Digital Security
Progress. Protected.

Anleitung:

MICROSOFT EXCHANGE POC

ESET.DE | ESET.AT | ESET.CH

Inhaltsverzeichnis

Beschreibung **des MS Exchange PoC**

Der MS Exchange PoC umfasst eine komplette Installation mit einem potentiellen Neukunden, der seine Exchange Server damit absichern möchte. Wir zeigen Ihnen, welche Möglichkeiten unsere Lösung beinhaltet und richten das Produkt entweder in einer Stand Alone Umgebung (ohne ESET PROTECT) oder in einer verwalteten Umgebung mit dem ESET PROTECT ein.

Zur Grundkonfiguration gehört auch, ein Regelwerk mit dem Kunden zu definieren, welche Postfächer in die Exchange Datenbank nach Malware gescannt werden. Darüber hinaus sichern wir auch die eingehenden E-Mails ab und scannen nach Malware und Spam. Die blockierten Objekte landen in der Quarantäne und wie diese im täglichen Umfeld bedient wird, zeigen wir ebenfalls in diesem Dokument.

Installation der Sicherheitslösung **für die ESET Mailsecurity for Exchange**

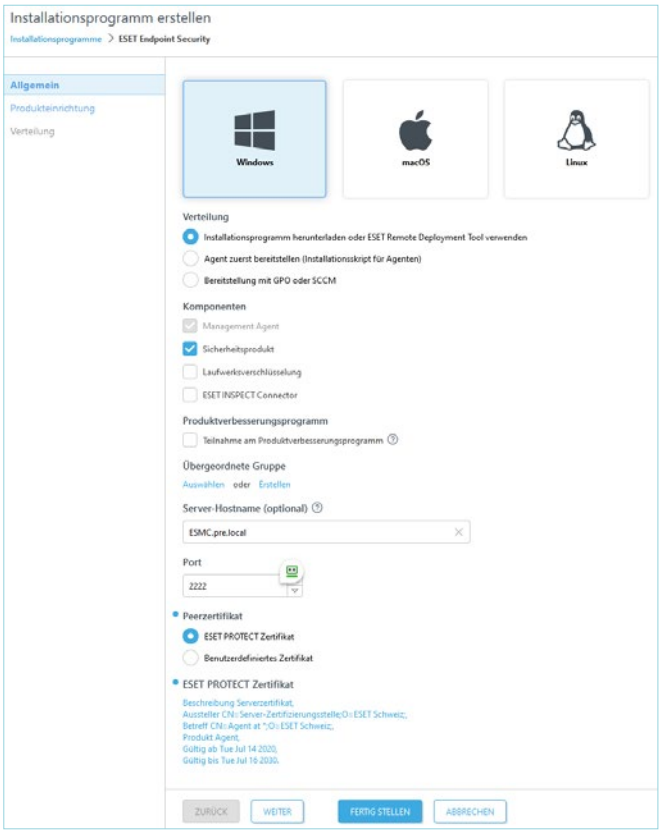
Die Installation kann auf den 3 möglichen Wegen erfolgen.

1. Erstellen eines Installers im ESET PROTECT
2. MSI direkt runterladen und installieren
3. Installation durch die Aktivierung des Cluster-Modus

Erstellen eines Installer im ESET PROTECT

Kunden, welche die Exchange Server über ESET PROTECT verwalten, können die Lösung direkt als Installer oder per Task auf die Server verteilen.

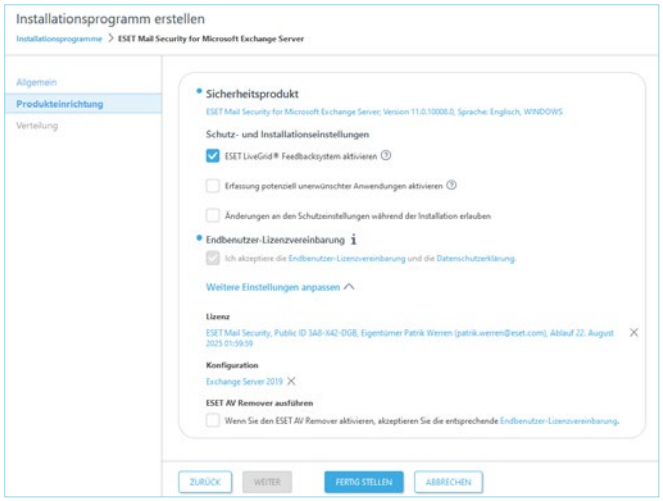
Gehen Sie hierzu auf *Installationsprogramme* und klicken auf *Installationsprogramm erstellen*. Im Anschluss öffnet sich diese Maske:



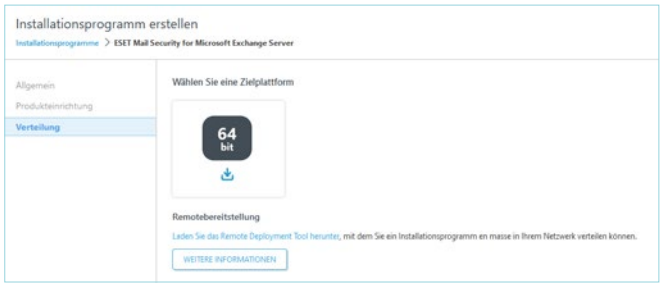
Konfigurieren Sie den Installer anhand dieser Maske mit Ihren vorgegebenen Einstellungen. Klicken Sie danach auf *Weiter*.

In der nächsten Maske wählen wir bei Sicherheitsprodukt den aktuellen Exchange Schutz und die gewünschte Sprache aus. Die Lizenz wird automatisch von ESET PROTECT ausgewählt.

Wenn Sie bereits eine Konfiguration für die ESET Mailsecurity for Exchange haben, kann sie hier hinterlegt werden.

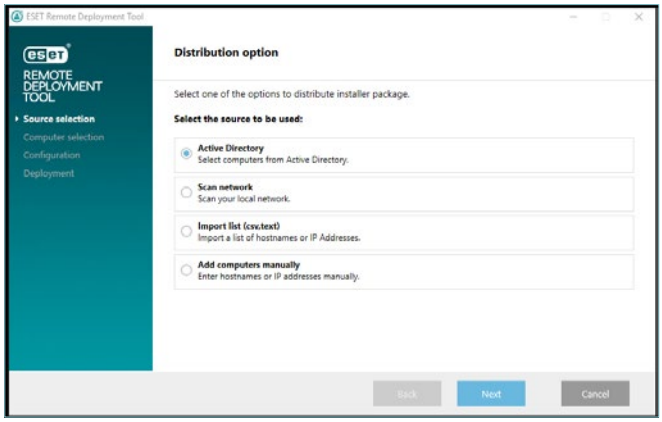


Klicken Sie auf *Fertig Stellen*, danach kann der Installer als 64-bit Version runtergeladen werden.



Sie können den Installer direkt auf die Server verteilen und mit einem *Doppelklick* ausführen. Das ist der schnellste Weg, wenn Sie nur wenige Exchange Server damit ausrollen möchten.

Bei einer größeren Anzahl Exchange Server können Sie den Installer auch über das ESET Remote Deployment Tool verteilen. ↗Link



Das Tool bietet die Möglichkeit, die Exchange Server über das Active Directory auszuwählen, was wir auch empfehlen. Alternativ können Sie die SharePoint Server über eine csv Liste oder von Hand erstellen, was allerdings einen erheblichen Mehraufwand für Sie bedeutet.

