

ESET PROTECT

Bereitstellungsanleitung für die virtuelle Appliance

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

Copyright ©2023 by ESET, spol. s r.o.

ESET PROTECT 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 Virtuelle ESET PROTECT-Appliance	1
1.1 Über die Hilfe	1
1.2 Voraussetzungen	2
1.2 Empfohlene Systemkonfigurationen	3
2 Unterstützte Hypervisoren	4
3 ESET PROTECT -VA: Implementierungsphasen und Wartung	4
4 Virtuelle ESET PROTECT-Appliance herunterladen	5
5 ESET PROTECT-VA-Passwörter	5
6 Bereitstellungsprozess für die virtuelle ESET PROTECT-Appliance	6
6.1 vSphere	6
6.2 VMware Workstation/Player	9
6.3 Microsoft Hyper-V	11
6.4 Oracle VirtualBox	13
6.5 Citrix	15
7 Konfiguration der virtuellen ESET PROTECT-Appliance	18
7.1 ESET PROTECT Server-Appliance	19
7.2 ESET PROTECT -MDM-Appliance	22
8 Verwaltungskonsole für die virtuelle ESET PROTECT-Appliance	27
8.1 Statische IP-Adresse festlegen	29
8.2 Remotezugriff aktivieren/deaktivieren	31
8.3 Datenbank sichern	32
8.4 Datenbank wiederherstellen	34
8.5 Reset nach Zurücksetzen einer Momentaufnahme	35
8.6 Datenbank-Pull von einem anderen Server ausführen	36
8.7 VM-Passwort ändern	40
8.8 Datenbankpasswort ändern	41
8.9 Domäne erneut beitreten	42
8.10 Domäne konfigurieren	44
8.11 Werkseinstellungen wiederherstellen	45
9 Webmin-Verwaltungsoberfläche	47
9.1 Dashboard	48
9.2 System	50
9.3 Server	51
9.3 ESET PROTECT	51
9.4 Tools	53
9.5 Netzwerk	54
10 ESET PROTECT Zertifikate	55
11 Upgrade/Migration der ESET PROTECT-VA	56
12 ESET PROTECT -VA-Notfallwiederherstellung	58
13 Fehlerbehebung	59
14 Häufig gestellte Fragen zur virtuellen ESET PROTECT-Appliance	60
14.1 Wie finde ich heraus, welche ESET PROTECT-Komponenten installiert sind?	61
14.2 Aktivieren der Ping-Funktion für die virtuelle ESET PROTECT-Appliance	62
14.3 Muss ich weitere Komponenten zu meiner ESET PROTECT-VA hinzufügen?	63
14.4 Wie kann ich den Apache HTTP-Proxy nach der Ausgangskonfiguration in meiner ESET PROTECT-VA aktivieren?	63
14.5 Wie kann ich LDAP so konfigurieren, dass statische Gruppen auf der ESET PROTECT-VA synchronisiert werden?	64
14.6 LDAPS-Verbindung zu einer Domäne konfigurieren	65
14.7 Wiederherstellen eines vergessenen Passworts für die ESET PROTECT-VA	66

14.8	Wie kann ich die ESET PROTECT-Datenbankverbindungszeichenfolge ändern?	66
14.9	Wie kann ich den Hyper-V Server für den RD Sensor einrichten?	66
14.10	Wie kann ich die Portnummern für die virtuelle ESET PROTECT-Appliance ändern?	67
14.11	Wie kann ich mehr Arbeitsspeicher für MySQL Server zuweisen?	68
14.12	Beim Ausführen von ESET PROTECT auf Hyper-V Server 2012 R2 treten Probleme auf	68
14.13	Wie kann ich die Leistung von Oracle VirtualBox verbessern?	69
14.14	So aktivieren Sie den YUM-Befehl für den HTTP-Proxyserver	69
14.15	Aktualisieren des Betriebssystems auf einem Computer, auf dem der ESET PROTECT VA Server ausgeführt wird	69
14.16	SELinux permanent deaktivieren	70
14.17	Neu starten der Verwaltungskonsole für die virtuelle Appliance	70
14.18	Proxy für Agenten-Verbindungen verwenden	70
14.19	Aktivieren von SSH	71
15	Endbenutzer-Lizenzvereinbarung	71
16	Datenschutzerklärung	78

Virtuelle ESET PROTECT-Appliance

Die virtuelle ESET PROTECT-Appliance (ESET PROTECT-VA) steht für Benutzer zur Verfügung, die ESET PROTECT in einer virtualisierten Umgebung ausführen möchten. Außerdem vereinfacht die virtuelle ESET PROTECT-Appliance die Bereitstellung von ESET PROTECT und bietet eine schnellere Lösung als die Verwendung des All-in-One-Installationsprogramms oder der Komponenteninstallationspakete.

Die ESET PROTECT-VA kann in den meisten virtuellen Umgebungen bereitgestellt werden. Sie unterstützt native Hypervisoren/Bare-Metal-Hypervisoren ((VMware vSphere/ESXi und Microsoft Hyper-V) und gehostete Hypervisoren, die üblicherweise auf einem Desktop-Betriebssystem ausgeführt werden (VMware Workstation, VMware Player und Oracle VirtualBox). Eine vollständige Liste finden Sie unter [Unterstützte Hypervisoren](#).

Hier finden Sie eine ausführliche Anleitung für die Bereitstellung und Verwaltung der ESET PROTECT-VA, inklusive der neuen Funktionen:

- Verwaltungskonsole für die virtuelle [ESET PROTECT-Appliance](#) – Eine einfache **textbasierte Benutzerschnittstelle** mit einem Hauptmenü. Diese Schnittstelle unterstützt Sie mit Textbefehlen und fordert Sie zur Eingabe von Werten auf. Auf diese Weise können auch Benutzer ohne umfassende Erfahrung mit CentOS 7 oder anderen Linuxsystemen die ESET PROTECT-VA mühelos konfigurieren. Wichtige Funktionen:
 - o [Statische IP-Adresse festlegen](#) – Geben Sie eine statische IP-Adresse manuell an, falls Ihre ESET PROTECT-VA keine IP-Adresse von einem DHCP-Server erhält.
 - o [Datenbank-Pull von einem anderen Server ausführen](#) – Für Upgrades oder Migrationen Ihrer ESET PROTECT-VA.
 - o [ESET PROTECT-Datenbank sichern oder wiederherstellen](#) – Mit diesen Funktionen können Sie eine Strategie für die Notfallwiederherstellung einrichten und Probleme im Zusammenhang mit der ESET PROTECT-VA beheben.
 - o [Werkseinstellungen wiederherstellen](#) – Setzt die Appliance auf ihren Originalzustand nach der Bereitstellung zurück. Diese Funktion ist hilfreich, falls Probleme mit der ESET PROTECT-VA auftreten. Halten Sie stets eine Sicherung der Datenbank vor, um Datenverluste zu vermeiden.
- [Webmin-Verwaltungsoberfläche](#) - Eine externe webbasierte Oberfläche zur Verwaltung von Linux-Systemen. Hier können Sie Ihre ESET PROTECT-VA aus der Ferne mit Ihrem Webbrowser und einer intuitiven Oberfläche verwalten. Die wichtigsten Webmin-Module werden in diesem Dokument beschrieben.

Über die Hilfe

Diese **VA-Bereitstellungsanleitung** enthält Anweisungen für die Bereitstellung und Konfiguration der virtuellen ESET PROTECT-Appliance (ESET PROTECT-VA). Diese Anleitung richtet sich an Personen, die ESET PROTECT-VA bereitstellen, verwalten und aktualisieren möchten.

Aus Konsistenzgründen und um Verwirrungen zu vermeiden, richtet sich die Terminologie in dieser gesamten Anleitung nach den ESET PROTECT-Parameternamen. Wir verwenden außerdem bestimmte Symbole, um besonders interessante oder wichtige Themen hervorzuheben.

 Hinweise können wichtige Informationen wie bestimmte Features oder einen Link zu einem verwandten Thema enthalten.



Auf diese Weise gekennzeichnete Informationen sind wichtig und sollten nicht übersprungen werden. Normalerweise handelt es sich um nicht-kritische, jedoch wichtige Informationen.



Kritische Informationen, die besondere Vorsicht erfordern. Warnungen haben den Zweck, Sie vor potenziell schädlichen Fehlern zu schützen. Der Text in Warnhinweisen weist auf besonders empfindliche Systemeinstellungen oder riskante Vorgänge hin und muss daher unbedingt gelesen und verstanden werden.



Beispielszenario mit einem relevanten Anwendungsfall für das jeweilige Thema. Beispiele werden eingesetzt, um komplexere Themen zu erklären.

Konvention	Bedeutung
Fettdruck	Namen von Elementen der Benutzeroberfläche, z. B. Schaltflächen und Optionsfelder.
<i>Kursivdruck</i>	Platzhalter für Informationen, die Sie eingeben. Dateiname oder Pfad bedeutet z. B., dass Sie den tatsächlichen Pfad oder den Namen einer Datei angeben.
Courier New	Codebeispiele oder Befehle.
Hyperlink	Schnellzugriff auf verwandte Themen oder externe Webadressen. Hyperlinks sind in blau hervorgehoben und können unterstrichen sein.
<code>%ProgramFiles%</code>	Das Windows-Systemverzeichnis, in dem installierte Windows-Programme und andere Anwendungen gespeichert werden.

- Die [Onlinehilfe](#) ist die primäre Quelle für Hilfeinhalte. Bei funktionierender Internetverbindung wird automatisch die neueste Version der Onlinehilfe angezeigt. Die ESET PROTECT-Onlinehilfe enthält vier aktive Registerkarten im oberen Navigationsbereich: [Installation/Upgrade](#), [Administration](#), [VA-Bereitstellung](#) und [SMB-Anleitung](#).
- Die Themen in diesem Handbuch sind in Kapitel und Unterkapitel eingeteilt. Verwenden Sie das Suchfeld im oberen Bereich, um nach relevanten Informationen zu suchen.



Nachdem Sie ein Benutzerhandbuch über die Navigationsleiste am oberen Seitenrand geöffnet haben, bezieht sich die Suche nur noch auf den Inhalt dieses Handbuchs. Wenn Sie z. B. das Administratorhandbuch geöffnet haben, werden keine Themen aus den Handbüchern für Installation/Upgrade und VA-Bereitstellung in den Suchergebnissen angezeigt.

- Die [ESET-Knowledgebase](#) enthält Antworten auf häufig gestellte Fragen sowie Lösungsvorschläge für zahlreiche Probleme. Die Knowledgebase wird regelmäßig von den ESET-Supportmitarbeitern aktualisiert und eignet sich daher hervorragend für die Lösung verschiedenster Probleme.
- Im [ESET-Forum](#) erhalten ESET-Benutzer schnell und einfach Hilfe und können anderen Benutzern helfen. Dort können Sie Themen zu beliebigen Fragen oder Problemen mit Ihren ESET-Produkten erstellen.

Voraussetzungen

Für die Bereitstellung der virtuellen ESET PROTECT-Appliance müssen die folgenden Voraussetzungen erfüllt sein:

- Sie müssen einen [unterstützten Hypervisor](#) verwenden.
- Vergewissern Sie sich, dass das Gastbetriebssystem (falls Sie einen gehosteten Hypervisor wie VMware Workstation/Player oder Oracle VirtualBox verwenden) unterstützt wird.

- Vergewissern Sie sich, dass die Uhren auf dem Host und den Gastbetriebssystemen synchronisiert sind.
- **VT muss im BIOS des Hostsystems aktiviert** sein. Diese Technologie wird auch als VT, Vanderpool Technology, Virtualization Technology, VMX oder Virtual Machine Extensions bezeichnet. Normalerweise finden Sie diese Einstellung im Sicherheitsbildschirm im BIOS. Die Position der Einstellung hängt vom Systemhersteller ab.
- Vergewissern Sie sich, dass die Verbindung für den Netzwerkadapter des virtuellen Computers auf **Bridged** (oder auch **NAT**) festgelegt ist. Während der Konfiguration der ESET PROTECT-VA können Sie Netzwerkeinstellungen inklusive Domänendetails angeben, mit denen der Task [Synchronisierung der statischen Gruppen](#) richtig ausgeführt werden kann.
- Wenn Sie den **NAT**-Modus verwenden, muss auf der virtuellen Maschine die Portweiterleitung konfiguriert sein, damit ESET PROTECT über das Internet erreichbar ist. Ports, die weitergeleitet werden müssen, werden nach der Bereitstellung und Konfiguration im Konsolenfenster der ESET PROTECT-VA angezeigt.
- Die virtuelle ESET PROTECT-Appliance unterstützt nur IPv4-Umgebungen. IPv6-Umgebungen können zwar manuell eingerichtet werden, aber IPv6 wird nicht unterstützt.

 Sie sollten eine Momentaufnahme der neu bereitgestellten und konfigurierten ESET PROTECT-VA erstellen und mit AD synchronisieren. Außerdem sollten Sie eine Momentaufnahme erstellen, bevor Sie den ESET Management Agent auf den Clientcomputern bereitstellen.

- ESET PROTECT -Zertifikate werden benötigt, um ESET PROTECT MDM bereitzustellen. Sie benötigen eine aktive ESET PROTECT Server-Instanz, um die [Zertifikate zu generieren](#), die die Kommunikation zwischen den ESET PROTECT-Komponenten verschlüsseln.

Empfohlene Systemkonfigurationen

Je nach Größe Ihrer Infrastruktur verwaltet Ihre virtuelle ESET PROTECT-Appliance eine bestimmte Anzahl von Clients. Beachten Sie dabei die empfohlenen Konfigurationen für virtuelle Computer und die Mindestanforderungen.

Die folgenden Größenangaben gelten für den ESET PROTECT Server und für die virtuelle ESET PROTECT-MDM-Appliance:

Anzahl Clients	Anzahl Prozessorkerne	Arbeitsspeichergröße	Sonstige
Weniger als 5.000 Clients	4	4 GB	Thick-Laufwerk mit manueller Konfigurationsänderung, um die Speichergröße für MySQL zu erhöhen .
Mehr als 5.000 Clients	8	8 GB	Erhöhen Sie die verfügbaren Ressourcen für Ihre ESET PROTECT-VA proportional, um Leistungsprobleme zu vermeiden.

 Falls Sie mehr als 5.000 Clients verwalten, sollten Sie ESET PROTECT Server/MDM unbedingt auf einem physischen Computer mit Microsoft Windows Server und Microsoft SQL Server installieren.

Unterstützte Hypervisoren

Die virtuelle ESET PROTECT-Appliance (*protect_appliance.ova*) ist eine virtuelle Hardware-Appliance. vom Typ „vmx-07“.

Die virtuelle Appliance wird nur für die aufgelisteten Hypervisoren unterstützt. Die Ausführung auf anderen Hypervisoren erfolgt auf eigene Gefahr des Benutzers.

Hypervisor	Version	ESET PROTECT Server-Appliance	ESET PROTECT - MDM-Appliance
VMware vSphere/ESXi	6.5 und höhere Versionen	✓	✓
VMware Workstation	9 und höhere Versionen	✓	✓
VMware Player	7 und höhere Versionen	✓	✓
Microsoft Hyper-V	Server 2012, 2012 R2, 2016, 2019	✓	✓
Oracle VirtualBox	6.0 und höhere Versionen	✓	✓
Citrix	7.0 und höhere Versionen	✓	✓



Sie sollten einen DHCP-Server in Ihrem Netzwerk verwenden, um der ESET PROTECT-VA eine IP-Adresse zuweisen zu können. Diese IP-Adresse ist für den Zugriff auf die [ESET PROTECT-VA-Konfigurationsweboberfläche](#) erforderlich. Wenn Sie keinen DHCP-Server in Ihrem Netzwerk verwenden, müssen Sie eine [statische IP-Adresse festlegen](#).

ESET PROTECT -VA: Implementierungsphasen und Wartung

Die Implementierung der virtuellen ESET PROTECT-Appliance umfasst die folgenden Phasen, die für eine erfolgreiche Bereitstellung und Konfiguration abgeschlossen werden müssen:

1. [Bereitstellung der ESET PROTECT-Appliance](#) – Die Bereitstellung der OVA-Datei für die virtuelle ESET PROTECT-Appliance auf Ihrem Hypervisor.
2. [ESET PROTECT Konfiguration der virtuellen ERA-Appliance](#) – Die Konfiguration im Anschluss an die Bereitstellung erfolgt über die Weboberfläche der ESET PROTECT-VA. Auf dieser Konfigurationsseite können Sie den Appliance-Typ auswählen und Details und Eigenschaften eingeben, die für den Betrieb des jeweiligen ESET PROTECT-VA-Typs benötigt werden.

Die weitere Konfiguration und Verwaltung erfolgt über die textbasierte Benutzerschnittstelle bzw. über Webmin:

1. [Verwaltungskonsole für die virtuelle ESET PROTECT-Appliance](#) - Wartungsoptionen wie z. B. Sicherung und Wiederherstellung, Passwortänderungen, Zurücksetzen der Werkseinstellungen usw.
2. [Webmin-Verwaltungsoberfläche](#) – Vereinfacht die Verwaltung Ihrer ESET PROTECT-VA.

Prozeduren für Upgrade, Migration und Notfallwiederherstellung:

[ESET PROTECT-VA-Upgrade/Migration](#) - Dieser Abschnitt enthält Details und eine schrittweise Anleitung, falls Sie ein Upgrade Ihrer ESET PROTECT-VA auf die aktuelle Version ausführen möchten. Mit derselben Prozedur können Sie auch Ihre ESET PROTECT-VA migrieren.

[ESET PROTECT-VA-Notfallwiederherstellung](#) - Führen Sie diese Prozedur aus, falls Ihre ESET PROTECT-VA nicht mehr funktioniert und Sie das Problem nicht beheben können oder falls Sie nicht in der Lage sind, eine defekte ESET PROTECT-VA-Instanz wiederherzustellen.

Virtuelle ESET PROTECT-Appliance herunterladen

Dier virtuelle ESET PROTECT-Appliance wird als OVA -Datei (Open Virtualization Appliance) bereitgestellt. Sie ist im [Downloadbereich](#) verfügbar. Die Appliance ist als [protect_appliance.ova](#) verfügbar.

Falls Sie Ihre VA mit Microsoft Hyper-V bereitstellen, verwenden Sie die Datei [protect_appliance.vhd.zip](#) anstelle der OVA-Datei.

- *protect_appliance.ova* – enthält mehrere [ESET PROTECT-Appliance-Typen](#). Stellen Sie diese Datei bereit und wählen Sie aus, welche Appliance ausgeführt werden soll. Sie können unter den folgenden Appliance-Typen wählen:

OESET PROTECT Server – Ein ESET PROTECT Server, der auf einer dedizierten VM ausgeführt wird. Enthält außerdem Rogue Detection Sensor.

OESET PROTECT MDM – Nur die Komponente für die Mobilgeräteverwaltung. Wenn Sie den ESET PROTECT Server nicht dem externen Netzwerk aussetzen möchten, können Sie die ESET PROTECT MDM-VM zur Verwaltung von Mobilgeräten über das Internet erreichbar machen.

Die OVA-Datei ist eine Vorlage, die ein funktionsfähiges CentOS 7-Betriebssystem enthält. [Folgen Sie den Anweisungen für Ihren Hypervisor](#), um die ESET PROTECT-VA OVA-Datei bereitzustellen. Wenn Sie *protect_appliance.ova* verwenden, können Sie auswählen, welcher Typ von ESET PROTECT-Appliance nach der Bereitstellung in Ihrer VM ausgeführt werden soll. Nachdem Sie den Typ ausgewählt haben, können Sie mit der Konfiguration der virtuellen ESET PROTECT-Appliance beginnen. Nach der Bereitstellung der OVA-Datei wählen Sie den Appliance-Typ aus und konfigurieren Sie die Einstellungen für Ihre VA. Die VA ist eine vollständige Umgebung mit ESET PROTECT (bzw. einer der Komponenten).

Stellen Sie vor der Bereitstellung sicher, dass alle [Voraussetzungen](#) erfüllt sind.

Nach dem Bereitstellungs- und Konfigurationsprozess können Sie mit der ESET PROTECT Web-Konsole eine Verbindung zum ESET PROTECT Server herstellen und [ESET PROTECT einsetzen](#).

i ESET stellt die virtuellen ESET PROTECT-Appliances bereit, ist jedoch nicht für den Support und die Wartung Ihres Betriebssystems oder der Betriebssystemkomponenten verantwortlich. Die virtuellen ESET PROTECT-Appliances sollen die Verwendung und Bereitstellung vereinfachen. Sie werden mit einem öffentlich verfügbaren Betriebssystem geliefert, das ESET-fremde Komponenten enthält. Die Verwaltung und Aktualisierung dieser Komponenten liegt in der alleinigen Verantwortung des Benutzers der virtuellen ESET PROTECT-Appliance. Sie sollten das Betriebssystem regelmäßig aktualisieren, um Sicherheitsprobleme zu vermeiden.

ESET PROTECT-VA-Passwörter

Die virtuelle ESET PROTECT-Appliance verwendet mehrere Benutzerkonten. In der folgenden Tabelle werden die unterschiedlichen Kontotypen beschrieben:

Kontotyp	Standardpasswort	Beschreibung und Zweck
Betriebssystem (CentOS) root	eraadmin	Dieses Konto dient zur Anmeldung bei Ihrer virtuellen ESET PROTECT-Appliance. Dort können Sie die ESET PROTECT-VA-Verwaltungskonsole und die Webmin-Verwaltungs Oberfläche öffnen, die Werkseinstellungen wiederherstellen oder einen Datenbank-Pull von einem anderen Server ausführen . Normalerweise werden Sie zur Eingabe Ihres VM-Passworts aufgefordert.
Datenbank (MySQL) root	eraadmin	Dies ist ein root-Konto für den MySQL-Datenbankserver. Dort können Sie zum Beispiel eine Datenbanksicherung ausführen oder die Datenbank wiederherstellen . Normalerweise werden Sie zur Eingabe Ihres Datenbank-root-Passworts aufgefordert.
ESET PROTECT Administrator der Web-Konsole	Bei der Konfiguration der ESET PROTECT-VA angegeben	Dieses Passwort ist wichtig und wird für die Anmeldung bei der ESET PROTECT Web-Konsole benötigt.

Das Standardpasswort wird bei der [Konfiguration der virtuellen ESET PROTECT-Appliance](#) geändert. Alle genannten Konten verwenden dasselbe Passwort, das Sie bei der Konfiguration der ESET PROTECT-VA eingerichtet haben. Sie können jedoch auch einzelne Passwörter für die Konten festlegen. Unterschiedliche Passwörter sind sicherer, erhöhen jedoch auch den Verwaltungsaufwand. Sie benötigen unter Umständen eine effektive Methode, um mehrere Passwörter für die ESET PROTECT-VA problemlos verwalten zu können.

i Ohne Konfiguration bereitgestellte ESET PROTECT-VAs verwenden das Passwort `eraadmin` für alle genannten Konten, bis Sie das Passwort bei der [Konfiguration der virtuellen ESET PROTECT-Appliance](#) ändern.

Falls Sie ein Passwort für eines der genannte Konten vergessen haben, lesen Sie das Kapitel [Vergessenes Passwort für die ESET PROTECT-VA wiederherstellen](#).

Bereitstellungsprozess für die virtuelle ESET PROTECT-Appliance

Klicken Sie auf den Hypervisor, den Sie verwenden, um die Bereitstellungsanweisungen anzuzeigen:

- [vSphere](#)
- [VMware Workstation/Player](#)
- [Microsoft Hyper-V](#)
- [Oracle VirtualBox](#)
- [Citrix](#)

vSphere

Bereitstellen einer ESET PROTECT-VA in einem vSphere-Client

1. Verbinden Sie sich über den vSphere-Client mit Ihrem vCenter-Server oder direkt mit dem ESXi-Server.
2. Falls Sie den vSphere-Client für Desktop verwenden, klicken Sie auf **Datei > OVF-Vorlage bereitstellen**. Falls Sie den vSphere-Web-Client verwenden, klicken Sie auf **Aktionen > OVF-Vorlage** bereitstellen.
3. Klicken Sie auf **Durchsuchen**, navigieren Sie zur Datei *protect_appliance.ova*, die Sie [von ESET.com heruntergeladen](https://www.eset.com) haben, und klicken Sie auf **Öffnen**.

 **Nicht unterstützte Versionen** von VMware ESXi akzeptieren keine SHA-256-Zertifikate. Wenn beim Importieren des ESET PROTECT VA 9.1 .ova-Pakets ein Zertifikatfehler angezeigt wird, müssen Sie die .cert-Datei aus .ova löschen, bevor Sie die Bereitstellung fortsetzen.

4. Klicken Sie im Fenster mit den OVF-Vorlagendetails auf **Weiter**.
5. Lesen und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung (EULA).
6. Befolgen Sie die Anweisungen auf dem Bildschirm, um die Installation fertig zu stellen. Geben Sie hierbei die folgenden Informationen für den virtuellen Client an:
 - **Name und Speicherort** – Geben Sie einen Namen für das bereitgestellte Template und den Ort an, unter dem die Dateien des virtuellen Computers gespeichert sind.
 - **Host / Cluster** – Wählen Sie den Host oder das Cluster aus, auf dem Sie das Template ausführen möchten.
 - **Ressourcenpool** – Wählen Sie den Ressourcenpool aus, in dem Sie das Template bereitstellen möchten.
 - **Speicher** – Wählen Sie einen Speicherort für die Dateien der virtuellen Maschine aus.
 - **Datenträgerformat** – Wählen Sie das Format für die virtuellen Datenträger aus.
 - **Netzwerkzuordnung** – Wählen Sie das Netzwerk aus, das der virtuelle Computer verwenden soll. Verwenden Sie für den virtuellen Computer unbedingt das Netzwerk aus, das zu dem von Ihnen erstellten IP-Pool zugeordnet ist.
7. Klicken Sie auf **Weiter**, überprüfen Sie die Bereitstellungszusammenfassung und klicken Sie auf **Fertig** stellen. Der Vorgang erstellt automatisch eine virtuelle Maschine mit den ausgewählten Einstellungen.
8. Nachdem die ESET PROTECT-VA bereitgestellt wurde, können Sie sie aktivieren. Die folgenden Informationen werden angezeigt:

```
ESET PROTECT Appliance  
(C) 202 ESET, spol. s r.o. - All rights reserved
```

```
First time appliance configuration needs to be performed.  
Please connect using a web browser to:  
https://
```

```
Static IP address for the connection can be set by these steps:
```

1. Enter management mode with password [eraadmin].
2. Select [Set static IP address] from the menu.
3. Enter network connection parameters.

```
<ENTER> Enter management mode
```

Öffnen Sie Ihren Webbrowser und geben Sie in der Adressleiste die IP-Adresse der neu bereitgestellten ESET PROTECT-Appliance ein. Die IP-Adresse wird im Konsolenfenster aufgeführt (wie oben dargestellt). Die folgende Meldung wird angezeigt: „**Die erstmalige Appliance-Konfiguration muss Über einen Webbrowser unter folgender Adresse ausgeführt werden:https://[IP address]**“.

