Offline Repository und Offline Signaturupdate einrichten

Wichtig: Für PROTECT 9.0 wird der Apache Tomcat 9.0 verwendet. Um auf dem gleichen Server einen Mirror Webserver laufen zu lassen, muss der ApacheHttpProxy zusätzlich nachinstalliert werden.

Die Offline Umgebung kann nur mit dem ApacheHttpProxy aufgebaut werden, die ESET-Bridge wird nicht unterstützt.

Dieser sollte, wenn möglich auf Port 80 laufen. Die Anpassungen im httpd.conf müssen im Editor im Format UTF-8 gespeichert werden. Die httpd.conf kann direkt in dem Apache Konfiguration-Ordner angepasst werden.

Warum Port 80? Dieser Port (http) ist in allen Firmen auf der lokalen Windows Firewall frei geschaltet. Verwendet man einen anderen Port muss dieser flächendeckend allen Endpoints in die Firewall Regeln integriert werden.

Es kann sein, dass sich der ApacheHttpProxy nach den Änderungen in der httpd.conf nicht mehr starten lässt. Hierzu muss der Apache Tomcat 9.0 (PROTECT) beendet werden, dann lässt sich der ApacheHttpProxy starten und im Anschluss ebenfalls der Apache Tomcat 9.0

Der ApacheHttpProxy kann getestet werden, indem man die **index.html** des Proxys in das c:\mirror Verzeichnis kopiert. Und danach den Aufruf macht:

http://localhost/index.html

Das originale index.html File findet man unter:

c:/programme/ApacheHTTPProxy2.4.51/htdocs/index.html

Ruft man den Webserver auf z.B. http://192.168.10.50/index.html, erscheint die Meldung

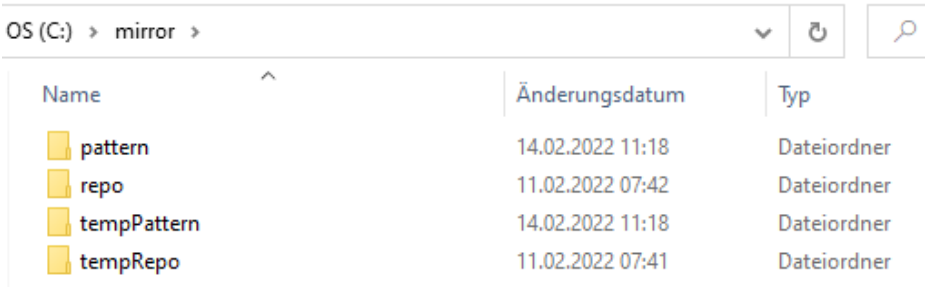
IT WORKS!

Die Offline Repository und Signaturdateien werden mittels dem MirrorTool runtergeladen und über den Apache HTTP Proxy im internen Netz verfügbar gemacht.

Wichtig, auf dem Mirror Server müssen folgende C++ Patches installiert sein:

- Visual C++ Redistributable for Visual Studio 2010
- Visual C++ 2015 Redistributable x86
- Visual C++ 2015 Redistributable x64

Verzeichnisstruktur auf dem PROTECT Server erstellen



Wir erstellen dabei ein Hauptverzeichnis auf dem C:\ oder D:\ Laufwerk namens «mirror». In dem mirror Verzeichnis erstellen wir 4 neue Unterordner:

- pattern : Das **pattern** Verzeichnis beinhaltet sämtliche Signaturen

- repo : Das **repo** beinhaltet alle Programm & Modulupdates die per Task aktualisiert werden

- tempPattern : Ladet alle Pattern-Dateien in das temporäre Verzeichnis

- tempRepo : Ladet alle Programm & Modulupdates in das temporäre Verzeichnis

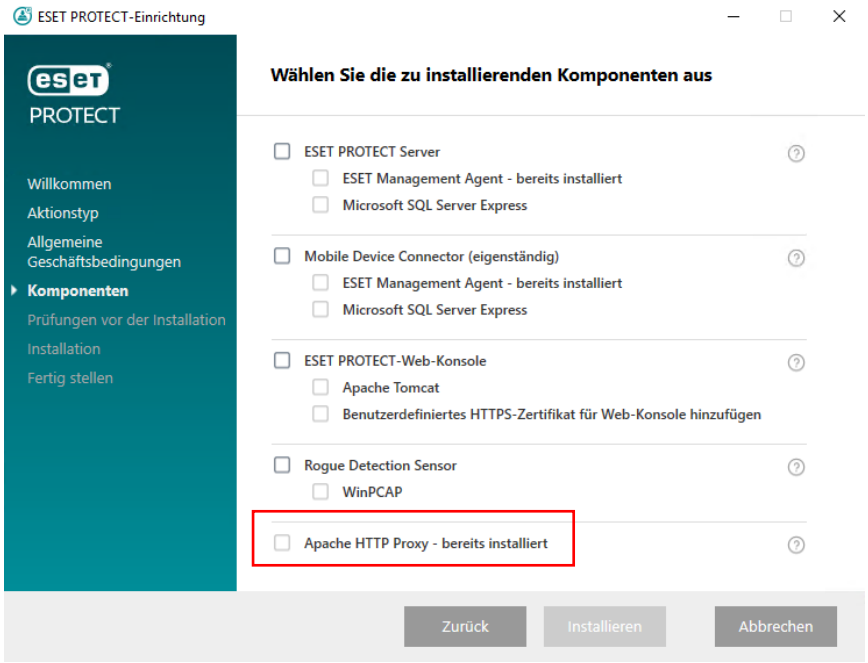
In das Hauptverzeichnis «**mirror**» installieren wir das MirrorTool.exe, welches wir einfach dort entpacken. Runterladen kann man das MirrorTool mit dem nachfolgenden Link:

https://download.eset.com/com/eset/apps/business/era/tools/mirror/latest/mirrortool_win32.zip

Damit AV-Signaturen (Pattern) geladen werden können, müssen wir über den ESET Business Account ein Offline Lizenzfile erstellen und diese danach zu «**offline.lf**» umbenennen und in das Verzeichnis «Mirror» kopieren.

Apache HTTP Proxy installieren

Die Installation erfolgt aus dem PROTECT Installationspaket



Den Hacken bei «Apache HTTP Proxy» setzen und auf Installieren klicken, danach wird der Proxy installiert. Dauer 2-3 Minuten.

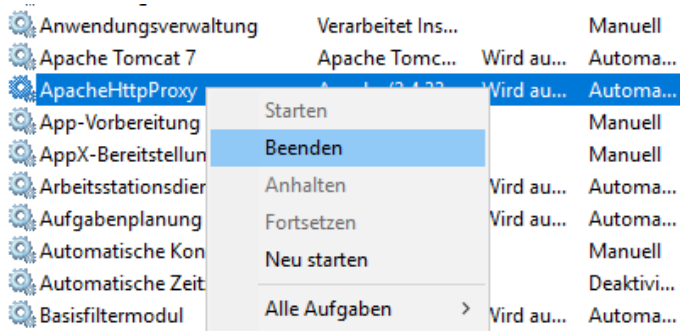
Apache HTTP Proxy «Webserver» konfigurieren

Der installierte Apache HTTP Proxy muss nun konfiguriert werden, so dass er auf Port 80 lauscht und ab dem Verzeichnis C:\mirror die Daten für das Offline Repository und die Offline Signaturen zur Verfügung stellt.

Die nötigen Anpassungen werden in der httpd.conf gemacht!

