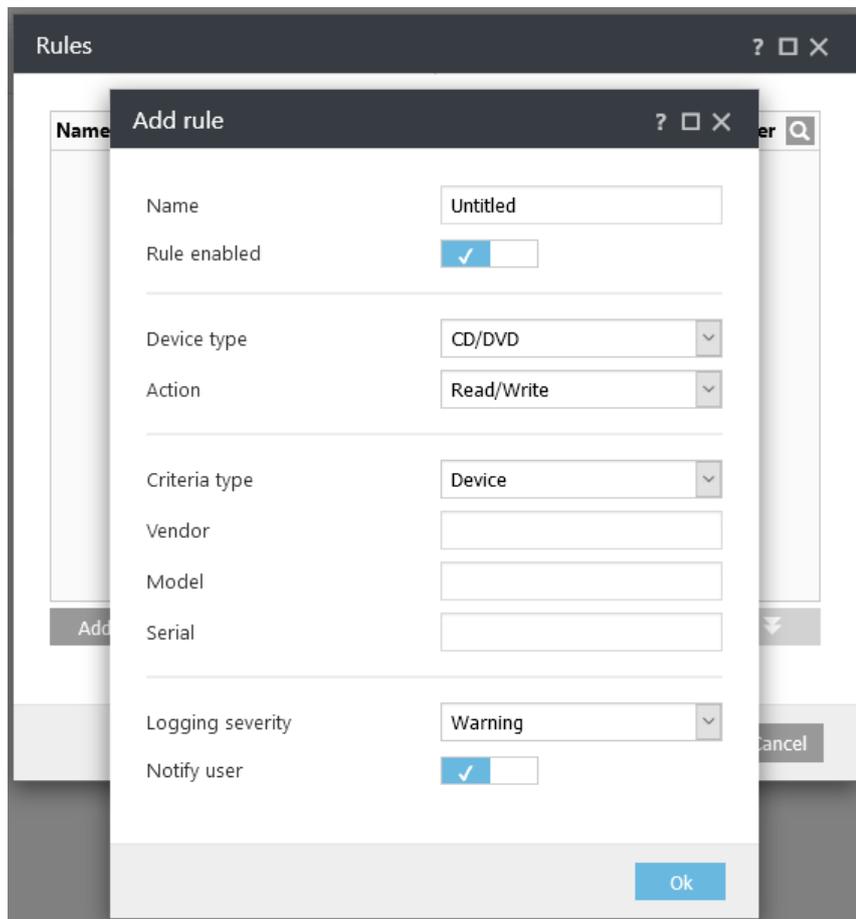
```
apt install linux-headers-$(uname -r)
```

2. Starten Sie den EEA-Dienst neu:

```
systemctl restart eea
```

# Bekannte Probleme

- [Medienkontrolle](#) kann interne CD/DVD-Laufwerke nicht blockieren



## Glossar

- **Daemon:** Eine Art von Programm in Unix-ähnlichen Betriebssystemen, das unbeaufsichtigt im Hintergrund ausgeführt wird anstatt unter der direkten Kontrolle eines Benutzers, und dort durch ein bestimmtes Ereignis oder eine bestimmte Bedingung aktiviert wird.

## Endbenutzer-Lizenzvereinbarung

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

Endbenutzer-Lizenzvereinbarung

Diese Endbenutzer-Lizenzvereinbarung (die "Vereinbarung") zwischen ESET, spol. s r. o., mit Sitz in Einsteinova 24, 851 01 Bratislava, Slovak Republic, Handelsregistereintrag 3586/B in der Rubrik Sro beim Amtsgericht Bratislava I, Firmennummer 31333532, (im Folgenden "ESET" oder "Anbieter") und Ihnen, einer natürlichen oder juristischen Person ("Sie" oder der "Endbenutzer"), berechtigt Sie zur Nutzung der in Abschnitt 1 dieser Vereinbarung

definierten Software. Die in Abschnitt 1 dieser Vereinbarung definierte Software darf unter den im Folgenden aufgeführten Bedingungen auf einem Datenträger gespeichert, per E-Mail versendet, aus dem Internet oder von Servern des Anbieters heruntergeladen oder auf andere Weise beschafft werden.