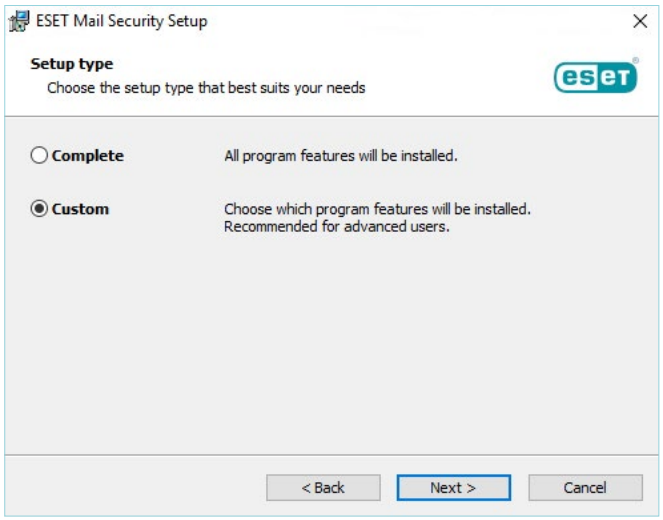
MSI direkt runterladen und installieren

Über den folgenden Link ist es möglich, den ESET Mail Security für Exchange Installer direkt von unserer Webseite herunterzuladen:

↗www.eset.com/ch-de/business/download/mail-security-exchange/

Mittels der MSI-Datei können Sie die Installation anpassen, sowohl die Komponenten, die Sie installieren möchten als auch die Installationspfade.

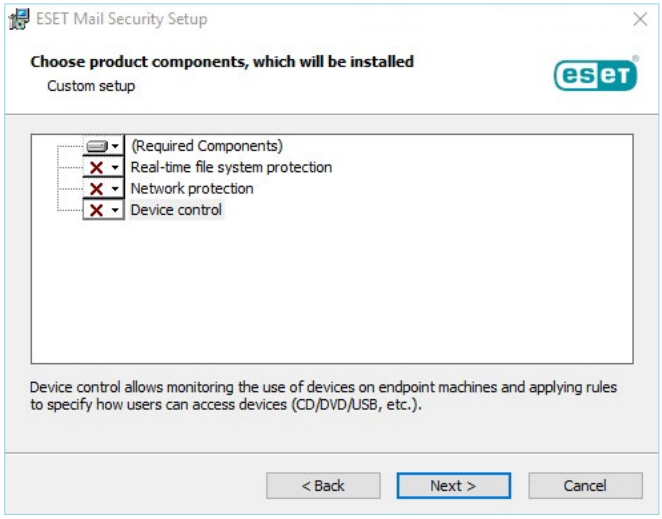
Klicken Sie auf *Next*.



Im zweiten Schritt, geben wir an, ob die Installation *Vollständig* oder *Benutzerdefiniert* erfolgen soll.

Falls Sie die bestehende Sicherheitslösung für den MS Exchange Server beibehalten möchten und von ESET nur die Exchange Applikation absichern wollen, dann ist eine benutzerdefinierte Installation erforderlich.

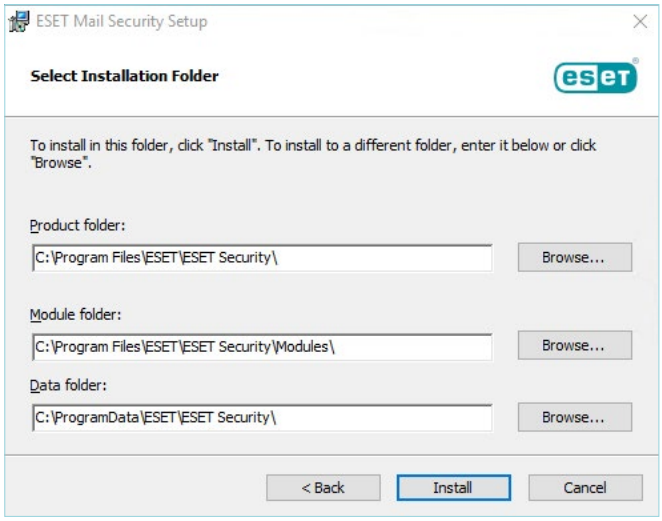
In diesem Fall wählen Sie *Benutzerdefiniert* und klicken auf *Weiter.*



Deaktivieren Sie folgende Komponenten:

1. Echtzeit-Dateischutz
2. Netzwerk-Schutz
3. Gerätesteuerung

Danach klicken Sie auf *Weiter.*



Im letzten Schritt besteht die Möglichkeit, die ESET Mailsecurity Exchange auf einem anderen Laufwerk als auf dem C:\-Laufwerk zu installieren, z. B. auf einem lokalen D:\-Laufwerk. Beachten Sie, dass Netzlaufwerke werden NICHT unterstützt werden.

Installation durch die Aktivierung des Cluster-Modus

Mit der Aktivierung des Cluster-Modus, wird auf sämtlichen ausgewählten Exchange Servern der ESET Schutz ausgerollt, falls er noch nicht installiert ist. Bei dieser Form der Einrichtung ist es erforderlich die ESET Software auf dem primären Exchange zu installieren und anschließend den Cluster-Modus zu aktivieren. Auf der nachfolgenden Seite finden Sie alle Informationen zum Cluster-Modus.

Konfiguration im PROTECT oder **im lokalen ESET Mailsecurity GUI**

Die Konfiguration für die ESET Mailsecurity for Exchange kann entweder über das ESET PROTECT Management oder lokal im GUI erfolgen.

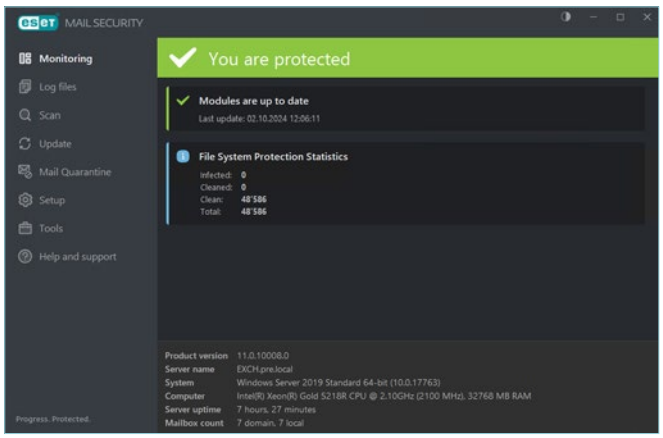
ESET PROTECT: Das Management repliziert regelmäßig die Mailsecurity for Exchange Policy auf sämtliche Exchange Server.

Lokales ESET Mailsecurity for Exchange GUI: Möchte der Kunde kein zentrales Management einsetzen, kann die Policy auch lokal in der GUI der ESET Mailsecurity for Exchange konfiguriert werden. Die Replikation der Policy auf sämtliche Exchange Server übernimmt der ESET Cluster-Modus.

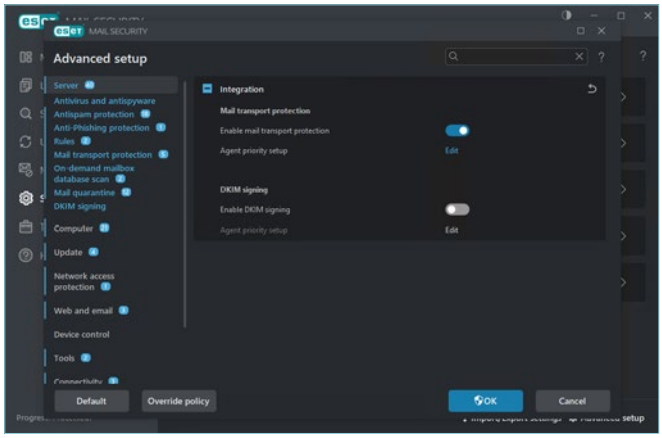
Es spielt dabei keine Rolle, auf welchem Server die Policy angepasst wird. Sobald auf einem Exchange Server eine Änderung an der Policy vorgenommen wird, ändert sich die Policy automatisch auf sämtlichen Exchange Servern.

Erklärung der wichtigsten **Einstellungen im ESET Exchange GUI**

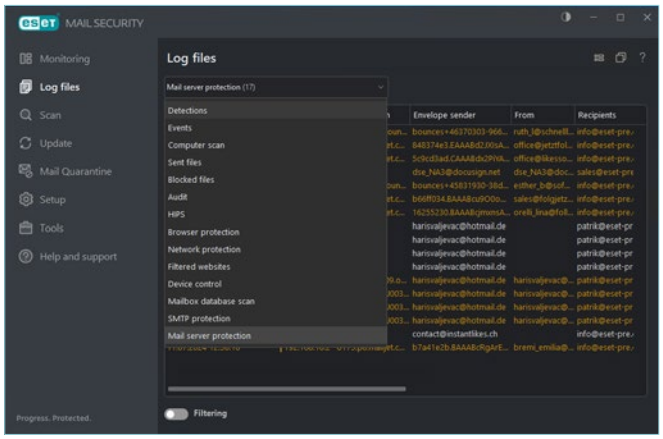
Ohne das zentrale Management ESET PROTECT lassen sich die meisten Einstellungen direkt auf den Exchange Servern einstellen. Wir zeigen diese Themen kurz in der Demo auf.