Vorgehen:

ApacheHttpProxy Dienst stoppen



- httpd.conf auf den Desktop kopieren und anpassen
- Originale httpd.conf umbenennen zu httpd.conf.old
- httpd.conf wieder in das Tomcat Verzeichnis kopieren
- ApacheHttpProxy Dienst starten

Anpassungen in der httpd.conf Datei

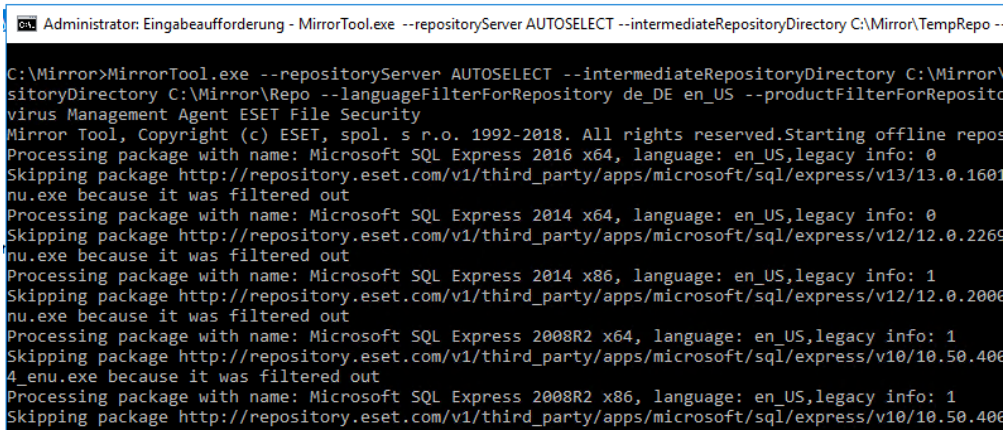
Nachfolgend sieht man die Anpassungen in der httpd.conf Datei.

```
Listen 80

…

ServerRoot "C:\Program Files\Apache HTTP Proxy 2.4.51"
DocumentRoot "C:\mirror"
<Directory "C:\mirror">
Options Indexes FollowSymLinks
AllowOverride None
Require all granted
</Directory>
CacheRoot "C:\ProgramData\Apache HTTP Proxy 2.4.51\cache"
```

Nach dem starten des Apache Tomcat Dienst, ist der Webserver auf Port 80 erreichbar und die Offline Dateien und Offline Pattern können bezogen werden.

Offline Repository und Pattern runterladen

Sämtliche Offline Dateien, werden über das MirrorTool runtergeladen.
Das MirrorTool wird dabei über das CMD gesteuert.



Um das MirrorTool aufzurufen muss zuerst im CMD in das Verzeichnis **c:\mirror** gewechselt werden.

Offline Repository runterladen:

Wichtig dabei, das CMD muss berechtigt sein, vom Internet Daten runterzuladen. Falls dies nur über einen internen Proxy möglich ist, muss dieser im Kommando berücksichtig werden.

*Kommando **ohne** Proxy:*
MirrorTool.exe --repositoryServer AUTOSELECT --intermediateRepositoryDirectory …

*Kommando **mit** Proxy:*
MirrorTool.exe --proxyHost **ProxyName** --proxyPort **8080** --repositoryServer AUTOSELECT --intermediateRepositoryDirectory …

*Kommando **ohne** Proxy für Pattern AV-Signaturen der Version 9.x*
MirrorTool.exe --mirrorType regular –intermediateUpdateDirectory …

*Kommando **mit** Proxy für Pattern AV-Signaturen der Version 9.*MirrorTool.exe --proxyHost **ProxyName** --proxyPort **8080** --mirrorType regular –intermediateUpdateDirectory …

Sobald die beiden Kommandos vollständig durchgelaufen sind, ist das Offline Repository und die Offline Pattern lokal über den http-Proxy verfügbar.

Download ESET AV-Signaturen

MirrorTool.exe --mirrorType regular --intermediateUpdateDirectory C:\mirror\tempPattern --offlineLicenseFilename C:\mirror\offline.lf --outputDirectory C:\mirror\pattern --excludedProducts ep4 ep5 ep6

Download Respository mit Filterwerten

MirrorTool.exe --repositoryServer AUTOSELECT --intermediateRepositoryDirectory c:\mirror\tempRepo --outputRepositoryDirectory c:\mirror\repo --filterFilePath c:\mirror\filter.txt

Filterdatei JSON Beispiel – filter.txt

Die Filterdatei muss direkt im Mirror Verzeichnis liegen c:/mirror

Inhalt:

```
{
"use_legacy": true,
"defaults": {
"languages": [ "de_DE", "en_US" ],
"platforms": [ "x64", "x86" ]
},
"products": [
{
"app_id": "com.eset.apps.business.ees.windows",
"version": "7.1.0.0 - 8.0.0.0"
},
{
"app_id": "com.eset.apps.business.eea.windows",
"version": ">7.1.0.0"
},
{
"app_id": "com.eset.apps.business.efs.windows",
"version": ">8.0.0.0"
},
{
```

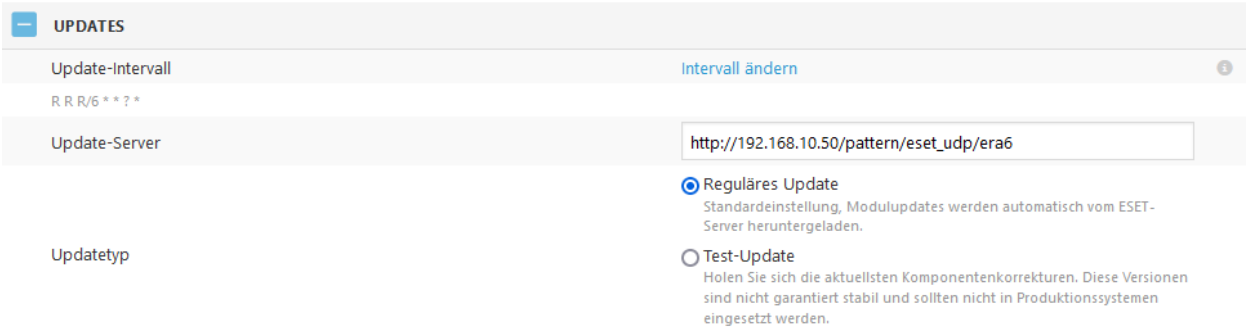
In diesem Beispiel werden nur die deutschen und englischen Pakete für 32-Bit und 64-Bit Windows Betriebssysteme in das Repository aufgenommen. Die ESET-Produkte sind ebenfalls eingeschränkt.

ees – ESET Endpoint Security : Versionen 7.1x bis 8.0
eea – ESET Endpoint AntiVirus : Versionen grösser 7.1.0.0
efs – ESET File Security : Versionen grösser 8.0.0.0

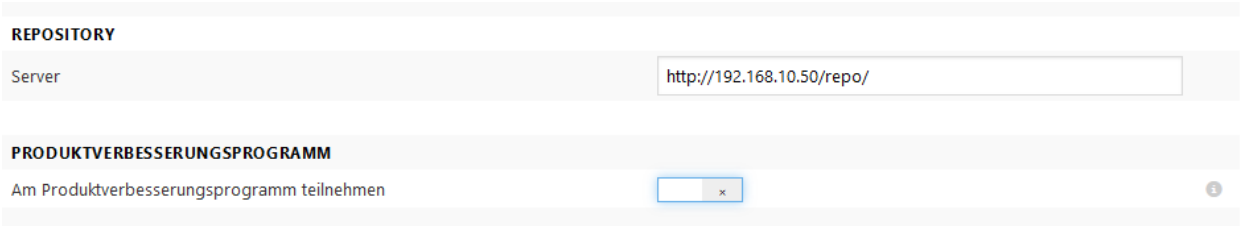
ESET PROTECT Konfiguration

Im ESET PROTECT muss unter den Serversettings das Offline Repository und die Offline Patterns eingetragen werden:

Servereinstellungen > Updates



Servereinstellungen > Erweiterte Einstellungen > Repository



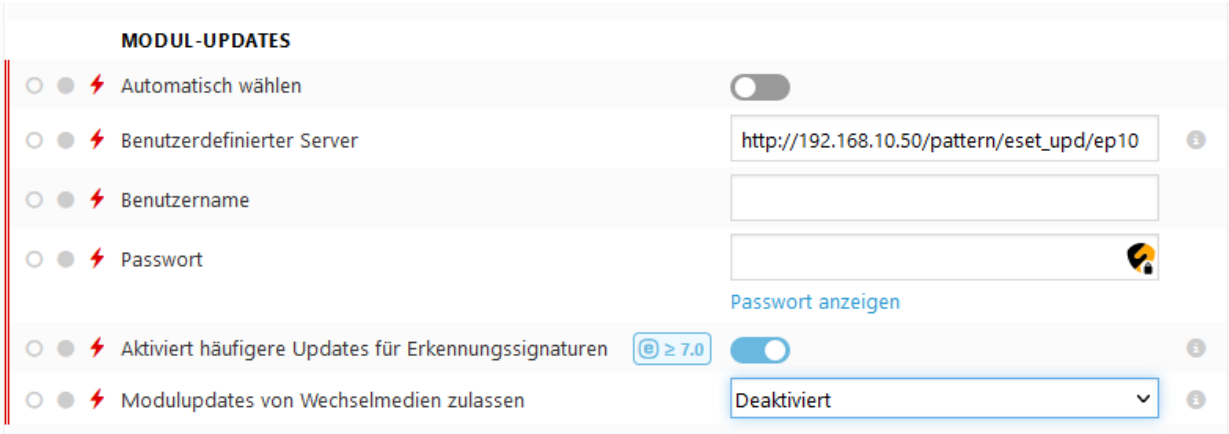
Die IP-Adresse 192.168.10.50 muss der tatsächlichen IP vom PROTECT entsprechen, es kann auch der FQDN eingetragen werden.

