ESET

REMOTE ADMINISTRATOR

ENDPOINT SECURITY

ENDPOINT ANTIVIRUS

FILE SECURITY für Windows Server

MAIL SECURITY für Microsoft

Best Practices für kleinere und mittlere Unternehmen

Veröffentlicht August 2013

Inhalt

Einleitung

In diesem Dokument werden mit Hilfe einer Beispielinstallation die typischen Schritte wie Installation, Einrichtung und Wartung von ESET Produkten im Businessumfeld mit 5 bis 199 Windows-Systemen gezeigt.

Es beschreibt eine homogene Windows-Landschaft, für heterogene Landschaften gelten die meisten Punkte analog. Dieses Dokument hilft bei der Ersteinrichtung einer ESET-Installation und beantwortet die häufigsten Fragen nach den Erfahrungen der ESET-Spezialisten.

In diesem Dokument wird häufig auf Artikel der ESET Knowledgebase verwiesen und mit der Artikelnummer in eckigen Klammern dargestellt. [SOLN146]

Kapitel 1 Vorbereitungen

1.1 Softwarekomponenten

Es gibt drei Ebenen von Softwarekomponenten mit denen in diesem Best Practice Guide gearbeitet wird: ESET Endpoint Security (EES) und ESET Endpoint Antivirus (EEA) auf der *Clientebene*, ESET File Security für Windows Server (EFSW), ESET Mail Security für Microsoft Exchange Server (EMSX) und ESET Security für Microsoft Sharepoint Server (ESHP) auf der *Serverebene*, sowie ESET Remote Administrator Server (ERAS) und ESET Remote Administrator Console (ERAC) auf der *Verwaltungsebene*.

ESET Endpoint Antivirus wird auf allen Windows Client Workstations installiert, die im lokalen Netzwerk hinter eine Gateway-Firewall eingesetzt werden.

ESET Endpoint Security kann auf allen Windows Client Notebooks installiert werden, die auch in potenziell unsicheren Netzwerken (z.B. öffentliche WLANs) eingesetzt werden.

ESET File Security für Windows Server wird auf Windows Server installiert, auf denen kein zu schützender Microsoft Exchange oder Microsoft Sharepoint installiert ist.
(Windows Server 2003 und höher, Datenbankserver, Terminalserver, Anwendungsserver, etc.)

ESET Mail Security für Microsoft Exchange Es braucht kein zusätzliches ESET-Produkt zum Virenschutz installiert zu werden, in EMSX sind alle Funktionen von EFSW enthalten.

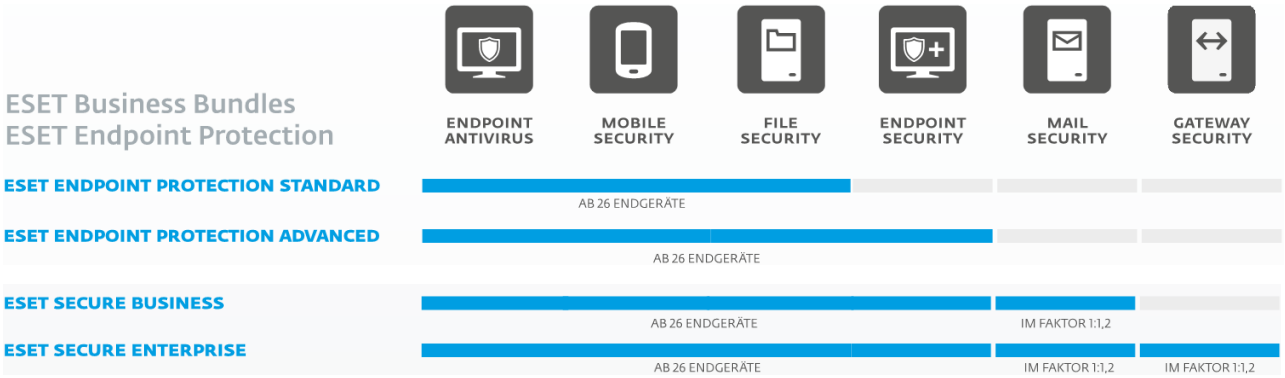
ESET Security für Microsoft Sharepoint Es braucht kein zusätzliches ESET-Produkt zum Virenschutz installiert zu werden, in ESHP sind alle Funktionen von EFSW enthalten.

