

ESET PROTECT Appliance Migration

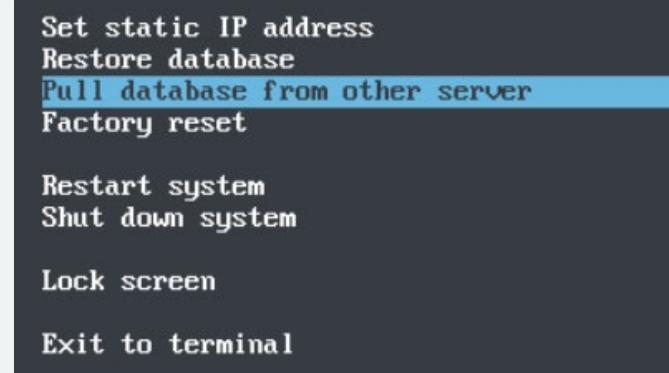
Virtuelle Maschine bereitstellen

Laden Sie die neueste [protect_appliance.ova](#) herunter (oder protect_appliance.vhdx.zip, wenn Sie Microsoft Hyper-V verwenden).

Datenbank von alter Appliance migrieren

Hierfür müssen Sie die Konsole der VM aufrufen und dort den Management Modus öffnen um anschließend „Pull database from other server“ auszuwählen.

Stellen Sie eine neue ESET PROTECT VA bereit. Siehe [ESET PROTECT Virtual Appliance Bereitstellungsprozess für Anweisungen](#). Konfigurieren Sie die neue ESET PROTECT VA nicht über die Weboberfläche.



Anschließend geben Sie die Zugangsdaten der alten Appliance ein (@-Zeichen mit Shift+2). Das Passwort muss dreimal hintereinander eingegeben:

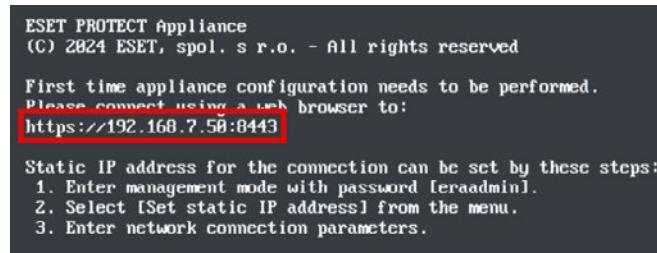
```
Enter connection to remote appliance in format 'admin@hostname' or 'root@hostname' for legacy appliance.
SSH connection: root@192.168.7.18
Enter 'root@192.168.7.18' password for elevated access on remote appliance: ←
Enter database 'root' password on remote appliance: ←
Connecting ...
root@192.168.7.18's password: ←
Stopping remote server ...
Last login: Tue Apr 2 10:01:01 CEST 2024 on cron
Backing up remote server database ...
Starting remote server ...
Last login: Tue Apr 2 10:01:43 CEST 2024
Remote server database was backed up. Review any errors and then press Enter to continue.
```

Nachdem das Backup erstellt wurde, müssen Sie das Passwort der alten Appliance erneut eingeben, um das Backup zu der neuen Appliance zu kopieren und einzuspielen:

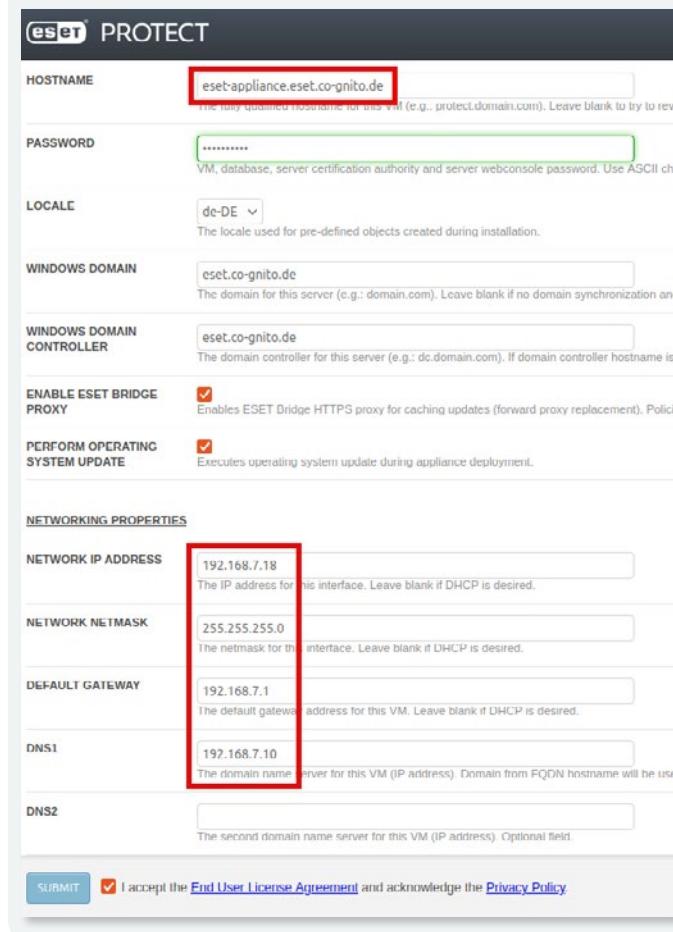
```
Copying backup to local appliance ...
root@192.168.7.18's password: ←
db-upgrade-backup.sql
Restoring database ...
Restoring of remote database backup is finished. Review any errors, then shutdown remote appliance and configure this appliance with same parameters. Press Enter to continue.
```

Neue Appliance konfigurieren

Schalten Sie die alte Appliance ab. Öffnen Sie per Browser das Webinterface der neuen Appliance.