In der ESET Mail Security for Exchange sehen Sie beim Reiter *Monitoring* den aktuellen Zustand der Module und die Statistiken zum Dateisystemschutz.



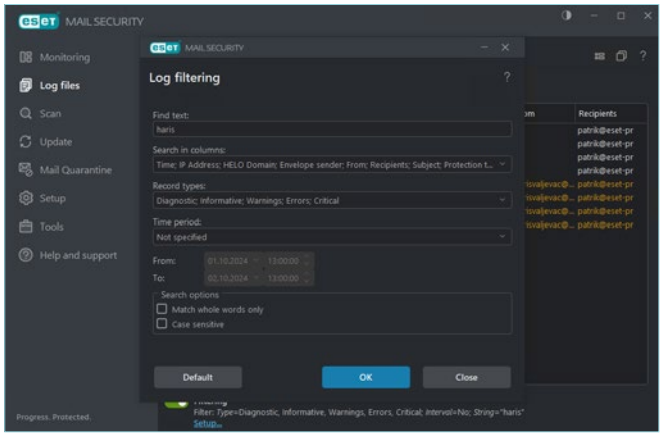
Die wichtigste Einstellung für den PoC ist die Aktivierung der Mail transport protection. Damit ist die ESET Sicherheitslösung in der Lage E-Mails, welche den Server erreichen, vor Speicherung in der Exchange Datenbank nach Malware zu scannen.



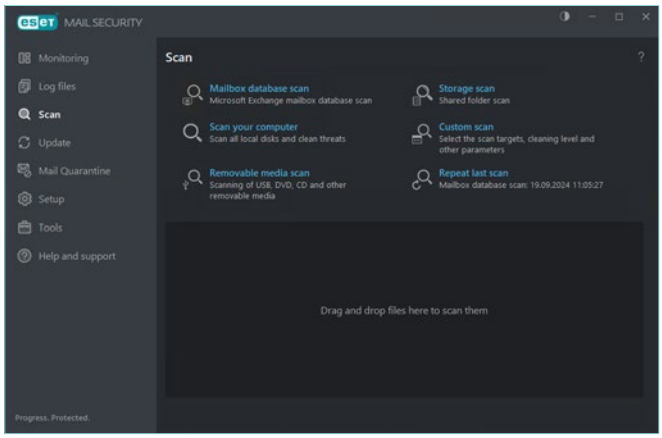
Im Bereich *Log files* finden wir folgende wichtige Reiter in Bezug auf die E-Mail Security:

- Sent files – Alle Dateien, welche in der ESET Cloud Sandbox analysiert werden
- Mailbox database scan – Informationen zu jedem einzelnen Mail Datenbank Scan
- SMTP protection – Zum Beispiel als Spam klassifizierte E-Mails anhand dem SPF
- Mail server protection – Sämtliche E-Mails die abgefangen wurden, mit Details der Herkunft und an welchen Benutzer sie ausgeliefert werden sollte

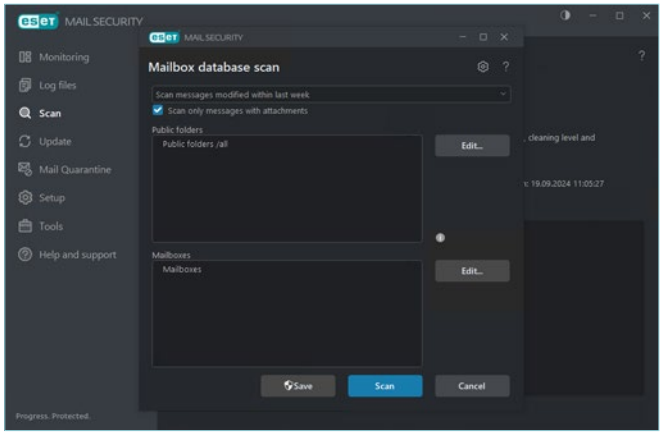
Suchen Sie gezielt nach einem Event, benutzen Sie den Filter.



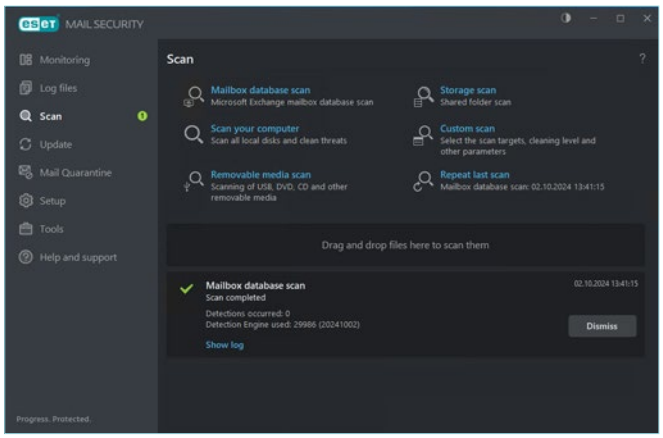
Der Log-Filter ermöglicht es nach Event-Namen, Spalten, Eintragstypen und über einen speziellen Zeitraum zu suchen.



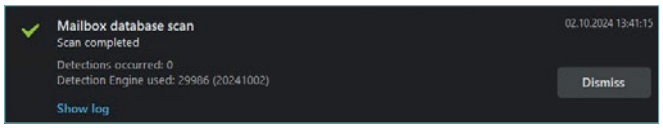
Die Mail Security Datenbank kann direkt über das GUI nach Malware durchsucht werden. Wir empfehlen den zeitgesteuerten Scan über einen Task.



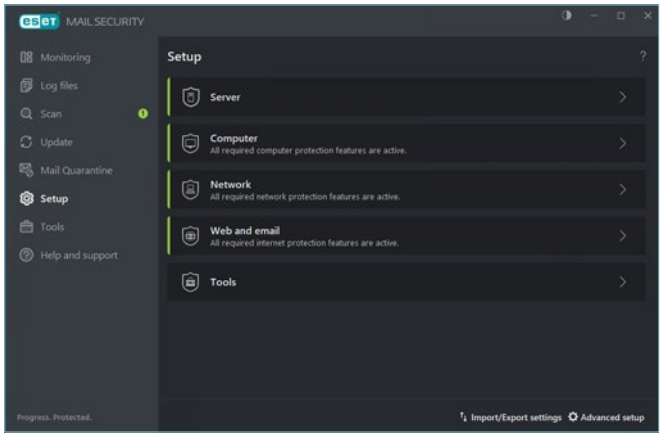
Beim manuellen Scan ist es möglich, sämtliche E-Mails oder nur jene mit Anhang zu prüfen. Ebenfalls werden bei einem Scan die *Public folder* und die *Mailboxes* nach Malware durchsucht. Über *Edit* lassen sich die Public Folder und die Mailboxen einschränken, so dass nicht alle gescannt werden.



Danach läuft die Prüfung auf Malware. Die Dauer variiert stark nach der Größe der Datenbank. Bei einer großen Datenbank kann es auch bis zu mehreren Stunden dauern.



Ist der Scan komplett abgeschlossen, erhalten Sie eine Meldung. Möchten Sie den Inhalt des Scans sehen, klicken Sie auf *Log anzeigen*.



Wichtige Einstellungen zur Mailsecurity for Exchange finden Sie im Register Server.