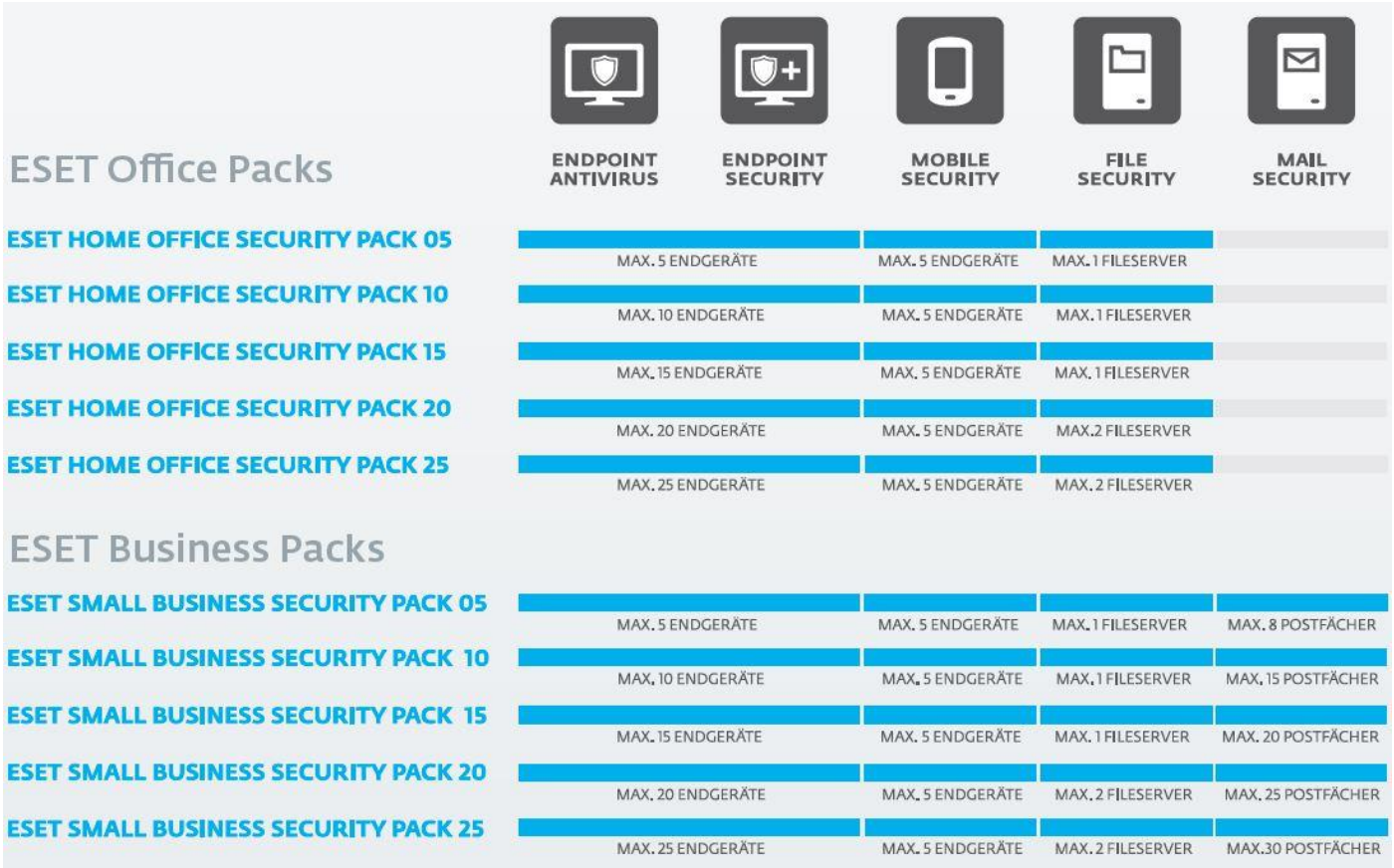
Es wird dringend empfohlen, auf Servern keine Endpoint-Produkte zu installieren, da es sonst zu unvorhergesehenen Komplikationen kommen kann.

ESET Remote Administrator Server sollte auf einem Computer (Server / Client) installiert werden, der dauerhaft läuft. Die ESET Remote Administrator Console kann auf alle Computer installiert werden, von denen der ESET Remote Administrator bedient werden soll.

1.2 Das richtige Produkt auswählen

Bei einer Lizenzgröße unter 25 bietet ESET Security Packs an. Darüber hinaus gibt es ESET Business Solutions.





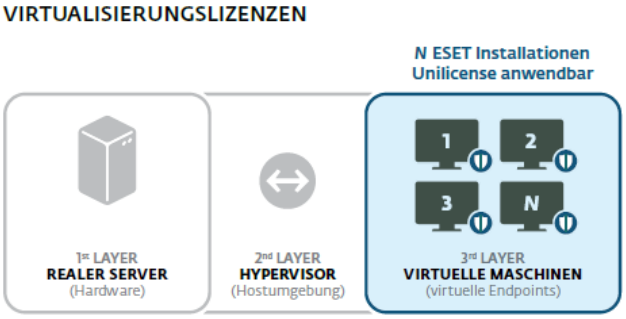
Lizenzgröße eines ESET Business Bundles = Anzahl Endpoints (inkl. Mobile) + Anzahl Server.

Beispiel: 2 File Server, 1 Exchange-Server mit 30 Postfächern, 5 Android-Smartphones, 10 Notebooks und 20 Workstations ergeben eine 38er ESET Secure Business Lizenz.

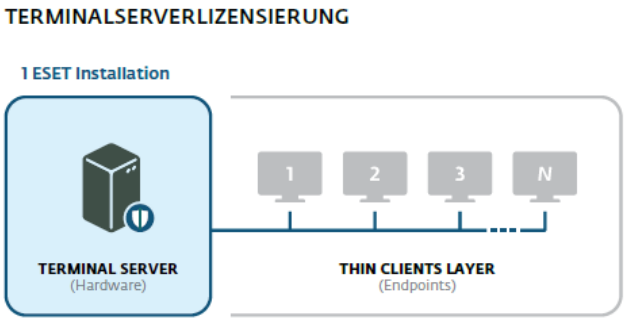
Postfächer: Es werden alle aktiven Nutzer mit einen Postfach (inkl. Gerätepostfach und Raumpostfach), Default-Konten jedoch nicht gezählt. Unter [SOLN2425] können Sie das EMSX Mailbox Count Tool mit /count starten, um die Anzahl der zu lizenzierenden Postfächer zu ermitteln.

Es gibt keine Möglichkeit einzustellen, welche Postfächer geschützt und welche vom Schutz ausgenommen werden sollen.

1.3 Lizenzierung virtueller Maschinen und Terminalserver



Virtuelle Maschine (virtueller Endpoint) = physischer Endpoint (N)
Ein virtueller Endpoint entspricht einem einzelnen physischen Endpoint. Die Anzahl an benötigten Lizenzen, um die virtuellen Endpoints abzudecken, richtet sich nach der Anzahl der virtuellen Endpoints, die auf dem 3. Layer laufen. Die ESET-Lösung wird auf dem 3. Layer – also den virtuellen Endpoints – installiert.



Thin Client = Endpoint
Die Anzahl an benötigten Lizenzen, um Terminal Server abzudecken, richtet sich nach der Anzahl an Thin Clients, die mit diesem Server verbunden sind. Die ESET-Lösung wird auf dem Terminal Server installiert.