Der nächste Schritt ist nun die [Konfiguration der Appliance](#) über die Weboberfläche.



Wenn Sie keinen DHCP-Server in Ihrem Netzwerk verwenden, müssen Sie in der Verwaltungskonsole eine [statische IP-Adresse für die ESET PROTECT-VA festlegen](#). Wenn keine IP-Adresse zugewiesen wurde, werden die folgenden Informationen angezeigt (für die URL wird keine IP-Adresse angezeigt). Wenn keine IP-Adresse zugewiesen wurde, kann der DHCP-Server möglicherweise keine Adresse zuweisen. Vergewissern Sie sich, dass im Subnetz der VA freie IP-Adressen vorhanden sind.

```
ESET PROTECT Appliance
(C) 2021 ESET, spol. s r.o. - All rights reserved
```

```
First time appliance configuration needs to be performed.
```

```
Please connect using a web browser to:
https://
```

```
Static IP address for the connection can be set by these steps:
```

1. Enter management mode with password [eraadmin].
2. Select [Set static IP address] from the menu.
3. Enter network connection parameters.

```
<ENTER> Enter management mode
```

i Es wird dringend empfohlen, die vCenter-Rollen und -Berechtigungen so zu konfigurieren, dass die VMware-Benutzer keinen Zugriff auf die virtuelle ESET PROTECT-Maschine haben. So wird vermieden, dass Benutzer die virtuelle ESET PROTECT-Maschine manipulieren. ESET PROTECT-Benutzer benötigen keinen Zugriff auf die VM. Den eigentlichen Zugriff auf ESET PROTECT können Sie im Bereich [Zugriffsrechte](#) in der ESET PROTECT Web-Konsole verwalten.

VMware Workstation/Player

Bereitstellen der ESET PROTECT-VA in VMware Workstation/Player

Verwenden Sie unbedingt die neueste Version von VMware Player. Legen Sie die Verbindung für den Netzwerkadapter auf der VM auf **bridged** oder **NAT** fest.

i Auf der virtuellen Maschine muss die Portweiterleitung konfiguriert sein, damit ESET PROTECT über das Netzwerk erreichbar ist.

1. Wählen Sie **Datei > OVF-Vorlage bereitstellen** aus.
2. Navigieren Sie zur Datei *protect_appliance.ova*, die Sie [von der ESET-Website heruntergeladen](#) haben, und klicken Sie auf **Öffnen**.
3. Geben Sie einen Namen und einen lokalen Speicherpfad für die neue virtuelle Maschine ein und klicken Sie auf **Importieren**.

4. Lesen und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung (EULA), falls Sie dieser zustimmen.

5. Nachdem die Appliance erstellt wurde, können Sie diese aktivieren. Die folgenden Informationen werden angezeigt:

```
ESET PROTECT Appliance
(C) 2021 ESET, spol. s r.o. - All rights reserved

First time appliance configuration needs to be performed.
Please connect using a web browser to:
https://[redacted]

Static IP address for the connection can be set by these steps:
1. Enter management mode with password [eraadmin].
2. Select [Set static IP address] from the menu.
3. Enter network connection parameters.

<ENTER> Enter management mode
```

Öffnen Sie Ihren Webbrowser und geben Sie in der Adressleiste die IP-Adresse der neu bereitgestellten ESET PROTECT-Appliance ein. Die IP-Adresse wird im Konsolenfenster aufgeführt (wie oben dargestellt). Die folgende Meldung wird angezeigt: „**Die erstmalige Appliance-Konfiguration muss Über einen Webbrowser unter folgender Adresse ausgeführt werden:https://[IP address]**“.

Der nächste Schritt ist nun die [Konfiguration der Appliance](#) über die Weboberfläche.



Wenn Sie keinen DHCP-Server in Ihrem Netzwerk verwenden, müssen Sie in der Verwaltungskonsole eine [statische IP-Adresse für die ESET PROTECT-VA festlegen](#). Wenn keine IP-Adresse zugewiesen wurde, werden die folgenden Informationen angezeigt (für die URL wird keine IP-Adresse angezeigt). Wenn keine IP-Adresse zugewiesen wurde, kann der DHCP-Server möglicherweise keine Adresse zuweisen. Vergewissern Sie sich, dass im Subnetz der VA freie IP-Adressen vorhanden sind.

```
ESET PROTECT Appliance
(C) 2021 ESET, spol. s r.o. - All rights reserved
```

```
First time appliance configuration needs to be performed.
```

```
Please connect using a web browser to:
https://
```

```
Static IP address for the connection can be set by these steps:
```

1. Enter management mode with password [eraadmin].
2. Select [Set static IP address] from the menu.
3. Enter network connection parameters.

```
<ENTER> Enter management mode
```

Microsoft Hyper-V

Bereitstellen der ESET PROTECT-VA in Microsoft Hyper-V

1. Extrahieren Sie die Datei `protect_appliance.vhd.zip` (die Sie [von ESET.com heruntergeladen](#) haben) mit einem Dienstprogramm wie Tar oder 7-Zip.
2. Starten Sie den Hyper-V-Manager und verbinden Sie sich mit dem entsprechenden Hyper-V.
3. Erstellen Sie einen **neuen** virtuellen Computer (Generation 1) mit mindestens 4 Prozessorkernen und 4 GB Arbeitsspeicher.
4. Nachdem die VM erstellt ist, können Sie sie aktivieren. Die folgenden Informationen werden angezeigt:

```
ESET PROTECT Appliance  
(C) 202 ESET, spol. s r.o. - All rights reserved
```

```
First time appliance configuration needs to be performed.  
Please connect using a web browser to:  
https://
```

```
Static IP address for the connection can be set by these steps:
```

1. Enter management mode with password [eraadmin].
2. Select [Set static IP address] from the menu.
3. Enter network connection parameters.

```
<ENTER> Enter management mode
```

Öffnen Sie Ihren Webbrowser und geben Sie in der Adressleiste die IP-Adresse der neu bereitgestellten ESET PROTECT-Appliance ein. Die IP-Adresse wird im Konsolenfenster aufgeführt (wie oben dargestellt). Die folgende Meldung wird angezeigt: **„Die erstmalige Appliance-Konfiguration muss Über einen Webbrowser unter folgender Adresse ausgeführt werden:https://[IP address]“**.

Der nächste Schritt ist nun die [Konfiguration der Appliance](#) über die Weboberfläche.



Wenn Sie keinen DHCP-Server in Ihrem Netzwerk verwenden, müssen Sie in der Verwaltungskonsolle eine [statische IP-Adresse für die ESET PROTECT-VA festlegen](#). Wenn keine IP-Adresse zugewiesen wurde, werden die folgenden Informationen angezeigt (für die URL wird keine IP-Adresse angezeigt). Wenn keine IP-Adresse zugewiesen wurde, kann der DHCP-Server möglicherweise keine Adresse zuweisen. Vergewissern Sie sich, dass im Subnetz der VA freie IP-Adressen vorhanden sind.

```
ESET PROTECT Appliance
(C) 2021 ESET, spol. s r.o. - All rights reserved
```

```
First time appliance configuration needs to be performed.
```

```
Please connect using a web browser to:
https://
```

```
Static IP address for the connection can be set by these steps:
```

1. Enter management mode with password [eraadmin].
2. Select [Set static IP address] from the menu.
3. Enter network connection parameters.

```
<ENTER> Enter management mode
```

Oracle VirtualBox

Bereitstellen der ESET PROTECT-VA in VirtualBox

Verwenden Sie unbedingt die neueste Version von VirtualBox. Verwenden Sie eine der Verbindungsoptionen **Bridged** oder **NAT** für den Netzwerkadapter der VM.

i Auf dem virtuellen Computer muss die Portweiterleitung konfiguriert sein, damit ESET PROTECT über das Internet erreichbar ist (sofern erforderlich).

1. Klicken Sie auf **File** und wählen Sie **Import Appliance** aus.
2. Klicken Sie auf **Browse**, navigieren Sie zur Datei *protect_appliance.ova*, die Sie [von ESET.com heruntergeladen](#) haben, und klicken Sie auf **Open**.
3. Klicken Sie auf **Next**.
4. Überprüfen Sie Ihre Appliance-Einstellungen und klicken Sie auf **Import**.
5. Lesen und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung (EULA), falls Sie dieser zustimmen.
6. Nachdem die ESET PROTECT-VA bereitgestellt wurde, können Sie sie aktivieren. Die folgenden Informationen werden angezeigt:

```
ESET PROTECT Appliance
(C) 202 ESET, spol. s r.o. - All rights reserved
```

```
First time appliance configuration needs to be performed.
Please connect using a web browser to:
https://
```

```
Static IP address for the connection can be set by these steps:
```

1. Enter management mode with password [eraadmin].
2. Select [Set static IP address] from the menu.
3. Enter network connection parameters.

```
<ENTER> Enter management mode
```

Öffnen Sie Ihren Webbrowser und geben Sie in der Adressleiste die IP-Adresse der neu bereitgestellten ESET PROTECT-Appliance ein. Die IP-Adresse wird im Konsolenfenster aufgeführt (wie oben dargestellt). Die folgende Meldung wird angezeigt: „**Die erstmalige Appliance-Konfiguration muss Über einen Webbrowser unter folgender Adresse ausgeführt werden:https://[IP address]**“.

Der nächste Schritt ist nun die [Konfiguration der Appliance](#) über die Weboberfläche.



Wenn Sie keinen DHCP-Server in Ihrem Netzwerk verwenden, müssen Sie in der Verwaltungskonsolle eine [statische IP-Adresse für die ESET PROTECT-VA festlegen](#). Wenn keine IP-Adresse zugewiesen wurde, werden die folgenden Informationen angezeigt (für die URL wird keine IP-Adresse angezeigt). Wenn keine IP-Adresse zugewiesen wurde, kann der DHCP-Server möglicherweise keine Adresse zuweisen. Vergewissern Sie sich, dass im Subnetz der VA freie IP-Adressen vorhanden sind.

```
ESET PROTECT Appliance
(C) 2021 ESET, spol. s r.o. - All rights reserved
```

```
First time appliance configuration needs to be performed.
```

```
Please connect using a web browser to:
https://
```

```
Static IP address for the connection can be set by these steps:
```

1. Enter management mode with password [eraadmin].
2. Select [Set static IP address] from the menu.
3. Enter network connection parameters.

```
<ENTER> Enter management mode
```

Citrix

Bereitstellen der ESET PROTECT-VA in Citrix:

Voraussetzungen

- Ihr IPv4-Netzwerk ist in der Citrix-Umgebung verfügbar. IPv6 wird in der ESET PROTECT-VA nicht unterstützt.
- Die Appliance-Datei *.ovf* ist auf dem Computer verfügbar, auf dem Sie die ESET PROTECT-VA bereitstellen werden.
- Zum Importieren des *OVF/OVA*-Pakets sind Pool-Administratorrechte erforderlich.
- Dem bereitstellenden Benutzer muss ausreichend Speicherplatz zur Verfügung stehen (mindestens 100 GB).

Bereitstellungsprozess

1. Wählen Sie **File > Import**.

2. Klicken Sie auf **Browse**, navigieren Sie zur *protect_appliance.ova*-Datei, die Sie [von der ESET-Website heruntergeladen](#) haben, und klicken Sie auf **Next**.

3. Aktivieren Sie das Kontrollkästchen **I accept the End User License Agreements** und klicken Sie auf **Next**.
4. Wählen Sie den gewünschten Pool oder eigenständigen Server für die Bereitstellung der ESET PROTECT-VA und klicken Sie auf **Next**.
5. Platzieren Sie den importierten virtuellen Datenträger in ein Speicher-Repository und klicken Sie auf **Next**.
6. Ordnen Sie die virtuellen Netzwerkschnittstellen zu, indem Sie **Target Network** auswählen, und klicken Sie auf **Next**.
7. Wählen Sie die Überprüfung der Digitalsignatur (optional) und klicken Sie auf **Next**.
8. Wählen Sie **Don't use Operating System Fixup** aus und klicken Sie auf **Next**.
9. Wählen Sie das Netzwerk (wie in Schritt 6 oben) aus, in dem die temporäre ESET PROTECT-VA für den Importvorgang installiert werden soll, und klicken Sie auf **Next**.
10. Überprüfen Sie die Einstellungen und klicken Sie auf **Finish**.

Der Bereitstellungsvorgang kann einige Zeit dauern. Während des Vorgangs wird der Citrix-Server als im Leerlauf angezeigt. Unterbrechen Sie den Vorgang nicht.

 Siehe [Dokumentation](#) des Herstellers zur *OVF/OVA*-Bereitstellung.

Nachdem die VM erstellt ist, können Sie sie aktivieren. Die folgenden Informationen werden angezeigt:

```
ESET PROTECT Appliance  
(C) 202 ESET, spol. s r.o. - All rights reserved
```

```
First time appliance configuration needs to be performed.  
Please connect using a web browser to:  
https://
```

```
Static IP address for the connection can be set by these steps:
```

1. Enter management mode with password [eraadmin].
2. Select [Set static IP address] from the menu.
3. Enter network connection parameters.

```
<ENTER> Enter management mode
```

Öffnen Sie Ihren Webbrowser und geben Sie in der Adressleiste die IP-Adresse der neu bereitgestellten ESET PROTECT-Appliance ein. Die IP-Adresse wird im Konsolenfenster aufgeführt (wie oben dargestellt). Die folgende Meldung wird angezeigt: „**Die erstmalige Appliance-Konfiguration muss Über einen Webbrowser unter folgender Adresse ausgeführt werden:https://[IP address]**“.

Der nächste Schritt ist nun die [Konfiguration der Appliance](#) über die Weboberfläche.



Wenn Sie keinen DHCP-Server in Ihrem Netzwerk verwenden, müssen Sie in der Verwaltungskonsole eine [statische IP-Adresse für die ESET PROTECT-VA festlegen](#). Wenn keine IP-Adresse zugewiesen wurde, werden die folgenden Informationen angezeigt (für die URL wird keine IP-Adresse angezeigt). Wenn keine IP-Adresse zugewiesen wurde, kann der DHCP-Server möglicherweise keine Adresse zuweisen. Vergewissern Sie sich, dass im Subnetz der VA freie IP-Adressen vorhanden sind.

```
ESET PROTECT Appliance
(C) 2021 ESET, spol. s r.o. - All rights reserved
```

```
First time appliance configuration needs to be performed.
```

```
Please connect using a web browser to:
https://
```

```
Static IP address for the connection can be set by these steps:
```

1. Enter management mode with password [eraadmin].
2. Select [Set static IP address] from the menu.
3. Enter network connection parameters.

```
<ENTER> Enter management mode
```

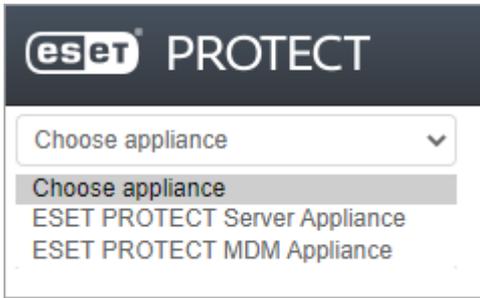
Konfiguration der virtuellen ESET PROTECT-Appliance

Sie können die virtuelle ESET PROTECT-Appliance (ESET PROTECT-VA) schnell und einfach über die Weboberfläche konfigurieren. Sie benötigen einen DHCP-Server in Ihrem Netzwerk, damit die ESET PROTECT-VA automatisch eine IP-Adresse erhält, die wiederum erforderlich ist, um auf die ESET PROTECT-VA-Konfigurationsweboberfläche zuzugreifen.

i Wenn Sie keinen DHCP-Server in Ihrem Netzwerk verwenden, müssen Sie eine [statische IP-Adresse für die ESET PROTECT-VA festlegen](#).

Nachdem Sie die VM der virtuellen ESET PROTECT-Appliance bereitgestellt haben, müssen Sie auswählen, welchen **ESET PROTECT-Appliance-Typ** Sie ausführen möchten. Wählen Sie im Dropdown-Menü in Ihrem Webbrowser den ESET PROTECT-Appliance-Typ aus, der auf der VM ausgeführt werden soll, und konfigurieren Sie ihn. Klicken Sie unten auf den entsprechenden Link, um Konfigurationsanweisungen für die verschiedenen Appliance-Typen anzuzeigen:

- [ESET PROTECT Server-Appliance](#)
- [ESET PROTECT -MDM-Appliance](#)



ESET PROTECT Server-Appliance

Dies ist die Konfigurationsseite für die ESET PROTECT Server-Appliance. Die Konfiguration umfasst die beiden Bereiche **Anwendung** und **Netzwerkeigenschaften**. Füllen Sie alle Pflichtfelder (rot markiert) aus. Bei Bedarf können Sie optionale Konfigurationsparameter angeben.

i Dieser Typ der virtuellen ESET PROTECT-Appliance führt den ESET PROTECT Server auf einer dedizierten VM aus. Diese Konfiguration wird für Netzwerke in kleinen und mittelgroßen Unternehmen empfohlen.

Pflichtfelder der Konfiguration für die ESET PROTECT Server-Appliance:

- **Password** – Dieses [Passwort](#) ist sehr wichtig, weil es in der VM, der ESET PROTECT-Datenbank, der ESET PROTECT-Server-Zertifizierungsstelle und der ESET PROTECT Web-Konsole verwendet wird.

i Der standardmäßige Benutzer der Web-Konsole ist **Administrator**.

APPLICATION

HOSTNAME
The fully qualified hostname for this VM (e.g.: protect.domain.com). Leave blank to try to reverse lookup the IP address.

PASSWORD
VM, database, server certification authority and server webconsole password. Use ASCII characters except reserved '[' and ']';

LOCALE
The locale used for pre-defined objects created during installation.

WINDOWS WORKGROUP
The workgroup or NetBIOS domain name for this server (e.g.: DOMAIN). Leave blank if workgroup should be extracted as first token from the domain and converted to upper case.

WINDOWS DOMAIN
The domain for this server (e.g.: domain.com). Leave blank if no domain synchronization and authorization will be performed.

WINDOWS DOMAIN CONTROLLER
The domain controller for this server (e.g.: dc.domain.com). If domain controller hostname is not recognized by default DNS server, please set this domain controller's IP address as DNS server for this VM. Leave blank if no domain actions will be performed.

WINDOWS DOMAIN ADMINISTRATOR
The administrator account used for joining domain.

WINDOWS DOMAIN ADMINISTRATOR PASSWORD
The administrator password used for joining domain. Leave blank if no domain joining will be performed.

SNMP MANAGER HOSTNAME
The SNMP manager hostname that will be receiving forwarded SNMP traps. Leave blank if no SNMP traps should be forwarded.

ENABLE HTTP FORWARD PROXY
Enables HTTP forward proxy for caching updates (mirror replacement). Policies to redirect HTTP traffic will be created and assigned to all managed products during clean appliance installation.

SUBMIT I accept the terms of the application [End User License Agreement](#) and acknowledge the [Privacy Policy](#).

Die optionalen Parameter sind nicht obligatorisch, es empfiehlt sich jedoch, sie festzulegen. Dies umfasst beispielsweise Parameter zu Domänenenddetails, DC-Details und Kontoinformationen des Domänenadministrators.

Diese Angaben sind für Domänenaktionen nützlich, beispielsweise für die Synchronisierung.

ENABLE HTTP FORWARD
PROXY



Enables HTTP forward proxy for caching updates (mirror replacement). Policies to redirect HTTP traffic will be created and assigned to all managed products during clean appliance installation.

[Bild vergrößern](#)

Sie können auch Apache HTTP Proxy aktivieren, um Updates im Cache zu speichern. Wählen Sie das Kontrollkästchen neben **Enable HTTP forward proxy** aus, um den Apache HTTP Proxy zu installieren und Policies (mit dem Namen **HTTP Proxy-Nutzung**, angewendet auf die Gruppe **Alle**) für die folgenden Produkte zu erstellen und anzuwenden:

OESET Endpoint für Windows

OESET Endpoint für macOS (OS X) und Linux

OESET Management Agent

OESET File Security für Windows Server (6+)

OESET Server Security für Windows (8+)

OESET Shared Local Cache

- Die Policy aktiviert den HTTP-Proxy für die jeweiligen Produkte. Als Proxyhost wird standardmäßig die lokale IP-Adresse des ESET PROTECT Servers zusammen mit Port 3128 konfiguriert. Authentifizierung ist deaktiviert. Sie können diese Einstellungen in andere Policies kopieren, um weitere Produkte einzurichten.
- Mit einem HTTP-Proxy können Sie die Bandbreitennutzung für Downloads aus dem Internet und die Downloadgeschwindigkeiten für Produktupdates drastisch verbessern. Daher sollten Sie das Kontrollkästchen neben **Apache HTTP Proxy** aktivieren, wenn Sie mehr als 37 Computer mit ESET PROTECT verwalten.
- Optional können Sie den Apache HTTP Proxy auch später installieren. Weitere Details finden Sie in unter [Häufige Fragen zur virtuellen ESET PROTECT-Appliance](#).

Netzwerkeigenschaften

Blättern Sie nach unten, um die folgenden Netzwerkeigenschaften festzulegen: **IP-Adresse**, **Netzmaske**, **Standardgateway**, **DNS1**, **DNS2**. Alle Felder sind optional.

Hinzufügen der virtuellen ESET PROTECT-Appliance zu einer Domäne

Sie können die ESET PROTECT-VA bei der Ausgangseinrichtung für den Einsatz in einer Domäne konfigurieren. Die folgenden Einstellungen müssen festgelegt werden, um die ESET PROTECT-VA in einer Domäne zu verwenden:

Windows workgroup – Ein Arbeitsgruppen- oder NETBIOS-Domänenname für diesen Server, zum Beispiel DOMAIN.

Windows domain – Eine Domäne für diesen Server, zum Beispiel *domain.com*.

Windows domain controller – Ein Domänencontroller für diesen Server. Geben Sie den vollqualifizierten Domänennamen (FQDN) des Domänencontrollers ein.

Windows domain administrator – Ein Konto zum Beitreten zur Domäne.

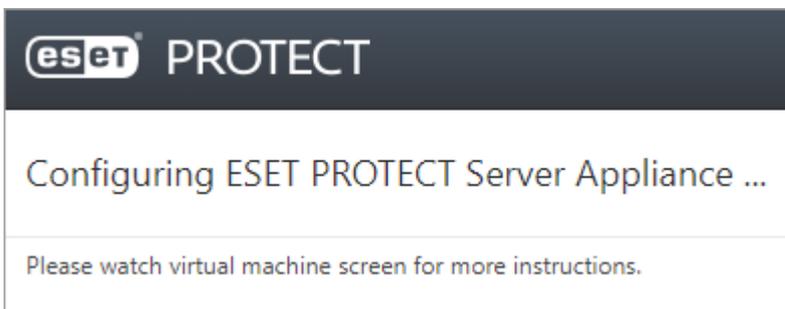
Windows domain administrator password – Ein Administratorpasswort zum Beitreten zur Domäne.

DNS1 – Ein Domänennamensserver für diese virtuelle Maschine. Geben Sie die IP-Adresse des Domänencontrollers ein.

Überprüfen Sie die angegebenen Konfigurationsparameter. Vergewissern Sie sich, dass die Konfiguration stimmt, weil keine zusätzlichen Konfigurationsänderungen möglich sind.

Aktivieren Sie das Kontrollkästchen **Ich stimme der Endbenutzer-Lizenzvereinbarung für die Anwendung und der Datenschutzerklärung zu**. Siehen Sie [Endbenutzer-Lizenzvereinbarung \(EULA\), Nutzungsbedingungen und Datenschutzerklärung für ESET-Produkte](#).

Nachdem Sie auf **Submit** geklickt haben, wird der folgende Hinweis angezeigt:



i Aktualisieren Sie diese Seite nicht im Webbrowser, schließen Sie die Registerkarte und wechseln Sie zum ESET PROTECT-VA-Konsolenfenster.

Im Konsolenfenster der virtuellen ESET PROTECT-Appliance werden Statusinformationen angezeigt. Die Version der ESET PROTECT-Komponenten und der Name, die IP-Adresse und die Portnummer des ESET PROTECT Servers werden angezeigt. Die Adresse der ESET PROTECT-Web-Konsole wird ebenfalls im Format *https://[hostname] and https://[IP address]* angezeigt.

```
ESET PROTECT Server Appliance
(C) 2022 ESET, spol. s r.o. - All rights reserved

Server version: ██████████
Agent version: ██████████
Rogue Detection Sensor version: ██████████

ESET PROTECT Server hostname: protect.local
ESET PROTECT Server IP address: ██████████
ESET PROTECT Server port: see configuration (default is 2222)

To open ESET PROTECT web console please use the following links:
https://protect.local
https://██████████

Please setup virtual machine backup for this server
or create a snapshot before connecting first agents.
```

<ENTER> Enter management mode



Erstellen Sie eine Momentaufnahme oder sichern Sie Ihren virtuellen Computer, bevor Sie die ersten ESET Management Agenten bereitstellen und verbinden.

Geben Sie die Adresse der ESET PROTECT Web-Konsole (wie oben gezeigt) im Webbrowser ein und melden Sie sich bei der ESET PROTECT Web-Konsole an. Der Hostname und die IP-Adresse oben dienen nur der Veranschaulichung und weichen sicherlich von denen von Ihnen anzugebenden Informationen ab. Nach der Anmeldung können Sie [beginnen, mit ESET PROTECT zu arbeiten](#).



Nach der ersten Anmeldung bei der ESET PROTECT-Web-Konsole empfehlen wir, den Client-Task [Betriebssystem-Update](#) auf dem Computer auszuführen, auf dem ESET PROTECT installiert ist.

ESET PROTECT -MDM-Appliance

Dies ist die Konfigurationsseite für die ESET PROTECT MDM Appliance. Die Konfiguration umfasst die beiden Bereiche **Anwendung** und **Netzwerkeigenschaften**. Füllen Sie alle Pflichtfelder (rot markiert) aus. Bei Bedarf können Sie weitere optionale Konfigurationsparameter angeben.



Dieser Typ der virtuellen ESET PROTECT-Appliance führt den ESET PROTECT MDM auf einer dedizierten VM aus. Dieses Produkt eignet sich für kleine ebenso wie für große Unternehmensnetzwerke.



Bevor Sie mit der Konfiguration der ESET PROTECT MDM-Appliance beginnen, [erstellen Sie ein Mobile Device Connector-Zertifikat](#) in der Web-Konsole des ESET PROTECT Servers, der sich mit Ihrer ESET PROTECT MDM-Appliance verbinden wird.