Regeln – **Postfachdatenbankschutz**

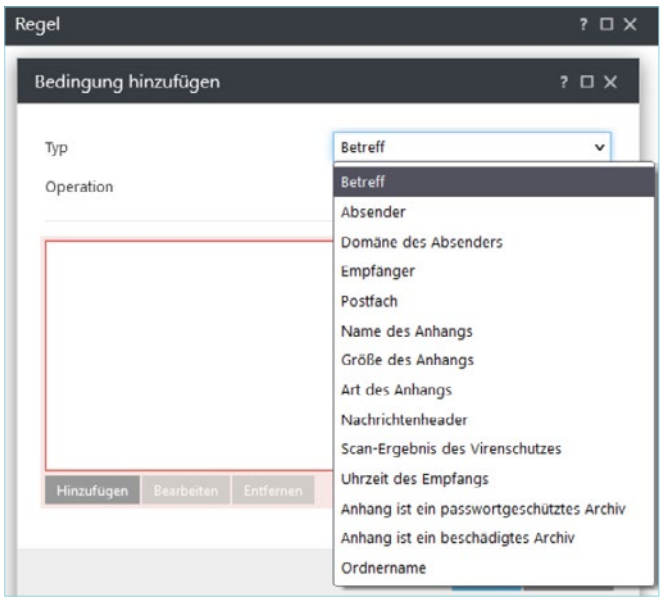
Die Regeln für den Postfachdatenbankschutz betrifft sämtliche E-Mails, die bereits in ein Postfach zugestellt wurden. Mit den Regeln ist es möglich, nachträglich E-Mails aus den Postfächern zu entfernen.

Die Regeln enthalten immer zwei Eingabefelder:

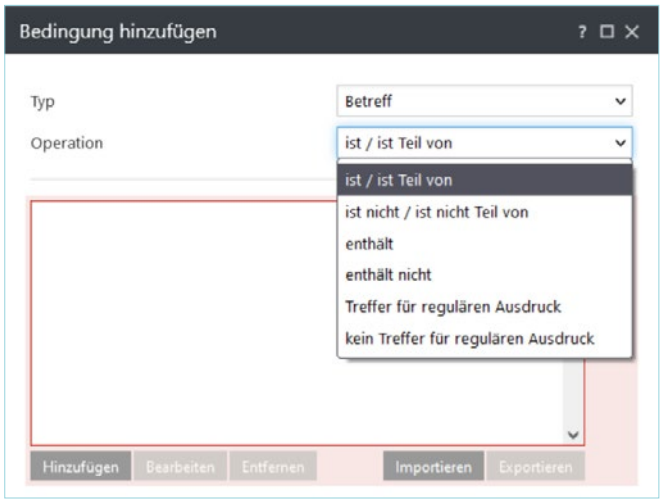
Feld Nr.1 – Bedingung: Typ und die Operation

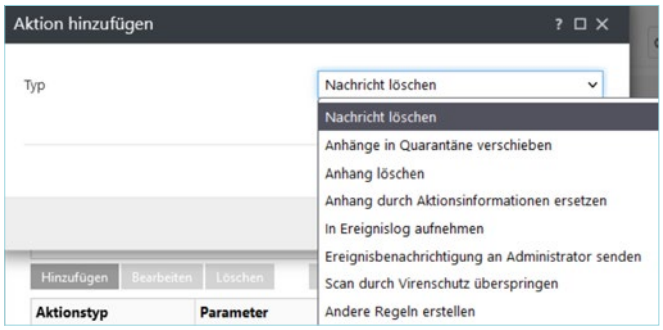
Feld Nr.2 – Aktion: Typ

Hierzu können z. B. Regeln erstellt werden, die nach einem Absender, einen Namen eines Anhangs oder auch nach einer bestimmten Uhrzeit filtern.

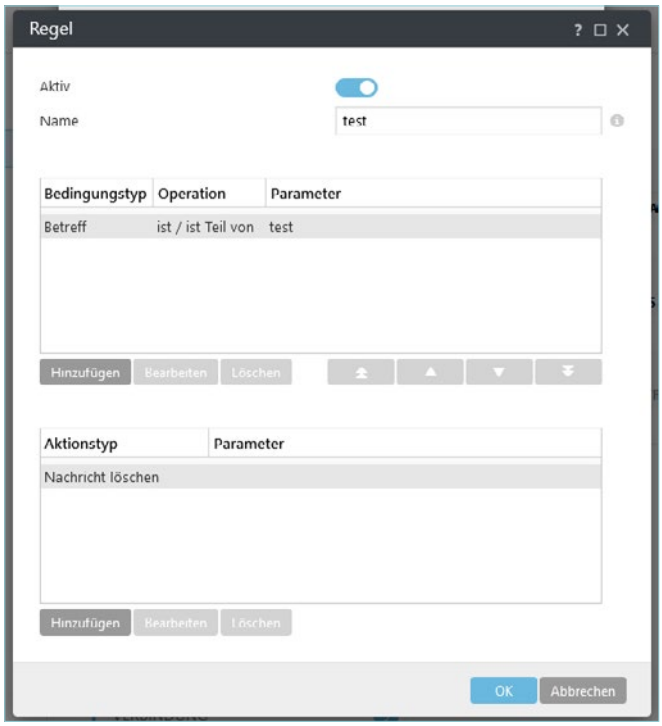


Im ersten Feld legen wir fest, nach was wir gezielt suchen.





Im zweiten Feld definieren wir die Operation wie z. B. *ist Teil von*, oder *enthält*.



In diesem Beispiel suchen wir nach sämtlichen E-Mails, in welchen *test* im Betreff steht und löschen diese.

Regeln – Mail-Transportschutz

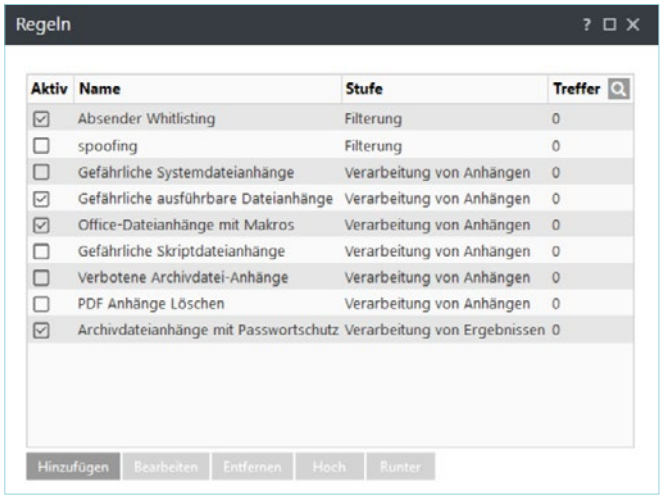
Die Regeln für den Mail-Transportschutz betrifft sämtliche E-Mails, die über den Mailtransport von extern nach innen zum Exchange-Server gelangen. Die Regeln lassen sich auch auf interne Verbindungen erweitern, wenn E-Mails zum Beispiel über mehrere Server geleitet werden.

Die Regeln enthalten immer zwei Eingabefelder:

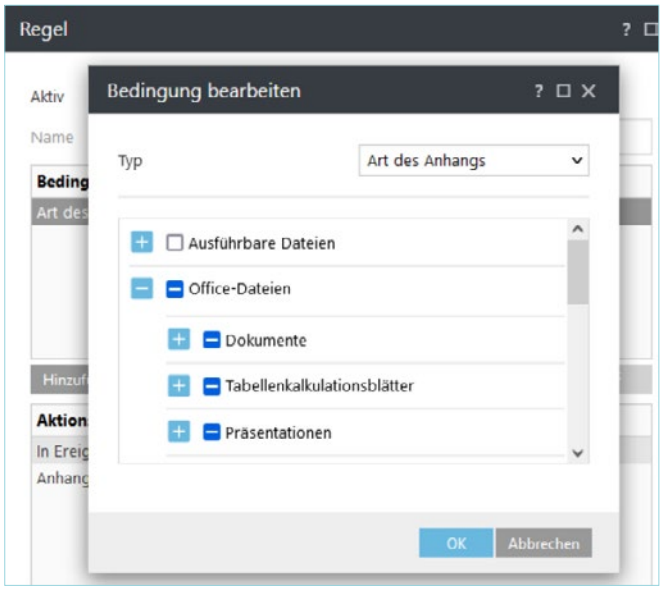
Feld Nr.1 – Bedingung: Typ und die Operation