1.4 Ihre ESET Software herunterladen

Umgebungen bis 25 Arbeitsplätze benötigen im Normalfall folgende Installationsdateien:

ERA-Server:	http://download.eset.com/download/ra/era_server_nt32_deu.msi
ERA-Console:	http://download.eset.com/download/ra/era_console_nt32_deu.msi
EEA 32Bit:	http://download.eset.com/download/win/eea/eea_nt32_deu.msi
EEA 64Bit:	http://download.eset.com/download/win/eea/eea_nt64_deu.msi
EMSX 64Bit:	http://download.eset.com/download/exchange/emsx_nt64_deu.msi

Umgebungen ab 26 Arbeitsplätzen benötigen oft zusätzlich folgende Installationsdateien

EFSW 32Bit:	http://download.eset.com/download/windows_file/efsw_nt32_deu.msi
EFSW 64Bit:	http://download.eset.com/download/windows_file/efsw_nt64_deu.msi
EMSX 32Bit:	http://download.eset.com/download/exchange/emsx_nt32_deu.msi
EES 32Bit:	http://download.eset.com/download/win/ees/ees_nt32_deu.msi
EES 64Bit:	http://download.eset.com/download/win/ees/ees_nt64_deu.msi

1.5 Zuordnung der Lizenzdateien

Beim Erhalt der Lizenzmail befinden sich in der angehängten Lizenzdateien.zip bis zu fünf Lizenzdateien:

MailSecurity.lic wird während der EMSX-Installation, anschließend in den erweiterten Einstellungen oder über eine ERA-Policy installiert.

ERA-Endpoint.lic und *ERA-MailSecurity.lic* werden im ERA-Lizenz-Manager installiert. Das Zusammen-fassen von mehreren Lizenzen ist unter bestimmten Voraussetzungen möglich.

Bei unterschiedlichen .lic-Dateien desselben Typs wird die beste anhand der Lizenzgröße automatisch ausgewählt.

Es wird empfohlen, bei ESET Endpoint Produkten und EFSW keine Lizenzdatei zu installieren, da dies lediglich für die Freischaltung der Mirror-Funktion benötigt wird. Eine installierte Lizenzdatei kann über ESET Remote Administrator Console nicht entfernt werden, und muss in diesem Fall bei jeder Verlängerung für alle Clients zusätzlich aktualisiert werden.

Kapitel 2 Installation

2.1 ESET Remote Administrator Server

Starten Sie die Installation, indem Sie die Datei *era_server_nt*32*_deu.msi* ausführen.

Nach Akzeptieren der Lizenzvereinbarungen wählen Sie die typische Installation und nach dem Klick auf Weiter die *ERA-Endpoint.lic* aus. Wir empfehlen, im Fenster Sicherheitseinstellungen ein Passwort für Konsole zu setzen. Alle definierbaren Passwörter in diesem Fenster sind jedoch optional. Tragen Sie im Fenster Updates den Benutzernamen und das Passwort von Ihrer Endpoint-Lizenz ein.

Im letzten Schritt ändern Sie den Standard HTTP-Port zum Zugriff auf das ESET Web-Dashboard, sofern auf dem Server bereits ein Webserver (bspw. Microsoft IIS) läuft.

2.2 ESET Remote Administrator Console

Nachdem die Installation des ESET Remote Administrator Servers abgeschlossen ist, führen Sie die Datei *era_console_nt*32*_deu.msi* aus. Wählen Sie die typische Installation aus und folgen den Bildschirmanweisungen.

ERA-Server und ERA-Console müssen immer die gleiche Version haben. Eine Serverversion 4 kann nicht mit einer Consolenversion 5 verwaltet werden.

2.3 Nachkonfiguration

2.3.1 Ports in der Windows-Firewall freischalten

Schalten Sie in der Firewall (*wf.msc*) folgende Ports in eingehender Richtung frei:

2221 – vom ERA-Mirror bereitgestellte Datenbanksignaturupdates

2222 – Kommunikation mit ERA-Clients

2223 – Kommunikation zwischen ERAS und ERAC

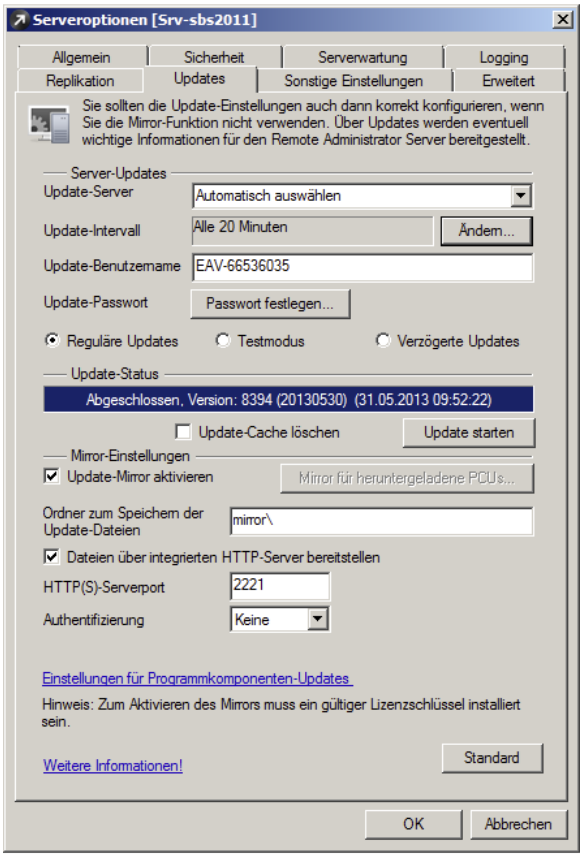
2224 –Roll-Out von Installationspaketen über PUSH-Installation

2225 – Web-Dashboard

2.3.2 Erstellen eines Mirror-Servers

Ein Mirror-Server stellt für alle ESET-Clients Signaturdatenbankupdates bereit.

Wählen Sie Extras → Serveroptionen → Updates



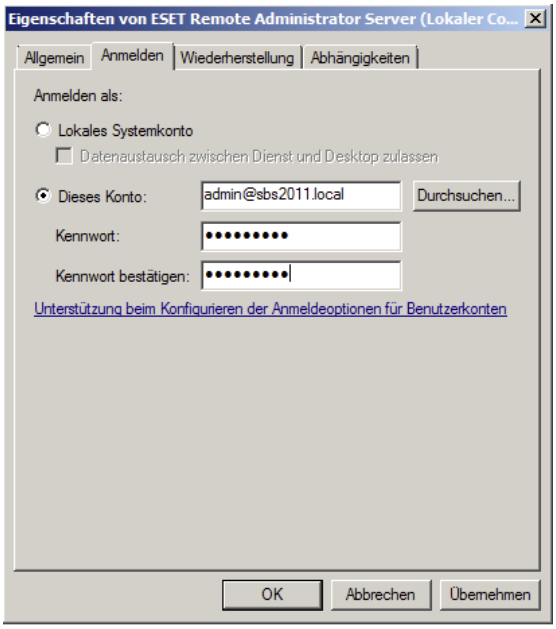
In den Feldern Update-Benutzername und Update-Passwort sind bereits Ihre Lizenzdaten der Endpoints eingetragen. Falls nicht, tragen Sie diese hier ein.

