

# ESET Cyber Security

## Benutzerhandbuch

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



Copyright ©2023 by ESET, spol. s r.o.

ESET Cyber Security 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 ESET Cyber Security .....	1
<b>1.1 Neuerungen in Version 6</b> .....	1
<b>1.2 Systemanforderungen</b> .....	1
2 Installation .....	2
<b>2.1 Standardinstallation</b> .....	2
<b>2.2 Benutzerdefinierte Installation</b> .....	4
<b>2.3 Systemerweiterungen erlauben</b> .....	5
<b>2.4 Vollständigen Laufwerkszugriff erlauben</b> .....	6
3 Produktaktivierung .....	6
4 Deinstallation .....	7
5 Übersicht .....	7
<b>5.1 Tastaturbefehle</b> .....	7
<b>5.2 Schutzstatus prüfen</b> .....	8
<b>5.3 Vorgehensweise bei fehlerhafter Ausführung des Programms</b> .....	8
6 Computerschutz .....	8
<b>6.1 Viren- und Spyware-Schutz</b> .....	9
6.1 Allgemein .....	9
6.1 Ausschlussfilter .....	9
6.1 Systemstart-Schutz .....	10
6.1 Echtzeit-Dateischutz .....	10
6.1 Erweiterte Einstellungen .....	10
6.1 Wann sollten die Einstellungen für den Echtzeit-Dateischutz geändert werden? .....	11
6.1 Echtzeit-Dateischutz prüfen .....	11
6.1 Vorgehensweise bei fehlerhaftem Echtzeit-Dateischutz .....	11
6.1 On-Demand-Prüfung .....	12
6.1 Prüfungstyp .....	13
6.1 Smart-Prüfung .....	13
6.1 Prüfen mit speziellen Einstellungen .....	13
6.1 Zu prüfende Objekte .....	13
6.1 Prüfprofile .....	14
6.1 Einstellungen für ThreatSense .....	14
6.1 Objekte .....	15
6.1 Optionen .....	16
6.1 Säubern .....	16
6.1 Ausschlussfilter .....	16
6.1 Grenzen .....	17
6.1 Sonstige .....	17
6.1 Eindringene Schadsoftware wurde erkannt .....	18
<b>6.2 Prüfen und Sperren von Wechselmedien</b> .....	19
7 Phishing-Schutz .....	19
8 Web- und E-Mail-Schutz .....	20
<b>8.1 Web-Schutz</b> .....	20
8.1 Ports .....	20
8.1 URL-Listen .....	20
<b>8.2 E-Mail-Schutz</b> .....	21
8.2 Prüfen von E-Mails per POP3-Protokoll .....	21
8.2 Prüfen von E-Mails per IMAP-Protokoll .....	22
9 Update .....	22
<b>9.1 Einstellungen für Updates</b> .....	22
9.1 Erweiterte Einstellungen .....	23

<b>9.2 So erstellen Sie Update-Tasks</b> .....	23
<b>9.3 Upgrade von ESET Cyber Security auf eine neue Version</b> .....	23
<b>9.4 System-Updates</b> .....	24
<b>10 Tools</b> .....	25
<b>10.1 Log-Dateien</b> .....	25
10.1 Log-Wartung .....	25
10.1 Log-Filter .....	26
<b>10.2 Taskplaner</b> .....	26
10.2 Erstellen von Tasks .....	27
10.2 Scannen als Verzeichnisbesitzer .....	28
10.2 Erstellen von benutzerdefinierten Tasks .....	29
<b>10.3 Quarantäne</b> .....	29
10.3 Quarantäne für Dateien .....	30
10.3 Wiederherstellen aus Quarantäne .....	30
10.3 Einreichen von Dateien aus der Quarantäne .....	30
<b>10.4 Ausgeführte Prozesse</b> .....	30
<b>10.5 Netzwerkverbindungen</b> .....	31
<b>10.6 Live Grid</b> .....	32
10.6 Live Grid-Einstellungen .....	32
<b>10.7 Probe zur Analyse einreichen</b> .....	33
<b>11 Benutzeroberfläche</b> .....	33
<b>11.1 Warnungen und Hinweise</b> .....	34
11.1 Warnungen anzeigen .....	34
11.1 Schutzstatus .....	35
<b>11.2 Berechtigungen</b> .....	35
<b>11.3 Kontextmenü</b> .....	35
<b>11.4 Einstellungen importieren/exportieren</b> .....	36
<b>11.5 Einstellungen für Proxyserver</b> .....	37
<b>12 Endbenutzer-Lizenzvereinbarung</b> .....	37
<b>13 Datenschutzrichtlinie</b> .....	44

# ESET Cyber Security

ESET Cyber Security stellt eine neue Herangehensweise an integrierte Computersicherheit dar. Die aktuelle Version des ThreatSense®-Prüfmoduls bietet schnellen, präzisen Schutz für Ihren Computer. Das Ergebnis ist ein intelligentes System, das Ihren Computer fortwährend auf Angriffe und Schadsoftware überwacht.

ESET Cyber Security ist als umfassende Sicherheitslösung das Ergebnis unserer langjährigen Entwicklungsarbeit für maximalen Schutz bei minimaler Systembelastung. Die auf künstlicher Intelligenz basierenden fortschrittlichen Technologien von ESET Cyber Security sind in der Lage, Bedrohungen durch Viren, Würmer, Trojaner, Spyware, Adware, Rootkits und andere Angriffe aus dem Internet proaktiv abzuwehren, ohne dabei die Systemleistung zu beeinträchtigen.

## Neuerungen in Version 6

ESET Cyber Security In Version 6 wurden folgende Neuerungen und Verbesserungen eingeführt:

- **64-Bit-Architekturunterstützung**
- **Phishing-Schutz** – Verhindert, dass als vertrauenswürdig getarnte Websites auf Ihre persönlichen Informationen zugreifen.
- **Systemupdates** – ESET Cyber Security Version 6 enthält verschiedene Korrekturen und Verbesserungen, unter anderem eine Benachrichtigungsfunktion für Betriebssystemupdates. Weitere Informationen hierzu finden Sie im Abschnitt [Systemupdates](#).
- **Schutzstatus** – Blendet Benachrichtigungen im Bildschirm „Schutzstatus“ aus (z. B. *E-Mail-Schutz deaktiviert* oder *Neustart des Computers erforderlich*).
- **Zu prüfender Datenträger** – Bestimmte Datenträger (lokale Laufwerke, Wechseldatenträger, Netzlaufwerke) können von der Echtzeitprüfung ausgeschlossen werden.
- **Netzwerkverbindungen** – Zeigt die Netzwerkverbindungen auf Ihrem Computer an und enthält eine Option, mit der Sie Regeln für diese Verbindungen erstellen können.

Weitere Details zu den neuen Funktionen in ESET Cyber Security finden Sie im [folgenden ESET Knowledgebase-Artikel](#):

## Systemanforderungen

Für den optimalen Betrieb von ESET Cyber Security sollte Ihr System die folgenden Hardware- und Softwareanforderungen erfüllen:

	Systemanforderungen:
Prozessorarchitektur	Intel 64-bit, M1, M2
Betriebssystem	macOS 10.12 und höher
Arbeitsspeicher	300 MB
Freier Speicherplatz auf dem Datenträger	200 MB

**!** Zusätzlich zu den bereits unterstützten Intel-Versionen unterstützen ESET Cyber Security Version 6.10.900.0 und neuere Versionen auch die Apple M1- und M2-Chips mit Rosetta 2.

## Installation

Schließen Sie alle laufenden Computerprogramme, bevor Sie mit der Installation beginnen. ESET Cyber Security enthält Komponenten, die Konflikte mit anderen auf Ihrem Computer installierten Virenschutzprogrammen verursachen könnten. ESET empfiehlt daher dringend, alle anderen Virenschutzprogramme zu deinstallieren, um Probleme zu vermeiden.

Führen Sie einen der folgenden Schritte aus, um den Installationsassistenten zu starten:

- Wenn Sie für die Installation eine von der ESET-Website heruntergeladene Datei verwenden, öffnen Sie diese und doppelklicken Sie auf das Symbol **Installieren**.
- Für die Installation per CD/DVD legen Sie diese in Ihren Computer ein, öffnen Sie sie über den Desktop oder ein **Finder**-Fenster und doppelklicken Sie auf das Symbol **Installieren**.



Der Installationsassistent führt Sie durch die grundlegende Einrichtung. Zu Beginn der Installation prüft das Installationsprogramm automatisch online auf die neueste Produktversion. Wird eine neuere Version gefunden, erhalten Sie die Möglichkeit, vor dem Fortsetzen der Installation die neueste Version herunterzuladen.

Nachdem Sie der Endbenutzer-Lizenzvereinbarung zugestimmt haben, werden Sie aufgefordert, eine der folgenden Installationsarten auszuwählen:

- [Standardinstallation](#)
- [Benutzerdefinierte Installation](#)

## Standardinstallation

Die Standardinstallation verwendet eine passende Konfiguration für die Anforderungen der meisten Benutzer. Diese Einstellungen bieten optimale Sicherheit und schonen gleichzeitig die Systemressourcen. Verwenden Sie

daher die Standardinstallation, wenn Sie keine speziellen Anforderungen an die Konfiguration haben.

1. Wählen Sie im Fenster **ESET LiveGrid** die gewünschte Option aus und klicken Sie auf **Weiter**. Wenn Sie diese Einstellung später ändern möchten, können Sie dazu das **LiveGrid-Setup** verwenden. Weitere Informationen zu ESET Live Grid finden Sie [in unserem Glossar](#).
2. Wählen Sie im Fenster **Potenziell unerwünschte Anwendungen** die gewünschte Option aus (siehe [Was ist eine potenziell unerwünschte Anwendung?](#)) und klicken Sie auf **Weiter**. Sie können diese Einstellung später in den **erweiterten Einstellungen** ändern.
3. Klicken Sie auf **Installieren**. Falls Sie dazu aufgefordert werden, geben Sie Ihr macOS-Passwort ein und klicken Sie auf **Software installieren**.

Nach der Installation von ESET Cyber Security:

## macOS Big Sur (11)

1. [Systemerweiterungen erlauben](#)
2. [Vollständigen Laufwerkszugriff erlauben](#).

3. Erlauben Sie ESET das Hinzufügen von Proxykonfigurationen. Sie erhalten die folgende Benachrichtigung: „ESET Cyber Security“ **möchte Proxykonfigurationen hinzufügen**. Wenn diese Benachrichtigung angezeigt wird, klicken Sie auf **Zulassen**. Wenn Sie auf **Nicht zulassen** klicken, können Sie den Web-Schutz nicht verwenden.

### ☐ [macOS 10.15 und älter](#)

1. Auf macOS 10.13 und neueren Versionen erhalten Sie die Benachrichtigung **Systemerweiterung blockiert** von Ihrem System, und die Benachrichtigung **Ihr Computer ist nicht geschützt** von ESET Cyber Security. Um den vollen Funktionsumfang von ESET Cyber Security nutzen zu können, müssen Sie Kernelerweiterungen auf Ihrem Gerät erlauben. Um Kernelerweiterungen auf Ihrem Gerät zu erlauben, navigieren Sie zu **Systemeinstellungen > Sicherheit & Datenschutz** und klicken Sie auf **Zulassen**, um Systemsoftware vom Entwickler **ESET, spol. s.r.o.** zu erlauben. Weitere Informationen finden Sie in unserem [Knowledgebase-Artikel](#).
2. Auf macOS 10.14 und höher wird die Benachrichtigung **Ihr Computer ist teilweise geschützt** in ESET Cyber Security angezeigt. Um den vollen Funktionsumfang von ESET Cyber Security nutzen zu können, müssen Sie ESET Cyber Security **vollständigen Laufwerkszugriff** erlauben. Klicken Sie auf **Systemeinstellungen öffnen > Sicherheit & Datenschutz**. Öffnen Sie die Registerkarte **Datenschutz** und wählen Sie die Option **Vollständiger Laufwerkszugriff** aus. Klicken Sie auf das Schlosssymbol, um die Einstellungen bearbeiten zu können. Klicken Sie auf das Pluszeichen und wählen Sie die ESET Cyber Security-Anwendung aus. Auf Ihrem Computer wird eine Benachrichtigung angezeigt, dass ein Neustart erforderlich ist. Klicken Sie auf **Später**. Starten Sie Ihren Computer zu diesem Zeitpunkt noch nicht neu. Klicken Sie im ESET Cyber Security-Benachrichtigungsfenster auf **Erneut starten** oder starten Sie Ihren Computer neu. Weitere Informationen finden Sie in unserem [Knowledgebase-Artikel](#).

Nach der Installation von ESET Cyber Security sollten Sie Ihren Computer auf Schadcode scannen. Klicken Sie dazu im Hauptprogrammfenster auf **Computer scannen > Smart-Scan**. Weitere Informationen zu On-Demand-Scans finden Sie im Abschnitt [On-Demand-Scan](#).

# Benutzerdefinierte Installation

Die benutzerdefinierte Installation eignet sich für fortgeschrittene Benutzer, die während der Installation die erweiterten Einstellungen ändern möchten.

- **Proxyserver**

Wenn Sie einen Proxyserver verwenden, können Sie die entsprechenden Parameter über die Option **Ich nutze einen Proxyserver** festlegen. Geben Sie im nächsten Fenster unter **Adresse** die IP-Adresse oder die URL des Proxyservers ein. Geben Sie im Feld **Port** den Port für eingehende Verbindungen auf dem Proxyserver an (standardmäßig 3128). Falls der Proxyserver Authentifizierung erfordert, geben Sie einen gültigen **Benutzernamen** und das **Passwort** ein. Wenn Sie keinen Proxyserver verwenden, wählen Sie die Option **Keinen Proxyserver verwenden**. Falls Sie unsicher sind, ob Sie einen Proxyserver verwenden, wählen Sie **Systemeinstellungen verwenden (empfohlen)** aus, um Ihre aktuellen Systemeinstellungen zu verwenden.

- **Privilegien**

Können Sie privilegierte Benutzer oder Gruppen definieren, die berechtigt sind, die Programmkonfiguration zu ändern. Wählen Sie aus der Liste links die Benutzer aus und fügen Sie sie über die Schaltfläche **Hinzufügen** zur Liste **Privilegierte Benutzer** hinzu. Um alle Systembenutzer anzuzeigen, wählen Sie die Option **Alle Benutzer anzeigen** aus. Wenn Sie die Liste der privilegierten Benutzer leer lassen, werden alle Benutzer als privilegiert betrachtet.

- **ESET LiveGrid®**

Weitere Informationen zu ESET LiveGrid finden Sie [in unserem Glossar](#).

- **Evtl. unerwünschte Anwendungen**

Weitere Informationen zu potenziell unerwünschten Anwendungen finden Sie [in unserem Glossar](#).

**Nach der Installation von ESET Cyber Security:**

## macOS Big Sur (11)

1. [Systemerweiterungen erlauben](#)

2. [Vollständigen Laufwerkszugriff erlauben](#).

3. Erlauben Sie ESET das Hinzufügen von Proxykonfigurationen. Sie erhalten die folgende Benachrichtigung: „ESET Cyber Security“ **möchte Proxykonfigurationen hinzufügen**. Wenn diese Benachrichtigung angezeigt wird, klicken Sie auf **Zulassen**. Wenn Sie auf **Nicht zulassen** klicken, können Sie den Web-Schutz nicht verwenden.

### [macOS 10.15 und älter](#)

1. Auf macOS 10.13 und höher und neueren Versionen erhalten Sie die Benachrichtigung **Systemerweiterung blockiert** von Ihrem System, und die Benachrichtigung **Ihr Computer ist nicht geschützt** von ESET Cyber Security. Um den vollen Funktionsumfang von ESET Cyber Security nutzen zu können, müssen Sie Kernelerweiterungen auf Ihrem Gerät erlauben. Um Kernelerweiterungen auf Ihrem Gerät zu erlauben, navigieren Sie zu **Systemeinstellungen > Sicherheit & Datenschutz** und klicken Sie auf **Zulassen**, um Systemsoftware vom Entwickler **ESET, spol. s.r.o.** zu erlauben. Weitere Informationen finden Sie in unserem [Knowledgebase-Artikel](#).