Policy Konfigurationen

Damit die Endpoints und Server die Offline Updates und Offline Patterns beziehen können, müssen die Agent, Endpoint und Server Policy angepasst werden.

Agent Policy

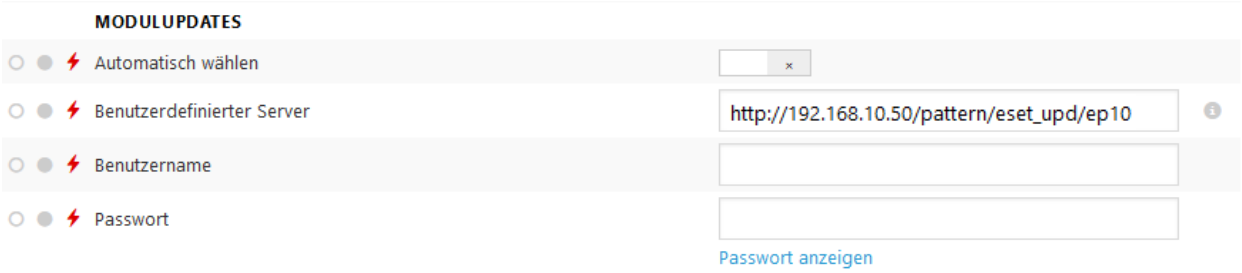
Einstellungen > Updates



Einstellungen > Erweiterte Einstellungen > Repository

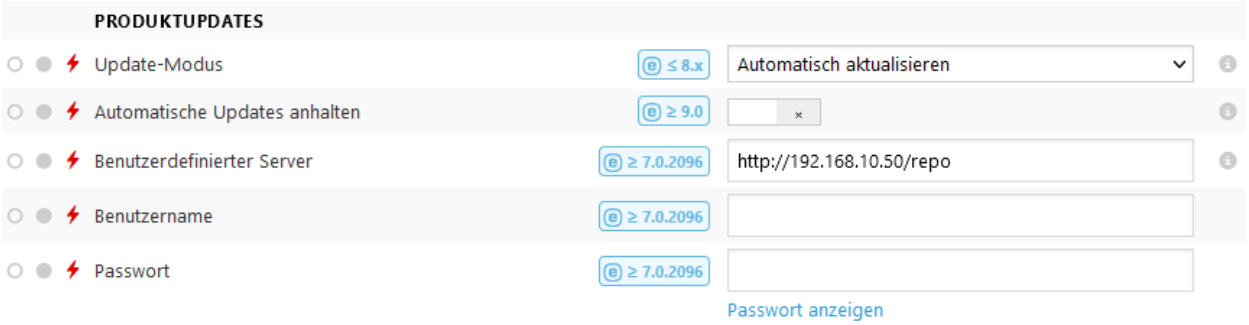
Endpoint Policy

Einstellungen > Update > Profile > Updates > Modulupdates



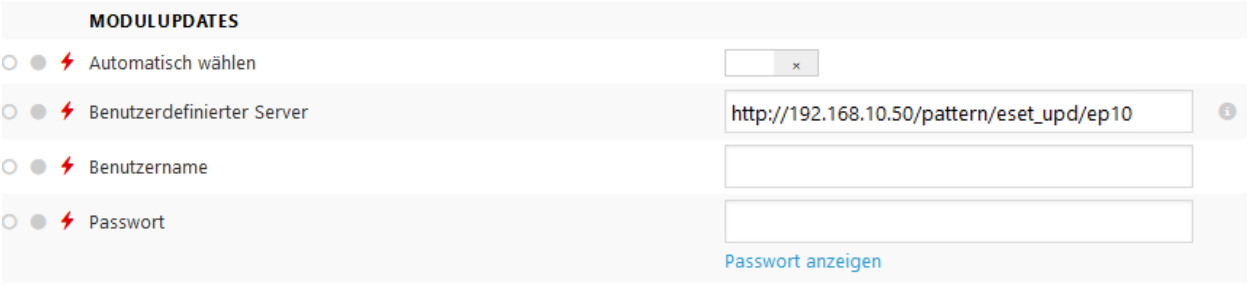
Dieses Beispiel bezieht sich auf eine v9 Umgebung. Sollten noch v8 Endpoints vorhanden sein, muss in dieser Policy anstelle ep9 der Pfad am Ende auf ep8 geändert werden. Es werden dann zwei Policies benötigt, für die v8 Endpoint und für die v9 Endpoints.

Einstellungen > Update > Profile > Updates > Produktupdates



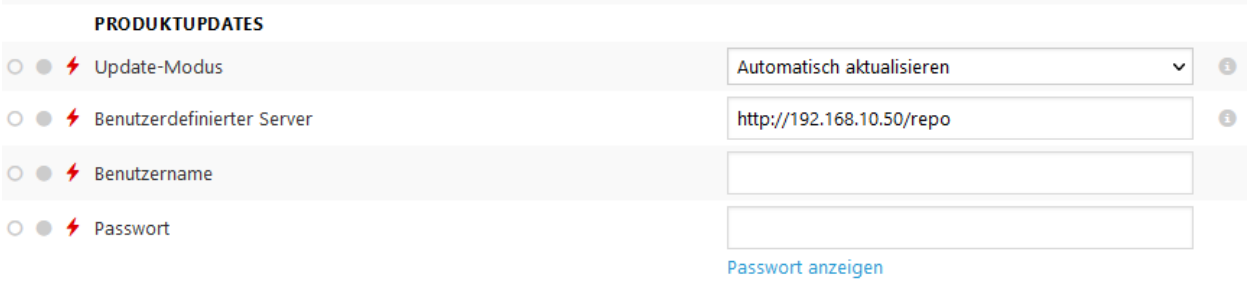
Server Security Policy

Einstellungen > Update > Profile > Updates > Modulupdates



Dieses Beispiel bezieht sich auf eine v9 Umgebung. Sollten noch v8 Endpoints vorhanden sein, muss in dieser Policy anstelle ep9 der Pfad am Ende auf ep8 geändert werden.

Einstellungen > Update > Profile > Updates > Produktupdates



Linux Server Security - Installation

Linux ist sehr speziell in der Installation und es müssen einiges Sachen beachtet werden. Der Linux Server muss in einer OFFLINE Umgebung getestet werden.

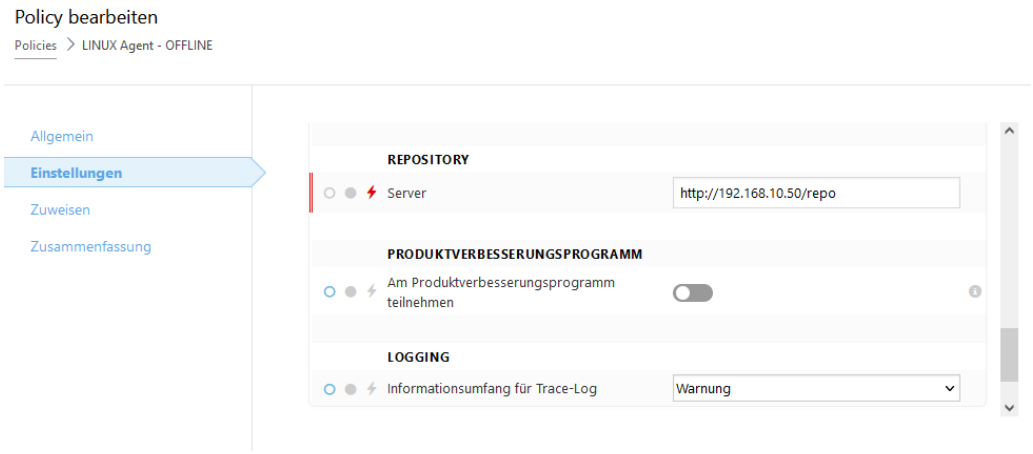
1. Der Linux Server ist so einzustellen, dass er **nicht** ins Internet kommunizieren kann. Die erreicht man am besten, mit einer falschen Default-Gateway IP-Adresse.