Feld Nr.2 – Aktion: Typ

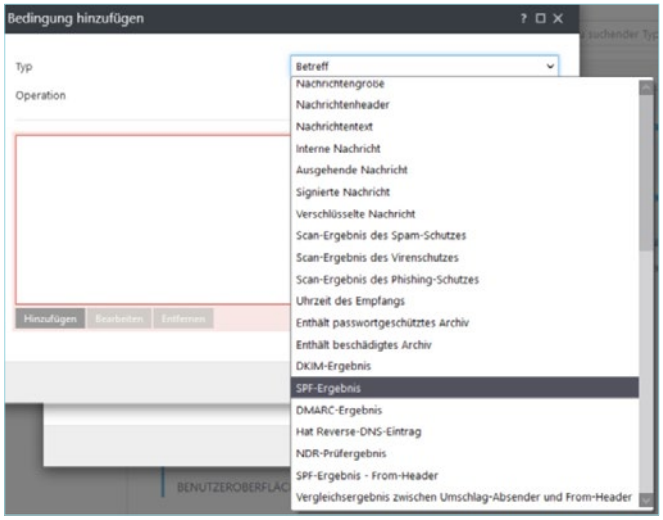
Hierzu können z. B. Regeln erstellt werden, die nach einem Absender, einen Namen eines Anhangs, oder auch nach einer bestimmten Uhrzeit filtern.



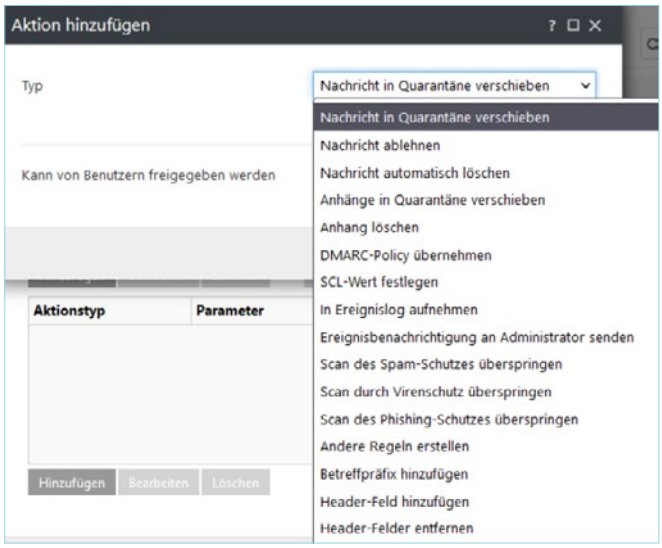
Im Regelwerk, können wir neue Regeln hinzufügen oder bestehende *ändern, aktivieren oder deaktivieren*.



In den Bedingungen ist es bspw. möglich, gezielt nach Office Dokumenten zu filtern. Angehängte Dateien werden durch das festgelegte Regelwerk in den E-Mails entfernt.

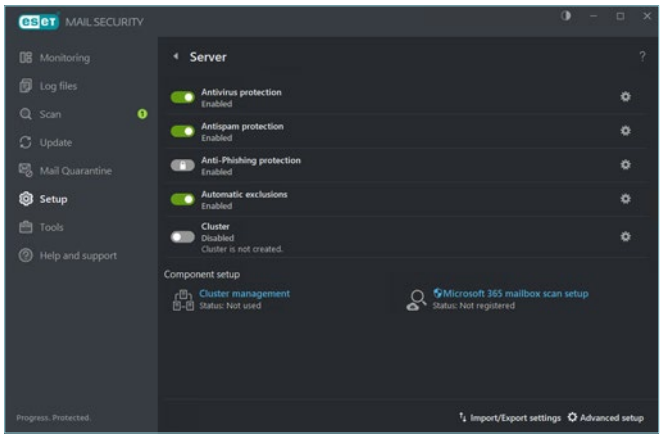


Es besteht auch die Möglichkeit, dass z. B. nach einem SPF-Ereignis gesucht wird.



Wird eine E-Mail mit einem SPF-Ereignis gefunden, kann diese abgelehnt, gelöscht oder auch in die Quarantäne verschoben werden.

Clustermodus – **Policy Synchronisation**



Im Enterprise PoC empfiehlt es sich immer den Cluster-Modus zu aktivieren.

Der ESET Cluster ist eine P2P-Kommunikationsinfrastruktur aus der ESET Produktlinie für Microsoft Windows Server.

Diese Infrastruktur ermöglicht, dass ESET Serverprodukte miteinander kommunizieren, Daten wie z. B. Konfigurationen und Benachrichtigungen austauschen und die für den ordnungsgemäßen Betrieb einer Gruppe von Produktinstanzen erforderlichen Daten synchronisieren können.

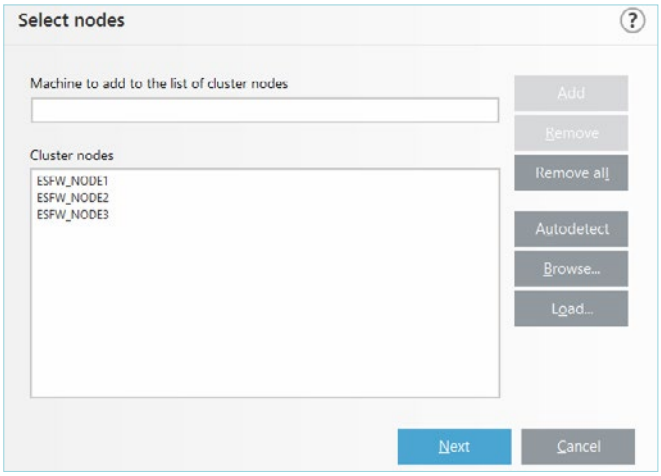
Ein Beispiel einer solchen Gruppe ist eine Knotengruppe in einem Windows-Failover-Cluster oder einem Network Load Balancing (NLB)-Cluster mit installiertem ESET Produkt, bei der das Produkt im gesamten Cluster gleich konfiguriert sein muss. ESET Cluster garantiert diese Einheitlichkeit zwischen den Instanzen.

Der Clustermodus ist für Exchange sinnvoll, um die Quarantäne zu synchronisieren. Es gibt dabei einen Quarantänen-Master, auf welchem sämtliche SPAM und Malware E-Mails gespeichert werden. Daneben wird auch die Policy auf sämtliche Exchange Server synchronisiert. Die Policy der ESET Mailsecurity for Exchange kann auf einem x-beliebigen Exchange Knotenpunkt angepasst werden. Die Änderung wird anschließend automatisch auf sämtliche Exchange Server synchronisiert.

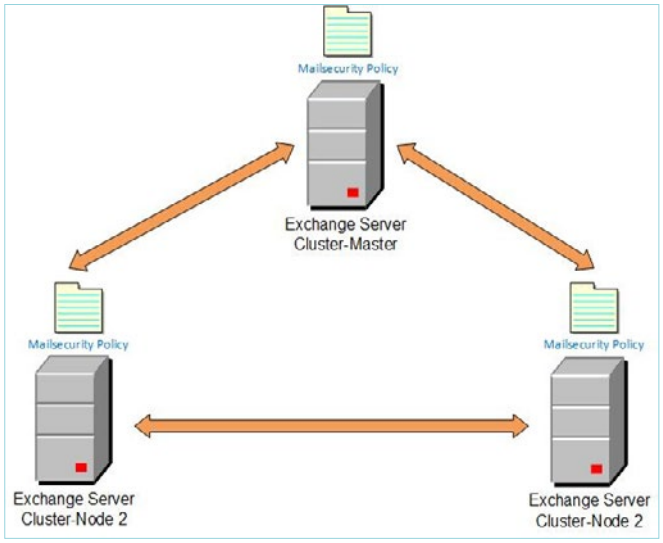
Cluster **aktivieren und konfigurieren**

1. Den Schiebregler Cluster einschalten.
2. Die Cluster-Member von Hand eintragen oder über die automatische Erkennung suchen.

   Wichtig: Der Standardport ist 9777, falls dieser Port bereits belegt ist, verwenden Sie eine andere Portnummer.