Aktivieren Sie die Kontrollkästchen Update-Mirror aktivieren und Dateien über integrierten http-Server bereitstellen und klicken anschließend auf Update starten.

- Sollten Sie den Pfad mirror\ ändern wollen, so tragen Sie bitte den absoluten, lokalen Pfad in dieses Feld ein, ohne den Ordner vorher im Windows-Explorer zu erstellen.
- Wenn Sie das Update-Intervall verkürzen (z.B. auf 20 Minuten), kann der Update-Mirror den Clients schneller aktuelle Signaturen bereitstellen
- Der Update-Mirror kann auch über Microsoft IIS freigegeben werden [SOLN2270]
- Proxyeinstellungen zum Download von Updates können optional unter Extras → Serveroptionen → Erweitert → Remote Administrator → ERA Server → Einstellungen → Update gesetzt werden.

2.3.3 Dienstanmeldung

Wir empfehlen, den Dienst ESET Remote Administrator Server auf die Anmeldung mit einem Domänen-Administrator-Konto umzustellen. Dazu Dienste (*services.msc*) ausführen → ESET Remote Administrator Server → Eigenschaften → im Karteireiter Anmelden die Daten des Domänen-Administrators eintragen. Damit haben Sie folgende Vorteile:



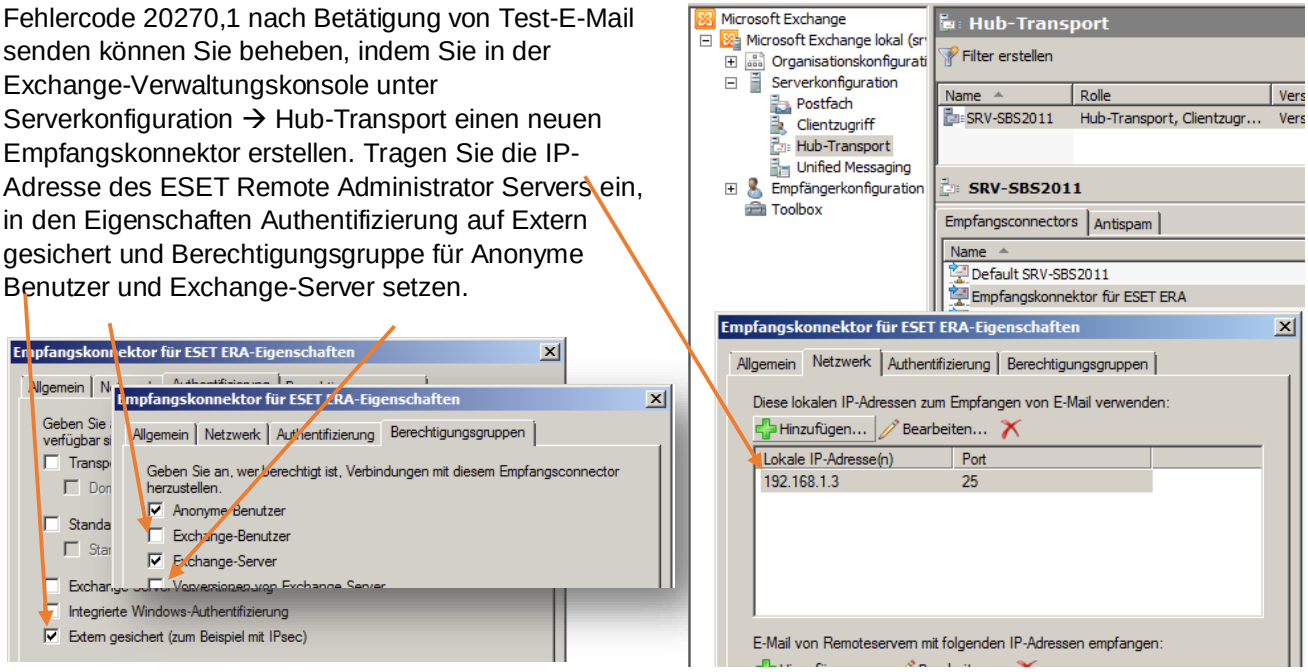
- Das Active Directory kann mit dem ESET Remote Administrator Console effektiver nach Computerkonten durchsucht werden
- Sie können die Kennwort-Abfrage bei der PUSH-Installation überspringen.
- Die PUSH-Installation ist bei NT 6.x Computern erfolgreicher

- Sie können optional zusätzlich LDAP-Informationen unter Extras → Serveroptionen → Erweitert → Remote Administrator → ERA Server → Einstellungen → Active Directory eines Domänen-Administrators eintragen.
- Wenn das Kennwort des Domänen-Administrators abgelaufen ist oder geändert wurde, muss es manuell im Dienst ESET Remote Administrator Server und im Feld Active Directory der erweiterten Einstellungen des ESET Remote Administrator Servers erneuert werden. Um dies dauerhaft zu umgehen, können Sie ein extra Benutzer-Konto für ESET erstellen.

2.3.4 Konfigurieren von SMTP-Einstellungen

Damit der ESET Remote Administrator Server E-Mails für Notifikationen oder Reports versenden kann, müssen SMTP-Einstellungen konfiguriert werden. Konfigurieren Sie die Mailserveradresse und zugehörige Kontodaten unter Extras → Serveroptionen → Sonstige Einstellungen.

Fehlercode 20270,1 nach Betätigung von Test-E-Mail senden können Sie beheben, indem Sie in der Exchange-Verwaltungskonsole unter Serverkonfiguration → Hub-Transport einen neuen Empfangskonnektor erstellen. Tragen Sie die IP-Adresse des ESET Remote Administrator Servers ein, in den Eigenschaften Authentifizierung auf Extern gesichert und Berechtigungsgruppe für Anonyme Benutzer und Exchange-Server setzen.