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

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

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

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

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

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

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

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

**c) Business Edition.** Für die Verwendung der Software auf E-Mail-Servern, E-Mail-Relays, E-Mail- oder Internet-Gateways ist die Business Edition der Software erforderlich.

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

**e) OEM-Software.** OEM-Software darf ausschließlich auf dem Computer genutzt werden, mit dem Sie sie erhalten haben. Eine Übertragung auf einen anderen Computer ist nicht gestattet.

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

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

**4. Funktionen mit Datenerfassung und Anforderungen an die Internetverbindung.** Für den korrekten Betrieb benötigt die Software eine Internetverbindung und muss in der Lage sein, sich in regelmäßigen Abständen mit den Servern des Anbieters, Servern einer Drittpartei und entsprechenden Datenerfassungen gemäß der Datenschutzrichtlinie zu verbinden. Die Verbindung mit dem Internet und den entsprechenden Datenerfassungen ist für die folgenden Funktionen der Software erforderlich:

**a) Software-Updates.** Der Anbieter hat das Recht, von Zeit zu Zeit Aktualisierungen für die Software („Updates“) bereitzustellen, ist hierzu jedoch nicht verpflichtet. Diese Funktion ist in den Standardeinstellungen der Software aktiviert. Die Updates werden also automatisch installiert, sofern der Endbenutzer dies nicht deaktiviert hat. Zur Bereitstellung von Aktualisierungen muss die Echtheit der Lizenz überprüft werden. Dazu gehören Informationen über den Computer und/oder die Plattform, auf der die Software installiert wurde, in Übereinstimmung mit der Datenschutzrichtlinie.

**b) Weiterleitung von eingedrungener Schadsoftware und anderen Informationen an den Anbieter.** Die Software

enthält Funktionen zur Erfassung neuer Computerviren und anderer schädlicher Computerprogramme sowie von verdächtigen, problematischen, potenziell unsicheren Objekten wie Dateien, URLs, IP-Pakete und Ethernet-Rahmen (im Folgenden "Infiltrationen"). Diese Daten werden zusammen mit Informationen über den Installationsprozess und die Plattform, auf der die Software installiert ist, oder anderen Informationen über Betrieb und Funktionsweise der Software (im Folgenden "Informationen") an den Anbieter übertragen. Die Informationen und die Infiltrationen können Daten über den Endbenutzer oder andere Benutzer des Computers enthalten, auf dem die Software installiert ist (inklusive zufällig oder unbeabsichtigt erfasste personenbezogene Daten), sowie von eingedrungener Schadsoftware betroffene Dateien mit den entsprechenden Metadaten.

Die folgenden Funktionen der Software können Informationen und Infiltrationen sammeln:

- i. Das LiveGrid Reputationssystem sammelt und sendet Einweg-Hashes im Zusammenhang mit eingedrungener Schadsoftware an den Anbieter. Diese Funktion ist in den Standardeinstellungen der Software aktiviert.
- ii. Das LiveGrid-Reputationssystem erfasst Infiltrationen und überträgt diese zusammen mit den entsprechenden Metadaten und anderen Informationen an den Anbieter. Diese Funktion kann vom Endbenutzer bei der Installation der Software aktiviert werden.

Der Anbieter verwendet die erhaltenen Informationen und Infiltrationen ausschließlich zur Analyse und Erforschung der Infiltrationen, zur Verbesserung der Software und zur Überprüfung der Echtheit von Lizenzen und unternimmt angemessene Anstrengungen, um die erhaltenen Infiltrationen und Informationen zu schützen. Wenn diese Softwarefunktion aktiviert wird, darf der Anbieter gemäß der Datenschutzrichtlinie und gemäß geltender Gesetze Infiltrationen und Informationen erfassen und verarbeiten. Sie können diese Funktionen jederzeit deaktivieren.