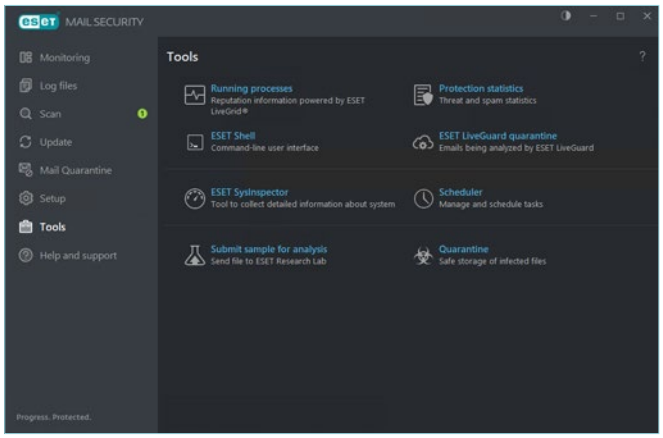
3. Klicken Sie auf *Next* und das Cluster wird automatisch gebaut. Sollte auf einem der Clusternodes noch keine ESET Mailsecurity Exchange Software installiert sein, wird diese automatisch über den Cluster Wizzard ausgerollt und installiert.



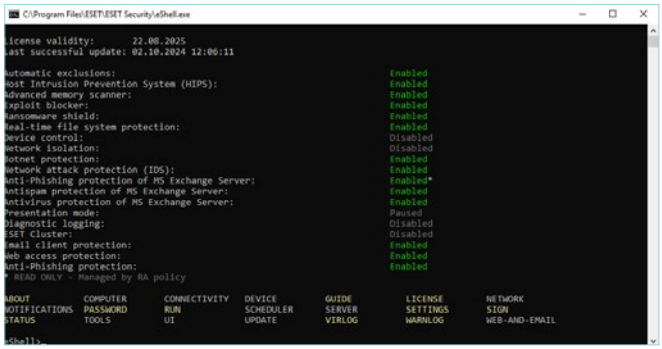
Der Quarantäne- bzw. Cluster-Master ist immer der Exchange Server, auf welchem der Cluster Wizzard initial ausgeführt wird.

Wichtig: Der Cluster-Master kann nicht an einen anderen Cluster-Node verschoben werden.

ESET Shell **Kommandos**



Unter Tools finden Sie den Taskplaner für zeitgesteuerte Exchange Mailbox Scans sowie den Aufruf der ESET Shell Kommandos:

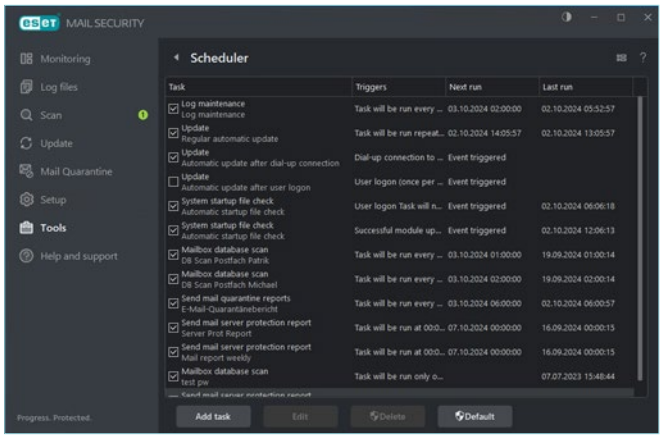


Die ESET-Shells können remote per PowerShell über einen Server Task im ESET PROTECT Management aufgerufen werden.

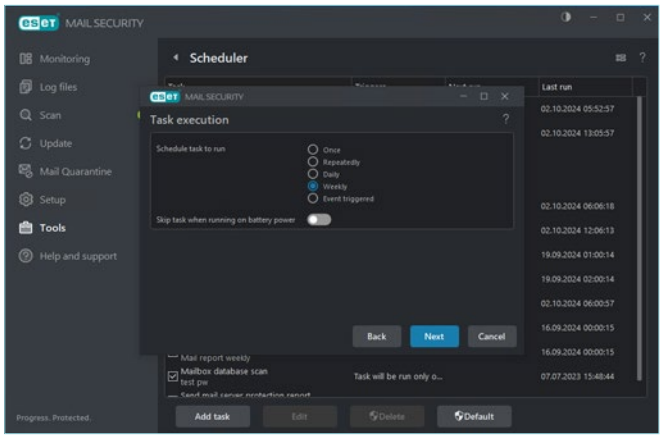
Hier finden Sie den Link zu der Beschreibung:

↗help.eset.com/eshp/11.0/de-DE/work_eshell.html

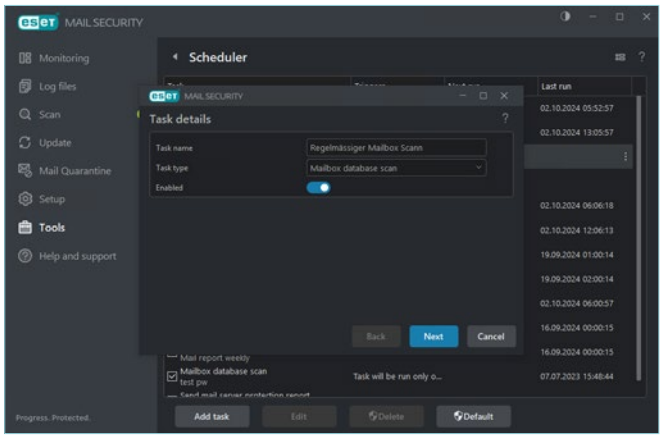
Lokale Tasks in der ESET Mailsecurity for Exchange anlegen und konfigurieren



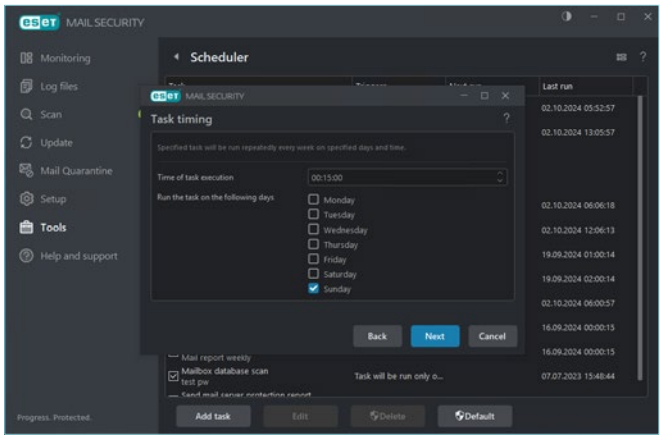
Im Taskplaner sind schon einige vorgefertigte Tasks hinterlegt, wie zum Beispiel die Log-Wartung, Update und die Prüfung der Systemstartdateien.



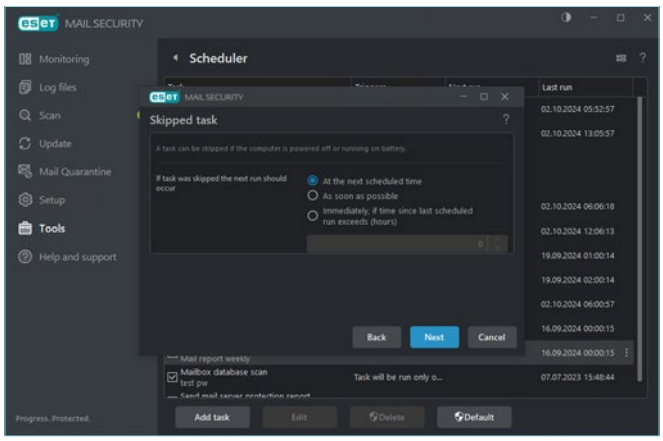
Den Mailbox Datenbank-Scan planen wir in einer wöchentlichen Ausführung.