2. Auf macOS 10.14 und höher wird die Benachrichtigung **Ihr Computer ist teilweise geschützt** in ESET Cyber Security angezeigt. Um den vollen Funktionsumfang von ESET Cyber Security nutzen zu können, müssen Sie ESET Cyber Security **vollständigen Laufwerkszugriff** erlauben. Klicken Sie auf

**Systemeinstellungen öffnen > Sicherheit & Datenschutz.** Öffnen Sie die Registerkarte **Datenschutz** und wählen Sie die Option **Vollständiger Laufwerkszugriff** aus. Klicken Sie auf das Schlosssymbol, um die Einstellungen bearbeiten zu können. Klicken Sie auf das Pluszeichen und wählen Sie die ESET Cyber Security-Anwendung aus. Auf Ihrem Computer wird eine Benachrichtigung angezeigt, dass ein Neustart erforderlich ist. Klicken Sie auf **Später**. Starten Sie Ihren Computer zu diesem Zeitpunkt noch nicht neu. Klicken Sie im ESET Cyber Security-Benachrichtigungsfenster auf **Erneut starten** oder starten Sie Ihren Computer neu. Weitere Informationen finden Sie in unserem [Knowledgebase-Artikel](#).

Nach der Installation von ESET Cyber Security sollten Sie Ihren Computer auf Schadcode scannen. Klicken Sie dazu im Hauptprogrammfenster auf **Computer scannen > Smart-Scan**. Weitere Informationen zu On-Demand-Scans finden Sie im Abschnitt [On-Demand-Scan](#).

## Systemerweiterungen erlauben

In macOS 11 (Big Sur) wurden Kernelerweiterungen durch Systemerweiterungen ersetzt. Diese Erweiterungen müssen vom Benutzer zugelassen werden, um neue Systemerweiterungen von Drittanbietern laden zu können.

Nach der Installation von ESET Cyber Security auf macOS Big Sur (11) und neueren Versionen erhalten Sie die Benachrichtigung „Systemerweiterung blockiert“ von Ihrem System, und die Benachrichtigung „Ihr Computer ist nicht geschützt“ von ESET Cyber Security. Um den vollen Funktionsumfang von ESET Cyber Security nutzen zu können, müssen Sie Systemerweiterungen auf Ihrem Gerät erlauben.



### Upgrade von älteren macOS-Versionen auf Big Sur.

Falls Sie ESET Cyber Security bereits installiert haben und auf macOS Big Sur umsteigen möchten, müssen Sie die ESET-Kernelerweiterungen nach dem Upgrade manuell zulassen. Dazu ist physischer Zugriff auf den Clientcomputer erforderlich. Die Schaltfläche „Aktivieren“ ist bei Remotezugriffen deaktiviert.

Wenn Sie das ESET-Produkt auf macOS Big Sur oder neuer installieren, müssen Sie die ESET-Systemerweiterungen manuell zulassen. Dazu ist physischer Zugriff auf den Clientcomputer erforderlich. Die Schaltfläche „Aktivieren“ ist bei Remotezugriffen deaktiviert.

## Systemerweiterungen manuell zulassen

1. Klicken Sie auf **Systemeinstellungen öffnen** oder auf **Sicherheitseinstellungen öffnen** in einem der Dialogfenster.
2. Klicken Sie unten links auf das Schlosssymbol, um Änderungen im Einstellungsfenster zu erlauben.
3. Verwenden Sie Ihre Touch ID oder klicken Sie auf **Passwort verwenden** und geben Sie Ihren Benutzernamen und Ihr Passwort ein. Klicken Sie dann auf **Entsperren**.
4. Klicken Sie auf **Details**.
5. Wählen Sie beide ESET Cyber Security.app-Optionen aus.
6. Klicken Sie auf **OK**.

Eine ausführliche Anleitung finden Sie in [unserem Knowledgebase Artikel](#) (Knowledgebase-Artikel sind nicht in allen Sprachen verfügbar).

# Vollständigen Laufwerkszugriff erlauben

Auf macOS 10.14 wird die Benachrichtigung **Ihr Computer ist teilweise geschützt** in ESET Cyber Security angezeigt. Um alle Funktionen von ESET Cyber Security nutzen zu können, müssen Sie ESET Cyber Security **vollständigen Laufwerkszugriff erlauben**.

1. Klicken Sie im Dialogfenster mit der Warnung auf **Systemeinstellungen öffnen**.
2. Klicken Sie unten links auf das Schlosssymbol, um Änderungen im Einstellungsfenster zu erlauben.
3. Verwenden Sie Ihre Touch ID oder klicken Sie auf **Passwort verwenden** und geben Sie Ihren Benutzernamen und Ihr Passwort ein. Klicken Sie dann auf **Entsperren**.
4. Wählen Sie ESET Cyber Security.app in der Liste aus.
5. Eine Benachrichtigung über den Neustart von ESET Cyber Security wird angezeigt. Klicken Sie auf „Später“.
6. Wählen Sie den ESET **Echtzeit-Dateischutz** in der Liste aus.



## ESET Echtzeit-Dateischutz nicht vorhanden

Falls die Option **Echtzeit-Dateischutz** nicht in der Liste vorhanden ist, müssen Sie [Systemerweiterungen für Ihr ESET-Produkt erlauben](#).

7. Klicken Sie im ESET Cyber Security-Dialogfenster auf „Neu starten“ oder starten Sie Ihren Computer neu. Weitere Informationen finden Sie in unserem [Knowledgebase-Artikel](#).

## Produktaktivierung

Nach der Installation wird das Fenster zur Produktaktivierung automatisch angezeigt. Klicken Sie auf das ESET Cyber Security-Symbol  in der OS X-Menüleiste oben auf dem Bildschirm und anschließend auf **Produktaktivierung**, um das Dialogfeld für die Produktaktivierung zu öffnen.

- **Lizenzschlüssel** – eine einmalige Zeichenfolge im Format XXXX-XXXX-XXXX-XXXX-XXXX oder XXXX-XXXXXXXX, die dem Lizenzinhaber zur Identifizierung und zur Aktivierung der Lizenz dient. Wenn Sie das Produkt in einer Einzelhandelsverpackung erworben haben, aktivieren Sie Ihr Produkt mit einem Lizenzschlüssel. Sie finden ihn normalerweise in der Produktverpackung oder auf deren Rückseite.
- **Benutzername und Passwort** – Wenn Sie einen Benutzernamen und ein Passwort haben und nicht wissen, wie Sie ESET Cyber Security aktivieren können, klicken Sie auf **Ich habe einen Benutzernamen und ein Passwort, was muss ich tun?**. Daraufhin werden Sie zu my.eset.com weitergeleitet, wo Sie Ihre Zugangsdaten in einen Lizenzschlüssel umwandeln können.
- **Kostenlose Testlizenz** – Wählen Sie diese Option aus, wenn Sie ESET Cyber Security vor dem Kauf zunächst testen möchten. Geben Sie Ihre E-Mail-Adresse ein, um ESET Cyber Security für begrenzte Zeit zu aktivieren. Sie erhalten die Testlizenz per E-Mail. Eine Testlizenz kann pro Kunde nur ein einziges Mal aktiviert werden.
- **Lizenz kaufen** – Wenn Sie noch keine Lizenz haben und eine Lizenz erwerben möchten, klicken Sie auf Lizenz kaufen. Daraufhin werden Sie zur Website Ihres örtlichen ESET-Vetriebshändlers weitergeleitet.
- **Später aktivieren** – Klicken Sie auf diese Option, wenn Sie Ihr Produkt zum jetzigen Zeitpunkt nicht aktivieren möchten.

# Deinstallation

Führen Sie einen der folgenden Schritte aus, um ESET Cyber Security zu deinstallieren:

- Legen Sie die ESET Cyber Security-Installations-CD/-DVD in den Computer ein, öffnen Sie sie über den Desktop oder das **Finder**-Fenster und doppelklicken Sie auf **Deinstallieren**
- Öffnen Sie die ESET Cyber Security-Installationsdatei (.dmg) und doppelklicken Sie auf **Deinstallieren**
- Starten Sie **Finder**, öffnen Sie den Ordner **Anwendungen** auf der Festplatte, klicken Sie bei gedrückter STRG-Taste auf das **ESET Cyber Security**-Symbol und wählen Sie **Paketinhalt zeigen**. Öffnen Sie den **Contents > Helpers**-Ordner und doppelklicken Sie auf das **Uninstaller**-Symbol.

## Übersicht

Das Hauptprogrammfenster von ESET Cyber Security ist in zwei Abschnitte unterteilt. Das primäre Fenster (rechts) zeigt Informationen zu den im Hauptmenü (links) ausgewählten Optionen an.

Über das Hauptmenü kann auf die folgenden Bereiche zugegriffen werden:

- **Startseite** – liefert Informationen zum Schutzstatus Ihres Computers sowie zum Web- und E-Mail-Schutz.
- **Scannen des Computers** – In diesem Bereich können Sie bei Bedarf einen [On-Demand-Scan des Computers](#) starten oder die Einstellungen dazu ändern.
- **Update** – Dieser Bereich zeigt Informationen zu Updates der Erkennungsroutine an.
- **Einstellungen** – Wählen Sie diese Option, um die Sicherheitsstufe Ihres Computers anzupassen.
- **Tools** – Zugriff auf [Log-Dateien](#), [Taskplaner](#), [Quarantäne](#), [Ausgeführte Prozesse](#) und andere Programmfunktionen.
- **Hilfe** – Zugriff auf die Hilfedateien, die Internet-Knowledgebase, Supportanfrageformulare und zusätzliche Informationen zum Programm.

## Tastaturbefehle

Folgende Tastaturbefehle können in Verbindung mit ESET Cyber Security verwendet werden:

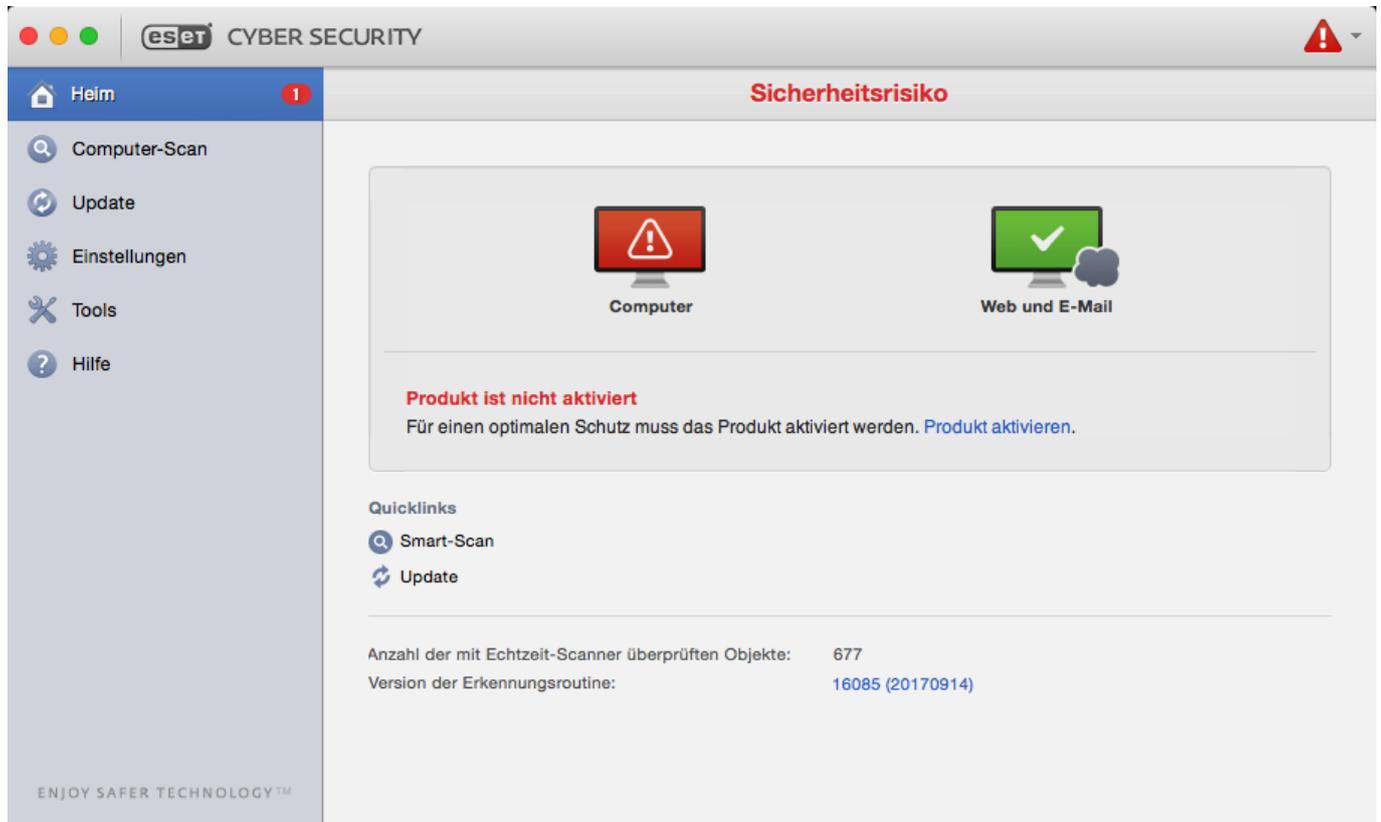
- cmd+, - zeigt ESET Cyber Security-Einstellungen an,
- cmd+O - setzt das ESET Cyber Security-Hauptprogrammfenster auf die Standardgröße zurück und positioniert es in der Bildschirmmitte.
- cmd+Q - blendet das ESET Cyber Security-Hauptprogrammfenster aus. Um es erneut zu öffnen, klicken Sie auf das ESET Cyber Security-Symbol  in der macOS-Menüleiste am oberen Bildschirmrand,
- cmd+W - schließt das ESET Cyber Security-Hauptprogrammfenster.

Die folgenden Tastaturbefehle funktionieren nur, wenn die Option **Standardmenü verwenden** unter **Einstellungen > Erweiterte Einstellungen ... > Schnittstelle** aktiviert ist:

- cmd+alt+L - öffnet den Abschnitt Log-Dateien,
- cmd+alt+S - öffnet den Abschnitt Taskplaner,
- cmd+alt+Q - öffnet den Abschnitt Quarantäne.

# Schutzstatus prüfen

Zur Anzeige des Schutzstatus klicken Sie im Hauptmenü auf **Startseite**. Im primären Fenster wird eine Darstellung des aktuellen Betriebszustands von ESET Cyber Security angezeigt.



## Vorgehensweise bei fehlerhafter Ausführung des Programms

Wenn ein Modul ordnungsgemäß funktioniert, wird ein grünes Symbol angezeigt. Funktioniert ein Modul nicht ordnungsgemäß, wird ein rotes Ausrufezeichen oder orangefarbenes Warnsymbol angezeigt. Zusätzlich werden in diesem Fall weitere Informationen zu dem Modul und ein Lösungsvorschlag angezeigt. Um den Status einzelner Module zu ändern, klicken Sie auf den blauen Link unter dem jeweiligen Hinweis.

Wenn Sie ein Problem mit den vorgeschlagenen Lösungen nicht beheben konnten, können Sie in der [ESET Knowledgebase](#) nach einer Lösung suchen oder sich an den [ESET-Support](#) wenden. Der Support widmet sich umgehend Ihrem Anliegen, um schnell eine Lösung für Ihr Problem mit ESET Cyber Security zu finden.