2. Der Linux Agent kann nur über ein im PROTECT erstelltes Linux Installationsskript installiert werden. Das Skript wird auf dem Linux Server lokal ausgeführt.

3. Sobald der Linux Agent ausgerollt ist und sich im PROTECT meldet, wird die Linux Server Security direkt über einen Software Installationstask aus dem PROTECT installiert werden.

Linux Agent Policy

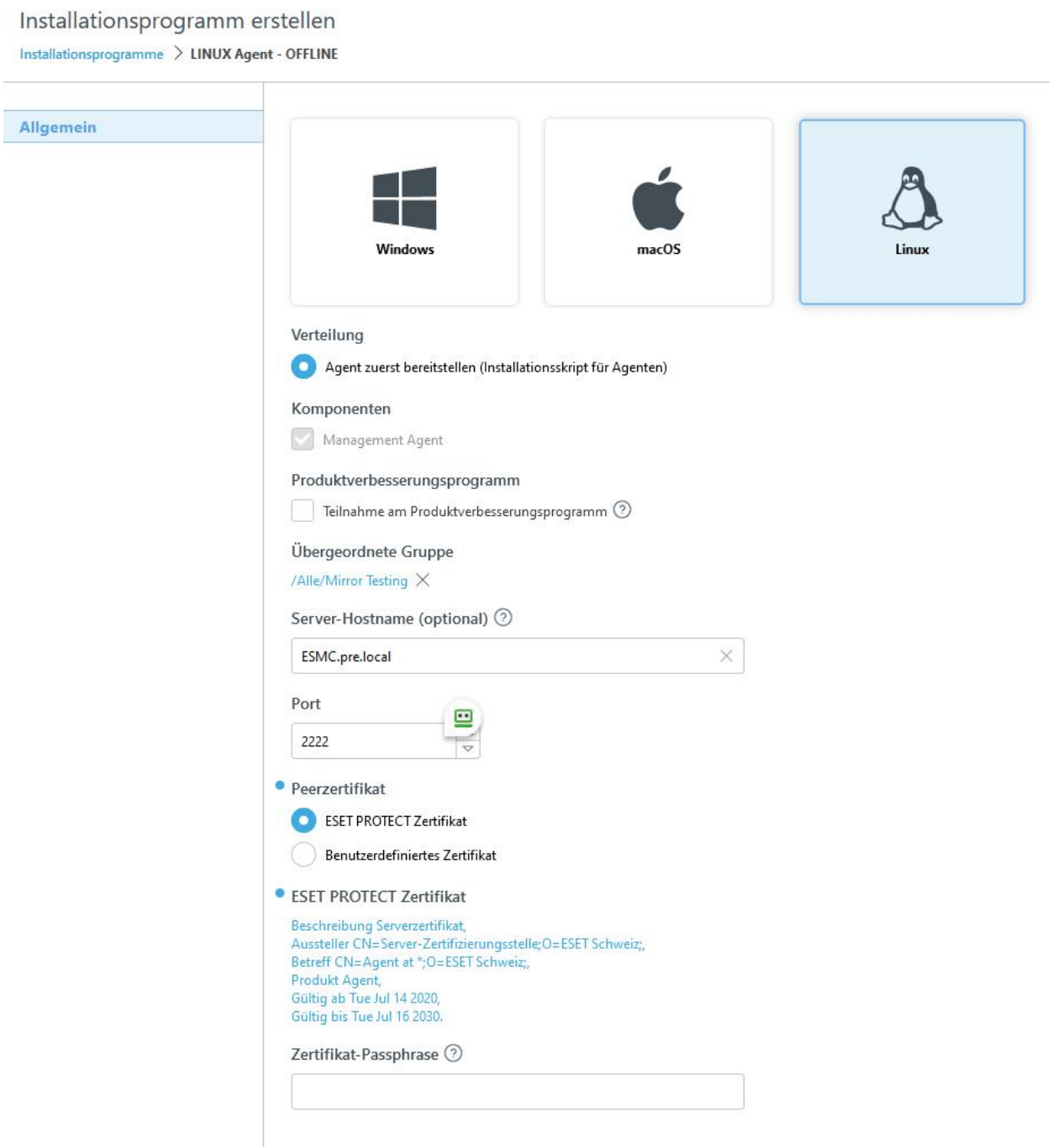
Wichtig, damit die Linux Server Security über den PROTECT ausgerollt werden kann, muss eine Linux-Agent Policy vorgängig erstellt werden, mit dem http://ip-adresse/repo Eintrag beim Repository.



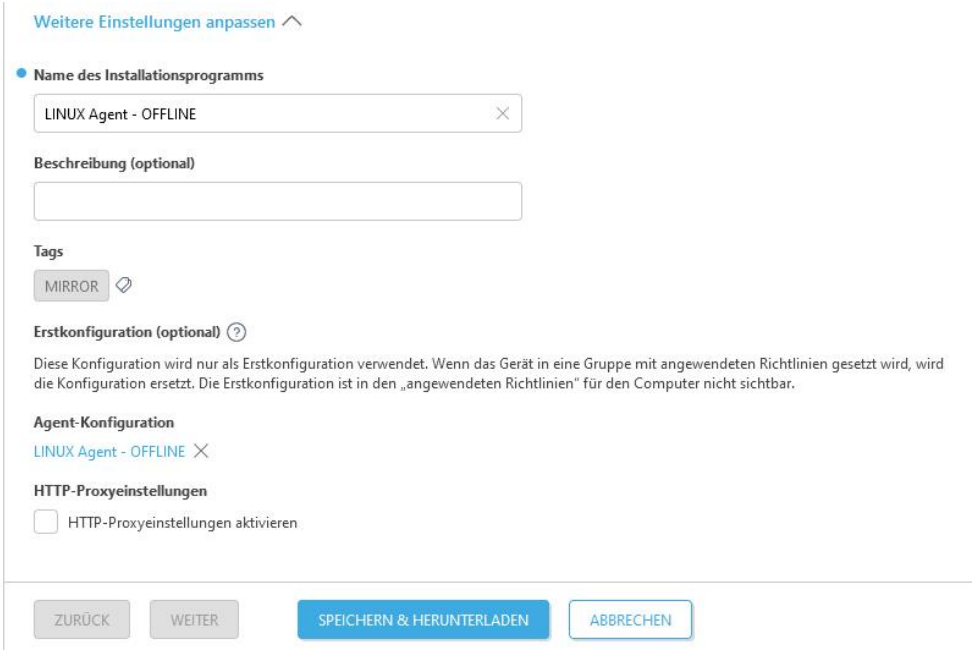
Linux Agent Installer erstellen

Mit dem erstellen des Linux Agent Installer wird ein .sh Skript erstellt, welches danach mit root Berechtigung auf dem Linux Server ausgeführt wird.

Wichtig ist, dass die vorgängig erstellte Linux Agent Policy in das Skript integriert wird, nur so ist eine offline Installation des Linux Agenten möglich, da ihn die Policy anweist, das Paket vom Mirror Server zu beziehen.



Bereits in diesem Schritt gibt man die **übergeordnete Gruppe** an.