Sie können ESET PROTECT MDM auf zwei Arten konfigurieren:

1. Konfiguration mit Web-Konsolen-Anmeldeinformationen

Pflichtfelder der Konfiguration für die ESET PROTECT MDM-Appliance:

- **Password** – Dieses [Passwort](#) ist sehr wichtig, weil es in der VM und der ESET PROTECT-Datenbank verwendet wird.
- **ESET PROTECT Server Hostname** – Geben Sie den Hostnamen oder die IP-Adresse des ESET PROTECT Servers ein, damit sich ESET PROTECT MDM mit dem ESET PROTECT Server verbinden kann.
- **ESET PROTECT Server Port** – Der standardmäßige ESET PROTECT Serverport ist 2222. Wenn Sie einen anderen Port verwenden, ersetzen Sie den standardmäßigen Port mit der benutzerdefinierten Portnummer.
- **Web Console Port** – Der Standardport für die Web-Konsole ist 2223. Wenn Sie einen anderen Port verwenden, ersetzen Sie den Standardport durch Ihre eigene Portnummer.
- **Password für die Web-Konsole** - Dieses [Passwort](#) ist wichtig, da Sie es für den Zugriff auf die [ESET PROTECT-Web-Konsole](#) brauchen.
- Optional können Sie den **Hostnamen** der **Web-Konsole** eingeben. Die Web-Konsole verwendet diesen Hostnamen, um sich mit dem Server zu verbinden. Wenn Sie dieses Feld nicht ausfüllen, wird automatisch der Wert für den **ESET PROTECT Server-Hostnamen** kopiert.
- **MDM-Hostname** - Geben Sie den MDM FQDN oder die IP-Adresse ein (genau wie im MDC-Zertifikat, das Sie [in der ESET PROTECT-Web-Konsole erstellt haben](#)).

2. Konfiguration mit Zertifikatnutzung

Pflichtfelder der Konfiguration für die ESET PROTECT MDM-Appliance:

- **Password** – Dieses [Passwort](#) ist sehr wichtig, weil es in der VM und der ESET PROTECT-Datenbank verwendet wird.
- **ESET PROTECT Server Hostname** – Geben Sie den Hostnamen oder die IP-Adresse des ESET PROTECT Servers ein, damit sich ESET PROTECT MDM mit dem ESET PROTECT Server verbinden kann.
- **ESET PROTECT Server Port** – Der standardmäßige ESET PROTECT Serverport ist 2222. Wenn Sie einen anderen Port verwenden, ersetzen Sie den standardmäßigen Port mit der benutzerdefinierten Portnummer.
- **Web Console Port** – Der Standardport für die Web-Konsole ist 2223. Wenn Sie einen anderen Port verwenden, ersetzen Sie den Standardport durch Ihre eigene Portnummer.
- **Zertifizierungsstelle Base64** – Fügen Sie das Zertifizierungsstellen-Zertifikat im Base64-Format ein. Informationen zum Abrufen des Zertifikats finden Sie unter [ESET PROTECT-Zertifikate](#).
- **Proxy-Zertifikat Base64** – Fügen Sie das Proxy-Zertifikat im Base64-Format ein. Informationen zum Abrufen des Zertifikats finden Sie unter [ESET PROTECT-Zertifikate](#). Für die Authentifizierung der Kommunikation zwischen ESET PROTECT Server und MDM wird ein Proxyzertifikat verwendet.
- **Agent-Zertifikat Base64** – Fügen Sie das Agent-Zertifikat im Base64-Format ein. Informationen zum Abrufen des Zertifikats finden Sie unter [ESET PROTECT-Zertifikate](#).

- **MDM-Hostname** - Geben Sie den MDM FQDN oder die IP-Adresse ein (genau wie im MDC-Zertifikat, das Sie [in der ESET PROTECT-Web-Konsole erstellt haben](#)).

Netzwerkeigenschaften

Blättern Sie nach unten, um die folgenden Netzwerkeigenschaften festzulegen: **IP-Adresse**, **Netzmaske**, **Standardgateway**, **DNS1**, **DNS2**. Alle Felder sind optional.

ESET PROTECT MDM Appliance

APPLICATION

HOSTNAME

The fully qualified hostname for this VM (e.g.: eset-protect-mdm.domain.com). Leave blank to try to reverse lookup the IP address.

PASSWORD

VM and database password. Use ASCII characters except reserved '[' and ']'.

ESET PROTECT SERVER
HOSTNAME

ESET PROTECT Server hostname or IP address for MDM to connect to.

ESET PROTECT SERVER PORT

ESET PROTECT Server port.

WEBCONSOLE HOSTNAME

Hostname used by webconsole to connect to the server (If left empty, value will be copied from 'ESET PROTECT Server Hostname')

WEBCONSOLE PORT

Port used by webconsole to connect to the server. (Default is '2223')

WEBCONSOLE USERNAME

Username used by webconsole to connect to the server. (Default is 'Administrator')

WEBCONSOLE PASSWORD

Password used by webconsole to connect to the server.

CERTIFICATION AUTHORITY
- BASE64

DER base64 encoded certification authority certificate used for signing server certificate. Not needed if webconsole connection is provided.

PROXY CERTIFICATE -
BASE64

PKCS12 base64 encoded proxy certificate. Not needed if webconsole connection is provided.

PROXY CERTIFICATE
PASSWORD

Proxy peer certificate password. Not needed if webconsole connection is provided.

AGENT CERTIFICATE -
BASE64

PKCS12 base64 encoded agent certificate. Not needed if webconsole connection is provided.

AGENT CERTIFICATE
PASSWORD

Agent peer certificate password. Not needed if webconsole connection is provided.

HTTPS CERTIFICATE -
BASE64

PKCS12 base64 encoded HTTPS certificate. If not present then self-signed certificate will be created.

HTTPS CERTIFICATE
PASSWORD

HTTPS certificate password.

MDM HOSTNAME

MDM hostname or IP address for mobile phones to connect to after enrollment. If empty, appliance IP address will be used.

NETWORKING PROPERTIES

NETWORK IP ADDRESS

The IP address for this interface. Leave blank if DHCP is desired.

NETWORK NETMASK

The netmask for this interface. Leave blank if DHCP is desired.

DEFAULT GATEWAY

The default gateway address for this VM. Leave blank if DHCP is desired.

DNS1

The domain name server for this VM (IP address). Domain from FQDN hostname will be used for short DNS names lookup. Optional for DHCP.

DNS2

The second domain name server for this VM (IP address). Optional field.

SUBMIT

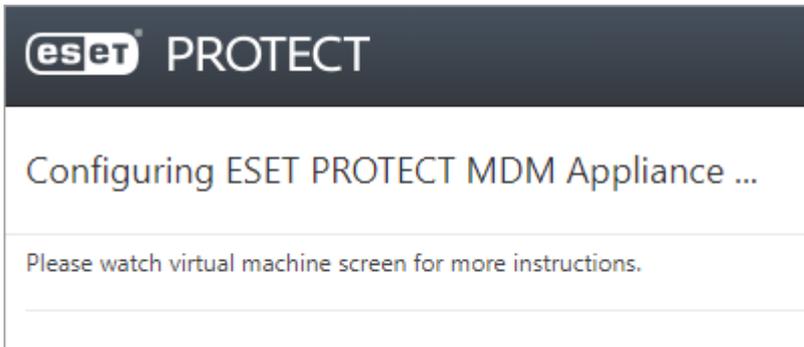
I accept the terms of the application [End User License Agreement](#) and acknowledge the [Privacy Policy](#).

Überprüfen Sie die Konfigurationsparameter. Vergewissern Sie sich, dass die Konfiguration korrekt ist, da später keine weiteren Konfigurationsänderungen möglich sind.

Aktivieren Sie das Kontrollkästchen **Ich stimme der Endbenutzer-Lizenzvereinbarung für die Anwendung und der Datenschutzerklärung zu**. Siehen Sie [Endbenutzer-Lizenzvereinbarung \(EULA\), Nutzungsbedingungen und Datenschutzerklärung für ESET-Produkte](#).

Klicken Sie auf **Absenden**, wenn Sie Ihre Änderungen abgeschlossen haben.

Nachdem Sie auf **Absenden** geklickt haben, wird der folgende Hinweis angezeigt:



i Aktualisieren Sie diese Seite nicht im Webbrowser, schließen Sie die Registerkarte und wechseln Sie zum ESET PROTECT-VA-Konsolenfenster.

Im Konsolenfenster der virtuellen ESET PROTECT-Appliance werden Statusinformationen angezeigt. Dort finden Sie die Version der ESET PROTECT-Komponenten und der Hostname, die IP-Adresse und die Portnummer des ESET PROTECT MDM werden angezeigt. Außerdem wird die MDM-Registrierungsadresse im Format *https://[Hostname]:9980* und *https://[IP-Adresse]:9980* angezeigt.

```
ESET PROTECT Mobile Device Connector Appliance
(C) 2021 ESET, spol. s r.o. - All rights reserved

Server certificate fingerprint (check carefully):
████████████████████████████████████████████████████████████████████████████████

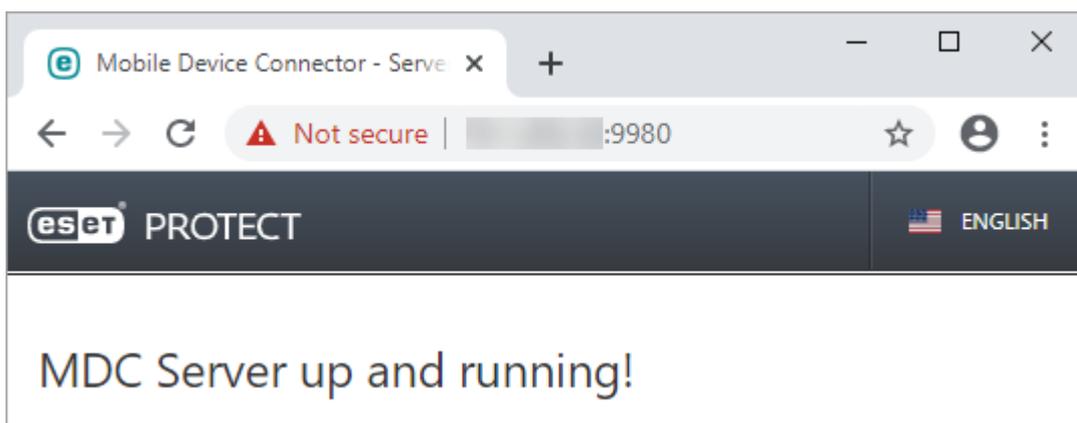
Mobile Device Connector version: ██████████
Agent version: ██████████

MDM hostname: protect.local
MDM IP address: ██████████
MDM enrollment port: see configuration (default is 9980)
MDM communication port: see configuration (default is 9981)

To verify if MDM is running, please use the following links:
https://protect.local:9980
https://██████████:9980

<ENTER> Enter management mode
```

Geben Sie die angezeigte MDM-Registrierungsadresse (siehe oben) in Ihrem Webbrowser ein, um zu überprüfen, ob der Mobile Device Connector korrekt ausgeführt wird. Der Hostname und die IP-Adresse oben dienen nur der Veranschaulichung und weichen sicherlich von denen von Ihnen anzugebenden Informationen ab. Wenn die Bereitstellung erfolgreich war, wird die folgende Meldung angezeigt:



Verwaltungskonsole für die virtuelle ESET PROTECT-Appliance

Öffnen Sie das Terminalfenster des virtuellen Computers, nachdem Sie die ESET PROTECT-VA erfolgreich bereitgestellt haben. Dort sehen Sie grundlegende Informationen zu Ihrer ESET PROTECT-VA und deren Status.

Dies ist der ESET PROTECT-VA-Hauptbildschirm. Hier können Sie sich bei der **ESET PROTECT-VA-Verwaltungskonsole** (auch bekannt als **Verwaltungsmodus**) anmelden, indem Sie die **Eingabetaste** auf Ihrer Tastatur drücken. Um den Verwaltungsmodus zu starten, geben Sie Ihr Passwort ein, das Sie bei der [Konfiguration der ESET PROTECT-VA](#) eingerichtet haben, und drücken Sie zweimal die **Eingabetaste**. Falls Sie Ihre ESET PROTECT-VA noch nicht konfiguriert haben, können Sie das [Standardpasswort](#) `eraadmin` verwenden, um den Verwaltungsmodus zu starten.

Nach der Anmeldung bei der Verwaltungskonsole für die ESET PROTECT-VA sind die folgenden Konfigurations- und Verwaltungsoptionen verfügbar:

- [Statische IP-Adresse festlegen](#)
- [Remotezugriff aktivieren/deaktivieren](#)
- [Datenbank sichern](#)
- [Datenbank wiederherstellen](#)
- [Reset nach Zurücksetzen einer Momentaufnahme](#)
- [Datenbank-Pull von einem anderen Server ausführen](#)
- [VM-Passwort ändern](#)
- [Datenbankpasswort ändern](#)
- [Domäne erneut beitreten](#)
- [Domäne konfigurieren](#)
- [Werkseinstellungen wiederherstellen](#)



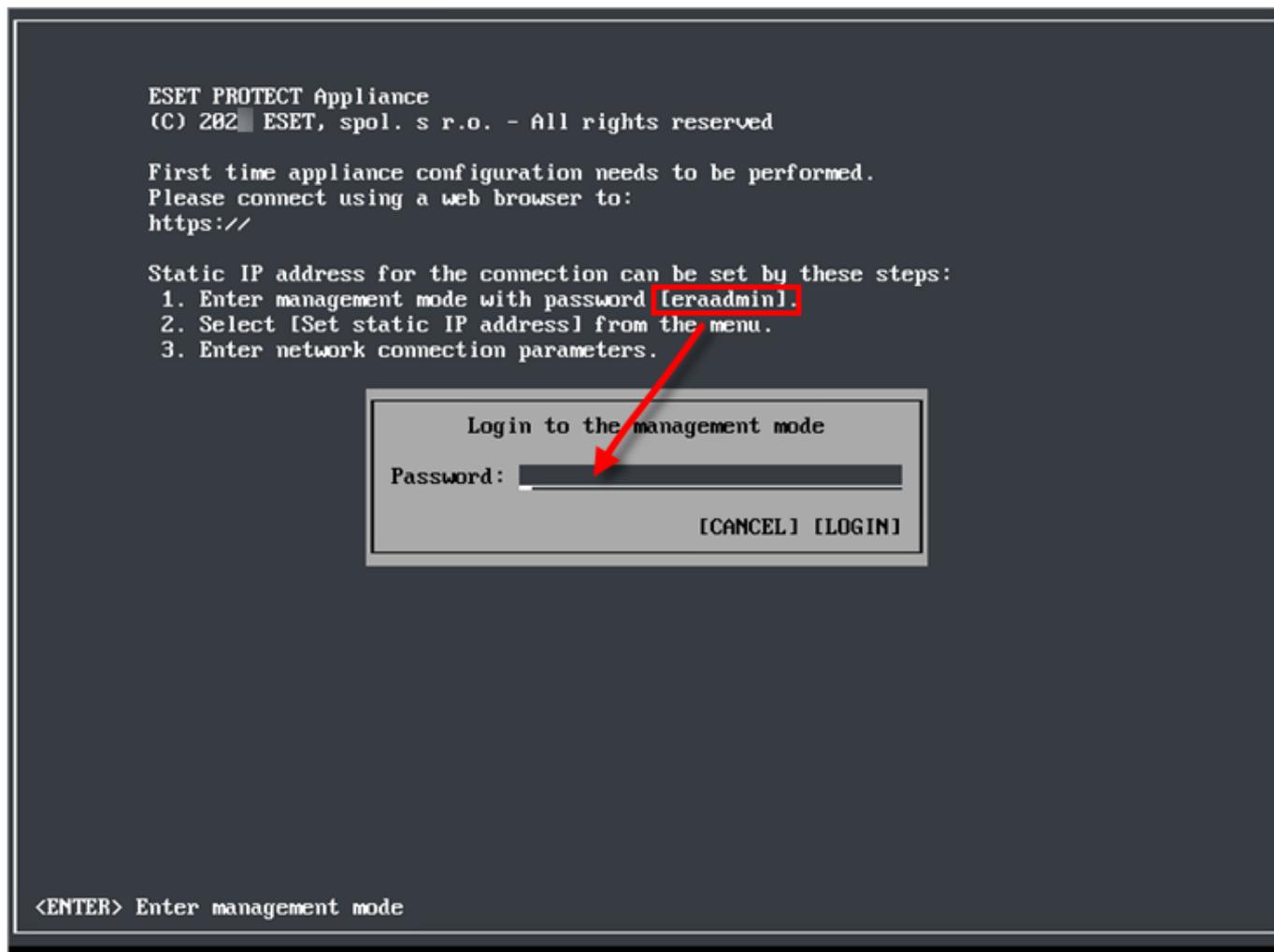
Die Verfügbarkeit mancher Optionen hängt von der Implementierungsphase der ESET PROTECT-VA und dem konfigurierten Appliance-Typ ab.

- **System neu starten** – Startet Ihre ESET PROTECT-VA neu
- **System herunterfahren** – Führt Ihre ESET PROTECT-VA herunter
- **Bildschirm sperren** – Sperren Sie den Bildschirm, um zu verhindern, dass andere Personen Ihre ESET PROTECT-VA verwenden und auf deren Dateien zugreifen. Mit der **Esc**-Taste können Sie den Bildschirm noch schneller sperren. Der Verwaltungsmodus wird geschlossen, und der ESET PROTECT-VA-Hauptbildschirm wird angezeigt.
- **Zurück zum Terminal** - Öffnet das Terminal des Betriebssystems. Dieser Befehl beendet die Verwaltungskonsole für die ESET PROTECT-VA und öffnet das Terminal. Um vom Terminal zum ESET PROTECT-VA-Hauptbildschirm zurückzukehren, geben Sie `exit` ein und drücken Sie die **Eingabetaste** (der Befehl `logout` hat denselben Effekt).

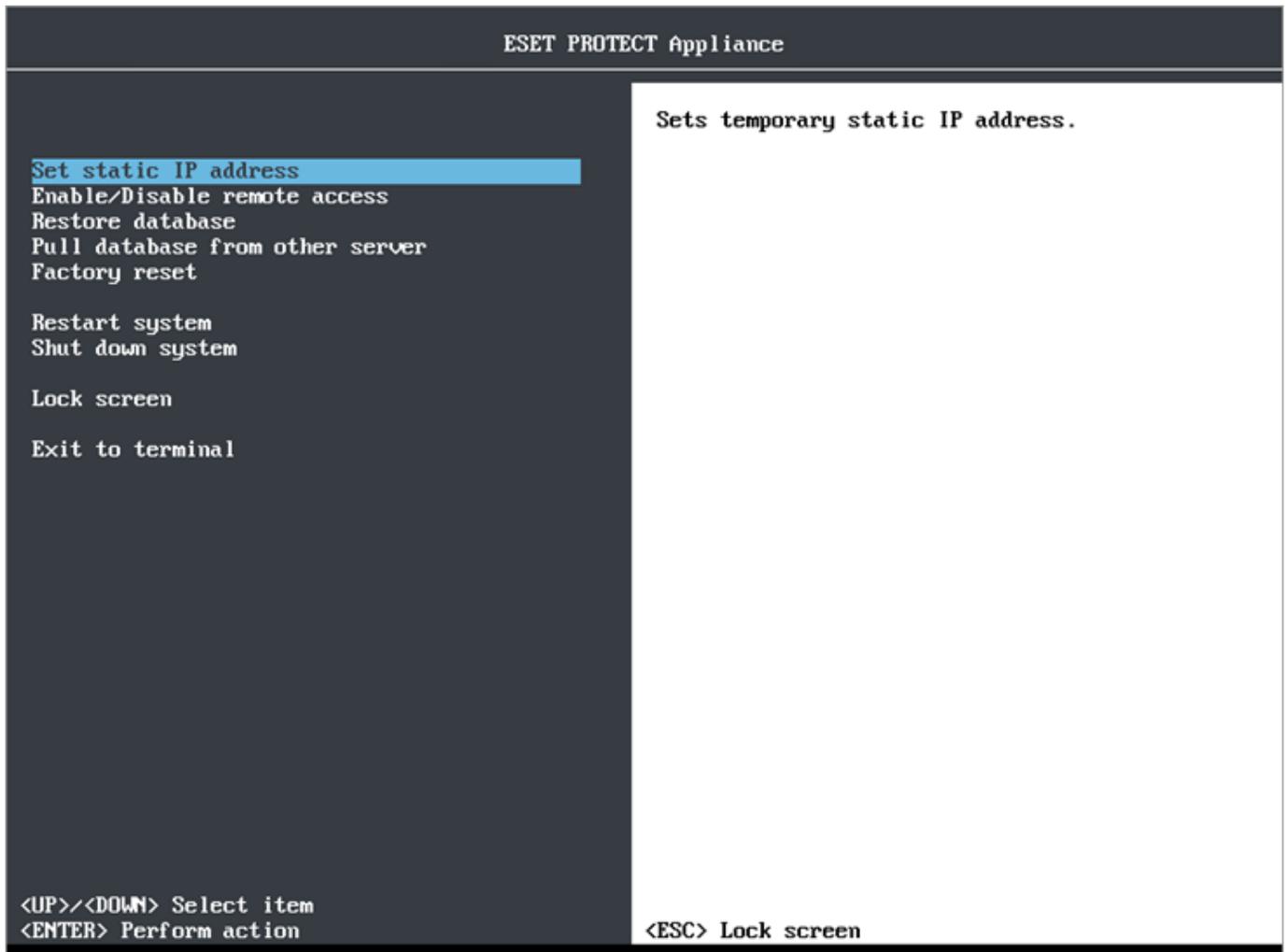
Statische IP-Adresse festlegen

Eine manuelle Konfiguration ist erforderlich, wenn Ihre ESET PROTECT-VA keine IP-Adresse von einem DHCP-Server erhält. Führen Sie die folgenden Anweisungen aus, um eine statische IP-Adresse manuell festzulegen:

1. Drücken Sie im Hauptbildschirm der VM-Konsole die **Eingabetaste** auf Ihrer Tastatur, um den **Verwaltungsmodus zu starten**. Geben Sie `eraadmin` ein und drücken Sie zweimal die **Eingabetaste**, um sich **anzumelden**.



2. Wählen Sie **Statische IP-Adresse festlegen** mit den Pfeiltasten aus und drücken Sie die **Eingabetaste**.



3. Daraufhin wird ein interaktiver Assistent für die Netzwerkkonfiguration gestartet, in dem Sie die folgenden Informationen eingeben müssen:

- Statische IP-Adresse
- Netzwerkmaske
- Gateway-Adresse
- Adresse des DNS-Servers

i Die Netzwerkparameter müssen in der IPv4-Dezimalschreibweise mit Punkt eingegeben werden, z. B. 192.168.1.10 (IP-Adresse) oder 255.255.255.0 (Netzwerkmaske).
Selbst in korrekt konfigurierten Netzwerken ist es **nicht** möglich, einen [Ping an den ESET PROTECT-VA-Computer zu senden](#).

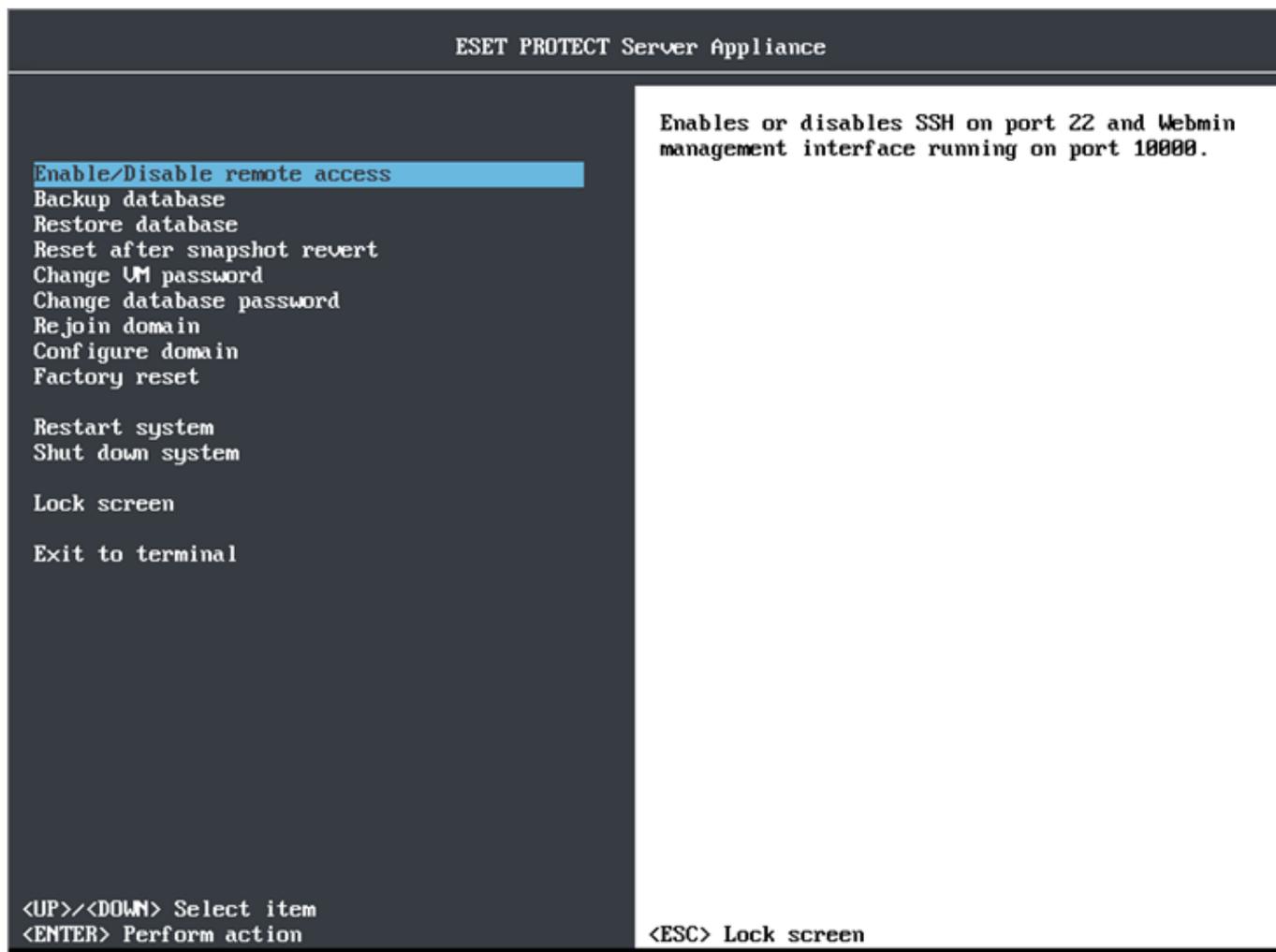
4. Drücken Sie die **Eingabetaste**, um fortzufahren, oder **Strg+C**, um weiterhin im Terminal zu **bleiben**.

Die ESET PROTECT-VA hat standardmäßig eine Netzwerkkarte. Wenn Sie jedoch mehrere Netzwerkkarten hinzufügen, gilt der Befehl **Statische IP-Adresse** festlegen nur für die Netzwerkkarte `eth0`.

Remotezugriff aktivieren/deaktivieren

Um den Remotezugriff ([Webmin-Verwaltungs Oberfläche](#) und [SSH](#)) verwenden zu können, müssen Sie die Funktion zunächst aktivieren.

Starten Sie den Verwaltungsmodus, indem Sie Ihr Passwort eingeben und zweimal die **Eingabetaste** drücken. Wählen Sie den Befehl **Enable/Disable remote access** mit den Pfeiltasten aus und drücken Sie die **Eingabetaste**.