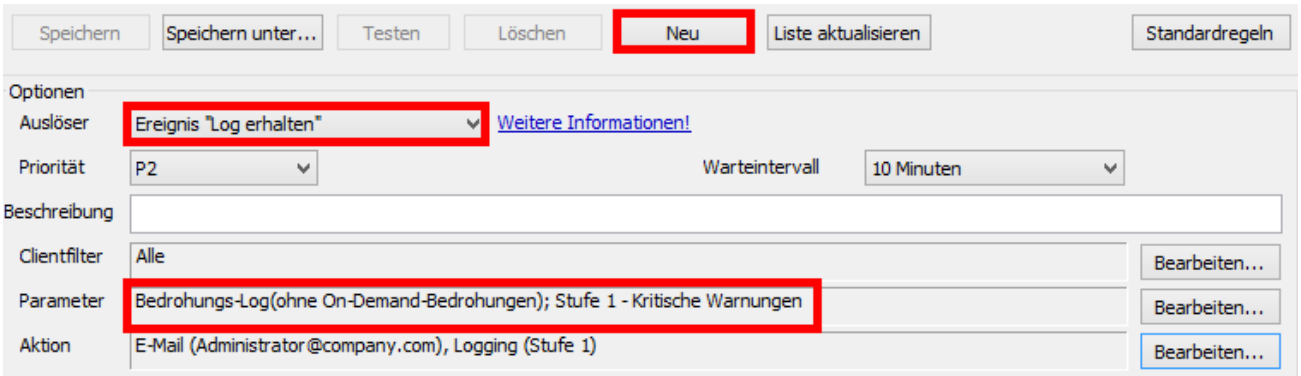


2.3.5 Einrichten von Notifikationen

Notifikationen helfen Ihnen schneller, auf Vorfälle reagieren zu können. Unter Extras → Notifikations-Manager sind bereits 20 vorinstallierte Notifikationen eingerichtet, die Sie aktivieren und editieren können.

Sie können die Notifikation via SNMP-Trap oder E-Mail versenden. Dazu unter Aktion → Bearbeiten die E-Mail-Adresse hinzufügen bzw. das Kontrollkästchen für SNMP-Trap aktivieren.

Empfehlenswerte Notifikationen sind: Lizenzablauf, Lizenzlimit, Server nicht aktualisiert. Erstellen Sie eine Notifikation für einen erkannten, jedoch nicht entfernten Virenfund: Klicken Sie Neu, wählen Ereignis Log erhalten →Parameter Bearbeiten → wählen Log-Typ Bedrohungs-Log und Kritische Warnungen aus.



Ist das Feld E-Mail unter Aktion → Bearbeiten einer Notifikation nicht anwählbar, so sind keine SMTP-Einstellungen konfiguriert (siehe 2.3.4).

Kapitel 3 Konfiguration mit dem Policy-Manager

Policies stellen die einfachste Möglichkeit dar, ESET Clienteinstellungen zu konfigurieren und Einstellungen des gesamten Netzwerks im Überblick zu behalten. Client Workstations erhalten die Clienteinstellungen der Policies automatisch, sobald sie sich am ESET Remote Administrator Server anmelden.

Wir empfehlen, Installationspakete mit nahezu Default-Werten zu erstellen, um nach erfolgreicher PUSH-Installation über eine automatische Zuordnung des Clients in die gewünschte Policy, die Clienteinstellungen automatisch an den Client zu übertragen.

Symbole im Konfigurationseditor:

- Kein Wert gesetzt, diese Option wird am Client nicht geändert.
- Dieser Wert wurde von einer übergeordneten Policy geerbt.
- Wert ist in dieser Policy gesetzt, diese Option wird am Client geändert.
- Ein Wert ist in dieser Policy-Kategorie gesetzt.

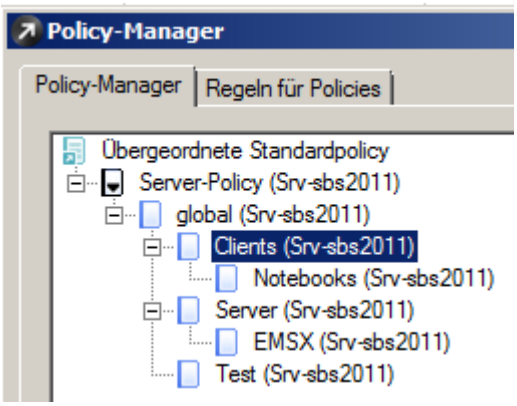
Falsche Werte im Policyzweig Remote Administration können zum Kommunikationsverlust zwischen Clients und ESET Remote Administrator Server führen. In diesem Fall müssen Sie die Werte an den betroffenen ESET-Clients lokal korrigieren oder die ESET Endpoint Software neu installieren.

Bei jeder Anmeldung des ESET-Clients am ESET Remote Administrator Server werden die Einstellungen der Policy gesetzt. Während eines lokalen Troubleshootings sollte daher temporär die regelmäßige Verbindung mit dem ESET Remote Administrator Server deaktiviert werden.

Öffnen Sie den Policy-Manager unter Extras → Policy-Manager

3.1 Beispiel einer Policystruktur

In den meisten Umgebungen ist eine Unterteilung zwischen Clients und Servern auf erster Hierarchieebene empfehlenswert. Untergeordnete Policies können für spezielle Einstellungen genutzt werden. Zum Troubleshooting kann eine Test-Policy hilfreich sein.



Symbole im Policy-Manager:

Das schwarze Policysymbol markiert die Standardpolicy für primäre Clients.

Das blaue Policysymbol markiert normale Policies.

Einstellungen blau ausgefüllter Policysymbole können von untergeordneten Policies nicht überschrieben werden.

Policysymbole mit einem Pfeil können auf untergeordnete Server repliziert werden.

Die Standardpolicy für primäre Clients wird allen Clients zugewiesen, die nicht über eine Policyregel oder manuell einer anderen Policy zugeordnet wurden. Diese Standardpolicy wird in den Globalen Policyeinstellungen definiert.

In der Policy global können Sie Einstellungen setzen, die für alle Clients gelten sollen. In den untergeordneten Policies setzen Sie Einstellungen für die speziellen Client-Gruppen.