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

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

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

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

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

- a) Sie dürfen eine Kopie der Software auf einem Medium zur dauerhaften Speicherung als Sicherungskopie erstellen, vorausgesetzt die Sicherungskopien werden nicht auf einem anderen Computer installiert oder verwendet. Das Erstellen jeder weiteren Kopie der Software verstößt gegen diese Vereinbarung.
- b) Jegliche von den Bestimmungen dieser Vereinbarung abweichende Nutzung, Modifikation, Übersetzung oder Reproduktion der Software sowie die Einräumung von Rechten zur Nutzung der Software oder von Kopien der Software ist untersagt.
- c) Die Software darf nicht an andere Personen verkauft, sublizenziert oder vermietet werden. Ebenso darf die Software nicht von einer anderen Person gemietet, einer anderen Person ausgeliehen oder zur gewerbsmäßigen Erbringung von Dienstleistungen verwendet werden.
- d) Der Quellcode der Software darf nicht durch Reverse-Engineering analysiert, dekompiert oder disassembliert oder auf andere Weise beschafft werden, soweit eine solche Beschränkung nicht ausdrücklich gesetzlichen Bestimmungen widerspricht.
- e) Sie verpflichten sich, die Software nur in Übereinstimmung mit allen am Verwendungsort geltenden gesetzlichen Bestimmungen zu verwenden, insbesondere gemäß den Beschränkungen, die sich aus dem Urheberrecht und anderen Rechten an geistigem Eigentum ergeben.
- f) Sie verpflichten sich, die Software und ihre Funktionen nur so zu nutzen, dass der Zugriff anderer Endbenutzer auf die betreffenden Dienste nicht eingeschränkt wird. Der Anbieter behält sich das Recht vor, den Leistungsumfang gegenüber einzelnen Endbenutzern einzuschränken, damit die Dienste von möglichst vielen Endbenutzern verwendet werden können. Dies kann auch bedeuten, dass die Nutzung beliebiger Softwarefunktionen vollständig gesperrt wird und dass Daten sowie Informationen im Zusammenhang mit bestimmten Funktionen der Software von den Servern des Anbieters bzw. Dritter gelöscht werden.
- g) Sie verpflichten sich hiermit, keine Aktivitäten im Zusammenhang mit dem Lizenzschlüssel auszuführen, die den Bestimmungen dieser Vereinbarung widersprechen oder die dazu führen, dass der Lizenzschlüssel an unbefugte Personen weitergegeben wird, z. B. durch die Übertragung von benutzten oder nicht benutzten Lizenzschlüsseln in jeglicher Form oder die nicht autorisierte Verteilung von duplizierten oder generierten Lizenzschlüsseln oder die Nutzung der Software im Zusammenhang mit einem Lizenzschlüssel, der aus einer anderen Quelle als direkt vom Anbieter beschafft wurde.

**7. Urheberrecht.** Die Software und alle Rechte einschließlich des Rechtstitels und der geistigen Eigentumsrechte daran sind Eigentum von ESET und/oder seiner Lizenzgeber. Sie unterliegen dem Schutz der Bestimmungen internationaler Abkommen und aller sonstigen geltenden Gesetze des Landes, in dem die Software verwendet wird. Die Struktur, die Aufteilung und der Code der Software sind Geschäftsgeheimnisse und vertrauliche Informationen von ESET und/oder seiner Lizenzgeber. Die Software darf nicht kopiert werden, wobei lediglich die in Abschnitt 6(a) angegebene Ausnahme gilt. Alle gemäß dieser Vereinbarung zulässigen Kopien müssen dieselben Urheberrechts- und Eigentümerhinweise wie die ursprüngliche Software enthalten. Wenn Sie in Verstoß gegen die Bestimmungen dieser Vereinbarung Quellcode durch Reverse-Engineering analysieren, dekompiieren oder disassemblieren oder versuchen, sich den Quellcode auf andere Weise zu beschaffen, gehen automatisch sämtliche dadurch gewonnenen Informationen unwiderruflich und unmittelbar in das Eigentum des Anbieters über. Weiterhin ist der Anbieter in diesem Fall berechtigt, etwaige weitere Ansprüche aus Ihrem Verstoß gegen diese Vereinbarung geltend zu machen.