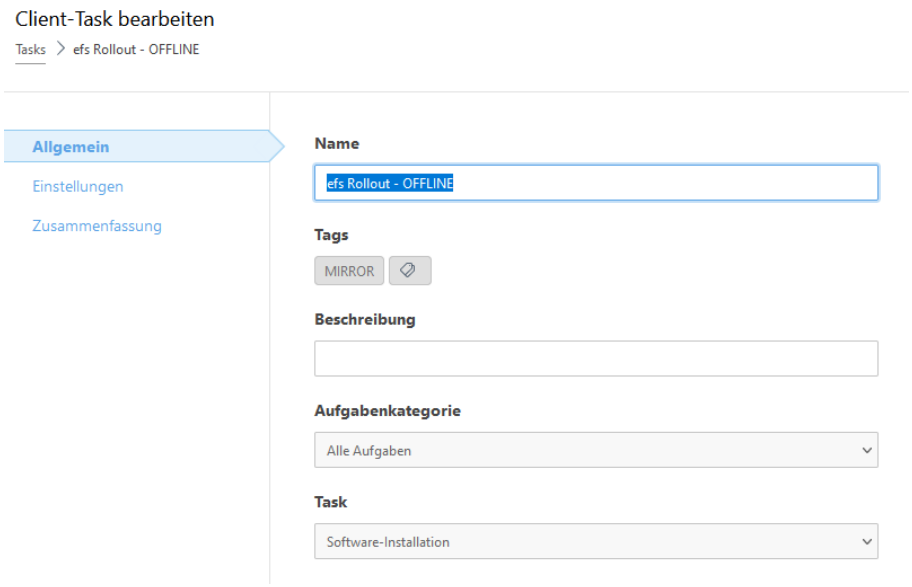
Im Punkt Agent-Konfiguration wird die vorgängig erstelle LINUX Agent – OFFLINE Policy hinzugefügt. Nach dem Speicher & Herunterladen wird dann ein PROTECTAgentInstaller.tar erstellt.

Dieses kann man mit 7-Zip entpacken und die PROTECTAgentInstaller.sh auf den Linux Server kopieren und mit root Berechtigung in einem Terminal ausführen.

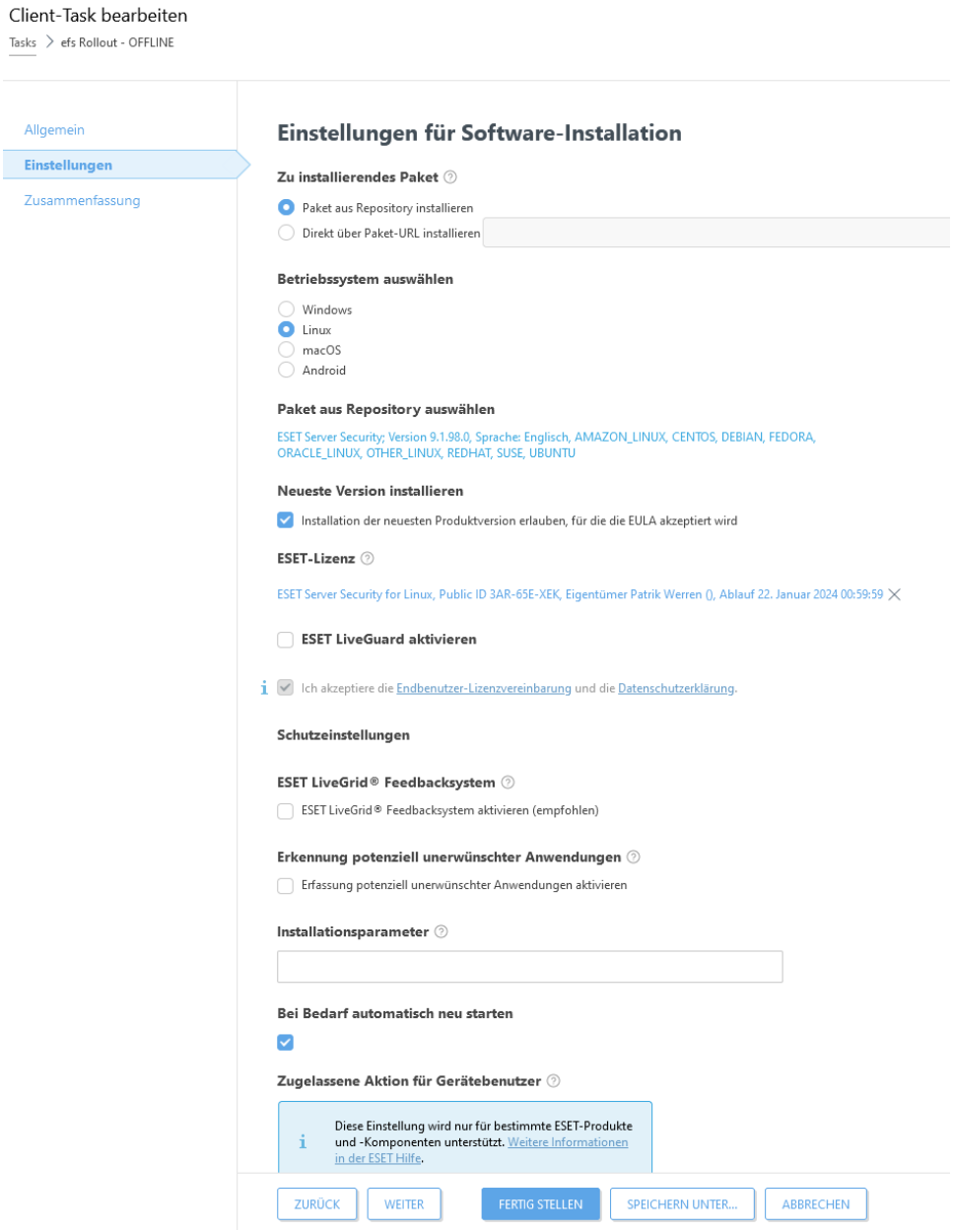
Im Anschluss meldet sich dann der Linux Agent beim PROTECT.

Linux ESET Server Security ausrollen

Die **efs** (ESET File Security) wird über einen Client Task ausgerollt. Wichtig für die Aktivierung während dem Rollout **muss eine Offline Lizenz** erstellt werden und im PROTECT hinterlegt sein. Diese Offline Lizenz wählt man dann im Software-Installations Task aus.



Einen Client-Task «**Software-Installation**» erstellen.



- Das Paket wird aus dem Offline Mirror Repository installiert
- Die ESET-Lizenz muss eine Offline Lizenz sein

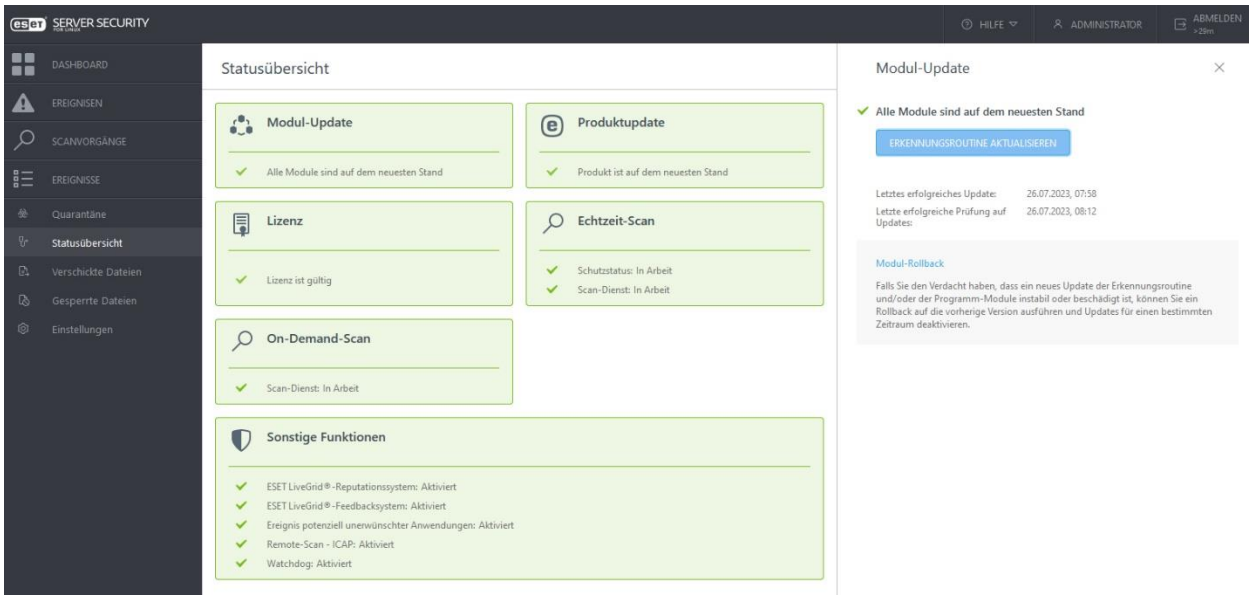
Danach den Task ausführen und das **efs Produkt** wird auf dem Linux Server installiert, aktiviert und im Anschluss werden die neusten Modul-Updates und AV-Signaturen vom Offline Repository geladen.