Sie können jetzt Folgendes verwenden:

- Webmin siehe [Webmin-Verwaltungs Oberfläche](#) für Details. Webmin verwendet HTTPS und wird auf Port 10000 ausgeführt. Verwenden Sie für den Zugriff auf die Webmin-Oberfläche die aufgelistete IP-Adresse und die Portnummer 10000 (*https://<host name or IP address>:10000*, z. B. *https://10.10.11.16:10000* oder *https://protect.local:10000*).
- Remotezugriff über SSH auf Port 22 (erforderlich, um [Datenbank-Pulls](#) zu aktivieren).

Die folgenden Informationen werden im Hauptbildschirm der ESET PROTECT-VA-Verwaltungskonsole angezeigt:

```
ESET PROTECT Server Appliance
(C) 2021 ESET, spol. s r.o. - All rights reserved

Server version: ██████████
Agent version: ██████████
Rogue Detection Sensor version: ██████████

ESET PROTECT Server hostname: protect.local
ESET PROTECT Server IP address: ██████████
ESET PROTECT Server port: see configuration (default is 2222)

To open ESET PROTECT web console please use the following links:
https://protect.local
https://██████████

SSH and Webmin access are enabled on ports 22 and 10000.
```

<ENTER> Enter management mode

Siehe auch [SSH-Fehlerbehebung](#).

Datenbank sichern

Sicherungen sind ein entscheidender Teil einer umfassenden Strategie für die Notfallwiederherstellung. Die Funktion **Datenbanksicherung** sichert Ihre **ESET PROTECT-Datenbank** und speichert sie in einer MySQL-Sicherungsdatei mit dem Namen *era-backup.sql* im Ordner *root*.

i Anstelle der Datenbanksicherung können Sie auch Momentaufnahmen der VM erstellen. Dabei wird die gesamte ESET PROTECT-VA inklusive aller Einstellungen sowie die ESET PROTECT-Datenbank gesichert. Wenn Sie jedoch eine Momentaufnahme Ihrer VM wiederherstellen, müssen Sie den Befehl [Reset nach Zurücksetzen einer Momentaufnahme](#) ausführen.

! Sie sollten Ihre ESET PROTECT-Datenbank häufig sichern und die Sicherungsdatei in einem externen Speichermedium ablegen. Auf diese Weise haben Sie im Notfall eine Kopie der gesamten ESET PROTECT-Datenbank an einem separaten Ort (nicht lokal auf Ihrer ESET PROTECT-VA). Zum Beispiel wenn Ihre ESET PROTECT-VA defekt ist oder gelöscht oder auf andere Weise zerstört wird. Mit einer frischen Sicherung der ESET PROTECT-Datenbank können Sie die ESET PROTECT-VA in einen Status kurz vor dem Notfall wiederherstellen. Weitere Details finden Sie unter [ESET PROTECT-VA-Notfallwiederherstellung](#).

1. Starten Sie den Verwaltungsmodus, indem Sie Ihr Passwort eingeben und zweimal die **Eingabetaste** drücken. Wählen Sie mit den Pfeiltasten den Befehl **Datenbanksicherung** aus und drücken Sie die **Eingabetaste**.

Enable/Disable remote access

Backup database

Restore database

Reset after snapshot revert

Change UM password

Change database password

Rejoin domain

Configure domain

Factory reset

Restart system

Shut down system

Lock screen

Exit to terminal

<UP>/<DOWN> Select item

<ENTER> Perform action

Backups ESET PROTECT database to '/root/era-backup.sql'. By moving and restoring this backup on a new appliance and then configuring it as ESET PROTECT server you will initiate database upgrade. Destination file will be rewritten. Please always copy created backup outside from this appliance to safe encrypted storage.

<ESC> Lock screen

2. Sie müssen Ihr [Datenbank-Root-Passwort](#) eingeben, bevor die Datenbanksicherung beginnt.

i Wenn Sie das Datenbank-Root-Passwort vergessen haben, können Sie es [ändern](#) und die Datenbanksicherung erneut ausführen.

```
Backing up ERA database ...
Enter database root password.
Enter password:

Database backup finished. Review any errors and then press Enter to continue.
```

! Dieser Prozess dauert je nach Größe Ihrer Datenbank zwischen einigen Sekunden und mehreren Stunden. Während der Datenbanksicherung wird der ESET PROTECT Server beendet, um die Datenkonsistenz zu gewährleisten.

i Überprüfen Sie den Bildschirm stets auf Fehler. Fehlermeldungen bedeuten, dass die Datenbanksicherung nicht erfolgreich abgeschlossen wurde. Führen Sie die **Datenbanksicherung** in diesem Fall erneut aus.

Sie finden die Datenbanksicherung unter: `/root/era-backup.sql`

! Laden Sie die Sicherungsdatei mit dem [Webmin-Dateimanager](#) an einen sicheren Ort herunter.

Datenbank wiederherstellen

Diese Funktion ersetzt Ihre aktuelle Datenbank durch eine Datenbank aus Ihrer [Sicherung](#).

i Legen Sie unbedingt eine Momentaufnahme der VM oder eine Sicherung der aktuellen Datenbank an. Dies ist ein Fallback, falls bei der Wiederherstellung Probleme auftreten.

Gehen Sie wie folgt vor, um die **Datenbank wiederherzustellen**:

1. Starten Sie den Verwaltungsmodus, indem Sie Ihr Passwort eingeben und zweimal die **Eingabetaste** drücken. Wählen Sie mit den Pfeiltasten den Befehl **Datenbank wiederherstellen** aus und drücken Sie die **Eingabetaste**.

```
ESET PROTECT Server Appliance

Enable/Disable remote access
Backup database
Restore database
Reset after snapshot revert
Change VM password
Change database password
Rejoin domain
Configure domain
Factory reset

Restart system
Shut down system

Lock screen

Exit to terminal

<UP>/<DOWN> Select item
<ENTER> Perform action

Restores ESET PROTECT database from
'/root/era-backup.sql'. You will lose current
state in ESET PROTECT server. Do not mix backups
from different servers and different server
versions. By restoring corrupted file you can
break ESET PROTECT server. Proceed with caution.

<ESC> Lock screen
```

! Laden Sie die *era-backup.sql*-Sicherungsdatei, die Sie wiederherstellen möchten, mit dem [Webmin-Dateimanager](#) in das *root*-Verzeichnis hoch. Die *era-backup.sql*-Zielfile wird überschrieben. Überspringen Sie diesen Schritt, falls sich die *era-backup.sql*-Datei, die Sie wiederherstellen möchten, bereits im *root*-Verzeichnis befindet.

! Mischen Sie keine Sicherungen von unterschiedlichen Servern oder Serverversionen. Verwenden Sie ausschließlich die *era-backup.sql*-Datei, die von derselben ESET PROTECT-VA [gesichert](#) wurde. Unter Umständen kann es jedoch sinnvoll sein, eine Datenbank auf eine andere ESET PROTECT-VA wiederherzustellen, jedoch nur, wenn diese VA frisch bereitgestellt und noch nicht [konfiguriert](#) wurde.

2. Möglicherweise müssen Sie Ihr **Datenbank-Root-Passwort eingeben**, bevor die Datenbank wiederhergestellt werden kann. Wenn Sie jedoch eine Datenbank auf einer frisch bereitgestellten ESET PROTECT-VA wiederherstellen, die noch nicht konfiguriert wurde, werden Sie nicht zur Eingabe Ihres Passworts aufgefordert.

```
Restoring ERA database ...  
Enter database root password:  
  
Restoral of database backup finished. Review any errors and then press Enter to continue.
```

Dieser Prozess dauert je nach Größe Ihrer Datenbank zwischen einigen Sekunden und mehreren Stunden.

i Überprüfen Sie den Bildschirm stets auf Fehler. Fehlermeldungen bedeuten, dass die Datenbank nicht erfolgreich wiederhergestellt wurde. Führen Sie die **Wiederherstellung der Datenbank** in diesem Fall erneut aus.

Reset nach Zurücksetzen einer Momentaufnahme

Wenn Sie eine Momentaufnahme Ihrer VM auf einen früheren Status zurückgesetzt haben, müssen Sie immer die Funktion **Reset after snapshot revert** ausführen, damit alle verbundenen Clients ihren Status mit dem jeweiligen Server synchronisieren.

1. Starten Sie den Verwaltungsmodus, indem Sie Ihr Passwort eingeben und zweimal die **Eingabetaste** drücken. Wählen Sie den Befehl **Reset after snapshot revert** mit den Pfeiltasten aus und drücken Sie die **Eingabetaste**.

```

Enable/Disable remote access
Backup database
Restore database
Reset after snapshot revert
Change UM password
Change database password
Rejoin domain
Configure domain
Factory reset

Restart system
Shut down system

Lock screen

Exit to terminal

```

```

<UP>/<DOWN> Select item
<ENTER> Perform action

```

```

Resets ESET PROTECT server realm and reboots.
This needs to be executed everytime this virtual
machine was reverted to some earlier snapshot.
Reset will force all connecting clients to
resynchronize their states with this server.

```

```
<ESC> Lock screen
```

2. Sie müssen Ihr [Datenbank-Root-Passwort](#) eingeben, bevor der **ESET PROTECT Server realm** zurückgesetzt wird.

```

Resetting ERA server realm ...
Enter database root password:

Reset of ERA server realm finished. Press Enter to reboot.
_

```

Datenbank-Pull von einem anderen Server ausführen

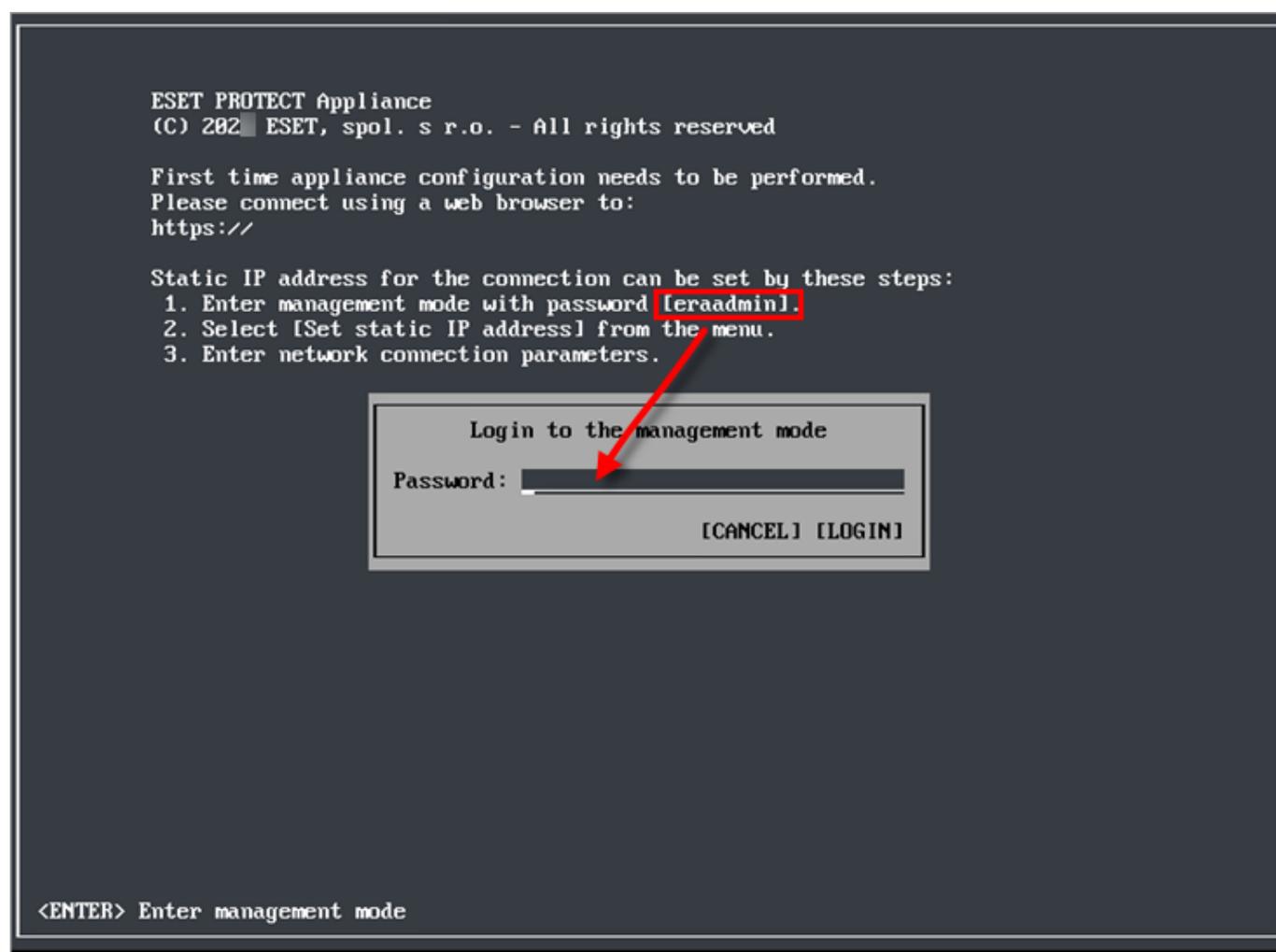
Mit dieser Funktion können Sie die ESET PROTECT-Datenbank von einer vorhandenen ESET PROTECT-VA in Ihrer Infrastruktur per Pull abrufen. Diese Funktion wird nur auf dem ESET PROTECT Server unterstützt, nicht auf den anderen Komponenten (MDM). Dies ist praktisch, wenn Sie Ihre ESMC-VA oder eine ältere ESET PROTECT-VA auf die neueste ESET PROTECT-VA [aktualisieren](#), oder wenn Sie Ihre ESET PROTECT-VA migrieren möchten.

Bei einer Migration muss die alte ESET PROTECT-VA weiterhin erreichbar sein, um die [Änderungs-Policy für Hostname/IP-Adresse](#) für alle Clientcomputer übernehmen zu können. Andernfalls können sich die Clients nicht mit Ihrer neuen ESET PROTECT-VA verbinden und werden weiterhin versuchen, sich mit der alten Instanz zu verbinden.

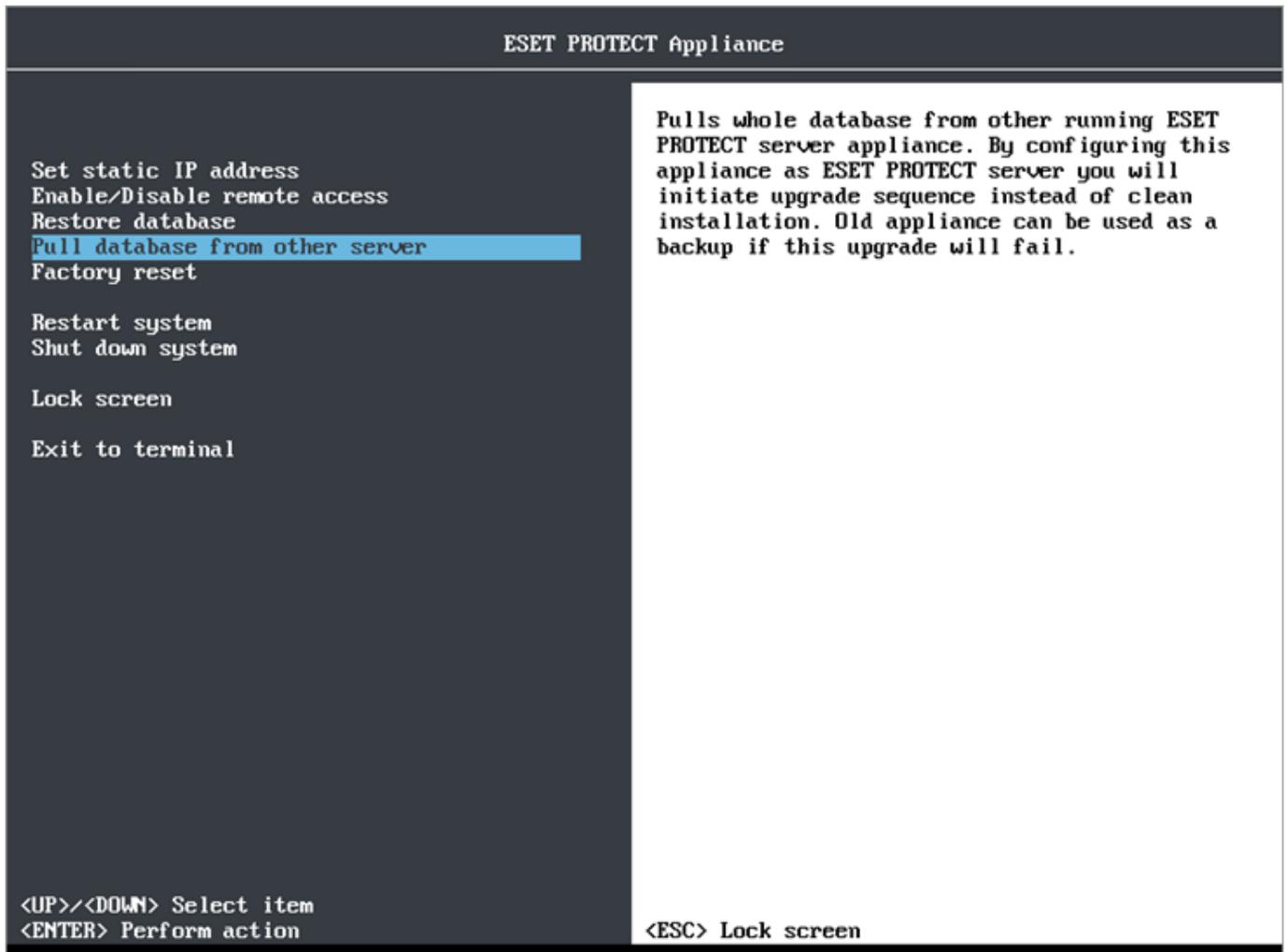
- ! Stellen Sie sicher, dass [SSH auf Ihrer alten ESET PROTECT-VA aktiviert ist](#). Führen Sie nur dann einen Datenbank-Pull durch, wenn Sie auf eine neuere oder dieselbe Version von ESET PROTECT Server migrieren. Während des Pull-Vorgangs wird die Datenbankstruktur aktualisiert, aber dieser Vorgang schlägt für ältere Server fehl. Der Datenbank-Pull ist eine von zwei Methoden, um [Ihre VA zu aktualisieren](#).

Führen Sie dazu die folgenden Schritte aus:

1. [Stellen Sie eine neue ESET PROTECT-VA](#) bereit, ohne diese jedoch zu konfigurieren.
2. Öffnen Sie die VM-Konsole und drücken Sie im Hauptbildschirm die **Eingabetaste**, um den **Verwaltungsmodus** für Ihre neu bereitgestellte ESET PROTECT-VA zu öffnen.
3. Geben Sie `eraadmin` ein und drücken Sie zweimal die **Eingabetaste**, um sich **anzumelden**.



4. Wählen Sie **Datenbank-Pull von einem anderen Server ausführen** mit den Pfeiltasten aus und drücken Sie die **Eingabetaste**.



5. **Geben Sie das Datenbank-Root-Passwort** für die Remote-ESET PROTECT-VA ein, von der Sie die ESET PROTECT-Datenbank abrufen möchten (Ihre alte ESET PROTECT-VA). Falls Sie nur ein Passwort für Ihre alte ESET PROTECT-VA verwenden, geben Sie dieses Passwort hier ein.

6. **Verbinden Sie sich per SSH mit der Remote-ESET PROTECT-VA** – Geben Sie Benutzername (`root`) und Hostname bzw. IP-Adresse Ihrer alten ESET PROTECT-VA im folgenden Format ein: `root@IPaddress` oder `root@hostname`

7. Geben Sie `yes` ein, wenn Sie nach der **Echtheit des Hosts** gefragt werden. Andernfalls können Sie diesen Schritt ignorieren.

8. Geben Sie das **VM-Passwort** Ihrer alten ESET PROTECT-VA ein und drücken Sie die **Eingabetaste**. Nach Abschluss des Sicherungsvorgangs wird die Nachricht **Datenbank des Remote-ERA Servers wurde gesichert** angezeigt.

i Die Dauer von Sicherungs- und Wiederherstellungsvorgängen hängt von der Größe Ihrer Datenbank ab.

9. Geben Sie das **VM-Passwort** Ihrer alten ESET PROTECT-VA erneut ein. Je nach Dauer des Datenbankkopiervorgangs müssen Sie das Passwort während des Kopiervorgangs unter Umständen mehrmals eingeben.

10. Warten Sie, bis die Datenbank wiederhergestellt wurde.

```

Enter database root password on remote ERA server:
Enter connection to remote ERA server appliance in format 'root@hostname'.
SSH connection: root@10.1.
Connecting ...
The authenticity of host '10.1. (10.1.)' can't be established.
ECDSA key fingerprint is 5b:60:dd:bf:d7:bd:a5:00:8d:3d:99:a6:58:17:9f:21.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.1.' (ECDSA) to the list of known hosts.
root@10.1.'s password:

Trying to stop remote ERA server (you may see errors as we are trying different methods) ...
bash: line 2: stop: command not found
Redirecting to /bin/systemctl stop eraserver.service

Backing up remote ERA server database ...

Starting remote ERA server (you may see errors as we are trying different methods) ...
bash: line 8: start: command not found
Redirecting to /bin/systemctl start eraserver.service

Remote ERA server database was backed up. Press Enter to continue.

Copying backup to local appliance ...
root@10.1.'s password:
era-upgrade-backup.sql          100% 2994KB   2.9MB/s   00:00

Restoring ERA database ...

Restoral of remote database backup finished. Shutdown remote appliance and configure this appliance
with same parameters. Press Enter to continue.

```

11. Wenn Sie ein Upgrade durchführen: Nach einem erfolgreichen Pull der ESET PROTECT-Datenbank können Sie die alte ESET PROTECT-VA herunterfahren und außer Betrieb nehmen.

- Bewahren Sie Ihre alte ESET PROTECT-VA jedoch so lange auf, bis Sie sichergestellt haben, dass die neue Instanz korrekt funktioniert.
- Wir empfehlen dringend, den alten ESET PROTECT VA Server nicht mit einem Deinstallationskript zu deinstallieren. Bei dieser Deinstallation werden alle Lizenzen von der neuen ESET PROTECT VA Server-Datenbank ebenfalls getrennt (entfernt). Um dies zu verhindern, löschen Sie die alte ESET PROTECT VA Server-Datenbank (`DROP DATABASE`) vor der Deinstallation.

12. [Konfigurieren Sie Ihre neue Appliance](#):

- **Upgrade** - Konfigurieren Sie Ihre neue VA exakt gleich wie Ihre alte ESET PROTECT-VA.
- **Migration** - Passen Sie die Konfiguration an die neuen Domänen- (Domäne [konfigurieren](#) oder [erneut beitreten](#)) oder Netzwerkeigenschaften an, wenn Sie Ihre ESET PROTECT-VA z. B. in ein neues Netzwerk migriert haben.

i Stellen Sie sicher, dass alle Daten vorhanden sind, dass sich alle Clients mit Ihrem neuen Server verbinden und dass sich Ihre neue ESET PROTECT-VA gleich verhält wie Ihre vorherige Instanz.

VM-Passwort ändern

Ihr VM-Passwort dient zur Anmeldung bei Ihrer bereitgestellten virtuellen ESET PROTECT-Appliance. Wenn Sie Ihr VM-Passwort ändern oder Ihre VM besser schützen möchten, sollten Sie [sichere Passwörter](#) verwenden und diese regelmäßig ändern.

Bei dieser Prozedur wird nur das Passwort für den virtuellen Computer geändert. Das Passwort für die ESET PROTECT Web-Konsole und das Datenbank-Root-Passwort wird nicht geändert. Weitere Informationen finden Sie unter [Passwort-Typen für die ESET PROTECT-VA](#).

Falls Sie Ihr Passwort vergessen haben, lesen Sie den Abschnitt [Vergessenes Passwort für die ESET PROTECT-VA wiederherstellen](#).

1. Starten Sie den **Verwaltungsmodus**, indem Sie Ihr Passwort eingeben und zweimal die **Eingabetaste** drücken. Wählen Sie mit den Pfeiltasten den Befehl **VM-Passwort ändern** aus und drücken Sie die **Eingabetaste**.

```
ESET PROTECT Server Appliance

Enable/Disable remote access
Backup database
Restore database
Reset after snapshot revert
Change VM password
Change database password
Rejoin domain
Configure domain
Factory reset

Restart system
Shut down system

Lock screen

Exit to terminal

<UP>/<DOWN> Select item
<ENTER> Perform action

Changes root password used to log into this
virtual machine.

<ESC> Lock screen
```

2. Geben Sie Ihr **neues Passwort** in das leere Feld ein, drücken Sie die **Eingabetaste** und geben Sie das Passwort zur Bestätigung **erneut** ein.

```
Changing password for user root.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
  
Press Enter to continue or Ctrl+C to stay in terminal.
```

Daraufhin wird die Nachricht Authentifizierungstoken wurden aktualisiert angezeigt, und Sie können sich mit Ihrem **neuen Passwort** anmelden.

Datenbankpasswort ändern

Mit dem Datenbank-`root`-Passwort haben Sie Vollzugriff auf den MySQL-Datenbankserver. Der MySQL-`root`-Benutzer hat volle Kontrolle über den MySQL-Server.

1. Starten Sie den **Verwaltungsmodus**, indem Sie Ihr Passwort eingeben und zweimal die **Eingabetaste** drücken. Wählen Sie den Befehl **Change database password** mit den Pfeiltasten aus und drücken Sie die **Eingabetaste**.

```
ESET PROTECT Server Appliance

Enable/Disable remote access
Backup database
Restore database
Reset after snapshot revert
Change VM password
Change database password
Rejoin domain
Configure domain
Factory reset

Restart system
Shut down system

Lock screen

Exit to terminal

<UP>/<DOWN> Select item
<ENTER> Perform action

Changes root database password. ESET PROTECT
server is connected to the database with
different user called 'era'. Its connection
string can be found at
'/etc/opt/eset/RemoteAdministrator/Server/Startu
pConfiguration.ini'.

<ESC> Lock screen
```

2. Wenn Sie zur **Eingabe des alten Datenbank-Root-Passworts** aufgefordert werden, geben Sie das [Passwort](#) ein, das Sie bei der [Konfiguration der virtuellen ESET PROTECT-Appliance](#) festgelegt haben. Dieses Passwort unterscheidet sich unter Umständen von Ihrem **VM-Passwort**, falls Sie es separat [geändert](#) haben.

```
Enter new database root password:
Enter old database root password.
Enter password:

Press Enter to continue or Ctrl+C to stay in terminal.
```

Das neue Datenbank-root-Passwort ist jetzt aktiv.