3.1.1 Konfiguration von ESET Endpoint Software

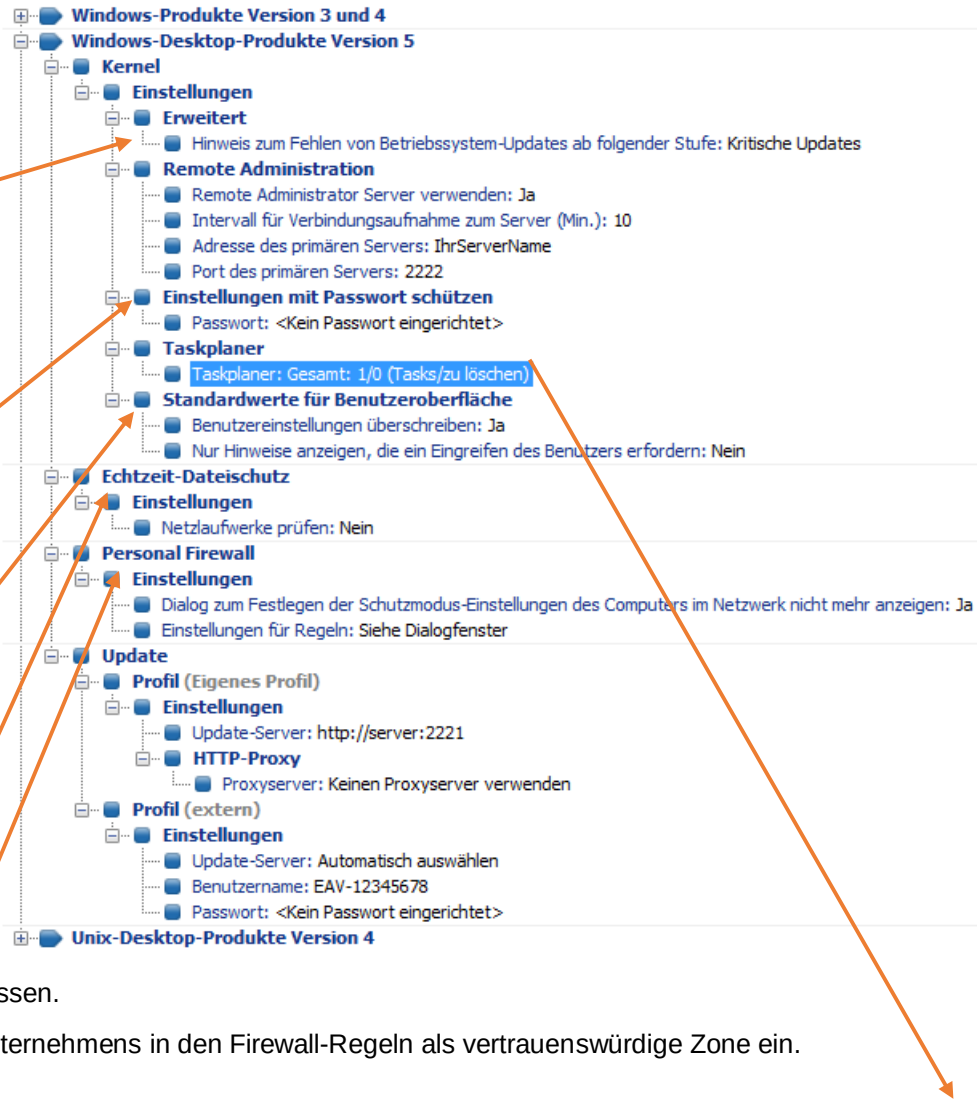
ESET-Sicherheitsprodukte prüfen auf Vollständigkeit der Windows-Updates. Die Prüfung auf fehlende Kritische Updates kann über Ändern auf Keine Updates deaktiviert werden.

Damit niemand außer Ihnen Einstellungen an der ESET Endpoint Software vornehmen kann, sollten Sie die Einstellungen mit einem Passwort schützen.

Änderungen an der Benutzeroberfläche der ESET Endpoint Software benötigen das Überschreiben der Benutzereinstellungen. Beispielsweise können Sie die Anzahl der Hinweisfenster in dieser Kategorie auf Minimum setzen.

Prüfen der Netzlaufwerke sollte deaktiviert werden.

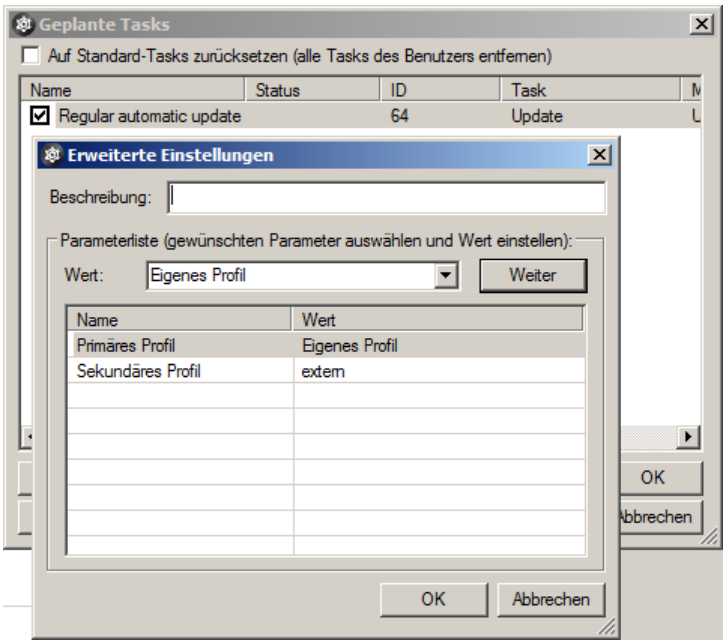
Wir empfehlen, den Dialog zum Festlegen des Schutzmodus Ihres Computers im Netzwerk nicht anzeigen zu lassen.



Tragen Sie das Subnetz Ihres Unternehmens in den Firewall-Regeln als vertrauenswürdige Zone ein. [SOLN2233]

Das Update-Profil (Eigenes Profil) konfigurieren Sie so, dass alle ESET Endpoint Software Updates von dem Update-Mirror erhalten. Tragen Sie dazu http://server:2221 als Update-Server ein, wobei „server“ Ihr Servername, bzw. Server-IP-Adresse ist. Wir empfehlen, die Proxyeinstellungen auf Keinen Proxyserver verwenden zu setzen.