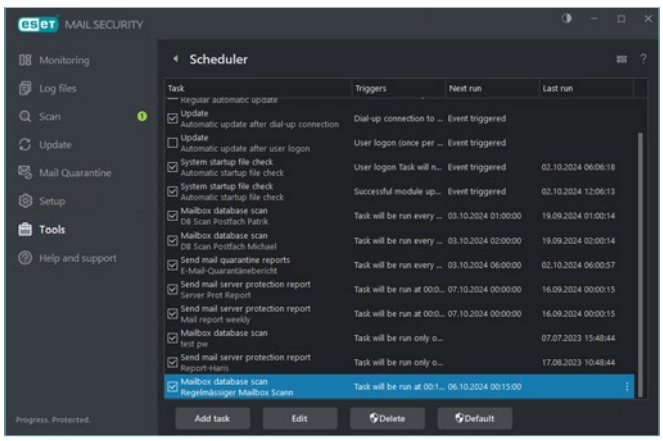
Als Beispiel erstellen wir im PoC eine Demo zum Thema Mailbox Scan. Hierzu klicken wir auf *Task hinzufügen* und vergeben in den Taskdetails einen Taskname. Bei Tasktyp wählen wir *Mailbox database scan* aus.



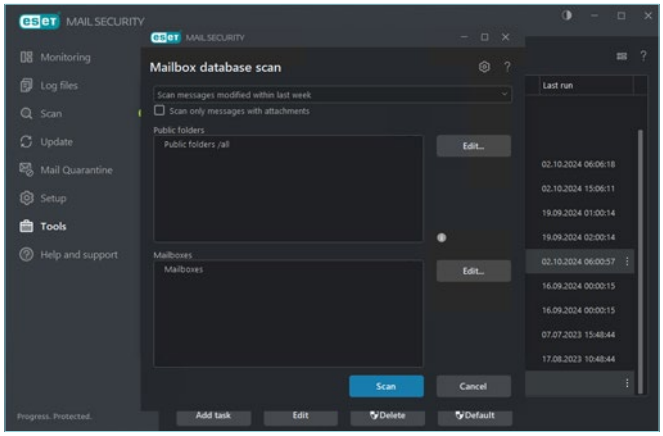
Damit der Exchange Server in der Leistung nicht beeinträchtigt wird, wird die Ausführung des Tasks auf Sonntag 00:15 Uhr gelegt.



Der Task soll zur nächsten geplanten Ausführungszeit ausgeführt werden.



Der Task wird hinzugefügt und wir finden ihn immer an unterster Stelle.



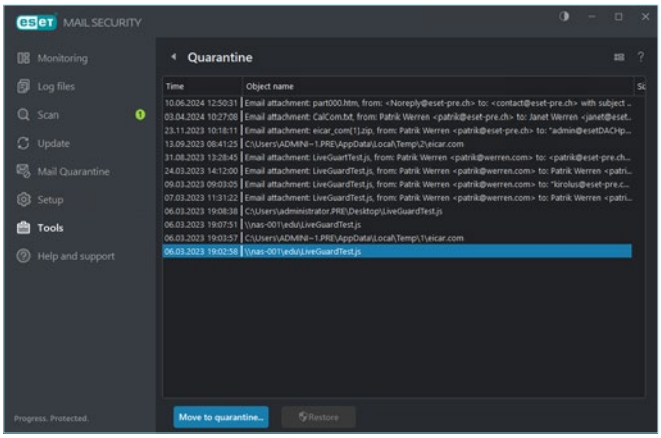
Per Default werden immer sämtliche Public Folder und alle Mailboxen gescannt. Änderungen lassen sich über *Edit* vornehmen. Damit ist es möglich die Public Folder und die Mailboxen der Mitarbeiter auszuwählen, welche gescannt werden sollen.

Lokale ESET Mailsecurity for Exchange **Quarantäne**

Sämtliche Objekte und E-Mails, welche sich in der Quarantäne befinden, können direkt auf dem Exchange Server wieder ins Postfach verschoben werden.

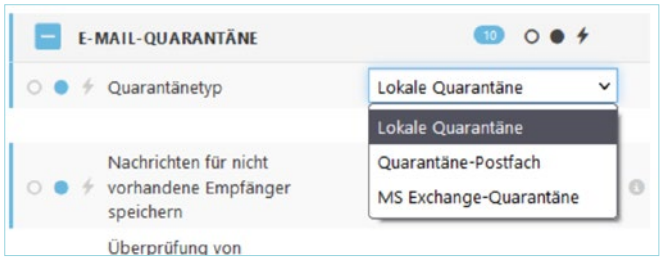
Wie oben beschrieben, liegt die Quarantäne bei einem ESET Cluster auf dem Master.

Werden die Exchange Server über ESET PROTECT verwaltet, finden Sie die Quarantäne Objekte direkt im Management und sie müssen dort freigegeben werden.



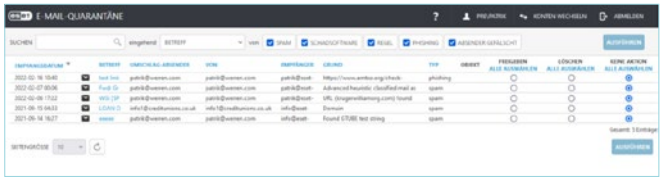
Weitere **Quarantäne Möglichkeiten**

Die ESET Mailsecurity for Exchange bietet 3 mögliche Quarantänetypen an:



Lokale Quarantäne

Die lokale Quarantäne stellt jedem ActiveDirectory Benutzer seine individuelle E-Mail-Quarantäne zur Verfügung. Zugriff hat der Benutzer über eine Web-Oberfläche, auf der er nur seine SPAM-E-Mails sieht.



Der Benutzer kann in diesem Portal als falsch klassifizierte SPAM-E-Mails selbständig freigeben. E-Mails, die Malware beinhalten, können durch den Benutzer nicht freigegeben werden. Der Exchange Administrator kann zusätzlich berechtigt werden.

Quarantäne-Postfach

ESET Mailsecurity for Exchange erstellt eine separate Wrapper-E-Mail mit zusätzlichen Informationen sowie den ursprünglichen E-Mails als Anhang, und stellt diese E-Mail ans Postfach zu.

Der SPAM-Administrator kann im Postfach die E-Mail falls nötig an die Mitarbeitenden weiterleiten. Der Mitarbeitende selbst hat keinen direkten Zugriff aufs Quarantäne-Postfach.

MS Exchange-Quarantäne

Der Exchange Server ist hierbei für die Zustellung der E-Mail ans definierte SPAM-Postfach verantwortlich. Das Postfach muss in ActiveDirectory auf der Organisationsebene als Quarantäne festgelegt werden. Sämtliche SPAM-E-Mails, die in das Postfach gelangen, werden im Original gespeichert.

Die interne Quarantäne ist in Microsoft Exchange Servern standardmäßig deaktiviert. Sie muss per nachfolgendem Power Shell-Befehl definiert und aktiviert werden:

Set-ContentFilterConfig-QuarantineMailbox name@domain.com

Konfiguration im **ESET PROTECT – NDR**

NDR steht für Non Delivery Report und ist eine Reaktion auf eine E-Mail die nicht zugestellt werden kann. Folgende Fehlermeldungen werden dabei vom E-Mail-Server ausgegeben:

- Zieldomäne nicht erreichbar
- Zielpostfach nicht erreichbar / existent
- Zielpostfach voll
- Zielsystem lehnt Mail ab

Der E-Mail-Server vom Absender muss so eingestellt sein, dass er NDR annimmt. Aus Sicht eines Spammers können Rückschlüsse gezogen werden, ob eine E-Mail auch tatsächlich ankommt. Er kann so einen Empfänger als positiv markieren und in weitere SPAM-Datenbanken als verifiziert integrieren.

Spammer tarnen auch teilweise Nachrichten als NDR, in der Hoffnung, dass sie vom Empfänger geöffnet werden.

NDR ist sinnvoll, es sollte aber gut überlegt sein, was Sie dem Absender übermitteln.

In der ESET Mailsecurity for Exchange kann NDR im Bereich Backscatter-Schutz aktiviert werden. Hierzu wird ein frei erfundener Signatur-Seed hinterlegt.

Die ESET Mailsecurity for Exchange prüft sämtliche NDR-Nachrichten, ob der Signatur-Seed vorhanden ist. Kommen gefälschte NDR-Nachrichten ohne den Signatur-Seed an, werden diese automatisch als SPAM klassifiziert und in die Quarantäne verschoben.

