ESET Mail Security

Benutzerhandbuch

Klicken Sie hier um die Hilfe-Version dieses Dokuments anzuzeigen

Digital Security
Progress. Protected.

ESET Mail Security wurde entwickelt von ESET, spol. s r.o.

Weitere Informationen finden Sie unter https://www.eset.com.

Technischer Support: https://support.eset.com

REV. 04.08.2023

Übersicht

ESET Mail Security für Microsoft Exchange Server ist eine integrierte Lösung, die E-Mail-Server und die Postfächer von Benutzern vor Schadsoftware schützt. Dazu gehören mit Würmern oder Trojanern infizierte E-Mail-Anhänge, bosärtige Strikts in Dokumenten, Phishing-Mails, Spam, gefälschte Absender und E-Mail-Spoofing.

ESET Mail Security bietet vier Schutzarten: Virenschutz, Spam-Schutz, Phishing-Schutz und Regeln. ESET Mail Security filtert bösartige Inhalte in Postfachdatenbanken sowie auf der E-Mail-Transportebene, bevor diese das Postfach des Benutzers erreichen.

ESET Mail Security unterstützt Microsoft Exchange Server ab Version 2010 und Microsoft Exchange Server in einer Cluster-Umgebung. Bestimmte Exchange-Serverrollen (Postfach, Hub, Edge) werden ebenfalls unterstützt.

Neben dem Schutz für Microsoft Exchange Server bietet ESET Mail Security auch verschiedene Funktionen für den Schutz des eigentlichen Servers (Echtzeit-Dateischutz, Netzwerk-Schutz, Web-Schutz und E-Mail-Client-Schutz).

Mit ESET Mail Security können Sie ESET PROTECT in größeren Netzwerken zentral verwalten. Sie können ESET Mail Security auch mit externen Tools für Remoteüberwachung und Verwaltung (RMM) einsetzen.

Hauptfunktionen

Die folgende Tabelle enthält eine Liste der in ESET Mail Security verfügbaren Funktionen.

Echter 64-Bit-Produktkern	Mehr Leistung und Stabilität für die wichtigsten Produktkomponenten.
Anti-Malware	Eine preisgekrönte und innovative Verteidigung gegen Schadsoftware. Diese hochmoderne Technologie schützt Sie vor Angriffen und eliminiert alle Arten von Bedrohungen inklusive Viren, Ransomware, Rootkits, Würmer und Spyware mit cloudgestützten Scans für noch bessere Erkennungsraten. Diese genügsame Anwendung schont Ihre Systemressourcen und wirkt sich nicht negativ auf die Leistung aus. Sie verwendet ein mehrschichtiges Sicherheitsmodell. Jede Schicht, auch als Phase bezeichnet, verwendet eine Reihe von Kerntechnologien. Vor der Ausführung kommen Technologien wie UEFI-Scanner, Netzwerkangriffsschutz, Reputation & Cache, produktinterne Sandbox und DNA-Erkennungen zum Einsatz. Während der Ausführung werden Technologien wie Exploit-Blocker, Ransomware-Schutz, erweiterter Speicher-Scan und Skript-Scanner (AMSI) eingesetzt, und nach der Ausführung kommen Botnetz-Schutz, Cloud-Malware-Schutz (CMPS) und Sandboxing zum Einsatz. Diese leistungsstarke Suite von Kerntechnologien bietet Ihnen beispiellosen Schutz.

Spam-Schutz	Der Spam-Schutz ist eine zentrale Komponente für jeden Mailserver. Das in ESET Mail Security enthaltene leistungsstarke Spam-Schutz-Modul schützt Sie mit extrem hohen Erkennungsraten vor Spam und Phishing-Versuchen. ESET Mail Security ist Seriensieger des Spamfiltertests von Virus Bulletin, einer führenden Einrichtung für Sicherheitstests, und wurde bereits mehrfach mit der VBSpam+-Zertifizierung ausgezeichnet. Das Spam-Schutz-Modul erreicht eine Erkennungsrate von 99,99 % ohne jegliche falsche Positivmeldungen und ist damit Branchenführer. Der ESET Mail Security Spam-Schutz verwendet verschiedene Technologien (RBL und DNSBL, Fingerprint-Datenbanken, Reputations-Prüfung, Inhaltsanalyse, Regeln, manuell geführte White-/Blacklists, Rückläuferschutz und Nachrichtenüberprüfung mit SPF und DKIM), um optimale Erkennungsraten zu erzielen. ESET Mail Security Antispam ist cloudbasiert, und ein Großteil der Clouddatenbanken befindet sich in ESET-Rechenzentren. Die Spamschutz-Cloud ermöglicht zügige Datenupdates mit einer kürzeren Reaktionszeit beim Aufkommen neuer Spam-Inhalte.
Phishing-Schutz	Diese Funktion verhindert, dass Benutzer auf Webseiten zugreifen, die für Phishing bekannt sind. E-Mails können Links zu Phishing-Webseiten enthalten. ESET Mail Security verwendet einen ausgeklügelten Parser, um den Text und den Betreff aller eingehenden Nachrichten zu analysieren und diese Links (URLs) zu identifizieren. Die Links werden mit der Phishing-Datenbank abgeglichen.
Regeln	Administratoren können Regeln verwenden, um unerwünschte E-Mails und Anhänge gemäß der Unternehmensrichtlinie zu filtern. Anhänge wie ausführbare Dateien, Multimediadateien, passwortgeschützte Archive usw. Für gefilterte E-Mail-Nachrichten und deren Anhänge können unterschiedliche Aktionen ausgeführt werden, z. B. in die Quarantäne verschieben, löschen, Benachrichtigungen verschicken oder im Ereignis-Log protokollieren.
In Syslog-Server exportieren (Arcsight)	Der Inhalt des E-Mail-Server-Schutz-Logs kann im Common Event Format (CEF) auf einen Syslog-Server dupliziert werden, um es in Logverwaltungslösungen wie Micro Focus ArcSight zu verarbeiten. Ereignisse können über SmartConnector an ArcSight weitergeleitet oder in Dateien exportiert werden. Auf diese Weise können Sie Sicherheitsereignisse bequem zentral überwachen und verwalten. Diese Funktion ist besonders hilfreich für komplexe Infrastrukturen mit einer großen Anzahl von Microsoft Exchange Servern mit ESET Mail Security-Lösung.
Office 365-Postfachprüfung	Unternehmen können jetzt Postfächer in ihrer Exchange-Hybridumgebung in der Cloud scannen.
ESET LiveGuard Advanced	Ein cloudbasierter ESET-Dienst. Wenn ESET Mail Security eine E-Mail-Nachricht als verdächtig einstuft, wird die Nachricht vorübergehend in die ESET LiveGuard Advanced-Quarantäne verschoben. Verdächtige E-Mail-Nachrichten werden automatisch zur Analyse durch modernsten Erkennungsroutinen an den ESET LiveGuard Advanced-Server übermittelt. Anschließend erhält ESET Mail Security das Ergebnis der Analyse, und die verdächtige E-Mail-Nachricht wird entsprechend verarbeitet.
E-Mail-Quarantäne-Manager mit Weboberfläche	Administratoren können Objekte in der Quarantäne inspizieren und entweder löschen oder freigeben. Dieses Feature bietet ein benutzerfreundliches Verwaltungstool. Mit der Web-Oberfläche für die E-Mail-Quarantäne können Sie Ihre Inhalte remote verwalten. Außerdem können Sie Administratoren auswählen und/oder den Zugriff delegieren. Außerdem können die Benutzeroberfläche ihre eigenen Spamnachrichten anzeigen und verwalten, nachdem sie sich bei der Web-Oberfläche für die E-Mail-Quarantäne angemeldet haben. Dort werden nur jeweils die eigenen Nachrichten angezeigt.

E-Mail-Quarantäneberichte	Quarantäneberichte werden per E-Mail an ausgewählte Benutzer oder Administratoren verschickt und enthalten Informationen zu allen E-Mail-Nachrichten in der Quarantäne. Außerdem können die Inhalte in der Quarantäne remote verwaltet werden.
On-Demand Postfachdatenbank-Scan	Mit dem On-Demand Postfachdatenbank-Scan können Administratoren ausgewählte Postfächer manuell scannen oder einen Scan außerhalb der Geschäftszeiten planen. Der Postfachdatenbank-Scan verwendet die API der Exchange-Webdienste (Exchange Web Services oder EWS), um sich per HTTP/HTTPS mit dem Microsoft Exchange Server zu verbinden. Außerdem führt das Modul parallele Scans durch, um die Leistung zu verbessern.
ESET-Cluster	Mit dem ESET-Cluster können Sie mehrere Server von einem zentralen Ort aus verwalten. Ähnlich wie in ESET File Security für Microsoft Windows Server werden Serverknoten zu einem Cluster hinzugefügt, um die Verwaltung zu vereinfachen, indem eine Konfiguration auf alle Mitgliedsknoten des Clusters verteilt wird. Das ESET Cluster kann auch zum Synchronisieren von Greylisting-Datenbanken und der Inhalte der lokalen E-Mail-Quarantäne verwendet werden.
Ausgeschlossene Prozesse	Bestimmte Prozesse werden von der Anti-Malware-Echtzeitprüfung ausgeschlossen. Die Anti-Malware-Echtzeitprüfung kann in bestimmten Situationen Konflikte verursachen, z. B. während eines Sicherungsvorgangs oder bei Live-Migrationen von virtuellen Computern. Mit den ausgeschlossenen Prozessen können Sie die Gefahr von Konflikten minimieren und die Leistung der ausgeschlossenen Anwendungen verbessern, was sich wiederum positiv auf die Leistung und Stabilität des gesamten Systems auswirkt. Prozesse und Anwendungen werden anhand ihrer ausführbaren Datei (.exe) ausgeschlossen.
eShell (ESET-Shell)	eShell 2.0 ist jetzt in ESET Mail Security verfügbar. eShell ist eine neue Kommandozeilen-Schnittstelle mit zusätzlichen Optionen für die Verwaltung von ESET-Serverprodukten für erfahrene Benutzern und Administratoren.
ESET PROTECT	Bessere Integration mit ESET PROTECT inklusive der Möglichkeit zur Planung verschiedener Tasks. Weitere Informationen finden Sie in der ESET PROTECT-Onlinehilfe.
Komponentenbasierte Installation	Maßgeschneiderte Installationen enthalten nur ausgewählte Teile des Produkts.
Absender-Spoofing-Schutz	Eine neue Funktion namens „Absender-Spoofing“, die vor gefälschten Absenderinformationen bei E-Mails schützt. Es ist unwahrscheinlich, dass ein E-Mail-Empfänger einen gültigen Absender von einem gefälschten Absender unterscheiden kann, da die E-Mail normalerweise so aussieht, als ob sie von einer legitimen Quelle stammt. Sie können den Absender-Spoofing-Schutz in den erweiterten Einstellungen aktivieren und konfigurieren oder benutzerdefinierte Regeln erstellen.
DKIM-Signierung	ESET Mail Security bietet eine DKIM-Signierfunktion, um die Sicherheit ausgehender E-Mails zu verbessern. Wählen Sie ein Clientzertifikat aus und geben Sie an, welche E-Mail-Header mit DKIM signiert werden sollen. Sie können DKIM-Signierung für jede Domäne einzeln konfigurieren, falls Sie mehrere Domänen verwenden.

Neuerungen

Neue Funktionen und Verbesserungen in ESET Mail Security:

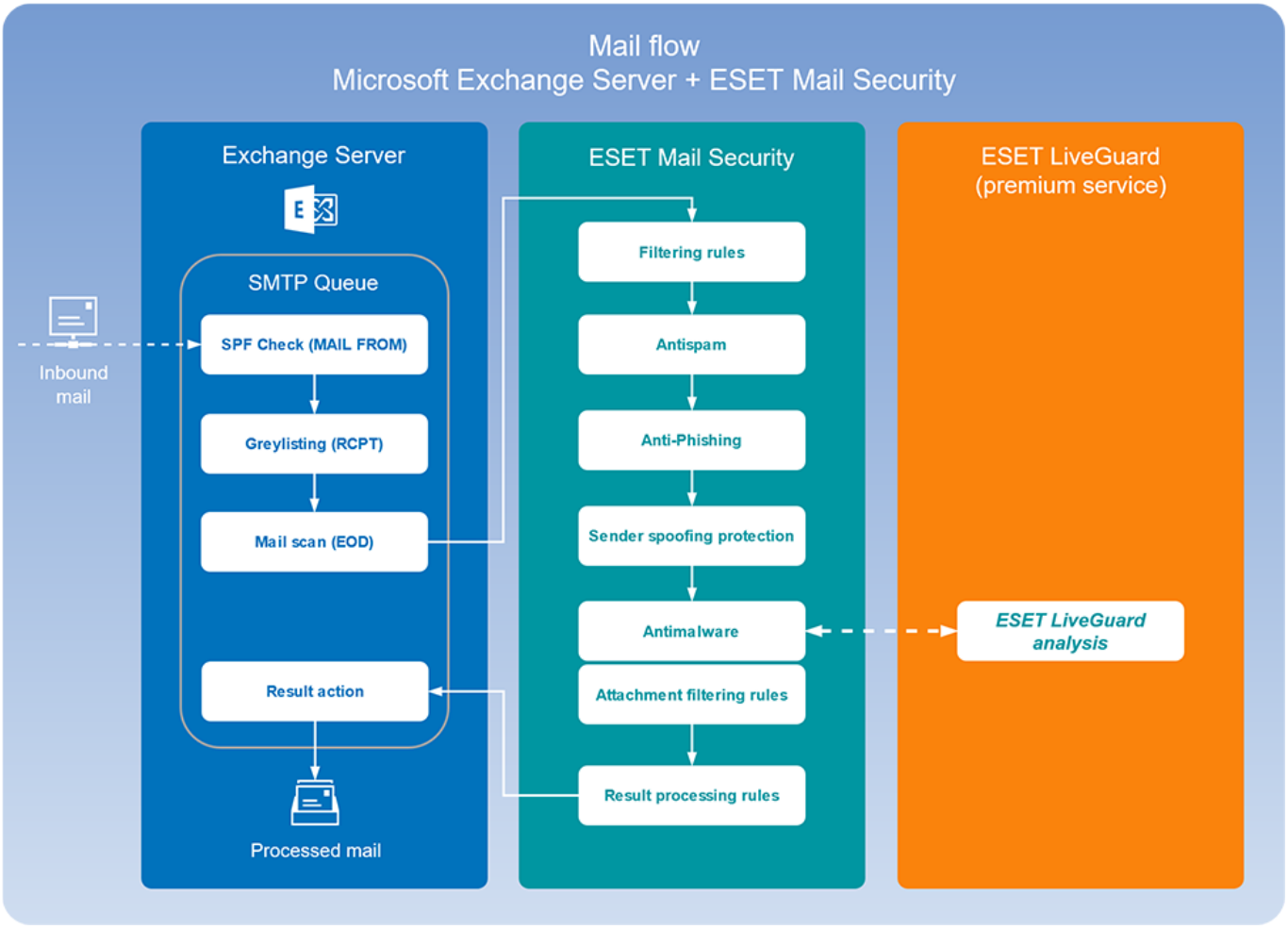
- Echter 64-Bit-Produktkern

- Office 365-Postfachprüfung
- E-Mail-Phishing-Schutz
- Backscatter-Schutz
- Administratorberichte für die E-Mail-Quarantäne
- Synchronisierung der lokalen E-Mail-Quarantäne über das ESET-Cluster
- SMTP-Schutz-Log
- ESET LiveGuard Advanced
- ESET Inspect support
- ESET RMM
- In Syslog-Server exportieren (Arcsight)
- Netzwerkisolierung
- Erkennung durch Machine Learning
- Audit-Logs
- Mikro-Updates für Programmkomponenten
- Absender-Spoofing-Schutz
- DKIM-Signierung
- Microsoft 365-Postfach-Scan

Siehe ausführliche Änderungslogs für ESET Mail Security.

E-Mail-Fluss

Das folgende Diagramm zeigt den E-Mail-Fluss in Microsoft Exchange Server und ESET Mail Security. Details zur Verwendung von ESET LiveGuard Advanced mit ESET Mail Security finden Sie in der ESET LiveGuard Advanced-Online-Hilfe.



ESET Mail Security-Funktionen und Exchange-Serverrollen

Die folgende Tabelle zeigt, welche Funktionen für die einzelnen unterstützten Versionen von Microsoft Exchange Server und deren Rollen verfügbar sind. Der ESET Mail Security Installations-Assistent überprüft Ihre Umgebung bei der Installation. Anschließend werden die Funktionen von ESET Mail Security gemäß der erkannten Exchange Server-Version und der entsprechenden Rollen angezeigt.

Exchange Server-Version und Serverrolle	Spam-Schutz	Phishing-Schutz	Regeln	Mail-Transport-Schutz	On-Demand Postfachdatenbank-Scan	Postfachdatenbank-Schutz
Microsoft Exchange Server 2010 (mehrere Rollen)	✓	✓	✓	✓	✓	✓
Microsoft Exchange Server 2010 (Edge)	✓	✓	✓	✓	?	?
Microsoft Exchange Server 2010 (Hub)	✓	✓	✓	✓	✓	?

Exchange Server-Version und Serverrolle	Spam-Schutz	Phishing-Schutz	Regeln	Mail-Transport-Schutz	On-Demand Postfachdatenbank-Scan	Postfachdatenbank-Schutz
Microsoft Exchange Server 2010 (Postfach)	☐	✓	✓	☐	✓	✓
Microsoft Exchange Server 2013 (mehrere Rollen)	✓	✓	✓	✓	✓	☐
Microsoft Exchange Server 2013 (Edge)	✓	✓	✓	✓	☐	☐
Microsoft Exchange Server 2013 (Postfach)	✓	✓	✓	✓	✓	☐
Microsoft Exchange Server 2016 (Edge)	✓	✓	✓	✓	☐	☐
Microsoft Exchange Server 2016 (Postfach)	✓	✓	✓	✓	✓	☐
Microsoft Exchange Server 2019 (Edge)	✓	✓	✓	✓	☐	☐
Microsoft Exchange Server 2019 (Postfach)	✓	✓	✓	✓	✓	☐

Exchange-Serverrollen

Vergleich: Edge-Rolle und Hub-Rolle

Spamschutz-Funktionen sind auf Edge-Transportservern und Hub-Transportservern standardmäßig deaktiviert. In Exchange-Organisationen mit Edge-Transport-Server ist dies die gewünschte Konfiguration. Sie sollten den Spam-Schutz von ESET Mail Security auf dem Edge-Transport-Server nach Möglichkeit so konfigurieren, dass die Nachrichten vor der Weiterleitung an die Exchange-Organisation gefiltert werden.

Der Spam-Scan sollte nach Möglichkeit auf dem Edge-Server ausgeführt werden, da ESET Mail Security Spam-Nachrichten auf diese Weise früher zurückweisen kann, ohne andere Netzwerkebenen unnötig zu belasten. Bei dieser Konfiguration werden eingehende Nachrichten von ESET Mail Security auf dem Edge-Transport-Server gefiltert, sodass sie sicher an den Hub-Transport-Server übermittelt werden können, ohne dass eine weitere Filterung erforderlich ist.

Angenommen, Ihre Organisation verwendet keinen Edge-Transportserver, sondern nur einen Hub-Transportserver. In diesem Fall empfehlen wir, die Spam-Schutz-Funktionen auf dem Hub-Transportserver zu aktivieren, der eingehende Nachrichten aus dem Internet über SMTP empfängt.

Aufgrund technischer Einschränkungen in Microsoft Exchange Server 2010 und neueren Versionen unterstützt ESET Mail Security keine Microsoft Exchange Server-Bereitstellungen nur mit Clientzugriffsserverrolle (CAS) (eigenständiger CAS).

Schutzmodule

Die Kernfunktion von ESET Mail Security umfasst die folgenden Schutzmodule:

Virenschutz

Der Virenschutz ist eine der grundlegenden Funktionen von ESET Mail Security. Virenschutzlösungen bieten durch Überwachung der Daten-, E-Mail- und Internet-Kommunikation Schutz vor bösartigen Systemangriffen. Wenn eine Bedrohung durch Schadcode erkannt wird, kann das Virenschutz-Modul den Code unschädlich machen, indem es die Ausführung des Codes blockiert und diesen säubert, löscht oder in die Quarantäne verschiebt.

Spam-Schutz

Spamschutzlösungen verwenden verschiedene Technologien (RBL, DNSBL, Fingerprint-Datenbanken, Reputations-Prüfung, Inhaltsanalyse, Regeln, manuell geführte Positiv-/Negativlisten usw.), um E-Mail-Bedrohungen wirksam zu erkennen.
Der ESET Mail Security Spam-Schutz ist cloudbasiert, und ein Großteil der Clouddatenbanken befindet sich in ESET Rechenzentren. Die Spamschutz-Cloud ermöglicht zügige Datenupdates mit einer kürzeren Reaktionszeit beim Aufkommen neuer Spam-Inhalte. Außerdem können so ungültige oder falsche Daten aus den ESET-Negativlisten entfernt werden. Die Kommunikation mit der Spamschutz-Cloud erfolgt wenn möglich über ein proprietäres Protokoll auf Port 53535. Wenn die Kommunikation über das ESET-Protokoll nicht möglich ist, werden stattdessen DNS-Dienste (Port 53) verwendet. DNS ist jedoch weniger effektiv, da für die Spam-Klassifizierung einer einzigen E-Mail-Nachricht mehrere Anfragen gesendet werden müssen.

Öffnen Sie nach Möglichkeit den TCP- und UDP-Port 53535 für die in diesem Knowledgebase-Artikel aufgelisteten IP-Adressen. ESET Mail Security verwendet diesen Port für den Versand von Anfragen.

Normalerweise werden bei der Spam-Klassifizierung keine E-Mails oder Teile von E-Mails übertragen. Angenommen, ESET LiveGrid® ist aktiviert, und Sie haben die Übermittlung von Samples zur Analyse explizit zugelassen. In diesem Fall werden nur Nachrichten gesendet, die als Spam (oder höchstwahrscheinlich als Spam) markiert sind, um eine gründliche Analyse und Verbesserung der Cloud-Datenbank zu unterstützen.
Falls Sie falsche Positiv- oder Negativklassifizierungen melden möchten, finden Sie weitere Informationen in unserem Knowledgebase-Artikel.
ESET Mail Security kann außerdem die Greylisting-Methode (standardmäßig deaktiviert) für den Spamfilter verwenden.

Phishing-Schutz

Der Phishing-Schutz in ESET Mail Security verhindert, dass Benutzer auf Webseiten zugreifen, die für Phishing bekannt sind. E-Mails können Links zu Phishing-Webseiten enthalten. ESET Mail Security verwendet einen ausgeklügelten Parser, um den Text und den Betreff aller eingehenden Nachrichten zu analysieren und diese Links (URLs) zu identifizieren. Die Links werden mit der Phishing-Datenbank abgeglichen, und Regeln mit der Bedingung Nachrichtentext werden ausgewertet.

Regeln

Die auf Ihrem System verfügbaren Regeln für Postfach-Datenbankschutz, On-Demand Postfachdatenbank-Scan und Mail-Transport-Schutz hängen davon ab, welche Version von Microsoft Exchange Server auf dem Server mit ESET Mail Security installiert ist.
Mit Regeln können Sie Filterbedingungen für E-Mails manuell definieren und Aktionen mit gefilterten E-Mails verknüpfen. Sie können verschiedene Bedingungen und Aktionen verwenden. Sie können individuelle Regeln erstellen und auch kombinieren. Wenn eine Regel mehrere Bedingungen enthält, werden diese durch ein logisches UND verknüpft. Dementsprechend wird die Regel nur ausgeführt, wenn alle Bedingungen erfüllt sind. Wenn mehrere Regeln erstellt werden, wird ein logisches ODERverwendet, d. h., das Programm führt die erste Regel aus, deren Bedingungen erfüllt sind.
In der Scan-Sequenz wird zunächst das Greylisting angewendet, falls aktiviert. Anschließend werden die folgenden Techniken angewendet: die Prüfung nach benutzerdefinierten Regeln, dann eine Virenprüfung und schließlich eine Spam-Prüfung.

Mehrschichtige Sicherheit

ESET Mail Security bietet umfassenden Schutz auf verschiedenen Ebenen:

- Postfachdatenbank-Schutz
- Mail-Transport-Schutz
- On-Demand Postfachdatenbank-Scan
- Microsoft 365-Postfachdatenbank-Scan

> Eine umfassende Ansicht finden Sie in der Matrix der ESET Mail Security-Features und Microsoft Exchange Server-Versionen und deren Rollen.

Postfachdatenbank-Schutz

Die Postfach-Prüfung wird vom Microsoft Exchange Server ausgelöst und gesteuert. E-Mails in der Datenbank von Microsoft Exchange Server werden ständig geprüft. Je nach Ihren benutzerdefinierten Einstellungen und je nachdem, welche Versionen von Microsoft Exchange Server und der VSAPI-Schnittstelle Sie verwenden, wird die Prüfung in den folgenden Situationen ausgelöst:

- Beim Zugriff des Benutzers auf dessen E-Mails in einem E-Mail-Programm (E-Mails werden immer mit der neuesten Erkennungsroutine gescannt).
- Im Hintergrund, wenn Microsoft Exchange Server nicht ausgelastet ist.
- Proaktiv (abhängig vom internen Algorithmus von Microsoft Exchange Server).

> Für Microsoft Exchange Server 2013, 2016 und 2019 ist der Postfach-Datenbankschutz nicht verfügbar.

Der Postfach-Datenbankschutz ist für die folgenden Systeme verfügbar:

Exchange Server-Version und Serverrolle	Spam-Schutz	Phishing-Schutz	Regeln	Mail-Transport-Schutz	On-Demand Postfachdatenbank-Scan	Postfachdatenbank-Schutz
Microsoft Exchange Server 2010 (Postfach)	☐	✓	✓	☐	✓	✓
Microsoft Exchange Server 2010 (mehrere Rollen)	✓	✓	✓	✓	✓	✓

Diese Prüfungsart kann als Installation mit einem einzigen Server mit mehreren Exchange Server-Rollen auf einem Computer installiert werden (sofern entweder Postfachserver- oder Backend-Rolle verwendet werden).

Mail-Transport-Schutz

Die Prüfung auf dem SMTP-Server wird mit einem speziellen Plug-In durchgeführt. In Microsoft Exchange Server 2010 ist das Plug-In als Transport-Agent in den Rollen Edge oder Hub von Microsoft Exchange Server registriert.

Die Prüfung durch einen Transport-Agenten auf dem SMTP-Server bietet Viren- und Spam-Schutz sowie die Möglichkeit, benutzerdefinierte Regeln zu erstellen. Im Gegensatz zur VSAPI-Prüfung findet die Prüfung auf dem SMTP-Server statt, noch bevor die geprüften E-Mails das Postfach von Microsoft Exchange Server erreichen.

Auch als E-Mail-Filterung auf SMTP-Serverebene bekannt. Dieser Schutz wird vom Transportagenten bereitgestellt und ist nur für Microsoft Exchange Server 2010 oder neuere Versionen verfügbar, wenn diese in der Rolle Edge-Transportserver bzw. Hub-Transportserver ausgeführt werden. Diese Prüfungsart kann als Installation mit einem einzigen Server mit mehreren Exchange Server-Rollen auf einem Computer installiert werden (sofern eine der genannten Rollen verwendet wird).

Der Mail-Transport-Schutz ist für die folgenden Systeme verfügbar:

Exchange Server-Version und Serverrolle	Spam-Schutz	Phishing-Schutz	Regeln	Mail-Transport-Schutz	On-Demand Postfachdatenbank-Scan	Postfachdatenbank-Schutz
Microsoft Exchange Server 2010 (mehrere Rollen)	✓	✓	✓	✓	✓	✓
Microsoft Exchange Server 2013 (mehrere Rollen)	✓	✓	✓	✓	✓	☐
Microsoft Exchange Server 2013 (Edge)	✓	✓	✓	✓	☐	☐
Microsoft Exchange Server 2013 (Postfach)	✓	✓	✓	✓	✓	☐

Exchange Server-Version und Serverrolle	Spam-Schutz	Phishing-Schutz	Regeln	Mail-Transport-Schutz	On-Demand Postfachdatenbank-Scan	Postfachdatenbank-Schutz
Microsoft Exchange Server 2016 (Edge)	✓	✓	✓	✓	☐	☐
Microsoft Exchange Server 2016 (Postfach)	✓	✓	✓	✓	✓	☐
Microsoft Exchange Server 2019 (Edge)	✓	✓	✓	✓	☐	☐
Microsoft Exchange Server 2019 (Postfach)	✓	✓	✓	✓	✓	☐

On-Demand Postfachdatenbank-Scan

Ermöglicht die Planung und Ausführung von Scans für Exchange-Postfachdatenbanken. Dieses Feature ist nur für Microsoft Exchange Server 20010 oder neuere Versionen verfügbar, wenn diese in der Rolle als Postfachserver bzw. als Hub-Transportserver ausgeführt werden. Dies gilt auch für Installationen mit einem einzigen Server und mehreren Exchange Server-Rollen auf einem Computer (sofern eine der genannten Rollen verwendet wird).

Die On-Demand Postfachdatenbank-Scan ist für die folgenden Systeme verfügbar:

Exchange Server-Version und Serverrolle	Spam-Schutz	Phishing-Schutz	Regeln	Mail-Transport-Schutz	On-Demand Postfachdatenbank-Scan	Postfachdatenbank-Schutz
Microsoft Exchange Server 2010 (mehrere Rollen)	✓	✓	✓	✓	✓	✓
Microsoft Exchange Server 2010 (Hub)	✓	✓	✓	✓	✓	☐
Microsoft Exchange Server 2010 (Postfach)	☐	✓	✓	☐	✓	✓
Microsoft Exchange Server 2013 (mehrere Rollen)	✓	✓	✓	✓	✓	☐
Microsoft Exchange Server 2013 (Postfach)	✓	✓	✓	✓	✓	☐

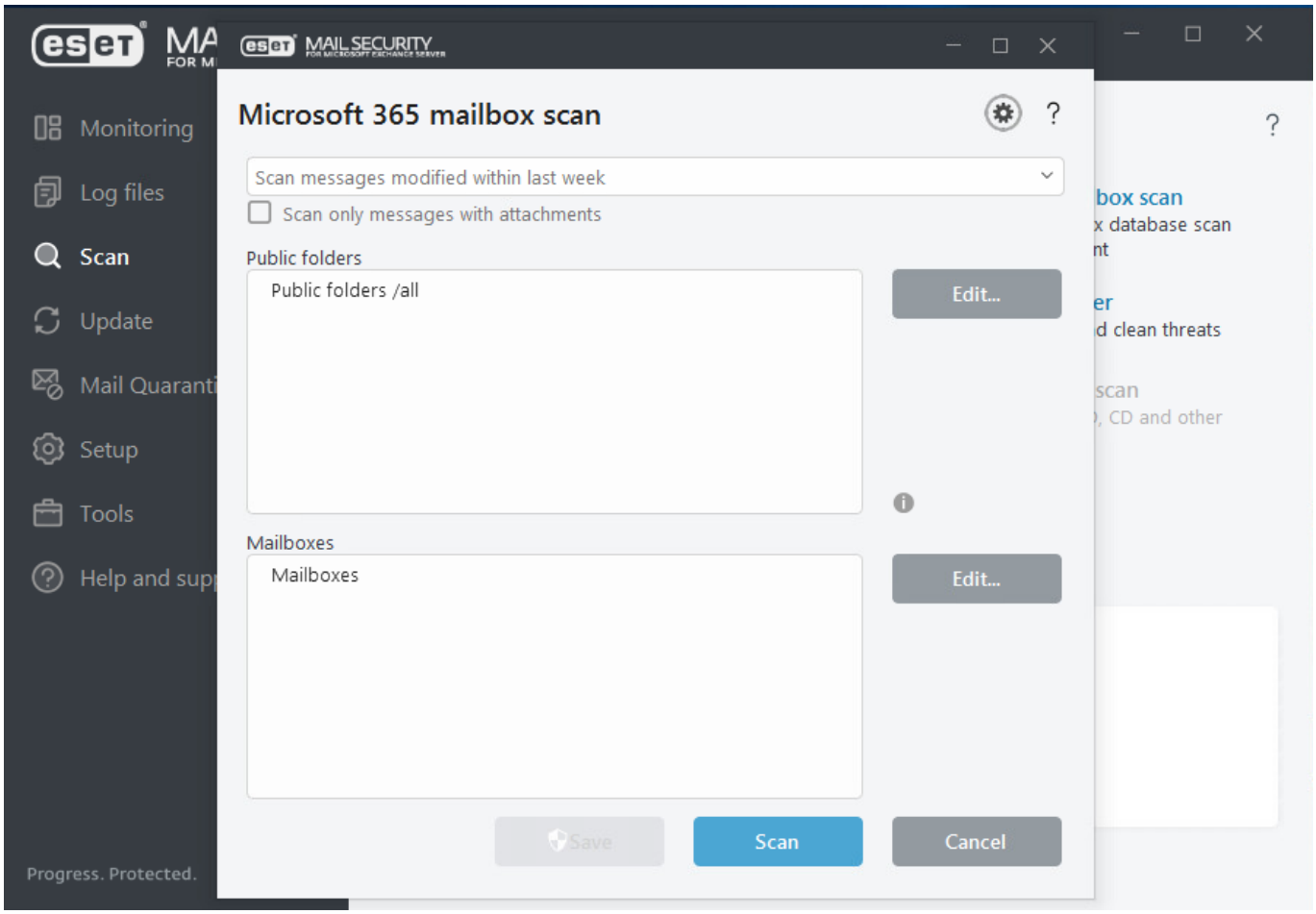
Exchange Server-Version und Serverrolle	Spam-Schutz	Phishing-Schutz	Regeln	Mail-Transport-Schutz	On-Demand Postfachdatenbank-Scan	Postfachdatenbank-Schutz
Microsoft Exchange Server 2016 (Postfach)	✓	✓	✓	✓	✓	?
Microsoft Exchange Server 2019 (Postfach)	✓	✓	✓	✓	✓	?

Microsoft 365-Postfachdatenbank-Scan

ESET Mail Security enthält Scan-Funktionen für Microsoft 365-Hybridumgebungen. Diese Funktionen sind in ESET Mail Security nur sichtbar und verfügbar, wenn Sie eine Exchange-Hybridumgebung verwenden (lokal und in der Cloud). Beide Routing-Szenarien werden unterstützt, sowohl über **Exchange Online** oder über eine **lokale** Organisation. Weitere Informationen finden Sie unter Transport-Routing in Exchange-Hybridbereitstellungen.

Registrieren Sie den ESET Mail Security Scanner, um diese Funktion zu aktivieren.

Sie können Microsoft 365-Remotepostfächer und öffentliche Ordner auf dieselbe Weise scannen wie mit der On-Demand Postfachdatenbank-Scan.



Eine vollständige Prüfung der E-Mail-Datenbank kann in einer großen Umgebung eine unerwünschte Systemlast verursachen. Daher können Sie auswählen, welche Datenbanken oder Postfächer geprüft werden sollen.

Verwenden Sie den Zeitfilter am oberen Fensterrand, um die Systemlast weiter zu reduzieren. Anstatt **alle Nachrichten zu scannen**, können Sie beispielsweise **alle in der letzten Woche geänderten Nachrichten scannen**.

Wir empfehlen, Microsoft 365 zu konfigurieren. Drücken Sie die Taste **F5** und klicken Sie auf **Server** > **On-Demand Postfachdatenbank-Scan**. Siehe auch Details des Kontos für den Datenbank-Scan.

Sie können die Aktivität des Office 365-Postfach-Scans unter **Log-Dateien** > **Postfachdatenbank-Scan** überprüfen.

Systemanforderungen

Unterstützte Betriebssysteme:

- Microsoft Windows Server 2022 (Server Core und Desktopdarstellung)
- Microsoft Windows Server 2019 (Server Core und Desktopdarstellung)
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012

Unterstützte Versionen von Microsoft Exchange Server:

- Microsoft Exchange Server 2019 bis CU13
- Microsoft Exchange Server 2016 bis CU23
- Microsoft Exchange Server 2013 bis CU23 (CU1 und CU4 werden nicht unterstützt)
- Microsoft Exchange Server 2010 SP1, SP2, SP3 bis RU32

> Die eigenständige CAS-Rolle (Client Access Server) wird nicht unterstützt. Weitere Details finden Sie unter Exchange-Serverrollen.
> Beachten Sie die ESET Mail Security-Funktionen und Exchange Server-Rollen, um die verfügbaren Funktionen für die einzelnen unterstützten Versionen von Microsoft Exchange Server und deren Rollen zu identifizieren.

Hardwareanforderungen:

Komponente	Anforderung
Prozessor	Intel oder AMD Single Core x64
Arbeitsspeicher	256 MB freier Arbeitsspeicher
Festplatte	700 MB freier Speicherplatz auf der Festplatte
Bildschirmauflösung	800 x 600 Pixel oder höher

ESET Mail Security hat dieselben empfohlenen Hardwareanforderungen wie Microsoft Exchange Server. Weitere Details finden Sie in den folgenden technischen Microsoft-Artikeln:

Microsoft Exchange Server 2010

Microsoft Exchange Server 2013

Microsoft Exchange Server 2016

> Installieren Sie unbedingt das neueste Service Pack für Ihr Microsoft Server-Betriebssystem und die jeweilige Anwendung, bevor Sie das ESET-Sicherheitsprodukt installieren. Installieren Sie nach Möglichkeit immer die neuesten verfügbaren Windows-Updates und Hotfixes.

Vorbereiten für die Installation

Bevor Sie Ihr Produkt installieren, sollten Sie einige Schritte ausführen:

- Laden Sie nach dem Kauf von ESET Mail Security das *.msi*-Installationspaket von der ESET-Webseite herunter.

- Vergewissern Sie sich, dass der Server, auf dem Sie ESET Mail Security installieren möchten, die Systemanforderungen erfüllt.

- Melden Sie sich mit einem Administratorkonto beim Server an.

- Für Upgrades einer vorhandenen Installation von ESET Mail Security empfehlen wir, die aktuelle Konfiguration mit der Funktion Einstellungen exportieren zu sichern.

- Entfernen bzw. deinstallieren Sie bei Bedarf alle externen Virenschutzlösungen von Ihrem System. Dazu empfehlen wir den ESET AV Remover. Eine Liste der Virenschutz-Software von Drittanbietern, die mit dem ESET AV Remover entfernt werden können, finden Sie in diesem Knowledgebase-Artikel.

- Falls Sie ESET Mail Security unter Windows Server 2016 installieren, empfiehlt Microsoft die Deinstallation der Windows Defender-Funktionen und das Aufheben der Windows Server ATP-Registrierung, um Probleme zu vermeiden, die durch mehrere parallel installierte Virenschutzprodukte verursacht werden können.

- Falls Sie ESET Mail Security unter Windows Server 2019 oder Windows Server 2022 installieren, empfiehlt Microsoft, Windows Defender in den passiven Modus zu versetzen, um Probleme zu vermeiden, die durch mehrere parallel auf einem Computer installierte Virenschutzprodukte verursacht werden können.

> Wenn während der Installation von ESET Mail Security auf Ihrem Windows Server 2016, 2019 oder 2022 **Windows Defender-Features** vorhanden sind, werden diese Funktionen von ESET Mail Security deaktiviert, um Konflikte zwischen dem Echtzeit-Dateischutz und verschiedenen anderen Virenschutzprodukten zu vermeiden. Außerdem deaktiviert ESET Mail Security die Windows Defender-Funktionen bei jedem Systemstart und Neustart.
> Dabei gibt es eine Ausnahme: Wenn Sie eine Komponenteninstallation die Komponente **Echtzeit-Dateischutz** durchführen, werden die Windows Defender-Funktionen unter Windows Server 2016 nicht deaktiviert.

- Eine umfassende Ansicht finden Sie in der Matrix der ESET Mail Security-Features und Microsoft Exchange Server-Versionen und deren Rollen.

- Führen Sie das Tool „Postfächer zählen“ aus, um die Anzahl der Postfächer zu überprüfen. Weitere Informationen finden Sie in unserem Knowledgebase-Artikel . Nachdem Sie ESET Mail Security installiert haben, wird die aktuelle Anzahl der Postfächer am unteren Rand des Überwachungsfensters angezeigt.

Sie können das ESET Mail Security-Installationsprogramm in zwei verschiedenen Modi ausführen:

- Programmfenster – Wir empfehlen, den Installationsassistenten für die Installation zu verwenden.

- Stille/unbeaufsichtigte Installation – Sie können ESET Mail Security anstatt mit dem Assistenten auch unbeaufsichtigt über die Befehlszeile installieren.

- Aktualisierung auf die neueste Version – Falls Sie eine ältere Version von ESET Mail Security verwenden, können Sie eine passende Upgrademethode auswählen.

Nachdem Sie Ihr ESET Mail Security erfolgreich installiert bzw. aktualisiert haben, können Sie zwischen den folgenden Aktivitäten wählen:

Produktaktivierung

Die Verfügbarkeit der einzelnen Aktivierungsmöglichkeiten im Aktivierungsfenster hängt vom Land und von der Vertriebsart ab.

Tasks nach der Installation

Eine Liste der empfohlenen Tasks nach der erfolgreichen Installation von ESET Mail Security.

Konfigurieren der allgemeinen Einstellungen

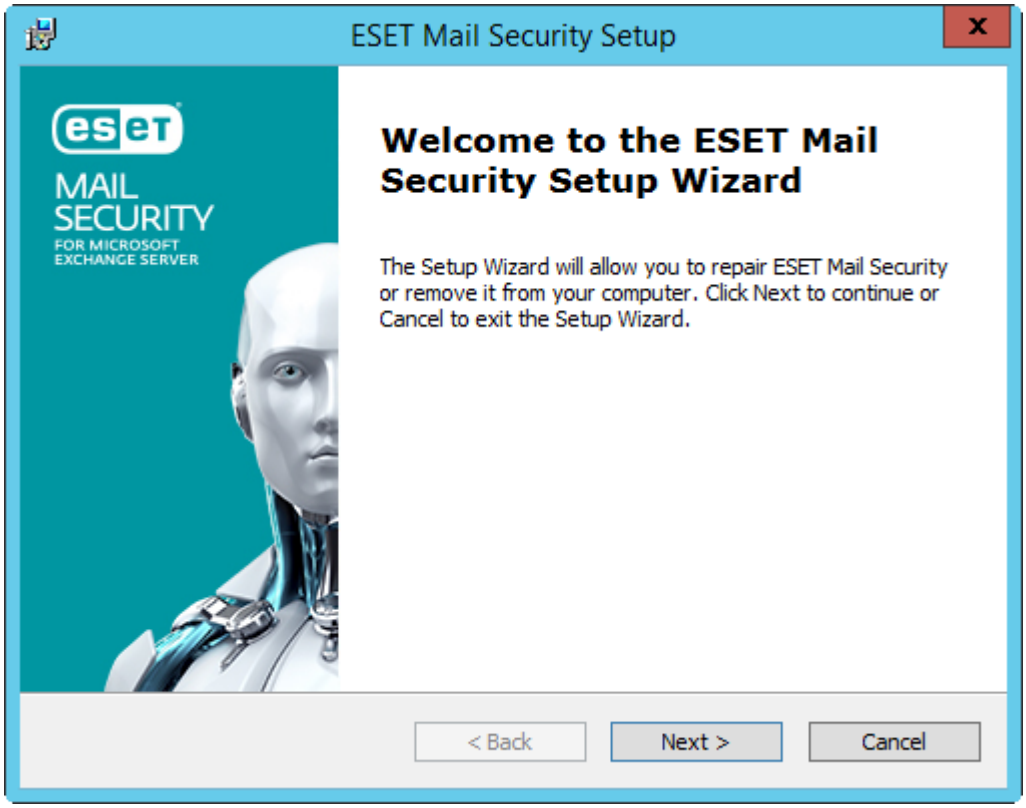
Sie können Feineinstellungen in ESET Mail Security vornehmen, indem Sie die erweiterten Einstellungen für die einzelnen Funktionen anpassen.

ESET Mail Security Installationsschritte

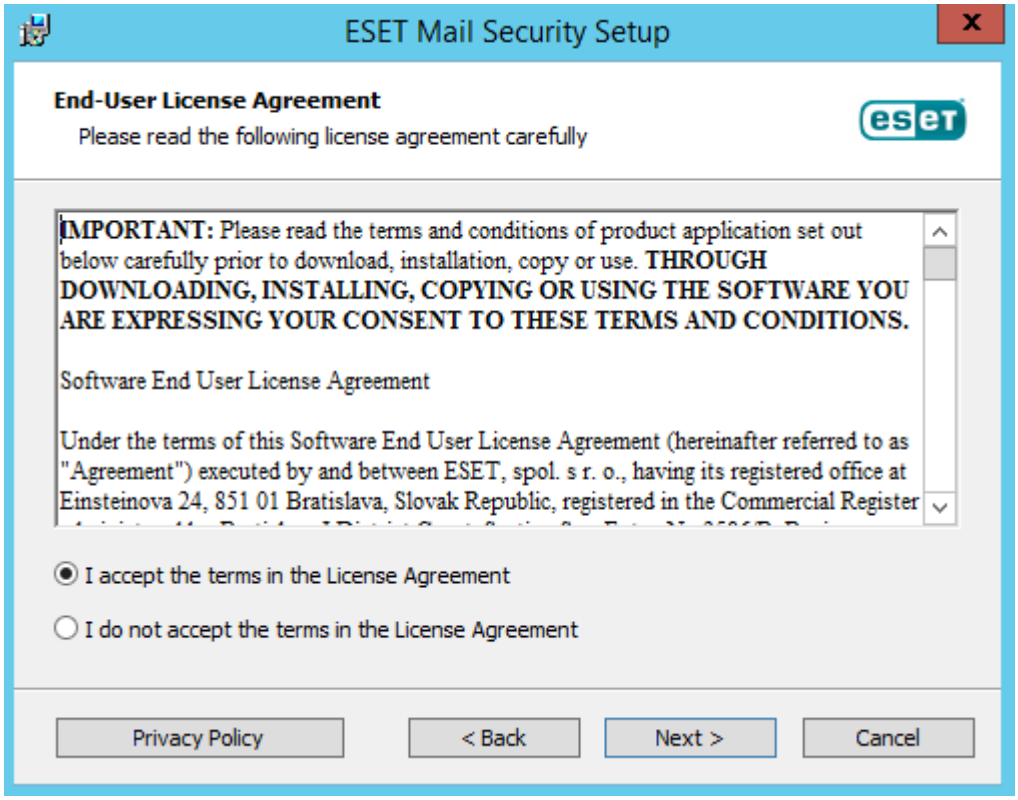
So sieht der Installationsassistent für das Programmfenster normalerweise aus. Doppelklicken Sie auf das .msi-Paket und folgen Sie den Schritten, um ESET Mail Security zu installieren:

1. Klicken Sie auf **Weiter**, um fortzufahren, oder auf **Abbrechen**, um die Installation abzubrechen.

2. Der Installationsassistent wird in der Sprache ausgeführt, die als **Standort** unter **Region** > **Ort** in Ihrem Betriebssystem (bzw. **Aktueller Aufenthaltsort** unter **Region und Sprache** > **Standort** in älteren Systemen) festgelegt ist. Wählen Sie im Dropdownmenü die **Produktsprache** aus, in der Ihr ESET Mail Security installiert werden soll. Die ausgewählte Sprache für ESET Mail Security ist unabhängig von der Sprache des Installationsassistenten.



3. Klicken Sie auf **Weiter**, um die Endbenutzer-Lizenzvereinbarung anzuzeigen. Bestätigen Sie, dass Sie die Endbenutzer-Lizenzvereinbarung und die Datenschutzerklärung akzeptieren, und klicken Sie auf **Weiter**.



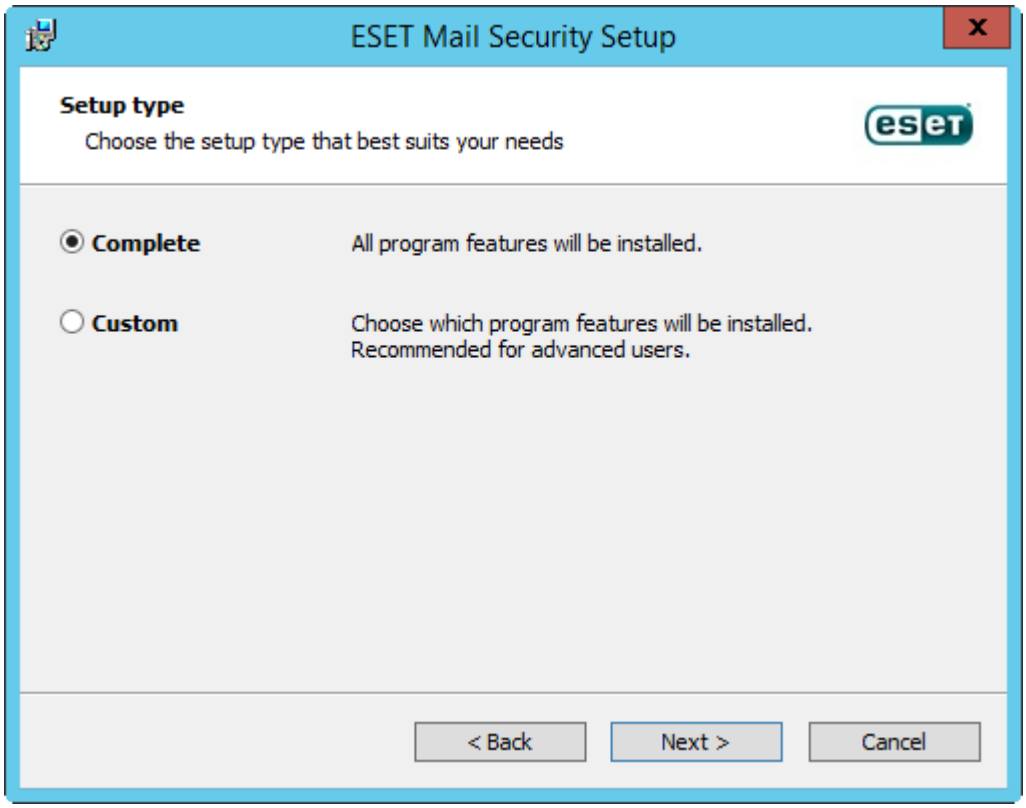
4. Wählen Sie eine der verfügbaren Installationsarten aus (Die Verfügbarkeit hängt von Ihrem Betriebssystem ab):

Abgeschlossen

Alle Features von ESET Mail Security werden installiert.

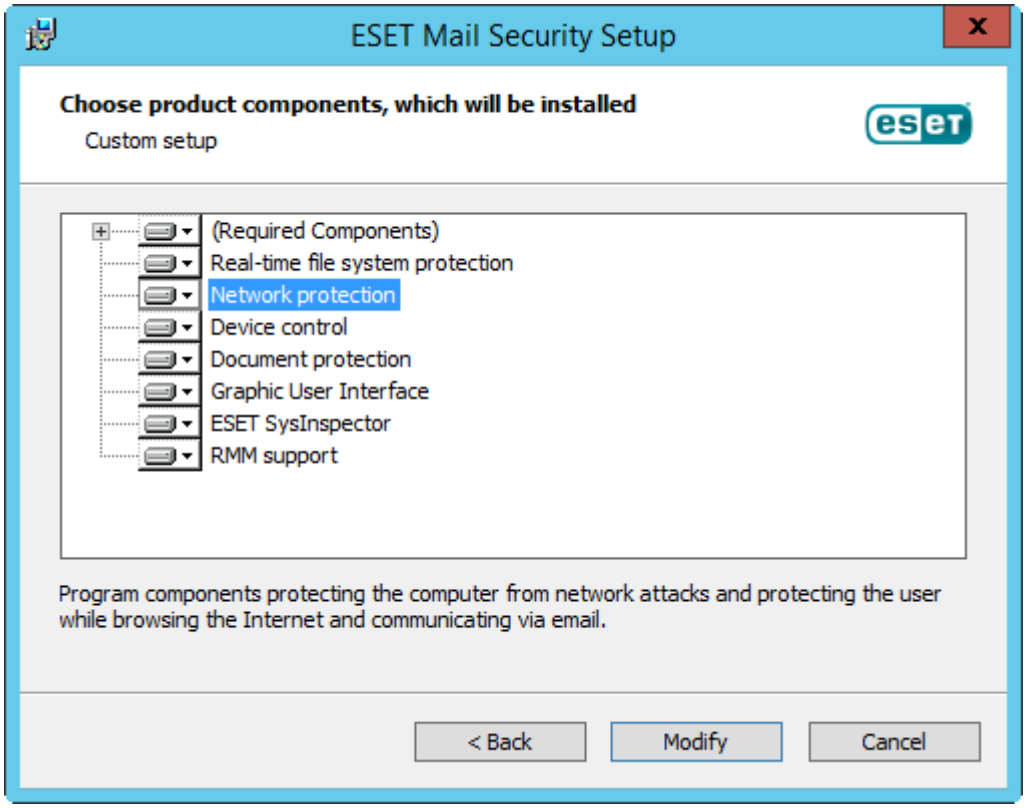
Das Installationsprogramm enthält nur die wichtigsten Module. Alle anderen Module werden beim ersten Modul-Update nach der Produktaktivierung heruntergeladen.

Falls Sie die lokale Quarantäne für E-Mails verwenden möchten und die Quarantäne-E-Mails nicht auf Ihrem C:-Laufwerk speichern möchten, legen Sie für den **Datenordner** das gewünschte Laufwerk und den Speicherort ein. Beachten Sie jedoch, dass in diesem Fall alle Datendateien von ESET Mail Security an diesem Ort gespeichert werden.

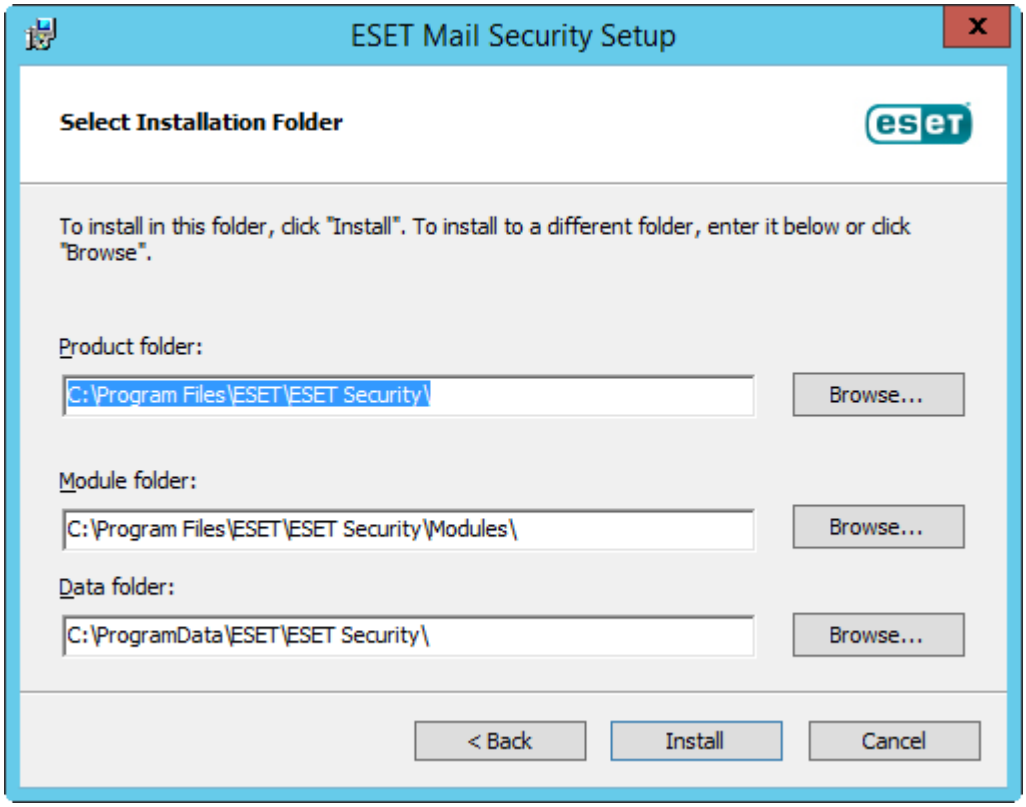


Benutzerdefiniert

Wählen Sie aus, welche Programmfunktionen von ESET Mail Security auf dem System installiert werden. Vor Beginn der Installation wird eine Liste von Produktmodulen und Features angezeigt. Dies ist nützlich, wenn Sie ESET Mail Security nur mit den benötigten Komponenten installieren möchten.



5. Sie werden aufgefordert, den Speicherort für die Installation von ESET Mail Security auszuwählen. Standardmäßig wird das Programm unter *C:\Program Files\ESET\ESET Mail Security* installiert. Klicken Sie auf **Durchsuchen**, um diesen Speicherort zu ändern (nicht empfohlen).

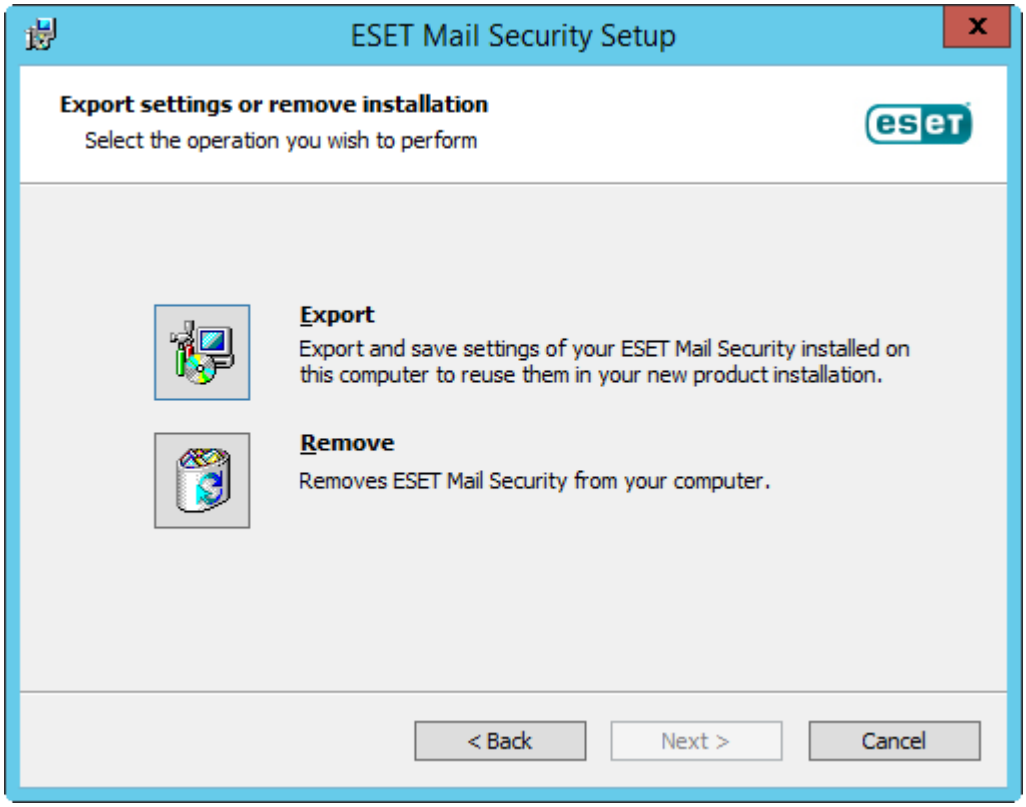


6. Klicken Sie auf **Installieren**, um die Installation zu starten. Nach der Installation werden Sie aufgefordert, ESET Mail Security zu aktivieren.

Einstellungen exportieren oder Installation entfernen

Sie können die Einstellungen exportieren und speichern oder die Installation entfernen. Führen Sie dazu entweder das *.msi*-Installationspaket aus, das Sie für die ursprüngliche Installation verwendet haben, oder öffnen Sie **Programme und Funktionen** in der Windows-Systemsteuerung, klicken Sie mit der rechten Maustaste auf ESET Mail Security und wählen Sie **Ändern** aus.

Sie können die ESET Mail Security Einstellungen **Exportieren** oder ESET Mail Security vollständig **Entfernen** (deinstallieren).



Anfängliches Modul-Update

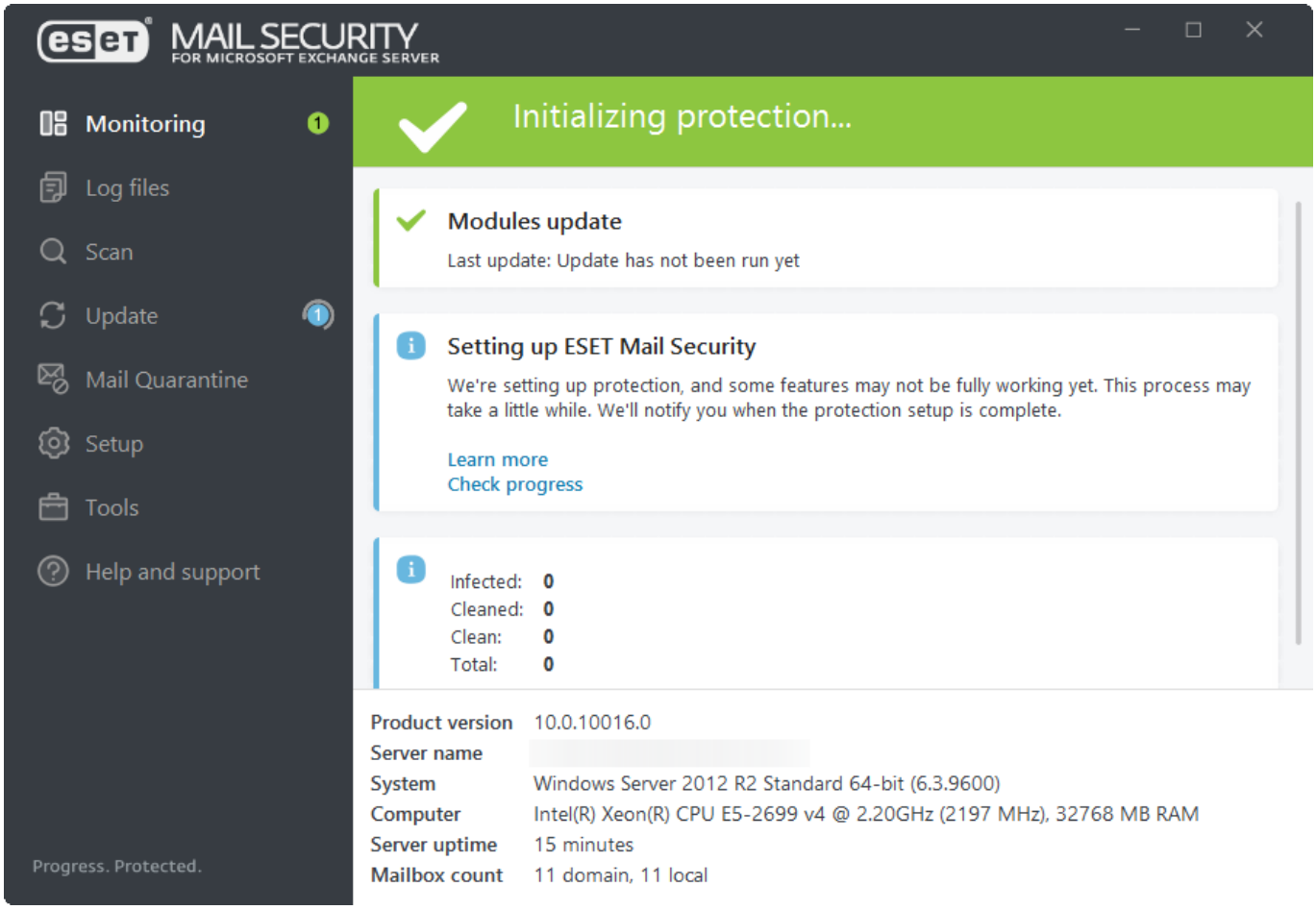
Um durch die Größe des Installationsprogramms verursachten Netzwerkverkehr zu reduzieren und Ressourcen zu sparen, enthält das Installationsprogramm nur die wichtigsten Module. Alle anderen Module werden beim ersten Modul-Update nach der Produktaktivierung heruntergeladen. Der Hauptvorteil ist ein deutlich kleineres Installationsprogramm, und ESET Mail Security lädt nach der Aktivierung die neuesten Anwendungsmodule herunter.

Das verkleinerte Installationsprogramm enthält die folgenden Module:

- Loaders
- Anti-Stealth-Unterstützung
- Direct Cloud-Kommunikation
- Lokalisierungsunterstützung

- Konfiguration
- SSL

Nach der Produktaktivierung wird der Status **Schutz wird aktiviert** angezeigt, um Sie über die Initialisierung der Funktionen zu informieren.



Falls beim Download der Module Probleme auftreten (z. B. keine Netzwerkverbindung, Firewall- oder Proxyeinstellungen), wird der Anwendungsstatus **Aufmerksamkeit erforderlich** angezeigt.
Klicken Sie im Programmfenster auf **Update** > **Nach Updates suchen**, um den Updateprozess erneut zu starten.
Nach mehreren erfolglosen Versuchen wird der Anwendungsstatus **Fehler beim Einrichten des Schutzes** in rot angezeigt. Falls Sie die Module nicht aktualisieren können, laden Sie das vollständige .msi Installationsprogramm für ESET Mail Security herunter.

Falls Ihr Server nicht mit dem Internet verbunden ist und Updates benötigt, können Sie die Updatedateien für Module wie folgt von den ESET Updateservern herunterladen:

- Aktualisieren über Update-Mirror
- Mit dem Mirror-Tool

Stille/unbeaufsichtigte Installation

Führen Sie den folgenden Befehl aus, um die Installation über die Befehlszeile zu starten: `msiexec /i <packagename> /qn /l*xv msi.log`

Überprüfen Sie das **Anwendungs-Log** in der Windows-Ereignisanzeige (suchen Sie nach Einträgen von der Quelle: MsiInstaller), um sicherzustellen, dass die Installation erfolgreich war, oder um Installationsprobleme zu untersuchen.

Vollständige Installation auf einem 64-Bit-System:
```
msiexec /i emsx_nt64.msi /qn /l*xv msi.log ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,SysInspector,SysRescue,Rmm,eula
```

Nach Abschluss der Installation wird die ESET-Benutzeroberfläche gestartet und das Windows-Benachrichtigungsbereichs-Icon wird im Windows-Benachrichtigungsbereich angezeigt.

Installation des Produkts in der **angegebenen Sprache** (z. B. Deutsch):
```
msiexec /i emsx_nt64.msi /qn ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,^
SysInspector,SysRescue,Rmm,eula PRODUCT_LANG=1031 PRODUCT_LANG_CODE=de-de
```
Weitere Details und eine Liste der Sprachcodes finden Sie unter **Sprachparameter** im Thema Installation über die Kommandozeile.

Wenn Sie Werte für den Parameter `REINSTALL` angeben, müssen Sie die restlichen Funktionen auflisten, die nicht als Werte für die Parameter `ADDLOCAL` oder `REMOVE` verwendet werden. Bei der Installation über die Kommandozeile müssen Sie alle Funktionen als Werte für die Parameter `REINSTALL, ADDLOCAL` und `REMOVE` angeben. Das Hinzufügen oder Entfernen kann fehlschlagen, wenn Sie den Parameter `REINSTALL` nicht verwenden.
Im Abschnitt Installation über die Kommandozeile finden Sie eine vollständige Liste der Features.

Vollständige Deinstallation auf einem 64-Bit-System:
```
msiexec /x emsx_nt64.msi /qn /l*xv msi.log
```

Ihr Server wird nach der erfolgreichen Deinstallation automatisch neu gestartet.

Installation über die Kommandozeile

Die folgenden Einstellungen sind **nur mit den Einstellungen reduziert**, einfach und **keine** der Benutzeroberfläche geeignet. Weitere Informationen zur `msiexec`-Version für die Befehlszeilenschalter finden Sie in der Dokumentation .

Unterstützte Parameter:

APPDIR=<path>

- Pfad: gültiger Verzeichnispfad
- Installationsverzeichnis der Anwendung
- Beispiel: `emsx_nt64.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

APPDATADIR=<path>

- Pfad: gültiger Verzeichnispfad
- Installationsverzeichnis der Anwendungsdaten

MODULEDIR=<path>

- Pfad: gültiger Verzeichnispfad
- Installationsverzeichnis des Moduls

ADDLOCAL=<list>

- Komponenteninstallation: Liste nicht obligatorischer Funktionen, die lokal installiert werden sollen.
- Verwendung mit *.msi*-Paketen von ESET: `emsx_nt64.msi /qn ADDLOCAL=<list>`
- Weitere Informationen zur `ADDLOCAL`-Eigenschaft finden Sie unter https://docs.microsoft.com/en-gb/windows/desktop/Msi/addlocal
- Die `ADDLOCAL`-Liste ist eine kommagetrennte Liste der Namen aller zu installierenden Funktionen.
- Wenn Sie eine Funktion für die Installation auswählen, muss der gesamte Pfad (alle übergeordneten Funktionen) explizit in der Liste aufgeführt werden.

REMOVE=<list>

- Komponenteninstallation – Übergeordnetes Feature, das Sie nicht lokal installieren möchten.
- Verwendung mit .msi-Paketen von ESET: `emsx_nt64.msi /qn REMOVE=<list>`
- Weitere Informationen zur `REMOVE`-Eigenschaft finden Sie unter https://docs.microsoft.com/en-gb/windows/desktop/Msi/remove
- Die `REMOVE`-Liste ist eine kommagetrennte Liste der übergeordneten Features, die nicht installiert bzw. entfernt werden, falls sie bereits installiert sind.
- Es reicht aus, das übergeordnete Feature anzugeben. Sie müssen nicht jedes untergeordnete Feature einzeln zur Liste hinzufügen.

ADDEXCLUDE=<list>

- Die `ADDEXCLUDE`-Liste ist eine kommagetrennte Liste der Namen aller Features, die nicht installiert werden sollen.
- Wenn Sie eine Funktion auswählen, die nicht installiert werden soll, müssen der gesamte Pfad (alle untergeordneten Features) sowie verwandte unsichtbare Features ausdrücklich in der Liste aufgeführt werden.
- Beispiel: `emsx_nt64.msi /qn ADDEXCLUDE=<list>`

> `ADDEXCLUDE` kann nicht zusammen mit `ADDLOCAL` verwendet werden.

Vorhandensein der Funktion

- **Obligatorisch** – Die Funktion wird immer installiert.
- **Optional** - Die Installation der Funktion kann abgewählt werden.
- **Unsichtbar** – logische Funktion, die für das Funktionieren anderer Funktionen erforderlich ist

Liste der ESET Mail Security-Features:

Die Namen der Features unterscheiden zwischen Groß- und Kleinschreibung. `RealtimeProtection` ist nicht gleich `REALTIMEPROTECTION`.

Funktionsname	Vorhandensein der Funktion
SERVER	Obligatorisch
RealtimeProtection	Obligatorisch
MAILSERVER	Obligatorisch
WMIProvider	Obligatorisch
HIPS	Obligatorisch
Updater	Obligatorisch
eShell	Obligatorisch
UpdateMirror	Obligatorisch
DeviceControl	Optional
DocumentProtection	Optional
WebAndEmail	Optional
ProtocolFiltering	Unsichtbar
NetworkProtection	Optional
IdsAndBotnetProtection	Optional
Rmm	Optional
WebAccessProtection	Optional
EmailClientProtection	Optional
MailPlugins	Unsichtbar
Cluster	Optional
_Base	
eula	
ShellExt	Optional
_FeaturesCore	
GraphicUserInterface	Optional
SysInspector	Optional
SysRescue	Optional
EnterpriseInspector	Optional

Falls Sie eines der folgenden Features entfernen möchten, müssen Sie die gesamte Gruppe entfernen, indem Sie alle Features in der Gruppe einzeln angeben. Andernfalls wird das Feature nicht entfernt. Hier sehen Sie zwei Gruppen (jede Zeile steht für eine Gruppe):

```
GraphicUserInterface,ShellExt
```

```
NetworkProtection,WebAccessProtection,IdsAndBotnetProtection,ProtocolFiltering,MailPlugins,EmailClientProtection
```

Schließen Sie den Bereich **NetworkProtection** (inklusive der untergeordneten Features mit dem Parameter `REMOVE` von der Installation aus und geben Sie nur das übergeordnete Feature an:

```
msiexec /i emsx_nt64.msi /qn ADDLOCAL=ALL REMOVE=NetworkProtection
```

✓ Alternativ können Sie den Parameter `ADDEXCLUDE` verwenden, in diesem Fall müssen Sie jedoch alle untergeordneten Features angeben:

```
msiexec /i emsx_nt64.msi /qn ADDEXCLUDE=NetworkProtection,WebAccessProtection,IdsAndBotnetProtection,^
ProtocolFiltering,MailPlugins,EmailClientProtection
```

Sie können einfache Konfigurationsparameter im Installationsbefehl angeben, um Ihr ESET Mail Security nach der Installation automatisch zu konfigurieren.

✓ ESET Mail Security installieren und ESET LiveGrid® deaktivieren:

```
msiexec /i emsx_nt64.msi /qn /l*xv msi.log CFG_LIVEGRID_ENABLED=0
```

Liste aller Konfigurationseigenschaften:

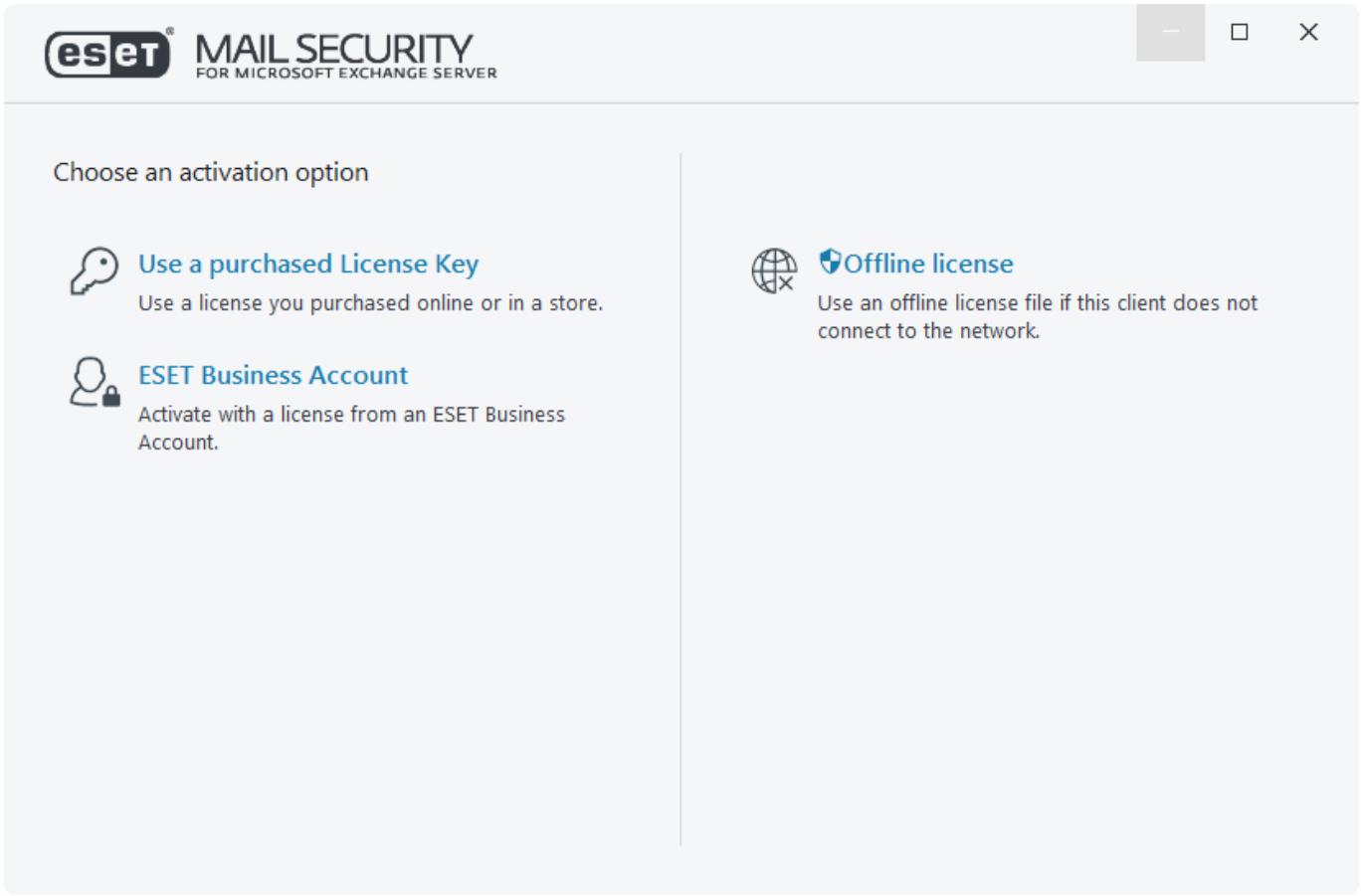
Schalter	Wert
`CFG_POTENTIALLYUNWANTED_ENABLED=1/0`	0 – deaktiviert, 1 – aktiviert
`CFG_LIVEGRID_ENABLED=1/0`	0 – deaktiviert, 1 – aktiviert
`FIRSTSCAN_ENABLE=1/0`	0 – deaktiviert, 1 – aktiviert
`CFG_PROXY_ENABLED=0/1`	0 – deaktiviert, 1 – aktiviert
`CFG_PROXY_ADDRESS=<ip>`	IP-Adresse des Proxyservers
`CFG_PROXY_PORT=<port>`	Proxy-Portnummer
`CFG_PROXY_USERNAME=<user>`	Nutzername für die Authentifizierung
`CFG_PROXY_PASSWORD=<pass>`	Passwort für die Authentifizierung

Sprachparameter: Produktsprache (beide Parameter müssen angegeben werden)

Schalter	Wert
`PRODUCT_LANG=`	LCID-Dezimalzahl (Gebietsschema-ID), zum Beispiel 1033 für English - United States (siehe auch Liste der Sprachcodes).
`PRODUCT_LANG_CODE=`	LCID-Zeichenfolge in Kleinbuchstaben, zum Beispiel en-us für English - United States (siehe auch Liste der Sprachcodes).

Produktaktivierung

Nach Abschluss der Installation werden Sie aufgefordert, Ihr Produkt zu aktivieren.



Sie können ESET Mail Security mit einer der folgenden Methoden aktivieren:

Gekauften Lizenzschlüssel

Geben Sie Ihren von ESET ausgestellten Lizenzschlüssel manuell oder per Kopieren/Einfügen in das Feld **Lizenzschlüssel** ein und klicken Sie auf **Weiter**. Geben Sie den Lizenzschlüssel genau so ein, wie er angezeigt wird, inklusive der Bindestriche. Falls Sie den Lizenzschlüssel kopieren und einfügen, stellen Sie sicher, dass Sie nicht versehentlich zusätzliche Leerzeichen um den Text herum auswählen.

ESET Business Account

Verwenden Sie diese Option, wenn Sie sich registriert haben und Ihre ESET Business Account-Lizenz in Ihr ESET Mail Security importiert haben.

Offline-Lizenzdatei

Dies ist eine automatisch generierte Datei, die an das ESET Produkt übertragen wird. Die Offline-Lizenzdatei wird im Lizenzportal generiert und in Umgebungen verwendet, in denen sich die Anwendung nicht mit der Lizenzierungsstelle verbinden kann.

Klicken Sie auf **Später mit ESET PROTECT aktivieren**, wenn der Computer Teil eines verwalteten Netzwerks ist und der Administrator die Aktivierung remote über ESET PROTECT ausführt. Wählen Sie diese Option nur aus, wenn der Client später aktiviert werden soll.

Sie können im Programmfenster auf **Hilfe und Support** > **Lizenz ändern** klicken, um Ihre Lizenzinformationen zu verwalten. Hier finden Sie die öffentliche Lizenz-ID, die Ihr Produkt und Ihre Lizenz identifiziert. Ihr Benutzername, unter dem der Computer registriert ist, befindet sich im Bereich Über, den Sie per Rechtsklick auf das Symbol im Windows-Benachrichtigungsbereich erreichen.

Nach der erfolgreichen Aktivierung von ESET Mail Security wird das Programmfenster geöffnet, und unter Überwachung wird der aktuelle Status angezeigt. Bei der ersten Verwendung sind möglicherweise einige Eingaben erforderlich, beispielsweise müssen Sie angeben, ob Sie an ESET LiveGrid® teilnehmen möchten.

Im Hauptprogrammfenster werden außerdem Benachrichtigungen zu anderen Elementen wie Systemupdates (Windows-Update) oder Updates der Erkennungsroutine angezeigt. Wenn alle Ereignisse behoben sind, die Ihre Aufmerksamkeit erfordern, wird der Überwachungsstatus in grün mit der Meldung **Sie sind geschützt** angezeigt.

Sie können das Produkt auch im Hauptmenü unter **Hilfe und Support** > **Produkt aktivieren** oder **Schutzstatus** > **Produkt ist nicht aktiviert** aktivieren.

ESET PROTECT kann Clientcomputer mithilfe von Lizenzen, die ein Administrator bereitstellt, im Hintergrund aktivieren.

Aktivierung erfolgreich

ESET Mail Security ist jetzt aktiviert. Ab jetzt erhält ESET Mail Security regelmäßige Updates, um die neuesten Bedrohungen zu erkennen und Ihren Computer zu schützen.

Klicken Sie auf **Fertig**, um die Produktaktivierung abzuschließen.

Aktivierungsfehler

Probleme bei der Aktivierung von ESET Mail Security können unter anderem die folgenden Ursachen haben:

- Lizenzschlüssel wird bereits verwendet
- Ungültiger Lizenzschlüssel – Fehler im Produktaktivierungsformular
- Fehlende oder ungültige Informationen müssen behoben werden
- Fehler bei der Kommunikation mit der Aktivierungsdatenbank. Versuchen Sie es in 15 Minuten erneut.
- Verbindung zu ESET Aktivierungsservern nicht verfügbar oder deaktiviert

Vergewissern Sie sich, dass Sie einen korrekten **Lizenzschlüssel** eingegeben oder eine **Offline-Lizenz** angehängt haben, und versuchen Sie es erneut.

Falls Sie ihr Produkt nicht aktivieren können, empfehlen wir den Fehlerbehebungsassistenten für die Aktivierung.

Lizenz

Sie werden aufgefordert, eine Lizenz für ESET Mail Security auszuwählen, die Ihrem Konto zugeordnet ist. Klicken Sie auf **Weiter**, um die Aktivierung fortzusetzen.

Aktualisierung auf die neueste Version

Neuere Versionen von ESET Mail Security werden veröffentlicht, um Verbesserungen bereitzustellen oder Probleme zu korrigieren, die mit einem automatischen Update der Programmmodule nicht behoben werden können.

Upgrademethoden:

• **Deinstallation / Installation** – Bei dieser Methode wird die zunächst die alte Version entfernt und anschließend die neue Version installiert. Laden Sie die neueste Version von ESET Mail Security. Exportieren Sie die Einstellungen aus Ihrem vorhandenen ESET Mail Security, falls Sie die Konfiguration behalten möchten. Deinstallieren Sie ESET Mail Security und starten Sie den Server neu. Führen Sie eine neue Installation mit dem heruntergeladenen Installationsprogramm durch. Importieren Sie die Einstellungen, um Ihre Konfiguration zu laden. Verwenden Sie dieses Verfahren, wenn Sie nur einen einzigen Server mit ESET Mail Security betreiben.

• **Vor Ort** – Bei dieser Upgrademethode wird die neue Version von ESET Mail Security über die vorhandene Version installiert, ohne diese zu entfernen.

Achten Sie darauf, dass auf Ihrem Server **keine Windows Updates ausstehen** und kein **Neustart** aufgrund von Windows Updates oder aus anderen Gründen geplant ist. Wenn Sie versuchen, ein Vor-Ort-Upgrade auf einem Computer mit ausstehendem Windows-Update oder Neustart auszuführen, wird die vorhandene Version von ESET Mail Security möglicherweise nicht korrekt entfernt. Außerdem können Probleme auftreten, wenn Sie anschließend versuchen, die alte Version von ESET Mail Security manuell zu entfernen.

Während des Upgrades von ESET Mail Security muss der Server neu gestartet werden.

• Remote - Für große Netzwerkumgebungen, die mit ESET PROTECT verwaltet werden. Dies ist eine saubere Upgrademethode, die remote ausgeführt wird. Dieses Verfahren ist hilfreich, wenn Sie mehrere Server mit ESET Mail Security betreiben.

• ESET-Clusterassistent - Kann auch als Upgrademethode verwendet werden. Verwenden Sie dieses Verfahren, falls Ihre Umgebung mindestens zwei Server mit ESET Mail Security enthält. Dies ist eine Vor-Ort-Upgrademethode, die über das ESET-Cluster ausgeführt wird. Außerdem können Sie das ESET-Cluster nach der Aktualisierung beibehalten und dessen Funktionen weiterhin nutzen.

Beim Upgrade von Version 4.x werden nicht alle Einstellungen beibehalten. Insbesondere Regeln können nicht migriert werden. Der Grund hierfür sind Änderungen an den Regeln, die in späteren Produktversionen vorgenommen wurden. Notieren Sie sich daher Ihre Regeleinstellungen, bevor Sie ein Upgrade von Version 4.x durchführen. Nach Abschluss des Upgrades können Sie Regeln einrichten. Die neuen Regeln bieten mehr Flexibilität und mehr Möglichkeiten im Vergleich zu den Regeln in früheren Versionen von ESET Mail Security.

Die folgenden Einstellungen werden aus früheren Versionen von ESET Mail Security übernommen:

• Allgemeine Konfiguration von ESET Mail Security.

Einstellungen des Spam-Schutzes:

• Alle Einstellungen, die in früheren Versionen identisch sind, werden übernommen. Für neue Einstellungen

werden die Standardwerte angewendet.

- Einträge in den Positiv- und Negativlisten.

Nach der Aktualisierung von ESET Mail Security sollten Sie die Einstellungen überprüfen, um sicherzustellen, dass die Software korrekt nach Ihren Anforderungen konfiguriert ist.

Upgrades über ESET PROTECT

Mit ESET PROTECT können Sie mehrere Server aktualisieren, auf denen eine ältere Version von ESET Mail Security ausgeführt wird. Mit dieser Methode können Sie eine große Anzahl an Servern gleichzeitig aktualisieren und dabei sicherstellen, dass ESET Mail Security auf allen Servern gleich konfiguriert ist (falls gewünscht).

Das Verfahren umfasst die folgenden Schritte:

- **Aktualisieren Sie den ersten Server** manuell, indem Sie die neueste Version von ESET Mail Security über Ihre vorhandene Version installieren, um Ihre Konfiguration beizubehalten, inklusive Regeln sowie mehrere White- und Blacklists. Dieser Schritt wird lokal auf dem Server ausgeführt, auf dem ESET Mail Security läuft.

- **Fordern Sie die Konfiguration** des auf Version 7.x aktualisierten ESET Mail Security an und konvertieren Sie die Konfiguration in ESET PROTECT zu einer Policy. Die Policy wird später auf alle aktualisierten Server angewendet. Dieser und die folgenden Schritte werden remote mithilfe von ESET PROTECT ausgeführt.

- **Führen Sie den Task Software-Deinstallation** auf allen Servern aus, auf denen eine alte Version von ESET Mail Security läuft.

- **Führen Sie den Task „Software-Installation“ auf allen Servern aus**, auf denen die neueste Version von ESET Mail Security installiert werden soll.

- **Weisen Sie die Konfigurationsrichtlinie** zu allen Servern zu, auf denen die aktuelle Version von ESET Mail Security läuft.

Führen Sie die folgenden Anweisungen aus, um ein Upgrade mit ESET PROTECT durchzuführen.

1. Melden Sie sich bei einem der Server an, auf denen ESET Mail Security läuft, und führen Sie ein Upgrade durch, indem Sie die aktuelle Version herunterladen und über die vorhandene Version installieren. Führen Sie die Schritte für eine normale Installation aus. Ihre ursprüngliche Konfiguration für ESET Mail Security bleibt bei der Installation erhalten.

2. Öffnen Sie die ESET PROTECT-**Web-Konsole**, wählen Sie einen Clientcomputer in einer statischen oder dynamischen Gruppe aus, und klicken Sie auf **Details anzeigen**.

3. Wählen Sie die Registerkarte Konfiguration aus und klicken Sie auf die Schaltfläche **Konfiguration anfordern**, um die Konfigurationen für Ihr verwaltetes Produkt abzurufen. Dieser Prozess kann einige Zeit dauern. Nachdem die aktuelle Konfiguration in der Liste angezeigt wird, klicken Sie auf **Sicherheitsprodukt** und wählen Sie **Konfiguration öffnen** aus.

4. Klicken Sie auf die Schaltfläche **In Policy umwandeln**, um eine Konfigurations-Policy zu erstellen. Geben Sie einen **Namen** für die neue Richtlinie ein und klicken Sie auf **Fertig stellen**.

5. Auswählen **Clienttasks** und wählen Sie den Task Software-Deinstallation aus. Achten Sie beim Erstellen des

Deinstallationstasks darauf, den Server nach der Deinstallation neu zu starten, indem Sie das Kontrollkästchen **Bei Bedarf automatisch neu starten** markieren. Erstellen Sie den Task und fügen Sie alle gewünschten Zielcomputer für die Deinstallation hinzu.

6. Vergewissern Sie sich, dass ESET Mail Security von allen Zielen deinstalliert wurde.

7. Erstellen Sie einen Task Software-Installation, um die aktuelle Version von ESET Mail Security auf allen Zielen zu installieren.

8. **Weisen Sie die Konfigurationsrichtlinie** zu allen Servern zu, auf denen ESET Mail Security läuft, idealerweise in einer Gruppe.

Upgrades per ESET-Cluster

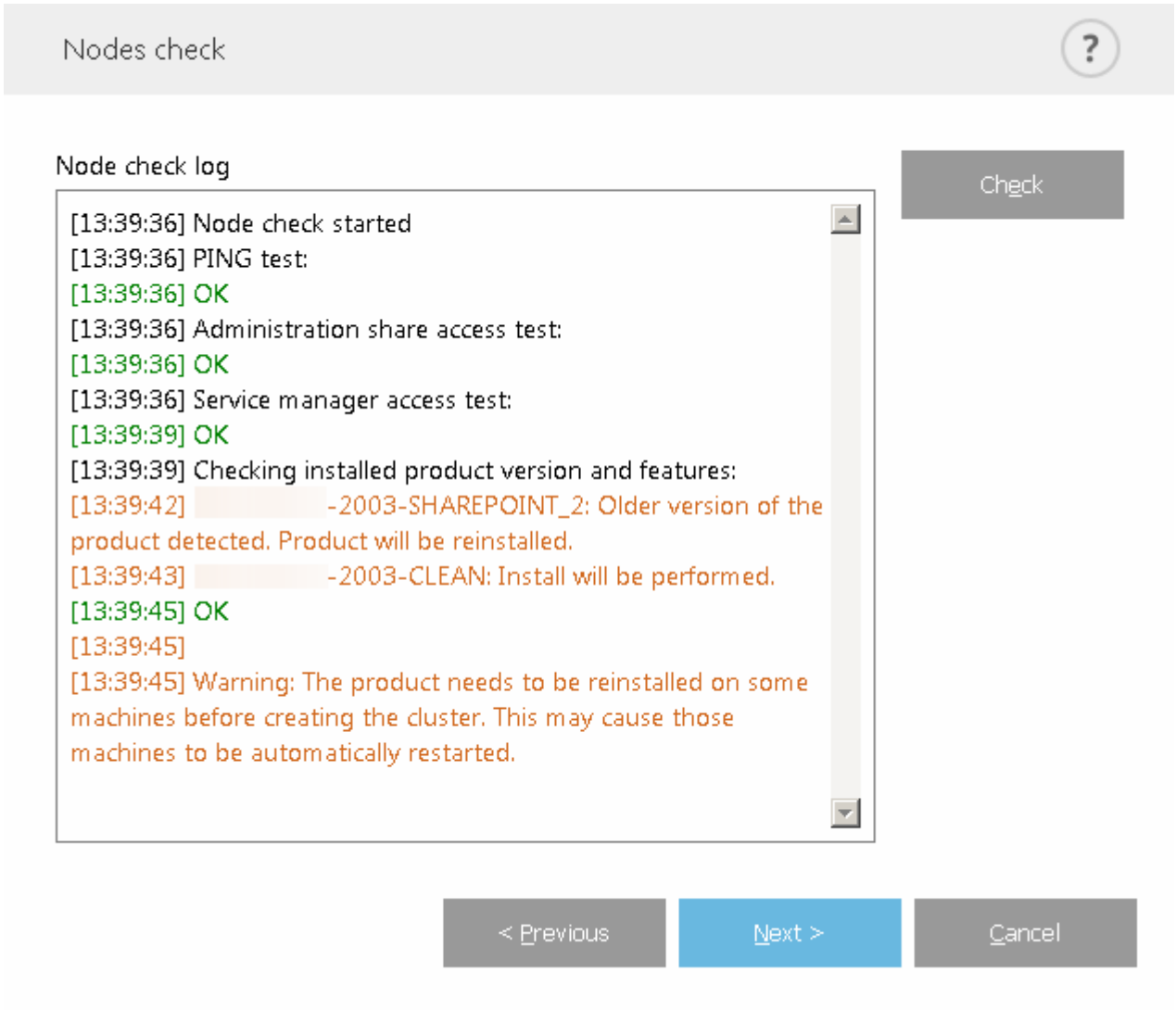
Mit einem ESET-Cluster können Sie mehrere Server aktualisieren, auf denen ältere Versionen von ESET Mail Security laufen. Wir empfehlen den Einsatz eines ESET-Clusters, wenn Ihre Umgebung mindestens zwei Server mit ESET Mail Security enthält. Außerdem können Sie mit dieser Upgrademethode weiterhin Ihr ESET-Cluster verwenden, um die Konfiguration von ESET Mail Security auf allen Mitgliedsknoten zu synchronisieren.

Führen Sie die folgenden Schritte aus, um ein Upgrade mit dieser Methode durchzuführen:

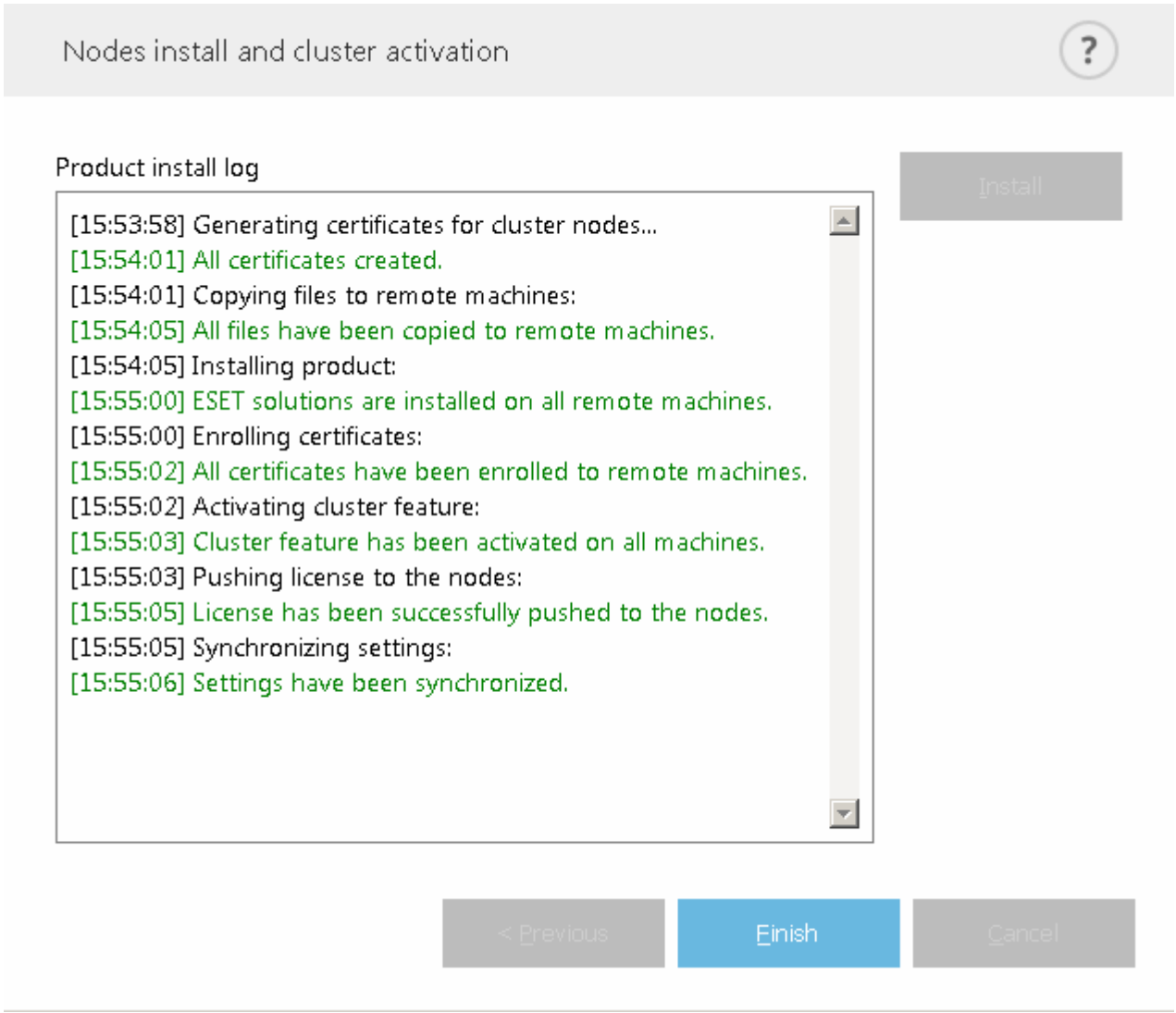
1. Melden Sie sich bei einem der Server an, auf denen ESET Mail Security läuft, und führen Sie ein Upgrade durch, indem Sie die aktuelle Version herunterladen und über die vorhandene Version installieren. Führen Sie die Schritte für eine normale Installation durch. Die gesamte Konfiguration Ihrer alten ESET Mail Security-Version bleibt bei der Installation erhalten.

2. Führen Sie den ESET-Cluster-Assistenten aus und fügen Sie Clusterknoten hinzu (Server, auf denen Sie ESET Mail Security aktualisieren möchten). Bei Bedarf können Sie weitere Server hinzufügen, auf denen ESET Mail Security noch nicht läuft. Auf diesen Servern wird eine Neuinstallation durchgeführt. Verwenden Sie bei der Angabe von Clustername und Installationstyp die Standardeinstellungen (aktivieren Sie die Option Lizenz auf Knoten ohne aktiviertes Produkt übertragen).

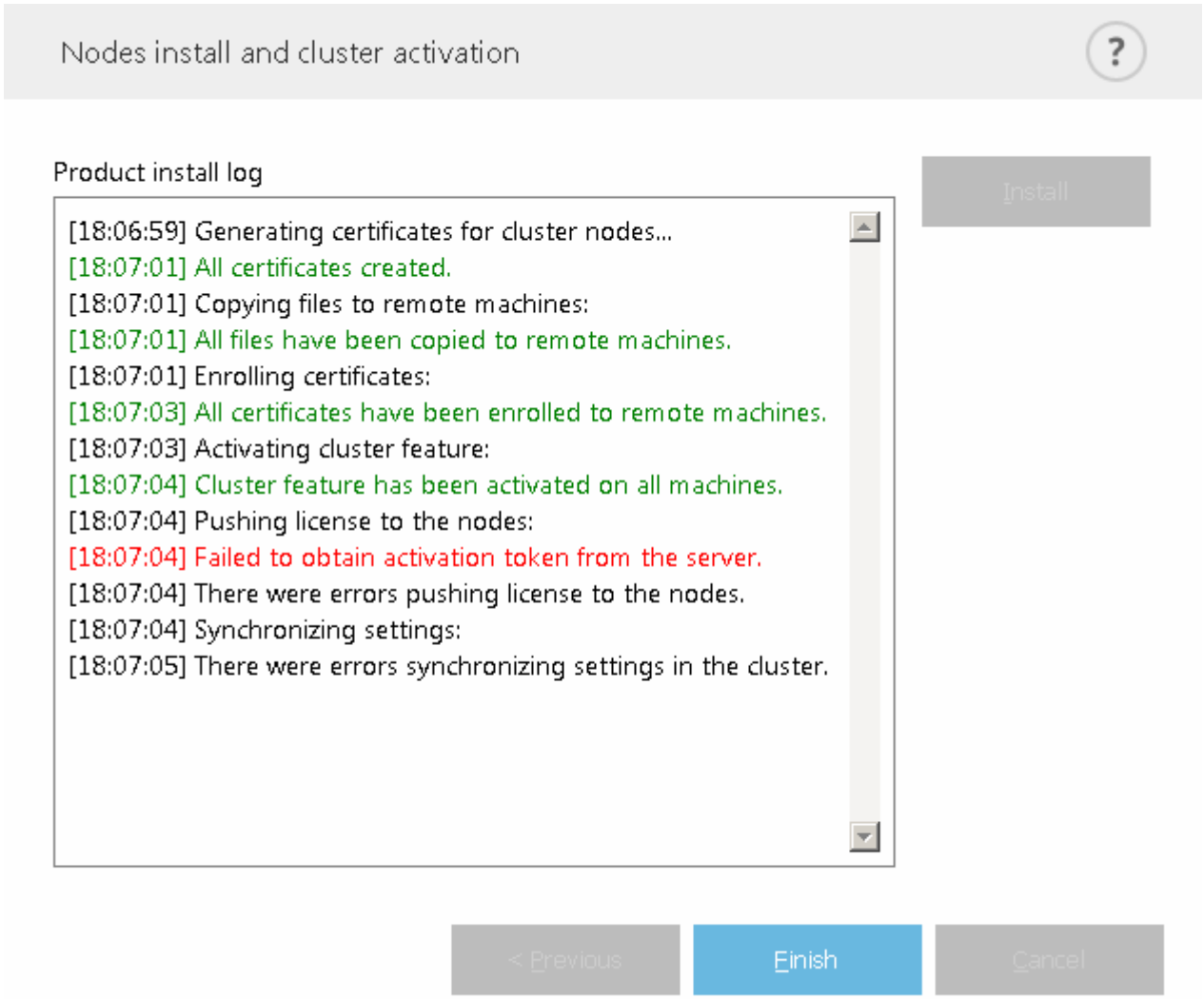
3. Überprüfen Sie den Bildschirm Knotenprüfungs-Log. Dort werden Server angezeigt, auf denen ältere Produktversionen laufen und auf denen eine Neuinstallation durchgeführt wird. ESET Mail Security wird auch auf allen hinzugefügten Servern installiert, auf denen das Produkt noch nicht installiert ist.



4. Auf dem Bildschirm **Knoteninstallation und Clusteraktivierung** wird der Installationsfortschritt angezeigt. Nach dem erfolgreichen Abschluss der Installation sollte ein Ergebnis angezeigt werden, das der folgenden Ausgabe ähnelt:



Falls Ihr Netzwerk oder Ihr DNS nicht korrekt konfiguriert ist, wird möglicherweise die Fehlermeldung **Fehler beim Abrufen des Aktivierungs-Tokens vom Server** angezeigt. Führen Sie in diesem Fall den ESET-Cluster-Assistenten erneut aus. Dabei wird das Cluster gelöscht und ein neues erstellt, ohne das Produkt neu zu installieren. Anschließend sollte die Aktivierung funktionieren. Überprüfen Sie Ihre Netzwerk- und DNS-Einstellungen, falls das Problem weiterhin auftritt.



Installation in einer Cluster-Umgebung

Sie können ESET Mail Security in einer Cluster-Umgebung bereitstellen (z. B. in einem Failover-Cluster). Dabei sollten Sie ESET Mail Security nach Möglichkeit auf einem aktiven Knoten installieren und die Installation anschließend mit der Funktion ESET Cluster von ESET Mail Security auf die passiven Knoten verteilen. Neben der Installation dient ESET Cluster auch als Replikation für die ESET Mail Security-Konfiguration, um sicherzustellen, dass die Clusterknoten für den korrekten Betrieb einheitlich konfiguriert sind.

Terminalserver

Wenn Sie ESET Mail Security auf einem Windows-Server installieren, der als Terminalserver eingerichtet ist, sollten Sie die grafische Benutzeroberfläche von ESET Mail Security deaktivieren, da diese sonst bei jeder Benutzeranmeldung gestartet wird. Nähere Informationen hierzu finden Sie im Abschnitt Deaktivieren der Benutzeroberfläche auf Terminalserver.

Multiserver / DAG-Umgebung

ESET Mail Security unterstützt Umgebungen mit mehreren Servern. In Infrastrukturen mit mehreren Servern, zum Beispiel Datenbankverfügbarkeitsgruppen, können Sie ESET Mail Security auf allen Exchange Server mit

Postfachrolle installieren.

Wir empfehlen, ESET Mail Security auf allen Servern über den ESET-Cluster zu installieren. Wir empfehlen außerdem, die Option ESET Cluster verwenden, um alle Nachrichten in der Quarantäne auf einem Knoten zu speichern in den Einstellungen für die E-Mail-Quarantäne zu aktivieren. Falls Sie Greylisting verwenden möchten, aktivieren Sie außerdem die Option Greylisting-Datenbanken im ESET-Cluster synchronisieren.

Erste Schritte

Die folgenden Themen helfen Ihnen bei den ersten Schritten mit ESET Mail Security.

Überwachung

Hier finden Sie eine kurze Übersicht über den aktuellen Status von ESET Mail Security und können mühelos erkennen, ob irgendein Problem Ihre Aufmerksamkeit erfordert.

Verwaltung über ESET PROTECT

Mit ESET PROTECT können Sie ESET Mail Security remote verwalten. Der folgende Abschnitt erleichtert Ihnen den Einstieg in ESET Mail Security.

Tasks nach der Installation

Hier erhalten Sie Hilfestellungen für Ihre Ausgangskonfiguration.

Tasks nach der Installation

Die folgenden empfohlenen Tasks befassen sich mit der Ausgangskonfiguration Ihrer ESET Mail Security-Installation.

Thema	Beschreibung
Produktaktivierung	Vergewissern Sie sich, dass Ihr ESET Mail Security aktiviert ist. Sie können die Aktivierung auf verschiedene Arten durchführen.
Update	Nach der Aktivierung des Produkts werden die Module automatisch aktualisiert. Überprüfen Sie den Updatestatus, um herauszufinden, ob das Update erfolgreich war.
E-Mail-Quarantäne-Manager	Machen Sie sich mit dem E-Mail-Quarantäne-Manager vertraut, den Sie über das Hauptprogrammfenster der Anwendung erreichen. Mit dieser Funktion können Sie Nachrichten in der Quarantäne wie Spam, infizierte Anhänge mit Malware, Phishing-Nachrichten und Nachrichten mit Regeltreffern verwalten. Sie können die Details der einzelnen Nachrichten anzeigen und eine Aktion ausführen (freigeben oder löschen).
Web-Oberfläche für die E-Mail-Quarantäne	Die Web-Oberfläche für die E-Mail-Quarantäne ist eine Alternative zum E-Mail-Quarantäne-Manager für die Remoteverwaltung der Elemente in der Quarantäne. In der Weboberfläche der E-Mail-Quarantäne können Benutzer (E-Mail-Empfänger) außerdem ihre in die Quarantäne verschobenen Nachrichten verwalten. Die Benutzer werden mit den per E-Mail verschickten E-Mail-Quarantäneberichten über neue Inhalte in der Quarantäne informiert. Wir empfehlen, die Berichte zu konfigurieren.

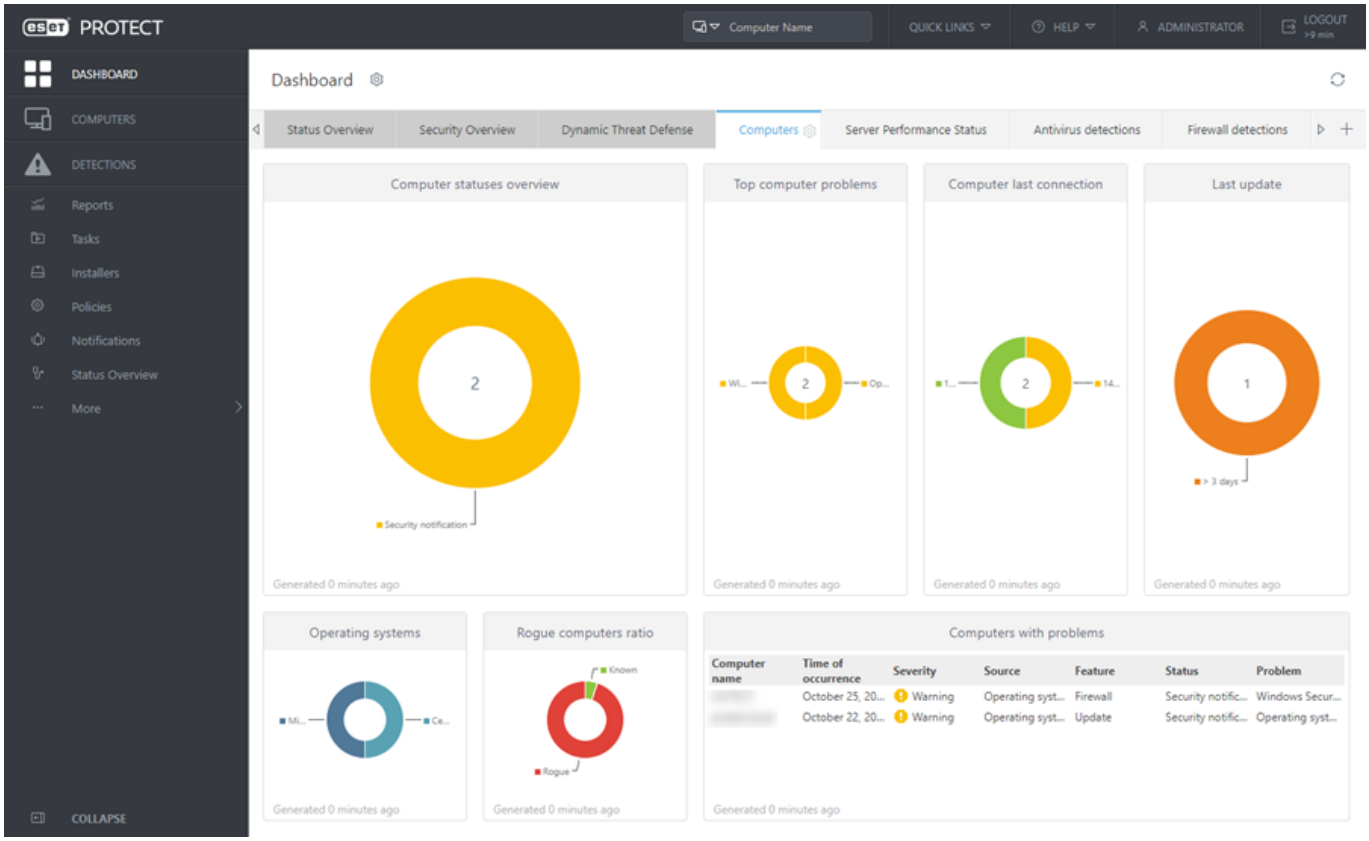
Thema	Beschreibung
E-Mail-Quarantäneberichte	Erstellen Sie einen geplanten Task, um die E-Mail-Quarantäneberichte an sich selbst und an ausgewählte Benutzer zu verschicken, damit diese bestimmte Arten von falsch positiven Nachrichten freigeben (zustellen) und den Inhalt ihrer Quarantäne über die Web-Oberfläche für die E-Mail-Quarantäne (Online-Viewer) verwalten können. Die Benutzer können auf einen Link in den E-Mail-Quarantäneberichten klicken und sich mit ihren Domänenanmeldedaten anmelden, um zur Weboberfläche zu gelangen.
Spam-Schutz – Filterung und Verifizierung	Der Spam-Schutz ist eine ausgeklügelte cloudbasierte Funktion, die Ihre Benutzer (E-Mail-Empfänger) vor Spam-Nachrichten schützt. Verwenden Sie die Filter- und Verifizierungsfunktionen und fügen Sie Ihre lokalen IP-Adressen zur Liste der ignorierten IP-Adressen hinzu. Anschließend werden die IP-Adressen in Ihrer Netzwerkinfrastruktur bei der Klassifizierung ignoriert. Außerdem können Sie den Rest der zugelassenen, blockierten und ignorierten Listen konfigurieren, um die Filter- und Verifizierungsfunktionen anzupassen. Bei Bedarf können Sie auch die Greylisting-Funktion aktivieren.
Regeln	Mit dieser leistungsstarken Funktion können Sie E-Mails anhand von definierten Bedingungen und Aktionen filtern. Sie können vordefinierte Regeln verwenden oder anpassen oder eigene, maßgeschneiderte Regeln für Ihre Anforderungen erstellen. Sie können Regeln für sämtliche Schutzebenen (Mail-Transport-Schutz, Postfach-Datenbankschutz oder On-Demand Postfachdatenbank-Scan) konfigurieren.
Virenschutz testen	Überprüfen, ob der Virenschutz korrekt funktioniert.
Spam-Schutz testen	Überprüfen, ob der Spam-Schutz korrekt funktioniert.
Phishing-Schutz testen	Überprüfen, ob der Phishing-Schutz korrekt funktioniert.

Verwaltung über ESET PROTECT

ESET PROTECT ist eine Anwendung, mit der Sie ESET-Produkte in einer Netzwerkumgebung von einem zentralen Standort aus verwalten können. Das Task-Management-System von ESET PROTECT ermöglicht das Installieren von ESET-Sicherheitslösungen auf Remotecomputern und eine schnelle Reaktion auf neue Probleme und Bedrohungen.

ESET PROTECT bietet keinen Schutz vor dem eigentlichen Schadcode, sondern verlässt sich dafür auf die auf jedem Client installierte ESET-Sicherheitslösung.

ESET-Sicherheitslösungen unterstützen Netzwerke mit verschiedenen Plattformtypen. Ihr Netzwerk kann eine Kombination aus aktuellen Microsoft-, Linux-basierten, macOS- und mobilen Betriebssystemen enthalten.



Weitere Informationen finden Sie in der ESET PROTECT-Onlinehilfe.

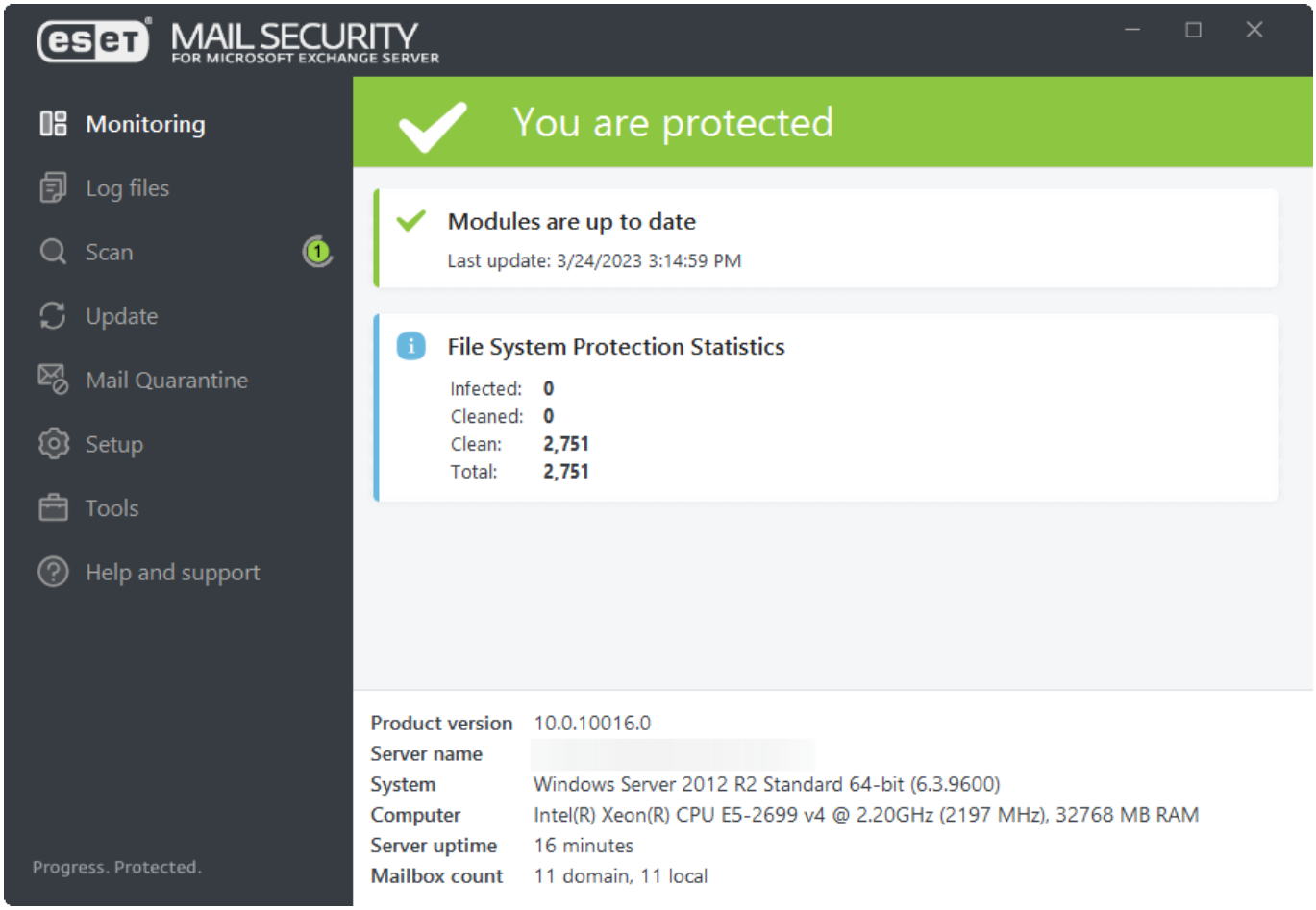
Überwachung

Der im Bereich **Überwachung** angezeigt Schutzstatus enthält Informationen über die aktuelle Schutzstufe Ihres Computers. Im Hauptfenster wird der aktuelle Betriebszustand von ESET Mail Security angezeigt.

Das grüne Schutzstatussymbol und die Meldung **Sie sind geschützt** zeigen an, dass der maximale Schutz gewährleistet ist.

Das rote Symbol weist auf kritische Probleme hin. Der maximale Schutz Ihres System ist nicht gewährleistet. Die Details zur Fehlermeldung enthalten zusätzliche Informationen zum aktuellen Status. Wenn Sie ein Problem nicht beheben können, öffnen Sie die ESET-Knowledgebase. Wenn Sie weiterhin Unterstützung benötigen, können Sie eine Supportanfrage übermitteln. Unser technischer Support wird sich zeitnah mit Ihnen in Verbindung setzen, um Ihre Fragen zu beantworten und Lösungen für Ihr Problem zu finden. Für eine vollständige Liste der Statusmeldungen öffnen Sie die **Erweiterten Einstellungen** (**F5**), navigieren Sie zu **Benachrichtigungen** > Anwendungsstatus und klicken Sie auf **Bearbeiten**.

Das orangefarbene Symbol weist auf ein nicht-kritisches Problem in Ihrem ESET-Produkt hin.



Richtig funktionierende Module sind mit einem grünen Häkchen gekennzeichnet. Nicht vollständig funktionsfähige Module werden mit einem roten Ausrufezeichen oder einem orangen Benachrichtigungssymbol gekennzeichnet. Weitere Informationen zum Modul werden im oberen Teil des Fensters eingeblendet. Unter anderem finden Sie dort einen Vorschlag zur Behebung des Problems.

Um den Status einzelner Module zu ändern, klicken Sie im Hauptmenü auf Einstellungen und wählen das gewünschte Modul aus.

Die Überwachungsseite enthält Informationen zu Ihrem System, darunter:

- Produktversion - Versionsnummer von ESET Mail Security.
- Servername - Hostname oder FQDN des Computers.
- System - Details zum Betriebssystem.
- Computer - Hardwaredetails.
- Betriebszeit des Servers - Zeigt an, wie lange das System bereits läuft.

Anzahl Postfächer

ESET Mail Security erkennt die Anzahl der Postfächer und zeigt die Anzahl für die folgenden Erkennungsmethoden an:

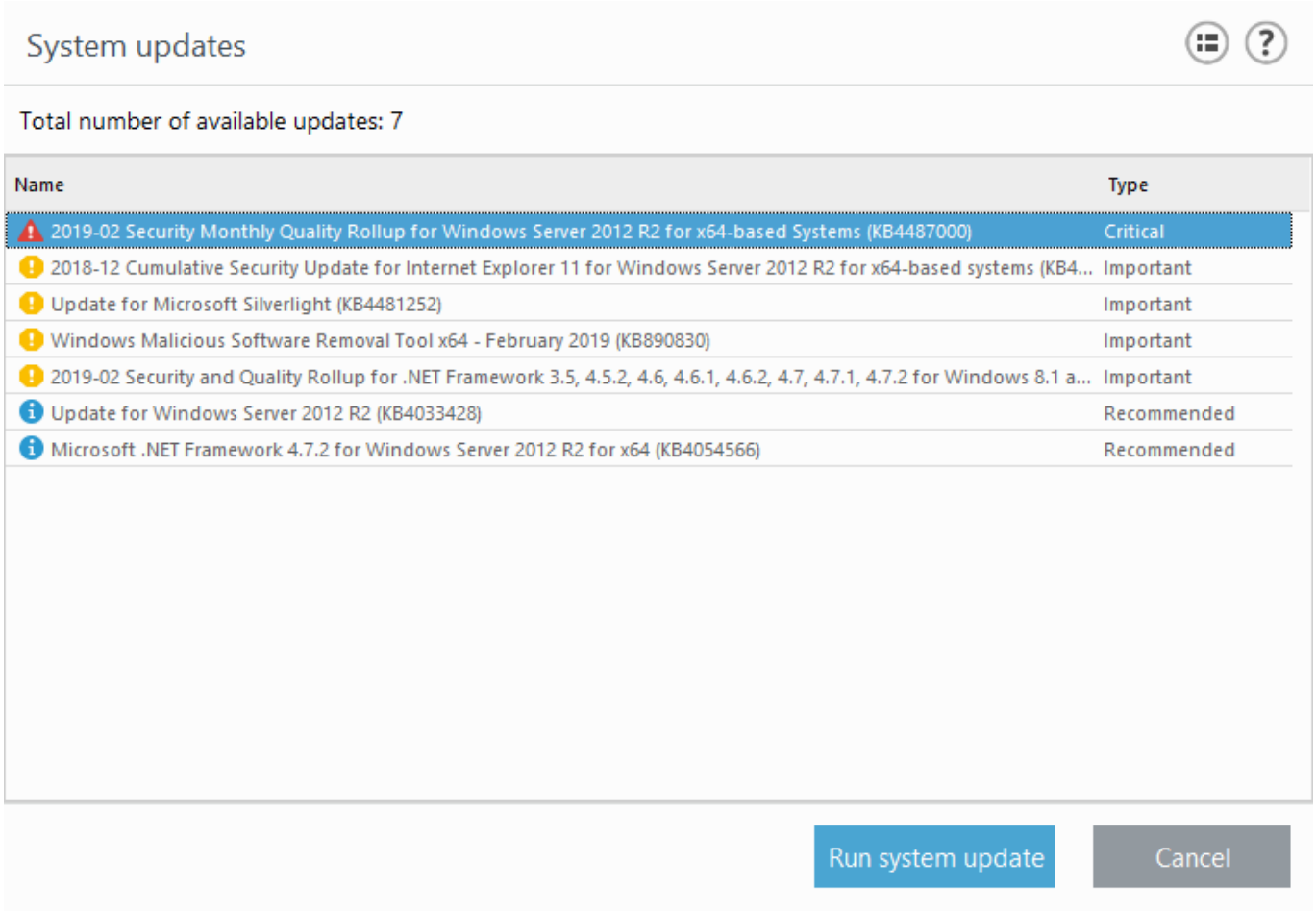
- **Domain** - Anzahl aller Postfächer in einer bestimmten Domäne, zu der der Exchange Server gehört. Diese Anzahl gilt auch für DAG-Umgebungen und die Gesamtzahl der Postfächer.

• **Lokal** – Gibt die Anzahl der Postfächer auf dem Exchange Server an, auf dem ESET Mail Security installiert ist. Wenn der Server zu einer DAG gehört, gibt dieser Wert die Anzahl der Postfächer auf dem lokalen Exchange-Server an, im Gegensatz zur Gesamtzahl in der Domäne.

Wenn Sie ein Problem mit den vorgeschlagenen Lösungen nicht beseitigen können, klicken Sie auf **Hilfe und Support**, um die Hilfedateien zu öffnen, oder durchsuchen Sie die ESET-Knowledgebase. Wenn Sie weiterhin Unterstützung benötigen, können Sie eine Supportanfrage übermitteln. Unser technischer Support wird sich zeitnah mit Ihnen in Verbindung setzen, um Ihre Fragen zu beantworten und Lösungen für Ihr Problem zu finden.

Windows-Update verfügbar

Das Fenster „System-Updates“ enthält verfügbare Updates, die heruntergeladen und installiert werden können. Neben dem Namen des Updates wird die Update-Priorität angezeigt. Klicken Sie mit der rechten Maustaste auf ein beliebiges Update und klicken Sie auf **Mehr Informationen**, um ein Fenster mit zusätzlichen Informationen zu öffnen:



Klicken Sie auf **System-Update durchführen**, um das Fenster **Windows Update** zu öffnen und die System-Updates zu installieren.

Netzwerkisolierung

Mit ESET Mail Security können Sie die Netzwerkverbindung Ihres Servers blockieren. Dies wird auch als Netzwerkisolation bezeichnet. In bestimmten extremen Situationen ist es sinnvoll, einen Server als vorbeugende Maßnahme vom Netzwerk zu isolieren. Zum Beispiel wenn Sie festgestellt haben, dass der Server mit Malware

infiziert ist oder auf eine andere Art und Weise gefährdet ist.

Wenn Sie die Netzwerkisolation aktivieren, wird der gesamte Netzwerkdatenverkehr blockiert, mit den folgenden Ausnahmen:

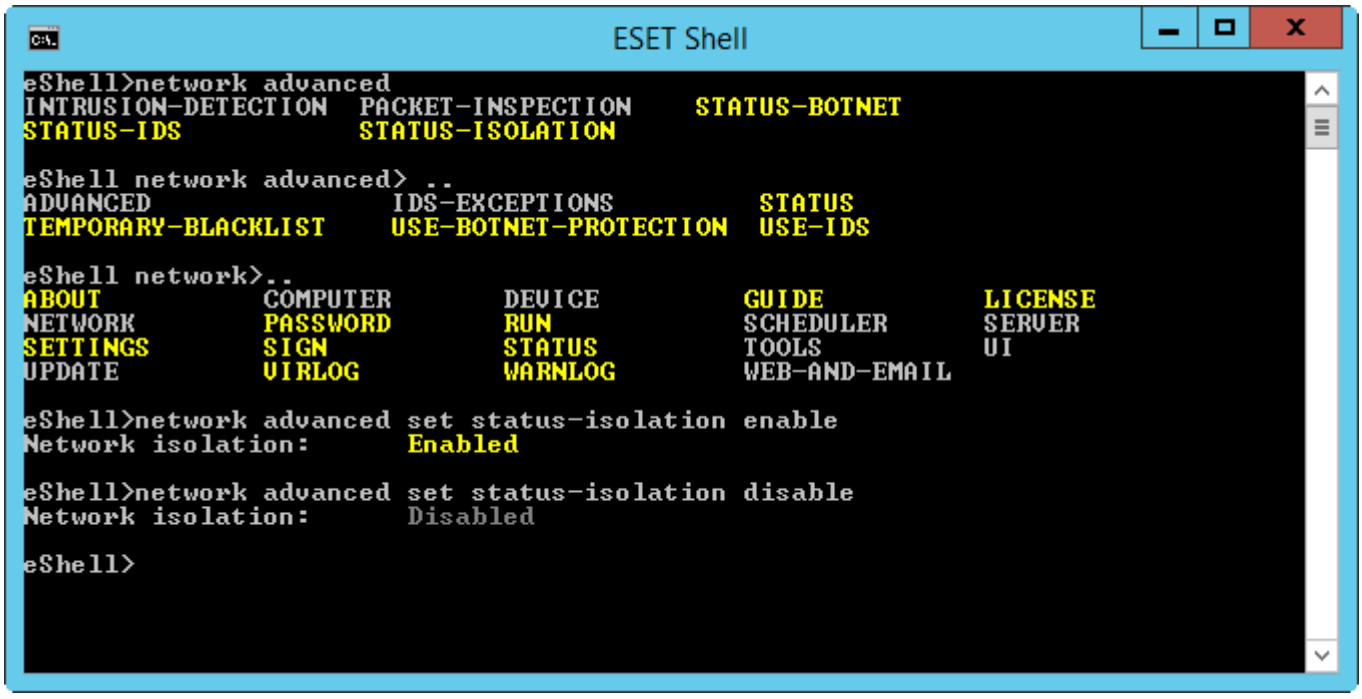
- Die Verbindung zum Domänencontroller bleibt erhalten
- ESET Mail Security kann weiterhin kommunizieren
- Falls vorhanden, können der ESET Management Agent und der ESET Inspect Connector über das Netzwerk kommunizieren

Aktivieren und deaktivieren Sie die Netzwerkisolierung mit dem Befehl eShell oder dem Clienttask ESET PROTECT.

eShell

Im interaktiven Modus:

- Netzwerkisolation aktivieren: `network advanced set status-isolation enable`
- Netzwerkisolation deaktivieren: `network advanced set status-isolation disable`



Alternativ können Sie eine Batch-Datei mit dem Batch-/Skriptmodus erstellen und ausführen.