Optional können Sie ein zweites Update-Profil (extern) erstellen, um ein duales Update zu konfigurieren. Rechtsklicken Sie das vorhandene Profil und erstellen ein neues. Tragen Sie in dieses Profil Benutzername und Passwort ein. Anschließend konfigurieren Sie im Standard-Task Automatische Updates in festen Zeitabständen das Primäre Profil auf Eigenes Profil und das Sekundäre Profil auf extern. [SOLN3036]



3.1.2 Konfiguration von ESET File Security

Sie können die unterstützten Dienste der Automatischen Ausschlüsse einsehen und konfigurieren. [SOLN3078]

Prüfen der Netzlaufwerke sollte deaktiviert werden.

Das Prüfen von Anwendungsprotokollen ist standardmäßig deaktiviert. [SOLN2567]

Das Update-Profil (Eigenes Profil) konfigurieren Sie so, dass alle ESET File Security Updates von dem Update-Mirror erhalten. Tragen Sie dazu http://server:2221 als Update-Server ein, wobei „server“ Ihr Servername, bzw. Server-IP-Adresse ist. Wir empfehlen, die Proxyeinstellungen auf Keinen Proxyserver verwenden zu setzen.

ESET-Sicherheitsprodukte prüfen auf Vollständigkeit der Windows-Updates. Die Prüfung auf fehlende Kritische Updates kann über Ändern auf Keine Updates deaktiviert werden.

3.1.3 Konfiguration von ESET Mail Security

In der Whitelist für Zugelassene Absender können E-Mail-Adressen und / oder E-Mail-Domänen eingetragen werden.

Die Hintergrundprüfung für die automatische Prüfung der Postfachdatenbank sollte deaktiviert werden. Die Stufe der Hintergrundprüfung setzen Sie auf Nachrichten aus der letzten Woche.

Um Spam-Mails an den Empfänger mit [ESETSPAM] weiterzuleiten, ändern Sie die Aktion für Spam-Mails auf Keine Aktion.

Prüfen der Netzlaufwerke sollte deaktiviert werden.

ESET Mail Security muss Updates von den ESET-Servern erhalten, da ausschließlich diese Server Signaturen für Antispamdefinitionen bereithalten. Tragen Sie dazu Benutzername und Passwort aus Ihrer Lizenzmail ein.

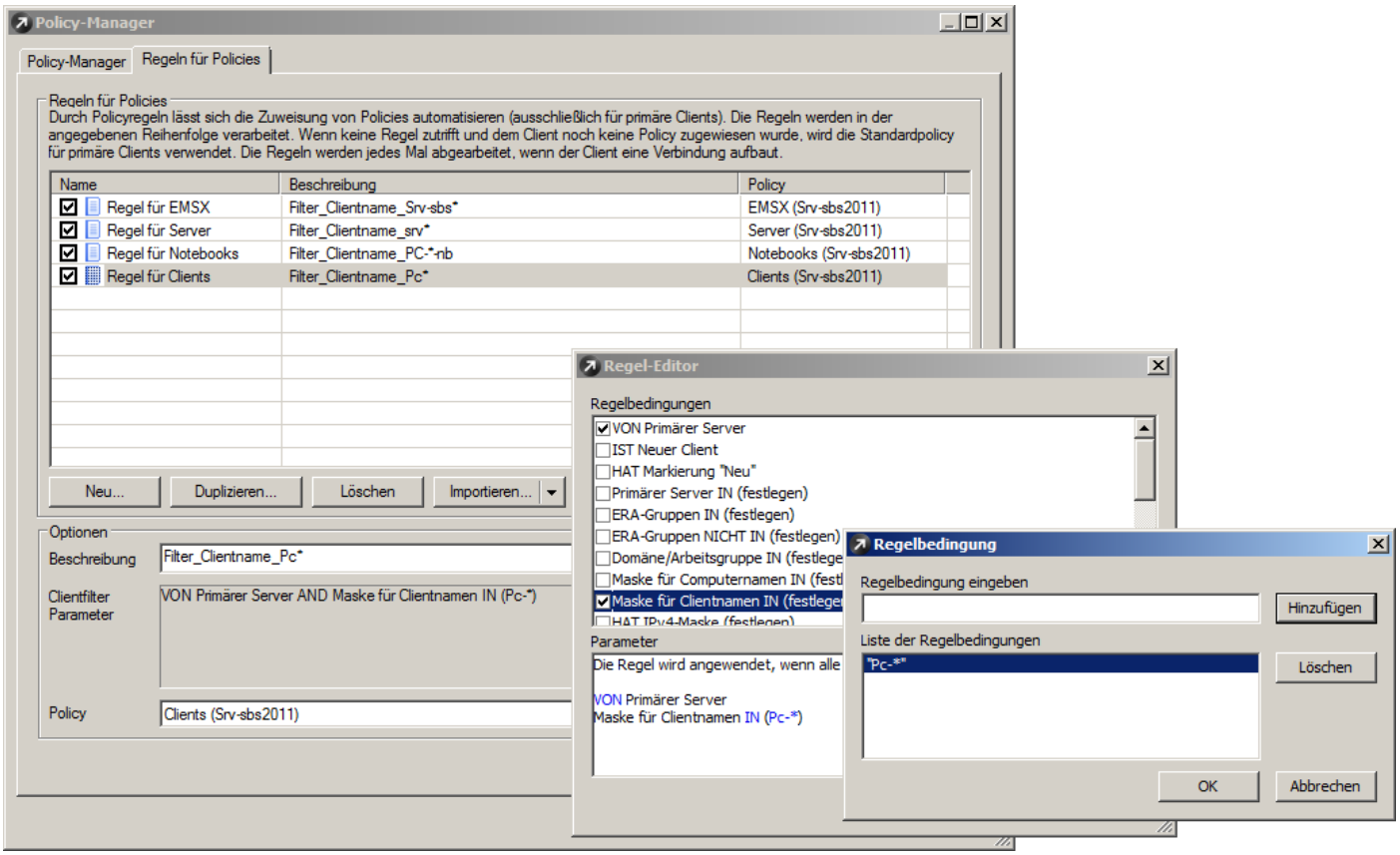
3.2 Regeln für Policies

Mit dem Werkzeug Regeln für Policies können Sie als Administrator die Zuweisung von Policies zu Clients umfassend und komfortabel automatisieren.