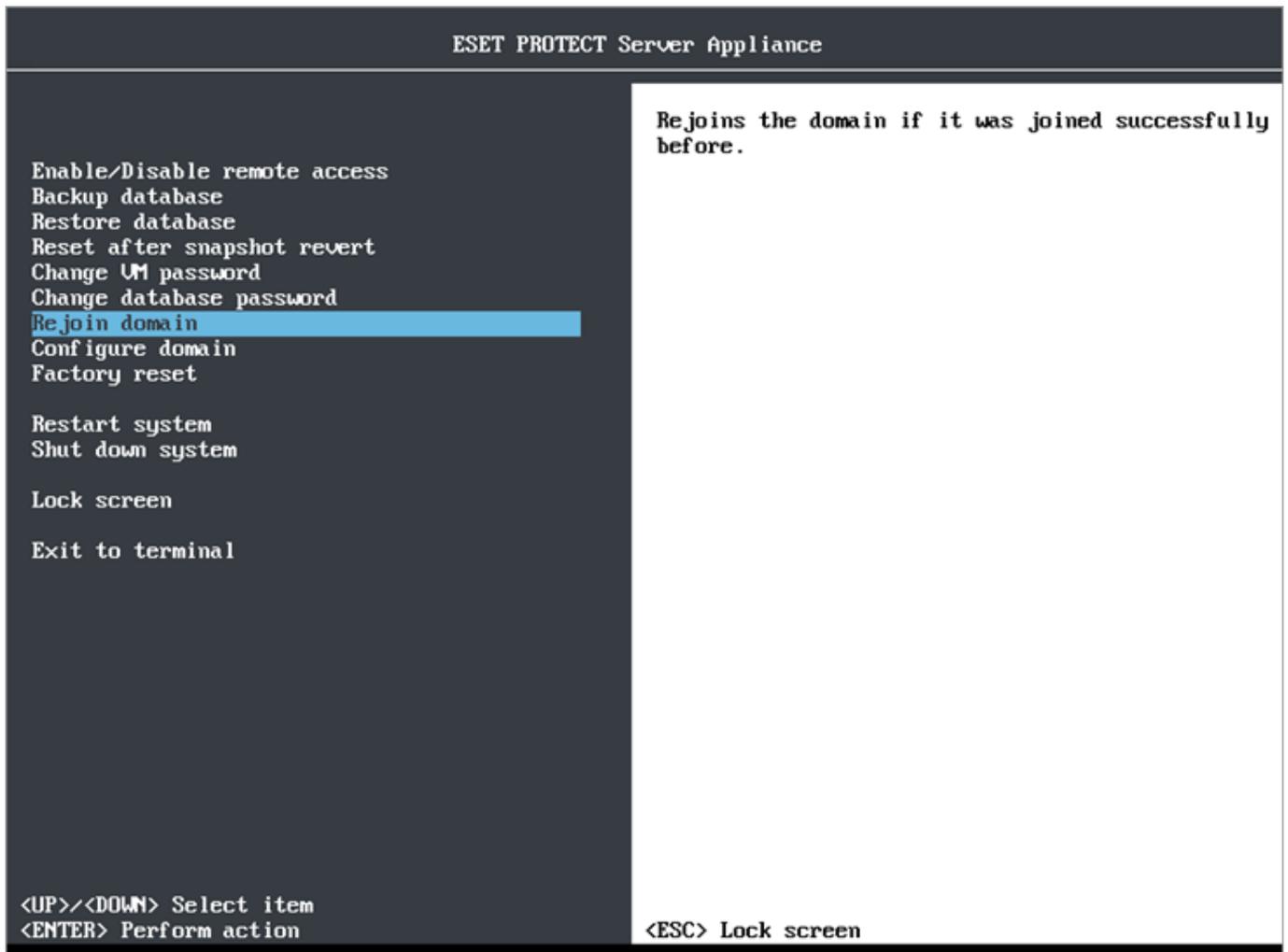
Domäne erneut beitreten

Verwenden Sie diese Funktion, wenn Probleme mit Active Directory oder Vertrauensstellungen innerhalb der Domäne auftreten.



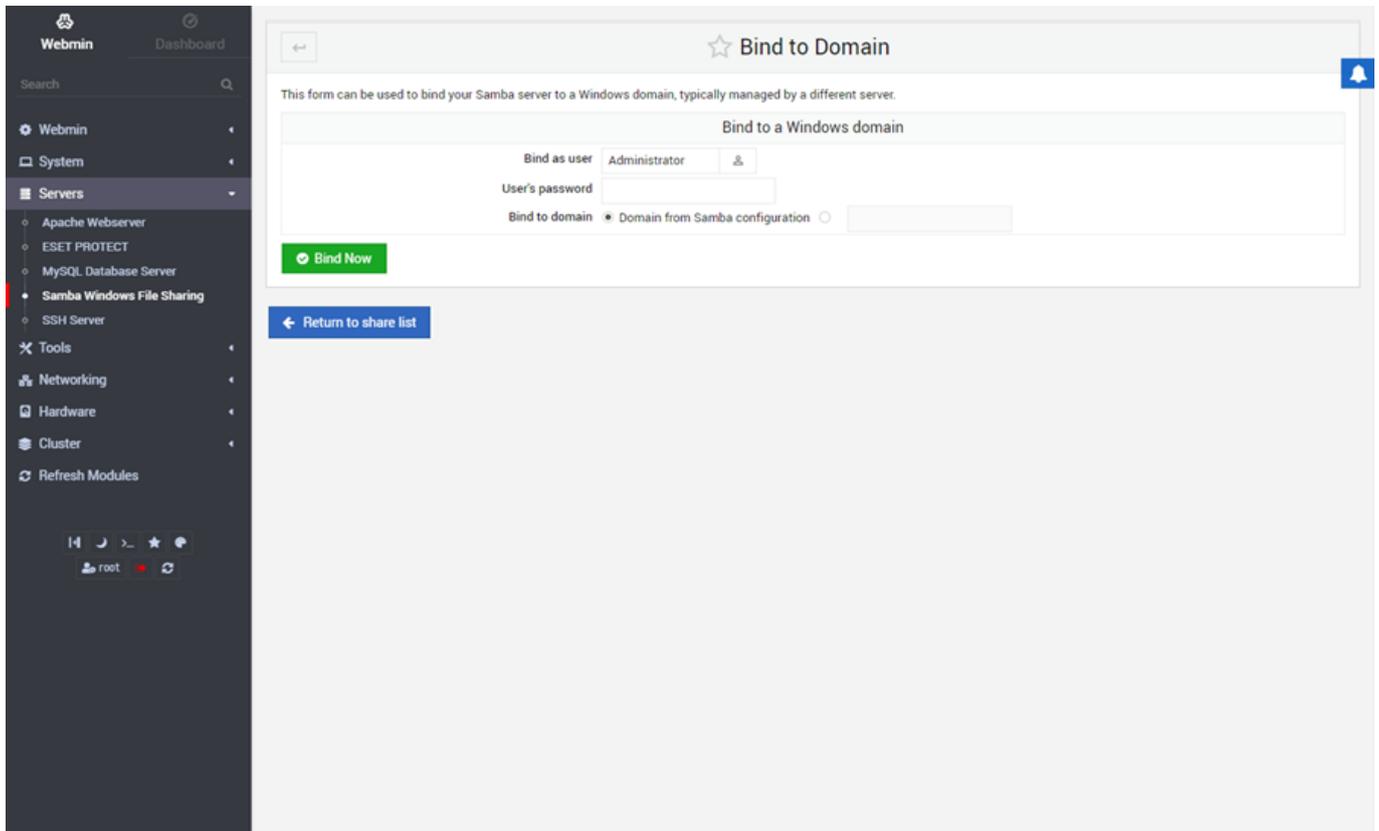
Es ist wichtig, dass Ihre [Domäne korrekt konfiguriert](#) ist. Andernfalls kann es passieren, dass dieser Befehl nicht funktioniert.

1. Starten Sie den Verwaltungsmodus, indem Sie Ihr Passwort eingeben und zweimal die **Eingabetaste** drücken. Wählen Sie den Befehl **Rejoin domain** mit den Pfeiltasten aus und drücken Sie die **Eingabetaste**.



2. Geben Sie den Domänen-Benutzernamen ein, der für den Beitritt zur Domäne verwendet werden soll.

Falls Sie nicht mit Linux und der Befehlszeile vertraut sind, können Sie [Webmin](#) und die Funktion **Bind to Domain** für die [Samba Windows-Dateifreigabe](#) verwenden.



Domäne konfigurieren

Wenn beim Beitreten zur Domäne ein Fehler auftritt, liegt dies oft an einer falschen Konfiguration der ESET PROTECT-VA-Dateien. **Configure Domain** Mit dem Befehl Domäne konfigurieren können Sie Konfigurationsdateien bearbeiten, um bestimmte Einstellungen für Ihre Umgebung zu integrieren. Die folgenden Konfigurationsdateien sind verfügbar:

Dateiname	Beschreibung
<i>/etc/hosts</i>	Die Datei Hosts muss auf den Namen und die IP-Adresse Ihres Domänencontrollers verweisen.
<i>/etc/krb5.conf</i>	Die Kerberos-Konfigurationsdatei muss fehlerfrei generiert werden. Stellen Sie sicher, dass <code>kinit <user-from-domain></code> funktioniert.
<i>/etc/ntp.conf</i>	Die NTP-Konfigurationsdatei muss einen Eintrag für regelmäßige Aktualisierungen der Systemzeit vom Domänencontroller enthalten.
<i>/etc/samba/smb.conf</i>	Die Samba-Konfigurationsdatei muss fehlerfrei generiert werden.

Diese Dateien sind vorkonfiguriert und erfordern minimale Änderungen, beispielsweise um einen Domänennamen, den Namen eines Domänencontrollers oder eines DNS-Servers anzugeben.

1. Starten Sie den **Verwaltungsmodus**, indem Sie Ihr Passwort eingeben und zweimal die **Eingabetaste** drücken. Wählen Sie den Befehl **Configure domain** mit den Pfeiltasten aus und drücken Sie die **Eingabetaste**.

i Diese Prozedur sollte nur von erfahrenen Administratoren ausgeführt werden.

```

Enable/Disable remote access
Backup database
Restore database
Reset after snapshot revert
Change UM password
Change database password
Rejoin domain
Configure domain
Factory reset

```

```

Restart system
Shut down system

```

```
Lock screen
```

```
Exit to terminal
```

```

<UP>/<DOWN> Select item
<ENTER> Perform action

```

Takes you through all necessary configuration files that are used in the domain join operation. You can also use Webmin to help you with the domain join.

```
<ESC> Lock screen
```

2. Drücken Sie die **Eingabetaste**, um die erste Konfigurationsdatei zu bearbeiten.

3. Drücken Sie die Tastenkombination **Strg+X**, um den Text-Editor zu schließen. Daraufhin werden Sie gefragt, ob Sie Ihre Änderungen speichern möchten. Drücken Sie **Y** zum Speichern oder **N** zum Verwerfen. Falls Sie keine Änderungen vorgenommen haben, wird der Texteditor einfach geschlossen. Falls Sie weitere Änderungen vornehmen möchten, drücken Sie **Strg+C** anstelle von **Strg+X**, um den Vorgang abzubrechen und zum Texteditor zurückzukehren. In diesem [Knowledgebase-Artikel](#) finden Sie Beispiele zum Bearbeiten der Konfigurationsdateien.

i Beachten Sie die Datei `/root/help-with-domain.txt` auf Ihrer ESET PROTECT-VA. Sie finden diese Datei, indem Sie im [Webmin-Dateimanager](#) nach `help-with-domain.txt` suchen. Alternativ können Sie die Hilfedatei mit dem Befehl `nano help-with-domain.txt` öffnen. Falls Sie nicht mit Linux und der Befehlszeile vertraut sind, können Sie die Domänenverbindung (Kerberos, NTP oder Netzwerkeinstellungen über die [Samba Windows-Dateifreigabe](#)) mit [Webmin](#) konfigurieren.

4. Wählen Sie nach Abschluss der Domänenkonfiguration die Option **Domäne erneut beitreten** aus und geben Sie den Administratornamen und das Passwort für die Domänenverbindung ein.

Werkseinstellungen wiederherstellen

Mit dem Befehl **Werkseinstellungen wiederherstellen** können Sie Ihre virtuelle ESET PROTECT-Appliance in den Originalzustand nach der Bereitstellung zurückversetzen. Sämtliche Konfigurationen und Einstellungen werden zurückgesetzt, und die gesamte ESET PROTECT-Datenbank wird gelöscht.

Sie sollten Ihre [ESET PROTECT-Datenbank unbedingt sichern](#), bevor Sie die **Werkseinstellungen wiederherstellen**. Nach der Wiederherstellung der Werkseinstellungen ist Ihre Datenbank leer. Beim **Wiederherstellen der Werkseinstellungen** werden nur Einstellungen zurückgesetzt, die bei der [Konfiguration der ESET PROTECT-VA](#) geändert wurden. Alle anderen Änderungen und Einstellungen bleiben erhalten. In seltenen Fällen kann es vorkommen, dass Ihre VA beim **Wiederherstellen der Werkseinstellungen** nicht komplett in den Originalzustand zurückversetzt wird. Falls Probleme mit der ESET PROTECT-VA auftreten, sollten Sie eine neue Instanz bereitstellen. Führen Sie die entsprechenden Schritte für [Upgrade/Migration](#) aus oder führen Sie eine [Notfallwiederherstellung](#) durch.

1. Starten Sie den Verwaltungsmodus, indem Sie Ihr Passwort eingeben und zweimal die **Eingabetaste** drücken. Wählen Sie den Befehl **Factory reset** mit den Pfeiltasten aus und drücken Sie die **Eingabetaste**.

```
ESET PROTECT Server Appliance

Enable/Disable remote access
Backup database
Restore database
Reset after snapshot revert
Change UM password
Change database password
Rejoin domain
Configure domain
Factory reset
Restart system
Shut down system

Lock screen

Exit to terminal

<UP>/<DOWN> Select item
<ENTER> Perform action

Resets the appliance to the factory state. All
database data will be lost. Please create a
backup before continuing.

<ESC> Lock screen
```

2. Drücken Sie die **Eingabetaste**, um Ihre ESET PROTECT-VA auf die **Werkseinstellungen wiederherstellen** oder können Sie an diesem Punkt **Strg+C** drücken, um das Menü zu verlassen.

! Sobald die **Wiederherstellung der Werkseinstellungen** begonnen hat, dürfen Sie **Strg+C** nicht mehr drücken, da andernfalls Ihre virtuelle Appliance beschädigt werden kann.

```
Press Enter to reset the appliance to the factory state or Ctrl+C to stop.
```

```
Clearing Webmin ...
```

```
Uninstalling ESET products ...  
Stopping running instance of eraserver.service  
Disabling eraserver.service  
Removed symlink /etc/systemd/system/multi-user.target.wants/eraserver.service.  
Removing service file /etc/systemd/system/eraserver.service  
Removing service file /etc/systemd/system/eraserver-xvfb.service  
Dissociating seat from ESET servers... done  
Removing database... done  
Uninstalling SELinux policy..._
```



Führen Sie die **Wiederherstellung** erneut aus, falls während des Vorgangs irgendwelche Fehlermeldungen angezeigt werden. Falls der Fehler durch ein erneutes **Zurücksetzen auf die Werkseinstellungen** nicht behoben wird oder Sie sich nicht sicher sind, sollten Sie eine neue Instanz bereitstellen. Führen Sie dazu die Schritte für [Upgrade/Migration](#) aus oder führen Sie eine [Notfallwiederherstellung](#) durch.

Beim **Zurücksetzen auf die Werkseinstellungen** werden die folgenden Aktionen ausgeführt:

- Netzwerkkonfiguration, alle [Passwörter](#) und ein Hostname werden zurückgesetzt
- Webmin, Appliance-Konfigurationsdateien, Pakete und Systemprotokolle werden zurückgesetzt
- Sämtliche Daten werden aus der ESET PROTECT-Datenbank gelöscht
- Das Benutzerpasswort für die ESET PROTECT-Datenbank wird zurückgesetzt

Nach einem Neustart ist Ihre ESET PROTECT-VA im Originalzustand wie nach einer neuen Bereitstellung und kann von Grund auf neu konfiguriert werden.



Spezielle Änderungen oder Einstellungen, die nicht mit ESET PROTECT zusammenhängen, werden nicht zurückgesetzt.

Webmin-Verwaltungsoberfläche

Webmin ist eine externe webbasierte Oberfläche zur Verwaltung von Linux-Systemen. Webmin wurde für Personen entwickelt, die über Linux-Erfahrung verfügen, sich jedoch nicht mit den Details der Systemadministration auskennen. Sie können verschiedene Aufgaben über eine intuitive Weboberfläche ausführen, und die entsprechenden Konfigurationsdateien werden automatisch aktualisiert. Dieses Modul erleichtert Ihnen die Verwaltung Ihres Systems.

- Sie können Webmin in einem Webbrowser öffnen oder sich von einem beliebigen System (Clientcomputer oder Mobilgerät) anmelden, das mit Ihrem Netzwerk verbunden ist. Dieses Modul ist einfacher über das Netzwerk zu verwenden als lokal mit anderen grafischen Konfigurationsprogrammen.

- Alle aktuellen Versionen von Webmin dürfen für die kommerzielle und nichtkommerzielle Nutzung frei verteilt und modifiziert werden. Weitere Informationen finden Sie auf den [Webmin-Webseiten](#).

Webmin ist in Ihrer virtuellen ESET PROTECT-Appliance enthalten. Sie müssen dieses Modul zunächst [aktivieren](#). Webmin verwendet HTTPS und den Port 10000. Die IP-Adresse für Webmin wird in der [ESET PROTECT-VA-Verwaltungskonsole](#) angezeigt.

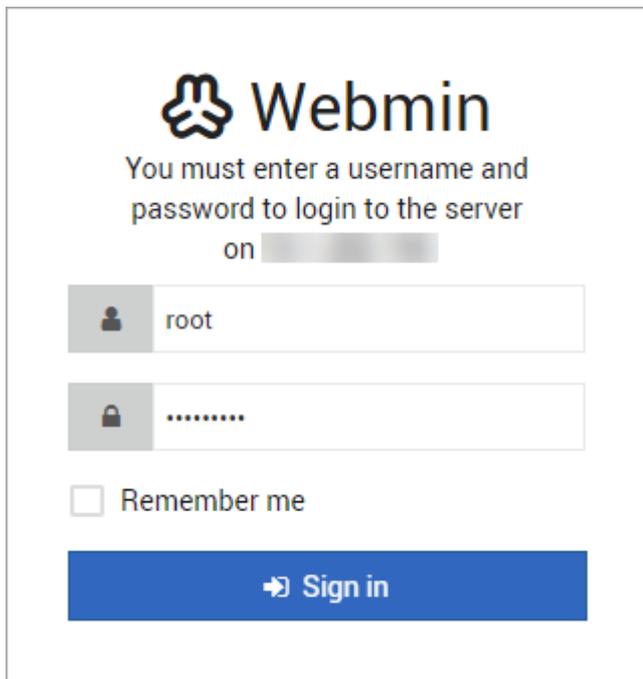
So verwenden Sie Webmin:

Öffnen Sie Ihren Webbrowser, und geben Sie die IP-Adresse oder den Hostnamen Ihrer bereitgestellten ESET PROTECT-VA zusammen mit Port 10000 in die Adressleiste ein. Die URL muss das folgende Format haben: *https://<host name or IP address>:10000*, z. B. *https://10.1.119.162:10000* oder *https://esmcva:10000*.

Geben Sie Benutzernamen und Passwort ein:

oDer Benutzername lautet **root**

oDas Standardpasswort ist **eraadmin**. Falls Sie das Passwort bereits geändert haben, verwenden Sie das Passwort, das Sie bei der [Konfiguration der ESET PROTECT-VA](#) eingerichtet haben.



Nach der Anmeldung wird das Webmin-[Dashboard](#) angezeigt.

Dashboard

Nach der Anmeldung bei Webmin wird das **Dashboard** mit Systeminformationen für Ihre ESET PROTECT-VA angezeigt. Dort finden Sie Informationen wie Hostname, Betriebssystem, Betriebszeit, Speicherauslastung, Paketupdates usw. Der Infobereich am unteren Seitenrand enthält Elemente, die Ihre Aufmerksamkeit erfordern. Wenn zum Beispiel eine neue Version von Webmin verfügbar ist, können Sie auf die Schaltfläche **Webmin jetzt aktualisieren** klicken, um diese zu installieren. Sie sollten die Upgrades unbedingt installieren. Nach Abschluss des Upgrades wird die Nachricht **Webmin-Installation abgeschlossen** angezeigt.

Das Hauptmenü enthält die folgenden Modulkategorien: **Webmin, System, Server, Tools, Netzwerk, Hardware**

und **Cluster**. Weitere Informationen zu Modulen finden Sie unter [Webmin-Module](#).

i Webmin erkennt die VA-Konfiguration automatisch und zeigt die relevanten Module entsprechend an.

Die wichtigsten Module für die Verwaltung Ihrer ESET PROTECT-VA sind:

- [System](#)
- [Server](#)
- [Tools](#)
- [Netzwerk](#)

! Webmin wird unter Linux mit **Root-Berechtigungen** ausgeführt und kann daher auf Ihrem System alle Dateien bearbeiten und alle Befehle ausführen. Bei einem Fehler kann es passieren, dass alle Dateien auf Ihrem System gelöscht werden oder dass Ihr System nicht mehr startet. Aus diesem Grund sollten Sie Webmin mit Vorsicht einsetzen. Webmin warnt Sie normalerweise vor Aktionen mit Fehlerpotenzial. Dennoch sollten Sie keine Änderungen an Konfigurationselementen vornehmen, mit denen Sie nicht vertraut sind.

The screenshot displays the Webmin dashboard interface. On the left is a dark sidebar with navigation options: Webmin, System, Servers, Tools, Networking, Hardware, Cluster, and Refresh Modules. The main content area is titled 'System Information' and features four circular progress indicators for CPU (2%), REAL MEMORY (48%), VIRTUAL MEMORY (0%), and LOCAL DISK SPACE (11%). Below these are system details in a grid format:

System hostname	protect.local	Operating system	CentOS Linux 7.9.2009
Webmin version	1.974	Authentic theme version	19.75
Time on system	Wednesday, October 20, 2021 10:55 AM	Kernel and CPU	Linux 3.10.0-1160.45.1.el7.x86_64 on x86_64
Processor information	Intel(R) Xeon(R) Platinum 8176 CPU @ 2.10GHz, 4 cores	System uptime	21 hours, 02 minutes
Running processes	138	CPU load averages	0.01 (1 min) 0.05 (5 mins) 0.05 (15 mins)
Real memory	1.76 GiB used / 1.04 GiB cached / 3.7 GiB total	Virtual memory	0 bytes used / 3.87 GiB total
Local disk space	7.14 GiB used / 52.88 GiB free / 60.02 GiB total	Package updates	All installed packages are up to date

A yellow warning banner at the bottom of the system information section states: 'Warning! Webmin version 1.981 is now available, but you are running version 1.974.' with an 'Upgrade Webmin Now' button. Below the main information are expandable sections for Stats History, Recent Logins, Network Interfaces, and Disk Usage.

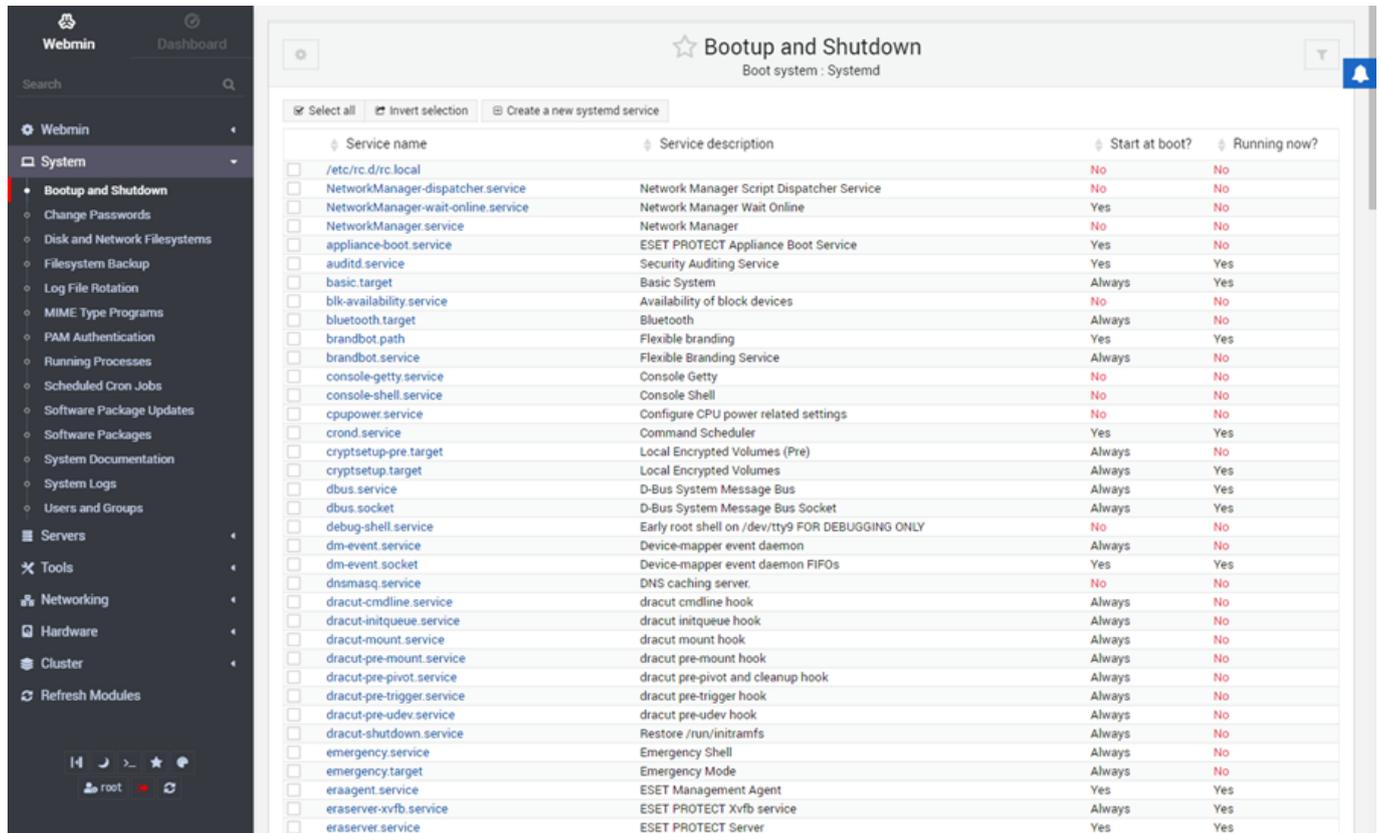
Benachrichtigung - Webmin zeigt Benachrichtigungen am unteren Rand des Dashboards an, um Sie auf wichtige Dinge hinzuweisen.

Abmeldung - Wenn Sie Ihre Webmin-Sitzung abgeschlossen haben, können Sie sich mit dem Abmeldungssymbol  im Menü auf der linken Seite abmelden.

System

In diesem Bereich können Sie bestimmte **Systemmodule** konfigurieren.

[Systemstart und Herunterfahren](#) - In diesem Modul können Sie Dienste verwalten und bearbeiten und einzelne Dienste oder mehrere Dienste auf einmal starten, beenden oder neu starten. Außerdem können Sie Skripts erstellen und bearbeiten, die beim Systemstart oder beim Herunterfahren ausgeführt werden. Mit den Schaltflächen am unteren Seitenrand können Sie die ESET PROTECT-VM **neu starten** oder **herunterfahren**.