Konfiguration in **ESET PROTECT – DKIM**

DomainKeys Identified Mail (DKIM) ist eine Methode zur E-Mail-Authentifizierung. Sie verhindert, dass sich Spammer und andere böswillige Parteien als legitime Domain ausgeben.

Alle E-Mail-Adressen haben eine Domain – das ist der Teil der Adresse, der nach dem „@"-Symbol kommt. Spammer und Angreifer versuchen, sich beim Senden von E-Mails als eine Domain auszugeben, um Phishing-Angriffe oder andere betrügerische Aktivitäten durchzuführen.

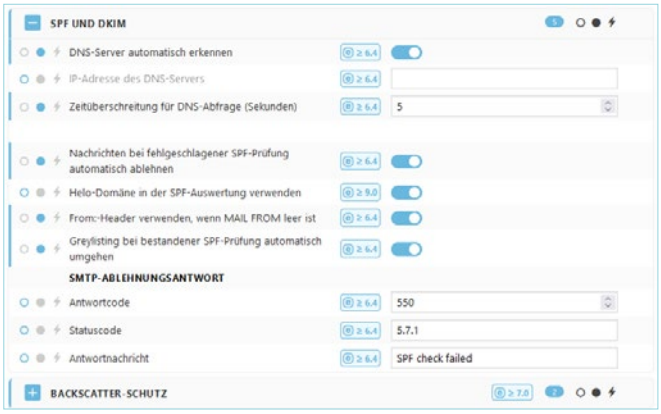
Angenommen, Chuck möchte Alice dazu bringen, ihm vertrauliche Unternehmensinformationen zu schicken. Alice arbeitet bei example.com. Also schickt er ihr eine E-Mail, die angeblich von *bob@example.com* stammt, damit sie glaubt, dass er auch für example.com arbeitet.

DKIM in Verbindung mit Sender Policy Framework (SPF) und Domain-based Message Authentication Reporting and Conformance (DMARC) macht es Angreifern viel schwerer, sich auf diese Weise als Domains auszugeben. E-Mails, die DKIM und SPF nicht bestehen, werden als „Spam" markiert oder von E-Mail-Servern gar nicht erst zugestellt. Wenn example.com DKIM, SPF und DMARC für ihre Domain eingerichtet hat, wird Alice die böswillige E-Mail von

Chuck wahrscheinlich nie lesen, da sie entweder in ihrem Spam-Ordner landet oder vom E-Mail-Server ganz abgelehnt wird.

DKIM wird dabei über einen Record Generator erstellt. Der Public Key wird anschließend auf dem E-Mail-Server abgelegt.

Konfigurationsmöglichkeiten in der ESET Mailsecurity for Exchange



ESET prüft dabei, ob die SPF-Prüfung erfolgreich war, oder nicht. Im zweiten Fall wird die E-Mail automatisch als SPAM klassifiziert und in die Quarantäne geschoben.

Konfiguration in **ESET PROTECT – SPF**

SPF steht für Sender Policy Framework.

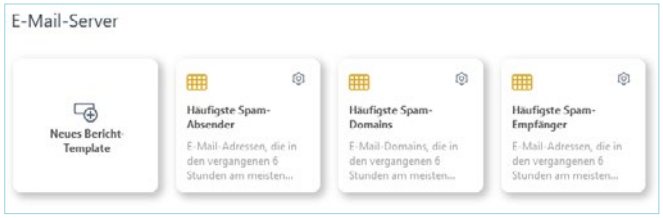
Der empfangende E-Mailserver prüft die Echtheit von Absenderadressen anhand einer IP-Adresse, welche er über den SPF-Record abfragen kann.

Befindet sich die sendende IP-Adresse auf der Liste, wird die E-Mail durch den E-Mailserver angenommen.

Bitte seien Sie sich bewusst, dass SPF nicht vor Spoofing schützt. Ein Betrüger kann trotzdem einen falschen Absender in der E-Mail anzeigen.

ESET Mailsecurity for Exchange **Berichte**

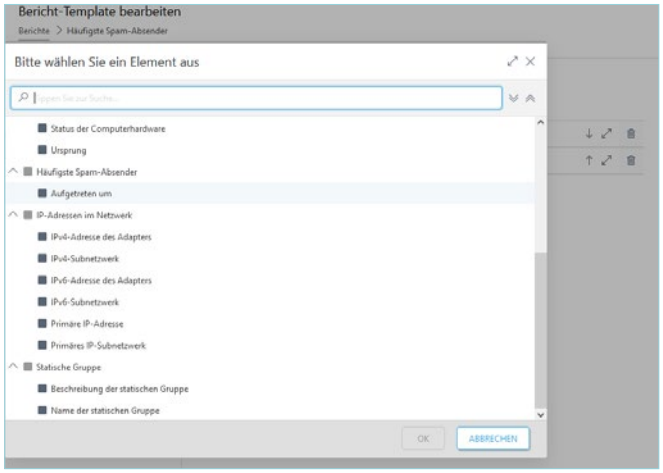
In ESET PROTECT gibt es 3 Berichte zur E-Mail-Quarantäne. Sie finden sie im Reiter *E-Mail-Server*:



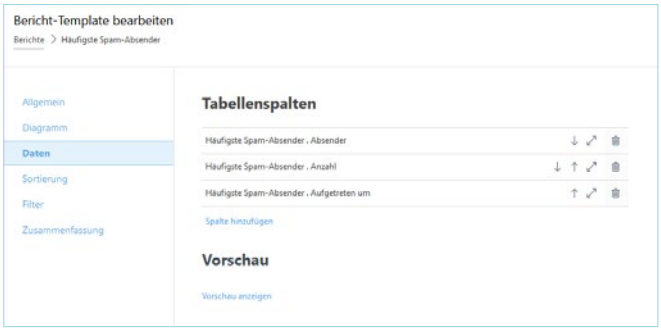
1. Häufigste Spam-Absender
2. Häufigste Spam-Domains
3. Häufigste Spam-Empfänger

Die Berichte können angepasst, bzw. erweitert werden. Hierzu klicken Sie auf das Zahnrad oberhalb des Berichtes und wählen *bearbeiten* aus.

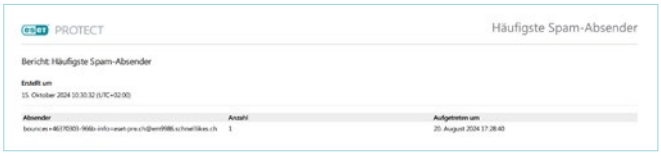
In diesem Beispiel erweitern wir die Tabelle um den Wert *Aufgetreten um*. So haben wir im Quarantäne Bericht zusätzlich die Uhrzeit.



Sobald der Wert selektiert ist, wird die Tabelle auf drei Tabellenspalten erweitert.



Der Bericht sieht im Anschluss folgendermaßen aus:



ÜBER ESET

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

Unsere Endpoint Detection and Response-Lösung, dedizierte Services wie z.B. Managed Detection and Response und Frühwarnsysteme in Form von Threat Intelligence ergänzen das Angebot im Hinblick auf Incident Management sowie den Schutz vor gezielter Cyberkriminalität und APTs. Dabei setzt ESET nicht allein auf modernste KI-Technologie, 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

BVB 09 CHAMPION PARTNER

Seit 2019 ein starkes Team
auf dem Platz und digital

Allianz Suisse

Seit 2016 durch ESET geschützt
Mehr als 4.000 Postfächer

ISP Security Partner seit 2008
2 Millionen Kunden

BEWÄHRT

Secur|Ty made in EU
Trust Seal www.teletrust.de/itsmie

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

ISO 9001 SYSTEM CERTIFICATION SGS
ISO/IEC 27001 SYSTEM CERTIFICATION SGS

Unsere Lösungen sind nach den Qualitäts- und Informationssicherheitsstandards ISO 9001:2015 und ISO/IEC 27001:2022 zertifiziert

KONTAKT

Bei Rückfragen können sich ESET Partner an die Partnerbetreuung wenden.

Tel: +49 (0) 3641 / 31 14 - 170 (Mo - Fr 8 - 17 Uhr)
E-Mail: partner@eset.de

welivesecurity by ESET
ESET Digital Security Guide