Zum Erstellen und Verwalten von Policyregeln gibt es eine eigene Registerkarte im Policy-Manager. Policyregeln werden von oben nach unten abgearbeitet. Demnach sollten spezielle Regeln oben, allgemeine Regeln unten erstellt werden. Um eine neue Regel zu erstellen, klicken Sie auf Neu. Tragen Sie dann die gewünschten Werte in die Felder Name, Beschreibung, Clientfilter-Parameter sowie Policy ein (letzteres ist die Policy, die den Clients zugewiesen wird, die die angegebenen Kriterien erfüllen).

Um die Filterkriterien zu konfigurieren, klicken Sie auf Bearbeiten.

In den meisten Fällen ist die automatische Zuordnung von Clients in Policies durch Clientname oder IP-Adresse möglich. Wählen Sie Maske für Clientname IN um die Zuordnung nach Clientnamen durchzuführen. In Regelbedingungen von Policyregeln können Sie Platzhalter verwenden, beispielsweise PC-* bei einer Workstation-Policy oder Srv-* bei einer Server-Policy.



Sobald Sie alle Policy-Regeln für die zugehörigen Policies erstellt haben, können Sie den Policy-Manager schließen und alle Clients werden fortan automatisch anhand dieser Policy-Regeln den zugehörigen Policies zugeordnet.

Sollten im ESET Remote Administrator Clients verbunden sein, die nicht über eine Policy-Regel in eine Policy zugeordnet werden können, so werden sie automatisch der Standardpolicy für primäre Clients zugeordnet.

Sie können beliebig viele Regelbedingungen miteinander kombinieren: Beispielsweise Maske für Clientname IN: „PC-*“ und HAT NICHT IPv4-Bereich: 192.168.1.20 - 192.168.1.30

Kapitel 4 Ausrollen von ESET Endpoint Software in Ihr Netzwerk

Nachdem der ESET Remote Administrator installiert, konfiguriert und für die Verwaltung von Clients vorbereitet wurde, kann nun die ESET Endpoint Software in Ihr Netzwerk ausgerollt werden. Dies mit Hilfe der Push-Installation möglich, um nicht alle Clients manuell installieren zu müssen.

Bevor Sie die Push-Installation nutzen können, müssen Sie ein Installationspaket erstellen.

Rollen Sie niemals ein Installationspaket vollkommen ohne Konfiguration aus. Der Client kann sich in diesem Fall nicht am ESET Remote Administrator Server anmelden und ist somit für die Remoteverwaltung nicht nutzbar.

4.1 Installationspaket erstellen

Zum Verwalten der Installationspakete in ESET Remote Administrator Console klicken Sie auf die Registerkarte Remoteinstallation, wählen die Registerkarte Computer, klicken dort mit der rechten Maustaste auf eine beliebige Stelle und wählen Pakete verwalten aus dem Kontextmenü. Der Installationspaket-Editor wird geöffnet.

Klicken Sie Hinzufügen… und wählen über ... eine in Abschnitt 1.4 heruntergeladene MSI-Datei aus. Alternativ können Sie die Software über Web-Download >> herunterladen (Sicherheitseinstellungen des Internet Explorers greifen).

Fügen Sie in das Paket 32-Bit und 64-Bit MSI-Dateien hinzu. Die Push-Installation erkennt die zu installierende Version und wählt diese automatisch aus.

Um die Konfiguration zu öffnen, klicken Sie Bearbeiten. In den Einstellungen für Remote Administration ändern Sie den Wert des Intervalls für Verbindungsaufnahme zum Server auf 1, um die automatische Zuordnung der Clients in die korrekte Policy über Policy-Regeln zu beschleunigen.

Wenn Sie ein Paket für ESET Endpoint Security erstellt haben, setzen Sie in der Kategorie Personal Firewall den Wert für Dialog zum Festlegen der Schutzmodus-Einstellungen des Computers im Netzwerk nicht mehr anzeigen auf Ja, um Kommunikationsprobleme zwischen ESET Endpoint Security und ESET Remote Administrator Server zu vermeiden.

Über Speichern unter… können Sie das Paket abspeichern. Wir empfehlen, dem Paket einen aussagekräftigen Namen zu geben, beispielsweise „*ESET Endpoint Antivirus* 5.0.2205.6“.

4.2 Installationspaket ausrollen

Zuerst müssen Sie die Clients anzeigen lassen, die Sie installieren möchten. Klicken Sie Remoteinstallation und wählen den Standard-Suchtask. Dieser Suchtask sollte Ihnen bereits alle Computerkonten des Active Directory anzeigen, andernfalls klicken Sie Ausführen.

- Nur nicht registrierte Computer anzeigen blendet alle bereits installierten ESET-Clients aus.
- Sie können über das Kontextmenü eine Diagnose vor Push-Installation für Windows ausführen, um alle Installations-Voraussetzungen zu testen. [SOLN82]
- Sie können einzelne Clients manuell hinzufügen, indem Sie eine Neue Suche… erstellen und in der Benutzerdefinierten Computerliste eine Liste mit IP-Adressen hinzufügen.

Markieren Sie mit gedrückter STRG-Taste alle Computer, die Sie dasselbe Installationspaket erhalten sollen und wählen nach einem Rechtsklick im Kontextmenü Push-Installation für Windows. Wenn Sie wie in Abschnitt 2.3.3 die Dienstanmeldung geändert haben, können Sie die erneute Eingabe von Benutzername und Passwort überspringen. Wählen Sie unter Name das zu installierende Installationspaket aus, beispielsweise *„ESET Endpoint Antivirus* 5.0.2205.6*“.* Im letzten Schritt definieren Sie den Ausführungszeitpunkt der Installation.

- Seit Version 4.2 der ESET-Sicherheitsprodukte können vorhandene ESET-Clients über die Funktion Upgrade für Windows-Clients aktualisiert werden. Das gilt für Major-Releases von 4.2 auf 5.0, sowie für Minor-Releases von 5.0.x auf 5.0.y.

Sie können die Remoteinstallation alternativ per Gruppenrichtlinien des Active Directory durchführen. [SOLN2185]

Vielen Dank, dass Sie sich für ESET entschieden haben