The screenshot shows the Webmin interface for the 'Bootup and Shutdown' module. The left sidebar contains a navigation menu with 'System' expanded to show 'Bootup and Shutdown'. The main content area displays a table of system services. The table has four columns: 'Service name', 'Service description', 'Start at boot?', and 'Running now?'. Each row includes a checkbox for selecting the service. The services listed include various system components like NetworkManager, ESET PROTECT, and basic system targets.

Service name	Service description	Start at boot?	Running now?
<input type="checkbox"/> /etc/rc.d/rc.local		No	No
<input type="checkbox"/> NetworkManager-dispatcher.service	Network Manager Script Dispatcher Service	No	No
<input type="checkbox"/> NetworkManager-wait-online.service	Network Manager Wait Online	Yes	No
<input type="checkbox"/> NetworkManager.service	Network Manager	No	No
<input type="checkbox"/> appliance-boot.service	ESET PROTECT Appliance Boot Service	Yes	No
<input type="checkbox"/> auditd.service	Security Auditing Service	Yes	Yes
<input type="checkbox"/> basic.target	Basic System	Always	Yes
<input type="checkbox"/> blk-availability.service	Availability of block devices	No	No
<input type="checkbox"/> bluetooth.target	Bluetooth	Always	No
<input type="checkbox"/> brandbot.path	Flexible branding	Yes	Yes
<input type="checkbox"/> brandbot.service	Flexible Branding Service	Always	No
<input type="checkbox"/> console-getty.service	Console Getty	No	No
<input type="checkbox"/> console-shell.service	Console Shell	No	No
<input type="checkbox"/> cpupower.service	Configure CPU power related settings	No	No
<input type="checkbox"/> crond.service	Command Scheduler	Yes	Yes
<input type="checkbox"/> cryptsetup-pre.target	Local Encrypted Volumes (Pre)	Always	No
<input type="checkbox"/> cryptsetup.target	Local Encrypted Volumes	Always	Yes
<input type="checkbox"/> dbus.service	D-Bus System Message Bus	Always	Yes
<input type="checkbox"/> dbus.socket	D-Bus System Message Bus Socket	Always	Yes
<input type="checkbox"/> debug-shell.service	Early root shell on /dev/tty9 FOR DEBUGGING ONLY	No	No
<input type="checkbox"/> dm-event.service	Device-mapper event daemon	Always	No
<input type="checkbox"/> dm-event.socket	Device-mapper event daemon FIFOs	Yes	Yes
<input type="checkbox"/> dnsmasq.service	DNS caching server	No	No
<input type="checkbox"/> dracut-cmdline.service	dracut cmdline hook	Always	No
<input type="checkbox"/> dracut-initqueue.service	dracut initqueue hook	Always	No
<input type="checkbox"/> dracut-mount.service	dracut mount hook	Always	No
<input type="checkbox"/> dracut-pre-mount.service	dracut pre-mount hook	Always	No
<input type="checkbox"/> dracut-pre-pivot.service	dracut pre-pivot and cleanup hook	Always	No
<input type="checkbox"/> dracut-pre-trigger.service	dracut pre-trigger hook	Always	No
<input type="checkbox"/> dracut-pre-udev.service	dracut pre-udev hook	Always	No
<input type="checkbox"/> dracut-shutdown.service	Restore /run/initramfs	Always	No
<input type="checkbox"/> emergency.service	Emergency Shell	Always	No
<input type="checkbox"/> emergency.target	Emergency Mode	Always	No
<input type="checkbox"/> eraagent.service	ESET Management Agent	Yes	Yes
<input type="checkbox"/> eraserver-xvfb.service	ESET PROTECT Xvfb service	Always	Yes
<input type="checkbox"/> eraserver.service	ESET PROTECT Server	Yes	Yes

[Passwörter ändern](#) - In diesem Modul können Sie die Passwörter für die Benutzer des VM-Betriebssystems ändern.



Verwenden Sie dieses Modul nicht, um das Passwort für die ESET PROTECT-VA oder die ESET PROTECT-Datenbank zu ändern. Verwenden Sie in diesem Fall stattdessen die Befehle [VM-Passwort ändern](#) bzw. [Datenbankpasswort ändern](#) in der [ESET PROTECT-VM-Verwaltungskonsole](#).

[Laufende Prozesse](#) - Mit Webmin können Sie sämtliche auf Ihrem System laufenden Prozesse verwalten. In diesem Modul können Sie die Prozesse auf Ihrem System anzeigen und beenden, Prioritäten ändern und Prozesse ausführen.

[Updates für Softwarepakete](#) - In diesem Modul können Sie verfügbare Updates abrufen und alle oder nur ausgewählte Pakete aktualisieren.

[Systemprotokolle](#) - In diesem Modul können Sie die Protokolldateien auf Ihrem System anzeigen und den Speicherort der Protokollnachrichten ändern.

Server

In diesem Bereich können Sie bestimmte **Servermodule** konfigurieren:

[Apache-Webserver](#) - Dies ist eines der komplexesten und umfangreichsten Webmin-Module und ermöglicht die Konfiguration fast aller Apache-Funktionen. Dieses Modul kann als HTTP-Server für Installationsdateien und Updates verwendet werden. Konfigurieren Sie die [Firewall](#), in dem Sie Regeln für die entsprechenden Ports hinzufügen.

i Dies ist nicht der Apache-Webserver, der für die ESET PROTECT-Web-Konsole verwendet wird. Sie können diesen Apache-Webserver jedoch bei Bedarf für andere Zwecke einsetzen.

[ESET PROTECT](#) – Mit diesem Modul können Sie das **Diagnose-Tool ausführen**, das **ESET PROTECT Server Administrator-Passwort zurücksetzen**, das **ESET PROTECT Server-Zertifikat** und die **Zertifizierungsstelle reparieren**, das **ESET Management Agent-Zertifikat** und die **Zertifizierungsstelle reparieren**, die **ESET Management Agenten-Verbindung reparieren** oder die Datei **server.xml für Apache Tomcat bearbeiten**, um das HTTPS-Zertifikat oder den Verschlüsselungsalgorithmus für die Web-Konsole zu ändern.

[MySQL-Datenbankserver](#) – Mit diesem Modul können Sie Benutzerberechtigungen verwalten, Passwörter ändern und Datenbankinhalte anzeigen.

! Verwenden Sie das MySQL-Datenbankservermodul nicht, um die ESET PROTECT-Datenbank zu sichern oder wiederherzustellen. Führen Sie diese Aufgaben stattdessen mit der Verwaltungskonsole für die virtuelle ESET PROTECT-Appliance durch. Weitere Details finden Sie unter [Datenbanksicherung](#).

[Samba Windows-Dateifreigabe](#) - Mit diesem Modul können Sie Verzeichnisse angeben, die über das SMB (Server Message Block)-Protokoll für Windows-Clients freigegeben werden sollen. Sie können Samba konfigurieren, um Dateien auf Ihrer ESET PROTECT-VA für Windows-Clients verfügbar zu machen. Außerdem können Sie eine Windows-Domäne konfigurieren und dieser beitreten. Wenn Freigaben aktiviert sind, müssen die Samba-Ports in der Firewall ebenfalls aktiviert werden.

[SSH-Server](#) – Mit diesem Modul können Sie SSH- und OpenSSH-Server konfigurieren. Die Benutzer benötigen Grundkenntnisse der entsprechenden Clientprogramme. Sie können SSH-Server und -Clients auf Ihrem System konfigurieren.

ESET PROTECT

Mit dem **ESET PROTECT**-Modul können Sie vordefinierte Befehle ausführen, z. B. um ESET PROTECT-Zertifikate zu reparieren, Diagnose-Tools auszuführen oder das Passwort für den ESET PROTECT Server zurückzusetzen.

Run Diagnostic Tool - Klicken Sie auf die Schaltfläche, um Protokolle und Informationen aus dem System abzurufen. Daraufhin werden Protokolle für ESET PROTECT Server und ESET Management Agent exportiert. Mit dem [Dateimanager](#)-Modul können Sie die exportierten Diagnoseprotokolle suchen und in einem komprimierten *.zip*-Format herunterladen.

■ Run Diagnostic Tool

Runs diagnostic tool to extract logs and information from the system.

Edit command

Results will be placed into /root directory as compressed files with a timestamp.

Reset ESET PROTECT Server Administrator Password – Falls Sie das Passwort für Ihren ESET PROTECT Server

vergessen haben oder das Passwort zurücksetzen möchten, geben Sie Ihr neues Passwort für das Administratorkonto auf dem ESET PROTECT Server ein und klicken Sie auf die Schaltfläche, um den Befehl auszuführen.

<input checked="" type="checkbox"/> Reset ESET PROTECT Server Administrator Password	Resets ESET PROTECT Server	<input type="button" value="Edit command"/>
Administrator password. Password	

Repair ESET PROTECT Server Certificate – Repariert das Zertifikat des ESET PROTECT Servers mit einem neuen PFX/PKCS12-Zertifikat. Klicken Sie auf die **Büroklammer**, suchen Sie nach der PFX- bzw. PKCS12-Zertifikatdatei für den ESET PROTECT Server und klicken Sie auf **Öffnen**. Geben Sie das Passwort für das Zertifikat des ESET PROTECT Servers ein und klicken Sie auf die Schaltfläche, um den Befehl auszuführen.

<input checked="" type="checkbox"/> Repair ESET PROTECT Server Certificate	Repairs ESET PROTECT Server certificate with new	<input type="button" value="Edit command"/>
PFX/PKCS12 certificate. Certificate	<input type="button" value="🔗"/>	Certificate password

Repair ESET PROTECT Server Certification Authority – Repariert die Zertifizierungsstelle des ESET PROTECT Servers mit einem DER-Zertifikat. Klicken Sie auf die **Büroklammer**, suchen Sie nach der *.der*-Zertifizierungsstellenzertifikatdatei und klicken Sie auf **Öffnen**.

<input checked="" type="checkbox"/> Repair ESET PROTECT Server Certification Authority	Repairs ESET PROTECT Server	<input type="button" value="Edit command"/>
certification authority with DER certificate. Certificate	<input type="button" value="🔗"/>	

Repair ESET Management Agent Connection – Repariert die Verbindung zwischen ESET Management Agent und ESET PROTECT Server. Geben Sie **Hostname** und **Portnummer** Ihres ESET PROTECT Servers ein und klicken Sie auf die Schaltfläche, um den Befehl auszuführen.

<input checked="" type="checkbox"/> Repair ESET Management Agent Connection	Repairs ESET Management Agent connection to	<input type="button" value="Edit command"/>
ESET PROTECT Server. Hostname	Port	

Repair ESET Management Agent Certificate – Repariert das Zertifikat des ESET Management Agent mit einem neuen PFX/PKCS12-Zertifikat. Klicken Sie auf die **Büroklammer**, suchen Sie nach der *PFX-* bzw. *PKCS12-*Zertifikatdatei für den ESET Management Agent und klicken Sie auf **Öffnen**. Geben Sie das Passwort für das Zertifikat des ESET Management Agent ein und klicken Sie auf die Schaltfläche, um den Befehl auszuführen.

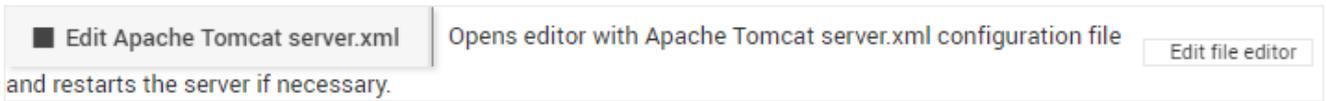
 Die Zertifikat-Passphrase darf die folgenden Zeichen nicht enthalten: " \ Diese Zeichen verursachen kritische Fehler bei der Initialisierung des Agenten.

<input checked="" type="checkbox"/> Repair ESET Management Agent Certificate	Repairs ESET Management Agent certificate with	<input type="button" value="Edit command"/>
new PFX/PKCS12 certificate. Certificate	<input type="button" value="🔗"/>	Certificate password

Repair ESET Management Agent Certification Authority – Repariert die Zertifizierungsstelle des ESET Management Agenten mit einem DER-Zertifikat. Klicken Sie auf die **Büroklammer**, suchen Sie nach der *.der*-Zertifizierungsstellenzertifikatdatei und klicken Sie auf **Öffnen**.

<input checked="" type="checkbox"/> Repair ESET Management Agent Certification Authority	Repairs ESET Management Agent	<input type="button" value="Edit command"/>
certification authority with DER certificate. Certificate	<input type="button" value="🔗"/>	

Edit Apache Tomcat server.xml - Sie können die Apache Tomcat server.xml-Konfigurationsdatei bearbeiten, um die HTTPS-Zertifikate und Verschlüsselungsalgorithmen für die Web-Konsole zu ändern. Klicken Sie auf die Schaltfläche, um einen Texteditor zu öffnen und die `/etc/tomcat/server.xml`-Datei zu bearbeiten. Klicken Sie auf **Speichern**, um Ihre Änderungen zu speichern. Falls ein Neustart erforderlich ist, wird dieser automatisch durchgeführt. Klicken Sie auf **Zurück zu den Befehlen**, falls Sie Ihre Änderungen nicht speichern möchten.

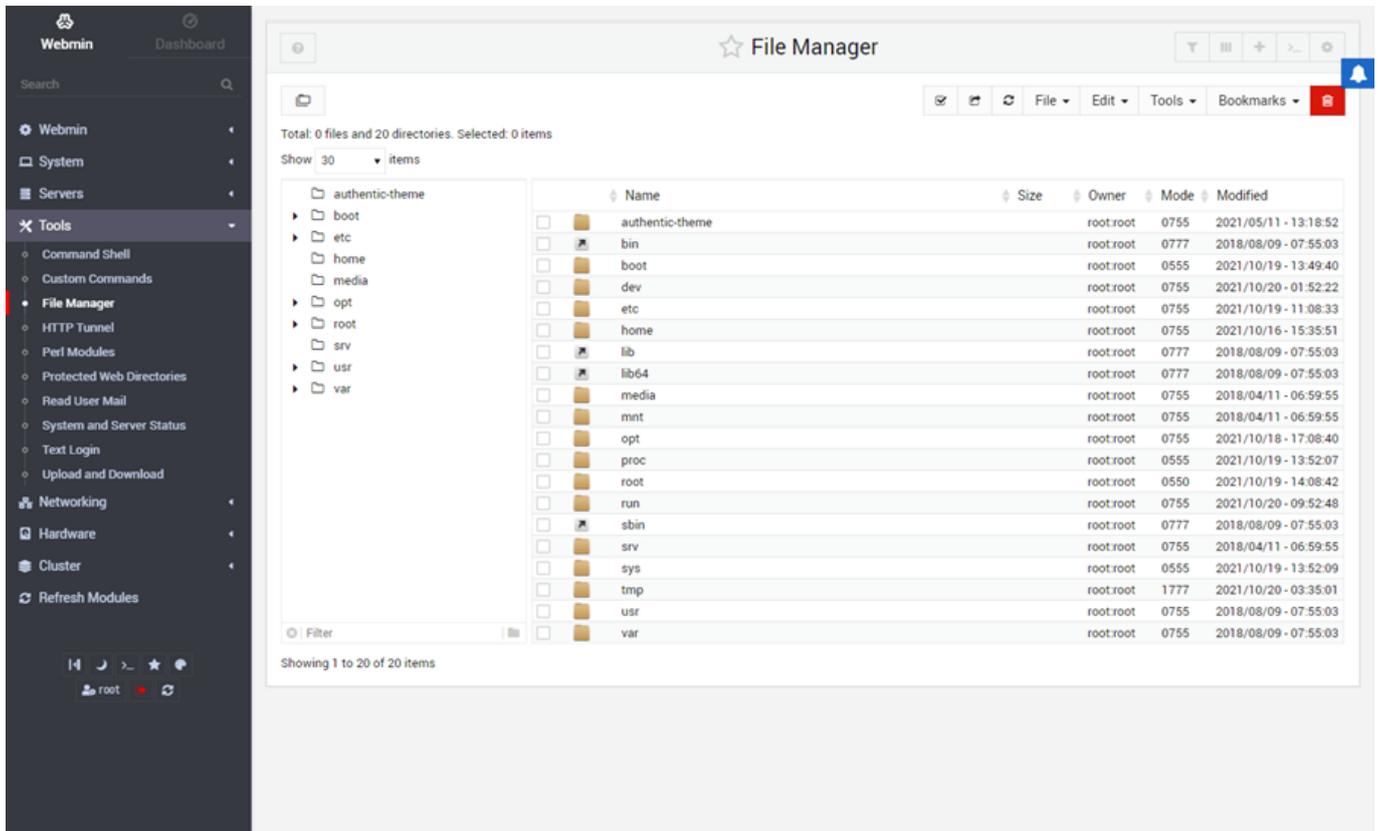


Tools

Diese Kategorie von Webmin enthält unterschiedliche Module. Es gibt zwei besonders nützliche Module:

[Dateimanager](#) – Mit diesem Modul können Sie Daten auf dem Server über eine HTML-Oberfläche anzeigen und bearbeiten. Wenn Sie den Dateimanager (auch bekannt als **Filemin**) zum ersten Mal laden, wird das Stammverzeichnis der ESET PROTECT-VA angezeigt, je nachdem, als welcher Benutzer Sie sich angemeldet haben.

- Navigieren Sie in der Verzeichnisstruktur, indem Sie auf den Verzeichnisnamen oder dessen Symbol (Ordner) klicken. Das aktuelle Verzeichnis wird oben links im Filemin-Fenster angezeigt. Klicken Sie auf einen beliebigen Teil des Pfads, um das entsprechende Verzeichnis anzuzeigen.
- Mit Filemin können Sie auch nach Dateien suchen. Klicken Sie auf **Tools** in der Symbolleiste (obere rechte Ecke des Filemin-Fensters) und wählen Sie **Suchen** aus. Geben Sie ein **Suchmuster**, nach dem Sie suchen möchten, in das Feld Suchabfrage ein.
- Klicken Sie auf einen Dateinamen bzw. auf ein Symbol, um eine Datei aus Ihrer ESET PROTECT-VA auf den Computer herunterzuladen, auf dem Ihr Webbrowser ausgeführt wird.
- Klicken Sie auf Datei und dann auf **In aktuelles Verzeichnis hochladen**, um eine Datei von dem Computer **hochzuladen**, auf dem Ihr Webbrowser ausgeführt wird. Daraufhin wird ein Dialogfeld geöffnet. Klicken Sie auf die Büroklammer, um die Dateien anzugeben, die Sie hochladen möchten. Wählen Sie eine oder mehrere Dateien aus und klicken Sie auf die Schaltfläche **Dateien hochladen**, um die Dateien hochzuladen. Die hochgeladenen Dateien werden in Ihrem aktuellen Verzeichnis abgelegt. Nach Ende des Uploads wird die Verzeichnisliste aktualisiert, und die hochgeladenen Dateien werden angezeigt.
- Sie können Dateien auch per Remote-URL abrufen. Klicken Sie dazu auf **Datei** und wählen Sie **Mit URL abrufen** aus.
- Klicken Sie auf das **Bearbeiten-Symbol** in der Spalte **Aktionen**, um die Inhalte beliebiger Dateien auf Ihrem System anzuzeigen und zu bearbeiten.
- Klicken Sie auf Datei, dann auf **Datei erstellen** und geben Sie den Namen der neuen Datei ein, um eine neue Datei zu **erstellen**.
- Klicken Sie auf das Umbenennen-Symbol im Rechtsklick-Kontextmenü, um eine Datei oder ein Verzeichnis umzubenennen.



[Upload und Download](#) – Ein weiteres nützliches Webmin-Modul in der Kategorie **Tools**. Mit diesem Modul können Sie drei verschiedene Dateiaktionen ausführen:

- **Internet-Download** – Geben Sie die URLs der Dateien ein, die Sie auf dem Internet auf Ihre ESET PROTECT-VA herunterladen möchten und geben Sie an, wo Sie die Dateien speichern möchten.
- **Auf Server hochladen** - Klicken Sie auf die Büroklammer, um die Dateien anzugeben, die Sie hochladen möchten. Sie können bis zu 4 Dateien gleichzeitig hochladen. Geben Sie an, wo Sie die Dateien speichern möchten.
- **Download von Server** – Geben Sie Pfad und Dateiname in das Textfeld **Herunterzuladende Datei** ein oder klicken Sie auf das Symbol neben dem Feld, um das ESET PROTECT-VA-Dateisystem nach der Datei zu durchsuchen, die Sie auf den Computer herunterladen möchten, auf dem Ihr Webbrowser ausgeführt wird. Klicken Sie auf die Schaltfläche **Herunterladen**, um die Datei herunterzuladen. Sie können nur eine Datei gleichzeitig herunterladen.

Netzwerk

Normalerweise müssen Sie die Netzwerkeinstellungen nicht ändern. Bei Bedarf finden Sie diese Einstellungen jedoch in der Kategorie **Netzwerk**. Dort können Sie bestimmte Module konfigurieren:

[Kerberos5-Konfiguration](#) - Die Kerberos-Tickets müssen für die AD-Synchronisierung korrekt konfiguriert sein. Sobald die Kerberos-Tickets konfiguriert sind, können Sie den Befehl [Domäne erneut beitreten](#) ausführen.

[Linux-Firewall](#) - Iptables-basierte Firewall. Hier können Sie Regeln hinzufügen oder bearbeiten, um Ports freizugeben.

[Netzwerkconfiguration](#) - Hier können Sie die Netzwerkkarte konfigurieren und IP-Adresse, Hostname sowie DNS-

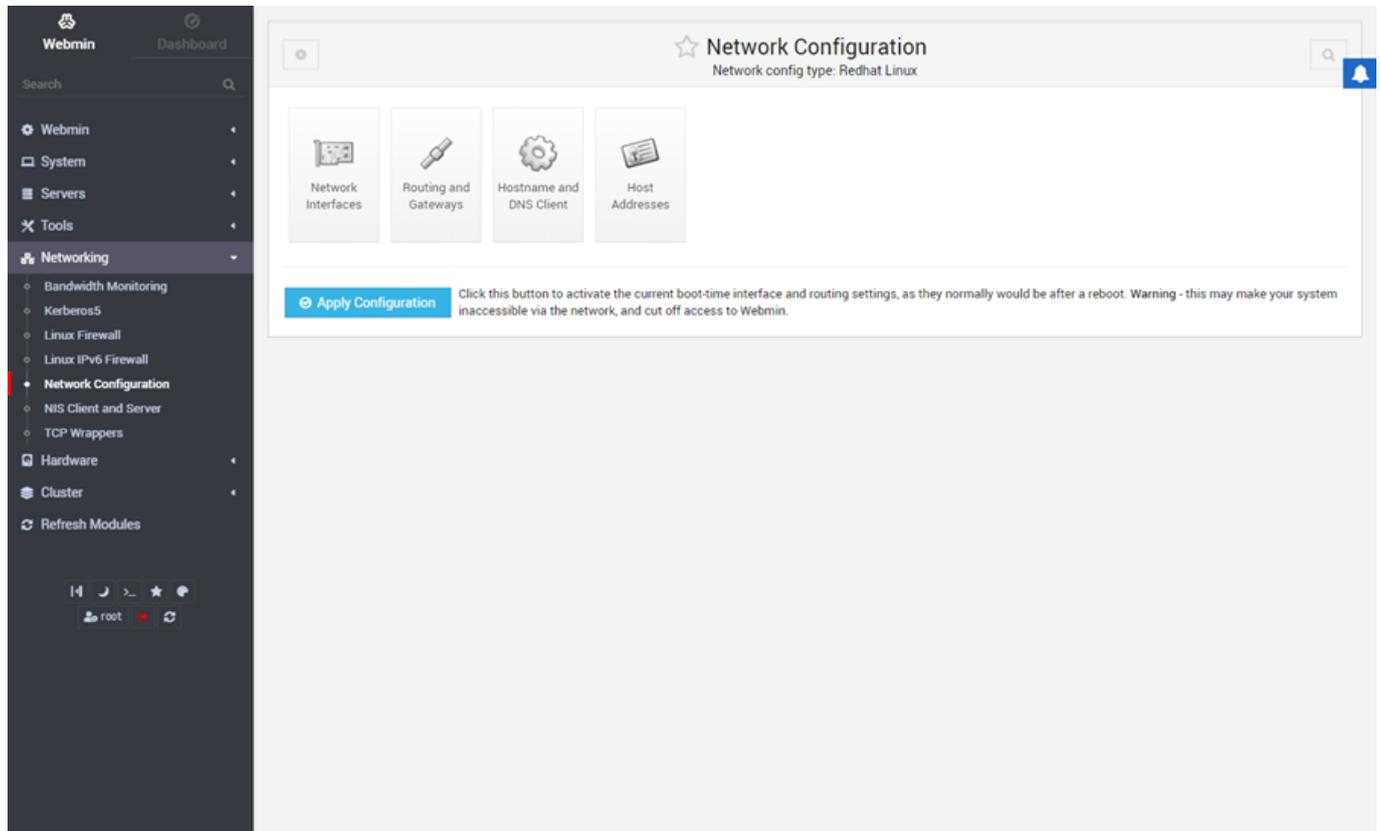
oder andere Netzwerkeinstellungen bearbeiten.



Bearbeiten Sie Ihre Konfiguration und klicken Sie anschließend auf **Konfiguration übernehmen**, um Ihre Änderungen zu übernehmen.



Dieses Modul sollte nur von erfahrenen Administratoren verwendet werden. Eine falsche Netzwerkkonfiguration kann dazu führen, dass Ihr System nicht mehr über das Netzwerk erreichbar ist und dass der Zugang zu Webmin unterbrochen wird. Sie haben jedoch weiterhin Zugriff auf die [ESET PROTECT-VA-Verwaltungskonsole](#) über das Terminalfenster des virtuellen Computers.