Linux Web GUI lässt sich nicht erreichen

Sollte das Web GUI der Linux Server Security efs einem SSL-Zertifikatsfehler melden, dann muss auf Linux-Ebene nochmals folgendes Kommando als root ausgeführt werden:

- Im Verzeichnis /opt/eset/efs/
- Kommando setgui -gre

Ist das Web GUI korrekt konfiguriert, dann sieht man das komplette Linux GUI über den Webbrowser.



Hier können wir dann in der Statusübersicht prüfen ob die Modul-Update und Produktupdate vom Mirror geladen werden können.

Wichtig: Der Linux-Server darf keinen Internetzugang haben um eine aussagekräftigen Funktionstest machen zu können.

Kommunikation zum Pattern & Repo Verzeichnis testen

Über den Internet Browser kann man grundsätzlich prüfen ob der Zugriff auf das /Pattern und /Repository Verzeichnis möglich ist:

Pattern Zugriff im Firefox, Google-Chrome, Internet Explorer testen:

http://192.168.10.50/pattern/eset_upd/ep9/nod00C4.nup

Repo Zugriff im Firefox, Google-Chrome, Internet Explorer testen:

http://192.168.10.50/Repository/com/eset/apps/business/efs/windows/v8/8.0.12011.0/efsw_nt64.msi

Repo Zugriff per Download im PowerShell testen:

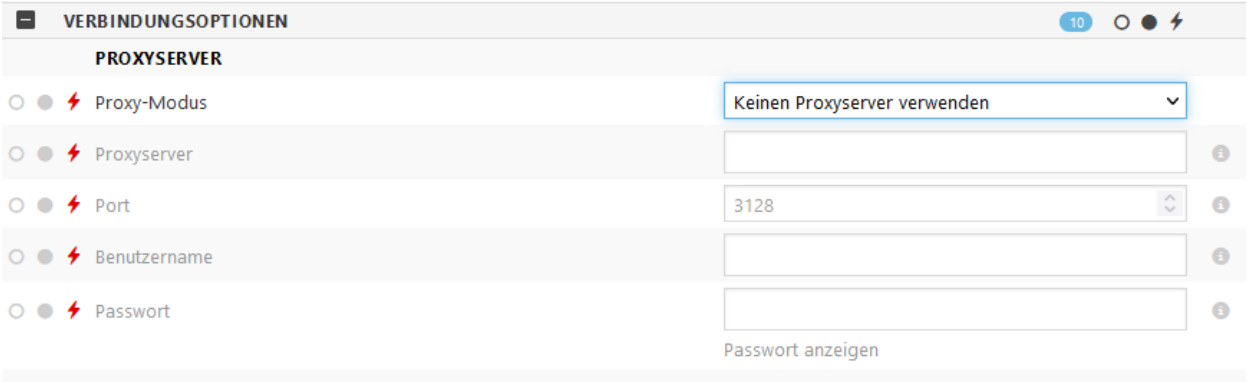
```
Start-BitsTransfer -Source http://192.168.10.50/Repository/com/eset/apps/business/efs/windows/v8/8.0.12011.0/efsw_nt64.msi -Destination c:\mirror\efsw_nt64.msi
```

Auch wenn der Zugriff auf das /Repository mittels einem Internet-Browser möglich ist, heisst das noch lange nicht, dass die ESET Endpoint Security über diesen Weg auf das Offline Repository zugreifen kann. Das Windows System kann einen anderen Proxy / Kommunikationsweg hinterlegt haben, wie der Internet Browser.

Das testet man am besten mittels dem PowerShell. Ist der Zugriff darüber möglich darf in der Endpoint Security kein Proxy Server hinterlegt sein!

Proxy Server Einstellung in allen Policies

Einstellungen > Update > Profile > Updates > Verbindungsoptionen



Keinen Proxyserver verwenden
Die Endpoint Security kommuniziert über den hinterlegten Weg auf dem Client System

Verbindung über Proxyserver
Eintragen, falls das Offline Repository nur über einen Proxyserver erreicht werden kann

Globale Proxyeinstellungen verwenden
Dieser Punkt bezieht sich nicht auf die Proxysettings des Kunden Endpoint sondern der ESET Endpoint Policy, siehe nachfolgende Konfiguration. Diese werden unter Tools > Proxyserver festgelegt.

Ganz Wichtig:

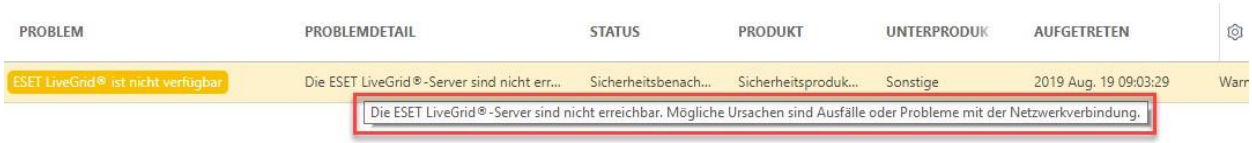
Wir verwenden an der Stelle keinen zusätzlichen Proxy, so dass die Endpoints direkt mit dem Mirror-Webserver kommunizieren können.

Ist der Proxy eingetragen, dann können keine Installationsprogramme im PROTECT erstellt werden.

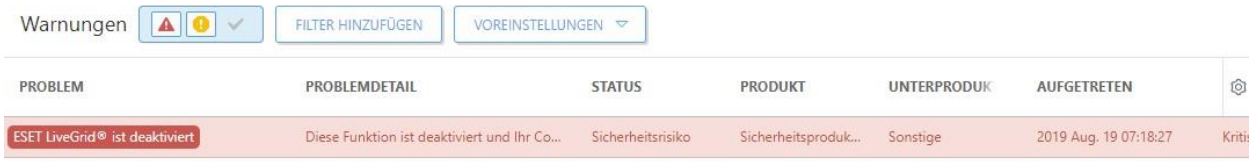
Umgang mit LiveGrid

In einer reinen Offline Umgebung, besteht keine Verbindung zu LiveGrid und dieser Umstand führt zu folgenden Fehlern:

1. LiveGrid aktiviert



2. LiveGrid deaktiviert

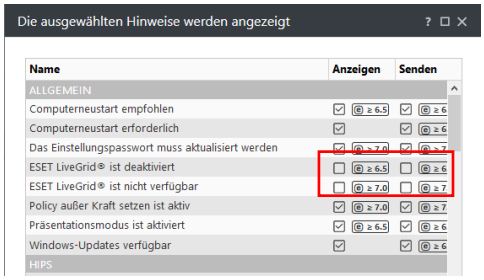


Damit diese Fehlermeldungen direkt am Endpoint oder im PROTECT als Sicherheitsrisiko angezeigt werden, muss die Benachrichtigung in der Endpoint Policy und Server Security Policy deaktiviert werden.

Die Einstellung dazu findet man unter:

Einstellungen > Benutzeroberfläche > Elemente der Benutzeroberfläche > Status

Auf «Bearbeiten» klicken und im nachfolgenden Dialog LiveGrid deaktivieren (abhacken):



Danach werden keine Events mehr bez. LiveGrid am Endpoint angezeigt und zum PROTECT übermittelt.