Geben Sie dort die **IP und den Hostnamen** der alten Appliance an und füllen Sie die restlichen Daten aus.



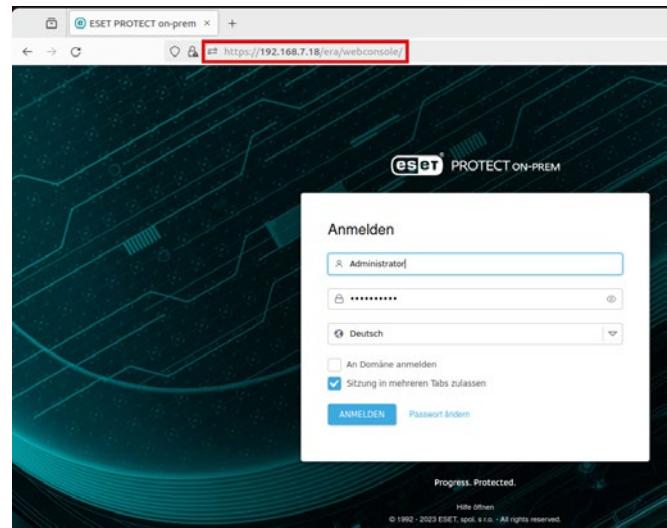
HOSTNAME: eset-appliance.eset.co-gnito.de
PASSWORD: (VM, database, server certification authority and server webconsole password. Use ASCII characters)
LOCALE: de-DE
WINDOWS DOMAIN: eset.co-gnito.de
WINDOWS DOMAIN CONTROLLER: eset.co-gnito.de
ENABLE ESET BRIDGE PROXY: (Enables ESET Bridge HTTPS proxy for caching updates (forward proxy replacement). Policies are applied to the proxy.)
PERFORM OPERATING SYSTEM UPDATE: (Executes operating system update during appliance deployment.)

NETWORKING PROPERTIES

NETWORK IP ADDRESS: 192.168.7.18
NETWORK NETMASK: 255.255.255.0
DEFAULT GATEWAY: 192.168.7.1
DNS1: 192.168.7.10
DNS2: (The second domain name server for this VM (IP address). Optional field.)

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

Sobald Sie die Daten bestätigen, wird die Appliance neu gestartet und ist unter der gewohnten Adresse der alten Appliance erreichbar.



Nachdem bei der neuen Appliance die IP und Daten der alten Appliance übernommen wurden, verbinden sich alle Management Agents wie gewohnt mit der neuen Appliance und es muss nichts weiter getan werden. Die Migration ist somit abgeschlossen.

Weitere Informationen finden Sie hier:

https://help.eset.com/protect_deploy_va/latest/en-US/va_upgrade_migrate.html#recommended

Über ESET

Als europäischer Hersteller mit mehr als 30 Jahren Erfahrung bietet ESET ein breites Portfolio an Sicherheitslösungen für jede Unternehmensgröße. Wir schützen betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie und halten Ihr Netzwerk mithilfe von Cloud Sandboxing frei von Zero Day-Bedrohungen. Mittels Multi-Faktor-Authentifizierung und zertifizierter Verschlüsselungsprodukte unterstützen wir Sie bei der Umsetzung von Datenschutzbestimmungen.

Unsere XDR-Basis mit Endpoint Detection and Response-Lösung, Frühwarnsysteme (bspw. Threat Intelligence) und dedizierte Services ergänzen das Angebot im Hinblick auf Forensik sowie den gezielten Schutz vor Cyberkriminalität und APTs. Dabei setzt ESET nicht allein auf modernste Technologien, sondern kombiniert Erkenntnisse aus der cloudbasierten Reputationsdatenbank ESET LiveGrid® mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten.

3 VON ÜBER 400.000 ZUFRIEDENEN KUNDEN



**CHAMPION
PARTNER**

Seit 2019 ein starkes Team
auf dem Platz und digital



Seit 2016 durch ESET geschützt
Mehr als 4.000 Postfächer



ISP Security Partner seit 2008
2 Millionen Kunden

BEWÄHRT

SecurITy

Trust Seal
www.telertrust.de/itsmle

made
in
EU

ESET wurde das Vertrauenssiegel
„IT Security made in EU“ verliehen



Unsere Lösungen sind nach den Qualitäts- und
Informationssicherheitsstandards ISO 9001:2015
und ISO/IEC 27001:2013 zertifiziert

KONTAKT

Bei Rückfragen können sich ESET Partner
an die Partnerbetreuung wenden.

Tel: +49 (0) 3641 / 3114 - 220 (Mo - Fr 8 - 17 Uhr)
E-Mail: partner@eset.de



**we live
security**™
BY **eset**®

eset®
Digital Security
Guide