## Computerschutz

Die Computerkonfiguration finden Sie unter **Einstellungen > Computer**. Dort wird der Status für die Optionen **Echtzeit-Dateischutz** und **Sperren von Wechselmedien** angezeigt. Um die einzelnen Module zu deaktivieren, ändern Sie den Status des gewünschten Moduls in **DEAKTIVIERT**. Beachten Sie, dass dies den Schutz Ihres Computers beeinträchtigen kann. Zugriff auf die detaillierten Einstellungen zu jedem Modul erhalten Sie durch Klicken auf **Einstellungen....**

# Viren- und Spyware-Schutz

Der Virenschutz bewahrt das System vor Attacken, indem er potenziell gefährliche Dateien verändert. Wird eine Bedrohung durch Schadcode erkannt, kann das Virenschutz-Modul den Code unschädlich machen, indem es die Ausführung des Codes blockiert und dann den Code entfernt bzw. die Datei löscht oder in die Quarantäne verschiebt.

## Allgemein

Im Bereich **Allgemein (Einstellungen > Erweiterte Einstellungen... > Allgemein)** können Sie die Erkennung der folgenden Arten von Anwendungen aktivieren:

- **Potenziell unerwünschte Anwendungen** - Grayware oder potenziell unerwünschte Anwendungen (PUA) sind verschiedenste Arten von Software, deren Ziel nicht so eindeutig bösartig ist wie bei anderen Arten von Malware wie Viren oder Trojanern. Diese Art von Software kann jedoch weitere unerwünschte Software installieren, das Verhalten des digitalen Geräts ändern oder Aktionen ausführen, denen der Benutzer nicht zugestimmt hat oder die er nicht erwartet. Weitere Informationen zu diesem Anwendungstyp finden Sie im [Glossar](#).
- **Potenziell unsichere Anwendungen** - In diese Kategorie fallen legitime Programme seriöser Hersteller, die jedoch von Angreifern ausgenutzt werden können, wenn sie ohne Wissen des Benutzers installiert werden. Da hierzu auch Programme für die Fernsteuerung von Computern gehören, ist diese Option standardmäßig deaktiviert.
- **Verdächtige Anwendungen** - Hierunter fallen Anwendungen, die mit sogenannten "Packer"- oder "Protector"-Programmen komprimiert wurden. Diese Art von Programmen wird oft von Malware-Autoren ausgenutzt, um einer Erkennung zu entgehen. Packer sind selbst-extrahierende Anwendungen, die zur Laufzeit mehrere Arten von Malware in ein einziges Paket verpacken. Die gängigsten Packer sind UPX, PE\_Compact, PKLite und ASPack. Dieselbe Malware kann unter Umständen unterschiedlich erkannt werden, wenn für die Kompression ein anderer Packer verwendet wurde. Packer können außerdem die "Signaturen" regelmäßig verändern, wodurch Malware schwieriger zu erkennen und zu entfernen ist.

Klicken Sie auf **Einstellungen**, um [Ausschlussfilter für Dateisystem bzw. Web- und E-Mail](#) einzurichten.

## Ausschlussfilter

Im Bereich **Ausschlussfilter** können Sie festlegen, dass bestimmte Dateien/Ordner, Anwendungen oder IP/IPv6-Adressen von Scans ausgenommen werden.

Dateien und Ordner, die auf der Registerkarte **Dateisystem** aufgeführt sind, werden von allen Scans ausgeschlossen: Prüfung der Systemstartdateien, Echtzeit-Prüfung und On-Demand-Prüfung.

- **Pfad** – Pfad zu den auszuschließenden Dateien/Ordnern
- **Bedrohung** – Steht neben einer ausgeschlossenen Datei der Name einer Bedrohung, so gilt die Ausnahme nicht generell für die Datei, sondern nur für diese bestimmte Bedrohung. Wird die Datei später durch andere Schadsoftware infiziert, erkennt der Virenschutz dies.
-  – Erstellen eines neuen Ausschlusses. Geben Sie den Pfad zum Objekt ein (Platzhalter \* und ? werden unterstützt) oder wählen Sie den Ordner bzw. die Datei in der Baumstruktur aus.

-  – Entfernt ausgewählte Einträge.
- **Standard** – annulliert alle Ausschlüsse

In der Registerkarte **Web und E-Mail** können Sie bestimmte **Anwendungen** oder **IP/IPv6-Adressen** von der Protokollprüfung ausschließen.

## Systemstart-Schutz

Bei der Prüfung der Systemstartdateien werden Dateien beim Systemstart automatisch untersucht. Dieser Scan wird standardmäßig als geplanter Task nach der Anmeldung eines Benutzers oder nach einem erfolgreichen Update der Erkennungsroutine ausgeführt. Klicken Sie auf **Einstellungen**, um die Einstellungen der ThreatSense-Engine für die Prüfung beim Systemstart zu ändern. Weitere Informationen zur Einrichtung der ThreatSense-Engine finden Sie in [diesem Abschnitt](#).

## Echtzeit-Dateischutz

Der Echtzeit-Dateischutz überwacht alle Datenträger auf das Eintreten bestimmter Ereignisse. Aufgrund unterschiedlicher ThreatSense-Technologien (siehe Abschnitt [ThreatSense-Einstellungen](#)) kann der Echtzeit-Dateischutz für neu erstellte Dateien von dem für bestehende Dateien abweichen. Neu erstellte Dateien können genauer kontrolliert werden.

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. Der Echtzeit-Dateischutz wird beim Systemstart geladen und fortlaufend ausgeführt. In besonderen Fällen (z. B. bei einem Konflikt mit einem anderen Echtzeit-Prüfprogramm) können Sie den Echtzeit-Dateischutz beenden, indem Sie auf das ESET Cyber Security-Symbol  in der oberen Menüleiste klicken und die Option **Echtzeit-Dateischutz deaktivieren** auswählen. Der Echtzeit-Dateischutz lässt sich auch im Hauptfenster beenden. Klicken Sie dazu auf **Einstellungen > Computer** und setzen Sie die Option **Echtzeit-Dateischutz** auf **DEAKTIVIERT**.

Die folgenden Medientypen können von der Real-time-Prüfung ausgeschlossen werden:

- **Lokale Laufwerke** - Systemlaufwerke
- **Wechselmedien** - CDs/DVDs, USB-Speichergeräte, Bluetooth-Geräte usw.
- **Netzlaufwerke** - Alle zugeordneten Netzlaufwerke

Sie sollten diese Einstellungen nur in Ausnahmefällen ändern, z. B. wenn die Prüfung bestimmter Datenträger die Datenübertragung deutlich verlangsamt.

Um die erweiterten Einstellungen für den Echtzeit-Dateischutz zu ändern, wechseln Sie zu **Einstellungen > Erweiterte Einstellungen ...** (oder drücken Sie *cmd+*) > **Echtzeit-Dateischutz** und klicken Sie auf **Einstellungen...** neben **Erweiterte Optionen** (siehe Abschnitt [Erweiterte Optionen für Prüfungen](#)).

## Erweiterte Einstellungen

In diesem Fenster können Sie die Objekttypen festlegen, die vom ThreatSense-Modul gescannt werden sollen. Weitere Informationen zu **selbstentpackenden Archiven**, **laufzeitkomprimierten Dateien** und **Advanced**

**Heuristik** finden Sie unter [ThreatSense-Einstellungen](#).

Die Werte im Abschnitt **Standard-Archiveinstellungen** sollten nur geändert werden, um konkrete Probleme zu lösen, da höhere Archivverschachtelungswerte die Systemleistung beeinträchtigen können.

**ThreatSense Parameter für ausführbare Dateien** - beim Ausführen der Dateien wird standardmäßig **Advanced Heuristik** verwendet. Smart-Optimierung und ESET Live Grid sollten unbedingt aktiviert bleiben, um die Auswirkungen auf die Systemleistung zu minimieren.

**Verbesserte Kompatibilität von Netzwerklaufwerken** - Diese Option verbessert die Leistung beim Dateizugriff über das Netzwerk. Aktivieren Sie diese Option, wenn beim Zugriff auf Netzlaufwerke Geschwindigkeitsprobleme auftreten. Dieses Feature verwendet System File Coordinator unter macOS 10.10 und neueren Versionen. Achtung: Der File Coordinator wird nicht von allen Anwendungen unterstützt. Microsoft Word 2011 wird nicht unterstützt, Word 2016 dagegen schon.

## Wann sollten die Einstellungen für den Echtzeit-Dateischutz geändert werden?

Der Echtzeit-Dateischutz ist die wichtigste Komponente für ein sicheres System mit ESET Cyber Security. Änderungen an den Parametern des Echtzeit-Dateischutzes sind mit Bedacht vorzunehmen. Es wird empfohlen, nur in einzelnen Fällen die Parameter zu verändern. Es kann beispielsweise erforderlich sein, wenn ein Konflikt mit einer bestimmten Anwendung vorliegt.

Bei der Installation von ESET Cyber Security werden alle Einstellungen optimal eingerichtet, um dem Benutzer die größtmögliche Schutzstufe für das System zu bieten. Um die Standardeinstellungen wieder herzustellen, klicken Sie auf **Standard** unten links im Fenster **Echtzeit-Dateischutz (Einstellungen > Erweiterte Einstellungen... > Echtzeit-Dateischutz)**.

## Echtzeit-Dateischutz prüfen

Um zu überprüfen, ob der Echtzeit-Dateischutz funktioniert und Viren erkannt werden, laden Sie die Testdatei [eicar.com](http://eicar.com) herunter und testen Sie, ob ESET Cyber Security sie als Bedrohung erkennt. Diese Testdatei ist harmlos und wird von allen Virenschutzprogrammen erkannt. Die Datei wurde vom EICAR-Institut (European Institute for Computer Antivirus Research) erstellt, um die Funktionalität von Virenschutzprogrammen zu testen.

## Vorgehensweise bei fehlerhaftem Echtzeit-Dateischutz

In diesem Kapitel werden mögliche Probleme mit dem Echtzeit-Dateischutz sowie Lösungsstrategien beschrieben.

### Echtzeit-Dateischutz ist deaktiviert

Der Echtzeit-Dateischutz wurde versehentlich von einem Benutzer deaktiviert und muss reaktiviert werden. Um den Echtzeit-Dateischutz über das Hauptmenü zu reaktivieren, klicken Sie auf **Einstellungen > Computer** und setzen den **Echtzeit-Dateischutz** auf **AKTIVIERT**. Alternativ dazu können Sie den Echtzeit-Dateischutz im Fenster mit erweiterten Einstellungen unter **Echtzeit-Dateischutz** aktivieren. Wählen Sie dazu die Option **Echtzeit-Dateischutz aktivieren**.

## Echtzeit-Dateischutz erkennt und entfernt keinen Schadcode

Stellen Sie sicher, dass keine anderen Virenschutzprogramme auf Ihrem Computer installiert sind. Zwei parallel ausgeführte Schutzprogramme können miteinander in Konflikt geraten. Wir empfehlen Ihnen, alle anderen Virusschutzprogramme zu deinstallieren.

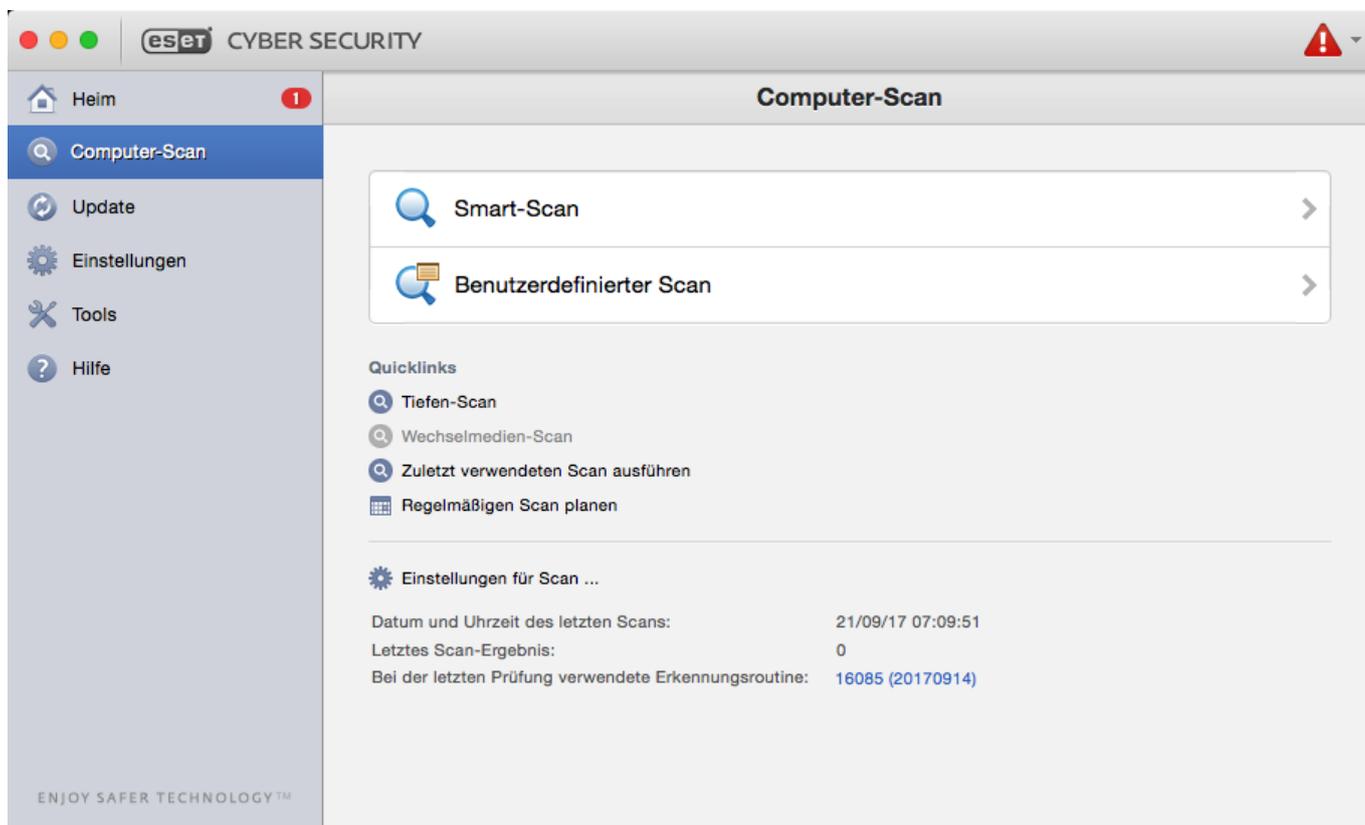
## Echtzeit-Dateischutz startet nicht

Wenn der Echtzeit-Dateischutz nicht automatisch beim Systemstart startet, können Konflikte mit anderen Programmen vorliegen. Sollte dies der Fall sein, wenden Sie sich an den ESET-Support.

## On-Demand-Prüfung

Wenn Sie den Verdacht haben, dass Ihr Computer infiziert ist (anormales Verhalten), starten Sie eine **Smart-Prüfung**, um Ihren Computer auf eingedrungene Schadsoftware zu untersuchen. Um maximalen Schutz zu gewährleisten, sollten Sie solche Prüfungen routinemäßig durchführen und nicht nur, wenn eine Infektion vermutet wird. Durch regelmäßige Prüfungen kann eingedrungene Schadsoftware erkannt werden, die vom Echtzeit-Dateischutz zum Zeitpunkt der Speicherung der Schadsoftware nicht erkannt wurde. Dies kommt z. B. vor, wenn der Echtzeit-Scan zum Zeitpunkt der Infektion deaktiviert war oder die Erkennungsroutinen nicht auf dem neuesten Stand sind.

Sie sollten mindestens einmal im Monat eine On-Demand-Prüfung vornehmen. Sie können die Scans als Task unter **Tools > Taskplaner** konfigurieren.



# Prüfungstyp

Es gibt zwei verschiedene Arten von On-Demand-Prüfungen. Bei der **Smart-Prüfung** (Standardprüfung) wird das System schnell überprüft, ohne dass Sie dafür weitere Prüfparameter konfigurieren müssen. Bei der Methode **Prüfen mit speziellen Einstellungen** können Sie ein vordefiniertes Prüfprofil und die zu prüfenden Objekte auswählen.