Parameter im MirrorTool

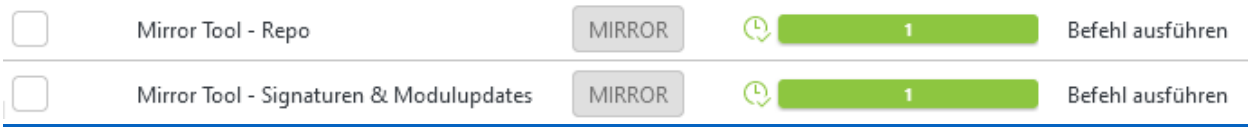
Das MirrorTool verfügt über zahlreiche Parameter und Ausschlussfilter.
Details dazu gibt der globale ESET KB Artikel:

https://help.eset.com/protect_install/90/de-DE/mirror_tool_windows.html

```
C:\Users\                    >MirrorTool.exe --help
Mirror Tool v1.0.1294.0, Copyright (c) ESET, spol. s r.o. 1992-2021. All rights
reserved.
Allowed options:
  --mirrorType arg                      [required for module update]
                                        Type of mirror. Possible values (case
                                        insensitive): regular, pre-release,
                                        delayed.
  --intermediateUpdateDirectory arg     [required for module update]
                                        Files will be downloaded to this
                                        directory to create mirror in output
                                        directory.
  --offlineLicenseFilename arg          [required for module update]
                                        Offline license file.
  --updateServer arg                    [optional]
                                        Update server. (e.g.:
                                        http://update.eset.com/eset_upd/ep6/)
                                        Mirror will be created in output
                                        directory, only specified path in
                                        server will be mirrored.
  --outputDirectory arg                 [required for module update]
                                        Directory where mirror will be created.
  --proxyHost arg                       [optional]
                                        Http proxy address (fqdn or IP).
  --proxyPort arg                       [optional]
                                        Http proxy port.
  --proxyUsername arg                   [optional]
                                        Http proxy username.
  --proxyPassword arg                   [optional]
                                        Http proxy password.
  --networkDriveUsername arg            [optional]
                                        Username used, when output directory is
                                        accessed using smb(e.g:\\hostname).
  --networkDrivePassword arg            [optional]
                                        Password used, when output directory is
                                        accessed using smb(e.g:\\hostname).
  --excludedProducts arg                [optional]
                                        Disable creating mirror for specified
                                        products. Use --listUpdatableProducts
                                        to see possible values.
  --listUpdatableProducts               Show list of all products which modules
                                        are downloaded by default.
  --repositoryServer arg                [required for repository update]
                                        Repository server for repository
                                        creation.
  --intermediateRepositoryDirectory arg [required for repository update]
                                        Files will be downloaded to this
                                        directory to create offline mirror in
                                        output directory.
  --outputRepositoryDirectory arg       [required for repository update]
                                        Directory where offline repository will
                                        be created.
  --trustDownloadedFilesInRepositoryTemp
                                        [optional]
                                        If set, hashes on already downloaded
                                        files are not checked.
  --mirrorOnlyLevelUpdates              [optional]
                                        If set, only level upgrades will be
                                        downloaded (nano/continuous updates
                                        will not be downloaded)
  --mirrorFileFormat arg                [optional]
                                        Specifies which type of update files
                                        will be downloaded. Possible values
                                        (case insensitive): dll, dat.
  --compatibilityVersion arg            [optional]
                                        Version of compatible products.
  --filterFilePath arg                  [optional]
                                        Path to filter file in json format.
                                        Parameter compatibilityVersion has to
                                        be higher than 7.1.0.0 to run program.
  --dryRun arg                          [optional]
                                        Specifies dry run of program with path
                                        to csv file where will be saved list of
                                        products to be downloaded with current
                                        filter configuration.
  --help                                [optional]
                                        Display this help and exit
```

PROTECT Task für Signaturen/Module – Repo

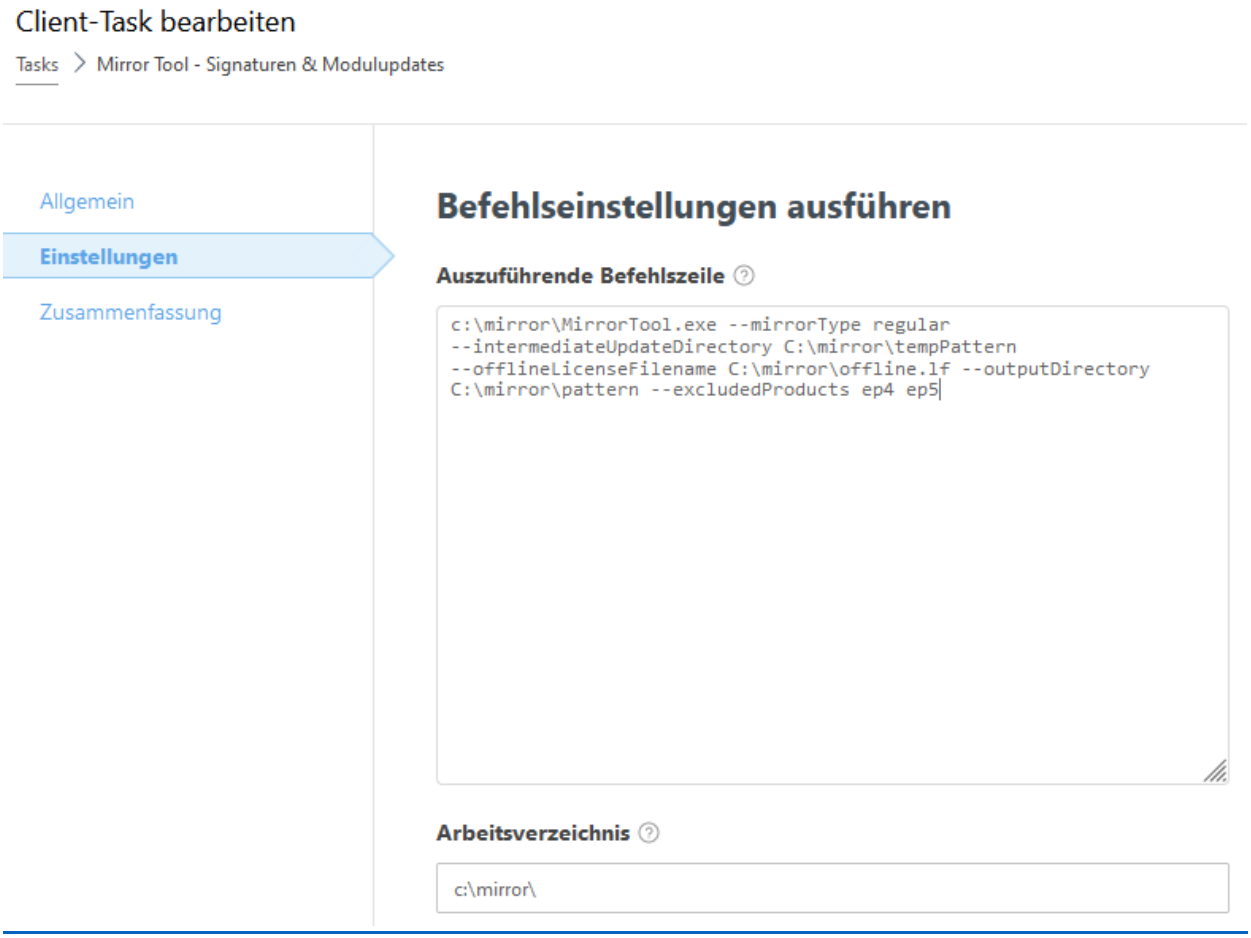
Wir benötigen zwei Task um die Signaturen/Module und das Repo mit dem MirrorTool regelmässig auf den neusten Stand zu bringen.



Task Mirror Tool – Signaturen & Modulupdates

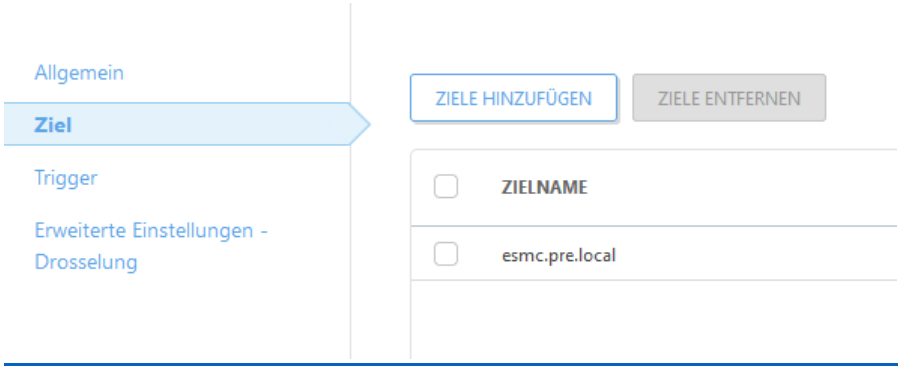
Den Task analog dem CMD-Befehl anlegen. Wichtig: Vor dem MirrorTool.exe muss unbedingt der Pfad angegeben werden, wo sich das Tool befindet.

Ebenfalls ist das korrekte Arbeitsverzeichnis anzugeben.