ESET PROTECT

- Netzwerkisolierung aktivieren per Client-Task.
- Netzwerkisolierung deaktivieren per Client-Task.

Wenn die Netzwerkisolation aktiviert ist, wird der Status von ESET Mail Security in rot angezeigt, zusammen mit der Nachricht **Netzwerkzugriff blockiert**.

Arbeiten mit ESET Mail Security

Dieser Abschnitt enthält eine ausführliche Beschreibung der Benutzeroberfläche des Programms und erklärt die Verwendung von ESET Mail Security.

In der Benutzeroberfläche können Sie schnell auf häufig verwendete Features zugreifen:

- Überwachung
- Log-Dateien
- Prüfen
- Update
- E-Mail-Quarantäne
- Einstellungen
- Tools

Prüfen

Das On-Demand-Prüfungsmodul ist ein wichtiger Bestandteil von ESET Mail Security. Diese Modul prüft Dateien und Ordner auf Ihrem Computer. Um Ihr Netzwerk zu schützen, ist es wichtig, dass die Computerprüfungen nicht nur bei Verdacht auf eine Infektion sondern regelmäßig im Rahmen der Routine-Sicherheitsmaßnahmen durchgeführt werden.

Wir empfehlen eine regelmäßige (z. B. einmal pro Monat) Tiefenprüfung Ihres Systems, um Viren zu finden, die der Echtzeit-Dateischutz nicht erkannt hat. Dies kommt z. B. vor, wenn der Echtzeit-Dateischutz deaktiviert oder die Erkennungsroutine nicht auf dem neuesten Stand ist, oder wenn die Datei beim Speichern auf dem Datenträger nicht als Virus erkannt wird.

Wählen Sie verfügbare On-Demand-Scans für ESET Mail Security aus:

Postfachdatenbankprüfung

Führen Sie eine On-Demand-Datenbankprüfung aus. Sie können die zu prüfenden öffentlichen Ordner, Mailserver und Postfächer auswählen. Außerdem können Sie den Taskplaner verwenden, um die Datenbankprüfung zu einem bestimmten Zeitpunkt oder bei einem bestimmten Ereignis auszuführen.

> Falls Sie Microsoft Exchange Server 2007, 2010, 2013 oder 2016 verwenden, können Sie zwischen Postfach-Datenbankschutz und On-Demand-Datenbankprüfung wählen. Sie können jedoch nur einen Schutztyp gleichzeitig aktivieren. Wenn Sie sich für die On-Demand-Datenbankprüfung entscheiden, müssen Sie die Integration für den Postfach-Datenbankschutz in den erweiterten Einstellungen unter Server deaktivieren. Andernfalls ist die On-Demand-Datenbankprüfung nicht verfügbar.

Microsoft 365-Postfach-Scan

Mit dieser Option können Sie Remote-Postfächer in Microsoft 365-Hybridumgebungen scannen.

Speicher prüfen

Überprüft alle freigegebenen Ordner auf dem lokalen Server. Wenn der Speicher-Scan nicht verfügbar ist, bedeutet dies, dass auf Ihrem Server keine Ordner freigegeben sind.

Scannen Sie Ihren Computer

Ermöglicht eine schnelle Prüfung des Computers und Säuberung infizierter Dateien ohne Eingriff des Benutzers. Ihr Vorteil ist die einfache Bedienung, ohne detaillierte Prüfeinstellungen festlegen zu müssen. Die Prüfung überprüft alle Dateien auf den lokalen Laufwerken und säubert oder löscht Schadsoftware automatisch. Für die Säuberungsstufe wird automatisch der Standardwert verwendet. Weitere Informationen zu den Säuberungstypen finden Sie unter Säuberung.

> Führen Sie nach Möglichkeit mindestens einmal pro Monat eine Computerprüfung durch. Sie können die Prüfung als geplanten Task.

Benutzerdefinierter Scan

Die benutzerdefinierte Prüfung ist eine optimale Lösung, wenn Sie Parameter wie Prüfziele und Prüfmethoden angeben möchten. Die benutzerdefinierte Prüfung bietet den Vorteil, dass Sie die Prüfparameter ausführlich konfigurieren können. Sie können die Konfigurationen in benutzerdefinierten Prüfprofilen speichern, um Prüfungen mit denselben Parametern mehrfach auszuführen.

Wechselmedienscan

Ähnlich der Smart-Prüfung: Starten Sie eine schnelle Prüfung der Wechselmedien (z. B. CD/DVD/USB), die mit Ihrem Computer verbunden sind. Dies ist hilfreich, wenn Sie einen USB-Speicherstick mit Ihrem Computer verbinden und dessen Inhalte auf Schadsoftware und andere Bedrohungen prüfen möchten. Sie können diese Prüfung auch über Benutzerdefinierter Scan starten, indem Sie im Dropdown-Menü Zu prüfende Objekte den Eintrag Wechselmedien auswählen und auf Prüfen klicken.

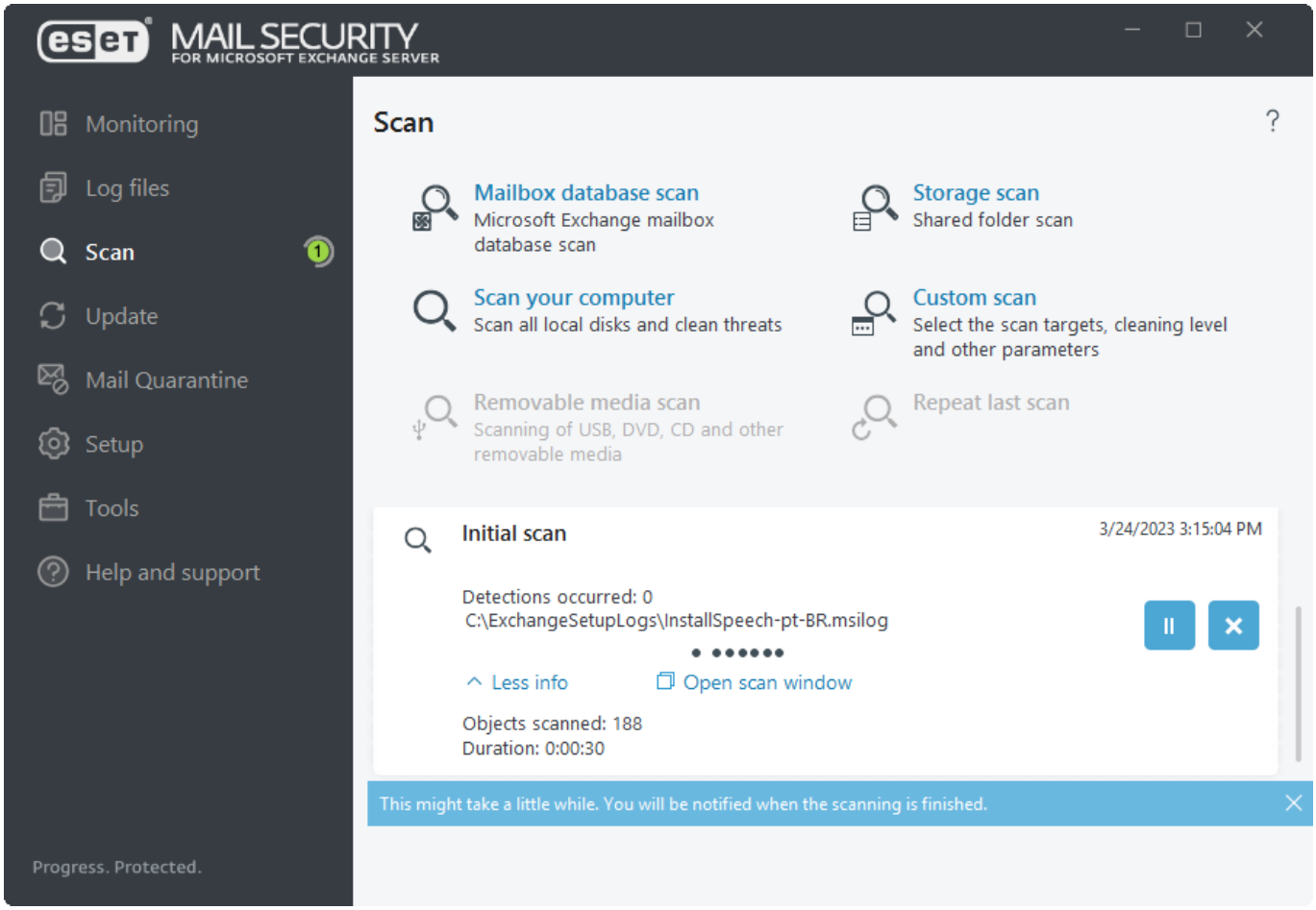
Hyper-V-Scan

Diese Option wird nur im Menü angezeigt, wenn ein Hyper-V-Manager auf dem Server installiert ist, auf dem ESET Mail Security ausgeführt wird. Mit dem Hyper-V-Scan können virtuelle Computerlaufwerke auf Microsoft Hyper-V-Servern geprüft werden, ohne auf der jeweiligen VM einen „Agent“ installieren zu müssen.

Letzte Prüfung wiederholen

Wiederholt Ihren letzten Scanvorgang mit denselben Einstellungen.

> Die Funktion zum Wiederholen der letzten Prüfung ist nicht verfügbar, wenn eine On-Demand-Datenbankprüfung ausgeführt wird.



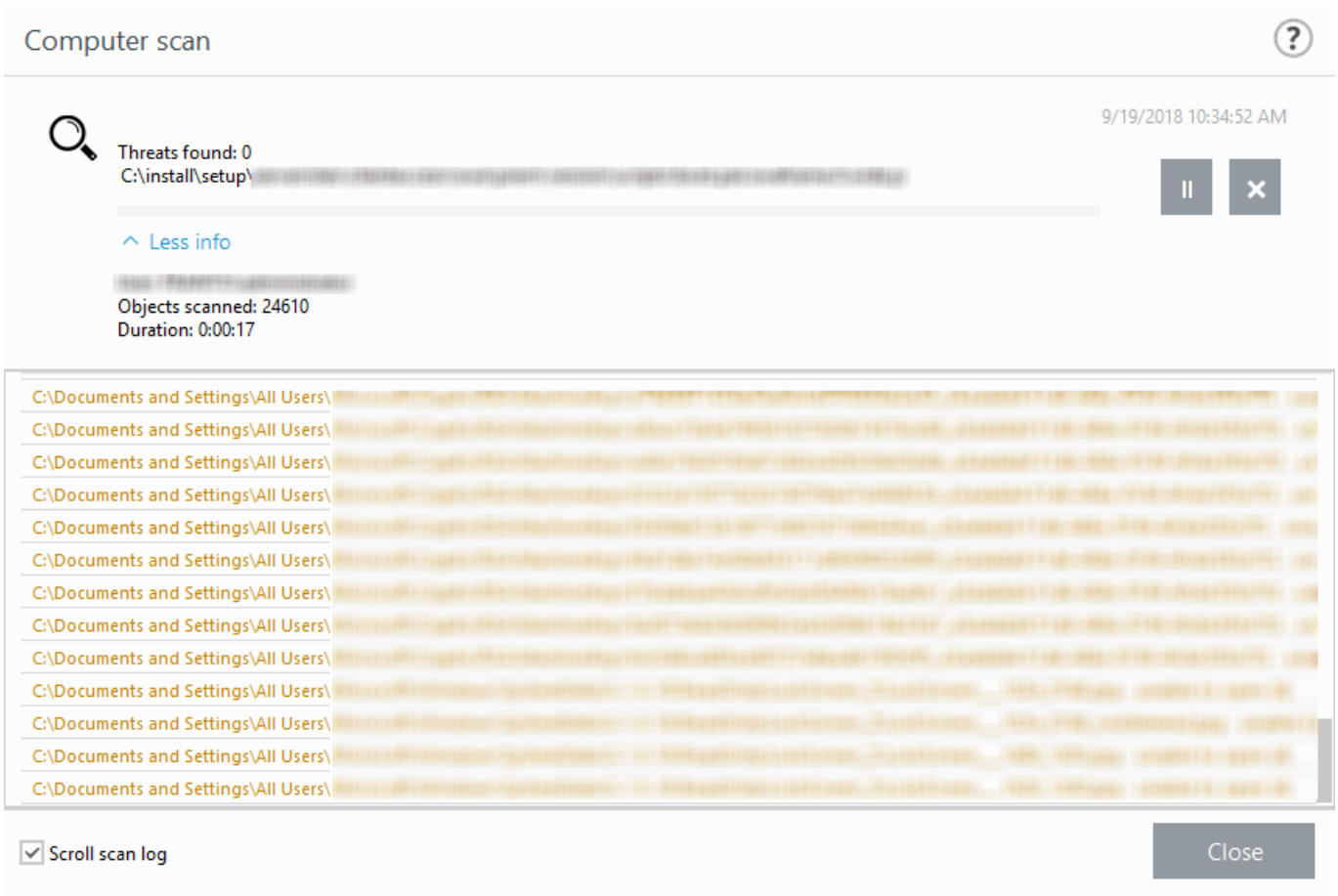
Sie können Optionen verwenden und weitere Informationen zum Scanstatus anzeigen:

Dateien ziehen und Ablegen	**Sie können Dateien mit der Maus ziehen und im ESET Mail Security-Scanfenster ablegen, um sie sofort nach Viren zu scannen. Diese Dateien werden sofort auf Viren gescannt.**
Verwerfen/Alle verwerfen	Angezeigte Nachrichten werden verworfen.
Scanstatus	Zeigt den Status des Erstscans an. Dieser Scan wurde entweder abgeschlossen oder vom Benutzer unterbrochen.
Log anzeigen	Zeigt ausführlichere Informationen an.
Weitere Informationen	Während eines Scans können Sie zusätzliche Details anzeigen, z. B. den Benutzer, der den Scanvorgang ausgeführt hat, die geprüften Objekte und die **Scandauer**. Wenn eine On-Demand-Datenbankprüfung ausgeführt wird, sehen Sie in diesem Fenster den Benutzer, der die Prüfung gestartet hat, und nicht das Datenbankprüfkonto, das für die Verbindung zu EWS (Exchange Web Services) bei der Prüfung verwendet wird.
Scanfenster öffnen	Die Fortschrittsanzeige enthält den aktuellen Stand der Prüfung und die Anzahl der bisher gefundenen infizierten Dateien.

Scanfenster und Scan-Log

Das Scanfenster enthält die aktuell gescannten Objekte zusammen mit ihrem Speicherort, die Anzahl der gefundenen Bedrohungen (falls vorhanden), die Anzahl gescannter Objekte und die Scandauer. Der untere Teil des Fensters enthält ein Scan-Log mit der Versionsnummer der Erkennungsroutine, den Zeitpunkt, zu dem der Scan gestartet wurde, und die Zielauswahl.

Wenn ein Scan ausgeführt wird, können Sie auf **Anhalten** klicken, um den Scan vorübergehend zu unterbrechen. Wenn ein Scan angehalten wurde, ist die Option **Fortsetzen** verfügbar.

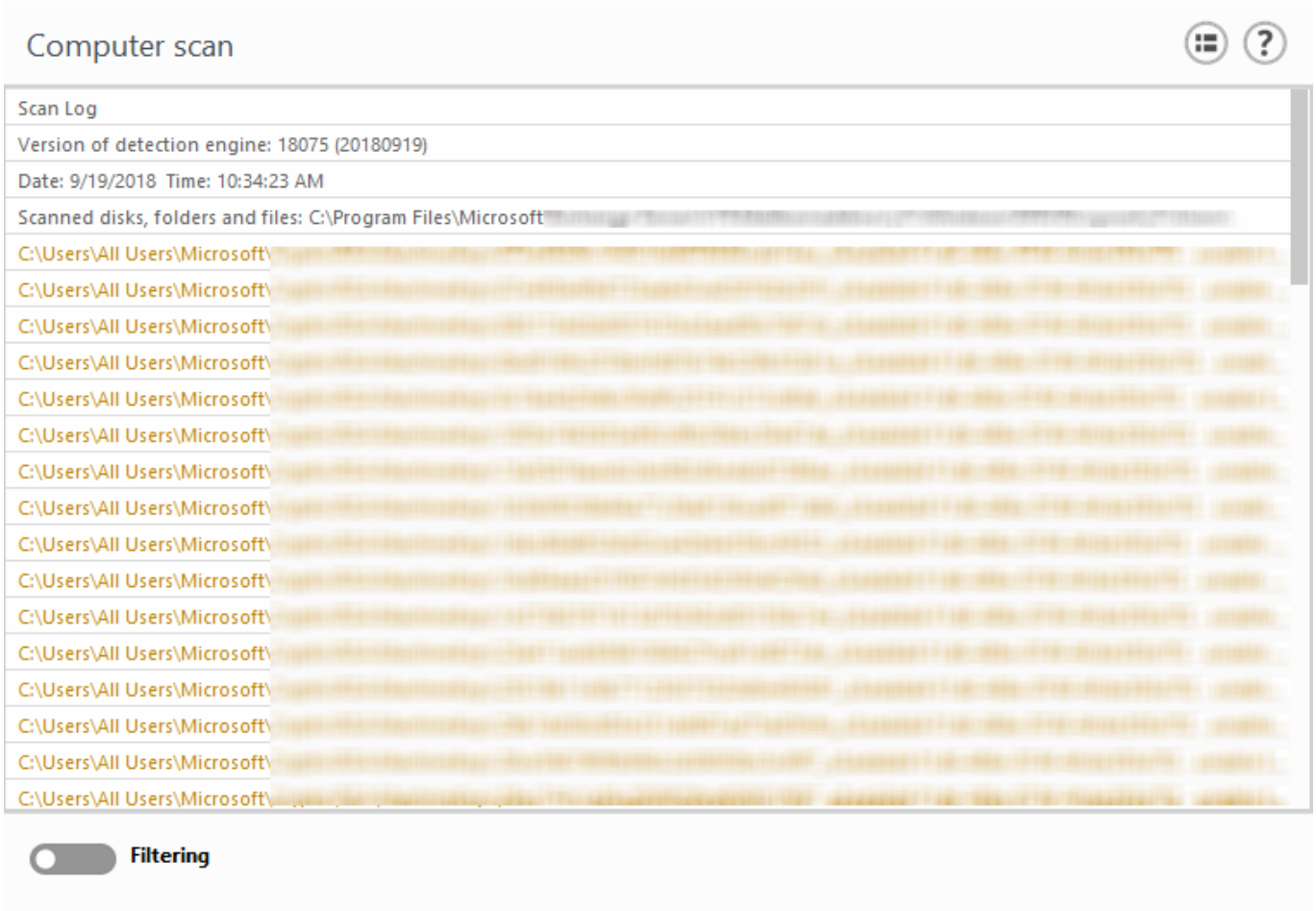


Bildlauf in Log-Anzeige aktivieren

Wenn diese Option aktiv ist, wandern alte Logs automatisch aus der Anzeige, sodass im Fenster der Log-Dateien die neuesten Einträge sichtbar sind.

> Es ist normal, dass u. a. passwortgeschützte Dateien oder Dateien, die ausschließlich vom System genutzt werden (in der Regel sind das *pagefile.sys* und bestimmte Log-Dateien), nicht geprüft werden können.

Nach Abschluss des Scans wird das Scan-Log mit allen relevanten Informationen zum Scanvorgang angezeigt.



Klicken Sie auf das Schaltersymbol **Filter**, um das Fenster Log-Filter zu öffnen, in dem Sie Filter- oder Suchkriterien definieren können. Klicken Sie mit der rechten Maustaste auf einen Logeintrag, um das Kontextmenü zu öffnen:

Aktion	Nutzung	Verknüpfung	Siehe auch
Gleiche Datensätze filtern	Diese Option aktiviert die Log-Filterung, sodass nur Einträge vom gleichen Typ wie der ausgewählte Eintrag angezeigt werden.	Strg + Umsch + F	
Filter...	Wenn Sie auf diese Option klicken, können Sie im Fenster „Log-Filterung“ Filterkriterien für bestimmte Log-Einträge festlegen.		Log-Filter
Filter aktivieren	Aktiviert die Filtereinstellungen. Wenn Sie die Filterung zum ersten Mal aktivieren, müssen Sie einige Einstellungen festlegen.		
Filter deaktivieren	Deaktiviert die Filterung (gleiche Funktion wie der Schalter am unteren Rand).		
Kopieren	Kopiert die Informationen der ausgewählten/hervorgehobenen Datensätze in die Zwischenablage.	Strg + C	
Alle kopieren	Kopiert die Informationen aller im Fenster angezeigten Einträge.		
Exportieren...	Exportiert die Informationen der ausgewählten/hervorgehobenen Datensätze in eine XML-Datei.		
Alle exportieren ...	Exportiert sämtliche Informationen aus dem Fenster in eine XML-Datei.		

Log-Dateien

Die Log-Dateien enthalten Informationen zu wichtigen aufgetretenen Programmereignissen und liefern einen Überblick über Scan-Ergebnisse, erkannte Bedrohungen usw. Logs sind unabdingbar für die Systemanalyse, die Erkennung von Problemen oder Risiken sowie die Fehlerbehebung. Die Logs werden im Hintergrund ohne Eingriffe des Benutzers erstellt. Welche Informationen aufgezeichnet werden, ist abhängig von den aktuellen Einstellungen für die Mindestinformation in Logs. Textnachrichten und Logs können direkt in ESET Mail Security angezeigt oder exportiert werden.

Wählen Sie im Dropdownmenü den gewünschten Log-Typ aus. Folgende Logs sind verfügbar:

Ereignisse

Das Ereignis-Log enthält detaillierte Informationen zu Infiltrationen, die von den ESET Mail Security Modulen erkannt wurden. Dazu gehören die Zeit der Erkennung, Name und Ort der Bedrohung, ausgeführte Aktionen und der Name des Benutzers, der zum Entdeckungszeitpunkt angemeldet war.

Doppelklicken Sie auf einen Log-Eintrag, um die Details in einem eigenen Fenster anzuzeigen. Erstellen Sie einen Ereignisausschluss, indem Sie mit der rechten Maustaste auf einen Log-Eintrag (Ereignis) klicken und auf **Ausschluss erstellen** klicken. Daraufhin wird der Ausschluss-Assistent mit vordefinierten Kriterien geöffnet. Wenn neben einer ausgeschlossenen Datei der Name eines Ereignisses angezeigt wird, bedeutet dies, dass die Datei nur für das jeweilige Ereignis ausgeschlossen wird. Wenn die Datei später mit einer anderen Malware infiziert wird, wird Sie erneut erkannt.

Ereigniss

Alle von ESET Mail Security ausgeführten wichtigen Aktionen werden im Ereignis-Log aufgezeichnet. Das Ereignis-Log enthält Informationen über Ereignisse und im Programm aufgetretene Fehler. Es unterstützt Systemadministratoren und Benutzer bei der Fehlerbehebung. Die hier aufgeführten Informationen sind oftmals hilfreich, um ein im Programm aufgetretenes Problem zu beheben.

Computerscan

Alle Scanergebnisse werden in diesem Fenster angezeigt. Jede Zeile entspricht der Überprüfung eines einzelnen Computers. Durch Doppelklicken auf einen Eintrag können Sie Einzelheiten zu der entsprechenden Prüfung anzeigen.

Gesperrte Dateien

Enthält Einträge für die Dateien, die gesperrt waren und auf die nicht zugegriffen werden konnte. Das Log enthält den Grund für die Sperrung und das Quellmodul, das die Datei gesperrt hat, sowie die Anwendung und den Benutzer, der die Datei ausgeführt hat.

Verschickte Dateien

Enthält Einträge für den cloudbasierten Schutz, ESET LiveGuard Advanced und ESET LiveGrid®.

Audit-Logs

Enthält Einträge für Änderungen an der Konfiguration oder am Schutzstatus und erstellt Snapshots zur späteren Verwendung. Klicken Sie mit der rechten Maustaste auf einen beliebigen Eintrag vom Typ Einstellungsänderung und wählen Sie Änderungen anzeigen im Kontextmenü aus, um ausführliche Informationen zur ausgeführten

Änderung anzuzeigen. Wählen Sie Wiederherstellen aus, um die vorherige Einstellung wiederherzustellen. Mit Alle löschen können Sie Logeinträge entfernen. Um das Audit-Logging zu aktivieren, navigieren Sie zu Erweiterte Einstellungen > Tools > Log-Dateien > Audit-Log.

HIPS

Enthält Einträge für spezifische Regeln, die zum Aufzeichnen markiert wurden. Das Protokoll zeigt die Anwendung an, die den Vorgang angefordert hat, das Ergebnis (ob der Vorgang zugelassen oder blockiert wurde) sowie den erstellten Regelnamen.

Netzwerk-Schutz

Enthält Einträge zu den Dateien, die vom Botnet-Schutz und dem IDS (Netzwerkangriffsschutz) blockiert wurden.

Gefilterte Websites

Diese Liste enthält die vom Web-Schutz und E-Mail-Phishing-Schutz. Die Logs enthalten die Uhrzeit, die URL, den Benutzer und die Anwendung, die eine Verbindung zur gegebenen Website hergestellt hat.

Gerätesteuerung

Enthält Einträge zu Wechselmedien oder externen Geräten, die an den Computer angeschlossen wurden. Nur Geräte mit einer Regel für die Medienkontrolle werden in die Log-Datei aufgenommen. Wenn auf ein angeschlossenes Gerät keine Regel zutrifft, wird für das Gerät kein Log-Eintrag erstellt. Hier können Sie außerdem Details wie Gerätetyp, Seriennummer, Herstellername und Mediengröße (je nach Verfügbarkeit der Informationen) anzeigen.

E-Mail-Server-Schutz

Enthält alle Nachrichten, die von ESET Mail Security als Spam oder wahrscheinlich Spam eingestuft werden. Diese Logs gelten für die folgenden Schutztypen: Spam-Schutz, Phishing-Schutz, Absender-Spoofing-Schutz, Regeln und Malware-Schutz.

Wenn Sie auf ein Element doppelklicken, wird ein Popupfenster mit zusätzlichen Informationen zur erkannten E-Mail geöffnet, inklusive IP-Adresse, HELO-Domäne, Nachrichten-ID und Scantyp mit der Schutzebene, auf der das Ereignis erkannt wurde. Außerdem können Sie das Scanergebnis für Malware-Schutz, Phishing-Schutz und Spam-Scan sowie den Grund anzeigen, aus dem eine Erkennung ausgelöst oder eine Regel aktiviert wurde.

> **i** Nicht alle verarbeiteten Nachrichten werden im E-Mail-Server-Schutz-Log registriert. Dagegen werden jedoch alle Nachrichten, die tatsächlich modifiziert wurden (Anhang gelöscht, benutzerdefinierte Zeichenfolge an Nachrichtenkopf angehängt usw.) in das Log geschrieben.

Postfachdatenbankprüfung

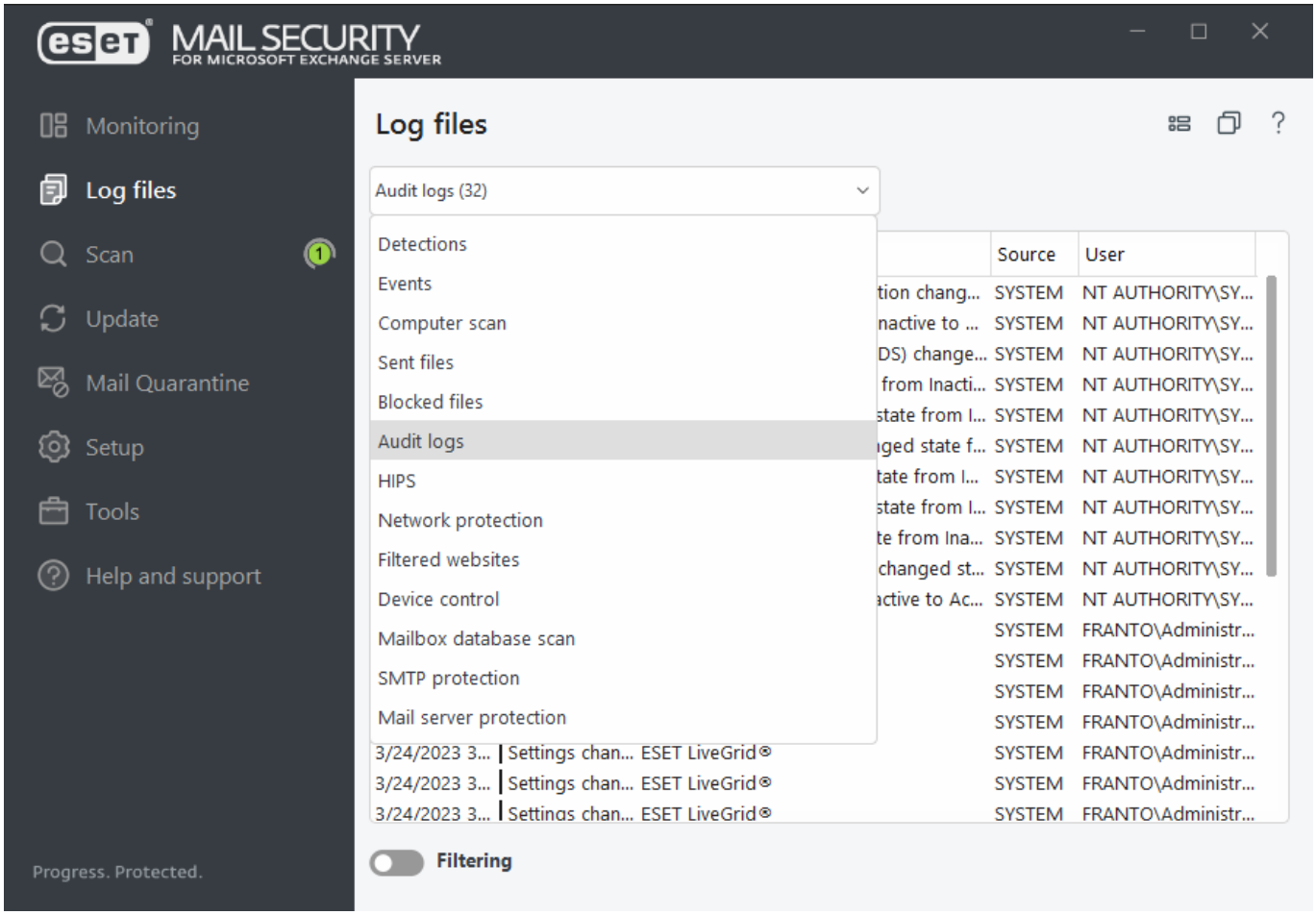
Enthält die Version der Erkannte Bedrohungen sowie Datum, geprüften Ort, Anzahl geprüfter Objekte, Anzahl erkannter Bedrohungen, Anzahl Regeltreffer und Abschlusszeitpunkt.

SMTP-Schutz

Dieses Log enthält alle Nachrichten, die mit der Greylisting-Methode geprüft wurden. SPF und Rückläufer werden hier ebenfalls angezeigt. Jeder Eintrag enthält die HELO-Domäne, IP-Adresse von Absender und Empfänger und Aktionsstatus (abgelehnt, abgelehnt (nicht geprüft) und verifizierte eingehende Nachrichten). Unterdomänen können mit einer neuen Aktion zur Greylisting-Whitelist hinzugefügt werden (siehe Tabelle unten).

Hyper-V-Scan

Enthält eine Liste mit den Ergebnissen der Hyper-V-Prüfung. Durch Doppelklicken auf einen Eintrag können Sie Einzelheiten zu der entsprechenden Prüfung anzeigen.



Im Kontextmenü (Rechtsklick) können Sie eine Aktion für den ausgewählten Logeintrag auswählen:

Aktion	Nutzung	Verknüpfung	Siehe auch
Anzeigen	Zeigt ausführlichere Informationen zum ausgewählten Log in einem neuen Fenster an (gleiche Aktion wie durch Doppelklicken).		
Gleiche Datensätze filtern	Diese Option aktiviert die Log-Filterung, sodass nur Einträge vom gleichen Typ wie der ausgewählte Eintrag angezeigt werden.	Strg + Umsch + F	
Filter...	Wenn Sie auf diese Option klicken, können Sie im Fenster „Log-Filterung“ Filterkriterien für bestimmte Log-Einträge festlegen.		Log-Filter
Filter aktivieren	Aktiviert die Filtereinstellungen. Wenn Sie die Filterung zum ersten Mal aktivieren, müssen Sie einige Einstellungen festlegen.		
Filter deaktivieren	Deaktiviert die Filterung (gleiche Funktion wie der Schalter am unteren Rand).		
Kopieren	Kopiert die Informationen der ausgewählten/hervorgehobenen Datensätze in die Zwischenablage.	Strg + C	
Alle kopieren	Kopiert die Informationen aller im Fenster angezeigten Einträge.		
Löschen	Löscht die ausgewählten/hervorgehobenen Datensätze. Für diese Aktion sind Administratorberechtigungen erforderlich.	Entf	

Aktion	Nutzung	Verknüpfung	Siehe auch
Alle löschen	Löscht alle Datensätze im Fenster. Für diese Aktion sind Administratorberechtigungen erforderlich.		
Exportieren...	Exportiert die Informationen der ausgewählten/hervorgehobenen Datensätze in eine XML-Datei.		
Alle exportieren ...	Exportiert sämtliche Informationen aus dem Fenster in eine XML-Datei.		
Suchen...	Öffnet das Fenster Im Log suchen, in dem Sie Suchkriterien festlegen können. Dort können Sie nach Einträgen suchen, auch während die Filterung aktiviert ist.	Strg + F	In Log suchen
Weitersuchen	Sucht den nächsten Eintrag für die zuvor definierten Suchkriterien.	F3	
Rückwärts suchen	Sucht den vorherigen Eintrag.	Umsch + F3	
Ausschluss erstellen	Um Objekte anhand von Erkennungsname, Pfad oder Hash von der Säuberung auszuschließen.		Ausschluss erstellen

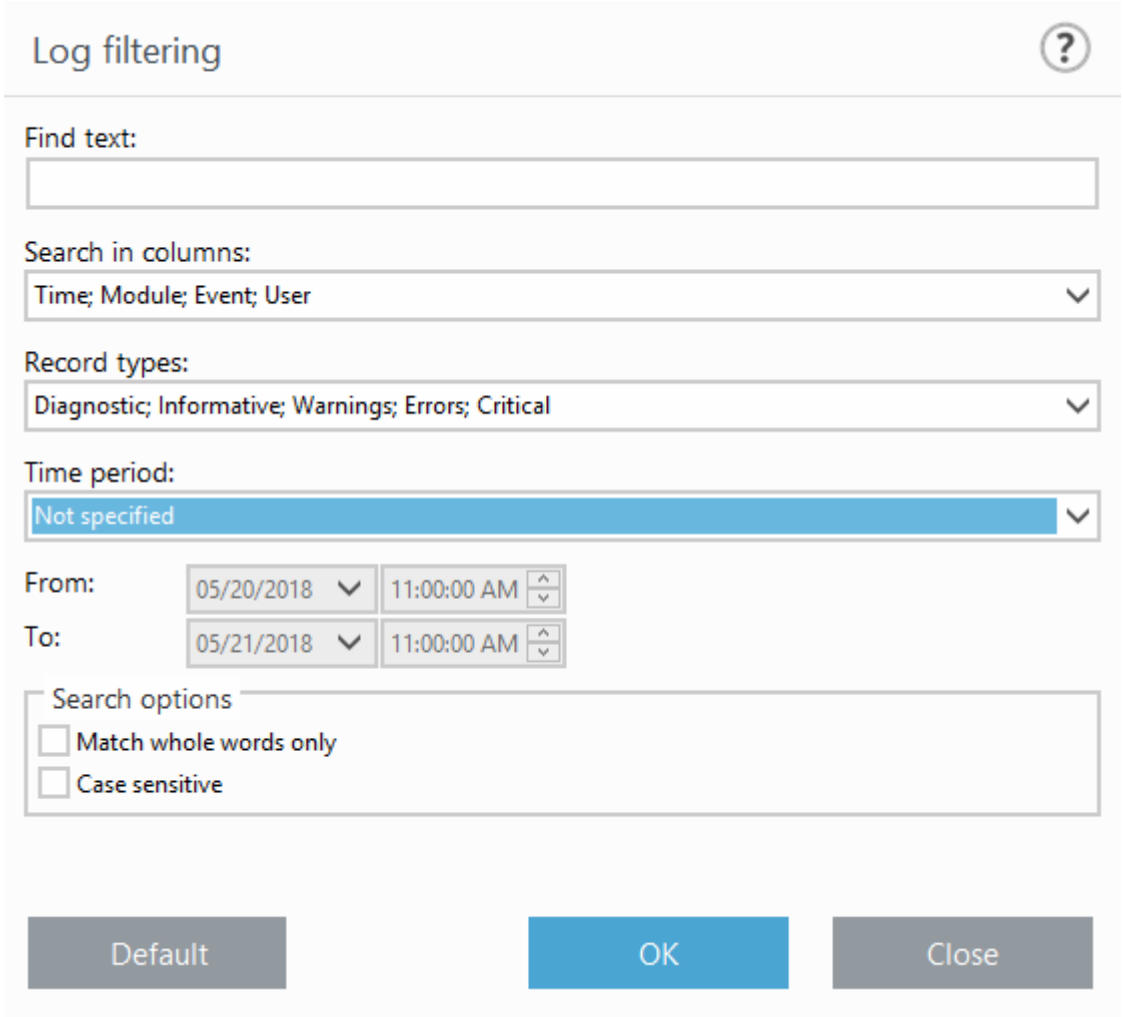
IP-Adresse zur Greylisting-Positivliste hinzufügen	Fügt die IP-Adresse des Absenders zur IP-Whitelist hinzu. Sie finden die IP-Whitelist im Abschnitt „Greylisting und SPF“ unter Filterung und Verifizierung. Diese Liste gilt für die von Greylisting und SPF geloggten Objekte.
Domäne zur Greylisting- und SPF-Whitelist hinzufügen	Fügt die Domäne des Absenders zur Domain-in-IP-Whitelist hinzu. Dabei wird nur die Domäne hinzugefügt, die Unterdomäne wird ignoriert. Wenn die Absenderadresse sub.domain.com lautet, wird nur domain.com zur Whitelist hinzugefügt. Sie finden die Domain-in-IP-Whitelist im Abschnitt „Greylisting und SPF“ unter Filterung und Verifizierung. Diese Liste gilt für die vom Greylisting geloggten Objekte.
Unterdomäne zur Greylisting- und SPF-Whitelist hinzufügen	Fügt die Unterdomäne des Absenders zur Domain-in-IP-Whitelist hinzu. Dabei wird die Domäne inklusive der Unterdomäne hinzugefügt (z. B. sub.domain.com). Diese Option ermöglicht genauere Filtermöglichkeiten. Sie finden die Domain-in-IP-Whitelist im Abschnitt „Greylisting und SPF“ unter Filterung und Verifizierung. Diese Liste gilt für die vom Greylisting geloggten Objekte.

Log-Filter

Mit dem Log-Filter finden Sie die gesuchten Informationen auch in großen Mengen von Datensätzen. Sie können Log-Datensätze eingrenzen, wenn Sie beispielsweise nach einem bestimmten Ereignistyp, Status oder Zeitraum suchen.

Wenn Sie Log-Datensätze nach Suchoptionen filtern, werden nur relevante Datensätze (gemäß der Suchoptionen) im Fenster „Log-Dateien“ angezeigt.

Geben Sie Ihren Suchbegriff in das Feld **Suchen nach** ein. Mit dem Dropdownmenü **In Spalten** können Sie Ihre Suche eingrenzen. Wählen Sie einen oder mehrere Einträge im Dropdownmenü **Eintragstypen** aus. Legen Sie fest, aus welchem **Zeitraum** die Suchergebnisse stammen sollen: Außerdem haben Sie weitere Suchoptionen wie **Nur ganze Wörter** oder **Groß-/Kleinschreibung beachten** zur Auswahl.



Suchen nach

Geben Sie eine Zeichenfolge ein (ein Wort oder einen Teil eines Wortes). Es werden nur Einträge angezeigt, die diese Zeichenfolge enthalten. Andere Einträge werden nicht berücksichtigt.

In Spalten

Wählen Sie die Spalten aus, die bei der Suche berücksichtigt werden sollen. Sie können mehr als eine Spalte für die Suche markieren.

Eintragstypen

Wählen Sie einen oder mehrere Log-Eintragstypen aus dem Dropdownmenü aus:

- **Diagnosedaten** - Alle Meldungen höherer Stufen und alle sonstigen Informationen, die für das Beheben von Fehlern wichtig sein können, werden protokolliert.
- **Informationen** - Meldungen wie erfolgreiche Updates und alle Meldungen höherer Stufen werden protokolliert.
- **Warnungen** - Kritische Fehler und Warnungen werden protokolliert.
- **Fehler** - Fehler wie „Fehler beim Herunterladen der Datei“ und kritische Fehler werden aufgezeichnet.
- **Kritisch** - Nur kritische Fehler werden protokolliert.

Zeitraum

Legen Sie fest, aus welchem Zeitraum die Suchergebnisse stammen sollen:

- Nicht angegeben (Standardeinstellung) - Begrenzt die Suche nicht auf einen Zeitraum, sondern durchsucht das gesamte Log.
- Gestern
- Letzte Woche
- Letzter Monat
- Zeitraum - Sie können einen genauen Zeitraum angeben (Von: und Bis:), um nur Einträge aus diesem Zeitraum zu suchen.

Nur ganze Wörter

Aktivieren Sie dieses Kontrollkästchen, wenn Sie mit ganzen Wörtern genauere Suchergebnisse erzielen möchten.

Groß-/Kleinschreibung beachten

Aktivieren Sie diese Option, wenn die Groß- oder Kleinschreibung der Suchwörter beachtet werden soll. Klicken Sie beim Konfigurieren Ihrer Filter- und Suchoptionen auf **OK**, um gefilterte Log-Datensätze anzuzeigen, oder auf **Suchen**, um die Suche zu starten.

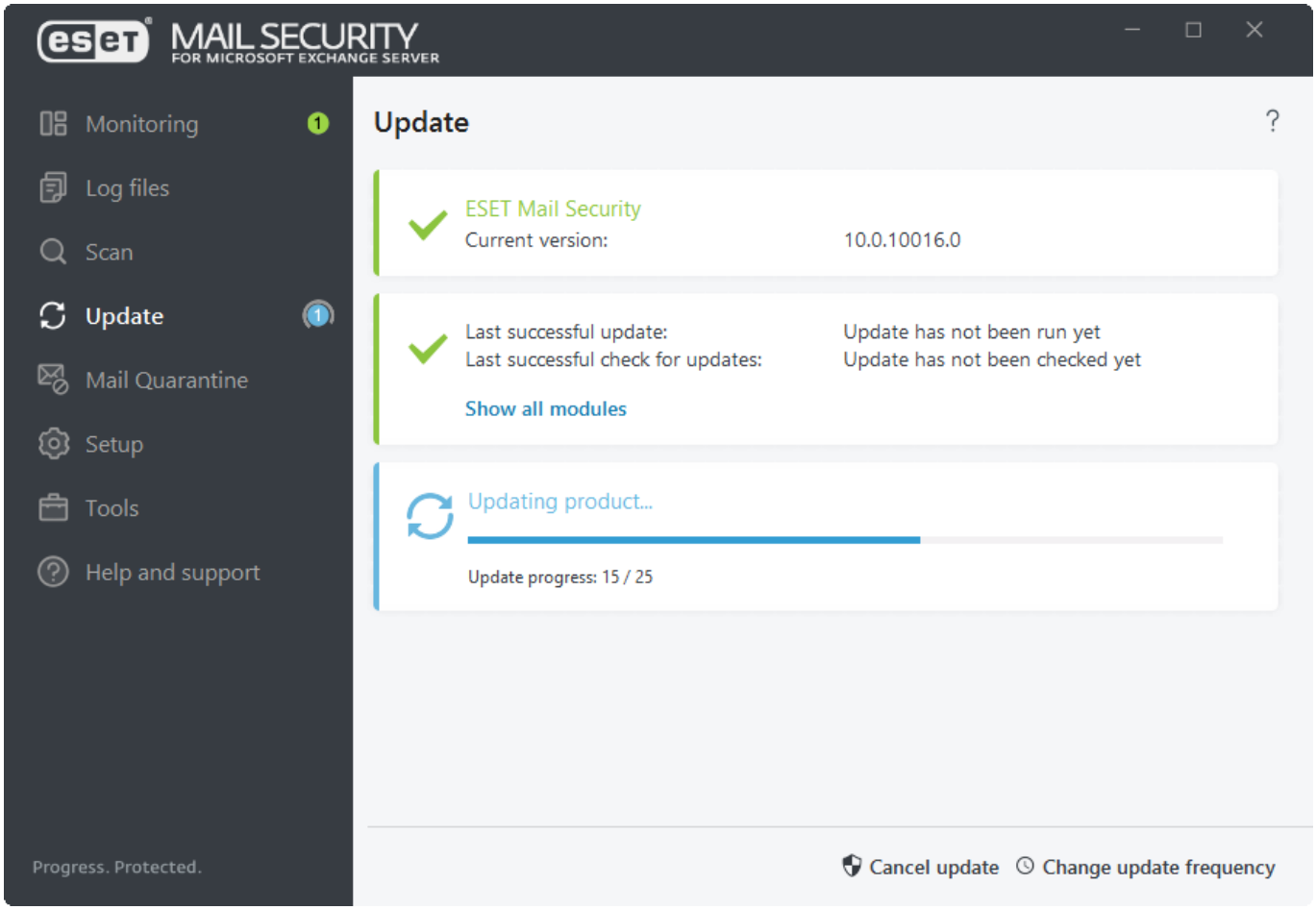
Die Log-Dateien werden von oben nach unten ab der aktuellen (hervorgehobenen) Position durchsucht. Die Suche wird gestoppt, sobald der erste übereinstimmende Eintrag gefunden wurde. Drücken Sie **F3**, um den nächsten Datensatz zu suchen, oder klicken Sie mit der rechten Maustaste und wählen Sie **Suchen** aus, um Ihre Suchoptionen zu verfeinern.

Update

Im Bereich „Update“ wird der aktuelle Updatestatus Ihres ESET Mail Security angezeigt, inklusive Datum und Uhrzeit der letzten erfolgreichen Aktualisierung. Den optimalen Schutz Ihres Computers gewährleisten Sie, indem Sie ESET Mail Security regelmäßig aktualisieren.

Das Updatemodul hält das Programm fortlaufend auf dem neuesten Stand, indem die Erkennungsroutine und die Systemkomponenten aktualisiert werden. Die Aktualisierungen von Erkennungsroutine und Programmkomponenten sind entscheidend für einen vollständigen Schutz vor Schadcode.

> Falls Sie noch keinen License Lizenzschlüssel eingegeben haben, erhalten Sie keine Updates und werden aufgefordert, Ihr Produkt zu aktivieren. Navigieren Sie dazu zu **Hilfe und Support** > **Produkt aktivieren**.



Aktuelle Version

Die Buildversion von ESET Mail Security.

Letztes erfolgreiches Update

Das Datum des letzten Updates. Hier sollte ein aktuelles Datum angezeigt werden, was auf eine kürzlich vorgenommene Aktualisierung hinweist.

Letzte erfolgreiche Prüfung auf Updates

Das Datum der letzten Überprüfung auf Modulupdates.

Alle Module anzeigen

Öffnet die Liste der installierten Module.

Nach Updates suchen

Updates der Module sind entscheidend für einen möglichst umfassenden Schutz vor Schadcode.

Updatehäufigkeit ändern

Sie können das Timing für den Taskplaner-Task Automatische Updates in festen Zeitabständen bearbeiten.

Wenn Sie nicht so schnell wie möglich nach Updates suchen, wird eine der folgenden Nachrichten angezeigt:

Fehlermeldung	Beschreibung
Die Module sind veraltet	Dieser Fehler wird angezeigt, wenn die Module trotz wiederholter Versuche nicht aktualisiert werden konnten. Überprüfen Sie in diesem Fall die Update-Einstellungen. Die häufigste Fehlerursache sind falsch eingegebene Lizenzdaten oder fehlerhaft konfigurierte Verbindungseinstellungen.
Modul-Update fehlgeschlagen - Produkt ist nicht aktiviert	Der Lizenzschlüssel wurde falsch in den Update-Einstellungen eingegeben. Wir empfehlen eine Überprüfung Ihrer Lizenzdaten. Das Fenster **Erweiterte Einstellungen** (**F5**) enthält zusätzliche Update-Optionen. Klicken Sie im Hauptmenü auf **Hilfe und Support** > Lizenzen verwalten, um einen neuen Lizenzschlüssel einzugeben.
Beim Herunterladen der Update-Dateien ist ein Fehler aufgetreten	Eine mögliche Fehlerursache sind die Internetverbindungseinstellungen. Überprüfen Sie die Internetverbindung, z. B. indem Sie eine beliebige Internetseite im Webbrowser aufrufen. Wenn die Website nicht aufgerufen werden kann, besteht mit ziemlicher Sicherheit keine Internetverbindung. Wenden Sie sich in diesem Fall an Ihren Internetdienstanbieter.
Fehler 0073 bei Modulupdate	Klicken Sie auf **Update** > **Nach Updates suchen**. Weitere Informationen finden Sie in diesem Knowledgebase-Artikel.

Verschiedene Update-Profile können unterschiedliche Proxyserver-Optionen verwenden. Konfigurieren Sie in diesem Fall die verschiedenen Update-Profile in den **erweiterten Einstellungen** (**F5**), indem Sie auf **Update** > Profil klicken.

E-Mail-Quarantäne

E-Mail-Nachrichten und deren Komponenten, z. B. Anlagen, werden anstelle der herkömmlichen Dateiquarantäne in die E-Mail-Quarantäne verschoben. Die E-Mail-Quarantäne ermöglicht eine komfortablere Verwaltung von Spam, infizierten Anlagen mit Malware oder Phishing-Nachrichten. Je nachdem, welches ESET Mail Security-Schutzmodul die Nachricht verarbeitet (Malware-Schutz, Spam-Schutz, Phishing-Schutz, Absender-Spoofing-Schutz oder Regeln), können E-Mails aus unterschiedlichen Gründen in die E-Mail-Quarantäne verschoben werden.

Filtern nach Symbolen

Sie können Symbole zum Filtern von Nachrichten verwenden, um nur Anlagen, E-Mails oder E-Mails mit Anlagen anzuzeigen.

Zeitspanne

Wählen Sie aus, für wie lange Sie die E-Mails in der Quarantäne sehen möchten. Wenn Sie **Benutzerdefiniert** auswählen, können Sie ein Intervall (Anfangs- und Enddatum) angeben.

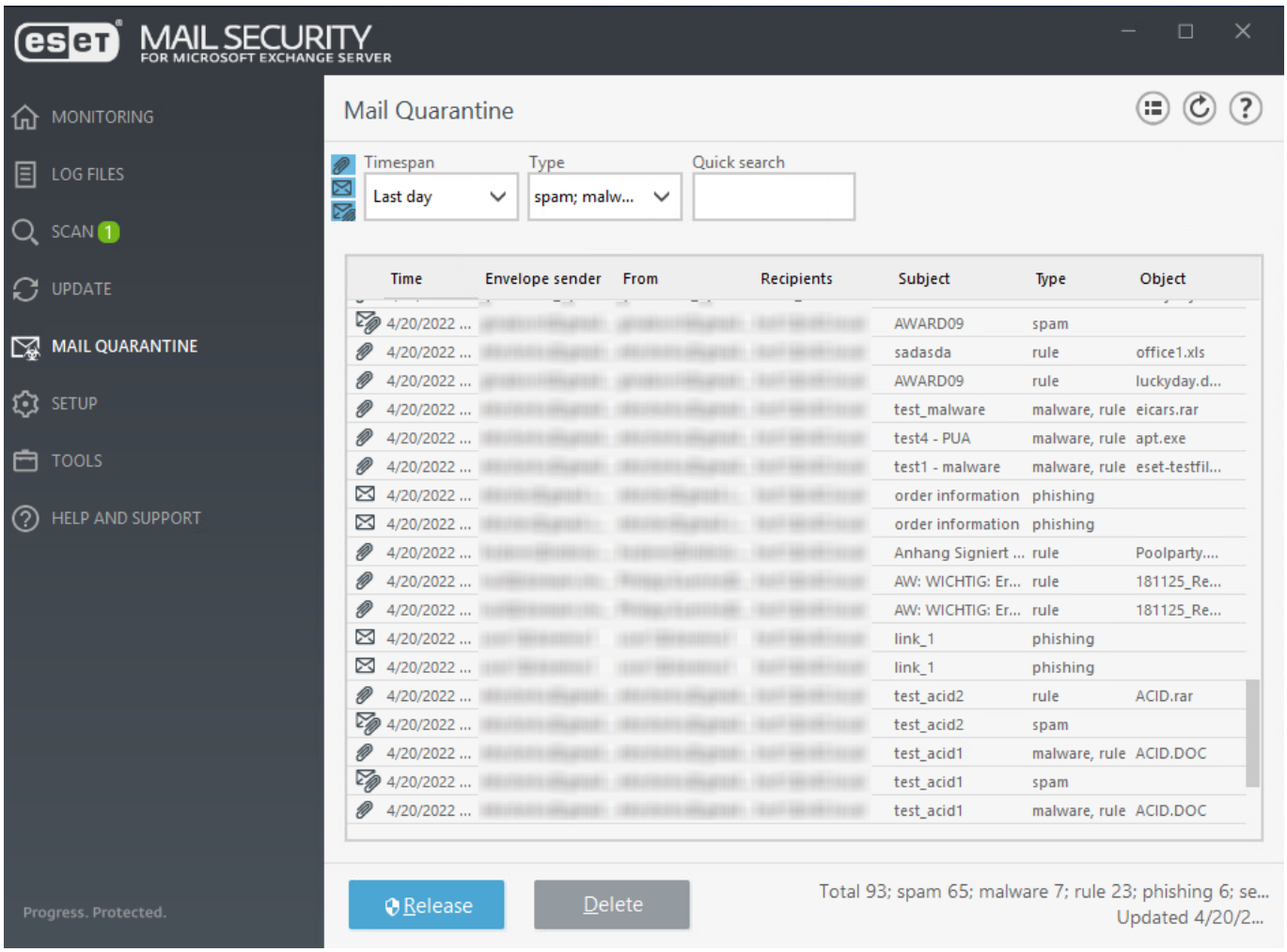
Schnellsuche

Geben Sie eine Zeichenfolge in dieses Textfeld ein, um die angezeigten E-Mails zu filtern (alle Spalten werden durchsucht).

Grund

Verwenden Sie die Kontrollkästchen, um nach verschiedenen Typen zu filtern (Spam, Malware, Regel, Phishing oder Absender gefälscht).

Die Daten aus dem E-Mail-Quarantäne-Manager werden nicht automatisch aktualisiert. Klicken Sie daher regelmäßig auf **Aktualisieren** , um die neuesten E-Mails in der Quarantäne anzuzeigen.



Freigeben

Freigeben - Gibt die E-Mail über das Replay-Verzeichnis an den bzw. die Originalempfänger frei, und löscht sie aus der Quarantäne. Klicken Sie auf Ja, um den Vorgang zu bestätigen. Wenn das Objekt in der Quarantäne ein Anhang aus einem öffentlichen Ordner mit deaktivierten E-Mails ist, ist die Freigeben-Schaltfläche nicht verfügbar.

Wenn Sie eine E-Mail aus der Quarantäne freigeben, ignoriert ESET Mail Security den `To:`-MIME-Header, da dieser sehr leicht zu fälschen ist. Stattdessen werden die Originaldaten des Empfängers aus der Ausgabe des Befehls `RCPT TO:` verwendet, der während der SMTP-Verbindung ausgeführt wurde. Damit wird sichergestellt, dass die aus der Quarantäne freigegebene E-Mail an den richtigen Empfänger zugestellt wird.

Wenn Sie eine geclusterte Umgebung ausführen und eine Nachricht aus der Quarantäne freigeben, wird die Nachricht von den anderen ESET Mail Security-Knoten nicht erneut in die Quarantäne verschoben. Dies wird durch die Synchronisierung der Regeln zwischen den Clusterknoten erreicht.

Löschen

Löscht ein Element aus der Quarantäne. Klicken Sie auf **Ja**, um den Vorgang zu bestätigen. Die im Programmfenster gelöschten Elemente werden zwar aus der Quarantäneansicht entfernt, bleiben aber im

Speicher erhalten. Sie werden später automatisch gelöscht (standardmäßig nach drei Tagen).

Wiederherstellen nach

Mit dieser Option können Sie Anhänge an einem angegebenen Ort wiederherstellen. Diese Funktion gilt nur für Anhänge und ist für Nachrichten deaktiviert. Verwenden Sie für komplette Nachrichten stattdessen die Funktion Freigeben.

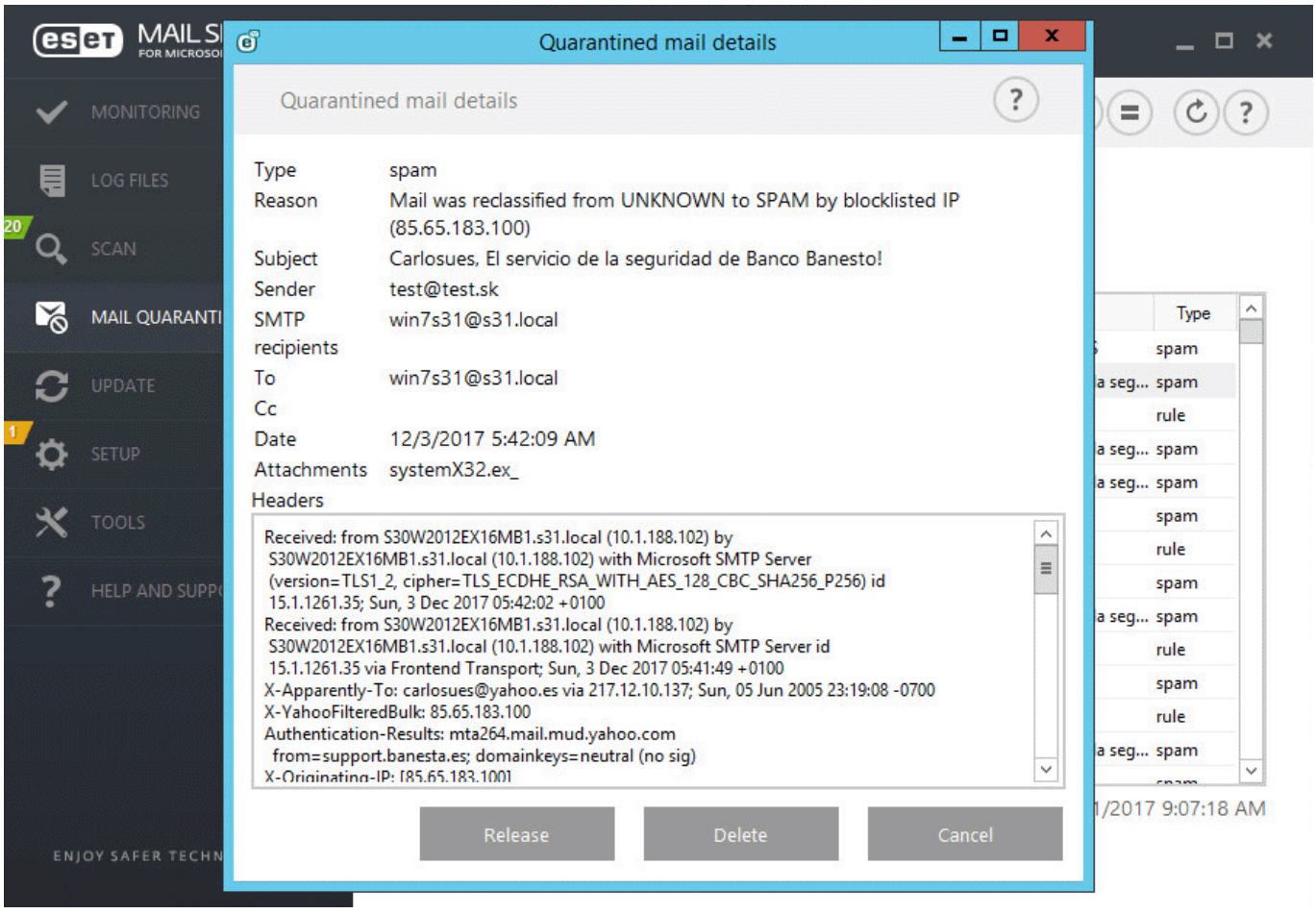
Details zur E-Mail in Quarantäne

Doppelklicken Sie auf die Quarantäne-Nachricht oder klicken Sie mit der rechten Maustaste und wählen Sie **Details anzeigen** aus. Daraufhin wird ein neues Fenster mit Details zur E-Mail-Nachricht angezeigt, die unter Quarantäne gestellt wurde. Außerdem können Sie die ursprünglichen RFC-E-Mail-Header auf weitere Details überprüfen.

Details zum Anhang in Quarantäne

Wenn Sie auf einen Anhang doppelklicken, wird ein Detaildialogfeld geöffnet, das sich von den Nachrichtendetails unterscheidet. Die RFC-Header sind nicht verfügbar, stattdessen wird ein Bereich mit dem Text des Anhang-Umschlags angezeigt. Beim Freigeben einer E-Mail aus der E-Mail-Quarantäne können Sie einen benutzerdefinierten Text für den Anhang-Umschlag eingeben.

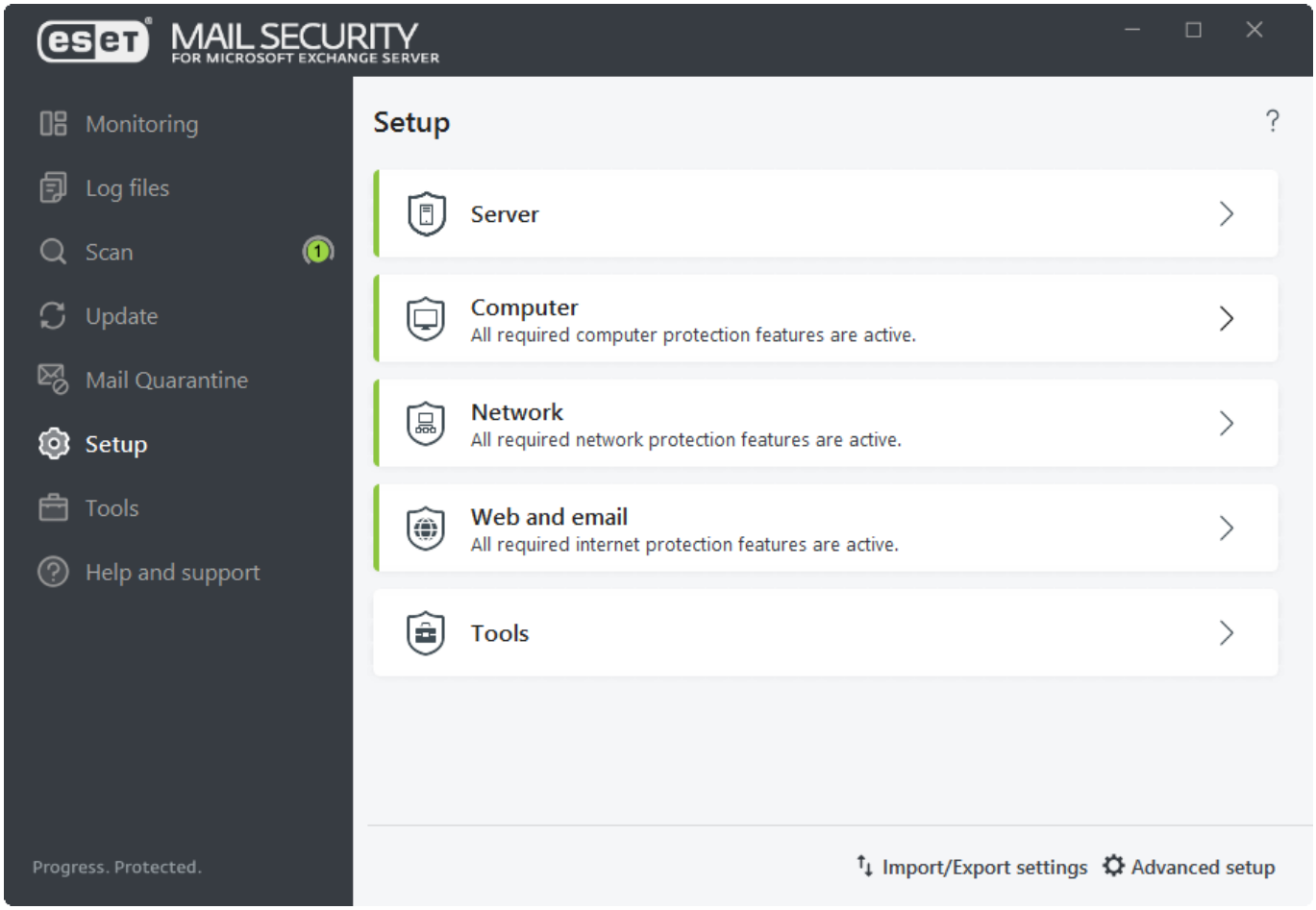
Im Kontextmenü sind verschiedene Aktionen verfügbar. Klicken Sie auf **Freigeben**, **Löschen** oder **Endgültig löschen**, um die entsprechende Aktion für die E-Mail in der Quarantäne auszuführen. Klicken Sie auf **Ja**, um den Vorgang zu bestätigen. Wenn Sie **Endgültig löschen** auswählen, wird die E-Mail auch aus dem Dateisystem gelöscht. **Löschen** entfernt die E-Mail dagegen nur aus der Anzeige des E-Mail-Quarantäne-Managers.



Einstellungen

Folgende Abschnitte stehen im Menü „Einstellungen“ zur Verfügung:

- Server
- Computer
- Netzwerk
- Web und E-Mail
- Tools - Diagnose-Logging



Um einzelne Module vorübergehend zu deaktivieren, klicken Sie neben dem entsprechenden Modul auf den grünen Schieberegler. Dabei wird möglicherweise die Schutzebene Ihres Servers reduziert.

Klicken Sie auf den roten Schieberegler, um eine deaktivierte Sicherheitskomponente erneut zu aktivieren. Die Komponente wird daraufhin erneut aktiviert.

Klicken Sie auf das Zahnradsymbol, um die ausführlichen Einstellungen für eine bestimmte Sicherheitskomponente zu öffnen.

Import-/Export-Einstellungen

Mit dieser Option können Sie die Einstellungen aus einer *.xml*-Konfigurationsdatei laden oder die aktuellen

Einstellungen in einer Konfigurationsdatei speichern.

Erweiterten Einstellungen

In den erweiterten Einstellungen können Sie Einstellungen und Funktionen an Ihre Anforderungen anpassen. Drücken Sie die Taste **F5** an einer beliebigen Stelle im Programm, um die **erweiterten Einstellungen** zu öffnen.

Server

Hier wird eine Liste der Komponenten angezeigt, die Sie mit dem Schieberegler  aktivieren/deaktivieren können. Um die Einstellungen für ein bestimmtes Element zu konfigurieren, klicken Sie auf das Zahnradsymbol  .

Virenschutz

Überwacht die Datei-, E-Mail- und Internet-Kommunikation, um Sie vor bösartigen Systemangriffen zu schützen.

Spam-Schutz

Verwendet verschiedene Technologien (RBL, DNSBL, Fingerprint-Datenbanken, Reputations-Prüfung, Inhaltsanalyse, Regeln, manuell geführte Positiv-/Negativlisten usw.), um E-Mail-Bedrohungen wirksam zu erkennen.

Phishing-Schutz

Analysiert den Nachrichtentext von eingehenden E-Mails auf Phishing-Links (URLs).

Microsoft 365-Postfachdatenbank-Scan

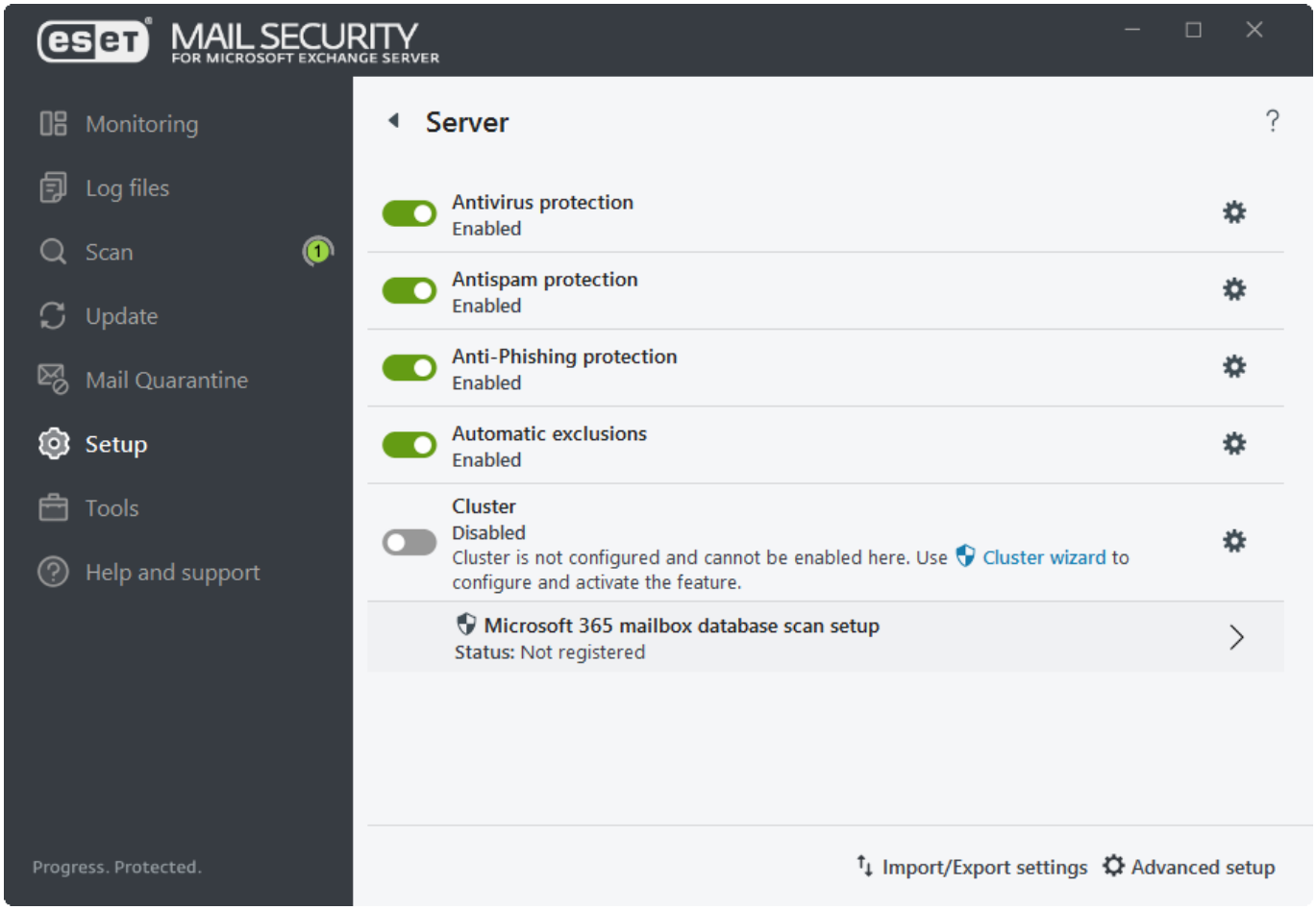
Registrieren Sie den ESET Mail Security Scanner, um diese Funktion zu aktivieren.

Automatische Ausschlüsse

Identifiziert Anwendungen und Betriebssystem-Dateien, die für den Server kritisch sind, und übernimmt sie automatisch in die Liste Ausgeschlossene Elemente. Auf diese Weise wird das Risiko von Konflikten durch die Bedrohungserkennungssoftware minimiert und die Gesamtleistung des Servers verbessert.

Cluster

Hier können Sie den ESET-Cluster konfigurieren und aktivieren.



Computer

ESET Mail Security enthält alle erforderlichen Komponenten, um den Server als Computer zu schützen. In diesem Modul können Sie die folgenden Komponenten aktivieren, deaktivieren und konfigurieren:

Echtzeit-Dateischutz

Alle Dateien werden beim Öffnen, Erstellen oder Ausführen auf Ihrem Computer auf Schadcode geprüft. Für den Echtzeit-Dateischutz können Sie Ausschlüsse **konfigurieren** oder **bearbeiten**. Über diese Option können Sie das Fenster zum Einrichten der Ausschlüsse öffnen, in dem Sie Dateien und Ordner vom Scannen ausschließen können.

Medienkontrolle

Mit diesem Modul können Sie Medien bzw. Geräte prüfen oder sperren oder erweiterte Filter- und Berechtigungseinstellungen anpassen und definieren, wie Benutzer auf diese Geräte zugreifen und mit ihnen arbeiten dürfen.

Host Intrusion Prevention System (HIPS)

Das HIPS-System überwacht Ereignisse auf Betriebssystemebene und führt Aktionen gemäß individueller Regeln aus.

- Advanced Memory Scanner
- Exploit-Blocker

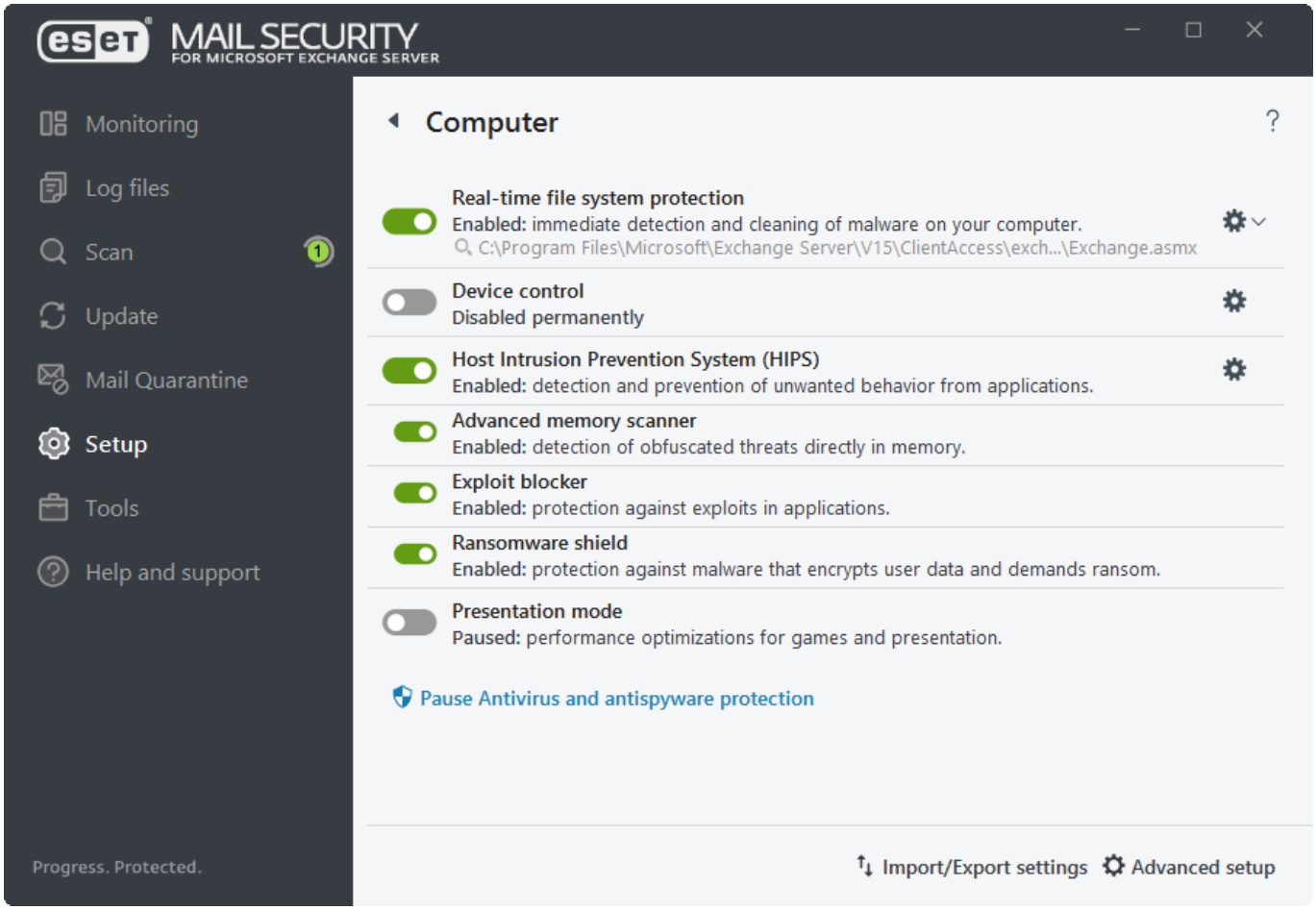
- Ransomware-Schutz

Präsentationsmodus

Eine Funktion für Benutzer, die ihre Software ununterbrochen nutzen, nicht durch Popup-Fenster gestört werden und die CPU-Auslastung reduzieren möchten. Nach der Aktivierung des Präsentationsmodus wird eine Warnung angezeigt (erhöhtes Sicherheitsrisiko) und das Hauptfenster wird in orange dargestellt.

Viren- und Spyware-Schutz anhalten

Viren- und Spyware-Schutz vorübergehend deaktivieren - Bei der vorübergehenden Deaktivierung des Viren- und Spyware-Schutzes können Sie im entsprechenden Dropdown-Menü den Zeitraum wählen, in dem die jeweilige Komponente deaktiviert werden soll. Klicken Sie anschließend auf **Übernehmen**, um die Sicherheitskomponente zu deaktivieren. Klicken Sie auf **Viren- und Spyware-Schutz aktivieren** oder verwenden Sie den Schieberegler, um den Schutz wieder zu aktivieren.



Netzwerk

Zu diesem Zweck können Sie einzelne Netzwerkverbindungen anhand Ihrer Filterregeln zulassen oder blockieren. Diese Funktion schützt Sie vor Angriffen von Remotecomputern und blockiert potenziell gefährliche Dienste.

Im Netzwerk-Modul können Sie folgende Komponenten aktivieren oder deaktivieren:

Netzwerkangriffsschutz (IDS)

Analysiert den Netzwerkdatenverkehr und schützt Sie vor Netzwerkangriffen. Als schädlich erkannter

Datenverkehr wird blockiert.

Botnetz-Schutz

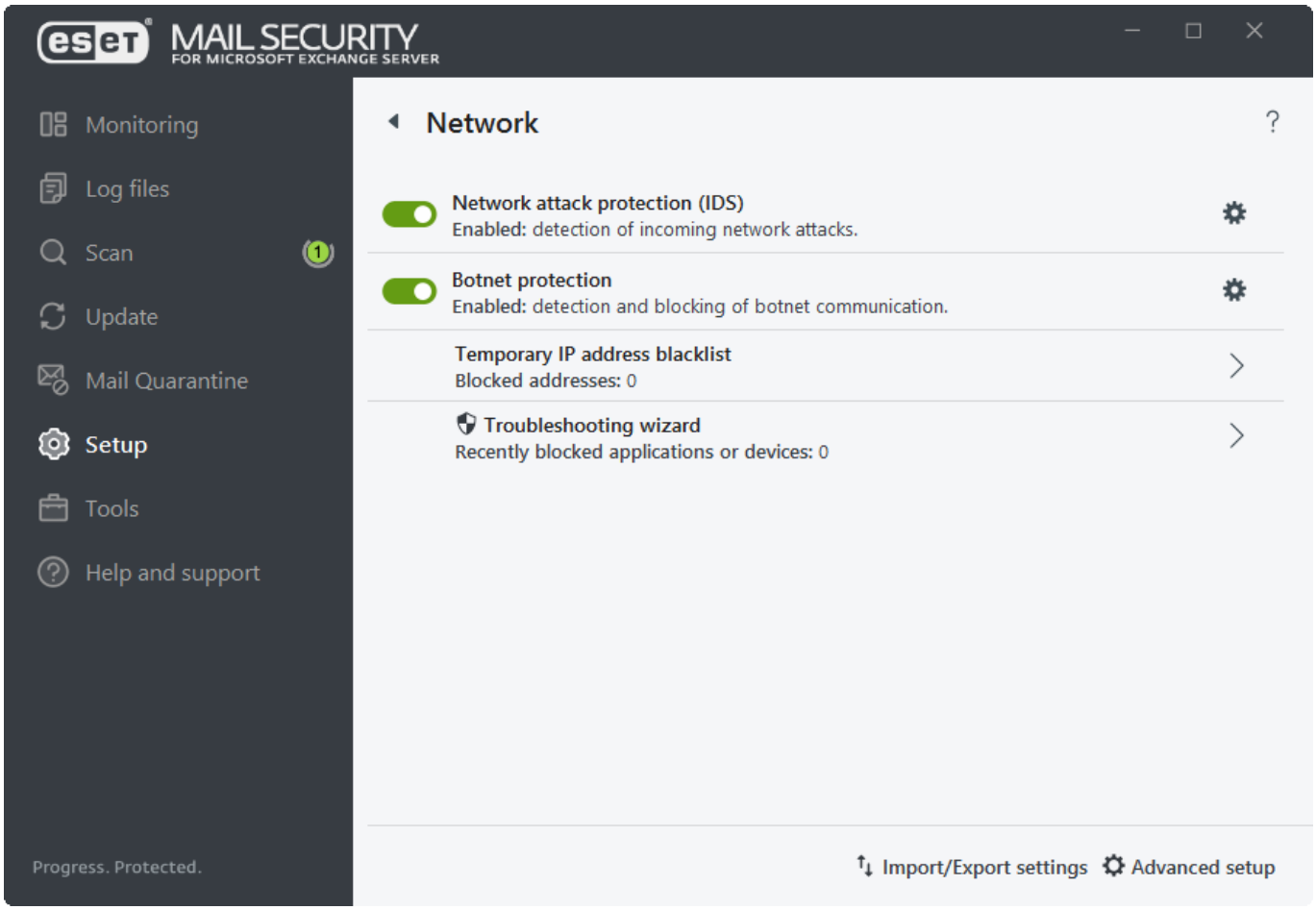
Erkennung und Sperrung von Botnet-Kommunikation. Schadsoftware im System wird schnell und akkurat identifiziert.

Vorübergehende Negativliste der IP-Adressen (blockierte Adressen)

Zeigt eine Liste von IP-Adressen an, die als Angriffsquellen identifiziert und zur Negativliste hinzugefügt wurden, um die Verbindung für einen bestimmten Zeitraum zu unterbinden.

Fehlerbehebungsassistent (kürzlich gesperrte Anwendungen oder Geräte)

Hilfreich zur Behebung von Verbindungsproblemen, die durch den Netzwerkangriffsschutz wurden.



Fehlerbehebungsassistent für das Netzwerk

Der Fehlerbehebungsassistent überwacht alle blockierten Verbindungen und führt Sie durch den Fehlerbehebungsprozess, um Probleme im Zusammenhang mit dem Netzwerkangriffsschutz und bestimmten Anwendungen oder Geräten zu beheben. Anschließend empfiehlt der Assistent bestimmte Regeln, die Sie genehmigen können.

Wählen Sie im Dropdownmenü einen Zeitraum aus, in dem die Kommunikation blockiert wurde. Die Liste der kürzlich blockierten Kommunikationen enthält eine Übersicht mit Anwendungstyp oder Gerät, Reputation und der Gesamtzahl der in diesem Zeitraum blockierten Anwendungen und Geräte. Klicken Sie auf **Details**, um weitere

Details zu einer blockierten Kommunikation anzuzeigen.

Im nächsten Schritt können Sie die Anwendungen bzw. Geräte entsperren, bei denen Konnektivitätsprobleme aufgetreten sind.

Wenn Sie auf Entsperren klicken, wird die zuvor gesperrte Kommunikation zugelassen. Falls weiterhin Probleme mit einer Anwendung auftreten oder Ihr Gerät nicht wie erwartet funktioniert, klicken Sie auf **Die Anwendung funktioniert immer noch nicht**. Daraufhin wird sämtliche bisher für das jeweilige Gerät gesperrte Kommunikation zugelassen. Starten Sie den Computer neu, falls das Problem weiterhin auftritt.

Klicken Sie auf **Änderungen anzeigen**, um die vom Assistenten erstellten Regeln anzuzeigen.

Klicken Sie auf **Weitere entsperren**, um Kommunikationsprobleme mit anderen Geräten oder Anwendungen zu beheben.

Web und E-Mail

In diesem Modul können Sie folgende Komponenten aktivieren oder deaktivieren:

Web-Schutz

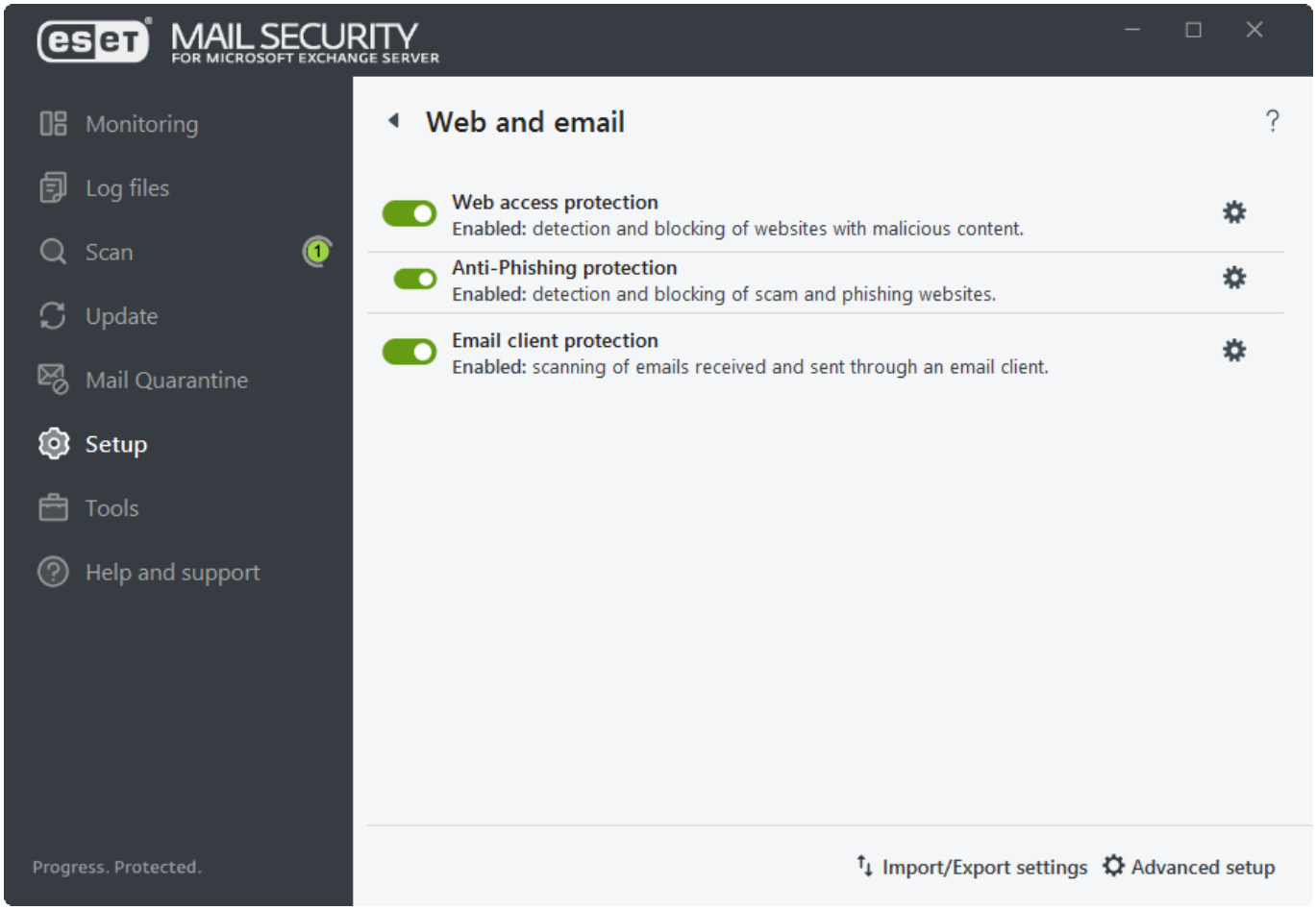
Wenn diese Option aktiviert ist, werden alle Daten auf Schadsoftware geprüft, die über HTTP oder HTTPS übertragen werden.

Phishing-Schutz

Schützt Sie vor Versuchen unseriöser Webseiten, an Passwörter, Bankdaten und andere sicherheitsrelevante Informationen zu gelangen, indem sie sich als seriöse Webseiten ausgeben.

E-Mail-Client-Schutz

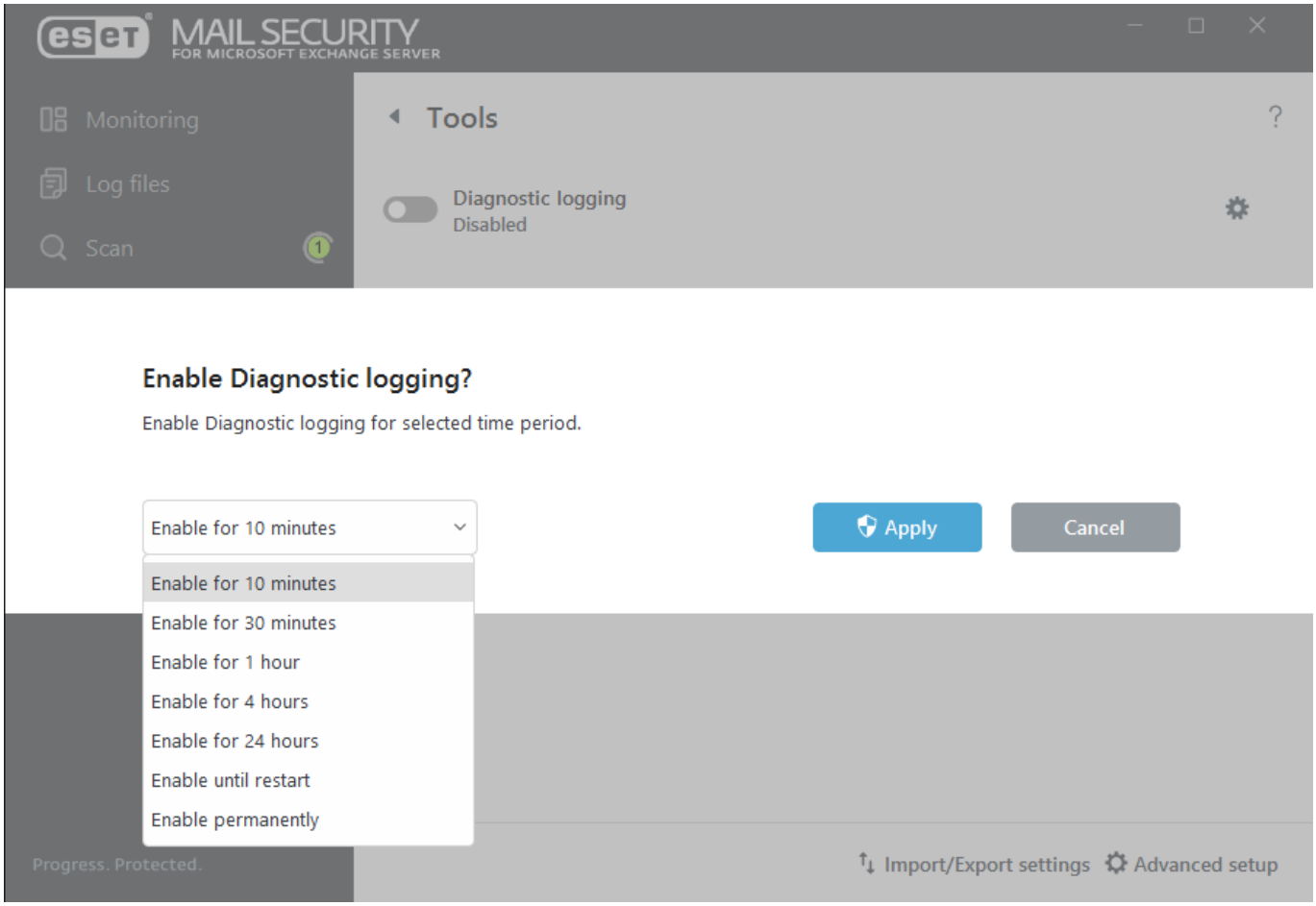
Überwacht eingehende E-Mails, die mit dem POP3- oder dem IMAP-Protokoll übertragen werden.



Tools - Diagnose-Logging

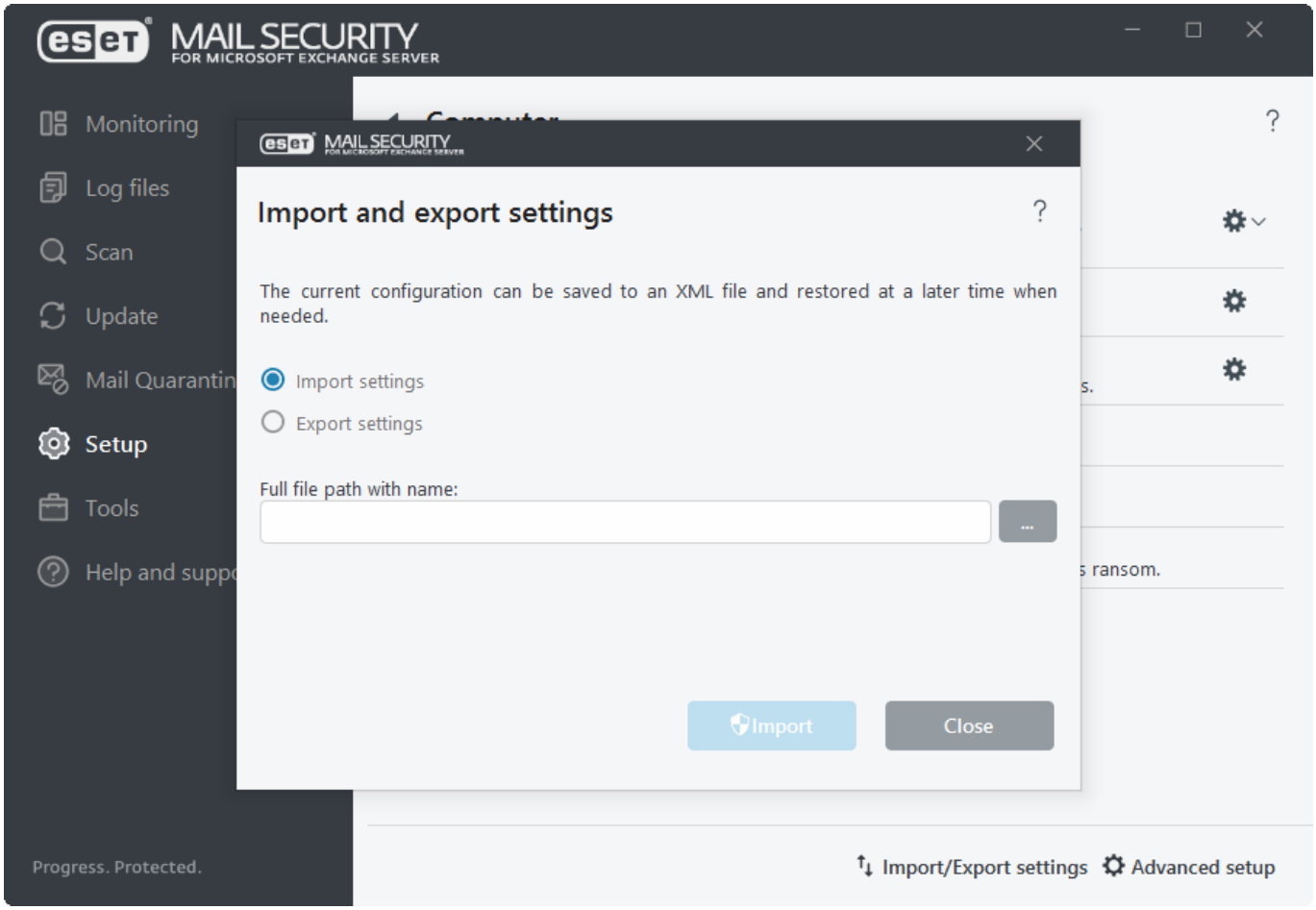
Aktivieren Sie das Diagnose-Logging, wenn Sie ausführliche Informationen zum Verhalten einer bestimmten ESET Mail Security-Funktion benötigen, z. B. für die Fehlerbehebung. Wenn Sie auf das Zahnradsymbol klicken, können Sie festlegen, für welche Funktionen Diagnose-Logs gesammelt werden sollen.

Wählen Sie aus, für welchen Zeitraum dieses Feature aktiviert werden soll (10 Minuten, 30 Minuten, 1 Stunde, 4 Stunden, 24 Stunden, bis zum nächsten Serverneustart oder permanent). Nachdem Sie das Diagnose-Logging aktiviert haben, sammelt ESET Mail Security ausführliche Logs für die ausgewählten Funktionen.



Einstellungen importieren/exportieren

Mit der Funktion zum Importieren und Exportieren von Einstellungen können Sie Ihre aktuelle ESET Mail Security-Konfiguration sichern. Außerdem können Sie diese Funktion verwenden, um dieselben Einstellungen auf anderen Servern mit ESET Mail Security zu verteilen oder anzuwenden. Die Einstellungen werden in eine *.xml*-Datei exportiert.

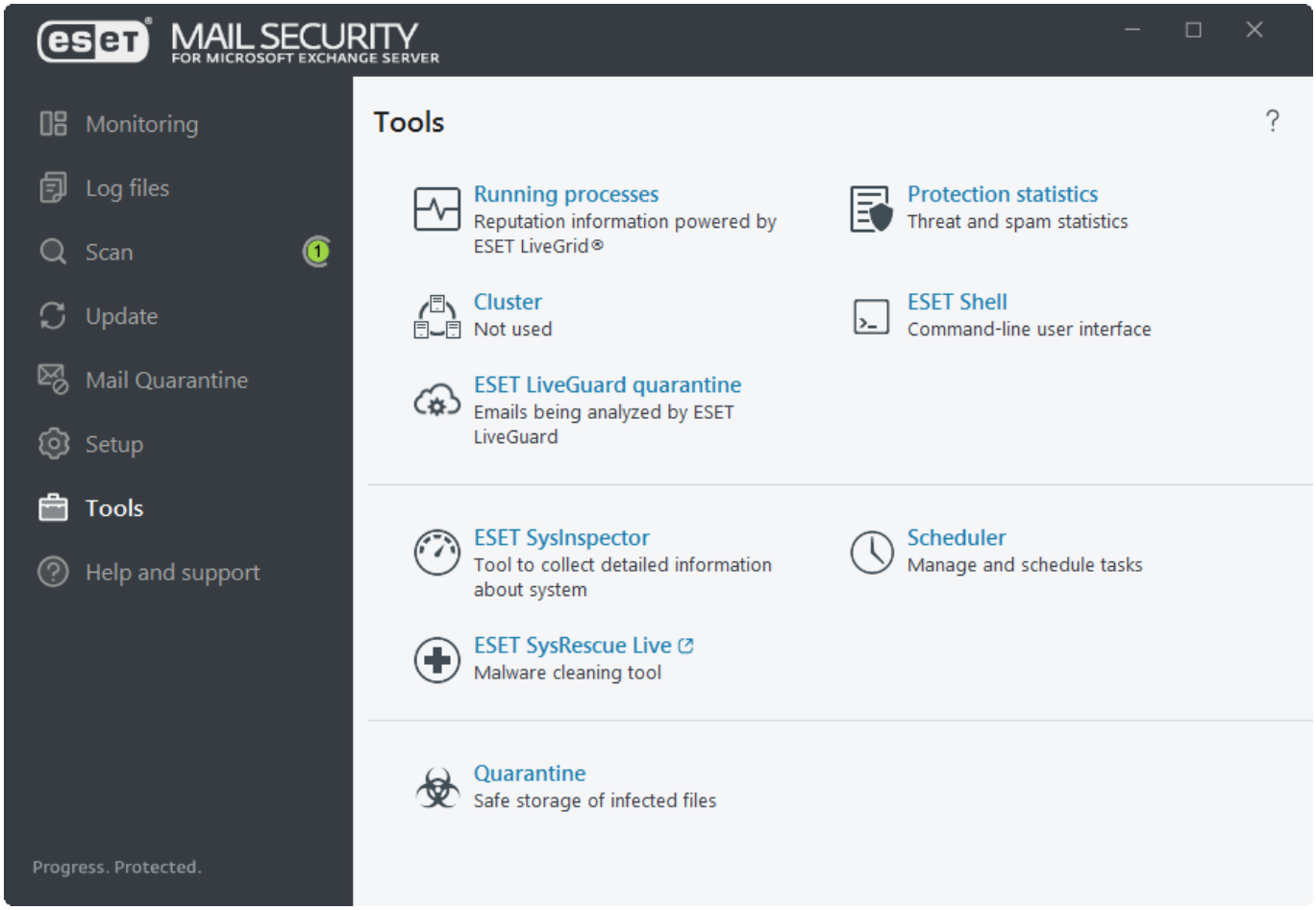


Beim Exportieren der Einstellungen kann ein Fehler auftreten, wenn Sie keine Berechtigung zum Schreiben der Datei in das angegebene Verzeichnis haben.

Tools

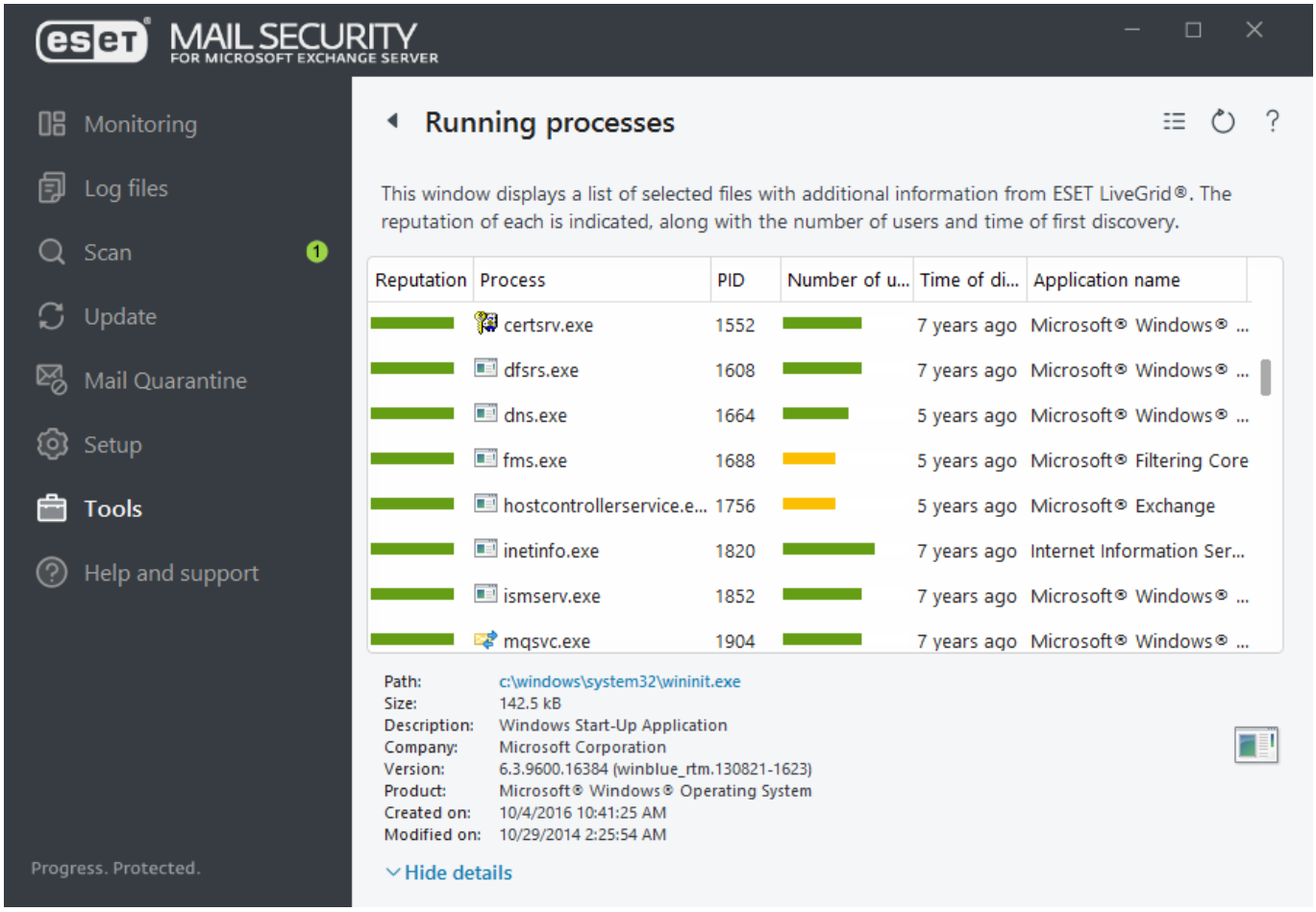
Für die ESET Mail Security-Verwaltung sind die folgenden Funktionen verfügbar:

- Ausgeführte Prozesse
- Schutzstatistiken
- Cluster
- ESET-Shell
- ESET LiveGuard Advanced
- ESET SysInspector
- ESET SysRescue Live
- Taskplaner
- Datei zur Analyse einreichen
- Quarantäne



Ausgeführte Prozesse

Die Informationen zu ausgeführten Prozessen zeigen die auf dem Computer ausgeführten Programme und Prozesse an und stellen dem ESET-Produkt laufend aktuelle Informationen zu neuen Infiltrationen bereit. ESET Mail Security bietet ausführliche Informationen zu ausgeführten Prozessen, um den Benutzern den Schutz der ESET LiveGrid®-Technologie zu bieten.



Bekannte Anwendungen, die als „Beste Reputation“ (grün) markiert sind, sind sauber (Whitelist) und werden vom Scannen ausgenommen. Dadurch wird der On-Demand-Scan bzw. der Echtzeit-Dateischutz auf Ihrem Computer beschleunigt.

Reputation	**Normalerweise bestimmen ESET Mail Security und die ESET LiveGrid®-Technologie die Reputation von Objekten mit einer Reihe heuristischer Regeln, bei denen die Eigenschaften der einzelnen Objekte (Dateien, Prozesse, Registrierungsschlüssel) untersuche und deren Potenzial für bösartige Aktivitäten eingeschätzt wird. Auf Basis dieser Heuristik wird den Objekten eine Reputationsstufe von 0 - Beste Reputation (grün) bis 9 - Schlechteste Reputation (rot) zugewiesen.**
Prozess	Zeigt den Namen des Programms oder Prozesses an, das/der derzeit auf dem Computer ausgeführt wird. Sie können alle auf Ihrem Computer ausgeführten Prozesse auch über den Windows-Taskmanager anzeigen. Öffnen Sie den Taskmanager, indem Sie mit der rechten Maustaste auf einen leeren Bereich auf der Taskleiste und dann auf „Taskmanager“ klicken oder indem Sie Strg+Umschalt+Esc auf Ihrer Tastatur drücken.
PID	Eine ID der in Windows-Betriebssystemen ausgeführten Prozesse.
Anzahl Benutzer	Die Anzahl der Benutzer, die eine bestimmte Anwendung verwenden. Diese Informationen werden von der ESET LiveGrid®-Technologie gesammelt.
Erkennungszeit	Die Zeitspanne seit der Erkennung der Anwendung durch die ESET LiveGrid®-Technologie.
Anwendungsname	Der festgelegte Name des Programms, zu dem der Prozess gehört.

Eine als unbekannt (orange) eingestufte Anwendung enthält nicht unbedingt Malware. In der Regel ist es einfach eine neuere Anwendung. Wenn Sie sich bei einer Datei unsicher sind, können Sie diese über die Funktion Datei zur Analyse einreichen an ESET übermitteln. Wenn sich herausstellt, dass die Datei Schadcode enthält, werden entsprechende Erkennungsfunktionen in zukünftigen Updates der Erkennungsroutine berücksichtigt.

Details anzeigen

Unten im Fenster werden die folgenden Informationen angezeigt:

- **Pfad** - Speicherort einer Anwendung auf Ihrem Computer.
- **Größe** - Dateigröße entweder in KB (Kilobyte) oder MB (Megabyte).
- **Beschreibung** - Dateieigenschaften auf Basis der Beschreibung des Betriebssystems.
- **Firma** - Name des Herstellers oder des Anwendungsprozesses.
- **Version** - Information vom Herausgeber der Anwendung.
- **Produkt** - Name der Anwendung und/oder Firmenname.
- **Erstellt** - Datum und Uhrzeit der Erstellung einer Anwendung.
- **Geändert** - Datum und Uhrzeit der letzten Änderung einer Anwendung.

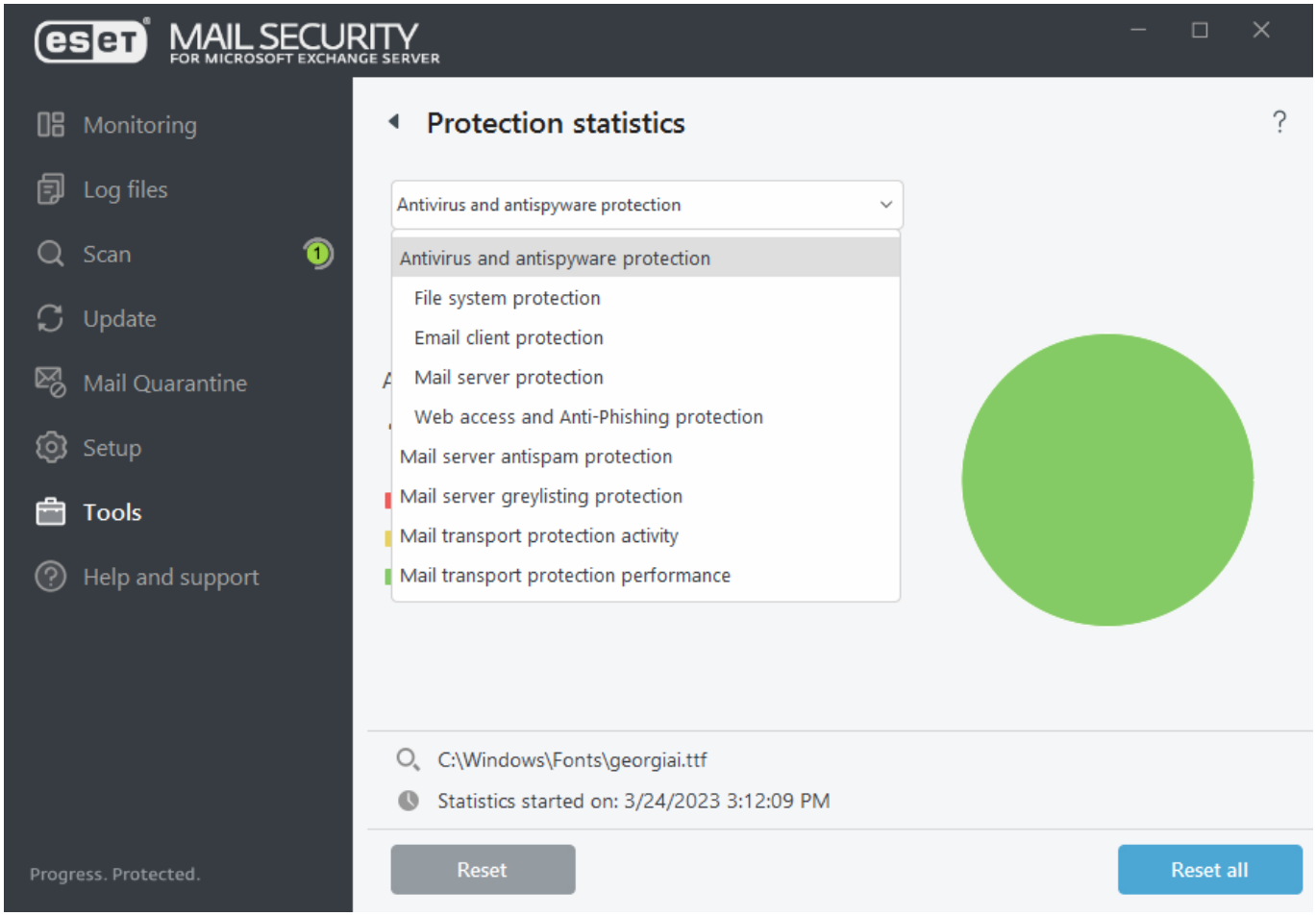
Zu ausgeschlossenen Prozessen hinzufügen

Klicken Sie mit der rechten Maustaste auf einen Prozess im Fenster „Ausgeführte Prozesse“, um den Prozess vom Scannen auszuschließen. Der entsprechende Pfad wird zur Liste der Ausgeschlossenen Prozesse hinzugefügt.

Schutzstatistiken

Wählen Sie das entsprechende Schutzmodul im Dropdownmenü aus, um Statistiken zu den Schutzmodulen von ESET Mail Security anzuzeigen. Neben dem Statistik-Diagramm wird die Gesamtanzahl der geprüften, infizierten, gesäuberten und sauberen Objekte angezeigt.

Bewegen Sie den Mauszeiger über ein Objekt neben dem Diagramm, um nur die Daten für das jeweilige Objekt im Diagramm anzuzeigen. Klicken Sie auf **Zurücksetzen**, um die Statistiken für das aktuelle Schutzmodul zurückzusetzen. Klicken Sie auf **Alle zurücksetzen**, um die Daten für alle Module zu löschen.



Folgende Statistikdiagramme stehen in ESET Mail Security zur Auswahl:

Viren- und Spyware-Schutz

Anzeige der Anzahl infizierter und gesäuberter Objekte.

Dateischutz

Anzeige von Objekten, die aus dem Dateisystem gelesen oder in das Dateisystem geschrieben wurden.

Hyper-V-Schutz

Anzeige der Anzahl infizierter, gesäuberter und sauberer Objekte (nur auf Systemen mit Hyper-V).

E-Mail-Client-Schutz

Anzeige von Objekten, die von E-Mail-Programmen gesendet oder empfangen wurden.

Web- und Phishing-Schutz

Anzeige von Objekten, die von einem Webbrowser heruntergeladen wurden.

E-Mail-Server-Schutz

Zeigt Anti-Malware-Statistiken für den E-Mail-Server an.

E-Mail-Server - Spam-Schutz

Anzeige des Verlaufs der Spam-Schutz-Statistiken. Die Anzahl unter Nicht geprüft bezieht sich auf Objekte, die von der Prüfung ausgeschlossen wurden (basierend auf Regeln, internen Nachrichten, authentifizierten Verbindungen usw.).

E-Mail-Server - Greylisting

Spam-Schutz-Statistiken für die Greylisting-Methode.

E-Mail-Transportschutz - Aktivität

Objekte, die vom E-Mail-Server geprüft/blockiert/gelöscht wurden.

E-Mail-Transportschutz - Leistung

Alle Daten, die mit VSAPI bzw. dem Transport-Agenten verarbeitet wurden (in B/s).

Postfach-Datenbankschutz - Aktivität

Objekte, die von VSAPI verarbeitet wurden (Anzahl geprüfter, in Quarantäne verschobener und gelöschter Objekte).

Postfach-Datenbankschutz - Leistung

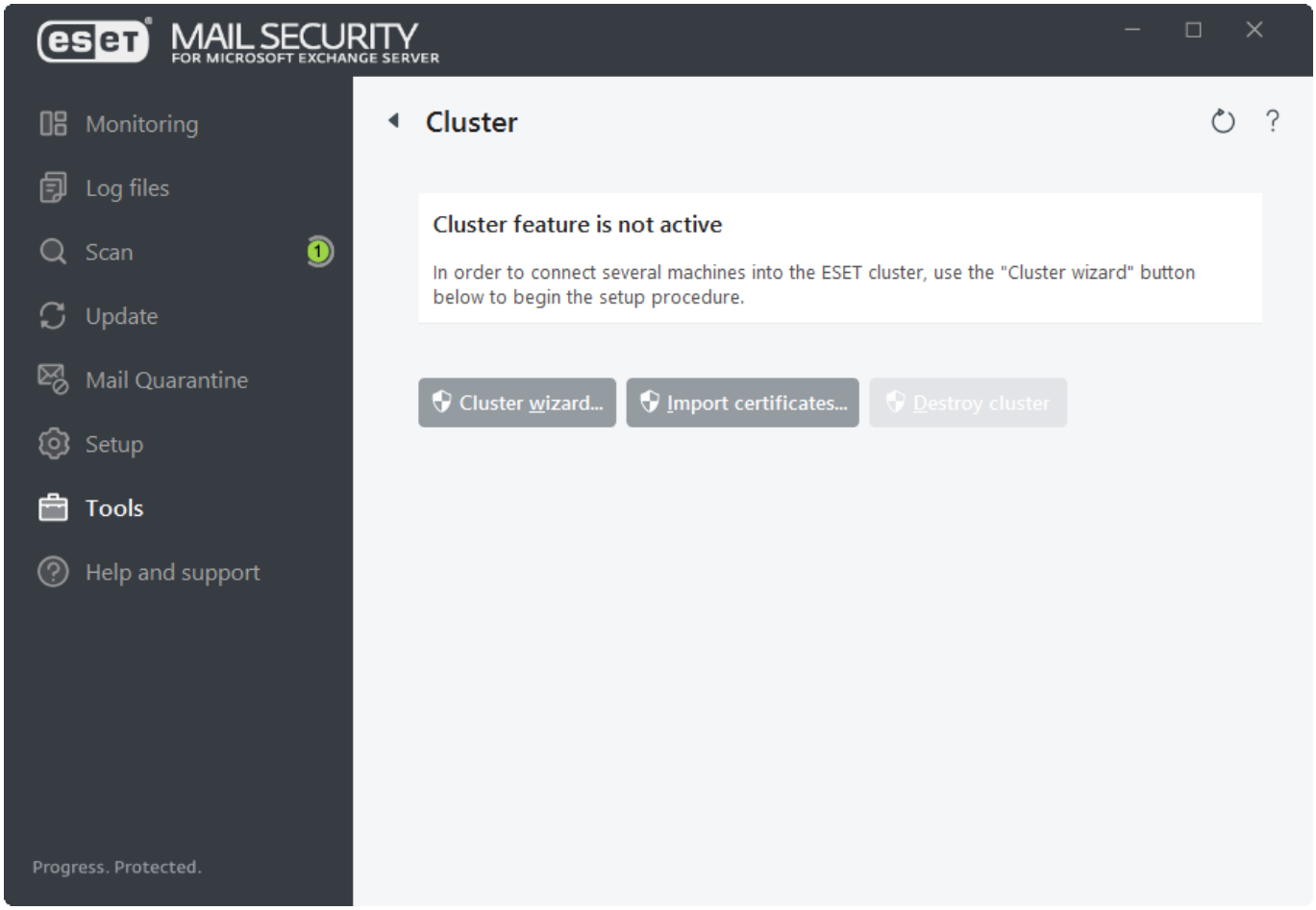
Alle von VSAPI verarbeiteten Daten (Anzahl der Mittelwerte für heute, für die letzten 7 Tage und Mittelwerte seit letztem Zurücksetzen).

Cluster

Der ESET-Cluster ist eine P2P-Kommunikationsinfrastruktur aus der ESET-Produktlinie für Microsoft Windows Server. Der ESET-Cluster eignet sich ideal für Exchange-Infrastrukturen mit mehreren Servern, z. B. als Datenbankverfügbarkeitsgruppe.

Mit dieser Infrastruktur können ESET-Serverprodukte miteinander kommunizieren, Daten wie Konfigurationsdaten und Benachrichtigungen austauschen, Greylisting-Datenbanken synchronisieren und die für den ordnungsgemäßen Betrieb einer Gruppe von Produktinstanzen erforderlichen Daten synchronisieren. 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.

i Die Einstellungen für die Benutzeroberfläche und geplante Tasks werden nicht zwischen ESET-Clusterknoten synchronisiert. Dies ist so gewollt. Damit wird beispielsweise verhindert, dass ein geplanter On-Demand-Datenbank-Scan auf allen Clusterknoten gleichzeitig ausgeführt wird, um Leistungsprobleme zu vermeiden.
Die Logs für den E-Mail-Server-Schutz werden pro Clusterknoten separat gespeichert und sind daher nicht synchronisiert. Mit der Funktion In Syslog-Server exportieren können Sie die Logs auf dem Syslog-Server im CEF-Format oder zur Verwendung mit einem SIEM-Tool duplizieren. Alternativ können Sie die Funktion „In Windows-Anwendungs- und -Dienst-Logs exportieren“ verwenden, falls Sie die Logs dort erfassen möchten.



Das Erstellen von ESET-Clustern zwischen ESET Mail Security und ESET File Security für Linux wird nicht unterstützt.

Beim Einrichten des ESET-Cluster können Sie Knoten auf zwei Arten hinzufügen:

- **Autom. erkennen** – Falls Sie ein vorhandenes Windows-Failovercluster oder NLB-Cluster haben, werden dessen Mitgliedsknoten automatisch zum ESET-Cluster hinzugefügt.
- **Durchsuchen** - Sie können Knoten manuell durch Eingeben der Servernamen hinzufügen (entweder Mitglieder der gleichen Arbeitsgruppe oder der gleichen Domäne).

Wenn Sie eine E-Mail aus der Quarantäne freigeben, ignoriert ESET Mail Security den `To:`-MIME-Header, da dieser sehr leicht zu fälschen ist. Stattdessen werden die Originaldaten des Empfängers aus der Ausgabe des Befehls `RCPT TO:` verwendet, der während der SMTP-Verbindung ausgeführt wurde. Damit wird sichergestellt, dass die aus der Quarantäne freigegebene E-Mail an den richtigen Empfänger zugestellt wird.

Nachdem Sie Knoten zum ESET-Cluster hinzugefügt haben, muss auf jedem Knoten ESET Mail Security installiert werden. Dies erfolgt automatisch während der Einrichtung des ESET-Cluster. Folgende Anmeldedaten sind für die Remote-Installation von ESET Mail Security auf anderen Clusterknoten erforderlich:

- **Domänenszenario**: Anmeldedaten des Domänenadministrators.
- **Arbeitsgruppenszenario**: Vergewissern Sie sich, dass alle Knoten die Anmeldedaten des gleichen lokalen Administratorkontos verwenden.

In einem ESET-Cluster können Sie auch eine Kombination aus automatisch hinzugefügten Knoten (Mitglieder eines

Windows-Failover-Cluster oder NLB-Cluster) und manuell hinzugefügten Knoten verwenden, sofern die Knoten sich in der gleichen Domäne befinden.

Domänenknoten und Arbeitsgruppenknoten können nicht kombiniert werden.

In einem ESET-Cluster muss außerdem die **Datei- und Druckerfreigabe** in der Windows-Firewall aktiviert werden, bevor ESET Mail Security auf die ESET-Clusterknoten verteilt wird.

Sie können jederzeit neue Knoten zu einem vorhandenen ESET-Cluster hinzufügen, indem Sie den Clusterassistenten ausführen.

Zertifikate importieren

Zertifikate ermöglichen eine sichere Computerauthentifizierung, wenn HTTPS verwendet wird. Jedes ESET-Cluster verwendet eine unabhängige Zertifikathierarchie. Die Hierarchie enthält ein Stammzertifikat und eine Reihe von Knotenzertifikaten, die mit dem Stammzertifikat signiert wurden. Der private Schlüssel des Stammzertifikats wird vernichtet, nachdem alle Knotenzertifikate erstellt wurden. Wenn Sie einen neuen Knoten zum Cluster hinzufügen, wird eine neue Zertifikathierarchie erstellt. Navigieren Sie zum Ordner, der die Zertifikate enthält, die vom Clusterassistenten erstellt wurden. Wählen Sie die Zertifikatdatei aus und klicken Sie auf **Öffnen**.

Cluster zerstören

ESET-Cluster können gelöscht werden. Jeder Knoten schreibt einen Eintrag zur Zerstörung des ESET-Clusters das eigene Ereignis-Log. Anschließend werden alle ESET-Firewall-Regeln aus der Windows-Firewall entfernt. Die ehemaligen Knoten werden in ihren vorherigen Zustand zurückversetzt und können bei Bedarf erneut in einem anderen ESET-Cluster verwendet werden.

Clusterassistent – Knoten auswählen

Der erste Schritt zur Einrichtung eines ESET-Clusters ist das Hinzufügen von Knoten. Verwenden Sie entweder die Option **Automatisch erkennen** oder fügen Sie die Knoten über die Funktion **Durchsuchen** manuell hinzu. Alternativ können Sie den Servernamen in das Textfeld eingeben und auf **Hinzufügen** klicken.

Autom. erkennen

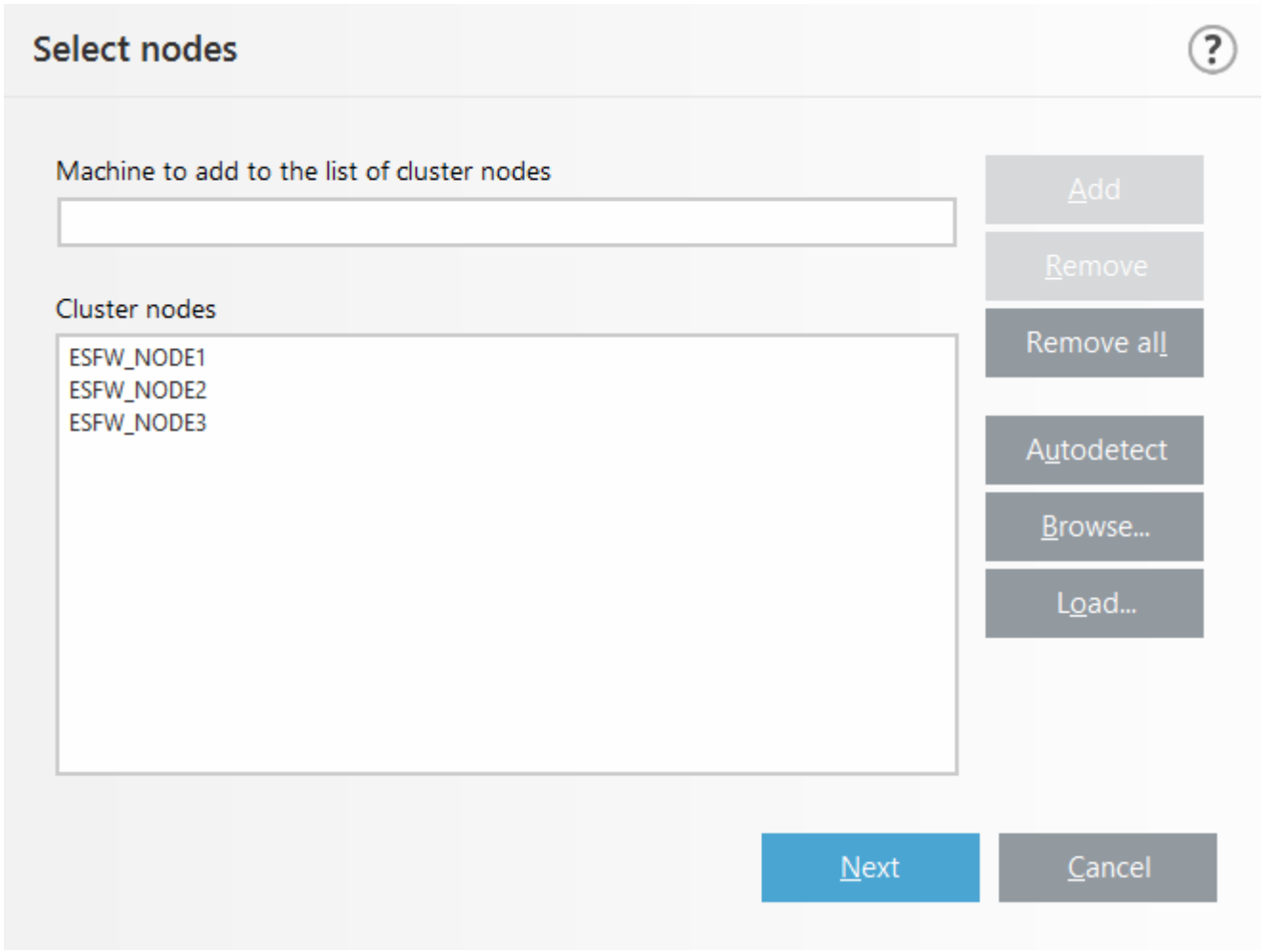
Fügt Knoten eines vorhandenen Windows Failover Cluster/Network Load Balancing (NLB) Cluster automatisch hinzu. Der Server, über den Sie den ESET-Cluster erstellen möchten, muss Mitglied eines Windows Failover Cluster/NLB Cluster sein, damit die Knoten automatisch hinzugefügt werden. Auf dem NLB-Cluster muss in den Clustereigenschaften die Option **Remotesteuerung zulassen** aktiviert sein, damit der die Knoten richtig erkennt. Nachdem die Liste der neu hinzugefügten Knoten erstellt wurde.