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

**9. Versionen in verschiedenen Sprachen/auf mehreren Datenträgern, mehrere Exemplare.** Wenn die Software mehrere Plattformen oder Sprachen unterstützt, oder wenn Sie mehrere Exemplare der Software erhalten haben, darf die Software nur auf derjenigen Anzahl von Computern und nur in den Versionen verwendet werden, für die

Sie eine Lizenz erworben haben. Es dürfen keine Versionen oder Kopien der Software, die von Ihnen nicht verwendet werden, an andere Personen verkauft, vermietet, sublizenziert, verliehen oder auf diese übertragen werden.

**10. Beginn und Gültigkeitsdauer der Vereinbarung.** Diese Vereinbarung tritt an dem Tag in Kraft, an dem Sie sich mit ihren Bestimmungen einverstanden erklären. Sie können diese Vereinbarung jederzeit kündigen, indem Sie die Software, alle Sicherungskopien und, falls vorhanden, alle vom Anbieter oder seinen Geschäftspartnern zur Verfügung gestellten zugehörigen Materialien dauerhaft löschen, sie zerstören bzw. auf eigene Kosten zurückgeben. Unabhängig von der Gültigkeitsdauer dieser Vereinbarung und der Art und Weise ihres Ablaufs bzw. ihrer Kündigung behalten die Bestimmungen der Abschnitte 7, 8, 11, 13, 19 und 21 auf unbegrenzte Zeit ihre Gültigkeit.

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

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

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

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

**15. Technischer Support.** ESET bzw. die von ESET beauftragten Dritten erbringen jeglichen technischen Support ausschließlich nach eigenem Ermessen und ohne diesbezügliche Zusicherungen oder Gewährleistungen. Endbenutzer sind verpflichtet, vor der Inanspruchnahme von Supportleistungen eine Sicherungskopie aller vorhandenen Daten, Softwareanwendungen und sonstigen Programme zu erstellen. ESET bzw. die von ESET beauftragten Dritten übernehmen keinerlei Haftung für Datenverluste, Sach- und Vermögensschäden (insb. Schäden an Software und Hardware) oder entgangene Gewinne infolge der Erbringung von Supportleistungen. ESET bzw. die von ESET beauftragten Dritten sichern nicht zu, dass ein bestimmtes Problem auf dem Wege des technischen Support gelöst werden kann, und behalten sich das Recht vor, die Arbeit an einem Problem ggf. einzustellen. ESET behält sich das Recht vor, die Erbringung von Supportleistungen nach eigenem Ermessen vorübergehend auszusetzen, ganz einzustellen oder im konkreten Einzelfall abzulehnen. Für die Bereitstellung des

technischen Supports sind unter Umständen Lizenzinformationen, Informationen und andere Daten gemäß der Datenschutzrichtlinie erforderlich.

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

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

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

#### **19. Einhaltung von Handelskontrollen.**

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

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

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

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

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

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

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

**20. Kündigungen.** Alle Kündigungen sowie zurückgegebene Software und Dokumentation sind an folgende Adresse zu senden: ESET, spol. s r. o., Einsteinova 24, 851 01 Bratislava, Slovak Republic.

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

**22. Allgemeine Bestimmungen.** Wenn eine der Bestimmungen dieser Vereinbarung ungültig oder uneinklagbar ist, beeinträchtigt dies nicht die Gültigkeit der übrigen Bestimmungen der Vereinbarung. Diese bleiben unter den hier festgelegten Bedingungen gültig und einklagbar. Bei Widersprüchen zwischen übersetzten Versionen dieser Vereinbarung hat die englische Version Vorrang. Änderungen an dieser Vereinbarung bedürfen der Schriftform und müssen von einem bevollmächtigten Vertreter des Anbieters unterzeichnet werden.