## Smart-Prüfung

Mit der Smart-Prüfung (Standardprüfung) können Sie schnell den Computer prüfen und infizierte Dateien säubern, ohne eingreifen zu müssen. Die Bedienung ist einfach, und es ist keine ausführliche Konfiguration erforderlich. Bei der Smart-Prüfung werden alle Dateien in allen Ordnern geprüft, und erkannte Infiltrationen werden automatisch entfernt. Als Säuberungsstufe wird automatisch der Standardwert festgelegt. Weitere Informationen zu den Säuberungsarten finden Sie unter [Säubern](#).

## Benutzerdefinierter Scan

Über die Option **Benutzerdefinierter Scan** können Sie Prüfparameter wie die zu prüfenden Objekte oder Prüfmethoden festlegen. Diese Methode bietet den Vorteil, dass sämtliche Parameter ausführlich konfigurierbar sind. Verschiedene Konfigurationen können als benutzerdefinierte Scanprofile gespeichert werden. Das ist sinnvoll, wenn Scans wiederholt mit denselben Parametern ausgeführt werden.

Zum Festlegen der zu scannenden Objekte wählen Sie **Computer scannen > Benutzerdefinierter Scan** und wählen dann bestimmte **Zu scannende Objekte** in der Baumstruktur aus. Sie können zu scannende Objekte auch über den jeweiligen Pfad zum Ordner oder zu den Dateien angeben. Wenn Sie nur das System ohne zusätzliche Säuberung prüfen möchten, wählen Sie die Option **Nur prüfen, keine Aktion** aus. Außerdem können Sie zwischen drei Säuberungsstufen wählen. Klicken Sie dazu auf **Einstellungen ... > Säubern**.



### Benutzerdefinierter Scan

Eine Prüfung des Computers mit dieser Methode wird nur fortgeschrittenen Benutzern empfohlen, die Erfahrung im Umgang mit Virenschutzprogrammen haben.

## Zu prüfende Objekte

In der Baumstruktur der zu prüfenden Objekte können Sie Dateien und Ordner auswählen, die auf Viren geprüft werden sollen. Im Prüfprofil können Sie die Prüfung von Ordnern festlegen.

Sie können ein zu prüfendes Objekt auch genauer definieren, indem Sie den Pfad zu dem Ordner oder den Dateien eingeben, die geprüft werden sollen. Wählen Sie die zu prüfenden Objekte aus der Baumstruktur aus, in der alle auf dem Computer verfügbaren Ordner aufgelistet werden, indem Sie das Kontrollkästchen zu einer Datei bzw. einem Ordner markieren.

# Prüfprofile

Ihre benutzerdefinierten Einstellungen 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).

Zur Erstellung eines neuen Profils klicken Sie im Hauptmenü auf **Einstellungen > Erweiterte Einstellungen...** (oder drücken *cmd+,*) > **Computer prüfen** und klicken auf **Bearbeiten...** neben der Liste der aktuell bestehenden Profile.



Eine Beschreibung der einzelnen Prüfeinstellungen finden Sie im Abschnitt [ThreatSense-Einstellungen](#). So können Sie ein Prüfprofil erstellen, das auf Ihre Anforderungen zugeschnitten ist.

Beispiel: Nehmen wir an, Sie möchten Ihr eigenes Prüfprofil erstellen. Die Smart-Prüfung eignet sich in gewissem Maße, aber Sie möchten nicht die laufzeitkomprimierten Dateien oder potenziell unsichere Anwendungen prüfen. Außerdem möchten Sie die Option „Automatisch säubern“ anwenden. Geben Sie im Fenster **Profile für On-Demand-Scanner** den Profilenames ein, klicken Sie auf **Hinzufügen** und bestätigen Sie mit **OK**. Passen Sie dann die Parameter unter **ThreatSense-Prüfmodul** und **Zu prüfende Objekte** an Ihre Anforderungen an.

Wenn das Betriebssystem nach Abschluss der On-Demand-Prüfung ausgeschaltet und der Computer heruntergefahren werden soll, wählen Sie die Option **Computer nach Abschluss der Prüfung herunterfahren**.

## Einstellungen für ThreatSense

ThreatSense ist eine proprietäre Technologie von ESET und besteht aus einer Kombination hochentwickelter Bedrohungserkennungsmethoden. Diese Prüftechnologie arbeitet proaktiv, d. h., sie schützt das System auch während der ersten Stunden eines neuen Angriffs. Eingesetzt wird eine Kombination verschiedener Methoden (Code-Analyse, Code-Emulation, allgemeine Signaturen usw.), die zusammen die Systemsicherheit deutlich erhöhen. Das Prüfmodul kann verschiedene Datenströme gleichzeitig kontrollieren und so die Effizienz und Erkennungsrate steigern. Die ThreatSense-Technologie entfernt auch Rootkits erfolgreich.

In den ThreatSense-Einstellungen können Sie verschiedene Prüfparameter festlegen:

- Dateitypen und -erweiterungen, die geprüft werden sollen

- Die Kombination verschiedener Erkennungsmethoden
- Säuberungsstufen usw.

Zum Öffnen des Einstellungsfensters klicken Sie auf **Einstellungen > Erweiterte Einstellungen** (oder drücken Sie *cmd+*) und klicken anschließend auf die Schaltfläche **Einstellungen** für das ThreatSense-Prüfmodul im Bereich **Systemstart-Schutz, Echtzeit-Schutz** bzw. **Scannen des Computers**, die allesamt die ThreatSense-Technologie verwenden (siehe unten). Je nach Anforderung sind eventuell verschiedene Sicherheitseinstellungen erforderlich. Dies sollte bei den individuellen ThreatSense-Einstellungen für die folgenden Schutzmodule berücksichtigt werden:

- **Systemstart-Schutz** - Automatische Prüfung der Systemstartdateien
- **Echtzeit-Dateischutz** - Echtzeit-Dateischutz
- **Computer prüfen** - On-Demand-Prüfung
- **Web-Schutz**
- **E-Mail-Schutz**

Die ThreatSense-Einstellungen sind für jedes Modul optimal eingerichtet, und eine Veränderung der Einstellungen kann den Systembetrieb deutlich beeinflussen. So kann zum Beispiel eine Änderung der Einstellungen für das Prüfen laufzeitkomprimierter Dateien oder die Aktivierung der Advanced Heuristik im Echtzeit-Dateischutz dazu führen, dass das System langsamer arbeitet. Es wird daher empfohlen, die ThreatSense-Standardeinstellungen für alle Module unverändert beizubehalten. Änderungen sollten nur im Modul „Computer prüfen“ vorgenommen werden.

## Objekte

Im Bereich **Objekte** können Sie festlegen, welche Dateien auf Infiltrationen geprüft werden sollen.

- **Symbolische Links** - (Nur bei Computerprüfung) Prüfung von Dateien, die eine Textfolge enthalten, die vom Betriebssystem ausgewertet und als Pfad zu einer anderen Datei oder einem anderen Verzeichnis genutzt wird.
- **E-Mail-Dateien** - (nicht verfügbar in Echtzeit-Dateischutz) Prüfung von E-Mail-Dateien.
- **Postfächer** - (nicht verfügbar in Echtzeit-Dateischutz) Prüfung von Benutzerpostfächern im System. Die unsachgemäße Anwendung dieser Option kann zu Konflikten mit Ihrem E-Mail-Programm führen. Für weitere Informationen über Vor- und Nachteile dieser Option lesen Sie den folgenden [Knowledgebase-Artikel](#).
- **Archive** - (nicht verfügbar in Echtzeit-Dateischutz) Prüfung komprimierter Archivdateien (.rar, .zip, .arj, .tar usw.).
- **Selbstentpackende Archive** - (nicht verfügbar in Echtzeit-Dateischutz) Prüfung von Dateien in selbstentpackenden Archiven.
- **Laufzeitkomprimierte Dateien** - Laufzeitkomprimierte Dateien werden (anders als Standard-Archivtypen) im Arbeitsspeicher dekomprimiert. Wenn diese Option ausgewählt ist, werden statisch laufzeitkomprimierte Dateien (UPX, yoda, ASPack, FGS etc.) ebenfalls geprüft.

# Optionen

Im Bereich **Optionen** können Sie die Methoden festlegen, die bei einer Prüfung des Systems auf Infiltrationen angewendet werden sollen. Folgende Optionen stehen zur Verfügung:

- **Heuristik** – Heuristische Methoden verwenden einen Algorithmus, der (böartige) Aktivitäten von Programmen analysiert. Hauptvorteil der heuristischen Erkennung ist die Fähigkeit, neue Schadsoftware erkennen zu können, die zuvor noch nicht vorhanden war.
- **Advanced Heuristik** – Als Advanced Heuristik werden besondere, von ESET entwickelte heuristische Verfahren bezeichnet, die für die Erkennung von Würmern und Trojanern optimiert sind, die in höheren Programmiersprachen geschrieben wurden. Die Erkennungsrate des Programms ist dadurch wesentlich gestiegen.

# Säubern

In den Säuberungseinstellungen wird festgelegt, wie der Scanner die infizierten Dateien säubert. Es gibt 3 Arten der Schadcodeentfernung:

- **Nicht säubern** – Der in infizierten Objekten erkannte Schadcode wird nicht automatisch entfernt. Eine Warnung wird angezeigt, und Sie werden aufgefordert, eine Aktion auszuwählen.
- **Normales Säubern** – Das Programm versucht, den Schadcode aus der Datei zu entfernen oder die infizierte Datei zu löschen. Wenn es nicht möglich ist, die passende Aktion automatisch zu bestimmen, wird der Benutzer aufgefordert, eine Aktion auszuwählen. Diese Auswahl wird dem Benutzer auch dann angezeigt, wenn eine vordefinierte Aktion nicht erfolgreich abgeschlossen werden konnte.
- **Automatisch säubern** – Das Programm entfernt den Schadcode aus infizierten Dateien oder löscht diese Dateien (einschließlich Archive). Ausnahmen gelten nur für Systemdateien. Wenn eine Datei nicht gesäubert werden kann, erhalten Sie eine Benachrichtigung und werden aufgefordert, die auszuführende Aktion auszuwählen.



## Archivdateien

Im Standardmodus „Normales Säubern“ werden ganze Archive nur gelöscht, wenn sie ausschließlich infizierte Dateien enthalten. Wenn ein Archiv saubere und infizierte Dateien enthält, wird es nicht gelöscht. Im Modus „Automatisch säubern“ wird die gesamte Archivdatei gelöscht, auch wenn sie nicht infizierte Dateien enthält.



## Archiv-Scan

Im Standardmodus „Normales Säubern“ werden ganze Archive nur gelöscht, wenn sie ausschließlich infizierte Dateien enthalten. Wenn ein Archiv saubere und infizierte Dateien enthält, wird es nicht gelöscht. Im Modus „Automatisch säubern“ wird die gesamte Archivdatei gelöscht, auch wenn sie nicht infizierte Dateien enthält.

# Ausschlussfilter

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

In der Standardeinstellung werden alle Dateien unabhängig von ihrer Erweiterung geprüft. Jede Erweiterung kann der Liste auszuschließender Dateien hinzugefügt werden. Mit den Schaltflächen + und - können Sie die Prüfung bestimmter Erweiterungen aktivieren oder deaktivieren.

Der Ausschluss bestimmter Dateien ist dann sinnvoll, wenn die Prüfung bestimmter Dateitypen die Funktion eines Programms beeinträchtigt. So empfiehlt es sich beispielsweise, Dateien vom Typ *log*, *cfg* und *tmp* auszuschließen. Das korrekte Format für die Angabe von Dateierweiterungen ist:

*log*

*cfg*

*tmp*

## Grenzen

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

- **Maximale Größe:** Definiert die maximale Größe von zu prüfenden Objekten. Wenn eine maximale Größe definiert ist, prüft der Virenschutz nur Elemente, deren Größe unter der angegebenen Maximalgröße liegt. Diese Option sollte nur von fortgeschrittenen Benutzern geändert werden, die bestimmte Gründe dafür haben, größere Objekte von der Prüfung auszuschließen.
- **Maximale Prüfzeit:** Definiert die maximale Dauer, die für die Prüfung eines Objekts zur Verfügung steht. 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.
- **Maximale Verschachtelungstiefe:** Legt die maximale Tiefe der Archivprüfung fest. Der Standardwert 10 sollte nicht geändert werden; unter normalen Umständen besteht dazu auch kein Grund. Wenn die Prüfung aufgrund der Anzahl verschachtelter Archive vorzeitig beendet wird, bleibt das Archiv ungeprüft.
- **Maximale Dateigröße:** Über diese Option können Sie die maximale Dateigröße der entpackten Dateien festlegen, die in zu prüfenden Archiven enthalten sind. Wenn die Prüfung aufgrund dieses Grenzwerts vorzeitig beendet wird, bleibt das Archiv ungeprüft.

## Weitere

### Smart-Optimierung aktivieren

Die Smart-Optimierung passt die Einstellungen so an, dass eine wirksame Prüfung bei gleichzeitig hoher Prüfgeschwindigkeit gewährleistet ist. Die verschiedenen Schutzmodule prüfen auf intelligente Weise unter Einsatz verschiedener Prüfmethoden. Die Smart-Optimierung ist innerhalb des Produkts nicht starr definiert. Das ESET-Entwicklungsteam fügt ständig neue Ergänzungen hinzu, die dann über die regelmäßigen Updates in Ihr ESET Cyber Security integriert werden. Wenn die Smart-Optimierung deaktiviert ist, werden nur die benutzerdefinierten Einstellungen im ThreatSense-Kern des entsprechenden Moduls für die Prüfung verwendet.

### Alternative Datenströme (ADS) prüfen (Nur bei On-Demand-Prüfung)

Bei den von Dateisystemen verwendeten alternativen Datenströmen die vom Dateisystem verwendet werden,

sind Datei- und Ordnerzuordnungen, die mit herkömmlichen Prüfetechniken nicht erkannt werden können. Eindringende Schadsoftware tarnt sich häufig als alternativer Datenstrom, um nicht erkannt zu werden.

## Eingedrungene Schadsoftware wurde erkannt

Schadsoftware kann auf vielen Wegen in das System gelangen. Mögliche Infektionswege sind Webseiten, freigegebene Ordner, E-Mails oder Wechselmedien (USB-Sticks, externe Festplatten, CDs, DVDs usw.).

Wenn Ihr Computer die Symptome einer Malware-Infektion aufweist (Computer arbeitet langsamer als gewöhnlich, hängt sich oft auf usw.), sollten Sie folgendermaßen vorgehen:

1. Klicken Sie auf **Computer prüfen**.
2. Klicken Sie auf **Smart-Prüfung** (weitere Informationen siehe Abschnitt [Smart-Prüfung](#)).
3. Nachdem die Prüfung abgeschlossen ist, überprüfen Sie im Log die Anzahl der geprüften, infizierten und gesäuberten Dateien.

Wenn Sie nur einen Teil Ihrer Festplatte prüfen möchten, wählen Sie **Benutzerdefinierte Prüfung** und anschließend die Bereiche, die auf Viren geprüft werden sollen.

Das folgende allgemeine Beispiel zeigt, wie ESET Cyber Security mit Schadsoftware umgeht. Angenommen, der Echtzeit-Dateischutz verwendet die Standard-Säuberungsstufe und erkennt eine eingedrungene Schadsoftware. Der Echtzeit-Dateischutz wird versuchen, den Schadcode aus der Datei zu entfernen oder die Datei zu löschen. Ist für den Echtzeitschutz keine vordefinierte Aktion angegeben, müssen Sie in einem Warnungsfenster zwischen verschiedenen Optionen wählen. In der Regel stehen die Optionen **Säubern**, **Löschen** und **Keine Aktion** zur Auswahl. Es wird nicht empfohlen, die Option **Keine Aktion** zu wählen, da sonst die infizierte(n) Datei(en) nicht behandelt werden. Wählen Sie diese Option nur, wenn Sie sich sicher sind, dass die Datei harmlos ist und versehentlich erkannt wurde.