Durchsuchen

Klicken Sie auf „Durchsuchen“, um Computer innerhalb einer Domain oder Workgroup zu suchen und auszuwählen. Mit dieser Methode können Sie Knoten manuell zum ESET-Cluster hinzufügen. Eine weitere Methode zum Hinzufügen von Knoten ist die Eingabe des Hostnamens des hinzuzufügenden Servers. Bestätigen Sie die Eingabe durch Klicken auf **Hinzufügen**.

Laden

Importiert eine Liste von Knoten aus einer Datei.



Um **Clusterknoten** in der Liste zu ändern, wählen Sie einen zu entfernenden Knoten aus und klicken Sie auf **Entfernen**. Klicken Sie alternativ auf **Alle entfernen**, um die Liste vollständig zu löschen.

Sie können jederzeit Knoten zu einem bereits vorhandenen ESET-Cluster hinzufügen. Die Schritte entsprechen der oben beschriebenen Vorgehensweise.

Alle in der Liste verbleibenden Knoten müssen online und erreichbar sein. Localhost wird standardmäßig zu den Clusterknoten hinzugefügt.

Clusterassistent – Clustereinstellungen

Definieren Sie einen Clusternamen und Netzwerkeinstellungen (falls erforderlich).

Clustername

Wählen Sie einen Namen für den Cluster aus und klicken Sie auf Weiter.

Listening Port - (Der Standardport ist 9777)

Falls Port 9777 in Ihrer Netzwerkumgebung bereits verwendet wird, geben Sie eine andere, nicht verwendete Portnummer ein.

Port in Windows-Firewall öffnen

Wenn diese Option aktiviert ist, wird in der Windows-Firewall eine Regel erstellt.

Clusterassistent - Einstellungen für die Clustereinrichtung

Legen Sie einen Zertifikatverteilungsmodus fest und geben Sie an, ob das Produkt auf den anderen Knoten installiert werden soll oder nicht.

Zertifikatverteilung

- **Automatisch** remote - Das Zertifikat wird automatisch installiert.
- **Manuell** - Klicken Sie auf **Erstellen** und wählen Sie den Ordner aus, in dem die Zertifikate gespeichert werden sollen. Es werden ein Stammzertifikat und ein Zertifikat für jeden Knoten erstellt, einschließlich für den Knoten (lokaler Computer), auf dem Sie den ESET-Cluster einrichten. Klicken Sie auf **Ja**, um das Zertifikat auf dem lokalen Computer zu registrieren.

Produktinstallation an anderen Knoten

- **Automatisch remote** - ESET Mail Security wird auf jedem Knoten automatisch installiert (sofern die Betriebssysteme der Knoten dieselbe Architektur haben).
- **Manuell** - Manuelle Installation von ESET Mail Security (beispielsweise falls einige der Knoten eine andere Betriebssystemarchitektur aufweisen).

Lizenz auf Knoten ohne aktiviertes Produkt übertragen

ESET Security aktiviert die auf Knoten ohne Lizenzen installierten ESET-Lösungen automatisch.

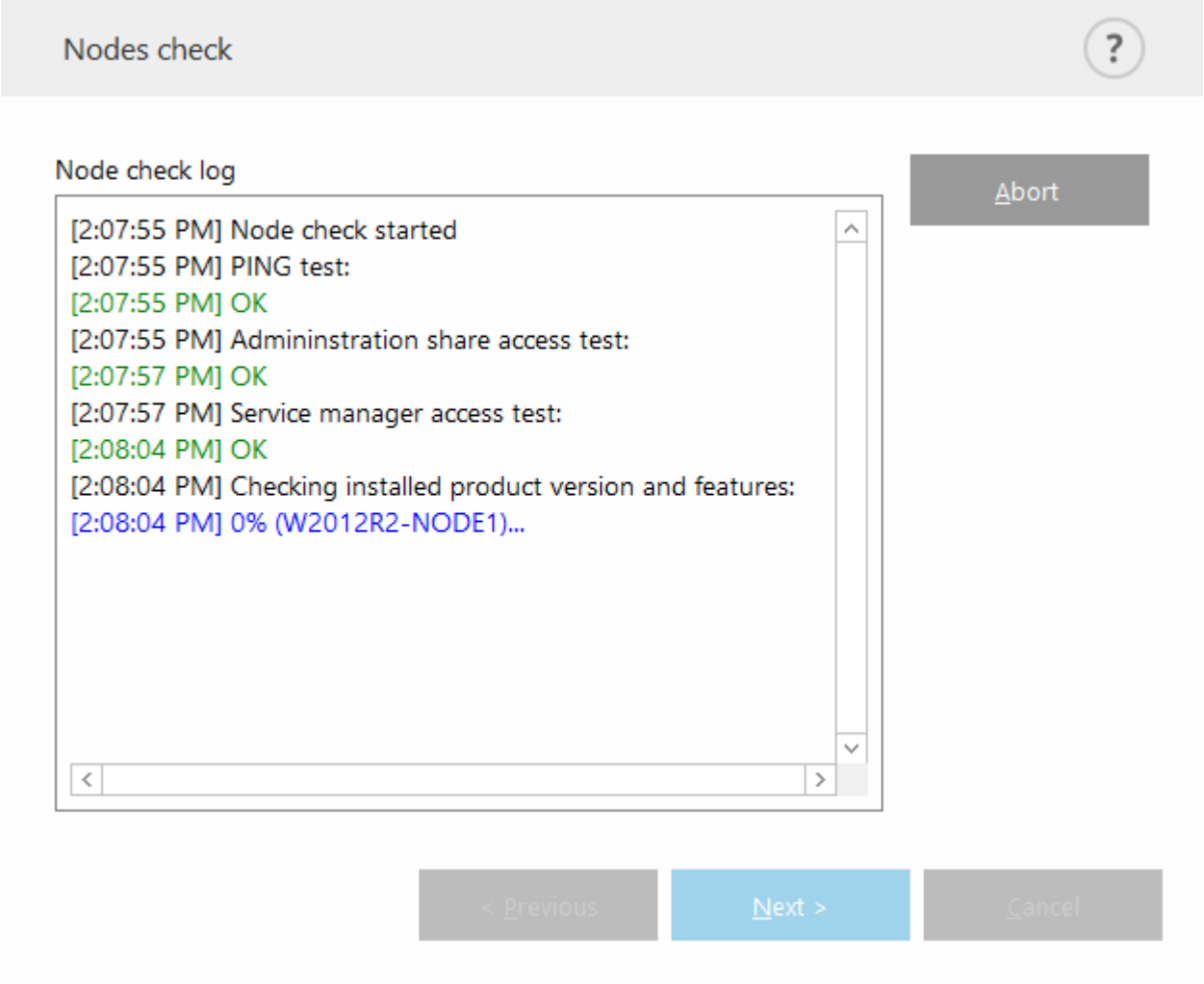
> Wenn Sie einen ESET-Cluster mit gemischten Betriebssystemarchitekturen (32-Bit und 64-Bit) erstellen möchten, müssen Sie ESET Mail Security manuell installieren. Die verwendeten Betriebssysteme werden in den nächsten Schritten ermittelt, und die Informationen werden im Log-Fenster angezeigt.

Clusterassistent – Knotenprüfung

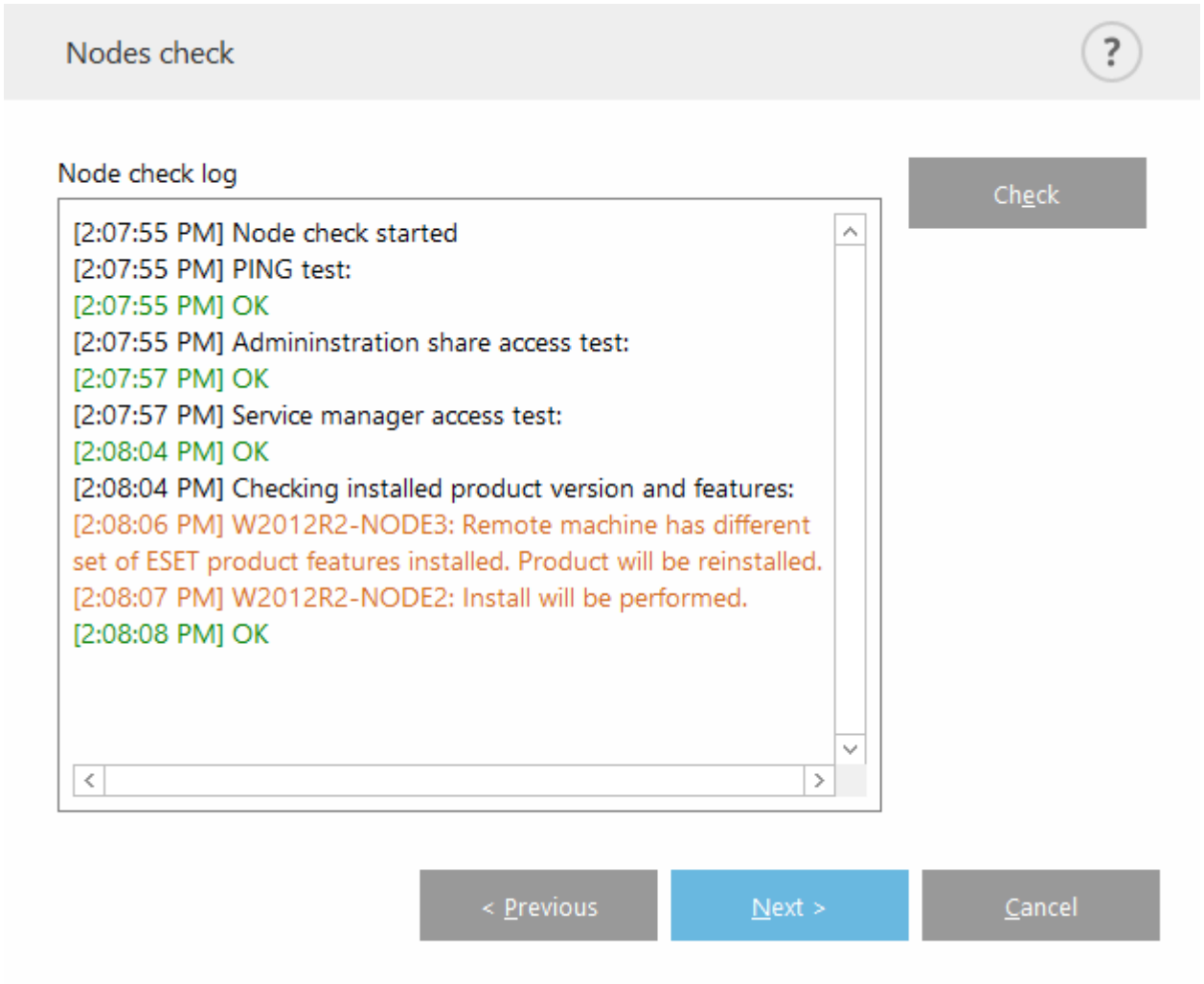
Nach dem Festlegen der Installationsdetails wird eine Knotenprüfung ausgeführt. Die folgenden Informationen werden im **Knotenprüfungs-Log** angezeigt:

- Alle vorhandenen Knoten sind online.
- Die neuen Knoten sind erreichbar.
- Der Knoten ist online.
- Der Zugriff auf die administrative Freigabe ist möglich.
- Die Remote-Ausführung ist möglich.
- Die richtigen Produktversionen sind installiert bzw. es ist kein Produkt installiert.

- Die neuen Zertifikate sind vorhanden.

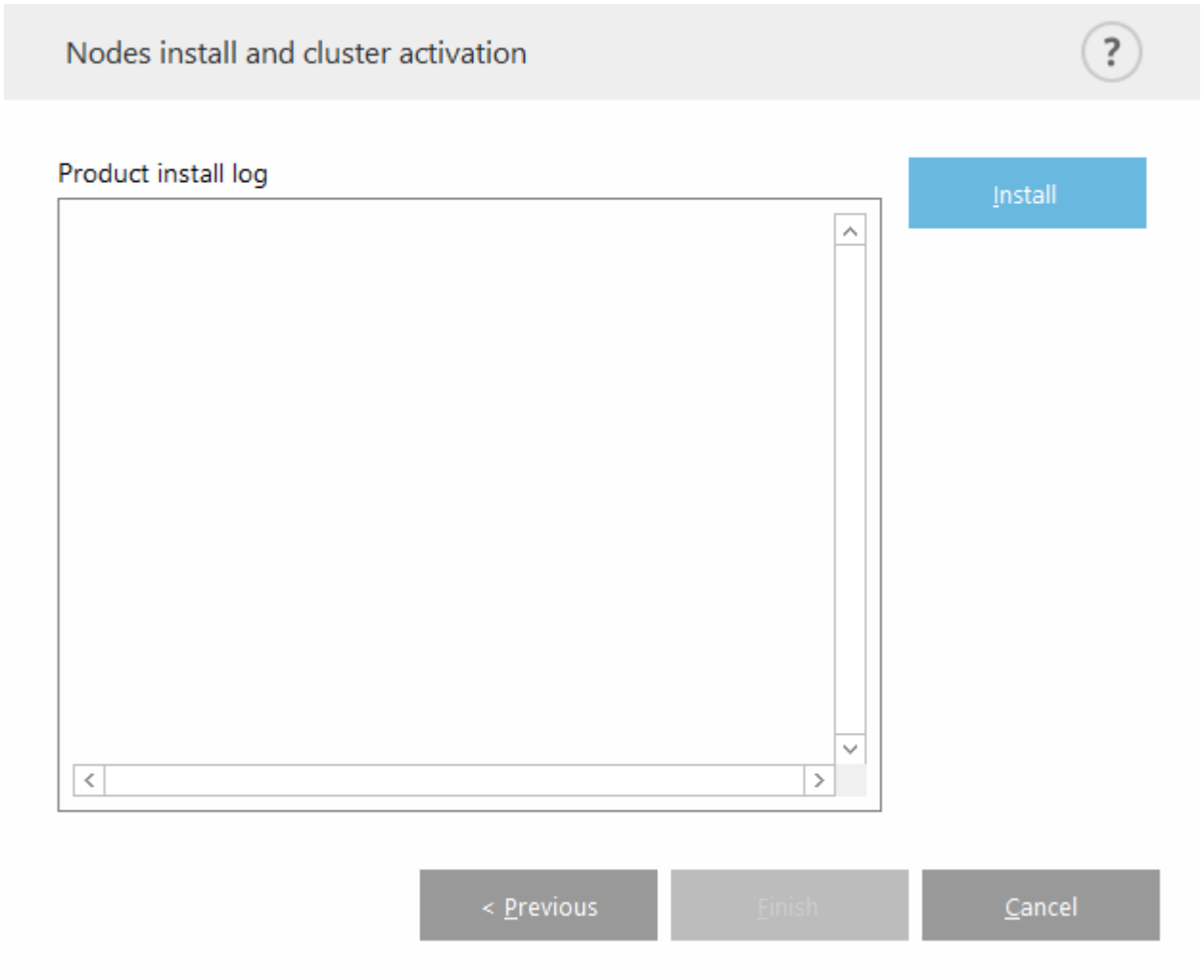


Nach dem Abschließen der Knotenprüfung wird der Bericht angezeigt:

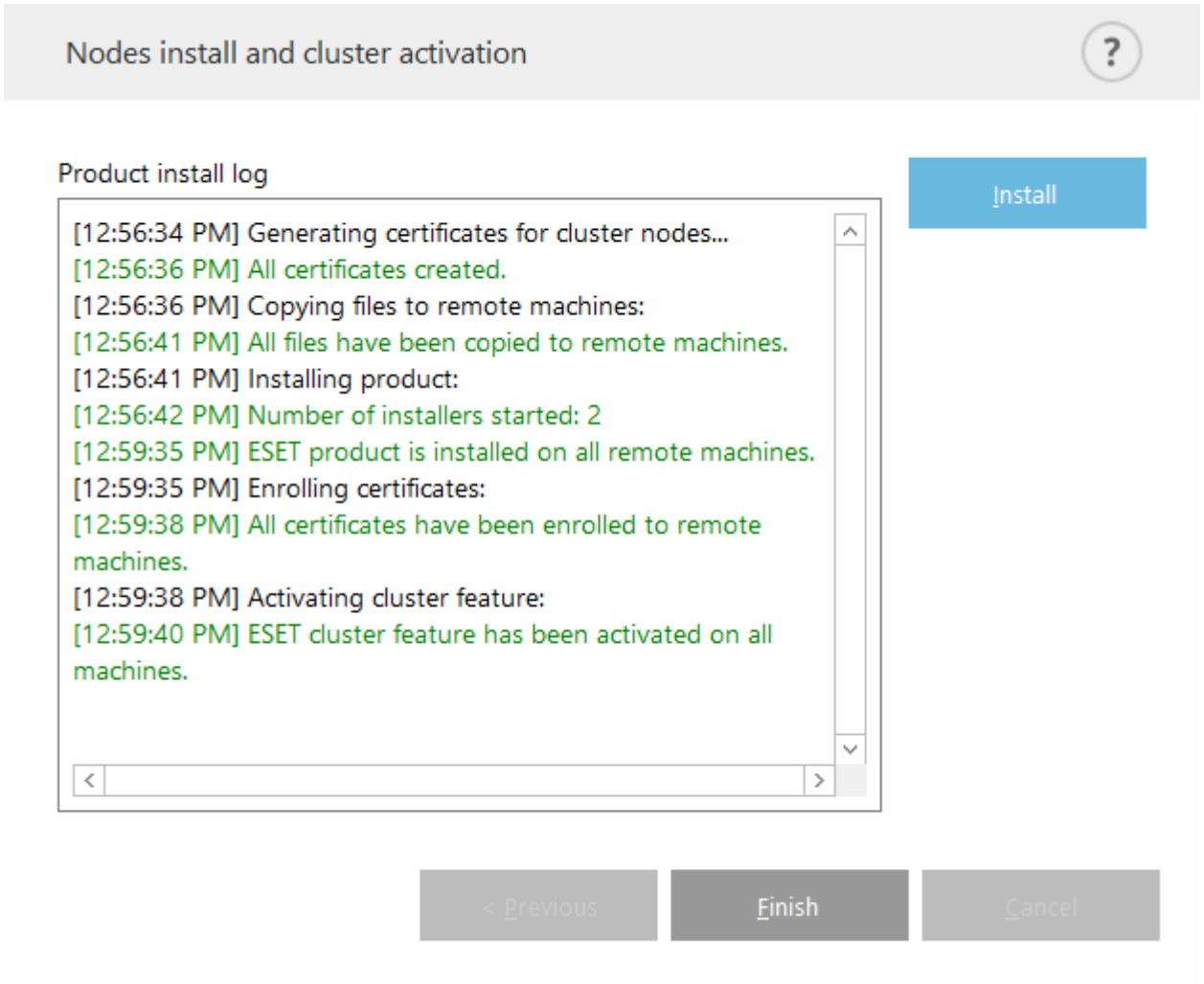


Clusterassistent - Knoteninstallation

Wenn Sie das Produkt bei der Initialisierung des ESET-Clusters auf einem Remotecomputer installieren, sucht der Assistent das Installationspaket im Verzeichnis *%ProgramData%\ESET\ESET Security\Installer*. Wenn das Installationspaket dort nicht gefunden wird, werden Sie aufgefordert, den Speicherort der Datei anzugeben.



Wenn Sie versuchen, eine automatische Remoteinstallation für einen Knoten einer anderen Plattform (32-Bit im Gegensatz zu 64-Bit) auszuführen, erkennt das Programm die Situation und fordert Sie auf, eine manuelle Installation auszuführen.



Nachdem Sie den ESET-Cluster richtig konfiguriert haben, wird er auf der Seite **Einstellungen** > **Server** mit dem Status „aktiviert“ angezeigt.

Wenn auf einigen Knoten bereits eine ältere Version von ESET Mail Security installiert ist, wird eine Benachrichtigung angezeigt, dass die aktuelle Version auf diesen Computern benötigt wird. Bei der Aktualisierung von ESET Mail Security wird unter Umständen ein Neustart durchgeführt.

Sie können den aktuellen Status auch auf der Clusterstatusseite (**Tools** > **Cluster**) überprüfen.

ESET-Shell

eShell (Abkürzung für ESET Shell) ist eine Kommandozeilen-Schnittstelle für ESET Mail Security. Über eShell haben Sie Zugriff auf alle Funktionen und Optionen, die Ihnen sonst über die Benutzeroberfläche zur Verfügung stehen. Mit eShell können Sie ohne die GUI das gesamte Programm konfigurieren und verwalten.

Neben der Bereitstellung aller Funktionen und Optionen, die über die Benutzeroberfläche steuerbar sind, bietet die Kommandozeile auch die Möglichkeit, Prozesse durch Skripte zu automatisieren. Mit ihnen können Sie das Programm konfigurieren, Änderungen vornehmen und Aktionen ausführen. Außerdem ist eShell nützlich für alle Benutzer, die eine Kommandozeile generell der Benutzeroberfläche vorziehen.

Um den vollständigen Funktionsumfang zu nutzen, sollten Sie eShell mit der Option Als Administrator ausführen starten. Dasselbe gilt für das Ausführen einzelner Befehle in der Windows-Eingabeaufforderung (cmd). Öffnen Sie die Eingabeaufforderung mit **Als Administrator ausführen**. Andernfalls können Sie manche Befehle mangels Berechtigungen nicht ausführen.

eShell kann in den folgenden beiden Modi ausgeführt werden:

1. **Interaktiver Modus** - Dieser Modus eignet sich, wenn Sie umfassend mit eShell arbeiten möchten (also nicht nur einzelne Befehle ausführen), z. B. zum Ändern der Konfiguration oder Anzeigen von Log-Dateien. Der interaktive Modus bietet sich auch an, wenn Sie noch nicht mit allen Befehlen vertraut sind. Der interaktive Modus erleichtert die Navigation durch eShell. In diesem Modus werden auch die im jeweiligen Kontext verfügbaren Befehle angezeigt.

2. **Einzelner Befehl/Batch-Modus** - Verwenden Sie diesen Modus, wenn Sie nur einen Befehl ausführen müssen, ohne dabei den interaktiven Modus von eShell zu verwenden. Geben Sie dazu in der Windows-Eingabeaufforderung `eshell` mit den entsprechenden Parametern ein.

```
eshell get status or eshell computer set real-time status disabled 1h
```

Um bestimmte Befehle (wie das zweite Beispiel oben) ausführen zu können, müssen Sie zunächst einige Einstellungen konfigurieren. Andernfalls erhalten Sie die Nachricht mit **Zugriff verweigert**. Dies ist aus Sicherheitsgründen erforderlich.

Sie benötigen die Berechtigung zur Ausführung von eShell-Befehlen in einer Windows-Eingabeaufforderung, um Einstellungen ändern zu können. Weitere Informationen zum Ausführen von Batch-Dateien finden Sie hier.

Sie können den interaktiven Modus in eShell auf zwei Arten aktivieren:

1. Über das **Windows-Startmenü**: Start > Alle Programme > ESET > ESET Mail Security > ESET-Shell

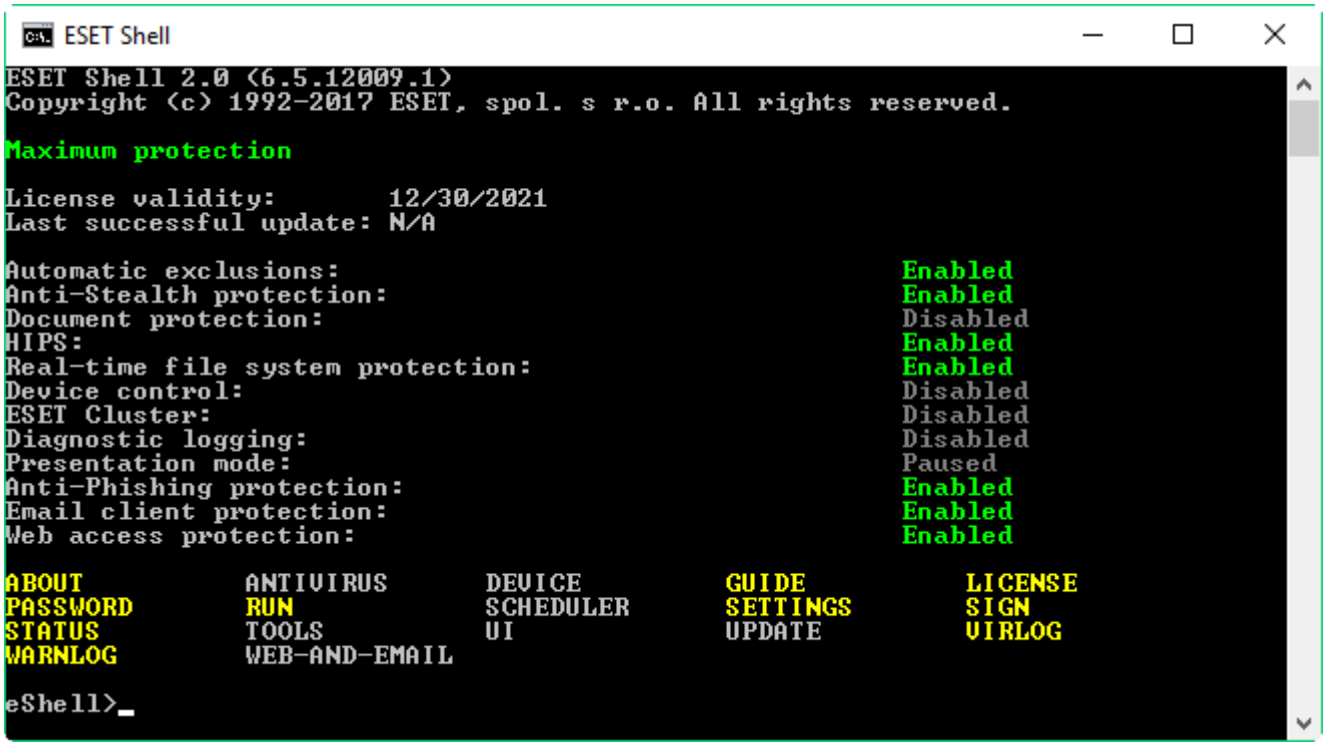
2. Über die **Windows-Eingabeaufforderung** Geben Sie `eshell` ein und drücken Sie die Eingabetaste

Falls der Fehler `'eshell' not recognized as an internal or external command` angezeigt wird, wurden die neuen Umgebungsvariablen nach der Installation von ESET Mail Security nicht vom System geladen.
Öffnen Sie eine neue Eingabeaufforderung und starten Sie eShell neu. Falls der Fehler weiterhin auftritt oder Sie eine Core-Installation von ESET Mail Security verwenden, starten Sie eShell mit dem absoluten Pfad, zum Beispiel `"%PROGRAMFILES%\ESET\ESET Mail Security\eShell.exe"` (Die Anführungszeichen `"""` sind erforderlich für den Befehl).

Wenn Sie eShell zum ersten Mal im interaktiven Modus ausführen, wird ein Willkommens- (Anleitungs-)bildschirm angezeigt.

Um diesen Bildschirm später erneut zu öffnen, geben Sie den Befehl `guide` ein. Hier finden Sie einfache Beispiele für die Verwendung von eShell sowie Informationen zu Syntax, Präfixen, Befehlspfaden, Abkürzungen, Aliasnamen usw.

Bei der nächsten Ausführung von eShell wird der folgende Bildschirm angezeigt:



Bei der Befehlseingabe müssen Sie nicht auf Groß- und Kleinschreibung achten. Der Befehl wird unabhängig davon ausgeführt, ob Sie Groß- oder Kleinbuchstaben verwenden.

Anpassen eShell

Sie können eShell im `ui eshell`-Kontext anpassen. Sie können Aliase, Farben, Sprache, Ausführungsrichtlinie für Skripts konfigurieren, ausgeblendete Befehle anzeigen und andere Einstellungen vornehmen.

Nutzung

Syntax

Die Befehle funktionieren nur dann ordnungsgemäß, wenn sie mit der richtigen Syntax eingegeben werden. Sie können aus einem Präfix, einem Kontext, Argumenten, Optionen usw. bestehen. Allgemein verwendet eShell die folgende Syntax:

[<prefix>] [<command path>] <command> [<arguments>]

Beispiel (aktiviert den Dokumentenschutz):
`SET COMPUTER SCANS DOCUMENT REGISTER ENABLED`

`SET` - Ein Präfix

`COMPUTER SCANS DOCUMENT` - Pfad zu einem bestimmten Befehl, also der Kontext des Befehls

`REGISTER` - Der eigentliche Befehl

`ENABLED` - Ein Argument für den Befehl

Wenn Sie `?` als Argument für einen Befehl angeben, wird die Syntax des entsprechenden Befehls angezeigt. `STATUS ?` zeigt beispielsweise die Syntax für den Befehl `STATUS` an:

SYNTAX:

```
[get] status
```

VORGÄNGE:

`get` - Status aller Schutzmodule anzeigen

Beachten Sie, dass `[get]` in Klammern steht. Dies bedeutet, dass das Präfix `get` das Standardpräfix für den Befehl `status` ist. Wird also dem Befehl `status` kein bestimmtes Präfix zugewiesen, wird das Standardpräfix verwendet (in diesem Fall `get status`). Wenn Sie das Präfix weglassen, sparen Sie Zeit beim Eingeben von Befehlen. Üblicherweise ist `get` das Standardpräfix der meisten Befehle. Dennoch sollten Sie das Standardpräfix des jeweiligen Befehls kennen und sich sicher sein, dass Sie ihn so ausführen möchten.

> **i** Bei der Befehlseingabe müssen Sie nicht auf Groß- und Kleinschreibung achten. Der Befehl wird unabhängig davon ausgeführt, ob Sie Groß- oder Kleinbuchstaben verwenden.

Präfix / Vorgang

Ein Präfix ist ein Vorgang. Das Präfix `GET` zeigt die Konfiguration einer bestimmten ESET Mail Security-Funktion oder den Status an (z. B. zeigt `GET COMPUTER REAL-TIME STATUS` den aktuellen Schutzstatus an). Das Präfix `SET` konfiguriert die Funktion bzw. ändert ihren Status (`SET COMPUTER REAL-TIME STATUS ENABLED` aktiviert den Schutz).

Die folgenden Präfixe sind in eShell verfügbar. Je nach Befehl werden bestimmte Präfixe unterstützt.

GET	gibt aktuelle Einstellung/aktuellen Status zurück
SET	legt Wert/Status fest
SELECT	element auswählen
ADD	element hinzufügen
REMOVE	element entfernen
CLEAR	entfernt alle Elemente/Dateien
START	aktion starten
STOP	aktion beenden
PAUSE	Aktion anhalten
RESUME	aktion fortsetzen
RESTORE	stellt Standardeinstellungen/-objekt/-datei wieder her
SEND	objekt/Datei senden
IMPORT	aus Datei importieren
EXPORT	in Datei exportieren

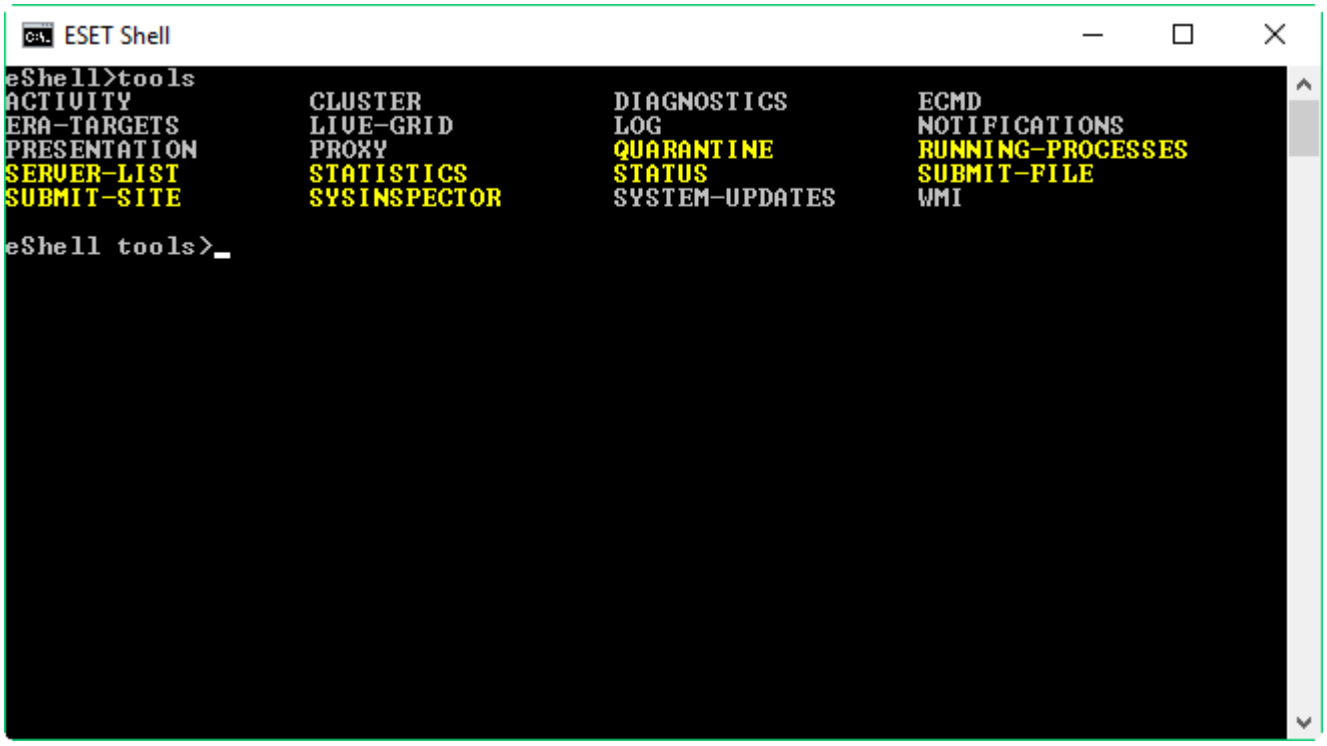
> **i** Präfixe wie `GET` und `SET` werden für viele, aber nicht alle Befehle verwendet. Der Befehl `EXIT` verwendet zum Beispiel kein Präfix.

Befehlspfad / Kontext

Befehle sind in einen Kontext in Form einer Baumstruktur eingebettet. Die höchste Ebene bildet der Kontext „root“. Beim Start von eShell befinden Sie sich also auf der Root-Ebene.

```
eShell>
```

Hier können Sie einen Befehl ausführen oder den Kontextnamen eingeben, um in der Baumstruktur zu navigieren. Wenn Sie zum Beispiel den Kontext `TOOLS` eingeben, werden alle dort verfügbaren Befehle und untergeordneten Kontexte aufgelistet.



Gelbe Elemente stellen ausführbare Befehle und graue Elemente stellen auswählbare untergordnete Kontexte dar. Ein untergeordneter Kontext enthält weitere Befehle.

Wenn Sie auf eine höhere Ebene zurückkehren möchten, geben Sie `..` ein (zwei Punkte).

> ✓ Nehmen wir beispielsweise an, Sie befinden sich hier:
> `eShell computer real-time>`
> Geben Sie „`..`“ ein, um zur nächsthöheren Ebene zu wechseln:
> `eShell computer>`

Wenn Sie dagegen von `eShell computer real-time>` wieder die zwei Ebenen zur Root-Ebene hochgehen möchten, geben Sie `.. ..` ein (zwei Punkte, Leerzeichen, zwei Punkte). So gelangen Sie zwei Ebenen höher (in diesem Fall zur Root-Ebene). Verwenden sie den umgekehrten Schrägstrich `\`, um von jeder beliebigen Ebene in der Kontextstruktur direkt zur Stammebene zu gelangen. Um zu einem bestimmten Kontext in höheren Ebenen zu gelangen, verwenden Sie die entsprechende Anzahl von `..`-Befehlen. Verwenden Sie Leerzeichen als Trennzeichen. Um drei Ebenen nach oben zu gelangen, verwenden Sie `.. .. ..`

Der Pfad ist relativ zum aktuellen Kontext. Geben Sie den Pfad nicht ein, wenn der Befehl im aktuellen Kontext enthalten ist. Um zum Beispiel `GET COMPUTER REAL-TIME STATUS` auszuführen, geben Sie Folgendes ein:

`GET COMPUTER STATUS` - wenn Sie sich im Root-Kontext befinden (Kommandozeile zeigt an `eShell>`)

`GET STATUS` - wenn Sie sich im Root-Kontext `COMPUTER` befinden (Kommandozeile zeigt an `eShell computer>`)

`.. GET STATUS` - wenn Sie sich im Root-Kontext `COMPUTER REAL-TIME` befinden (Kommandozeile zeigt an `eShell computer real-time>`)

Sie können einen einfachen Punkt (`.`) verwenden, weil ein einzelner Punkt eine Abkürzung für zwei Punkte (`..`)

ist.

✓ `. GET STATUS` - wenn Sie sich im Root-Kontext `COMPUTER REAL-TIME` befinden (Kommandozeile zeigt an `eShell computer real-time>`)

Argument

Ein Argument ist eine Aktion, die für einen bestimmten Befehl ausgeführt wird. Der Befehl `CLEAN-LEVEL` (unter `COMPUTER REAL-TIME ENGINE`) kann beispielsweise mit den folgenden Argumenten verwendet werden:

`rigorous` - Ereignis immer beheben

`safe` - Ereignis beheben, falls sicher, andernfalls beibehalten

`normal` - Ereignis beheben, falls sicher, andernfalls nachfragen

`none` – Endbenutzer immer fragen

Weitere Beispiele sind die Argumente `ENABLED` oder `DISABLED`, mit denen Sie bestimmte Optionen oder Funktionen aktivieren oder deaktivieren können.

Kurzformen

In eShell können Sie Kontexte, Befehle und Argumente abkürzen (falls es sich bei dem Argument um einen Switch oder eine alternative Option handelt). Die Abkürzung eines Präfixes oder eines Arguments in Form eines konkreten Wertes (z. B. Nummer, Name oder Pfad) ist nicht möglich. Sie können die Ziffern `1` und `0` anstelle der Argumente „enabled“ und „disabled“ verwenden.

✓
```
computer set real-time status enabled        =>        com set real stat 1
computer set real-time status disabled        =>        com set real stat 0
```

Beispiele für die Kurzform:

✓
```
computer set real-time status enabled        =>        com set real stat en
computer exclusions add detection-excludes object C:\path\file.ext        =>        com excl add det obj C:\path\file.ext
computer exclusions remove detection-excludes 1        =>        com excl rem det 1
```

Wenn zwei Befehle oder Kontexte gleich beginnen (z. B. `ADVANCED` and `AUTO-EXCLUSIONS`) und Sie `A` als verkürzte Befehlsform wählen, kann eShell nicht bestimmen, welchen der beiden Befehle Sie ausführen möchten. In diesem Fall wird eine Fehlermeldung und eine Liste der verfügbaren Befehle mit dem Anfangsbuchstaben `A` angezeigt:

```
eShell>a
```

Der folgende Befehl ist nicht eindeutig: `a`

Die folgenden Unterkontexte sind im Kontext `COMPUTER` verfügbar:

`ADVANCED`

`AUTO-EXCLUSIONS`

Wenn Sie mehrere Buchstaben eingeben (z. B. `AD` anstelle von `A`), wechselt eShell zum Unterkontext `ADVANCED`, da der Befehl jetzt eindeutig ist. Dasselbe gilt für abgekürzte Befehle.

Um den Befehl korrekt auszuführen, sollten Sie Befehle, Argumente usw. nicht abkürzen, sondern vollständig angeben. Auf diese Weise führt eShell die Befehle genau wie angegeben aus, und unerwünschte Fehler werden vermieden. Dies gilt vor allem für Batch-Dateien und Skripte.

Automatische Vervollständigung

Diese mit Version eShell 2.0 eingeführte Funktion entspricht der automatischen Vervollständigung in der Windows-Befehlszeile. Während die Windows-Befehlszeile nur Dateipfade vervollständigt, verwendet eShell diese Funktion auch für Befehle, Kontext- und Vorgangsnamen. Die Vervollständigung von Argumenten wird nicht unterstützt.

Drücken Sie bei der Eingabe eines Befehls die TAB-Taste, um den Befehl zu vervollständigen oder durch die möglichen Variationen zu blättern.

Drücken Sie UMCH + TAB, um rückwärts zu blättern. Mischungen zwischen abgekürzter Form und automatischer Vervollständigung werden nicht unterstützt. Sie können jeweils nur eine der beiden Formen verwenden.

Wenn Sie zum Beispiel `computer real-time additional` eingeben, bewirkt TAB nichts. Geben Sie stattdessen `com` ein und drücken Sie TAB, um `computer` zu vervollständigen, geben Sie dann `real` + TAB und `add` + TAB ein und drücken Sie die Eingabetaste. Geben Sie `on` + TAB ein und drücken Sie mehrfach auf TAB, um alle möglichen Variationen zu durchlaufen: `on-execute-ah, on-execute-ah-removable, on-write-ah, on-write-archive-default` usw..

Aliasnamen

Ein Alias ist ein alternativer Name, um einen Befehl auszuführen (vorausgesetzt, dass diesem Befehl ein Alias zugewiesen wurde). Dies sind die Standard-Aliase:

`(global) close` - exit

`(global) quit` - exit

`(global) bye` - exit

`warnlog` - tools log events

`virlog` - tools log detections

`(global)` bedeutet, dass der Befehl unabhängig vom aktuellen Kontext überall ausgeführt werden kann. Einem Befehl können mehrere Aliasnamen zugewiesen werden. Der Befehl `EXIT` hat beispielsweise die Aliasnamen `CLOSE`, `QUIT` und `BYE`. Wenn Sie eShell beenden möchten, können Sie den Befehl `EXIT` oder einen seiner Aliasnamen verwenden.

Der Aliasname `VIRLOG` bezieht sich auf den Befehl `DETECTIONS` im Kontext `TOOLS LOG`. Mit diesem Alias ist der Befehl im Kontext `ROOT` verfügbar und so leichter erreichbar (Sie müssen nicht erst in die Kontexte `TOOLS` und dann `LOG` wechseln, sondern starten den Befehl direkt in `ROOT`).

In eShell können Sie eigene Aliasnamen definieren. Der Befehl `ALIAS` befindet sich im Kontext `UI ESHELL`.

Einstellungen mit Passwort schützen

Die ESET Mail Security-Einstellungen können mit einem Passwort geschützt werden. Sie können das Passwort in der Benutzeroberfläche oder in eShell mit dem Befehl `set ui access lock-password`.

Anschließend müssen Sie dieses Passwort interaktiv für bestimmte Befehle eingeben (z. B. beim Ändern von Einstellungen oder von Daten). Wenn Sie über längere Zeit mit eShell arbeiten und das Passwort nicht ständig eingeben möchten, können Sie es in eShell mit dem Befehl `set password` speichern (als `root` ausgeführt). Das Passwort wird anschließend automatisch für alle Befehle ausgefüllt, für die ein Passwort erforderlich ist. Es bleibt gespeichert, bis Sie eShell verlassen. Sie müssen `set password` also erneut ausführen, wenn Sie Ihr Passwort in einer neuen eShell-Sitzung erneut speichern möchten.

Guide / Help

Wenn Sie den Befehl `GUIDE` oder `HELP` ausführen, wird ein Bildschirm mit Benutzungshinweisen für eShell angezeigt. Dieser Befehl ist nur im Kontext `ROOT` verfügbar (`eShell>`).

Befehlsverlauf

eShell speichert einen Verlauf der bereits ausgeführten Befehle. Gespeichert werden aber nur die Befehle der aktuellen interaktiven eShell-Sitzung. Wenn Sie eShell beenden, wird der Befehlsverlauf gelöscht. Mit den Pfeiltasten nach oben und unten auf Ihrer Tastatur können Sie durch den Verlauf navigieren. Wenn Sie den gesuchten Befehl gefunden haben, können Sie ihn erneut ausführen oder ändern, ohne den gesamten Befehl erneut eingeben zu müssen.

CLS / Bildschirm löschen

Der Befehl `CLS` löscht den Bildschirm. Der Befehl funktioniert genauso wie über die Windows-Eingabeaufforderung oder ähnliche Kommandozeilenprogramme.

EXIT / CLOSE / QUIT / BYE

Zum Schließen oder Beenden von eShell stehen Ihnen diese vier Befehle zur Verfügung (`EXIT`, `CLOSE`, `QUIT` oder `BYE`).

Befehle

Dieser Abschnitt enthält einige grundlegende eShell-Befehle mit einer Beschreibung.

> **i** Bei der Befehlseingabe müssen Sie nicht auf Groß- und Kleinschreibung achten. Der Befehl wird unabhängig davon ausgeführt, ob Sie Groß- oder Kleinbuchstaben verwenden.

Beispielbefehle (Befehle im Kontext `ROOT`):

ABOUT

Zeigt Programminformationen an. Hier finden Sie die folgenden Informationen:

- Name und Versionsnummer des installierten ESET-Sicherheitsprodukts.
- Betriebssystem und allgemeine Hardwareinformationen.
- Benutzername (inklusive Domäne), vollständiger Computername (FQDN, falls Ihr Server Mitglied einer Domäne ist) und Lizenzname.
- Installierte Komponenten Ihres ESET-Sicherheitsprodukts inklusive der Versionsnummern aller

Komponenten.

KONTEXTPFAD:

`root`

PASSWORT

Wenn Sie passwortgeschützte Befehle ausführen möchten, werden Sie aus Sicherheitsgründen in der Regel aufgefordert, ein Passwort einzugeben. Dies betrifft Befehle, die zum Beispiel die Deaktivierung des Schutzes zur Folge haben oder die Konfiguration von ESET Mail Security beeinflussen könnten. Jedes Mal, wenn ein solcher Befehl ausgeführt werden soll, muss das Passwort eingegeben werden. Sie können dieses Passwort definieren, um nicht jedes Mal ein Passwort eingeben zu müssen. eShell speichert das Passwort und gibt es automatisch ein, wenn ein passwortgeschützter Befehl ausgeführt wird.

Das festgelegte Passwort gilt nur für die aktuelle eShell-Sitzung im interaktiven Modus. Wenn Sie eShell beenden, wird das festgelegte Passwort gelöscht. Für die nächste Ausführung von eShell müssen Sie das Passwort erneut festlegen.

Das festgelegte Passwort kann auch für die Ausführung unsignierter Batchdateien oder Skripts verwendet werden. Legen Sie die ESET-Shell-Ausführungsrichtlinie auf Vollzugriff fest, wenn Sie unsignierte Batchdateien ausführen möchten. Hier ein Beispiel für eine solche Batch-Datei:

```
eshell set password plain <yourpassword> "&" computer set real-time status disabled
```

Dieser verkettete Befehl legt das Passwort fest und deaktiviert den Schutz.

Verwenden Sie nach Möglichkeit immer signierte Batchdateien. Auf diese Weise müssen Sie keine Klartextpasswörter in den Batchdateien verwenden (mit der oben beschriebenen Methode). Unter Batchdateien / Skripts (Abschnitt „Signierte Batchdateien“) finden Sie weitere Details.

KONTEXTPFAD:

`root`

SYNTAX:

```
[get] | restore password

set password [plain <password>]
```

VORGÄNGE:

`get` - Passwort anzeigen

`set` - Passwort speichern oder löschen

`restore` - Passwort löschen

ARGUMENTE:

`plain` – Passwort als Parameter eingeben

`password` - Passwort

`set password plain <yourpassword>` - Legt das Passwort für passwortgeschützte Befehle fest
`restore password` - Löscht das Passwort

`get password` - Mit diesem Befehl können Sie überprüfen, ob ein Passwort konfiguriert wurde. Es werden nur Sternchen `"*"` angezeigt, nicht das eigentliche Passwort. Wenn keine Sternchen sichtbar sind, dann wurde auch kein Passwort festgelegt
`set password plain <yourpassword>` - Festgelegtes Passwort speichern
`restore password` - Festgelegtes Passwort löschen

STATUS

Zeigt den aktuellen Echtzeit-Schutzstatus von ESET Mail Security an, und Sie können den Schutz anhalten oder fortsetzen (ähnlich wie im Programmfenster).

KONTEXTPFAD:

```
computer real-time
```

SYNTAX:

```
[get] status

set status enabled | disabled  [ 10m | 30m | 1h | 4h | temporary ]

restore status
```

VORGÄNGE:

`get` - Aktuelle Einstellung/Status zurückgeben

`set` - Wert/Status festlegen

`restore` - Standardeinstellungen/-objekt/-datei wiederherstellen

ARGUMENTE:

`enabled` - Schutz/Funktion aktivieren

`disabled` - Schutz/Funktion deaktivieren

`10m` - 10 Minuten lang deaktivieren

`30m` - 30 Minuten lang deaktivieren

`1h` - 1 Stunde lang deaktivieren

`4h` - 4 Stunden lang deaktivieren

`temporary` - Bis zum Neustart deaktivieren

Es ist nicht möglich, alle Schutzfunktionen mit einem einzigen Befehl zu deaktivieren. Mit dem Befehl `status` können Sie die Schutzfunktionen und Module einzeln verwalten. Jede Schutzfunktion und jedes Modul verwendet einen eigenen `status`-Befehl.

Liste der Funktionen mit `status`-Befehl:

Funktion	Kontext und Befehl
Automatische Ausschlüsse	`COMPUTER AUTO-EXCLUSIONS STATUS`
Host Intrusion Prevention System (HIPS)	`COMPUTER HIPS STATUS`
Echtzeit-Dateischutz	`COMPUTER REAL-TIME STATUS`
Gerätesteuerung	`DEVICE STATUS`
Botnetz-Schutz	`NETWORK ADVANCED STATUS-BOTNET`
Netzwerkangriffsschutz (IDS)	`NETWORK ADVANCED STATUS-IDS`
Netzwerkisolierung	`NETWORK ADVANCED STATUS-ISOLATION`
ESET-Cluster	`TOOLS CLUSTER STATUS`
Diagnose-Logging	`TOOLS DIAGNOSTICS STATUS`
Präsentationsmodus	`TOOLS PRESENTATION STATUS`
Phishing-Schutz	`WEB-AND-EMAIL ANTIPHISHING STATUS`
E-Mail-Client-Schutz	`WEB-AND-EMAIL MAIL-CLIENT STATUS`
Web-Schutz	`WEB-AND-EMAIL WEB-ACCESS STATUS`

VIRLOG

Alias für den Befehl `DETECTIONS`. Er eignet sich, wenn Sie sich Informationen zu erkannter eingedrungener Schadsoftware anzeigen lassen wollen.

WARNLOG

Alias für den Befehl `EVENTS`. Er eignet sich, wenn Sie sich Informationen zu verschiedenen Ereignissen anzeigen lassen wollen.

Tastaturbefehle

eShell unterstützt Tastaturbefehle (ähnlich wie die Microsoft Windows-Eingabeaufforderung *cmd.exe*). Verwenden Sie bestimmte Tasten oder Tastenkombinationen, um Aktionen in eShell auszuführen. Beispielsweise können Sie den Befehlsverlauf anzeigen, einen Teil des Befehlsverlaufs erneut ausführen, Wörter verschieben oder einzelne Zeilen löschen.

Verfügbare Tastenbefehle:

F1 – Gibt den aktuellen Verlaufsbefehl Zeichen um Zeichen aus.

F2, X – Wiederholt einen Teil des Verlaufsbefehls bis zum Zeichen X.

F3 – Aktuellen Verlaufsbefehl schreiben.

F4, X – Löscht die Zeichen von der aktuellen Cursorposition bis Zeichen X im aktuellen Befehl.

F5 – Gleiche Funktion wie PFEIL NACH OBEN.

F7 – Zeigt den Befehlsverlauf an.

ALT + F7 – Löscht den Befehlsverlauf.

F8 – Blättert rückwärts durch den Befehlsverlauf, zeigt aber nur Befehle an, die mit dem aktuellen Text in der

Eingabeaufforderung übereinstimmen.

F9 – Führt einen bestimmten Befehl aus dem Befehlsverlauf aus.

PFEIL NACH RECHTS – Gleiche Funktion wie F1.

STRG + POS1 – Löscht die Zeile links vom Cursor.

STRG + ENDE – Löscht die Zeile rechts vom Cursor.

STRG + PFEIL NACH LINKS – Bewegt den Cursor ein Wort nach links.

STRG + PFEIL NACH RECHTS – Bewegt den Cursor ein Wort nach rechts.

Batchdateien / Skripts

Sie können eShell als leistungsstarkes Skripting-Tool für die Automatisierung verwenden. Um eine Batch-Datei mit eShell zu verwenden, erstellen Sie eine Datei mit einem eShell-Befehl.

```
✔ eshell get computer real-time status
```

Sie können Befehle auch verketten. Geben Sie z. B. Folgendes ein, um den Typ eines bestimmten geplanten Tasks abzurufen:

```
eshell select scheduler task 4 "&" get scheduler action
```

Die Auswahl eines Elements (Task Nummer 4 in diesem Fall) bezieht sich nur auf eine aktuell laufende Instanz von eShell. Wenn Sie diese beiden Befehle nacheinander ausführen, schlägt der zweite Befehl mit der Fehlermeldung `""No task selected or selected task no longer exists""` fehl.

Aus Sicherheitsgründen ist die Ausführungsrichtlinie standardmäßig auf **Eingeschränktes Skripting** beschränkt. Mit dieser Einstellung können Sie eShell als Überwachungstool verwenden, jedoch keine skriptgesteuerten Konfigurationsänderungen an ESET Mail Security vornehmen. Wenn Sie ein Skript mit sicherheitsrelevanten Befehlen ausführen, z. B. zum Deaktivieren des Schutzes, erhalten Sie die Nachricht **Zugriff verweigert**. Verwenden Sie nach Möglichkeit signierte Batchdateien, um Befehle mit Konfigurationsänderungen auszuführen.

Um die Konfiguration mit einzelnen Befehlen in der Windows-Eingabeaufforderung zu ändern, müssen Sie eShell Vollzugriff gewähren (nicht empfohlen). Um den Vollzugriff zu gewähren, verwenden Sie den Befehl `ui eshell shell-execution-policy` im interaktiven Modus von eShell oder in der Benutzeroberfläche unter **Erweiterte Einstellungen** (**F5**)> **Benutzeroberfläche** > ESET-Shell.

Mit signierten Batchdateien

Mit eShell können Sie gewöhnliche Batchdateien (**.bat*) mit einer Signatur sichern. Skripts werden mit demselben Passwort signiert, das für den Schutz der Einstellungen verwendet wurde. Um ein Skript zu signieren, müssen Sie zunächst die Option Einstellungen schützen aktivieren. Entweder im Programmfenster oder in eShell mit dem Befehl `set ui access lock-password`. Sobald Sie das Passwort für den Schutz der Einstellungen eingerichtet haben, können Sie Batchdateien signieren.

Sie müssen alle Skripts erneut signieren, wenn Sie das Passwort für den Einstellungsschutz ändern. Andernfalls können die Skripts nach der Passwortänderung nicht mehr ausgeführt werden. Das beim Signieren der Skripte eingegebene Passwort muss mit dem Passwort für den Schutz der Einstellungen auf dem Zielsystem übereinstimmen.

Um eine Batchdatei zu signieren, führen Sie `sign <script.bat>`s im Stammkontext von eShell aus, wobei *script.bat* der Pfad zum Skript ist, das Sie signieren möchten. Geben Sie das Signierungspasswort ein und bestätigen Sie es. Dieses Passwort muss mit Ihrem Passwort für den Schutz der Einstellungen übereinstimmen. Die Signatur wird in Form eines Kommentars an das Ende der Batchdatei angehängt. Falls das Skript bereits signiert war, wird die vorhandene Signatur durch die neue Signatur ersetzt.

Wenn Sie eine zuvor signierte Batchdatei bearbeiten, müssen Sie diese anschließend erneut signieren.

Geben Sie den folgenden Befehl ein, um eine signierte Batchdatei in der Windows-Befehlszeile oder als geplanten Task auszuführen:

```
eshell run <script.bat>
```

script.bat ist in diesem Fall der Pfad zur Batchdatei.

```
eshell run d:\myeshellscript.bat
```

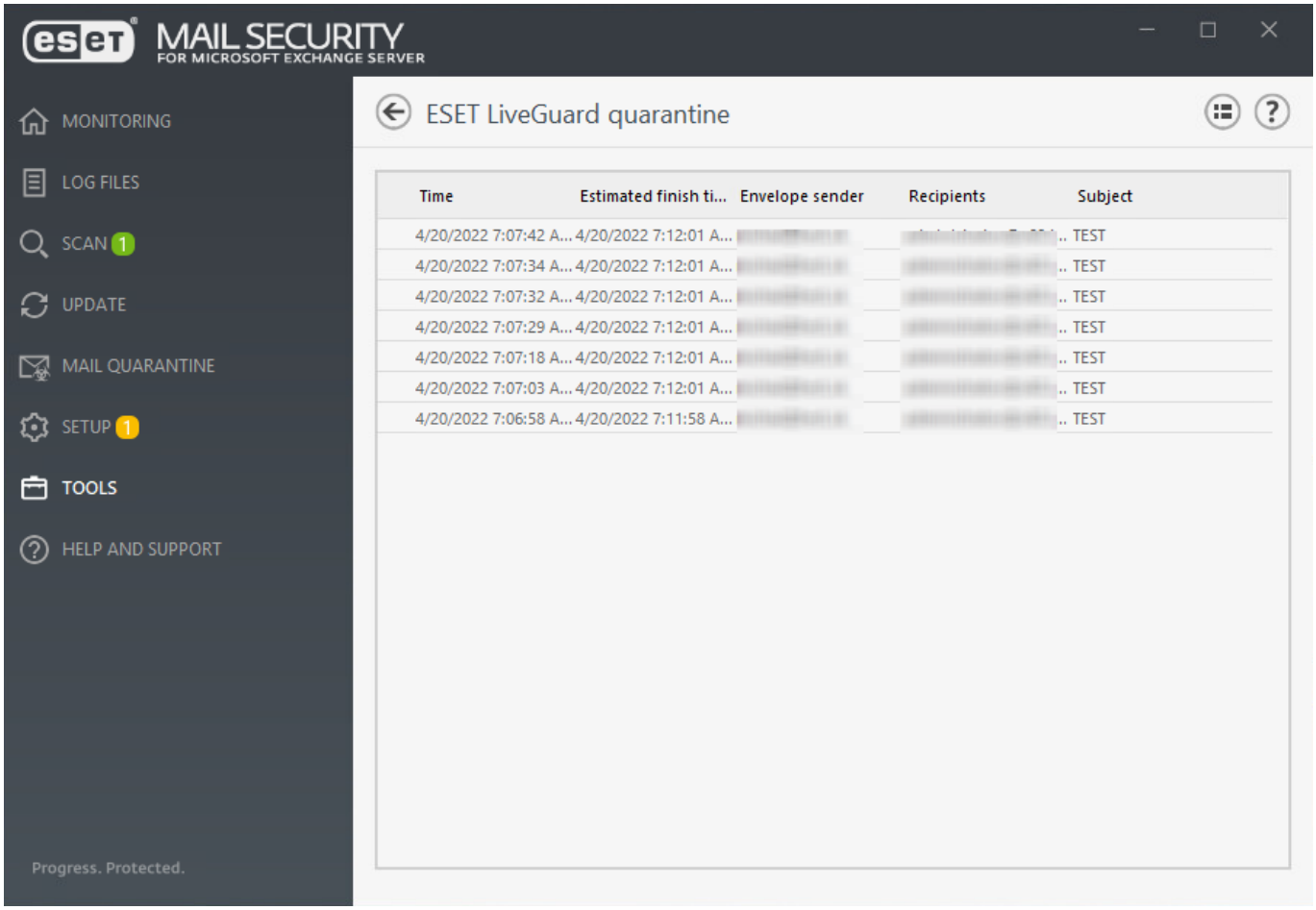
ESET LiveGuard Advanced

ESET LiveGuard Advanced verwendet cloudbasierte Technologien, um neue, noch nie aufgetretene Bedrohungsarten zu analysieren und zu erkennen, und um Ihnen eine zusätzliche Schutzebene zu bieten. Dieser zahlungspflichtige Dienst ähnelt zwar ESET LiveGrid®, aber ESET LiveGuard Advanced bietet Ihnen zusätzlichen Schutz vor möglichen Konsequenzen durch neue Bedrohungen. Wenn ESET LiveGuard Advanced verdächtigen Code oder verdächtige Verhaltensweisen entdeckt, wird die Bedrohung in die ESET LiveGuard Advanced-Quarantäne verschoben, um weitere Aktivitäten zu unterbinden.

Ein Sample (Datei oder E-Mail) wird automatisch an die ESET Cloud übermittelt und dort vom ESET LiveGuard Advanced Server mit modernsten Malware-Erkennungsmodulen analysiert. Die Dateien oder E-Mails befinden sich weiterhin in der ESET LiveGuard Advanced Quarantäne, und ESET Mail Security wartet auf die Ergebnisse vom ESET LiveGuard Advanced Server.

Nach Abschluss der Analyse erhält ESET Mail Security einen Zusammenfassungsbericht für das Verhalten des analysierten Samples. Falls die Probe harmlos ist, wird sie aus der ESET LiveGuard Advanced-Quarantäne freigegeben, andernfalls wird sie dort belassen. Falls es sich um ein falsch positives Ergebnis handelt und Sie sicher sind, dass die Datei oder E-Mail keine Bedrohung ist, können Sie sie manuell aus der ESET LiveGuard Advanced-Quarantäne freigeben, bevor ESET Mail Security die Ergebnisse vom ESET LiveGuard Advanced-Server erhält.

ESET LiveGuard Advanced übermittelt Ergebnisse der Samples für E-Mail-Nachrichten normalerweise innerhalb weniger Minuten. Das Standard-Warteintervall ist jedoch auf 5 Minuten festgelegt. In seltenen Fällen kann es vorkommen, dass die ESET LiveGuard Advanced-Ergebnisse nicht innerhalb des Intervalls ankommen und die Nachricht freigegeben wird. Sie können das Intervall nach Ihren Wünschen anpassen (5 bis 60 Minuten in Abständen von einer Minute).



Die ESET LiveGuard Advanced-Funktion ist in ESET Mail Security unabhängig von ihrem Aktivierungsstatus sichtbar. Falls Sie keine Lizenz haben, ist ESET LiveGuard Advanced inaktiv. Die ESET LiveGuard Advanced-Lizenz wird von ESET PROTECT verwaltet, und die Aktivierung muss aus ESET PROTECT mit einer Policy erfolgen.

Sobald Sie ESET LiveGuard Advanced aktiviert haben, wird Ihr eigenes ESET LiveGuard Advanced-Profil auf dem ESET LiveGuard Advanced-Server erstellt. In diesem Profil werden alle ESET LiveGuard Advanced-Analyseergebnisse für Proben gespeichert, die von Ihrem ESET Mail Security übermittelt wurden.

Für die ESET LiveGuard Advanced-Funktion gelten die folgenden Voraussetzungen:

ESET Mail Security verwaltung über ESET PROTECT

ESET Mail Security mit ESET LiveGuard Advanced-Lizenz aktiviert

ESET LiveGuard Advanced muss in Ihrem ESET Mail Security mit einer ESET PROTECT-Policy aktiviert werden

Anschließend können Sie den vollen Funktionsumfang von ESET LiveGuard Advanced nutzen und Probedateien manuell zur ESET LiveGuard Advanced-Analyse einreichen.

ESET SysInspector

ESET SysInspector ist eine Anwendung, die Ihren Computer gründlich durchsucht und eine genaue (Risikostufen-)Analyse Ihrer Systemkomponenten erstellt. Hierzu zählen u. a. installierte Treiber und Anwendungen, Netzwerkverbindungen oder wichtige Registrierungseinträge.

Diese Informationen helfen Ihnen beim Aufspüren der Ursache für verdächtiges Systemverhalten, welches

möglicherweise durch Software- oder Hardwareinkompatibilität oder eine Infektion mit Schadcode hervorgerufen wurde.

Klicken Sie auf **Erstellen** und geben Sie einen kurzen **Kommentar** ein, der das zu erstellende Log beschreibt. Warten Sie, bis das ESET SysInspector-Log erstellt wurde (Status ist 'Erstellt'). Je nach Hardwarekonfiguration und Systemdaten kann die Log-Erstellung eine gewisse Zeit in Anspruch nehmen.

Das ESET SysInspector-Fenster zeigt folgende Informationen zu erstellten Logs an:

- **Zeit** - Zeitpunkt der Log-Erstellung.
- **Kommentar** - Eine kurze Beschreibung.
- **Benutzer** - Der Name des Benutzers, der das Log erstellt hat.
- **Status** - Status bei der Log-Erstellung.

Folgende Aktionen stehen zur Verfügung:

- **Anzeigen** - Öffnet das erstellte Log. Sie können auch mit der rechten Maustaste auf eine Log-Datei klicken und im Kontextmenü die Option „**Anzeigen**“ auswählen.
- **Erstellen** - Erstellt ein neues Log. Geben Sie einen kurzen Kommentar zum neuen Log ein und klicken Sie auf **„Erstellen“**. Warten Sie, bis das ESET SysInspector-Log erstellt wurde (**Status** wird als „Erstellt“ angezeigt).
- **Löschen** - Entfernt die ausgewählten Logs aus der Liste.

Mit einem Rechtsklick auf ein oder mehrere ausgewählte Logs stehen im Kontextmenü die folgenden Optionen zur Verfügung:

- **Anzeigen** - Anzeige des ausgewählten Logs in ESET SysInspector (entspricht einem Doppelklick auf einen beliebigen Eintrag).
- **Erstellen** - Erstellt ein neues Log. Geben Sie einen kurzen Kommentar zum neuen Log ein und klicken Sie auf **„Erstellen“**. Warten Sie, bis das ESET SysInspector-Log erstellt wurde (**Status** wird als „Erstellt“ angezeigt).
- **Löschen** - Entfernt die ausgewählten Logs aus der Liste.
- **Alle löschen** - Löschen aller Logs.
- **Exportieren** – Exportiert das Log als *.esil*-Datei. Alternativ können Sie eine *.xml*-Datei oder eine gezippte *.xml*-Datei auswählen.

ESET SysRescue Live

ESET SysRescue Live ist ein kostenloses Hilfsprogramm, mit dem Sie ein bootfähiges Rettungsmedium (CD/DVD oder USB-Laufwerk) erstellen können. Anschließend können Sie einen infizierten Computer mit diesem Medium starten, nach Malware scannen und infizierte Dateien säubern.

ESET SysRescue Live Bietet den wichtigen Vorteil, dass die ESET Security-Lösungen unabhängig vom Host-

Betriebssystem ausgeführt werden, aber direkten Zugriff auf die Festplatte und das Dateisystem haben. Auf diese Weise lassen sich auch Bedrohungen entfernen, bei denen dies normalerweise (z. B. bei laufendem Betriebssystem) nicht möglich wäre.

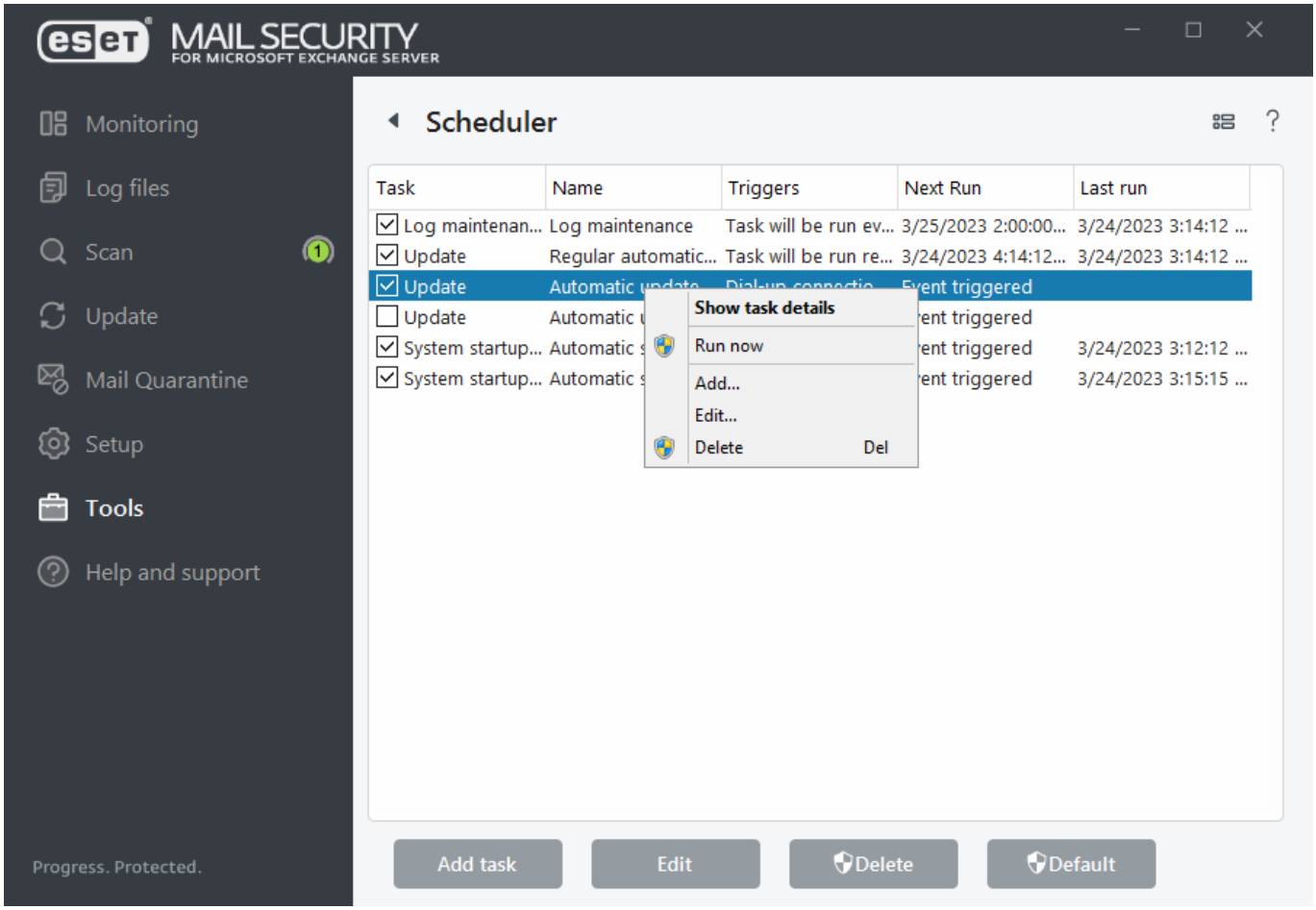
Taskplaner

Der Taskplaner verwaltet und startet geplante Tasks anhand definierter Parameter. Hier können Sie eine Liste aller geplanten Tasks als Tabelle mit Parametern wie Typ und Name des Tasks, Startzeit und Zeitpunkt der letzten Ausführung anzeigen. Sie können neue geplante Tasks erstellen, indem Sie auf Task hinzufügen klicken. Um die Konfiguration eines vorhandenen geplanten Tasks zu bearbeiten, klicken Sie auf die Schaltfläche **Bearbeiten**. Setzt die Liste der geplanten Tasks auf die **Standard** einstellungen zurück. Klicken Sie auf **„Rückgängig machen“**, um alle Änderungen zu verwerfen. Dieser Schritt kann nicht rückgängig gemacht werden.

Es gibt einen Satz vordefinierter Standard-Tasks:

- Log-Wartung
- Automatische Updates in festen Zeitabständen (dieser Task legt die Updatehäufigkeit fest)
- Automatische Updates beim Herstellen von DFÜ-Verbindungen
- Automatische Updates beim Anmelden des Benutzers
- Prüfung Systemstartdateien (nach Benutzeranmeldung)
- Prüfung Systemstartdateien (nach erfolgreichem Modul-Update)

> Wählen Sie die entsprechenden Kontrollkästchen aus, um Tasks zu aktivieren oder zu deaktivieren.



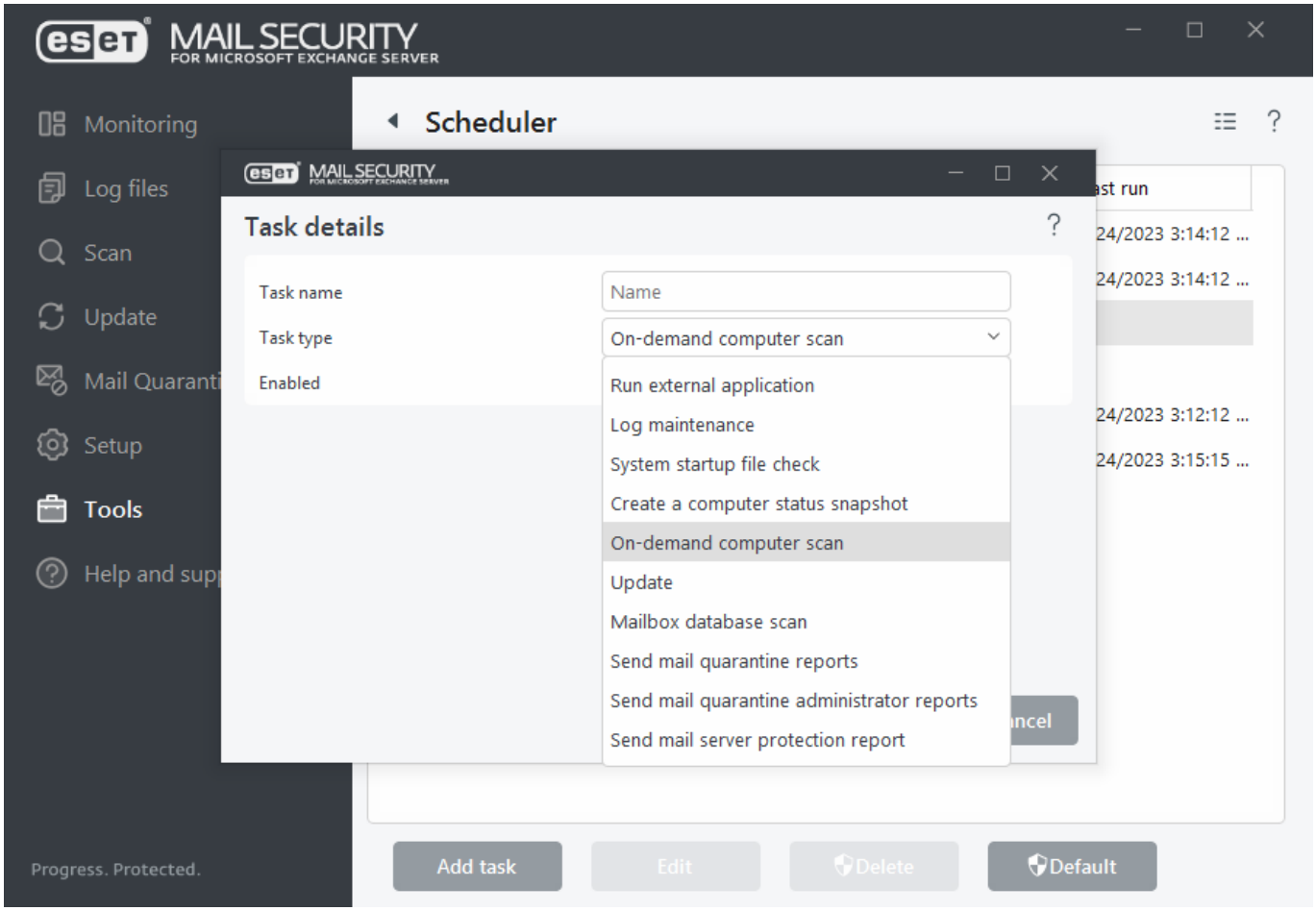
Klicken Sie mit der rechten Maustaste auf einen Task, um eine der folgenden Aktionen auszuführen:

Task-Eigenschaften anzeigen	Zeigt detaillierte Informationen zum geplanten Task an, wenn Sie auf einen Task doppelklicken oder mit der rechten Maustaste klicken.
Jetzt ausführen	Führt den ausgewählten geplanten Task sofort aus.
Hinzufügen...	Startet einen Assistenten, mit dem Sie einen neuen geplanten Task erstellen können.
Bearbeiten...	Bearbeiten Sie einen vorhandenen geplanten Task (Standardtasks und benutzerdefinierte Tasks).
Löschen	Löschen Sie einen vorhandenen Task.

Taskplaner - Task hinzufügen

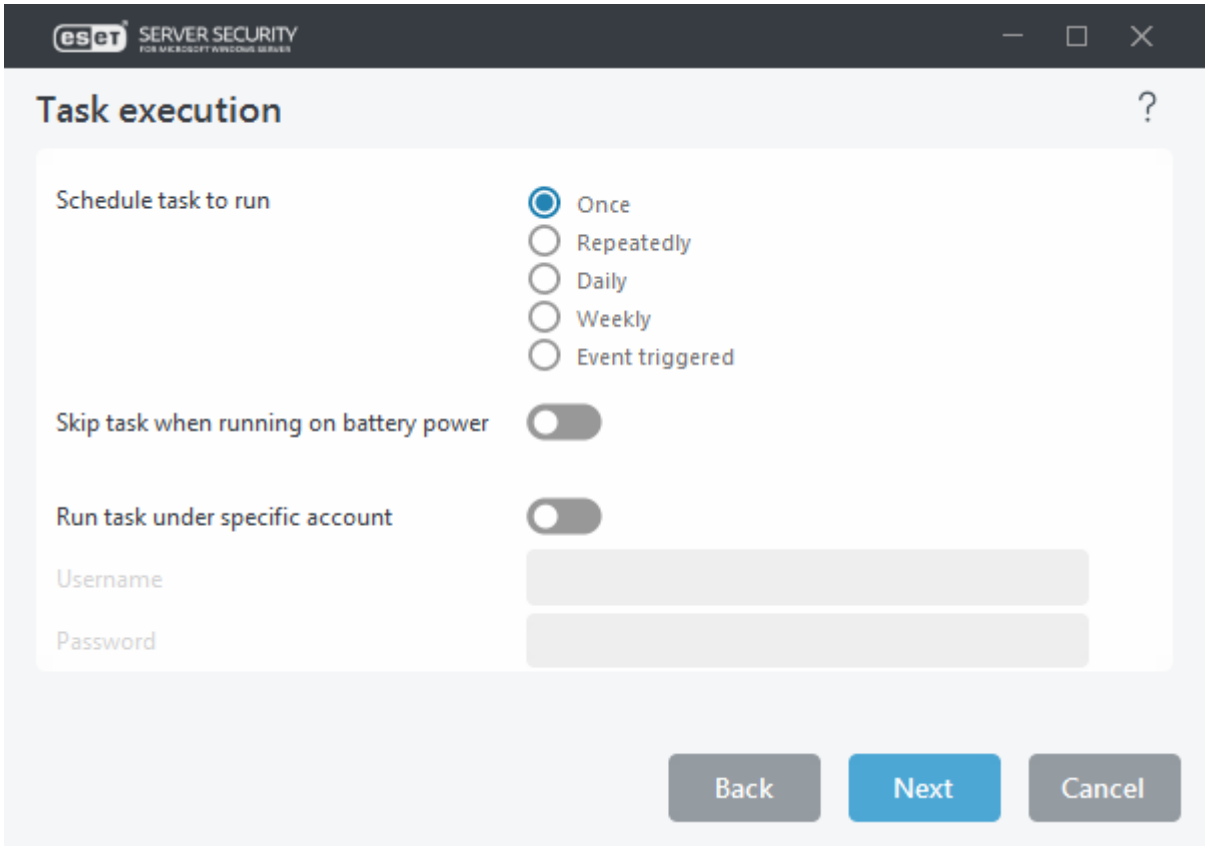
So erstellen Sie einen neuen geplanten Task:

1. Klicken Sie auf **Task hinzufügen**.
2. Geben Sie einen **Tasknamen** ein und konfigurieren Sie Ihren benutzerdefinierten geplanten Task.
3. Tasktyp – Wählen Sie den passenden **Tasktyp** im Dropdownmenü aus.

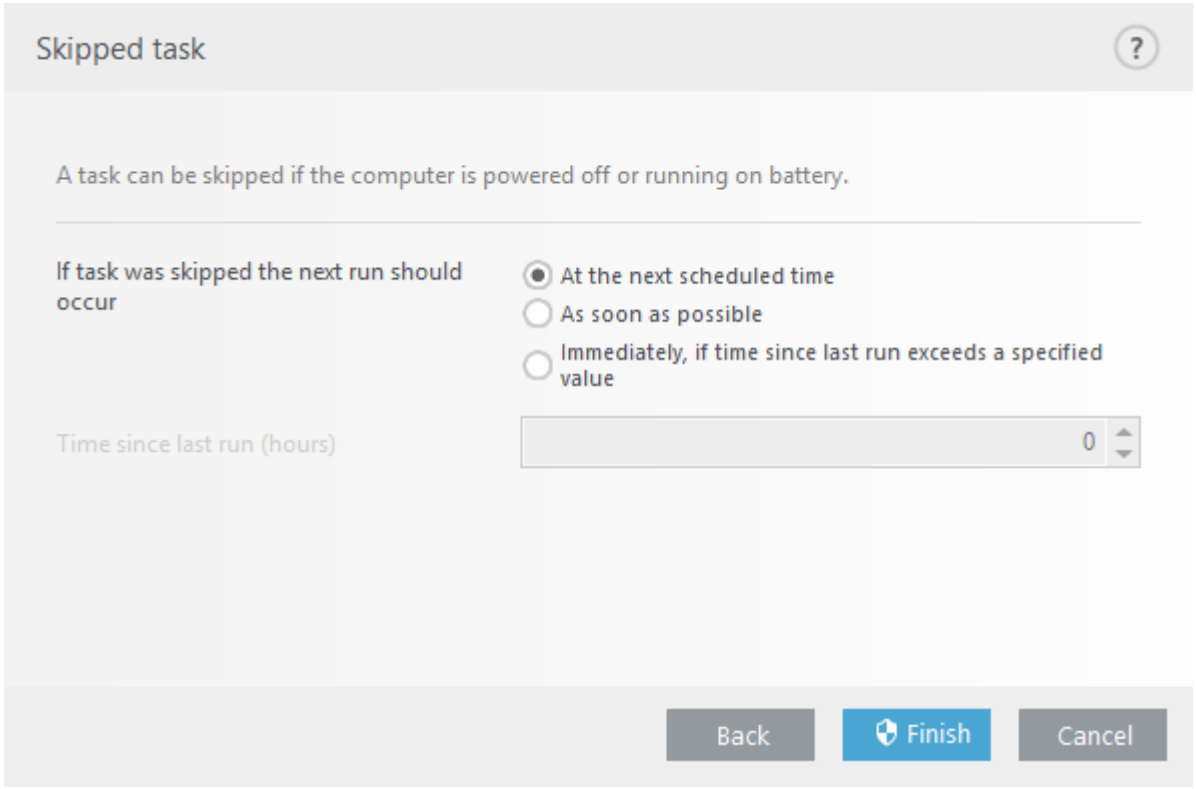


Klicken Sie auf den Schalter neben **Aktiviert**, um den Task zu deaktivieren. Sie können den Task später über das Kontrollkästchen in der Ansicht Taskplaner erneut aktivieren.

4. Taskausführung - Wählen Sie eine der Optionen aus, um festzulegen, wann Uhr Task ausgeführt werden soll. Je nach Ihrer Auswahl müssen Sie eine Uhrzeit, einen Tag, ein Intervall oder ein Ereignis auswählen.



5. Übersprungener Task - Wenn der Task nicht zur festgelegten Zeit ausgeführt werden konnte, können Sie einen Zeitpunkt für die nächste Ausführung angeben.



6. Anwendung starten - Wählen Sie eine ausführbare Datei in der Verzeichnisstruktur aus, falls der Task eine externe Anwendung ausführen soll.

7. Falls Sie Änderungen vornehmen möchten, klicken Sie auf **Zurück**, um zu den vorherigen Schritten zurückzukehren und die Parameter zu ändern.

8. Klicken Sie auf **Fertig stellen**, um den Task zu erstellen oder die Änderungen zu übernehmen.

Der neu erstellte Task in der Ansicht Taskplaner angezeigt.

Tasktyp

Dieser Konfigurationsassistent hängt vom jeweiligen Typ eines geplanten Tasks ab. Geben Sie den **Tasknamen** ein und wählen Sie den gewünschten **Tasktyp** im Dropdownmenü aus:

- **Externe Anwendung ausführen** - Planen der Ausführung einer externen Anwendung. Sie können den geplanten Task mit einem bestimmten Benutzerkonto ausführen (Option Task mit bestimmtem Konto ausführen).

- **Log-Wartung** - Log-Dateien enthalten auch unbenutzte leere Einträge von gelöschten Datensätzen. Dieser Task optimiert regelmäßig die Einträge in Log-Dateien.

- **Prüfung der Systemstartdateien** - Prüft Dateien, die beim Systemstart oder bei der Anmeldung ausgeführt werden.

- **Snapshot des Computerstatus erstellen** - Erstellt einen ESET SysInspector-Snapshot und eine genaue Risikostufen-Analyse Ihrer Systemkomponenten (z. B. Treiber und Anwendungen).

- **On-Demand-Computer-Scan** – Scannt Dateien und Ordner in lokalen Speichermedien oder in Netzwerkfreigaben (freigegebene Datenträger, wie etwa NAS). Führen Sie den geplanten Task mit einem bestimmten Benutzerkonto aus (Option Task mit bestimmtem Konto ausführen).

- **Update** - Erstellt einen Update-Task, um die Erkennungsroutine und die Programmmodule zu aktualisieren.

- **Postfachdatenbank-Scan** – Mit dieser Option können Sie einen Datenbankscan planen und die zu scannenden Elemente auswählen. Diese Funktion entspricht einem On-Demand-Datenbankscan.

> Wenn Sie die Funktion Postfach-Datenbankschutz aktiviert haben, können Sie diesen Task zwar planen, erhalten jedoch einen Fehler im Bereich Scan in der Hauptbenutzeroberfläche mit der Meldung „Postfachdatenbank-Scan – Scan aufgrund eines Fehlers unterbrochen“. Vergewissern Sie sich, dass der Postfach-Datenbankschutz während des Postfatenbank-Scans deaktiviert ist, um diesen Fehler zu vermeiden.

- **Quarantäneberichte per E-Mail senden** - Mit diesem Task wird ein Bericht zur E-Mail-Quarantäne per E-Mail verschickt.

- **Quarantäne-Administratorberichte per E-Mail senden** - Mit diesem Task wird ein Bericht zur E-Mail-Quarantäne per E-Mail verschickt.

- **Hintergrundprüfung** - Diese Option ermöglicht dem Exchange-Server bei Bedarf die Durchführung von Datenbankprüfungen im Hintergrund.

- **Hyper-V-Scan** - Plant eine Steuerung der virtuellen Datenträger in Hyper-V.

- **Office 365-Scan** – Plant einen Scan für Office 365-Hybridumgebungen.

Klicken Sie auf den Schalter neben **Aktiviert**, um den Task nach der Erstellung zu deaktivieren. Sie können den

Task später über das Kontrollkästchen in der Ansicht Taskplaner erneut aktivieren. Klicken Sie auf **Weiter**, um mit dem nächsten Schritt fortzufahren.

Taskausführung

Wählen Sie eine der folgenden Optionen für die Zeitplanung aus:

- **Einmalig** - Der Task wird nur einmalig zum angegebenen Zeitpunkt ausgeführt. Führt den Task einmalig zu einem bestimmten Zeitpunkt aus. Geben Sie Datum und Uhrzeit für die einmalige **Taskausführung** an.
- **Wiederholt** - Der Task wird in den (in Minuten) angegebenen Zeitabständen ausgeführt. Geben Sie unter **Taskausführung** an, zu welcher Uhrzeit der Task jeden Tag ausgeführt werden soll.
- **Täglich** - Der Task wird jeden Tag zur festgelegten Uhrzeit ausgeführt.
- **Wöchentlich** - Der Task wird an einem oder mehreren Wochentagen zur festgelegten Uhrzeit ausgeführt. Geben Sie die Startzeit unter „Uhrzeit Taskausführung“ ein. Geben Sie die Startzeit unter „Uhrzeit Taskausführung“ an. Wählen Sie einen oder mehrere Wochentage aus, an denen der Task ausgeführt werden soll.
- Bei Ereignis - Der Task wird ausgeführt, wenn ein bestimmtes Ereignis eintritt.

Wenn Sie die Option **Task im Akkubetrieb überspringen** aktivieren, wird der Task nicht gestartet, wenn sich der Computer zum geplanten Startzeitpunkt im Akkubetrieb befindet. Zum Beispiel für Computer, die an eine USV (unterbrechungsfreie Stromversorgung) angeschlossen sind.

Task mit bestimmtem Konto ausführen – Geben Sie Benutzername und Passwort für ein Konto an, um den geplanten Task **Externe Anwendung ausführen** oder **On-Demand-Computer-Scan** auszuführen. Mit dieser Option können Sie **On-Demand-Computer-Scans** in Netzwerkfreigaben ausführen, etwa in einem NAS oder einem anderen freigegebenen Speichertyp.

> Stellen Sie sicher, dass das unter **Task mit bestimmtem Konto ausführen** angegebene Benutzerkonto die Berechtigung **Anmelden als Stapelverarbeitungsauftrag** (SeBatchLogonRight) hat. Sie können die Richtlinieneinstellungen im Gruppenrichtlinienverwaltungs-Editor (Sicherheitseinstellungen > Lokale Richtlinien > Zuweisen von Benutzerrechten > Anmelden als Stapelverarbeitungsauftrag) anpassen.

Durch Ereignis ausgelöst

Beim Planen eines Vorgangs, der durch ein Ereignis ausgelöst wird, können Sie einen Mindestzeitraum zwischen Ausführungen des Tasks angeben.

Der Task wird durch eines der folgenden Ereignisse ausgelöst:

- Bei jedem Computerstart
- Jeden Tag beim ersten Start des Computers
- Wählverbindung zum Internet/VPN
- Erfolgreiches Modulupdate

- Erfolgreiches Produktupdate

- Benutzeranmeldung - Der Task wird bereitgestellt, wenn sich der Benutzer beim System anmeldet. Wenn Sie sich mehrmals täglich bei Ihrem Computer anmelden, können Sie „24 Stunden“ auswählen, um den Task nur bei der ersten Anmeldung des Tages und dann erst wieder am nächsten Tag auszuführen.

- Erkennung von Bedrohungen

Anwendung starten

Mit diesem Task können Sie die Ausführung einer externen Anwendung planen.

- **Ausführbare Datei** - Wählen Sie eine ausführbare Datei aus dem Verzeichnis, klicken Sie auf die Option Durchsuchen (...) oder geben Sie den Pfad manuell ein.

- **Arbeitsverzeichnis** - Legen Sie das Arbeitsverzeichnis der externen Anwendung fest. Alle temporären Dateien der gewählten Ausführbaren Datei werden in diesem Verzeichnis gespeichert.

- **Parameter** - Befehlszeilenparameter für die Anwendung (optional).

Übersprungener Task

Wenn der Vorgang nicht zur festgelegten Zeit ausgeführt werden konnte, können Sie einen Zeitpunkt für die Ausführung angeben:

- **Zur nächsten geplanten Ausführungszeit** - Der Task wird zum festgelegten Zeitpunkt (z. B. nach 24 Stunden) ausgeführt.

- **Baldmöglichst** - Der Task wird baldmöglichst ausgeführt, d. h. wenn die Aktionen, die seine Ausführung ursprünglich verhindert haben, nicht mehr wirksam sind.

- **Sofort ausführen, wenn Intervall seit letzter Ausführung überschritten** – Zeit seit letzter Ausführung (Stunden). Wenn Sie diese Option aktivieren, wird der Task immer wieder nach Ablauf einer festgelegten Zeitspanne (in Stunden) ausgeführt.

Übersicht über geplante Tasks

In diesem Dialogfenster werden detaillierte Informationen zum geplanten Task angezeigt, wenn Sie in der Ansicht **Taskplaner** auf einen Task doppelklicken oder mit der rechten Maustaste auf einen geplanten Task klicken und anschließend **Taskdetails anzeigen** auswählen.

Datei zur Analyse einreichen

Im Dialogfenster zum Einreichen von Samples können Sie Dateien zur Analyse an ESET übermitteln. Wenn Ihnen eine Datei auf Ihrem Computer oder eine Webseite verdächtig erscheint, können Sie die Datei zur Analyse an ESET senden. Wenn sich herausstellt, dass die Datei bzw. Webseite Schadcode enthält, werden entsprechende Erkennungsfunktionen in zukünftigen Updates berücksichtigt.

Um eine Datei per E-Mail einzusenden, komprimieren Sie sie mit einem Programm wie WinRAR oder WinZip, schützen Sie das Archiv mit dem Passwort `infected` und senden Sie es an samples@eset.com. Formulieren Sie eine aussagekräftige Betreffzeile, und notieren Sie möglichst viele ergänzende Informationen zu den eingesandten Dateien (z. B. von welcher Website Sie die Dateien heruntergeladen haben).

Die an ESET übermittelten Proben sollten mindestens eines der folgenden Kriterien erfüllen:
- Die Datei oder Website wird nicht als Bedrohung erkannt
- Die Datei oder Website wird als Bedrohung erkannt, obwohl sie keinen Schadcode enthält
- Wir akzeptieren keine persönlichen Dateien, die Sie gerne von ESET auf Malware gescannt haben möchten, als Samples. Das ESET Research Lab führt keine On-Demand-Scans für Benutzer durch.
- Formulieren Sie eine aussagekräftige Betreffzeile, und notieren Sie möglichst viele ergänzende Informationen zu den eingesandten Dateien (z. B. von welcher Website Sie die Dateien heruntergeladen haben).

Falls mindestens eine dieser Anforderungen nicht erfüllt ist, erhalten Sie erst eine Antwort, wenn weitere Informationen angegeben wurden.

Wählen Sie im Dropdownmenü **Grund für Einreichen der Probe** die Beschreibung aus, die am besten auf Ihre Mitteilung zutrifft:

- Verdächtige Datei
- Verdächtige Webseite (eine Webseite, die mit Schadsoftware infiziert ist)
- Fehlalarm Datei (als Infektion erkannte Datei, die jedoch nicht infiziert ist)
- Fehlalarm Webseite
- Sonstige

Site:

Der Pfad zu der Datei oder Webseite, die eingesandt werden soll.

E-Mail-Adresse für Rückfragen

Diese E-Mail-Adresse wird zusammen mit verdächtigen Dateien an ESET übermittelt. ESET kann über diese Adresse Kontakt mit Ihnen aufnehmen, wenn zusätzliche Angaben für die Dateianalyse benötigt werden. Diese Angabe ist freiwillig. Sie erhalten nur eine Antwort von ESET, falls wir weitere Informationen benötigen, da täglich mehrere Zehntausend Dateien auf unseren Servern eingehen und wir nicht jede Meldung einzeln beantworten können.

Anonym übermitteln

Verwenden Sie das Kontrollkästchen **Anonym übermitteln**, um verdächtige Dateien oder Websites ohne Angabe Ihrer E-Mail-Adresse zu übermitteln.

Verdächtige Datei

Beobachtete Anzeichen und Symptome einer Infektion durch Schadsoftware

Beschreiben Sie, wie sich die verdächtige Datei auf Ihrem Computer verhält.

Herkunft der Datei (URL oder Hersteller)

Geben Sie an, woher die Datei stammt (Quelle) und wie Sie sie entdeckt haben.

Hinweise und Zusatzangaben

Hier können Sie zusätzliche Informationen oder eine Beschreibung eingeben, um die Identifizierung der verdächtigen Datei zu erleichtern.

> Der erste Parameter **Beobachtete Anzeichen und Symptome einer Malware-Infektion** muss stets ausgefüllt werden, Zusatzangaben helfen dem Virenlabor jedoch erheblich bei der Identifizierung und Probenauswertung.

Verdächtige Webseite

Wählen Sie eine der folgenden Optionen im Dropdownmenü Was stimmt mit der Site nicht aus:

Infiziert

Eine Webseite, die Viren oder sonstige Schadsoftware enthält, die auf verschiedenen Wegen verbreitet werden.

Phishing

Wird oft eingesetzt, um Zugriff auf vertrauliche Daten wie Kontonummern oder PIN-Codes zu erlangen. Weitere Informationen zu dieser Angriffsart finden Sie im Glossar.

Betrug

Betrügerische Webseite.

Sonstige

Verwenden Sie diese Option, wenn keine der anderen Optionen auf die Website zutrifft.

Hinweise und Zusatzangaben

Hier können Sie zusätzliche Informationen oder eine Beschreibung eingeben, um die Analyse der verdächtigen Webseite zu erleichtern.

Fehlalarm Datei

Wenn eine Datei als Infektion erkannt wird, tatsächlich aber nicht infiziert ist, bitten wir Sie, diese Datei einzusenden, damit wir unseren Viren- und Spyware-Schutz für Sie und andere Benutzer verbessern können. Fehlerkennungen können auftreten, wenn eine Datei einem Muster entspricht, das in einer Erkennungsroutine gespeichert ist.

> Ersten drei Angaben sind notwendig, um legitime Anwendungen zu identifizieren und von Schadcode zu unterscheiden. Zusatzangaben helfen dem Virenlabor erheblich bei der Identifizierung einer Bedrohung und der Auswertung von Proben.

Name und Version der Anwendung

Bezeichnung und Version des Programms (z. B. Nummer, Aliasname oder Programmname).

Herkunft der Datei (URL oder Hersteller)

Bitte geben Sie an, woher die Datei stammt (Quelle) und wie Sie sie entdeckt haben.

Zweck der Anwendung

Eine allgemeine Beschreibung der Anwendung, die Art der Anwendung (z. B. Browser, Media-Player usw.) und ihre Funktion.

Hinweise und Zusatzangaben

Hier können Sie zusätzliche Informationen oder eine Beschreibung eingeben, die die Auswertung der verdächtigen Datei erleichtern.

Fehlalarm Webseite

Wir bitten Sie, Webseiten, die fälschlicherweise als infiziert, Betrug oder Phishing erkannt werden, einzusenden. Fehlerkennungen können auftreten, wenn eine Seite einem Muster entspricht, das in einer Erkennungsroutine gespeichert ist. Wenn Sie solche Webseiten einsenden, helfen Sie uns dabei, unseren Viren- und Spyware-Schutz für Sie und andere Benutzer zu verbessern.

Hinweise und Zusatzangaben

Hier können Sie zusätzliche Informationen oder eine Beschreibung eingeben, die die Auswertung der verdächtigen Datei erleichtern.

Sonstige

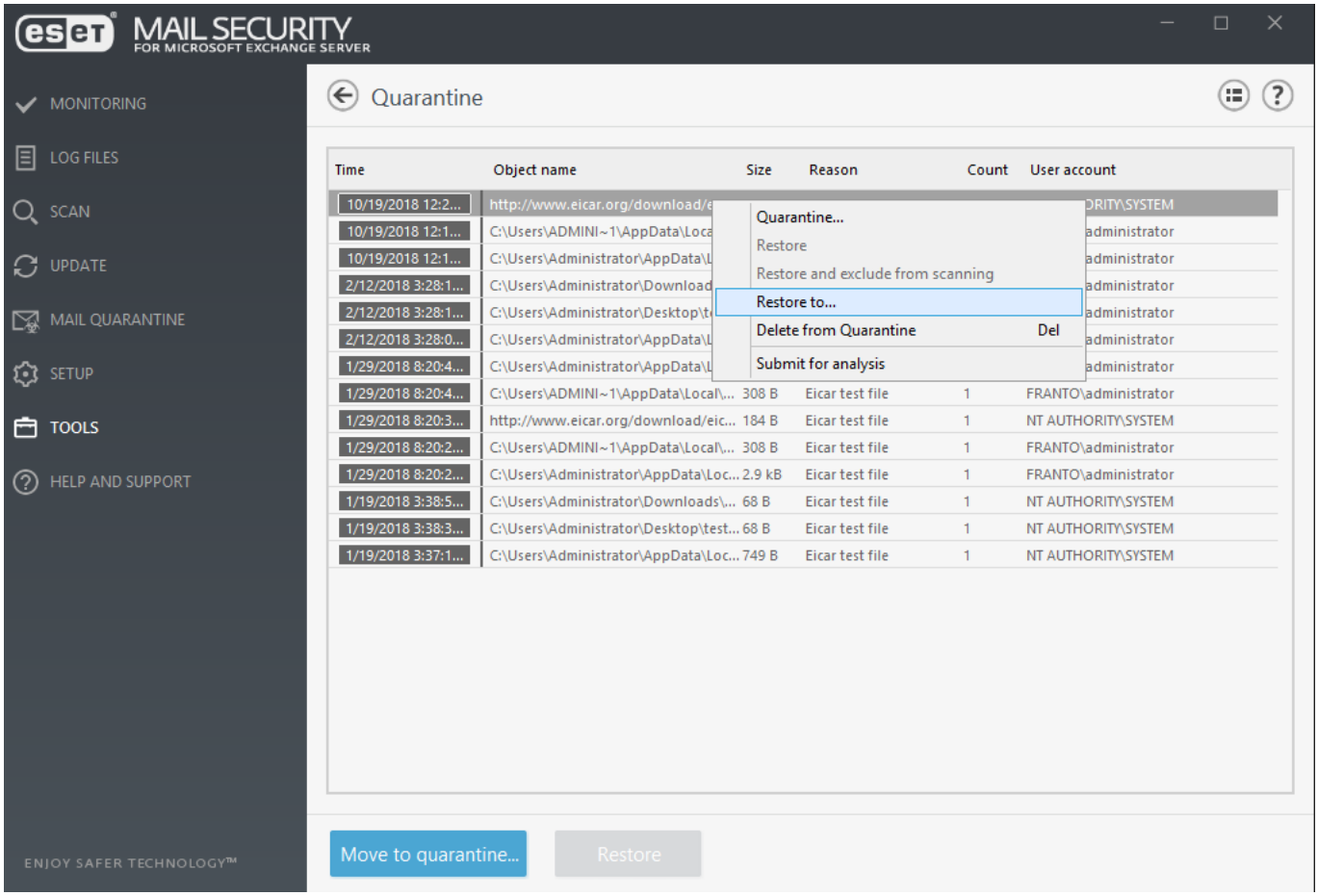
Verwenden Sie diese Auswahlmöglichkeit, wenn die Datei keine Verdächtige Datei und kein Fehlalarm ist.

Grund für Einreichen der Datei

Geben Sie eine genaue Beschreibung und den Grund für das Einreichen der Datei ein.

Quarantäne

Die Quarantäne dient hauptsächlich dazu, infizierte Dateien sicher aufzubewahren. Dateien sollten in die Quarantäne verschoben werden, wenn sie nicht gesäubert werden können, wenn es nicht sicher oder ratsam ist, sie zu löschen, oder wenn sie von ESET Mail Security fälschlicherweise erkannt wurden. Sie können beliebige Dateien gezielt in die Quarantäne verschieben. Dies macht Sinn für Dateien, die sich verdächtig verhalten, aber vom Malware-Scanner nicht erkannt werden. Dateien aus der Quarantäne können zur Analyse an ESET eingereicht werden.



Die Dateien im Quarantäneordner können in einer Tabelle angezeigt werden, die Datum und Uhrzeit der Quarantäne, den Pfad zum ursprünglichen Speicherort der infizierten Datei, ihre Größe in Byte, einen Grund (z. B. Objekt hinzugefügt durch Benutzer) und die Anzahl der Bedrohungen (z. B. bei Archiven, in denen an mehreren Stellen Schadcode erkannt wurde) enthält.

Wenn E-Mail-Nachrichtenobjekte in die Dateiquarantäne verschoben werden, wird ein Pfad zum Postfach/Ordner/Dateinamen angezeigt.

Quarantäne für Dateien

ESET Mail Security verschiebt gelöschte Dateien automatisch in den Quarantäneordner (sofern diese Option nicht im Warnfenster deaktiviert wurde). Klicken Sie auf **Quarantäne**, um eine verdächtige Datei manuell in die Quarantäne zu verschieben. In die Quarantäne verschobene Dateien werden von ihrem ursprünglichen Speicherort entfernt. Alternativ können Sie das Kontextmenü verwenden: Klicken Sie mit der rechten Maustaste in das Fenster **Quarantäne**, und wählen Sie **Quarantäne** aus.

Wiederherstellen aus Quarantäne

Dateien aus der Quarantäne können auch an ihrem ursprünglichen Speicherort wiederhergestellt werden. Verwenden Sie dazu die Funktion **Wiederherstellen** aus dem Kontextmenü, das Sie per Rechtsklick auf die entsprechende Datei im Fenster „Quarantäne“ aufrufen können. Wenn eine Datei als eventuell unerwünschte Anwendung gekennzeichnet ist, wird die Funktion **Wiederherstellen und von Prüfung ausschließen** verfügbar. Das Kontextmenü enthält außerdem die Option **Wiederherstellen nach**, mit der Dateien an einem anderen als ihrem ursprünglichen Speicherort wiederhergestellt werden können.

Wenn versehentlich eine harmlose Datei in die Quarantäne versetzt wurde, schließen Sie die Datei nach der Wiederherstellung vom Scan aus und senden Sie sie an den ESET-Support.

Einreichen einer Datei aus der Quarantäne

Wenn Sie eine verdächtige, nicht vom Programm erkannte Datei in Quarantäne versetzt haben oder wenn eine Datei fälschlich als infiziert eingestuft wurde (etwa durch die heuristische Analyse des Codes) und infolgedessen in den Quarantäneordner verschoben wurde, senden Sie die Datei zur Analyse an ESET. Um eine Datei zu senden, die in der Quarantäne gespeichert ist, klicken Sie mit der rechten Maustaste auf die Datei und wählen im angezeigten Kontextmenü die Option Datei zur Analyse einreichen.

Aus Quarantäne löschen

Klicken Sie mit der rechten Maustaste auf ein Element und wählen Sie **Zur Analyse einreichen** aus. Alternativ können Sie das zu löschende Element auswählen und die **Entf**-Taste auf der Tastatur drücken.

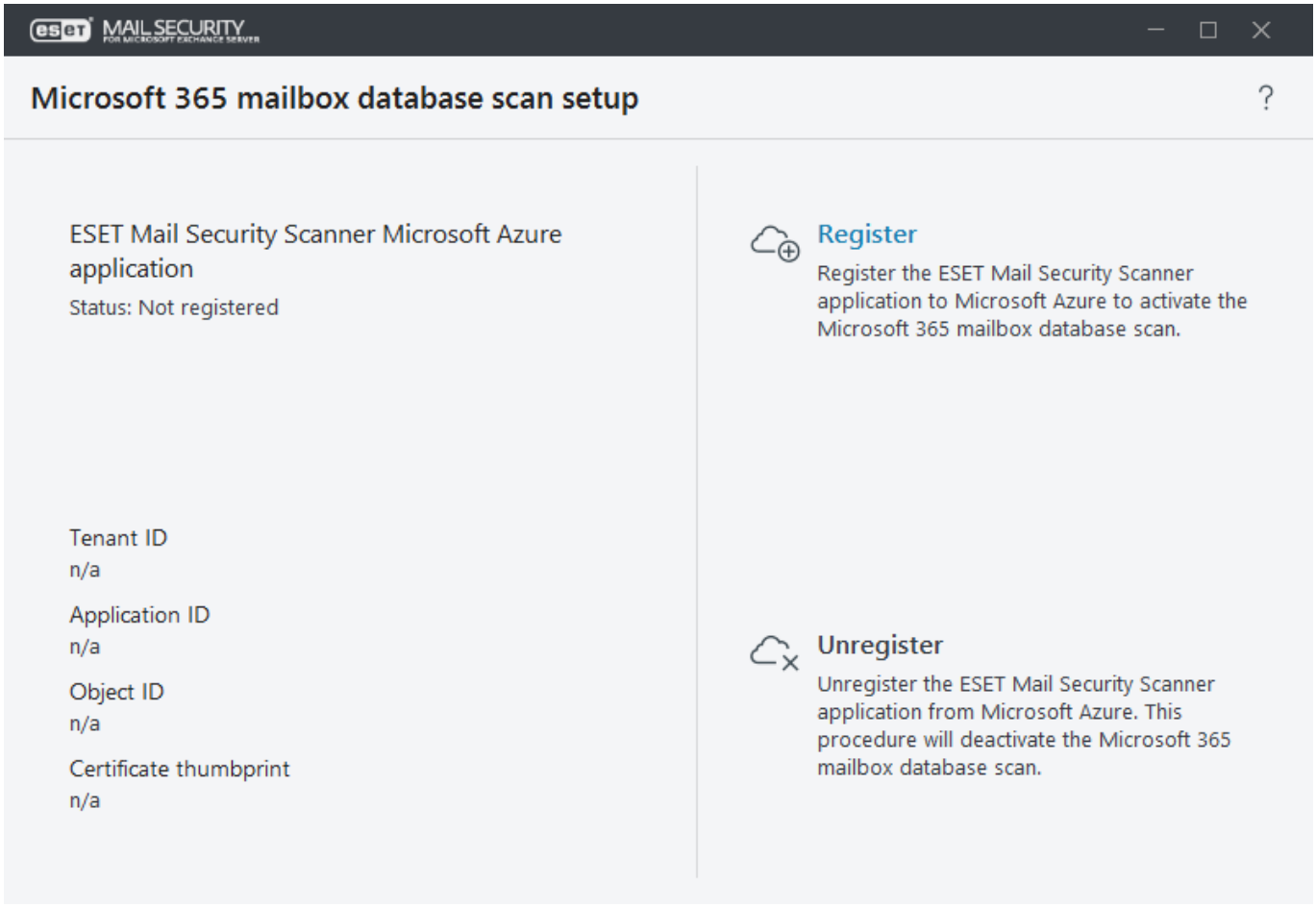
Assistent für Microsoft 365-Postfach-Scan

Mit ESET Mail Security können Sie Microsoft 365-Remotepostfächer und öffentliche Ordner wie mit einem gewöhnlichen On-Demand-Postfachdatenbank-Scan scannen. Registrieren Sie Ihren ESET Mail Security Scanner, um diese Funktion zu aktivieren.

Quick Links

- ESET Mail Security Scanner registrieren
- Registrierung des ESET Mail Security Scanners aufheben

Um Ihren ESET Mail Security Microsoft 365 Postfachdatenbank-Scan nutzen zu können, müssen Sie die ESET Mail Security Scanner-Anwendung in Microsoft Azure registrieren. Auf der Einrichtungsseite für den Microsoft 365-Postfach-Scan wird der Registrierungsstatus angezeigt. Falls Sie bereits registriert sind, werden Details (Mandanten-ID, Anwendungs-ID, Objekt-ID und Zertifikatfingerabdruck) angezeigt. Sie können Ihren ESET Mail Security Scanner registrieren oder die Registrierung aufheben:



Nach der erfolgreichen Registrierung wird der Microsoft 365-Postfachdatenbank-Scan im Menü Scannen angezeigt, zusammen mit einer Liste von Postfächern (und öffentlichen Ordnern), die zum Scannen ausgewählt werden können.

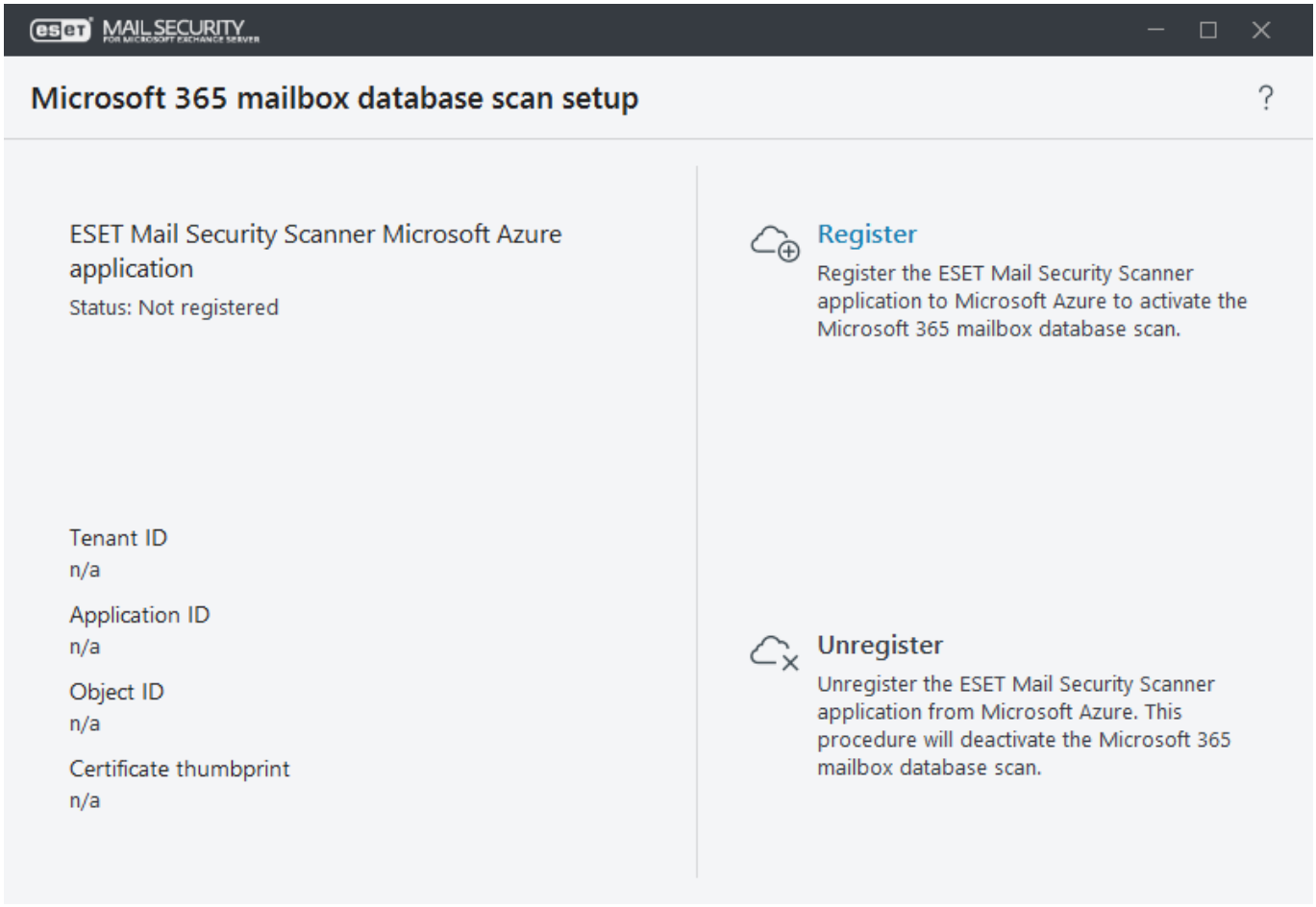
> Registrieren Sie sich mit einem anderen Konto erneut: Um den ESET Mail Security Scanner mit einem neuen Microsoft 365-Konto zu registrieren, müssen Sie zunächst die Registrierung des ESET Mail Security Scanner in Ihrem vorherigen Konto aufheben und die App anschließend im neuen Microsoft 365-Administratorkonto registrieren.

Sie finden Ihren ESET Mail Security Scanner als registrierte Anwendung in Microsoft Azure. Klicken Sie auf **Azure Active Directory** > **App-Registrierungen** und dann auf **Alle Anwendungen anzeigen**, um die ESET Mail Security Scanner-App in der Liste anzuzeigen. Klicken Sie auf die App, um weitere Details anzuzeigen.

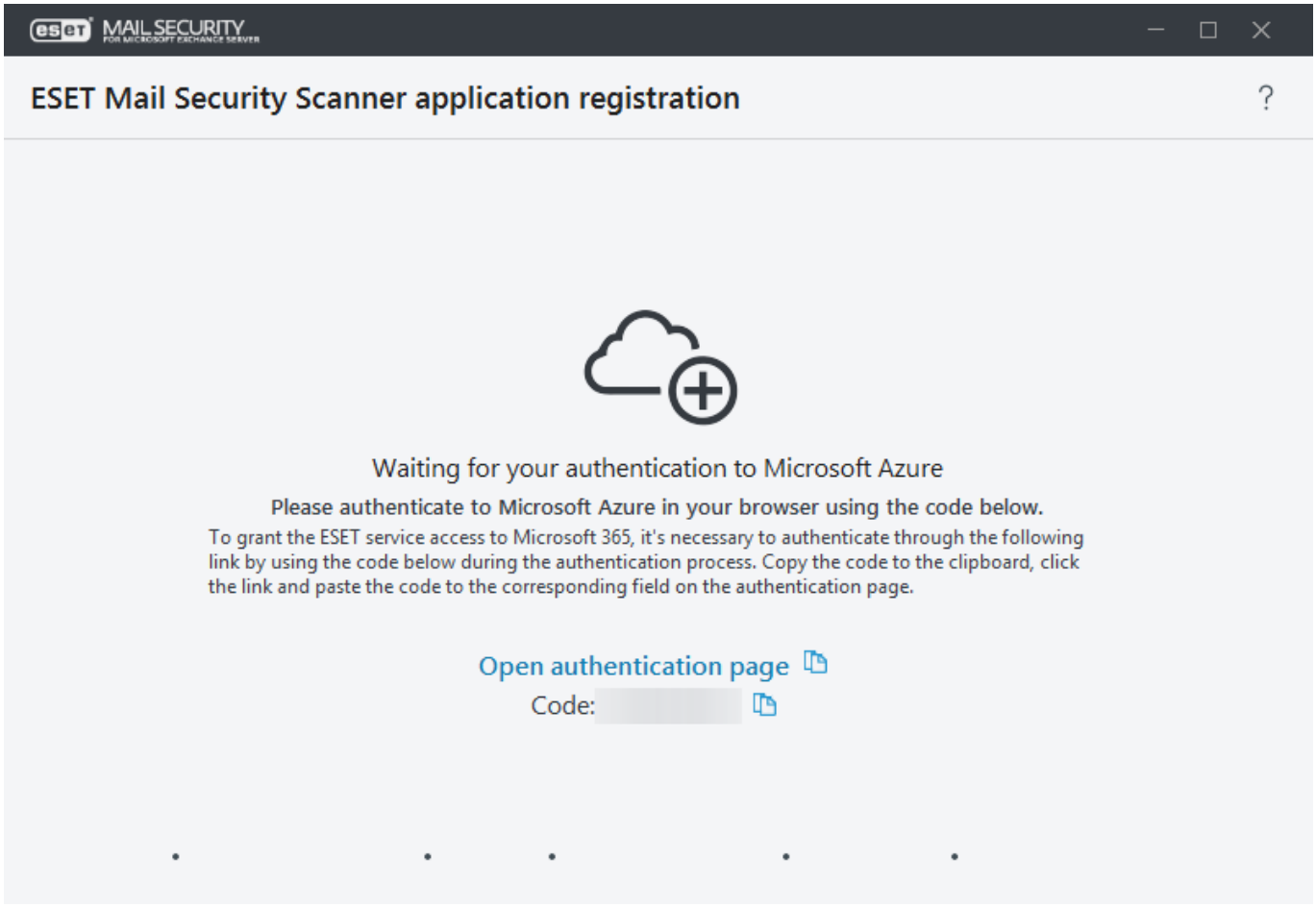
ESET Mail Security Scanner registrieren

Gehen Sie wie folgt vor, um die ESET Mail Security Scanner-App in Microsoft Azure registrieren, um den Microsoft 365-Postfachdatenbank-Scan zu aktivieren:

1. Klicken Sie auf **Registrieren**, um die Registrierung des ESET Mail Security Scanners zu starten. Daraufhin wird ein Registrierungsassistent geöffnet.

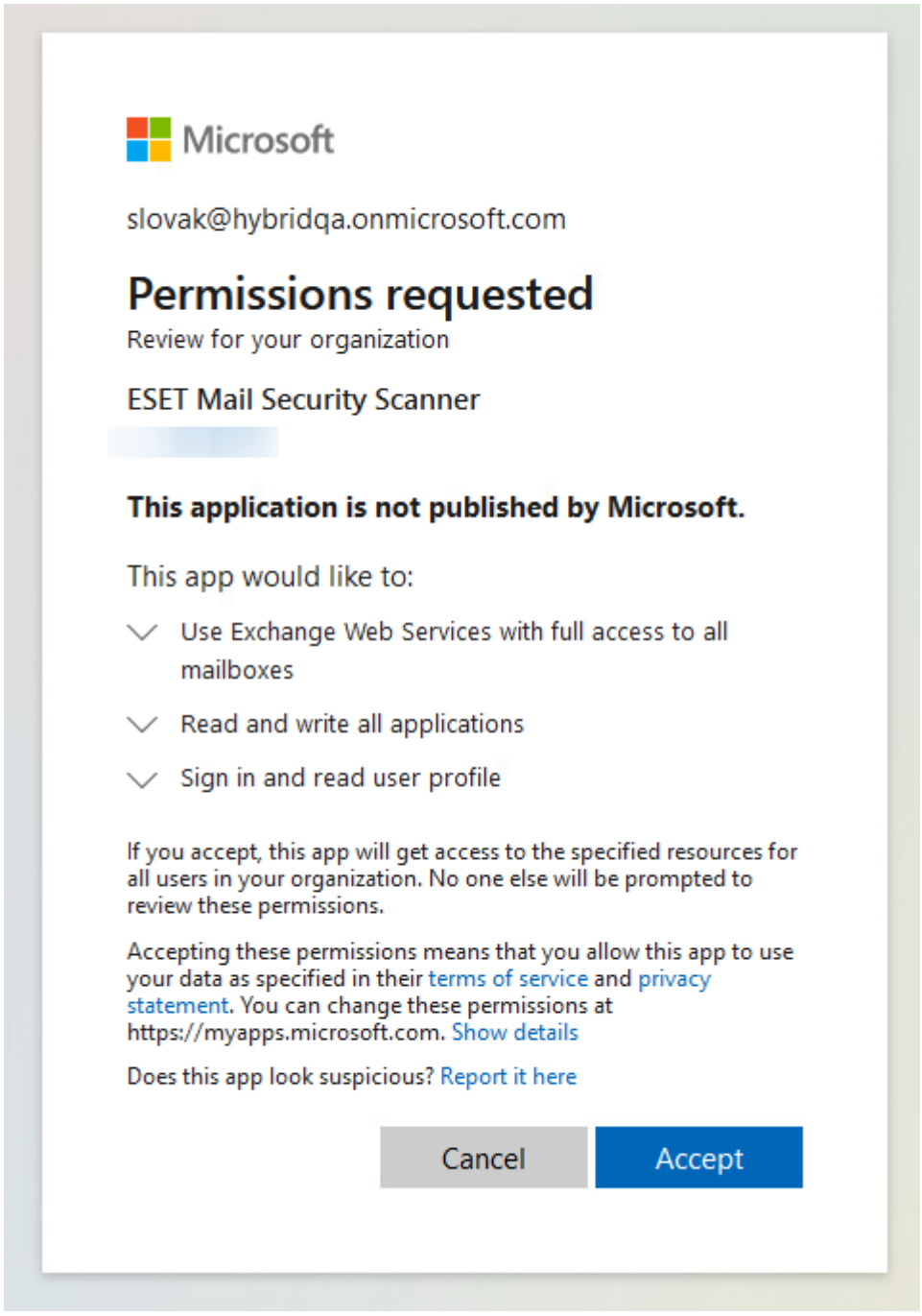


2. Kopieren Sie den angegebenen Code, klicken Sie auf **Authentifizierungsseite öffnen** und geben Sie den Code ein.

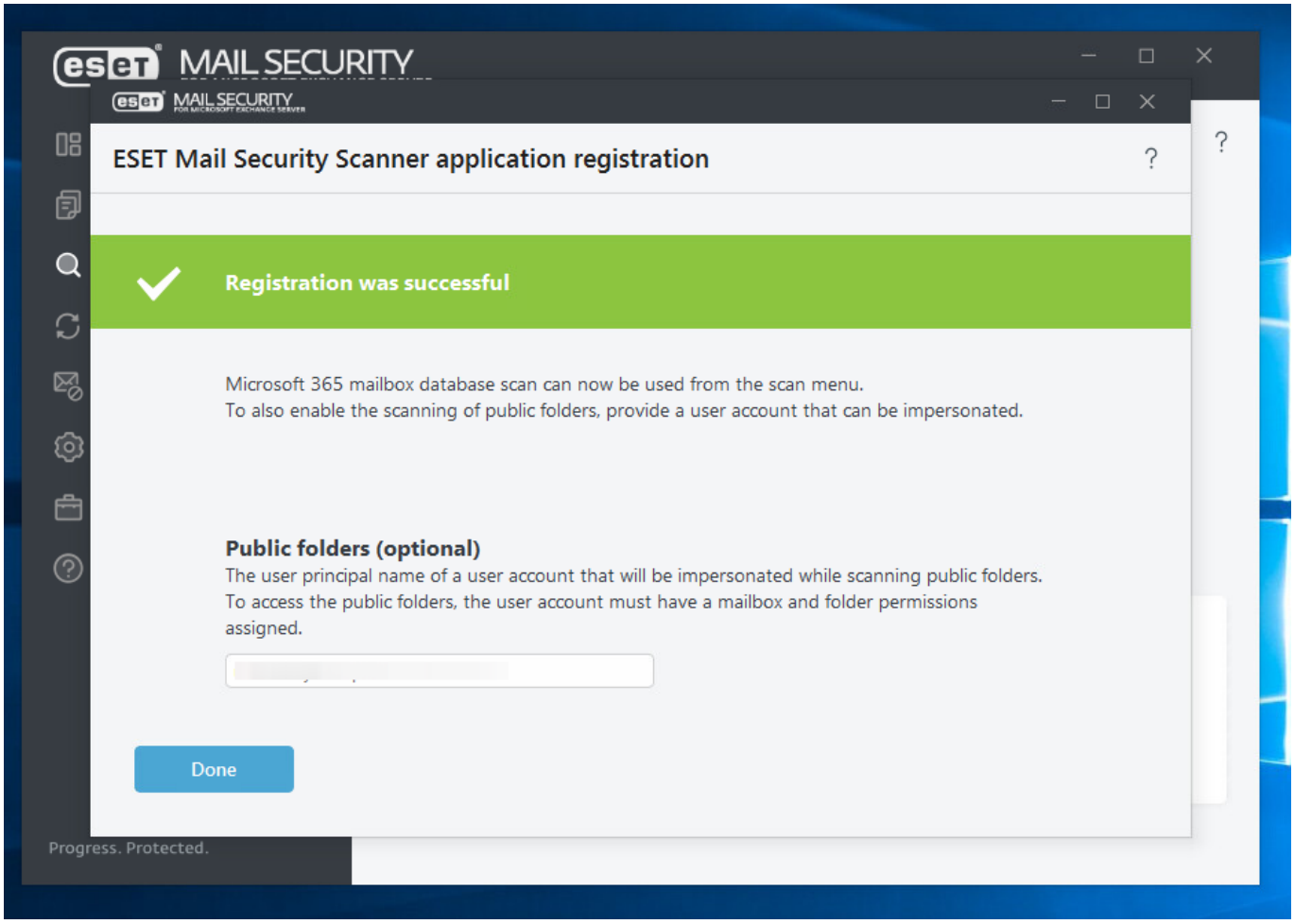


3. Daraufhin wird ein Webbrowser mit einer Microsoft-Seite geöffnet, in der Sie ein **Konto auswählen** können. Klicken Sie auf das aktuell verwendete Konto oder geben Sie die Anmeldeinformationen für Ihr Microsoft 365-Administratorkonto ein und klicken Sie auf **Anmelden**.

4. Die ESET Mail Security Scanner-App fragt in einer Bestätigungsmeldung nach drei verschiedenen Berechtigungen. Klicken Sie auf **Akzeptieren**, um dem ESET Mail Security Scanner den Zugriff auf Ihre Microsoft 365-Daten zu erlauben.



5. Schließen Sie den Webbrowser und warten Sie, bis die Registrierung des ESET Mail Security Scanners abgeschlossen wurde. Die Meldung **„Registrierung erfolgreich abgeschlossen“** wird angezeigt.