ESET PROTECT Zertifikate

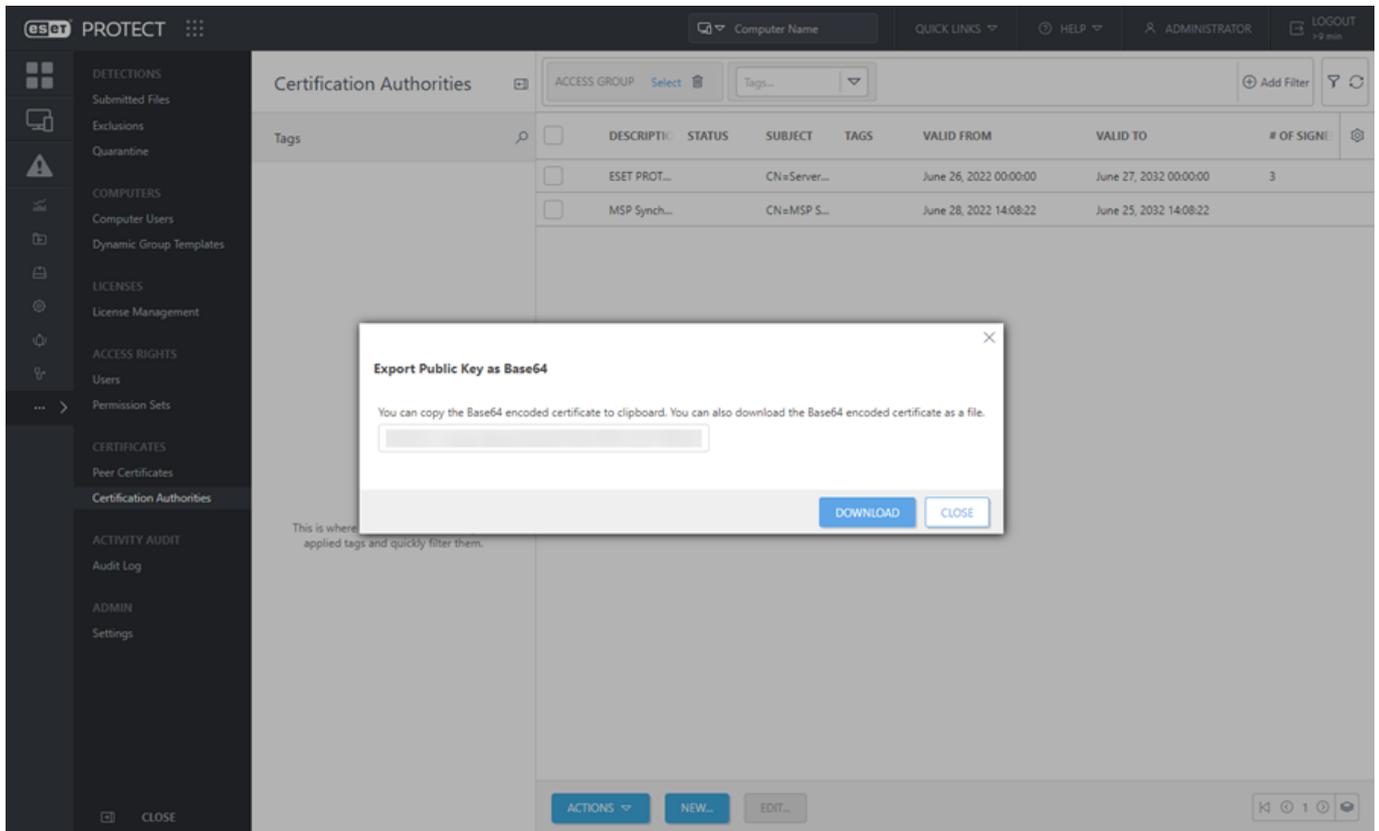
ESET PROTECT-[Zertifikate](#) werden benötigt, um die ESET PROTECT-MDM- und ESET PROTECT-Appliance-Typen bereitzustellen.

Die Zertifikate für ESET PROTECT-Komponenten sind in der Web-Konsole verfügbar.

So kopieren Sie den Inhalt eines Zertifikats im Base64-Format:

1. Klicken Sie auf **Mehr > Peerzertifikate**.
2. Wählen Sie ein Zertifikat aus und wählen Sie [Als Base64 exportieren](#) aus. Sie können das Base64-kodierte Zertifikat auch als Datei herunterladen.

Wiederholen Sie diesen Schritt für weitere Komponentenzertifikate und für Ihre [Zertifizierungsstelle](#).



i Benutzer benötigen **Ausführungsberechtigungen** für **Zertifikate**, um die Zertifikate exportieren zu können. Weitere Informationen finden Sie in der [vollständigen Liste der Zugriffsrechte](#).

Upgrade/Migration der ESET PROTECT-VA

Gehen Sie wie folgt vor, um Ihre VA zu aktualisieren oder zu migrieren:

- **Upgrade** - Installieren Sie eine neue Version der ESET PROTECT-Komponenten.
- **Migration** - Verschieben Sie die virtuelle ESET PROTECT-Appliance auf eine andere Instanz mit derselben Version.
- **Migration & Upgrade** - Verschieben Sie die virtuelle ESET PROTECT-Appliance auf eine andere Instanz mit einer höheren Version.

i Bei neuen Bereitstellungen der virtuellen ESET PROTECT-Appliance 8.1 und neueren Versionen ist die [erweiterte Sicherheit](#) standardmäßig aktiviert. Wenn Sie ESMC oder die virtuelle ESET PROTECT-Appliance 8.0 mit deaktivierter erweiterter Sicherheit verwenden und ein Upgrade auf die virtuelle ESET PROTECT-Appliance 8.1 oder eine neuere Version durchführen, ist die erweiterte Sicherheit weiterhin deaktiviert.

Vor der Aktualisierung/Migration

[Sichern Sie Ihre Datenbank](#) und [exportieren Sie Ihre Zertifizierungsstelle](#) und Ihre [Peerzertifikate](#) von Ihrer alten ESMC-/ESET PROTECT-VA, bevor Sie eine Migration oder ein Upgrades des ESET PROTECT Servers durchführen.

Vergleich: Datenbank-Pull und Komponenten-Upgrade

Sie können Ihre VA auf zwei verschiedene Arten aktualisieren:

- [Mit dem Datenbank-Pull](#) wird Ihre gesamte Appliance (das zugrunde liegende Betriebssystem) aktualisiert und nicht nur der ESET PROTECT Server. Diese Methode Prozess ist komplizierter und erfordert zwei parallele Appliances während der Übergangsphase. Wir empfehlen, den Datenbank-Pull für Upgrades auf Hauptversionen oder zur Fehlerbehebung zu verwenden.
- [Upgrade mit dem Task „Komponenten-Upgrade“ in der Web-Konsole](#) - Dieser Prozess ist einfacher und erfordert keinen Zugriff auf die Appliance, sondern nur auf die Web-Konsole. Wir empfehlen dieses Verfahren für kleinere Aktualisierungen und Hotfix-Upgrades.

Migrations- und Upgradeprozess (empfohlenes Upgradeverfahren)

Gehen Sie wie folgt vor, um Ihre ESET PROTECT-VA zu migrieren und zu aktualisieren.

1. [Laden](#) Sie die neueste *protect_appliance.ova* herunter (oder *protect_appliance.vhd.zip*, falls Sie Microsoft Hyper-V verwenden).
2. Stellen Sie die neue ESET PROTECT-VA bereit. Weitere Anweisungen finden Sie unter [Bereitstellungsprozess für die ESET PROTECT-Appliance](#). **Konfigurieren Sie die neue ESET PROTECT-VA noch nicht** über die Weboberfläche.
3. Führen Sie einen Datenbank-Pull von Ihrer alten VA aus. Eine komplette Anleitung finden Sie unter [Datenbank-Pull von einem anderen Server ausführen](#).

 Sie sollten Ihren alten VA Server noch nicht deinstallieren oder stilllegen.

4. [Konfigurieren Sie die virtuelle ESET PROTECT-Appliance](#) über die Weboberfläche.
5. Stellen Sie sicher, dass sich Ihre neue ESET PROTECT-VA gleich verhält wie die alte Instanz.

o Falls die neue ESET PROTECT-VA eine **andere IP-Adresse** hat:

- a) Erstellen Sie eine Policy auf Ihrer alten -VA, um [eine neue IP-Adresse für den ESET PROTECT Server festzulegen](#) und weisen Sie sie zu allen Computern zu.
- b) Warten Sie, bis die Policy auf alle ESET Management Agenten verteilt wurde.
- c) Vergewissern Sie sich, dass sich alle Computer mit der neuen ESET PROTECT-VA verbinden.
- d) Deaktivieren Sie die alte VA und nehmen Sie sie außer Betrieb.



Wir empfehlen dringend, den alten ESET PROTECT VA Server nicht mit einem Deinstallationskript zu deinstallieren. Bei dieser Deinstallation werden alle Lizenzen von der neuen ESET PROTECT VA Server-Datenbank ebenfalls getrennt (entfernt). Um dies zu verhindern, löschen Sie die alte ESET PROTECT VA Server-Datenbank (`DROP DATABASE`) vor der Deinstallation.

o Falls die neue ESET PROTECT-VA **dieselbe IP-Adresse** hat:



Stellen sie sicher, dass die Netzwerkkonfiguration auf Ihrem neuen ESET PROTECT Server (IP-Adresse, FQDN, Computername, DNS SRV-Eintrag) mit der Konfiguration Ihres alten VA Servers übereinstimmt. Sie können auch den Hostnamen verwenden, indem Sie den DNS-Eintrag ändern und auf den neuen Server verweisen.

- a) Deaktivieren Sie die alte VA.
- b) Aktivieren Sie die neue ESET PROTECT-VA.
- c) Vergewissern Sie sich, dass sich alle Computer mit der neuen ESET PROTECT-VA verbinden.
- d) Nehmen Sie die alte VA außer Betrieb.



Wir empfehlen dringend, den alten ESET PROTECT VA Server nicht mit einem Deinstallationskript zu deinstallieren. Bei dieser Deinstallation werden alle Lizenzen von der neuen ESET PROTECT VA Server-Datenbank ebenfalls getrennt (entfernt). Um dies zu verhindern, löschen Sie die alte ESET PROTECT VA Server-Datenbank (`DROP DATABASE`) vor der Deinstallation.

6. Aktualisieren Sie eine Testgruppe von ESET Management Agenten mit einem [ESET PROTECT Task „Komponenten-Upgrade“](#).

7. Wenn die Testgruppe erfolgreich aktualisiert wurde und sich die Agenten weiterhin verbinden, können Sie mit den restlichen Agenten fortfahren.

Upgradeprozess (alternatives Upgradeverfahren)



Wenn Sie ESMC oder ein älteres ESET PROTECT auf die neueste Version von ESET PROTECT auf derselben VA aktualisieren, wird die restliche VA-Software nicht aktualisiert (Betriebssystem und für den ordnungsgemäßen Betrieb des ESET PROTECT Servers erforderliche Pakete). Wir empfehlen, den Server nach einem reinen Upgrade zu migrieren.

Aktualisieren Sie die VA mit einem [Task „Komponenten-Upgrade“](#):

1. Aktualisieren Sie zunächst den ESET PROTECT Server.
2. Aktualisieren Sie eine Testgruppe von ESET Management Agenten.
3. Wenn die Testgruppe erfolgreich aktualisiert wurde und sich die Agenten weiterhin verbinden, können Sie mit den restlichen Agenten fortfahren.

ESET PROTECT -VA-Notfallwiederherstellung

Falls Ihre ESET PROTECT-VA defekt ist und nicht neu gestartet werden kann, oder falls sie aus dem Speicher gelöscht oder auf andere Weise zerstört wurde, können Sie eine Notfallwiederherstellung durchführen.



Für eine erfolgreiche Wiederherstellung benötigen Sie die [Datenbanksicherung](#) Ihrer ESET PROTECT-VA.

1. **Laden** Sie die neueste Version von `protect_appliance.ova`, oder `protect_appliance.vhd.zip` herunter, falls Sie Microsoft Hyper-V verwenden. Diese Wiederherstellungsprozedur hat den Vorteil, dass Ihre ESET PROTECT-VA dabei aktualisiert wird.

2. **Stellen Sie eine neue ESET PROTECT-VA** bereit, ohne diese jedoch zu konfigurieren. Weitere Anweisungen finden Sie unter [Bereitstellungsprozess für die ESET PROTECT-Appliance](#).
3. **Aktivieren Sie Webmin**, um die MySQL-Sicherungsdatei hochladen zu können. Weitere Details finden Sie im Abschnitt [Remotezugriff aktivieren/deaktivieren](#).
4. **Stellen Sie die Datenbank** mit Ihrer aktuellsten Sicherungsdatei wieder her. Führen Sie dazu die unter [Datenbank wiederherstellen](#) beschriebenen Schritte aus.
5. **Konfigurieren** Sie Ihre neu bereitgestellte ESET PROTECT-VA und die wiederhergestellte Datenbank auf dieselbe Weise wie Ihre VA. Details finden Sie unter [Konfiguration der ESET PROTECT-VA](#).

Fehlerbehebung

Die folgenden Protokolldateien helfen bei der Problembehandlung Ihrer virtuellen ESET PROTECT-Appliance. Außerdem werden Sie unter Umständen vom ESET-Support aufgefordert, Logdateien einzuschicken. Sie können die folgenden Dateien zur Analyse einschicken:

Protokollname	Standort	Beschreibung
Konfiguration der ESET PROTECT-VA	<i>/root/appliance-configuration-log.txt</i>	Falls bei der Bereitstellung Ihrer ESET PROTECT-VA ein Fehler auftritt, starten Sie die Appliance nicht neu. Überprüfen Sie die Log-Datei.
ESET PROTECT Server	<i>/var/log/eset/RemoteAdministrator/EraServerInstaller.log</i> <i>/var/log/eset/RogueDetectionSensor/RDSensorInstaller.log</i>	ESET PROTECT Server-Installations-Log Die restlichen ESET PROTECT-Komponenten verwenden ähnliche Pfade und entsprechende Dateinamen.
ESET PROTECT Server- Tracelog ESET Management Agent-Tracelog	<i>/var/log/eset/RemoteAdministrator/Server/</i> <i>/var/log/eset/RemoteAdministrator/Agent/</i>	Überprüfen Sie die Tracelogs: <i>trace.log</i> <i>status.html</i> <i>last-error.html</i> Die restlichen ESET PROTECT-Komponenten verwenden ähnliche Pfade und Dateinamen.
Apache HTTP-Proxy	<i>/opt/apache/logs/</i> <i>/var/log/httpd</i>	Protokolldatei für ältere Versionen der virtuellen ESET PROTECT-Appliance Protokolldatei für neuere Versionen der virtuellen ESET PROTECT-Appliance
ESET PROTECT Server- Absturzabbilder	<i>/var/opt/eset/RemoteAdministrator/Server/Dumps/</i>	

Protokollname	Standort	Beschreibung
ESET PROTECT Server- oder ESET Management Agent-Diagnose-Tool	<i>/root/RemoteAdministratorAgentDiagnostic.zip</i>	Wenn Probleme mit Ihrer ESET PROTECT-VA auftreten, können Sie das Diagnose-Tool ausführen . Weitere Details finden Sie im Abschnitt zum ESET PROTECT Webmin-Modul.

Wenn ein Server oder ein Agent abstürzt und Sie den Logging-Informationsumfang nicht in der Web-Konsole ändern können, erstellen Sie die folgende leere Datei, um das vollständige Ablaufverfolgungslog zu aktivieren:

Für den Agent:

```
touch /var/log/eset/RemoteAdministrator/Agent/traceAll
```

Für den Server:

```
touch /var/log/eset/RemoteAdministrator/Server/traceAll
```

i Mit dem [Webmin-Dateimanager](#) können Sie Dateien schnell und einfach suchen und Protokolle herunterladen.

Falls der Hinweis **EPNS-Dienstserver sind nicht erreichbar** angezeigt wird, finden Sie weitere Hinweise in den Schritten zur [Fehlerbehebung](#).

Häufig gestellte Fragen zur virtuellen ESET PROTECT-Appliance

In diesem Kapitel werden einige der häufigsten Fragen und Probleme behandelt. Klicken Sie auf die jeweilige Themenüberschrift, um Hilfestellung bei der Lösung Ihres Problems zu erhalten:

- [Wie finde ich heraus, welche ESET PROTECT-Komponenten installiert sind?](#)
- [Aktivieren der Ping-Funktion für die virtuelle ESET PROTECT-Appliance](#)
- [Muss ich weitere Komponenten zu meiner ESET PROTECT-VA hinzufügen?](#)
- [Wie kann ich den Apache HTTP-Proxy nach der Ausgangskonfiguration in meiner ESET PROTECT-VA aktivieren?](#)
- [Wie kann ich LDAP so konfigurieren, dass statische Gruppen auf der ESET PROTECT-VA synchronisiert werden?](#)
- [LDAPS-Verbindung zu einer Domäne konfigurieren](#)
- [Wie kann ich ein vergessenes Passwort für die ESET PROTECT-VA wiederherstellen?](#)
- [Wie kann ich die ESET PROTECT-Datenbankverbindungszeichenfolge ändern?](#)

- [Wie kann ich den Hyper-V Server für den RD Sensor einrichten?](#)
- [Wie kann ich die Portnummern für die virtuelle ESET PROTECT-Appliance ändern?](#)
- [Wie kann ich mehr Arbeitsspeicher für MySQL Server zuweisen?](#)
- [Beim Ausführen von ESET PROTECT auf Hyper-V Server 2012 R2 treten Probleme auf](#)
- [Wie kann ich die Leistung von Oracle VirtualBox verbessern?](#)
- [Wie kann ich den YUM-Befehl für den HTTP-Proxy aktivieren?](#)
- [Aktualisieren des Betriebssystems auf einem Computer, auf dem der ESET PROTECT VA Server ausgeführt wird](#)
- [SELinux permanent deaktivieren](#)
- [Neu starten der Verwaltungskonsole für die virtuelle Appliance](#)
- [Proxy für Agenten-Verbindungen verwenden](#)
- [Aktivieren von SSH](#)

Wenn Sie Ihr Problem nicht in der oben aufgeführten Liste der Hilfeseiten finden, suchen Sie es auf den ESET PROTECT-Hilfeseiten über ein [Schlagwort oder eine Formulierung](#) zu Ihrem Problem.

Wenn Sie die Lösung für Ihr Problem bzw. die Antwort auf Ihre Frage nicht auf den Hilfeseiten finden können, steht Ihnen auch unsere regelmäßig aktualisierte Online-[Knowledgebase](#) zur Verfügung.

Falls erforderlich, können Sie sich mit Ihren Fragen und Problemen auch direkt an die Online-Supportzentrale wenden. Sie finden das Kontaktformular in der ESET PROTECT-Web-Konsole unter **Hilfe > Support kontaktieren**.

Wie finde ich heraus, welche ESET PROTECT-Komponenten installiert sind?

Im Konsolenfenster der virtuellen ESET PROTECT-Appliance finden Sie eine Liste der installierten ESET PROTECT-Komponenten und ihrer Versionen. Starten Sie die VA neu, um diesen Dialog nach einem Komponentenupgrade zu aktualisieren. Alternativ können Sie den Verwaltungsmodus starten, den Befehl **Exit to terminal** auswählen und vom Terminal aus zum Sperrbildschirm wechseln.

```
ESET PROTECT Server Appliance
(C) 2021 ESET, spol. s r.o. - All rights reserved
```

```
Server version: [REDACTED]
Agent version: [REDACTED]
Rogue Detection Sensor version: [REDACTED]
```

```
ESET PROTECT Server hostname: protect.local
ESET PROTECT Server IP address: [REDACTED]
ESET PROTECT Server port: see configuration (default is 2222)
```

```
To open ESET PROTECT web console please use the following links:
https://protect.local
https://[REDACTED]
```

```
<ENTER> Enter management mode
```

Aktivieren der Ping-Funktion für die virtuelle ESET PROTECT-Appliance

Öffnen Sie ein Terminal und führen Sie die folgenden Befehle als root aus, um die Ping-Funktion auf einem Computer mit virtueller ESET PROTECT-Appliance zu aktivieren.

Vor dem Start sollten Sie mit dem Befehl `hostnamectl` überprüfen, welche Version von CentOS auf Ihrem System ausgeführt wird. Führen Sie anschließend die entsprechenden Befehle für Ihre Betriebssystemversion aus.

CentOS 7:

1. iptables-befehl aufrufen:

```
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
```

2. iptables speichern:

```
service iptables save
```

Jetzt können Sie einen Ping von anderen Computern im gleichen Subnetz an die virtuelle ESET PROTECT-Appliance senden.

Muss ich weitere Komponenten zu meiner ESET PROTECT-VA hinzufügen?

Nein. Die virtuelle ESET PROTECT-Appliance ist betriebsbereit. Sie müssen die Appliance lediglich [bereitstellen](#) und [konfigurieren](#). Dies ist die einfachste Methode, um ESET PROTECT bereitzustellen, falls Sie einen [unterstützten Hypervisor](#) verwenden.

Wie kann ich den Apache HTTP-Proxy nach der Ausgangskonfiguration in meiner ESET PROTECT-VA aktivieren?

Der Apache HTTP Proxy wird hauptsächlich verwendet, um Updates der Erkennungsroutine und Cachinginformationen aus ESET LiveGrid® zwischenspeichern. Öffnen Sie die Befehlszeile und führen Sie die entsprechenden Befehle für Ihre Betriebssystemversion Befehle als root aus, um den Apache HTTP-Proxy zu aktivieren:

- Der Speicherort von `apachectl` und `htcacheclean` hängt von Ihrem System ab. Vergewissern Sie sich, bevor Sie das Skript ausführen.
- Der Parameter `/var/cache/httpd/proxy` gibt den Ort des Cachingordners an. Dieser Speicherort wird in `/etc/httpd/conf.d/proxy.conf` unter `CacheRoot` festgelegt.

CentOS 7:

1. `systemctl enable httpd`
2. `sudo mkdir -p /etc/systemd/system/httpd.service.requires`
3. `sudo ln -s /usr/lib/systemd/system/htcacheclean.service /etc/systemd/system/httpd.service.requires`
4. `systemctl start httpd`
5. `htcacheclean -d60 -t -i -p/var/cache/httpd/proxy -l10000M`

- Sie können die Parameter für die Bereinigung des Apache HTTP-Proxy-Cache anpassen: `-d` definiert das Bereinigungsintervall in Minuten, `-p` gibt den Pfad für das Stammverzeichnis des Datenträgercache an, `-t` löscht alle leeren Verzeichnisse, `-i` führt eine intelligente Löschung des Cache durch, falls der Datenträgercache geändert wurde, `-l` definiert das Größenlimit für den Datenträgercache.

6. Port 3128 in einer Firewall aktivieren:
 - a) `iptables -A INPUT -p tcp --dport 3128 -j ACCEPT`
 - b) `ip6tables -A INPUT -p tcp --dport 3128 -j ACCEPT`

```
c)service iptables save
```

```
d)service ip6tables save
```

7. Sie müssen Policies für alle ESET-Produkte und ESET PROTECT-Komponenten erstellen, damit diese über den Apache HTTP-Proxy kommunizieren können, um die Zwischenspeicherung von Installationsdateien und Update-Dateien für ESET-Produkte zu ermöglichen. Stellen Sie sicher, dass die Apache-Konfiguration das [ProxyMatch-Segment](#) für Ihren Server-Host enthält. Weitere Informationen finden Sie in Teil II unseres [Knowledgebase-Artikels](#). **Konfigurieren der Policy-Einstellungen für Clientcomputer.**

Fehlerbehebung

Falls der Hinweis **EPNS-Dienstserver sind nicht erreichbar** angezeigt wird, führen Sie die folgenden Schritte aus, um die Zeitüberschreitungslimits für die Verbindung zu deaktivieren:

1. Erstellen Sie die Konfigurationsdatei *reqtimeout.conf*:

```
sudo touch /etc/httpd/conf.d/reqtimeout.conf
```

2. Öffnen Sie die Datei in einem Text-Editor:

```
nano /etc/httpd/conf.d/reqtimeout.conf
```

3. Fügen Sie die folgende Einstellung in die Datei ein:

```
RequestReadTimeout header=0 body=0
```

4. Speichern Sie die Änderungen und schließen Sie die Datei:
Strg+X > Y drücken > **Enter** drücken

5. Öffnen Sie die Datei *httpd.conf*:

```
nano /etc/httpd/conf/httpd.conf
```

6. Fügen Sie am Ende die folgende Zeile hinzu:

```
IncludeOptional conf.d/reqtimeout.conf
```

7. Speichern Sie die Änderungen und schließen Sie die Datei:
Strg+X > Y drücken > **Enter** drücken

8. Starten Sie den Apache HTTP Proxy-Dienst neu:

```
systemctl restart httpd
```

Wie kann ich LDAP so konfigurieren, dass statische Gruppen auf der ESET PROTECT-VA synchronisiert werden?

Wenn beim Beitreten zur Domäne ein Fehler auftritt, liegt dies normalerweise an einer fehlerhaften Konfiguration der ESET PROTECT-VA. Weitere Informationen finden Sie in unserem [Knowledgebase-Artikel](#).

LDAPS-Verbindung zu einer Domäne konfigurieren

ESET PROTECT Server unter Windows verwendet standardmäßig das verschlüsselte LDAPS-Protokoll (LDAP over SSL) für sämtliche Active Directory-Verbindungen.

Führen Sie die folgenden Schritte aus, um die virtuelle ESET PROTECT-Appliance für die LDAPS-Verbindung mit Active Directory zu konfigurieren.

Voraussetzungen

- [LDAPS auf dem Domänencontroller einrichten](#) - Stellen Sie sicher, dass Sie den öffentlichen Schlüssel der DC-Zertifizierungsstelle exportieren.
- Stellen Sie sicher, dass [Kerberos](#) auf Ihrer ESET PROTECT-VA korrekt konfiguriert ist.

Aktivieren Sie LDAPS auf der ESET PROTECT-VA.

1. Öffnen Sie ein Terminal der virtuellen Maschine, auf der die ESET PROTECT-VA ausgeführt wird.
2. Geben Sie Ihr Passwort ein, das Sie bei der [Konfiguration der ESET PROTECT-VA](#) eingerichtet haben, und drücken Sie zweimal die **Eingabetaste**.
3. Wählen Sie **Zurück zum Terminal** aus und drücken Sie die **Eingabetaste**.
4. Halten Sie den ESET PROTECT Server-Dienst an.

```
systemctl stop eraserver
```

5. Geben Sie den folgenden Befehl aus:

```
nano /etc/systemd/system/eraserver.service
```

6. Fügen Sie die folgende Zeile zum Abschnitt **[Service]** hinzu:

```
Environment="ESMC_ENABLE_LDAPS=1"
```

7. Drücken Sie **Strg+X** und dann **Y**, um die Dateiänderungen zu speichern. Drücken Sie die **Eingabetaste**, um den Editor zu verlassen.

8. Führen Sie den folgenden Befehl aus, um die Konfiguration neu zu laden:

```
systemctl daemon-reload
```

9. Starten Sie den ESET PROTECT Server-Dienst an.

```
systemctl start eraserver
```

10. Kopieren Sie die auf dem Domänencontroller generierte Zertifikatdatei an den folgenden Speicherort auf Ihrem ESET PROTECT VA Server:

```
/etc/pki/ca-trust/source/anchors/
```

11. Führen Sie den folgenden Befehl aus:

```
update-ca-trust
```

Wiederherstellen eines vergessenen Passworts für die ESET PROTECT-VA

Starten Sie Ihre ESET PROTECT-VA im Einzelbenutzermodus. Anweisungen finden Sie in der [CentOS 7-Dokumentation](#). Wenn Sie die Befehlszeile im Einzelbenutzermodus gestartet haben, können Sie Ihr root-Passwort mit dem Befehl `passwd`.

Falls die Nachricht „`passwd: Authentication token manipulation error`“ angezeigt wird, führen Sie [diese Fehlerbehebungsschritte aus](#).

Wie kann ich die ESET PROTECT-Datenbankverbindungszeichenfolge ändern?

Sie können die Verbindungszeichenfolge für die ESET PROTECT-Datenbank in Ihrer ESET PROTECT-VA ändern, indem Sie die Datei `StartupConfiguration.ini` bearbeiten.