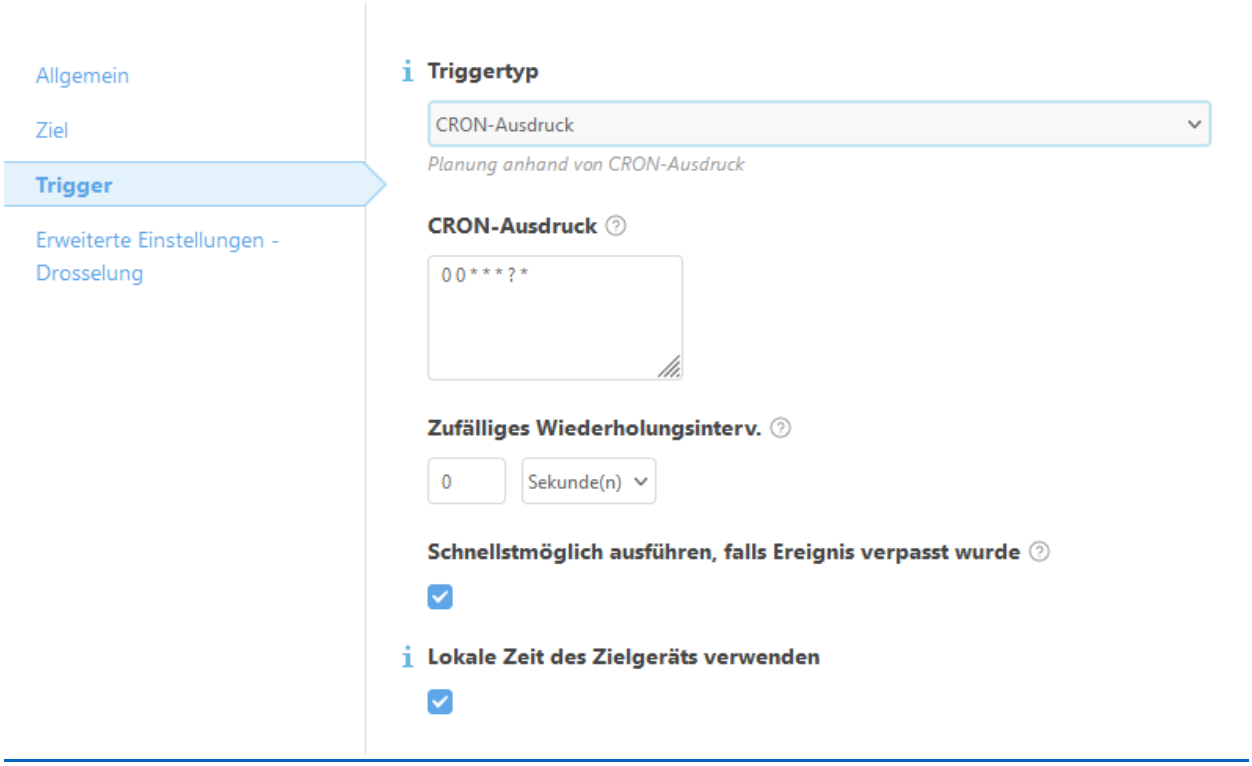


Trigger: Mirror - Signaturen & Module

Schritt 1. Das Ziel angeben, auf welchem Server sich das MirrorTool befindet.



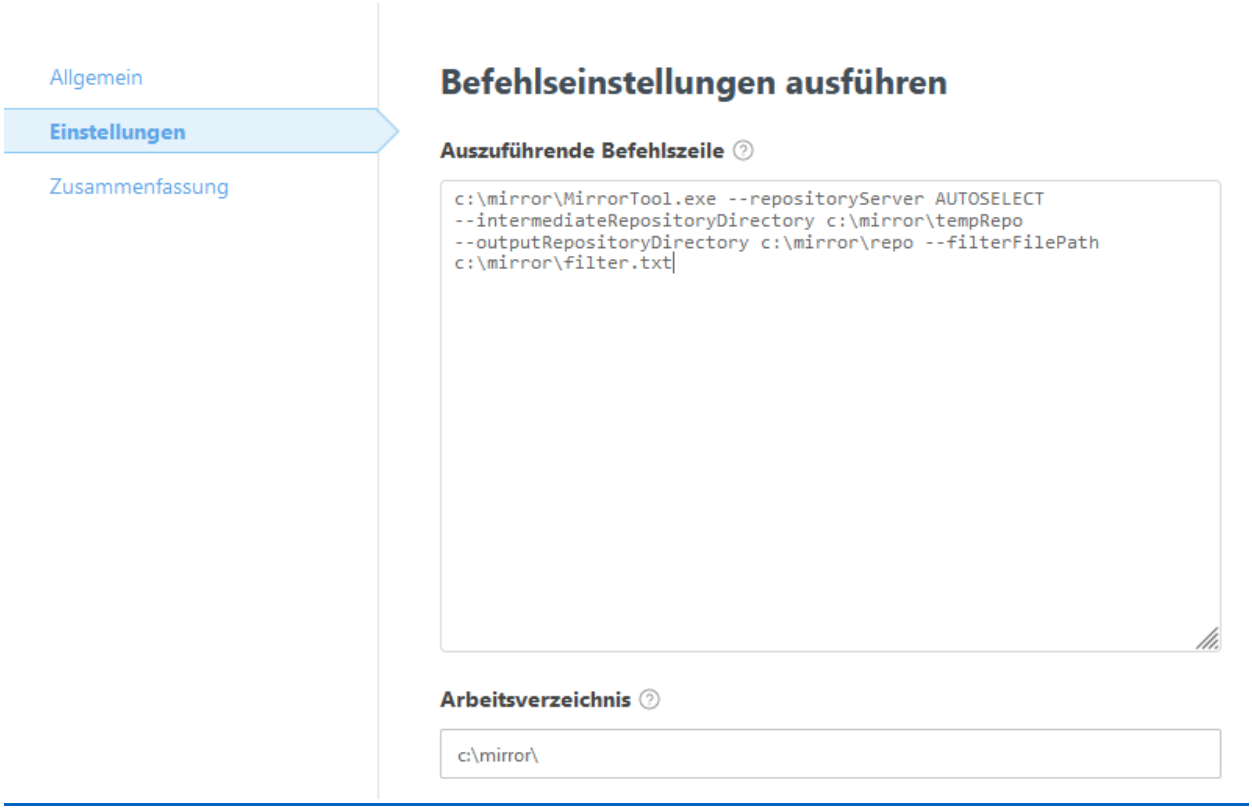
Schritt 2. Den CRON-Ausdruck hinterlegen. In diesem Beispiel werden die Signaturen stündlich heruntergeladen.



Task Mirror Tool – Repo

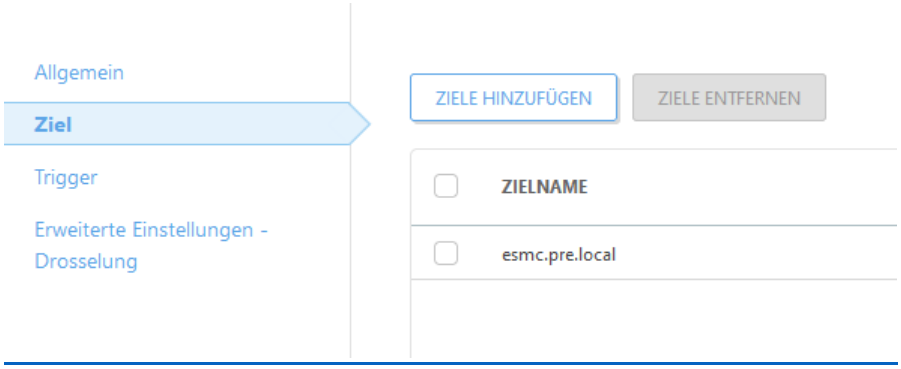
Den Task analog dem CMD-Befehl anlegen. Wichtig: Vor dem MirrorTool.exe muss unbedingt der Pfad angegeben werden, wo sich das Tool befindet.

Ebenfalls ist das korrekte Arbeitsverzeichnis anzugeben.



Trigger: Mirror - Repo

Schritt 1. Das Ziel angeben, auf welchem Server sich das MirrorTool befindet.



Schritt 2. Den CRON-Ausdruck hinterlegen. In diesem Beispiel wird das Repo täglich um 04.00 heruntergeladen.