### Säubern und löschen

Wählen Sie „Säubern“, wenn eine Datei von einem Virus mit Schadcode infiziert wurde. In einem solchen Fall sollten Sie zuerst versuchen, den Schadcode aus der infizierten Datei zu entfernen und ihren Originalzustand wiederherzustellen. Wenn die Datei ausschließlich Schadcode enthält, wird sie gelöscht.



## Dateien in Archiven löschen

Im Standardmodus der Aktion „Säubern“ wird das gesamte Archiv nur gelöscht, wenn es ausschließlich infizierte Dateien enthält. Archive, die auch nicht infizierte Dateien enthalten, werden also nicht gelöscht. Die Option **Automatisch säubern** sollten Sie hingegen mit Bedacht einsetzen, da in diesem Modus alle Archive gelöscht werden, die mindestens eine infizierte Datei enthalten, und zwar unabhängig vom Status der übrigen Archivdateien.

# Prüfen und Sperren von Wechselmedien

Mit ESET Cyber Security können Sie einen On-Demand-Scan für angeschlossene Wechselmedien (CD, DVD, USB usw.) ausführen. Auf macOS 10.15 kann ESET Cyber Security auch andere externe Mediengeräte scannen.



### Wechselmedien-Scan auf macOS 11 und neuer

Auf macOS 11 und neueren Betriebssystemen kann ESET Cyber Security nur Speichergeräte scannen.



Auf Wechselmedien kann sich Schadcode befinden, der eine Gefahr für Ihren Computer darstellt. Um Wechselmedien zu sperren, klicken Sie entweder auf **Einstellungen für Wechselmedien-Sperre** (siehe Abbildung oben) oder im Hauptfenster auf **Einstellungen > Erweiterte Einstellungen > Medien** und aktivieren Sie die Option **Sperre für Wechselmedien aktivieren**. Um den Zugriff auf bestimmte Medientypen zuzulassen, deaktivieren Sie das jeweilige Kontrollkästchen.



### CD-ROM-Zugriff

Um den Zugriff auf externe CD-ROM-Laufwerke zuzulassen, die über ein USB-Kabel an Ihren Computer angeschlossen sind, deaktivieren Sie die Option **CD-ROM**.

# Phishing-Schutz

Der Begriff Phishing bezeichnet eine kriminelle Vorgehensweise, die sich Social Engineering-Techniken (Manipulation von Benutzern zur Erlangung vertraulicher Informationen) zunutze macht. Phishing wird oft eingesetzt, um Zugriff auf vertrauliche Informationen wie Bankkontonummern, Kreditkartendaten, PIN-Nummer oder Benutzernamen und Passwörter zu erlangen.

Wir empfehlen, den Phishing-Schutz aktiviert zu lassen (**Einstellungen > Erweiterte Einstellungen > Phishing-Schutz**). Alle potenziellen Phishing-Angriffe von gefährlichen Webseiten oder Domänen werden blockiert, und Sie erhalten einen Warnhinweis über den Angriffsversuch.

# Web- und E-Mail-Schutz

Um den Web- und E-Mail-Schutz aus dem Hauptmenü zu öffnen, klicken Sie auf **Einstellungen > Web und E-Mail**. Dort können Sie auch auf ausführliche Einstellungen für die einzelnen Module zugreifen, indem Sie auf **Einstellungen** klicken.

- **Web-Schutz** – Der Web-Schutz überwacht die HTTP-Kommunikation zwischen Webbrowsern und Remoteservern.
- **E-Mail-Client-Schutz** – Überwacht eingehende E-Mails, die mit dem POP3- und dem IMAP-Protokoll übertragen werden.
- **Phishing-Schutz** – Blockiert potenzielle Phishing-Angriffe von Websites oder Domänen.



## Scan-Ausnahmen

ESET Cyber Security führt keine Scans der verschlüsselten Protokolle HTTPS, POP3S und IMAPS durch.

## Web-Schutz

Der Web-Schutz dient zur Überwachung von Verbindungen zwischen Webbrowsern und Remote-Servern nach dem HTTP-Protokoll (Hypertext Transfer Protocol).

Sie können die Webfilterung aktivieren, indem Sie [Portnummern für die HTTP-Kommunikation](#) und/oder [URL-Adressen](#) definieren.

## Ports

Auf der Registerkarte **Ports** können Sie die für HTTP-Verbindungen verwendeten Portnummern definieren. In der Standardeinstellung sind die Portnummern 80, 8080 und 3128 vorgegeben.

## URL-Listen

Im Bereich **URL-Listen** können Sie HTTP-Adressen angeben, die gesperrt, zugelassen oder von der Prüfung ausgeschlossen werden sollen. Auf Websites in der Liste der gesperrten Adressen kann nicht zugegriffen werden. Auf Websites in der Liste der ausgeschlossenen Adressen kann zugegriffen werden, ohne dass diese auf Schadcode überprüft werden.

Wenn Sie nur die unter **Zugelassene URL** aufgeführten URL-Adressen zulassen möchten, wählen Sie die Option **URL-Zugriff einschränken**.

Um eine Liste zu aktivieren, markieren Sie **Aktiviert** neben dem Listennamen. Wenn Sie benachrichtigt werden möchten, wenn Sie eine Adresse aus der gegenwärtigen Liste eingeben, wählen Sie die Option **Hinweise anzeigen**.

In allen Listen können die Platzhalterzeichen \* (Sternchen) und ? (Fragezeichen) verwendet werden. Das Sternchen steht für eine beliebige Zeichenfolge, das Fragezeichen für ein beliebiges Zeichen. Die Liste der

ausgeschlossenen Adressen sollten Sie mit Bedacht zusammenstellen. Geben Sie ausschließlich vertrauenswürdige und sichere Adressen an. Achten Sie außerdem darauf, dass die Zeichen „\*“ und „?“ korrekt verwendet werden.

## E-Mail-Schutz

Der E-Mail-Schutz dient der Überwachung eingehender E-Mails, die mit dem POP3-Protokoll übertragen werden. Für die Prüfung eingehender Nachrichten verwendet ESET Cyber Security alle erweiterten ThreatSense-Prüfmethoden. Die POP3- und IMAP-Kommunikation wird unabhängig vom verwendeten E-Mail-Programm geprüft.

**ThreatSense-Modul: Einstellungen** – In den erweiterten Prüfeinstellungen können Sie zu prüfende Objekte, Erkennungsmethoden usw. konfigurieren. Klicken Sie auf **Einstellungen**, um die ausführlichen Prüfeinstellungen anzuzeigen.

**Prüfhinweise am Ende der E-Mail hinzufügen** – An jede geprüfte E-Mail wird ein Prüfhinweis mit den Prüfergebnissen angehängt. Tag-Nachrichten sind hilfreich, sollten aber nicht zur abschließenden Bestimmung der Sicherheit einer Nachricht verwendet werden, da sie in problematischen HTML-Nachrichten unter Umständen ausgelassen und von bestimmten Bedrohungen gefälscht werden können. Folgende Optionen stehen zur Verfügung:

- **Nie** – Es werden keine Prüfhinweise hinzugefügt.
- **Nur bei infizierten E-Mails** – Nur Nachrichten mit Schadsoftware werden als geprüft gekennzeichnet.
- **Bei allen geprüften E-Mails** – Alle geprüften E-Mails werden mit Prüfhinweisen versehen.

**Prüfhinweis an den Betreff empfangener und gelesener infizierter E-Mails anhängen** – Aktivieren Sie dieses Kontrollkästchen, um infizierte E-Mails zu kennzeichnen. Auf diese Weise können infizierte Nachrichten leicht gefiltert werden. Die Warnung erhöht außerdem die Glaubwürdigkeit beim Empfänger und bietet beim Erkennen einer Infiltration wertvolle Informationen zur Gefährdung durch eine bestimmte E-Mail oder einen Absender.

**Text, der zur Betreffzeile infizierter E-Mails hinzugefügt wird** – Hier können Sie das Betreffpräfix für infizierte E-Mails bearbeiten.

- %avstatus% – Fügt den Infektionsstatus der E-Mail hinzu („nicht infiziert“, „infiziert“ usw.)
- %virus% – Fügt den Namen der Bedrohung hinzu
- %aspmstatus% – Ändert den Betreff je nach Ergebnis des Spamschutz-Scans
- %product% – Fügt den Namen Ihres ESET-Produkts hinzu (in diesem Fall „ESET Cyber Security“)
- %product\_url% – Fügt einen Link zur ESET-Website hinzu ([www.eset.com](http://www.eset.com))

Im unteren Teil dieses Fensters können Sie die Prüfung für E-Mails aktivieren/deaktivieren, die über die POP3- und IMAP-Protokolle empfangen wurden. Weitere Informationen finden Sie in den folgenden Artikeln:

- [Prüfen von E-Mails per POP3-Protokoll](#)
- [Scannen des IMAP-Protokolls](#)

## Prüfen von E-Mails per POP3-Protokoll

Das POP3-Protokoll ist das am weitesten verbreitete Protokoll für den Empfang von E-Mails mit einer E-Mail-Client-Anwendung. ESET Cyber Security bietet Schutz für dieses Protokoll unabhängig vom verwendeten E-Mail-Client.

Das Modul für diesen Schutz wird beim Systemstart automatisch gestartet und bleibt danach im Arbeitsspeicher aktiv. Vergewissern Sie sich, dass das Modul aktiviert ist, damit die Protokollfilterung ordnungsgemäß funktioniert. Die POP3-Prüfung erfolgt automatisch; Sie brauchen ihren E-Mail-Client nicht neu zu konfigurieren. Standardmäßig wird der gesamte Datenverkehr über Port 110 geprüft; weitere Kommunikationsports können bei Bedarf hinzugefügt werden. Die Portnummern müssen mit einem Komma voneinander getrennt werden.

Wenn die Option **POP3-Prüfung aktivieren** aktiviert ist, wird der gesamte POP3-Datenverkehr auf Schadsoftware geprüft.

## Prüfen von E-Mails per IMAP-Protokoll

Das Internet Message Access Protocol (IMAP) ist ein weiteres Internetprotokoll für den Abruf von E-Mails. IMAP bietet gegenüber POP3 einige Vorteile. Beispielsweise können sich mehrere Clients gleichzeitig beim selben Postfach anmelden und Statusinformationen zu den Nachrichten pflegen, z. B. ob die Nachricht gelesen, beantwortet oder gelöscht wurde. ESET Cyber Security schützt dieses Protokoll unabhängig vom eingesetzten E-Mail-Programm.

Das Modul für diesen Schutz wird beim Systemstart automatisch gestartet und bleibt danach im Arbeitsspeicher aktiv. Vergewissern Sie sich, dass die IMAP-Prüfung aktiviert ist, damit das Modul ordnungsgemäß funktioniert. Die IMAP-Prüfung erfolgt automatisch; Sie brauchen ihren E-Mail-Client nicht neu zu konfigurieren. Standardmäßig wird der gesamte Datenverkehr über Port 143 geprüft; weitere Kommunikationsports können bei Bedarf hinzugefügt werden. Die Portnummern müssen mit einem Komma voneinander getrennt werden.

Wenn die Option **IMAP-Prüfung aktivieren** aktiviert ist, wird der gesamte IMAP-Datenverkehr auf Schadsoftware geprüft.

## Update

Für optimalen Schutz muss ESET Cyber Security regelmäßig aktualisiert werden. Das Modul-Update lädt fortlaufend die neuesten Erkennungsroutinen herunter, um das Programm stets auf dem neuesten Stand zu halten.

Über den Punkt **Update** im Hauptmenü können Sie sich den aktuellen Update-Status von ESET Cyber Security anzeigen lassen. Hier sehen Sie Datum und Uhrzeit des letzten Updates und können feststellen, ob ein Update erforderlich ist. Klicken Sie auf **Modul-Update**, um den Update-Vorgang manuell zu starten.

Wenn beim Update-Download keinerlei Zwischenfälle auftreten, wird im Update-Fenster der Hinweis **Update nicht erforderlich - die installierten Module sind auf dem neuesten Stand** angezeigt. Wenn das Modul-Update fehlschlägt, sollten Sie die [Update-Einstellungen](#) überprüfen. Die häufigste Fehlerursache sind falsch eingegebene Lizenzdaten (Benutzername/Passwort) oder fehlerhaft konfigurierte [Verbindungseinstellungen](#).

Die Versionsnummer der Erkennungsroutine wird ebenfalls im Update-Fenster angezeigt. Die Versionsnummer ist mit der ESET-Webseite verknüpft, die Informationen zum Update der Erkennungsroutine enthält.

## Einstellungen für Updates

Um alle vorübergehend gespeicherten Update-Daten zu löschen, klicken Sie auf **Leeren** neben **Update-Cache leeren**. Dies kann helfen, wenn Probleme beim Update auftreten.

## Erweiterte Einstellungen

Um die Benachrichtigungen zu erfolgreichen Updates zu deaktivieren, wählen Sie **Keine Benachrichtigung über erfolgreiche Updates anzeigen** aus.

Aktivieren Sie die Option **Pre-Release-Update**, um Entwicklungmodule herunterzuladen, die sich in der letzten Testphase befinden. Pre-Release-Updates enthalten oft Korrekturen für Probleme im Produkt. Mit der Option **Verzögerte Updates** werden Updates einige Stunden nach der Veröffentlichung heruntergeladen, um sicherzustellen, dass die Kunden diese Updates erst dann erhalten, wenn diese nachweislich frei von Problemen sind.

ESET Cyber Security zeichnet Snapshots der Erkennungsroutine und der Programmmodule zur späteren Verwendung mit der Funktion **Update-Rollback** auf. Lassen Sie **Snapshots der Update-Dateien erstellen** aktiviert, um diese Snapshots automatisch in ESET Cyber Security zu erfassen. Wenn Sie befürchten, dass ein neues Update der Erkennungsroutine und/oder eines Programmmoduls beschädigt oder nicht stabil ist, können Sie einen Rollback zur vorigen Version ausführen und Updates für einen bestimmten Zeitraum deaktivieren. Klicken Sie auf **Rollback**, um Updates auf die älteste Version im Verlauf zurückzusetzen. Alternativ können Sie zuvor deaktivierte Updates, die Sie auf unbestimmte Zeit verschoben haben, aktivieren. Wenn Sie mit der Update-Rollback-Funktion ein früheres Update wiederherstellen möchten, geben Sie im Dropdown-Menü **Dauer für Aussetzen festlegen auf** die Dauer an, für die Updates ausgesetzt werden sollen. Mit der Option **bis zum Widerrufen** finden normale Updates erst wieder statt, wenn Sie sie manuell wiederherstellen. Klicken Sie auf **Erlauben**, um Updates manuell wiederherzustellen. Gehen Sie beim Festlegen der Zeitdauer zum Aussetzen von Updates mit Bedacht vor.

**Maximales Alter der Erkennungsroutine automatisch festlegen** – Hier können Sie eine Zeitdauer (in Tagen) festlegen, nach der die Erkennungsmodule spätestens als veraltet gemeldet werden. Der Standardwert ist 7 Tage.

## So erstellen Sie Update-Tasks

Updates können manuell durch Klicken auf **Update** im Hauptmenü und anschließendes Klicken auf **Modul-Update** ausgelöst werden.

Darüber hinaus können Sie Updates auch als geplante Tasks einrichten. Um einen Task zu konfigurieren, klicken Sie auf **Tools > Taskplaner**. Standardmäßig sind in ESET Cyber Security folgende Tasks aktiviert:

- **Automatische Updates in festen Zeitabständen**
- **Automatische Updates beim Anmelden des Benutzers**

Diese Update-Tasks können bei Bedarf bearbeitet werden. Neben den standardmäßig ausgeführten Update-Tasks können zusätzliche Update-Tasks mit benutzerdefinierten Einstellungen erstellt werden. Weitere Informationen zum Erstellen und Konfigurieren von Update-Tasks finden Sie im Abschnitt [Taskplaner](#).

## Upgrade von ESET Cyber Security auf eine neue Version

Um maximalen Schutz zu gewährleisten, ist es wichtig, immer das neueste Build von ESET Cyber Security zu verwenden. Klicken Sie auf **Startseite** im Hauptmenü, um zu prüfen, ob eine neue Version verfügbar ist. Wenn ein neues Build verfügbar ist, wird eine entsprechende Meldung angezeigt. Klicken Sie auf **Mehr Informationen**, um ein neues Fenster mit der Versionsnummer des neuen Builds und dem Änderungsprotokoll anzuzeigen.

Klicken Sie auf **Ja**, um das aktuelle Build herunterzuladen, oder auf **Jetzt nicht**, um das Fenster zu schließen und das Upgrade später herunterzuladen.

Wenn Sie auf **Ja** geklickt haben, wird die Datei heruntergeladen und in Ihrem Download-Ordner (oder in dem von Ihrem Browser festgelegten Standardordner) abgelegt. Führen Sie nach Abschluss des Downloads die Datei aus und folgen Sie den Installationsanweisungen. Ihr Benutzername und Passwort werden automatisch bei der neuen Installation übernommen. Es wird empfohlen, regelmäßig auf verfügbare Upgrades zu prüfen, insbesondere wenn ESET Cyber Security von einer CD oder DVD installiert wird.

## Systemupdates

Die Systemupdatefunktion für macOS ist eine wichtige Komponente zum Schutz des Benutzers vor Schadcode. Zur Gewährleistung des bestmöglichen Schutzes empfohlen wird, die Updates möglichst umgehend zu installieren, sobald sie verfügbar sind. ESET Cyber Security zeigt je nach den von Ihnen festgelegten Einstellungen Benachrichtigungen zu fehlenden Updates an. Sie können diese Benachrichtigungseinstellungen für Updates unter **Einstellungen > Erweiterte Einstellungen ...** (oder drücken Sie *cmd+,*) > **Warnungen und Hinweise > Einstellungen...** anpassen. Ändern Sie dazu die Optionen unter **Anzeigebedingungen** neben dem Eintrag **Betriebssystem-Updates**.

- **Alle Updates anzeigen** - Benachrichtigungen werden für alle fehlenden Updates angezeigt.
- **Nur empfohlene Updates anzeigen** - Benachrichtigungen werden nur für empfohlene Updates angezeigt.

Wenn Sie keine Benachrichtigungen zu fehlenden Updates erhalten möchten, deaktivieren Sie das Kontrollkästchen neben **Betriebssystem-Updates**.

Das Benachrichtigungsfenster enthält eine Übersicht der verfügbaren Updates für das macOS-Betriebssystem und für die Anwendungen, die über das native macOS-Tool für Software-Updates aktualisiert werden. Sie können das Update direkt über das Benachrichtigungsfenster ausführen oder über die **Startseite** von ESET Cyber Security, indem Sie hier auf **Fehlendes Update installieren** klicken.

Das Benachrichtigungsfenster enthält den Anwendungsnamen, die Version, die Größe, Eigenschaften (Flags) und zusätzliche Informationen zu den verfügbaren Updates. Die Flags-Spalte enthält folgende Informationen:

- **[empfohlen]** - Der Hersteller des Betriebssystem empfiehlt die Installation dieses Updates, um die Sicherheit und Stabilität des Systems zu verbessern.
- **[Neustart]** - Nach der Installation ist ein Neustart des Computers erforderlich.
- **[Herunterfahren]** - Der Computer muss heruntergefahren und nach der Installation wieder eingeschaltet werden.

Das Benachrichtigungsfenster zeigt die vom Befehlszeilenwerkzeug 'softwareupdate' abgerufenen Updates an. Die von diesem Werkzeug abgerufenen Updates können sich von den in der Anwendung 'Software Updates' angezeigten Updates unterscheiden. Wenn Sie alle im Fenster 'Fehlende Systemupdates' angezeigten, verfügbaren Updates installieren möchten, einschließlich der nicht in der Anwendung 'Software Updates' angezeigten Updates, verwenden Sie das Befehlszeilenwerkzeug 'softwareupdate'. Weitere Informationen zu diesem Werkzeug finden Sie im Handbuch zu 'softwareupdate', auf das Sie durch Eingabe des Befehls `man softwareupdate` in einem Terminalfenster zugreifen können. Wir empfehlen die Nutzung des Werkzeugs nur für fortgeschrittene Benutzer.

# Tools

Das Menü **Tools** enthält Module zur einfacheren Verwaltung des Programms sowie zusätzliche Optionen für fortgeschrittene Benutzer.

## Log-Dateien

Die Log-Dateien enthalten Informationen zu wichtigen aufgetretenen Programmereignissen und geben einen Überblick über erkannte Bedrohungen. Das Erstellen von Logs ist unabdingbar für die Systemanalyse, die Erkennung von Problemen oder Risiken sowie die Fehlerbehebung. Die Logs werden im Hintergrund ohne Eingriffe des Benutzers erstellt. Welche Informationen aufgezeichnet werden, ist abhängig von den aktuellen Einstellungen für die Mindestinformation in Logs. Textnachrichten und Logs können direkt aus ESET Cyber Security heraus angezeigt werden. Das Archivieren von Logs erfolgt ebenfalls direkt über das Programm.

Log-Dateien können über das Hauptfenster von ESET Cyber Security aufgerufen werden, indem Sie auf **Tools > Logs** klicken. Wählen Sie in der Liste **Log** im oberen Bereich des Fensters das gewünschte Log aus. Folgende Logs sind verfügbar:

1. **Erkannte Bedrohungen** - Über diese Option können Sie sämtliche Informationen über Ereignisse bezüglich der Erkennung eingedrungener Schadsoftware anzeigen.
2. **Ereignisse** - Diese Option unterstützt Systemadministratoren und Benutzer bei der Behebung von Problemen. Alle von ESET Cyber Security ausgeführten wichtigen Aktionen werden in den Ereignis-Logs aufgezeichnet.
3. **Computer prüfen** - In diesem Log werden die Ergebnisse aller durchgeführten Prüfungen angezeigt. Durch Doppelklicken auf einen Eintrag können Sie Einzelheiten zu der entsprechenden On-Demand-Prüfung anzeigen.
4. **Gefilterte Websites** - Diese Liste ist nützlich, wenn Sie sehen möchten, welche Websites vom Web-Schutz blockiert wurden. Diese Logs bieten Aufschluss über Uhrzeit, URL, Status, IP-Adresse, Benutzer und Anwendung, von der aus eine Verbindung zur jeweiligen Website hergestellt wurde.

In jedem Abschnitt können die angezeigten Informationen direkt in die Zwischenablage kopiert werden. Dazu wählen Sie die gewünschten Einträge aus und klicken auf **Kopieren**.

## Log-Wartung

Die Log-Konfiguration für ESET Cyber Security können Sie aus dem Hauptprogrammfenster aufrufen. Klicken Sie auf **Einstellungen > Erweiterte Einstellungen** (oder drücken Sie *cmd+,*) > **Log-Dateien**. Für Log-Dateien können die folgenden Einstellungen vorgenommen werden:

- **Alte Log-Einträge automatisch löschen** - Log-Einträge, die älter als die angegebene Anzahl Tage sind, werden automatisch gelöscht (der Standardwert beträgt 90 Tage).
- **Log-Dateien automatisch optimieren** - Die Logs werden beim Erreichen des vordefinierten Fragmentierungsgrads automatisch optimiert (der Standardwert beträgt 25 %).

Alle relevanten Informationen in der grafischen Benutzeroberfläche sowie Bedrohungs- und Ereignisnachrichten können in menschenlesbarer Textform gespeichert werden, z. B. in Nur-Text- oder CSV-Dateien (Comma-

separated values). Wenn Sie diese Dateien zur weiteren Verarbeitung in Drittanbieter-Tools verfügbar machen möchten, aktivieren Sie das Kontrollkästchen neben **Protokollierung in Textdateien aktivieren**.

Um den Zielordner für die Log-Dateien festzulegen, klicken Sie auf **Einstellungen** neben **Erweiterte Einstellungen**.

Je nach den unter **Log-Textdateien: Bearbeiten** ausgewählten Optionen können Log-Dateien mit folgenden Informationen gespeichert werden:

o Ereignisse wie *Ungültiger Benutzername/ungültiges Passwort, Module konnten nicht aktualisiert werden* usw. werden in der Datei eventslog.txt gespeichert.

o Durch den Systemstart-Scanner, den Echtzeit-Dateischutz oder die Computerprüfung erkannte Bedrohungen werden in der folgenden Datei gespeichert: threatslog.txt

o Die Ergebnisse aller durchgeführten Scans werden im Format scanlog.NUMMER.txt gespeichert.

Um die Filter für **Standardcomputer-Scanprotokolleinträge** zu konfigurieren, klicken Sie auf **Bearbeiten** und aktivieren bzw. deaktivieren Sie die einzelnen Log-Typen je nach Bedarf. Weitere Erläuterungen zu diesen Log-Typen finden Sie unter [Log-Filter](#).

## Log-Filter

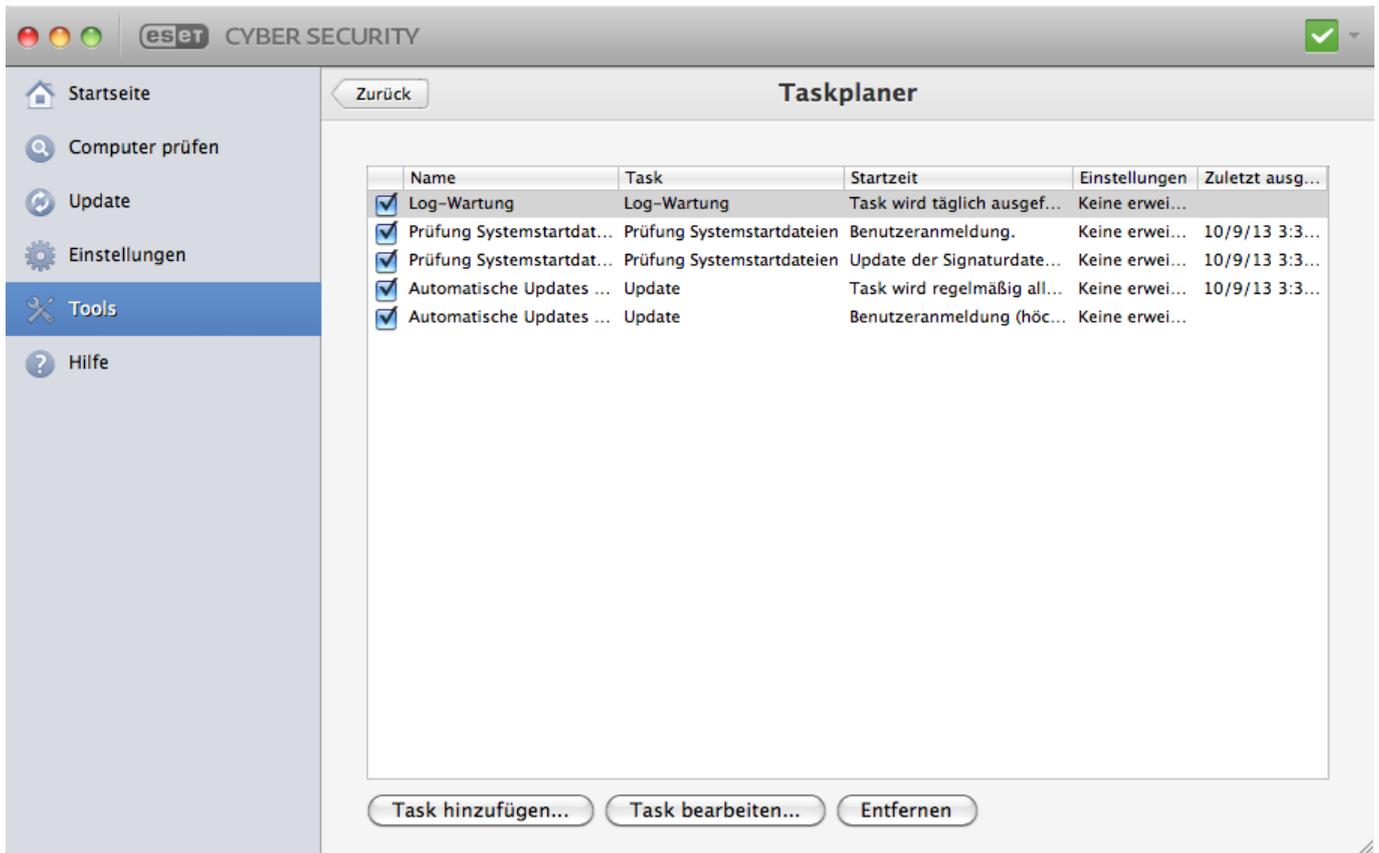
In den Logs werden Informationen über wichtige Systemereignisse gespeichert. Mit dem Log-Filter können Sie sich gezielt Einträge zu einer bestimmten Ereignisart anzeigen lassen.

Die gängigsten Eintragsarten sind:

- **Kritische Warnungen** - Kritische Systemfehler (z. B. „Virenschutz konnte nicht gestartet werden“)
- **Fehler** - Fehler wie z. B. „Fehler beim Herunterladen einer Datei“ und kritische Fehler
- **Warnungen** - Warnmeldungen
- **Informationen** - Meldungen wie erfolgreiche Updates, Warnungen usw.
- **Diagnosedaten** - Alle bisher genannten Einträge sowie Informationen, die für die Feineinstellung des Programms erforderlich sind.

## Taskplaner

Um den Taskplaner zu öffnen, klicken Sie im Hauptmenü von ESET Cyber Security unter **Tools** auf **Taskplaner**. Der **Taskplaner** umfasst eine Liste aller geplanten Tasks sowie deren Konfigurationseigenschaften, inklusive des vordefinierten Datums, der Uhrzeit und des verwendeten Prüfprofils.



Der Taskplaner verwaltet und startet geplante Tasks mit vordefinierter Konfiguration und voreingestellten Eigenschaften. Konfiguration und Eigenschaften enthalten Informationen wie Datum und Uhrzeit und bestimmte Profile, die bei Ausführung des Tasks verwendet werden.

Standardmäßig werden im Taskplaner die folgenden Tasks angezeigt:

- Log-Wartung (nach Aktivieren der Option **System-Tasks anzeigen** in den Taskplaner-Einstellungen)
- Prüfung Systemstartdateien nach Anmeldung des Benutzers
- Scannen der Systemstartdateien nach erfolgreichem Update der Erkennungsroutinen
- Automatische Updates in festen Zeitabständen
- Automatische Updates beim Anmelden des Benutzers

Um die Konfiguration eines vorhandenen Standardtasks oder eines benutzerdefinierten Tasks zu ändern, halten Sie die Ctrl-Taste gedrückt und klicken Sie auf den Task und dann auf **Bearbeiten**. Alternativ können Sie den Task, den Sie ändern möchten, auswählen und dann auf **Task bearbeiten** klicken.

## Erstellen von Tasks

Um einen Task im Taskplaner zu erstellen, klicken Sie auf **Task hinzufügen...** oder halten die Strg-Taste gedrückt, klicken auf das leere Feld und wählen im Kontextmenü die Option **Hinzufügen...** aus. Es gibt fünf Arten von Tasks:

- **Anwendung starten**
- **Update**
- **Log-Wartung**

- On-Demand-Scan
- Scan der Systemstartdateien



### Anwendung starten

Wenn Sie **Anwendung ausführen** auswählen, können Sie Programme mit dem Systembenutzer „nobody“ („niemand“) ausführen. Die Berechtigungen zum Ausführen von Anwendungen über den Taskplaner werden in macOS definiert. Falls Sie nicht den Standardbenutzer verwenden möchten, geben Sie den Benutzernamen gefolgt von einem Doppelpunkt (:) vor dem Befehl ein. Sie können auch den Benutzer **root** für diese Funktion verwenden.



### Beispiel: Task als Benutzer ausführen

In diesem Beispiel starten wir die Rechner-App zu einer festgelegten Uhrzeit als Benutzer **UserOne**:

1. Wählen Sie im **Taskplaner** die Option **Task hinzufügen** aus.
2. Geben Sie einen Tasknamen ein. Wählen Sie **Anwendung ausführen** für den **geplanten Task** aus. Wählen Sie im Fenster **Task ausführen** die Option **Einmalig** aus, um den Task ein einziges Mal auszuführen. Klicken Sie auf **Weiter**.
3. Klicken Sie auf „Durchsuchen“, und wählen Sie die Rechner-App aus.
4. Geben Sie **UserOne:** vor dem Anwendungspfad ein (UserOne:'/Applications/Calculator.app/Contents/MacOs/Calculator') und klicken Sie auf **Weiter**.
5. Wählen Sie eine Uhrzeit für die Ausführung des Tasks aus und klicken Sie auf **Weiter**.
6. Wählen Sie eine alternative Option aus, falls der Task nicht ausgeführt werden kann, und klicken Sie auf **Weiter**.
7. Klicken Sie auf **Fertig stellen**.
8. Der ESET-Taskplaner startet die Rechner-App zu dem Zeitpunkt, den Sie ausgewählt haben.



### Beispiel: Update-Task

In diesem Beispiel erstellen wir einen Update-Task, der zu einer bestimmten Uhrzeit ausgeführt wird.

1. Wählen Sie im Dropdownmenü **Geplanter Task** die Option **Update** aus.
2. Geben Sie im Feld **Taskname** den Namen des Tasks ein.
3. Wählen Sie im Dropdownmenü **Task ausführen** das gewünschte Ausführungsintervall aus. Je nach ausgewähltem Intervall werden Sie aufgefordert, verschiedene Update-Parameter festzulegen. Wenn Sie **Benutzerdefiniert** auswählen, werden Sie aufgefordert, Datum und Uhrzeit im cron-Format anzugeben (weitere Informationen finden Sie unter [Erstellen eines benutzerdefinierten Tasks](#)).
4. Im nächsten Schritt legen Sie eine Aktion für den Fall fest, dass der Task zur geplanten Zeit nicht ausgeführt oder abgeschlossen werden kann.
5. Im letzten Schritt wird eine Übersicht der Einstellungen zum geplanten Task angezeigt. Klicken Sie auf **Fertig stellen**. Der neue geplante Task wird der Liste der aktuellen Tasks hinzugefügt.

Einige Tasks sind für die ordnungsgemäße Funktion des Systems unerlässlich und standardmäßig in ESET Cyber Security enthalten. Diese System-Tasks sind standardmäßig ausgeblendet und sollten nicht modifiziert werden. Um diese Tasks anzuzeigen, klicken Sie im Hauptmenü auf **Einstellungen > Erweiterte Einstellungen** (oder drücken *cmd+,*) > **Taskplaner** und aktivieren die Option **System-Tasks anzeigen**.

## Scannen als Verzeichnisbesitzer

Sie können Verzeichnisse als Besitzer scannen:

```
root:for VOLUME in /Volumes/*; do sudo -u \#`stat -  
f %u "$VOLUME" ` '/Applications/ESET Cyber Security.app/Contents/MacOS/esets_scan' -  
f /tmp/scan_log "$VOLUME"; done
```

Außerdem können Sie den Ordner /tmp als aktuell angemeldeter Benutzer scannen:

```
root:sudo -u \#`stat -  
f %u /dev/console ` '/Applications/ESET Cyber Security.app/Contents/MacOS/esets_scan'  
/tmp
```

## Erstellen von benutzerdefinierten Tasks

Datum und Uhrzeit von **benutzerdefinierten** Tasks müssen im cron-Langformat mit Jahr angegeben werden (Zeichenfolge aus 6 Feldern, jeweils getrennt durch ein Whitespace-Zeichen):

Minute(0-59) Stunde(0-23) Tag(1-31) Monat(1-12) Jahr(1970-2099)  
Wochentag(0-7) (Sonntag = 0 oder 7)

Beispiel:

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

In cron-Ausdrücken werden die folgenden Sonderzeichen unterstützt:

- Sternchen (\*) - Steht für alle möglichen Werte des betreffenden Felds. Beispiel: Sternchen im dritten Feld (Tag) = jeder Tag im Monat
- Bindestrich (-) - Definition von Zeiträumen, z. B. 3-9
- Komma (,) - Trennt mehrere Einträge einer Liste, z. B. 1,3,7,8
- Schrägstrich (/) -Definition von Intervallen in Zeiträumen, z. B. 3-28/5 im dritten Feld (Tag des Monats) = am 3. des Monats und anschließend alle 5 Tage.

Textbezeichnungen für Tage (Monday-Sunday) und Monate (January-December) werden nicht unterstützt.



### Ausführen von Befehlen

Werden sowohl Tag als auch Wochentag angegeben, so wird der Befehl nur ausgeführt, wenn beide Bedingungen erfüllt sind.

## 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 Cyber Security fälschlicherweise erkannt worden sind.

Sie können beliebige Dateien gezielt in die Quarantäne verschieben. Geschehen sollte dies bei Dateien, die sich verdächtig verhalten, bei der Virenprüfung jedoch nicht erkannt werden. Dateien aus der Quarantäne können zur Analyse an ESET eingereicht werden.

Die Dateien im Quarantäneordner können in einer Tabelle angezeigt werden, die Datum und Uhrzeit der Quarantäne, den Pfad zum ursprünglichen Speicherort der infizierten Datei, ihre Größe in Byte, einen Grund (Hinzugefügt durch Benutzer...) und die Anzahl der Bedrohungen (z. B. bei Archiven, in denen an mehreren Stellen Schadcode erkannt wurde) enthält. Das Quarantäneverzeichnis () verbleibt auch nach der Deinstallation von ESET Cyber Security im System. Die Quarantäne-dateien werden sicher verschlüsselt gespeichert und können nach der Reinstallation von ESET Cyber Security wiederhergestellt werden.

## Quarantäne für Dateien

ESET Cyber Security kopiert gelöschte Dateien automatisch in den Quarantäneordner (sofern diese Option nicht im Warnfenster deaktiviert wurde). Auf Wunsch können Sie beliebige verdächtige Dateien manuell in die Quarantäne verschieben, indem Sie auf **Quarantäne** klicken. . Alternativ kann auch das Kontextmenü zu diesem Zweck verwendet werden: Halten Sie die Ctrl-Taste gedrückt, klicken Sie in das leere Feld, wählen Sie **Quarantäne**, wählen Sie die Datei, die in die Quarantäne verschoben werden soll, und klicken Sie auf **Öffnen**.

## Wiederherstellen aus Quarantäne

in Quarantäne befindliche Dateien können auch an ihrem ursprünglichen Speicherort wiederhergestellt werden. Wählen Sie hierzu eine Datei aus dem Quarantäneordner aus und klicken Sie auf **Wiederherstellen**. Die Option „Wiederherstellen“ ist auch im Kontextmenü verfügbar. Klicken Sie bei gedrückter STRG-Taste auf eine Datei im Fenster „Quarantäne“ und anschließend auf **Wiederherstellen**. Das Kontextmenü enthält außerdem die Option **Wiederherstellen nach**, mit der Dateien an einem anderen als ihrem ursprünglichen Speicherort wiederhergestellt werden können.

## Einreichen von Dateien aus der Quarantäne

Wenn Sie eine verdächtige, nicht vom Programm erkannte Datei in Quarantäne versetzt haben oder wenn eine Datei fälschlich als infiziert eingestuft wurde (etwa durch die heuristische Analyse des Codes) und infolgedessen in den Quarantäneordner verschoben wurde, senden Sie die Datei zur Analyse an ESET. Um eine Datei zu senden, die in der Quarantäne gespeichert ist, klicken Sie mit der rechten Maustaste darauf und wählen im angezeigten Kontextmenü die Option **Datei zur Analyse einreichen**.

## Ausgeführte Prozesse

Die Liste **Ausgeführte Prozesse** zeigt die auf Ihrem Computer ausgeführten Prozesse an. ESET Cyber Security liefert detaillierte Informationen zu den ausgeführten Prozessen, um Benutzern den Schutz der ESET Live Grid-Technologie zu bieten.

- **Prozess** - Name des aktuell auf Ihrem Computer ausgeführten Prozesses. Sie können sämtliche ausgeführten Prozesse auch in der Aktivitätsanzeige (*/Programme/Dienstprogramme*) anzeigen.
- **Risikostufe** - In den meisten Fällen weisen ESET Cyber Security und die ESET Live Grid-Technologie den Objekten (Dateien, Prozesse usw.) eine Risikostufe zu. Dies erfolgt unter Einsatz einer Reihe heuristischer Regeln, die die Eigenschaften des Objekts untersuchen und auf dieser Grundlage den Verdacht auf Schadcode abwägen. Den Objekten wird auf Grundlage dieser heuristischen Regeln eine Risikostufe zugewiesen. Bekannte Anwendungen, die grün markiert und bekanntermaßen keinen Schadcode enthalten (Positivliste), werden von der Prüfung ausgeschlossen. Dies sorgt für eine schnellere On-Demand- und Echtzeit-Prüfung. Eine als

unbekannt eingestufte Anwendung (gelb) enthält nicht unbedingt Schadcode. Meist handelt es sich einfach um eine neuere Anwendung. Wenn Sie sich bei einer Datei nicht sicher sind, können Sie sie zur Analyse an unser Virenlabor einreichen. Wenn sich herausstellt, dass die Datei Schadcode enthält, wird deren Signatur zukünftigen Updates hinzugefügt.

- **Anzahl Benutzer** - gibt die Anzahl der Benutzer an, die eine bestimmte Anwendung verwenden. Diese Information wird durch die ESET Live Grid-Technologie erfasst.
- **Erkennungszeit** - gibt an, wann die Anwendung von der ESET LiveGrid®-Technologie erkannt wurde.
- **Anwendungspaket-ID** - Name des Herstellers oder des Anwendungsprozesses.

Wenn Sie auf einen Prozess klicken, werden am unteren Bildschirmrand folgende Informationen angezeigt:

- **Datei** - Speicherort der Anwendung auf Ihrem Computer
- **Dateigröße** - physikalische Größe der Datei auf dem Datenträger
- **Dateibeschreibung** - Dateieigenschaften auf Grundlage der Beschreibung vom Betriebssystem
- **Anwendungspaket-ID** - Name des Herstellers oder des Anwendungsprozesses.
- **Dateiversion** - Informationen vom Herausgeber der Anwendung
- **Produktname** - Anwendungs- und/oder Firmenname

## Netzwerkverbindungen

Unter „Netzwerkverbindungen“ finden Sie eine Liste der aktiven Netzwerkverbindungen für Ihren Computer. ESET Cyber Security liefert ausführliche Informationen zu den einzelnen Verbindungen, und Sie können Regeln zum Blockieren der Verbindungen erstellen.

### Blockierregel für diese Verbindung erstellen

Mit ESET Cyber Security können Sie im **Netzwerkverbindungsmanager** Regeln zum Blockieren von Verbindungen erstellen. Klicken Sie mit der rechten Maustaste auf die jeweilige Verbindung und wählen Sie **Blockierregel für diese Verbindung erstellen** aus, um eine Blockierregel zu erstellen.

1. Wählen Sie das **Verbindungsprofil** aus, für das Sie die Regel erstellen möchten, und geben Sie einen Namen für die Regel ein. Wählen Sie die Anwendung aus, für die die Regel gelten soll, oder aktivieren Sie das Kontrollkästchen, um die Regel auf alle Anwendungen anzuwenden.
2. Wählen Sie aus, ob die Verbindung abgelehnt (blockiert) oder erlaubt werden soll. Wählen Sie aus, auf welche Kommunikationsrichtung die Regel angewendet werden soll. Klicken Sie auf **Regel in Log schreiben**, um eine Log-Datei für die Regel zu erstellen.
3. Wählen Sie das Verbindungsprotokoll und die Porttypen aus. Port für Dienst angeben oder Portbereich festlegen (Format: von-bis)
4. Wählen Sie das Ziel aus und geben Sie die Informationen je nach ausgewähltem Ziel in das entsprechende Feld ein.

# Live Grid

Dank des Live Grid-Frühwarnsystems erhält ESET unmittelbar und fortlaufend aktuelle Informationen zu neuen Infiltrationen. Das Live Grid-Frühwarnsystem funktioniert in zwei Richtungen, hat jedoch nur einen Zweck: die Verbesserung des Schutzes, den wir Ihnen bieten. Die einfachste Möglichkeit zur Erkennung neuer Bedrohungen bei deren Auftreten besteht darin, möglichst viele Kunden als Virenscoots einzusetzen. Als Benutzer haben Sie zwei Möglichkeiten:

1. Sie können sich entscheiden, das Live Grid-Frühwarnsystem nicht zu aktivieren. Es steht Ihnen dennoch der volle Funktionsumfang der Software zur Verfügung, und Sie erhalten auch in diesem Fall den bestmöglichen Schutz.
2. Sie können das Live Grid-Frühwarnsystem so konfigurieren, dass Informationen über neue Bedrohungen und Fundstellen von gefährlichem Code übermittelt werden. Die Informationen bleiben anonym. Diese Informationen können zur detaillierten Analyse an ESET gesendet werden. ESET analysiert diese Bedrohungen, um die Erkennungsroutine zu ergänzen und die Fähigkeit der Software zur Erkennung von Bedrohungen zu verbessern.

Das Live Grid-Frühwarnsystem 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.

Auch wenn es möglich ist, dass das ESET-Virenlabor auf diese Weise gelegentlich einige Informationen über Sie oder Ihren Computer erhält (zum Beispiel Benutzernamen in einem Verzeichnispfad usw.), werden diese Daten für keinen anderen Zweck als zur Verbesserung der unmittelbaren Reaktion auf neue Bedrohungen verwendet.

Um die Live Grid-Einstellungen zu öffnen, klicken Sie im Hauptmenü auf **Einstellungen > Erweiterte Einstellungen** (oder drücken Sie *cmd+*) > **Live Grid**. Wählen Sie **Live Grid-Frühwarnsystem aktivieren** aus, um Live Grid zu aktivieren. Klicken Sie anschließend neben **Erweiterte Einstellungen** auf **Einstellungen**.

## Live Grid-Einstellungen

ESET Cyber Security ist standardmäßig so konfiguriert, dass verdächtige Dateien zur genauen Analyse an ESET eingereicht werden. Deaktivieren Sie die Option **Dateien übermitteln**, wenn Sie diese Dateien nicht automatisch einreichen möchten.

Wenn Sie eine verdächtige Datei finden, können Sie sie zur Analyse an unser Virenlabor einreichen. Klicken Sie hierzu im Hauptprogrammfenster auf **Tools > Probe zur Analyse einreichen**. Wenn es sich um eine schadhafte Anwendung handelt, wird ihre Erkennung zu einem folgenden Update hinzugefügt.

**Anonyme Statistiken senden** – Das ESET Live Grid-Frühwarnsystem erfasst anonyme Informationen zu Ihrem Computer in Bezug auf neu erkannte Bedrohungen. Erfasst werden der Name der Bedrohung, Datum und Uhrzeit der Erkennung, die Versionsnummer des ESET Security-Produkts sowie Versionsdaten und die Regionaleinstellung des Betriebssystems. Diese Statistikpakete werden normalerweise einmal oder zweimal täglich an ESET übermittelt.

**Ausschlussfilter** – Über diese Option können Sie bestimmte Dateitypen vom Senden ausschließen. Hier können Dateien eingetragen werden, die eventuell vertrauliche Informationen enthalten, wie zum Beispiel

Textdokumente oder Tabellen. Die üblichsten Dateitypen sind bereits in der Standardeinstellung in die Liste eingetragen (.doc, .rtf usw.). Sie können der Ausschlussliste weitere Dateitypen hinzufügen.

**E-Mail-Adresse für Rückfragen (optional)** – Ihre E-Mail-Adresse kann dazu verwendet werden, Sie bei Rückfragen zu kontaktieren. Bitte beachten Sie, dass Sie nur dann eine Antwort von ESET erhalten, wenn weitere Informationen von Ihnen benötigt werden.

## Probe zur Analyse einreichen

Wenn Sie eine verdächtige Datei auf Ihrem Computer finden, können Sie sie zur Analyse an das ESET-Virenlabor senden.



### Bevor Sie Sample an ESET übermitteln

Übermitteln Sie die Probe nur, wenn sie mindestens eines der folgenden Kriterien erfüllt:

- Ihr ESET-Produkt erkennt die Probe überhaupt nicht
- Die Probe wird fälschlicherweise als Bedrohung erkannt
- Wir akzeptieren keine persönlichen Dateien, die Sie gerne von ESET auf Malware gescannt hätten, als Sample. Das ESET-Virenlabor führt keine On-Demand-Scans für unsere Benutzer durch.
- Formulieren Sie eine aussagekräftige Betreffzeile und geben Sie möglichst viele Informationen zu der eingesandten Datei an (z. B. einen Screenshot oder die Website, von der Sie die Datei heruntergeladen haben).

Um ein Sample einzureichen, verwenden Sie das Übermittlungsformular in Ihrem Produkt unter **Tools > Datei zur Analyse einreichen**.

Geben Sie im Formular **Datei zur Analyse einreichen** Folgendes an:

**Datei** - Der Pfad zur Datei, die Sie einreichen möchten.

**Kommentar** - Beschreiben Sie, warum Sie die Datei einsenden.

**E-Mail-Adresse für Rückfragen** – Diese E-Mail-Adresse wird zusammen mit verdächtigen Dateien an ESET übermittelt. Möglicherweise wird ESET über diese Adresse Kontakt mit Ihnen aufnehmen, wenn zusätzliche Angaben für die Dateianalyse benötigt werden. Diese Angabe ist freiwillig.



### Sie erhalten möglicherweise keine Antwort von ESET

Sie erhalten nur eine Antwort von ESET, wenn wir weitere Informationen von Ihnen benötigen, da täglich mehrere Zehntausend Dateien auf unseren Servern eingehen und wir nicht jede Meldung individuell beantworten können.

Wenn sich herausstellt, dass die Datei bzw. Webseite Schadcode enthält, werden entsprechende Erkennungsfunktionen in einem zukünftigen ESET-Update berücksichtigt.

## Benutzeroberfläche

Über die Konfigurationsoptionen für die Benutzeroberfläche können Sie die Arbeitsumgebung an Ihre Anforderungen anpassen. Diese Optionen sind unter **Einstellungen > Erweiterte Einstellungen ...** (oder `cmd+`, drücken) > **Schnittstelle** verfügbar.

- Um das ESET Cyber Security-Startbild beim Programmstart zu aktivieren, aktivieren Sie die Option **Startbild anzeigen**.
- Mit der Option **Anwendung in Dock anzeigen** wird das ESET Cyber Security-Symbol  im macOS-Dock angezeigt, und Sie können mit der Tastenkombination `cmd+tab` zwischen ESET Cyber Security und anderen geöffneten Anwendungen wechseln. Die Änderungen werden beim nächsten Start von ESET Cyber Security (in der Regel nach einem Neustart des Computers) wirksam.
- Mit der Option **Standardmenü verwenden** können Sie bestimmte Tastaturbefehle verwenden (siehe [Tastenkombinationen](#)) und Standardmenüeinträge (Benutzeroberfläche, Einstellungen und Tools) in der macOS-Menüleiste am oberen Bildschirmrand anzeigen.
- Um QuickInfos für bestimmte Optionen in ESET Cyber Security anzuzeigen, aktivieren Sie **QuickInfo anzeigen**.
- Wenn **Versteckte Dateien anzeigen** aktiviert ist, können Sie im Einstellungsbereich **Zu prüfende Objekte** der Funktion **Computer prüfen** auch versteckte Dateien sehen und diese auswählen.
- Standardmäßig wird das ESET Cyber Security-Symbol  in den Menüleisten-Extras rechts neben der macOS-Menüleiste am oberen Bildschirmrand angezeigt. Deaktivieren Sie die Option **Symbol in Menüleisten-Extras anzeigen**, um diese Funktion zu deaktivieren. Die Änderungen werden beim nächsten Start von ESET Cyber Security (in der Regel nach einem Neustart des Computers) übernommen.

## Warnungen und Hinweise

Im Bereich **Warnungen und Hinweise** können Sie konfigurieren, wie Warnungen und Systemhinweise in ESET Cyber Security behandelt werden.

Bei Deaktivieren der Option **Warnungen anzeigen** werden keine Warnmeldungen mehr angezeigt. Diese Einstellung wird nur in einigen speziellen Situationen empfohlen. Für die meisten Benutzer empfiehlt es sich, die Standardeinstellung (aktiviert) beizubehalten. Die erweiterten Einstellungen sind [in diesem Kapitel](#) beschrieben.

Wenn Sie die Option **Hinweise auf dem Desktop anzeigen** aktivieren, werden Warnfenster, die keinen Benutzereingriff erfordern, auf dem Desktop angezeigt (standardmäßig oben rechts auf dem Bildschirm). Wie lang solche Hinweise erscheinen, können Sie über den Wert **Hinweise automatisch schließen nach X Sekunden** festlegen (der Standardwert beträgt 5 Sekunden).

Seit ESET Cyber Security Version 6.2 können Sie außerdem bestimmte **Schutzstatusanzeigen** im Hauptbildschirm des Programms (Fenster **Schutzstatus**) deaktivieren. Weitere Informationen hierzu finden Sie unter [Schutzstatus](#).

## Warnungen anzeigen

Bei neuen Programmversionen und Betriebssystem-Updates, beim Deaktivieren bestimmter Programmkomponenten, beim Löschen von Logs usw. werden in ESET Cyber Security Warn- und Hinweisfenster angezeigt. Diese können Sie mit Wirkung für die Zukunft unterdrücken, indem Sie im jeweiligen Dialogfenster die Option **Dialogfenster nicht mehr anzeigen** aktivieren.

Unter **Liste der Dialogfenster (Einstellungen > Erweiterte Einstellungen > Warnungen und Hinweise > Einstellungen)** finden Sie eine Liste all dieser Warn- und Hinweisfenster in ESET Cyber Security. Um die Benachrichtigungen zu aktivieren oder zu deaktivieren, markieren Sie das Kontrollkästchen links neben dem **Dialogfensternamen**. Außerdem können Sie **Anzeigebedingungen** für Hinweise zu neuen Programmversionen und Betriebssystem-Updates definieren.

# Schutzstatus

Der aktuelle Schutzstatus von ESET Cyber Security kann durch Aktivieren oder Deaktivieren von Statusmeldungen in **Einstellungen > Erweiterte Einstellungen... > Warnungen und Benachrichtigungen > Im Bildschirm Schutzstatus anzeigen: Einstellungen** geändert werden. Der Status verschiedener Programmfunktionen wird im ESET Cyber Security-Hauptbildschirm (Fenster **Schutzstatus**) ein- oder ausgeblendet.

Sie können den Schutzstatus der folgenden Programmfunktionen ausblenden:

- Phishing-Schutz
- Web-Schutz
- E-Mail-Client-Schutz
- Betriebssystem-Update
- Lizenzablauf
- Computerneustart erforderlich

## Privilegien

Die Konfiguration von ESET Cyber Security ist entscheidend für die Sicherheitsrichtlinien Ihres Unternehmens. Unbefugte Änderungen können die Stabilität und den Schutz Ihres Systems gefährden. Aus diesem Grund können Sie festlegen, welche Benutzer zum Bearbeiten der Programmkonfiguration berechtigt sind.

Zum Festlegen der privilegierten Benutzer klicken Sie auf **Einstellungen > Erweiterte Einstellungen** (oder drücken *cmd+,*) > **Berechtigungen**. Wählen Sie alle Benutzer oder Gruppen in der Liste auf der linken Seite aus und klicken Sie auf **Hinzufügen**. Um alle Systembenutzer/Gruppen anzuzeigen, wählen Sie die Option **Alle Benutzer/Gruppen anzeigen** aus. Um einen Benutzer zu entfernen, wählen Sie ihn in der Liste **Ausgewählte Benutzer** auf der rechten Seite aus und klicken Sie auf **Entfernen**.



### Über Upgrades

Wenn Sie die Liste der ausgewählten Benutzer leer lassen, werden alle Benutzer als privilegiert betrachtet.

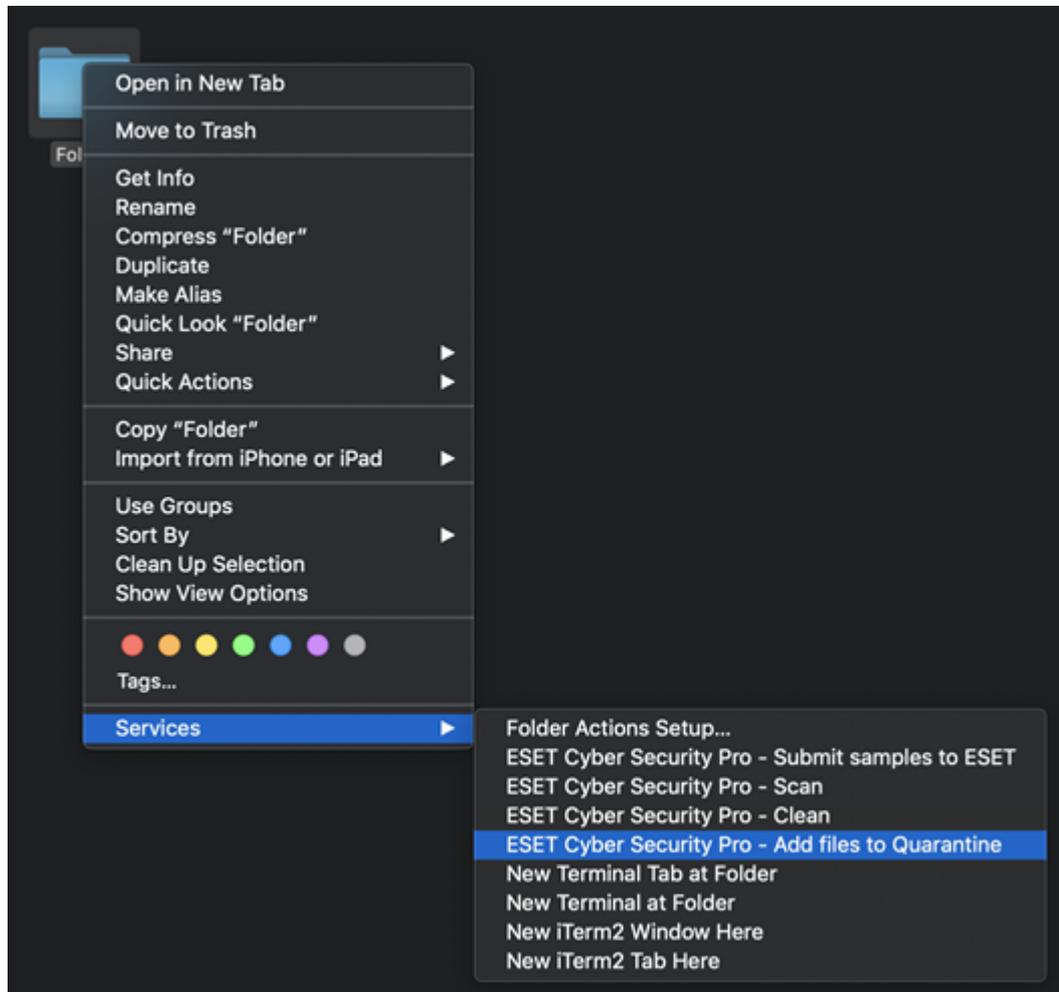
## Kontextmenü

Die Kontextmenü-Integration kann unter **Einstellungen > Erweiterte Einstellungen** (oder *cmd+,*) > **Kontextmenü** durch Auswahl der Option **In Kontextmenü integrieren** aktiviert werden. Die Änderungen werden nach dem Abmelden bzw. einem Neustart des Computers wirksam. Die Optionen des Kontextmenüs werden im **Finder**-Fenster angezeigt, wenn Sie bei gedrückter STRG-Taste auf eine beliebige Datei klicken.

Sie können Optionen auswählen, die im Kontextmenü angezeigt werden. Mit der Option **Nur scannen** können Sie die ausgewählte Datei scannen, mit **Nur säubern** können Sie die ausgewählte Datei über das Kontextmenü säubern. Wählen Sie „Säubern“ aus, wenn eine Datei von einem Virus mit Schadcode infiziert wurde. Versuchen Sie in einem solchen Fall zuerst, den Schadcode aus der infizierten Datei zu entfernen und ihren Originalzustand wiederherzustellen. Wenn die Datei ausschließlich Schadcode enthält, wird sie gelöscht.

Wenn Sie die Option **Alle** auswählen, können Sie die folgenden Tasks im Kontextmenü ausführen:

- Proben an ESET einreichen
- Scannen
- Sauber
- [Dateien zu Quarantäne hinzufügen](#)



## Einstellungen importieren/exportieren

Um eine vorhandene Konfiguration zu importieren oder die aktuelle Konfiguration von ESET Cyber Security zu exportieren, klicken Sie auf **Einstellungen** > **Einstellungen importieren und exportieren**.

Diese Funktionen sind nützlich, wenn Sie die aktuelle Konfiguration von ESET Cyber Security für eine spätere Verwendung sichern möchten. Die Exportfunktion bietet sich auch für Benutzer an, die ihre bevorzugte Konfiguration von ESET Cyber Security auf mehreren Systemen verwenden möchten. Sie können die Konfigurationsdatei einfach importieren, um ihre gewünschten Einstellungen zu übertragen.



Um eine Konfiguration zu importieren, wählen Sie **Einstellungen importieren** aus und klicken Sie auf **Durchsuchen**, um nach der zu importierenden Konfigurationsdatei zu suchen. Um eine Konfiguration zu exportieren, wählen Sie **Einstellungen exportieren** aus und navigieren Sie mit Ihrem Browser zu einem Speicherort auf Ihrem Computer, an dem die Konfigurationsdatei gespeichert werden soll.

## Einstellungen für Proxyserver

Die Proxyserver-Einstellungen lassen sich unter **Einstellungen > Erweiterte Einstellungen** (oder *cmd+*, drücken) > **Proxyserver** konfigurieren. So legen Sie die allgemeinen Proxyserver-Einstellungen für alle Funktionen von ESET Cyber Security fest. Die hier definierten Parameter werden von allen Modulen verwendet, die eine Verbindung zum Internet erfordern. ESET Cyber Security unterstützt die Authentifizierungsarten „Basic Authentication“ und „NTLM“ (NT LAN Manager).

Um die Proxyserver-Einstellungen für diese Ebene festzulegen, aktivieren Sie das Kontrollkästchen **Proxyserver verwenden** und geben im Feld **Proxyserver** die entsprechende IP-Adresse bzw. URL ein. Geben Sie dann im Feld „Port“ den Port an, über den Verbindungen auf dem Proxyserver eingehen (standardmäßig 3128). Wenn Sie auf **Erkennen** klicken, werden beide Felder vom Programm ausgefüllt.

Wenn der Proxyserver eine Authentifizierung benötigt, aktivieren Sie das Kontrollkästchen **Proxyserver erfordert Authentifizierung** und geben Sie einen gültigen **Benutzernamen** sowie das entsprechende **Passwort** ein.

## 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, 85101 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 beigefügt 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, sublizenziiert 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. Rechtevorbehalt.** 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, sublizenziiert, 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, 85101 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: HOM-ECS-20-01

## Datenschutzrichtlinie

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:

O 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;

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

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

O 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