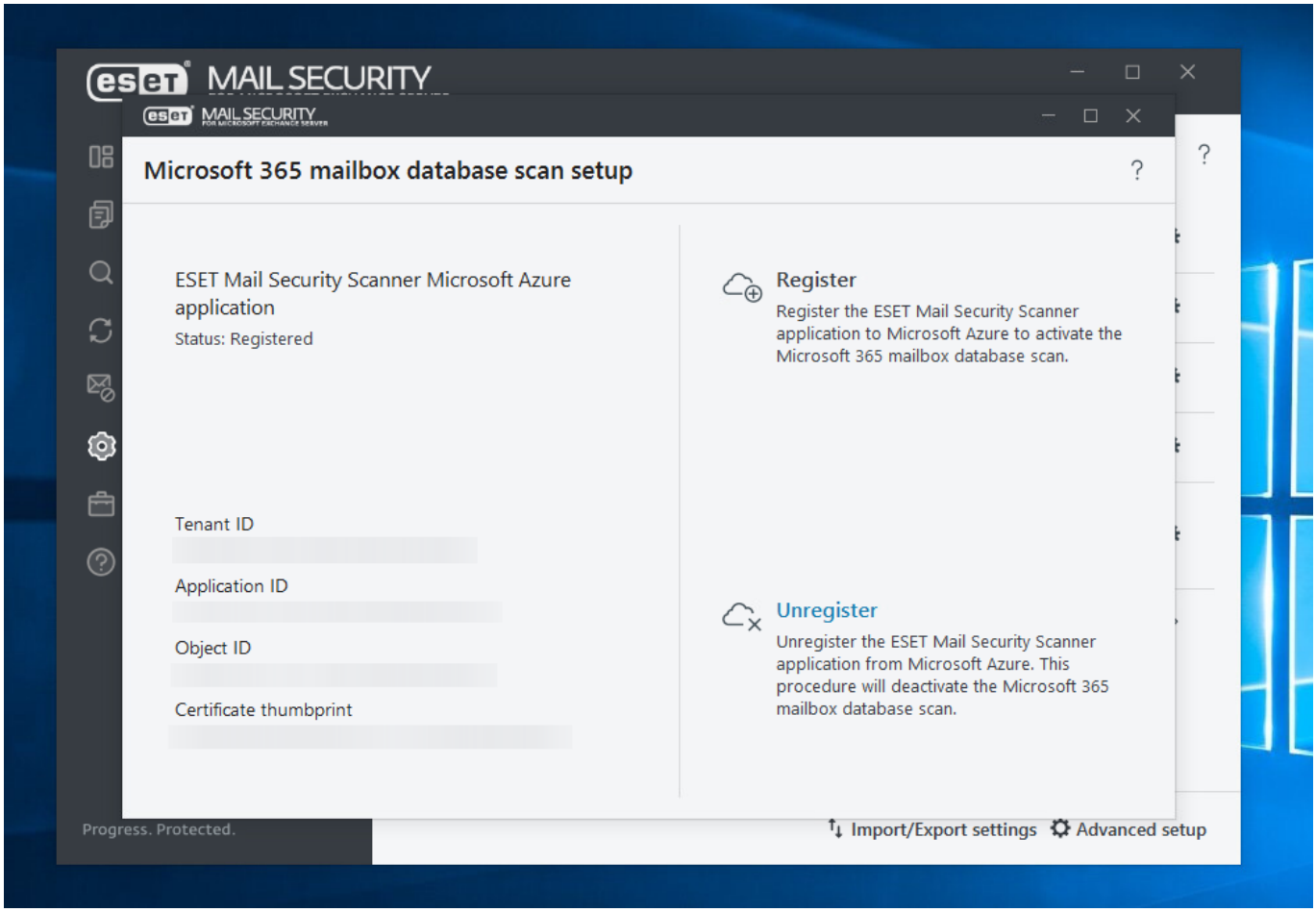
6. **Öffentliche Ordner (optional)**

Falls Sie öffentliche Ordner scannen möchten, geben Sie einen Namen für das Prinzipalbenutzerkonto für den Identitätswechsel ein (Passwort nicht erforderlich). Stellen Sie sicher, dass dieses Benutzerkonto auf alle öffentlichen Ordner zugreifen kann. Klicken Sie auf **Fertig**.

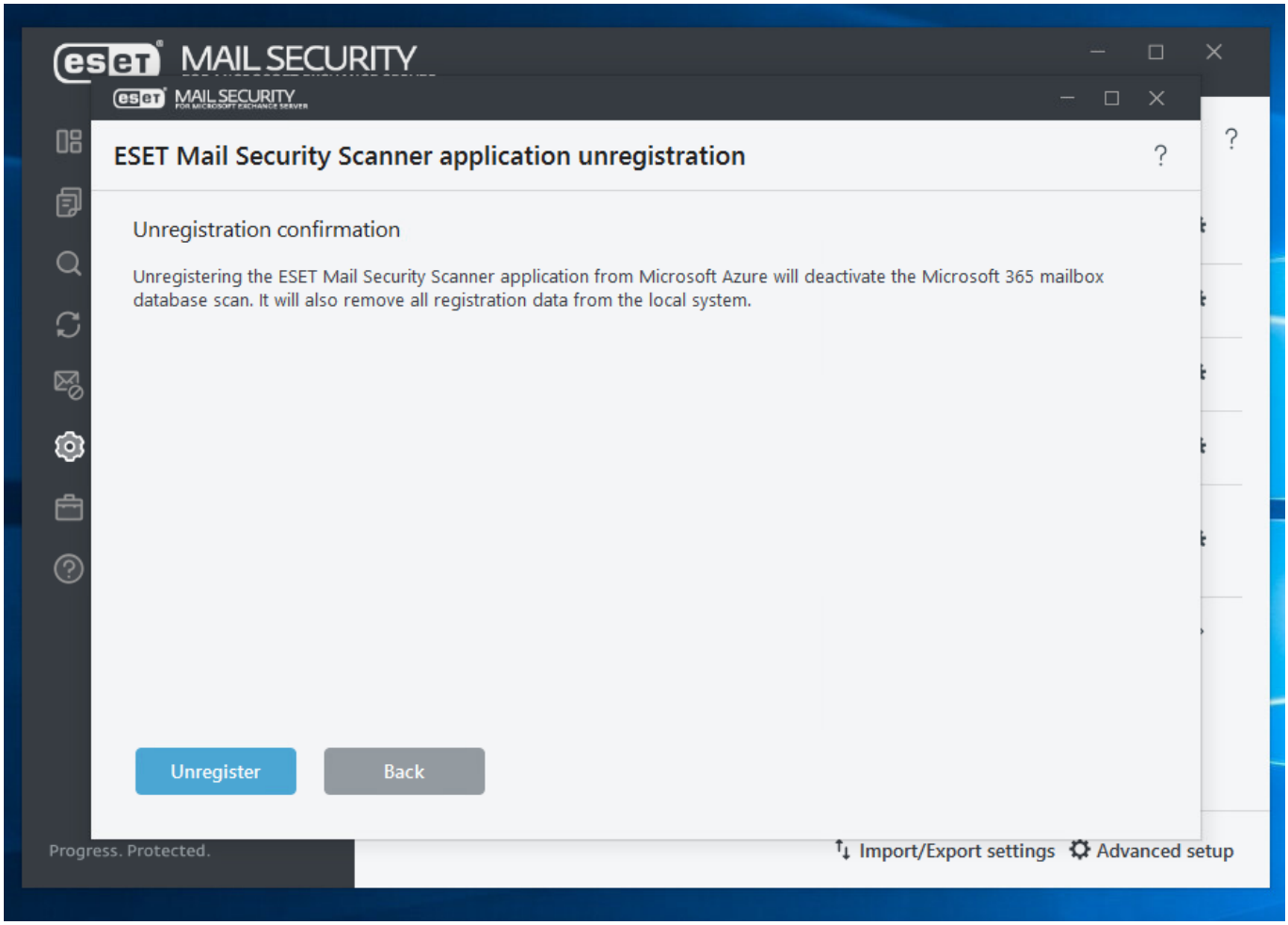
Registrierung des ESET Mail Security Scanners aufheben

Wenn Sie die Registrierung aufheben, werden das Zertifikat und die ESET Mail Security Scanner-App aus Microsoft Azure entfernt. Außerdem werden lokale Abhängigkeiten entfernt, und die Option zum Registrieren ist anschließend wieder verfügbar.

1. Klicken Sie auf **Einstellungen** > **Server** > **Microsoft 365-Postfach-Scan** und dann auf **Registrierung aufheben**, um die Entfernung des ESET Mail Security Scanners zu starten. Ein Assistent zum Aufheben der Registrierung wird geöffnet.



2. Klicken Sie auf **Registrierung aufheben**, um zu bestätigen, dass Sie den ESET Mail Security Scanner entfernen möchten. Warten Sie, bis die Registrierung in Microsoft Azure abgeschlossen wurde.



3. Wenn die Registrierung erfolgreich abgeschlossen wurde, wird im Assistenten die Nachricht **Registrierung erfolgreich aufgehoben** angezeigt.

Server-Schutzeinstellungen

Die Server-Schutzeinstellungen sind die wichtigste Integrationsoption. Klicken Sie auf den Umschalter, um die Integration von Postfach-Datenbankschutz, Mail-Transportschutz oder DKIM-Anmeldung bei Ihrem Exchange Server zu aktivieren oder zu deaktivieren. Wenn diese Option aktiviert ist, können Sie in den entsprechenden Bereichen ausführliche Einstellungen für die einzelnen Schutztypen konfigurieren. Außerdem können Sie die Agenten-Priorität bearbeiten (belassen Sie den ESET DKIM Agent auf der untersten Position).

Falls Sie Microsoft Exchange Server 2010 verwenden, können Sie zwischen Postfach-Datenbankschutz und On-Demand-Postfachdatenbankprüfung wählen. Sie können jedoch nur einen Schutztyp gleichzeitig aktivieren. Wenn Sie sich für den On-Demand Postfachdatenbank-Scan entscheiden, müssen Sie den Postfach-Datenbankschutz deaktivieren. Andernfalls ist die On-Demand Postfachdatenbank-Scan nicht verfügbar.

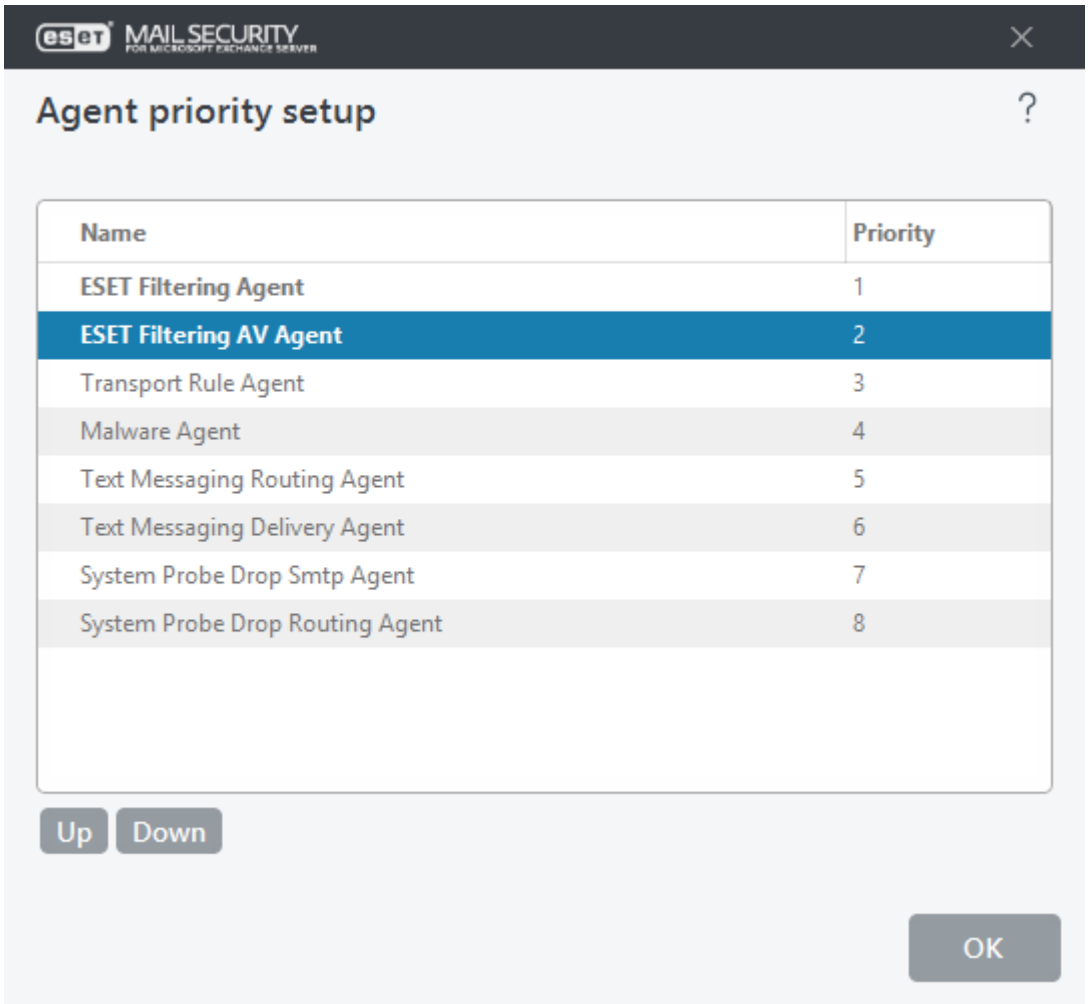
ESET Mail Security bietet mit den folgenden Funktionen herausragenden Schutz für Ihren Microsoft Exchange Server:

- Viren- und Spyware-Schutz
- Spam-Schutz
- Phishing-Schutz

- Regeln
- E-Mail-Transportschutz (Exchange Server 2010, 2013.2016, 2013, 2016)
- Postfachdatenbank-Schutz (Exchange Server 2010)
- On-Demand-Postfachdatenbankprüfung (Exchange Server 2010, 2013, 2016, 2019)
- E-Mail-Quarantäne (Einstellungen für E-Mail-Quarantäne)
- DKIM-Signierung

Einstellungen für Agentenpriorität

Legen Sie bei Bedarf fest, in welcher Reihenfolge die ESET Mail Security Agenten nach dem Start von Microsoft Exchange Server aktiviert werden. Der numerische Wert definiert die Priorität. Niedrigere Zahlen bedeuten eine höhere Priorität. Gilt für Microsoft Exchange Server 2010 und neuere Versionen.



Nach oben/nach unten

Erhöhen oder reduzieren Sie die Priorität eines ausgewählten Agenten, indem Sie ihn in der Liste nach oben oder unten verschieben. Sie können die Priorität für relevante Agenten ändern (hervorgehoben in Fettdruck).

Wir empfehlen, den ESET DKIM Agent an der untersten Stelle zu belassen, um sicherzustellen, dass die Header erst nach den Änderungen durch vorherige Agenten signiert werden.

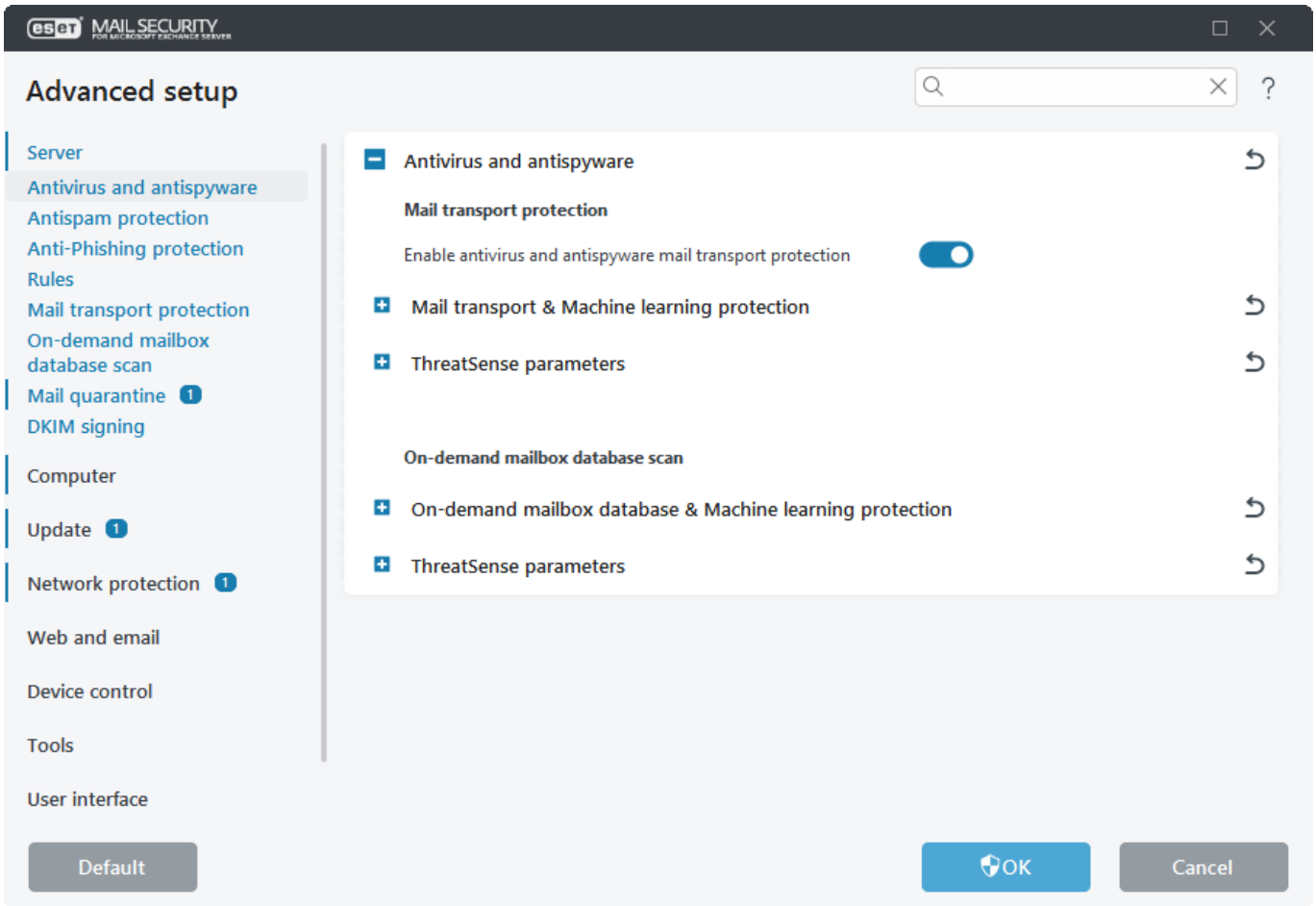
Viren- und Spyware-Schutz

In diesem Bereich können Sie die Optionen für den Viren- und Spyware-Schutz für Ihren E-Mail-Server konfigurieren.

Der Transport-Agent ist für den Mail-Transportschutz zuständig. Er ist nur für Microsoft Exchange Server 2010 oder neuere Versionen verfügbar, wenn Ihr Microsoft Exchange-Server in der Rolle Edge-Transportserver bzw. Hub-Transportserver ausgeführt wird. Dies gilt auch für Installationen mit einem einzigen Server und mehreren Exchange Server-Rollen auf einem Computer (sofern eine der genannten Rollen verwendet wird).

Mail-Transport-Schutz

Wenn Sie die Option **Viren- und Spyware-Schutz für den Mailtransport aktivieren** deaktivieren, wird das ESET Mail Security-Plug-In für Exchange-Server nicht aus dem Exchange-Serverprozess entfernt. Stattdessen werden die E-Mails dann ohne Virenprüfung auf der Transportebene weitergeleitet. Die E-Mails werden weiterhin in der Datenbankebene auf Viren und Spam geprüft, und vorhandene Regeln werden angewendet.



Postfachdatenbank-Schutz

Wenn Sie die Option **Viren- und Spyware-Schutz für Postfach-Datenbank aktivieren** deaktivieren, wird das ESET Mail Security-Plug-In für Exchange-Server nicht aus dem Exchange-Serverprozess entfernt. Stattdessen werden

die E-Mails dann ohne Virenprüfung auf der Datenbankebene weitergeleitet. Die E-Mails werden weiterhin in der Transportebene auf Viren und Spam geprüft, und vorhandene Regeln werden angewendet.

On-Demand Postfachdatenbank-Scan

Der On-Demand Postfachdatenbank-Scan ist verfügbar, nachdem Sie den **Postfach-Datenbankschutz** im Abschnitt Server deaktiviert haben.

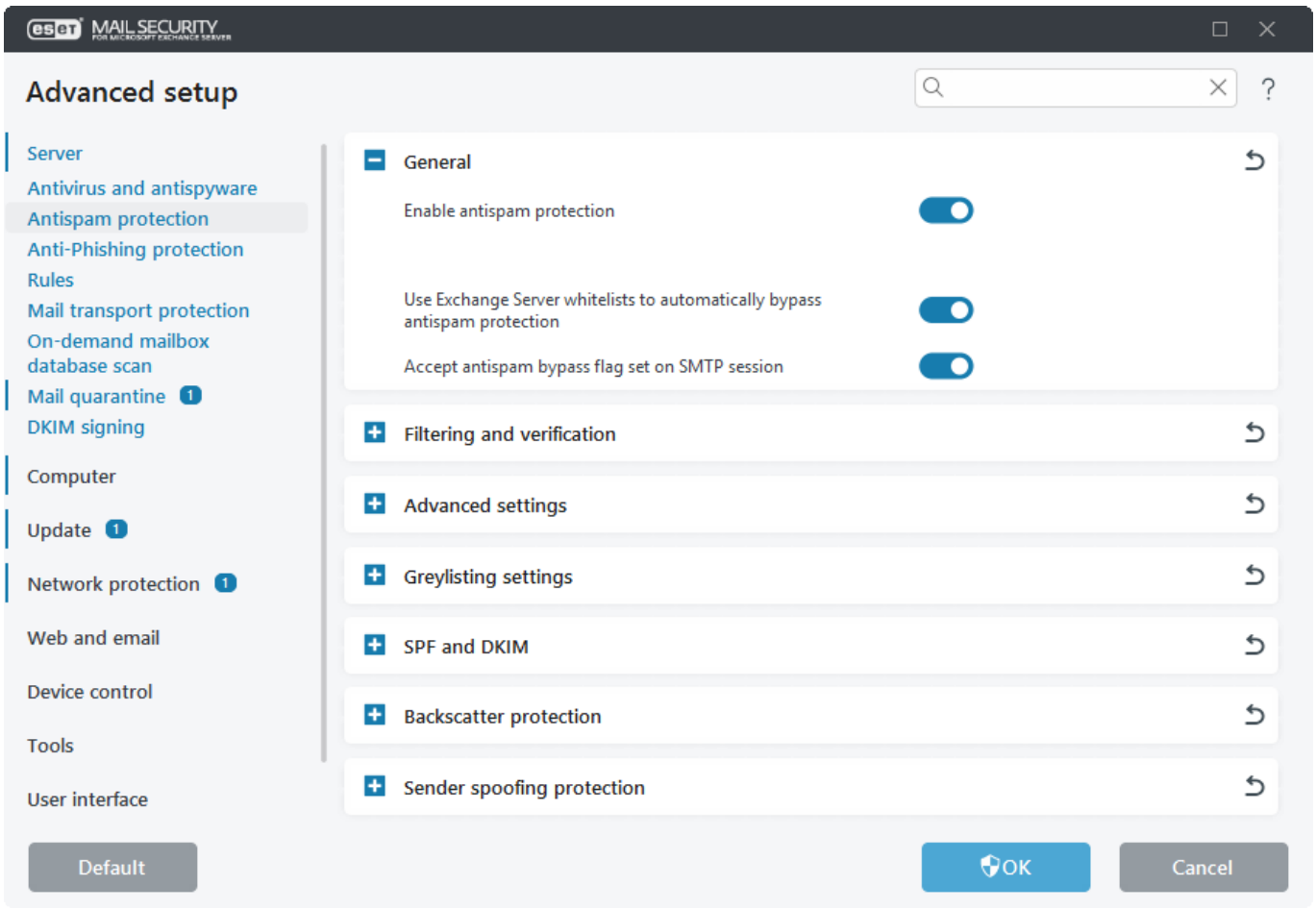
ThreatSense-Parameter

Legen Sie die Scan-Parameter für Mail-Transport-Schutz, Postfach-Datenbankschutz und On-Demand Postfachdatenbank-Scan fest.

Spam-Schutz

Der Spam-Schutz Ihres E-Mail-Servers ist standardmäßig aktiviert. Klicken Sie auf den Schalter neben **Spam-Schutz aktivieren**, um den Spam-Schutz zu deaktivieren.

> Wenn Sie den Spam-Schutz deaktivieren, ändert sich der Schutzstatus nicht. Auch bei deaktiviertem Spam-Schutz wird weiterhin der grüne Hinweis **Sie sind geschützt** im Bereich **Überwachung** des Programmfensters angezeigt. Eine Deaktivierung des Spamschutzes gilt nicht als Senkung der Schutzebene.



Whitelists des Exchange-Servers verwenden, um den Spam-Schutz automatisch zu umgehen

Geben Sie an, ob ESET Mail Security bestimmte Exchange-Positivlisten verwenden soll. Wenn dies aktiviert ist, wird Folgendes berücksichtigt:

- Die IP-Adresse des Servers ist in der Liste zugelassener IP-Adressen des Exchange-Servers enthalten
- Der Nachrichtenempfänger hat in seinem Postfach die Markierung für die Spamschutz-Umgehung gesetzt
- Die Absenderadresse ist in der Liste sicherer Absender des Empfängers enthalten (dafür muss die Synchronisierung der Liste sicherer Absender und die Aggregation der Liste in der Exchange Server-Umgebung konfiguriert sein)

Wenn einer der oben genannten Punkte auf eine eingehende Nachricht zutrifft, wird die Spamprüfung für diese Nachricht übersprungen. Die Nachricht wird nicht auf Spam untersucht und an das Postfach des Empfängers zugestellt.

Antispam-Umgehungs-Markierung in SMTP-Sitzung akzeptieren

Diese Option ist hilfreich für authentifizierte SMTP-Sitzungen zwischen Exchange-Servern, die diese Option verwenden. Wenn Sie beispielsweise einen Edge- und einen Hub-Server einsetzen, muss der Datenverkehr zwischen diesen beiden Servern nicht überprüft werden. Die Option **Markierung der SMTP-Sitzung zur Umgehung des Spam-Schutzes zulassen** ist standardmäßig aktiviert, wird jedoch nur angewendet, wenn auf Ihrem Exchange-Server für SMTP-Sitzungen die Option zur Umgehung des Spamschutzes gesetzt ist. Wenn Sie die Option **Markierung der SMTP-Sitzung zur Umgehung des Spam-Schutzes zulassen** deaktivieren, prüft ESET Mail Security die SMTP-Sitzung auf Spam, auch wenn auf dem Exchange Server die Option zur Umgehung gesetzt ist.

> Sie müssen die Antispamdatenbank regelmäßig aktualisieren, um sich mit dem Spam-Schutzmodul optimal zu schützen. Stellen Sie sicher, dass ESET Mail Security auf die korrekten IP-Adressen und die entsprechenden Ports zugreifen kann, um regelmäßige Updates der Spamschutz-Datenbank zu ermöglichen. Weitere Informationen zu den IP-Adressen und Ports, die dafür in Ihrer Firewall aktiviert werden müssen, finden Sie in unserem Knowledgebase-Artikel.

Sie finden die Funktionseinstellungen in den jeweiligen Abschnitten:

- Filterung und Verifizierung
- Erweiterte Einstellungen
- Einstellungen für die Greylist
- SPF und DKIM
- Rückläuferschutz
- Absender-Spoofing-Schutz

Filterung und Verifizierung

Sie können zugelassene, blockierte und ignorierte Listen anhand von Kriterien wie IP-Adresse, IP-Adressenbereich, Domänenname usw. konfigurieren. Um Kriterien hinzuzufügen, zu ändern oder zu entfernen, klicken Sie in der entsprechenden Liste auf **Bearbeiten**.

Die in den **ignorierten Listen** enthaltenen IP-Adressen und Domänen werden nicht vom Spam-Schutz getestet. Andere Spamschutz-Techniken werden jedoch angewendet.
Die ignorierten Listen sollten alle IP-Adressen und Domänennamen der internen Infrastruktur enthalten. Sie können auch die IP-Adressen und Domänennamen Ihres ISP oder der externen Mailversandserver angeben, die aktuell Teil der Blacklist von RBL oder DNSBL sind (Cloud-Blacklist – ESET Blackhole-Liste oder externe Blackhole-Liste).
Auf diese Weise können Sie E-Mails von Quellen aus den ignorierten Listen empfangen, auch wenn deren IP-Adressen Teil einer Cloud-Blacklist sind. Diese eingehenden E-Mails werden empfangen, und ihr Inhalt wird durch andere Spamschutz-Technologien weiter geprüft.

Liste zugelassener IP-Adressen	E-Mails von den angegebenen IP-Adressen werden automatisch zur Whitelist hinzugefügt. E-Mail-Inhalte werden nicht gescannt.
Liste blockierter IP-Adressen	E-Mails von den angegebenen IP-Adressen werden automatisch blockiert.
Liste ignorierter IP-Adressen	Liste mit IP-Adressen, die bei der Klassifizierung ignoriert werden. E-Mail-Inhalte werden gescannt. Verwenden Sie den Schieberegler Teil der internen Infrastruktur, um die lokalen IP-Adressen in Ihrem Netzwerk in die Positivliste aufzunehmen (siehe Beispiel unten).
Liste blockierter Domains im E-Mail-Body	E-Mails, die bestimmte Domains im Nachrichtenkörper enthalten, werden blockiert. Nur Domains mit echten Top-Level-Domains werden akzeptiert.
Liste ignorierter Domains im E-Mail-Body	Die angegebenen Domains im Nachrichtenkörper werden bei der Klassifizierung ignoriert. Nur Domains mit echten Top-Level-Domains werden akzeptiert.
Liste blockierter IP-Adressen im E-Mail-Body	E-Mails, die bestimmte IP-Adressen im Nachrichtenkörper enthalten, werden blockiert.
Liste ignorierter IP-Adressen im E-Mail-Body	Die angegebenen IP-Adressen im Nachrichtenkörper werden bei der Klassifizierung ignoriert.
Liste zugelassener Absender	E-Mails von bestimmten Absendern werden zur Whitelist hinzugefügt. Gemäß der folgenden Priorität wird nur eine Absenderadresse oder eine komplette Domäne für die Überprüfung verwendet: 1.SMTP 'MAIL FROM' adresse 2.E-Mail-Header-Feld "Return-Path:" 3.E-Mail-Header-Feld "X-Env-Sender:" 4.E-Mail-Header-Feld "From:" 5.E-Mail-Header-Feld "Sender:" 6.E-Mail-Header-Feld "X-Apparently-From:"
Liste blockierter Absender	E-Mails von bestimmten Absendern werden blockiert. Für die Verifizierung werden alle identifizierten Absenderadressen oder ganze Domänen verwendet: SMTP 'MAIL FROM' adresse E-Mail-Header-Feld "Return-Path:" E-Mail-Header-Feld "X-Env-Sender:" E-Mail-Header-Feld "From:" E-Mail-Header-Feld "Sender:" E-Mail-Header-Feld "X-Apparently-From:"
Liste genehmigte Domäne zu IP	E-Mails von IP-Adressen, die über Domänen in dieser Liste aufgelöst wurden, werden automatisch zur Positivliste hinzugefügt. SPF-Einträge (Sender Policy Framework) werden beim Auflösen von IP-Adressen erkannt.
Liste blockierter Domänen zu IP	E-Mails von IP-Adressen, die über Domänen in dieser Liste aufgelöst wurden, werden automatisch blockiert. SPF-Einträge werden beim Auflösen von IP-Adressen erkannt.
Liste ignorierte Domäne zu IP	Eine Liste mit Domänen, deren entsprechende IP-Adressen bei der Klassifizierung nicht überprüft werden. SPF-Einträge werden beim Auflösen von IP-Adressen erkannt.

Liste blockierter Länder	E-Mails aus bestimmten Ländern werden blockiert. Die Blockierung erfolgt anhand von GeoIP. Wenn eine Spam-Nachricht von einem E-Mail-Server mit einer IP-Adresse gesendet wird, die in der Geolocation-Datenbank zu einem Ihrer blockierten Länder zugeordnet ist, wird diese Nachricht automatisch als Spam markiert, und die konfigurierte Aktion für Spam-Mails unter Mail-Transport-Schutz wird ausgeführt.

> Die Listen der Körper-Domains akzeptieren nur echte Top-Level-Domains gemäß der offiziellen Root Zone-TLD-Datenbank.

Klicken Sie im Popupfenster auf **Mehrere Werte eingeben**, um mehrere Einträge gleichzeitig **anzulegen**. Wählen Sie anschließend das gewünschte Trennzeichen aus. Dies kann eine neue Zeile, ein Komma oder ein Semikolon sein.

> Ziel: Sie möchten die lokalen IP-Adressen in Ihrer Infrastruktur zu den freigegebenen IP-Adressen hinzufügen, um sie vom Spam-Schutz auszuschließen.
> Navigieren Sie zu **Erweiterte Einstellungen (F5)** > **Server** > **Spam-Schutz** > **Filterung und Verifizierung**.
> Klicken Sie auf **Bearbeiten** neben **Freigegebene IP-Adressen**.
> Klicken Sie auf **Hinzufügen** und geben Sie den IP-Adressbereich Ihrer Netzwerkinfrastruktur an (im Format *1.1.1.1-1.1.1.255*). Bei Bedarf können Sie weitere Bereiche oder einzelne IP-Adressen zur Liste hinzufügen.
> Verwenden Sie den Schieberegler **Teil der internen Infrastruktur**.

Greylisting und SPF

Fügen Sie Domänen oder IP-Adressen zur Positivliste hinzu, um Greylisting und SPF automatisch zu umgehen. Sie finden die Log-Dateien unter SMTP-Schutz-Log. Um diese Optionen verwenden zu können, müssen Sie Greylisting, SPF aktivieren. Für SPF müssen Sie die Option **Nachrichten bei fehlgeschlagener SPF-Prüfung automatisch ablehnen** und/oder **Greylisting bei bestandener SPF-Prüfung automatisch umgehen** aktivieren.

Spam-Schutzlisten verwenden, um Greylisting und SPF automatisch zu umgehen

Mit dieser Option werden die Listen mit genehmigten und ignorierten IP-Adressen zusammen mit den IP- und Domain-in-IP-Positivlisten verwendet, um Greylisting und SPF automatisch zu umgehen.

IP-Positivliste

In diesem Abschnitt können Sie IP-Adressen, IP-Adressen mit Maske und IP-Bereiche eingeben. Klicken Sie auf **Hinzufügen**, **Bearbeiten** oder **Löschen**, um die Liste zu bearbeiten. Alternativ können Sie auch Ihre eigene Liste aus einer Datei importieren, anstatt die einzelnen Einträge manuell anzulegen. Klicken Sie auf **Importieren** und suchen Sie die Datei mit den Einträgen, die Sie zur Liste hinzufügen möchten. Außerdem können Sie Ihre vorhandene Liste in eine Datei exportieren, indem Sie den Eintrag **Exportieren** im Kontextmenü auswählen.

> Whitelists haben Vorrang vor Blacklists. Wenn also eine E-Mail sowohl Adressen aus der Whitelist und aus der Blacklist enthält, wird sie als Whitelist betrachtet. Nur die letzte Absenderadresse und die maximale Anzahl der überprüften Adressen aus "Received:"-Headern werden mit den Whitelists abgeglichen. Alle Adressen werden mit den lokalen Blacklists abgeglichen.

Domain in IP-Positivliste

Mit dieser Option können Sie Domänen angeben (z. B. domainname.local). Klicken Sie auf **Hinzufügen**, **Entfernen** oder **Alle entfernen**, um die Liste zu verwalten. Falls Sie eine eigene Liste aus einer Datei importieren möchten, anstatt die einzelnen Einträge manuell anzulegen, klicken Sie auf **Importieren** und suchen Sie die Datei mit den Einträgen, die Sie zur Liste hinzufügen möchten. Außerdem können Sie Ihre vorhandene Liste in eine Datei exportieren, indem Sie den Eintrag **Exportieren** im Kontextmenü auswählen.

Greylisting und SPF werden vom Mail-Transport-Schutz ausgewertet und verwenden IP- und Domain-in-IP-Positivlisten sowie Listen mit genehmigten und ignorierten IP-Adressen. Falls Sie jedoch SPF-Regeln verwenden, wird keine dieser Positivlisten für die Regeln berücksichtigt.

Spam-Schutz – Erweiterte Einstellungen

Konfigurieren Sie diese Einstellungen, um E-Mails anhand von vordefinierten Kriterien durch externe Server (definiert als **RBL** – Realtime Blackhole List, **DNSBL** – DNS Blocklist) zu verifizieren. RBL-Server werden mit IP-Adressen abgefragt, die aus *Received:*-Headern extrahiert werden, und DNSBL-Server werden mit IP-Adressen und Domänen abgefragt, die aus dem Nachrichtentext extrahiert werden. Weitere Erläuterungen finden Sie in den Artikeln zu RBL und DNSBL.

Maximale Anzahl der überprüften Adressen in "Received:"-Headern

Sie können einschränken, wie viele IP-Adressen vom Spam-Schutz überprüft werden sollen. Diese Einstellung gilt für die IP-Adressen in den `Received: from`-Headern. Der Standardwert ist 0. In diesem Fall wird nur die IP-Adresse des letzten identifizierten Absenders überprüft.

Absenderadresse gegen Negativliste des Endbenutzers überprüfen

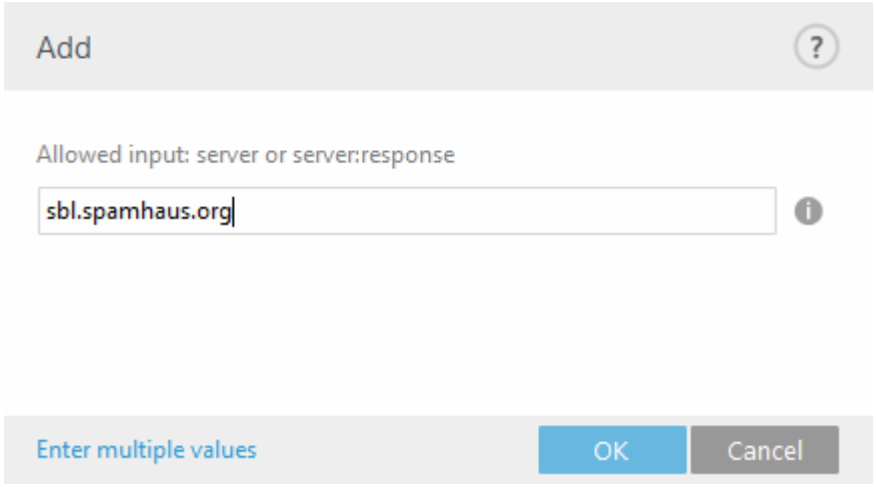
E-Mails, die nicht von E-Mail-Servern stammen (Computer, die nicht als E-Mail-Server aufgelistet sind), werden überprüft, um sicherzustellen, dass der Absender nicht in der Negativliste aufgeführt wird. Diese Option ist standardmäßig aktiviert. Sie können diese Option bei Bedarf deaktivieren, in diesem Fall werden Nachrichten, die nicht von E-Mail-Servern stammen, jedoch nicht gegen die Negativliste geprüft.

Die Ergebnisse externer Blocklisten haben Vorrang vor der Blacklist der Endbenutzer für IP-Adressen in `Received: from`-Headern. Alle IP-Adressen (bis zur festgelegten Obergrenze an überprüften Adressen) werden zur Überprüfung an externe Server gesendet.

Zusätzliche RBL-Server

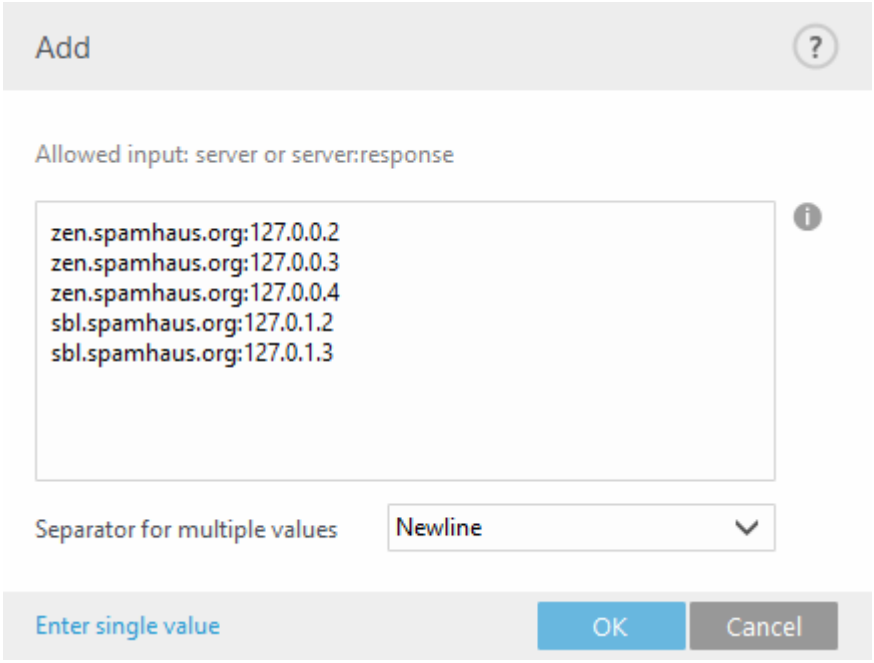
Liste der RBL (Realtime Blackhole List)-Server, die bei der E-Mail-Analyse abgefragt werden.

Geben Sie beim Hinzufügen zusätzlicher RBL-Server den Domänennamen des Servers ein (z. B. `sbl.spamhaus.org`). Diese Funktion verarbeitet alle Rückgabecodes, die vom Server unterstützt werden.



Alternativ können Sie einen Servernamen mit einem Rückgabecode im Format: `server:response` (z. B.

`zen.spamhaus.org:127.0.0.4`). Wenn Sie dieses Format verwenden, sollten Sie außerdem Servernamen und Rückgabecodes separat hinzufügen, um eine komplette Liste zu erhalten. Klicken Sie im Fenster „**Hinzufügen**“ auf **Mehrere Werte eingeben**, um alle Servernamen mit dem jeweiligen Rückgabecode einzugeben. Die Einträge sollten dem folgenden Beispiel ähneln, wobei die tatsächlichen Hostnamen und Rückgabecodes für Ihre RBL-Server abweichen:



Obergrenze für RBL-Abfragen (in Sekunden)

Legen Sie ein Zeitlimit für RBL-Abfragen fest. Nur die RBL-Antworten von den RBL-Servern, die rechtzeitig geantwortet haben, werden verwendet. Wenn der Wert auf "0" festgelegt ist, wird kein Zeitlimit verwendet.

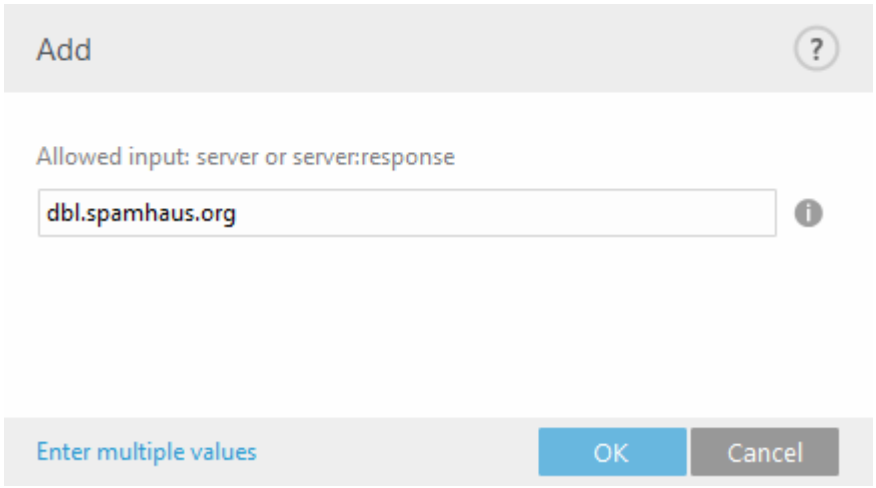
Maximale Anzahl gegen RBL überprüfter Adressen

Mit dieser Option können Sie die Zahl der IP-Adressen begrenzen, die auf dem RBL-Server abgerufen werden. Die Gesamtzahl der RBL-Abfragen entspricht der Anzahl der IP-Adressen in den „Empfangen:“ -Headers (maximal „RBL maxcheck“), multipliziert mit der Anzahl der RBL-Server, die in der RBL-Liste angegeben sind. Wenn der Wert auf "0" festgelegt ist, wird eine unbegrenzte Anzahl von "Received:"-Headern geprüft. Beachten Sie, dass IP-Adressen in der Liste ignorierter IP-Adressen nicht für die RBL-IP-Adresszahl berücksichtigt werden.

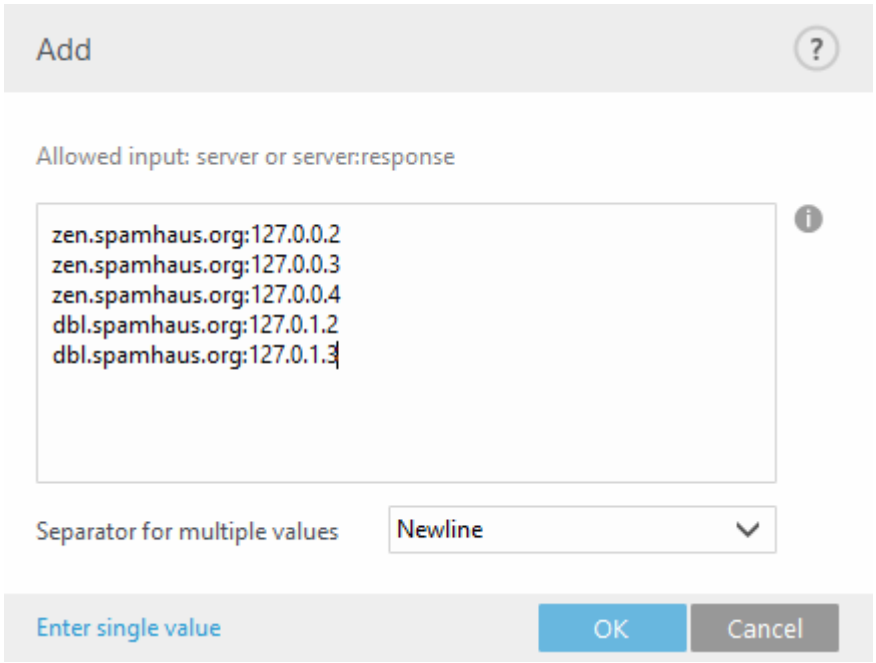
Zusätzliche DNSBL-Server

Liste der DNSBL (DNS-Blocklist)-Server, die mit Domänen und IP-Adressen aus dem Nachrichteninhalt abgefragt werden sollen.

> Geben Sie beim Hinzufügen zusätzlicher DNSBL-Server den Domänennamen des Servers ein (z. B. `dbl.spamhaus.org`). Diese Funktion verarbeitet alle Rückgabecodes, die vom Server unterstützt werden.



Alternativ können Sie einen Servernamen mit einem Rückgabecode im Format: `server:response` (z. B. `zen.spamhaus.org:127.0.0.4`). In diesem Fall sollten Sie außerdem Servernamen und Rückgabecodes separat hinzufügen, um eine komplette Liste zu erhalten. Klicken Sie im Fenster „**Hinzufügen**“ auf **Mehrere Werte eingeben**, um alle Servernamen mit dem jeweiligen Rückgabecode einzugeben. Die Einträge sollten dem folgenden Beispiel ähneln, wobei die tatsächlichen Hostnamen und Rückgabecodes für Ihre DNSBL-Server abweichen:



Obergrenze für DNSBL-Abfragen (in Sekunden)

Legen Sie ein Zeitlimit für DNSBL-Abfragen fest.

Höchstzahl der über DNSBL verifizierten Adressen

Mit dieser Option können Sie die Zahl der IP-Adressen begrenzen, die auf dem DNSBL-Server abgerufen werden.

Maximale Anzahl gegen DNSBL überprüfter Domänen

Mit dieser Option können Sie die Zahl der IP-Adressen begrenzen, die auf dem DNSBL-Server abgerufen werden.

Max. Größe zu scannender Nachrichten (kB)

Schränkt die Spamschutzprüfung für Nachrichten ein, die größer als der angegebene Wert sind. Der Standardmäßig 0 legt fest, dass Nachrichten aller Größen geprüft werden. Die Größe der zu prüfenden Nachrichten muss nur in speziellen Situationen auf einen bestimmten Wert limitiert werden. Wenn diese Option festgelegt ist, verarbeitet das Spam-Schutz-Modul Nachrichten bis zur festgelegten Größe und ignoriert größere Nachrichten.

Das kleinstmögliche Limit ist 12 kB. Wenn Sie einen Wert zwischen 1 und 12 festlegen, verwendet das Spam-Schutz-Modul automatisch mindestens den Wert 12 kB.

Vorübergehendes Ablehnen unbestimmter Nachrichten aktivieren

Wenn das Spamschutzmodul nicht ermitteln kann, ob es sich bei einer Nachricht um Spam handelt, z. B. wenn eine Nachricht zwar Spam-Charakteristiken enthält, diese jedoch nicht für eine Spam-Klassifizierung ausreichen (z. B. der die erste E-Mail einer Kampagne oder eine E-Mail von einer Absender-IP mit gemischten Bewertungen), dann kann ESET Mail Security mit dieser Einstellung solche Nachrichten vorübergehend ablehnen. Dabei wird dasselbe Verfahren wie beim Greylisting verwendet. Die Nachricht wird für eine bestimmte Dauer abgelehnt, bis Folgendes eintritt:

- Das Intervall ist abgelaufen, und die Nachricht wird beim nächsten Zustellversuch akzeptiert. Die Nachricht behält ihre ursprüngliche Klassifizierung (SPAM bzw. HAM).
- Die Spamschutz-Cloud hat genügend Daten gesammelt, um die Nachricht korrekt zu klassifizieren, bevor das Intervall abgelaufen ist.

ESET Mail Security bewahrt die abgelehnte Nachricht nicht auf, da diese gemäß SMTP RFC vom E-Mail-Server des Absenders erneut gesendet werden muss.

Einreichen von vorübergehend abgelehnten Nachrichten zur Analyse aktivieren

Der Nachrichteninhalt wird automatisch zur weiteren Analyse übertragen. Diese Funktion erleichtert die Klassifizierung zukünftiger E-Mail-Nachrichten.

Es kann vorkommen, dass vorübergehend abgelehnte Nachrichten, die zur Analyse übermittelt wurden, kein SPAM sind. In seltenen Fällen können vorübergehend abgelehnte Nachrichten für die manuelle Prüfung verwendet werden. Aktivieren Sie diese Funktion nur, wenn keine Gefahr besteht, dass sensible Daten übertragen werden.

Einstellungen für die Greylist

Mit der Option **Greylisting aktivieren** starten Sie eine Programmfunktion, die Benutzer mit der folgenden Technologie vor Spam schützt: Der Transport-Agent sendet den SMTP-Rückgabewert „vorübergehend abgelehnt“ (standardmäßig 451/4.7.1) für jede E-Mail von einem unbekannten Absender. Ein rechtmäßiger Server wird nach kurzer Wartezeit erneut versuchen, die E-Mail zu senden. Spam-Server unternehmen gewöhnlich keinen zweiten Zustellversuch, da sie Tausende von E-Mail-Adressen abarbeiten müssen und diese zeitraubende Aktion daher unterlassen. Die Greylisting-Technik erhöht den Spam-Schutz, ohne die Spam-Erkennung des Spam-Schutz-Moduls zu beeinflussen.

Beim Prüfen des Absenders berücksichtigt die Greylisting-Technik neben den AntispamBypass-Einstellungen für das Postfach des Empfängers auch die Einstellungen für die folgenden Listen auf dem Exchange-Server: Freigegebene IP-Adressen, Ignorierte IP-Adressen, Sichere Absender und IP-Adressen zulassen. Bei E-Mails von den gespeicherten IP-Adressen/Absendern bzw. E-Mails, die an ein Postfach mit aktivierter AntispamBypass-

Option gesendet werden, findet kein Greylisting statt.

Nur den Domänenteil der Absenderadresse verwenden

Diese Funktion ignoriert den Absendernamen in der E-Mail-Adresse und berücksichtigt nur die Domäne.

Greylisting-Datenbanken im ESET-Cluster synchronisieren

Die Greylisting-Datenbankeinträge werden in Echtzeit zwischen den Servern im ESET-Cluster geteilt. Wenn einer der Server eine mit Greylisting verarbeitete Nachricht erhält, wird diese Information per Broadcast von ESET Mail Security an die restlichen Knoten im ESET-Cluster übertragen.

Zeitlimit für die ausgängliche Verbindungsablehnung (Min.)

Legt die Zeitspanne fest, nach der die E-Mail, die beim ersten Sendeversuch vorübergehend abgelehnt wurde, immer abgelehnt wird (ab der ersten Ablehnung). Ist diese Zeitspanne vorüber, kann die E-Mail erfolgreich gesendet werden. Der Mindestwert beträgt 1 Minute.

Ablaufzeit für ungeprüfte Verbindungen (Stunden)

Legt fest, wie lange die drei Hauptinformationen einer E-Mail gespeichert werden. Ein rechtmäßiger Server muss die erwartete Nachricht vor dem Ablauf dieses Intervalls erneut senden. Der Wert muss größer sein als der Wert für **Zeitbegrenzung für das Abweisen der ursprünglichen Verbindung**.

Ablaufzeit für geprüfte Verbindungen (Tage)

Legt fest, für wie viele Tage E-Mail-Informationen mindestens gespeichert werden. Während dieser Zeit werden E-Mails von bestimmten Absendern ohne Zeitverzögerung empfangen. Dieser Wert muss größer sein als der Wert für **Ablauf nicht verifizierter Verbindungen**.

SMTP-Antwort für vorübergehend abgelehnte Verbindungen

Legen Sie **Antwortcode**, **Statuscode** und **Antwortnachricht** an den SMTP-Server für die vorübergehende Ablehnung einer E-Mail fest. Beispiel für eine SMTP Reject-Antwort:

Antwortcode	Statuscode	Antwortnachricht
451	4.7.1	Bitte später erneut versuchen

Für die Konfiguration des SMTP-Rejects können Sie auch Systemvariablen verwenden.

SMTP-Antworten mit falscher Syntax können zu einem Fehlverhalten im Greylisting-Schutzmodul führen. Möglicherweise werden dann Spam-Mails an Clients weitergeleitet bzw. E-Mails überhaupt nicht zugestellt.

Das SMTP-Schutz-Log enthält alle Nachrichten, die mit der Greylisting-Methode geprüft wurden.

SPF und DKIM

Sender Policy Framework (SPF) und DomainKeys Identified Mail (DKIM) sind Validierungsmethoden, um eingehende E-Mail-Nachrichten von bestimmten Domänen zu überprüfen, die vom Besitzer der jeweiligen Domäne autorisiert wurden. Auf diese Weise werden Empfänger vor gefälschten E-Mail-Nachrichten geschützt. ESET Mail Security verwendet außerdem DMARC (Domain-based Message Authentication, Reporting and Conformance) als Ergänzung zu SPF und DKIM.

SPF

Die SPF-Prüfung ermittelt, ob eine E-Mail von einem legitimen Absender stammt. Eine DNS-Abfrage für SPF-Einträge der Absenderdomäne wird ausgeführt, um eine Liste von IP-Adressen zu erhalten. Falls eine der IP-Adressen aus den SPF-Einträgen mit der tatsächlichen IP-Adresse des Absenders übereinstimmt, gilt die SPF-Prüfung als **Bestanden**. Wenn die tatsächliche IP-Adresse des Absenders nicht übereinstimmt, wird ein **Fehler** ausgegeben. Allerdings haben nicht alle Domänen SPF-Einträge im DNS. Falls keine SPF-Einträge im DNS vorhanden sind, lautet das Ergebnis **Nicht verfügbar**. Bei DNS-Anfragen kann gelegentlich eine Zeitüberschreitung auftreten. In diesem Fall ist das Ergebnis ebenfalls **Nicht verfügbar**.

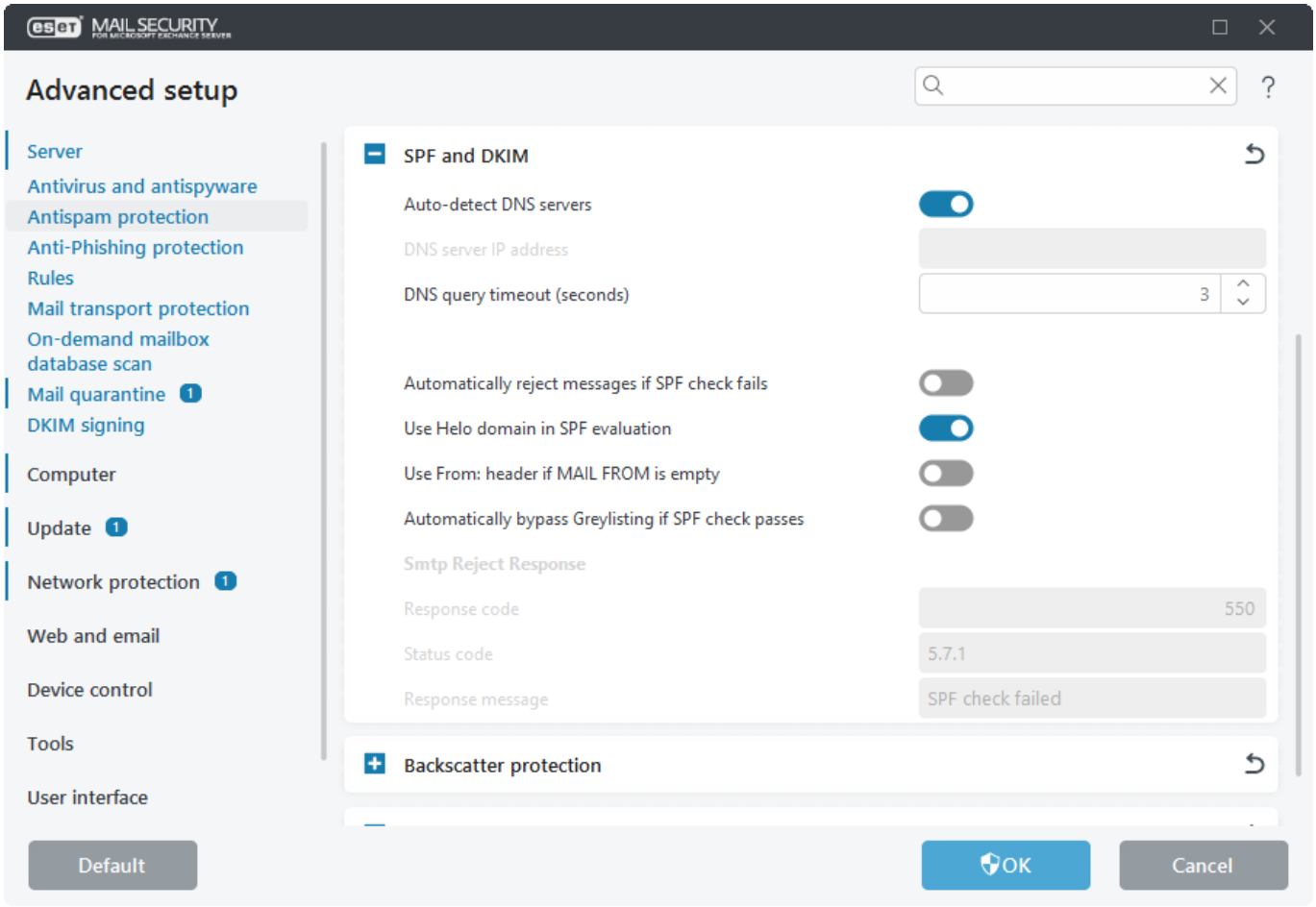
DKIM

Organisationen setzen diese Technologie ein, um gefälschte E-Mail-Nachrichten (Spoofing) zu verhindern, indem an die Header ausgehender Nachrichten eine digitale Signatur gemäß des DKIM-Standards angefügt wird. Dieses Verfahren verwendet einen privaten Domänenschlüssel, um die Header in den ausgehenden E-Mails Ihrer Domäne zu verschlüsseln, und fügt eine öffentliche Version des Schlüssels zum DNS-Eintrag der Domäne hinzu. ESET Mail Security kann anschließend den öffentlichen Schlüssel abrufen, um eingehende Header zu entschlüsseln und sicherzustellen, dass die Nachricht tatsächlich von Ihrer Domäne stammt und die Header auf dem Weg nicht verändert wurden.

> **i** Exchange Server 2010 und ältere Versionen sind nicht vollständig mit DKIM kompatibel, da die Header in digital signierten eingehenden Nachrichten unter Umständen bei der DKIM-Validierung verändert werden.

DMARC

DMARC basiert auf den SPF- und DKIM-Techniken. Sie können Mail-Transport-Schutzregeln verwenden, um das **DMARC-Ergebnis** und die Aktion **DMARC-Policy übernehmen** auszuwerten.



DNS-Server automatisch erkennen

Die automatische Erkennung verwendet die Einstellungen Ihres Netzwerkadapters.

IP-Adresse des DNS-Servers

Falls Sie bestimmte DNS-Server für SPF und DKIM verwenden möchten, können Sie deren IP-Adressen (im IPv4- oder IPv6-Format) hier eingeben.

Zeitüberschreitung für DNS-Abfrage (Sekunden)

Geben Sie eine Zeitüberschreitung für die DNS-Antwort an.

Nachrichten bei fehlgeschlagener SPF-Prüfung automatisch ablehnen

Wenn Ihre SPF-Prüfung sofort einen Fehler ergibt, kann die E-Mail noch vor dem Download verworfen werden.

Die SPF-Prüfung erfolgt auf der SMTP-Ebene. Die Ablehnung kann jedoch entweder automatisch auf DER SMTP-Ebene oder bei der Regelauswertung erfolgen.
Abgelehnte Nachrichten können nicht im Ereignis-Log protokolliert werden, wenn die automatische Ablehnung auf der SMTP-Ebene erfolgt. Dies liegt daran, dass das Logging durch die Regelaktion ausgeführt wird, und die automatische Ablehnung erfolgt direkt auf der SMTP-Ebene noch vor der Regelauswertung. Da die Nachrichten noch vor der Regelauswertung abgelehnt werden, sind zum Zeitpunkt der Regelauswertung keine zu protokollierenden Informationen vorhanden.
Abgelehnte Nachrichten können nur protokolliert werden, wenn die Nachricht von einer Regelaktion abgelehnt wurde. Um Nachrichten abzulehnen, die die SPF-Prüfung nicht bestanden haben, und diese abgelehnten Nachrichten zu loggen, deaktivieren Sie die Option **Nachrichten bei fehlgeschlagener SPF-Prüfung automatisch ablehnen** und erstellen Sie die folgende Regel für den **Mail-Transport-Schutz**:
Bedingung
- Typ: SPF-Ergebnis
- Operation: ist
- Parameter: Nicht bestanden

Aktionen
- Typ: Nachricht ablehnen
- Typ: Logging in Ereignissen

Helo-Domäne in der SPF-Auswertung verwenden

Diese Funktion verwendet die HELO-Domäne für die SPF-Auswertung. Wenn Sie die HELO-Domäne nicht angeben, wird stattdessen der Hostname des Computers verwendet.

From:-Header verwenden, wenn MAIL FROM leer ist

Der MAIL FROM-Header kann leer sein und lässt sich außerdem leicht fälschen. Wenn diese Option aktiviert ist und MAIL FROM leer ist, wird die Nachricht heruntergeladen und stattdessen der Header From: verwendet.

Greylisting bei bestandener SPF-Prüfung automatisch umgehen

Greylisting bietet keine Vorteile für die Nachricht, wenn die SPF-Prüfung bestanden wurde.

SMTP-Ablehnungsantwort

Sie können **Antwortcode**, **Statuscode** und **Antwortnachricht** an den SMTP-Server für die SMTP vorübergehende Ablehnung einer E-Mail festlegen. Sie können eine Antwortnachricht in folgendem Format eingeben:

Antwortcode	Statuscode	Antwortnachricht
550	5.7.1	SPF-Prüfung fehlgeschlagen

Rückläuferschutz

Spam-Rückläufer sind fehlgeleitete Bounce-Nachrichten von Mailservern und sind ein unerwünschter Nebeneffekt von Spam. Wenn der E-Mail-Server des Empfängers eine Spam-Nachricht ablehnt, sendet er einen Unzustellbarkeitsbericht, auch bekannt als Bounce-Nachricht, an den angeblichen Absender (eine gefälschte E-Mail-Adresse, als die sich der Absender der Spam-Nachricht ausgibt), von dem die Nachricht jedoch nicht stammt. Der Besitzer der E-Mail-Adresse erhält eine Unzustellbarkeitsmeldung, obwohl er nicht an der ursprünglichen Spamnachricht beteiligt war. An dieser Stelle greift der **Rückläuferschutz** ein. Mit dem Rückläuferschutz von ESET Mail Security können Sie verhindern, dass Spam-Rückläufer an die Postfächer der Benutzer in Ihrem Unternehmen zu gestellt werden.

Wenn Sie die **NDR-Überprüfung aktivieren**, müssen Sie einen **NDR-Überprüfung aktivieren** angeben (eine Zeichenfolge mit mindestens 8 Zeichen, ähnlich einer Passphrase). Der Rückläuferschutz von ESET Mail Security schreibt `X-Eset-NDR: <hash>` in den Header aller ausgehenden E-Mail-Nachrichten. Der `<hash>` ist eine verschlüsselte Signatur und enthält den von Ihnen angegebenen **Signatur-Seed**.

Wenn eine legitime E-Mail nicht zugestellt werden kann, erhält Ihr E-Mail-Server normalerweise einen Unzustellbarkeitsbericht, in dessen Headern ESET Mail Security anschließend nach `X-Eset-NDR: <hash>` sucht. Wenn der Header `X-Eset-NDR:` vorhanden ist und die Signatur `<hash>` übereinstimmt, wird der Unzustellbarkeitsbericht an den Absender der legitimen E-Mail-Nachricht mit der Meldung zugestellt, dass die Nachricht nicht zugestellt werden konnte. Wenn `Eset-NDR:` nicht vorhanden ist oder der Signatur-`<hash>` nicht übereinstimmt, handelt es sich um Spam-Rückläufer, und der Unzustellbarkeitsbericht wird abgelehnt.

NDR-Nachrichten automatisch verwerfen, wenn die Prüfung fehlschlägt

Wenn Ihre NDR-Prüfung sofort einen Fehler ergibt, kann die E-Mail noch vor dem Download verworfen werden.

Die Aktivitäten des **Rückläuferschutzes** werden im SMTP-Schutz-Log protokolliert.

Absender-Spoofing-Schutz

E-Mail-Absender-Spoofing ist eine gängige Praxis, bei der ein Angreifer den Namen oder die E-Mail-Adresse des Absenders fälscht, um den Empfänger zu täuschen. Für den Empfänger der E-Mail unterscheidet sich eine solche gefälschte E-Mail nicht von einer echten E-Mail, was ein Risiko darstellt. Eine Art von Absender-Spoofing wird als CEO-Betrug bezeichnet (Angreifer gibt sich als CEO aus).

Mitarbeiter hinterfragen solche E-Mails oft nicht, was die Erfolgschancen des Angriffs erhöht. Dies gilt nicht nur für CEOs. Beim Absender-Spoofing wird häufig die Identität echter Absender vorgetäuscht, in der Regel von Personen im Active Directory der entsprechenden Organisation. Eine gefälschte E-Mail sieht dann für einen ahnungslosen Empfänger sehr überzeugend aus und erlangt leicht sein Vertrauen.

ESET Mail Security schützt Sie vor E-Mail-Absender-Spoofing. Der Absender-Spoofing-Schutz prüft mit mehreren Methoden, ob die Informationen des Absenders gültig sind.

Der Absender-Spoofing-Schutz sucht nach der Domäne, die in der „Von:“-Kopfzeile der E-Mail und im Absender enthalten ist, und vergleicht die gefundene Domäne mit den Domänenlisten. Wenn die Domäne nicht übereinstimmt, wird die Nachricht als gültig (nicht gefälscht) betrachtet und von anderen ESET Mail Security Schutzschichten weiterverarbeitet. Wenn die Domäne mit einer Domäne in der Liste überstimmt, kann sie jedoch als gefälscht eingestuft werden, und eine weitere Verifizierung ist nötig.

Je nach Einstellung werden weitere Verifizierungen durchgeführt: SPF-Prüfung, Abgleich der Umschlag-IP-Adresse mit IP-Listen oder automatische Einstufung der Nachricht als gefälscht. Wenn das SPF-Prüfergebnis negativ ist oder die Umschlag-IP mit einer IP aus der Liste übereinstimmt, ist die Nachricht gültig; andernfalls wird sie als gefälscht eingestuft. Die gefälschte Nachricht wird weiterverarbeitet.

Sie können den Absender-Spoofing-Schutz auf zwei verschiedene Weisen anwenden:

- Aktivieren Sie den **Absender-Spoofing-Schutz**, konfigurieren Sie dessen Einstellungen und geben Sie optional Domänen und IP-Listen an. Die Standardaktion bei gefälschten E-Mail-Nachrichten **E-Mail in Quarantäne verschieben.** Um die Aktion zu ändern, wechseln Sie zu den erweiterten Einstellungen für den E-Mail-Transportschutz.

- Verwenden Sie Regeln für den Mail-Transportschutz: Verwenden Sie die **Regeln für den Mail-**

Transportschutz mithilfe von -Ergebnis – Von Kopfzeile oder **Vergleichsergebnis zwischen Umschlag-Absender und From-Header** mit einer Aktion Ihrer Wahl. Regeln bieten zusätzliche Optionen und Kombinationsmöglichkeiten, wenn Sie bestimmte Verhaltensmuster im Zusammenhang mit gefälschten E-Mails einrichten möchten.

Wenn Sie den **Absender-Spoofing-Schutz** verwenden oder einen Regelaktionstyp **Logging in Ereignissen** angeben, werden alle Nachrichten, die vom **Absender-Spoofing-Schutz** geprüft wurden, in den Log-Dateien aufgezeichnet. Außerdem finden Sie gefälschte E-Mail-Nachrichten in der Nachrichten-Quarantäne, wenn die Aktion **Nachrichten-Quarantäne** im E-Mail-Transportschutz oder in einer Regel definiert ist.

Absender-Spoofing-Schutz aktivieren

Aktivieren Sie den Absender-Spoofing-Schutz, um E-Mail-Angriffe zu verhindern, die versuchen, für den Empfänger die Herkunft der Nachricht zu verschleiern (gefälschter Absender).

Eingehende E-Mails mit meiner eigenen Domäne als Absenderadresse aktivieren

E-Mails, die Ihre eigene Domäne in der "From:"-Kopfzeile der E-Mail oder im Umschlagabsender enthalten (mit Verdacht auf Fälschung), können weiter geprüft werden:

- **Nur nach bestandener SPF-Prüfung** – dazu muss SPF aktiviert sein. Wenn das SPF-Ergebnis negativ ist, wird die Nachricht als gültig betrachtet und zur Zustellung verarbeitet. Wenn das SPF-Ergebnis positiv ist, wird die Nachricht als gefälscht eingestuft (Aktion findet statt). Optional können Sie auch Nachrichten bei positiver SPF-Prüfung automatisch ablehnen.

- **Nur wenn IP-Adresse in der IP-Liste der Infrastruktur enthalten ist** – Vergleicht die Umschlag-IP-Adresse mit den IP-Listen (eine Liste Ihrer eigenen IP-Adressen und die Liste ignorierter IP-Adressen werden als **Teil der internen Infrastruktur** markiert). Wenn die IP-Adresse übereinstimmt, ist die Nachricht gültig und wird zugestellt. Wenn die IP-Adresse nicht übereinstimmt, wird die Nachricht als gefälscht eingestuft und eine Aktion findet statt.

- **Nie** – Wenn eine eingehende Nachricht Ihre eigene Domäne in der „Von:“-Kopfzeile der E-Mail oder im Umschlag-Absender enthält, wird sie automatisch als gefälschte Nachricht eingestuft ohne weitere Prüfung. Die Nachricht löst eine Aktion aus, siehe E-Mail-Transportschutz für Aktionsoptionen.

Meine eigenen Domänen automatisch aus der Liste der akzeptierten Domänen laden

Wir empfehlen dringend, diese Option zu aktivieren, um den größtmöglichen Schutz zu gewährleisten. Auf diese Weise werden die Domänen und IP-Adressen Ihrer Infrastruktur bei der Prüfung durch den Absender-Spoofing-Schutz berücksichtigt.

Liste meiner eigenen Domänen

Diese Domänen werden als Ihnen gehörend betrachtet. Fügen Sie Domänen hinzu, die zusätzlich zu den automatisch geladenen Domänen aus Ihrem Active Directory bei der Auswertung verwendet werden sollen. Die Domäne(n) des Absenders werden mit den Domänen in diesen Listen verglichen. Wenn die Domäne nicht übereinstimmt, ist die Nachricht gültig. Wenn die Domäne übereinstimmt, wird eine weitere Verifizierung gemäß der Einstellung **Eingehende E-Mails mit meiner eigenen Domäne als Absenderadresse aktivieren** durchgeführt.

Liste meiner eigenen IP-Adressen

IP-Adressen, die als vertrauenswürdig gelten. Fügen Sie IP-Adressen hinzu, die bei der Auswertung verwendet werden zusätzlich zu den IP-Adressen in der Liste ignorierter IP-Adressen, die als **Teil der internen Infrastruktur**

markiert sind. Die Umschlag-IP-Adresse des Absenders wird mit den IP-Adressen in diesen Listen verglichen. Wenn die IP-Adresse des Umschlags übereinstimmt, ist die Nachricht gültig. Wenn die IP-Adresse nicht übereinstimmt, wird die Nachricht als gefälscht eingestuft und eine Aktion findet statt.

Phishing-Schutz

Beim Phishing wird versucht, sensible Informationen wie Benutzernamen, Passwörter, Bankkonten oder Kreditkartendaten und PIN-Nummern über E-Mails oder Webseiten abzugreifen, die sich als vertrauenswürdige Entitäten ausgeben. Diese Aktivität erfolgt normalerweise aus bösartigen Beweggründen. Häufig wird dabei Social Engineering (Manipulation von Benutzern zum Erlangen vertraulicher Informationen) eingesetzt.

Der Phishing-Schutz in ESET Mail Security verhindert, dass Benutzer auf Webseiten zugreifen, die für Phishing bekannt sind. E-Mails können Links zu Phishing-Webseiten enthalten. ESET Mail Security verwendet einen ausgeklügelten Parser, um den Betreff und den Text aller eingehenden Nachrichten zu analysieren und gefährliche Links (URLs) zu identifizieren.

Die Links werden mit einer Phishing-Datenbank abgeglichen. Bei einem positiven Ergebnis, wird die E-Mail als Phishing-Nachricht behandelt, und ESET Mail Security verarbeitet sie gemäß der Einstellung **Auszuführende Aktion bei Phishing-E-Mail** für die jeweilige Schutzebene (Mail-Transportschutz, Postfach-Datenbankschutz und On-Demand Postfachdatenbank-Scan). Regelaktionen werden ebenfalls ausgeführt.

Unterstützte Standards für E-Mail-Formate:

- Nur-Text
- Nur HTML
- MIME
- Multipart-MIME (E-Mails mit HTML und Nur-Text)

Unterstützte HTML-Entitäten:

Phishing-Nachrichten können HTML-Entitäten enthalten, um das Phishing-Schutzmodul zu verwirren. Der Phishing-Schutz analysiert und übersetzt auch HTML-Symbole, um verschleierte URLs zu finden und korrekt auszuwerten.

Einzelne Zeichen können oft auf mehrere Arten dargestellt werden. Ein Punkt kann beispielsweise auf die folgenden Arten dargestellt werden:

Normale Anzeige von Links in E-Mail-Nachrichten an Benutzer	Wert	Verschleierte Links im Nachrichtentext	Typ
http://www.example-phishing-domain.com/Fraud	.	http://www.example-phishing-domain.com/Fraud	Zeichen
http://www.example-phishing-domain.com/Fraud	&period;	http://www.example-phishing-domain.com/Fraud	Entität name
http://www.example-phishing-domain.com/Fraud	&#x0002E;	http://www.example-phishing-domain.com/Fraud	Entität als hexadezimale Zahl
http://www.example-phishing-domain.com/Fraud	&#46;	http://www.example-phishing-domain.com/Fraud	Entität als Dezimal-Zahl

Unter **Log-Dateien** > E-Mail-Server-Schutz-Log können Sie die Aktivitäten des E-Mail-Phishing-Schutzes anzeigen. Das Log enthält Informationen zu E-Mail-Nachrichten und darin enthaltenen Phishing-Links.

Phishing-Seite melden

Klicken Sie auf Melden, um ESET über Phishing- oder bösartige Websites zu informieren.

Regeln

Sie können Filterbedingungen für E-Mails manuell definieren und Aktionen für gefilterte E-Mails zuweisen. Außerdem können Sie separate Bedingungen und Aktionen für den Mail-Transportschutz, den Postfach-Datenbankschutz und den On-Demand Postfachdatenbank-Scan definieren. Dies ist hilfreich, da jeder Schutztyp bei der Verarbeitung von Nachrichten einen etwas anderen Ansatz verwendet, insbesondere der Mail-Transportschutz.

Die auf Ihrem System verfügbaren Regeln für Postfach-Datenbankschutz, On-Demand Postfachdatenbank-Scan und Mail-Transportschutz hängen davon ab, welche Version von Microsoft Exchange Server auf dem Server mit ESET Mail Security installiert ist.

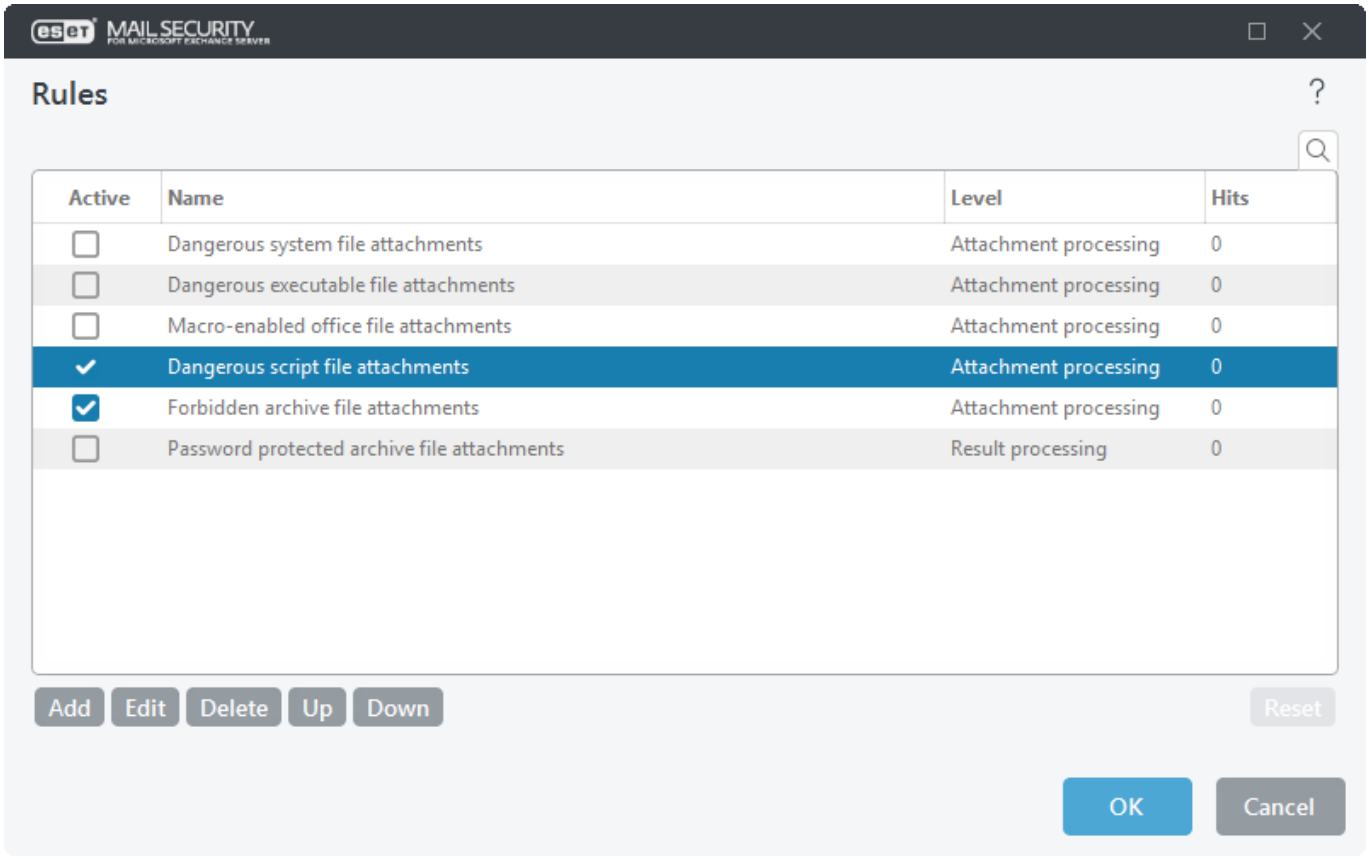
Falsch definierte Regeln für die **On-Demand Postfachdatenbank-Scan** können unumkehrbare Änderungen an den Postfachdatenbanken verursachen. Stellen Sie immer sicher, dass Sie eine aktuelle Sicherung Ihrer Postfachdatenbanken haben, bevor Sie einen On-Demand Postfachdatenbank-Scan mit neuen Regeln zum ersten Mal ausführen. Überprüfen Sie unbedingt, ob die Regeln Ihren Erwartungen entsprechen. Definieren Sie für diese Überprüfung Regeln nur mit der Aktion **Logging in Ereignissen** da alle anderen Aktionen Änderungen an Ihren Postfachdatenbanken vornehmen können. Wenn Sie mit der Überprüfung zufrieden sind, können Sie destruktive Regelaktionen wie z. B. **Anhang löschen** hinzufügen.

Regeln sind in drei Stufen unterteilt und werden in der folgenden Reihenfolge ausgewertet:

- **Filterregeln** (1) – Diese Regeln werden vor den Spam-Schutz-, Virenschutz- und Phishing-Scans ausgewertet.
- **Regeln für Anhänge** (2) – Diese Regeln werden während eines Virenschutz-Scans ausgewertet.
- **Regeln für Ergebnisse** (3) – Diese Regeln werden nach den Spam-Schutz-, Virenschutz- und Phishing-Scans ausgewertet.

Regeln mit der gleichen Auswertungsstufe werden in der Reihenfolge ausgewertet, in der sie im Regelfenster angezeigt werden. Sie können die Reihenfolge nur für Regeln auf derselben Stufe anpassen. Wenn Sie mehrere Filterregeln verwenden, können Sie deren Reihenfolge festlegen. Sie können dagegen keine **Regeln für Dateianhänge** vor die **Filterregeln** verschieben, da die Schaltflächen **Nach oben**/**Nach unten** nicht verfügbar sind. Sie können also keine Regeln aus unterschiedlichen **Ebenen** mischen.

Die Spalte **Treffer** zeigt an, wie oft die Regel erfolgreich ausgeführt wurde. Wenn Sie das Kontrollkästchen links neben dem Namen einer Regel deaktivieren, wird die entsprechende Regel deaktiviert, bis Sie das Kontrollkästchen erneut aktivieren.



Klicken Sie auf **Zurücksetzen**, um den Zähler für die ausgewählte Regel zurückzusetzen (Spalte **Treffer**) Wählen Sie **Anzeigen** aus, um eine per ESET PROTECT Policy angewendete Konfiguration anzuzeigen.

Wenn die Bedingungen einer Regel erfüllt sind, endet normalerweise die Auswertung von Regeln mit niedrigerer Priorität. Bei Bedarf können Sie jedoch eine spezielle Regelaktion mit dem Namen **Andere Regeln bewerten** verwenden, um die Auswertung fortzusetzen.

Die Überprüfung der Nachrichten mit Anwendung der Regeln erfolgt durch den Mail-Transport-Schutz, den Postfach-Datenbankschutz oder die On-Demand Postfachdatenbank-Scan. Jede Schutzebene verfügt über einen separaten Regelsatz.

Wenn die Regelbedingungen für den Postfach-Datenbankschutz oder die On-Demand Postfachdatenbank-Scan erfüllt sind, kann es passieren, dass der Regelzähler um 2 oder mehr erhöht wird. Die Schutzebenen greifen separat auf Text und Anhänge einer E-Mail zu, daher werden die Regeln für die verschiedenen Komponenten einzeln angewendet. Die Regeln für den Postfach-Datenbankschutz werden auch bei den Hintergrund-Scans (z. B. wenn ESET Mail Security nach dem Download einer neuen Erkennungsroutine einen Postfach-Scan ausführt) angewendet. Dadurch kann der Regel- bzw. Trefferzähler steigen.

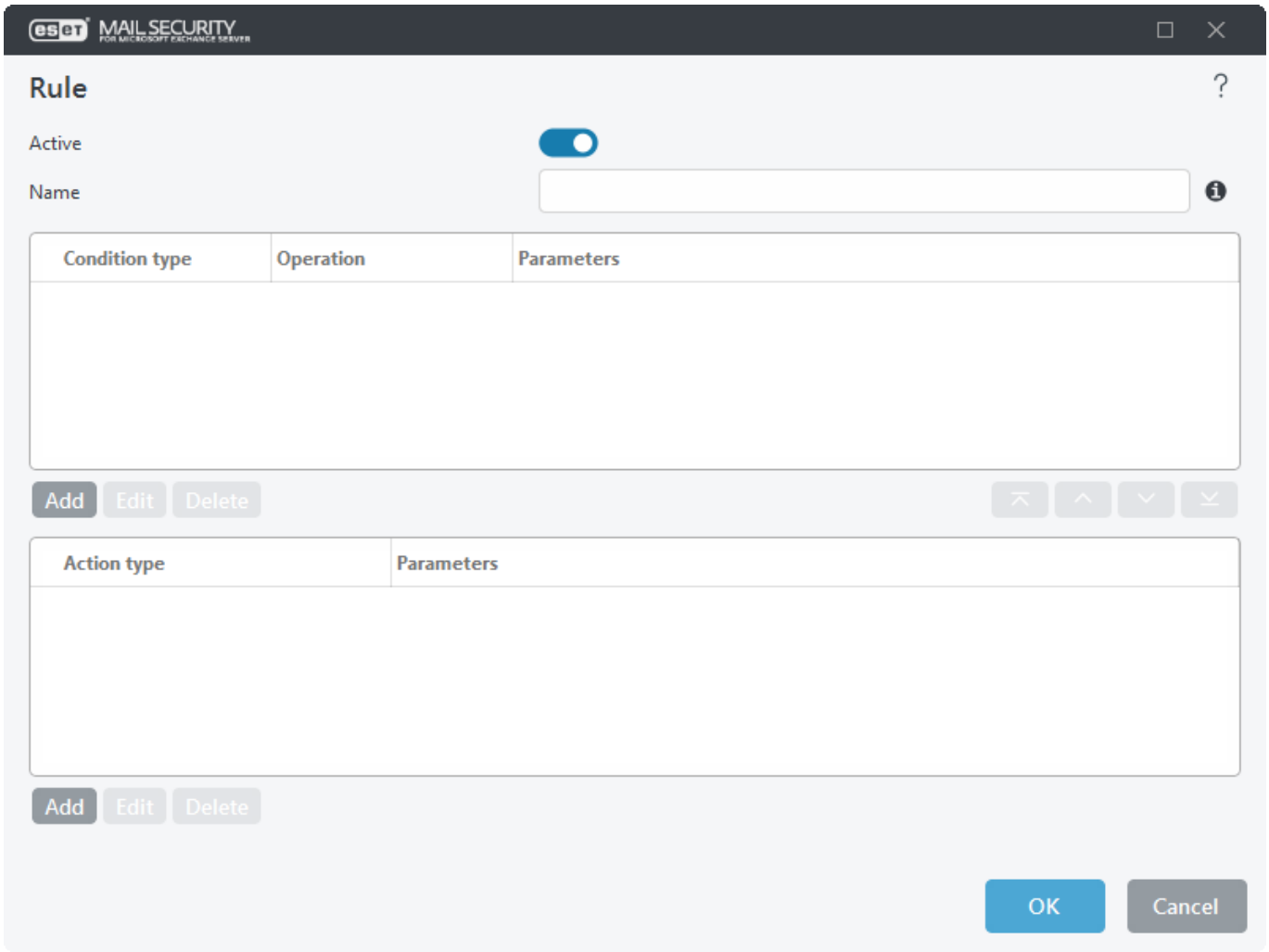
Regelassistent

1. Klicken Sie auf **Hinzufügen** (in der Mitte), um ein Fenster für Regelbedingungen zu öffnen, in dem Sie Bedingungstyp, Vorgang und Wert festlegen können. Definieren Sie zunächst Bedingungen, und anschließend Aktionen.

Sie können mehrere Bedingungen festlegen. In diesem Fall wird die Regel nur angewendet, wenn alle Bedingungen erfüllt sind. Alle Bedingungen werden mit dem logischen Operator **UND** verknüpft. Selbst wenn die meisten Bedingungen erfüllt sind und nur eine Bedingung nicht erfüllt ist, gilt das Auswertungsergebnis als *nicht erfüllt* und die Aktion für die Regel wird nicht ausgeführt.

2. Klicken Sie unten auf **Hinzufügen**, um eine Regelaktion hinzuzufügen.

Sie können mehrere Aktionen für eine Regel hinzufügen.



3. Definieren Sie Bedingungen und Regeln, und geben Sie anschließend einen **Namen** ein, um die Regel leicht wiederzuerkennen. Dieser Name wird anschließend in der Regelliste angezeigt. Name ist ein Pflichtfeld. Falls dieses Feld rot hervorgehoben ist, geben Sie einen Regelnamen in das Textfeld ein und klicken Sie auf **OK**, um die Regel zu erstellen. Die rote Hervorhebung verschwindet nicht, nachdem Sie einen Regelnamen eingegeben haben, sondern erst, nachdem Sie auf **OK** geklickt haben.

4. Wenn Sie eine Regel für die spätere Verwendung vorbereiten möchten, können Sie den Schalter neben **Aktiv** anklicken, um die Regel zu deaktivieren. Um eine Regel zu aktivieren, aktivieren Sie das Kontrollkästchen neben der entsprechenden Regel.

Wenn eine neue Regel hinzugefügt oder eine vorhandene Regel bearbeitet wird, beginnt automatisch ein erneuter E-Mail-Scan mit den neuen bzw. geänderten Regeln.

Unter Regelbeispiele erfahren Sie, wie Sie die Regeln anwenden können.

Regelbedingung

Mit diesem Assistenten können Sie Bedingungen für eine Regel anlegen. Wählen Sie den **Bedingungstyp** und eine **Operation** im Dropdownmenü aus. Die Liste der Operationen ändert sich je nach ausgewähltem Regeltyp. Wählen

Sie anschließend einen **Parameter** aus. Die Parameterfelder ändern sich je nach ausgewähltem Regeltyp und Vorgang.

Wählen Sie beispielsweise Dateigröße > ist größer als aus und geben Sie im Feld Parameter den Wert 10 MB ein. Mit dieser Einstellung werden alle Nachrichten mit einem Anhang größer als 10 MB mit den Regelaktionen verarbeitet, die Sie ausgewählt haben. Wählen Sie daher die gewünschte Aktion beim Auslösen der Regel aus, falls Sie dies beim Festlegen der Parameter für die Regel noch nicht getan haben.

Falls Sie eine eigene Liste aus einer Datei importieren möchten, anstatt die Einträge manuell anzulegen, klicken Sie mit der rechten Maustaste in die Fenstermitte und wählen Sie **Importieren** im Kontextmenü aus. Navigieren Sie anschließend zu Ihrer Datei (*.xml* oder *.txt* mit den Einträgen (durch Zeilenumbrüche getrennt), die Sie zur Liste hinzufügen möchten. Außerdem können Sie Ihre vorhandene Liste in eine Datei exportieren, indem Sie den Eintrag **Exportieren** im Kontextmenü auswählen.

Alternativ können Sie einen **regulären Ausdruck** angeben und die **Operation Treffer für regulären Ausdruck** oder **Kein Treffer für regulären Ausdruck** auswählen.

ESET Mail Security verwendet std::regex. Weitere Informationen zu regulären Ausdrücken finden Sie in der ECMAScript-Syntax. Die Syntax für reguläre Ausdrücke unterscheidet nicht zwischen Groß- und Kleinschreibung, einschließlich der Suchergebnisse.

Sie können mehrere Bedingungen festlegen. In diesem Fall wird die Regel nur angewendet, wenn alle Bedingungen erfüllt sind. Alle Bedingungen werden mit dem logischen Operator **UND** verknüpft. Selbst wenn die meisten Bedingungen erfüllt sind und nur eine Bedingung nicht erfüllt ist, gilt das Auswertungsergebnis als *nicht erfüllt* und die Aktion für die Regel wird nicht ausgeführt.

Die folgenden Bedingungstypen sind für den Mail-Transport-Schutz, den Postfach-Datenbankschutz und für die On-Demand Postfachdatenbank-Scan verfügbar (je nach ausgewählten Bedingungen werden möglicherweise nicht alle Optionen angezeigt):

Bedingungsname	Mail-Transport-Schutz	Postfachdatenbank-Schutz	On-Demand Postfachdatenbank-Scan	Beschreibung
Betreff	✓	✓	✓	Gilt für Nachrichten, deren Betreff eine bestimmte Zeichenfolge (bzw. einen regulären Ausdruck) enthält bzw. nicht enthält.
Absender	✓	✓	✓	Gilt für Nachrichten von einem bestimmten Absender.
Umschlag-Absender (SMTP-Absender)	✓	?	?	„MAIL FROM“-Umschlagattribut für die SMTP-Verbindung. Wird auch für die SPF-Verifizierung verwendet.
IP-Adresse des Absenders	✓	?	?	Gilt für Nachrichten von einer bestimmten Absender-IP-Adresse.
Domäne des Umschlag-Absenders/Domäne des Absenders	✓	✓	✓	Gilt für Nachrichten von Absendern mit einer bestimmten Domäne in der E-Mail-Adresse.
SMTP-Domäne des Absenders	✓	?	?	Gilt für Nachrichten von Absendern mit einer bestimmten Domäne in der E-Mail-Adresse.

Bedingungsname	Mail-Transport-Schutz	Postfachdatenbank-Schutz	On-Demand Postfachdatenbank-Scan	Beschreibung
Absender-Header – Adresse	✓	☐	☐	"From:"-Wert aus den Nachrichtenheadern. Diese Adresse wird dem Empfänger angezeigt. Allerdings wird nicht überprüft, ob das sendende System dazu berechtigt ist, im Namen dieser Adresse zu senden. Dieser Wert wird oft verwendet, um einen falschen Absender vorzutäuschen.
Absender-Header – Anzeigename	✓	☐	☐	"From:"-Wert aus den Nachrichtenheadern. Dieser Anzeigename wird dem Empfänger angezeigt. Allerdings wird nicht überprüft, ob das sendende System dazu berechtigt ist, im Namen dieser Adresse zu senden. Dieser Wert wird oft verwendet, um einen falschen Absender vorzutäuschen.
Empfänger	✓	✓	✓	Gilt für Nachrichten an einen bestimmten Empfänger.
Organisationseinheiten des Empfängers	✓	☐	☐	Gilt für Nachrichten an Empfänger in einer bestimmten Organisationseinheit.
Ergebnis der Empfängerprüfung	✓	☐	☐	Gilt für Nachrichten an Empfänger, die in Active Directory überprüft wurden.
Name des Anhangs	✓	✓	✓	Gilt für Nachrichten, die Anhänge mit einem bestimmten Namen enthalten.
Größe des Anhangs	✓	✓	✓	Gilt für Nachrichten, deren Anhang eine bestimmte Größe nicht erfüllt, in einem angegebenen Bereich zwischen zwei Größen liegt oder eine bestimmte Größe überschreitet.
Art des Anhangs[1]	✓	✓	✓	Gilt für Nachrichten mit einem bestimmten Dateityp als Anhang. Dateitypen sind zur einfachen Auswahl in Gruppen geordnet. Sie können mehrere Dateitypen oder ganze Kategorien auswählen. ESET Mail Security erkennt den tatsächlichen Dateityp unabhängig von der Dateierweiterung. Dasselbe gilt für den Inhalt eines Archivs.

Bedingungsname	Mail-Transport-Schutz	Postfachdatenbank-Schutz	On-Demand Postfachdatenbank-Scan	Beschreibung
Nachrichtengröße	✓	☐	☐	Gilt für Nachrichten mit Anhängen, die eine bestimmte Größe nicht erfüllen, in einem angegebenen Bereich zwischen zwei Größen liegen oder eine bestimmte Größe überschreiten.
Postfach	☐	✓	☐	Gilt für Nachrichten in einem bestimmten Postfach.
Nachrichtenköpfe	✓	✓	☐	Gilt für Nachrichten mit bestimmten Daten im Nachrichtenheader.
Nachrichtentext	✓	☐	✓	Der Nachrichtentext wird nach dem angegebenen Satz durchsucht. Mit der Funktion „HTML-Tags entfernen“ können Sie HTML-Tags, Attribute und Werte entfernen und nur den Text beibehalten. Anschließend wird der Nachrichtentext durchsucht.
Interne Nachricht	✓	☐	☐	Gilt für interne bzw. nicht interne Nachrichten.
Ausgehende Nachricht	✓	☐	☐	Gilt für ausgehende Nachrichten.
Signierte Nachricht	✓	☐	☐	Gilt für signierte Nachrichten.
Verschlüsselte Nachricht	✓	☐	☐	Gilt für verschlüsselte Nachrichten.
Scan-Ergebnis des Spam-Schutzes	✓	☐	☐	Gilt für Nachrichten, die als Ham oder Spam markiert bzw. nicht markiert wurden.
Scan-Ergebnis des Virenschutzes	✓	✓	✓	Gilt für Nachrichten, die bösartig bzw. nicht bösartig markiert wurden.
Scan-Ergebnis des Phishing-Schutzes	✓	☐	✓	Gilt für Nachrichten, die als Phishing klassifiziert wurden.
Uhrzeit des Empfangs	✓	✓	✓	Gilt für Nachrichten, die vor oder nach einem bestimmten Zeitpunkt oder während eines angegebenen Zeitintervalls empfangen wurden.
Enthält passwortgeschütztes Archiv	✓	✓	☐	Gilt für Nachrichten mit Archivanhängen, die mit einem Passwort geschützt sind.
Enthält beschädigtes Archiv	✓	✓	☐	Gilt für Nachrichten mit beschädigtem Archivanhang (kann verm. nicht geöffnet werden).
Anhang ist ein passwortgeschütztes Archiv	☐	☐	✓	Gilt für Anhänge, die mit einem Passwort geschützt sind.
Anhang ist ein beschädigtes Archiv	☐	☐	✓	Gilt für beschädigte Anhänge (kann verm. nicht geöffnet werden).

Bedingungsname	Mail-Transport-Schutz	Postfachdatenbank-Schutz	On-Demand Postfachdatenbank-Scan	Beschreibung
Ordnername	☐	☐	✓	Gilt für Nachrichten in einem bestimmten Ordner. Falls der Ordner nicht existiert, wird er erstellt. Gilt nicht für öffentliche Ordner.
DKIM ergebnis	✓	☐	☐	Gilt für Nachrichten mit bestandener bzw. fehlgeschlagener DKIM-Prüfung, alternativ falls nicht verfügbar.
SPF ergebnis	✓	☐	☐	Gilt für Nachrichten mit dem SPF-Auswertungsergebnis: • **Bestanden** – Die IP-Adresse wird für den Versand von der Domain autorisiert (SPF-Kennzeichner "+") • **Nicht bestanden** – Der Server oder die IP-Adresse des Absenders ist nicht im SPF-Eintrag enthalten (SPF-Kennzeichner "-") • **Behebbarer Fehler** – Die IP-Adresse wird möglicherweise für den Versand von der Domain autorisiert (SPF-Kennzeichner "~") • **Neutral** – Der Domain-Eigentümer hat im SPF-Eintrag angegeben, dass die IP-Adresse nicht für den Versand von der Domain autorisiert werden soll (SPF-Kennzeichner "?") • **Nicht verfügbar** – Das SPF-Ergebnis None bedeutet, dass die Domain keine Einträge veröffentlicht hat oder dass keine überprüfbare Absender-Domain für die angegebene Identität gefunden wurde. Unter RFC 4408 finden Sie weitere Details zu SPF. Falls Sie SPF-Ergebnisse verwenden, werden die Positivlisten im Bereich Filterung und Verifizierung für die Regeln nicht berücksichtigt.
DMARC ergebnis	✓	☐	☐	Gilt für Nachrichten mit bestandener bzw. fehlgeschlagener SPF-, DKIM- oder beiden Prüfungen, alternativ falls nicht verfügbar.
Hat Reverse-DNS-Eintrag	✓	☐	☐	Gilt für Nachrichten mit einer Absenderdomäne, die einen Reverse-DNS-Eintrag hat.

Bedingungsname	Mail-Transport-Schutz	Postfachdatenbank-Schutz	On-Demand Postfachdatenbank-Scan	Beschreibung
NDR ergebnis	✓	☐	☐	Gilt für Nachrichten mit fehlgeschlagener NDR-Prüfung.
SPF-Ergebnis - From-Header	✓	☐	☐	Gilt für Nachrichten mit dem SPF-Auswertungsergebnis: • **Bestanden** – Die IP-Adresse wird für den Versand von der Domain autorisiert (SPF-Kennzeichner "+") • **Nicht bestanden** – Der Server oder die IP-Adresse des Absenders ist nicht im SPF-Eintrag enthalten (SPF-Kennzeichner "-") • **Behebbarer Fehler** – Die IP-Adresse wird möglicherweise für den Versand von der Domain autorisiert (SPF-Kennzeichner "~") • **Neutral** – Der Domain-Eigentümer hat im SPF-Eintrag angegeben, dass die IP-Adresse nicht für den Versand von der Domain autorisiert werden soll (SPF-Kennzeichner "?") • **Nicht verfügbar** – Das SPF-Ergebnis None bedeutet, dass die Domain keine Einträge veröffentlicht hat oder dass keine überprüfbare Absender-Domain für die angegebene Identität gefunden wurde. Unter RFC 4408 finden Sie weitere Details zu SPF. Falls Sie SPF-Ergebnisse verwenden, werden die Positivlisten im Bereich Filterung und Verifizierung für die Regeln nicht berücksichtigt.
Vergleichsergebnis zwischen Umschlag-Absender und From-Header	✓	☐	☐	Vergleicht die Domäne(n) in der "From:"-Kopfzeile der E-Mail und den Absender des Umschlags mit den Domänenlisten.

Bedingungsname	Mail-Transport-Schutz	Postfachdatenbank-Schutz	On-Demand Postfachdatenbank-Scan	Beschreibung
SPF-ErgebnisHELO	✓	?	?	Gilt für Nachrichten mit dem HELO-Auswertungsergebnis: • **Bestanden** – Die IP-Adresse wird für den Versand von der Domain autorisiert (SPF-Kennzeichner "+") • **Nicht bestanden** – Der Server oder die IP-Adresse des Absenders ist nicht im SPF-Eintrag enthalten (SPF-Kennzeichner "-") • **Behebbarer Fehler** – Die IP-Adresse wird möglicherweise für den Versand von der Domain autorisiert (SPF-Kennzeichner "~") • **Neutral** – Der Domain-Eigentümer hat im SPF-Eintrag angegeben, dass die IP-Adresse nicht für den Versand von der Domain autorisiert werden soll (SPF-Kennzeichner "?") • **Nicht verfügbar** – Das SPF-Ergebnis None bedeutet, dass die Domain keine Einträge veröffentlicht hat oder dass keine überprüfbare Absender-Domain für die angegebene Identität gefunden wurde. Unter RFC 4408 finden Sie weitere Details zu SPF. Falls Sie SPF-Ergebnisse verwenden, werden die Positivlisten im Bereich Filterung und Verifizierung für die Regeln nicht berücksichtigt.

[1] Für die Regelbedingung **Art des Anhangs** gilt eine bekannte Einschränkung: Die ESET Mail Security Erkennungsroutine kann zusätzliche kleine Textdateien mit einer Länge von weniger als 10 Byte in ASCII/ANSI-Codierung nicht erkennen.

Der Bedingungstyp unterstützt die folgenden **Operationen**:

- **Zeichenfolge:** ist, ist nicht, enthält, enthält nicht, stimmt überein, stimmt nicht überein, enthalten in, nicht enthalten in, ist in der Liste, ist nicht in der Liste, Treffer für regulären Ausdruck, kein Treffer für regulären Ausdruck
- **Zahl:** ist weniger als, ist größer als, ist zwischen
- **Text:** enthält, enthält nicht, stimmt überein, stimmt nicht überein
- **Zeitstempel:** ist niedriger als, ist größer als, ist zwischen
- **Enum:** ist, ist nicht, enthalten in, nicht enthalten in

Wenn der **Anhangsname** oder **Anhangstyp** eine Microsoft Office-Datei ist, wird diese von ESET Mail Security als Archiv behandelt. In diesem Fall wird der Inhalt extrahiert, und jede Datei im Office-Dateiarchiv (z. B. *.docx*, *.xlsx*, *.xltx*, *.pptx*, *.ppsx*, *.potx* usw.) wird separat geprüft.

Wenn Sie den **Virenschutz** im Setup-Menü oder unter **Erweiterte Einstellungen** (F5) > **Server** > **Viren- und Spyware-Schutz** für die **E-Mail-Transportebene und die Postfach-Datenbankschutzebene** deaktivieren, sind die folgenden Regelbedingungen betroffen:

- Name des Anhangs
- Größe des Anhangs
- Art des Anhangs
- Scan-Ergebnis des Virenschutzes
- Anhang ist passwortgeschützt
- Anhang ist ein beschädigtes Archiv
- Enthält beschädigtes Archiv
- Enthält passwortgeschütztes Archiv

Regelaktionen

Sie können Aktionen für Nachrichten und/oder Anhänge hinzufügen, die die Regelbedingungen erfüllen.

Sie können mehrere Aktionen für eine Regel hinzufügen.

Die Liste der verfügbaren Aktionen für den Mail-Transport-Schutz, den Postfach-Datenbankschutz und die On-Demand Postfachdatenbank-Scan (je nach ausgewählten Bedingungen werden möglicherweise nicht alle Optionen angezeigt):

Aktionsname	Mail-Transport-Schutz	Postfachdatenbank-Schutz	On-Demand Postfachdatenbank-Scan	Beschreibung
E-Mail in Quarantäne verschieben	✓	?	?	Die Nachricht wird nicht an den Empfänger zugestellt, sondern stattdessen in die E-Mail-Quarantäne verschoben. Nicht-Administratoren können E-Mails freigeben, die von dieser Regel in die Quarantäne verschoben wurden (über die Web-Oberfläche oder über Quarantäneberichte).
Quarantäne-Anhang	✓	✓	✓	Verschiebt den E-Mail-Anhang in die Datei-Quarantäne. Die E-Mail wird an den Empfänger zugestellt, und der Anhang wird auf Nulllänge abgeschnitten.

Aktionsname	Mail-Transport-Schutz	Postfachdatenbank-Schutz	On-Demand Postfachdatenbank-Scan	Beschreibung
Anhang löschen	✓	✓	✓	Löscht einen Nachrichtenanhang. Die Nachricht wird ohne Anhang an den Empfänger zugestellt.
Nachricht ablehnen	✓	⍰	⍰	Löscht eine Nachricht. Für per SMTP empfangene E-Mails sollte der Absenderserver einen Unzustellbarkeitsbericht (Non-Delivery Report, NDR) generieren.
Nachricht automatisch löschen	✓	⍰	⍰	Die Nachricht wird ohne NDR gelöscht.
SCL-Wert festlegen	✓	⍰	⍰	Ändert einen bestimmten SCL-Wert bzw. legt diesen fest.
Ereignisbenachrichtigung an Administrator senden	✓	✓	✓	Schickt Ereignisbenachrichtigungen an den unter E-Mail-Benachrichtigungen festgelegten Empfänger. Dazu müssen Sie die Option Ereignisbenachrichtigungen per E-Mail versenden aktivieren. Anschließend können Sie das Format der Ereignisnachrichten anpassen (In der QuickInfo werden Vorschläge angezeigt) und die Regel erstellen. Außerdem können Sie den Umfang der Ereignisnachrichten auswählen. Diese Einstellung hängt jedoch von der Mindestinformation ab, die im Bereich E-Mail-Benachrichtigungen festgelegt wurde.
E-Mail-Benachrichtigung verschicken				Schickt E-Mail-Benachrichtigungen an den unter E-Mail-Benachrichtigungen festgelegten Empfänger.
Scan des Spam-Schutzes überspringen	✓	⍰	⍰	Die Nachricht wird nicht vom Spam-Schutz-Modul geprüft.
Scan des Virenschutzes überspringen	✓	✓	✓	Die Nachricht wird nicht vom Antivirenprogramm geprüft.
Scan des Phishing-Schutzes überspringen	✓	⍰	✓	Die Nachricht wird nicht vom Phishing-Schutz geprüft.
ESET LiveGuard Advanced-Scan überspringen	✓	⍰	⍰	Nachricht wird vom ESET LiveGuard Advanced-Schutz nicht geprüft.

Aktionsname	Mail-Transport-Schutz	Postfachdatenbank-Schutz	On-Demand Postfachdatenbank-Scan	Beschreibung
Andere Regeln bewerten	✓	✓	✓	Mit der Auswertung weiterer Regeln können Benutzer verschiedene Sätze von Bedingungen definieren und entsprechende Aktionen festlegen.
Logging in Ereignissen	✓	✓	✓	Schreibt Informationen über die angewendete Regel in das Programm-Log und legt das Format für die Ereignisnachrichten fest (In der QuickInfo werden Vorschläge angezeigt). Wenn Sie die Aktionsart Logging in Ereignissen für den Postfach-Datenbankschutz mit dem Parameter %IPAddress% konfigurieren, ist die Spalte Ereignis in den Log-Dateien für dieses Ereignis leer. Dies liegt daran, dass auf der Ebene des Postfach-Datenbankschutzes keine IP-Adresse existiert. Bestimmte Optionen sind nicht für alle Schutzebenen verfügbar: %IPAddress% – Wird von On-Demand Postfachdatenbank-Scan und Postfach-Datenbankschutz ignoriert %Mailbox% – wird vom Mail-Transport-Schutz ignoriert Die folgenden Optionen gelten nur für Regeln für Anhänge: %Attname% – Wird von Filterregeln und Regeln für Ergebnisse ignoriert %Attsize% – Wird von Filterregeln und Regeln für Ergebnisse ignoriert
Headerfeld hinzufügen	✓	☐	☐	Fügt eine benutzerdefinierte Zeichenfolge zu einem Nachrichtenheader hinzu.
Betreffpräfix hinzufügen	✓	☐	☐	Fügt ein Präfix zu einem Betreff hinzu.
Anhang durch Aktionsinformationen ersetzen	☐	✓	✓	Ersetzt den Anhang durch eine Textdatei mit ausführlichen Informationen zur ausgeführten Aktion.
Header-Felder entfernen	✓	☐	☐	Entfernt Felder gemäß der angegebenen Parameter aus dem Nachrichtenkopf.
E-Mail löschen	☐	✓	✓	Löscht eine infizierte Nachricht.
Nachricht in Ordner verschieben	☐	☐	✓	Die Nachricht wird in den angegebenen Ordner verschoben.

Aktionsname	Mail-Transport-Schutz	Postfachdatenbank-Schutz	On-Demand Postfachdatenbank-Scan	Beschreibung
Nachricht in Papierkorb verschieben	☐	☐	✓	Verschiebt eine E-Mail auf der Seite des E-Mail-Clients in den Papierkorb.
DMARC-Policy anwenden	✓	☐	☐	Wenn eine DMARC-Ergebnisbedingung erfüllt ist, wird die Nachricht gemäß der im DMARC DNS-Eintrag für die Domäne des Absenders festgelegten Richtlinie behandelt.

Wenn Sie den **Virenschutz** im Setup-Menü oder unter **Erweiterte Einstellungen** (F5) > **Server** > **Viren- und Spyware-Schutz** für den **Mail-Transport-Schutz** deaktivieren, sind die folgenden Regelaktionen betroffen:

- Quarantäne-Anhang
- Anhang löschen

Regelbeispiele

Nachrichten in die Quarantäne verschieben, die Malware oder passwortgeschützte, verschlüsselte oder beschädigte Anhänge enthalten

Ziel: Nachrichten in die Quarantäne verschieben, die Malware oder passwortgeschützte, verschlüsselte oder beschädigte Anhänge enthalten
Erstellen Sie die folgende Regel für den **Mail-Transport-Schutz**
Bedingung
- Typ: Scan-Ergebnis des Virenschutzes
- Operation: ist nicht
- Parameter: Säubern

Aktion
Typ: E-Mail in Quarantäne verschieben

Nachrichten, die die SPF-Prüfung nicht bestehen, in einen Spam-Ordner verschieben

Ziel: Nachrichten, die die SPF-Prüfung nicht bestehen, in einen Spam-Ordner verschieben
Erstellen Sie die folgende Regel für den **Mail-Transport-Schutz**
Bedingung
- Typ: SPF-Ergebnis
- Operation: ist
- Parameter: Nicht bestanden

Aktion
- Typ: SCL-Wert festlegen
- Wert: 5

Definieren Sie den Wert gemäß des Parameters `SCLJunkThreshold` im Cmdlet `Get-OrganizationConfig` auf Ihrem Exchange-Server. Weitere Informationen finden Sie im Artikel Aktionen für SCL-Schwellenwerte)

E-Mail-Nachricht verifizieren, die von Absender-Spoofing betroffen sein könnte

Ziel: E-Mail-Nachricht verifizieren, die von Absender-Spoofing betroffen sein könnte. Falls die Nachricht ihre eigene Domäne in der „Von:“-Kopfzeile der E-Mail oder im Umschlag-Absender enthält, überprüfen Sie dies anhand des SPF-Ergebnisses weiter. Wenn das SPF-Ergebnis neutral ist, verschieben Sie die Nachricht in Quarantäne, nehmen Sie sie in das Ereignislog auf und benachrichtigen Sie den Administrator.

Bedingung

- Typ: Vergleichsergebnis zwischen Umschlag-Absender und From-Header
- Operation: ist
- Parameter: Übereinstimmung
- Typ: SPF-Ergebnis - From-Header
- Operation: ist
- Parameter: Neutral

Aktion

Typ: E-Mail in Quarantäne verschieben, Logging in Ereignissen und Ereignisbenachrichtigung an Administrator senden

Nachrichten von bestimmten Absendern löschen

Ziel: Nachrichten von bestimmten Absendern löschen
Erstellen Sie die folgende Regel für den **Mail-Transport-Schutz**

Bedingung

- Typ: Absender
- Operation: ist / ist Teil von
- Parameter: spammer1@domain.com, spammer2@domain.com

Aktion

Typ: **Nachricht automatisch löschen**

Liste blockierter IP-Adressen

Ziel: Nachricht von einer IP-Adresse in der Liste blockierter IP-Adressen in die Quarantäne verschieben, Administrator benachrichtigen und Ereignis protokollieren.
Details: Wenn eine E-Mail von einer IP-Adresse in der Liste blockierter IP-Adressen eingeht, verschiebt <%PM%> die Nachricht in die Quarantäne und benachrichtigt Sie per E-Mail. Anschließend können Sie die Nachricht aus der Quarantäne freigeben oder dauerhaft löschen. Andernfalls würde <%PM%> die Nachricht löschen, ohne Ihnen weitere Optionen anzubieten.
Öffnen **Mail-Transportschutz**

Bedingung

- Typ: IP-Adresse des Absenders
- Vorgang: Ist in der Liste
- Liste: Liste blockierter IP-Adressen

Aktion

Typ: E-Mail in Quarantäne verschieben, Logging in Ereignissen und Ereignisbenachrichtigung an Administrator senden

Vordefinierte Regel anpassen

Ziel: Vordefinierte Regel anpassen
Details: Archivanhänge in Nachrichten von bestimmten IP-Adressen werden erlaubt (z. B. für interne Systeme), während gleichzeitig die Regel für verbotene Archivdatei-Anhänge angewendet wird.
Öffnen Sie den Regelsatz **Mail-Transport-Schutz**, wählen Sie **Verbotene Archivdatei-Anhänge** aus und klicken Sie auf **Bearbeiten**.
Bedingung
- Typ: IP-Adresse des Absenders
- Operation: ist nicht / ist nicht Teil von
- Parameter: 1.1.1.2, 1.1.1.50-1.1.1.99

Nachrichtentext

Ziel: Nachrichten in die Quarantäne verschieben, die eine bestimmte Zeichenfolge im Nachrichtentext enthalten
Erstellen Sie die folgende Regel für den **Mail-Transport-Schutz**
Bedingung
- Typ: Nachrichtentext
- Operation: enthält, klicken Sie auf **Hinzufügen**, und geben Sie eine Website-URL oder einen Teil einer URL ein.

Aktion
Typ: E-Mail in Quarantäne verschieben

Nachrichten für nicht vorhandene Empfänger speichern

Ziel: Nachrichten für nicht vorhandene Empfänger speichern
Details: Wenn Sie alle Nachrichten an nicht vorhandene Empfänger in die Quarantäne verschieben möchten (unabhängig von der Markierung durch Viren- oder Spam-Schutz)
Bedingung
- Typ: Ergebnis der Empfängerprüfung
- Operation: ist
- Parameter: Enthält ungültigen Empfänger

Aktion
Typ: E-Mail in Quarantäne verschieben

Mail-Transport-Schutz

Sie können Aktionen für erkannte Bedrohungen auf der Transportebene für jedes ESET Mail Security-Modul (Virenschutz, Phishing-Schutz und Spam-Schutz) separat konfigurieren.

Auszuführende Aktionen, falls keine Säuberung möglich ist:

- **Keine Aktion** – Infizierte E-Mails, die nicht gesäubert werden können, bleiben erhalten
- **Nachricht in Quarantäne verschieben** – Infizierte Nachrichten werden in das Quarantäne-Postfach verschoben.
- **Nachricht ablehnen** – Infizierte E-Mails werden abgelehnt
- **Nachricht automatisch löschen** - E-Mails werden ohne Unzustellbarkeitsbericht gelöscht

Wenn Sie **Keine Aktion** auswählen und Ihre **Säuberungsstufe** in den ThreatSense Parametern für den Viren- und Spyware-Schutz auf **Nicht säubern** festgelegt ist, wird der Schutzstatus in gelb angezeigt. Dies liegt daran, dass diese Kombination ein Sicherheitsrisiko darstellt und nicht verwendet werden sollte. Ändern Sie eine der Einstellungen, um sich optimal zu schützen.

Auszuführende Aktion für Phishing-Nachrichten:

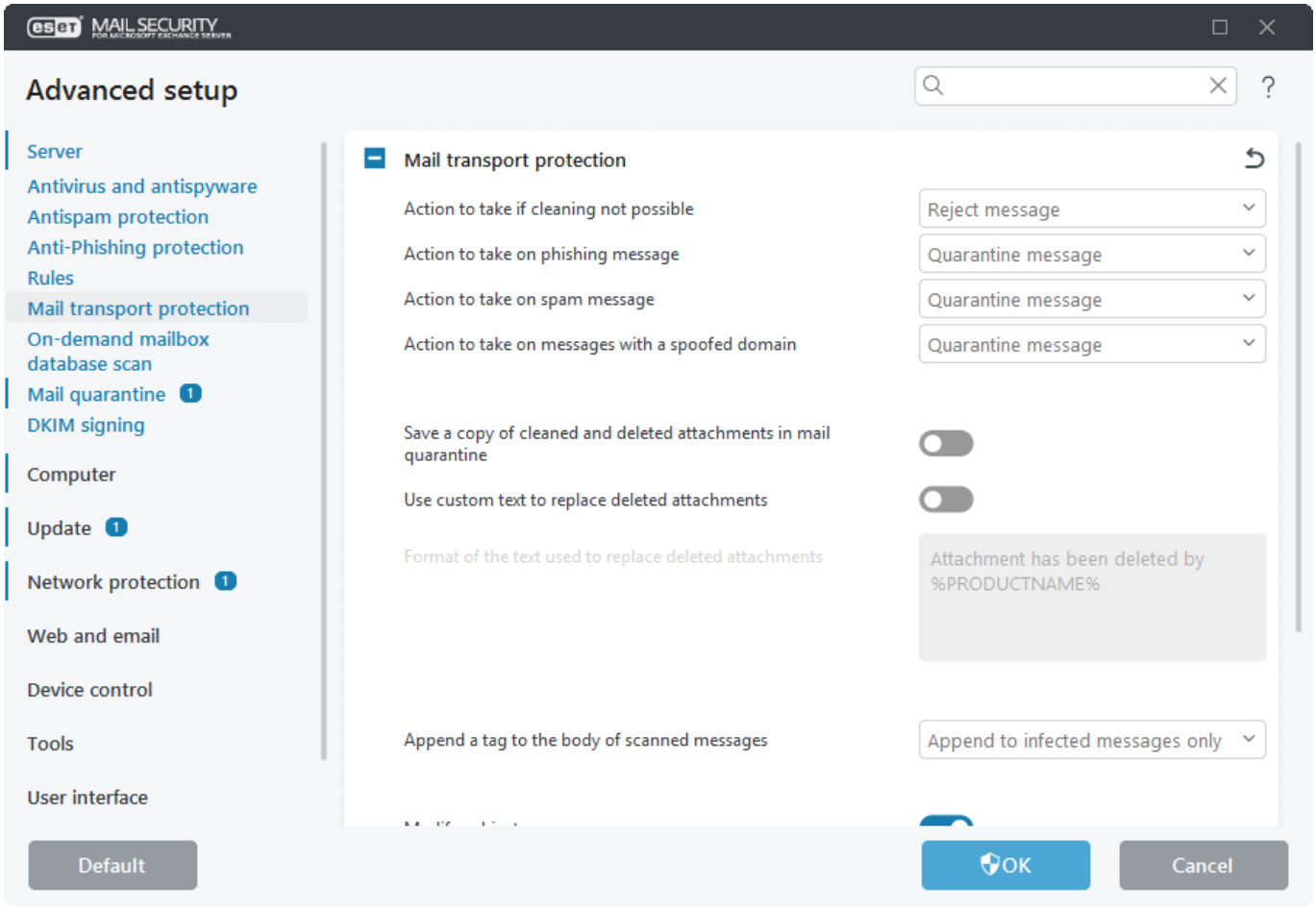
- **Keine Aktion** – Nachrichten werden beibehalten.
- **Nachricht in Quarantäne verschieben** – Als Phishing eingestufte Nachrichten werden in das Quarantäne-Postfach verschoben.
- **Nachricht ablehnen** – Als Phishing eingestufte E-Mails werden abgelehnt
- **Nachricht automatisch löschen** - E-Mails werden ohne Unzustellbarkeitsbericht gelöscht

Auszuführende Aktion bei Spam-E-Mails:

- **Keine Aktion** – Nachrichten werden beibehalten.
- **Nachricht in Quarantäne verschieben** – Als Spam eingestufte Nachrichten werden in das Quarantäne-Postfach verschoben.
- **Nachricht ablehnen** – Als Spam eingestufte E-Mails werden abgelehnt
- **Nachricht automatisch löschen** - E-Mails werden ohne Unzustellbarkeitsbericht gelöscht

Aktion für Nachrichten mit gefälschter Domäne:

- **Keine Aktion** – Nachrichten werden beibehalten.
- **Nachricht in Quarantäne verschieben** – Als gefälscht eingestufte E-Mails werden in das Quarantäne-Postfach verschoben.
- **Nachricht ablehnen** – Als gefälscht eingestufte E-Mails werden abgelehnt.
- **Nachricht automatisch löschen** - E-Mails werden ohne Unzustellbarkeitsbericht gelöscht



Kopie von gesäuberten und gelöschten Anhängen in der E-Mail-Quarantäne speichern

Eine Kopie des ursprünglichen Dateianhangs wird in der E-Mail-Quarantäne gespeichert.

Gelöschte Anhänge durch benutzerdefinierten Text ersetzen

Wenn diese Option aktiviert ist, können Sie einen benutzerdefinierten Text eingeben, mit dem die gelöschten Anhänge ersetzt werden.

Format des Texts zum Ersetzen gelöschter Anhänge

Ersetzt den Anhang durch eine Textdatei mit ausführlichen Informationen zur ausgeführten Aktion. Wenn Sie die obige Einstellung aktiviert haben (**Benutzerdefinierten Text verwenden**), können Sie den Standardtext bei Bedarf mit benutzerdefinierten Details und Variablen anpassen.

Fügen Sie Variablen in Ihren benutzerdefinierten Text ein, die als Ersatz für die gelöschten Anhänge in einer E-Mail-Nachricht verwendet werden.
%PRODUCTNAME%
%FILENAME%
%VIRUSNAME%
%DETECTIONNAME%
%FILESIZE%
Anhang %FILENAME% mit einer Größe von %FILESIZE% wurde von %PRODUCTNAME% wegen %DETECTIONNAME% gelöscht.
Im benutzerdefinierten Textformat wird die folgende Ausgabe angezeigt:
Anhang eicar_com.zip mit einer Größe von 184 B wurde von ESET Mail Security aufgrund der Eicar test-Datei gelöscht.

SMTP-Ablehnungsantwort

Sie können **Antwortcode**, **Statuscode** und **Antwortnachricht** an den SMTP-Server für die vorübergehende Ablehnung einer E-Mail festlegen. Sie können eine Antwortnachricht in folgendem Format verfassen:

Antwortcode	Statuscode	Antwortnachricht
250	2.5.0	Angeforderte E-Mail-Aktion OK, abgeschlossen
451	4.5.1	Angeforderte Aktion abgebrochen:lokaler Verarbeitungsfehler
550	5.5.0	Angeforderte Aktion unterlassen:Postfach nicht verfügbar
554	5.6.0	Ungültiger Inhalt

Für die Konfiguration von SMTP-Rejects können Sie auch Systemvariablen verwenden.

Nachricht zum Text der geprüften E-Mails hinzufügen bietet drei Optionen:

- **Nicht an Nachrichten anhängen** – Informationen werden nicht hinzugefügt.
- **Nur an infizierte Nachrichten anhängen** – Betrifft nur infizierte Nachrichten.
- **An alle Nachrichten anhängen** (gilt nicht für interne Nachrichten) – Alle Nachrichten werden markiert.

Betreff ändern

Mit dieser Option können Sie die Vorlagen bearbeiten, die zur Betreffzeile infizierter E-Mails sowie zu Spam- oder Phishing-Nachrichten hinzugefügt werden.

Text, der zur Betreffzeile infizierter E-Mails hinzugefügt wird

ESET Mail Security hängt einen Hinweis an den E-Mail-Betreff an. Der Hinweis ist im Textfeld **Vorlage für Text, der zur Betreffzeile von infizierter E-Mails hinzugefügt wird** hinterlegt (der Standardtext lautet `[found threat %VIRUSNAME%]`). Mit dieser Änderung können Sie die Filterung infizierter Nachrichten automatisieren, indem z. B. E-Mails mit einem bestimmten Betreff anhand von Regeln oder direkt im Client (falls der E-Mail-Client dies unterstützt) gefiltert und in einem separaten Ordner abgelegt werden.

Text, der zur Betreffzeile von Spam-E-Mails hinzugefügt wird

ESET Mail Security hängt einen Hinweis an den E-Mail-Betreff an. Der Hinweis ist im Textfeld **Vorlage für Text, der zur Betreffzeile von Spam-E-Mails hinzugefügt wird** hinterlegt (der Standardtext lautet `[SPAM]`). Mit dieser Änderung kann der Spamfilter automatisiert werden, indem z. B. E-Mails mit einem bestimmten Betreff anhand von Regeln oder direkt im Client (falls der Client dies unterstützt) gefiltert und in einem separaten Ordner abgelegt werden.

Text, der zur Betreffzeile von Phishing-Nachrichten hinzugefügt wird

ESET Mail Security hängt einen Hinweis an den E-Mail-Betreff an. Der Hinweis ist im Textfeld **Vorlage für Text, der zur Betreffzeile von Phishing-Mails hinzugefügt wird** hinterlegt (der Standardtext lautet `[PHISH]`). Mit dieser Änderung kann der Spamfilter automatisiert werden, indem z. B. E-Mails mit einem bestimmten Betreff anhand von Regeln oder direkt im Client (falls der Client dies unterstützt) gefiltert und in einem separaten Ordner abgelegt werden.