Führen Sie die folgenden Anweisungen aus, um die Verbindungszeichenfolge für die ESET PROTECT-Datenbank zu ändern:

1. Starten Sie den **Verwaltungsmodus**, indem Sie Ihr Passwort eingeben und zweimal die **Eingabetaste** drücken. Wählen Sie den Befehl **Exit to terminal** mit den Pfeiltasten aus und drücken Sie die **Eingabetaste**.

2. Typ:

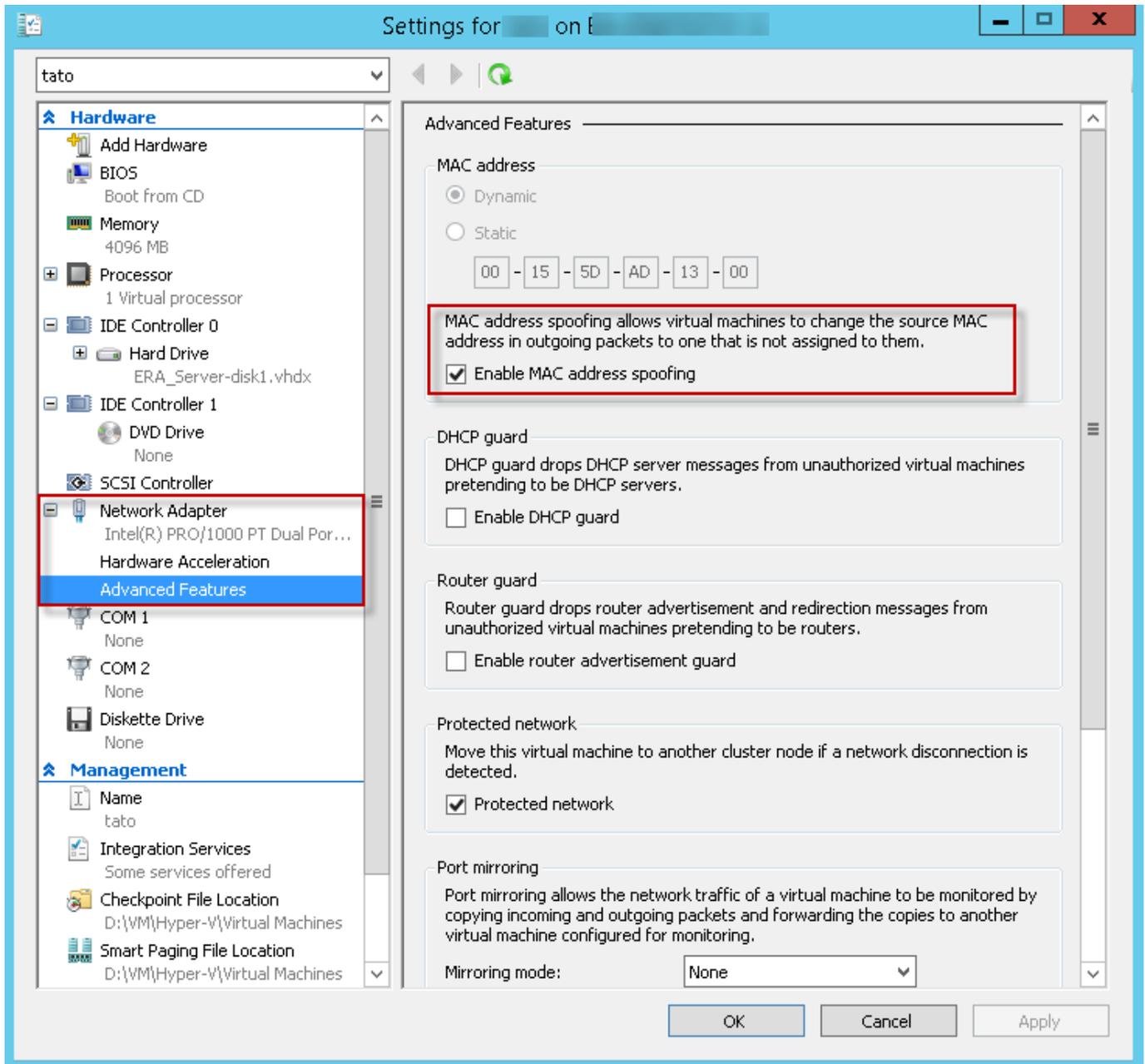
```
nano /etc/opt/eset/RemoteAdministrator/Server/StartupConfiguration.ini
```

3. Bearbeiten Sie die Daten in der Verbindungszeichenfolge für die ESET PROTECT-Datenbank.

4. Drücken Sie `Ctrl+X` und `y`, um die Änderungen zu speichern.

Wie kann ich den Hyper-V Server für den RD Sensor einrichten?

Stellen Sie sicher, dass die Option MAC-Adressen-Spoofing in den Einstellungen Ihres Hyper-V-Managers aktiviert ist (siehe unten).



Wie kann ich die Portnummern für die virtuelle ESET PROTECT-Appliance ändern?

Nehmen Sie die folgenden Änderungen an den entsprechenden ESET PROTECT-Komponenten vor, um Portnummern zu ändern:

Port der ESET PROTECT-Web-Konsole (Standard: 8443)

1. Öffnen Sie [Webmin](#).
2. Navigieren Sie zu **Server > ESET PROTECT** und klicken Sie auf **Edit Apache Tomcat server.xml**.
3. Fügen Sie den benutzerdefinierten Port in die Zeile `<Connector port="8443"` ein und klicken Sie auf **Speichern und schließen**.

4. Öffnen Sie die Datei *EraWebServerConfig.properties*:

```
sudo nano /var/lib/tomcat/webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties
```

5. Fügen Sie den benutzerdefinierten Port in die Zeile `server_port=` ein und speichern Sie die Änderungen.

6. Starten Sie den Tomcat-Dienst neu: `systemctl restart tomcat`

ESET PROTECT Server-Ports (Standard: 2222, 2223) - Melden Sie sich bei der [ESET PROTECT Web-Konsole](#) an, navigieren Sie zu **Mehr > Einstellungen > Verbindung** und nehmen Sie die gewünschten Änderungen vor.



Wenn Sie einen der genannten Ports ändern, müssen Sie die Firewall-Einstellungen ebenfalls anpassen. Öffnen Sie [Webmin](#), navigieren Sie zu **Netzwerk > Linux-Firewall** und ändern Sie die Portnummern in den vorhandenen Regeln. Alternativ können Sie neue Regeln hinzufügen.

Wie kann ich mehr Arbeitsspeicher für MySQL Server zuweisen?

Führen Sie diese Schritte aus, um den zugewiesenen Speicher für einen MySQL Server zu vergrößern:

1. Starten Sie den **Verwaltungsmodus**, indem Sie Ihr Passwort eingeben und zweimal die Eingabetaste drücken. Wählen Sie mit den **Pfeiltasten** den Befehl Zurück zum Terminal aus und drücken Sie die **Eingabetaste**.

2. Typ:

```
nano /etc/my.cnf
```

3. Suchen Sie die Zeile `innodb_buffer_pool_size = 1024M` und ändern Sie den Wert zu 50% des Arbeitsspeichers der VM. `1024M` bedeutet 1024 Megabyte.

4. Drücken Sie `Strg+X`, um den Text-Editor zu verlassen, und anschließend `Y` zum Speichern.

5. Starten Sie die Appliance mit der Option **System neu starten** im **Verwaltungsmodus** neu.

Beim Ausführen von ESET PROTECT auf Hyper-V Server 2012 R2 treten Probleme auf

Nach dem Anmelden bei der ESET PROTECT Web-Konsole wird die Fehlermeldung "Unable to handle Kernel NULL pointer dereference at (null)" angezeigt.

Deaktivieren Sie den dynamischen Arbeitsspeicher in den Einstellungen des virtuellen Computers, um dieses Problem zu beheben.

Wie kann ich die Leistung von Oracle VirtualBox verbessern?

Sie können die Anzahl der Prozessoren (CPU-Kerne) in den **Einstellungen** der virtuellen ESET PROTECT-Appliance ändern. Öffnen Sie dazu die Registerkarte **System > Prozessor**. Reduzieren Sie die Anzahl der Prozessoren für die VA. Beispiel: Wenn Sie 4 physische CPUs haben, reduzieren Sie die Anzahl der Prozessoren für die VA auf 2.

So aktivieren Sie den YUM-Befehl für den HTTP-Proxyserver

Wenn Ihr lokales Netzwerk einen Proxyserver als Zwischenstelle für den Internetzugriff verwendet, ist der Befehl `yum` möglicherweise nicht korrekt konfiguriert und funktioniert nicht.

So konfigurieren Sie `yum` für den Einsatz mit einem Proxy:

1. Starten Sie den Verwaltungsmodus, indem Sie Ihr Passwort eingeben und zweimal die **Eingabetaste** drücken. Wählen Sie mit den **Pfeiltasten** den Befehl Zurück zum Terminal aus und drücken Sie die **Eingabetaste**.

2. Typ:

```
nano /etc/yum.conf
```

3. Fügen Sie eine Zeile mit Informationen zu Ihrem Proxy hinzu. Beispiel:

```
proxy=http://proxysvr.yourdom.com:3128
```

4. Fügen Sie ggf. Benutzernamen und Passwort für den Proxy hinzu. Beispiel:

```
proxy=http://proxysvr.yourdom.com:3128
```

```
proxy_username=YourProxyUsername
```

```
proxy_password=YourProxyPassword
```

5. Drücken Sie `Strg+X` und `y`, um die Änderungen zu speichern.



Die Datei `/etc/yum.conf` muss für alle Benutzer lesbar sein, um den Befehl `yum` verwenden zu können. Dies bedeutet, dass andere Benutzer Ihr Proxy-Passwort lesen können. Verwenden Sie dieses Passwort daher nicht für andere Dienste.

Weitere Informationen finden Sie in der [Dokumentation](#) des Anbieters.

Aktualisieren des Betriebssystems auf einem Computer, auf dem der ESET PROTECT VA Server ausgeführt wird

Falls in der ESET PROTECT-Web-Konsole eine Meldung angezeigt wird, dass das ESET PROTECT VA Server-Betriebssystem **nicht auf dem neuesten Stand ist**, müssen Sie das Betriebssystem auf dem ESET PROTECT VA Server aktualisieren. Führen Sie den Task [Betriebssystem-Update](#) in der ESET PROTECT-Web-Konsole aus. Nach

Abschluss des Updates wird die Warnmeldung nicht mehr angezeigt.



Wenn Sie das Betriebssystem-Update über die Webmin-Oberfläche, im Terminal oder mit einem externen Tool ausführen, wird die Warnmeldung weiterhin angezeigt, auch nachdem das Betriebssystem aktualisiert wurde. Führen Sie in diesem Fall den Task **Betriebssystem-Update** in der ESET PROTECT-Web-Konsole aus.

SELinux permanent deaktivieren

SELinux ist in der virtuellen Appliance standardmäßig aktiviert. Gehen Sie wie folgt vor, um diese Komponente permanent zu deaktivieren:

1. Wählen Sie **Exit to Terminal** in der [Verwaltungskonsole für die virtuelle Appliance](#) aus.
2. Führen Sie den folgenden Befehl aus:
`nano /etc/selinux/config`
3. Ändern Sie die folgende Zeile:
`SELINUX=permissive`
bis
`SELINUX=disabled`
4. Speichern Sie die Änderungen und verlassen Sie den Editor.
5. Führen Sie den folgenden Befehl aus, um den Computer neu zu starten und die neue Einstellung zu übernehmen.
`reboot`

Neu starten der Verwaltungskonsole für die virtuelle Appliance

Sie können die grafische Benutzeroberfläche der virtuellen Appliance neu starten, ohne den virtuellen Computer neu zu starten. Dabei werden sämtliche Daten in der Konsole aktualisiert. (Zum Beispiel wenn eine geänderte Einstellung in der Verwaltungskonsole für die virtuelle Appliance nicht übernommen wird.)

1. Wählen Sie **Exit to Terminal** in der [Verwaltungskonsole für die virtuelle Appliance](#) aus.
2. Führen Sie den folgenden Befehl aus:
`./appliance-gui restart`

Proxy für Agenten-Verbindungen verwenden

Proxy zum Weiterleiten von ESET Management Agenten verwenden - ESET PROTECT Server-Verbindungen in ESET PROTECT können über einen Apache HTTP Proxy hergestellt werden. Folgen Sie den [Linux-Anweisungen](#), um Apache HTTP Proxy zu installieren.

Aktivieren von SSH

Informationen zur SSH-Aktivierung für die ESET PROTECT-VA (bzw. die ESMC-VA) finden Sie unter [Remotezugriff aktivieren/deaktivieren](#).

SSH-Fehlerbehebung

Öffnen Sie das Terminal führen Sie die folgenden Befehle aus:

- `sudo systemctl status sshd` – Überprüfen, ob SSH ausgeführt wird. Falls SSH nicht ausgeführt wird, starten Sie den Dienst: `sudo systemctl start sshd`
- `sudo iptables -S` – Wenn Port 22 offen ist, wird die folgende Zeile angezeigt: `-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT`. Führen Sie den folgenden Befehl aus, um Port 22 zu iptables hinzuzufügen: `sudo iptables -A INPUT -p tcp -m tcp --dport 22 -j ACCEPT`

Endbenutzer-Lizenzvereinbarung

Gültig ab dem 19. Oktober 2021.

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 ERKENNEN DIE [DATENSCHUTZERKLÄRUNG AN](#).**

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, ("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 und akzeptieren die Datenschutzerklärung. Wenn Sie mit einer der Bestimmungen dieser Vereinbarung und/oder der Datenschutzerklärung nicht einverstanden sind, klicken Sie auf die Schaltfläche „Ablehnen“ oder „Ich stimme nicht zu“. Brechen Sie den Download oder die Installation der Software ab, vernichten oder geben Sie die Software, das Installationsmedium, die zugehörige Dokumentation und den Erwerbsnachweis an den Anbieter oder an dem Ort, an dem Sie die Software erworben haben, zurück.

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

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

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

3. Lizenz. Unter der Voraussetzung, dass Sie sich mit dieser Vereinbarung einverstanden erklärt 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; oder (ii) wenn sich der Umfang einer Lizenz nach der Anzahl von Postfächern richtet, ist ein Endbenutzer ein Computerbenutzer, der E-Mails 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) **Home/Business Edition.** Die Home Edition der Software darf ausschließlich in privaten und/oder nichtkommerziellen Umgebungen für den Haus- und Familiengebrauch eingesetzt werden. Für die Verwendung der Software in kommerziellen Umgebungen sowie 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.** Als „OEM“ klassifizierte Software darf ausschließlich auf dem Computer genutzt werden, mit dem sie ausgeliefert wurde. 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. Eine Internetverbindung und die entsprechende Datenerfassung ist für den Betrieb der Software sowie für deren Updates und Upgrades erforderlich. Der Anbieter hat das Recht, Aktualisierungen für die Software („Updates“) oder Upgrades bereitzustellen, ist dazu 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 Datenschutzerklärung.

Die Bereitstellung von Updates unterliegt möglicherweise der End-of-Life-Richtlinie („EOL-Richtlinie“), die auf https://go.eset.com/eol_business verfügbar ist. Nachdem die Software oder eine ihrer Funktionen das in der EOL-Policy festgelegte End-of-Life-Datum erreicht hat, werden keine Aktualisierungen mehr bereitgestellt.

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.

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

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

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

a) Sie dürfen eine Kopie der Software auf einem Medium zur dauerhaften Speicherung als Sicherungskopie erstellen, vorausgesetzt die Sicherungskopien werden nicht auf einem anderen Computer installiert oder verwendet. Das Erstellen jeder weiteren Kopie der Software verstößt gegen diese Vereinbarung.

b) Jegliche von den Bestimmungen dieser Vereinbarung abweichende Nutzung, Modifikation, Übersetzung oder Reproduktion der Software sowie die Einräumung von Rechten zur Nutzung der Software oder von Kopien der Software ist untersagt.

c) Die Software darf nicht an andere Personen verkauft, sublizenziert oder vermietet werden. Ebenso darf die Software nicht von einer anderen Person gemietet, einer anderen Person ausgeliehen oder zur gewerbsmäßigen Erbringung von Dienstleistungen verwendet werden.

d) Der Quellcode der Software darf nicht durch Reverse-Engineering analysiert, dekompiert oder disassembliert oder auf andere Weise beschafft werden, soweit eine solche Beschränkung nicht ausdrücklich gesetzlichen Bestimmungen widerspricht.

e) Sie verpflichten sich, die Software nur in Übereinstimmung mit allen am Verwendungsort geltenden gesetzlichen Bestimmungen zu verwenden, insbesondere gemäß den Beschränkungen, die sich aus dem Urheberrecht und anderen Rechten an geistigem Eigentum ergeben.

f) Sie verpflichten sich, die Software und ihre Funktionen nur so zu nutzen, dass der Zugriff anderer Endbenutzer auf die betreffenden Dienste nicht eingeschränkt wird. Der Anbieter behält sich das Recht vor, den Leistungsumfang gegenüber einzelnen Endbenutzern einzuschränken, damit die Dienste von möglichst vielen Endbenutzern verwendet werden können. Dies kann auch bedeuten, dass die Nutzung beliebiger Softwarefunktionen vollständig gesperrt wird und dass Daten sowie Informationen im Zusammenhang mit bestimmten Funktionen der Software von den Servern des Anbieters bzw. Dritter gelöscht werden.

g) Sie verpflichten sich hiermit, keine Aktivitäten im Zusammenhang mit dem Lizenzschlüssel auszuführen, die den Bestimmungen dieser Vereinbarung widersprechen oder die dazu führen, dass der Lizenzschlüssel an unbefugte Personen weitergegeben wird, z. B. durch die Übertragung von benutzten oder nicht benutzten Lizenzschlüsseln in jeglicher Form oder die nicht autorisierte Verteilung von duplizierten oder generierten Lizenzschlüsseln oder die Nutzung der Software im Zusammenhang mit einem Lizenzschlüssel, der aus einer anderen Quelle als direkt vom Anbieter beschafft wurde.

7. Urheberrecht. Die Software und alle Rechte einschließlich des Rechtstitels und der geistigen Eigentumsrechte daran sind Eigentum von ESET und/oder seiner Lizenzgeber. Sie unterliegen dem Schutz der Bestimmungen internationaler Abkommen und aller sonstigen geltenden Gesetze des Landes, in dem die Software verwendet wird. Die Struktur, die Aufteilung und der Code der Software sind Geschäftsgeheimnisse und vertrauliche Informationen von ESET und/oder seiner Lizenzgeber. Die Software darf nicht kopiert werden, wobei lediglich die in Abschnitt 6(a) angegebene Ausnahme gilt. Alle gemäß dieser Vereinbarung zulässigen Kopien müssen dieselben Urheberrechts- und Eigentümerhinweise wie die ursprüngliche Software enthalten. Wenn Sie in Verstoß gegen

die Bestimmungen dieser Vereinbarung Quellcode durch Reverse-Engineering analysieren, dekompileieren oder disassemblieren oder versuchen, sich den Quellcode auf andere Weise zu beschaffen, gehen automatisch sämtliche dadurch gewonnenen Informationen unwiderruflich und unmittelbar in das Eigentum des Anbieters über. Weiterhin ist der Anbieter in diesem Fall berechtigt, etwaige weitere Ansprüche aus Ihrem Verstoß gegen diese Vereinbarung geltend zu machen.

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

9. Versionen in verschiedenen Sprachen/auf mehreren Datenträgern, mehrere Exemplare. Wenn die Software mehrere Plattformen oder Sprachen unterstützt, oder wenn Sie mehrere Exemplare der Software erhalten haben, darf die Software nur auf derjenigen Anzahl von Computern und nur in den Versionen verwendet werden, für die Sie eine Lizenz erworben haben. Es dürfen keine Versionen oder Kopien der Software, die von Ihnen nicht verwendet werden, an andere Personen verkauft, vermietet, sublizenziert, verliehen oder auf diese übertragen werden.

10. Beginn und Gültigkeitsdauer der Vereinbarung. Diese Vereinbarung tritt an dem Tag in Kraft, an dem Sie sich mit ihren Bestimmungen einverstanden erklären. Sie können diese Vereinbarung jederzeit kündigen, indem Sie die Software, alle Sicherungskopien und, falls vorhanden, alle vom Anbieter oder seinen Geschäftspartnern zur Verfügung gestellten zugehörigen Materialien dauerhaft löschen, sie zerstören bzw. auf eigene Kosten zurückgeben. Ihr Recht zur Nutzung der Software und deren Funktionen unterliegt möglicherweise einer EOL-Richtlinie. Wenn die Software oder deren Funktionen das in der EOL-Richtlinie definierte Ende des Lebenszyklus erreichen, erlischt Ihr Nutzungsrecht für die Software. 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. HAFTUNGS AUSSCHLUSS. 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 INSTALLATION, NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DER SOFTWARE ENTSTEHEN. DA IN BESTIMMTEN LÄNDERN UND UNTER BESTIMMTEN GESETZEN EIN HAFTUNGS AUSSCHLUSS 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. Nachdem die Software oder eine ihrer Funktionen das in der EOL-Policy festgelegte End-of-Life-Datum erreicht hat, wird kein technischer Support mehr bereitgestellt. 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 („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

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.

(die in den Punkten i und ii genannten Gesetze zusammengefasst als „Handelskontrollgesetze“).

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. ESET behält sich das Recht vor, Sie über alle Änderungen an dieser Vereinbarung, der Datenschutzerklärung, der EOL-Richtlinie und der Dokumentation gemäß Art. 22 der Vereinbarung zu informieren. ESET kann Ihnen E-Mails oder In-App-Benachrichtigungen über die Software schicken oder die Kommunikation auf unserer Website veröffentlichen. Sie stimmen zu, rechtliche Mitteilungen von ESET in elektronischer Form zu erhalten, inklusive Mitteilungen zu Änderungen an Bedingungen, Sonderbedingungen oder Datenschutzerklärungen, Benachrichtigungen oder Einladungen zu Vertragsverlängerungen, Kündigungen oder andere rechtliche Mitteilungen. Diese elektronische Kommunikation gilt als schriftlich empfangen, sofern nicht durch geltendes Recht eine andere Kommunikationsform vorgeschrieben ist.

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. Diese Vereinbarung wird auf Englisch getroffen. Falls eine Übersetzung der Vereinbarung aus Gründen der Annehmlichkeit bereitgestellt wird, sind die Bestimmungen der englischen Version maßgeblich, falls Abweichungen bestehen.

ESET behält sich das Recht vor, Änderungen an der Software vorzunehmen und die Bestimmungen dieser Vereinbarung, deren Anhänge und Ergänzungen, die Datenschutzerklärung, die EOL-Richtlinie und die

Dokumentation ganz oder in Teilen jederzeit zu ändern, indem das entsprechende Dokument aktualisiert wird, (i) um Änderungen an der Software oder der Funktionsweise von ESET zu berücksichtigen, (ii) aus rechtlichen, regulatorischen oder Sicherheitsgründen oder (iii) um Missbrauch oder Schaden zu verhindern. Bei Änderungen an dieser Vereinbarung werden Sie per E-Mail, per In-App-Benachrichtigung oder über andere elektronische Kommunikationsformen informiert. Wenn Sie den Änderungen der Vereinbarung nicht zustimmen, können Sie diese gemäß Artikel 10 innerhalb von 30 Tagen nach Erhalt der Änderungsbenachrichtigung kündigen. Sofern Sie die Vereinbarung nicht innerhalb dieser Frist kündigen, gelten die Änderungen als von Ihnen akzeptiert und wirksam ab dem Tag, an dem Sie die Änderungsbenachrichtigung erhalten haben.

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.

ANHANG ZUR VEREINBARUNG

Weiterleitung von Informationen an den Anbieter. Zur Weiterleitung von Informationen an den Anbieter gelten die folgenden zusätzlichen Bestimmungen:

Die Software enthält Funktionen zur Erfassung von Informationen über den Installationsprozess, den Computer und/oder die Plattform, auf der die Software installiert ist, anderen Informationen über Betrieb und Funktionsweise der Software sowie Informationen zu verwalteten Geräten (im Folgenden "Informationen"). Diese Daten werden anschließend an den Anbieter übertragen. Diese Informationen können Daten (inklusive zufällig oder versehentlich erfasster persönlicher Daten) zu den verwalteten Geräten enthalten. Wenn diese Softwarefunktion aktiviert wird, darf der Anbieter gemäß der Datenschutzerklärung und gemäß geltender Gesetze Informationen erfassen und verarbeiten.

Die Software setzt voraus, dass auf dem verwalteten Computer eine Komponente installiert wird, um die Informationen zwischen dem verwalteten Computer und der Remoteverwaltungssoftware übertragen zu können. Zu den übertragenen Informationen gehören Verwaltungsdaten wie Hardware- und Softwareinformationen der verwalteten Computer, sowie Verwaltungsanweisungen von der Remoteverwaltungssoftware. Alle sonstigen vom verwalteten Computer übertragenen Daten werden durch die Einstellungen der auf dem verwalteten Computer installierten Software bestimmt. Der Inhalt der Anweisungen von der Remoteverwaltungssoftware wird durch die Einstellungen der Remoteverwaltungssoftware bestimmt.

EULAID: EULA-PRODUCT-PROTECT; 3537.0

Datenschutzerklärung

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

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

Verarbeitung persönlicher Daten

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

- Für die Verwaltung der ESET-Sicherheitsprodukte werden Informationen gesammelt und lokal gespeichert, wie etwa ID und Name des Lizenzplatzes, Produktname, Lizenzinformationen, Aktivierungs- und Ablaufinformationen, Hardware- und Softwareinformationen über den verwalteten Computer, auf dem das ESET-Sicherheitsprodukt installiert wurde. Logs zu den Aktivitäten der verwalteten ESET-Sicherheitsprodukte und Geräte werden erfasst und sind verfügbar für verschiedene Funktionen und Dienste zur Verwaltung und Überwachung. Diese Logs werden nicht automatisch an ESET übertragen.
- Informationen zum Installationsprozess, inklusive der Plattform, auf der unser Produkt installiert wird sowie Informationen zum Betrieb und zur Funktionsweise unserer Produkte, wie etwa Hardwarefingerabdrücke, Installations-IDs, Absturzabbilder, Lizenz-IDs, IP-Adressen, MAC-Adressen und Konfigurationseinstellungen des Produkts, wozu auch verwaltete Geräte gehören können.
- 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. Auf Basis des von Ihnen gewählten Kontaktkanals erfassen wir unter Umständen Ihre E-Mail-Adresse, Telefonnummer, Lizenzinformationen, Produktdetails und eine Beschreibung Ihres Supportfalls. Möglicherweise werden Sie aufgefordert, uns weitere Informationen wie generierte Log-Dateien bereitzustellen, um die Bearbeitung der Supportanfrage zu erleichtern.
- Die Daten zur Nutzung unserer Dienste werden zum Ende der Sitzung vollständig anonymisiert. Nach dem Ende der Sitzung werden keinerlei personenbezogene Daten gespeichert.

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