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

EULA ID: BUS-STANDARD-20-01

## Datenschutzerklärung

ESET, spol. s r. o., mit eingetragenem Firmensitz in Einsteinova 24, 851 01 Bratislava, Slowakei, eingetragen im Handelsregister Bratislava I, Abschnitt Sro, Eintragsnummer 3586/B, Firmenregisternummer 31333532 als Datenverarbeiter („ESET“ oder „Wir“) hat das Ziel, die persönlichen Daten und die Privatsphäre seiner Kunden transparent zu behandeln. Daher veröffentlichen wir diese Datenschutzerklärung mit dem ausschließlichen Ziel, unsere Kunden („Endkunde“ oder „Sie“) über die folgenden Themen zu informieren:

- Verarbeitung persönlicher Daten,
- Vertraulichkeit der Daten,
- Rechte betroffener Personen.

## Verarbeitung persönlicher Daten

Die von ESET angebotenen und in unserem Produkt implementierten Dienste werden unter den Bestimmungen der Endbenutzer-Lizenzvereinbarung („EULA“) bereitgestellt. Einige dieser Dienste erfordern jedoch möglicherweise zusätzliche Aufmerksamkeit. Wir möchten Ihnen weitere Details zur Datensammlung im Zusammenhang mit der Bereitstellung unserer Dienste liefern. Wir bieten verschiedene in der EULA und der Produktdokumentation beschriebene Dienste an, darunter die Upgrade- und Updatedienste, ESET LiveGrid®, den

Schutz vor dem Missbrauch von Daten, Support usw. Für die Erbringung dieser Dienste erfassen wir die folgenden Informationen:

- Update- und sonstige Statistiken und Informationen zum Installationsprozess und Ihrem Computer, z. B. die Plattform, auf der unser Produkt installiert wird, oder Informationen zum Betrieb und Funktionsumfang unserer Produkte wie Betriebssystem, Hardwareinformationen, Installations- und Lizenz-IDs, IP-Adresse, MAC-Adresse und Konfigurationseinstellungen des Produkts.
- Einweg-Hashes für Schadsoftware als Teil unseres LiveGrid®-Reputationssystems, das die Wirksamkeit der Sicherheitslösungen verbessert, indem es gescannte Dateien mit Positiv- und Negativlisten in einer Datenbank in der Cloud vergleicht.
- Verdächtige Samples und Metadaten „aus freier Wildbahn“ als Teil unseres ESET LiveGrid®-Reputationssystems, mit denen ESET unmittelbar auf die Anforderungen unserer Kunden reagieren und sie vor den neuesten Bedrohungen schützen kann. Wir benötigen die folgenden Daten von Ihnen:

- Eingedrungene Schadsoftware, z. B. potenzielle Sample von Viren und anderen Schadprogrammen, sowie verdächtige, problematische, potenziell unerwünschte oder potenziell unsichere Objekte wie ausführbare Dateien oder E-Mail-Nachrichten, die von Ihnen als Spam markiert oder von unserem Produkt markiert wurden;

- Informationen zu Geräten im lokalen Netzwerk wie Art, Hersteller, Modell und/oder Name des Geräts;

- Informationen zur Internetnutzung wie IP-Adresse und geografische Informationen, IP-Pakete, URLs und Ethernet-Frames;

- Absturzabbilder und darin enthaltenen Informationen.

Wir haben kein Interesse daran, Daten außerhalb des genannten Umfangs zu erfassen, allerdings lässt sich dies manchmal nicht vermeiden. Versehentlich erfasste Daten können in der Schadsoftware (ohne Ihr Wissen oder Ihre Zustimmung erfasst) oder als Teil von Dateinamen oder URLs enthalten sein. Es ist nicht unsere Absicht, diese Daten in unseren Systemen oder für die in dieser Datenschutzerklärung genannten Zwecke zu verarbeiten.

- Lizenzinformationen wie die Lizenz-ID und persönliche Daten wie Vor- und Nachname, Adresse und E-Mail-Adresse werden zu Abrechnungszwecken, zur Überprüfung der Echtheit der Lizenz und zur Erbringung unserer Dienste benötigt.
- Kontaktinformationen und andere Daten in Ihren Supportanfragen werden für möglicherweise für die Erbringung von Supportdiensten benötigt. Je nachdem, über welchen Kanal Sie uns kontaktieren, speichern wir möglicherweise Ihre E-Mail-Adresse, Telefonnummer, Lizenzinformationen, Produktdetails und eine Beschreibung Ihres Supportfalls. Möglicherweise werden Sie aufgefordert, uns weitere Informationen bereitzustellen, um die Bearbeitung der Supportanfrage zu erleichtern.

## Vertraulichkeit der Daten

ESET ist ein weltweit operierendes Unternehmen über angeschlossene Unternehmen oder Partner im Rahmen unseres Distributions-, Dienst- und Supportnetzwerks. Die von ESET verarbeiteten Informationen können zur Erbringung der EULA von und zu angeschlossenen Unternehmen übertragen werden, beispielsweise für die Bereitstellung von Diensten, Supportleistungen oder Abrechnungen. Je nach Ihrem Standort und den von Ihnen ausgewählten Diensten müssen wir Ihre Daten unter Umständen in Länder ohne Gleichstellungsbeschluss der Europäischen Kommission übertragen. Selbst in diesem Fall unterliegen alle Datenübertragungen den Datenschutzbestimmungen und finden nur bei Bedarf statt. Übliche Vertragsklauseln, bindende Unternehmensregeln oder andere geeignete Mechanismen müssen ausnahmslos umgesetzt werden.

Wir unternehmen größte Anstrengungen, um zu verhindern, dass Ihre Daten bei der Bereitstellung von Diensten

im Rahmen der EULA länger als notwendig gespeichert werden. Unser Aufbewahrungszeitraum ist unter Umständen länger als die Gültigkeitsdauer Ihrer Lizenz, um Ihnen eine problemlose und komfortable Erneuerung zu ermöglichen. Minimierte und pseudonymisierte Statistiken und sonstige Daten aus ESET LiveGrid® können zu statistischen Zwecken weiterverarbeitet werden.

ESET implementiert angemessene technische und organisatorische Maßnahmen, um einen angemessenen Schutz vor potenziellen Risiken zu bieten. Wir bemühen uns nach Kräften, die fortlaufende Vertraulichkeit, Integrität, Verfügbarkeit und Ausfallsicherheit der Verarbeitungssysteme und Dienste zu gewährleisten. Falls jedoch Ihre Rechte und Freiheiten durch einen Datenangriff gefährdet sind, müssen wir die Aufsichtsbehörden sowie die betroffenen Personen informieren. Betroffene Personen haben das Recht, Beschwerde bei einer Aufsichtsbehörde einzulegen.

## Rechte betroffener Personen

ESET unterliegt slowakischem Recht und ist als Teil der Europäischen Union an die Datenschutzgesetze gebunden. Im Rahmen der geltenden Datenschutzgesetze haben Sie als betroffene Person die folgenden Rechte:

- das Recht, Ihre persönlichen Daten von ESET anzufordern,
- das Recht, Ihre persönlichen Daten bei Bedarf zu berichtigen (Sie haben auch das Recht, unvollständige persönliche Daten zu vervollständigen),
- das Recht, die Löschung Ihrer persönlichen Daten anzufordern,
- das Recht, eine Einschränkung der Verarbeitung Ihrer persönlichen Daten anzufordern,
- Einlegen von Einspruch gegen die Verarbeitung
- Einlegen von Beschwerden sowie
- das Recht auf Übertragbarkeit der Daten.

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

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