Im Text, der zum Betreff hinzugefügt wird, können Sie auch Systemvariablen verwenden.

Mail-Transport-Schutz – Erweiterte Einstellungen

Sie können die Einstellungen für den Mail-Transportschutz anpassen.

E-Mails von authentifizierten oder internen Verbindungen ebenfalls prüfen mit

Sie können auswählen, wie Nachrichten von authentifizierten Quellen oder lokalen Servern gescannt werden sollen. Das Scannen dieser Nachrichten wird empfohlen, um den Schutz zu verbessern, und ist erforderlich, wenn Sie den integrierten Microsoft SBS POP3 Connector zum Abrufen von E-Mails von externen POP3-Servern oder E-Mail-Diensten (wie etwa Gmail.com, Outlook.com, Yahoo.com oder gmx.de) nutzen. Weitere Informationen finden Sie unter POP3-Connector und Spam-Schutz.

Wählen Sie eine Schutzebene im Dropdownmenü aus. Wir empfehlen die Option **Virenschutz** (Standardeinstellung), insbesondere für interne Verbindungen, da es unwahrscheinlich ist, dass Ihre lokalen Server Phishing- oder Spam-Nachrichten verteilen. Sie können jedoch den Schutz für den Microsoft SBS POP3 Connector verbessern, indem Sie **Viren- und Phishing-Schutz** oder sogar **Viren-, Phishing- und Spam-Schutz**.

> Diese Einstellung aktiviert/deaktiviert den Spam-Schutz für authentifizierte Benutzer und interne Verbindungen. E-Mails von nicht authentifizierten Verbindungen werden immer gescannt, auch wenn Sie **Nicht scannen** auswählen.

> Interne Outlook-E-Mails innerhalb der Organisation werden im TNEF-Format verschickt (Transport Neutral Encapsulation Format). TNEF wird vom Spam-Schutz nicht unterstützt. Daher werden interne E-Mails im TNEF-Format nicht auf Spam gescannt, unabhängig von der Einstellung unter **E-Mails von authentifizierten oder internen Verbindungen ebenfalls scannen mit**.

Vorhandenen SCL-Header vor der Prüfung entfernen

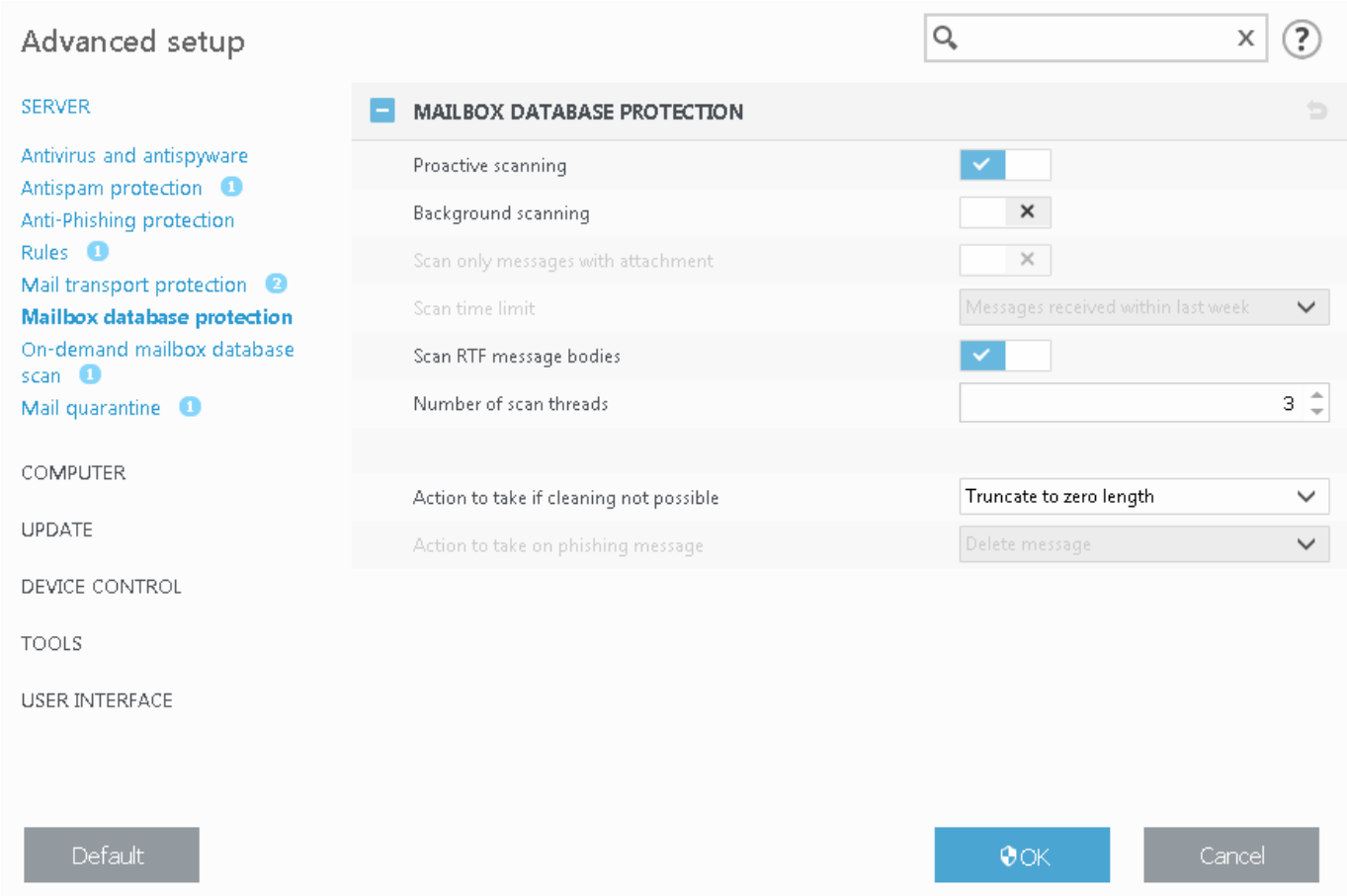
Diese Option ist standardmäßig aktiviert. Deaktivieren Sie diese Option bei Bedarf, um den Spam Confidence Level (SCL)-Header zu behalten.

Scan-Ergebnisse in Nachrichtenköpfe schreiben

Mit dieser Option werden die Scan-Ergebnisse in die Nachrichtenköpfe geschrieben. Diese Nachrichtenköpfe beginnen mit `X_ESET`, um die Erkennung zu erleichtern (z. B. `X_EsetResult` oder `X_ESET_Antispam`).

Postfachdatenbank-Schutz

Wenn die Option **Proaktiver Scan** aktiviert ist, werden neue eingehende E-Mails in der Eingangsreihenfolge geprüft. Wenn diese Option deaktiviert ist und ein Benutzer eine ungeprüfte E-Mail öffnet, wird diese Nachricht vor den anderen E-Mails in der Warteschlange geprüft.



Hintergrund-Scan

Ermöglicht die Prüfung aller E-Mails im Hintergrund (die Prüfung wird im Speicherbereich für Postfächer und öffentliche Ordner ausgeführt, z. B. in der Exchange-Datenbank. Microsoft Exchange Server entscheidet anhand verschiedener Faktoren, ob eine Hintergrundprüfung durchgeführt wird. Dazu zählen die aktuelle Systemauslastung, die Anzahl der aktiven Benutzer usw. Microsoft Exchange Server protokolliert, welche E-Mails geprüft wurden und welche Signaturdatenbank verwendet wurde.

Wenn Sie eine E-Mail öffnen, die noch nicht mit der aktuellen Signaturdatenbank geprüft wurde, wird sie von Microsoft Exchange Server an ESET Mail Security gesendet. Sie können die Option **Nur E-Mails mit Anhang scannen** auswählen und die Nachrichten mit den folgenden Optionen unter Zeitlimit für Scan filtern:

- Alle E-Mails
- Innerhalb des letzten Jahres empfangene E-Mails
- Innerhalb der letzten 6 Monate empfangene E-Mails
- Innerhalb der letzten 3 Monate empfangene E-Mails
- Nachrichten aus dem letzten Monat
- Nachrichten aus der letzten Woche

Hintergrund-Scans können das System belasten (nach jedem Update der Erkennungsroutine findet ein Scan statt) und sollten daher nach Möglichkeit außerhalb der Geschäftszeiten stattfinden. Sie können die Hintergrundprüfung mit einem speziellen Task starten.

Wenn Sie einen Task für die Hintergrundprüfung erstellen, können Sie die Startzeit, Anzahl der Wiederholungen und andere Parameter im Taskplaner festlegen. Nach dem Erstellen des Tasks wird dieser in der Task-Liste angezeigt, und Sie können die Parameter ändern, den Task löschen oder ihn vorübergehend deaktivieren.

Anzahl der Scanthreads

Die Anzahl der Scanthreads (ein Wert von 1 bis 21). Legen Sie die Anzahl der parallel ausgeführten Scanthreads fest. Mehrere Threads können die Scangeschwindigkeit auf Computern mit mehreren Prozessoren verbessern. Verwenden Sie dieselbe Anzahl für ThreatSense-Scanmodule und Scanthreads, um ein optimales Leistungsergebnis zu erzielen.

RTF-E-Mails prüfen

Aktiviert Scans für RTF-Nachrichtentexte. E-Mail-Texte im Format Rich-Text können Makroviren enthalten.

E-Mail-Inhalte im Format Nur-Text werden nicht mit VSAPI geprüft.

Auszuführende Aktionen, falls keine Säuberung möglich ist:

- **Keine Aktion** – An der Nachricht werden keine Änderungen vorgenommen.
- **Auf Nulllänge abschneiden** – Der Anhang wird auf Nulllänge abgeschnitten.
- **Inhalt durch Aktionsinformationen ersetzen** – Der Originaltext wird durch Aktionsinformationen ersetzt. Der Inhalt des Anhangs wird durch Aktionsinformationen ersetzt.
- **E-Mail löschen** – Nachricht wird gelöscht.

Auszuführende Aktion bei Phishing-E-Mail:

- **Keine Aktion** – An der Nachricht werden keine Änderungen vorgenommen.
- **E-Mail löschen** – Nachricht wird gelöscht.

Öffentliche Ordner werden auf dieselbe Weise verarbeitet wie Postfächer. Dies bedeutet, dass öffentliche Ordner ebenfalls geprüft werden.

Scan im Hintergrund

Mit diesem Tasktyp können Sie eine Datenbankprüfung mit VSAPI im Hintergrund durchführen. Mit dieser Funktion kann Ihr Exchange Server bei Bedarf Hintergrund-Scans durchführen. Die Prüfung wird direkt vom Exchange Server ausgelöst. Es hängt also vom Exchange Server ab, ob die Prüfung innerhalb des erlaubten Intervalls abgeschlossen wird.

Führen Sie diesen Task nach Möglichkeit außerhalb der Zeiten mit hoher Last durch, wenn Ihr Exchange Server nicht ausgelastet ist, zum Beispiel nachts. Dies ist wichtig, da die Datenbankhintergrundprüfung eine gewisse Last auf Ihrem System erzeugt. Außerdem sollte der Zeitrahmen nicht mit Sicherungen auf Ihrem Exchange Server kollidieren, um Leistungs- und Verfügbarkeitsprobleme zu vermeiden.

Der Postfach-Datenbankschutz muss aktiviert sein, um diesen geplanten Task ausführen zu können. Dieser Schutz ist für Microsoft Exchange Server 2010 nur verfügbar, wenn diese als Postfachserver ausgeführt werden.

Zeitüberschreitung (Stunden)

Legen Sie fest, wie lange Ihr Exchange Server den Datenbankhintergrundscan ausführen darf. Das Zeitlimit gilt ab der Ausführung des geplanten Tasks. Nach Erreichen der Zeitüberschreitung wird Exchange angewiesen, die Hintergrundprüfung zu beenden.

On-Demand Postfachdatenbank-Scan

Falls Sie Microsoft Exchange Server 2010 verwenden, können Sie zwischen Postfach-Datenbankschutz und **On-Demand-Datenbankprüfung** wählen. Nur ein Schutztyp kann gleichzeitig aktiv sein. Wenn Sie sich für die **On-Demand Postfachdatenbank-Scan** entscheiden, müssen Sie die Integration für den **Postfach-Datenbankschutz** in den **erweiterten Einstellungen** (**F5**) unter Server deaktivieren. Andernfalls ist die **On-Demand Postfachdatenbank-Scan** nicht verfügbar.

Host-Adresse - Name oder IP-Adresse des Servers, auf dem die Exchange-Webdienste ausgeführt werden.

Benutzername – Geben Sie die Anmeldedaten eines Benutzers an, der entsprechenden Zugriff auf EWS hat.

Benutzerpasswort - Klicken Sie auf **Festlegen** neben **Benutzerpasswort**, und geben Sie das Passwort für dieses Benutzerkonto ein.

Um öffentliche Ordner scannen zu können, benötigt das für die On-Demand Postfachdatenbank-Scan verwendete Benutzerkonto ein Postfach. Andernfalls wird *Failed to load public folders* im Log der Datenbankprüfung zusammen mit einer anderen von Exchange zurückgegebenen Meldung angezeigt.

Postfach-Zugriffsmethode – Wählen Sie Ihre bevorzugte Postfach-Zugriffsmethode aus:

- **Einstellungen** – Der Identitätswechsel lässt sich schnell und einfach einrichten, indem Sie die **ApplicationImpersonation-Rolle** zum Scan-Konto zuweisen.

Einem Benutzer die Rolle „ApplicationImpersonation“ zuweisen

Wenn diese Option nicht verfügbar ist, müssen Sie einen **Benutzernamen** angeben. Klicken Sie auf **Zuweisen**, um dem ausgewählten Benutzer automatisch die ApplicationImpersonation-Rolle zuzuweisen. Alternativ können Sie die ApplicationImpersonation-Rolle manuell zu einem Benutzerkonto zuweisen. Eine neue unbegrenzte EWS-Drosselungsrichtlinie wird für das Benutzerkonto erstellt. Details dazu finden Sie unter Details des Kontos für den Datenbank-Scan.

- **Delegierung** – Dieser Zugriffstyp macht Sinn, falls Sie Zugriffsrechte für einzelne Postfächer festlegen möchten, ist jedoch unter Umständen schneller bei der Prüfung großer Datenmengen.

Einem Benutzer delegierten Zugriff zuweisen

Wenn diese Option nicht verfügbar ist, müssen Sie einen **Benutzernamen** angeben. Klicken Sie auf **„Zuweisen“**, um dem ausgewählten Benutzer automatisch Vollzugriff auf alle Benutzer- und gemeinsam genutzten Postfächer zu erteilen. Eine neue unbegrenzte EWS-Drosselungsrichtlinie wird für das Benutzerkonto erstellt. Details dazu finden Sie unter Details des Kontos für den Datenbank-Scan.

SSL verwenden

SSL muss aktiviert sein, wenn für EWS in IIS die Option „SSL erforderlich“ festgelegt ist. Wenn SSL aktiviert ist, muss das Exchange Server-Zertifikat auf dem System mit ESET Mail Security importiert werden (falls sich die Exchange-Serverrollen auf unterschiedlichen Servern befinden). Sie finden die Einstellungen für die Exchange-Webdienste in IIS unter Sites/Default website/EWS/SSL Settings.

> Deaktivieren Sie die Option **SSL verwenden** nur, wenn EWS in IIS nicht mit „SSL erforderlich“ konfiguriert ist.

Serverzertifikatfehler ignorieren – Falls Sie ein selbstsigniertes Zertifikat verwenden, können Sie Serverzertifikatfehler ignorieren.

Clientzertifikat – Muss nur festgelegt werden, wenn EWS ein Clientzertifikat erfordert. Klicken Sie auf **Aktivieren**, um ein Zertifikat auszuwählen.

Aktion, wenn Säubern nicht möglich ist - Mit diesem Aktionsfeld können Sie infizierte Inhalte sperren.

- **Keine Aktion** - Der infizierte Inhalt der Nachricht bleibt unverändert.
- **Nachricht in Papierkorb verschieben** - Diese Aktion wird für Elemente vom Typ „Öffentlicher Ordner“ nicht unterstützt. Stattdessen wird die Aktion Objekt löschen ausgeführt.
- **Objekt löschen** - Der infizierte Inhalt der Nachricht wird gelöscht.
- **E-Mail löschen** - Die gesamte Nachricht inklusive des infizierten Inhalts wird gelöscht.
- **Objekt durch Aktionsinformationen ersetzen** – Entfernt ein Objekt und fügt Informationen über das entfernte Objekt ein.

Auszuführende Aktion bei Phishing-E-Mail:

- **Keine Aktion** – Erhält die Nachricht, auch wenn sie als Phishing eingestuft wurde.
- **Nachricht in Papierkorb verschieben** - Diese Aktion wird für Elemente vom Typ „Öffentlicher Ordner“ nicht unterstützt. Stattdessen wird die Aktion Objekt löschen ausgeführt.
- **E-Mail löschen** - Die gesamte Nachricht inklusive des infizierten Inhalts wird gelöscht.

Anzahl der Scanthreads

Sie können festlegen, wie viele Threads ESET Mail Security beim Datenbank-Scan verwenden soll. Je höher die Anzahl, desto besser die Leistung. Diese Leistungssteigerung ist jedoch mit einem höheren Ressourcenverbrauch verbunden. Passen Sie diese Einstellung gemäß Ihren Anforderungen auf den gewünschten Wert an. Mit dem Standardwert werden vier Scanthreads eingesetzt.

> Eine zu hohe Anzahl von Threads für die On-Demand Postfachdatenbank-Scan kann Ihr System stark belasten, was wiederum andere Prozesse oder auch das gesamte System verlangsamen kann. Möglicherweise erhalten Sie die Meldung "*Zu viele parallele Verbindungen geöffnet*".

Microsoft 365

Nur sichtbar, falls Sie eine Microsoft 365-Hybridumgebung verwenden.

Benutzerkonto zum Scannen öffentlicher Ordner

Falls Sie öffentliche Ordner scannen möchten, geben Sie einen Namen für das Prinzipalbenutzerkonto für den Identitätswechsel ein (Passwort nicht erforderlich). Stellen Sie sicher, dass dieses Benutzerkonto auf alle öffentlichen Ordner zugreifen kann.

Postfachdatenbankprüfung

Eine vollständige Prüfung der E-Mail-Datenbank kann in großen Umgebungen eine unerwünschte Systemlast verursachen. Daher können Sie auswählen, welche Datenbanken oder Postfächer geprüft werden sollen. Sie können die Systemlast weiter reduzieren, indem Sie die Prüfziele anhand von Nachrichtenzeitstempeln filtern.

> Falsch definierte Regeln für die On-Demand Postfachdatenbank-Scan können unumkehrbare Änderungen an den Postfachdatenbanken verursachen. Stellen Sie immer sicher, dass Sie eine aktuelle Sicherung Ihrer Postfachdatenbanken haben, bevor Sie eine On-Demand Postfachdatenbank-Scan mit neuen Regeln zum ersten Mal ausführen. Überprüfen Sie außerdem dringend, ob die Regeln gemäß Ihren Erwartungen ausgeführt werden.
> Definieren Sie für diese Überprüfung Regeln nur mit der Aktion Logging in Ereignissen da andere Aktionen Ihre Postfachdatenbanken verändern können. Nach der Überprüfung können Sie destruktive Regelaktionen wie **Anhang löschen** hinzufügen.

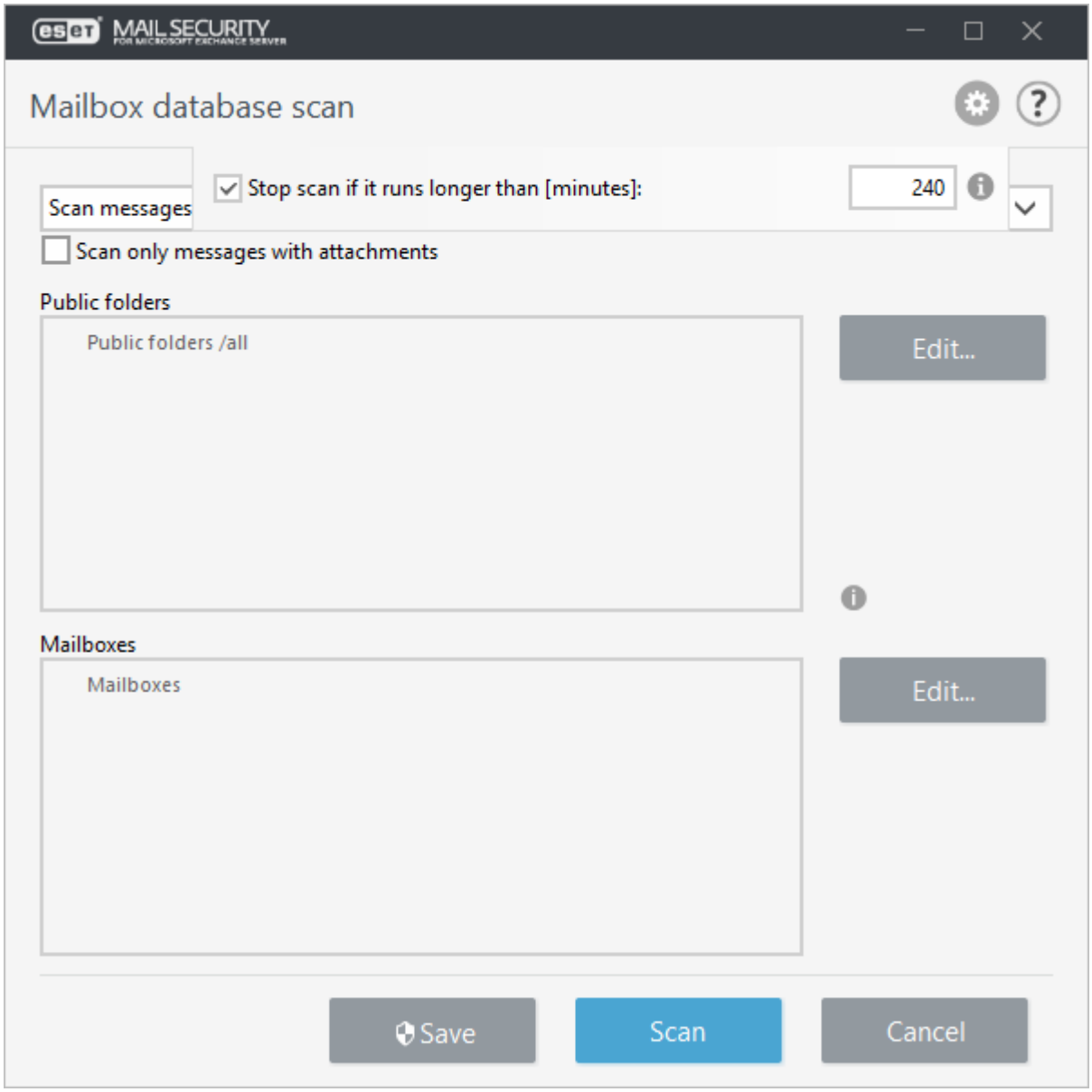
Die folgenden Elementtypen werden in **öffentlichen Ordnern** und in Benutzer-**Postfächern** geprüft:

- E-Mail
- Beiträge
- Kalendereinträge (Meetings/Besprechungen)
- Tasks
- Kontakte
- Journal

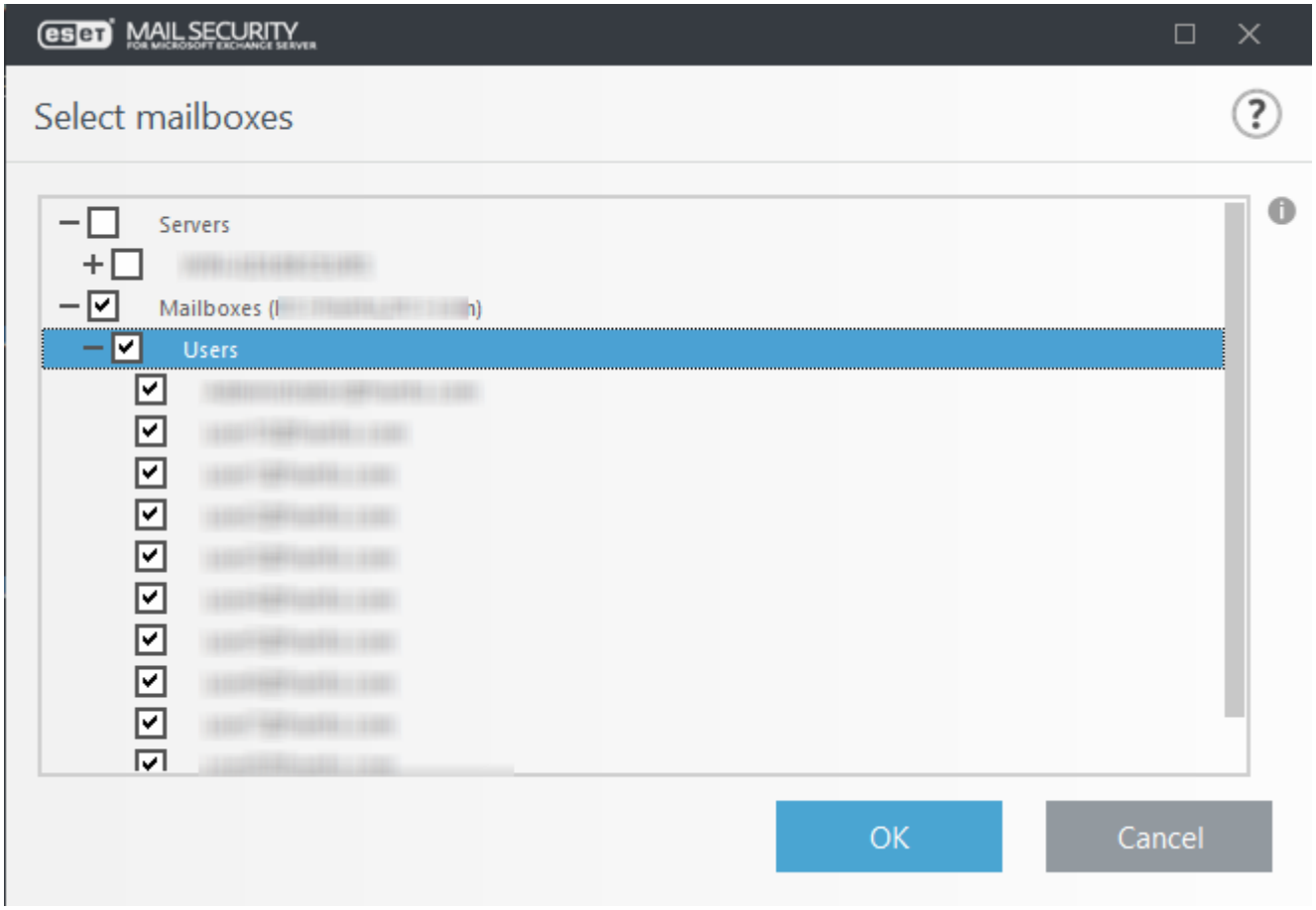
Wählen Sie in der Dropdownliste anhand eines Zeitstempels aus, welche E-Mails geprüft werden sollen. Sie können beispielsweise **alle in der vergangenen Woche veränderten Nachrichten prüfen** oder bei Bedarf auch **alle Nachrichten prüfen**.

Klicken Sie auf das Kontrollkästchen neben **Nur E-Mails min Anhang scannen**, um die Überprüfung der Nachrichtenanhänge zu aktivieren bzw. zu deaktivieren. Klicken Sie auf **Bearbeiten**, um auszuwählen, welcher öffentliche Ordner geprüft werden soll.

Klicken Sie auf das Symbol , ändern Sie das Intervall zu **Scan beenden, wenn dieser länger dauert als [Minuten]** und legen Sie den gewünschten Zeitraum fest (zwischen 1 und 2.880 Minuten).



Markieren Sie die Kontrollkästchen neben den Serverdatenbanken und Postfächern, die geprüft werden sollen. Mit Filtern können Sie schnell nach Datenbanken und Postfächern suchen. Dies ist insbesondere in Exchange-Strukturen mit vielen Postfächern hilfreich.



Klicken Sie auf **Speichern**, um die Prüfziele und Parameter im On-Demand-Prüfungsprofil zu speichern. Klicken Sie anschließend auf **Prüfen**. Falls Sie noch keine Details des Kontos für den Datenbank-Scan eingegeben haben, werden Sie in einem Popupfenster nach den Anmeldeinformationen gefragt. Andernfalls beginnt die On-Demand Postfachdatenbank-Scan.

Falls das Postfach des integrierten Administratorkontos nicht angezeigt wird, vergewissern Sie sich, dass das Attribut *UserPrincipalName* nicht leer ist.

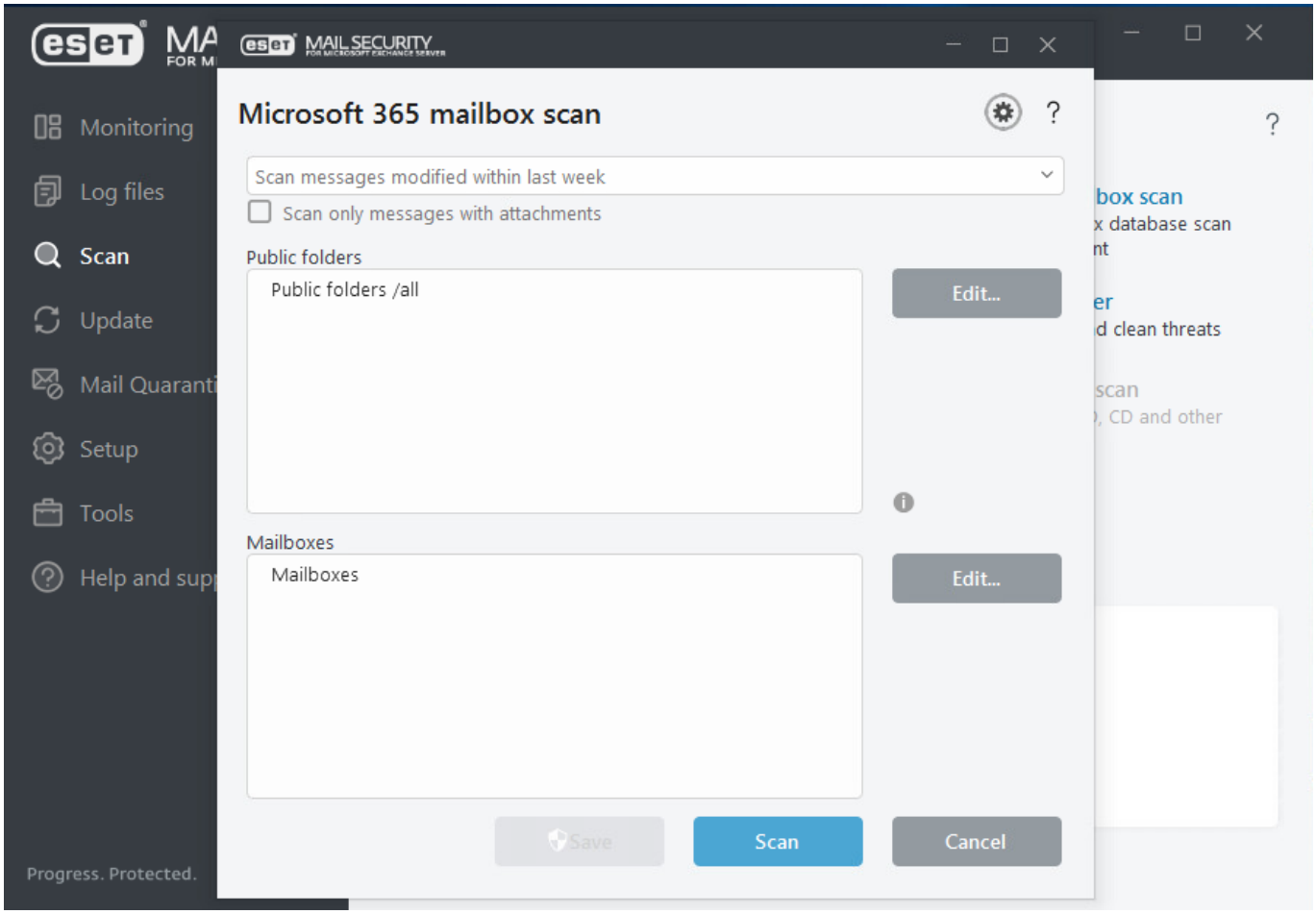
Falls Sie Microsoft Exchange Server 2010 verwenden, können Sie zwischen Postfach-Datenbankschutz und On-Demand-Postfachdatenbankprüfung wählen. Sie können jedoch nur einen Schutztyp gleichzeitig aktivieren. Wenn Sie sich für die **On-Demand Postfachdatenbank-Scan** entscheiden, müssen Sie die Integration für den **Postfach-Datenbankschutz** in den **erweiterten Einstellungen** unter **Server** deaktivieren. Andernfalls ist die On-Demand Postfachdatenbank-Scan nicht verfügbar.

Microsoft 365-Postfach-Scan

ESET Mail Security enthält Scan-Funktionen für Microsoft 365-Hybridumgebungen. Diese Funktionen sind in ESET Mail Security nur sichtbar und verfügbar, wenn Sie eine Exchange-Hybridumgebung verwenden (lokal und in der Cloud). Beide Routing-Szenarien werden unterstützt, sowohl über **Exchange Online** oder über eine **lokale** Organisation. Weitere Informationen finden Sie unter Transport-Routing in Exchange-Hybridbereitstellungen.

Registrieren Sie den ESET Mail Security Scanner, um diese Funktion zu aktivieren.

Sie können Microsoft 365-Remotepostfächer und öffentliche Ordner auf dieselbe Weise scannen wie mit der On-Demand Postfachdatenbank-Scan.



Eine vollständige Prüfung der E-Mail-Datenbank kann in einer großen Umgebung eine unerwünschte Systemlast verursachen. Daher können Sie auswählen, welche Datenbanken oder Postfächer geprüft werden sollen. Verwenden Sie den Zeitfilter am oberen Fensterrand, um die Systemlast weiter zu reduzieren. Anstatt **alle Nachrichten zu scannen**, können Sie beispielsweise **alle in der letzten Woche geänderten Nachrichten scannen**.

Wir empfehlen, Microsoft 365 zu konfigurieren. Drücken Sie die Taste **F5** und klicken Sie auf **Server** > **On-Demand Postfachdatenbank-Scan**. Siehe auch Details des Kontos für den Datenbank-Scan.

Sie können die Aktivität des Office 365-Postfach-Scans unter **Log-Dateien** > **Postfachdatenbank-Scan** überprüfen.

Zusätzliche Postfachelemente

In den Einstellungen für den On-Demand-Postfachdatenbankscan können Sie die Prüfung weiterer Postfachelemente aktivieren oder deaktivieren:

- Kalender scannen
- Aufgaben scannen
- Kontakte scannen
- Journal scannen

Falls Leistungsprobleme auftreten, können Sie das Scannen dieser Elemente deaktivieren. Die Scans dauern länger, wenn diese Elemente aktiviert sind.

Proxyserver

Falls Sie einen Proxyserver zwischen Ihrem Exchange Server mit der CAS-Rolle und dem Exchange Server, auf dem ESET Mail Security installiert ist, verwenden, geben Sie hier die Parameter für Ihren Proxyserver ein. Dies ist erforderlich, da sich ESET Mail Security per HTTP/HTTPS mit der API der Exchange-Webdienste (EWS) verbindet. Andernfalls funktionieren die Postfach-Quarantäne und die Microsoft Exchange-Quarantäne nicht.

Proxyserver

Geben Sie die IP-Adresse oder den Namen des Proxyservers ein.

Port

Geben Sie die Portnummer des Proxyservers ein.

Benutzername, Passwort

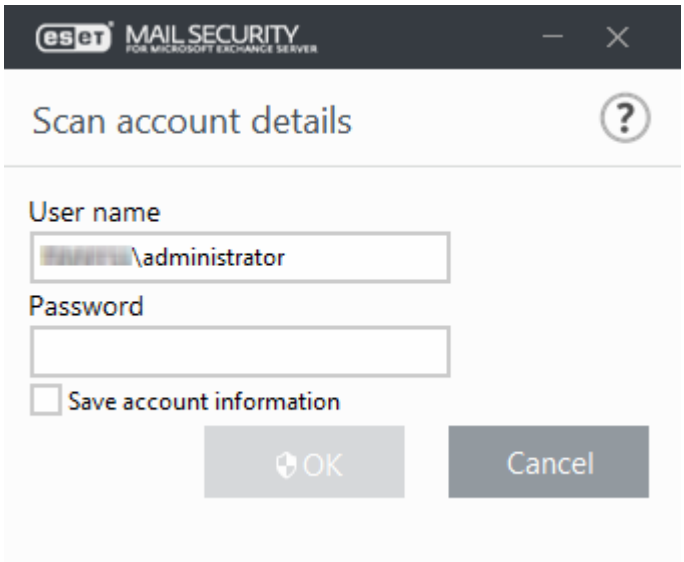
Geben Sie die Anmeldeinformationen ein, falls Ihr Proxyserver Authentifizierung verwendet.

Details des Kontos für den Datenbank-Scan

Dieser Dialog wird angezeigt, wenn Sie dennoch Benutzername und Passwort für den Datenbank-Scan angeben müssen. Geben Sie die Anmeldeinformationen des Benutzers an, der Zugriff auf die Exchange-Webdienste (EWS, Exchange Web Services) in diesem Fenster ein und klicken Sie auf **OK**. Alternativ können Sie zu **Erweiterte Einstellungen** > **Server** > On-Demand Postfachdatenbank-Scan gehen.

1. Geben Sie Ihren **Benutzernamen** ein , klicken Sie auf **Festlegen**, geben Sie ein Passwort für das Benutzerkonto ein und klicken Sie auf **OK**.

2. Klicken Sie auf das Kontrollkästchen neben **Kontoinformationen speichern**, um die Kontoeinstellungen zu speichern. Andernfalls müssen Sie die Kontoinformationen bei jeder On-Demand Postfachdatenbank-Scan erneut eingeben.



Falls ein Benutzerkonto keine ausreichenden Berechtigungen für die Exchange-Webdienste (EWS) hat, können Sie **Zuweisung für Rolle „ApplicationImpersonation“** erstellen auswählen, um diese Rolle zu einem Konto

zuzuweisen. Alternativ können Sie die Rolle **„ApplicationImpersonation role“** manuell zu einem Benutzerkonto zuweisen.

> Das Prüfkonto benötigt die Berechtigung **ApplicationImpersonation**, um die Benutzerpostfächer in Exchange-Postfachdatenbanken prüfen zu können. Falls Sie Exchange Server 2010 oder eine neuere Version verwenden, wird eine neue unbegrenzte EWS-Drosselungsrichtlinie für das Benutzerkonto erstellt. Konfigurieren Sie die EWS-Drosselungsrichtlinie für das Prüfkonto, um zu vermeiden, dass ESET Mail Security zu viele Vorgangsanforderungen stellt. Andernfalls können Zeitüberschreitungen bei den Anforderungen auftreten. Weitere Informationen zu Drosselungsrichtlinien finden Sie in den Artikeln EWS – Bewährte Methoden und Client-Drosselungsrichtlinien. Der Artikel Drosselungseinstellungen für bestimmte Benutzer anpassen enthält weitere Details und Beispiele.

Sie können die folgenden Befehle verwenden, um die **Rolle ApplicationImpersonation** manuell zu einem Benutzerkonto zuzuweisen und eine neue EWS-Drosselungsrichtlinie für das Konto zu erstellen (ersetzen Sie `ESET-user` durch einen tatsächlichen Kontonamen in Ihrem System. Legen Sie Einschränkungen für die EWS-Drosselungsrichtlinie fest, indem Sie `$null` durch Zahlen ersetzen):

Exchange Server 2010

```
New-ManagementRoleAssignment -Name:ESET-ApplicationImpersonation -
Role:ApplicationImpersonation -User ESET-user
```

Dieser Vorgang kann einige Zeit in Anspruch nehmen

```
New-ThrottlingPolicy -Name ESET-ThrottlingPolicy -EWSFindCountLimit $null -
EWSFastSearchTimeoutInSeconds $null -EWSMaxConcurrency $null -
EWSPercentTimeInAD $null -EWSPercentTimeInCAS $null -
EWSPercentTimeInMailboxRPC $null

Set-ThrottlingPolicyAssociation -Identity user-ESET -ThrottlingPolicy ESET-
ThrottlingPolicy
```

Exchange Server 2013, 2016 und 2019

```
New-ManagementRoleAssignment -Name:ESET-ApplicationImpersonation -
Role:ApplicationImpersonation -User ESET-user
```

Dieser Vorgang kann einige Zeit in Anspruch nehmen

```
New-ThrottlingPolicy -Name ESET-ThrottlingPolicy -EWSMaxConcurrency Unlimited -
EwsCutoffBalance Unlimited -EwsMaxBurst Unlimited -EwsRechargeRate Unlimited

Set-ThrottlingPolicyAssociation -Identity ESET-user -ThrottlingPolicy ESET-
ThrottlingPolicy
```

Arten der E-Mail-Quarantäne

Der E-Mail-Quarantäne-Manager ist für alle drei Quarantänetypen verfügbar:

- Lokale Quarantäne
- Quarantäne-Postfach

- Microsoft Exchange-Quarantäne

Sie können den Inhalt der E-Mail-Quarantäne im E-Mail-Quarantäne-Manager anzeigen. Außerdem können Sie die lokale Quarantäne in der Web-Oberfläche für die E-Mail-Quarantäne anzeigen.

Nachrichten für nicht vorhandene Empfänger speichern

Diese Einstellung gilt für Nachrichten, die vom Virenschutz, dem Spam-Schutz oder aufgrund von Regeln für die Quarantäne markiert wurden. Mit dieser Option werden Nachrichten an Empfänger, die nicht in Ihrem Active Directory existieren, in der E-Mail-Quarantäne gespeichert. Deaktivieren Sie diese Funktion, wenn Sie diese Nachrichten nicht in Ihrer E-Mail-Quarantäne speichern möchten. Wenn diese Option deaktiviert ist, werden Nachrichten an unbekannte Empfänger ohne Meldung gelöscht.

Siehe Beispiel – Wenn Sie alle Nachrichten an nicht vorhandene Empfänger in die Quarantäne verschieben möchten.

Überprüfung von Regeln bei der Freigabe von E-Mails überspringen

Wenn Sie eine Nachricht aus der Quarantäne freigeben, erfolgt keine Überprüfung anhand der Regeln. Auf diese Weise können Sie verhindern, dass die Nachricht zurück in die Quarantäne verschoben wird, und stellen sicher, dass der Empfänger die Nachricht erhält. Diese Funktion wird nur verwendet, wenn die Nachricht vom Administrator freigegeben wird. Wenn Sie diese Funktion deaktivieren oder eine Nachricht von einem anderen Benutzer als einem Administrator freigegeben wird, werden die Regeln auf die Nachricht angewendet.

> **i** Wenn Sie eine geclusterte Umgebung ausführen und eine Nachricht aus der Quarantäne freigeben, wird die Nachricht von den anderen ESET Mail Security-Knoten nicht erneut in die Quarantäne verschoben. Dies wird durch die Synchronisierung der Regeln zwischen den Clusterknoten erreicht.

E-Mail-Signatur-Startwert für Multi-Server-Umgebung

Mit dieser Funktion können Sie die Überprüfung von Regeln bei der Freigabe von E-Mails in einer Multi-Server-Umgebung überspringen. Geben Sie auf allen Servern, zwischen denen Sie eine Vertrauensstellung einrichten möchten, den gleichen Seed-Wert (eine Zeichenfolge, ähnlich einer Passphrase) ein.

Format des Anhangsumschlags

Wenn Sie eine E-Mail-Nachricht aus der Quarantäne freigeben, wird sie als Anhangsumschlag an eine neue Nachricht angehängt, die anschließend an den Empfänger zugestellt wird. Der Empfänger erhält die Originalnachricht, die aus der E-Mail-Quarantäne freigegeben wurde, als Anhang. Sie können das vordefinierte Umschlagformat verwenden oder mit den verfügbaren Variablen ein eigenes Format festlegen.

ESET Cluster verwenden, um alle Nachrichten in der Quarantäne auf einem Knoten zu speichern

Diese Option ist verfügbar, falls Sie einen ESET Cluster verwenden. Verwenden Sie diese Funktion wenn möglich, um die lokale Quarantänedatei an einem zentralen Ort auf dem Master-Knoten zu speichern.

Master-Knoten

Geben Sie an, welcher Server der Masterknoten Ihres ESET Clusters ist. Anschließend können Sie Ihre lokale Quarantäne auf dem Master-Knoten abrufen und verwalten (mit dem E-Mail-Quarantäne-Manager in der Hauptanwendung oder mit der Web-Oberfläche für die E-Mail-Quarantäne).

Lokale Quarantäne

Die lokale Quarantäne verwendet Ihr lokales Dateisystem als Speicher für die E-Mail-Quarantäne und eine SQLite-Datenbank als Index. Die in der Quarantäne gespeicherten E-Mail-Dateien und die Datenbankdateien werden aus Sicherheitsgründen verschlüsselt. Diese Dateien befinden sich unter C:\ProgramData\ESET\ESET Mail Security\MailQuarantine (Windows Server 2012).

> **i** Wenn Sie die Quarantänedateien auf einem anderen Datenträger als dem normalen Laufwerk speichern möchten, legen Sie den Datenordner bei der Installation von ESET Mail Security auf den gewünschten Ordner fest.

Merkmale der lokalen Quarantäne:

- SPAM- und Quarantäne-E-Mails werden im lokalen Dateisystem gespeichert und nicht in einer Exchange-Postfachdatenbank gespeichert.
- Lokal gespeicherte E-Mail-Dateien in der Quarantäne werden verschlüsselt und komprimiert.
- Web-Oberfläche für die E-Mail-Quarantäne als Alternative zum E-Mail-Quarantäne-Manager.
- Quarantäneberichte werden als geplanter Task an eine angegebene E-Mail-Adresse verschickt.
- E-Mail-Dateien werden aus dem Quarantänefenster entfernt (standardmäßig nach 21 Tagen), bleiben jedoch im Dateisystem erhalten (bis zur automatischen Löschung nach einer festgelegten Anzahl von Tagen).
- E-Mail-Dateien werden automatisch gelöscht (standardmäßig nach drei Tagen). Weitere Informationen finden Sie in den Einstellungen für die Dateispeicherung.
- Sie können die aus der Quarantäne entfernten E-Mail-Dateien mit eShell wiederherstellen (falls diese noch nicht aus dem Dateisystem gelöscht wurden).
- Sie können E-Mails in der Quarantäne prüfen und entscheiden, ob Sie diese löschen oder freigeben möchten. Sie können die E-Mails in der lokalen Quarantäne mit dem E-Mail-Quarantäne-Manager in der Hauptprogrammfenster oder mit der Web-Oberfläche für die E-Mail-Quarantäne verwalten.

> **i** Die lokale Quarantäne hat den Nachteil, dass sie pro Server separat verwaltet werden muss, falls Sie mehrere ESET Mail Security Server mit der Hub-Transport-Serverrolle betreiben. Je mehr E-Mail-Server Sie betreiben, desto mehr Quarantäne-Instanzen müssen Sie verwalten.

Dateispeicherung

In diesem Bereich können Sie Einstellungen für den Dateispeicher vornehmen, den die lokale Quarantäne verwendet.

Dateien in Quarantäne komprimieren

Komprimierte Dateien beanspruchen weniger Speicherplatz in der Quarantäne. Falls Sie die Dateien jedoch nicht komprimieren möchten, können Sie auf den Umschalter klicken, um die Komprimierung zu deaktivieren.

Alte Dateien löschen nach (Tage)

Nachrichten werden nach einer bestimmten Anzahl an Tagen aus dem Quarantänefenster entfernt. Die Dateien werden jedoch nicht vom Datenträger gelöscht. Da die Dateien nicht aus dem Dateisystem gelöscht werden, können Sie sie mit eShell wiederherstellen.

Gelöschte Dateien entfernen nach (Tage)

Mit dieser Einstellung werden Dateien nach der angegebenen Anzahl an Tagen vom Datenträger gelöscht und können anschließend nicht wiederhergestellt werden (es sei denn, Sie verwenden eine Sicherungslösung für Ihr Dateisystem).

Web-Oberfläche

Die Web-Oberfläche für die E-Mail-Quarantäne ist eine Alternative zum E-Mail-Quarantäne-Manager, ist jedoch nur für die lokale Quarantäne verfügbar.

> Die Web-Oberfläche für die E-Mail-Quarantäne ist auf Servern mit der Rolle „Edge-Transportserver“ nicht verfügbar, da Active Directory nicht für die Authentifizierung zur Verfügung steht.

In der Web-Oberfläche für die E-Mail-Quarantäne können Sie den Status der E-Mail-Quarantäne anzeigen. Außerdem können Sie die E-Mail-Objekte in der Quarantäne verwalten. Sie erreichen diese Web-Oberfläche über Links in den Quarantäne-Berichten, oder indem Sie einen Link in Ihren Webbrowser eingeben.

Sie müssen sich mit Domänenanmeldeinformationen anmelden, um die Web-Oberfläche für die E-Mail-Quarantäne zu öffnen. Microsoft Internet Explorer oder Edge authentifiziert Domänenbenutzer automatisch. Dafür muss die Webseite ein gültiges Zertifikat enthalten, die automatische Anmeldung muss in Microsoft Internet Explorer aktiviert sein, und Sie müssen die Web-Oberfläche für die E-Mail-Quarantäne zu den lokalen Intranet-Sites hinzufügen.

Die Weboberfläche der E-Mail-Quarantäne ist für alle Active Directory-Benutzer verfügbar, zeigt jedoch nur die Quarantäne-Elemente an, die an die entsprechende E-Mail-Adresse gesendet wurden (einschließlich der Aliase des Benutzers). Administratoren können alle Quarantäne-Elemente für alle Empfänger sehen.

> ESET Mail Security verwendet nicht IIS für die Web-Oberfläche der E-Mail-Quarantäne. Stattdessen wird die HTTP Server API mit SSL-Unterstützung verwendet, um Daten über sichere HTTP-Verbindungen auszutauschen.

Web-URL

Unter dieser URL ist die Weboberfläche der E-Mail-Quarantäne erreichbar. Standardmäßig handelt es sich um den FQDN des Servers mit `/quarantine` (z. B. `mailserver.company.com/quarantine`). Sie können ein eigenes virtuelles Verzeichnis anstelle des Standardwerts `/quarantine` angeben. Sie können die Web-URL jederzeit bearbeiten, indem Sie den Wert ändern.

Geben Sie die Webadresse ohne Schema (HTTP, HTTPS) oder Portnummer an. Verwenden Sie ausschließlich das fqdn/virtualdirectory-Formular. Sie können auch Platzhalter anstelle des FQDN verwenden.

Nachdem Sie die Web-URL geändert haben, können Sie nicht mehr zur Standardeinstellung zurückkehren, indem Sie auf das Symbol zum Zurücksetzen klicken. Löschen Sie den Eintrag und lassen Sie das Textfeld leer. Starten Sie den Server neu. Wenn die URL beim Start von ESET Mail Security leer ist, füllt das Programm dieses Feld automatisch mit dem Standardwert `fqdn/quarantine` aus.

ESET Mail Security Web-URLs werden in vier verschiedenen Formaten unterstützt:
Starker Platzhalter (+/quarantine)
Explizit (mydomain.com/quarantine)
IP-gebundener schwacher Platzhalter (192.168.0.0/quarantine)
Schwacher Platzhalter (*/quarantine)
Weitere Informationen finden Sie im Abschnitt **Kategorien für die Host-Angabe** des Artikels UrlPrefix-Zeichenfolgen.

Web- und Berichtssprache

Mit dieser Funktion können Sie die Sprache der Weboberfläche der E-Mail-Quarantäne und der Quarantäneberichte festlegen.

HTTPS-Port

Der HTTPS-Port wird für die Weboberfläche verwendet. Der Standardport ist 443.

HTTP-Port

HTTP-Port - Dient zur Freigabe von E-Mails aus der Quarantäne über E-Mail-Berichte.

Falls Sie kein SSL-Zertifikat in IIS installiert haben, konfigurieren Sie die HTTPS-Portbindung. Falls Sie die HTTP- oder HTTPS-Portnummer ändern, müssen Sie auch eine entsprechende Portbindung in IIS hinzufügen.

Freigabeaktionen in Log der Ereignisse schreiben

Beim Freigeben von Elementen aus der E-Mail-Quarantäne wird eine Aktion in die Log-Dateien geschrieben.

Standardadministratoren aktivieren

Mitglieder der Gruppe „Administratoren“ erhalten standardmäßig Zugriff auf die Weboberfläche der E-Mail-Quarantäne. Der Admin-Zugriff ist uneingeschränkt, und Administratoren haben Zugriff auf sämtliche Quarantäne-Elemente aller Empfänger. Wenn Sie diese Option deaktivieren, können nur die Administratorbenutzerkonten auf die Weboberfläche der E-Mail-Quarantäne zugreifen.

Zusätzliche Zugriffsrechte

Mit dieser Funktion können Benutzer die E-Mail-Quarantäne anderer Benutzer verwalten. Legen Sie Quarantäneadministratoren fest, indem Sie einem Benutzer (oder einer Gruppe) Zugriff auf die Weboberfläche der E-Mail-Quarantäne eines anderen Benutzers (oder aller Gruppenmitglieder) erteilen, um die dorthin verschobenen Elemente verwalten zu können.

1. Klicken Sie auf **Bearbeiten**, um das Fenster „Zusätzliche Zugriffsrechte“ zu öffnen, und klicken Sie auf **Hinzufügen**.

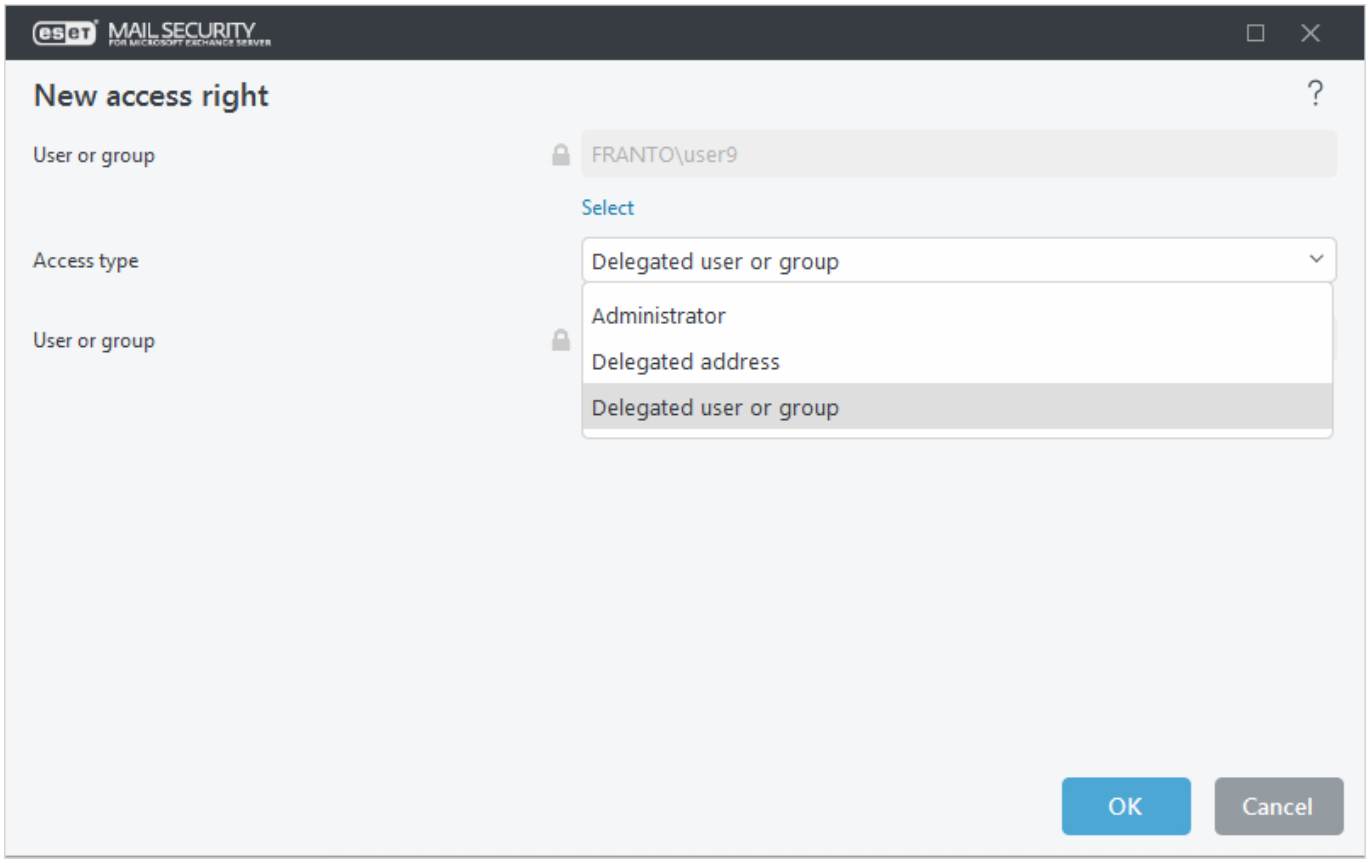
2. Klicken Sie auf **Auswählen** und verwenden Sie die Active Directory-Objektauswahl, um einen Benutzer oder eine Gruppe auszuwählen, deren Mitglieder Zugriff auf die E-Mail-Quarantäne erhalten sollen.

3. Wählen Sie den **Zugriffstyp** im Dropdownmenü aus:

- **Administrator** - Der Benutzer erhält Admin-Zugriff auf die Web-Oberfläche für die E-Mail-Quarantäne.

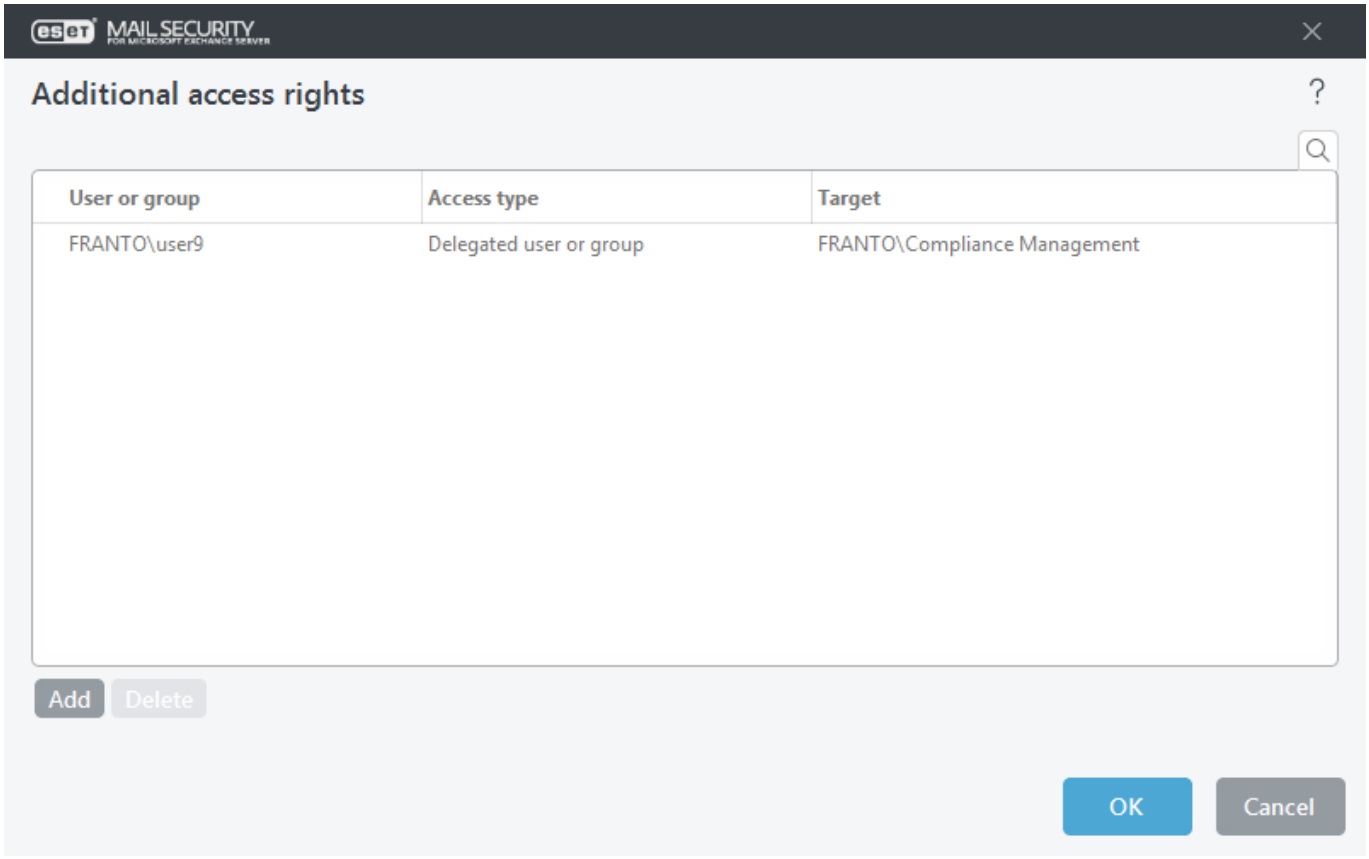
• **Delegierter Zugriff** – Benutzer mit diesem Zugriffstyp dürfen Nachrichten, die an andere Empfänger gerichtet waren, in der Quarantäne anzeigen und verwalten. Wählen Sie die Empfängeradresse aus, indem Sie die E-Mail-Adresse eines Benutzers eingeben, dessen Quarantäne-Nachrichten vom Delegat-Benutzer verwaltet werden sollen. Wenn ein Benutzer Aliasnamen im Active Directory hat, können Sie bei Bedarf zusätzliche Zugriffsrechte für die einzelnen Aliasnamen festlegen.

• **Delegierter Benutzer oder delegierte Gruppe** – Gleich wie delegierter Zugriff, und der Benutzer kann außerdem die Active Directory-Objektauswahl verwenden, um einen Benutzer oder eine Gruppe auszuwählen, für deren Mitglieder die Quarantäne verwaltet werden soll.

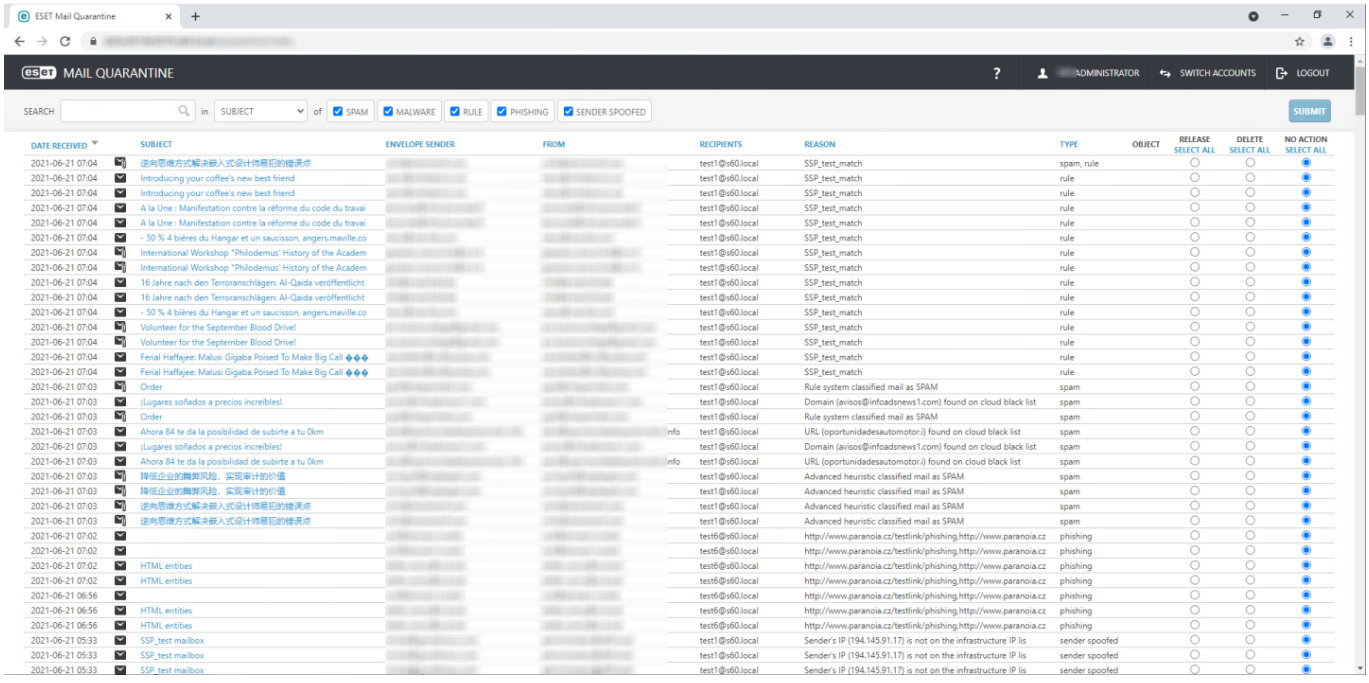


4. Klicken Sie auf **Auswählen** und wählen Sie einen Benutzer oder eine Gruppe aus, für deren Mitglieder die in Schritt 2 ausgewählte Person die Quarantäne verwalten soll.

Ein Beispiel für Benutzer, die zusätzliche Zugriffsrechte für die Web-Oberfläche für die E-Mail-Quarantäne erhalten haben:



Um die Web-Oberfläche der E-Mail-Quarantäne zu erreichen, öffnen Sie Ihren Webbrowser und verwenden Sie die URL, die unter **Erweiterte Einstellungen** (**F5**) > **Server** > **E-Mail-Quarantäne** > **Web-Oberfläche** > **Web-URL** festgelegt wurde.



Freigeben

Gibt die E-Mails über das Replay-Verzeichnis an den bzw. die Originalempfänger frei, und löscht sie aus der Quarantäne. Klicken Sie auf **Senden**, um den Vorgang zu bestätigen.

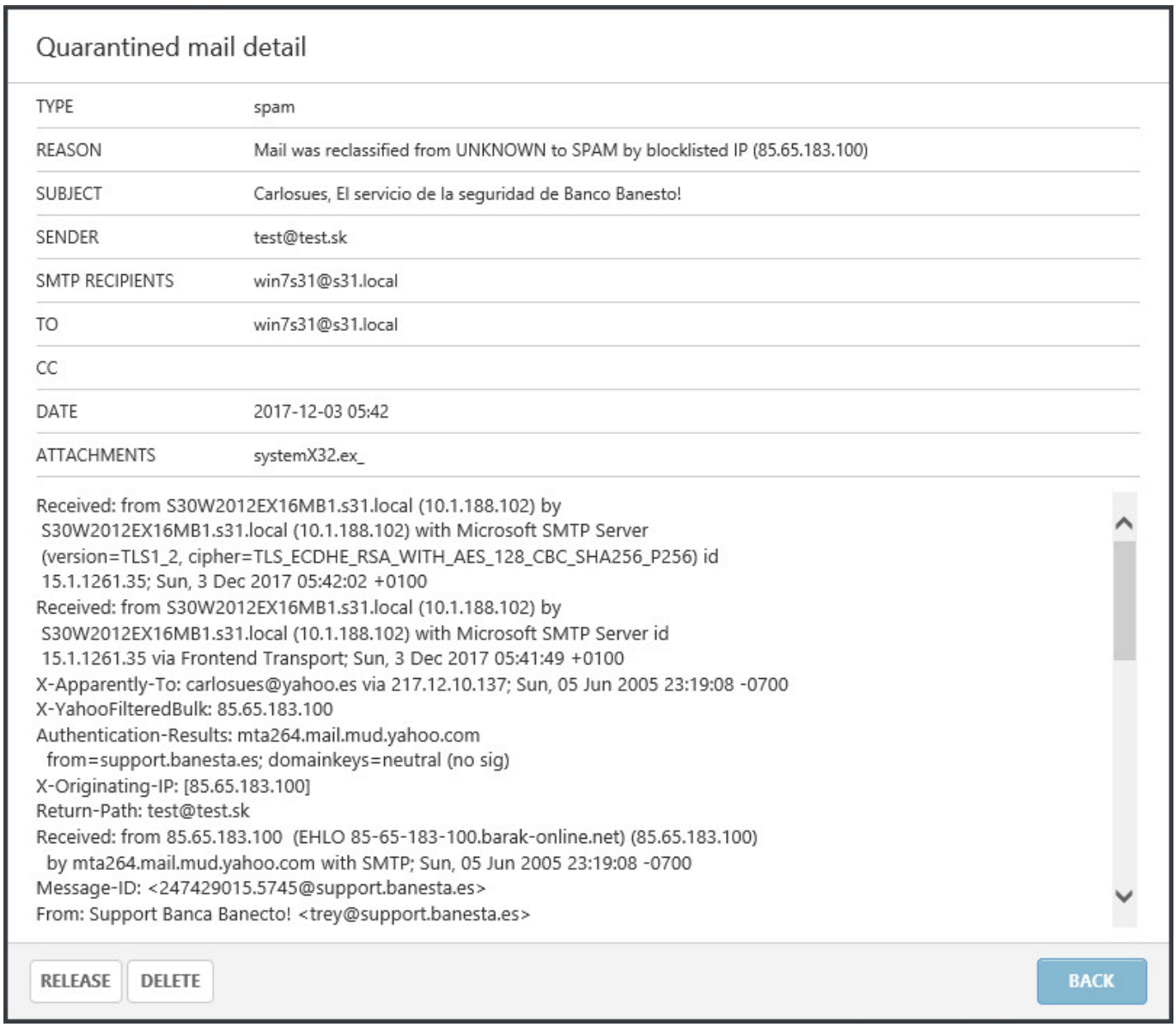
Wenn Sie eine E-Mail aus der Quarantäne freigeben, ignoriert ESET Mail Security den To:-MIME-Header, da dieser sehr leicht zu fälschen ist. Stattdessen werden die Originaldaten des Empfängers aus der Ausgabe des Befehls `RCPT TO:` verwendet, der während der SMTP-Verbindung ausgeführt wurde. Damit wird sichergestellt, dass die aus der Quarantäne freigegebene E-Mail an den richtigen Empfänger zugestellt wird.

Löschen

Diese Funktion löscht ein Element aus der Quarantäne. Klicken Sie auf **Senden**, um den Vorgang zu bestätigen.

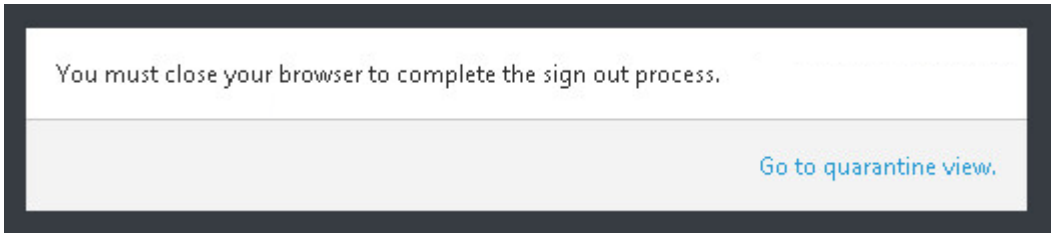
Klicken Sie auf **Betreff**, um ein Popupfenster mit Details für eine E-Mail in der Quarantäne anzuzeigen, wie z. B. Typ, Grund, Absender, Datum, Anhänge usw.

Klicken Sie auf **Header anzeigen**, um die Header der in die Quarantäne verschobenen E-Mail zu überprüfen.



Klicken Sie ggf. auf **Freigeben** oder auf **Löschen**, um die entsprechende Aktion für die E-Mail in der Quarantäne auszuführen.

Schließen Sie Ihr Browserfenster, um sich vollständig aus der Web-Oberfläche für die E-Mail-Quarantäne abzumelden. Klicken Sie andernfalls auf **Quarantäneansicht öffnen**, um zum vorherigen Bildschirm zurückzukehren.



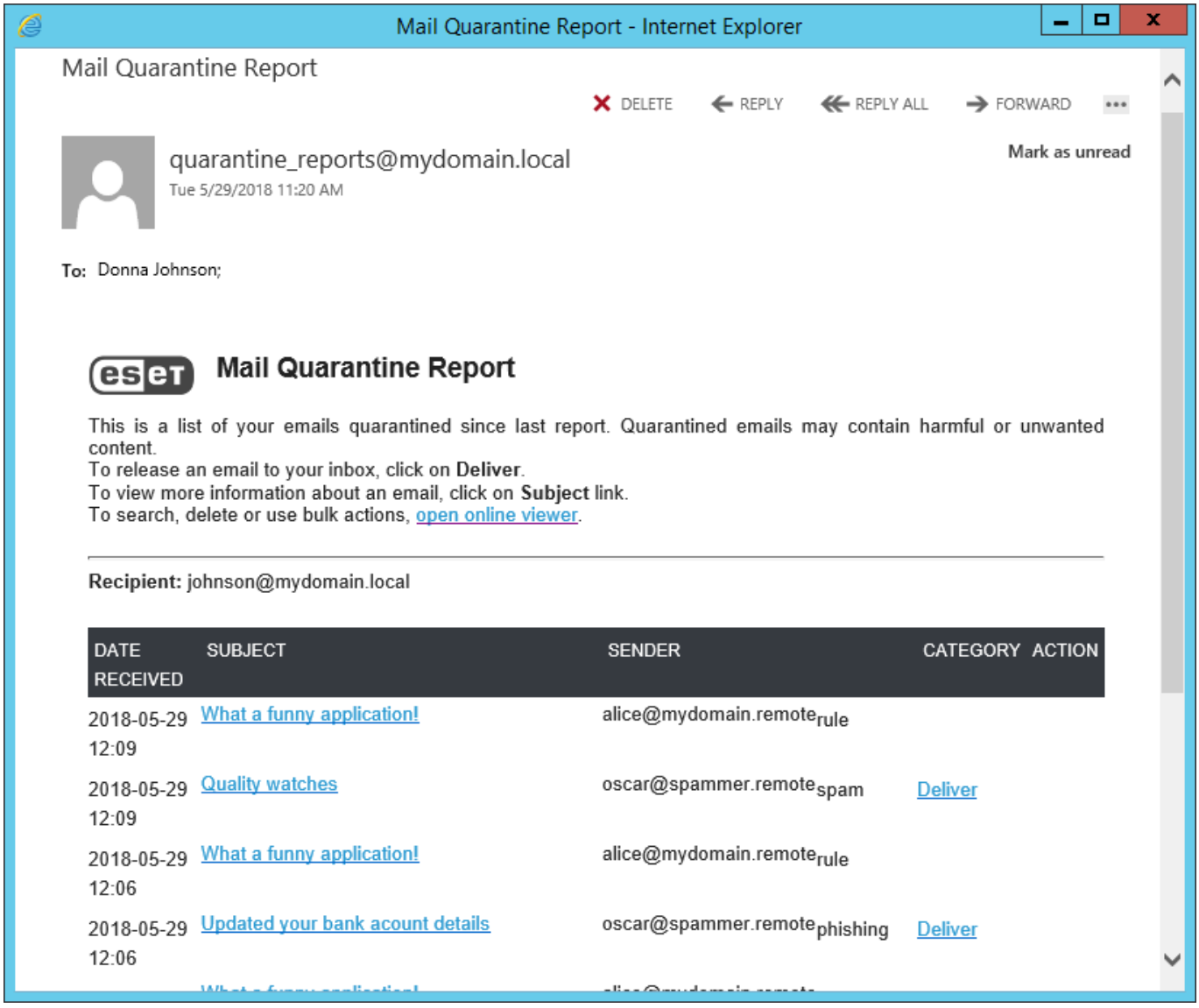
Falls Sie Probleme beim Zugriff auf die Web-Oberfläche für die E-Mail-Quarantäne mit Ihrem Browser haben oder die Meldung HTTP Error 403.4 - Forbidden oder ein ähnlicher Fehler angezeigt wird, stellen Sie sicher, dass unter Quarantänetyp der Wert **Lokale Quarantäne** ausgewählt ist und dass die Option **Web-Oberfläche aktivieren** aktiviert ist.

Quarantäneberichte per E-Mail senden – geplanter Task

E-Mail-Quarantäneberichte werden per E-Mail an ausgewählte Benutzer und Administratoren verschickt und enthalten Informationen zu E-Mails, die von ESET Mail Security in die Quarantäne verschoben wurden. Mit den in Berichten enthaltenen Links können Sie und andere Empfänger der E-Mail-Quarantäneberichte E-Mail-Nachrichten mit falsch positivem Ergebnis direkt löschen oder freigeben (zustellen). Nachrichten, die durch Regeln oder vom Virenschutz in die E-Mail-Quarantäne verschoben werden, können von normalen Benutzern nicht zugestellt werden.

Um Quarantäneberichte zu senden, erstellen Sie einen geplanten Task (Tools > Taskplaner > Task hinzufügen) und wählen Sie einen der Tasktypen Quarantäneberichte per E-Mail senden oder Quarantäne-Administratorberichte per E-Mail senden aus. Bei der Auswahl der Empfänger werden auch verknüpfte Postfächer in der Liste der verfügbaren Postfächer angezeigt.

Der Task „Quarantäneberichte per E-Mail senden / Quarantäne-Administratorberichte per E-Mail senden“ verschickt einen Bericht zur E-Mail-Quarantäne per E-Mail gemäß des angegebenen geplanten Tasks. Hier sehen Sie ein Beispiel für einen E-Mail-Quarantänebericht:



Der E-Mail-Quarantänebericht enthält außerdem einen Link zur Web-Oberfläche für die E-Mail-Quarantäne (Online-Viewer öffnen).

> Der Task „Quarantäneberichte per E-Mail senden“ ist nur verfügbar, wenn Sie die **lokale Quarantäne** verwenden. Der Task ist für das Quarantäne-Postfach und die MS Exchange-Quarantäne nicht verfügbar.

Absenderadresse

Die Adresse, die als Absender des E-Mail-Quarantäneberichts angezeigt wird.

Maximale Anzahl der Datensätze im Bericht

Sie können die Anzahl der Einträge pro Bericht eingrenzen. Der Standardwert ist 50.

Web URL

Diese URL ist im E-Mail-Quarantänebericht enthalten und kann angeklickt werden, um die Web-Oberfläche für die E-Mail-Quarantäne zu öffnen.

Empfänger

Wählen Sie Benutzer aus, die die E-Mail-Quarantäneberichte erhalten sollen. Klicken Sie auf **Bearbeiten**, um Postfächer für einzelne Empfänger auszuwählen (verknüpfte Postfächer werden ebenfalls unterstützt).

> Der E-Mail-Quarantänebericht wird nur verschickt, wenn die Quarantäne Nachrichten enthält. Wenn die Quarantäne leer ist oder seit dem letzten Bericht keine neuen Elemente in die Quarantäne verschoben wurden, wird der Bericht nicht verschickt. In jedem Fall enthält der E-Mail-Quarantänebericht nur Elemente, die seit dem letzten Bericht neu hinzugefügt wurden (nicht den gesamten Inhalt der Quarantäne).

> Ziel: Erstellen Sie einen geplanten Task, um die E-Mail-Quarantäneberichte regelmäßig als Administrator zu erhalten, oder um Benutzer über ihre Spamnachrichten zu informieren, die sich aktuell in der E-Mail-Quarantäne befinden.
> Navigieren Sie zu **Tools** > **Taskplaner** > **Task hinzufügen** und öffnen Sie den Assistenten.
> Geben Sie den **Tasknamen** ein und wählen Sie einen **Tasktyp** im Dropdownmenü aus.
> **Quarantäneberichte per E-Mail senden** (der Bericht enthält nur die Spamnachrichten eines bestimmten Benutzers) oder **Quarantäne-Administratorberichte per E-Mail senden** (der Bericht enthält sämtliche Nachrichten in der Quarantäne), und klicken Sie auf **Weiter**.
> Wählen Sie eine Option für die Ausführung des geplanten Tasks aus. Beispiel: **Wöchentlich** um **10.00.00 Uhr** am **Freitag**.
> Geben Sie eine **Absenderadresse** ein (administrator@mydomain.com).
> Klicken Sie auf **Bearbeiten**, um **Empfänger** aus der Liste hinzuzufügen. Wählen Sie Postfächer von Benutzern aus, die die E-Mail-Quarantäneberichte erhalten sollen.

Web-Oberfläche für die E-Mail-Quarantäne

Ihnen wurde Zugriff auf eine Web-Oberfläche erteilt, in der Sie Quarantäne-Nachrichten wie Spam, gefälschter Absender oder Phishing oder Nachrichten verwalten können, die von den Regeln Ihres Administrators herausgefiltert wurden. Normalerweise werden nur Nachrichten angezeigt, die an Ihre E-Mail-Adressen verschickt und in die Quarantäne verschoben wurden. Wenn Ihnen jedoch die Verwaltung der Quarantäne-Nachrichten anderer Benutzer delegiert wurde, sehen Sie auch die Nachrichten dieser Benutzer. Sie können die Nachrichten nach Empfängern unterscheiden. Verwenden Sie die Suchfunktion, um die Nachrichten nach Empfängern zu

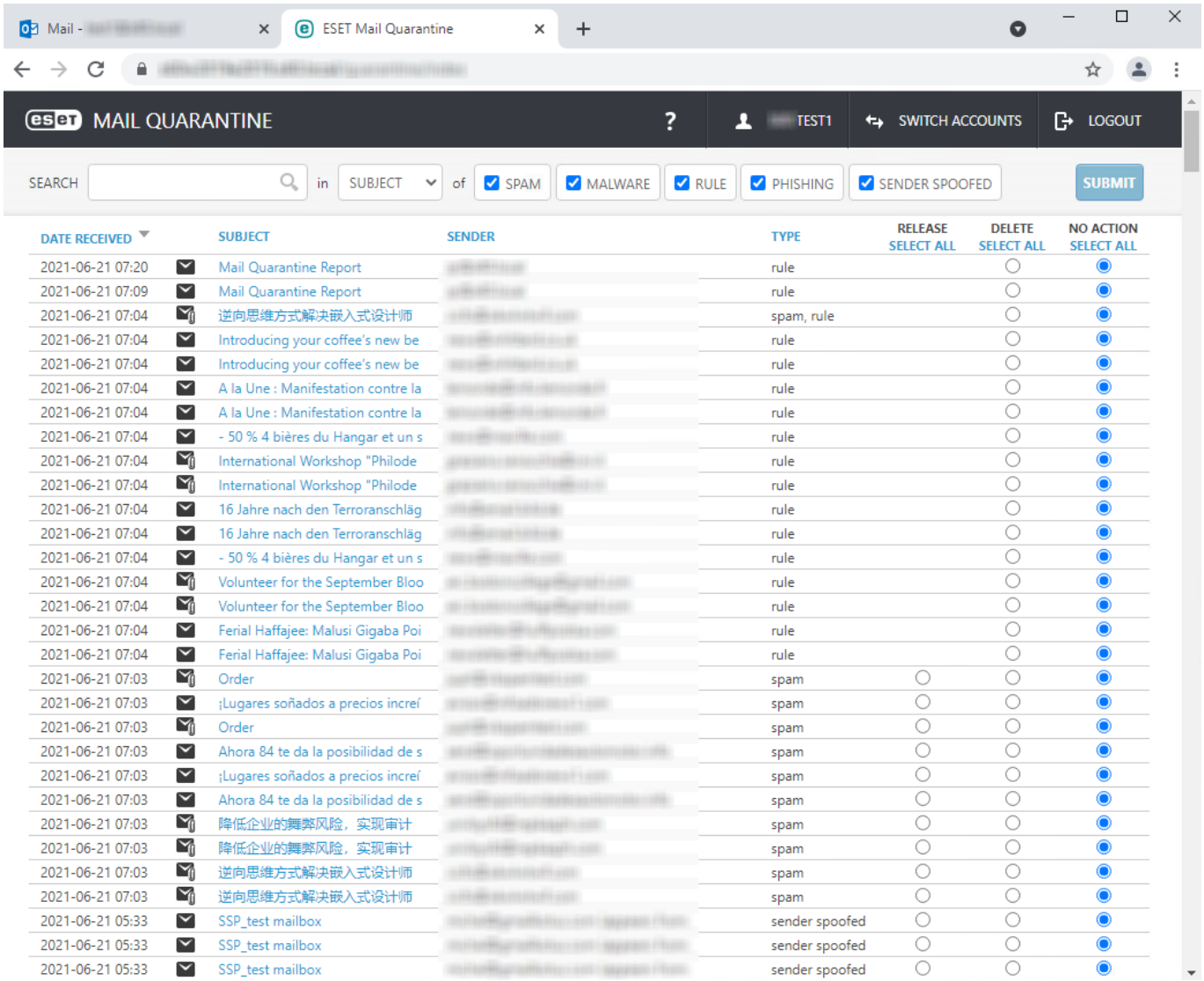
filtern.

Sie können mehrere Nachrichten auswählen und eine Aktion wie **Freigeben**, **Löschen** oder auch **keine Aktion** auswählen. Die Verfügbarkeit der Aktionen hängt von der Zugriffsebene und den Regeleinstellungen ab. Möglicherweise können Sie bestimmte Arten von Nachrichten nicht freigeben oder löschen.

Falls Ihnen Administratorzugriff erteilt wurde, sehen Sie alle Quarantäne-Nachrichten für alle Benutzer und können alle Aktionen ausführen.

Verwalten Ihrer Quarantäne-Nachrichten

In der Web-Oberfläche für die E-Mail-Quarantäne können Sie sämtliche Inhalte in der Quarantäne anzeigen. Falls Ihnen delegierter oder Administratorzugriff erteilt wurde, sehen Sie auch die Quarantäne-Nachrichten anderer Benutzer.



Sie können die Anzahl der Einträge pro Seite (Seitengröße) in der unteren linken Ecke des Fensters festlegen.

Falls zu viele Nachrichten angezeigt werden, können Sie mit der Suchfunktion in der oberen Leiste nach einer bestimmten E-Mail suchen oder die Inhalte nach Betreff, Absender oder Empfänger filtern (Nur Benutzer mit delegiertem oder Administratorzugriff können nach Empfängern filtern). Außerdem können Sie die Kontrollkästchen markieren, um nur Nachrichten von einem bestimmten Typ (**Spam**, **Malware**, **Regel**, **Phishing** und **gefälschter Absender**) anzuzeigen.

Um eine Nachricht freizugeben (zuzustellen), die durch ein falsch positives Ergebnis bei der Klassifizierung in die Quarantäne verschoben wurde, verwenden Sie die Optionsfelder auf der rechten Seite und wählen Sie **Freigeben** aus. Wählen Sie die Aktion **Löschen** aus, um eine Nachricht zu löschen.

Sie können mehrere Nachrichten auswählen und die gewünschte Aktion gleichzeitig ausführen. Treffen Sie Ihre Auswahl und klicken Sie auf **Übermitteln**.

Für die Freigabe markierte Nachrichten werden anschließend an Ihr Postfach bzw. an das Postfach des Empfängers zugestellt, falls Sie delegierten Zugriff haben und Nachrichten für andere Benutzer freigeben. Für die Löschung markierte Nachrichten werden permanent aus der Quarantäne gelöscht.

> Die Aktionen **Freigeben** und **Löschen** können nicht mehr rückgängig gemacht werden, nachdem Sie auf **Übermitteln** geklickt haben.

Die Ansicht wird automatisch aktualisiert, wenn Sie auf „Übermitteln“ klicken. Sie können jedoch auch Ihren Browser aktualisieren oder die Taste **F5** auf Ihrer Tastatur drücken, um die Ansicht manuell zu aktualisieren.

> Nur Spam und Nachrichten mit gefälschtem Absender können freigegeben werden. Es ist nicht zulässig, Malware, Phishing- und regelbasierte Nachrichten freizugeben. Wenden Sie sich an Ihren Administrator, falls Sie eine solche Nachricht freigeben möchten.

Die Nachrichten in der Quarantäne werden automatisch nach einem vom Administrator festgelegten Zeitraum gelöscht und müssen daher nicht regelmäßig entfernt werden.

> Schließen Sie Ihr Browserfenster, um sich vollständig aus der Web-Oberfläche für die E-Mail-Quarantäne abzumelden. Klicken Sie andernfalls auf Quarantäneansicht öffnen, um zum vorherigen Bildschirm zurückzukehren.

Quarantäne-Postfach und Microsoft Exchange-Quarantäne

Falls Sie sich entschließen, die lokale Quarantäne nicht zu verwenden, haben Sie zwei Optionen: das Quarantäne-Postfach oder die MS Exchange-Quarantäne. Für beide Optionen müssen Sie einen Benutzer mit einem Postfach anlegen (zum Beispiel quarantäne@firma.de), das anschließend für die Speicherung der in Quarantäne-E-Mails verwendet wird. Der E-Mail-Quarantäne-Manager verwendet diesen Benutzer und das Postfach auch, um die Elemente in der Quarantäne anzuzeigen und zu verwalten. Geben Sie die Kontoinformationen dieses Benutzers in den Einstellungen für den Quarantäne-Manager an.

> Quarantäne-Postfach und Microsoft Exchange-Quarantäne haben gegenüber der lokalen Quarantäne den Vorteil, dass die Quarantäne-E-Mails an einem zentralen Ort verwaltet werden, egal wie viele Server mit Hub-Transport-Serverrolle vorhanden sind. Im Gegensatz zur lokalen Quarantäne werden Spam- und Quarantäne-E-Mails im Quarantäne-Postfach und in der MS Exchange-Quarantäne in Exchange-Postfachdatenbanken gespeichert. Jeder Benutzer mit Zugriff auf das Quarantäne-Postfach kann die Nachrichten in der Quarantäne verwalten.

Sowohl Quarantäne-Postfach als auch MS Exchange-Quarantäne verwenden ein dediziertes Postfach zur Speicherung der Nachrichten in der Quarantäne, allerdings werden die E-Mail-Nachrichten auf unterschiedliche Arten an das Postfach zugestellt. Vergleich: Quarantäne-Postfach und MS Exchange-Quarantäne:

Quarantäne-Postfach

ESET Mail Security erstellt eine separate Wrapper-E-Mail mit zusätzlichen Informationen und den ursprünglichen E-Mails als Anhang, und stellt diese E-Mail an das Postfach zu.

Geben Sie die Adresse des Quarantäne-Postfachs an (z. B. quarantäne@firma.de).

Das Administrator-Benutzerkonto sollte nicht als Quarantäne-Postfach verwendet werden.

MS Exchange-Quarantäne

Der Microsoft Exchange Server ist für die Zustellung der E-Mail an das Postfach verantwortlich. Das Postfach muss in Active Directory auf der Organisationsebene als Quarantäne festgelegt werden. Verwenden Sie dazu den unten gezeigten PowerShell-Befehl.

Die interne Quarantäne ist in Microsoft Exchange Server standardmäßig deaktiviert. Falls Sie diese Funktion nicht aktiviert haben, führen Sie den folgenden Befehl in der Exchange-Verwaltungsshell aus (ersetzen Sie `Name@domain.com` durch die tatsächliche Adresse Ihres Quarantäne-Postfachs): `Set-ContentFilterConfig -QuarantineMailbox name@domain.com`

ESET Mail Security verwendet das Microsoft Exchange-Quarantänesystem (gilt ab Microsoft Exchange Server 2010). Eine interne Funktion des Servers speichert dabei potenziell infizierte Nachrichten und Spam.

Einstellungen für Quarantäne-Manager

Host-Adresse

Wird automatisch ausgefüllt, wenn Ihr Exchange Server mit Clientzugriffsserver (CAS)-Rolle lokal vorhanden ist. Falls sich die CAS-Rolle nicht auf demselben Server wie ESET Mail Security befindet, diese jedoch im Active Directory (AD) auffindbar ist, wird die Host-Adresse automatisch ausgefüllt. Falls kein Wert angezeigt wird, können Sie den Hostnamen manuell eingeben. Die automatische Erkennung funktioniert nicht für die Edge-Transportserverrolle. IP-Adressen werden nicht unterstützt. Sie müssen den Hostnamen des CAS-Servers verwenden.

Benutzername

Ein speziell eingerichtetes Quarantäne-Benutzerkonto, das Sie für die Speicherung der E-Mails in der Quarantäne angelegt haben (bzw. ein Benutzerkonto, das per Zugriffsdelegierung Zugriff auf dieses Postfach hat). Für Edge-Transportserverrollen, die sich nicht in derselben Domäne befinden, müssen Sie die komplette E-Mail-Adresse angeben (z. B. *main_quarantine@company.com*).

Passwort

Geben Sie das Passwort für Ihr Quarantänekonto ein.

SSL verwenden

Diese Option muss aktiviert werden, wenn für die Exchange-Webdienste (EWS) die Option **SSL erforderlich** in IIS festgelegt ist. Wenn SSL aktiviert ist, muss das Exchange Server-Zertifikat auf dem System mit ESET Mail Security importiert werden (falls sich die Exchange-Serverrollen auf unterschiedlichen Servern befinden). Sie finden die Einstellungen für die Exchange-Webdienste in IIS unter Sites/Default web site/EWS/SSL Settings.

Deaktivieren Sie die Option **SSL verwenden** nur, wenn die Exchange-Webdienste (EWS) in IIS nicht für die Verwendung von SSL konfiguriert sind.

Serverzertifikatfehler ignorieren

Folgende Status werden ignoriert: self-signed, wrong name in certificate, wrong usage, expired.

Proxyserver

Falls Sie einen Proxyserver zwischen Ihrem Exchange Server mit der CAS-Rolle und dem Exchange Server, auf dem ESET Mail Security installiert ist, verwenden, geben Sie hier die Parameter für Ihren Proxyserver ein. Dies ist erforderlich, da sich ESET Mail Security per HTTP/HTTPS mit der API der Exchange-Webdienste (EWS) verbindet. Andernfalls funktionieren die Postfach-Quarantäne und die Microsoft Exchange-Quarantäne nicht.

Proxyserver

Geben Sie die IP-Adresse oder den Namen des Proxyservers ein.

Port

Geben Sie die Portnummer des Proxyservers ein.

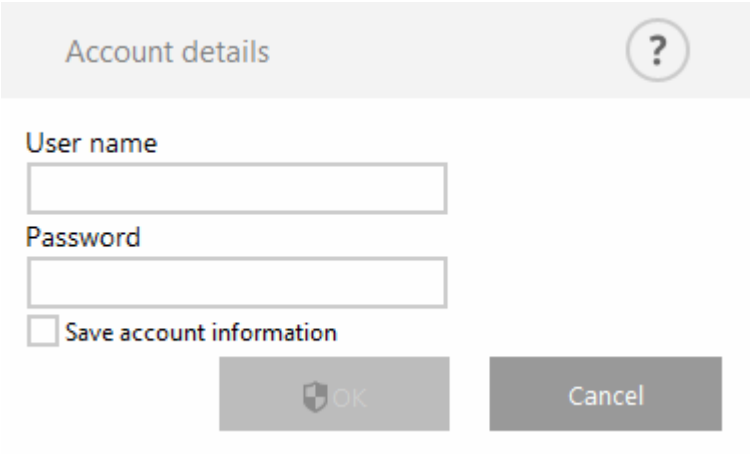
Benutzername, Passwort

Geben Sie die Anmeldeinformationen ein, falls Ihr Proxyserver Authentifizierung verwendet.

Quarantäne-Manager-Kontodetails

Dieser Dialog wird angezeigt, wenn Sie keine Kontodetails (Benutzername und Passwort) für Ihren Quarantäne-Manager eingegeben haben. Geben Sie die Anmeldeinformationen eines Benutzers ein, der Zugriff auf das Quarantäne-Postfach hat und klicken Sie auf **OK**. Alternativ können Sie mit **F5** die **erweiterten Einstellungen** öffnen und zum Eintrag **Server** > **E-Mail-Quarantäne** > Einstellungen für Quarantäne-Manager navigieren.

Geben Sie **Benutzername** und **Passwort** für Ihr Quarantäne-Postfach ein.



Sie können die **Kontoinformationen speichern**, um sie bei zukünftigen Zugriffen auf den Quarantäne-Manager nicht erneut eingeben zu müssen.

DKIM-Signierung

Die DKIM-Signierung (DomainKeys Identified Mail) ist eine Methode zum Sichern ausgehender E-Mails und zur Erleichterung der Überprüfung. Mit dieser Methode können E-Mail-Server echte Nachrichten präzise von Spam unterscheiden.

Die DKIM-Authentifizierung funktioniert folgendermaßen:

- Die Header ausgehender E-Mails werden mit dem privaten DKIM-Schlüssel signiert.
- Der E-Mail-Server überprüft den DNS-DKIM-Eintrag, der einen öffentlichen Schlüssel enthält.
- Wenn die Signatur mit dem privaten Schlüssel in den Nachrichtenköpfen mit dem öffentlichen Schlüssel des DNS DKIM-Eintrags übereinstimmt, gilt die E-Mail als echt und wird an die Empfänger zugestellt.
- Wenn die Signatur und der öffentliche Schlüssel nicht übereinstimmen, hängt es von der Konfiguration des empfangenden E-Mail-Servers ab, was mit der E-Mail geschieht (Unter Umständen gelten bestimmte Regeln, ESET Mail Security verwendet in diesem Fall beispielsweise die DKIM-Ergebnisregelbedingung).

Um die ESET Mail Security DKMI-Signierungsfunktion zu verwenden, müssen Sie sicherstellen, dass Sie den DNS DKIM-Eintrag für Ihre Domäne konfiguriert haben. Weitere Informationen zum Erstellen eines DKIM-Eintrags finden Sie im Artikel Was ist ein DKIM-Eintrag und wie wird erstellt?. Der Artikel enthält außerdem ein Beispiel für einen DKIM-Eintrag. Sie können auch versuchen, einen Online-DKIM-Generator zu verwenden, um private und öffentliche DKIM-Schlüssel zu generieren.

Wenn Sie fertig sind, sollten Sie entweder DKIM Record Checker oder MXToolBox verwenden, um sicherzustellen, dass der öffentliche DKIM-Schlüssel vorhanden ist und dass die Syntax korrekt implementiert wurde.

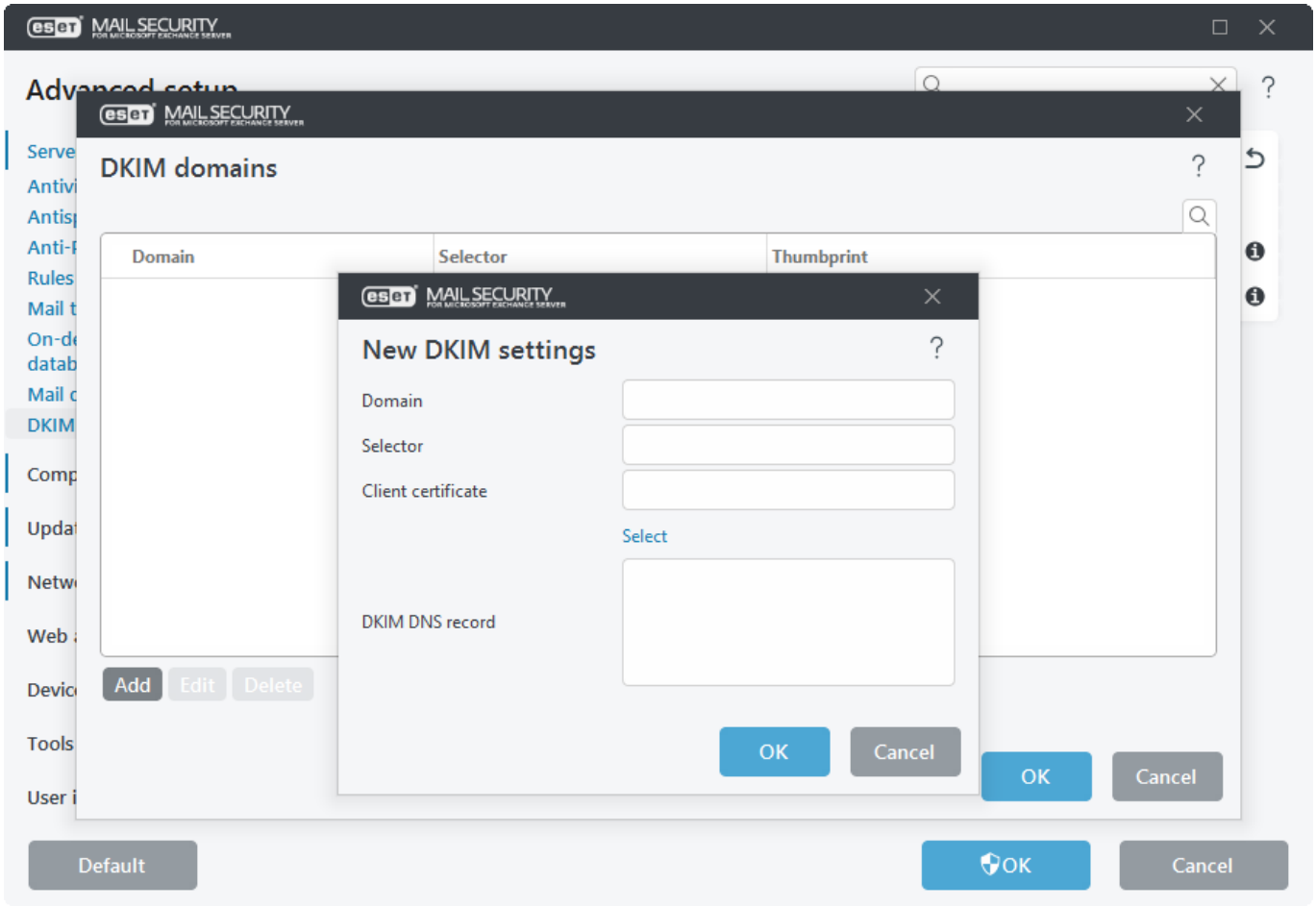
Konfigurieren Sie die DKIM-Signierung in ESET Mail Security, indem Sie DKIM-Domänen und eine Liste der zu signierenden E-Mail-Header angeben. Die DKIM-Signatur wird zu den ausgewählten Nachrichten-Headern hinzugefügt. Jede DKIM-Signatur enthält Informationen, mit denen Mailserver die Authentizität von E-Mails überprüfen können, bevor sie diese an das endgültige Ziel weiterleiten. Wenn Sie mehrere Domänen für ausgehende Nachrichten verwenden, können Sie die DKIM-Signierung für jede Domäne separat konfigurieren.

> Aktivieren Sie **DKIM-Signierung** unter **Server** > Integration in den **Erweiterte Einstellungen**. In den Einstellungen für die Agentenpriorität empfehlen wir, den ESET DKIM Agent an der untersten Stelle zu belassen, um sicherzustellen, dass die Header erst nach den Änderungen durch vorherige Agenten signiert werden.

DKIM-Domänen

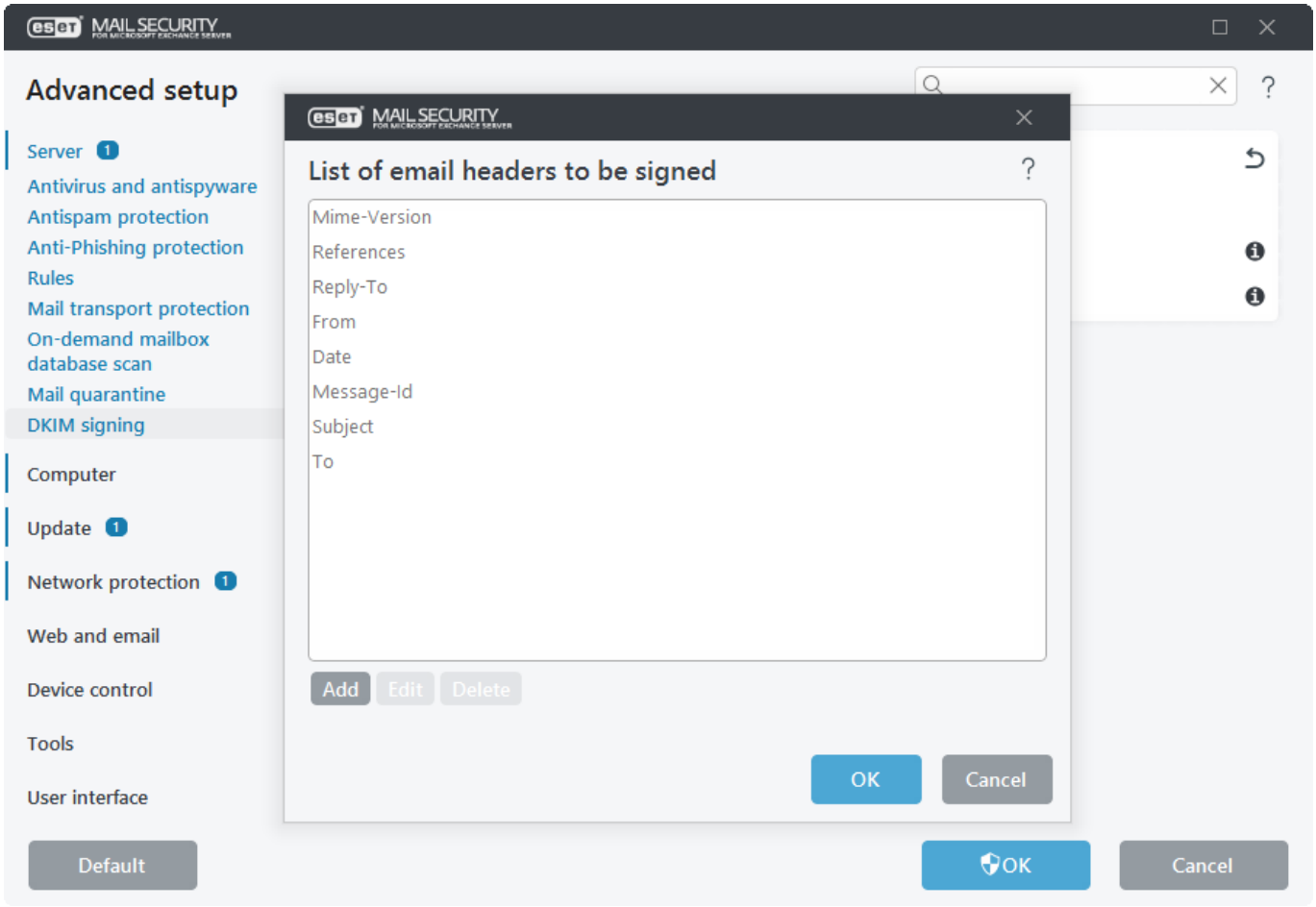
Legen Sie Einstellungen für die DKIM-Signierung pro Domäne fest. Klicken Sie auf **Bearbeiten**, um das Fenster für DKIM-Domänen zu öffnen. Klicken Sie auf **Hinzufügen**, um **neue DKIM-Einstellungen** zu erstellen, oder auf „Bearbeiten“, um vorhandene Einstellungen zu bearbeiten.

- **Domäne** – Geben Sie die Domäne ein (z. B. *domainname.local*).
- **Auswahl** – Geben Sie die Auswahl als Attribut für eine DKIM-Signatur an, das anschließend im Header-Feld für die DKIM-Signatur erfasst wird.
- **Clientzertifikat** – Klicken Sie auf **Auswählen** und wählen Sie das Clientzertifikat für die DKIM-Signierung aus.



Liste der zu signierenden E-Mail-Header

Klicken Sie auf **Bearbeiten**, um die Liste der zu signierenden E-Mail-Header zu öffnen. Klicken Sie auf **Hinzufügen**, um neue Header hinzuzufügen, oder auf **Bearbeiten**, um vorhandene Header in der Liste zu bearbeiten.



Virenschutz testen

Verwenden Sie eine Testdatei von eicar.com, um zu testen, ob der Echtzeit-Schutz aktiv ist und Viren erkennt. Dies ist eine harmlose Datei, die von der Firma EICAR (European Institute for Computer Antivirus Research) erstellt wurde und die von allen Virenschutzprogrammen erkannt wird.

Um Ihre Virenschutzfunktion zu testen, erstellen Sie eine Textdatei, die die folgende Zeichenfolge enthält:

```
X50!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Weitere Informationen und zum Herunterladen von Testdateien finden Sie unter https://www.eicar.org/download-anti-malware-testfile/

Spam-Schutz testen

Mit einer GTUBE-Testzeichenfolge (Generic Test for Unsolicited Bulk Email) können Sie überprüfen, ob die ESET Mail Security Antispam-Funktion eingehende Spam-Nachrichten erkennt.

Um den Spam-Schutz zu testen, verschicken Sie eine E-Mail mit der folgenden 68 Byte-Zeichenfolge im Nachrichtentext:

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

Verwenden Sie die Zeichenfolge wie angegeben (eine Zeile, ohne Leerzeichen oder Zeilenumbrüche). Sie können eine passende E-Mail-Nachricht im RFC-822-Format herunterladen.

Phishing-Schutz testen

Um den Phishing-Schutz zu testen, senden Sie eine E-Mail mit dem folgenden Link (URL) im Nachrichtentext oder im Betreff:

https://www.amtso.org/check-desktop-phishing-page/

Unter **Log-Dateien** > E-Mail-Server-Schutz-Log können Sie die Aktivitäten des E-Mail-Phishing-Schutzes anzeigen. Dieses Log enthält Informationen über E-Mail-Nachrichten und gefundene Phishing-Links.

Allgemeine Einstellungen

In diesem Fenster können Sie allgemeine Einstellungen vornehmen und Funktionen konfigurieren. Das Menü auf der linken Seite enthält die folgenden Kategorien:

Computer

Aktivieren bzw. deaktivieren Sie die Erkennung potenziell unerwünschter, unsicherer, und verdächtiger Anwendungen und die Anti-Stealth-Technologie. Legen Sie Ausschlüsse für Prozesse, Dateien oder Ordner fest. Konfigurieren Sie den Echtzeit-Dateischutz, ThreatSense Parameter, Cloudbasiert Schutz (ESET LiveGrid®), Malware-Scans (On-Demand-Scan und andere Scanoptionen), Hyper-V-Scan und HIPS.

Update

Konfigurieren Sie Updateoptionen wie Profile, Alter der Erkennungsroutine, Momentaufnahmen für Modul-Rollbacks, Updatetyp, benutzerdefinierte Updateserver, Verbindungs- und Proxyserver, Updatemirror, Zugriff auf Update-Dateien, HTTP-Server, Details der Benutzerkonten für Netzwerkverbindungen usw.

Netzwerkschutz

Netzwerkschutz verwalten – Bekannte Netzwerke, Zonen, Schutz vor Netzwerkangriffen (IDS), Brute-Force-Angriffsschutz und Botnet-Erkennung.

Web und E-Mail

Konfigurieren Sie Protokollfilter und Ausschlüsse (ausgeschlossene Anwendungen und IP-Adressen), Optionen für die SSL/TLS-Protokollfilterung, E-Mail-Client-Schutz (Integration, E-Mail-Protokolle, Warnungen und Benachrichtigungen), Web-Schutz (HTTP/HTTPS-Webprotokolle und URL-Adressverwaltung) und den Phishing-Schutz für E-Mail-Clients.

Medienkontrolle

Aktivieren Sie die Integration und konfigurieren Sie Regeln und Gruppen für die Medienkontrolle.

Tools

Konfigurieren Sie Tools wie ESET CMD, ESET RMM, WMI-Anbieter, ESET PROTECT-Scanziele, Windows Update-Benachrichtigungen, Logdateien, Proxyserver, E-Mail-Benachrichtigungen, Diagnose, Cluster usw.

Benachrichtigungen

Konfigurieren Sie Benachrichtigungen, die auf dem Desktop angezeigt oder per E-Mail verschickt werden sollen, für Anwendungsstatus, Desktopbenachrichtigungen, interaktive Warnungen und Weiterleitung.

Benutzeroberfläche

Konfigurieren Sie das Programmfenster, die Lizenzinformationen, den Passwortschutz, die eShell Ausführungsrichtlinie und mehr.

Computer

Die Erkennungsroutine schützt Sie vor bösartigen Systemangriffen, indem Dateien, E-Mails und die Netzwerkkommunikation gescannt werden. Wenn ein als Malware eingestuftes Objekt erkannt wird, wird die Behebung gestartet. Die Erkennungsroutine kann das Ereignis zunächst blockieren und anschließend säubern, löschen oder in die Quarantäne verschieben.

Echtzeit- & Machine-Learning-Schutz

Advanced Machine Learning ist jetzt als zusätzliche Schutzebene in der Erkennungsroutine enthalten, um die Erkennung auf Basis von Machine Learning zu verbessern. Weitere Informationen zu diesem Schutztyp finden Sie im Glossar. Sie können Berichterstellung und Schutzebenen für die folgenden Kategorien konfigurieren:

Malware

Computerviren sind Schadcode, der den vorhandenen Dateien auf Ihrem Computer vorangestellt oder angefügt wird. Allerdings wird der Begriff „Virus“ oft falsch angewendet. „Malware“ (Schadcode) ist ein genauerer Begriff. Die Malware-Erkennung wird von der Erkennungsroutine zusammen mit der Machine-Learning-Komponente ausgeführt. Weitere Informationen zu diesem Anwendungstyp finden Sie im Glossar.

Eventuell unerwünschte Anwendungen

Eine eventuell unerwünschte Anwendung ist ein Programm, das nicht zwangsläufig nur böse Absichten verfolgt, jedoch zusätzliche unerwünschte Software installieren, das Verhalten des digitalen Geräts manipulieren, unerwünschte oder unerwartete Aktionen ausführen kann oder sonstige unklare Ziele verfolgt.

Zu dieser Kategorie gehören: Software für Werbeeinblendungen, Download-Wrapper, verschiedene Browser-Werkzeugleisten, Software mit irreführenden Verhaltensweisen, Bundleware, Trackware usw. Weitere Informationen zu diesem Anwendungstyp finden Sie im Glossar.

Verdächtige Anwendungen

Diese Kategorie umfasst Programme, die mit Pack- oder Schutzprogrammen komprimiert wurden. Diese Methoden werden häufig eingesetzt, um Reverse-Engineering zu verhindern oder um den Inhalt des Programms mit proprietären Kompressions- und/oder Verschlüsselungsmethoden zu verschleiern, z. B. um Malware zu verbergen.

In diese Kategorie gehören alle unbekannten Anwendungen, die mit Pack- oder Schutzprogrammen komprimiert wurden.

Potenziell unsichere Anwendungen

Diese Klassifizierung wird für gewerbliche und legitime Software vergeben, die jedoch für bösartige Zwecke missbraucht werden kann. Potenziell unsichere Anwendungen sind gewerbliche Programme, die zu bösartigen Zwecken missbraucht werden können.

Zu dieser Kategorie gehören: Cracker- und Hackerwerkzeuge, Programme zum Generieren von Lizenzschlüsseln, Suchprogramme für Produktschlüssel, Programme für Fernzugriff oder Fernsteuerung, Programme zum Entschlüsseln von Passwörtern, Keylogger usw. Diese Option ist in der Voreinstellung deaktiviert.
Weitere Informationen zu diesem Anwendungstyp finden Sie im Glossar.

Lesen Sie die folgenden Informationen, bevor Sie einen Schwellenwert (oder eine Stufe) für die Berichterstellung oder den Schutz ändern:

Berichterstellung

Die Berichterstellung wird von der Erkennungsroutine und der Machine-Learning-Komponente ausgeführt. Sie können den Schwellenwert für Berichte an Ihre Umgebung und Ihre Anforderungen anpassen. Es gibt keine allgemein gültige Konfiguration. Überwachen Sie das Verhalten in Ihrer Umgebung und passen Sie die Einstellung für die Berichterstellung entsprechend an.
Bei der Berichterstellung werden keine Aktionen an Objekten ausgeführt, sondern nur Informationen an die jeweilige Schutzebene weitergeleitet. Die Schutzebene ist für die entsprechenden Aktionen zuständig.

Aggressiv	**Berichterstellung mit maximaler Empfindlichkeit. Weitere Ereignisse werden gemeldet. Die aggressive Einstellung ist zwar am sichersten, ist jedoch oft zu empfindlich, was sogar kontraproduktiv sein kann.** Bei der aggressiven Einstellung können Objekte fälschlicherweise als bösartig erkannt werden und Aktionen mit solchen Objekten ausgeführt werden (je nach Schutzeinstellungen).
Ausgewogen	Diese Einstellung ist eine optimale Balance zwischen Leistung und Genauigkeit der Erkennungsraten und der Anzahl fälschlich gemeldeter Objekte.
Vorsichtig	Berichte zur Minimierung falsch erkannter Objekte unter Beibehaltung eines ausreichenden Schutzniveaus. Objekte werden nur gemeldet, wenn die Erkennung sehr wahrscheinlich ist und mit dem Verhalten von Malware übereinstimmt.
Aus	Die Berichterstellung ist nicht aktiv. Ereignisse werden nicht gefunden, gemeldet oder gesäubert. Malware-Berichte können nicht deaktiviert werden. Daher ist die Einstellung Aus für Malware nicht verfügbar.

Wenn Sie die Einstellungen in diesem Bereich auf die Standardwerte zurücksetzen möchten, klicken Sie auf den Umkehren-Pfeil neben der Abschnittsüberschrift. Alle in diesem Abschnitt vorgenommenen Änderungen werden verworfen.

Schutz

Wenn ein Objekt gemäß der obigen Konfiguration und der Machine-Learning-Ergebnisse gemeldet wird, wird es gesperrt und eine Aktion wird ausgeführt (säubern, löschen oder in die Quarantäne verschieben).

Aggressiv	Gemeldete ausgewogene (oder niedrigere) Ereignisse werden blockiert und die automatische Behebung (z. B. Säuberung) wird gestartet.
Ausgewogen	Gemeldete ausgewogene (oder niedrigere) Ereignisse werden blockiert und die automatische Behebung (z. B. Säuberung) wird gestartet.
Vorsichtig	Gemeldete ausgewogene Ereignisse werden gesperrt und die automatische Behebung (z. B. Säuberung) wird gestartet.
Aus	Die Berichterstellung ist nicht aktiv, und es werden keine Ereignisse gefunden, gemeldet oder gesäubert. i Malware-Berichte können nicht deaktiviert werden. Daher ist die Option Aus für Malware nicht verfügbar.

Wenn Sie die Einstellungen in diesem Bereich auf die Standardwerte zurücksetzen möchten, klicken Sie auf den Umkehren-Pfeil neben der Abschnittsüberschrift. Alle in diesem Abschnitt vorgenommenen Änderungen werden verworfen.

i Die oben genannten Machine-Learning-Schutzeinstellungen gelten standardmäßig auch für On-Demand-Scans. Bei Bedarf können Sie die Einstellungen für **On-Demand- und Machine-Learning-Schutz** separat konfigurieren. Klicken Sie auf das Schaltersymbol, um die Option **Einstellungen für den Echtzeit-Schutz verwenden** zu deaktivieren und die Konfiguration fortzusetzen.

Erkennung durch Machine Learning

Die Erkennungsroutine schützt Sie vor bösartigen Systemangriffen, indem Dateien, E-Mails und die Netzwerkkommunikation gescannt werden. Wenn ein als Malware eingestuftes Objekt erkannt wird, wird die Behebung gestartet. Die Erkennungsroutine kann das Ereignis zunächst blockieren und anschließend säubern, löschen oder in die Quarantäne verschieben.

Echtzeit- & Machine-Learning-Schutz

Advanced Machine Learning ist jetzt als zusätzliche Schutzebene in der Erkennungsroutine enthalten, um die Erkennung auf Basis von Machine Learning zu verbessern. Weitere Informationen zu diesem Schutztyp finden Sie im Glossar. Sie können Berichterstellung und Schutzebenen für die folgenden Kategorien konfigurieren:

Malware

Computerviren sind Schadcode, der den vorhandenen Dateien auf Ihrem Computer vorangestellt oder angefügt wird. Allerdings wird der Begriff „Virus“ oft falsch angewendet. „Malware“ (Schadcode) ist ein genauerer Begriff. Die Malware-Erkennung wird von der Erkennungsroutine zusammen mit der Machine-Learning-Komponente ausgeführt. Weitere Informationen zu diesem Anwendungstyp finden Sie im Glossar.

Eventuell unerwünschte Anwendungen

Eine eventuell unerwünschte Anwendung ist ein Programm, das nicht zwangsläufig nur böse Absichten verfolgt, jedoch zusätzliche unerwünschte Software installieren, das Verhalten des digitalen Geräts manipulieren, unerwünschte oder unerwartete Aktionen ausführen kann oder sonstige unklare Ziele verfolgt.

Zu dieser Kategorie gehören: Software für Werbeeinblendungen, Download-Wrapper, verschiedene Browser-Werkzeugleisten, Software mit irreführenden Verhaltensweisen, Bundleware, Trackware usw. Weitere Informationen zu diesem Anwendungstyp finden Sie im Glossar.

Verdächtige Anwendungen

Diese Kategorie umfasst Programme, die mit Pack- oder Schutzprogrammen komprimiert wurden. Diese Methoden werden häufig eingesetzt, um Reverse-Engineering zu verhindern oder um den Inhalt des Programms mit proprietären Kompressions- und/oder Verschlüsselungsmethoden zu verschleiern, z. B. um Malware zu verbergen.

In diese Kategorie gehören alle unbekannten Anwendungen, die mit Pack- oder Schutzprogrammen komprimiert wurden.

Potenziell unsichere Anwendungen

Diese Klassifizierung wird für gewerbliche und legitime Software vergeben, die jedoch für bösartige Zwecke missbraucht werden kann. Potenziell unsichere Anwendungen sind gewerbliche Programme, die zu bösartigen Zwecken missbraucht werden können.

Zu dieser Kategorie gehören: Cracker- und Hackerwerkzeuge, Programme zum Generieren von Lizenzschlüsseln, Suchprogramme für Produktschlüssel, Programme für Fernzugriff oder Fernsteuerung, Programme zum Entschlüsseln von Passwörtern, Keylogger usw. Diese Option ist in der Voreinstellung deaktiviert.
Weitere Informationen zu diesem Anwendungstyp finden Sie im Glossar.

Lesen Sie die folgenden Informationen, bevor Sie einen Schwellenwert (oder eine Stufe) für die Berichterstellung oder den Schutz ändern:

^ Berichterstellung

Die Berichterstellung wird von der Erkennungsroutine und der Machine-Learning-Komponente ausgeführt. Sie können den Schwellenwert für Berichte an Ihre Umgebung und Ihre Anforderungen anpassen. Es gibt keine allgemein gültige Konfiguration. Überwachen Sie das Verhalten in Ihrer Umgebung und passen Sie die Einstellung für die Berichterstellung entsprechend an.
Bei der Berichterstellung werden keine Aktionen an Objekten ausgeführt, sondern nur Informationen an die jeweilige Schutzebene weitergeleitet. Die Schutzebene ist für die entsprechenden Aktionen zuständig.

Aggressiv	**Berichterstellung mit maximaler Empfindlichkeit. Weitere Ereignisse werden gemeldet. Die aggressive Einstellung ist zwar am sichersten, ist jedoch oft zu empfindlich, was sogar kontraproduktiv sein kann.** i Bei der aggressiven Einstellung können Objekte fälschlicherweise als bösartig erkannt werden und Aktionen mit solchen Objekten ausgeführt werden (je nach Schutzeinstellungen).
Ausgewogen	Diese Einstellung ist eine optimale Balance zwischen Leistung und Genauigkeit der Erkennungsraten und der Anzahl fälschlich gemeldeter Objekte.
Vorsichtig	Berichte zur Minimierung falsch erkannter Objekte unter Beibehaltung eines ausreichenden Schutzniveaus. Objekte werden nur gemeldet, wenn die Erkennung sehr wahrscheinlich ist und mit dem Verhalten von Malware übereinstimmt.
Aus	Die Berichterstellung ist nicht aktiv. Ereignisse werden nicht gefunden, gemeldet oder gesäubert. i Malware-Berichte können nicht deaktiviert werden. Daher ist die Einstellung Aus für Malware nicht verfügbar.

Wenn Sie die Einstellungen in diesem Bereich auf die Standardwerte zurücksetzen möchten, klicken Sie auf den Umkehren-Pfeil neben der Abschnittsüberschrift. Alle in diesem Abschnitt vorgenommenen Änderungen werden verworfen.

^ E-Mail-Transport- und Machine-Learning-Schutz

Berichterstellung
Wird von der Erkennungsroutine und der Machine-Learning-Komponente ausgeführt. Bei der Berichterstellung werden keine Aktionen an Objekten ausgeführt (dafür ist die jeweilige Schutzebene zuständig).
Schutz
Konfigurieren Sie die Parameter unter E-Mail-Transportschutz, um festzulegen, welche Aktionen an gemeldeten Objekten ausgeführt werden. Außerdem können Sie benutzerdefinierte Regeln konfigurieren:

Beispiel für Kerninstallation:
Ziel: Nachrichten in die Quarantäne verschieben, die Malware oder passwortgeschützte, verschlüsselte oder beschädigte Anhänge enthalten
Erstellen Sie die folgende Regel für den **Mail-Transport-Schutz**
Bedingung
Typ: **Scan-Ergebnis des Virenschutzes**
Operation: **ist**
Parameter: **Infiziert - nicht gesäubert**
Aktion
Typ: **E-Mail in Quarantäne verschieben**

Wenn Sie die Einstellungen in diesem Bereich auf die Standardwerte zurücksetzen möchten, klicken Sie auf den Umkehren-Pfeil neben der Abschnittsüberschrift. Alle in diesem Abschnitt vorgenommenen Änderungen werden verworfen.
Konfigurieren Sie den Machine-Learning-Schutz mit eShell. Der Kontextname in eShell ist **MLP**. Öffnen Sie eShell im interaktiven Modus und navigieren Sie zu MLP:

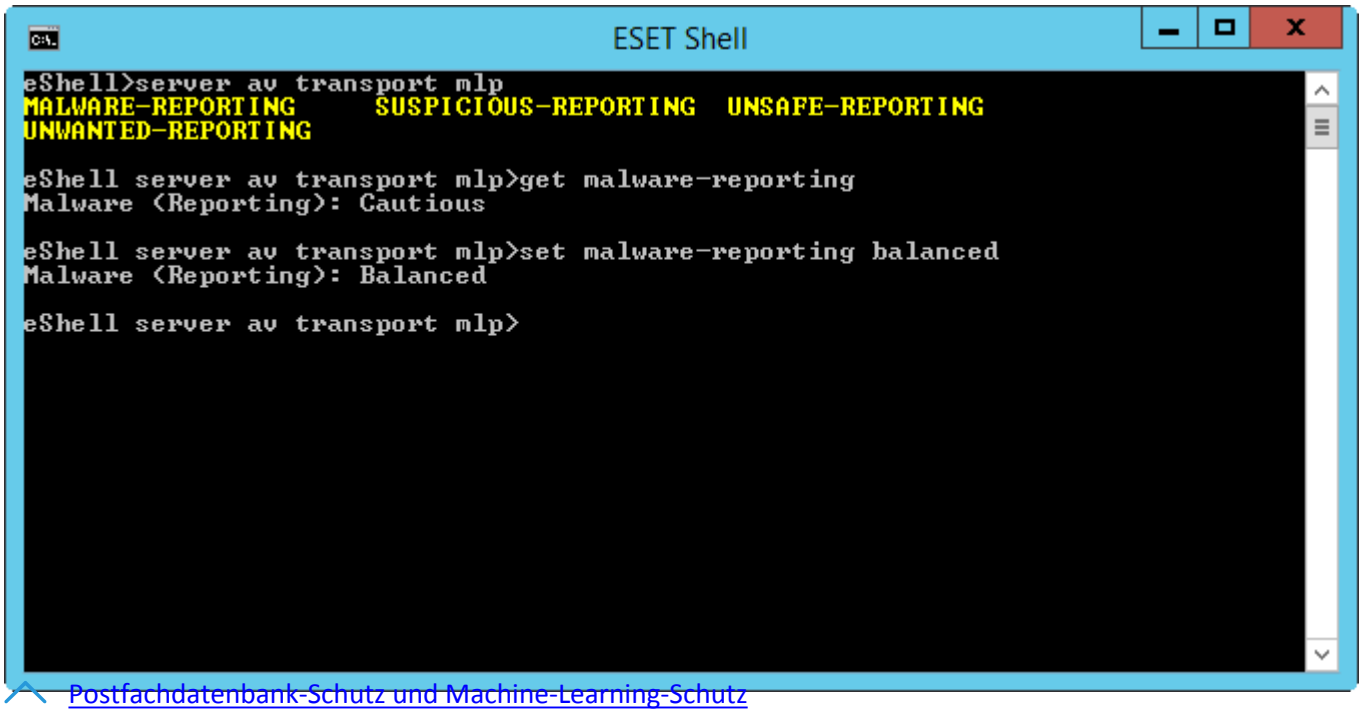
```
server av transport mlp
```

Aktuelle Berichterstellungseinstellung für verdächtige Anwendungen anzeigen:

```
get suspicious-reporting
```

Ändern Sie die Einstellung zu „Vorsichtig“, um die Berichterstellungseinstellungen zu lockern:

```
set suspicious-reporting cautious
```



Postfachdatenbank-Schutz und Machine-Learning-Schutz

Berichterstellung
Wird von der Erkennungsroutine und der Machine-Learning-Komponente ausgeführt. Bei der Berichterstellung werden keine Aktionen an Objekten ausgeführt (dafür ist die jeweilige Schutzebene zuständig).
Schutz
Konfigurieren Sie die Parameter unter Postfach-Datenbankschutz, um festzulegen, welche Aktionen an gemeldeten Objekten ausgeführt werden.
Wenn Sie die Einstellungen in diesem Bereich auf die Standardwerte zurücksetzen möchten, klicken Sie auf den Umkehren-Pfeil neben der Abschnittsüberschrift. Alle in diesem Abschnitt vorgenommenen Änderungen werden verworfen.
Konfigurieren Sie den Machine-Learning-Schutz mit eShell. Der Kontextname in eShell ist **MLP**. Öffnen Sie eShell im interaktiven Modus und navigieren Sie zu MLP:

```
server av database mlp
```

Aktuelle Berichterstellungseinstellung für verdächtige Anwendungen anzeigen:

```
get suspicious-reporting
```

Ändern Sie die Einstellung zu „Vorsichtig“, um die Berichterstellungseinstellungen zu lockern:

```
set suspicious-reporting cautious
```

^ On-Demand-Postfachdatenbank-Scan und Machine-Learning-Schutz

Berichterstellung
Wird von der Erkennungsroutine und der Machine-Learning-Komponente ausgeführt. Bei der Berichterstellung werden keine Aktionen an Objekten ausgeführt (dafür ist die jeweilige Schutzebene zuständig).
Schutz
Konfigurieren Sie die Parameter unter On-Demand-Postfachdatenbank-Scan, um festzulegen, welche Aktionen an gemeldeten Objekten ausgeführt werden.
Wenn Sie die Einstellungen in diesem Bereich auf die Standardwerte zurücksetzen möchten, klicken Sie auf den Umkehren-Pfeil neben der Abschnittsüberschrift. Alle in diesem Abschnitt vorgenommenen Änderungen werden verworfen.
Konfigurieren Sie den Machine-Learning-Schutz mit eShell. Der Kontextname in eShell ist **MLP**. Öffnen Sie eShell im interaktiven Modus und navigieren Sie zu MLP:

```
server av on-demand mlp
```

Aktuelle Berichterstellungseinstellung für verdächtige Anwendungen anzeigen:

```
get suspicious-reporting
```

Ändern Sie die Einstellung zu „Vorsichtig“, um die Berichterstellungseinstellungen zu lockern:

```
set suspicious-reporting cautious
```

Ausschlussfilter

Mit dem Ausschlussfilter können Sie festlegen, welche Dateien und Ordner von Prüfungen ausgenommen werden sollen. Um zu gewährleisten, dass möglichst alle Objekte auf Bedrohungen gescannt werden, empfehlen wir, nur bei dringendem Bedarf Ausnahmen zu erstellen. In bestimmten Fällen kann es jedoch erforderlich sein, ein Objekt vom Scan auszuschließen, beispielsweise bei großen Datenbankeinträgen, deren Scannen die Computerleistung zu stark beeinträchtigen würde, oder bei Software, die Konflikte mit dem Scan verursacht (z. B. Backup-Software).

Nicht zu verwechseln mit ausgeschlossenen Erweiterungen, Prozessausschlüssen oder dem Ausschlussfilter.

Eine Bedrohung, die sich in einer Datei befindet, die die Kriterien des Ausschlussfilters erfüllt, kann vom Echtzeit-Dateischutz und beim Scannen des Computers nicht erkannt werden.

Wählen Sie den Ausschlusstyp aus und klicken Sie auf **Bearbeiten**, um neue Elemente hinzuzufügen oder vorhandene zu ändern:

- Leistungsausschlüsse - Dateien und Ordner vom Scannen ausschließen.
- Ereignisausschlüsse - Objekte anhand von bestimmten Kriterien von der Prüfung ausschließen: Pfad, Dateihash oder Ereignisname.

Leistungsausschlüsse

Mit dieser Funktion können Sie Dateien und Ordner vom Scannen ausschließen. Leistungsausschlüsse sind hilfreich, um unternehmenskritische Anwendungen auf Dateiebene vom Scannen auszuschließen, oder wenn die Scans ein anormales Systemverhalten verursachen oder die Leistung beeinträchtigen.

Pfad

Schließt einen bestimmten Pfad (Datei oder Verzeichnis) für diesen Computer aus. Verwenden Sie keine Platzhalter (Sternchen *) in der Mitte von Pfaden. Weitere Informationen finden Sie im folgenden Knowledgebase-Artikel .

Vergessen Sie beim Ausschließen von Ordnerinhalten nicht, das Sternchen (*) am Ende des Pfades hinzuzufügen (*C:\Tools**).
C:\Tools wird nicht ausgeschlossen, da *Tools* aus der Perspektive des Scanners ebenfalls ein Dateiname sein könnte.

Kommentar

Fügen Sie einen optionalen Kommentar hinzu, um den Ausschluss in Zukunft leicht erkennen zu können.

Pfadausschlüsse mit Sternchen:
C:\Tools* - Pfad muss mit umgekehrtem Schrägstrich (\) und Sternchen (*) enden, um anzugeben, dass es sich um einen Ordner handelt und dass sämtliche Ordnerinhalte (Dateien und Unterordner) ausgeschlossen werden.
C:\Tools*.* - Dasselbe Verhalten wie C:\Tools*, also rekursive Funktionsweise
C:\Tools*.dat – Schließt dat-Dateien im Ordner „Tools“ aus.
C:\Tools\sg.dat – Schließt eine bestimmte Datei im Ordner „Tools“ aus.

Geben Sie den Pfad zum Ordner mit der Maske „*.*“ ein, um alle Dateien in einem bestimmten Ordner auszuschließen. Verwenden Sie die Maske „*.doc“, um nur doc-Dateien auszuschließen.
Wenn der Name einer ausführbaren Datei aus einer bestimmten Anzahl von (variierenden) Zeichen besteht und Sie nur den ersten sicher wissen (zum Beispiel „D“), verwenden Sie folgendes Format:
D????.exe (Die Fragezeichen ersetzen die fehlenden oder unbekannten Zeichen)

Sie können Systemvariablen wie %PROGRAMFILES% verwenden, um Scan-Ausschlüsse zu definieren.
Um den Ordner „Programme“ mit dieser Systemvariable auszuschließen, verwenden Sie den Pfad %PROGRAMFILES%\ (achten Sie auf den umgekehrten Schrägstrich am Ende des Pfads, wenn Sie Ausschlüsse angeben).
Um alle Dateien in einem Unterverzeichnis von %HOMEDRIVE% auszuschließen, verwenden Sie den Pfad %HOMEDRIVE%\Excluded_Directory*.*.
Im Format für Pfad-Ausschlüsse können die folgenden Variablen verwendet werden:
%ALLUSERSPROFILE%
%COMMONPROGRAMFILES%
%COMMONPROGRAMFILES(X86)%
%COMSPEC%
%HOMEDRIVE%
%HOMEPATH%
%PROGRAMFILES%
%PROGRAMFILES(X86)%
%SystemDrive%
%SystemRoot%
%WINDIR%
%PUBLIC%
Benutzerspezifische Systemvariablen (z. B. %TEMP% oder %USERPROFILE%) oder Umgebungsvariablen (z. B. %PATH%) werden nicht unterstützt.

Ereignisausschlüsse

Dies ist eine andere Methode, um Objekte anhand von Ereignisname, Pfad oder Hash vom Scannen auszuschließen. Ereignisausschlüsse schließen im Gegensatz zu Leistungsausschlüssen keine Dateien und Ordner vom Scannen aus. Ereignisausschlüsse schließen Objekte nur aus, wenn diese von der Erkennungsroutine erkannt wurden und eine entsprechende Regel in der Ausschlussliste existiert.

Sie können einen erkennungsbasierten Ausschluss mit einem vorhandenen Ereignis unter **Log-Dateien** > Ereignisse erstellen. Klicken Sie mit der rechten Maustaste auf einen Log-Eintrag (Ereignis) und klicken Sie auf **Ausschluss erstellen**. Daraufhin wird der Ausschluss-Assistent mit vordefinierten Kriterien geöffnet.

Um einen Erkennungsausschluss manuell zu erstellen, Klicken Sie auf **Bearbeiten** > **Hinzufügen** (oder **Bearbeiten**, falls Sie ein vorhandenes Element bearbeiten) und geben Sie eines oder mehrere der folgenden Kriterien an (Kombinationen sind möglich):

Pfad

Schließt einen bestimmten Pfad (Datei oder Verzeichnis) aus. Sie können nach einem Speicherort oder einer Datei suchen oder die Zeichenfolge manuell eingeben. Verwenden Sie keine Platzhalter (Sternchen *) in der Mitte von Pfaden. Weitere Informationen finden Sie im folgenden Knowledgebase-Artikel .

Vergessen Sie beim Ausschließen von Ordnerinhalten nicht, das Sternchen (*) am Ende des Pfades hinzuzufügen (C:\Tools*).
C:\Tools wird nicht ausgeschlossen, da *Tools* aus der Perspektive des Scanners ebenfalls ein Dateiname sein könnte.

Hash

Schließt eine Datei basierend auf dem angegebenen Hash (SHA1) und unabhängig von Dateityp, Speicherort, Name oder Erweiterung aus.

Ereignisname

Geben Sie einen gültigen Ereignisnamen (Bedrohungsname) ein. Ausschlüsse allein anhand des Ereignisnamens können ein Sicherheitsrisiko darstellen. Wir empfehlen, den Ereignisnamen mit dem Pfad zu kombinieren. Diese Ausschlusskriterien können nur für bestimmte Arten von Ereignissen verwendet werden.

Kommentar

Fügen Sie einen optionalen **Kommentar** hinzu, um den Ausschluss in Zukunft leicht erkennen zu können.

Mit ESET PROTECT können Sie Ereignisausschlüsse verwalten, um Ereignisausschlüsse zu erstellen und sie auf mehreren Computern/Gruppen anzuwenden.

Mit Hilfe von Platzhaltern können Sie Gruppen von Dateien ausschließen. Dabei steht ein Fragezeichen (*?*) für genau ein beliebiges Zeichen, ein Sternchen (*) steht für beliebig viele Zeichen oder „kein Zeichen“.

✓ Pfadausschlüsse mit Sternchen:
C:\Tools* - Pfad muss mit umgekehrtem Schrägstrich (\) und Sternchen (*) enden, um anzugeben, dass es sich um einen Ordner handelt und dass sämtliche Ordnerinhalte (Dateien und Unterordner) ausgeschlossen werden.
C:\Tools*.* - Dasselbe Verhalten wie C:\Tools*, also rekursive Funktionsweise
C:\Tools*.dat – Schließt dat-Dateien im Ordner „Tools“ aus.
C:\Tools\sg.dat – Schließt eine bestimmte Datei im Ordner „Tools“ aus.

✓ Um eine Bedrohung auszuschließen, geben Sie einen gültigen Ereignisnamen im folgenden Format an:
@NAME=Win32/Adware.Optmedia
@NAME=Win32/TrojanDownloader.Delf.QQI
@NAME=Win32/Bagle.D

✓ Geben Sie den Pfad zum Ordner mit der Maske „*.*“ ein, um alle Dateien in einem bestimmten Ordner auszuschließen. Verwenden Sie die Maske „*.doc“, um nur doc-Dateien auszuschließen.
Wenn der Name einer ausführbaren Datei aus einer bestimmten Anzahl von (variierenden) Zeichen besteht und Sie nur den ersten sicher wissen (zum Beispiel „D“), verwenden Sie folgendes Format:
D????.exe (Die Fragezeichen ersetzen die fehlenden oder unbekannten Zeichen)

Sie können Systemvariablen wie *%PROGRAMFILES%* verwenden, um Scan-Ausschlüsse zu definieren. Um den Ordner „Programme“ mit dieser Systemvariable auszuschließen, verwenden Sie den Pfad %PROGRAMFILES%\ (achten Sie auf den umgekehrten Schrägstrich am Ende des Pfads, wenn Sie Ausschlüsse angeben).
Um alle Dateien in einem Unterverzeichnis von %HOMEDRIVE% auszuschließen, verwenden Sie den Pfad %HOMEDRIVE%\Excluded_Directory*.*.
Im Format für Pfad-Ausschlüsse können die folgenden Variablen verwendet werden:
%ALLUSERSPROFILE%
%COMMONPROGRAMFILES%
%COMMONPROGRAMFILES(X86)%
%COMSPEC%
%HOMEDRIVE%
%HOMEPATH%
%PROGRAMFILES%
%PROGRAMFILES(X86)%
%SystemDrive%
%SystemRoot%
%WINDIR%
%PUBLIC%
Benutzerspezifische Systemvariablen (z. B. %TEMP% oder %USERPROFILE%) oder Umgebungsvariablen (z. B. %PATH%) werden nicht unterstützt.

Assistent zum Erstellen von Ausschlüssen

Der empfohlene Ausschluss wird anhand des Ereignistyps vorab ausgewählt, Sie können jedoch weitere Ausschlusskriterien für Ereignisse festlegen. Klicken Sie auf **Kriterien ändern**:

- **Exakte Dateien** - Dateien nach ihrem SHA-1-Hash ausschließen.
- **Ereignis** - Geben Sie den Ereignisnamen an, um die Dateien auszuschließen, die dieses Ereignis enthalten.
- **Pfad + Ereignis** - Geben Sie den Ereignisnamen und -Pfad (inklusive Dateiname) an, um alle Dateien mit einem Ereignis am angegebenen Speicherort auszuschließen.

Fügen Sie einen optionalen **Kommentar** hinzu, um den Ausschluss in Zukunft leicht erkennen zu können.

Erweiterte Optionen

Anti-Stealth-Technologie

Ein fortschrittliches System zur Erkennung gefährlicher Programme wie Rootkits, die versuchen, sich vor dem Betriebssystem zu verstecken. Diese Programmtypen werden mit Standardtechniken oft nicht erkannt.

AMSI

Mit der Microsoft Anti-Malware-Scan-Oberfläche (AMSI) können Sie PowerShell-Skripts scannen, die vom Windows Script Host ausgeführt werden.

Automatische Ausschlüsse

Die Entwickler von Server-Anwendungen und -Betriebssystemen empfehlen für die meisten ihrer Produkte, kritische Arbeitsdateien und -ordner vom Virenschutz auszuschließen. Malware-Scans können die Serverleistung beeinträchtigen, Konflikte verursachen und sogar die Ausführung mancher Anwendungen auf dem Server verhindern. Mit Ausschlussfiltern können Sie das Konfliktrisiko beim Ausführen Ihres Malware-Schutzes minimieren und die Gesamtleistung des Servers verbessern. Machen Sie sich mit der Liste der von der Prüfung ausgeschlossenen Dateien für ESET-Serverprodukte vertraut.

Die Funktion „Automatische Ausschlüsse“ wird aktiviert, wenn Sie ESET Mail Security mit einer gültigen Lizenz aktiviert und ein erstes Update durchführen, um die neuesten Module einzubinden.

Automatische Ausschlüsse für Microsoft SQL Server-Datenbankdateien verwenden den standardmäßigen Speicherort. Falls Sie Eine Microsoft SQL Server-Datenbank an einem anderen Ort als dem Standardspeicherort verwenden, haben Sie zwei Optionen zur Auswahl. Sie können die Ausschlüsse manuell hinzufügen oder die Datenbankdateien automatisch ausschließen lassen. Für den automatischen Ausschluss benötigt ESET Mail Security Lesezugriff auf die Microsoft SQL Server-Instanz, um herauszufinden, unter welchen Pfaden sich die Datenbankdateien befinden. Falls ESET Mail Security eine Fehlermeldung über unzureichende Berechtigungen anzeigt, erteilen Sie dem Konto NO_AUTHORITY\SYSTEM die Berechtigung **VIEW ANY DEFINITION** für alle Microsoft SQL Server-Instanzen auf dem Server, auf dem ESET Mail Security ausgeführt wird.
Weitere Informationen finden Sie im Knowledgebase-Artikel zum Hinzufügen von Berechtigungen zum Abrufen von Datenbankdatenspeicherorten, um automatische Ausschlüsse für Microsoft SQL Server zu generieren.

ESET Mail Security identifiziert Anwendungen und Betriebssystem-Dateien, die für den Server kritisch sind, und übernimmt sie automatisch in die Liste Ausgeschlossene Elemente. Standardmäßig sind alle automatischen Ausschlüsse aktiviert. Sie können ausgeschlossene Serveranwendungen mit dem Schieberegler einzeln aktivieren oder deaktivieren. Dabei geschieht Folgendes:

- Wenn Sie eine Anwendung aktivieren, werden alle zugehörigen kritischen Dateien und Ordner zur Liste der vom Scannen ausgeschlossenen Elemente hinzugefügt. Bei jedem Neustart des Servers überprüft das System die Ausschlüsse automatisch und aktualisiert die Liste, falls Änderungen am System oder den Anwendungen vorgenommen wurden (z. B. wenn eine neue Serveranwendung installiert wurde). Diese Einstellung sorgt dafür, dass die empfohlenen automatischen Ausschlüsse immer angewendet werden.

- Beim Deaktivieren werden die ausgeschlossenen Dateien und Ordner aus der Liste entfernt. Vom Benutzer manuell definierte Ausschlüsse sind davon nicht betroffen.

Die automatischen Ausschlüsse für Exchange-Server basieren auf den Empfehlungen von Microsoft. ESET Mail Security wendet nur „Verzeichnis- und Ordnerausschlüsse“ an („Prozessausschlüsse“ und „ausgeschlossene Dateierweiterungen“ werden nicht angewendet). Weitere Informationen finden Sie in den folgenden Artikeln der Microsoft-Knowledgebase:

Update zu den Exchange Server-Virenschutzausschlüssen

Empfehlungen für die Virenprüfung auf Unternehmenscomputern, auf denen unterstützte Windows-Versionen ausgeführt werden

Antivirenprüfungen auf Dateiebene für Exchange 2010

Antivirensoftware im Betriebssystem auf Exchange-Servern (Exchange 2013)

Ausführen von Windows-Virenschutzsoftware auf Exchange 2016-Servern

> In der Datenbankverfügbarkeitsgruppe (Database Availability Group, DAG) auf dem lokalen Server existieren ebenfalls ausgeschlossene Exchange-Datenbankdateien für aktive und passive Datenbanken. Die Liste der automatisch ausgeschlossenen Dateien wird alle 30 Minuten aktualisiert. Neu erstellte Exchange-Datenbankdateien werden unabhängig von ihrem Status (aktiv oder passiv) automatisch ausgeschlossen.

ESET Mail Security verwendet die dedizierte Anwendung eAutoExclusions.exe im Installationsordner, um automatische Ausschlüsse zu identifizieren und zu generieren. Dazu ist kein Eingreifen Ihrerseits erforderlich, aber Sie können eAutoExclusions.exe -servers in der Befehlszeile ausführen, um die auf Ihrem System erkannten Serveranwendungen aufzulisten. Mit `eAutoExclusions.exe -?` können Sie die vollständige Syntax anzeigen.

Eingedrungene Schadsoftware wurde erkannt

Schadsoftware kann auf vielen Wegen in das System gelangen. Mögliche Eintrittsstellen sind Websites, freigegebene Ordner, E-Mails oder Wechselmedien (USB-Sticks, externe Festplatten, CDs, DVDs, Disketten usw.).

Standardmäßiges Verhalten

ESET Mail Security kann Bedrohungen mit einem der folgenden Module erkennen:

- Echtzeit-Dateischutz
- Web-Schutz
- E-Mail-Client-Schutz
- On-Demand-Prüfung

Standardmäßig wenden die Module die normale Säuberungsstufe an und versuchen, die Datei zu säubern und in die Quarantäne zu verschieben, oder die Verbindung zu beenden. Im Infobereich der Taskleiste rechts unten auf dem Bildschirm wird ein Hinweisfenster angezeigt. Weitere Informationen zu den Säuberungsstufen und zum Verhalten des Produkts finden Sie unter Säubern.

Schadcode entfernen und löschen

Ist für den Echtzeit-Dateischutz keine vordefinierte Aktion angegeben, werden Sie in einem Warnungsfenster aufgefordert, zwischen verschiedenen Optionen zu wählen. In der Regel stehen die Optionen **Säubern**, **Löschen** und **Keine Aktion** zur Auswahl. Die Auswahl der Option **Keine Aktion** ist nicht empfehlenswert, da infizierte Dateien mit dieser Einstellung nicht gesäubert werden. Einzige Ausnahme: Sie sind sich sicher, dass die Datei harmlos ist und versehentlich erkannt wurde.

Wenden Sie die Option „Säubern“ an, wenn eine Datei von einem Virus mit Schadcode infiziert wurde. In diesem Fall sollten Sie versuchen, den Schadcode aus der infizierten Datei zu entfernen und ihren Originalzustand wiederherzustellen. Wenn die Datei ausschließlich Schadcode enthält, wird sie gelöscht.

Wenn eine infizierte Datei „gesperrt“ ist oder von einem Systemprozess verwendet wird, muss die Datei in der Regel erst freigegeben werden (häufig ist dazu ein Systemneustart erforderlich), bevor sie gelöscht werden kann.

Mehrere Bedrohungen

Falls infizierte Dateien während der Prüfung des Computers nicht gesäubert wurden (oder die Säuberungsstufe

auf **Nicht säubern** festgelegt wurde), so wird ein Warnfenster angezeigt. In diesem wird danach gefragt, wie mit den Dateien verfahren werden soll.

Wählen Sie individuelle Aktionen für einzelne Bedrohungen in der Liste aus oder **wählen Sie eine Aktion für alle aufgelisteten Bedrohungen aus**, wählen Sie eine Aktion für alle Bedrohungen in der Liste aus und klicken Sie auf **Fertig stellen**.

Dateien in Archiven löschen

Im Standard-Säuberungsmodus wird das gesamte Archiv nur gelöscht, wenn es ausschließlich infizierte Dateien enthält. Archive, die auch nicht infizierte Dateien enthalten, werden also nicht gelöscht.

Verwenden Sie die Option „Immer versuchen, automatisch zu entfernen“ mit Bedacht, da in diesem Modus alle Archive gelöscht werden, die mindestens eine infizierte Datei enthalten, und zwar unabhängig vom Status der restlichen Dateien im Archiv.

Echtzeit-Dateischutz

Der Echtzeit-Dateischutz überwacht alle für den Virenschutz relevanten Systemereignisse. Alle Dateien werden beim Öffnen, Erstellen oder Ausführen auf Ihrem Computer auf Schadcode geprüft. Der Echtzeit-Dateischutz wird standardmäßig beim Systemstart geladen und fortlaufend ausgeführt.

In Ausnahmefällen (z. B. bei einem Konflikt mit einem anderen Echtzeit-Scanner) kann der Echtzeit-Schutz deaktiviert werden. Deaktivieren Sie dazu die Option **Echtzeit-Dateischutz automatisch starten** in den **erweiterten Einstellungen** (**F5**) unter **Echtzeit-Dateischutz** > **Einfach**.

ESET Mail Security ist mit Computern kompatibel, die Azure File Sync den Agenten mit aktiviertem Cloud-Tiering verwenden. ESET Mail Security erkennt Dateien mit dem Attribut *FILE_ATTRIBUTE_RECALL_ON_DATA_ACCESS*.

Zu scannende Datenträger

In der Standardeinstellung werden alle Datenträger auf mögliche Bedrohungen geprüft:

- **Lokale Laufwerke** - Geprüft werden alle lokalen Laufwerke
- **Wechselmedien** - Geprüft werden CDs/DVDs, USB-Speichergeräte, Bluetooth-Geräte usw.
- **Netzlaufwerke** - Geprüft werden alle zugeordneten Netzlaufwerke

Es wird empfohlen, diese Einstellungen nur in Ausnahmefällen zu ändern, z. B. wenn die Prüfung bestimmter Datenträger die Datenübertragung deutlich verlangsamt.

Prüfen beim

Standardmäßig werden alle Dateien beim Öffnen, Erstellen und Ausführen geprüft. Wir empfehlen Ihnen, die Standardeinstellungen beizubehalten. So bietet der Echtzeit-Dateischutz auf Ihrem Computer maximale Sicherheit:

- **Öffnen von Dateien** - Scannen von Dateien beim Öffnen / Zugreifen.
- **Erstellen von Dateien** - Scannen von Dateien beim Erstellen / Bearbeiten.

- **Ausführen von Dateien** - Scannen von Dateien beim Ausführen.

- **Zugriff auf Wechselmedien** - Scannen beim Zugriff auf Wechselmedien. Wenn Wechselmedien, die einen Bootsektor enthalten, in das Gerät eingefügt werden, wird der Bootsektor sofort gescannt. Mit dieser Option wird das Scannen von Dateien auf Wechselmedien nicht aktiviert. Die Option zum Scannen von Dateien auf Wechselmedien befindet sich unter **Zu scannende Datenträger** > **Wechselmedien**. Lassen Sie die Option Bootsektoren/UEFI in den ThreatSense-Parametern aktiviert, um Wechselmedien mit Bootsektoren korrekt scannen zu können.

Ausgeschlossene Prozesse

Mit dieser Funktion können Sie bestimmte Prozesse ausschließen. Wenn Sie z. B. die Prozesse Ihrer Sicherungssoftware ausschließen, werden alle Dateioperationen dieser Prozesse ignoriert und als sicher betrachtet, um Wechselwirkungen mit dem Sicherungsprozess zu minimieren.

ThreatSense-Parameter

Der Echtzeit-Dateischutz überwacht alle Datenträger auf das Eintreten bestimmter Ereignisse wie den Zugriff auf eine Datei. Der Echtzeit-Dateischutz kann so konfiguriert werden, dass neu erstellte und vorhandene Dateien unterschiedlich behandelt werden. Sie können den Echtzeit-Dateischutz z. B. so konfigurieren, dass neu erstellte Dateien genauer überwacht werden.

Bereits gescannte Dateien werden nicht erneut gescannt (sofern sie nicht geändert wurden), um die Systembelastung durch den Echtzeit-Dateischutz zu minimeren. Nach einem Update der Erkennungsroutine werden die Dateien sofort wieder gescannt. Dieses Verhalten wird mit der **Smart-Optimierung** gesteuert. Wenn die **Smart-Optimierung** deaktiviert ist, werden alle Dateien bei jedem Zugriff gescannt.

Um diese Einstellung zu ändern, drücken Sie **F5**, um die **erweiterten Einstellungen** zu öffnen und erweitern Sie den Bereich **Computer** > **Echtzeit-Dateischutz**. Klicken Sie auf **ThreatSense Parameter** > **Sonstige** und aktivieren bzw. deaktivieren Sie die Option **Smart-Optimierung aktivieren**.

Zusätzliche ThreatSense-Parameter

Sie können die Optionen für **Zusätzliche ThreatSense-Parameter für neu erstellte und geänderte Dateien** bzw. **Zusätzliche ThreatSense-Parameter für ausführbare Dateien** ausführlich bearbeiten.

ThreatSense-Parameter

ThreatSense ist eine Technologie, die verschiedene Methoden zur Erkennung von Bedrohungen verwendet. Die Technologie arbeitet proaktiv, d. h. sie schützt das System auch während der ersten Ausbreitung eines neuen Angriffs. Eingesetzt wird eine Kombination aus Code-Analyse, Code-Emulation, allgemeinen Signaturen und Virussignaturen verwendet, die zusammen die Systemsicherheit deutlich erhöhen. Die Prüfengine kann verschiedene Datenströme gleichzeitig kontrollieren und so die Effizienz und Erkennungsrate steigern. Die ThreatSense-Technologie entfernt auch erfolgreich Rootkits.

> Weitere Hinweise zur Prüfung der Systemstartdateien finden Sie unter Prüfung Systemstartdateien.

in den Einstellungen für ThreatSense können Sie verschiedene Prüfparameter festlegen:

- Dateitypen und -erweiterungen, die geprüft werden sollen

- Die Kombination verschiedener Erkennungsmethoden
- Säuberungsstufen usw.

Um das Einstellungsfenster zu öffnen, klicken Sie im Fenster **Erweiterte Einstellungen** (**F5**) auf **ThreatSense-Einstellungen**. Dies gilt für beliebige Module, die ThreatSense verwenden (siehe unten). Verschiedene Sicherheitsszenarien erfordern unterschiedliche Konfigurationen. Daher können Sie ThreatSense für die folgenden Schutzmodule individuell konfigurieren:

- Mail-Transport-Schutz
- On-Demand-Postfach-Datenbankschutz
- Postfachdatenbank-Schutz
- Hyper-V-Scan
- Echtzeit-Dateischutz
- Malware-Prüfungen
- Prüfen im Leerlaufbetrieb
- Prüfung der Systemstartdateien
- Dokumentenschutz
- E-Mail-Client-Schutz
- Web-Schutz

Die ThreatSense-Parameter sind für jedes Modul optimal eingerichtet. Eine Veränderung der Einstellungen kann den Systembetrieb deutlich beeinflussen. So kann zum Beispiel eine Änderung der Einstellungen für das Prüfen laufzeitkomprimierter Dateien oder die Aktivierung der Erweiterte Heuristik im Modul „Echtzeit-Dateischutz“ dazu führen, dass das System langsamer arbeitet (normalerweise werden mit diesen Methoden nur neu erstellte Dateien geprüft). Es wird empfohlen, die Standard-Parameter für ThreatSense in allen Modulen unverändert beizubehalten. Änderungen sollten nur im Modul „Computer prüfen“ vorgenommen werden.

Zu prüfende Objekte

In diesem Bereich können Sie festlegen, welche Dateien und Komponenten Ihres Computers auf Schadcode gescannt werden sollen.

Arbeitsspeicher

Scannt nach Bedrohungen für den Arbeitsspeicher des Systems.

Bootsektoren/UEFI

Scannt die Bootsektoren auf Viren im Master Boot Record. Im Fall von virtuellen Hyper-V-Computern wird der Laufwerks-MBR im schreibgeschützten Modus geprüft.

WMI-Datenbank

Scannt die gesamte WMI-Datenbank und sucht nach Verweisen auf infizierte Dateien oder als Daten eingebettete Malware.

System-Registry

Scannt die gesamte Systemregistrierung, inklusive aller Schlüssel und Unterschlüssel. Sucht nach Verweisen auf infizierte Dateien oder als Daten eingebettete Malware.

E-Mail-Dateien

Folgende Erweiterungen werden vom Programm unterstützt: DBX (Outlook Express) und EML.

Archive

Folgende Erweiterungen werden vom Programm unterstützt: *ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE* und viele andere.

Selbstentpackende Archive

Selbstentpackende Archive (SFX) sind Archive, die ohne externe Programme dekomprimiert werden können.

Laufzeitkomprimierte Dateien

Im Unterschied zu Standardarchiven werden laufzeitkomprimierte Dateien nach dem Start im Arbeitsspeicher dekomprimiert. Neben statischen laufzeitkomprimierten Dateiformaten (UPX, yoda, ASPack, FSG usw.) kann die Prüfung durch Code-Emulation viele weitere SFX-Typen erkennen.

> Der Postfach-Datenbankschutz prüft angehängte E-Mail-Dateien (z. B. *.eml files*) unabhängig von der Einstellung unter **Zu scannende Objekte**. Dies liegt daran, dass der Exchange Server die angehängte .eml-Datei prüft, bevor sie zur Prüfung an ESET Mail Security weitergegeben wird. Das VSAPI-Plug-In erhält die extrahierten Dateien aus dem .eml-Anhang anstelle der .eml-Originaldatei.

Prüfungseinstellungen

Wählen Sie die Methoden aus, mit denen das System auf Infiltrationen gescannt werden soll. Folgende Optionen stehen zur Verfügung:

Heuristik

Heuristische Methoden sind Verfahren, die (bösartige) Aktivitäten von Programmen analysieren. Auf diese Weise können auch bösartige Programme erkannt werden, die noch nicht in der Malware Scan Engine verzeichnet sind.

Erweiterte Heuristik/DNA-Signaturen

Erweiterte Heuristik beschreibt besondere heuristische Verfahren, die von ESET entwickelt wurden, um eine verbesserte Erkennung von Würmern und Trojanern zu ermöglichen und um Schadprogramme zu finden, die in höheren Programmiersprachen geschrieben wurden. Mit Erweiterte Heuristik werden die Fähigkeiten von ESET-Produkten zur Erkennung von Bedrohungen beträchtlich gesteigert. Mit Signaturen können Viren zuverlässig erkannt werden. Mit automatischen Updates sind Signaturen für neue Bedrohungen innerhalb weniger Stunden verfügbar. Signaturen haben den Nachteil, dass nur bekannte Viren und gering modifizierte Varianten bekannter Viren erkannt werden können.

Säubern

Die Säuberungseinstellungen legen fest, wie sich der Scanner beim Säubern infizierter Dateien verhält. Für den Echtzeit-Schutz und andere Schutzmodule sind die folgenden Behebungs- oder Säuberungsstufen verfügbar.

Ereignis immer beheben

Es wird versucht, Ereignisse beim Säubern von Objekten ohne Benutzereingriff zu beheben. Eine Ausnahme sind Systemdateien. Diese Objekte verbleiben an ihrem ursprünglichen Speicherort, falls ein Ereignis nicht behoben werden kann.

Ereignis beheben, falls sicher, andernfalls beibehalten

Es wird versucht, Ereignisse beim Säubern von Objekten ohne Benutzereingriff zu beheben. Wenn ein Ereignis für Systemdateien oder Archive, die saubere und infizierte Dateien enthalten, nicht behoben werden kann, verbleibt das gemeldete Objekt an seinem ursprünglichen Speicherort.

Ereignis beheben, falls sicher, andernfalls nachfragen

Versucht, das Ereignis beim Säubern von Objekten zu beheben. Wenn ESET Mail Security keine automatische Aktion ausführen kann, werden Sie unter Umständen aufgefordert, eine Aktion auszuwählen (löschen oder ignorieren). Diese Einstellung wird für die meisten Fälle empfohlen.

Immer den Endbenutzer fragen

ESET Mail Security versucht nicht, eine automatische Aktion auszuführen. Sie werden aufgefordert, eine Aktion auszuwählen.

Ausschlussfilter

Die Erweiterung ist der Teil des Dateinamens nach dem Punkt. Die Erweiterung definiert den Typ und den Inhalt einer Datei. In diesem Teil der ThreatSense-Einstellungen können Sie die Dateitypen festlegen, die nicht gescannt werden sollen.

Sonstige

Bei der Konfiguration der Einstellungen für ThreatSense für eine On-Demand-Prüfung des Computers sind folgende Optionen im Abschnitt **Sonstige** verfügbar:

Alternative Datenströme (ADS) prüfen

Bei den von NTFS-Dateisystemen verwendeten alternativen Datenströmen (ADS) handelt es sich um Datei- und Ordnerzuordnungen, die mit herkömmlichen Scan-Techniken nicht erkannt werden. Eingedrungene Schadsoftware tarnt sich häufig als alternativer Datenstrom, um nicht erkannt zu werden.

Hintergrundprüfungen mit geringer Priorität ausführen

Jeder Scanvorgang nimmt eine bestimmte Menge von Systemressourcen in Anspruch. Wenn Sie mit Anwendungen arbeiten, welche die Systemressourcen stark beanspruchen, können Sie einen Hintergrund-Scan mit geringer Priorität aktivieren, um Ressourcen für die Anwendungen zu sparen.

Alle Objekte in Log aufnehmen

Wenn Sie diese Option auswählen, enthält die Logdatei alle gescannten Dateien, und nicht nur infizierte Dateien.

Smart-Optimierung aktivieren

Die Smart-Optimierung verwendet die optimalen Einstellungen, um möglichst effiziente Scanvorgänge bei höchster Geschwindigkeit zu gewährleisten. Die verschiedenen Schutzmodule scannen intelligent und verwenden unterschiedliche Scanmethoden für die jeweiligen Dateitypen. Wenn die Smart-Optimierung deaktiviert ist, werden nur die benutzerdefinierten Einstellungen im ThreatSense-Kern der entsprechenden Module für die Prüfung verwendet.

Datum für 'Geändert am' beibehalten

Aktivieren Sie diese Option, um den Zeitpunkt des ursprünglichen Zugriffs auf geprüfte Dateien beizubehalten (z. B. für die Verwendung mit Datensicherungssystemen), anstatt ihn zu aktualisieren.

Grenzen

Im Bereich „Grenzen“ können Sie die Maximalgröße von Elementen und Stufen verschachtelter Archive festlegen, die geprüft werden sollen:

Standard-Einstellungen Objektprüfung

Aktivieren Sie diese Option, um die Standardeinstellungen zu verwenden (keine Einschränkungen). ESET Mail Security ignoriert Ihre benutzerdefinierten Einstellungen.

Maximale Objektgröße

Definiert die maximale Größe der zu scannenden Objekte. Das entsprechende Schutzmodul scannt nur Elemente, die kleiner als die angegebene Maximalgröße sind. Diese Option sollte nur von erfahrenen Benutzern geändert werden, die größere Elemente aus bestimmten Gründen vom Scannen ausschließen möchten. Der Standardwert ist unbegrenzt.

Maximale Scanzeit pro Objekt (Sek.)

Definiert die maximale Scan-Dauer für Elemente. Wenn hier ein benutzerdefinierter Wert eingegeben wurde, beendet das Schutzmodul das Scannen von Elementen, sobald diese Zeit abgelaufen ist, egal ob der Scanvorgang abgeschlossen wurde. Der Standardwert ist unbegrenzt.

Einstellungen für Archivprüfung

Deaktivieren Sie die Option **Standardeinstellungen Archivprüfung**, um die Scaneinstellungen für Archive zu ändern.

Archiv-Verschachtelungstiefe

Legt die maximale Tiefe der Virenprüfung von Archiven fest. Standardwert: 10. Für Objekte mit Mail-Transportschutz gilt die Verschachtelungstiefe +1, da der Archivanhang in einer E-Mail bereits als erste Ebene gilt.

Wenn Sie die Verschachtelungstiefe auf 3 festgelegt haben, werden Archivdateien mit der Verschachtelungstiefe 3 auf der Transportebene nur bis zur Ebene 2 geprüft. Wenn der Mail-Transportschutz Archive bis zur Ebene 3 prüfen soll, müssen Sie den Wert für die **Archiv-Verschachtelungstiefe** auf 4 festlegen.

Maximalgröße von Dateien im Archiv

Mit dieser Option können Sie die maximale Dateigröße für Dateien in Archiven (nach der Extraktion) angeben, die geprüft werden sollen. Der Standardwert ist unbegrenzt.

Die Standardwerte sollten nicht geändert werden; unter normalen Umständen besteht dazu auch kein Grund.

Zusätzliche ThreatSense-Parameter

Zusätzliche ThreatSense-Parameter für neu erstellte und geänderte Dateien

Standardmäßig werden Archive unabhängig von ihrer Größe bis zur zehnten Verschachtelungstiefe geprüft. Deaktivieren Sie die Option **Standardeinstellungen Archivprüfung**, um die Einstellungen für Archivscans zu ändern.

Das Infektionsrisiko für neu erstellte oder geänderte Dateien ist vergleichsweise größer als für vorhandene Dateien. Daher prüft das Programm solche Dateien mit zusätzlichen Scanparametern. Zusätzlich zu den üblichen Prüfmethoden auf Signaturbasis wird die Erweiterte Heuristik verwendet. Diese Methode erkennt neue Bedrohungen, bevor ein Update des Moduls veröffentlicht wird. Neben neu erstellten Dateien werden auch selbstentpackende Archive (SFX) und Laufzeit-Packprogramme (intern komprimierte, ausführbare Dateien) gescannt.

Zusätzliche ThreatSense-Parameter für ausführbare Dateien

Standardmäßig wird bei der Dateiausführung keine Erweiterte Heuristik verwendet. Wenn diese Option aktiviert ist, sollten Smart-Optimierung und ESET LiveGrid® unbedingt aktiviert bleiben, um die Auswirkungen auf die Systemleistung gering zu halten.

Von der Prüfung ausgeschlossene Dateiendungen

Die Erweiterung ist der Teil des Dateinamens nach dem Punkt. Die Erweiterung definier den Typ einer Datei. Normalweise werden alle Dateien geprüft. Falls Sie jedoch Dateien mit einer bestimmten Erweiterung ausschließen möchten, können Sie mit dem ThreatSense-Parameter Dateien anhand ihrer Erweiterung von der Prüfung ausschließen. Diese Methode ist hilfreich, wenn die Prüfung bestimmter Dateitypen dazu führt, dass eine Anwendung nicht korrekt ausgeführt wird.

Klicken Sie auf „**Hinzufügen**“, um eine neue Erweiterung zur Liste hinzuzufügen. Geben Sie die Erweiterung in das Textfeld ein (z. B. tmp), und klicken Sie auf **OK**. Mit der Option **Mehrere Werte eingeben** können Sie mehrere durch Zeilenumbrüche, Kommas oder Semikolon getrennte Erweiterungen eingeben (wählen Sie z. B. **Semikolon** als Trennzeichen im Dropdownmenü aus, und geben Sie `edb;eml;tmp` ein).
Sie können das ? (Fragezeichen) als Sonderzeichen verwenden. Das Fragezeichen steht für ein beliebiges Symbol (z. B. `?db`).

Um die Erweiterung (den Dateityp) für alle Dateien unter Windows anzuzeigen, müssen Sie die Markierung der Option **Erweiterungen bei bekannten Dateitypen ausblenden** unter **Systemsteuerung** > **Ordneroptionen** > **Ansicht** aufheben.

Ausgeschlossene Prozesse

Mit dieser Funktion können Sie Anwendungsprozesse von den Echtzeit-Scans des Malware-Schutzes ausschließen. Aufgrund der entscheidenden Rolle wichtiger Server (Anwendungsserver, Speicherserver usw.) müssen unbedingt regelmäßig Sicherungen angelegt werden, um die Server bei einem Incident wiederherstellen zu können.

Zur Verbesserung von Sicherungsgeschwindigkeit, Prozessintegrität und Dienstverfügbarkeit werden bei Sicherungen bestimmte Techniken angewendet, die zu Konflikten mit Malware-Schutzlösungen auf der Dateiebene führen können. Bei Live-Migrationen virtueller Computer können ähnliche Probleme auftreten.

Die einzig effektive Lösung zur Vermeidung dieser beiden Situationen ist eine Deaktivierung der Malware-Schuzsoftware. Wenn Sie einen Prozesse ausschließen (z. B. die Prozesse der Sicherungssoftware), werden alle Dateioperationen dieser Prozesse ignoriert und als sicher betrachtet. Auf diese Weise werden Wechselwirkungen mit dem Sicherungsprozess minimiert. Wir empfehlen Vorsicht beim Ausschließen von Prozessen, da ausgeschlossene Sicherungssoftware zum Beispiel auf infizierte Dateien zugreifen kann, ohne einen Alarm auszulösen. Aus diesem Grund sind erweiterte Berechtigungen nur für den Echtzeitschutz erlaubt.

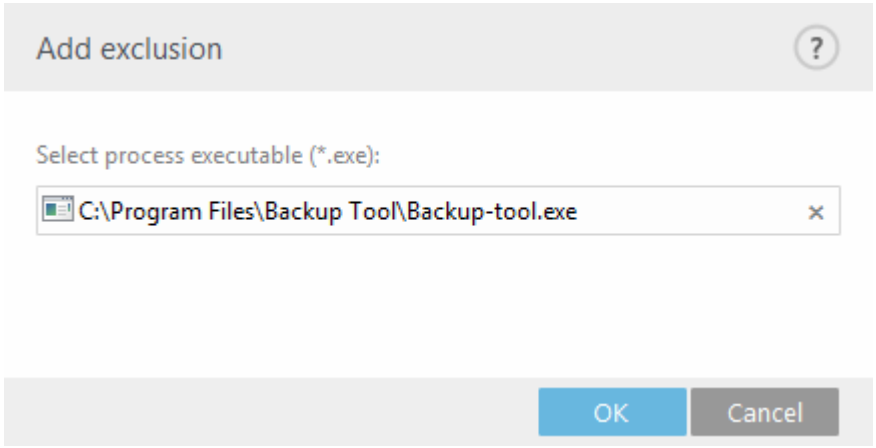
Durch Ausschließen von Prozessen können Sie die Gefahr von Konflikten minimieren und die Leistung der ausgeschlossenen Anwendungen verbessern, was sich wiederum positiv auf die Gesamtleistung des Betriebssystems auswirkt. Prozesse und Anwendungen werden anhand ihrer ausführbaren Datei (*.exe*) ausgeschlossen.

Sie können ausführbare Dateien unter **Erweiterte Einstellungen (F5)** > **Computer** > **Echtzeit-Dateischutz** >**Allgemein** > **Ausgeschlossene Prozesse** zur Liste der ausgeschlossenen Prozesse hinzufügen oder die Liste der ausgeführten Prozesse im Hauptmenü unter **Tools** > **Ausgeführte Prozesse** verwenden.

Diese Funktion wurde entwickelt, um Sicherungstools auszuschließen. Durch das Ausschließen des Sicherungsprozesse wird die Systemstabilität gewährleistet und die Leistung der Sicherung verbessert, da die Sicherung bei der Ausführung nicht verlangsamt wird.

Klicken Sie auf **Bearbeiten**, um das Fenster **Ausgeschlossene Prozesse** zu öffnen, in dem Sie Ausschlüsse **hinzufügen** und nach ausführbaren Dateien (z. B. Backup-tool.exe) suchen können, die Sie vom Scannen ausschließen möchten.
Sobald Sie die *.exe*-Datei zu den Ausschlüssen hinzugefügt haben, wird die Aktivität des Prozesses nicht mehr von ESET Mail Security überwacht, und die Dateiaktivitäten dieses Prozesses werden nicht mehr gescannt.

Falls Sie die ausführbare Datei nicht über die Durchsuchen-Funktion auswählen, müssen Sie deren vollständigen Pfad manuell angeben. Andernfalls funktioniert der Ausschluss nicht korrekt, und HIPS meldet möglicherweise Fehler.



Sie können vorhandene Prozesse **bearbeiten** oder aus den Ausschlüssen **löschen**.

Der Web-Schutz berücksichtigt diese Liste dagegen nicht. Wenn Sie also die ausführbare Datei Ihres Webbrowsers ausschließen, werden heruntergeladene Dateien dennoch gescannt. Auf diese Weise können Angriffe weiterhin erkannt werden. Dieses Szenario ist lediglich ein Beispiel und keine Empfehlung, Webbrowser auszuschließen.

Cloudbasierter Schutz

ESET LiveGrid® ist ein Frühwarnsystem, das aus verschiedenen cloudbasierten Technologien besteht. Es unterstützt die Erkennung neuer Bedrohungen auf Grundlage einer Reputationstechnologie und verbessert durch die Verwendung von Positivlisten die Scan-Leistung. Neue Bedrohungsinformationen werden in Echtzeit zur Cloud gesendet, sodass das ESET-Virenlabor jederzeit einen schnellen und konsistenten Schutz vor Bedrohungen bieten kann. Benutzer können sich direkt im Programmfenster oder im jeweiligen Kontextmenü anzeigen lassen, wie ausgeführte Prozesse oder Dateien eingeschätzt werden. Zudem sind über ESET LiveGrid® weitere Informationen verfügbar.

Wählen Sie bei der Installation von ESET Mail Security eine der folgenden Optionen aus:

- Sie haben die Möglichkeit, ESET LiveGrid® nicht zu aktivieren. Die Funktionalität in der Software geht nicht verloren, in einigen Fällen reagiert ESET Mail Security jedoch möglicherweise langsamer auf neue Bedrohungen als ein Update der Datenbank der Malware Scan Engine.

- Sie können ESET LiveGrid® so konfigurieren, dass Informationen über neue Bedrohungen und Fundstellen von gefährlichem Code übermittelt werden. Diese Datei kann zur detaillierten Analyse an ESET gesendet werden. Durch die Untersuchung dieser Bedrohungen kann ESET die Fähigkeit seiner Software zur Erkennung von Schadsoftware aktualisieren und verbessern.

ESET LiveGrid® sammelt Daten über neue Bedrohungen, die auf Ihrem Computer erkannt wurden. Dazu können auch Proben oder Kopien der Datei gehören, in der eine Bedrohung aufgetreten ist, der Pfad zu dieser Datei, der Dateiname, Datum und Uhrzeit, der Prozess, über den die Bedrohung auf Ihrem Computer in Erscheinung getreten ist, und Informationen zum Betriebssystem des Computers.

ESET Mail Security Ist standardmäßig so konfiguriert, dass verdächtige Dateien zur Analyse an ESET eingereicht werden. Dateien mit bestimmten Erweiterungen (z. B. .docx oder .xlsx) sind immer von der Übermittlung ausgeschlossen. Sie können andere Dateierweiterungen hinzufügen, wenn es bestimmte Dateitypen gibt, die Sie oder Ihr Unternehmen nicht übermitteln möchten.

ESET LiveGrid®-Reputationssystem aktivieren (empfohlen)

Das ESET LiveGrid®-Reputationssystem verbessert die Wirksamkeit der ESET-Sicherheitslösungen, indem es gescannte Dateien mit Positiv- und Negativlisten in einer Datenbank in der Cloud vergleicht.

ESET LiveGrid®-Feedbacksystem aktivieren (empfohlen)

Die Daten werden zur weiteren Analyse an das ESET-Virenlabor übermittelt.

Absturzberichte und Diagnosedaten senden

Reichen Sie Daten wie Absturzberichte, Module und Arbeitsspeicherdumps ein.

Anonyme Statistiken senden

Ermöglicht ESET die Erfassung von Informationen über neu erkannte Bedrohungen wie Name, Datum und Uhrzeit der Erkennung, Erkennungsmethode und verknüpfte Metadaten, gescannte Dateien (Hash, Dateiname, Ursprung der Datei, Telemetrie), gesperrte oder verdächtige URLs und die Produktversion und -konfiguration, einschließlich Daten zum System.

E-Mail-Adresse für Rückfragen (optional)

Sie können mit den verdächtigen Dateien eine E-Mail-Adresse für Rückfragen angeben, wenn zur Analyse weitere Informationen erforderlich sind. Beachten Sie, dass Sie nur dann eine Antwort von ESET erhalten, wenn weitere Informationen von Ihnen benötigt werden.

Samples einreichen

Infizierte Sample automatisch einreichen
Diese Option sendet alle infizierten Proben zur Analyse und Verbesserung der zukünftigen Erkennung an ESET.
- Alle infizierten Proben
- Alle Proben mit Ausnahme von Dokumenten
- Nicht übermitteln

Verdächtige Sample automatisch einreichen
Verdächtige Dateien mit möglichen Bedrohungen und/oder Dateien mit ungewöhnlichen Eigenschaften oder Verhaltensweisen werden zur Analyse an ESET gesendet.
- **Ausführbar** - Ausführbare Dateien: .exe, .dll, .sys
- **Archive** - Archivdateien: .zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab
- **Skripts** - Skriptdateien: .bat, .cmd, .hta, .js, .vbs, .js, .ps1
- **Andere** - Andere Dateitypen:.jar, .reg, .msi, .swf, .lnk
- **Mögliche Spam-E-Mails** – Verbessert die globale Spam-Erkennung.
- **Dokumente** – Umfasst Microsoft Office-Dokumente und PDFs mit aktiven Inhalten

Ausschlussfilter
Klicken Sie auf Bearbeiten neben „Ausschlussfilter“ in ESET LiveGrid®, um festzulegen, wie Bedrohungen zur Analyse an ESET gesendet werden.
Maximalgröße für Proben (MB)
Definiert die maximale Größe der zu scannenden Proben.

ESET LiveGuard Advanced

So aktivieren Sie ESET LiveGuard Advanced in der ESET PROTECT-Web-Konsole auf einem Clientcomputer: Erstellen Sie in der ESET PROTECT-Web-Konsole eine neue Policy oder bearbeiten Sie eine vorhandene Policy und weisen Sie sie zu den Computern zu, auf denen Sie ESET LiveGuard Advanced verwenden möchten.

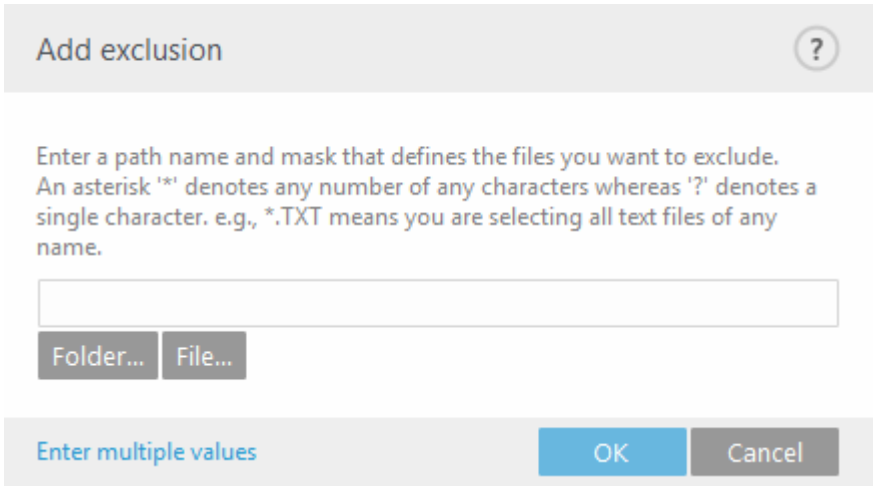
Ausschlussfilter

Über diese Option können Sie bestimmte Dateien oder Ordner vom Senden ausschließen. Hier können Dateien eingetragen werden, die eventuell vertrauliche Informationen enthalten, wie zum Beispiel Textdokumente oder Tabellen.

Hier aufgelistete Dateien werden nicht zur Analyse an ESET übermittelt, auch wenn sie verdächtigen Code enthalten.

Einige typische Dateitypen sind bereits in der Standardeinstellung in die Liste eingetragen (z. B. *.doc*). Sie können der Ausschlussliste weitere Dateien hinzufügen.

Wenn Sie ESET LiveGrid® einige Zeit verwendet haben, kann es sein, dass auch nach dem Deaktivieren des Systems noch einige Datenpakete zum Senden vorliegen. Derartige Datenpakete werden auch nach der Deaktivierung noch an ESET gesendet. Nachdem alle aktuellen Informationen versendet wurden, werden keine weiteren Pakete mehr erstellt.



Wenn Sie eine verdächtige Datei finden, können Sie sie zur Analyse an unser Virenlabor einreichen. Sollte dabei schädlicher Code zu Tage treten, wird dieser beim nächsten Update des Erkennungsmoduls berücksichtigt.

Malware-Scans

Dieser Abschnitt enthält Optionen für die Auswahl von Scanparametern.

Diese Scanprofil-Auswahl gilt für **On-Demand-** und für Hyper-V-Scans.

Ausgewähltes Profil

Diese Parameter werden vom On-Demand-Scanner verwendet. Sie können eines der vordefinierten Scanprofile verwenden oder ein neues Profil erstellen. Die Scanprofile verwenden jeweils unterschiedliche Parameter für das ThreatSense-Modul.

Profilliste

Klicken Sie auf **Bearbeiten**, um ein neues Profil zu erstellen. Geben Sie einen Namen für das Profil ein und klicken Sie auf **Hinzufügen**. Das neue Profil wird im Dropdownmenü **Ausgewähltes Profil** neben den vorhandenen Scanprofilen angezeigt.

Scanziele

Wenn nur ein bestimmtes Objekt gescannt werden soll, können Sie auf **Bearbeiten** klicken und eine Option im Dropdownmenü oder bestimmte Objekte aus der Ordnerstruktur auswählen.

ThreatSense-Parameter

Hier können Sie die Einstellungen für den On-Demand-Scanner ändern.

On-Demand- & Machine-Learning-Schutz

Die Berichterstellung wird von der Erkennungsroutine und der Machine-Learning-Komponente ausgeführt.

Profilmanager

Im Dropdownmenü Scanprofil können Sie vordefinierte Scanprofile auswählen:

- Smart-Prüfung
- Prüfung in Kontextmenüs
- Tiefenprüfung
- Mein Profil (gilt für Hyper-V-Scan, Updateprofile)

Eine Beschreibung der einzelnen Scan-Profile finden Sie im Abschnitt Einstellungen für ThreatSense. So können Sie ein Scan-Profil erstellen, das auf Ihre Anforderungen zugeschnitten ist.

Der Profilmanager wird an drei Stellen in ESET Mail Security verwendet.

On-Demand-Prüfung

Ihre bevorzugten Einstellungen können für zukünftige Prüfungen gespeichert werden. Wir empfehlen Ihnen, für jede regelmäßig durchgeführte Prüfung ein eigenes Profil zu erstellen (mit verschiedenen zu prüfenden Objekten, Prüfmethoden und anderen Parametern).

Update

Mit dem Profil-Editor können Benutzer neue Update-Profile erstellen. Es macht nur dann Sinn, benutzerdefinierte Updateprofile zu erstellen, wenn Ihr Computer sich auf mehrere Arten mit den Updateservern verbindet.

Hyper-V-Scan

Erstellen Sie ein neues Profil, indem Sie neben **Profilliste** auf **Bearbeiten** klicken. Das neue Profil wird im Dropdownmenü **Ausgewähltes Profil** neben den vorhandenen Scanprofilen angezeigt.

Profil-Ziele

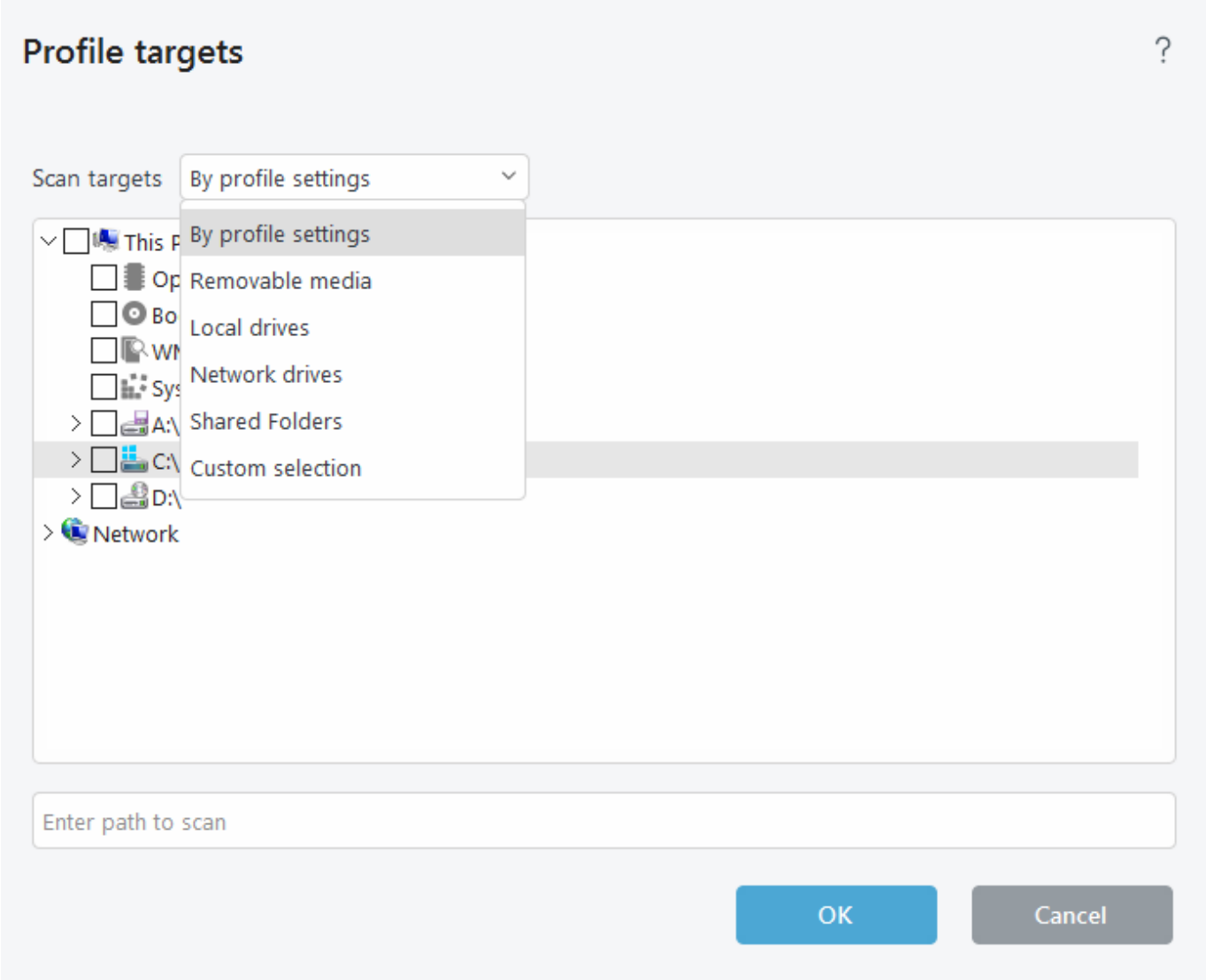
Sie können die Ziele festlegen, die auf Schadcode gescannt werden. Wählen Sie Objekte (Arbeitsspeicher, Bootsektoren und UEFI, Laufwerke, Dateien und Ordner oder Netzwerk) in der Baumstruktur aus, die alle verfügbaren Ziele auf Ihrem System enthält. Klicken Sie auf das Zahnradsymbol in der oberen linken Ecke, um die Dropdownmenüs **Scanziele** und **Scanprofil** zu öffnen.

Diese Scanprofil-Auswahl gilt für On-Demand- und für Hyper-V-Scans.

Arbeitsspeicher	Scannt alle aktuell im Arbeitsspeicher vorhandenen Prozesse und Daten.
Bootsektoren/UEFI	Scannt Bootsektoren und UEFI auf Malware. Weitere Informationen zum UEFI-Scanner finden Sie im Glossar.
WMI-Datenbank	Scannt die gesamte Windows Management Instrumentation-Datenbank (WMI), inklusive aller Namespaces, Klasseninstanzen und Eigenschaften. Sucht nach Verweisen auf infizierte Dateien oder als Daten eingebettete Malware.

Arbeitsspeicher	Scannt alle aktuell im Arbeitsspeicher vorhandenen Prozesse und Daten.
System-Registry	Scannt die gesamte Systemregistrierung, inklusive aller Schlüssel und Unterschlüssel. Sucht nach Verweisen auf infizierte Dateien oder als Daten eingebettete Malware. Beim Säubern der Ereignisse bleibt der Verweis in der Registrierung erhalten, um sicherzustellen, dass keine wichtigen Daten verloren gehen.

Um schnell zu einem Scan-Ziel zu navigieren oder Ordner oder Dateien als Ziele hinzuzufügen, geben Sie das Zielverzeichnis in das leere Textfeld unter der Ordnerliste ein.



Im Dropdownmenü **Scanziele** können Sie ein vordefiniertes Scanziele auswählen:

Nach Profileinstellungen	Die im Scanprofil ausgewählten Ziele werden verwendet.
Wechselmedien	Disketten, USB-Speichergeräte, CDs/DVDs.
Lokale Laufwerke	Alle lokalen Systemlaufwerke.
Netzlaufwerke	Alle zugeordneten Netzlaufwerke.
Freigegebene Ordner	Alle freigegebenen Ordner auf dem lokalen Server.
Benutzerdefinierte Auswahl	Löscht die bisherige Auswahl. Anschließend können Sie Ihre eigene Auswahl treffen.

Geben Sie den Pfad eines Scanziels (Datei oder Ordner) in das Textfeld unter der Baumstruktur ein, um schnell zum entsprechenden Ziel zu navigieren und es zum Scan hinzuzufügen. Die Pfadangabe unterscheidet zwischen Groß- und Kleinschreibung.

Im Dropdownmenü **Scanprofil** können Sie vordefinierte Scanprofile auswählen:

- Smart-Prüfung
- Prüfung in Kontextmenüs
- Tiefenprüfung
- Computerscan

Diese Scanprofile verwenden jeweils unterschiedliche ThreatSense-Einstellungen.

Prüfungsfortschritt anzeigen

Wählen Sie **Nur Prüfen, keine Aktion** aus, wenn Sie das System ohne zusätzliche Säuberungsaktionen prüfen möchten. Auf diese Weise können Sie feststellen, ob Infektionen vorliegen und ggf. Details zu den Infektionen herausfinden. Außerdem können Sie zwischen drei Säuberungsstufen wählen. Klicken Sie dazu auf **Einstellungen** > **ThreatSense -Parameter** > **Säubern**. Die Informationen zur Prüfung werden in einem Log gespeichert.

Prüfen, ohne zu säubern

Wenn Sie Ausschlüsse ignorieren auswählen, können Sie einen Scan ohne die Ausschlüsse durchführen, die normalerweise gelten würden.

Scanziele

Wenn Sie nur bestimmte Objekte prüfen möchten, verwenden Sie die **benutzerdefinierte Prüfung** und wählen Sie die zu prüfenden Objekte im Dropdownmenü **Scan-Ziele** oder in der Ordnerstruktur (Baumstruktur) aus.

Die Auswahl der Scan-Ziele gilt für:

- On-Demand-Scan
- Hyper-V-Scan

Um schnell zu einem zu prüfenden Objekt zu navigieren oder um ein neues Ziel (Ordner oder Dateien) hinzuzufügen, geben Sie den Pfad in das leere Textfeld unter der Ordnerliste ein. Dies ist nur möglich, wenn keine Objekte aus der Baumstruktur zur Prüfung ausgewählt wurden und im Menü **Prüfziele** die Option **Keine Auswahl** festgelegt ist.

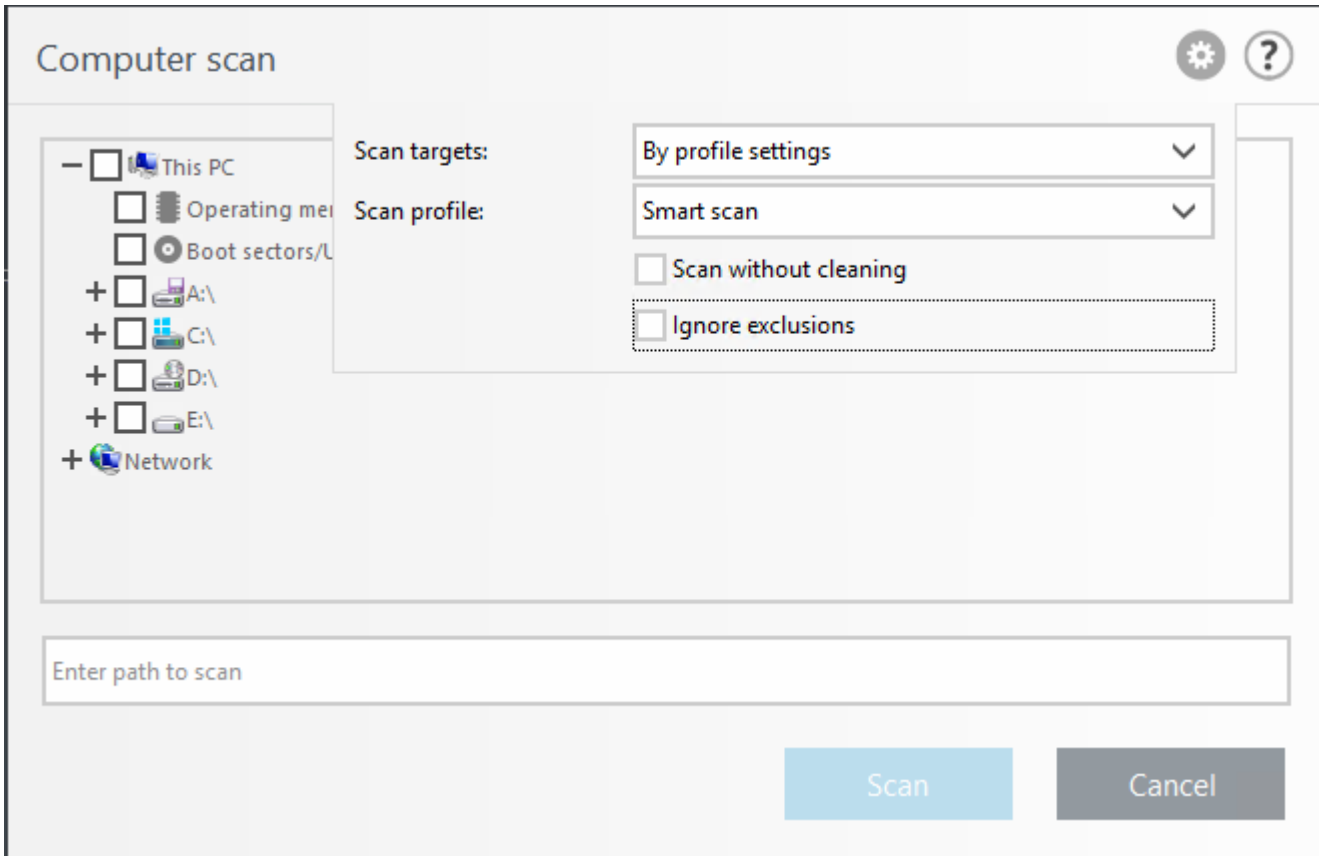
Arbeitsspeicher	Scannt alle aktuell im Arbeitsspeicher vorhandenen Prozesse und Daten.
Bootsektoren/UEFI	Scannt Bootsektoren und UEFI auf Malware. Weitere Informationen zum UEFI-Scanner finden Sie im Glossar.
WMI-Datenbank	Scannt die gesamte Windows Management Instrumentation-Datenbank (WMI), inklusive aller Namespaces, Klasseninstanzen und Eigenschaften. Sucht nach Verweisen auf infizierte Dateien oder als Daten eingebettete Malware.
System-Registry	Scannt die gesamte Systemregistrierung, inklusive aller Schlüssel und Unterschlüssel. Sucht nach Verweisen auf infizierte Dateien oder als Daten eingebettete Malware. Beim Säubern der Ereignisse bleibt der Verweis in der Registrierung erhalten, um sicherzustellen, dass keine wichtigen Daten verloren gehen.

Im Dropdownmenü **Scan-Ziele** können Sie vordefinierte Scanziele auswählen.

Nach Profileinstellungen	Die im Scanprofil ausgewählten Ziele werden verwendet.
Wechselmedien	Disketten, USB-Speichergeräte, CDs/DVDs.
Lokale Laufwerke	Alle lokalen Systemlaufwerke.
Netzlaufwerke	Alle zugeordneten Netzlaufwerke.
Freigegebene Ordner	Alle freigegebenen Ordner auf dem lokalen Server.
Benutzerdefinierte Auswahl	Löscht die bisherige Auswahl. Anschließend können Sie Ihre eigene Auswahl treffen.

Im Dropdownmenü Scan-Profil können Sie ein Profil auswählen, um ausgewählte Objekte zu prüfen. Das Standardprofil ist Smart-Scan. Das Standardprofil ist **Smart-Scan**. Es stehen außerdem zwei weitere vordefinierte Prüfprofile zur Verfügung: Tiefenprüfung und **Kontextmenü-Prüfung**. Diese Scanprofile verwenden jeweils unterschiedliche ThreatSense-Einstellungen.

Das Fenster **Benutzerdefinierter Scan**:



Scannen, ohne zu säubern – Wählen Sie Nur Prüfen, keine Aktion aus, wenn Sie das System ohne zusätzliche Säuberungsaktionen prüfen möchten. Auf diese Weise können Sie feststellen, ob Infektionen vorliegen und ggf. Details zu den Infektionen herausfinden. Außerdem können Sie zwischen drei Säuberungsstufen wählen. Klicken Sie dazu auf Einstellungen > ThreatSense -Parameter > Säubern. Die Informationen zur Prüfung werden in einem Log gespeichert.

Ausschlüsse ignorieren – Führt einen Scan ohne die Ausschlüsse durch, die normalerweise gelten würden.

Aktion nach dem Scan – Wählen Sie im Dropdownmenü aus, welche Aktion nach Abschluss des Scans ausgeführt werden soll.

Scan kann nicht unterbrochen werden – Mit dieser Option können gewöhnliche Benutzer die nach dem Scannen ausgeführten Aktionen nicht unterbrechen.

Benutzer darf den Scan anhalten (Min.) – Gewöhnliche Benutzer können den Computer-Scan für das angegebene Zeitlimit anhalten.

Scan automatisch unterbrechen nach (Min.) – Wenn ein Scan länger als das angegebene Zeitlimit dauert, wird der Vorgang abgebrochen.

Als Administrator scannen – Führt die Prüfung mit dem Administratorkonto aus. Wählen Sie diese Option, wenn der aktuell angemeldete Benutzer keine ausreichenden Zugriffsrechte für die zu scannenden Dateien hat. Diese Schaltfläche ist nur verfügbar, wenn der aktuell angemeldete Benutzer UAC-Vorgänge als Administrator aufrufen kann.

Scan im Leerlaufbetrieb

Wenn der Computer im Leerlauf ist, wird auf allen lokalen Festplatten eine Prüfung ausgeführt. **Die Prüfung im Leerlaufbetrieb** erfolgt, wenn sich der Computer im folgenden Zustand befindet:

- Bildschirm ausgeschaltet oder Bildschirmschoner
- Computersperre
- Benutzerabmeldung

Auch ausführen, wenn der Computer im Akkubetrieb läuft

Diese Prüfung wird nicht ausgeführt, wenn sich der Computer (Notebook) im Batteriebetrieb befindet.

Logging aktivieren

Legt das Ergebnis eines Computer-Scans in den Log-Dateien ab (Klicken Sie im Hauptprogrammfenster auf „Log-Dateien“ und wählen Sie „Computer-Scan“ im Dropdownmenü „Log“ aus).

ThreatSense-Parameter

Ändern Sie die Einstellungen für das Scannen im Leerlaufbetrieb.

Prüfung der Systemstartdateien

Die automatische Prüfung der Systemstartdateien wird standardmäßig beim Systemstart (Benutzeranmeldung) und nach einem erfolgreichen Modulupdate ausgeführt. Die Ausführung des Scans ist abhängig davon, wie der Taskplaner konfiguriert ist und welche Tasks eingerichtet wurden.

Die Optionen für die Prüfung der Systemstartdateien sind Bestandteil des Tasks **Prüfung der Systemstartdateien**.

Navigieren Sie zu **Tools** > **Taskplaner**, wählen Sie einen der Tasks mit dem Namen **Prüfung Systemstartdateien** (Benutzeranmeldung oder Modulupdate) aus und klicken Sie auf **Bearbeiten**. Wenn Sie sich durch den Assistenten klicken, können Sie im letzten Schritt ausführliche Optionen für die Prüfung der Systemstartdateien konfigurieren.

Prüfung Systemstartdateien

Beim Erstellen eines geplanten Tasks für die Prüfung der Systemstartdateien stehen Optionen zum Anpassen der folgenden Parameter zur Verfügung:

Im Dropdown-Menü **Prüfziel** können Sie die Prüftiefe für Dateien festlegen, die beim Systemstart ausgeführt werden. Die Dateien werden auf Grundlage der folgenden Kriterien in aufsteigender Reihenfolge sortiert:

- Alle registrierten Dateien (größte Anzahl gescannter Dateien)
- Selten verwendete Dateien
- Regelmäßig verwendete Dateien
- Häufig verwendete Dateien
- Nur die am häufigsten verwendeten Dateien (kleinste Anzahl gescannter Dateien)

Außerdem stehen zwei besondere Gruppen als Prüfziel zur Verfügung:

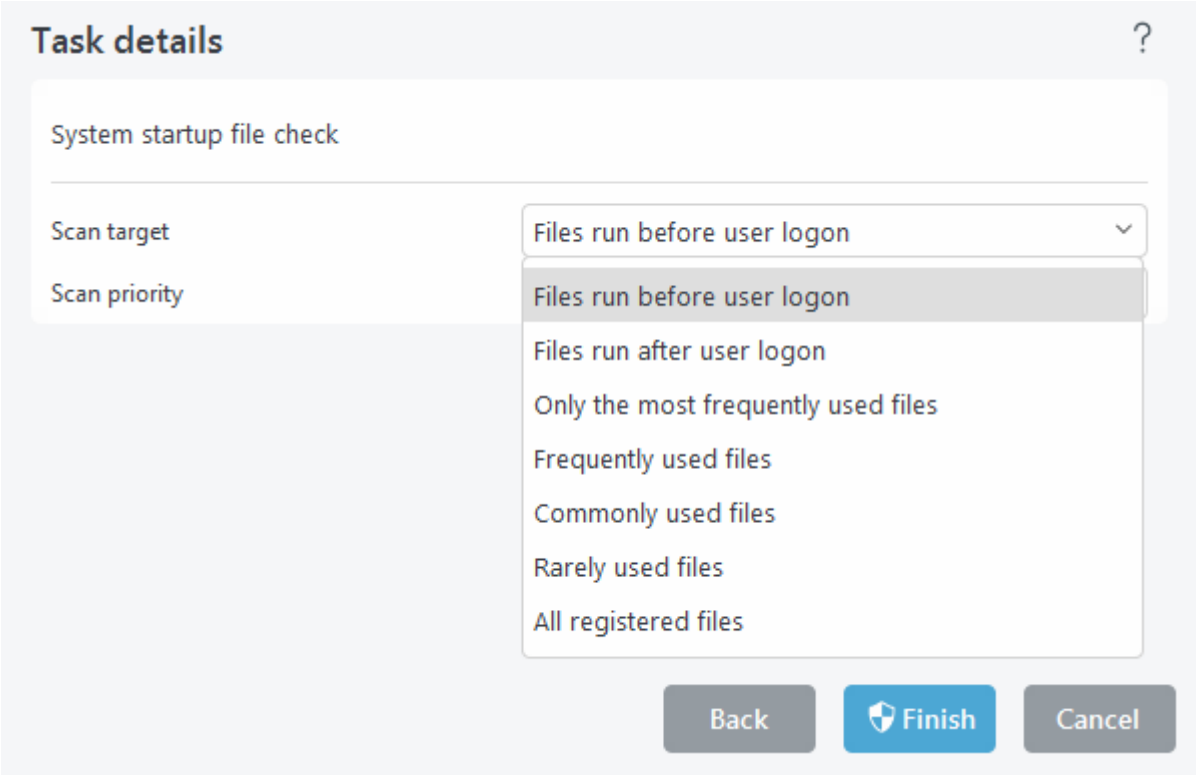
Vor der Benutzeranmeldung ausgeführte Dateien

Enthält Dateien von Standorten, auf die ohne Benutzeranmeldung zugegriffen werden kann (nahezu alle Systemstartstandorte wie Dienste, Browserhilfsobjekte, Windows-Anmeldungshinweise, Einträge im Windows-Taskplaner, bekannte DLL-Dateien usw.).

Nach der Benutzernanmeldung ausgeführte Dateien

Enthält Dateien von Standorten, auf die erst nach einer Benutzeranmeldung zugegriffen werden kann (umfasst Dateien, die nur für einen bestimmten Benutzer ausgeführt werden, üblicherweise im Verzeichnis *HKEY_CURRENT_USER**SOFTWARE**Microsoft**Windows**CurrentVersion**Run*).

Die Liste der zu scannenden Dateien ist für jede der zuvor genannten Gruppen unveränderbar.



Scan-Priorität

Die Priorität, mit der der Scan-Beginn ermittelt wird:

- **Normal** - bei durchschnittlicher Systemlast
- **Niedrig** - bei geringer Systemlast
- **Minimal** - bei minimaler Systemlast
- **Bei Leerlauf** - Der Task wird nur ausgeführt, wenn das System im Leerlauf ist.

Wechselmedien

ESET Mail Security bietet automatische Prüfmethoden für Wechselmedien (CD/DVD/USB). Dieses Modul ermöglicht das Einrichten eines Scans für eingelegte Medien. Dies ist sinnvoll, wenn der Administrator verhindern möchte, dass Benutzer Wechselmedien mit unerwünschten Inhalten verwenden.

Beim Einlegen eines Wechselmediums wird folgender Dialog angezeigt:

- **Jetzt scannen** - Dies löst den Wechselmedienscan aus.
- **Nicht scannen** –Wechselmedien werden nicht gescannt.
- **Einstellungen** – Öffnet die erweiterten Einstellungen.
- **Immer die ausgewählte Option verwenden** – Wenn diese Option aktiviert ist, wird bei jedem Einlegen eines Wechselmediums die gleiche Aktion ausgeführt.

Außerdem enthält ESET Mail Security die Medienkontrolle, mit der Sie Regeln für die Nutzung externer Geräte an einem bestimmten Computer festlegen können.

Um auf die Einstellungen für den Wechselmedien-Scan zu öffnen, navigieren Sie zu **Erweiterte Einstellungen** (**F5**) > **Benachrichtigungen** > **Interaktive Warnungen** > **Bearbeiten**. Wenn **Benutzer fragen** nicht ausgewählt ist, müssen Sie die Aktion auswählen, die ausgeführt werden soll, wenn ein Wechselmedium in den Computer eingelegt wird:

- **Nicht scannen** - Es wird keine Aktion ausgeführt und das Fenster **Neues Gerät** erkannt wird geschlossen.
- **Automatischer Gerätescan** - Eine On-Demand-Prüfung des eingelegten Wechselmediums wird durchgeführt.
- **Erzwungener Geräte-Scan** – Ein Computer-Scan des eingelegten Wechselmediums wird durchgeführt und kann nicht abgebrochen werden.
- **Scanoptionen anzeigen** – Öffnet die Einstellungen für **interaktive Warnungen**.

Dokumentenschutz

Dokumentenschutz - Der Dokumentenschutz überprüft Microsoft Office-Dokumente vor dem Öffnen sowie automatisch von Internet Explorer heruntergeladene Dateien wie Microsoft ActiveX-Elemente. Der Dokumentenschutz bietet eine zusätzliche Schutzebene zum Echtzeit-Dateischutz und kann deaktiviert werden, um auf Systemen, die keiner großen Anzahl an Microsoft Office-Dokumenten ausgesetzt sind, die Leistung zu verbessern.

Systemintegration

Diese Option verbessert den Schutz von Microsoft Office-Dokumenten (unter normalen Umständen nicht benötigt).

ThreatSense-Parameter

Ändern Sie die Parameter für den Dokumentenschutz.

> Die Funktion wird von Anwendungen aktiviert, die Microsoft Antivirus API verwenden (beispielsweise Microsoft Office 2000 und höher oder Microsoft Internet Explorer 5.0 und höher).

Hyper-V-Scan

Die aktuelle Version des Hyper-V-Scans unterstützt Scanvorgänge von virtuellen Systemen in Hyper-V im Online- oder Offlinezustand. Die unterstützten Scan-Typen hängen vom gehosteten Hyper-V-System und vom Zustand des virtuellen Systems ab:

Virtuelle Systeme mit Hyper-V-Funktion	Online-VM	Offline-VM
Windows Server 2022 Hyper-V	Schreibgeschützt	Schreibgeschützt/säubern
Windows Server 2019 Hyper-V	Schreibgeschützt	Schreibgeschützt/säubern
Windows Server 2016 Hyper-V	Schreibgeschützt	Schreibgeschützt/säubern
Windows Server 2012 R2 Hyper-V	Schreibgeschützt	Schreibgeschützt/säubern
Windows Server 2012 Hyper-V	Schreibgeschützt	Schreibgeschützt/säubern

Hardwareanforderungen

Der Server darf keine Performanceprobleme bei der Ausführung virtueller Computer haben. Der Scan verwendet hauptsächlich CPU-Ressourcen. Zum Scannen von Online-VMs wird freier Festplattenplatz benötigt. Es wird mindestens der doppelte freie Speicherplatz benötigt, der von Checkpoints/Snapshots und virtuellen Laufwerken belegt wird.

Spezielle Einschränkungen

- Prüfungen in RAID-Speichern, übergreifenden Volumes und dynamischen Datenträgern werden aufgrund der Funktionsweise dynamischer Datenträger nicht unterstützt. Daher sollten Sie den Einsatz dynamischer Datenträger in Ihren VMs nach Möglichkeit vermeiden.
- Der Scan wird immer für die aktuelle VM ausgeführt. Checkpoints und Snapshots sind nicht betroffen.
- Hyper-V auf Hosts in einem Cluster wird momentan von ESET Mail Security nicht unterstützt.

> Die ESET-Sicherheitsprodukte unterstützen zwar Prüfungen des MBR für virtuelle Datenträger, allerdings können diese Prüfungen für diese Ziele nur im schreibgeschützten Modus durchgeführt werden. Sie finden diese Einstellung unter **Erweiterte Einstellungen** (**F5**) > **Computer** > **Hyper-V-Scan** > ThreatSense-Parameter > **Bootsektoren**.

Zu scannende virtuelle Maschine ist offline – (ausgeschaltet)

ESET Mail Security verwendet den Hyper-V-Manager, um virtuelle Datenträger zu erkennen und zu verbinden. Auf diese Weise hat ESET Mail Security denselben Zugriff auf den Inhalt der virtuellen Laufwerke wie beim Zugriff auf Daten und Dateien auf herkömmlichen Laufwerken.

Zu scannende virtuelle Maschine ist online – (in Betrieb, angehalten, gespeichert)

ESET Mail Security verwendet den Hyper-V-Manager, um virtuelle Datenträger zu erkennen. Eine Verbindung zu diesen Datenträgern ist nicht möglich. Daher erstellt ESET Mail Security einen Checkpoint/Snapshot der virtuellen Maschine und verbindet sich anschließend mit diesem Checkpoint/Snapshot. Nach Abschluss der Prüfung wird der Checkpoint/Snapshot gelöscht. In diesem Fall wird also eine schreibgeschützte Prüfung durchgeführt, da die laufenden virtuellen Maschinen nicht von der Prüfung betroffen sind.

Warten Sie ca. eine Minute, bis ESET Mail Security beim Scannen einen Snapshot bzw. Checkpoint erstellt hat. Dies ist hilfreich, falls Sie vorhaben, einen Hyper-V-Scan auf einer größeren Anzahl virtueller Maschinen auszuführen.

Namenskonvention

Das Modul für die Hyper-V-Scan verwendet die folgende Namenskonvention:

```
VirtualMachineName\DiskX\VolumeY
```

Wobei X die Nummer des Laufwerks und Y die Nummer des Volumes ist. Beispiel:

```
Computer\Disk0\Volume1
```

Die Zahlen werden in der Reihenfolge der Ereignisse angefügt. Diese Reihenfolge stimmt mit der Reihenfolge im Manager für virtuelle Datenträger überein. Die Namenskonvention wird in der Baumstruktur im Dropdownmenü der Scan-Ziele, in der Fortschrittsleiste und in den Log-Dateien verwendet.

Ausführung einer Prüfung

- On-Demand – Klicken Sie auf **Hyper-V-Scan**, um eine Liste der zum Scannen verfügbaren virtuellen Maschinen und Laufwerke anzuzeigen. Wählen Sie die gewünschten VMs, Laufwerke oder Volumes für die Prüfung aus und klicken Sie auf **Prüfung**.
- So erstellen Sie einen Taskplaner-Task.
- Über ESET PROTECT in Form eines Clienttasks mit dem Namen Serverprüfung.
- Sie können Hyper-V-Scans in eShell verwalten und starten.

Sie können mehrere Hyper-V-Scans parallel ausführen. Nach Abschluss der Prüfung wird eine Benachrichtigung mit einem Link zu den Log-Dateien angezeigt.

Mögliche Probleme

- Beim Scannen von virtuellen Maschinen muss ein Checkpoint oder Snapshot der jeweiligen virtuellen Maschine erstellt werden. Während der Erstellung von Checkpoints oder Snapshots werden einige allgemeine Aktionen der virtuellen Maschine unter Umständen eingeschränkt oder deaktiviert.
- Inaktive virtuelle Computer können nicht eingeschaltet werden, solange eine Prüfung ausgeführt wird.
- Im Hyper-V Manager können Sie zwei virtuelle Maschinen mit identischem Namen anlegen. Dies kann zu Problemen bei der Unterscheidung der Computer in den Scan-Logs führen.

Um ein neues Profil zu erstellen, klicken Sie neben **Profilliste** auf **Bearbeiten**. Geben Sie den **Namen des Profils** ein und klicken Sie auf **Hinzufügen**. Das neue Profil wird im Dropdownmenü **Ausgewähltes Profil** neben den vorhandenen Scanprofilen angezeigt.

Im Dropdownmenü **Scanziele** für **Hyper-V** können Sie vordefinierte Scanziele auswählen:

Nach Profileinstellungen	Die im Scanprofil ausgewählten Ziele werden verwendet.
Alle virtuellen Computer	Wählt alle virtuellen Computer aus.
Eingeschaltete virtuelle Computer	Wählt alle Online-VMs aus.
Ausgeschaltete virtuelle Computer	Wählt alle Offline-VMs aus.
Keine Auswahl	Löscht die bisherige Auswahl.

Klicken Sie auf das Symbol  , ändern Sie das Intervall zu **Scan beenden, wenn dieser länger dauert als [Minuten]** und legen Sie den gewünschten Zeitraum fest (zwischen 1 und 2.880 Minuten).

Klicken Sie auf **Prüfen**, um die Prüfung mit den von Ihnen festgelegten Parametern auszuführen. Sehen Sie nach Abschluss der Scans unter **Log-Dateien** > Hyper-V-Scan nach.

Hyper-V- und Machine-Learning-Schutz

Die Berichterstellung wird von der Erkennungsroutine und der Machine-Learning-Komponente ausgeführt.

ThreatSense-Parameter

In diesem Bereich können Sie die Scan-Parameter für den Hyper-V-Scan anpassen.

HIPS

Das Host Intrusion Prevention System (HIPS) schützt Ihr System vor Schadsoftware und unerwünschten Programmaktivitäten, die negative Auswirkungen auf Ihren Computer haben könnten. HIPS analysiert das Verhalten von Programmen genau und nutzt Netzwerkfilter zur Überwachung von ausgeführten Prozessen, Dateien und Registrierungsschlüsseln. HIPS stellt eine zusätzliche Funktion zum Echtzeit-Dateischutz dar und ist keine Firewall, da nur die im Betriebssystem ausgeführten Prozesse überwacht werden.

Nur erfahrene Benutzer sollten die Einstellungen von HIPS ändern. Eine falsche Konfiguration der HIPS-Einstellungen kann zur Instabilität des Systems führen.

Selbstschutz aktivieren

ESET Mail Security enthält eine integrierte Selbstschutz-Technologie, um zu verhindern, dass Ihr Viren- und Spyware-Schutz durch Malware beschädigt oder deaktiviert werden kann und um Ihr System ununterbrochen zu schützen. Änderungen an den Optionen „HIPS aktivieren“ und „Selbstschutz aktivieren“ treten nach einem Neustart des Windows-Betriebssystems in Kraft. Zum Deaktivieren von HIPS ist ebenfalls ein Computer-Neustart erforderlich.

Protected Service aktivieren

Microsoft hat mir Microsoft Windows Server 2012 R2 das neue Konzept der geschützten Dienste eingeführt. Es verhindert, dass ein Dienst vor Malware-Angriffen schützt. Der Kernel von ESET Mail Security wird standardmäßig als geschützter Dienst ausgeführt. Diese Funktion ist unter Microsoft Windows Server 2012 R2 und neueren Betriebssystemen verfügbar.

Advanced Memory Scanner aktivieren

Diese Funktion bietet zusammen mit dem Exploit-Blocker einen noch besseren Schutz vor Malware, die darauf ausgelegt ist, der Erkennung durch Anti-Malware-Produkte mittels Verschleierung oder Verschlüsselung zu entgehen. Die erweiterte Speicherprüfung ist standardmäßig aktiviert. Weitere Informationen zu diesem Schutztyp finden Sie im Glossar.

Exploit-Blocker aktivieren

Sichert besonders anfällige Anwendungstypen wie Webbrowser, PDF-Leseprogramme, E-Mail-Programme und Microsoft Office-Komponenten. Der Exploit-Blocker ist standardmäßig aktiviert. Weitere Informationen zu diesem Schutztyp finden Sie im Glossar.

Ransomware-Schutz aktivieren

Aktivieren Sie HIPS und ESET Live Grid, um diese Funktion zu verwenden. Weitere Informationen zu Ransomware finden Sie im Glossar.

Filtermodus

Wählen Sie einen der folgenden Filtermodi aus:

- **Automatischer Modus** - Vorgänge werden ausgeführt, mit Ausnahme der Vorgänge, die durch vorab definierte Regeln zum Schutz Ihres Systems blockiert wurden. Alle Vorgänge sind erlaubt, mit Ausnahme von

Aktionen, die durch eine Regel blockiert werden.

- **Smart-Modus** - Der Benutzer wird nur über sehr verdächtige Ereignisse benachrichtigt.

- **Interaktiver Modus** - Der Benutzer wird zur Bestätigung von Vorgängen aufgefordert. Zugriff erlauben / verweigern, Regel erstellen, Diese Aktion vorübergehend anwenden.

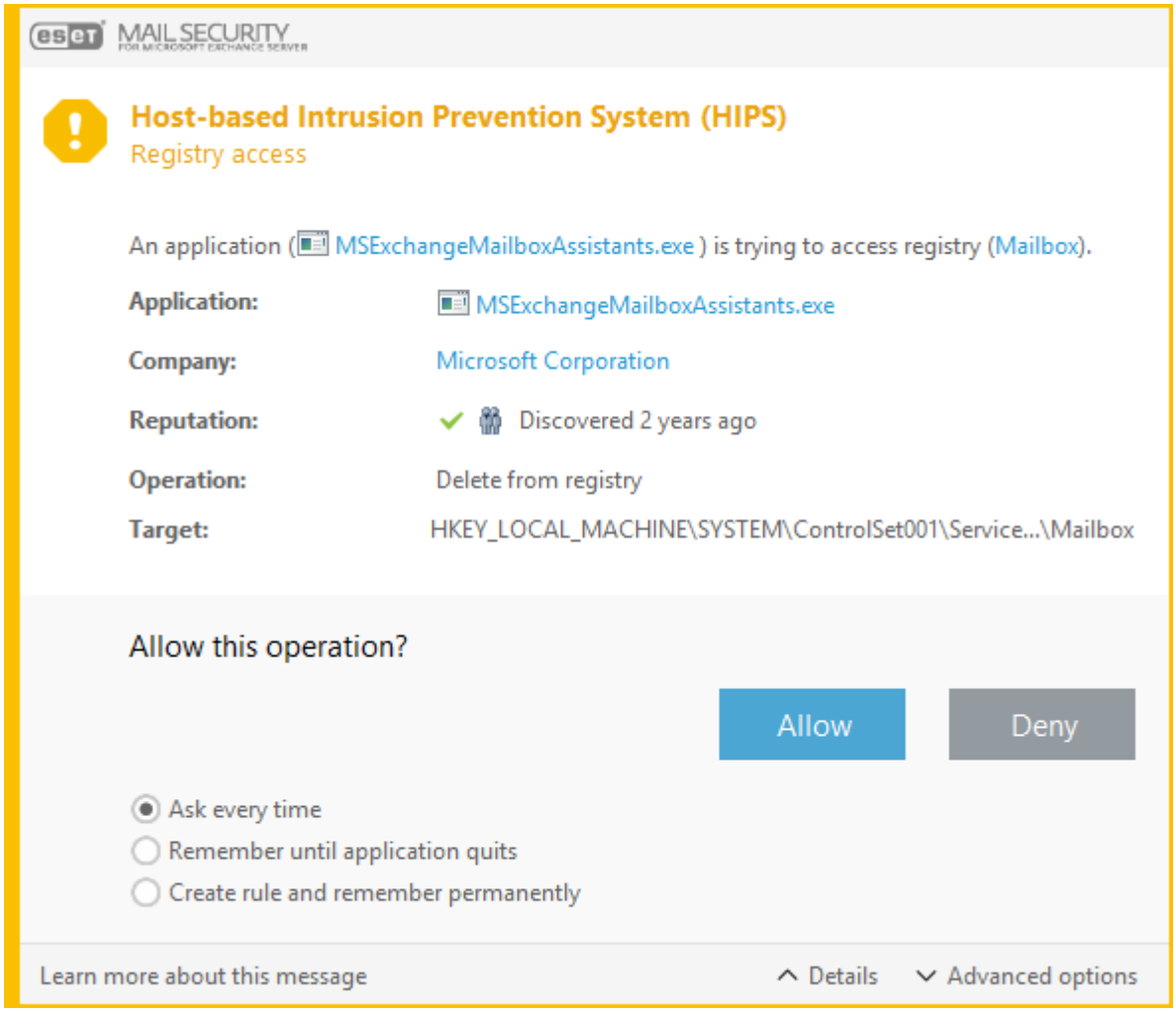
- **Policy-basierter Modus** - Vorgänge werden blockiert. Akzeptiert nur Benutzer- oder vordefinierte Regeln.

- **Trainingsmodus** - Vorgänge werden ausgeführt und nach jedem Vorgang wird eine Regel erstellt. Die in diesem Modus erstellten Regeln können im Regel-Editor angezeigt werden, doch sie haben geringere Priorität als manuell erstellte Regeln oder Regeln, die im automatischen Modus erstellt wurden. Wenn Sie im Dropdownmenü für den HIPS-Filtermodus den Trainingsmodus auswählen, wird die Einstellung Ende des Trainingsmodus verfügbar. Wählen Sie eine Dauer für den Trainingsmodus aus. Die maximale Dauer ist 14 Tage. Wenn die festgelegte Dauer verstrichen ist, werden Sie aufgefordert, die von HIPS im Trainingsmodus erstellten Regeln zu bearbeiten. Sie können auch einen anderen Filtermodus auswählen oder die Entscheidung verschieben und den Trainingsmodus weiterverwenden.

Regeln

Regeln legen fest, welche Anwendungen auf welche Dateien, Registrierungsbereiche oder andere Anwendungen zugreifen dürfen. HIPS überwacht Ereignisse im Betriebssystem und führt Aktionen gemäß Regeln aus, die den Regeln für die Personal Firewall ähneln. Klicken Sie auf Bearbeiten, um das Fenster für die HIPS-Regelverwaltung zu öffnen. Wenn die Standardaktion zu einer Regel **Nachfragen** lautet, wird bei jedem Auslösen der Regel ein Dialogfeld angezeigt. Dort können Sie den Vorgang entweder **Blockieren** oder **Zulassen**. Wenn Sie innerhalb des vorgegebenen Zeitrahmens keine Aktion festlegen, wird gemäß den Regeln eine neue Aktion ausgewählt.

Im Dialogfenster können Sie eine Regel erstellen, die auf einer beliebigen neuen Aktion basiert, die HIPS erkennt. Definieren Sie dann die Bedingungen, unter denen die Aktion **zugelassen** oder **blockiert** werden soll. Unter **Details** finden Sie weitere Informationen. Auf diese Weise erstellte Regeln und manuell erstellte Regeln sind gleichrangig. Daher können erstere allgemeiner sein als die Regel, die das Dialogfenster ausgelöst hat. Nach dem Erstellen einer solchen Regel kann derselbe Vorgang also dasselbe Fenster auslösen.



Jedes Mal fragen

Bei jedem Auslösen der Regel wird ein Dialogfeld angezeigt. Dort können Sie den Vorgang entweder **Blockieren** oder **Zulassen**.

Bis zum Beenden der Anwendung merken

Wenn Sie eine der Aktionen **Blockieren** oder **Zulassen** auswählen, wird eine temporäre HIPS-Regel erstellt und verwendet, bis die entsprechende Anwendung geschlossen wird. Wenn Sie den Filtermodus ändern, Regeln bearbeiten oder das HIPS-Modul aktualisieren und Ihr System neu starten, werden die temporären Regeln ebenfalls gelöscht.

Regel erstellen und dauerhaft merken

Erstellt eine neue HIPS-Regel. Sie können diese Regel später in der HIPS-Regelverwaltung bearbeiten.

HIPS-Regeleinstellungen

Dieses Fenster enthält eine Übersicht vorhandener HIPS-Regeln.

Regel	Benutzerdefinierter oder automatisch ausgewählter Regelname.
Aktiviert	Deaktivieren Sie diesen Schalter, wenn Sie die Regel nicht verwenden, jedoch nicht aus der Liste löschen möchten.

Regel	Benutzerdefinierter oder automatisch ausgewählter Regelname.
Aktion	Die Regel legt eine Aktion fest (Zulassen, Blockieren oder Fragen), die bei Eintreten der Bedingungen ausgeführt wird.
Quellen	Die Regel wird nur angewendet, wenn das Ereignis von einer Anwendung ausgelöst wird.
Ziele	Die Regel wird nur angewendet, wenn sich die Operation auf eine bestimmte Datei, eine Anwendung oder einen Registrierungseintrag bezieht.
Log-Schweregrad	Wenn Sie diese Option aktivieren, werden Informationen zu dieser Regel im HIPS-Log gespeichert.
Hinweis anzeigen	Im Windows-Benachrichtigungsbereich wird ein kleines Fenster angezeigt, wenn ein Ereignis ausgelöst wird.

Erstellen Sie eine neue Regeln, indem Sie auf **Hinzufügen** klicken und neue HIPS-Regeln erstellen, oder **Bearbeiten** Sie ausgewählte Einträge.

Regelname

Benutzerdefinierter oder automatisch ausgewählter Regelname.

Aktion

Die Regel legt eine Aktion fest (**Zulassen**, **Blockieren** oder **Fragen**), die bei Eintreten der Bedingungen ausgeführt wird.

Vorgänge in Bezug auf

Wählen Sie die Art des Vorgangs aus, auf den die Regel angewendet werden soll. Die Regel wird nur bei dieser Art Vorgang und für das ausgewählte Ziel angewendet. Die Regel besteht aus mehreren Teilen, mit denen die Auslösebedingungen der Regel beschrieben werden.

Quellanwendungen

Die Regel wird nur angewendet, wenn das Ereignis von der jeweiligen Anwendung ausgelöst wird. Wählen Sie **Bestimmte Anwendungen** im Dropdownmenü aus und klicken Sie auf **Hinzufügen**, um neue Dateien oder Ordner hinzuzufügen, oder wählen Sie den Eintrag **Alle Anwendungen** aus, um alle Anwendungen hinzuzufügen.

> Bestimmte, von HIPS vordefinierte Regeln und die aus ihnen resultierenden Vorgänge können nicht blockiert werden, da sie standardmäßig zugelassen sind. Hinzu kommt, dass nicht alle Systemvorgänge von HIPS überwacht werden. HIPS überwacht Vorgänge, die als unsicher eingestuft werden könnten.

Beschreibungen der wichtigsten Vorgänge:

Dateibezogene Vorgänge

Datei löschen	Anwendung versucht, die Zieldatei zu löschen.
In Datei schreiben	Anwendung versucht, in die Zieldatei zu schreiben.
Direkter Zugriff auf Datenträger	Die Anwendung versucht, einen Datenträger auf nicht standardmäßige Art auszulesen oder zu beschreiben (die üblichen Windows-Verfahren werden umgangen). So könnten Dateien verändert werden, ohne dass die entsprechenden Regeln in Kraft treten. Verursacher dieses Vorgangs könnte Malware sein, die versucht, ihre Erkennung zu verhindern. Es könnte sich aber auch um Backup-Software handeln, die versucht, die genaue Kopie eines Datenträgers herzustellen, oder eine Partitionsverwaltung beim Versuch, Festplattenvolumes zu reorganisieren.

Datei löschen	Anwendung versucht, die Zieldatei zu löschen.
Globalen Hook installieren	Bezieht sich auf das Aufrufen der Funktion SetWindowsHookEx aus der MSDN-Bibliothek.
Treiber laden	Lädt und installiert Treiber im System.

Die Regel wird nur angewendet, wenn sich der Vorgang auf eines dieser Ziele bezieht. Wählen Sie die Option **Bestimmte Dateien** im Dropdownmenü aus und klicken Sie auf **Hinzufügen**, um neue Dateien oder Ordner hinzuzufügen. Alternativ können Sie im Dropdownmenü **Alle Dateien** auswählen, um alle Anwendungen hinzuzufügen.

Anwendungsbezogene Vorgänge

Andere Anwendung debuggen	Verknüpfen eines Debuggers mit dem Prozess. Beim Debuggen einer Anwendung können Informationen zu deren Verhalten angezeigt und verändert werden, und die Daten der Anwendung sind verfügbar.
Ereignisse von anderer Anwendung abfangen	Die Quellanwendung versucht, für die Zielanwendung bestimmte Ereignisse abzufangen (Beispiel: ein Keylogger versucht, Ereignisse im Browser aufzuzeichnen).
Andere Anwendung beenden/unterbrechen	Die Anwendung unterbricht einen Prozess, setzt ihn fort oder beendet ihn (direkter Zugriff aus dem Prozess-Explorer oder im Fenster „Prozesse“ möglich).
Neue Anwendung starten	Starten neuer Anwendungen oder neuer Prozesse.
Zustand einer anderen Anwendung ändern	Die Quellanwendung versucht, in den Speicher der Zielanwendung zu schreiben oder in ihrem Namen bestimmten Code auszuführen. Diese Funktion kann wichtige Anwendungen schützen, indem diese in einer Regel zum Blockieren des Vorgangs als Zielanwendungen konfiguriert werden.

Die Regel wird nur angewendet, wenn sich der Vorgang auf eines dieser Ziele bezieht. Wählen Sie die Option **Bestimmte Anwendungen** im Dropdownmenü aus und klicken Sie auf **Hinzufügen**, um neue Dateien oder Ordner hinzuzufügen. Alternativ können Sie im Dropdownmenü **Alle Anwendungen** auswählen, um alle Anwendungen hinzuzufügen.

Registrierungsvorgänge

Starteinstellungen ändern	Alle Veränderungen der Einstellungen, die festlegen, welche Anwendungen beim Windows-Start ausgeführt werden. Diese können beispielsweise über den Schlüssel „Run“ in der Windows-Registrierung ermittelt werden.
Aus Registrierung löschen	Registrierungsschlüssel oder -wert löschen.
Registrierungsschlüssel umbenennen	Umbenennen von Registrierungsschlüsseln.
Registrierung ändern	Neue Werte für Registrierungsschlüssel erstellen, vorhandene Werte ändern, Daten im Verzeichnisbaum der Datenbank verschieben oder Benutzer- bzw. Gruppenrechte für Registrierungsschlüssel einrichten.

Die Regel wird nur angewendet, wenn sich der Vorgang auf eines dieser Ziele bezieht. Wählen Sie die Option **Bestimmte Dateien** im Dropdownmenü aus und klicken Sie auf **Hinzufügen**, um neue Dateien oder Ordner hinzuzufügen. Alternativ können Sie im Dropdownmenü **Alle Einträge** auswählen, um alle Anwendungen hinzuzufügen.

Sie können eingeschränkt Platzhalter bei der Eingabe des Ziels verwenden. Anstatt eines bestimmten Schlüssels können Sie das Sonderzeichen * (Sternchen) im Registrierungspfad eingeben. *HKEY_USERS*\software can mean HKEY_USER\.default\software* Bedeuten, jedoch nicht *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*. *HKEY_LOCAL_MACHINE\system\ControlSet** ist kein gültiger Pfad für einen Registrierungsschlüssel. *** in einem Registrierungspfad bedeutet „dieser Pfad oder jeder untergeordnete Pfad nach diesem Symbol“. Platzhalter können nur auf diese Weise für Zieldateien verwendet werden. Zuerst wird der spezifische Teil des Pfades überprüft, dann der Pfad nach dem Platzhalter (*).

Sie erhalten eine Benachrichtigung, wenn Sie eine zu allgemeine Regel erstellen.

Erweiterte HIPS-Einstellungen

Die folgenden Optionen helfen bei der Fehlerbehebung und der Analyse des Verhaltens einer Anwendung:

Treiber dürfen immer geladen werden

Ausgewählte Treiber werden unabhängig vom konfigurierten Filtermodus immer zugelassen, sofern sie nicht durch eine Benutzerregel ausdrücklich blockiert werden. In dieser Liste angezeigte Treiber werden unabhängig vom HIPS-Filtermodus immer zugelassen, sofern sie nicht ausdrücklich durch eine Benutzerregel blockiert werden. Sie können neue Treiber **hinzufügen** oder ausgewählte Treiber in dieser Liste **bearbeiten** oder **löschen**.

Klicken Sie nur auf **Zurücksetzen**, wenn Sie keine manuell hinzugefügten Treiber einschließen möchten. Diese Funktion kann nützlich sein, wenn Sie mehrere Treiber hinzugefügt haben und sie nicht manuell aus der Liste löschen können.

Alle blockierten Vorgänge in Log aufnehmen

Alle blockierten Vorgänge werden in das HIPS-Log geschrieben. Verwenden Sie diese Funktion nur zur Fehlerbehebung oder auf Anfrage des technischen Supports von ESET, da sie eine sehr große Protokolldatei generieren und das System verlangsamen kann.

Änderungen an Autostart-Einträgen melden

Zeigt einen Desktophinweis an, wenn eine Anwendung vom Systemstart entfernt bzw. zum Systemstart hinzugefügt wird.

Update-Konfiguration

Dieser Abschnitt beschreibt Quellinformationen für Updates wie die verwendeten Updateserver und die Authentifizierungsdaten für diese Server.

Um Updates fehlerfrei herunterladen zu können, müssen Sie alle Update-Einstellungen ordnungsgemäß eingeben. Falls Sie eine Firewall verwenden, stellen Sie sicher, dass sich das ESET-Programm mit dem Internet verbinden darf (zum Beispiel per HTTP).

Einfach

Standardupdateprofil auswählen
Wählen Sie ein Standardprofil für Updates aus, oder erstellen Sie ein neues Profil.
Automatischer Profilwechsel
Weisen Sie ein Updateprofil für bekannte Netzwerke in der Firewall zu. Mit dem automatischen Profilwechsel können Sie je nach Einstellung im Taskplaner das Profil für ein bestimmtes Netzwerk ändern. Weitere Informationen finden Sie auf den Hilfeseiten.
Update-Benachrichtigungen konfigurieren
Klicken Sie auf **Bearbeiten**, um auszuwählen, welche Anwendungsbenachrichtigungen angezeigt werden sollen. Sie können auswählen, ob die Benachrichtigungen auf dem Desktop angezeigt oder als E-Mail weitergeleitet werden.
Update-Cache löschen
Wenn Probleme mit einem Update auftreten, klicken Sie auf **Löschen**, um den temporären Update-Cache zu leeren.

Produktupdates

Automatische Updates
Standardmäßig aktiviert. Mit dem Schieberegler können Sie automatische Updates deaktivieren, wenn Sie ESET Mail Security vorübergehend nicht aktualisieren möchten. Wir empfehlen, diese Einstellung aktiviert zu lassen, um sicherzustellen, dass ESET Mail Security die neuesten Updates für Programmkomponenten (PCU) und Mikro-Updates für Programmkomponenten (µPCU) erhält, sobald ein neues Update verfügbar ist.

Die Updates werden nach dem nächsten Serverneustart angewendet.

Warnungen für veraltete Erkennungsroutine

Maximales Alter der Erkennungsroutine automatisch festlegen / Maximales Alter der Erkennungsroutine (Tage)
Mit dem Schieberegler können Sie das automatisch festgelegte Alter der Erkennungsroutine deaktivieren und die maximale Zeit (in Tagen) manuell festlegen, nach der die Erkennungsroutine als veraltet gemeldet wird. Der Standardwert ist 7.

Modul-Rollback

Wenn Sie befürchten, dass ein neues Update der Erkennungsroutine oder der Programmmodule beschädigt oder nicht stabil ist, können Sie einen Rollback zur vorigen Version ausführen und Updates für einen bestimmten Zeitraum deaktivieren. Hier können Sie auch zuvor für einen unbegrenzten Zeitraum deaktivierte Updates wieder aktivieren. ESET Mail Security zeichnet Snapshots der Erkennungsroutine und der Programmmodule zur späteren Verwendung mit der Rollback-Funktion auf. Um Snapshots der Erkennungsroutine zu erstellen, lassen Sie die Option **Snapshots der Module erstellen** aktiviert.
Anzahl der lokal gespeicherten Snapshots
Definiert die Anzahl der gespeicherten älteren Modul-Snapshots.
Rollback auf frühere Module ausführen
Klicken Sie auf Rollback, um die Programm-Module auf die vorherige Version zurückzusetzen und Updates vorübergehend zu deaktivieren.

Profile
Um ein benutzerdefiniertes Updateprofil zu erstellen, wählen Sie **Bearbeiten** neben **Profilliste** aus. Geben Sie einen **Profilnamen** ein, und klicken Sie auf **Hinzufügen**. Wählen Sie das zu bearbeitende Profil aus und bearbeiten Sie die Parameter für Arten von Modulupdates, oder erstellen Sie einen **Update-Mirror**.

Updates

Wählen Sie den Updatetyp im Dropdownmenü aus:
• **Reguläres Update** – Standardmäßig ist der Update-Typ „Reguläres Update“ ausgewählt. Mit dieser Option werden Updates automatisch vom ESET-Server mit der geringsten Last heruntergeladen.
• **Pre-Release-Update** – Diese Updates wurden intern umfassend geprüft und werden demnächst allgemein veröffentlicht. Wenn Sie den Testmodus aktivieren, können Sie früher von den neuesten Erkennungsmethoden und Fehlerkorrekturen profitieren. Da jedoch letzte Fehler nicht ausgeschlossen werden können, sind diese Updates ausdrücklich NICHT für Rechner im Produktivbetrieb vorgesehen, die durchgängig stabil und verfügbar laufen müssen.
• **Verzögerte Updates** – Diese Option führt Updates über besondere Update-Server aus, die neue Versionen der Signaturdatenbank mit einer Verzögerung von mindestens X Stunden zur Verfügung stellen. Die Datenbanken wurden also bereits in einer Produktionsumgebung getestet und sind daher stabil.

Optimierung der Update-Zustellung aktivieren
Wenn diese Option aktiviert ist, werden Update-Dateien aus einem CDN (Content Delivery Network) heruntergeladen. Wenn Sie diese Einstellung deaktivieren, können Downloadunterbrechungen und Verzögerungen auftreten, wenn die dedizierten ESET Updateserver überlastet sind. Das Deaktivieren ist hilfreich, wenn eine Firewall nur auf die IP-Adressen des ESET Updateservers zugreifen kann oder keine Verbindung zu CDN-Diensten möglich ist.

Vor dem Download von Updates fragen
Wenn ein neues Update verfügbar ist, erhalten Sie vor dessen Download eine Aufforderung.

Nachfragen, falls Update größer ist als (KB)
Wenn die Größe der Updatedatei den in diesem Feld angegebenen Wert überschreitet, wird eine Benachrichtigung angezeigt.

Modulupdates

Modulupdates sind standardmäßig auf **Automatische Auswahl** eingestellt. Der Update-Server dient als Speicher für die Updates. Falls Sie einen ESET-Server verwenden, sollten Sie die Standardoption beibehalten.

Wenn Sie einen lokalen HTTP-Server (auch als „Update-Mirror“ bezeichnet) verwenden, konfigurieren Sie den Server wie folgt: http://computer_name_or_its_IP_address:2221
Wenn Sie einen lokalen HTTP-Server mit SSL verwenden, konfigurieren Sie den Server wie folgt: https://computer_name_or_its_IP_address:2221
Wenn Sie einen lokalen freigegebenen Ordner verwenden, konfigurieren Sie den Server wie folgt: \\computer_name_or_its_IP_address\shared_folder

Aktiviert häufigere Updates für Erkennungssignaturen
Die Erkennungsroutine wird in kürzeren Abständen aktualisiert. Wenn Sie diese Option deaktivieren, kann sich dies negativ auf die Erkennungsrate auswirken.

Modulupdates von Wechselmedien zulassen
Updates werden von Wechselmedien ausgeführt, die einen Mirror enthalten. Mit der Option **Automatisch** werden die Updates im Hintergrund ausgeführt. Wählen Sie **Immer nachfragen** aus, um Update-Dialogfelder anzuzeigen.

Produktupdates

Wenn Sie die automatischen Updates für bestimmte Update-Profile anhalten, werden automatische Produktupdates vorübergehend deaktiviert, wenn diese beispielsweise über andere Netzwerke oder getaktete Verbindungen mit dem Internet verbunden sind. Aktivieren Sie diese Einstellung, um stets die neuesten Funktionen und den bestmöglichen Schutz zu erhalten.

In manchen Fällen muss der Server neu gestartet werden, um die Updates zu übernehmen.

Verbindungsoptionen

Proxyserver

Um auf die Optionen der Proxyserver-Einstellungen für ein bestimmtes Updateprofil zuzugreifen, klicken Sie auf die Registerkarte Proxy-Modus und wählen Sie eine dieser drei Optionen aus:

- **Keinen Proxyserver verwenden** – ESET Mail Security verwendet keinen Proxyserver für Updates.
- **Globale Proxyeinstellungen verwenden** – Die unter Erweiterte Einstellungen (F5) > Tools > Proxyserver festgelegte Proxyserver-Konfiguration wird übernommen.
- **Verbindung über Proxyserver** – Verwenden Sie diese Option in den folgenden Fällen:

Verwenden Sie für Updates von ESET Mail Security einen anderen Proxyserver als den in den allgemeinen Einstellungen festgelegten Proxyserver (Tools > Proxyserver). In diesem Fall sind an dieser Stelle Einstellungen erforderlich: Proxyserver-Adresse, Kommunikations-Port (standardmäßig 3128) sowie Benutzername und Passwort für den Proxyserver, falls erforderlich.

Die Proxyserver-Einstellungen nicht für das gesamte Programm festgelegt wurden, ESET Mail Security jedoch Updates über einen Proxyserver herunterladen soll.

Ihr Computer ist über einen Proxyserver mit dem Internet verbunden. Während der Installation werden die Einstellungen aus Internet Explorer übernommen. Falls Sie später Änderungen vornehmen (zum Beispiel wenn Sie den Internetanbieter wechseln), müssen Sie hier die HTTP-Proxy-Einstellungen prüfen und gegebenenfalls ändern. Sonst kann keine Verbindung zu den Update-Servern hergestellt werden.

Die Felder mit den Anmeldedaten (**Benutzername** und **Passwort**) sind nur für den Zugriff auf den Proxyserver vorgesehen. Geben Sie in diesen Feldern nur Daten ein, wenn diese für den Zugriff auf den Proxyserver erforderlich sind. Beachten Sie, dass in diese Felder nicht das Passwort und der Benutzername für ESET Mail Security eingetragen werden. Eine Eingabe ist nur dann erforderlich, wenn Sie für die Internetverbindung über den Proxyserver ein Passwort benötigen.

Direktverbindung verwenden, wenn der Proxy nicht verfügbar ist

Wenn in der Produktkonfiguration die Nutzung eines HTTP-Proxys vorgesehen ist und der Proxy nicht erreichbar ist, umgeht das Produkt den Proxy und kommuniziert direkt mit ESET-Servern.

Windows-Freigaben

Beim Aktualisieren von einem lokalen Windows-Server ist standardmäßig eine Authentifizierung für jede Netzwerkverbindung erforderlich.

Verbindung mit LAN herstellen als

Wählen Sie eine der folgenden Optionen aus, um Ihr Konto zu konfigurieren:

- **Systemkonto (Standard)** – Verwendet das Systemkonto für die Authentifizierung. Normalerweise findet keine Authentifizierung statt, wenn in den Haupteinstellungen für Updates keine Anmeldedaten angegeben sind.
- **Aktueller Benutzer** – Das Programm meldet sich mit dem Konto des aktuell angemeldeten Benutzers an. Diese Lösung hat den Nachteil, dass sich das Programm nicht mit dem Update-Server verbinden kann, wenn kein Benutzer angemeldet ist.
- **Folgender Benutzer** – Mit dieser Option können Sie ein bestimmtes Benutzerkonto für die Authentifizierung angeben. Verwenden Sie diese Option, wenn eine Anmeldung mit dem standardmäßigen Systemkonto nicht möglich ist. Das ausgewählte Benutzerkonto benötigt Zugriffsrechte für den Ordner mit den Update-Dateien. Wenn der Benutzer keinen Zugriff hat, kann sich das Programm nicht verbinden und kann keine Updates herunterladen.

Wenn entweder **Aktueller Benutzer** oder **Folgender Benutzer** aktiviert ist, kann ein Fehler beim Wechsel der Identität zum gewünschten Benutzer auftreten. Aus diesem Grund sollten Sie die LAN-Anmeldedaten in den Haupteinstellungen für Updates eingeben. Geben Sie die Anmeldedaten dort wie folgt ein: domain_name\user (workgroup_name\name für eine Arbeitsgruppe) und das Passwort. Für Aktualisierungen von der HTTP-Version des lokalen Servers ist keine Authentifizierung erforderlich.

Serververbindung nach Update trennen

Die Verbindung zum Server wird getrennt, wenn sie nach dem Abrufen von Update-Dateien weiterhin aktiv ist.

Update-Mirror

Sie finden die Konfigurationsoptionen für den lokalen Mirror-Server in den **Erweiterten Einstellungen** (F5) unter **Update** > **Profile** > Update-Mirror.

Update-Rollback

Falls Sie befürchten, dass ein neues Update der Erkennungsroutine oder der Programm-Module instabil oder beschädigt ist, können Sie ein Rollback auf die vorherige Version ausführen und Updates vorübergehend deaktivieren. Sie können auch zuvor deaktivierte Updates aktivieren, falls Sie diese für unbegrenzte Zeit ausgesetzt hatten.

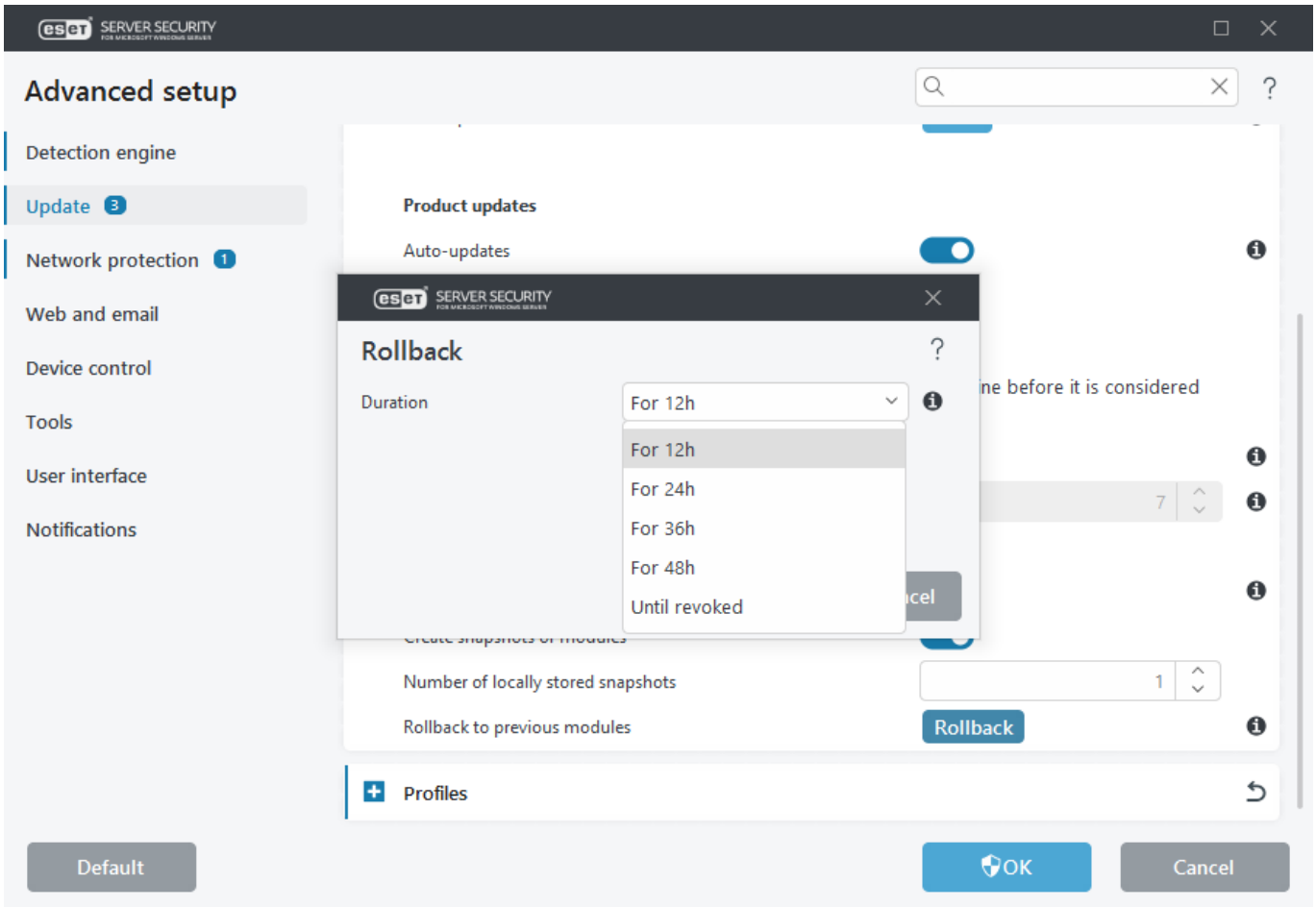
ESET Mail Security erfasst Snapshots der Erkennungsroutine und der Programm-Module für den Einsatz mit der Rollback-Funktion. Aktivieren Sie die Option **Snapshots der Module erstellen** erstellen, um Snapshots der Virusdatenbank zu erstellen.

Wenn die Option **Snapshots der Module erstellen** aktiviert ist, wird der erste Snapshot beim ersten Update erstellt. Der nächste Snapshot wird 48 Stunden später erstellt.

Das Feld **Anzahl der lokal gespeicherten Snapshots** legt fest, wie viele Snapshots der Erkennungsroutine gespeichert werden.

> Wenn die maximale Anzahl an Snapshots erreicht ist (z. B. drei), wird der älteste Snapshot alle 48 Stunden durch einen neuen Snapshot ersetzt. ESET Mail Security führt ein Rollback der Versionen für Erkennungsroutine und Programm-Module auf den ältesten Snapshot durch.

Wenn Sie auf **Rollback** klicken, müssen Sie im Dropdownmenü einen Zeitraum auswählen. Dieser Wert legt fest, wie lange die Updates der Datenbank der Erkennungsroutine und der Programm-Module angehalten werden.



Wählen Sie **Bis zur Aufhebung**, um keine regelmäßigen Updates auszuführen, bis die Update-Funktion manuell wieder aktiviert wird. Diese Option ist mit potenziellen Sicherheitsrisiken verbunden und sollte daher nach

Möglichkeit nicht ausgewählt werden.

Wenn Sie ein Rollback durchführen, wird die Schaltfläche **Rollback** zu **Updates erlauben** geändert. Während des im Dropdownmenü **Updates aussetzen** ausgewählten Zeitintervalls sind keine Updates möglich.

Die Version der Datenbank der Malware Scan Engine wird auf die älteste verfügbare Version herabgestuft und als Snapshot im lokalen Dateisystem des Computers gespeichert.

Geplanter Task - Update

Um das Programm mit zwei Update-Servern zu aktualisieren, müssen zwei Update-Profile erstellt werden. Falls das Herunterladen der Update-Dateien von einem der Server fehlschlägt, wechselt das Programm automatisch zum anderen Server. Dies eignet sich z. B. für Notebooks, die normalerweise über einen Update-Server im lokalen Netzwerk aktualisiert werden, jedoch häufig über das Internet mit anderen Netzwerken verbunden sind. Falls das erste Profil nicht funktioniert, lädt das zweite automatisch die Update-Dateien von den ESET-Update-Servern herunter.

Mit den folgenden Schritten können Sie einen Task erstellen, um den vorhandenen Task **Automatische Updates in festen Zeitabständen** zu bearbeiten.
1. Wählen Sie im Hauptbildschirm des **Taskplaners** den Task **Update** mit dem Namen **Automatische Updates in festen Zeitabständen** aus, und klicken Sie auf **Bearbeiten**, um den Konfigurationsassistenten zu öffnen.
2. Wählen Sie eine der folgenden Zeitangaben für die Ausführung des geplanten Tasks aus.
3. Wenn Sie verhindern möchten, dass der Task ausgeführt wird, wenn das System im Akkubetrieb läuft (z. B. mit USV), klicken Sie auf den Schalter neben **Task im Akkubetrieb überspringen**.
4. Wählen Sie das gewünschte Update-Profil für das Update aus. Wählen Sie aus, welche Aktion stattfinden soll, falls der Task nicht ausgeführt werden kann.
5. Klicken Sie auf **Fertig stellen**, um den Task zu übernehmen.

Update-Mirror

ESET Mail Security bietet Ihnen die Möglichkeit, Kopien der Update-Dateien zu erstellen. Diese können Sie dann zur Aktualisierung anderer Workstations im Netzwerk verwenden. Das Verwenden eines „Update-Mirrors“ - das Vorhalten von Kopien der Update-Dateien im lokalen Netzwerk - kann vorteilhaft sein, da die Dateien dann nicht von allen Arbeitsplatzcomputern einzeln über das Internet heruntergeladen werden müssen. Updates werden auf den lokalen Mirror-Server heruntergeladen und von dort an die Arbeitsstationen verteilt. Die Internetverbindung wird erheblich entlastet.

Das Aktualisieren der Clientcomputer von einem Update-Mirror optimiert die Lastenverteilung im Netzwerk und entlastet Internetverbindungen.

Falls in Ihrem Netzwerk viele Clients mit ESET PROTECT verwaltet werden, können Sie ESET Bridge verwenden, anstatt einen Client als Mirror zu konfigurieren, um den Internetdatenverkehr zu minimieren. ESET Bridge kann zusammen mit ESET PROTECT entweder mit dem All-in-One-Installationsprogramm oder als eigenständige Komponente installiert werden. Weitere Informationen und Unterschiede zwischen ESET Bridge, Apache HTTP Proxy, Mirror Tool und direkter Konnektivität finden Sie in der Online-Hilfe für ESET PROTECT.

Update-Mirror

Update-Mirror erstellen
Aktiviert die Mirror-Konfigurationsoptionen.

Zugriff auf Update-Dateien

HTTP-Server aktivieren
Wenn diese Option aktiviert ist, können Update-Dateien ohne Anmeldedaten per HTTP abgerufen werden.
Speicherordner
Klicken Sie auf **Bearbeiten**, um einen lokalen oder Netzwerkordner anzugeben. Wenn für den angegebenen Ordner eine Authentifizierung erforderlich ist, müssen die Anmeldedaten in die Felder „Benutzername“ und „Passwort“ eingegeben werden.
Klicken Sie auf **Löschen**, falls Sie den Standardordner für die Speicherung der Update-Dateien (*C:\ProgramData\ESET\ESET Security\mirror*) ändern möchten.

HTTP-Server

Server-Port
Der Standardport ist auf 2221 festgelegt. Ändern Sie diesen Wert, falls Sie einen anderen Port verwenden.
Authentifizierung
Definiert die Authentifizierungsmethode für den Zugriff auf die Update-Dateien. Folgende Optionen stehen zur Verfügung: **Keine**, **Einfach** und **NTLM**.
• Wählen Sie **Einfach** aus, um die Base64-Verschlüsselung und die einfache Authentifizierung mit Benutzername und Passwort zu verwenden.
• Bei Auswahl von **NTLM** wird eine sichere Verschlüsselungsmethode verwendet. Zur Authentifizierung wird der auf dem Computer erstellte Benutzer verwendet, der die Update-Dateien freigegeben hat.
• Die Standardeinstellung ist **Keine**, sodass für den Zugriff auf die Update-Dateien keine Authentifizierung erforderlich ist.

> ⚠ Wenn Sie den Zugriff auf die Update-Dateien über einen HTTP-Server zulassen möchten, muss sich der Ordner mit den Kopien der Update-Dateien auf demselben Computer befinden wie die Instanz von ESET Mail Security, mit der dieser Ordner erstellt wird.

SSL für HTTP-Server
Hängen Sie die **Zertifikatskettendatei** an oder generieren Sie ein selbstsigniertes Zertifikat, wenn Sie den HTTP-Server mit HTTPS (SSL)-Unterstützung ausführen möchten. Folgende Zertifikattypen stehen zur Verfügung: PEM, PFX und ASN. Für zusätzliche Sicherheit können Update-Dateien mit dem HTTPS-Protokoll heruntergeladen werden. Das Nachverfolgen der übertragenen Daten und Anmeldeberechtigungen ist bei der Verwendung dieses Protokolls nahezu unmöglich.
Die Option **Typ des privaten Schlüssels** wird standardmäßig auf **Integriert** eingestellt, und die Option Datei mit privatem Schlüssel ist standardmäßig deaktiviert. Dies bedeutet, dass der private Schlüssel Bestandteil der ausgewählten Zertifikatskettendatei ist.

Verbindungsoptionen

Windows-Freigaben
Beim Aktualisieren von einem lokalen Windows-Server ist standardmäßig eine Authentifizierung für jede Netzwerkverbindung erforderlich.
Verbindung mit LAN herstellen als
Wählen Sie eine der folgenden Optionen aus, um Ihr Konto zu konfigurieren:
• **Systemkonto (Standard)** – Verwendet das Systemkonto für die Authentifizierung. Normalerweise findet keine Authentifizierung statt, wenn in den Haupteinstellungen für Updates keine Anmeldedaten angegeben sind.
• **Aktueller Benutzer** – Das Programm meldet sich mit dem Konto des aktuell angemeldeten Benutzers an. Diese Lösung hat den Nachteil, dass sich das Programm nicht mit dem Update-Server verbinden kann, wenn kein Benutzer angemeldet ist.
• **Folgender Benutzer** – Mit dieser Option können Sie ein bestimmtes Benutzerkonto für die Authentifizierung angeben. Verwenden Sie diese Option, wenn eine Anmeldung mit dem standardmäßigen Systemkonto nicht möglich ist. Das ausgewählte Benutzerkonto benötigt Zugriffsrechte für den Ordner mit den Update-Dateien. Wenn der Benutzer keinen Zugriff hat, kann sich das Programm nicht verbinden und kann keine Updates herunterladen.

⚠ Wenn entweder **Aktueller Benutzer** oder **Folgender Benutzer** aktiviert ist, kann ein Fehler beim Wechsel der Identität zum gewünschten Benutzer auftreten. Aus diesem Grund sollten Sie die LAN-Anmeldedaten in den Haupteinstellungen für Updates eingeben. Geben Sie die Anmeldedaten dort wie folgt ein: *domain_name**user* (*workgroup_name**name* für eine Arbeitsgruppe) und das Passwort. Für Aktualisierungen von der HTTP-Version des lokalen Servers ist keine Authentifizierung erforderlich.

Serververbindung nach Update trennen
Die Verbindung zum Server wird getrennt, wenn sie nach dem Abrufen von Update-Dateien weiterhin aktiv ist.

Netzwerk-Schutz

Verwalten Sie den Netzwerkschutz. Klicken Sie auf **Bearbeiten**, um neue Elemente hinzuzufügen oder vorhandene zu ändern:

- Bekannte Netzwerke
- Zonen

Bekannte Netzwerke

Wenn Sie einen Computer verwenden, der häufig mit öffentlichen Netzwerken oder Netzwerken außerhalb Ihres normalen Arbeitsnetzwerks verbunden ist, sollten Sie die Glaubwürdigkeit neuer Netzwerke überprüfen, mit denen Sie sich verbinden. Wenn Sie Netzwerke definiert haben, kann ESET Mail Security vertrauenswürdige Netzwerke (Heim-/Büronetzwerke) anhand verschiedener in der Netzwerkidentifikation konfigurierter Netzwerkparameter erkennen.

Computer verwenden in Netzwerke oft IP-Adressen, die dem vertrauenswürdigen Netzwerk ähneln. In solchen Fällen stuft ESET Mail Security ein unbekanntes Netzwerk unter Umständen als vertrauenswürdig ein (Heim-/Büronetzwerk). Verwenden Sie die Netzwerkauthentifizierung, um diese Art von Situation zu vermeiden.

Wenn ein Netzwerkadapter mit einem Netzwerk verbunden wird oder die Netzwerkeinstellungen neu konfiguriert werden, durchsucht ESET Mail Security die Liste bekannter Netzwerke nach einem Eintrag, der mit dem neuen Netzwerk übereinstimmt. Wenn Netzwerkidentifikation und Netzwerkauthentifizierung (optional) übereinstimmen, wird das Netzwerk in dieser Schnittstelle als verbunden markiert.

Wenn kein bekanntes Netzwerk gefunden wird, erstellt die Netzwerkidentifikation eine neue Netzwerkverbindung, um das Netzwerk beim nächsten Verbindungsaufbau zu identifizieren. Die

Netzwerkverbindung verwendet standardmäßig den Schutztyp „Öffentliches Netzwerk“.

Im Dialogfenster „Neue Netzwerkverbindung erkannt“ werden Sie aufgefordert, einen der Schutztypen „Öffentliches Netzwerk“, „Heim-/Büronetzwerk“ oder „Windows-Einstellungen verwenden“ zu wählen. Wenn ein Netzwerkadapter mit einem bekannten Netzwerk verbunden ist, das als Heim- oder Büronetzwerk markiert ist, werden lokale Subnetze des Adapters zur vertrauenswürdigen Zone hinzugefügt.

Schutztyp für neue Netzwerke

Wählen Sie aus, welche der folgenden Optionen standardmäßig für neue Netzwerke verwendet werden sollen: **Windows-Einstellung verwenden**, **Benutzer fragen** oder **Als öffentlich markieren**. Wenn Sie **Windows-Einstellung verwenden** auswählen, wird kein Dialogfeld angezeigt, und das Netzwerk, mit dem Sie verbunden sind, wird gemäß Ihren Windows-Einstellungen markiert. In diesem Fall sind bestimmte Funktionen (z. B. Dateifreigabe und Remotedesktop) in neuen Netzwerken verfügbar.

Bekannte Netzwerke können manuell im Editorfenster Bekannte Netzwerke konfiguriert werden.

Netzwerk hinzufügen

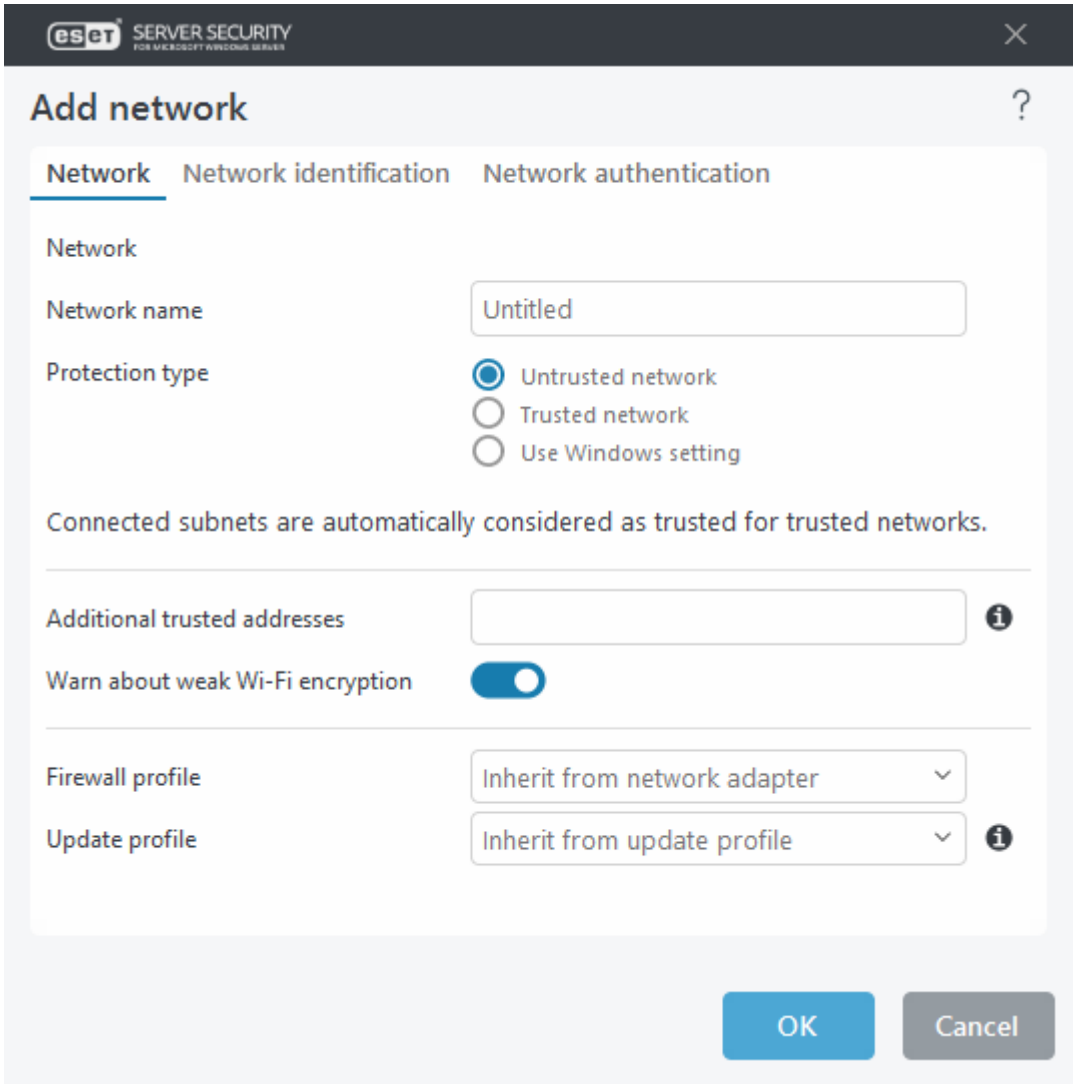
Die Netzwerkkonfiguration ist in die folgenden Registerkarten unterteilt:

Netzwerk

Sie können den **Netzwerknamen** definieren und den **Schutztyp** für das Netzwerk auswählen. Zeigt an, ob das Netzwerk die Einstellung **Vertrauenswürdiges Netzwerk**, **Nicht vertrauenswürdiges Netzwerk** oder **Windows-Einstellung verwenden** verwendet.

Außerdem werden die unter **Weitere vertrauenswürdige Adressen** hinzugefügten Adressen unabhängig vom Schutztyp des Netzwerks immer zur vertrauenswürdigen Zone der mit diesem Netzwerk verbundenen Adapter hinzugefügt.

- **Vor unsicherer WLAN-Verschlüsselung warnen** – ESET Mail Security informiert Sie, wenn Sie sich mit einem gar nicht oder nur schwach geschützten WLAN-Netzwerk verbinden.
- Das **Firewall-Profil** wird vom Netzwerkadapter übernommen.
- **Updateprofil** – Wählen Sie das Updateprofil aus, das bei Verbindungen zu diesem Netzwerk verwendet werden soll.



Netzwerkidentifikation

Wird anhand der Parameter des lokalen Netzwerkadapters ausgeführt. Alle ausgewählten Parameter werden mit den tatsächlichen Parametern aktiver Netzwerkverbindungen verglichen. IPv4- und IPv6-Adressen sind zulässig.

Netzwerkauthentifizierung

Sucht nach einem bestimmten Server im Netzwerk und verwendet eine asymmetrische Verschlüsselung (RSA) für die Authentifizierung des Servers. Der Name des authentifizierten Netzwerks muss mit dem Zonennamen in den Einstellungen des Authentifizierungsservers übereinstimmen, inklusive Groß- und Kleinschreibung. Geben Sie einen Servernamen, einen Listening-Port des Servers und einen öffentlichen Schlüssel, der zu dem privaten Serverschlüssel passt. Geben Sie einen Servernamen, einen Listening-Port des Servers und einen öffentlichen Schlüssel, der zu dem privaten Serverschlüssel passt. Der Servername kann als IP-Adresse, DNS- oder NetBios-Name angegeben werden. Im Anschluss können Sie den Pfad zum Speicherort des Schlüssels auf dem Server angeben (z. B. *server_name_/directory1/directory2/authentication*). Sie können alternative Server mit Semikolon getrennt an den Pfad anhängen.

Der öffentliche Schlüssel kann als einer der folgenden Dateitypen importiert werden:

- PEM-verschlüsselter öffentlicher Schlüssel (.pem). Dieser Schlüssel kann mit dem ESET-Authentifizierungsserver generiert werden.
- Verschlüsselter öffentlicher Schlüssel

- Zertifikatdatei für öffentlichen Schlüssel (.crt)

Klicken Sie auf **Testen**, um Ihre Einstellungen zu testen. Wenn die Authentifizierung erfolgreich war, wird eine Erfolgsmeldung angezeigt. Wenn die Authentifizierung nicht korrekt konfiguriert ist, werden die folgenden Fehlermeldungen angezeigt:

Fehler bei der Serverauthentifizierung. Ungültige oder falsche Signatur.	**Die Serversignatur stimmt nicht mit dem eingegebenen öffentlichen Schlüssel überein.**
Fehler bei der Serverauthentifizierung. Netzwerkname stimmt nicht überein.	Deaktivieren Sie diesen Schalter, wenn Sie die Regel nicht verwenden, jedoch nicht aus der Liste löschen möchten.
Fehlgeschlagene Serverauthentifizierung. Ungültige oder keine Antwort vom Server.	Wenn der Server nicht ausgeführt wird oder nicht erreichbar ist, wird keine Antwort empfangen. Wenn ein anderer HTTP-Server unter der angegebenen Adresse ausgeführt wird, kann eine ungültige Antwort zurückgegeben werden.
Ungültiger öffentlicher Schlüssel eingegeben.	Stellen Sie sicher, dass die eingegebene öffentliche Schlüsseldatei nicht beschädigt ist.

Zonen

Eine Zone ist eine Sammlung von Netzwerkadressen, die eine logische Gruppe von IP-Adressen bilden. Dies ist hilfreich, wenn Sie mehrere Adressen in verschiedenen Regeln wiederverwenden möchten. Jeder Adresse in einer bestimmten Gruppe werden ähnliche Regeln zugewiesen, die zentral für die gesamte Gruppe definiert wurden. Ein Beispiel für eine solche Gruppe ist eine **vertrauenswürdige Zone**. Eine vertrauenswürdige Zone ist eine Gruppe von Netzwerkadressen, die von der Firewall nicht blockiert werden.

So fügen Sie eine vertrauenswürdige Zone hinzu:

1. Navigieren Sie zu **Erweiterte Einstellungen** (**F5**) > **Netzwerkschutz** > **Einfach** > **Zonen**.

2. Klicken Sie auf **Bearbeiten** neben den **Zonen**.

3. Klicken Sie auf **Hinzufügen**, geben Sie **Name** und **Beschreibung** für die neue Zone ein und fügen Sie eine Remote-IP-Adresse zum Feld **„Adresse des Remotecomputers (IPv4/IPv6, Bereich, Maske)“** hinzu.

4. Klicken Sie auf **OK**.

Spalten

- **Name** – Der Name einer Gruppe von Remotecomputern.

- **IP-Adressen** – Remote-IP-Adressen, die zu einer Zone gehören.

Steuerelemente

Beim Hinzufügen oder Bearbeiten von Zonen sind die folgenden Felder verfügbar:

- **Name** – Der Name einer Gruppe von Remotecomputern.

- **Beschreibung** – Eine allgemeine Beschreibung der Gruppe.

- **Adresse des Remote-Computers (IPv4, IPv6, Bereich, Maske)** – Eine Remoteadresse, ein Adressbereich

oder ein Subnetz.

- **Löschen** – Entfernt eine Zone aus der Liste.

> Vordefinierte Zonen können nicht entfernt werden.

Netzwerkangriffsschutz

Netzwerkangriffsschutz (IDS) aktivieren

Mit dieser Option können Sie den Zugriff auf bestimmte Dienste konfigurieren, die auf Ihrem Computer in der vertrauenswürdigen Zone ausgeführt werden, und können die Erkennung bestimmter Angriffsarten und Exploits aktivieren oder deaktivieren, die Ihrem Computer schaden könnten.

Botnetz-Schutz aktivieren

Erkennt und blockiert die Kommunikation mit bösartigen Steuerungszentralen anhand typischer Muster, wenn ein Computer infiziert wird und ein Bot versucht, zu kommunizieren.

IDS-Ausnahmen

Sie können sich Intrusion Detection System (IDS)-Ausnahmen als eine Art Netzwerkschutzregeln vorstellen. Klicken Sie auf Bearbeiten, um IDS-Ausnahmen zu definieren.

> Falls Ihre Umgebung ein Hochgeschwindigkeitsnetzwerk (10 GbE und höher) enthält, lesen Sie den KB-Artikel mit Informationen zur Leistung der Netzwerkgeschwindigkeit und ESET Mail Security.

Schutz vor Brute-Force-Angriffen

ESET Mail Security prüft den Inhalt des Netzwerkverkehrs und blockiert Angriffe, bei denen versucht wird, Passwörter zu erraten.

Erweiterte Optionen

Konfigurieren Sie die erweiterten Filteroptionen, um die verschiedenen Arten von Angriffen und Schwachstellen zu erkennen, die auf Ihrem Computer ausgeführt werden können.

Angriffsversuche (Intrusion) erkennen:

SMB-Protokoll - Erkennt und blockiert verschiedene Sicherheitsprobleme im SMB-Protokoll.
RPC-Protokoll - Erkennt und blockiert verschiedene CVEs im System für Remoteprozeduraufrufe, das für die Distributed Computing Environment (DCE) entwickelt wurde.
RDP-Protokoll - Erkennt und blockiert verschiedene CVEs im RDP-Protokoll (siehe oben).
Unsichere Adresse nach erkanntem Angriff blockieren - IP-Adressen, die als Angriffsquellen identifiziert wurden, werden zur Negativliste hinzugefügt, um die Verbindung für einen bestimmten Zeitraum zu unterbinden.
Hinweis bei erkanntem Angriff anzeigen – Aktiviert die Benachrichtigung im Windows-Benachrichtigungsbereich unten rechts auf dem Bildschirm.
Benachrichtigung auch bei eingehenden Angriffen auf Sicherheitslücken anzeigen - Warnt Sie, wenn Angriffe auf Sicherheitslücken erkannt werden oder wenn eine Bedrohung versucht, sich auf diese Weise Zugang zum System zu verschaffen.

Paketprüfung:

Eingehende Verbindungen zu administrativen Freigaben per SMB-Protokoll zulassen - Die administrativen Freigaben (Admin-Freigaben) sind Standardnetzwerkfreigaben für Festplattenpartitionen (C$, D$, ...) im System sowie für den Systemordner (ADMIN$). Deaktivieren Sie Verbindungen zu Admin-Freigaben, um sich vor zahlreichen Sicherheitsrisiken zu schützen. Der Conficker-Wurm verwendet beispielsweise Wörterbuchangriffe, um sich mit Admin-Freigaben zu verbinden.
Alte (nicht unterstützte) SMB-Dialekte blockieren - SMB-Sitzungen, die einen alten und nicht von IDS unterstützten SMB-Dialekt verwenden, werden blockiert. Moderne Windows-Betriebssysteme unterstützen alte SMB-Dialekte für die Abwärtskompatibilität mit älteren Betriebssystemen wie Windows 95. Angreifer können einen alten Dialekt in einer SMB-Sitzung verwenden, um die Datenverkehrsanalyse zu umgehen. Blockieren Sie alte SMB-Dialekte, falls Ihr Computer keine Dateien mit älteren Windows-Versionen teilen oder allgemein per SMB mit diesen Versionen kommunizieren muss.
SMB-Sitzungen ohne Sicherheitserweiterungen blockieren - Mit der erweiterten Sicherheit kann bei der SMB-Sitzungsaushandlung ein besserer Authentifizierungsmechanismus als die LAN Manager Challenge/Response (LM)-Authentifizierung bereitgestellt werden. Das LM-Schema gilt als unsicher und sollte nach Möglichkeit nicht verwendet werden.
Verbindungen zur Sicherheitskontenverwaltung (SAM) zulassen - Weitere Informationen zu diesem Dienst finden Sie unter [MS-SAMR].
Verbindungen zur Local Security Authority (LSASS) zulassen - Weitere Informationen zu diesem Dienst finden Sie unter [MS-LSAD] und [MS-LSAT].
Verbindungen zu Remoteregistrierung zulassen - Weitere Informationen zu diesem Dienst finden Sie unter [MS-RRP].
Verbindungen zum Service Control Manager (SCM) zulassen - Weitere Informationen zu diesem Dienst finden Sie unter [MS-SCMR].
Verbindungen zu Serverdienst zulassen - Weitere Informationen zu diesem Dienst finden Sie unter [MS-SRVS].
Verbindungen zu anderen Diensten zulassen - Andere MSRPC-Dienste.

IDS-Ausnahmen

Ausnahmen für das Intrusion Detection System (IDS) sind eine Art von Schutzregeln für das Netzwerk. Die Ausnahmen werden von oben nach unten ausgewertet. Im Editor für IDS-Ausnahmen können Sie das Verhalten des Netzwerkschutzes für verschiedene IDS-Ausnahmen festlegen. Die erste übereinstimmende Ausnahme wird für jeden Aktionstyp (Sperren, Benachrichtigen, Log) separat angewendet. Mit den Optionen **Anfang/Nach oben/Nach unten/Ende** könne Sie die Prioritäten der Ausnahmen festlegen. Um eine neue IDS-Ausnahme zu erstellen, klicken Sie auf **Hinzufügen**. Klicken Sie auf **Bearbeiten**, um eine vorhandene IDS-Ausnahme zu bearbeiten, oder auf **Löschen**, um sie zu löschen.

Wählen Sie einen **Warnungstyp** in der Dropdownliste aus. Geben Sie den **Bedrohungsnamen** und die **Richtung** aus. Suchen Sie nach einer **Anwendung**, für die Sie die Ausnahme erstellen möchten. Geben Sie eine Liste von IP-Adressen (IPv4 oder IPv6) oder Subnetzen an. Mehrere Einträge können durch Komma voneinander getrennt werden.

Konfigurieren Sie die **Aktion** für die IDS-Ausnahme, indem Sie eine der Optionen im Dropdownmenü auswählen (**Standard**, **Ja**, **Nein**). Wiederholen Sie diesen Vorgang für alle Aktionstypen (**Sperren**, **Benachrichtigen**, **Log**).

Falls Sie bei einer IDS-Ausnahmenwarnung eine Benachrichtigung anzeigen und den Zeitpunkt des Ereignisses loggen möchten, lassen Sie für den Aktionstyp **Sperren** den Wert **Standard** eingestellt und wählen Sie für die anderen zwei Aktionstypen (**Benachrichtigen** und **Log**) jeweils die Option **Ja** im Dropdownmenü aus.

Bedrohungverdacht blockiert

Diese Situation kann auftreten, wenn eine Anwendung auf Ihrem Computer versucht, unter Ausnutzung einer Sicherheitslücke schädlichen Datenverkehr an einen anderen Computer im Netzwerk zu übertragen, oder wenn jemand versucht, Ports in Ihrem Netzwerk zu scannen.

- Bedrohung – Bedrohungsname.
- Quelle – Quelladresse im Netzwerk
- Ziel – Zieladresse im Netzwerk
- Nicht mehr blockieren – Erstellt eine IDS-Regel für die vermutete Bedrohung, um die Kommunikation zu erlauben.
- Weiterhin blockieren – Blockiert die erkannte Bedrohung. Um eine IDS-Regel mit Einstellungen zum Blockieren der Kommunikation für diese Bedrohung zu erstellen, wählen Sie Nicht mehr benachrichtigen aus.

> Die in diesem Benachrichtigungsfenster angezeigten Informationen hängen von der Art der erkannten Bedrohung ab. Weitere Informationen zu Bedrohungen und anderen verwandten Begriffen finden Sie unter Arten von Remoteangriffen oder Arten von Ereignissen.

Vorübergehende Negativliste der IP-Adressen

Enthält eine Liste von IP-Adressen, die als Angriffsquellen identifiziert und zur Blacklist hinzugefügt wurden, um Verbindungen für einen bestimmten Zeitraum (bis zu einer Stunde) zu blockieren. Zeigt die blockierten **IP-Adressen** an.

Blockierungsgrund

Zeigt den Angriffstyp an, der von dieser Adresse verhindert wurde (z. B. TCP-Portscan-Angriff).

Zeitüberschreitung

Zeigt das Datum und die Uhrzeit an, zu der die Adresse aus der Negativliste entfernt wird.

Entfernen / Alle entfernen

Entfernt die ausgewählte IP-Adresse aus der vorübergehenden Negativliste, bevor sie automatisch entfernt wird, oder entfernt alle Adressen sofort aus der Negativliste.

Ausnahme hinzufügen

Fügt eine Firewallausnahme für die ausgewählte IP-Adresse zum IDS-Filter hinzu.

Schutz vor Brute-Force-Angriffen

Der Brute-Force-Angriffsschutz blockiert Passwortermittlungsversuche für RDP- und SMB-Dienste. Brute-Force-Angriffe versuchen, durch systematisches Ausprobieren sämtlicher möglicher Kombinationen aus Buchstaben, Zahlen und Symbolen das richtige Passwort zu erraten.

- **Brute-Force-Angriffsschutz aktivieren** – ESET Mail Security prüft den Inhalt des Netzwerkverkehrs und blockiert Angriffe, bei denen versucht wird, Passwörter zu erraten.

- Regeln – Hier können Sie Regeln für ein- und ausgehende Netzwerkverbindungen erstellen, bearbeiten und anzeigen.

- Ausschlüsse – Liste der ausgeschlossenen Ereignisse, die durch eine IP-Adresse oder einen Anwendungspfad definiert sind. Sie können Ausschlüsse in ESET PROTECT-Web-Konsole erstellen und bearbeiten.

Regeln für Schutz vor Brute-Force-Angriffen

Sie können Regeln für Schutz vor Brute-Force-Angriffen für ein- und ausgehende Netzwerkverbindungen erstellen, bearbeiten und anzeigen. Die vordefinierten Regeln können nicht bearbeitet oder gelöscht werden.

Erstellen Sie eine neue Regel, klicken Sie auf **Hinzufügen** für eine neue Regel zum Schutz vor Brute-Force-Angriffen oder **bearbeiten** Sie ausgewählte Einträge.

Dieses Fenster enthält eine Übersicht der vorhandenen Regeln zum Schutz vor Brute-Force-Angriffen.

Name	Benutzerdefinierter oder automatisch ausgewählter Regelname.
Aktiviert	Deaktivieren Sie diesen Schalter, wenn Sie die Regel nicht verwenden, jedoch nicht aus der Liste löschen möchten.
Aktion	Die Regel legt eine Aktion fest (Zulassen oder Verweigern), die bei Eintreten der Bedingungen ausgeführt wird.
Protokoll	Das Kommunikationsprotokoll, das von dieser Regel geprüft wird.
Profil	Benutzerdefinierte Regeln können für bestimmte Profile festgelegt und angewendet werden.
Max. Versuche	Die maximale Anzahl zulässiger Wiederholungsversuche bei Angriffen, bevor die IP-Adresse blockiert und zur Blacklist hinzugefügt wird.
Aufbewahrungszeitraum für Blacklist (Min.)	Legt den Zeitpunkt fest, an dem die Adresse aus der Blacklist abläuft. Der Standardzeitraum für das Zählen der Anzahl der Versuche beträgt 30 Minuten.
Quell-IP	Eine Liste von IP-Adressen, Adressbereichen oder Subnetzen. Mehrere Adressen können durch Komma getrennt angegeben werden.
Quellzonen	Klicken Sie auf „Hinzufügen“, um eine vordefinierte oder erstellte Zone mit einem Bereich von IP-Adressen hinzuzufügen.

Ausschlüsse für Brute-Force-Angriffsschutz

Brute-Force-Ausschlüsse können verwendet werden, um die Brute-Force-Erkennung nach bestimmten Kriterien zu unterdrücken. Diese Ausschlüsse werden von ESET PROTECT auf Basis der Brute-Force-Erkennung erstellt. Die Ausschlüsse werden angezeigt, wenn ein Administrator Brute-Force-Ausschlüsse in der ESET PROTECT Web

Console erstellt. Ausschlüsse können nur permissive Regeln (zulassen) enthalten und werden vor den IDS-Regeln ausgewertet.

- **Ereignis** – Ereignistyp.
- **Anwendung** – Wählen Sie den Dateipfad einer Anwendung aus, indem Sie auf ... klicken (zum Beispiel *C:\Program Files\Firefox\Firefox.exe*). Geben Sie nicht den Namen der Anwendung ein.
- **Remote-IP** - Eine Liste von Remote-IPv4- oder -IPv6-Adressen, Adressbereichen oder Subnetzen. Mehrere Adressen müssen durch Komma getrennt angegeben werden.

Web und E-Mail

Sie können die Protokollprüfung, den E-Mail-Client-Schutz den Web-Schutz und den Phishing-Schutz so konfigurieren, dass Ihr Server bei der Kommunikation mit dem Internet geschützt wird.

E-Mail-Client-Schutz

Überwacht den gesamten E-Mail-Verkehr, schützt Sie vor Schadcode und bietet Ihnen eine Auswahl an Handlungsmöglichkeiten, wenn eine Infektion erkannt wurde.

Web-Schutz

Überwacht den Datenverkehr zwischen Webbrowsern und Remoteservern gemäß den für HTTP und HTTPS festgelegten Standards. Mit dieser Funktion können Sie außerdem bestimmte URLs blockieren, zulassen oder ausschließen.

Protokollprüfung

Bietet erweiterten Schutz für die verwendeten Anwendungsprotokolle durch das ThreatSense-Prüfmodul. Die Prüfung findet automatisch statt, egal ob ein Webbrowser oder ein E-Mail-Programm verwendet wird. Auch verschlüsselte Verbindungen (SSL/TLS) werden geprüft.

Phishing-Schutz

Hier können Sie Webseiten sperren, die Phishing-Inhalte verteilen.

Prüfen von Anwendungsprotokollen

Die Scan Engine von ThreatSense bietet Malware-Schutz für Anwendungsprotokolle und enthält mehrere erweiterte Scan-Methoden. Die Protokollprüfung funktioniert unabhängig vom eingesetzten E-Mail-Programm oder Webbrowser. Wenn die Protokollprüfung aktiviert ist, überprüft ESET Mail Security sämtliche Kommunikation, die das SSL/TLS-Protokoll verwendet. Navigieren Sie zu **Web und E-Mail** > SSL/TLS.

Prüfen von anwendungsspezifischen Protokollen aktivieren

Mit dieser Option können Sie die Protokollprüfung deaktivieren. Zahlreiche Komponenten von ESET Mail Security wie Web-Schutz, E-Mail-Schutz und Phishing-Schutz hängen jedoch von dieser Option ab und funktionieren ohne sie nicht ordnungsgemäß.

Ausgeschlossene Anwendungen

Wählen Sie aus der Liste die Netzwerk-Anwendungen, für deren Datenkommunikation keine Inhaltsprüfung erfolgen soll. Dies schließt die HTTP/POP3-Datenkommunikation ausgewählter Anwendungen von der Prüfung auf Bedrohungen aus. Schließen Sie bestimmte Anwendungen von der Protokollprüfung aus. Klicken Sie auf **Bearbeiten** bzw. auf **Hinzufügen**, um eine ausführbare Datei in der Liste der Anwendungen auszuwählen und von der Protokollprüfung auszuschließen.

Aktivieren Sie diese Option nach Möglichkeit nur für Anwendungen, deren Datenkommunikation mit aktivierter Prüfung nicht ordnungsgemäß funktioniert.

Ausgeschlossene IP-Adressen

Ermöglicht das Ausschließen bestimmter Remoteadressen von der Protokollprüfung. Die IP-Adressen in dieser Liste werden von der Prüfung von Protokollen ausgenommen. Die HTTP/POP3/IMAP-Datenkommunikation von/zu den ausgewählten Adressen wird nicht auf Bedrohungen geprüft.

Wir empfehlen, diese Option nur für Adressen zu aktivieren, die als vertrauenswürdig bekannt sind.

Klicken Sie auf **Bearbeiten** bzw. **Hinzufügen**, um eine IP-Adresse, einen Adressbereich oder ein Subnetz auszuschließen. Mit der Option **Mehrere Werte eingeben** können Sie mehrere durch Zeilenumbrüche, Kommas oder Semikolon getrennte IP-Adressen eingeben. Wenn die Mehrfachauswahl aktiviert ist, werden die Adressen in der Liste der ausgeschlossenen IP-Adressen angezeigt.

Ausschlüsse sind nützlich, wenn die Protokollprüfung Kompatibilitätsprobleme verursacht.

Webbrowser und E-Mail-Programme

Da im Internet Sicherheitsbedrohungen allgegenwärtig sind, ist sicheres Internetsurfen besonders wichtig. Durch Sicherheitslücken in Webbrowsern und gefälschte Hyperlinks kann Schadcode unbemerkt in Ihr System eindringen. Deshalb bietet ESET Mail Security besondere Funktionen zur Verbesserung der Sicherheit von Webbrowsern an. Sie können beliebige Anwendungen, die auf das Internet zugreifen, als Webbrowser einstufen. Anwendungen, die bereits kommunikations- oder anwendungsspezifische Protokolle aus dem ausgewählten Pfad verwenden, können zur Liste der Webbrowser und E-Mail-Programme hinzugefügt werden.

SSL/TLS

ESET Mail Security kann Verbindungen die das Secure Sockets Layer (SSL)- / Transport Layer Security (TLS)-Protokoll verwenden, auf Bedrohungen überprüfen.

Für die Untersuchung von SSL-geschützten Verbindungen gibt es verschiedene Scan-Modi mit vertrauenswürdigen und unbekannten Zertifikaten sowie Zertifikaten, die von der Prüfung SSL-geschützter Verbindungen ausgeschlossen sind.

SSL/TLS-Protokollfilterung aktivieren

Wenn die Protokollfilterung deaktiviert ist, werden SSL/TLS-Verbindungen nicht geprüft. Für den Secure Sockets Layer (SSL)- / Transport Layer Security (TLS)-Protokollfiltermodus sind die folgenden Optionen verfügbar:

- **Automatischer Filtermodus** - Aktivieren Sie diese Option, um jegliche SSL/TLS-geschützte Kommunikation zu scannen (außer wenn Zertifikate verwendet werden, die von der Prüfung ausgeschlossen sind). Wird eine

Verbindung mit einem unbekannten, signierten Zertifikat erstellt, so wird sie ohne gesonderten Hinweis automatisch geprüft. Wenn Sie auf einen Server mit einem nicht vertrauenswürdigen Zertifikat, das sich in der Liste der vertrauenswürdigen Zertifikate befindet und damit als vertrauenswürdig eingestuft wurde, zugreifen, wird die Kommunikation zugelassen und der Inhalt des Kommunikationskanals geprüft.

- **Interaktiver Filtermodus** - Bei Eingabe einer neuen, mit SSL/TLS geschützten Seite (mit unbekanntem Zertifikat) wird ein Dialogfeld mit möglichen Aktionen angezeigt. In diesem Modus können Sie eine Liste von SSL/TLS-Zertifikaten erstellen, die von der Prüfung ausgeschlossen sind.

- **Policy-Modus** - Alle SSL/TLS-Verbindungen mit Ausnahme der konfigurierten Ausschlüsse werden gefiltert.

Liste der vom SSL/TLS-Filter betroffenen Anwendungen

Fügen Sie eine gefilterte Anwendung hinzu und legen Sie eine Scanaktion fest. Mit der Liste der vom SSL/TLS-Filter betroffenen Anwendungen können Sie das Verhalten von ESET Mail Security für bestimmte Anwendungen anpassen und ausgewählte Aktionen speichern, wenn der **Interaktive Modus** unter **Filtermodus für SSL/TLS-Protokoll** ausgewählt ist.

Liste bekannter Zertifikate

Mit der Liste bekannter Zertifikate können Sie das Verhalten von ESET Mail Security für bestimmte SSL-Zertifikate anpassen. Klicken Sie auf Bearbeiten neben der **Liste bekannter Zertifikate**, um die Liste anzuzeigen und zu verwalten.

Kommunikation mit vertrauenswürdigen Domains ausschließen

Schließt die Kommunikation mit erweiterten Validierungszertifikaten von der Protokollprüfung aus (Internetbanking).

Verschlüsselte Kommunikation sperren, die das veraltete SSL v2-Protokoll verwendet

Verbindungen, die die frühere Version des SSL-Protokolls verwenden, werden automatisch blockiert.

Stammzertifikat

Damit die SSL/TLS-Kommunikation in Ihren Browsern/E-Mail-Programmen ordnungsgemäß funktioniert, muss das Stammzertifikat für ESET der Liste der bekannten Stammzertifikate (Herausgeber) hinzugefügt werden. Bekannten Browsern das Stammzertifikat hinzufügen sollte aktiviert sein.

Wählen Sie diese Option aus, um das ESET-Stammzertifikat automatisch zu den bekannten Browsern (z. B. Opera oder Firefox) hinzuzufügen. Wenn ein Browser den Systemzertifizierungsspeicher verwendet, wird das Zertifikat automatisch hinzugefügt (z. B. Internet Explorer).

Um das Zertifikat für nicht unterstützte Browser zu übernehmen, klicken Sie auf **Zertifikat anzeigen** > **Details** > **In die Datei kopieren** ..., und importieren Sie es anschließend manuell in den Browser.

Gültigkeit des Zertifikats

Falls das Zertifikat nicht über die VSZS-Zertifikatablage geprüft werden kann

In manchen Fällen kann das Zertifikat nicht über den **Speicher vertrauenswürdiger Stammzertifizierungsstellen** geprüft werden. Das bedeutet, dass jemand das Zertifikat signiert hat (z. B. der Administrator eines Webservers oder ein Kleinunternehmen). Das Zertifikat als vertrauenswürdig einzustufen, stellt nicht immer ein Risiko dar. Die

meisten großen Unternehmen (z. B. Banken) verwenden Zertifikate, die von einer vertrauenswürdigen Stammzertifizierungsstelle signiert sind.

Wenn die Option **Gültigkeit des Zertifikats erfragen** ausgewählt ist (Standardeinstellung), muss der Benutzer eine Aktion festlegen, die ausgeführt werden soll, wenn verschlüsselte Verbindungen aufgebaut werden. Aktivieren Sie die Option **Kommunikation blockieren, die das Zertifikat verwendet**, um verschlüsselte Verbindungen zu Sites, die nicht verifizierte Zertifikate verwenden, immer zu beenden.

Wenn das Zertifikat ungültig oder beschädigt ist

Ungültige Zertifikate sind entweder abgelaufen oder wurden fehlerhaft signiert. In diesem Fall sollten Sie die Option **Kommunikation blockieren, die das Zertifikat verwendet** aktiviert lassen.

Liste bekannter Zertifikate

Sie können das Verhalten von ESET Mail Security für Secure Sockets Layer (SSL) / Transport Layer Security (TLS)-Zertifikate festlegen und ausgewählte Aktionen speichern, wenn der **Interaktive Modus** unter SSL/TLS-Protokollprüfungsmodus ausgewählt ist. Sie können das ausgewählte Zertifikat konfigurieren oder ein neues Zertifikat aus einer URL oder einer Datei **hinzufügen**.

Klicken Sie im Fenster **Zertifikat hinzufügen** auf **URL** oder auf **Datei** und geben Sie eine Zertifikat-URL an bzw. navigieren Sie zu einer Zertifikatdatei. Die folgenden Felder werden automatisch mit Daten aus dem Zertifikat ausgefüllt:

- **Zertifikatname** - Name des Zertifikats.
- **Zertifikataussteller** - Name des Zertifikaterstellers.
- **Zertifikatbetreff** - Das Betrefffeld enthält die Entität, die mit dem öffentlichen Schlüssel verknüpft ist, welcher im entsprechenden Feld des Betreffs gespeichert ist.

Zugriffsaktion

- **Auto** - vertrauenswürdige Zertifikate zulassen, bei nicht vertrauenswürdigen Zertifikaten nachfragen.
- **Zulassen oder Blockieren** - um die von diesem Zertifikat gesicherte Verbindung unabhängig von ihrer Vertrauenswürdigkeit zuzulassen oder zu blockieren.
- **Nachfragen** - um eine Nachfrage zu erhalten, wenn ein bestimmtes Zertifikat vorgefunden wird.

Scan-Aktion

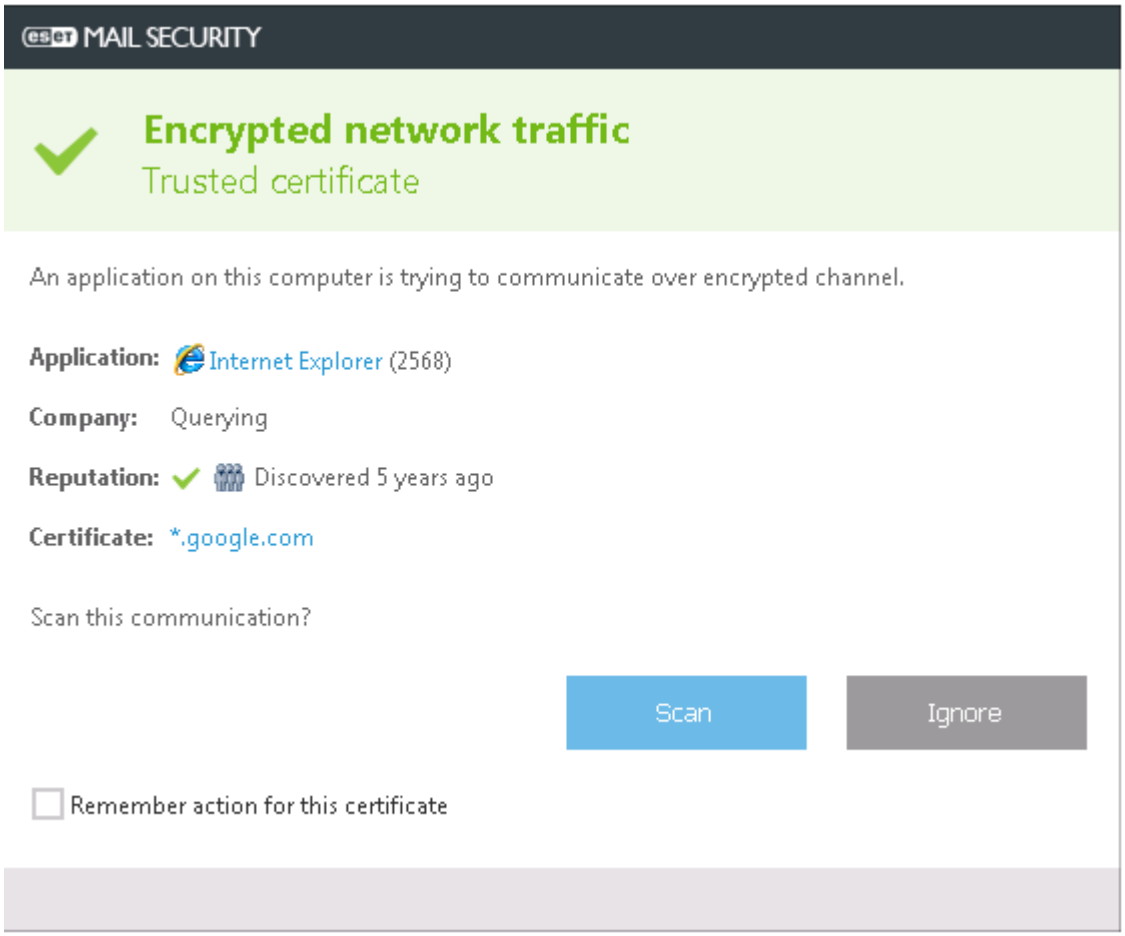
- **Auto** - um im automatischen Modus zu scannen und im interaktiven Modus nachzufragen.
- **Scannen oder ignorieren** - um die mit diesem Zertifikat gesicherte Kommunikation zu scannen oder zu ignorieren.
- **Nachfragen** - um eine Nachfrage zu erhalten, wenn ein bestimmtes Zertifikat vorgefunden wird.

Verschlüsselte SSL-Kommunikation

Wenn das System für SSL-Protokollüberprüfung eingerichtet ist, werden Sie in den folgenden beiden Situationen in einem Dialogfenster aufgefordert, eine Aktion auszuwählen:

Wenn eine Website ein nicht überprüfbares oder ungültiges Zertifikat verwendet und ESET Mail Security so konfiguriert ist, dass der Benutzer in solchen Fällen gefragt werden soll (standardmäßig „ja“ bei nicht überprüfbaren und „nein“ bei ungültigen Zertifikaten), werden Sie in einem Dialogfeld gefragt, ob die Verbindung **zugelassen** oder **blockiert** werden soll.

Wenn die **SSL-Protokollprüfung** auf **Interaktiver Modus** eingestellt ist, werden Sie zu jeder Website in einem Dialogfeld aufgefordert, für den Datenverkehr **Scannen** oder **Ingorieren** auszuwählen. Einige Anwendungen überprüfen, ob ihr SSL-Datenverkehr von jemandem geändert oder untersucht wurde. In diesem Fall muss ESET Mail Security den Datenverkehr **ignorieren**, damit die Anwendung ordnungsgemäß funktioniert.



In beiden Fällen kann der Benutzer die ausgewählte Aktion speichern. Gespeicherte Aktionen werden in der Liste bekannter Zertifikate gespeichert.

E-Mail-Client-Schutz

Die Integration von ESET Mail Security mit E-Mail-Programmen verbessert den aktiven Schutz gegen Schadcode in E-Mail-Nachrichten. Wenn Ihr E-Mail-Programm dies unterstützt, kann die Integration in ESET Mail Security aktiviert werden. Wenn die Integration aktiviert ist, wird die ESET Mail Security-Symbolleiste direkt in das E-Mail-Programm integriert und ermöglicht einen effizienteren E-Mail-Schutz (bei neueren Versionen von Windows Live

Mail wird die Symbolleiste nicht integriert).

Integration in E-Mail-Programme

Zu den derzeit unterstützten E-Mail-Programmen gehören Microsoft Outlook, Outlook Express, Windows Mail und Windows Live Mail. Der E-Mail-Schutz ist ein Plug-In für diese Programme. Das Plugin funktioniert unabhängig vom eingesetzten Protokoll. Wenn beim E-Mail-Client eine verschlüsselte Nachricht eingeht, wird diese entschlüsselt und an das Virenschutz-Prüfmodul weitergeleitet. Auch bei nicht aktivierter Integration ist die E-Mail-Kommunikation durch den E-Mail-Client-Schutz (POP3, IMAP) weiterhin geschützt.

Eine vollständige Liste der unterstützten E-Mail-Clients und der entsprechenden Versionen finden Sie im folgenden Knowledgebase-Artikel.

Prüfen neuer Elemente im Posteingang deaktivieren

Falls das System bei der Arbeit mit Ihrem E-Mail-Programm verlangsamt wird (nur Microsoft Outlook). Dies kann beispielsweise vorkommen, wenn Sie E-Mails vom Kerio Outlook Connector Store abrufen.

E-Mail-Schutz durch Client-Plugins aktivieren

Deaktiviert den E-Mail-Client-Schutz, ohne die Integration in Ihrem E-Mail-Programm zu entfernen. Sie können entweder alle Plugins deaktivieren, oder die folgenden Plugins einzeln auswählen:

- **Eingehende E-Mails** - Aktiviert/deaktiviert die Überprüfung empfangener Nachrichten.
- **Ausgehende E-Mails** - Aktiviert/deaktiviert die Überprüfung ausgehender Nachrichten.
- **E-Mails, die zum Lesen geöffnet werden** - Aktiviert/deaktiviert die Überprüfung gelesener Nachrichten.

Aktion für infizierte E-Mails

- **Keine Aktion** - Infizierte Anhänge werden erkannt, aber es werden keine Aktionen für E-Mails durchgeführt.
- **E-Mail löschen** - Es werden Hinweise zu Bedrohungen angezeigt. Betroffene E-Mails werden gelöscht.
- **In den Ordner „Gelöschte Objekte“ verschieben** - Infizierte E-Mails werden automatisch in den Ordner „Gelöschte Objekte“ verschoben.
- **In folgenden Ordner verschieben** - Infizierte E-Mails werden automatisch in den angegebenen Ordner verschoben.
- **Ordner** - Geben Sie den Ordner an, in den erkannte infizierte E-Mails verschoben werden sollen.

Scan nach Signaturdatenbank-Update wiederholen

Aktiviert/deaktiviert das erneute Scannen nach einem Signaturdatenbank-Update.

Scanergebnisse von anderen Modulen akzeptieren

Wenn diese Option aktiviert ist, nimmt das E-Mail-Schutz-Modul Scanergebnisse von anderen Modulen entgegen (POP3-, IMAP-Protokollprüfung).

E-Mail-Protokolle

E-Mail-Schutz durch Protokollfilterung aktivieren

IMAP und POP3 sind die gängigsten Protokolle für den Empfang von E-Mails in E-Mail-Clientanwendungen. ESET Mail Security schützt diese Protokolle unabhängig vom eingesetzten E-Mail-Programm.

ESET Mail Security unterstützt außerdem die Prüfung von IMAPS- und POP3S-Protokollen, die Daten zwischen Server und Client über einen verschlüsselten Kanal übertragen. ESET Mail Security überwacht die über die Protokolle SSL (Secure Socket Layer) und TLS (Transport Layer Security) abgewickelte Kommunikation. Unabhängig von der Version des Betriebssystems wird nur Datenverkehr an Ports gescannt, die in „Vom **IMAPS-/POP3S-Protokoll** verwendete Ports“ definiert wurden.

Einstellungen für IMAPS / POP3-Scanner

Verschlüsselter Datenverkehr wird mit den Standardeinstellungen nicht geprüft. Sie können die Prüfung von verschlüsseltem Datenverkehr in den erweiterten Einstellungen unter SSL/TLS-Protokollprüfung aktivieren.

Die Portnummer gibt an, um welchen Typ von Port es sich handelt. Eine Liste der Standardports für E-Mails:

Portname	Portnummern	Beschreibung
POP3	110	Standardport für unverschlüsseltes POP3.
IMAP	143	Standardport für unverschlüsseltes IMAP.
Sicheres IMAP (IMAP4-SSL)	585	SSL/TLS-Protokollfilterung aktivieren. Mehrere Portnummern müssen durch ein Komma voneinander getrennt sein.
IMAP4 über SSL (IMAPS)	993	SSL/TLS-Protokollfilterung aktivieren. Mehrere Portnummern müssen durch ein Komma voneinander getrennt sein.
Sicheres POP3 (SSL-POP)	995	SSL/TLS-Protokollfilterung aktivieren. Mehrere Portnummern müssen durch ein Komma voneinander getrennt sein.

E-Mail-Tags

Der E-Mail-Schutz dient der Überwachung eingehender E-Mails, die mit dem POP3-Protokoll übertragen werden. Mithilfe der Plug-In-Software für Microsoft Outlook und andere E-Mail-Programme stellt ESET Mail Security Kontrollfunktionen für die gesamte E-Mail-Kommunikation (POP3, MAPI, IMAP, HTTP) bereit.

Für die Prüfung eingehender Nachrichten verwendet das Programm alle erweiterten ThreatSense-Scan-Methoden. Die Erkennung von Schadcode findet also noch vor dem Abgleich mit der Virenerkennungsdatenbank statt. Das Scannen der POP3-Kommunikation erfolgt unabhängig vom verwendeten E-Mail-Programm.

Nach erfolgter Prüfung kann ein Prüfhinweis mit dem Scan-Ergebnis zu der E-Mail-Nachricht hinzugefügt werden. Wählen Sie entweder **Prüfhinweis an eingehende/gelesene E-Mails anhängen** oder **Prüfhinweis an ausgehende E-Mails anhängen** aus.

Es kann jedoch nicht ausgeschlossen werden, dass bestimmte Bedrohungen Prüfhinweise in problematischen HTML-Nachrichten fälschen oder löschen. Prüfhinweise können zu empfangenen und gelesenen E-Mails und/oder zu gesendeten E-Mails hinzugefügt werden.

Verfügbare Optionen:

- **Nie** - Es werden keine Prüfhinweise zu E-Mails hinzugefügt.
- **Wenn ein Ereignis auftritt** – Prüfhinweise werden nur E-Mails hinzugefügt, in denen Schadcode erkannt wurde (Standardeinstellung).
- **Für alle E-Mails beim Scannen** – Alle gescannten E-Mails werden mit Prüfhinweisen versehen.

Text, der zum Betreff der erkannten E-Mail hinzugefügt wird

Geben Sie hier den Text ein, der das Präfix in der Betreffzeile einer infizierten E-Mail ersetzen soll. Diese Funktion ersetzt den Nachrichtenbetreff `Hello` durch das folgende Format: `[Ereignis %DETECTIONNAME%] Hello`. Die Variable `%DETECTIONNAME%` enthält den Ereignisnamen.

Symbolleiste für Microsoft Outlook

Für den Schutz von Microsoft Outlook wird ein Plug-In verwendet. Nach der Installation von ESET Mail Security wird diese Symbolleiste mit Malware-Schutzoptionen zu Microsoft Outlook hinzugefügt:

ESET Mail Security

Klicken Sie auf das Symbol, um das Programmfenster von ESET Mail Security zu öffnen.

E-Mails erneut prüfen

E-Mail-Prüfung manuell starten. Sie können E-Mails festlegen, die gescannt werden sollen, und das erneute Prüfen empfangener E-Mails aktivieren. Weitere Informationen finden Sie unter E-Mail-Schutz.

Einstellungen für Prüfung

Anzeige der Optionen für den E-Mail-Schutz.

Symbolleisten für Outlook Express und Windows Mail

Für den Schutz in Outlook Express und Windows Mail wird ein Plug-In verwendet. Nach der Installation von ESET Mail Security wird diese Symbolleiste mit Malware-Schutzoptionen zu Outlook Express bzw. Windows Mail hinzugefügt:

ESET Mail Security

Klicken Sie auf das Symbol, um das Programmfenster von ESET Mail Security zu öffnen.

E-Mails erneut prüfen

Mit dieser Funktion können Sie die E-Mail-Prüfung manuell starten. Sie können E-Mails festlegen, die gescannt werden sollen, und das erneute Prüfen empfangener E-Mails aktivieren. Weitere Informationen finden Sie unter E-Mail-Schutz.

Einstellungen für Prüfung

Anzeige der Optionen für den E-Mail-Schutz.

Anzeige anpassen

Sie können die Anzeige der Symbolleiste für Ihr E-Mail-Programm ändern. Deaktivieren Sie die Option für die Anpassung der Anzeige unabhängig von den Parametern des E-Mail-Programms.

- **Symboltitel anzeigen** - Beschreibung für Symbole anzeigen.
- **Symboltitel rechts** - Die Beschreibungen werden vom unteren zum seitlichen Bereich der Symbole verschoben.
- **Große Symbole** - Große Symbole für Menüeinstellungen.

Bestätigungsfenster

Mit diesem Hinweis wird geprüft, ob die ausgewählte Aktion wirklich durchgeführt werden soll. Dadurch sollen mögliche Fehler vermieden werden. In diesem Dialogfeld können Sie außerdem die Bestätigungen deaktivieren.

E-Mails erneut prüfen

Die in E-Mail-Programmen integrierte ESET Mail Security-Symbolleiste bietet Benutzern verschiedene Optionen zum Prüfen von E-Mails. Die Option **E-Mails erneut prüfen** bietet zwei Prüfmodi:

- **Alle E-Mails im aktuellen Ordner** - Alle E-Mails im aktuell angezeigten Ordner werden geprüft.
- **Nur markierte E-Mails** - Nur markierte E-Mails werden geprüft.
- **Bereits geprüfte E-Mails erneut prüfen** - Option einer erneuten Prüfung bereits geprüfter E-Mails.

Web-Schutz

Der Web-Schutz besteht in der Überwachung der Kommunikation zwischen Webbrowsern und Remoteservern, schützt Sie vor Onlinebedrohungen und entspricht den Regeln für HTTP (Hypertext Transfer Protocol) und HTTPS (verschlüsselte Kommunikation).

Der Zugriff auf Webseiten, die bekannterweise Schadcode enthalten, wird vor dem Herunterladen von Inhalten blockiert. Alle anderen Webseiten werden beim Laden vom ThreatSense-Modul gescannt und blockiert, wenn Schadcode gefunden wird. Der Web-Schutz bietet zwei Schutzebenen: Blockieren nach Negativliste und Blockieren nach Inhalt.

Einfach

Der **Web-Schutz** sollte unbedingt immer aktiviert sein. Sie finden diese Option auch im Hauptfenster von ESET Mail Security unter **Einstellungen** > **Web und E-Mail** > **Web-Schutz**.
Erweiterte Überprüfung von Browser-Skripts aktivieren
Die Erkennungsroutine scannt standardmäßig alle in Webbrowsern ausgeführten JavaScript-Programme.

Webprotokolle

Hier können Sie die Überwachung dieser von den meisten Internetbrowsern verwendeten Standardprotokolle konfigurieren. ESET Mail Security Ist standardmäßig so konfiguriert, dass das von den meisten Webbrowsern verwendete HTTP-Protokoll überwacht wird.
ESET Mail Security unterstützt auch die HTTPS-Protokollprüfung. Bei der HTTPS-Kommunikation wird zur Datenübertragung zwischen Server und Client ein verschlüsselter Kanal verwendet. ESET Mail Security überwacht die mit Hilfe der Protokolle SSL (Secure Socket Layer) und TLS (Transport Layer Security) abgewickelte Kommunikation. Unabhängig von der Version des Betriebssystems wird nur Datenverkehr an Ports gescannt, die unter **Vom HTTPS-Protokoll verwendete Ports** definiert wurden.
Verschlüsselter Datenverkehr wird mit den Standardeinstellungen nicht gescannt. Sie können das Scannen des verschlüsseltem Datenverkehrs in den **erweiterten Einstellungen** (**F5**) unter **Web und E-Mail** > SSL/TLS aktivieren.

ThreatSense-Parameter

Legen Sie Einstellungen für Scan-Typen (E-Mails, Archive usw.) und Erkennungsmethoden für den Web-Schutz fest.

URL-Adressverwaltung

URL-Adressverwaltung - Hier können Sie festlegen, welche HTTP-Adressen blockiert, zugelassen oder von der Prüfung ausgeschlossen werden sollen. Der Zugriff auf Websites in der Liste der blockierten Adressen ist nur dann möglich, wenn diese sich auch in der Liste der zulässigen Adressen befinden. Websites, die in der Liste der von der Prüfung ausgenommenen Adressen aufgeführt sind, werden vor dem Zugriff nicht auf Schadcode gescannt. Wenn neben HTTP-Webseiten auch HTTPS-Adressen gefiltert werden sollen, müssen Sie die Option SSL/TLS-Protokollfilterung aktivieren. Andernfalls werden nur die Domänen besuchter HTTPS-Sites hinzugefügt, jedoch nicht die kompletten URLs.

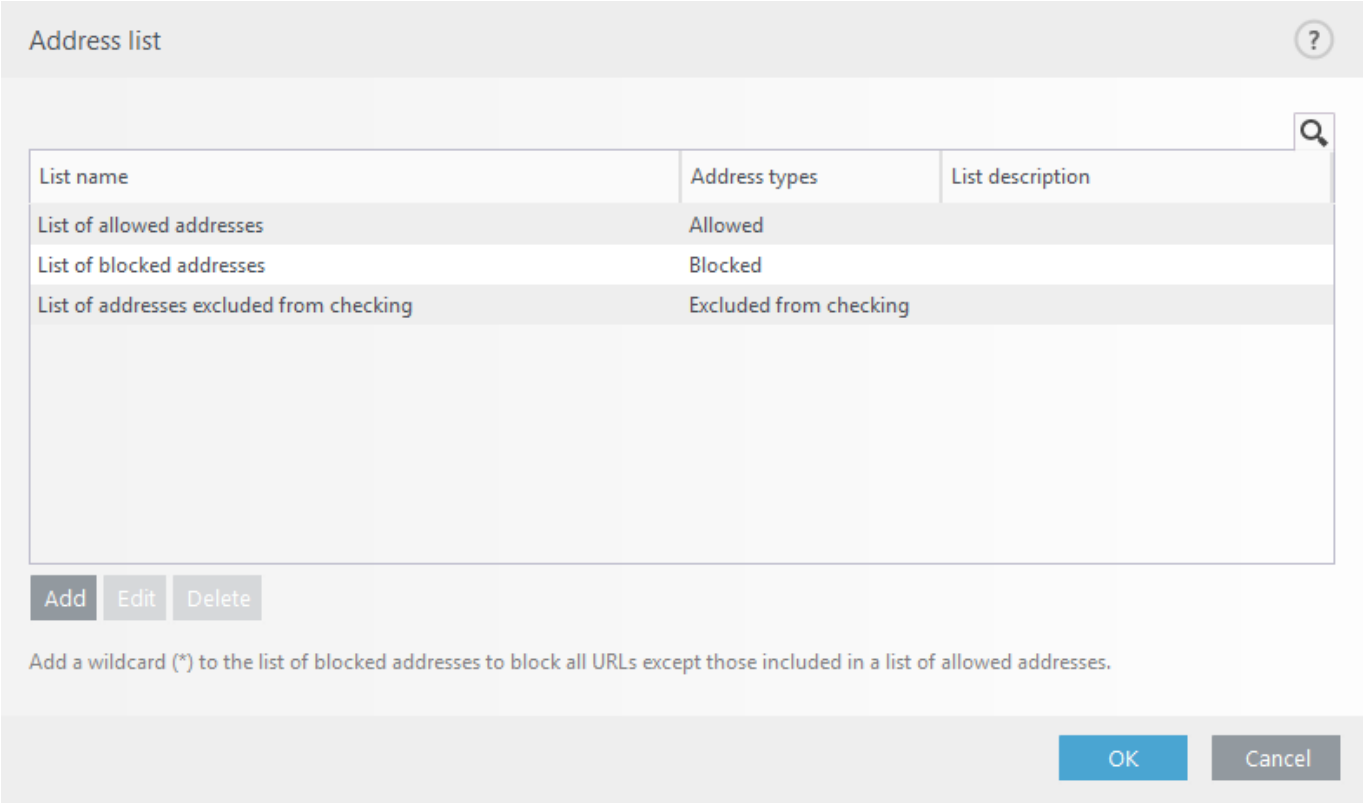
Eine Liste blockierter Adressen kann Adressen aus einer externen öffentlichen Negativliste und eine zweite Ihre eigene Negativliste enthalten. Auf diese Weise können Sie die externe Liste einfacher aktualisieren, während Ihre Liste intakt bleibt.

Klicken Sie auf **Bearbeiten**, um eine neue Adressliste zu den vordefinierten Listen **hinzuzufügen**. Dies ist hilfreich, wenn Sie verschiedene Gruppen und Adressen auf logische Art und Weise aufteilen möchten. Standardmäßig stehen die drei folgenden Listen zur Verfügung:

- **Liste von der Prüfung ausgeschlossener Adressen** - Für die Adressen in dieser Liste wird keine Prüfung auf Schadcode ausgeführt.

- **Liste zugelassener Adressen** - Wenn die Option Nur Zugriff auf HTTP-Adressen aus der Liste zulässiger Adressen erlauben aktiviert ist und die Liste blockierter Adressen ein Sternchen (*) enthält, darf der Benutzer nur auf Adressen in dieser Liste zugreifen. Die Adressen in der Liste sind zugelassen, auch wenn Sie ebenfalls in der Liste blockierter Adressen enthalten sind.

- **Liste blockierter Adressen** - Auf die in dieser Liste genannten Adressen kann der Benutzer nicht zugreifen, es sei denn, die Adressen sind auch in der Liste zugelassener Adressen enthalten.



Sie können eine neue URL-Adresse zur Liste **hinzufügen**. Geben Sie mehrere Werte mit einem Trennzeichen ein. Klicken Sie auf **Bearbeiten**, um eine vorhandene Adresse in der Liste zu bearbeiten, oder auf **Löschen**, um sie zu löschen. Die Löschfunktion ist nur für die mit der Funktion **Hinzufügen** erstellten Adressen möglich, nicht für importierte Adressen.

In allen Listen können Sie die Platzhalterzeichen * (Sternchen) und ? (Fragezeichen) verwenden. Das Sternchen ersetzt eine beliebige Zahl oder ein beliebiges Zeichen, das Fragezeichen ein beliebiges Zeichen. Die Liste der ausgeschlossenen Adressen sollten Sie mit Bedacht zusammenstellen. Geben Sie ausschließlich vertrauenswürdige und sichere Adressen an. Achten Sie darauf, dass die Zeichen „*“ und „?“ korrekt verwendet werden.

> Wenn alle HTTP-Adressen außer denen in der aktiven Liste zugelassener Adressen blockiert werden sollen, fügen Sie der aktiven Liste blockierter Adressen ein Sternchen (*) hinzu.

Neue Liste erstellen

Die Liste legt fest, welche URL-Adressen/Masken blockiert, zugelassen oder vom Scannen ausgeschlossen werden sollen. Geben Sie bei der Erstellung einer neuen Liste Folgendes an:

- **Typ der Adressliste** - Wählen Sie den Typ (Von der Prüfung ausgeschlossen, Blockiert oder Erlaubt) aus der Dropdownliste aus.
- **Listenname** - Geben Sie den Namen der Liste ein. Bei der Bearbeitung einer der drei vordefinierten Listen ist dieses Feld ausgegraut.
- **Listenbeschreibung** - Geben Sie eine kurze Beschreibung für die Liste ein (optional). Wird bei der Bearbeitung einer der drei vordefinierten Listen ausgegraut.
- **Liste aktiv** - Mit diesem Schalter können Sie die Liste deaktivieren. Sie können die Liste später bei Bedarf

aktivieren.

• **Bei Anwendung benachrichtigen** - Wenn Sie benachrichtigt werden möchten, wenn eine bestimmte Liste bei der Prüfung einer von Ihnen besuchten HTTP-Site verwendet wird. Mit dieser Option wird eine Benachrichtigung ausgegeben, wenn eine Website blockiert oder zugelassen wird, weil sie in der Liste der blockierten oder zugelassenen Adressen enthalten ist. Die Benachrichtigung enthält den Namen der Liste mit der angegebenen Website.

• Wählen Sie den **Logging-Schweregrad** (Kein, Diagnose, Information oder Warnung) in der Dropdownliste aus. Einträge mit dem Schweregrad Warnung können von ESET PROTECT gesammelt werden.

ESET Mail Security kann den Zugriff auf bestimmte Webseiten sperren, sodass der Browser deren Inhalte nicht anzeigt. Darüber hinaus können Adressen angegeben werden, die nicht geprüft werden sollen. Wenn der vollständige Name des Remoteservers nicht bekannt ist oder eine ganze Gruppe von Remoteservern angegeben werden soll, können Sie sogenannte Masken verwenden.

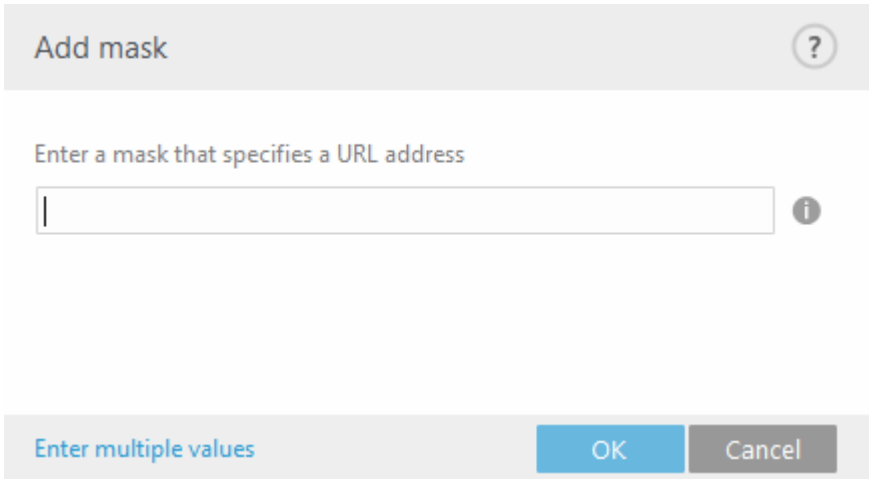
Diese Masken verwenden die Symbole „?“ und „*“:

• Mit „?“ können Sie ein einzelnes Zeichen ersetzen.

• Mit „*“ können Sie eine Textfolge ersetzen.

✓ **.c?m* deckt alle Adressen ab, deren erster Buchstabe c ist, die mit dem Buchstaben „m“ enden und dazwischen ein unbekanntes Zeichen enthalten (*.com*, *.cam* usw.).

Die vorangestellte Sequenz *. am Anfang eines Domänennamens hat eine Sonderbedeutung. Zunächst erfasst der *-Platzhalter in diesem Fall nicht den Schrägstrich (/). Auf diese Weise wird eine Umgehung der Maske vermieden. Die Maske *.domain.com erfasst z. B. nicht die URL *https://anydomain.com/anypath#.domain.com* (dieses Suffix kann an beliebige URLs angehängt werden, ohne den Download zu beeinträchtigen). Außerdem erfasst die Sequenz "*." in diesem Sonderfall auch eine leere Zeichenfolge. Auf diese Weise ist es möglich, eine gesamte Domäne inklusive aller Unterdomänen mit einer einzigen Maske zu erfassen. Die Maske *.domain.com erfasst z. B. auch *https://domain.com*. *domain.com wäre dagegen nicht korrekt, da diese Maske auch https://anotherdomain.com. erfasst.



Mehrere Werte eingeben

Geben Sie mehrere durch Zeilenumbrüche, Kommas oder Semikolon getrennte URL-Adressen ein. Wenn die Mehrfachauswahl aktiviert ist, werden die Adressen in der Liste angezeigt.

Importieren

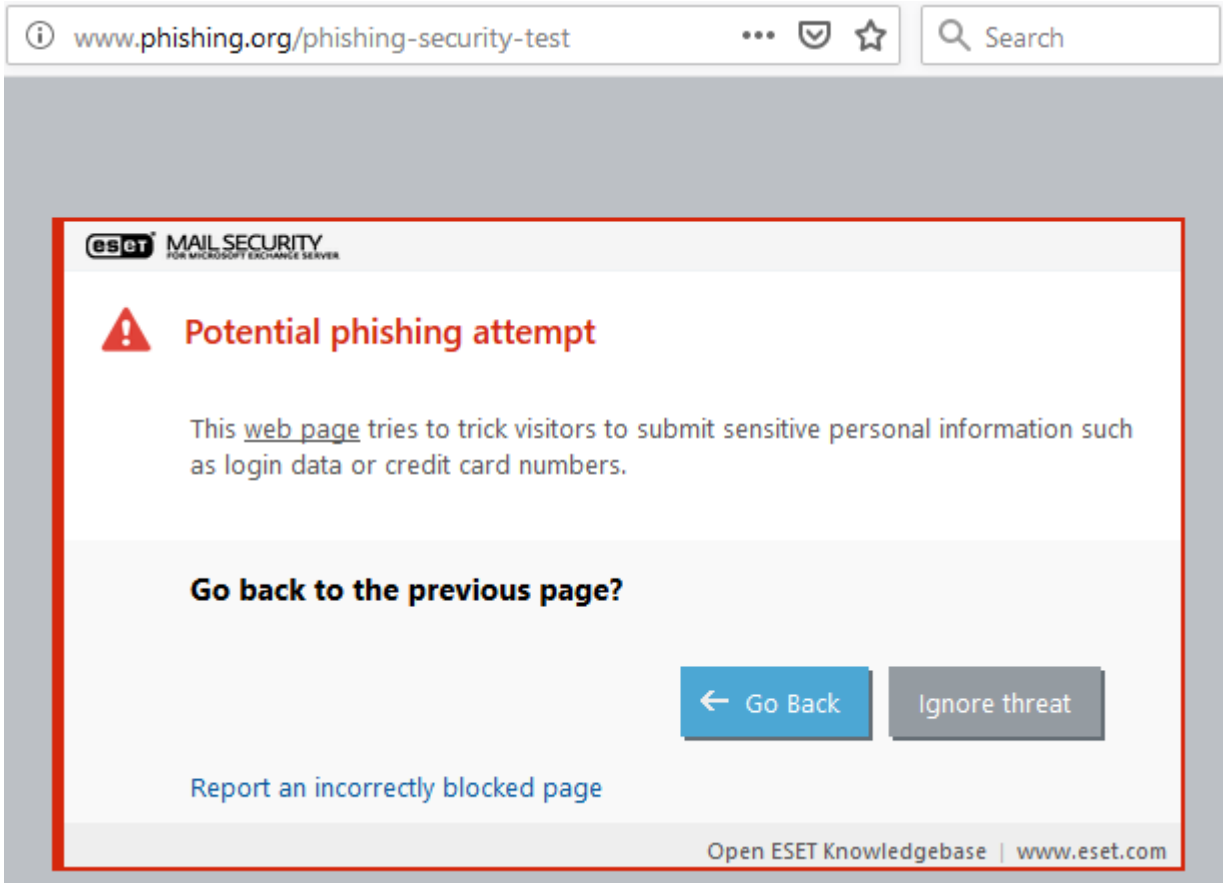
Importiert eine Datei mit URL-Adressen (trennen Sie die Werte mit Zeilenumbrüchen, z. B. `*.txt` mit UTF-8).

Web-Phishing-Schutz

Der Begriff „Phishing“ bezeichnet eine kriminelle Vorgehensweise, die sich Techniken des Social Engineering (Manipulation von Benutzern zur Erlangung vertraulicher Informationen) zunutze macht. Phishing wird oft eingesetzt, um Zugriff auf vertrauliche Daten wie Kontonummern oder PIN-Codes zu erlangen.

ESET Mail Security umfasst den Phishing-Schutz, der Webseiten sperrt, die für diese Arten von Inhalten bekannt sind. Der Phishing-Schutz in ESET Mail Security sollte unbedingt aktiviert werden. In unserem Knowledgebase-Artikel finden Sie weitere Informationen zum Phishing-Schutz von ESET Mail Security.

Wenn Sie auf eine erkannte Phishing-Website zugreifen, wird das folgende Dialogfenster im Webbrowser angezeigt. Wenn Sie die Website trotzdem öffnen möchten, klicken Sie auf **Bedrohung ignorieren** (nicht empfohlen).



Potenzielle Phishing-Websites, die zur Positivliste hinzugefügt wurden, werden standardmäßig nach einigen Stunden wieder von der Liste gelöscht. Verwenden Sie die URL-Adressverwaltung, um eine Website dauerhaft zuzulassen.

Phishing-Seite melden

Falls Sie eine verdächtige Website bemerken, auf der Sie Phishing oder andere bösartige Aktivitäten vermuten, können Sie diese zur Analyse an ESET übermitteln. Auf Websites, die Sie bei ESET melden, sollte mindestens eines der folgenden Kriterien zutreffen:

- Die Website wird nicht als Bedrohung erkannt.
- Die Website wird als Bedrohung erkannt, obwohl sie keinen Schadcode enthält. In diesem Fall können Sie einen Phishing-Fehlalarm melden.

Sie können Websites auch per E-Mail melden. Senden Sie die E-Mail an samples@eset.com. Verwenden Sie einen treffenden Text in der Betreffzeile und liefern Sie möglichst viele Informationen zur Website (wie Sie auf die Website gelangt sind, wo Sie von der Website erfahren haben usw.).

Gerätesteuerung

ESET Mail Security bietet Methoden zur automatischen Prüfung von Geräten (CD/DVD/USB/...). Mit diesem Modul können Sie Medien bzw. Geräte prüfen oder sperren oder erweiterte Filter- und Berechtigungseinstellungen anpassen und definieren, wie Benutzer auf diese Geräte zugreifen und mit ihnen arbeiten dürfen. Dies ist sinnvoll, wenn der Administrator verhindern möchte, dass Benutzer Geräte mit unerwünschten Inhalten verwenden.

Mit dem Schalter **Systemintegration** können Sie die Gerätesteuerung von ESET Mail Security aktivieren. Die Änderung tritt jedoch erst nach einem Neustart des Systems in Kraft.

Die Gerätesteuerung wird aktiviert, und Sie können die Einstellungen bearbeiten. Wenn das System ein von einer bestehenden Regel blockiertes Gerät erkennt, wird ein Hinweisfenster angezeigt und es wird kein Zugriff auf das Gerät gewährt.

Regeln

Eine Regel für die Medienkontrolle definiert die Aktion, die ausgeführt wird, wenn ein Gerät, das die Regelkriterien erfüllt, an den Computer angeschlossen wird.

Gruppen

Klicken Sie auf Bearbeiten, um Gerätegruppen zu verwalten. Erstellen Sie eine neue Gerätegruppe oder wählen Sie eine vorhandene Gerätegruppe aus, um Geräte zur Liste hinzuzufügen oder daraus zu entfernen.

Sie finden die Log-Einträge der Gerätesteuerung in den Log-Dateien.

Geräteregeln

Bestimmte Gerätetypen können für Benutzer oder Benutzergruppen oder auf Grundlage weiterer, in der Regelkonfiguration festgelegter Parameter zugelassen oder gesperrt werden. Die Regelliste beschreibt die Regeln mit Namen, Gerätetyp, Aktion nach der Erkennung eines Geräts und Log-Schweregrad.

Sie können eine neuen Regel **hinzufügen** oder die Einstellungen einer vorhandenen Regeln bearbeiten. Geben Sie zur leichteren Identifizierung der Regel im Feld **Name** eine Beschreibung ein. Über den Schalter neben **Regel aktiviert** wird die Regel deaktiviert bzw. aktiviert. Dies ist nützlich, wenn Sie eine Regel deaktivieren, jedoch nicht dauerhaft löschen möchten.

Anwendungszeitraum

Sie können Regeln mit Zeitfenstern einschränken. Ihre erstellten Zeitfenster werden im Dropdownmenü angezeigt.

Gerätetyp

Wählen Sie im Dropdown-Menü den Typ des externen Geräts aus (Datenträgerspeicher/tragbares Gerät/Bluetooth/FireWire/...). Die Gerätetypen werden vom Betriebssystem übernommen und können im Geräte-Manager angezeigt werden, sofern ein Gerät an den Computer angeschlossen ist. Zu den Speichergeräten gehören externe Laufwerke und herkömmliche Speicherkartenleser, die per USB oder FireWire angeschlossen sind. Smartcard-Lesegeräte umfassen Kartenlesegeräte für Smartcards mit eingebettetem integriertem Schaltkreis, beispielsweise SIM-Karten oder Authentifizierungskarten. Bildverarbeitungsgeräte sind beispielsweise Scanner oder Kameras. Diese Geräte liefern keine Informationen über Benutzer, sondern nur über deren Aktionen. Dies bedeutet, dass Bildverarbeitungsgeräte nur global gesperrt werden können.

Aktion

Der Zugriff auf andere Geräte als Speichergeräte kann entweder zugelassen oder gesperrt werden. Im Gegensatz dazu ist es für Speichergeräte möglich, eines der folgenden Rechte für die Regel auszuwählen:

- **Lese-/Schreibzugriff** - Der vollständige Zugriff auf das Gerät wird zugelassen.
- **Sperren** - Der Zugriff auf das Gerät wird gesperrt.
- **Nur Lesezugriff** - Nur Lesezugriff auf das Gerät wird zugelassen.
- **Warnen** - Jedes Mal, wenn ein Gerät angeschlossen wird, erhält der Benutzer eine Benachrichtigung, die angibt, ob das Gerät zugelassen oder gesperrt ist. Außerdem wird ein Log-Eintrag erstellt. Die Geräteinformationen werden nicht gespeichert, d. h. bei einem erneuten, späteren Anschluss des gleichen Geräts wird die Benachrichtigung erneut angezeigt.

> Bestimmte Rechte (Aktionen) sind nur für bestimmte Gerätetypen verfügbar. Wenn das Gerät Speicherplatz enthält, sind alle vier Aktionen verfügbar. Bei anderen Geräten als Speichergeräten sind nur zwei Aktionen verfügbar. (Die Aktion **Nur Lesezugriff** ist für Bluetooth-Geräte nicht verfügbar. Diese Geräte können daher nur entweder gesperrt oder zugelassen werden).

Kriterientyp

Weitere Parameter zur Feinanpassung der Regeln und Anpassung an bestimmte Geräte. Die Parameter unterscheiden zwischen Groß- und Kleinschreibung und unterstützen Platzhalter (*, ?):

- **Hersteller**– Filtern Sie die Liste nach Herstellername oder -ID.
- **Modell**– Die Bezeichnung des Geräts.
- **Seriennummer** - Externe Geräte verfügen üblicherweise über eigene Seriennummern. Bei CDs/DVDs bezieht sich die Seriennummer auf das Exemplar, nicht auf das Laufwerk.

> Wenn diese Parameter nicht festgelegt sind, ignoriert die Regel diese Felder beim Abgleich. Die Filterparameter in den Textfeldern unterscheiden zwischen Groß- und Kleinschreibung und unterstützen Platzhalter (ein Fragezeichen (?) steht für ein einzelnes Zeichen und ein Sternchen (*) für null bis mehrere Zeichen).

Um die Parameter eines Geräts zu ermitteln, erstellen Sie eine Regel für den entsprechenden Gerätetyp, schließen Sie das Gerät an den Computer an und überprüfen Sie dann die Gerätedetails im Gerätesteuerung-Log.

Wählen Sie den **Logging-Schweregrad** in der Dropdownliste aus:

- **Immer** - Alle Ereignisse werden protokolliert.
- **Diagnose** - Informationen, die für die Feineinstellung des Programms benötigt werden, werden protokolliert.
- **Informationen**– Meldungen wie erfolgreiche Updates und alle Meldungen höherer Stufen werden protokolliert.
- **Warnung** - Kritische Fehler und Warnungen werden protokolliert.
- **Keine** - Es werden keine Logs aufgezeichnet.

Die Regeln können auf bestimmte Benutzer oder Benutzergruppen beschränkt werden, indem Sie diese zur Benutzerliste hinzufügen: Klicken Sie auf **Bearbeiten**, um die **Benutzerliste** zu bearbeiten.

- **Hinzufügen** - Öffnet das Dialogfenster Objekttypen: Benutzer oder Gruppen, in dem Sie bestimmte Benutzer auswählen können.

- **Löschen** - Löscht den ausgewählten Benutzer aus dem Filter.

> Nicht alle Geräte können über Benutzerregeln eingeschränkt werden (Bildverarbeitungsgeräte liefern beispielsweise keine Informationen über Benutzer, sondern nur über aufgerufene Aktionen).

Folgende Funktionen stehen zur Verfügung:

Bearbeiten

Mit dieser Option können Sie den Namen der ausgewählten Regel oder die Parameter der enthaltenen Geräte (Hersteller, Modell, Seriennummer) ändern.

Kopieren

Erstellt eine neue Regel mit den Parametern der ausgewählten Regel.

Löschen

Löscht die ausgewählte Regel. Alternativ können Sie eine Regel mit dem benachbarten Kontrollkästchen deaktivieren. Dies ist besonders dann hilfreich, wenn Sie eine Regel nicht dauerhaft löschen möchten, um sie gegebenenfalls zu einem späteren Zeitpunkt wieder verwenden zu können.

Auslesen

Bietet einen Überblick über alle aktuell angeschlossenen Geräte nebst Informationen zu Gerätetyp, Gerätehersteller, Modell und Seriennummer (sofern verfügbar). Wenn Sie ein Gerät (in der Liste der erkannten Geräte) auswählen und auf **OK** klicken, wird ein Regel-Editorfenster mit vordefinierten Informationen angezeigt (Sie können alle Einstellungen anpassen).

Die Regeln sind nach absteigender Priorität geordnet (Regeln mit höchster Priorität werden an oberster Stelle angezeigt). Sie können mehrere Regeln auswählen und Aktionen wie z. B. Löschen anwenden. Mit der Option **Oben**/**Nach oben**/**Nach unten**/**Unten** (Pfeilschaltflächen) können Sie außerdem alle Regeln in der Liste nach oben oder nach unten verschieben.

Gerätegruppen

Das Fenster „Gerätegruppen“ ist in zwei Bereiche unterteilt. Im rechten Bereich des Fensters wird eine Liste der Geräte angezeigt, die in der betroffenen Gruppe enthalten sind. Links werden die vorhandenen Gruppen angezeigt. Wählen Sie rechts die Gruppe aus, in der die Geräte enthalten sind, die Sie anzeigen möchten.

Sie können unterschiedliche Gerätegruppen für Geräte erstellen, auf die jeweils unterschiedliche Regeln angewendet werden sollen. Sie können auch eine einzige Gerätegruppe erstellen, die als **Lesen**/**Schreiben** oder **Schreibgeschützt** festgelegt wird. So werden nicht erkannte Geräte durch die Gerätesteuerung gesperrt, wenn sie an den Computer angeschlossen werden.

> Externe Geräte, die an Ihren Computer angeschlossen sind, können ein Sicherheitsrisiko darstellen.

Folgende Funktionen stehen zur Verfügung:

Hinzufügen

Je nachdem, in welchem Fensterbereich Sie auf diese Schaltfläche klicken, können Sie eine Gruppe durch Eingabe ihres Namens hinzufügen oder einer vorhandenen Gruppe ein Gerät hinzufügen (optional können Sie auch Details wie Herstellername, Modell und Seriennummer eingeben).

Bearbeiten

Mit dieser Option können Sie den Namen der ausgewählten Gruppe oder die Parameter der in der Gruppe enthaltenen Geräte (Hersteller, Modell, Seriennummer) ändern.

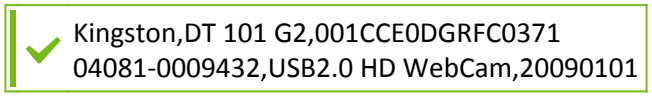
Löschen

Löscht die ausgewählte Gruppe bzw. das ausgewählte Gerät, je nachdem, in welchem Bereich des Fensters Sie auf die Schaltfläche klicken. Alternativ können Sie eine Regel mit dem benachbarten Kontrollkästchen deaktivieren. Dies ist besonders dann hilfreich, wenn Sie eine Regel nicht dauerhaft löschen möchten, um sie gegebenenfalls zu einem späteren Zeitpunkt wieder verwenden zu können.

Importieren

Importiert eine Liste von Geräteseriennummern aus einer Datei. Jedes Gerät wird in einer eigenen Zeile aufgeführt.

Hersteller, **Modell** und **Seriennummer** müssen für jedes Gerät angegeben und mit Kommas voneinander getrennt werden.



Auslesen

Bietet einen Überblick über alle aktuell angeschlossenen Geräte nebst Informationen zu Gerätetyp, Gerätehersteller, Modell und Seriennummer (sofern verfügbar). Wenn Sie ein Gerät (in der Liste der erkannten Geräte) auswählen und auf **OK** klicken, wird ein Regel-Editorfenster mit vordefinierten Informationen angezeigt (Sie können alle Einstellungen anpassen).

Gerät hinzufügen

Klicken Sie rechts auf „Hinzufügen“, um ein Gerät zu einer vorhandenen Gruppe hinzuzufügen. Mit den unten gezeigten zusätzlichen Parametern können Sie die Regeln für verschiedene Geräte differenziert festlegen. Die Parameter unterscheiden zwischen Groß- und Kleinschreibung und unterstützen Platzhalter (*, ?):

- **Hersteller** - Filtern Sie die Liste nach Herstellername oder -ID.
- **Modell** - Die Bezeichnung des Geräts.
- **Seriennummer** - Externe Geräte verfügen üblicherweise über eigene Seriennummern. Bei CDs/DVDs bezieht sich die Seriennummer auf das Exemplar, nicht auf das Laufwerk.
- **Beschreibung** – Beschreibung des Geräts zur besseren Unterscheidung.

Wenn diese Parameter nicht festgelegt sind, ignoriert die Regel diese Felder beim Abgleich. Die Filterparameter in den Textfeldern unterscheiden zwischen Groß- und Kleinschreibung und unterstützen Platzhalter (ein Fragezeichen (?) steht für ein einzelnes Zeichen und ein Sternchen (*) für null bis mehrere Zeichen).

Nachdem Sie eine Gerätegruppe erstellt haben, müssen Sie eine neue Regel für die Medienkontrolle für die erstellte Gerätegruppe hinzufügen und die auszuführende Aktion auswählen.

Klicken Sie auf **OK**, wenn Sie die Bearbeitung abgeschlossen haben. Klicken Sie auf **Abbrechen**, um das Fenster **Gerätegruppen** zu schließen, ohne die Änderungen zu speichern.

Bestimmte Rechte (Aktionen) sind nur für bestimmte Gerätetypen verfügbar. Wenn das Gerät Speicherplatz enthält, sind alle vier Aktionen verfügbar. Bei anderen Geräten als Speichergeräten sind nur zwei Aktionen verfügbar. (Die Aktion Nur Lesezugriff ist für Bluetooth-Geräte nicht verfügbar. Diese Geräte können daher nur entweder gesperrt oder zugelassen werden).

Tool-Konfiguration

In diesem Abschnitt können Sie die folgenden erweiterten Einstellungen anpassen:

- Zeitfenster
- Microsoft Windows® Update
- ESET CMD
- ESET RMM
- Lizenz
- WMI-Anbieter
- Scan-Ziele für die ESET Management-Konsole
- Log-Dateien
- Proxyserver
- Präsentationsmodus
- Diagnose
- Cluster

Zeitfenster

Zeitfenster werden in Regeln für die Gerätesteuerung verwendet, um festzulegen, wann die Regeln angewendet werden. Erstellen Sie ein Zeitfenster und wählen Sie es beim Erstellen oder Bearbeiten von Regeln aus (Parameter **Anwendungszeitraum**). Auf diese Weise können Sie häufig verwendete Zeitfenster (Geschäftszeiten, Wochenende usw.) definieren und für mehrere Regeln wiederverwenden. Zeitfenster sollten für alle relevanten Regeltypen anwendbar sein, die eine zeitbasierte Kontrolle unterstützen.

Microsoft Windows Update

Windows-Updates stellen wichtige Korrekturen für möglicherweise gefährliche Schwachstellen bereit und verbessern das allgemeine Sicherheitsniveau des Computers. Aus diesem Grund ist es essenziell, dass Sie verfügbare Microsoft Windows-Updates sofort installieren. Entsprechend der von Ihnen festgelegten Richtlinien benachrichtigt Sie ESET Mail Security über fehlende Updates. Folgende Richtlinien sind verfügbar:

- **Keine Updates** - Es werden keine Updates zum Download angeboten.
- **Optionale Updates** - Updates mit beliebiger Priorität werden zum Download angeboten.
- **Empfohlene Updates** - Updates mit normaler Priorität und höher werden zum Download angeboten.
- **Wichtige Updates** - Updates mit hoher Priorität und kritische Updates werden zum Download angeboten.
- **Kritische Updates** - Nur kritische Updates werden zum Download angeboten.

Klicken Sie auf **OK**, um die Änderungen zu speichern. Das Fenster „System-Updates“ wird nach erfolgter Statusverifizierung durch den Update-Server angezeigt. Die aktualisierten Systemdaten stehen möglicherweise nicht unmittelbar nach Speicherung der Änderungen zur Verfügung.

Befehlszeilenscanner

Als Alternative zu eShell können Sie den ESET Mail Security On-Demand-Scanner über die Befehlszeile mit `ecls.exe` im Installationsordner ausführen.

Hier finden Sie eine Liste der Parameter und Optionen:

Optionen:

`/base-dir=FOLDER`	module aus ORDNER laden
`/quar-dir=FOLDER`	Quarantäne-ORDNER
`/exclude=MASK`	Dateien, die mit der MASKE übereinstimmen, von Prüfungen ausschließen
`/subdir`	Unterordner scannen (Standard)
`/no-subdir`	Unterordner nicht scannen
`/max-subdir-level=LEVEL`	Maximale Suchtiefe von Unterordnern bei Scans
`/symlink`	Symbolischen Links folgen (Standards)
`/no-symlink`	Symbolischen Links nicht folgen
`/ads`	ADS scannen (Standard)
`/no-ads`	ADS nicht scannen
`/log-file=FILE`	Ausgabe in DATEI protokollieren
`/log-rewrite`	Ausgabedatei überschreiben (Standard: Anhängen)
`/log-console`	Ausgabe in Konsole protokollieren (Standard)
`/no-log-console`	Ausgabe nicht in Konsole protokollieren
`/log-all`	Sauber Dateien auch in Log aufnehmen
`/no-log-all`	Saubere Dateien nicht in Log aufnehmen (Standard)

/aind	Aktivitätsanzeige anzeigen
/auto	Alle lokalen Laufwerke scannen und automatisch säubern

Einstellungen für Prüfungen:

/files	Dateien scannen (Standard)
/no-files	Dateien nicht scannen
/memory	Speicher scannen
/boots	Bootsektoren scannen
/no-boots	Bootsektoren nicht scannen (Standard)
/arch	Archive scannen (empfohlen)
/no-arch	Archive nicht scannen
/max-obj-size=SIZE	Nur Dateien scannen, die kleiner als GRÖSSE Megabyte sind (Standard: 0 = unbegrenzt)
/max-arch-level=LEVEL	Maximale Verschachtelungstiefe von Archiven bei Scans
/scan-timeout=LIMIT	Archive maximal MAXIMALE PRÜFDAUER Sekunden scannen
/max-arch-size=SIZE	Nur Dateien in Archiven scannen, die kleiner als SIZE sind (Standard: 0 = unbegrenzt)
/max-sfx-size=SIZE	Nur Dateien in selbstentpackenden Archiven scannen, die kleiner als GRÖSSE Megabyte sind (Standard: 0 = unbegrenzt)
/mail	E-Mails scannen (Standard)
/no-mail	E-Mails nicht scannen
/mailbox	postfächer scannen (Standard)
/no-mailbox	postfächer nicht scannen
/sfx	Selbstentpackende Archive scannen (Standard)
/no-sfx	Selbstentpackende Archive nicht scannen
/rtp	Laufzeitkomprimierte Dateien scannen (Standard)
/no-rtp	Laufzeitkomprimierte Dateien nicht scannen
/unsafe	nach potenziell unsicheren Anwendungen scannen
/no-unsafe	nicht nach potenziell unsicheren Anwendungen scannen (Standard)
/unwanted	nach evtl. unerwünschten Anwendungen scannen
/no-unwanted	nicht nach evtl. unerwünschte Anwendungen scannen (Standard)
/suspicious	nach verdächtigen Anwendungen scannen (Standard)
/no-suspicious	nicht nach verdächtigen Anwendungen scannen
/pattern	Signaturdatenbank verwenden (Standard)
/no-pattern	Signaturdatenbank nicht verwenden
/heur	Heuristik aktivieren (Standard)
/no-heur	Heuristik deaktivieren
/adv-heur	Erweiterte Heuristik aktivieren (Standard)
/no-adv-heur	Erweiterte Heuristik deaktivieren
/ext-exclude=EXTENSIONS	Mit Doppelpunkt angegebene ERWEITERUNGEN vom Scannen ausschließen

/clean-mode=MODE	Säuberungs-MODUS für infizierte Objekte verwenden Folgende Optionen stehen zur Verfügung: • none (Standard) – Es wird keine automatische Säuberung ausgeführt. • standard – ecls.exe versucht, infizierte Dateien automatisch zu säubern oder zu löschen. • strict – ecls.exe versucht, infizierte Dateien ohne Benutzereingriff automatisch zu säubern oder zu löschen (Sie werden nicht gefragt, bevor Dateien gelöscht werden). • rigorous – ecls.exe löscht Dateien ohne vorherigen Säuberungsversuch unabhängig von der Art der Datei. • delete – ecls.exe löscht Dateien ohne vorherigen Säuberungsversuch, löscht jedoch keine sensiblen Dateien wie Windows-Systemdateien.
/quarantine	Infizierte Dateien (falls gesäubert) in die Quarantäne kopieren (ergänzt die beim Säubern ausgeführte Aktion)
/no-quarantine	Infizierte Dateien nicht in die Quarantäne kopieren

Allgemeine Optionen:

/help	Hilfe anzeigen und beenden
/version	Versionsinformationen anzeigen und beenden
/preserve-time	Datum für 'Geändert am' beibehalten

Exitcodes:

0	keine Bedrohungen gefunden
1	bedrohungen gefunden und entfernt
10	einige Dateien konnten nicht geprüft werden (evtl. Bedrohungen)
50	Bedrohung gefunden
100	Fehler (Exitcodes größer 100 bedeuten, dass die Datei nicht gescannt wurde und nicht als sauber gilt)

ESET CMD

Diese Funktion unterstützt erweiterte ecmd-Befehle. Sie können Einstellungen über die Befehlszeile (ecmd.exeecmd.exe) importieren und exportieren. Bisher konnten Einstellungen nur über die Benutzeroberfläche exportiert werden. Die ESET Mail Security-Konfiguration kann in eine *.xml*-Datei exportiert werden.

Wenn Sie ESET CMD aktiviert haben, stehen zwei Autorisierungsmethoden zur Verfügung:

- **Keine** – Keine Autorisierung. Diese Methode sollte nicht verwendet werden, da andernfalls beliebige unsignierte Konfigurationen importiert werden können, was ein Sicherheitsrisiko darstellt.

- **Passwort für die erweiterten Einstellungen** - Wenn Sie eine Konfiguration aus einer .xml-Datei importieren, benötigen Sie ein Passwort und müssen die Datei zunächst signieren (siehe „Signieren von .xml-Konfigurationsdateien“ weiter unten). Sie müssen das unter Einstellungen für den Zugriff festgelegte Passwort eingeben, um eine neue Konfiguration importieren zu können. Wenn Sie diese Einstellungen nicht festgelegt haben, das Passwort nicht übereinstimmt oder die .xml-Konfigurationsdatei nicht signiert ist, wird die Konfiguration nicht importiert.

Nachdem Sie ESET CMD aktiviert haben, können Sie ESET Mail Security-Konfigurationen über die Befehlszeile

importieren und exportieren. Sie können diesen Vorgang manuell ausführen oder ein Skript für die Automatisierung erstellen.

Sie müssen die erweiterten ecmd-Befehle entweder mit Administratorberechtigungen oder in einer Windows-Befehlszeile (cmd) mit der Option **Als Administrator ausführen** verwenden. Andernfalls erhalten Sie die Nachricht **Fehler beim Ausführen des Befehls**. Außerdem muss der ausgewählte Zielordner beim Exportieren einer Konfiguration vorhanden sein. Der Befehl zum Exportieren funktioniert auch, wenn die ESET CMD-Einstellung deaktiviert ist.

Befehl zum Exportieren von Einstellungen:
`ecmd /getcfg c:\config\settings.xml`

Befehl zum Importieren von Einstellungen:
`ecmd /setcfg c:\config\settings.xml`

Die erweiterten ecmd-Befehle können nur lokal ausgeführt werden. Der Client-Task **Befehl ausführen** in ESET PROTECT unterstützt diese Befehle nicht.

Signieren einer *.xml*-Konfigurationsdatei:

1. Laden Sie das ausführbare XmlSignTool herunter.

2. Öffnen Sie eine Windows-Eingabeaufforderung (cmd) mit der Option **Als Administrator ausführen**.

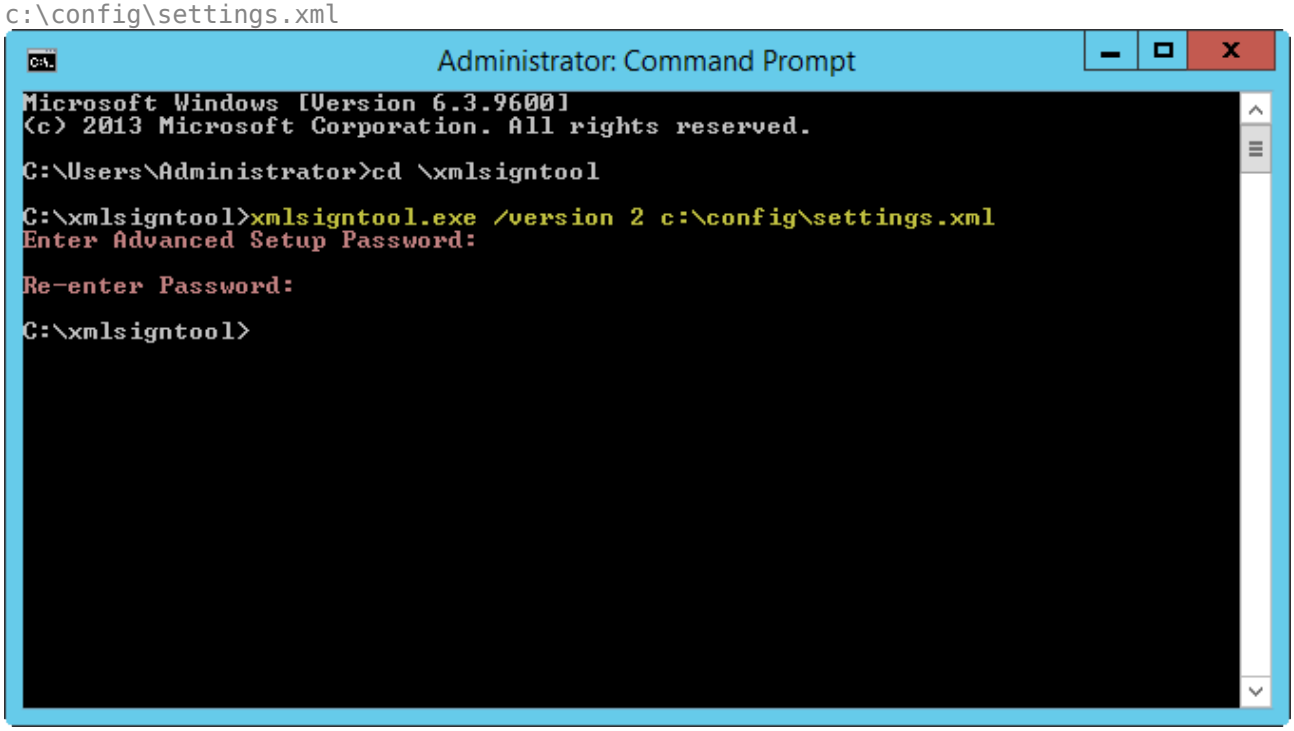
3. Navigieren Sie zum Speicherort von `xmlsigntool.exe`.

4. Führen Sie den Befehl zum Signieren der *.xml*-Konfigurationsdatei mit der folgenden Syntax aus:
`xmlsigntool /version 1|2 <xml_file_path>`

Der Wert des Parameters `/version` hängt von Ihrer ESET Mail Security-Version ab. Verwenden Sie `/version 2` für ESET Mail Security 7 und neuere Versionen.

5. Geben Sie das Passwort für die erweiterten Einstellungen ein und bestätigen Sie es, wenn Sie vom XmlSignTool dazu aufgefordert werden. Ihre .xml.*xml*-Konfigurationsdatei ist jetzt signiert und kann in einer anderen Instanz von ESET Mail Security mit ESET CMD und der Passwortautorisierungsmethode importiert werden.

Befehl zum Signieren einer exportierten Konfigurationsdatei: `xmlsigntool /version 2 c:\config\settings.xml`



Wenn sich das Passwort für die erweiterten Einstellungen geändert hat und Sie eine Konfiguration importieren möchten, die mit dem alten Passwort signiert wurde, können Sie die *.xml*-Konfigurationsdatei mit Ihrem aktuellen Passwort erneut signieren. Auf diese Weise können Sie eine ältere Konfigurationsdatei wiederverwenden, ohne sie vor dem Importieren auf einem anderen Computer mit ESET Mail Security erneut zu exportieren.

ESET RMM

Remote Monitoring and Management (RMM) bezieht sich auf die Überwachung und Kontrolle von Softwaresystemen (auf Desktops, Servern und Mobilgeräten) durch einen lokal installierten Agent, auf den über einen Verwaltungs-Dienstanbieter zugegriffen wird.

RMM aktivieren

Befehl zum Aktivieren von Remoteüberwachung und Verwaltung. Sie benötigen Administratorberechtigungen, um das RMM-Hilfsprogramm verwenden zu können.

Arbeitsmodus

Wählen Sie den RMM-Arbeitsmodus im Dropdownmenü aus.

- **Nur sichere Trennung** - Wenn Sie die RMM-Schnittstelle für sichere und schreibgeschützte Vorgänge aktivieren möchten
- **Alle Vorgänge** - Wenn Sie die RMM-Schnittstelle für alle Vorgänge aktivieren möchten

Autorisierungsmethode

Wählen Sie die RMM-Autorisierungsmethode im Dropdownmenü aus:

- **Keine** - Anwendungspfade werden nicht überprüft, Sie können ermm.exe mit beliebigen Anwendungen

ausführen.

- **Anwendungspfad** - Geben Sie einen Anwendungspfad an, mit dem ermm.exe ausgeführt werden darf.

Die ESET Mail Security installation umfasst die Datei *ermm.exe* unter ESET Mail Security (Standardpfad: *c:\Program Files\ESET\ESET Mail Security*). *ermm.exe* tauscht Daten mit dem RMM-Plug-In aus, das mit dem RMM-Agent kommuniziert, der wiederum mit einem RMM-Server verbunden ist.

- *ermm.exe* - Ein von ESET entwickeltes Befehlszeilenhilfsprogramm zur Verwaltung von Endpoint-Produkten und für die Kommunikation ohne RMM-Plug-In.

- RMM-Plug-In - Eine externe Anwendung, die lokal auf dem Endpunkt-Windows-System ausgeführt wird. Das Plug-In wurde entwickelt, um mit einem bestimmten RMM-Agent (z. B. nur Kaseya) und mit *ermm.exe* zu kommunizieren.

- RMM-Agent - Eine externe Anwendung (z. B. von Kaseya), die lokal auf dem Endpunkt-Windows-System ausgeführt wird. Der Agent kommuniziert mit dem RMM-Plug-In und mit dem RMM-Server.

- RMM-Server - Wird als Dienst auf einem externen Server ausgeführt. Unterstützte RMM-Systeme sind von Kaseya, Labtech, Autotask, Max Focus und Solarwinds N-able verfügbar.

In unserem Knowledgebase-Artikel finden Sie weitere Informationen zu ESET RMM in ESET Mail Security.

ESET Direct Endpoint Management-Plugins für RMM-Lösungen von Drittanbietern

Der RMM-Server wird als Dienst auf einem Drittanbieterserver gestartet. Weitere Informationen finden Sie in den folgenden Online-Anleitungen für ESET Direct Endpoint Management:

- ESET Direct Endpoint Management-Plugin für die ConnectWise-Automatisierung
- ESET Direct Endpoint Management-Plugin für DattoRMM
- ESET Direct Endpoint Management für SolarWinds N-Central
- ESET Direct Endpoint Management für NinjaRMM

Lizenz

ESET Mail Security verbindet sich mehrmals pro Stunde mit dem ESET-Lizenzserver, um Prüfungen auszuführen. Der Parameter **Intervallprüfung** ist standardmäßig auf **Automatisch** festgelegt. Wenn Sie den Netzwerkdatenverkehr für Lizenzprüfungen reduzieren möchten, ändern Sie die Intervallprüfung zu **eingeschränkt**, und die Lizenzprüfung wird nur noch einmal pro Tag (und nach Serverneustarts) ausgeführt.

Wenn die Intervallprüfung auf **Eingeschränkt** festgelegt ist, werden lizenzbezogene Änderungen an ESET Mail Security via ESET Business Account und am ESET MSP Administrator möglicherweise erst nach bis zu einem Tag übernommen.

WMI-Anbieter

Windows Management Instrumentation (WMI) ist die Microsoft-Implementierung von Web-Based Enterprise Management (WBEM), einer Brancheninitiave zur Entwicklung einer Standardtechnologie für den Zugriff auf

Verwaltungsinformationen in einer Unternehmensumgebung.

Weitere Informationen zu WMI finden Sie bei
http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642(v=vs.85).aspx

ESET WMI-Anbieter

Mit dem ESET WMI-Anbieter können Sie ESET-Produkte in einem Unternehmensnetzwerk ohne ESET-spezifische Software oder Tools remote überwachen. Die Bereitstellung von grundlegenden Produktinformationen, Statusinformationen und Statistiken über WMI bietet Administratoren umfangreiche neue Möglichkeiten bei der Überwachung von ESET-Produkten.

Administratoren können die zahlreichen von WMI gebotenen Zugriffsmethoden nutzen (Befehlszeile, Skripte und Überwachungstools von Drittanbietern), um den Status ihrer ESET-Produkte zu überwachen.

In der aktuellen Bereitstellung steht ein Lesezugriff auf die grundlegenden Produktinformationen, auf Informationen zu installierten Funktionen und deren Schutzstatus, auf Statistiken einzelner Scan-Module und auf Produkt-Log-Dateien zur Verfügung.

Mit dem WMI-Anbieter können Sie Sie die Windows WMI-Standardinfrastruktur und -Tools verwenden, um den Status von Produkt und Produkt-Logs auszulesen.

Bereitgestellte Daten

Alle WMI-Klassen in Bezug auf das ESET-Produkt befinden sich im Namespace „root\ESET“. Folgende Klassen sind derzeit implementiert und werden nachfolgend ausführlich beschrieben:

Allgemein

- ESET_Product
- ESET_Features
- ESET_Statistics

Logs

- ESET_ThreatLog
- ESET_EventLog
- ESET_ODFileScanLogs
- ESET_ODFileScanLogRecords
- ESET_ODServerScanLogs
- ESET_ODServerScanLogRecords
- ESET_HIPSLog
- ESET_URLLog

- ESET_DevCtrlLog
- ESET_GreylistLog
- ESET_MailServeg
- ESET_HyperVScanLogs
- ESET_HyperVScanLogRecords

ESET_Product-Klasse

Es darf nur eine Instanz der ESET_Product-Klasse vorhanden sein. Die Eigenschaften dieser Klasse beziehen sich auf grundlegende Informationen zum installierten ESET-Produkt:

- ID - Produkttyp-ID, zum Beispiel „esml“
- Name - Produktbezeichnung, zum Beispiel „ESET Mail Security“
- FullName - Vollständiger Name des Produkts, zum Beispiel „ESET Mail Security for IBM Domino“
- Version - Produktversion, zum Beispiel „6.5.14003.0“
- VirusDBVersion - Version der Signaturdatenbank, zum Beispiel „14533 (20161201)“
- VirusDBLastUpdate - Zeitstempel des letzten Update der Signaturdatenbank. Die Zeichenkette enthält den Zeitstempel im WMI-Format für Datum und Uhrzeit, zum Beispiel „20161201095245.000000+060“.
- LicenseExpiration - Lizenzablaufzeitpunkt. Die Zeichenkette enthält den Zeitstempel im WMI-Format
- KernelRunning - Boolescher Wert, der angibt, ob der ekrn-Dienst auf dem Computer ausgeführt wird, zum Beispiel „TRUE“
- StatusCode - Zahl, die den Schutzstatus des Produkts angibt: 0 - grün (OK), 1 - gelb (Warnung), 2 - rot (Fehler)
- StatusText - Beschreibung der Ursache, falls der Statuscode nicht null ist (andernfalls ist dieser Text leer)

ESET_Features-Klasse

Je nach Anzahl der Produktfunktionen hat die ESET_Features-Klasse mehrere Instanzen. Jede Instanz enthält Folgendes:

- Name - Name der Funktion (eine Liste der Namen finden Sie unten)
- Status - Status der Funktion: 0 - inaktiv, 1 - deaktiviert, 2 - aktiviert

Liste der Zeichenfolgen für aktuell erkannte Produktfunktionen:

- CLIENT_FILE_AV - Virenschutz des Echtzeit-Dateischutzes
- CLIENT_WEB_AV - Virenschutz für den Webzugriff des Client
- CLIENT_DOC_AV - Virenschutz für Dokumente auf dem Client

- CLIENT_NET_FW - Personal Firewall des Clients
- CLIENT_EMAIL_AV - Virenschutz für E-Mail-Programm auf dem Client
- CLIENT_EMAIL_AS - Spam-Schutz für E-Mail-Programm auf dem Client
- SERVER_FILE_AV - Echtzeit-Dateischutz für das geschützte Dateiserverprodukt, zum Beispiel Dateien in der SharePoint-Inhaltsdatenbank im Fall von ESET Mail Security
- SERVER_EMAIL_AV - Virenschutz für E-Mails auf dem geschützten Serverprodukt, zum Beispiel E-Mails in Microsoft Exchange oder IBM Domino
- SERVER_EMAIL_AS - Spam-Schutz für E-Mails auf dem geschützten Serverprodukt, zum Beispiel E-Mails in Microsoft Exchange oder IBM Domino
- SERVER_GATEWAY_AV - Virenschutz für geschützte Netzwerkprotokolle auf dem Gateway
- SERVER_GATEWAY_AS - Spam-Schutz für geschützte Netzwerkprotokolle auf dem Gateway

ESET_Statistics-Klasse

Je nach Anzahl der Scanner des Produkts hat die ESET_Statistics-Klasse mehrere Instanzen. Jede Instanz enthält Folgendes:

- Scanner – Zeichenkettencode für den jeweiligen Scanner, zum Beispiel „CLIENT_FILE“
- Total - Gesamtzahl der gescannten Dateien
- Infected - Anzahl der gefundenen infizierten Dateien
- Cleaned - Anzahl der gesäuberten Dateien
- Timestamp - Zeitstempel der letzten Änderung dieser Statistik. Im WMI-Format für Datum und Uhrzeit, zum Beispiel „20130118115511.000000+060”
- ResetTime - Zeitstempel des letzten Zurücksetzens des Statistikzählers. Im WMI-Format für Datum und Uhrzeit, zum Beispiel „20130118115511.000000+060”

Liste der Zeichenketten der derzeit erkannten Scanner:

- CLIENT_FILE
- CLIENT_EMAIL
- CLIENT_WEB
- SERVER_FILE
- SERVER_EMAIL
- SERVER_WEB

ESET_ThreatLog-Klasse

Die ESET_ThreatLog-Klasse hat mehrere Instanzen. Jede Instanz stellt einen Log-Eintrag aus dem Log „Erkannte Bedrohungen“ dar. Jede Instanz enthält Folgendes:

- ID - eindeutige ID dieses Prüflog-Eintrags
- Timestamp - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- LogLevel - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung
- Scanner - Name des Scanners, der den Log-Eintrag erstellt hat
- ObjectType - Art des Objekts, das das Log-Ereignis ausgelöst hat
- ObjectName - Name des Objekts, das das Log-Ereignis ausgelöst hat
- Threat - Name der Bedrohung, die im Objekt mit den Eigenschaften „ObjectName“ und „ObjectType“ gefunden wurde
- Action - Aktion, die nach der Identifizierung der Bedrohung ausgeführt wurde
- User - Benutzerkonto, unter dem das Log-Ereignis erzeugt wurde
- Information - zusätzliche Beschreibung des Ereignisses
- Hash - Hash des Objekts, das das Log-Ereignis ausgelöst hat

ESET_EventLog

Die ESET_EventLog-Klasse hat mehrere Instanzen. Jede Instanz stellt einen Log-Eintrag aus dem Log „Ereignisse“ dar. Jede Instanz enthält Folgendes:

- ID - eindeutige ID dieses Prüflog-Eintrags
- Timestamp - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- LogLevel - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung
- Module - Name des Moduls, das den Log-Eintrag erstellt hat
- Event - Beschreibung des Ereignisses
- User - Benutzerkonto, unter dem das Log-Ereignis erzeugt wurde

ESET_ODFileScanLogs

Die ESET_ODFileScanLogs-Klasse hat mehrere Instanzen. Jede stellt einen Eintrag des On-Demand-Datei-Scans dar. Dies entspricht der Log-Liste „On-Demand-Scan“ in der Benutzeroberfläche. Jede Instanz enthält Folgendes:

- ID - eindeutige ID dieses Prüflog-Eintrags

- Timestamp - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- Targets - Zielordner/-objekte für die Prüfung
- TotalScanned - Gesamtzahl der geprüften Objekte
- Infected - Anzahl der gefundenen infizierten Objekte
- Cleaned - Anzahl der gesäuberten Objekte
- Status - Status des Scan-Vorgangs

ESET_ODFileScanLogRecords

Die ESET_ODFileScanLogRecords-Klasse hat mehrere Instanzen. Jede stellt einen Log-Eintrag in einem der Prüflogs dar, die jeweils einer Instanz der ESET_ODFileScanLogs-Klasse entsprechen. Die Instanzen dieser Klasse entsprechen den Log-Einträgen aller On-Demand-Scans/-Logs. Wenn nur die Instanz eines bestimmten Prüflogs benötigt wird, können Sie die Elemente über die Eigenschaft „LogID“ filtern. Jede Klasse enthält Folgendes:

- LogID - ID des Prüflogs, zu dem der Eintrag gehört (ID einer der Instanzen der ESET_ODFileScanLogs-Klasse)
- ID - eindeutige ID dieses Prüflog-Eintrags
- Timestamp - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- LogLevel - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung
- Log - die eigentliche Log-Meldung

ESET_ODServerScanLogs

Die ESET_ODServerScanLogs-Klasse hat mehrere Instanzen. Jede stellt einen ausgeführten Lauf des On-Demand-Server-Scans dar. Jede Instanz enthält Folgendes:

- ID - eindeutige ID dieses Prüflog-Eintrags
- Timestamp - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- Targets - Zielordner/-objekte für die Prüfung
- TotalScanned - Gesamtzahl der geprüften Objekte
- Infected - Anzahl der gefundenen infizierten Objekte
- Cleaned - Anzahl der gesäuberten Objekte
- RuleHits - Gesamtzahl der Regeltreffer
- Status - Status des Scan-Vorgangs

ESET_ODServerScanLogRecords

Die ESET_ODServerScanLogRecords-Klasse hat mehrere Instanzen. Jede stellt einen Log-Eintrag in einem der Prüflogs dar, die jeweils einer Instanz der ESET_ODServerScanLogs-Klasse entsprechen. Die Instanzen dieser Klasse entsprechen den Log-Einträgen aller On-Demand-Scans/-Logs. Wenn nur die Instanz eines bestimmten Prüflogs benötigt wird, können Sie die Elemente über die Eigenschaft „LogID“ filtern. Jede Klasse enthält Folgendes:

- LogID - ID des Prüflogs, zu dem der Eintrag gehört (ID einer der Instanzen der ESET_ODServerScanLogs-Klasse)
- ID - eindeutige ID dieses Prüflog-Eintrags
- Timestamp - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- LogLevel - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung
- Log - die eigentliche Log-Meldung

ESET_SmtpProtectionLog

Die ESET_SmtpProtectionLog-Klasse hat mehrere Instanzen. Jede Instanz stellt einen Log-Eintrag aus dem „Smtp protection“-Log dar. Jede Instanz enthält Folgendes:

- ID - eindeutige ID dieses Prüflog-Eintrags
- Timestamp - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- LogLevel - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung
- HELODomain - Name der HELO-Domäne
- IP - Quell-IP-Adresse
- Sender - Absender der E-Mail
- Recipient - Empfänger der E-Mail
- Schutzart – Art des verwendeten Schutzes
- Action - ausgeführte Aktion
- Grund – Grund für Aktion
- TimeToAccept - Anzahl der Minuten, nach der die E-Mail akzeptiert wird

ESET_HIPSLog

Die ESET_HIPSLog-Klasse hat mehrere Instanzen. Jede Instanz stellt einen Log-Eintrag aus dem „HIPS“-Log dar. Jede Instanz enthält Folgendes:

- ID - eindeutige ID des Log-Eintrags

- Timestamp - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)

- LogLevel - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung

- Application - Quellanwendung

- Target - Art der Operation

- Action - Von HIPS ausgeführte Aktion, z. B. erlauben, verweigern usw.

- Rule - Name der Regel, die für die Aktion verantwortlich ist

- AdditionalInfo

ESET_URLLog

Die ESET_URLLog-Klasse hat mehrere Instanzen. Jede Instanz stellt einen Log-Eintrag aus dem Log „Gefilterte Websites“ dar. Jede Instanz enthält Folgendes:

- ID - eindeutige ID des Log-Eintrags

- Timestamp - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)

- LogLevel - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung

- URL - Die URL

- Status - Was ist mit der URL geschehen, z. B. „Gesperrt durch Web-Kontrolle“

- Application - Die Anwendung, die versucht hat, die URL zu öffnen

- User - Das Benutzerkonto, das die Anwendung ausgeführt hat

ESET_DevCtrlLog

Die ESET_DevCtrlLog-Klasse hat mehrere Instanzen. Jede Instanz stellt einen Log-Eintrag aus dem Log „Gerätesteuerung“ dar. Jede Instanz enthält Folgendes:

- ID - eindeutige ID des Log-Eintrags

- Timestamp - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)

- LogLevel - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung

- Device - Gerätename

- User - Name des Benutzerkontos

- UserSID - SID des Benutzerkontos
- Group - Name der Benutzergruppe
- GroupSID - SID der Benutzergruppe
- Status - Was ist mit dem Gerät passiert, z. B. „Schreibzugriff gesperrt“
- DeviceDetails - Zusätzliche Informationen zum Gerät
- EventDetails - Zusätzliche Informationen zum Ereignis

ESET_MailServerLog

Die ESET_MailServerLog-Klasse hat mehrere Instanzen. Jede Instanz stellt einen Log-Eintrag aus dem „E-Mail-Server“-Log dar. Jede Instanz enthält Folgendes:

- ID - eindeutige ID des Log-Eintrags
- Timestamp - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- LogLevel - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung
- IPAddr - Quell-IP-Adresse
- HELODomain - Name der HELO-Domäne
- Sender - Absender der E-Mail
- Recipient - Empfänger der E-Mail
- Subject - E-Mail-Betreff
- ProtectionType - Schutztyp, der die im aktuellen Logeintrag beschriebene Aktion ausgeführt hat, z. B. Malware-Schutz, Spam-Schutz oder Regeln.
- Action - ausgeführte Aktion
- Reason - Der Grund, aus dem die Aktion für den jeweiligen „ProtectionType“ auf dem Objekt ausgeführt wurde.

ESET_HyperVScanLogs

Die ESET_HyperVScanLogs-Klasse hat mehrere Instanzen. Jede stellt eine Ausführung des Hyper-V-Datei-Scans dar. Dies entspricht der Log-Liste „Hyper-V-Scan“ in der Benutzeroberfläche. Jede Instanz enthält Folgendes:

- ID - eindeutige ID des Log-Eintrags
- Timestamp - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- Targets - Zielcomputer/-laufwerke/-volumes für die Prüfung

- TotalScanned - Gesamtzahl der geprüften Objekte
- Infected - Anzahl der gefundenen infizierten Objekte
- Cleaned - Anzahl der gesäuberten Objekte
- Status - Status des Scan-Vorgangs

ESET_HyperVScanLogRecords

Die ESET_HyperVScanLogRecords-Klasse hat mehrere Instanzen. Jede stellt einen Log-Eintrag in einem der Scan-Logs dar, die jeweils einer Instanz der ESET_HyperVScanLogs-Klasse entsprechen. Die Instanzen dieser Klasse entsprechen den Log-Einträgen aller Hyper-V-Scans/-Logs. Wenn Sie nur die Instanz eines bestimmten Scan-Logs benötigen, können Sie die Elemente über die Eigenschaft „LogID“ filtern. Jede Klasse enthält Folgendes:

- LogID - ID des Scan-Logs, zu dem der Eintrag gehört (ID einer der Instanzen der ESET_HyperVScanLogs-Klasse)
- ID - eindeutige ID des Log-Eintrags
- Timestamp - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- LogLevel - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung
- Log - die eigentliche Log-Meldung

ESET_NetworkProtectionLog

Die ESET_NetworkProtectionLog-Klasse hat mehrere Instanzen. Jede Instanz stellt einen Log-Eintrag aus dem „Network protection“-Log dar. Jede Instanz enthält Folgendes:

- ID - eindeutige ID des Log-Eintrags
- Timestamp - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- LogLevel - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung
- Event – Ereignis, das die Netzwerkschutzaktion auslöst
- Action – vom Netzwerkschutz ausgeführte Aktion
- Source – Quelladresse des Netzwerkgeräts
- Target – Zieladresse des Netzwerkgeräts
- Protocol – Netzwerkkommunikationsprotokoll
- RuleOrWormName – Name der Regel oder des Wurms, die/der mit dem Ereignis verknüpft ist
- Application – Anwendung, die die Netzwerkkommunikation initiiert hat

- User - Benutzerkonto, unter dem das Log-Ereignis erzeugt wurde

ESET_SentFilesLog

Die ESET_SentFilesLog-Klasse hat mehrere Instanzen. Jede Instanz stellt einen Log-Eintrag aus dem „Sent files“-Log dar. Jede Instanz enthält Folgendes:

- ID - eindeutige ID des Log-Eintrags
- Timestamp - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- LogLevel - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung
- Sha1 – SHA-1-Hash der gesendeten Datei
- File – gesendete Datei
- Size – Größe der gesendeten Datei
- Category – Kategorie der gesendeten Datei
- Reason – Grund für das Senden der Datei
- SentTo – ESET-Abteilung, an die die Datei gesendet wurde
- User - Benutzerkonto, unter dem das Log-Ereignis erzeugt wurde

ESET_OneDriveScanLogs

Die ESET_OneDriveScanLogs-Klasse hat mehrere Instanzen. Jede stellt eine Ausführung des OneDrive-Scans dar. Dies entspricht der Log-Liste „OneDrive Scan“ in der Benutzeroberfläche. Jede Instanz enthält Folgendes:

- ID – eindeutige ID des OneDrive-Logs
- Timestamp - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- Targets - Zielordner/-objekte für die Prüfung
- TotalScanned - Gesamtzahl der geprüften Objekte
- Infected - Anzahl der gefundenen infizierten Objekte
- Cleaned - Anzahl der gesäuberten Objekte
- Status - Status des Scan-Vorgangs

ESET_OneDriveScanLogRecords

Die ESET_OneDriveScanLogRecords-Klasse hat mehrere Instanzen. Jede stellt einen Log-Eintrag in einem der Scan-Logs dar, die jeweils einer Instanz der ESET_OneDriveScanLogRecords-Klasse entsprechen. Die Instanzen dieser Klasse entsprechen den Log-Einträgen aller OneDrive-Scans/-Logs. Wenn nur die Instanz eines bestimmten Prüflogs benötigt wird, können Sie die Elemente über die Eigenschaft „LogID“ filtern. Jede Instanz enthält

Folgendes:

- LogID – ID des Scan-Logs, zu dem der Eintrag gehört (ID einer der Instanzen der ESET_OneDriveScanLogs-Klasse)
- ID – eindeutige ID des OneDrive-Logs
- Timestamp - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- LogLevel - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung
- Log - die eigentliche Log-Meldung

Zugriff auf die bereitgestellten Daten

Hier finden Sie einige Beispiele dazu, wie Sie über die Windows-Befehlszeile und PowerShell auf die ESET-WMI-Daten zugreifen können. Beide Methoden funktionieren in allen aktuellen Windows-Betriebssystemen. Beide Methoden funktionieren in allen aktuellen Windows-Betriebssystemen. Es stehen jedoch mit anderen Skriptsprachen und Tools zahlreiche weitere Möglichkeiten für den Zugriff auf die Daten zur Verfügung.

Befehlszeile ohne Skripts

Kommandozeile `wmic` können Sie auf verschiedene vordefinierte und beliebige benutzerdefinierte WMI-Klassen zugreifen.

So zeigen Sie die vollständigen Informationen zum Produkt auf dem lokalen Computer an:

```
wmic /namespace:\\root\ESET Path ESET_Product
```

So zeigen Sie nur die Produktversion des Produkts auf dem lokalen Computer an:

```
wmic /namespace:\\root\ESET Path ESET_Product Get Version
```

So zeigen Sie die vollständigen Informationen zum Produkt auf dem Remote-Computer mit der IP-Adresse 10.1.118.180 an:

```
wmic /namespace:\\root\ESET /node:10.1.118.180 /user:Administrator Path ESET_Product
```

PowerShell

So rufen Sie die vollständigen Informationen zum Produkt auf dem lokalen Computer ab und zeigen Sie an:

```
Get-WmiObject ESET_Product -namespace 'root\ESET'
```

So rufen Sie die vollständigen Informationen zum Produkt auf dem Remote-Computer mit der IP-Adresse 10.1.118.180 ab und zeigen Sie an:

```
$cred = Get-
Credential # promts the user for credentials and stores it in the variable
Get-WmiObject ESET_Product -namespace 'root\ESET' -computername '10.1.118.180' -
```

```
cred $cred
```

Scan-Ziele für die ESET Management-Konsole

Mit dieser Funktion kann ESET PROTECT das Scan-Ziel (On-Demand-Postfachdatenbank-Scan und Hyper-V-Scan) verwenden, wenn der Client-Task Server-Scan auf einem Server mit ESET Mail Security ausgeführt wird. Die Einstellung für ESET PROTECT-Scan-Ziele ist nur verfügbar, wenn der ESET Management Agent installiert ist. Andernfalls ist die Funktion deaktiviert.

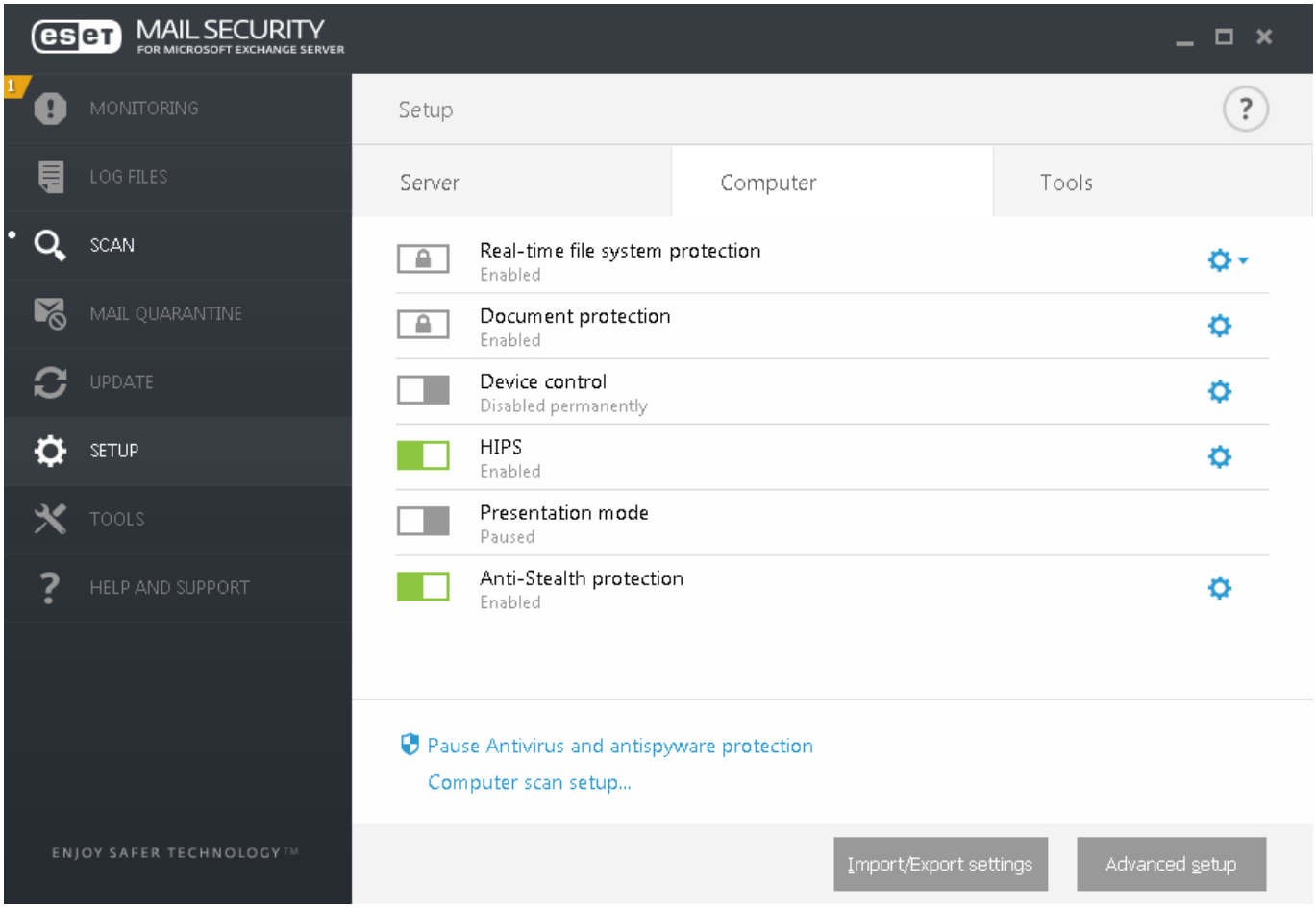
Mit der Funktion **Liste der Ziele generieren** erstellt ESET Mail Security eine Liste der aktuell verfügbaren Prüfziele. Diese Liste wird regelmäßig gemäß dem festgelegten **Updateintervall** generiert.

> Wenn Sie Option **Liste der Ziele generieren** zum ersten Mal aktivieren, braucht ESET PROTECT ca. die Hälfte des angegebenen **Updateintervalls** für die Erfassung. Bei einem **Updateintervall** von 60 Minuten braucht ESET PROTECT also ca. 30 Minuten, um die Liste der Prüfziele zu empfangen. Falls ESET PROTECT die Liste früher abrufen soll, können Sie ein kleineres Updateintervall festlegen. Sie können das Intervall später jederzeit verlängern.

Wenn ESET PROTECT den Clienttask **Server-Scan** ausführt, wird die Liste abgerufen, und Sie können die Scan-Ziele für die Hyper-V-Scan auf dem entsprechenden Server auswählen.

Override-Modus

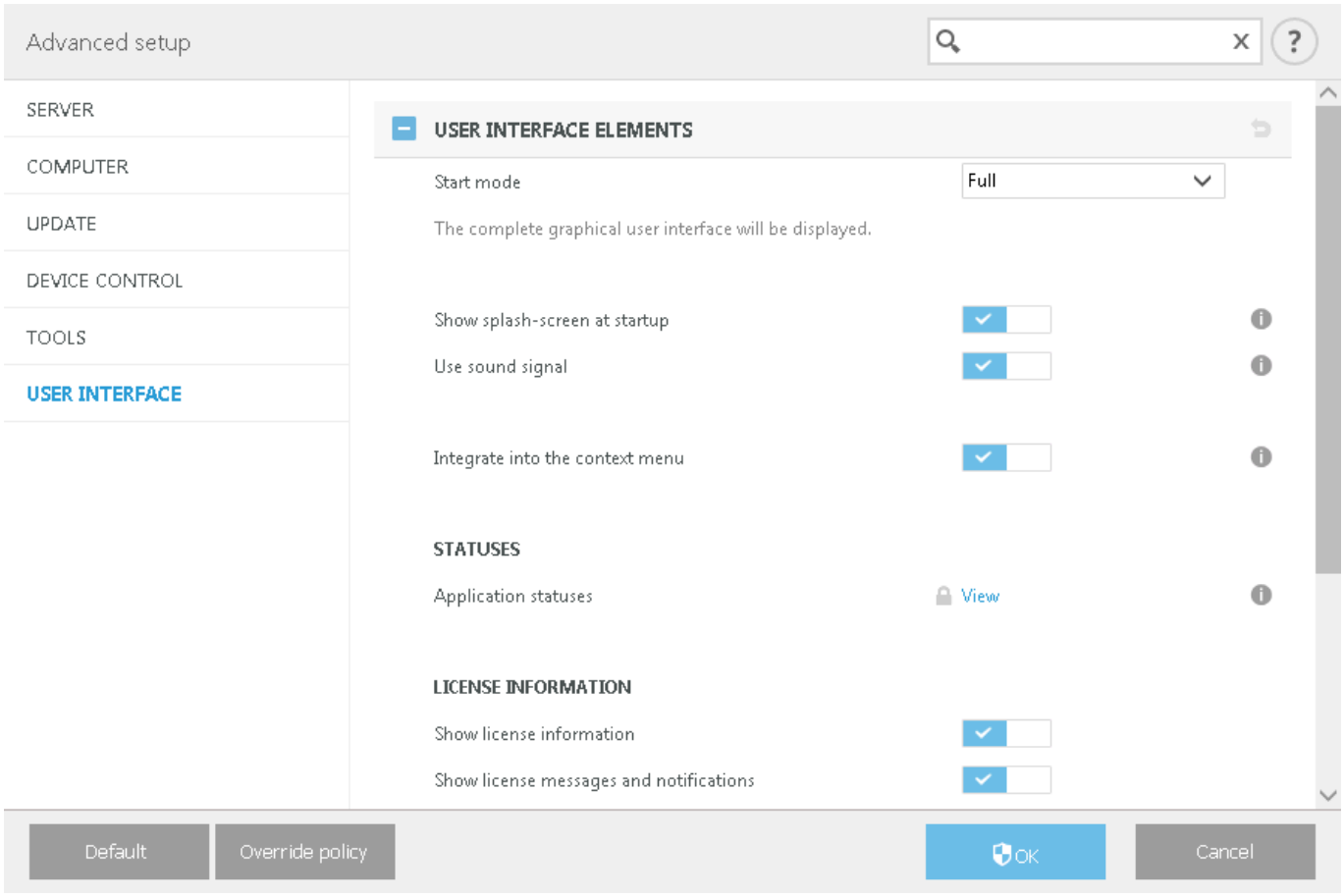
Wenn Sie die ESET PROTECT-Policy für ESET Mail Security anwenden, wird je ein Sperrsymbol  anstelle des Schalters zum Aktivieren und Deaktivieren in den Einstellungen und neben dem Schalter in den **Erweiterten Einstellungen** angezeigt.



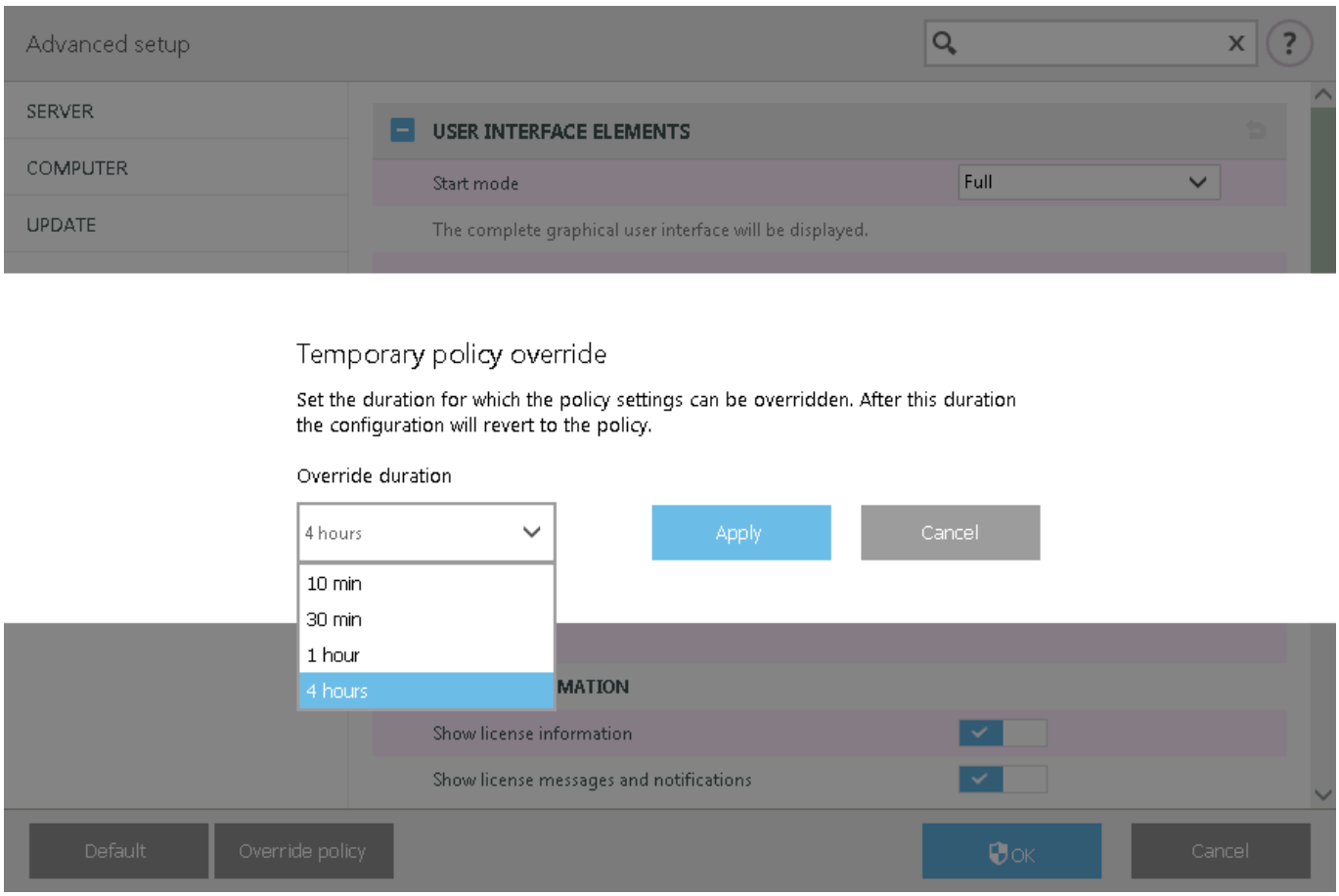
Einstellungen, die per ESET PROTECT-Policy konfiguriert wurden, können normalerweise nicht geändert werden. Mit dem Override-Modus können Sie diese Einstellungen vorübergehend außer Kraft setzen. Dazu müssen Sie jedoch den **Override-Modus** mit einer ESET PROTECT-Policy aktivieren.

Melden Sie sich bei der ESET PROTECT-Web-Konsole an, navigieren Sie zu **Policies**, und bearbeiten Sie entweder eine auf ESET Mail Security angewendete vorhandene Policy oder erstellen Sie eine neue Policy. Klicken Sie in den **Einstellungen** auf **Override-Modus**, aktivieren Sie den Modus, und konfigurieren Sie die restlichen Einstellungen inklusive des Authentifizierungstyps (Active Directory-Benutzer oder Passwort).

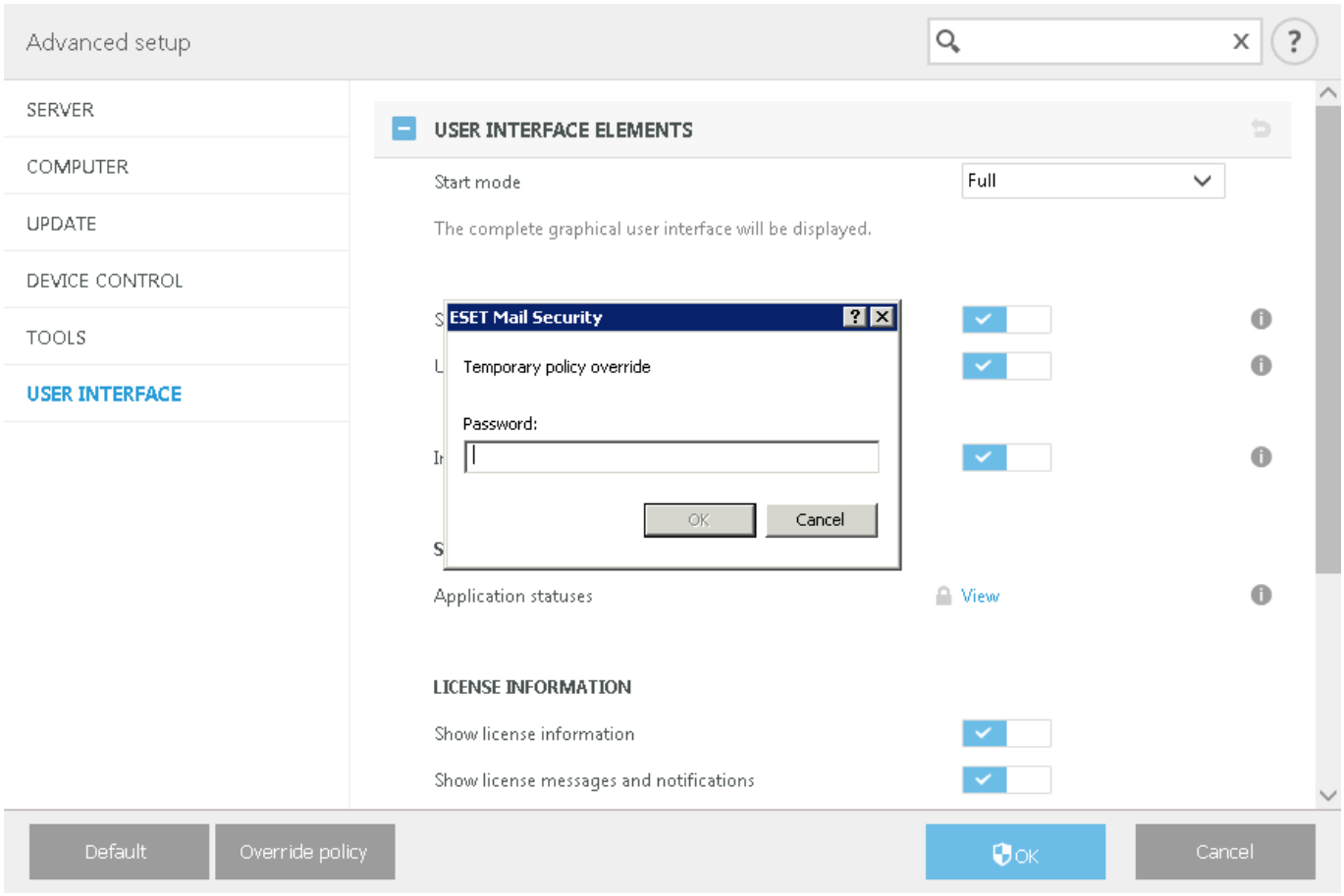
Nachdem Sie die Policy bearbeitet bzw. die neue Policy auf ESET Mail Security angewendet haben, wird die Schaltfläche Policy außer Kraft setzen im Fenster **Erweiterte Einstellungen** angezeigt.



Klicken Sie auf die Schaltfläche **Policy außer Kraft setzen**, legen Sie die Dauer fest und klicken Sie auf **Übernehmen**.



Falls Sie den Authentifizierungstyp **Passwort** ausgewählt haben, müssen Sie das Override-Passwort eingebe.



Nach Ablauf des Override-Modus werden alle vorgenommenen Konfigurationsänderungen wieder auf die ESET PROTECT-Policyeinstellungen zurückgesetzt. Vor dem Ablauf des Override-Modus wird eine Benachrichtigung angezeigt.

Sie können den **Override-Modus** jederzeit auf der Überwachungsseite oder in den Erweiterten Einstellungen vorzeitig beenden.

Log-Dateien

In diesem Bereich können Sie die Logging-Konfiguration von ESET Mail Security ändern.

Log-Datensätze

Alle Einträge werden in das Ereignis-Log (*C:\ProgramData\ESET\ESET Security\Logs*) geschrieben und können mit dem Anzeigeprogramm für Log-Dateien geöffnet werden. Mit den Schaltern können Sie einzelne Features aktivieren bzw. deaktivieren:
Mail-Transportfehler loggen
Wenn diese Option aktiviert ist und ein Problem auf der E-Mail-Transportebene auftritt, wird eine Fehlermeldung in das Ereignis-Log geschrieben.
Mail-Transportausnahmen loggen
Wenn Ausnahmefehler auf der E-Mail-Transportebene auftreten, werden die entsprechenden Details in das Ereignis-Log geschrieben.

Loggingfilter

Produziert eine große Menge an Daten, da standardmäßig alle Loggingoptionen aktiviert werden. Deaktivieren Sie nach Möglichkeit das Logging für die Komponenten, die für Ihr Problem nicht relevant sind.

Um das allgemeine Logging zu aktivieren, müssen Sie die **Diagnose-Logs** im Hauptmenü unter **Einstellungen** > Tools aktivieren. Nachdem Sie die Loggingfunktion aktiviert haben, sammelt ESET Mail Security ausführliche Logs, je nachdem, welche Funktionen in diesem Bereich aktiviert sind.

Mit den Schaltern können Sie einzelne Features aktivieren oder deaktivieren. Diese möglichen Kombinationen für diese Optionen hängen von der Verfügbarkeit einzelner Komponenten in ESET Mail Security ab.

• Diagnose-Logging für den Mail-Transport

Wenn Sie Probleme mit dem Datenbank-Scan im normalen Betrieb beheben, sollten Sie das **Diagnose-Logging für den Mail-Transport** nach Möglichkeit deaktivieren. Andernfalls kann es passieren, dass das resultierende Log stark anwächst und schwer zu analysieren ist.

- **Diagnose-Logging für On-Demand-Datenbankprüfung** - Schreibt ausführliche Informationen in die Logs, insbesondere für die Problembehandlung.
- **Cluster-Diagnose-Logging** - Das Cluster-Logging ist in den allgemeinen Diagnose-Logs enthalten.
- **OneDrive-Diagnose-Logging** – Das OneDrive-Logging ist in den allgemeinen Diagnose-Logs enthalten.
- **Diagnose-Logging für das Spam-Schutz-Modul** - Wenn Sie einen Fehler beheben müssen, werden ausführliche Informationen zum Spam-Schutz-Modul in den Logs angezeigt. Schreibt ausführliche Informationen über das Spamschutzmodul zu Diagnosezwecken in die Log-Datei. Das Spamschutzmodul schreibt nicht in das Ereignis-Log (Datei warnlog.dat) und ist daher nicht im Anzeigeprogramm für Log-Dateien sichtbar. Dieses Modul schreibt seine Einträge direkt in eine spezielle Textdatei (z. B. C:\ProgramData\ESET\ESET Mail Security\Logs\antispam.0.log), um alle Diagnosedaten für das Spamschutzmodul an einem zentralen Ort zu sammeln. Auf diese Weise wird die Leistung von ESET Mail Security auch bei einem starken Anstieg des E-Mail-Verkehrs nicht beeinträchtigt.

Log-Dateien

Hier können Sie Einstellungen für Logs festlegen. Diese Einstellungen sind wichtig, um zu verhindern, dass die Festplatte vollgeschrieben wird. Mit den Standardeinstellungen werden ältere Logs automatisch gelöscht, um Platz auf der Festplatte zu sparen.

Einträge automatisch löschen

Log-Einträge, die älter sind als die angegebene Anzahl an Tagen (unter), werden automatisch gelöscht.

Einträge löschen, die älter sind als (Tage)

Geben Sie die Anzahl der Tage ein.

Bei Überschreitung der Log-Größe automatisch alte Einträge löschen

Wenn die Log-Größe **Max Log-Größe [MB]** überschreitet, werden alte Log-Einträge gelöscht, bis die **Reduzierte Log-Größe [MB]** erreicht ist.

Automatisch gelöschte Einträge sichern

Automatisch gelöschte Log-Einträge und -Dateien werden im angegebenen Verzeichnis gesichert und optional als ZIP-Datei komprimiert.

Diagnose-Logs sichern

Automatisch gelöschte Diagnose-Logs werden gesichert. Wenn diese Option nicht aktiviert ist, werden die Einträge der Diagnose-Logs nicht gesichert.

Sicherungsordner

Ordner, in dem die Log-Sicherungen gespeichert werden. Sie können festlegen, dass die Log-Sicherungen als ZIP-Datei komprimiert werden sollen.

Log-Dateien automatisch optimieren

Diese Option defragmentiert die Log-Dateien automatisch, wenn die Fragmentierung höher ist als der unter **Wenn ungenutzte Einträge größer als (%)** angegebene Wert. Klicken Sie zum Defragmentieren der Log-Dateien auf **Optimieren**. Bei diesem Prozess werden alle leeren Log-Einträge gelöscht, wodurch Leistung und Log-Verarbeitung verbessert werden. Eine starke Verbesserung ist insbesondere dann erkennbar, wenn die Logs eine große Anzahl an Einträgen enthalten.

Textprotokoll aktivieren

Diese Option aktiviert die Speicherung von Logs in einem anderen, von den Log-Dateien getrennten Format:

- **Zielverzeichnis** - Das Verzeichnis, in dem Log-Dateien gespeichert werden (nur für **Text**/**CSV**). Jeder Log-Bereich verfügt über eine eigene Datei mit einem vordefinierten Dateinamen (z. B. *virlog.txt* für den Bereich Erkannte Bedrohungen in Log-Dateien, wenn Logs im Nur-Text-Format gespeichert werden).
- **Typ** - Mit dem Dateiformat **Text** werden Logs in einer Textdatei gespeichert, wobei die Daten durch Tabulatorzeichen getrennt werden. Dasselbe gilt für das kommagetrennte Dateiformat **CSV**. Mit der Option **Ereignis** werden die Logs im Windows-Ereignis-Log anstatt in einer Datei gespeichert (dieses kann in der Ereignisanzeige in der Systemsteuerung eingesehen werden).
- **Alle Log-Dateien löschen** – Löscht alle im Dropdownmenü **Typ** ausgewählten Logs.

> Um ein Problem schneller beheben zu können, werden Sie vom ESET-Support möglicherweise gebeten, Logs von Ihrem Computer bereitzustellen. Mit dem ESET Log Collector können Sie die benötigten Informationen ganz einfach sammeln. Weitere Informationen zum ESET Log Collector finden Sie in unserem Knowledgebase-Artikel .

Auditlog

Überwacht Änderungen an der Konfiguration und den Schutzfunktionen von. Da Änderungen an der Produktkonfiguration dramatische Auswirkungen auf die Funktionsweise des Produkts haben können, ist es hilfreich, die Änderungen zu Auditingzwecken nachzuverfolgen. Sie finden das Änderungs-Log im Abschnitt **Log-Dateien** > Audit-Log.

Log exportieren

In Windows-Anwendungs- und -Dienst-Logs exportieren
Dupliziert die Einträge aus dem E-Mail-Server-Schutz-Log in die Anwendungs- und Dienst-Logs. Um das E-Mail-Server-Schutz-Log anzuzeigen, öffnen Sie die Windows-**Ereignisanzeige** und navigieren Sie zu **Anwendungs- und Dienstprotokolle** > **ESET** > **Sicherheit** > **ExchangeServer** > **MailProtection**. Die Anwendungs- und Dienst-Logs werden unter Microsoft Windows Server 2012 und neueren Versionen unterstützt.
In Syslog-Server exportieren
Sie können die E-Mail-Server-Schutz-Log im Common Event Format (CEF) an einen Syslog-Server duplizieren. CEF ist ein standardisiertes, textbasiertes und erweiterbares Format, das die Datenerfassung und -Aggregation zur späteren Analyse in einem Enterprise-Management-System vereinfacht. In diesem Fall können Sie die Lösung zusammen mit Systemen für Security Information and Event Management (SIEM) und Log-Management wie etwa Micro Focus ArcSight verwenden. Unter Syslog-Ereigniszuordnung finden Sie Details und Beschreibungen zu den exportierten Ereignisfeldern.
Serveradresse
Geben Sie die IP-Adresse oder den Hostnamen des Servers ein. Falls Sie ArcSight verwenden, geben Sie einen Server mit installiertem SmartConnector an.
Protokoll
Wählen Sie das Protokoll aus, das Sie verwenden möchten: TCP oder UDP.
Port
Der Standardwert ist 514 für beide Protokolle.
In Datei exportieren
Die Logs können lokal in eine Datei im CEF-Format exportiert werden. Die Speicherkapazität für Logs ist begrenzt, daher werden die Logs rotiert. Einträge werden sequenziell in die Dateien geschrieben (von `mailserver.0.log` bis `mailserver.9.log`). Die neuesten Einträge werden in `mailserver.0.log` gespeichert und wenn diese Datei das Größenlimit erreicht, wird die älteste Datei (`mailserver.9.log`) gelöscht, und die restlichen Log-Dateien werden nacheinander umbenannt (`mailserver.0.log` wird zu `mailserver.1.log` umbenannt usw.).
Dateipfad
Als Standardpfad wird „C:\ProgramData\ESET\ESET Security\Logs“ verwendet. Sie können diesen Speicherort bei Bedarf ändern.

Syslog-Ereigniszuordnung

Die folgenden Tabellen enthalten die Zuordnung zwischen Ereignissen in ESET Mail Security und den ArcSight-Datenfeldern. Verwenden Sie diese Tabellen als Referenz für die Daten, die über den SmartConnector an ArcSight übermittelt werden.

Header		
Device Vendor	"ESET"	
Device Product	"EMSX"	"EMSX" or "ESET Mail Security for MS Exchange Server"
Device Version	e.g. "7.1.10005.0"	
Device Event Class ID	e.g. "101"	Device Event Category unique identifier: 100-199 malware 200-299 phish 300-399 spam 400-499 policy
Event Name	e.g. "MailScanResult: malware"	A brief description of what happened in the event: MailScanResult: malware MailScanResult: phishing link MailScanResult: spam MailScanResult: policy

CEF Key Name	CEF Key Full Name (Size)	Field Description	Detailed Field Description
rt	deviceReceiptTime	Time event was generated	The time at which the event was generated, in milliseconds since Jan 1st 1970
src	sourceAddress	Sender's IP	IP address of the sending mail server
shost	sourceHostName (1023)	Sender's HELO domain	HELO domain of the sending mail server
flexString1	flexString1	Message-ID	Message-ID header from the email
dhost	destinationHostName (1023)	Receiving server	Hostname of the machine that received the communication
msg	message (1023)	Message subject	Subject of the message, from the RFC5233 header "Subject:"
suser	sourceUserName (1023)	SMTP sender	SMTP sender of the email (MAIL FROM)
duser	destinationUserName (1023)	SMTP recipient(s)	SMTP recipient(s) of the email (RCPT TO)
act	deviceAction (63)	Action taken	Action taken (cleaned, quarantined, etc.)
cat	deviceEventCategory (1023)	Detection category	Most significant detection (malware >> phish >> spam >> SPF/DKIM >> policy)
sourceServiceName	sourceServiceName	Type of protection	SMTP Transport agent, On-demand database scan
deviceExternalId	deviceExternalId	Engine version	Anti-Malware engine version, Antispam engine version, e.g. "18620,7730"
cs1	deviceCustomString1	Anti-Malware result	Result of Anti-Malware scan, including threat name
cs1Label	deviceCustomString1Label	"Anti-Malware result"	
cs2	deviceCustomString2	Antispam result	Result of Antispam scan, including reason for marking as spam
cs2Label	deviceCustomString2Label	"Antispam result"	
cs3	deviceCustomString3	Anti-Phishing result	Result of Anti-Phishing scan, including detected URL
cs3Label	deviceCustomString3Label	"Anti-Phishing result"	
cs4	deviceCustomString4	SPF/DKIM/DMARC result	Result of SPF/DKIM/DMARC check, in RFC7601 format
cs4Label	deviceCustomString4Label	"SPF/DKIM/DMARC result"	
cs5	deviceCustomString5	"From:" sender	Sender address from RFC5322 header "From:"
cs5Label	deviceCustomString5Label	"From header"	
cs6	deviceCustomString6	"To:" and "Cc:" recipients	Recipients addresses from RFC5322 headers "To:" and "Cc:"
cs6Label	deviceCustomString6Label	"To and Cc headers"	
fname	filename (1023)	Attachment name	Name of the first detected attachment

CEF Key Name	CEF Key Full Name (Size)	Field Description	Detailed Field Description
fileHash	fileHash (255)	Attachment hash	Hash of the first detected attachment
fsize	fileSize	Attachment size	Size of the first detected attachment
reason	reason (1023)	Rule/policy activated	Name of the policy triggered by the email or it's content
ESETEMSXFileDetails	ESETEMSXFileDetails	File details	Information about all detected attachments, their names, hashes and sizes

Optional

CEF Key Name	CEF Key Full Name (Size)	Field Description	Detailed Field Description
end	endTime	Time event has ended	The time at which the activity ended, in milliseconds since Jan 1st 1970. Useful only if sand boxing technology is used ESET LiveGuard Advanced.
dtz	deviceTimeZone (255)	Timezone of the server	
request	requestURL	Detected URL	Malign or blacklisted URL extracted from mail body or mail headers. ESET Mail Security does not provide single URL in logs due to the fact that multiple URL's can be detected in email messages by various detection components.

Proxyserver

In großen lokalen Netzwerken wird die Verbindung zum Internet häufig über Proxyserver vermittelt. Wenn dies der Fall ist, müssen die nachfolgend beschriebenen Einstellungen vorgenommen werden. Andernfalls ist es unter Umständen nicht möglich, Updates automatisch über das Internet zu beziehen. Die Proxyserver-Einstellungen in ESET Mail Security können in zwei verschiedenen Bereichen der **erweiterten Einstellungen** (**F5**) konfiguriert werden:

1. **Erweiterte Einstellungen** (F5) > **Update** > **Profile** > **Updates** > **Verbindungsoptionen** > HTTP-Proxy. Diese Einstellung gilt für das entsprechende Update-Profil und wird für Laptops empfohlen, da diese die Updates der Signaturdatenbank oft aus verschiedenen Quellen beziehen.

2. **Erweiterte Einstellungen** (F5) > **Tools** > **Proxyserver**. Auf dieser Ebene können Sie die globalen Proxyservereinstellungen für alle Funktionen von ESET Mail Security festlegen. Diese Parameter werden von allen Modulen verwendet, die sich mit dem Internet verbinden.

Um die Proxyserver-Einstellungen für diese Ebene festzulegen, aktivieren Sie das Kontrollkästchen **Proxyserver verwenden** und geben im Feld **Proxyserver** die entsprechende Adresse zusammen mit dem **Port** des Proxyservers ein.

Proxyserver erfordert Authentifizierung

Falls für die Netzwerkkommunikation über den Proxyserver eine Authentifizierung erforderlich ist, aktivieren Sie diese Option und geben Sie **Benutzername** und **Passwort** an.

Proxyserver automatisch erkennen

Klicken Sie auf **Erkennen**, wenn die Einstellungen des Proxyservers automatisch erkannt und ausgefüllt werden sollen. Die in Internet Explorer festgelegten Einstellungen werden kopiert.

> Diese Funktion ruft keine Anmeldedaten (Benutzername und Passwort) ab; Sie müssen diese Informationen selbst eingeben.

Direktverbindung verwenden, wenn der Proxy nicht verfügbar ist

Wenn in der Produktkonfiguration die Nutzung eines HTTP-Proxys vorgesehen ist und der Proxy nicht erreichbar ist, umgeht das Produkt den Proxy und kommuniziert direkt mit ESET-Servern.

Präsentationsmodus

Der Präsentationsmodus ist eine Funktion für Benutzer, die ihre Software ununterbrochen nutzen, nicht durch Popup-Fenster gestört werden und die CPU-Auslastung reduzieren möchten. Der Präsentationsmodus kann auch für Präsentationen verwendet werden, die nicht durch Aktivitäten von ESET Mail Security unterbrochen werden dürfen. Wenn er aktiviert ist, werden alle Benachrichtigungsfenster deaktiviert und geplante Tasks werden nicht ausgeführt. Der Systemschutz läuft weiter im Hintergrund, aber es sind keine Eingaben durch den Benutzer erforderlich.

Präsentationsmodus automatisch aktivieren, wenn Anwendungen im Vollbildmodus ausgeführt werden

Der Präsentationsmodus wird automatisch aktiviert, wenn Sie eine Vollbildanwendung ausführen. Im Präsentationsmodus werden keine Benachrichtigungen oder Statusänderungen von ESET Mail Security angezeigt.

Präsentationsmodus automatisch deaktivieren nach

Mit dieser Option können Sie die Zeit in Minuten festlegen, nach der der Präsentationsmodus automatisch deaktiviert wird.

Diagnose

Mit der Diagnose können Speicherabbilddateien von ESET-Prozessen erstellt werden (z. B. *ekrn*). Im Falle eines Absturzes einer Anwendung wird eine Speicherabbilddatei erstellt. Diese hilft Entwicklern bei der Erkennung und Korrektur verschiedener ESET Mail Security Probleme.

Klicken Sie auf das Dropdownmenü neben **Typ des Speicherabbilds** und wählen Sie eine von drei Optionen aus:

- **Deaktivieren** – Deaktiviert diese Funktion.
- **Mini** – (Standardeinstellung) Protokolliert die kleinste Menge an Daten, die helfen könnten, die Ursache für den Absturz der Anwendung herauszufinden. Dieser Dumpdateityp ist eher zu empfehlen, wenn der Speicherplatz begrenzt ist. Da jedoch die enthaltene Datenmenge ebenfalls begrenzt ist, könnten Fehler, die nicht direkt von dem Thread ausgelöst wurden, der zum Absturzzeitpunkt ausgeführt wurde, bei einer Dateianalyse unentdeckt bleiben.
- **Vollständig** - Zeichnet den gesamten Inhalt des Arbeitsspeichers auf, wenn die Anwendung unerwartet beendet wird. Ein vollständiges Speicherabbild kann Daten von Prozessen enthalten, die ausgeführt wurden, als

das Speicherabbild geschrieben wurde.

Zielverzeichnis

Verzeichnis, in dem die Speicherabbilddatei während des Absturzes erstellt wird.

Diagnoseverzeichnis öffnen

Klicken Sie auf '**Öffnen**', um dieses Verzeichnis in einem neuen *Windows Explorer*-Fenster zu öffnen.

Diagnoseabbild erstellen

Klicken Sie auf **Erstellen**, um Diagnoseabbilder im Zielverzeichnis zu erstellen.

Erweitertes Logging

Erweitertes Logging für Computer-Scanner aktivieren – Erfasst alle Ereignisse, die beim Scannen von Dateien und Ordnern mit Computer-Scans oder mit dem Echtzeit-Dateischutz auftreten.
Erweitertes Logging für die Medienkontrolle aktivieren – Erfassen Sie alle in der Medienkontrolle aufgetretenen Ereignisse zu Diagnose- und Problembehebungszwecken.
Erweitertes Direct Cloud-Logging aktivieren – Erfassen Sie die gesamte Kommunikation zwischen dem Produkt und den Direct Cloud-Servern.
Erweitertes Logging für Dokumentenschutz aktivieren – Erfassen Sie alle im Dokumentenschutz aufgetretenen Ereignisse zu Diagnose- und Problembehebungszwecken.
Erweitertes Kernel-Logging aktivieren – Erfassen Sie alle im ESET-Kerneldienst (ekrn) aufgetretenen Ereignisse zu Diagnose- und Problembehebungszwecken.
Erweitertes Logging für Lizenzierung aktivieren – Gesamte Produktkommunikation mit dem Lizenzserver aufzeichnen.
Speicherablaufverfolgung aktivieren – Erfassen Sie alle Ereignisse, um den Entwicklern bei der Diagnose von Speicherlecks zu helfen.
Erweitertes Logging für den Netzwerkschutz aktivieren – Erfasst alle Daten, die den Netzwerkschutz durchlaufen, im PCAP-Format, um den Entwicklern bei der Diagnose und Behebung von Problemen im Zusammenhang mit dem Netzwerkschutz zu helfen.
Betriebssystem-Logging aktivieren – Zusätzliche Informationen zum Betriebssystem wie ausgeführte Prozesse, CPU-Aktivität und Laufwerksoperationen werden erfasst. Mit diesen Informationen können die Entwickler Probleme im Zusammenhang mit dem ESET-Produkt auf Ihrem Betriebssystem verstehen und beheben.
Erweitertes Logging für Protokollfilterung aktivieren – Erfasst alle Daten, die die Protokollprüfung durchlaufen, im PCAP-Format, um die Entwicklern bei der Diagnose und Behebung von Problemen im Zusammenhang mit der Protokollfilterung zu helfen.
Erweitertes Logging für Push-Messaging aktivieren – Erfasst alle Ereignisse, die beim Push-Messaging auftreten, zu Diagnose- und Problembehebungszwecken.
Erweiterte Logging für Echtzeit-Dateischutz aktivieren – Erfasst alle im Echtzeit-Dateischutz aufgetretenen Ereignisse zu Diagnose- und Problembehebungszwecken.
Erweitertes Logging für Update-Modul aktivieren – Erfasst alle Ereignisse, die während des Updates auftreten, um den Entwicklern bei der Diagnose und Behebung von Problemen im Zusammenhang mit dem Update-Modul zu helfen.

Speicherort der Log-Dateien

C:\ProgramData\ESET\ESET Security\Diagnostics

Technischer Support

Systemkonfigurationsdaten senden

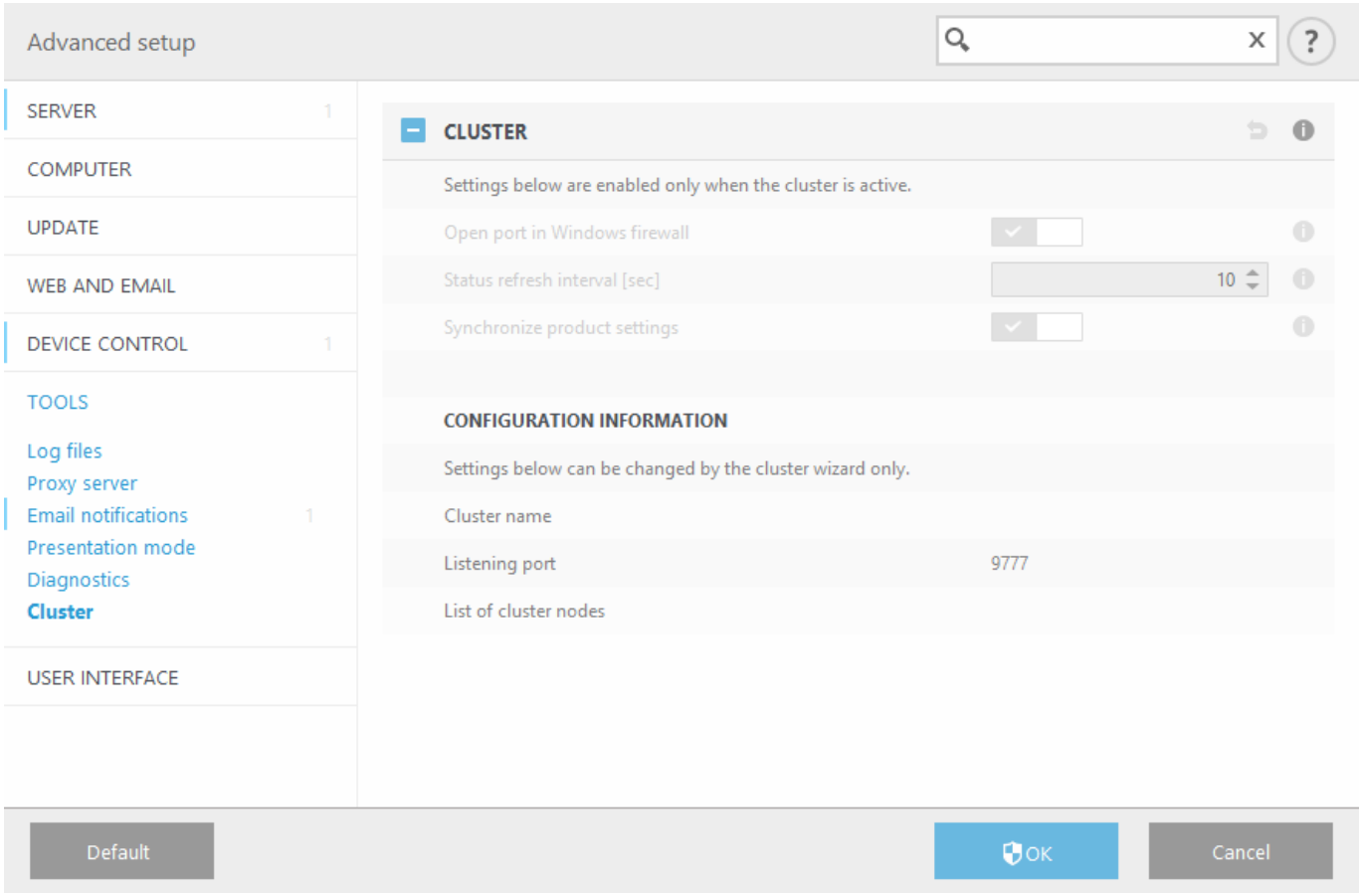
Wählen Sie **Immer senden** aus, um vor dem Senden Ihrer ESET Mail Security-Konfigurationsdaten nicht gefragt zu

werden, oder verwenden Sie die Option **Vor dem Senden nachfragen**.

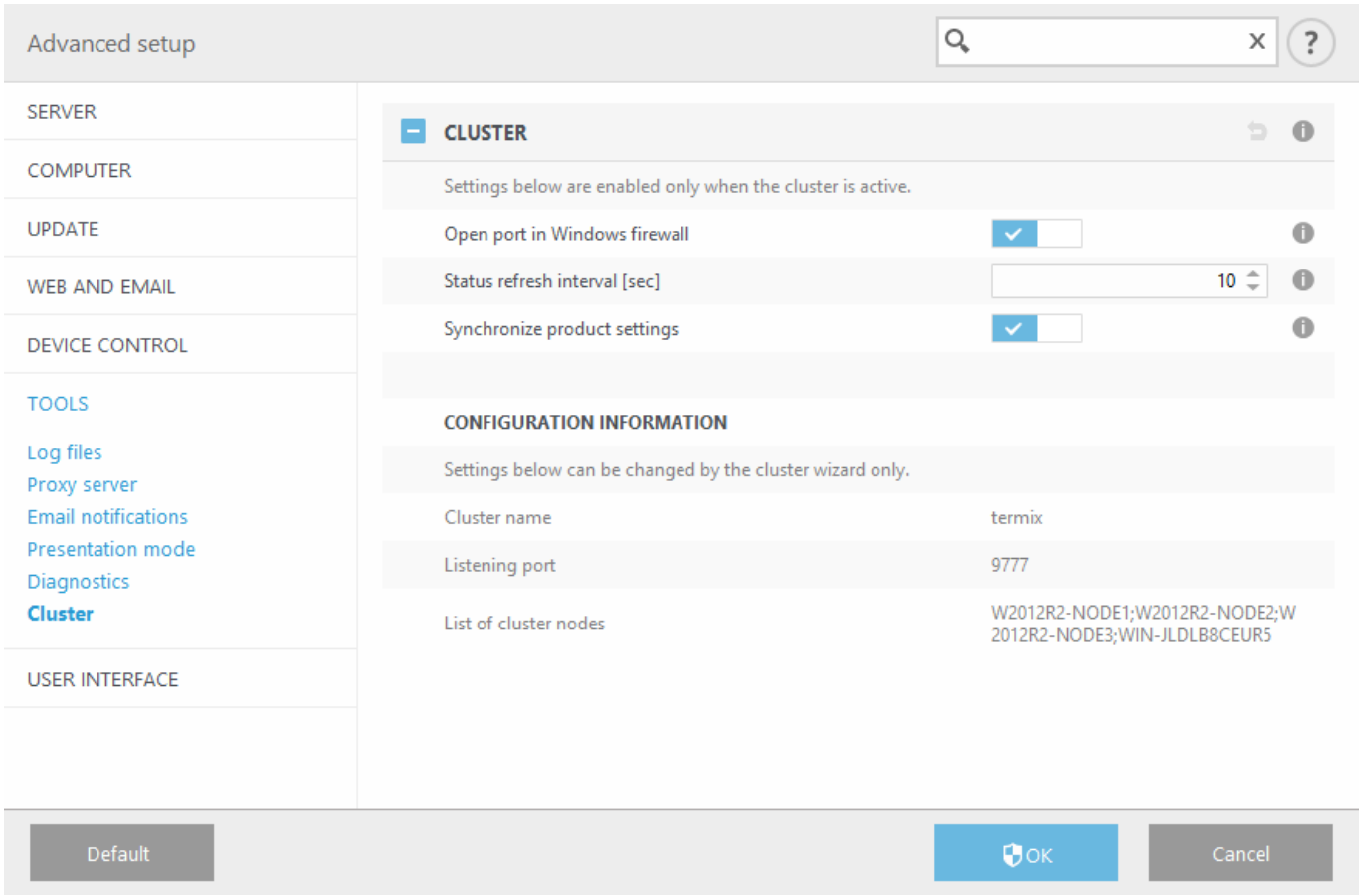
Cluster

„Cluster aktivieren“ wird automatisch aktiviert, wenn der ESET-Cluster konfiguriert wird. Sie können den Cluster manuell im Fenster **Erweiterte Einstellungen** (F5) deaktivieren, indem Sie auf das Schaltersymbol klicken (wenn Sie z. B. die Konfiguration ändern möchten, ohne andere Knoten im ESET-Cluster zu beeinflussen). Der Schalter dient nur dem Aktivieren und Deaktivieren der ESET-Clusterfunktion. Zum Einrichten oder Zerstören eines Cluster müssen Sie den Clusterassistenten verwenden bzw. die Option **Cluster zerstören** im Bereich Tools > Cluster im Hauptprogrammfenster.

ESET-Cluster nicht konfiguriert und deaktiviert:



ESET-Cluster richtig mit Details und Optionen konfiguriert:



Benutzeroberfläche

Konfigurieren Sie das Verhalten der grafischen Benutzeroberfläche (GUI) von ESET Mail Security. Sie können das Erscheinungsbild und die grafischen Effekte des Programms anpassen.

Im Dropdownmenü „GUI-Startmodus“ können Sie die folgenden Startmodi für die grafische Benutzeroberfläche (GUI) auswählen:

- **Vollständig** – Die komplette Benutzeroberfläche wird angezeigt.

- **Terminal** - Es werden keine Warnungen und Benachrichtigungen angezeigt. Die grafische Benutzeroberfläche kann nur vom Administrator gestartet werden. Die Benutzeroberfläche sollte auf Terminal eingestellt werden, wenn die grafischen Elemente die Leistung des Computers beeinträchtigen oder andere Probleme auftreten. Außerdem können Sie die grafische Benutzeroberfläche für Terminalserver deaktivieren. Weitere Informationen zur Installation von ESET Mail Security auf einem Terminalserver finden Sie im Thema Deaktivieren der Benutzeroberfläche auf Terminalserver.

Farbmodus

Wählen Sie das Farbschema der grafischen Benutzeroberfläche (GUI) von ESET Mail Security im Dropdownmenü aus:

- **Gleiche Farbe wie das System** – Das Farbschema von ESET Mail Security richtet sich nach Ihren Betriebssystemeinstellungen.

- **Dunkel** – ESET Mail Security verwendet ein dunkles Farbschema (dunkler Modus).

- **Hell** – ESET Mail Security verwendet ein helles Farbschema (Standard).

Startbildschirm anzeigen – Deaktivieren Sie diese Option, wenn beim Start des Programmfensters von ESET Mail Security kein Startbildschirm angezeigt werden soll, z. B. wenn Sie sich beim System anmelden.

Hinweistöne wiedergeben – ESET Mail Security spielt bei wichtigen Ereignissen wie z. B. der Erkennung einer Bedrohung oder nach Abschluss einer Prüfung einen Warnton ab.

In Kontextmenü integrieren – Diese Funktion integriert Steuerelemente von ESET Mail Security in das Kontextmenü. Das Kontextmenü wird angezeigt, wenn Sie mit der rechten Maustaste auf ein Element (eine Datei) klicken. Das Menü enthält alle Optionen, die auf das Objekt angewendet werden können.

Lizenzinformationen

Wenn diese Option aktiviert ist, werden Nachrichten und Benachrichtigungen zu Ihrer Lizenz angezeigt.

Lizenzinformationen anzeigen – Wenn diese Option deaktiviert ist, wird das Ablaufdatum der Lizenz unter **Schutzstatus** und **Hilfe und Support** nicht angezeigt.

Lizenzbezogene Statusmeldungen konfigurieren – Öffnet die Liste der lizenzbezogenen Anwendungs-Statusmeldungen.

Lizenzbenachrichtigungen konfigurieren – Wenn diese Option deaktiviert ist, werden Benachrichtigungen und Nachrichten erst angezeigt, wenn die Lizenz abgelaufen ist.

Einstellungen für den Zugriff - Um einen maximalen Sicherheitsstandard zu gewährleisten, können Sie unbefugte Änderungen mit dem Tool **Einstellungen für den Zugriff** verhindern.

ESET-Shell - Sie können die Zugriffsrechte auf Produkteinstellungen, Funktionen und Daten in eShell konfigurieren, indem Sie die ESET-Shell-Ausführungsrichtlinie ändern.

Symbol im Windows-Benachrichtigungsbereich

Alle Einstellungen in diesem Bereich zurücksetzen

Einstellungen für den Zugriff

Um Ihr System optimal zu schützen ist es entscheidend, dass ESET Mail Security korrekt konfiguriert ist. Unbedachte Änderungen können zu Problemen oder sogar zum Verlust wichtiger Daten führen. Sie können Ihre ESET Mail Security-Konfiguration mit einem Passwort schützen, um unerwünschte Änderungen zu vermeiden.

Falls Sie ESET Mail Security mit aktiviertem Sicherheitspasswort deinstallieren, werden Sie zur Eingabe des Passworts aufgefordert. Andernfalls können Sie ESET Mail Security nicht deinstallieren.

Einstellungen mit Passwort schützen

Sperrt/entsperrt die Programmeinstellungen. Klicken Sie auf diese Option, um das **Passwortfenster** zu öffnen.

Passwort festlegen

Klicken Sie auf **Festlegen**, um ein Passwort für den Schutz der Einstellungen anzugeben oder um es zu ändern. Zum Schutz der Einstellungsparameter von ESET Mail Security vor unbefugten Änderungen muss ein neues

Passwort festgelegt werden. Wenn Sie ein bestehendes Passwort ändern möchten, geben Sie Ihr altes Passwort in das Feld **Altes Passwort** und Ihr neues Passwort in die Felder **Neues Passwort** und **Neues Passwort bestätigen** ein. Klicken Sie anschließend auf **OK**. Um anschließend Änderungen an der Konfiguration von ESET Mail Security vorzunehmen, müssen Sie dieses Passwort eingeben.

Volle Administratorrechte für eingeschränkte Administratorkonten anfordern

Mit dieser Option werden Benutzer ohne Administratorrechte zur Eingabe von Administratoranmeldeinformationen aufgefordert, wenn sie bestimmte Systemeinstellungen ändern möchten. Dazu gehört das Deaktivieren von Schutzmodulen.

> Wenn sich das Passwort für erweiterte Einstellungen geändert hat und Sie eine vorhandene .xml-Konfigurationsdatei importieren möchten, die vor der Passwortänderung signiert wurde, dann müssen Sie die Datei mit der ESET CMD-Befehlszeile erneut mit dem aktuellen Passwort signieren. Auf diese Weise können Sie eine ältere Konfigurationsdatei wiederverwenden, ohne sie vor dem Importieren auf einem anderen Computer mit ESET Mail Security erneut zu exportieren.

ESET-Shell

Sie können die Zugriffsrechte auf Produkteinstellungen, Funktionen und Daten in eShell konfigurieren, indem Sie die **ESET-Shell-Ausführungsrichtlinie** ändern. Die Standardeinstellung ist **Eingeschränktes Scripting**. Sie können dies jedoch bei Bedarf zu „Deaktiviert“, „Nur Lesezugriff“ oder „Vollzugriff“ ändern.

Deaktiviert

eShell kann nicht verwendet werden. Nur die Konfiguration von eShell ist erlaubt - im ui eshell-Kontext. Sie können das Erscheinungsbild von eShell konfigurieren, jedoch auf keinerlei Einstellungen oder Daten zugreifen.

Schreibgeschützt

eShell kann als Überwachungstool verwendet werden. Sie können alle Einstellungen im interaktiven und im Batch-Modus anzeigen, jedoch keinerlei Einstellungen, Features oder Daten bearbeiten.

Eingeschränktes Scripting

Im interaktiven Modus können Sie alle Einstellungen, Features und Daten bearbeiten. Im Batch-Modus verhält sich eShell wie im schreibgeschützten Modus. Sie können jedoch signierte Batchdateien verwenden, um Einstellungen und Daten zu bearbeiten.

Vollzugriff

Uneingeschränkter Zugriff auf alle Einstellungen im interaktiven und im Batch-Modus (bei der Ausführung von Batchdateien). Sie können alle Einstellungen anzeigen und bearbeiten. Sie benötigen ein Administratorkonto, um eShell mit Vollzugriff auszuführen. Falls UAC aktiviert ist, benötigen Sie außerdem erhöhte Rechte.

Deaktivieren der Benutzeroberfläche auf

Terminalserver

In diesem Kapitel wird beschrieben, wie Sie die grafische Benutzeroberfläche von ESET Mail Security für Benutzersitzungen deaktivieren können, wenn das Produkt auf einem Windows-Terminalserver läuft.

Die Benutzeroberfläche von ESET Mail Security wird bei jeder Anmeldung eines Remote-Benutzers auf dem Terminalserver gestartet. Für gewöhnlich ist dies auf Terminalservern nicht erwünscht. Sie können die Benutzeroberfläche für Terminalsitzungen deaktivieren, indem Sie in eShell den Befehl `set ui ui gui-start-mode none` ausführen. Dieser Befehl versetzt die Benutzeroberfläche in den Terminalmodus. Die Benutzeroberfläche kann in zwei verschiedenen Modi gestartet werden:

```
set ui ui gui-start-mode full
```

```
set ui ui gui-start-mode none
```

Führen Sie den Befehl `get ui ui gui-start-mode` aus, um den aktuellen Modus herauszufinden.

> Falls Sie ESET Mail Security auf einem Citrix-Server installiert haben, sollten Sie die in unserem Knowledgebase-Artikel beschriebenen Einstellungen verwenden.

Symbol im Windows-Benachrichtigungsbereich

Einige der wichtigsten Einstellungsoptionen und -Funktionen können per Rechtsklick auf das Symbol in der Taskleiste (Windows-Benachrichtigungsbereich) geöffnet werden.

> Um das Symbolmenü in der Taskleiste (Windows-Benachrichtigungsbereich) verwenden zu können, muss der Startmodus von Elemente der Benutzeroberfläche auf „Vollständig“ festgelegt sein.

Weitere Informationen

Öffnet die Seite Überwachung mit dem aktuellen Schutzstatus und aktuellen Nachrichten.

Schutz vorübergehend deaktivieren

Zeigt ein Dialogfenster an, in dem Sie bestätigen müssen, dass der Viren- und Spyware-Schutz deaktiviert werden soll, der Dateivorgänge sowie die Internet- und E-Mail-Kommunikation überwacht und so Ihr System vor Angriffen schützt. Im Dropdownmenü **Zeitintervall** können Sie festlegen, wie lange der Schutz deaktiviert werden soll.

Erweiterten Einstellungen

Öffnet die erweiterten Einstellungen für ESET Mail Security.

Log-Dateien

Log-Dateien enthalten Informationen zu allen wichtigen aufgetretenen Programmereignissen sowie einen Überblick über erkannte Bedrohungen.

Fensterlayout zurücksetzen

Stellt die standardmäßige Fenstergröße und die Standardposition von ESET Mail Security auf dem Bildschirm wieder her.

Farbmodus

Öffnet die Einstellungen für die Benutzeroberfläche, in denen Sie das Farbschema der grafischen Benutzeroberfläche ändern können.

Nach Updates suchen

Beginnt mit der Aktualisierung der Module, um den Schutz vor Schadcode zu gewährleisten.

Über

Enthält Systeminformationen zur installierten Version von ESET Mail Security und zu den installierten Programmmodulen und zeigt das Ablaufdatum der Lizenz an. Informationen zum Betriebssystem und zu den Systemressourcen befinden sich unten auf der Seite.

Benachrichtigungen

Hinweise auf dem Desktop und Sprechblasen dienen ausschließlich zu Informationszwecken; Eingaben des Benutzers sind nicht erforderlich. Sie werden im Infobereich der Taskleiste rechts unten auf dem Bildschirm angezeigt. Weitere Optionen, wie Anzeigedauer und Transparenzkönnen unten geändert werden.

Um die ESET Mail Security Benachrichtigungen zu verwalten, navigieren Sie zu **Erweiterte Einstellungen** (**F5**) > **Benachrichtigungen**. Sie können die folgenden Typen konfigurieren:

Anwendungsstatus – Klicken Sie auf **Bearbeiten**, um auszuwählen, welche Anwendungs-Statusmeldungen im Startbereich des Programmfensters angezeigt werden sollen.

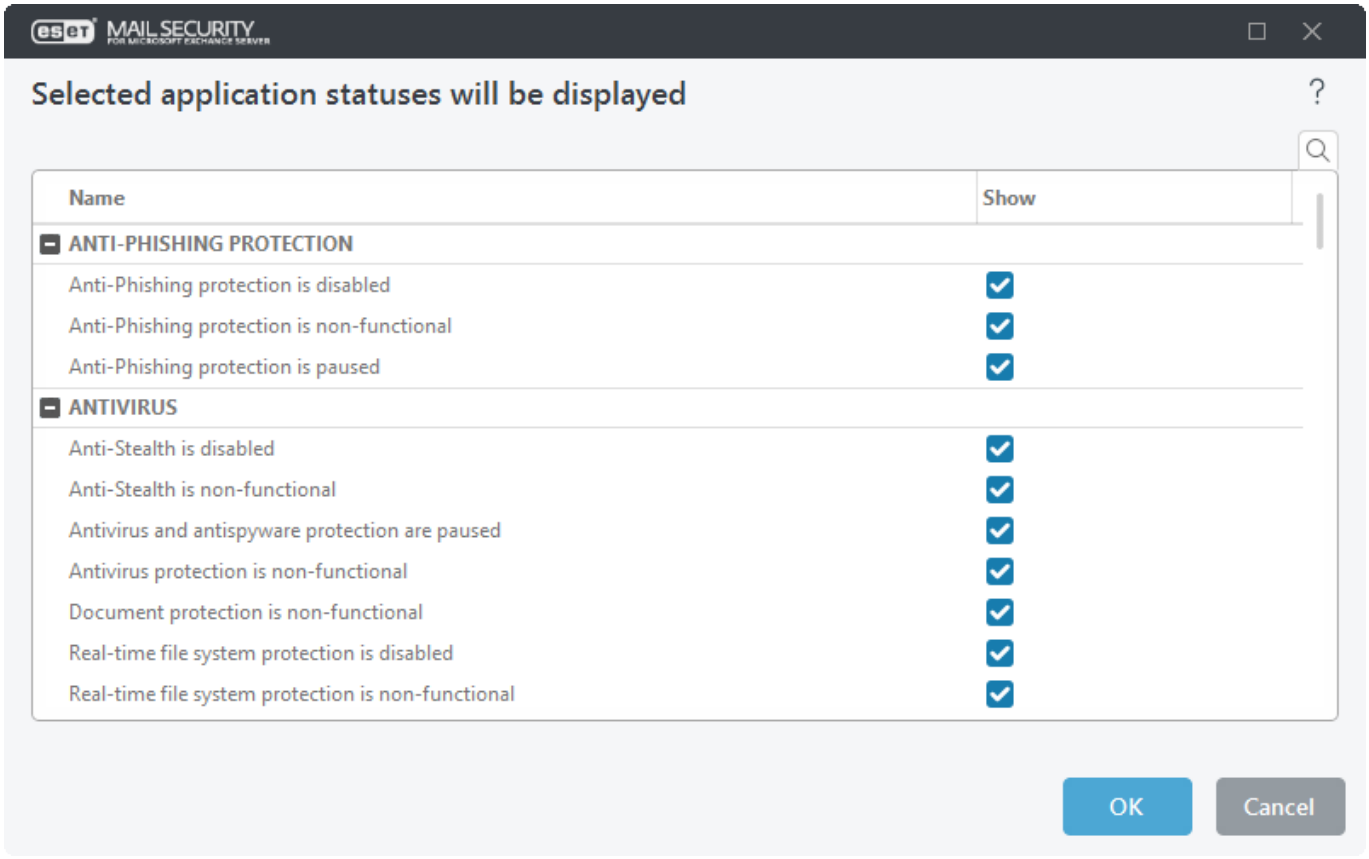
Desktopbenachrichtigungen – Kleine Popupfenster neben der System-Taskleiste.

Interaktive Warnungen – Warnungsfenster und Hinweismeldungen, die ein Eingreifen der Benutzer erfordern.

Weiterleitung (E-Mail-Benachrichtigungen) – Benachrichtigungen werden an eine angegebene E-Mail-Adresse gesendet.

Anwendungsstatus

In diesem Fenster können Sie auswählen, welche Anwendungs-Statusmeldungen angezeigt werden sollen. Wenn Sie beispielsweise den Viren- und Spywareschutz anhalten, führt dies dazu, dass in der Seite Überwachung eine Änderung des Schutzstatus angezeigt wird. Ein Anwendungsstatus wird auch angezeigt, wenn Ihr Produkt nicht aktiviert oder Ihre Lizenz abgelaufen ist. Der Anwendungsstatus kann über ESET PROTECT-Policies verwaltet werden.



Deaktivierte Nachrichten und Statusmeldungen

Bestätigungsmeldungen

Zeigt eine Liste von Bestätigungsnachrichten an. Sie können auswählen, welche dieser Meldungen angezeigt werden sollen.

Anwendungsstatus

Aktiviert oder deaktiviert die Statusanzeige auf der Seite Überwachung im Hauptmenü.

Desktophinweise

Desktopbenachrichtigungen werden als kleines Benachrichtigungsfenster neben der System-Taskleiste angezeigt. Diese Fenster werden standardmäßig 10 Sekunden lang angezeigt und verblassen dann langsam. ESET Mail Security kommuniziert mit dem Benutzer, indem Nachrichten für erfolgreiche Produktupdates, neu angeschlossene Geräte, Viren-Scans, abgeschlossene Tasks oder erkannte Ereignisse angezeigt werden.

Desktopbenachrichtigungen anzeigen

Wir empfehlen, diese Option aktiviert zu lassen, damit das Produkt Sie über neue Ereignisse informieren kann.

Desktophinweise

Klicken Sie auf **Bearbeiten**, festzulegen, welche Desktopbenachrichtigungen für verschiedene Ereignisse angezeigt werden sollen.

Aktivieren Sie **Desktopbenachrichtigungen nicht anzeigen, wenn Anwendungen im Vollbildmodus ausgeführt werden**, wenn keine nicht-interaktiven Benachrichtigungen angezeigt werden sollen.

Zeit in Sekunden anzeigen

Legen Sie die Anzeigedauer für die Benachrichtigung fest. Der Wert muss zwischen 3 und 30 Sekunden liegen.

Transparenz

Legen Sie die Transparenz der Benachrichtigung als Prozentwert fest. Der unterstützte Bereich reicht von 0 (keine Transparenz) bis 80 (sehr hohe Transparenz).

Im Dropdownmenü **Mindestinformationen anzuzeigender Ereignisse** können Sie den Schweregrad für Warnungen und Benachrichtigungen auswählen. Folgende Optionen stehen zur Verfügung:

- **Diagnosedaten** - Alle Meldungen höherer Stufen und alle sonstigen Informationen, die für das Beheben von Fehlern wichtig sein können, werden protokolliert.
- **Informationen** - Meldungen wie erfolgreiche Updates und alle Meldungen höherer Stufen werden protokolliert.
- **Warnungen** - Kritische Fehler und Warnungen werden protokolliert.
- **Fehler** - Fehler wie „Fehler beim Herunterladen der Datei“ und kritische Fehler werden aufgezeichnet.
- **Kritisch** - Nur kritische Fehler werden protokolliert.

Mit dem Feld **Auf Mehrbenutzersystemen** Benachrichtigungen auf dem Bildschirm des folgenden Benutzers ausgeben können Sie festlegen, bei welchem Benutzer Warnungen und Benachrichtigungen angezeigt werden, wenn mehrere Benutzer gleichzeitig angemeldet sind. Üblicherweise wird hier der System- oder Netzwerkadministrator gewählt. Besonders sinnvoll ist diese Option bei Terminalservern, sofern alle Systemmeldungen an den Administrator gesendet werden.

Zulassen, dass Benachrichtigungen im Fokus angezeigt werden – Benachrichtigungen werden im Fokus angezeigt und können mit Alt+Tab ausgewählt werden.

Anpassen

In diesem Fenster können Sie die Texte der Benachrichtigungen anpassen.

Benachrichtigungen – Eine Standardnachricht, die in der Fußzeile von Benachrichtigungen angezeigt wird.

Ereignis

Ereignisbenachrichtigungen nicht automatisch schließen

Benachrichtigungen für Ereignis müssen manuell geschlossen werden.

Standardnachricht verwenden

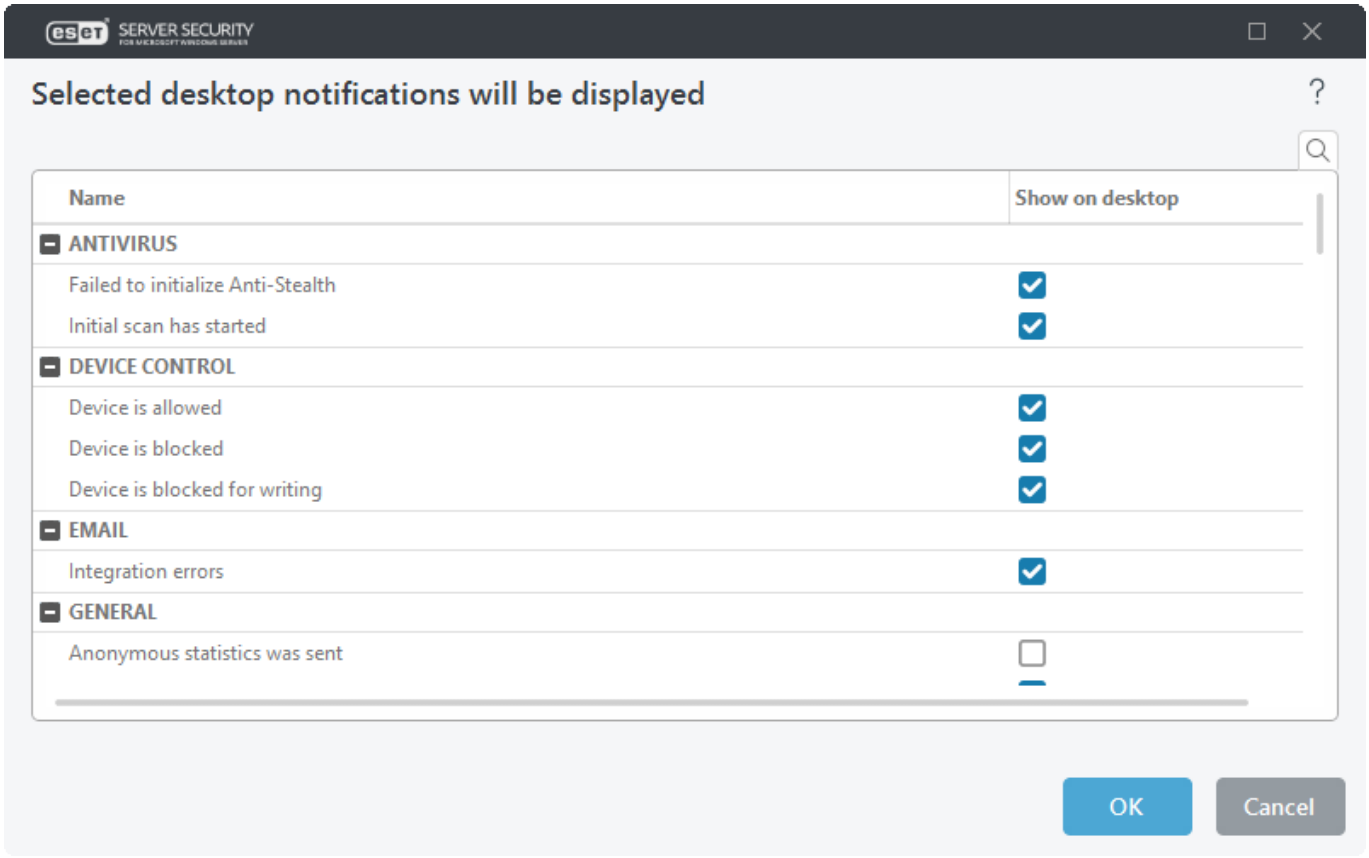
Sie können die Standardnachricht deaktivieren und eine benutzerdefinierte Ereignismeldung festlegen, die angezeigt wird, wenn ein Ereignis blockiert wurde.

Ereignis-Standardbenachrichtigung

Geben Sie eine benutzerdefinierte Nachricht an, die angezeigt wird, wenn ein Ereignis blockiert wurde.

Desktophinweise

Sie können festlegen, ob die ESET Mail Security Benachrichtigungen auf dem Desktop angezeigt werden sollen.



Interaktive Warnungen

Sie können festlegen, wie ESET Mail Security Bedrohungswarnungen und Systembenachrichtigungen (z. B. erfolgreiche Updates) verarbeiten soll. Konfigurieren Sie die **Anzeigedauer** und **Transparenz** von Meldungen im Windows-Benachrichtigungsbereich (nur für Systeme, die Benachrichtigungen unterstützen).

Interaktive Warnungen anzeigen

Wenn Sie diese Funktion deaktivieren, zeigt ESET Mail Security keine Warnungen im Windows-Benachrichtigungsbereich an.

Liste der interaktiven Warnungen

Nützlich für die Automatisierung. Deaktivieren Sie die Option **Benutzer fragen** für Elemente, die Sie automatisieren möchten, und wählen Sie die Aktion aus, die anstelle des Hinweisfensters ausgeführt werden soll.

Hinweisfenster enthalten kurze Textmitteilungen oder Fragen.

Hinweisfenster automatisch schließen

Benachrichtigungsfenster werden nach einer bestimmten Zeit automatisch geschlossen. Die Hinweise werden nach Ablauf der festgelegten Zeit automatisch geschlossen, sofern sie nicht bereits vom Benutzer geschlossen wurden.

Bestätigungsmeldungen

Klicken Sie auf **Bearbeiten**, um ein Popupfenster mit einer Liste der Bestätigungsmeldungen zu öffnen, die ESET Mail Security vor dem Ausführen einer Aktion anzeigt. Mit den Kontrollkästchen können Sie die Einstellungen für Bestätigungsmeldungen anpassen.

Weiterleitung

ESET Mail Security kann automatisch Ereignismeldungen senden, wenn ein Ereignis mit dem ausgewählten Informationsumfang auftritt.

Per E-Mail weiterleiten

Aktivieren Sie die Option „Benachrichtigungen per E-Mail weiterleiten“, um E-Mail-Benachrichtigungen zu aktivieren.

Weitergeleitete Benachrichtigungen

Wählen Sie aus, welche Desktopbenachrichtigungen per E-Mail weitergeleitet werden sollen.

E-Mail-Einstellungen

Informationsumfang der Meldungen - Hier können Sie festlegen, für welche Ereignistypen Benachrichtigungen verschickt werden sollen.

- **Diagnosedaten** – Alle Meldungen höherer Stufen und alle sonstigen Informationen, die für die Feinabstimmung des Programms wichtig sein können, werden protokolliert.
- **Information** – Informationsmeldungen wie vom Standard abweichende Netzwerkereignisse, inklusive erfolgreiche Updates sowie alle Meldungen höherer Stufen werden protokolliert.
- **Warnungen** – Kritische Fehler und Warnmeldungen werden erfasst (Anti-Stealth wird nicht ordnungsgemäß ausgeführt oder Update fehlgeschlagen).
- **Fehler** - Fehler wie „Fehler beim Herunterladen der Datei“ und kritische Fehler werden aufgezeichnet.
- **Kritisch** - Nur kritische Fehler werden protokolliert.

Jede Benachrichtigung in einer getrennten E-Mail senden

Wenn diese Option aktiviert ist, erhält der Empfänger für jede einzelne Benachrichtigung eine separate E-Mail. Dies kann dazu führen, dass innerhalb kurzer Zeit eine große Anzahl E-Mails verschickt wird.

Intervall bis zum Senden neuer Benachrichtigungs-E-Mails (Min.)

Intervall in Minuten, nach dem eine neue Benachrichtigung per E-Mail gesendet wird. Legen Sie für diese Einstellung den Wert „0“ fest, wenn die Benachrichtigungen sofort gesendet werden sollen.

Absenderadresse

Absenderadresse - Geben Sie die Absenderadresse ein, die in der Kopfzeile von Benachrichtigungs-E-Mails angezeigt werden soll. Diese Adresse wird dem Empfänger als **Absender** angezeigt.

Empfängeradresse

Geben Sie die E-Mail-Adresse des Empfängers an, die im Header von Benachrichtigungs-E-Mails angezeigt werden soll. Verwenden Sie ein Semikolon „;“, um mehrere E-Mail-Adressen voneinander zu trennen.

SMTP-Server

Der Name des SMTP-Servers für den Versand von Warnungen und Benachrichtigungen. Dies ist normalerweise der Name Ihres Microsoft Exchange-Servers.

ESET Mail Security unterstützt keine SMTP-Server mit TLS-Verschlüsselung.

Benutzername und Passwort

Falls für den SMTP-Server Zugangsdaten zur Authentifizierung erforderlich sind, geben Sie hier einen gültigen Benutzernamen und das Passwort ein.

TLS aktivieren

Aktiviert die der TLS-Verschlüsselung unterstützten Warnungen und Benachrichtigungen.

SMTP-Verbindung testen

Eine Test-E-Mail wird an die E-Mail-Adresse des Empfängers gesendet.

Format von Meldungen

Ereignismeldungen werden als E-Mails oder LAN-Nachrichten (Windows Messenger-Dienst) an Remotebenutzer oder Systemadministratoren weitergeleitet. Das Standardformat für Warnungen und Benachrichtigungen ist für die meisten Situationen optimal. Sie können das Format der Meldungen bei Ereignissen jedoch auch anpassen.

Format der Meldungen bei Ereignissen

Geben Sie das Format der E-Mail-Ereignisbenachrichtigungen an.

Format der Meldungen bei Bedrohungen

Warnungen und Benachrichtigungen besitzen ein vordefiniertes Standardformat. Dieses Format sollte nicht geändert werden. Unter bestimmten Umständen (etwa, wenn Sie ein automatisiertes E-Mail-Verarbeitungssystem verwenden) ist es jedoch möglicherweise erforderlich, das Meldungsformat zu ändern.

Schlüsselwörter (durch %-Zeichen getrennte Zeichenfolgen) in der Meldung werden durch entsprechende Informationen ersetzt. Folgende Schlüsselwörter sind verfügbar:

- %TimeStamp% – Datum und Uhrzeit des Ereignisses
- %Scanner% – betroffenes Modul

- %ComputerName% – Name des Computers, auf dem die Warnmeldung aufgetreten ist
- %ProgramName% – Programm, das die Warnung erzeugt hat
- %DetectionObject% – Name der infizierten Datei, Nachricht usw.
- %DetectionName% – Angabe des Infektionsverursachers
- %ErrorDescription% – Beschreibung eines nicht durch einen Virus ausgelösten Ereignisses

Die Schlüsselwörter **%DetectionObject%** und **%DetectionName%** werden nur in Warnmeldungen bei Bedrohungen verwendet, **%ErrorDescription%** nur in Ereignismeldungen.

Zeichensatz

Wählen Sie eine Kodierung im Dropdownmenü aus. Die E-Mail-Nachricht wird gemäß der ausgewählten Zeichenkodierung konvertiert. Konvertiert eine E-Mail-Nachricht anhand der Windows-Ländereinstellungen in eine ANSI-Zeichenkodierung (z. B. Windows-1250, Unicode (UTF-8), ACSII 7-bit oder Japanisch (ISO-2022-JP)). In diesem Fall wird „á“ zu „a“ geändert, und unbekannte Symbole zu „?“.

Quoted-Printable-Kodierung verwenden

Die E-Mail-Nachrichtenquelle wird in das QP-Format (Quoted Printable) konvertiert, das ASCII-Zeichen verwendet und besondere regionale Zeichen in der E-Mail korrekt im 8-Bit-Format überträgt (áéíóú).

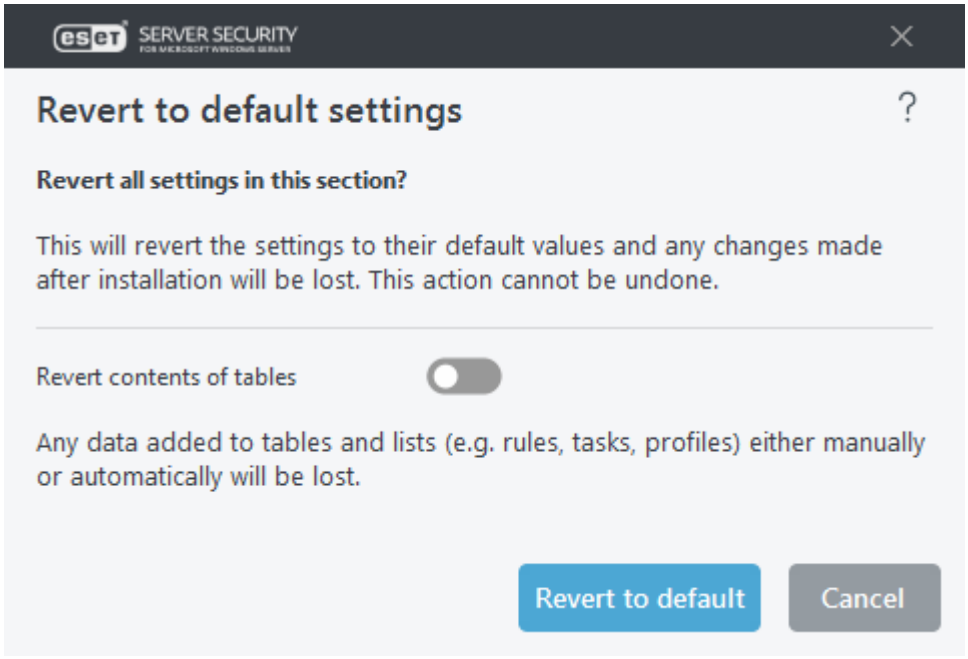
Auf Standardeinstellungen zurücksetzen

Sie können die Einstellungen in den **erweiterten Einstellungen** auf die Standardwerte zurücksetzen. Sie haben zwei Optionen zur Auswahl: Sie können entweder alles oder nur die Einstellungen in einem bestimmten Abschnitt zurücksetzen (die restlichen Einstellungen bleiben erhalten).

Alle Einstellungen zurücksetzen – Alle Einstellungen in sämtlichen Abschnitten der erweiterten Einstellungen werden auf die Standardwerte nach der Installation von ESET Mail Security zurückgesetzt. Dies entspricht dem Zurücksetzen auf die Werkseinstellungen.

> Klicken Sie auf **Rückgängig machen**, um alle Änderungen zu verwerfen. Diese Aktion kann nicht rückgängig gemacht werden.

Alle Einstellungen in diesem Bereich zurücksetzen – Setzt die Moduleinstellungen im ausgewählten Abschnitt auf die Standardwerte zurück. Alle in diesem Abschnitt vorgenommenen Änderungen werden verworfen.



Inhalte von Tabellen zurücksetzen – Wenn diese Option aktiviert ist, gehen manuell oder automatisch hinzugefügte Regeln, Tasks oder Profile verloren.

Hilfe und Support

ESET Mail Security enthält Tools für die Fehlerbehebung und Support-Informationen, die Ihnen bei der Lösung von möglichen Problemen behilflich sind.

Installiertes Produkt

Produkt- und Lizenzinformationen

- Über ESET Mail Security – Informationen zu Ihrer Kopie von ESET Mail Security.
- Fehlerbehebung für das Produkt – um Lösungen für die häufigsten Probleme zu finden. Bevor Sie sich an den Support wenden, sollten Sie diesen Abschnitt unbedingt lesen.
- Fehlerbehebung für Lizenzen – Unterstützt Sie bei Problemen im Zusammenhang mit der Aktivierung oder mit Lizenzänderungen.
- Lizenz ändern – Klicken Sie hier, um das Aktivierungsfenster zu öffnen und Ihr Produkt zu aktivieren.

Hilfeseiten

Öffnet die Onlinehilfe für ESET Mail Security.

Knowledgebase

ESET-Knowledgebase durchsuchen - Die ESET-Knowledgebase enthält Antworten auf die am häufigsten gestellten Fragen sowie Lösungsvorschläge für zahlreiche Problemstellungen. Die Knowledgebase wird regelmäßig von den ESET-Supportmitarbeitern aktualisiert und ist daher hervorragend für die Lösung verschiedenster Probleme geeignet.

Technischer Support

- Erweiterte Logging – Erstellen Sie erweiterte Logs für alle verfügbaren Funktionen, um die Entwickler bei der Diagnose und Behebung von Problemen zu unterstützen.

- Support anfordern – Wenn Sie Ihr Problem nicht lösen können, wenden Sie sich an unseren technischen Support.

- Details für den technischen Support – Zeigt Detailinformationen (Produktname, Produktversion usw.) für den technischen Support an.

- ESET Log Collector – ESET Log Collector dient zum automatischen Erfassen von Informationen wie Konfigurationsdetails und Logs von Ihrem Server zur schnelleren Fehlerbehebung.

Supportanfrage senden

Um möglichst schnell und effizient Hilfe bieten zu können, benötigt der ESET-Support Informationen zu Ihrer Konfiguration von ESET Mail Security, detaillierte Systeminformationen, Informationen zu ausgeführten Prozessen (ESET SysInspector-Log-Datei) und Registrierungsdaten. ESET nutzt diese Daten ausschließlich zum Bereitstellen technischer Unterstützung für den Kunden. Sie können diese Einstellung auch in den **erweiterten Einstellungen** (**F5**) unter **Tools** > **Diagnose** > **Technischer Support** konfigurieren.

> Wenn Sie Systemdaten einreichen möchten, müssen Sie das Webformular ausfüllen und einreichen. Andernfalls wird kein Ticket erstellt und die Systemdaten werden nicht übermittelt.

Wenn Sie das Webformular übermitteln, werden Ihre Systemkonfigurationsdaten an ESET gesendet. Wählen Sie **Diese Informationen immer senden** aus, wenn Sie diese Aktion für den Prozess speichern möchten.

Keine Daten senden - Verwenden Sie diese Option, falls Sie keine Daten übermitteln möchten. Sie werden zur Webseite des technischen ESET-Supports weitergeleitet.

Über ESET Mail Security

Dieses Fenster enthält Details zur installierten Version von ESET Mail Security. Im oberen Fensterbereich sehen Sie Informationen zu Ihrem Betriebssystem und den Systemressourcen, den aktuell angemeldeten Benutzer und den vollständigen Computernamen.

Installierte Komponenten

Dieser Bereich enthält Informationen zu den Modulen, um eine Liste der Komponenten und deren Details zu öffnen. Klicken Sie auf **Kopieren**, um die Liste in Ihre Zwischenablage zu kopieren. Dies kann bei der Fehlerbehebung oder beim Kontakt zum Support hilfreich sein.

Glossar

Besuchen Sie die Seite Glossar, um weitere Informationen zu technischen Begriffen, zu Bedrohungen und zur Internetsicherheit zu erhalten.

Endbenutzer-Lizenzvereinbarung

Gültig ab dem 19. Oktober 2021.

WICHTIG: Vor dem Herunterladen, Installieren, Kopieren oder Verwenden des Produkts lesen Sie bitte die folgenden Nutzungsbedingungen. **DURCH DAS HERUNTERLADEN, INSTALLIEREN, KOPIEREN ODER VERWENDEN DER SOFTWARE ERKLÄREN SIE SICH MIT DEN NUTZUNGSBEDINGUNGEN EINVERSTANDEN UND ERKENNEN DIE DATENSCHUTZERKLÄRUNG AN.**

Endbenutzer-Lizenzvereinbarung

Diese Endbenutzer-Lizenzvereinbarung (die "Vereinbarung") zwischen ESET, spol. s r. o., mit Sitz in Einsteinova 24, 85101 Bratislava, Slovak Republic, Handelsregistereintrag 3586/B in der Rubrik Sro beim Amtsgericht Bratislava I, Firmennummer 31333532, ("ESET" oder "Anbieter") und Ihnen, einer natürlichen oder juristischen Person ("Sie" oder der "Endbenutzer"), berechtigt Sie zur Nutzung der in Abschnitt 1 dieser Vereinbarung definierten Software. Die in Abschnitt 1 dieser Vereinbarung definierte Software darf unter den im Folgenden aufgeführten Bedingungen auf einem Datenträger gespeichert, per E-Mail versendet, aus dem Internet oder von Servern des Anbieters heruntergeladen oder auf andere Weise beschafft werden.

DIESES DOKUMENT IST KEIN KAUFVERTRAG, SONDERN EINE VEREINBARUNG ÜBER DIE RECHTE DES ENDBENUTZERS. Der Anbieter bleibt Eigentümer des Exemplars der Software und, soweit vorhanden, des physischen Mediums, auf dem die Software für den Verkauf vorliegt, sowie aller Kopien der Software, zu deren Erstellung der Endbenutzer unter den Bedingungen dieser Vereinbarung berechtigt ist.

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

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

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

2. **Installation, Computer und ein Lizenzschlüssel**. Die auf einem Datenträger bereitgestellte, per E-Mail verschickte, aus dem Internet oder von den Servern des Anbieters heruntergeladene oder auf anderem Weg beschaffte Software muss installiert werden. Sie müssen die Software auf einem korrekt konfigurierten Computer

installieren, der die in der Dokumentation genannten Mindestvoraussetzungen erfüllt. Die Installationsmethode ist in der Dokumentation beschrieben. Auf dem Computer, auf dem Sie die Software installieren, darf kein Computerprogramm und keine Hardware vorhanden sein, die sich negativ auf die Software auswirken könnte. Die Bezeichnung "Computer" erstreckt sich auf Hardware inklusive, jedoch nicht ausschließlich, Personal Computer, Laptops, Arbeitsstationen, Palmtop-Computer, Smartphones, tragbare elektronische Geräte oder andere elektronische Geräte, für die die Software entwickelt wurde und auf denen die Software installiert und/oder eingesetzt wird. Der Begriff "Lizenzschlüssel" bezeichnet die eindeutige Abfolge von Symbolen, Buchstaben und Zahlen, die dem Endbenutzer bereitgestellt wird, um die legale Nutzung der Software in der jeweiligen Version bzw. die Verlängerung der Lizenz gemäß dieser Vereinbarung zu ermöglichen.

3. **Lizenz**. Unter der Voraussetzung, dass Sie sich mit dieser Vereinbarung einverstanden erklärt haben und sämtliche darin enthaltenen Bestimmungen einhalten, gewährt Ihnen der Anbieter die folgenden Rechte (die "Lizenz"):

a) **Installation und Nutzung**. Sie erhalten das nicht exklusive und nicht übertragbare Recht, die Software auf der Festplatte eines Computers oder einem ähnlichen Medium zur dauerhaften Datenspeicherung zu installieren, die Software im Arbeitsspeicher eines Computers zu speichern und die Software auf Computern zu implementieren, zu speichern und anzuzeigen.

b) **Anzahl der Lizenzen.** Das Nutzungsrecht für die Software ist durch die Anzahl der Endbenutzer beschränkt. Unter einem „Endbenutzer“ ist Folgendes zu verstehen: (i) die Installation der Software auf einem Computer; oder (ii) wenn sich der Umfang einer Lizenz nach der Anzahl von Postfächern richtet, ist ein Endbenutzer ein Computerbenutzer, der E-Mails über ein E-Mail-Programm empfängt. Wenn das E-Mail-Programm E-Mail empfängt und diese anschließend automatisch an mehrere Benutzer weiterleitet, richtet sich die Anzahl der Endbenutzer nach der tatsächlichen Anzahl von Benutzern, an die auf diesem Weg E-Mail-Nachrichten gesendet werden. Wenn ein Mailserver die Funktion eines E-Mail-Gateways ausführt, entspricht die Zahl der Endbenutzer der Anzahl von Mailservern, für die dieses Gateway Dienste bereitstellt. Wenn mehrere E-Mail-Adressen (z. B. durch Aliasnamen) von einem Benutzer verwendet werden und nur ein Benutzer über diese Adressen E-Mail empfängt, während auf Clientseite keine E-Mail-Nachrichten automatisch an mehrere Benutzer verteilt werden, ist nur eine Lizenz für einen Computer erforderlich. Die gleichzeitige Nutzung derselben Lizenz auf mehreren Computern ist untersagt. Der Endbenutzer darf den Lizenzschlüssel für die Software nur in dem Umfang eingeben, für den er die entsprechende Anzahl von Lizenzen zur Nutzung der Software vom Anbieter erworben hat. Der Lizenzschlüssel ist vertraulich, und die Lizenz darf nicht mit Drittparteien geteilt oder von Drittparteien genutzt werden, sofern dies nicht in dieser Vereinbarung oder vom Anbieter erlaubt wurde. Benachrichtigen Sie den Anbieter unverzüglich, falls Ihr Lizenzschlüssel kompromittiert wurde.

c) **Home/Business Edition.** Die Home Edition der Software darf ausschließlich in privaten und/oder nichtkommerziellen Umgebungen für den Haus- und Familiengebrauch eingesetzt werden. Für die Verwendung der Software in kommerziellen Umgebungen sowie auf E-Mail-Servern, E-Mail-Relays, E-Mail- oder Internet-Gateways ist die Business Edition der Software erforderlich.

d) **Laufzeit der Lizenz.** Ihr Nutzungsrecht für die Software ist zeitlich beschränkt.

e) **OEM-Software.** Als „OEM“ klassifizierte Software darf ausschließlich auf dem Computer genutzt werden, mit dem sie ausgeliefert wurde. Eine Übertragung auf einen anderen Computer ist nicht gestattet.

f) **Nicht für den Wiederverkauf bestimmte Software und Testversionen.** Nicht für den Wiederverkauf („not for resale“, NFR) oder als Testversion bereitgestellte Software darf nicht veräußert, sondern ausschließlich zum Vorführen oder Testen der Softwarefunktionen verwendet werden.

g) **Ablauf und Kündigung der Lizenz**. Die Lizenz läuft automatisch zum Ende des jeweiligen Lizenzzeitraums aus. Sollten Sie eine Ihrer Pflichten aus dieser Vereinbarung verletzen, ist der Anbieter berechtigt, diese

außerordentlich zu kündigen und, ggf. auf dem Rechtsweg, etwaige weitere Ansprüche geltend zu machen. Bei Ablauf oder Kündigung der Lizenz müssen Sie die Software und ggf. alle Sicherungskopien sofort löschen, zerstören oder auf eigene Kosten an ESET oder das Geschäft zurückgeben, in dem Sie die Software erworben haben. Nach Ablauf oder Kündigung der Lizenz ist der Anbieter berechtigt, das Recht des Endbenutzers zur Nutzung der Softwarefunktionen zurückzuziehen, für die eine Verbindung zu Servern des Anbieters oder zu Servern von Drittanbietern erforderlich ist.

4. **Funktionen mit Datenerfassung und Anforderungen an die Internetverbindung.** Für den korrekten Betrieb benötigt die Software eine Internetverbindung und muss in der Lage sein, sich in regelmäßigen Abständen mit den Servern des Anbieters, Servern einer Drittpartei und entsprechenden Datenerfassungen gemäß der Datenschutzrichtlinie zu verbinden. Die Verbindung mit dem Internet und den entsprechenden Datenerfassungen ist für die folgenden Funktionen der Software erforderlich:

a) **Software-Updates.** Der Anbieter hat das Recht, von Zeit zu Zeit Aktualisierungen für die Software („Updates“) oder Upgrades bereitzustellen, ist dazu jedoch nicht verpflichtet. Diese Funktion ist in den Standardeinstellungen der Software aktiviert. Die Updates werden also automatisch installiert, sofern der Endbenutzer dies nicht deaktiviert hat. Zur Bereitstellung von Aktualisierungen muss die Echtheit der Lizenz überprüft werden. Dazu gehören Informationen über den Computer und/oder die Plattform, auf der die Software installiert wurde, in Übereinstimmung mit der Datenschutzerklärung.

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

b) **Weiterleitung von eingedrungener Schadsoftware und anderen Informationen an den Anbieter**. Die Software enthält Funktionen zur Erfassung neuer Computerviren und anderer schädlicher Computerprogramme sowie von verdächtigen, problematischen, potenziell unsicheren Objekten wie Dateien, URLs, IP-Pakete und Ethernet-Rahmen ("Infiltrationen"). Diese Daten werden zusammen mit Informationen über den Installationsprozess, den Computer und/oder die Plattform, auf der die Software installiert ist und Informationen über Betrieb und Funktionsweise der Software ("Informationen") an den Anbieter übertragen. Die Informationen und die Infiltrationen können Daten über den Endbenutzer oder andere Benutzer des Computers enthalten, auf dem die Software installiert ist (inklusive zufällig oder unbeabsichtigt erfasste personenbezogene Daten), sowie von eingedrungener Schadsoftware betroffene Dateien mit den entsprechenden Metadaten.

Die folgenden Funktionen der Software können Informationen und Infiltrationen sammeln:

i. Das LiveGrid Reputationssystem sammelt und sendet Einweg-Hashes im Zusammenhang mit eingedrungener Schadsoftware an den Anbieter. Diese Funktion ist in den Standardeinstellungen der Software aktiviert.

ii. Das LiveGrid-Reputationssystem erfasst Infiltrationen und überträgt diese zusammen mit den entsprechenden Metadaten und anderen Informationen an den Anbieter. Diese Funktion kann vom Endbenutzer bei der Installation der Software aktiviert werden.

Der Anbieter verwendet die erhaltenen Informationen und Infiltrationen ausschließlich zur Analyse und Erforschung der Infiltrationen, zur Verbesserung der Software und zur Überprüfung der Echtheit von Lizenzen und unternimmt angemessene Anstrengungen, um die erhaltenen Infiltrationen und Informationen zu schützen. Wenn diese Softwarefunktion aktiviert wird, darf der Anbieter gemäß der Datenschutzrichtlinie und gemäß geltender Gesetze Infiltrationen und Informationen erfassen und verarbeiten. Sie können diese Funktionen jederzeit deaktivieren.

Für die in dieser Vereinbarung festgelegten Zwecke werden Daten gesammelt, verarbeitet und gespeichert, mit denen der Anbieter Sie gemäß der Datenschutzrichtlinie identifizieren kann. Für die in dieser Vereinbarung festgelegten Zwecke werden Daten gesammelt, verarbeitet und gespeichert, mit denen der Anbieter Sie gemäß

der Datenschutzrichtlinie identifizieren kann. Sie stimmen zu, dass der Anbieter mit eigenen Mitteln überprüfen darf, ob Sie die Software in Übereinstimmung mit den Bestimmungen dieser Vereinbarung nutzen. Sie erkennen an, dass es für die in dieser Vereinbarung festgelegten Zwecke erforderlich ist, dass Ihre Daten zwischen der Software und den Computersystemen des Anbieters bzw. denen seiner Geschäftspartner im Rahmen des Distributions- und Verteilungsnetzwerks des Anbietersübertragen werden, um die Funktionstüchtigkeit der Software und die Genehmigung zu deren Nutzung sowie die Rechte des Anbieters zu schützen.

Mit Abschluss dieser Vereinbarung willigen Sie zudem in die Übertragung, Verarbeitung und Speicherung Ihrer personenbezogenen Daten durch den Anbieter bzw. seine Geschäftspartner ein, soweit eine solche Nutzung zur Abrechnung und zur Erfüllung dieser Vereinbarung und zum Übertragen von Benachrichtigungen auf Ihren Computer erforderlich ist.

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

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

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

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

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

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

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

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

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

g) Sie verpflichten sich hiermit, keine Aktivitäten im Zusammenhang mit dem Lizenzschlüssel auszuführen, die den Bestimmungen dieser Vereinbarung widersprechen oder die dazu führen, dass der Lizenzschlüssel an unbefugte

Personen weitergegeben wird, z. B. durch die Übertragung von benutzten oder nicht benutzten Lizenzschlüsseln in jeglicher Form oder die nicht autorisierte Verteilung von duplizierten oder generierten Lizenzschlüsseln oder die Nutzung der Software im Zusammenhang mit einem Lizenzschlüssel, der aus einer anderen Quelle als direkt vom Anbieter beschafft wurde.

7. **Urheberrecht**. Die Software und alle Rechte einschließlich des Rechtstitels und der geistigen Eigentumsrechte daran sind Eigentum von ESET und/oder seiner Lizenzgeber. Sie unterliegen dem Schutz der Bestimmungen internationaler Abkommen und aller sonstigen geltenden Gesetze des Landes, in dem die Software verwendet wird. Die Struktur, die Aufteilung und der Code der Software sind Geschäftsgeheimnisse und vertrauliche Informationen von ESET und/oder seiner Lizenzgeber. Die Software darf nicht kopiert werden, wobei lediglich die in Abschnitt 6(a) angegebene Ausnahme gilt. Alle gemäß dieser Vereinbarung zulässigen Kopien müssen dieselben Urheberrechts- und Eigentümerhinweise wie die ursprüngliche Software enthalten. Wenn Sie in Verstoß gegen die Bestimmungen dieser Vereinbarung Quellcode durch Reverse-Engineering analysieren, dekompilieren oder disassemblieren oder versuchen, sich den Quellcode auf andere Weise zu beschaffen, gehen automatisch sämtliche dadurch gewonnenen Informationen unwiderruflich und unmittelbar in das Eigentum des Anbieters über. Weiterhin ist der Anbieter in diesem Fall berechtigt, etwaige weitere Ansprüche aus Ihrem Verstoß gegen diese Vereinbarung geltend zu machen.

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

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

10. **Beginn und Gültigkeitsdauer der Vereinbarung.** Diese Vereinbarung tritt an dem Tag in Kraft, an dem Sie sich mit ihren Bestimmungen einverstanden erklären. Sie können diese Vereinbarung jederzeit kündigen, indem Sie die Software, alle Sicherungskopien und, falls vorhanden, alle vom Anbieter oder seinen Geschäftspartnern zur Verfügung gestellten zugehörigen Materialien dauerhaft löschen, sie zerstören bzw. auf eigene Kosten zurückgeben. Ihr Recht zur Nutzung der Software und deren Funktionen unterliegt möglicherweise einer EOL-Richtlinie. Wenn die Software oder deren Funktionen das in der EOL-Richtlinie definierte Ende des Lebenszyklus erreichen, erlischt Ihr Nutzungsrecht für die Software. Unabhängig von der Gültigkeitsdauer dieser Vereinbarung und der Art und Weise ihres Ablaufs bzw. ihrer Kündigung behalten die Bestimmungen der Abschnitte 7, 8, 11, 13, 19 und 21 auf unbegrenzte Zeit ihre Gültigkeit.

11. **AUSDRÜCKLICHE ERKLÄRUNGEN DES ENDBENUTZERS**. ALS ENDBENUTZER ERKENNEN SIE AN, DASS DIE SOFTWARE IM JEWEILIGEN IST-ZUSTAND UND OHNE JEGLICHE AUSDRÜCKLICHE ODER KONKLUDENTE GEWÄHRLEISTUNG BEREITGESTELLT WIRD, SOWEIT DIES IM RAHMEN DER GELTENDEN GESETZE ZULÄSSIG IST. WEDER DER ANBIETER NOCH SEINE LIZENZGEBER ODER DIE RECHTEINHABER GEWÄHREN AUSDRÜCKLICHE ODER KONKLUDENTE ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN, INSBESONDERE KEINE ZUSICHERUNGEN HINSICHTLICH DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER DER NICHTVERLETZUNG VON PATENTEN, URHEBER- UND MARKENRECHTEN ODER SONSTIGEN RECHTEN DRITTER. ES BESTEHT VON SEITEN DES ANBIETERS ODER DRITTER KEINERLEI GEWÄHRLEISTUNG, DASS DIE IN DER SOFTWARE ENTHALTENEN FUNKTIONEN IHREN ANFORDERUNGEN ENTSPRECHEN ODER DASS DIE SOFTWARE STÖRUNGS- UND FEHLERFREI AUSGEFÜHRT WIRD. SIE ÜBERNEHMEN DIE VOLLE VERANTWORTUNG UND DAS VOLLE RISIKO HINSICHTLICH DER AUSWAHL DER SOFTWARE ZUM ERREICHEN DER VON IHNEN BEABSICHTIGTEN ERGEBNISSE SOWIE FÜR INSTALLATION UND NUTZUNG DER SOFTWARE UND DEN MIT DIESER ERZIELTEN ERGEBNISSEN.

12. **Keine weiteren Verpflichtungen**. Aus dieser Vereinbarung ergeben sich für den Anbieter und seine

Lizenzgeber keine weiteren Verpflichtungen außer den explizit aufgeführten.

13. **HAFTUNGSAUSSCHLUSS**. SOWEIT IM RAHMEN DER GELTENDEN GESETZE ZULÄSSIG, ÜBERNEHMEN DER ANBIETER, SEINE ANGESTELLTEN UND SEINE LIZENZGEBER KEINERLEI HAFTUNG FÜR ENTGANGENE GEWINNE, ERTRÄGE ODER VERKÄUFE. VON DER HAFTUNG AUSGESCHLOSSEN SIND AUSSERDEM DATENVERLUSTE, BESCHAFFUNGSKOSTEN FÜR ERSATZTEILE ODER DIENSTE, SACH- UND PERSONENSCHÄDEN, GESCHÄFTSUNTERBRECHUNGEN, DER VERLUST VON GESCHÄFTSINFORMATIONEN SOWIE JEGLICHE ANDERE NEBEN-, VERMÖGENS- ODER FOLGESCHÄDEN, DIE INFOLGE DER INSTALLATION, NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DER SOFTWARE ENTSTEHEN. DA IN BESTIMMTEN LÄNDERN UND UNTER BESTIMMTEN GESETZEN EIN HAFTUNGSAUSSCHLUSS NICHT ZULÄSSIG IST, EINE HAFTUNGSBESCHRÄNKUNG JEDOCH MÖGLICH, BESCHRÄNKT SICH DIE HAFTUNG DES ANBIETERS, SEINER ANGESTELLTEN UND LIZENZGEBER AUF DEN FÜR DIE LIZENZ ENTRICHTETEN PREIS.

14. Gesetzlich verankerte Verbraucherrechte haben im Konfliktfall Vorrang vor den Bestimmungen dieser Vereinbarung.

15. **Technischer Support**. ESET bzw. die von ESET beauftragten Dritten erbringen jeglichen technischen Support ausschließlich nach eigenem Ermessen und ohne diesbezügliche Zusicherungen oder Gewährleistungen. Nachdem die Software oder eine ihrer Funktionen das in der EOL-Policy festgelegte End-of-Life-Datum erreicht hat, wird kein technischer Support mehr bereitgestellt. Endbenutzer sind verpflichtet, vor der Inanspruchnahme von Supportleistungen eine Sicherungskopie aller vorhandenen Daten, Softwareanwendungen und sonstigen Programme zu erstellen. ESET bzw. die von ESET beauftragten Dritten übernehmen keinerlei Haftung für Datenverluste, Sach- und Vermögensschäden (insb. Schäden an Software und Hardware) oder entgangene Gewinne infolge der Erbringung von Supportleistungen. ESET bzw. die von ESET beauftragten Dritten sichern nicht zu, dass ein bestimmtes Problem auf dem Wege des technischen Support gelöst werden kann, und behalten sich das Recht vor, die Arbeit an einem Problem ggf. einzustellen. ESET behält sich das Recht vor, die Erbringung von Supportleistungen nach eigenem Ermessen vorübergehend auszusetzen, ganz einzustellen oder im konkreten Einzelfall abzulehnen. Für die Bereitstellung des technischen Supports sind unter Umständen Lizenzinformationen, Informationen und andere Daten gemäß der Datenschutzrichtlinie erforderlich.

16. **Übertragung der Lizenz**. Die Software darf von einem Computersystem auf ein anderes übertragen werden, sofern dabei nicht gegen Bestimmungen dieser Vereinbarung verstoßen wird. Sofern in dieser Vereinbarung nicht anderweitig geregelt, ist es dem Endbenutzer gestattet, die Lizenz und alle Rechte aus dieser Vereinbarung an einen anderen Endbenutzer zu übertragen, sofern der Anbieter dem zustimmt und die folgenden Voraussetzungen beachtet werden: (i) Der ursprüngliche Endbenutzer darf keine Kopien der Software zurückbehalten. (ii) Die Übertragung der Rechte muss direkt erfolgen, d. h. vom ursprünglichen Endbenutzer an den neuen Endbenutzer. (iii) Der neue Endbenutzer muss sämtliche Rechte und Pflichten des ursprünglichen Endbenutzers aus dieser Vereinbarung übernehmen. (iv) Der ursprüngliche Endbenutzer muss dem neuen Endbenutzer einen der in Abschnitt 17 genannten Nachweise für die Gültigkeit des Softwarelizenz übereignen.

17. **Gültigkeitsnachweis für die Softwarelizenz.** Der Endbenutzer kann seine Nutzungsrechte an der Software auf eine der folgenden Arten nachweisen: (i) über ein Lizenzzertifikat, das vom Anbieter oder einem von diesem beauftragten Dritten ausgestellt wurde; (ii) über eine schriftliche Lizenzvereinbarung, falls abgeschlossen; (iii) durch Vorlage einer E-Mail des Anbieters mit den Lizenzdaten (Benutzername und Passwort). Zur Überprüfung der Echtheit der Software sind unter Umständen Lizenzinformationen und Identifikationsdaten des Endbenutzers gemäß der Datenschutzrichtlinie erforderlich.

18. **Lizenzvergabe an Behörden und die US-Regierung**. Für die Lizenzvergabe an Behörden, insbesondere an Stellen der US-Regierung, gelten ausschließlich die in dieser Vereinbarung beschriebenen Lizenzrechte und Einschränkungen.

19. **Einhaltung von Handelskontrollen**.

(a) Sie werden die Software nicht direkt oder indirekt an andere Personen exportieren, reexportieren, übertragen oder auf andere Arten verfügbar machen, auf eine Art verwenden oder sich an Handlungen beteiligen, die zu einer Verletzung der Handelskontrollgesetze durch oder zu sonstigen negativen Folgen für ESET oder eines der übergeordneten Unternehmen, die Tochtergesellschaften von ESET oder die Tochtergesellschaften der übergeordneten Unternehmen sowie die Entitäten unter der Kontrolle der übergeordneten Unternehmen („angeschlossene Unternehmen“) führen könnten. Zu diesen Handelskontrollgesetzen zählen:

i. alle Gesetze, die Lizenzierungsanforderungen zum Export, Reexport oder zur Übertragung von Waren, Software, Technologie oder Dienstleistungen kontrollieren, einschränken oder auferlegen und die von Regierungen, Bundesstaaten/Bundesländern oder Regulierungsbehörden in den USA, in Singapur, in Großbritannien, der Europäischen Union oder ihren Mitgliedsstaaten oder in anderen Ländern eingeführt oder übernommen wurden, in denen die Verpflichtungen der Vereinbarung gelten, oder in denen ESET oder eines der angeschlossenen Unternehmen sesshaft oder tätig ist

ii. alle sonstigen wirtschaftlichen, finanziellen oder handelsbezogenen Sanktionen, Einschränkungen, Embargos, Import- oder Exportbeschränkungen, Verbote von Vermögens- oder Assetübertragungen oder von Dienstleistungen sowie alle gleichwertigen Maßnahmen, die von Regierungen, Bundesstaaten/Bundesländern oder Regulierungsbehörden in den USA, in Singapur, in Großbritannien, der Europäischen Union oder ihren Mitgliedsstaaten oder in anderen Ländern eingeführt oder übernommen wurden, in denen die Verpflichtungen der Vereinbarung gelten, oder in denen ESET oder eines der angeschlossenen Unternehmen sesshaft oder tätig ist.

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

b) ESET behält sich das Recht vor, die eigenen Verpflichtungen im Rahmen dieser Bestimmungen fristlos aufzuheben oder die Bestimmungen fristlos aufzukündigen, falls Folgendes eintritt:

i. ESET hat nach eigenem Ermessen festgestellt, dass ein Benutzer die Bestimmungen in Artikel 19 a) dieser Vereinbarung verletzt hat oder vermutlich verletzen wird; oder

ii. ein Endbenutzer und/oder die Software fällt unter die Handelskontrollgesetze, und ESET ist nach eigenem Ermessen der Ansicht, dass die weitere Erfüllung der Verpflichtungen aus der Vereinbarung dazu führen könnte, dass ESET oder ein angeschlossenes Unternehmen die Handelskontrollgesetze verletzt oder dass sonstige negative Folgen zu erwarten sind.

c) Die Vereinbarung ist nicht darauf ausgelegt und darf nicht so interpretiert oder ausgelegt werden, dass eine der Parteien dazu aufgefordert oder verpflichtet wird, auf irgendeine Weise zu handeln oder Handlungen zu unterlassen (oder Handlungen bzw. deren Unterlassung zuzustimmen), die geltende Handelskontrollgesetze verletzt oder gemäß dieser Gesetze unter Strafe steht oder verboten ist.

20. **Kündigungen**. Alle Kündigungen sowie zurückgegebene Software und Dokumentation sind an folgende Adresse zu senden: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic. ESET behält sich das Recht vor, Sie über alle Änderungen an dieser Vereinbarung, der Datenschutzerklärung, der EOL-Richtlinie und der Dokumentation gemäß Art. 22 der Vereinbarung zu informieren. ESET kann Ihnen E-Mails oder In-App-Benachrichtigungen über die Software schicken oder die Kommunikation auf unserer Website veröffentlichen. Sie stimmen zu, rechtliche Mitteilungen von ESET in elektronischer Form zu erhalten, inklusive Mitteilungen zu Änderungen an Bedingungen, Sonderbedingungen oder Datenschutzerklärungen, Benachrichtigungen oder Einladungen zu Vertragsverlängerungen, Kündigungen oder andere rechtliche Mitteilungen. Diese elektronische Kommunikation gilt als schriftlich empfangen, sofern nicht durch geltendes Recht eine andere Kommunikationsform vorgeschrieben ist.

21. **Geltendes Recht, Gerichtsstand**. Diese Vereinbarung unterliegt slowakischem Recht. Endbenutzer und Anbieter vereinbaren, dass gesetzliche Bestimmungen zur Konfliktlösung und UN-Kaufrecht nicht zur Anwendung

kommen. Sie erklären sich ausdrücklich damit einverstanden, dass als Gerichtsstand für alle Streitfälle mit dem Anbieter oder bezüglich Ihrer Verwendung der Software das Amtsgericht Bratislava I, Slowakische Republik vereinbart wird.

22. **Allgemeine Bestimmungen**. Wenn eine der Bestimmungen dieser Vereinbarung ungültig oder uneinklagbar ist, beeinträchtigt dies nicht die Gültigkeit der übrigen Bestimmungen der Vereinbarung. Diese bleiben unter den hier festgelegten Bedingungen gültig und einklagbar. Diese Vereinbarung wird auf Englisch getroffen. Falls eine Übersetzung der Vereinbarung aus Gründen der Annehmlichkeit bereitgestellt wird, sind die Bestimmungen der englischen Version maßgeblich, falls Abweichungen bestehen.

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

Dies ist die vollständige Vereinbarung zwischen dem Anbieter und Ihnen in Bezug auf die Software. Sie ersetzt alle vorigen Darstellungen, Diskussionen, Unternehmungen, Kommunikationen und Werbungen in Bezug auf die Software.

EULAID: EULA-PRODUCT-LG; 3537.0

Datenschutzerklärung

Der Schutz personenbezogener Daten genießt absolute Priorität bei ESET, spol. s r. o. mit eingetragenem Firmensitz in Einsteinova 24, 851 01 Bratislava, Slovak Republic, dem Handelsregistereintrag 3586/B vor dem Bezirksgericht Bratislava I, Rubrik Sro und der eingetragenen Unternehmensnummer 31333532 als Datenverantwortlicher („ESET“ oder „wir“). Wir möchten die Transparenzanforderungen erfüllen, die in der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union gesetzlich festgelegt sind. Aus diesem Grund veröffentlichen wir diese Datenschutzerklärung mit dem ausschließlichen Ziel, unsere Kunden („Endbenutzer“ oder „Sie“) als betroffene Person über die folgenden Themen im Hinblick auf den Schutz personenbezogener Daten zu informieren:

- Rechtliche Grundlage der Verarbeitung personenbezogener Daten
- Datenweitergabe und Vertraulichkeit
- Datensicherheit
- Ihre Rechte als betroffene Person
- Verarbeitung personenbezogener Daten
- Kontaktinformationen.

Verarbeitung personenbezogener Daten

Die von ESET angebotenen und in unserem Produkt implementierten Dienste werden gemäß den Bestimmungen der Endbenutzer-Lizenzvereinbarungangeboten, bedürfen jedoch mitunter zusätzlicher Maßnahmen. Wir möchten Ihnen weitere Details zur Datensammlung im Zusammenhang mit der Bereitstellung unserer Dienste liefern. Wir bieten verschiedene in der EULA und der Dokumentation. Für die Erbringung dieser Dienste erfassen

wir die folgenden Informationen:

- Update- und sonstige Statistiken und Informationen zum Installationsprozess und Ihrem Computer, z. B. die Plattform, auf der unser Produkt installiert wird, oder Informationen zum Betrieb und Funktionsumfang unserer Produkte wie Betriebssystem, Hardwareinformationen, Installations- und Lizenz-IDs, IP-Adresse, MAC-Adresse und Konfigurationseinstellungen des Produkts.
- Einweg-Hashes für Schadsoftware als Teil unseres LiveGrid®-Reputationssystems, das die Wirksamkeit der Sicherheitslösungen verbessert, indem es gescannte Dateien mit Positiv- und Negativlisten in einer Datenbank in der Cloud vergleicht.
- Verdächtige Samples und Metadaten „aus freier Wildbahn“ als Teil unseres ESET LiveGrid®-Reputationssystems, mit denen ESET unmittelbar auf die Anforderungen unserer Kunden reagieren und sie vor den neuesten Bedrohungen schützen kann. Wir benötigen die folgenden Daten von Ihnen:
    - Eingedrungene Schadsoftware, z. B. potenzielle Sample von Viren und anderen Schadprogrammen, sowie verdächtige, problematische, potenziell unerwünschte oder potenziell unsichere Objekte wie ausführbare Dateien oder E-Mail-Nachrichten, die von Ihnen als Spam markiert oder von unserem Produkt markiert wurden;
    - Informationen zu Geräten im lokalen Netzwerk wie Art, Hersteller, Modell und/oder Name des Geräts;
    - Informationen zur Internetnutzung wie IP-Adresse und geografische Informationen, IP-Pakete, URLs und Ethernet-Frames;
    - Absturzabbilder und darin enthaltenen Informationen.

Wir haben kein Interesse daran, Daten außerhalb des genannten Umfangs zu erfassen, allerdings lässt sich dies manchmal nicht vermeiden. Versehentlich erfasste Daten können in der Schadsoftware (ohne Ihr Wissen oder Ihre Zustimmung erfasst) oder als Teil von Dateinamen oder URLs enthalten sein. Es ist nicht unsere Absicht, diese Daten in unseren Systemen oder für die in dieser Datenschutzerklärung genannten Zwecke zu verarbeiten.

- Lizenzinformationen wie die Lizenz-ID und persönliche Daten wie Vor- und Nachname, Adresse und E-Mail-Adresse werden zu Abrechnungszwecken, zur Überprüfung der Echtheit der Lizenz und zur Erbringung unserer Dienste benötigt.
- Kontaktinformationen und andere Daten in Ihren Supportanfragen werden für möglicherweise für die Erbringung von Supportdiensten benötigt. Je nachdem, über welchen Kanal Sie uns kontaktieren, speichern wir möglicherweise Ihre E-Mail-Adresse, Telefonnummer, Lizenzinformationen, Produktdetails und eine Beschreibung Ihres Supportfalls. Möglicherweise werden Sie aufgefordert, uns weitere Informationen bereitzustellen, um die Bearbeitung der Supportanfrage zu erleichtern.

Datenweitergabe und Vertraulichkeit

Wir geben Ihre Daten nicht an Dritte weiter. Allerdings ist ESET ein internationales Unternehmen, das weltweit durch angeschlossene Unternehmen oder Partner im Rahmen unseres Vertriebs-, Dienstleistungs- und Supportnetzwerks vertreten ist. Die von ESET verarbeiteten Informationen zu Lizenzierung, Abrechnung und technischem Support können zur Einhaltung der EULA an angeschlossene Unternehmen oder Partner übertragen und von diesen weitergeleitet werden, beispielsweise zur Bereitstellung von Diensten und zur Erbringung von Supportleistungen.

ESET bevorzugt die Verarbeitung seiner Daten in der Europäischen Union (EU). Je nach Ihrem Standort (Nutzung unserer Produkte und/oder Dienste außerhalb der EU) und/oder der von Ihnen ausgewählten Dienste kann es jedoch erforderlich sein, die Daten in ein Land außerhalb der EU zu übertragen. Im Zusammenhang mit Cloud-Computing nehmen wir beispielsweise Dienste von Drittanbietern in Anspruch. In diesen Fällen wählen wir unsere Dienstanbieter sorgfältig aus und gewährleisten durch vertragliche sowie technische und organisatorische Maßnahmen einen angemessenen Datenschutz. In der Regel werden EU-Standardvertragsklauseln vereinbart, bei

Bedarf ergänzt durch vertragliche Bestimmungen.

In einigen Ländern außerhalb der EU, z. B. dem Vereinigten Königreich und der Schweiz, hat die EU bereits ein vergleichbares Datenschutzniveau beschlossen. Aufgrund dieses vergleichbaren Datenschutzstandards bedarf es zur Übertragung von Daten in diese Länder keiner besonderen Genehmigung oder Vereinbarung.

Rechte betroffener Personen

Die Rechte aller Endbenutzer liegen uns am Herzen, und wir möchten Ihnen versichern, dass ESET allen Endbenutzern (aus einem EU-Land oder anderen Nicht-EU-Ländern) die nachstehenden Rechte garantiert. Zur Ausübung Ihrer Rechte als betroffene Person kontaktieren Sie uns mithilfe des Supportformulars, oder schreiben Sie eine E-Mail an dpo@eset.sk. Zu Identifizierungszwecken bitten wir Sie um die folgenden Informationen: Name, E-Mail-Adresse und, sofern vorhanden, Lizenzschlüssel oder Kundennummer sowie Firmenmitgliedschaft. Bitte senden Sie uns keine anderen personenbezogenen Daten wie beispielweise Ihr Geburtsdatum. Wir weisen zudem darauf hin, dass wir zur Abwicklung Ihrer Anfrage sowie zu Identifizierungszwecken Ihre personenbezogenen Daten verarbeiten.

Recht auf Widerruf der Zustimmung: Das Recht auf Widerruf der Zustimmung gilt nur im Falle einer Verarbeitung auf Grundlage einer Zustimmung. Wenn wir Ihre personenbezogenen Daten auf Grundlage Ihrer Zustimmung verarbeiten, können Sie Ihre Zustimmung jederzeit und ohne Angabe von Gründen widerrufen. Der Widerruf der Zustimmung gilt nur für die Zukunft und hat keinen Einfluss auf die Rechtmäßigkeit der vor dem Widerruf verarbeiteten Daten.

Recht auf Einspruch: Das Recht auf Einspruch gilt im Falle einer Verarbeitung auf Grundlage eines berechtigten Interesses von ESET oder eines Dritten. Wenn wir Ihre personenbezogenen Daten verarbeiten, um ein legitimes Interesse zu schützen, haben Sie als betroffene Person jederzeit das Recht, dem von uns angegebenen legitimen Interesse und der Verarbeitung Ihrer personenbezogenen Daten zu widersprechen. Ihr Einspruch gilt nur für die Zukunft und hat keinen Einfluss auf die Rechtmäßigkeit der vor dem Einspruch verarbeiteten Daten. Sofern wir Ihre personenbezogenen Daten zu Direktwerbungszwecken verarbeiten, müssen Sie Ihren Einspruch nicht begründen. Dies gilt auch für die Profilerstellung, insofern diese mit einer solchen Direktvermarktung in Zusammenhang steht. In allen anderen Fällen bitten wir Sie, uns die Beschwerde bezüglich des legitimen Interesses von ESET an der Verarbeitung Ihrer personenbezogenen Daten unverzüglich zukommen zu lassen.

Beachten Sie, dass wir in manchen Fällen trotz des Widerrufs Ihrer Zustimmung berechtigt sind, Ihre personenbezogenen Daten auf einer anderen rechtlichen Grundlage weiter zu verarbeiten, z. B. zur Erfüllung eines Vertrags.

Recht auf Auskunft: Als betroffene Person haben Sie das Recht, jederzeit kostenlos Informationen über Ihre bei ESET gespeicherten Daten zu verlangen.

Recht auf Berichtigung: Sollten wir versehentlich falsche personenbezogene Daten über Sie verarbeiten, haben Sie das Recht, diese berichtigen zu lassen.

Recht auf Löschung und auf Einschränkung der Verarbeitung: Als betroffene Person haben Sie das Recht, die Löschung Ihrer personenbezogenen Daten oder die Einschränkung der Verarbeitung dieser zu verlangen. Wenn wir Ihre personenbezogenen Daten verarbeiten, z. B. mit Ihrer Zustimmung, Sie diese Zustimmung widerrufen und keine andere gesetzliche Grundlage wie beispielsweise ein Vertrag vorliegt, löschen wir Ihre personenbezogenen Daten umgehend. Ihre personenbezogenen Daten werden auch gelöscht, sobald sie zum Ende der Aufbewahrungsdauer zu den genannten Zwecken nicht mehr benötigt werden.

Wenn wir Ihre personenbezogenen Daten ausschließlich für Direktmarketing verwenden und Sie Ihre Zustimmung widerrufen oder Einspruch gegen das berechtigte Interesse von ESET erheben, schränken wir die Verarbeitung

Ihrer personenbezogenen Daten soweit ein, dass wir Ihre Kontaktdaten in unsere interne Negativliste aufnehmen, um derartige unerwünschte Kontaktaufnahmen zu vermeiden. Andernfalls werden Ihre personenbezogenen Daten gelöscht.

Beachten Sie, dass wir unter Umständen verpflichtet sind, Ihre Daten bis zum Ablauf der von Gesetzgeber und Aufsichtsbehörden vorgegebenen Aufbewahrungsdauer zu speichern. Aufbewahrungspflichten und Aufbewahrungsdauer können sich auch aus der slowakischen Gesetzgebung ergeben. Anschließend werden die entsprechenden Daten routinemäßig gelöscht.

Das Recht auf Übertragbarkeit der Daten. Als betroffene Person stellen wir Ihnen gerne die von ESET verarbeiteten personenbezogenen Daten im XLS-Format zur Verfügung.

Recht auf Beschwerde: Betroffene Personen haben das Recht, jederzeit Beschwerde bei einer Aufsichtsbehörde einzulegen. ESET unterliegt slowakischem Recht und ist als Teil der Europäischen Union an die Datenschutzgesetze gebunden. Die zuständige Aufsichtsbehörde ist das Büro für den Schutz personenbezogener Daten der Slowakischen Republik mit Sitz in Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Kontaktinformationen

Falls Sie Ihre Rechte als betroffene Person in Anspruch nehmen möchten oder Fragen oder Bedenken haben, schicken Sie uns eine Nachricht an:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk