ESET MAIL SECURITY

FÜR MICROSOFT EXCHANGE SERVER

Installations- und Benutzerhandbuch

Microsoft® Windows® Server 2003 / 2008 / 2008 R2 / 2012 / 2012 R2

Klicken Sie hier, um die neueste Version dieses Dokuments herunterzuladen

ENJOY SAFER TECHNOLOGY™

ESET **MAIL SECURITY**

Support: www.eset.com/support

Versionsstand 15/03/2016

Inhalt

Inhalt

1. Einführung

ESET Mail Security 6 für Microsoft Exchange Server ist eine integrierte Lösung, die Ihre Postfächer vor Schadsoftware schützt, darunter mit Würmern oder Trojanern infizierte E-Mail-Anlagen, mit bösartigen Skripten versehene Dokumente sowie Phishing-Mails und Spam. ESET Mail Security bietet drei Schutzarten: Virenschutz, Spam-Schutz und benutzerdefineirte Regeln. ESET Mail Security erkennt Schadsoftware auf dem E-Mail-Server, bevor sie den Posteingang des E-Mail-Empfängers erreicht.

ESET Mail Security unterstützt Microsoft Exchange Server ab Version 2003 und Microsoft Exchange Server in einer Cluster-Umgebung. In neueren Versionen (ab Microsoft Exchange Server 2003) werden auch bestimmte Rollen unterstützt (Postfach, Hub, Edge). Mithilfe von ESET Remote Administrator können Sie ESET Mail Security in größeren Netzwerken zentral verwalten.

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

1.1 Was ändert sich mit Version 6?

- E-Mail-Quarantäne-Manager - Administratoren können Objekte in diesem Speicherbereich inspizieren und entweder löschen oder freigeben. Dieses Feature vereinfacht die Verwaltung der E-Mails, die vom Transport-Agenten in die Quarantäne verschoben wurden.
- Web-Oberfläche für die E-Mail-Quarantäne - eine webbasierte Alternative zum E-Mail-Quarantäne-Manager.
- Spam-Schutz - Diese wichtige Komponente wurde grundlegend überarbeitet und verwendet nun ein brandneues preisgekröntes Modul mit verbesserter Leistung.
- On-Demand-Datenbankprüfung - Dieses Modul 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 Prüfungen durch, um die Leistung zu verbessern.
- Regeln - Über den Menübefehl Regeln können Administratoren manuell Filterbedingungen für E-Mails definieren und Aktionen damit verknüpfen. Die Regeln in der neuesten Version von <%PN%> wurden neu gestaltet, um Benutzern noch mehr Möglichkeiten mit maximaler Flexibilität zu bieten.
- ESET-Cluster - Funktioniert ähnlich wie ESET File Security 6 für Microsoft Windows Server. Arbeitsstationen werden zu Knoten hinzugefügt, um die Verwaltung zusätzlich zu automatisieren, indem eine Konfigurationsrichtlinie auf alle Elemente des Clusters verteilt werden. Die eigentliche Erstellung von Clustern erfolgt über den installierten Knoten, der anschließend sämtliche Knoten aus der Ferne installieren und starten kann. ESET-Serverprodukte kommunizieren miteinander, tauschen Daten wie z. B. Konfigurationsdaten und Benachrichtigungen aus und synchronisieren die für den ordnungsgemäßen Betrieb einer Gruppe von Produktinstanzen erforderlichen Daten. Auf diese Weise wird eine einheitliche Konfiguration des Produkts im gesamten Cluster gewährleistet. ESET Mail Security unterstützt Windows-Failover-Cluster und Network Load Balancing(NLB)-Cluster. Zusätzliche können Sie manuell ESET-Clustermitglieder hinzufügen, ohne dass ein bestimmtes Windows-Cluster erforderlich ist. ESET-Cluster funktionieren in Domänen- und Arbeitsgruppenumgebungen.
- Speicher-Scan - Scannt alle freigegebenen Dateien auf dem lokalen Server. Mit dieser Option können Sie bequem nur Benutzerdaten scannen, die auf dem Dateiserver gespeichert sind.
- Komponentenbasierte Installation - Wählen Sie aus, welche Komponenten Sie hinzufügen oder entfernen möchten.
- Ausgeschlossene Prozesse - Die Prozesse werden nur von der Virenschutz-Echtzeitprüfung ausgeschlossen. Aufgrund der entscheidenden Rolle wichtiger Server (Anwendungsserver, Speicherserver usw.) müssen unbedingt regelmäßig Sicherungen angelegt werden, um die Server im Fall einer gravierenden Störung wiederherstellen zu können. Zur Verbesserung von Sicherungsgeschwindigkeit, Prozessintegrität und Dienstverfügbarkeit werden bei Sicherungen bestimmte Techniken verwendet, die zu Konflikten mit Virenschutzlösungen 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 Virenschutzsoftware. 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.

- ESET Log Collector - Sammelt automatisch Informationen wie z. B. Angaben zur Konfiguration von ESET Mail Security sowie zahlreiche Logs. Mit dem ESET Log Collector können Sie ganz einfach die Diagnoseinformationen zusammenstellen, die unsere ESET-Techniker benötigen, um möglichst schnelle Hilfe beim Beheben eines Problems bieten zu können.
- eShell (ESET Shell) – eShell 2.0 ist nun in ESET Mail Security verfügbar. eShell ist eine Befehlszeilenschnittstelle, die fortgeschrittenen Benutzern und Administratoren noch umfassendere Optionen zur Verwaltung der ESET-Serverprodukte bietet.
- Hyper-V-Scan – Eine neue Technologie, mit der Virtual Machine (VM)-Datenträger auf einem Microsoft Hyper-V-Server gescannt werden können, ohne dass hierzu ein „Agent“ auf der VM erforderlich ist.
- Bessere Integration mit ESET Remote Administrator inklusive der Möglichkeit zur Planung von On-Demand-Scans.

1.2 Hilfeseiten

Lieber Kunde, wir freuen uns, Sie bei ESET Mail Security begrüßen zu dürfen. Dieses Handbuch soll Sie dabei unterstützen, ESET Mail Security optimal einzusetzen.

Die Themen in diesem Handbuch sind in Kapiteln und Unterkapiteln angeordnet. Im **Inhalt** der Hilfeseiten können Sie schnell nach einer bestimmten Information suchen. Alternativ können Sie den **Index** nach Schlüsselwörtern durchsuchen oder über die Funktion **Suchen** eine Volltextsuche ausführen.

Weitere Informationen zu einem bestimmten Fenster im Programm können Sie jederzeit durch Drücken der Taste F1 im betreffenden Fenster anzeigen. Die Hilfeseite zu dem aktuell angezeigten Fenster wird angezeigt.

Sie können in ESET Mail Security mit Schlüsselwörtern oder durch Eingabe von Wörtern und Ausdrücken nach Themen im Benutzerhandbuch suchen. Der Unterschied zwischen diesen beiden Methoden ist, dass ein Stichwort logisch mit einer Hilfeseite verknüpft sein kann, ohne dass das Stichwort selbst im Text vorkommt. Bei der Suche nach Wörtern und Formulierungen wird der gesamte Inhalt aller Seiten durchsucht, und es werden nur diejenigen Seiten angezeigt, die das gesuchte Wort bzw. die gesuchte Formulierung im Text enthalten.

1.3 Verwendete Prüfmethoden

Für die Prüfung von E-Mails stehen die folgenden drei Methoden zur Verfügung:

- Postfach-Datenbankschutz - Auch als Postfachprüfung per VSAPI bekannt. Dieser Schutz ist nur für Microsoft Exchange Server 2010, 2007 und 2003 verfügbar, wenn diese in der Rolle als Postfachserver (Microsoft Exchange 2010 und 2007) bzw. Backend-Server (Microsoft Exchange 2003) ausgeführt werden. 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).
- E-Mail-Transportschutz - Auch als E-Mail-Filterung auf SMTP-Serverebene bekannt. Dieser Schutz wird vom Transportagenten bereitgestellt und ist nur für Microsoft Exchange Server 2007 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).
- On-Demand-Datenbankprüfung - ermöglicht die Planung und Ausführung von Prüfungen für Exchange-Postfächer. Dieses Feature ist nur für Microsoft Exchange Server 2007 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). Unter Rollen in Exchange Server 2013 finden Sie weitere Informationen zu Rollen in Exchange 2013.

1.3.1 Schutz für E-Mail-Datenbank

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, z. B. in einem E-Mail-Programm (E-Mails werden immer mit der neuesten Version der Signaturdatenbank geprüft)
- Im Hintergrund, wenn Microsoft Exchange Server nicht ausgelastet ist
- Proaktiv (abhängig vom internen Algorithmus von Microsoft Exchange Server)

Derzeit wird die VSAPI-Schnittstelle für den Virenschutz und den regelbasierten Schutz verwendet.

1.3.2 Mail-Transportschutz

Die Prüfung auf dem SMTP-Server wird mit einem speziellen Plug-In durchgeführt. In Microsoft Exchange Server 2000 und 2003 ist das entsprechende Plug-In (Ereignissenke) als Teil der Internetinformationsdienste (IIS) auf dem SMTP-Server registriert. In Microsoft Exchange Server 2007/2010 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.

1.3.3 On-Demand-Datenbankprüfung

Eine vollständige Prüfung der E-Mail-Datenbank kann in großen Umgebungen eine unerwünschte Systemlast verursachen. Daher können Sie auswählen, welche Datenbanken und welche enthaltenen Postfächer geprüft werden. Sie können die Ziele weiter eingrenzen, indem Sie einen Zeitpunkt für die zu prüfenden E-Mails auswählen, um die Auswirkungen auf die Systemressourcen des Servers weiter zu senken.

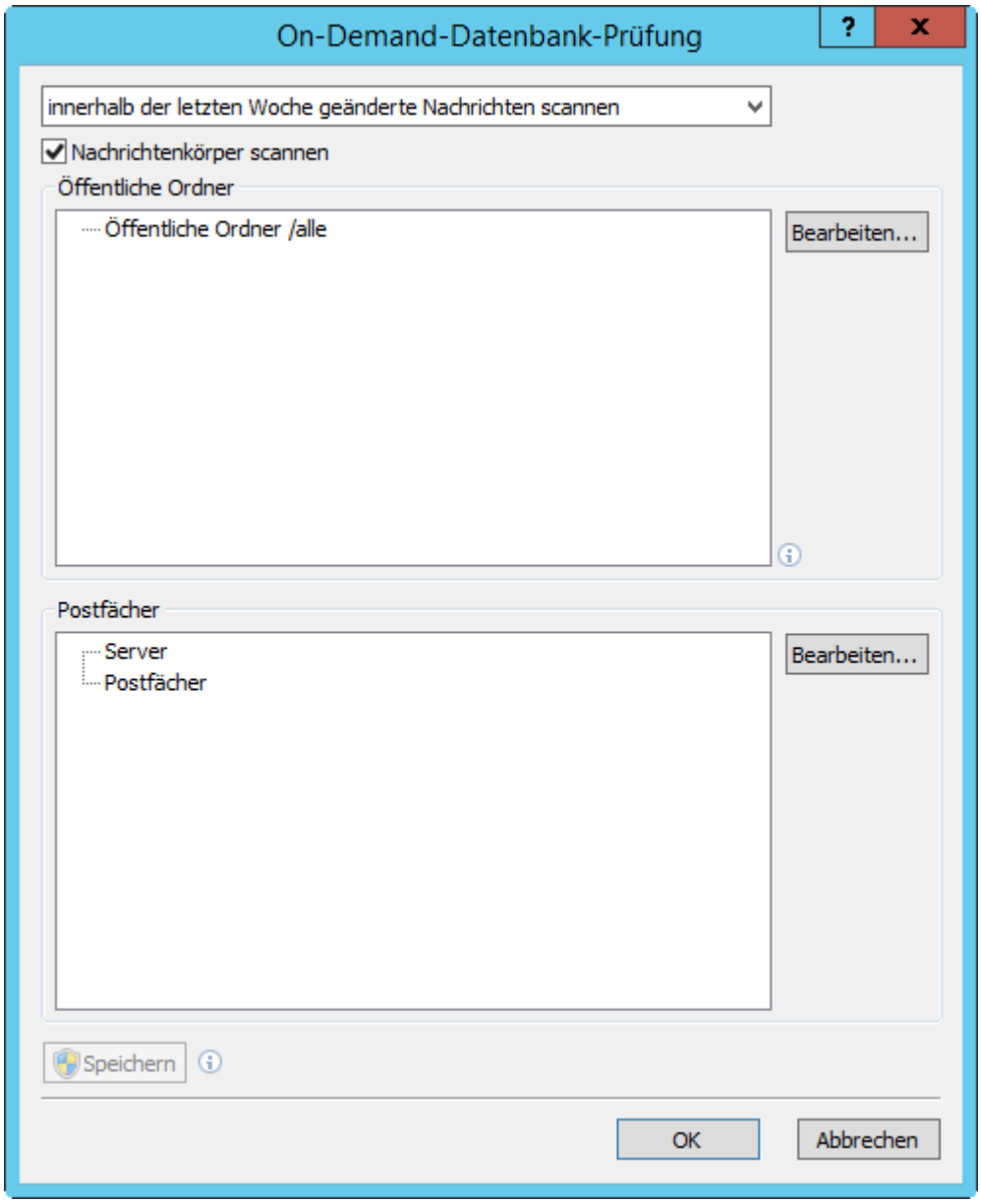
Die folgenden Elementtypen werden in öffentlichen Ordnern und in Benutzer-Postfächern geprüft:

- E-Mails
- Beiträge
- Kalendereinträge (Meetings/Besprechungen)
- Tasks
- Kontakte
- Journal

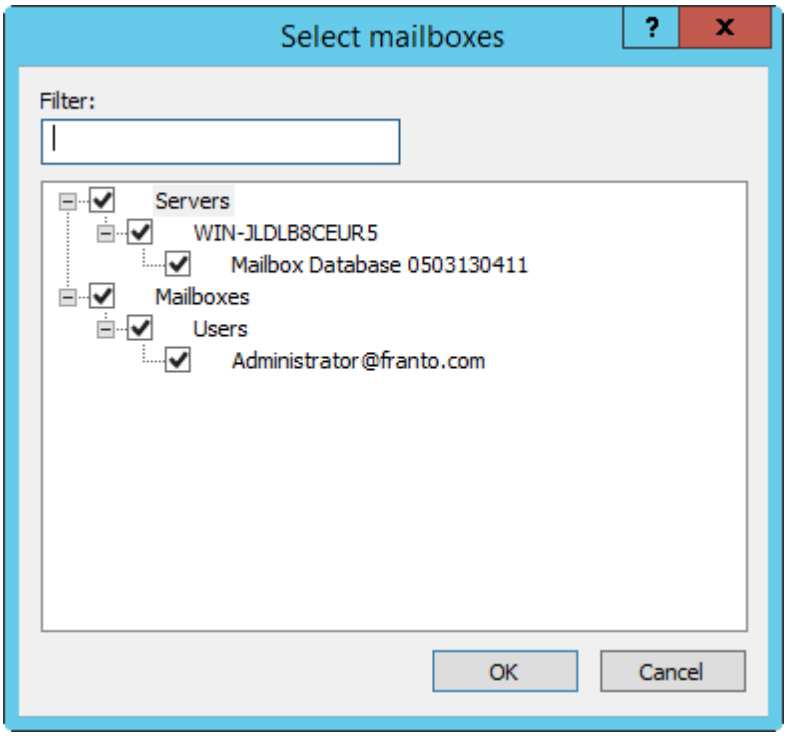
In der Dropdownliste können Sie anhand eines Zeitstempels auswählen, welche E-Mails geprüft werden sollen. Wählen Sie z. B. alle E-Mails aus, die in der letzten Woche verändert wurden. Alternativ können Sie bei Bedarf auch alle Nachrichten prüfen.

Klicken Sie auf das Kontrollkästchen neben **Nachrichtentext prüfen**, um die Überprüfung der Nachrichtentexte zu aktivieren bzw. zu deaktivieren.

Klicken Sie auf **Bearbeiten**, um auszuwählen, welcher öffentliche Ordner geprüft werden soll.


On-Demand-Datenbank-Prüfung
innerhalb der letzten Woche geänderte Nachrichten scannen
Nachrichtenkörper scannen
Öffentliche Ordner
Öffentliche Ordner /alle
Bearbeiten...
Postfächer
Server
Postfächer
Bearbeiten...
Speichern
OK
Abbrechen

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 Scan-Ziele und Parameter im On-Demand-Scan-Profil zu speichern.

1.4 Schutzarten

Es gibt drei Schutzarten:

- Virenschutz
- Spam-Schutz
- Anwendung benutzerdefinierter Regeln

1.4.1 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.

1.4.2 Spam-Schutz

Spamschutzlösungen verwenden verschiedene Technologien (RBL, DNSBL, Fingerprint-Datenbanken, Reputations-Prüfung, Inhaltsanalyse, Bayesscher Filter, Regeln, manuell geführte Whitelists/Blacklists usw.), um E-Mail-Bedrohungen wirksam zu erkennen. Das Spamschutz-Modul berechnet einen Wahrscheinlichkeitswert in Form einer Prozentzahl von 0 bis 100 für jede geprüfte E-Mail.

kann außerdem die Greylisting-Methode (standardmäßig deaktiviert) für den Spamfilter verwenden. Diese Methode basiert auf der Spezifikation RFC 821, wonach aufgrund der prinzipiellen Unzuverlässigkeit des Sendeprotokolls SMTP jeder MTA (Message Transfer Agent) nach einem temporären Fehler beim Versenden der E-Mail wiederholte Zustellversuche unternehmen sollte. Viele Spam-E-Mails werden nur einmal an automatisch erstellte Empfängerlisten zugestellt. Beim Greylisting wird ein Kontrollwert (Hashwert) aus der E-Mail-Adresse des Absenders, der E-Mail-Adresse des Empfängers und der IP-Adresse des absendenden MTA berechnet. Wenn der Server den aus diesen drei Komponenten errechneten Kontrollwert nicht in seiner Datenbank findet, verweigert er die Annahme der E-Mail und meldet einen temporären Fehler (z. B. 451). Ein rechtmäßiger Server unternimmt nach

einer einstellbaren Zeitspanne einen erneuten Zustellversuch. Beim zweiten Versuch wird der Kontrollwert aus den drei Komponenten in einer Datenbank für geprüfte E-Mail-Adressen gespeichert, sodass ab dann E-Mails mit den entsprechenden Merkmalen zugestellt werden können.

1.4.3 Anwendung benutzerdefinierter Regeln

Sowohl die VSAPI-Prüfung als auch die Prüfung mit einem Transport-Agenten bietet Schutz auf Basis von Regeln. Mit der ESET Mail Security-Benutzeroberfläche können Sie 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 ODER verwendet, d. h., das Programm führt die erste Regel aus, deren Bedingungen erfüllt sind.

Bei der Prüfung wird zuerst die Greylisting-Technik angewendet, sofern sie aktiviert ist. Anschließend werden die folgenden Techniken angewendet: die Prüfung nach benutzerdefinierten Regeln, dann eine Virenprüfung und schließlich eine Spam-Prüfung.

1.5 Benutzeroberfläche

Die intuitive Benutzeroberfläche von ESET Mail Security ist auf hohe Benutzerfreundlichkeit ausgelegt. Sie ermöglicht dem Benutzer schnell und unkompliziert Zugang zu den Hauptfunktionen des Programms.

Zusätzlich zur allgemeinen Benutzeroberfläche können Sie an jeder Stelle des Programms durch Drücken auf F5 das Fenster **Erweiterte Einstellungen** öffnen.

Über das Fenster der erweiterten Einstellungen können Sie persönliche Einstellungen vornehmen und Funktionen konfigurieren. Das Menü auf der linken Seite enthält folgende Kategorien: **Virenschutz**, **Computer**, **Update**, **Web und E-Mail**, **Medienkontrolle**, **Tools** und **Benutzeroberfläche**. Einige der Hauptkategorien enthalten auch Unterkategorien. Wenn Sie im Menü links auf einen Eintrag klicken (Kategorie oder Unterkategorie), wird rechts die entsprechende Einstellung für das ausgewählte Element angezeigt.

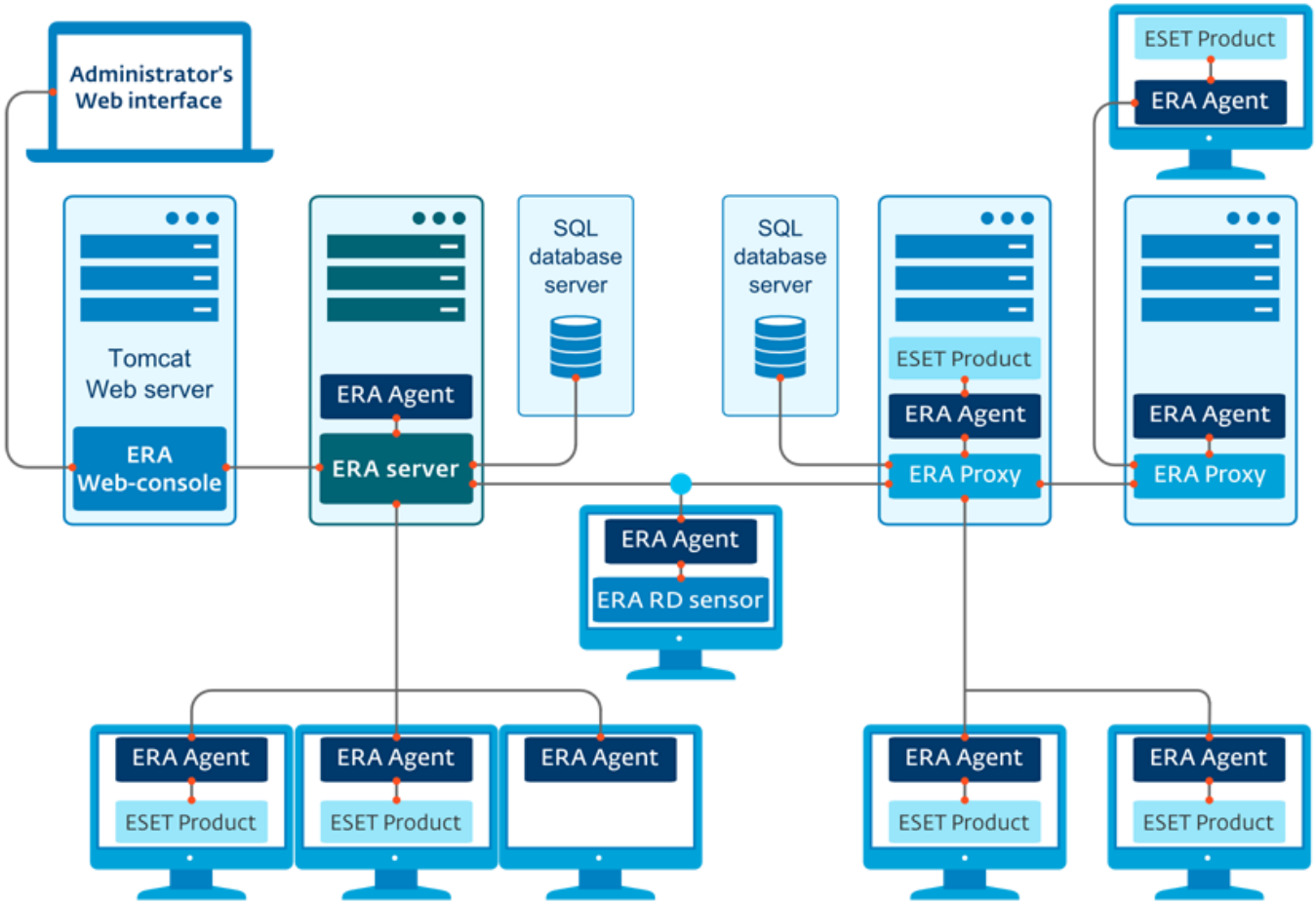
Weitere Informationen zur grafischen Benutzeroberfläche finden Sie hier.

1.6 Verwaltung über ESET Remote Administrator

Mit (ERA) können Sie ESET-Produkte in einer Netzwerkumgebung von einem zentralen Standort aus verwalten. Das Task-Management-System von ESET Remote Administrator ermöglicht das Installieren von ESET-Sicherheitslösungen auf Remotecomputern und eine schnelle Reaktion auf neue Probleme und Bedrohungen. ESET Remote Administrator bietet keinen Schutz vor Schadcode selbst, sondern stützt sich hierzu auf die auf jedem Client installierte ESET-Sicherheitslösung.

ESET-Sicherheitslösungen unterstützen Netzwerke, die verschiedene Plattformtypen umfassen. Ihr Netzwerk kann aus einer Kombination aktueller Microsoft-, Linux- und OS X-Betriebssysteme und Betriebssysteme für mobile Geräte (Mobiltelefone und Tablets) bestehen.

In der nachstehenden Abbildung sehen Sie eine Beispielarchitektur eines Netzwerks, das durch ESET-Sicherheitslösungen geschützt ist, die über ERA verwaltet werden:



HINWEIS: Weitere Informationen zu ERA finden Sie in der ESET Remote Administrator-Onlinehilfe.

1.6.1 ERA-Server

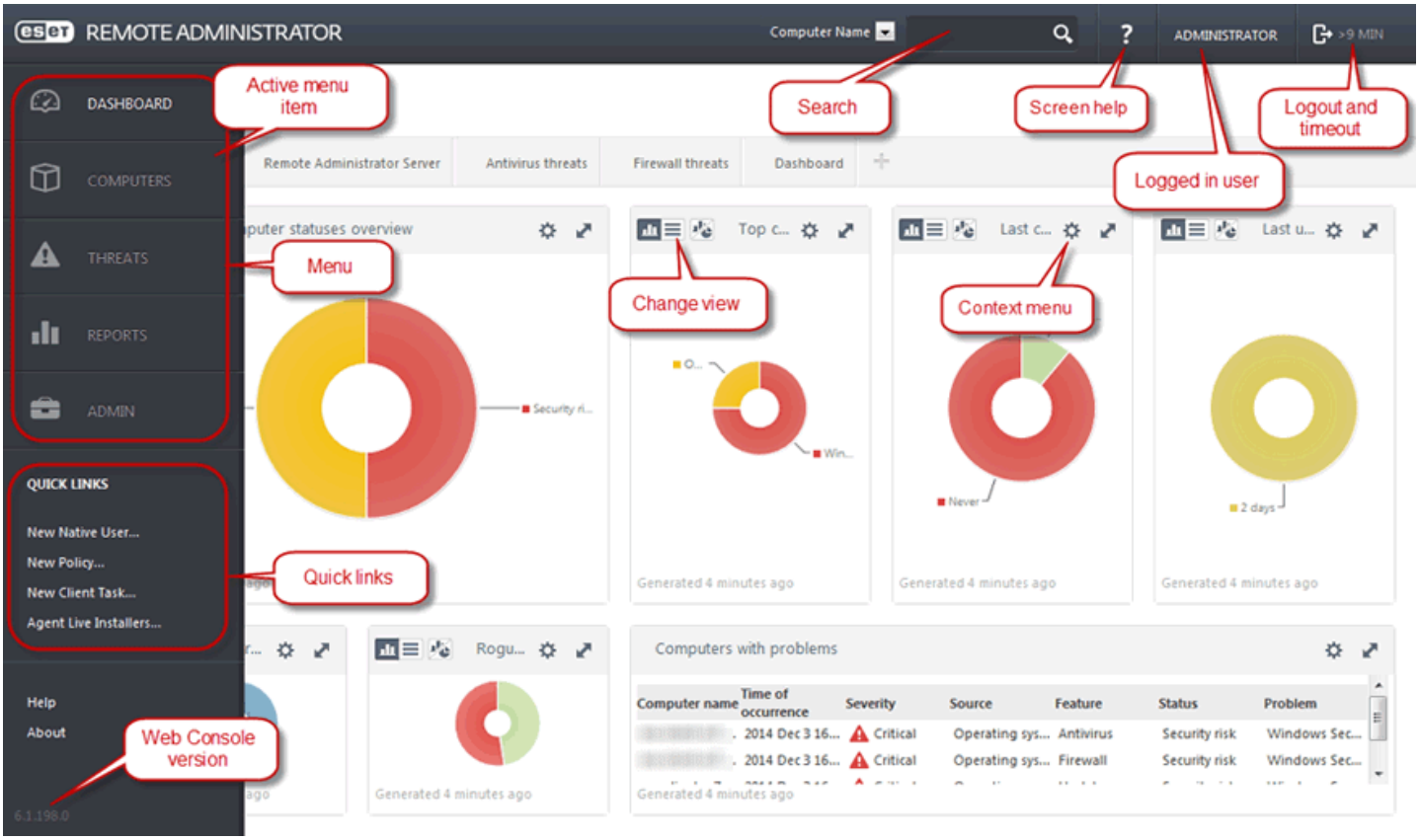
ESET Remote Administrator Server ist eine Hauptkomponente von ESET Remote Administrator. Diese Komponente verarbeitet alle Daten von den Clients, die über den ERA-Agenten mit dem Server kommunizieren. Der ESET-Agent erleichtert die Kommunikation zwischen Client und Server. Daten wie Client-Logs, Konfigurationseinstellungen oder Agentreplikationen werden in einer Datenbank gespeichert. Zur ordnungsgemäßen Verarbeitung der Daten benötigt der ERA-Server eine stabile Verbindung zum Datenbankserver. Zum Zwecke der Leistungsoptimierung wird empfohlen, den ERA-Server und die Datenbank auf separaten Servern zu installieren. Der Computer, auf dem der ERA-Server installiert wird, muss so konfiguriert sein, dass alle Agent-/Proxy-/RD Sensor-Verbindungen, welche anhand von Zertifikaten überprüft werden, akzeptiert werden. Nachdem der ERA-Server installiert ist, können Sie die ERA-Web-Konsole öffnen, die eine Verbindung zum ERA-Server herstellt (siehe Abbildung). In der Web-Konsole können Sie alle Vorgänge des ERA-Servers zur Verwaltung der ESET-Sicherheitslösungen in Ihrem Netzwerk

ausführen.

1.6.2 Web-Konsole

Die ERA-Web-Konsole ist eine webbasierte Benutzeroberfläche, in der Sie Daten vom ERA-Server anzeigen und die ESET-Sicherheitslösungen in Ihrer Umgebung verwalten können. Der Zugriff auf die Web-Konsole erfolgt über einen Browser. Sie bietet eine Übersicht über den Status der Clients im Netzwerk und kann zur Remote-Bereitstellung von ESET-Lösungen auf unverwalteten Computern verwendet werden. Wenn Sie den Zugriff über Internet auf den Webserver zulassen, können Sie ESET Remote Administrator von nahezu jedem beliebigen Standort und Gerät mit aktiver Internetverbindung aus verwenden.

Dies ist das Dashboard der Web-Konsole:



In der oberen Leiste der Web-Konsole befindet sich das Tool **Schnellsuche**. Wählen Sie im Dropdownmenü entweder **Computername**, **IPv4-/IPv6-Adresse** oder **Bedrohungsname** aus und geben Sie im Textfeld eine Zeichenfolge für die Suche ein. Klicken Sie dann auf das Lupensymbol oder drücken Sie die **Eingabetaste**, um die Suche auszuführen. Sie werden zum Abschnitt "Gruppen" weitergeleitet. Hier werden die Suchergebnisse angezeigt (ein Client bzw. eine Liste mehrerer Clients). Alle Clients werden über die Web-Konsole verwaltet. Der Zugriff auf die Web-Konsole ist über die meisten gängigen Geräte und Browser möglich.

HINWEIS: Weitere Informationen finden Sie in der ESET Remote Administrator-Onlinehilfe.

1.6.3 Agent

Der ERA-Agent ist eine wichtige Komponente von ESET Remote Administrator. Der Agent dient der Kommunikation zwischen einem ESET-Produkt auf einem Clientcomputer (z. B. ESET Endpoint Security für Windows) und dem ERA-Server. Dank dieser Kommunikation können Sie ESET-Produkte auf Remoteclients von einem zentralen Standort aus verwalten. Der Agent erfasst Informationen vom Client und sendet sie an den Server. Wenn der Server dem Client einen Task übermittelt, wird dieser Task an den Agenten gesendet, der ihn an den Client weitergibt. Der gesamte Netzwerkverkehr findet zwischen dem Agenten und dem oberen Teil des ERA-Netzwerks (Server und Proxy) statt.

HINWEIS: Weitere Informationen finden Sie in der ESET Remote Administrator-Onlinehilfe.

Der ESET-Agent stellt mit einer der folgenden drei Methoden eine Verbindung zum Server her:

1. Der Agent des Client ist direkt mit dem Server verbunden.
2. Der Agent des Client ist über einen Proxy mit dem Server verbunden.
3. Der Agent des Client ist über mehrere Proxys mit dem Server verbunden.

Der ESET-Agent kommuniziert mit ESET-Lösungen auf einem Client, sammelt Daten aus Programmen auf diesem Client und leitet vom Server erhaltene Konfigurationsdaten an den Client weiter.

HINWEIS: Der ESET-Proxy verfügt über einen eigenen Agenten, der alle Kommunikationstasks zwischen Clients, anderen Proxys und dem Server abwickelt.

1.6.4 RD Sensor

Rogue Detection Sensor (RD Sensor) ist ein Tool für die Suche nach Computern im Netzwerk. RD Sensor ist Bestandteil von ESET Remote Administrator und dient der Erkennung von Computern im Netzwerk. Mit dieser Komponente können neue Computer bequem ohne manuelles Suchen zu ESET Remote Administrator hinzugefügt werden. Alle im Netzwerk gefundenen Computer werden in der Web-Konsole angezeigt. Anschließend können Sie Aktionen an den einzelnen Clientcomputern durchführen.

RD Sensor ist ein passives Überwachungstool, das Computer erkennt, die im Netzwerk vorhanden sind, und Informationen über diese Computer an den ERA-Server sendet. Der ERA-Server bewertet dann, ob die im Netzwerk gefundenen PCs dem ERA-Server unbekannt oder ob sie bereits verwaltet sind.

HINWEIS: Weitere Informationen finden Sie in der ESET Remote Administrator-Onlinehilfe.

1.6.5 Proxy

Der ERA-Proxy ist ein weiterer Bestandteil von ESET Remote Administrator und erfüllt zwei Aufgaben. In mittelgroßen Netzwerken oder Unternehmensnetzwerken mit vielen Clients (10.000 Clients oder mehr) können Sie mit einem ERA-Proxy die Last zwischen mehreren ERA-Proxys verteilen und so den primären ERA-Server entlasten. Sie können den ERA-Proxy außerdem für Verbindungen zu entfernt liegenden Büros mit schwacher Bandbreite einsetzen. In diesem Fall wird der ERA-Agent auf den Clients nicht direkt mit dem ERA-Hauptserver verbunden, sondern kommuniziert über den ERA-Proxy, der sich im gleichen lokalen Netzwerk wie der Client befindet. Dies reduziert die Last auf der Netzwerkverbindung zum Zweigstellenbüro. Der ERA-Proxy nimmt Verbindungen von allen lokalen ERA-Agenten an, fasst die Daten zusammen und lädt sie zum ERA-Hauptserver (oder zu einem anderen ERA-Proxy) hoch. Auf diese Weise ist im Netzwerk Platz für mehr Clients, ohne dass die Leistungsfähigkeit des Netzwerks und der Datenbankabfragen beeinträchtigt wird.

Je nach Netzwerkkonfiguration kann ein ERA-Proxy eine Verbindung zu einem anderen ERA-Proxy und anschließend zum ERA-Server herstellen.

Damit der ERA-Proxy ordnungsgemäß funktioniert, muss auf dem Hostcomputer, auf dem sich der ERA-Proxy befindet, ein ESET-Agent installiert sein, und er muss mit der oberen Ebene (entweder dem ERA-Server oder, sofern vorhanden, dem oberen ERA-Proxy) des Netzwerks verbunden sein.

HINWEIS: Beispiele für Bereitstellungsszenarien mit einem ERA-Proxy finden Sie in der ESET Remote Administrator-Onlinehilfe.

2. Systemanforderungen

Unterstützte Betriebssysteme:

- Microsoft Windows Server 2003 SP2 (x86 und x64)
- Microsoft Windows Server 2003 R2 (x86 und x64)
- Microsoft Windows Server 2008 (x86 und x64)
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Small Business Server 2003 (x86)
- Microsoft Windows Small Business Server 2003 R2 (x86)
- Microsoft Windows Small Business Server 2008 (x64)
- Microsoft Windows Small Business Server 2011 (x64)

HINWEIS: Das älteste unterstützte Betriebssystem ist Microsoft Windows Server 2003 SP2.

Unterstützte Versionen von Microsoft Exchange Server:

- Microsoft Exchange Server 2003 SP1, SP2
- Microsoft Exchange Server 2007 SP1, SP2, SP3
- Microsoft Exchange Server 2010 SP1, SP2, SP3
- Microsoft Exchange Server 2013 CU2, CU3, CU4 (SP1), CU5, CU6, CU7, CU8
- Microsoft Exchange Server 2016

Die Hardware-Anforderungen sind abhängig von der verwendeten Version des Betriebssystems. Beachten Sie die weiteren Informationen zu Hardware-Anforderungen in der Produktdokumentation zu Microsoft Windows Server.

3. Installation

Nach dem Kauf von ESET Mail Security können Sie das Installationsprogramm von der ESET-Website (www.eset.com) als .msi-Dateipaket herunterladen.

Hinweis: Das Installationsprogramm muss unter dem integrierten Administratorkonto ausgeführt werden. Andere Benutzer haben nicht die erforderlichen Zugriffsrechte (auch dann nicht, wenn sie der Gruppe „Administratoren“ angehören). Verwenden Sie also immer das integrierte Administratorkonto „Administrator“, da die Installation ansonsten nicht abgeschlossen werden kann.

Zum Starten des Installationsprogramms gibt es zwei Möglichkeiten:

- Sie können sich lokal mit dem Konto „Administrator“ anmelden und das Installationsprogramm dann einfach wie gewohnt starten.
- Wenn Sie mit einem anderen Konto angemeldet sind, öffnen Sie über den Befehl „Ausführen als“ eine Kommandozeilensitzung (cmd) unter der Identität des Benutzers „Administrator“. Geben Sie dann den Befehl zum Ausführen des Installationsprogramms ein, z. B. emsx_nt64_ENU.msi ein. Ersetzen Sie dabei emsx_nt64_ENU.msi durch den Dateinamen des heruntergeladenen MSI-Installationspakets.

Nachdem Sie das Installationsprogramm gestartet und der Endbenutzer-Lizenzvereinbarung (EULA) zugestimmt haben, führt der Installationsassistent Sie durch die Einrichtung. Wenn Sie die Lizenzvereinbarung nicht annehmen, wird der Assistent nicht fortgesetzt.

Vollständig
Dies ist die empfohlene Installationsart. Mit dieser Option werden alle Funktionen von ESET Mail Security installiert. Wenn Sie diese Installationsart auswählen, müssen Sie danach nur den Installationsordner für das Produkt angeben oder die vordefinierten Installationsordner übernehmen (empfohlen). Das Installationsprogramm installiert dann automatisch alle Programmfunktionen.

Benutzerdefiniert
Bei der benutzerdefinierten Installation können Sie auswählen, welche Programmfunktionen von ESET Mail Security auf dem System installiert werden. Eine Liste der Funktionen/Komponenten wird angezeigt, aus der Sie die Inhalte der Installation auswählen können.

Sie können die Installation von ESET Mail Security statt mit dem Assistenten auch unbeaufsichtigt über die Befehlszeile ausführen. Bei dieser Installationsart ist keine Benutzerinteraktion wie im Installationsassistenten erforderlich. Dies bietet sich zur automatisierten oder schnellen Installation auf mehreren Computern an. Diese Art der Installation wird auch als „unbeaufsichtigt“ bezeichnet, weil der Benutzer zu keiner Aktion aufgefordert wird.

Stille/unbeaufsichtigte Installation
Vollständige Installation über die Befehlszeile: `msiexec /i <packagename> /qn /l*xv msi.log`

HINWEIS: Wenn möglich, wird die Installation von ESET Mail Security auf einem neu installierten und konfigurierten Betriebssystem dringend empfohlen. Wenn Sie die Installation jedoch auf einem bereits vorhandenen System vornehmen müssen, ist am ratsamsten, die alte Version von ESET Mail Security zu deinstallieren, den Server neu zu starten und danach die neue Version von ESET Mail Security zu installieren.

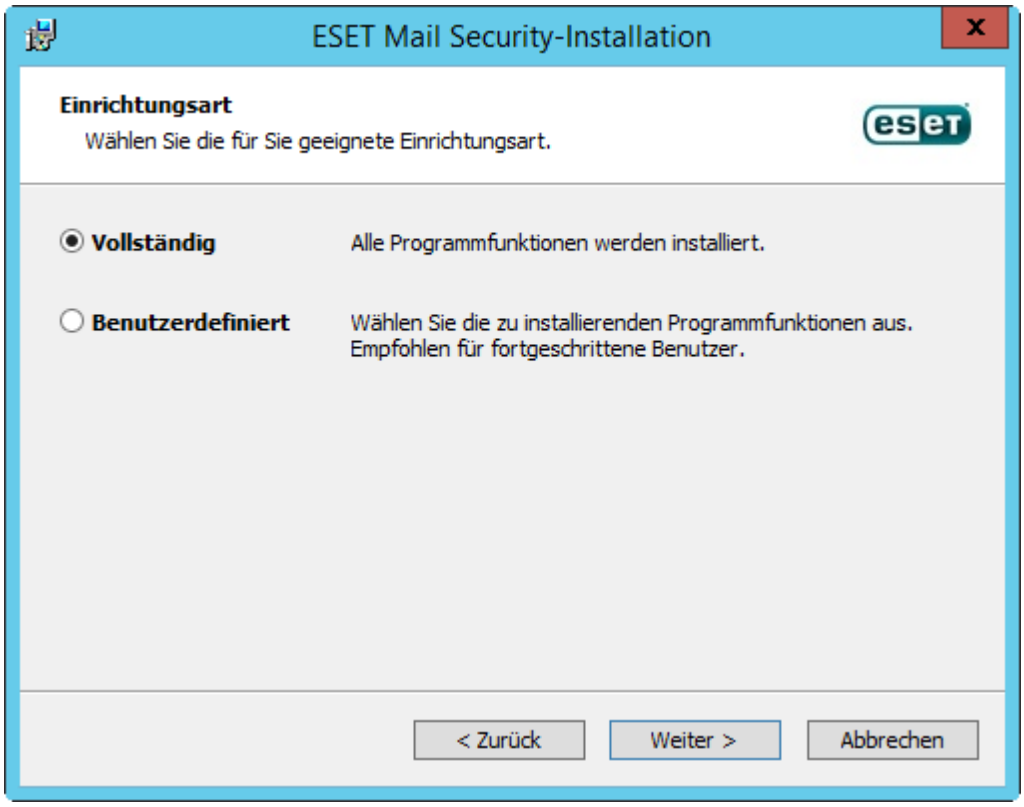
HINWEIS: Wenn Sie zuvor eine Virenschutz-Software eines Drittanbieters auf dem System verwendet haben, sollten Sie sie vor der Installation von ESET Mail Security vollständig deinstallieren. Das ESET AV Removal Tool bietet eine einfache Option für die Deinstallation.

3.1 Installationsschritte für ESET Mail Security

Führen Sie die folgenden Schritte aus, um ESET Mail Security mit dem Einrichtungsassistenten zu installieren:

Nachdem Sie die EULA akzeptiert haben, können Sie eine der folgenden Installationsarten auswählen:

- **Komplett** - Alle Features von ESET Mail Security werden installiert. Dies ist die empfohlene Installationsart.
- **Benutzerdefiniert** - Bei dieser Installationsart können Sie auswählen, welche Features von ESET Mail Security in Ihrem System installiert werden.



Vollständige Installation:

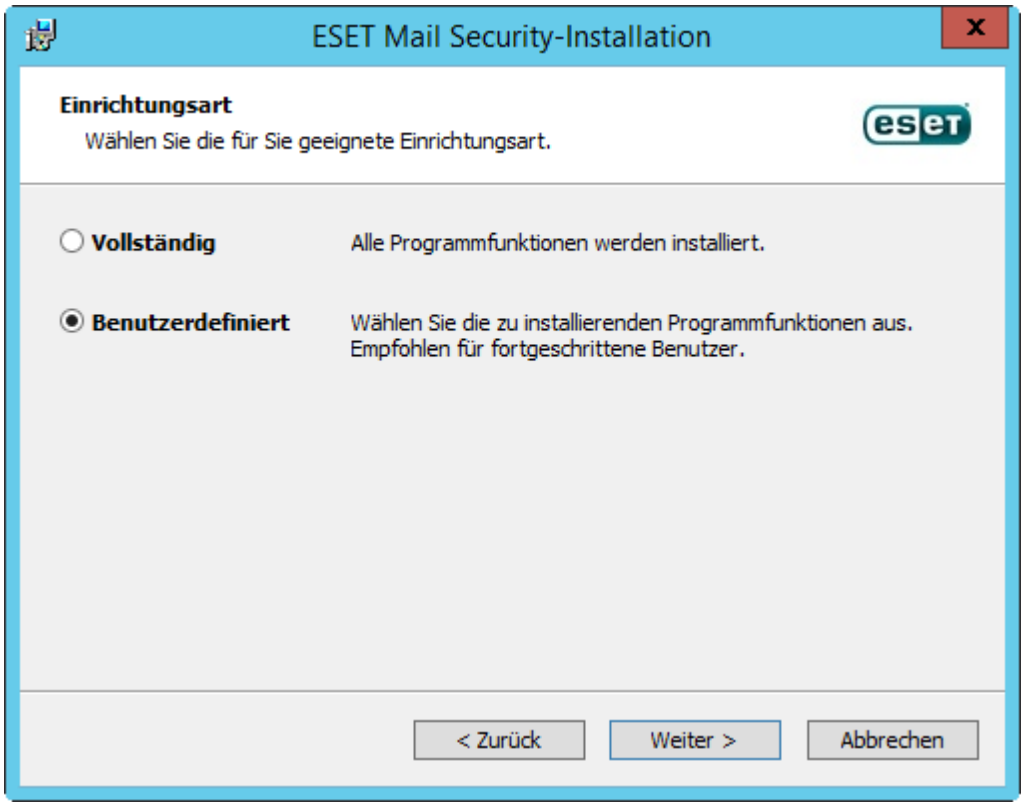
Auch komplette Installation genannt. Mit dieser Installationsart werden alle Komponenten von ESET Mail Security installiert. Sie werden aufgefordert, einen Zielordner für die Installation von ESET Mail Security auszuwählen. Standardmäßig schlägt das Programm den Speicherort C:\Programme\ESET\ESET Mail Security vor. Klicken Sie auf **Durchsuchen**, um diesen Speicherort zu ändern (nicht empfohlen).

HINWEIS: Unter Windows Server 2008 und Windows Server 2008 R2 ist die Installation der Komponente **Web und E-Mail** standardmäßig deaktiviert. Wählen Sie den Installationstyp **Benutzerdefiniert** aus, um diese Komponente zu installieren.

HINWEIS: 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.

Benutzerdefinierte Installation:

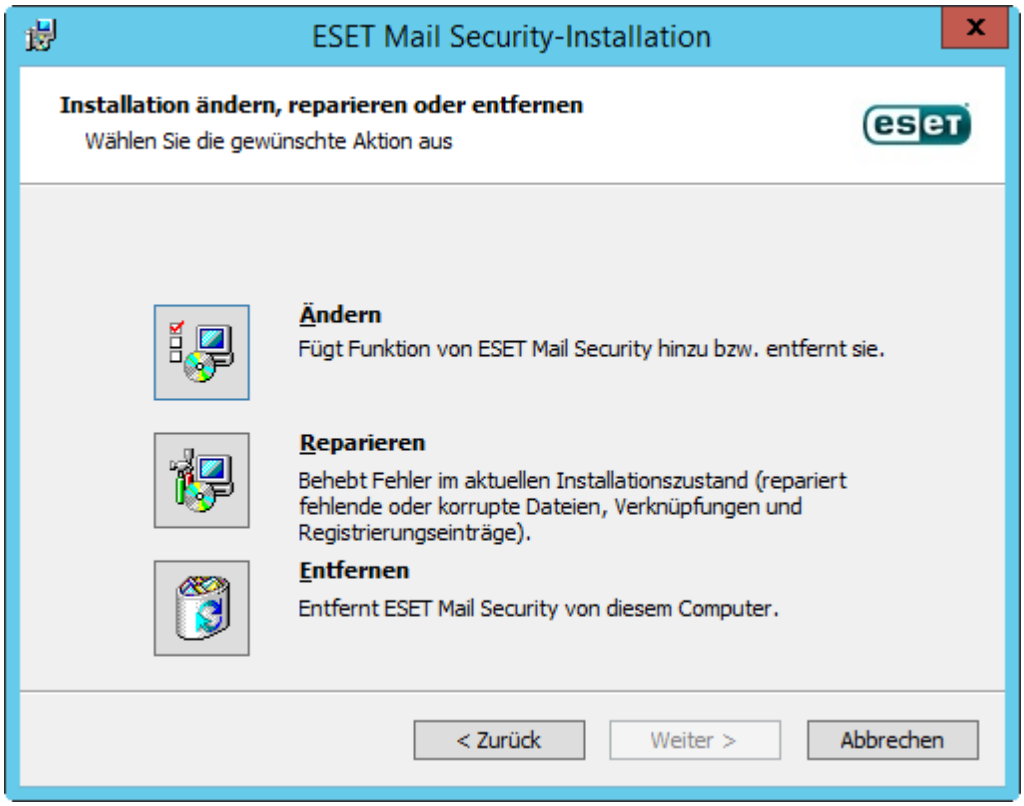
Hier können Sie auswählen, welche Funktionen installiert werden sollen. Dies ist nützlich, wenn Sie ESET Mail Security benutzerdefiniert so anpassen möchten, dass es nur die gewünschten Komponenten enthält.



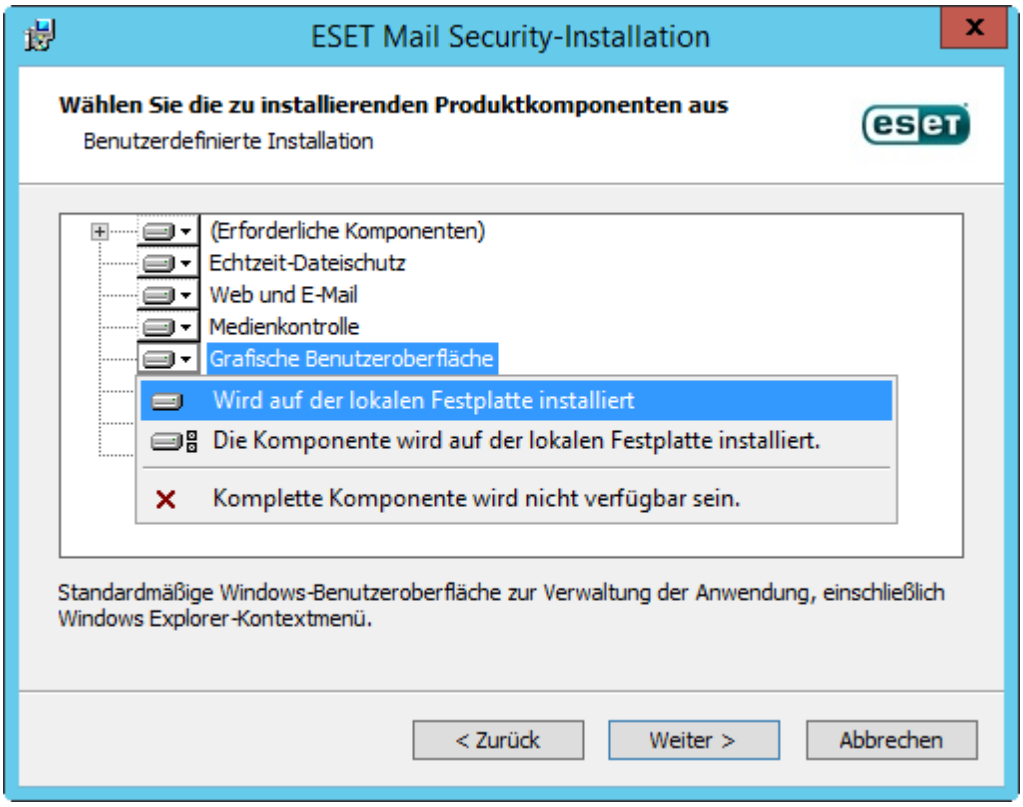
Sie können Komponenten für die vorhandene Installation hinzufügen oder entfernen. Führen Sie dazu entweder das MSI-Installationspaket aus, das Sie für die ursprüngliche Installation verwendet haben, oder öffnen Sie **Programme und Funktionen** in der Windows-Systemsteuerung, klicken Sie mit der rechten Maustaste auf ESET Mail Security und wählen Sie **Ändern** aus. Befolgen Sie die nachstehenden Schritte, um Komponenten hinzuzufügen oder zu entfernen.

Änderung von Komponenten (Hinzufügen/Entfernen), Reparieren und Entfernen:

Sie haben drei Optionen zur Auswahl. Installierte Komponenten **ändern**, Installation von ESET Mail Security **reparieren** oder **Entfernen** bzw. vollständig deinstallieren.



Wenn Sie **Ändern** auswählen, wird eine Liste der verfügbaren Programmkomponenten angezeigt. Wählen Sie aus, welche Komponenten hinzugefügt oder entfernt werden sollen. Sie können mehrere Komponenten gleichzeitig hinzufügen/entfernen. Klicken Sie auf die Komponente und wählen Sie im Dropdown-Menü eine Option aus:



Wählen Sie eine Option aus und klicken Sie auf **Ändern**, um die Änderungen vorzunehmen.

HINWEIS: Sie können installierte Komponenten jederzeit ändern, indem Sie das Installationsprogramm ausführen. Für die meisten Komponenten ist kein Serverneustart erforderlich, um die Änderungen zu übernehmen. Die grafische Benutzeroberfläche wird neu gestartet, und es werden nur die zur Installation ausgewählten Komponenten angezeigt. Falls ein Serverneustart erforderlich ist, werden Sie vom Windows-Installationsprogramm dazu aufgefordert, und die Komponenten sind verfügbar, sobald der Server wieder online ist.

3.1.1 Installation über die Kommandozeile

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

Unterstützte Parameter:

APPDIR=<Pfad>
- Pfad: gültiger Verzeichnispfad
- Installationsverzeichnis der Anwendung.
- Beispiel: `emsx_nt64_ENU.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

APPDATADIR=<Pfad>
- Pfad: gültiger Verzeichnispfad
- Installationsverzeichnis der Anwendungsdaten.

MODULEDIR=<Pfad>
- Pfad: gültiger Verzeichnispfad
- Installationsverzeichnis des Moduls.

ADDLOCAL=<Liste>
- Komponenteninstallation: Liste nicht obligatorischer Funktionen, die lokal installiert werden sollen.
- Verwendung mit .msi-Paketen von ESET: `emsx_nt64_ENU.msi /qn ADDLOCAL=<list>`
- Weitere Informationen zur ADDLOCAL-Eigenschaft finden Sie unter http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx

Regeln

- Die **ADDLOCAL**-Liste ist eine kommagetrennte Liste der Namen aller zu installierenden Funktionen.
- Wenn Sie eine Funktion zur Installation auswählen, muss der gesamte Pfad (alle übergeordneten Funktionen) explizit in der Liste aufgeführt werden.
- Weitere Informationen zur richtigen Verwendung finden Sie unter „Zusätzliche Regeln“.

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
- **Platzhalter** - Funktion ohne Auswirkung auf das Produkt, die jedoch mit den untergeordneten Funktionen aufgeführt werden muss

Der Funktionsbaum sieht folgendermaßen aus:

Funktionsbaum	Funktionsname	Vorhandensein der Funktion
Computer	Computer	Obligatorisch
Computer/Viren- und Spyware-Schutz	Virenschutz	Obligatorisch
Computer/Viren- und Spyware-Schutz > Echtzeit-Dateischutz	RealtimeProtection	Obligatorisch
Computer/Viren- und Spyware-Schutz > Computer-Scan	Prüfung	Obligatorisch
Computer/Viren- und Spyware-Schutz/ Dokumentenschutz	Dokumentenschutz	Optional
Computer/Medienkontrolle	DeviceControl	Optional
Netzwerk	Netzwerk	Platzhalter
Netzwerk/Personal Firewall	Firewall	Optional
Web und E-Mail	WebAndEmail	Platzhalter
Web- und E-Mail-Protokollprüfung	ProtocolFiltering	Unsichtbar
Web und E-Mail/Web-Schutz	WebAccessProtection	Optional
Web und E-Mail/E-Mail-Schutz	EmailClientProtection	Optional
Web und E-Mail/E-Mail-Schutz/E-Mail-Plugins	MailPlugins	Unsichtbar
Web und E-Mail/E-Mail-Schutz/Spam-Schutz	Spam-Schutz	Optional
Web und E-Mail/Web-Kontrolle	WebControl	Optional
Update-Mirror	UpdateMirror	Optional
Microsoft NAP-Unterstützung	MicrosoftNAP	Optional

Zusätzliche Regeln

- Wenn eine der Funktionen aus **Web und E-Mail** zur Installation ausgewählt ist, muss die unsichtbare Funktion **ProtocolFiltering** explizit zur Liste hinzugefügt werden.
- Wenn eine der Unterfunktionen aus **E-Mail-Schutz** zur Installation ausgewählt ist, muss die unsichtbare Funktion **MailPlugins** explizit zur Liste hinzugefügt werden.

Beispiele:

```
efsw_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,WebAccessProtection,ProtocolFiltering
```

```
efsw_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,EmailClientProtection,Antispam,MailPlugins
```

Liste der CFG_-Eigenschaften:

CFG_POTENTIALLYUNWANTED_ENABLED=1/0
• 0 – deaktiviert, 1 – aktiviert
• Eventuell unerwünschte Anwendungen

CFG_LIVEGRID_ENABLED=1/0
• 0 – deaktiviert, 1 – aktiviert
• LiveGrid

FIRSTSCAN_ENABLE=1/0
• 0 – deaktiviert, 1 – aktiviert
• Planen Sie einen neuen FirstScan nach der Installation.

CFG_EPFW_MODE=0/1/2/3
• 0 – automatisch, 1 – interaktiv, 2 – Policy, 3 – Lernen

CFG_PROXY_ENABLED=0/1
• 0 – deaktiviert, 1 – aktiviert

CFG_PROXY_ADDRESS=<IP>
• IP-Adresse des Proxyservers.

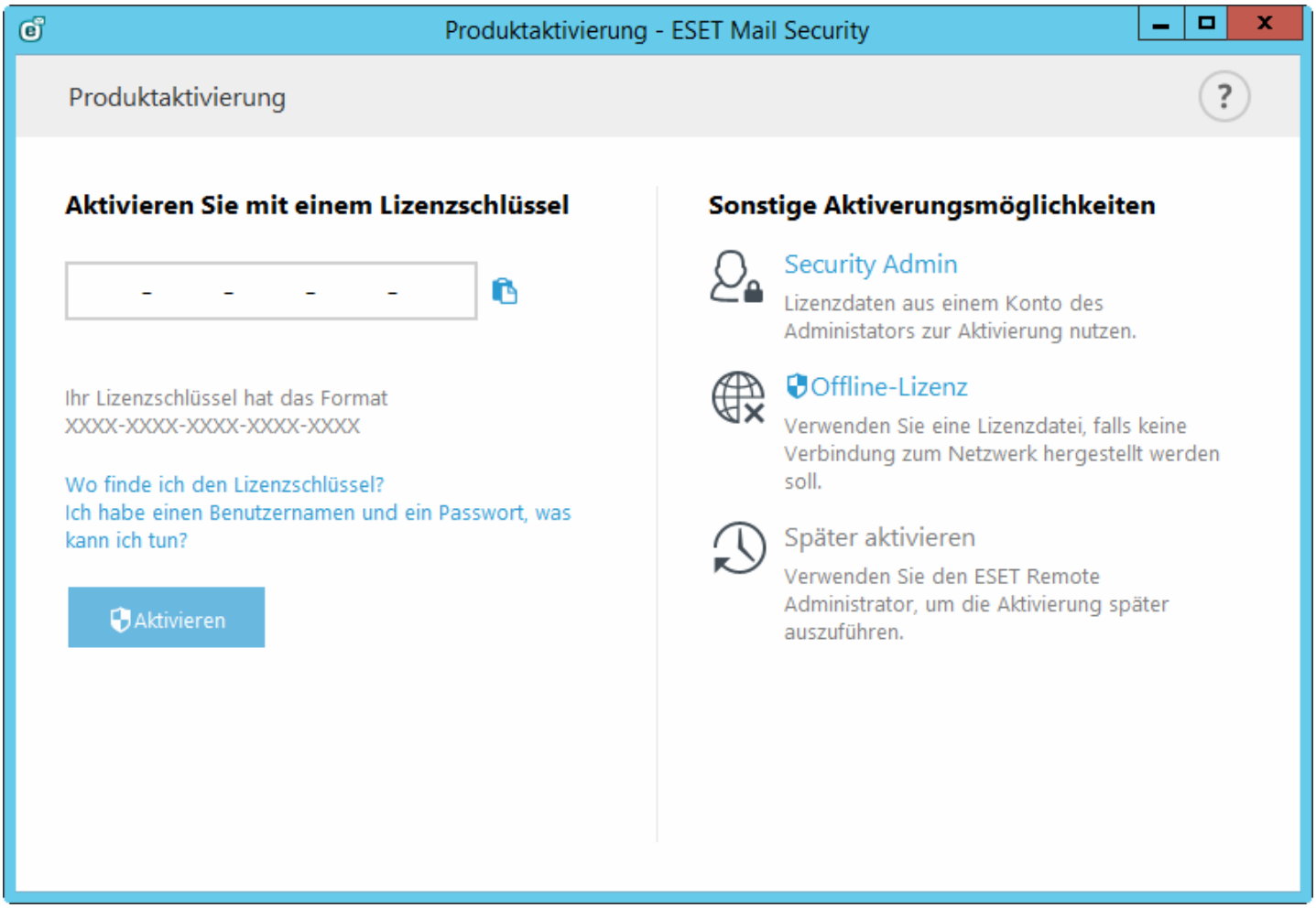
CFG_PROXY_PORT=<Port>
• Proxy-Portnummer.

CFG_PROXY_USERNAME=<Benutzer>
• Benutzername für die Authentifizierung.

CFG_PROXY_PASSWORD=<Passwort>
• Passwort für die Authentifizierung.

3.2 Produktaktivierung

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



Aktivieren Sie ESET Mail Security mit einer der verfügbaren Methoden. Weitere Informationen finden Sie unter So aktivieren Sie ESET Mail Security.

Nach der erfolgreichen Aktivierung von ESET Mail Security wird das Hauptprogrammfenster geöffnet. Es zeigt auf der Seite Überwachung den aktuellen Status an.

Das Hauptprogrammfenster zeigt außerdem Benachrichtigungen zu anderen Elementen wie System-Updates (Windows-Update) oder Updates der Signaturdatenbank an. Wenn alle Elemente, die Ihre Aufmerksamkeit erfordern, aufgelöst sind, wird der Überwachungsstatus grün und es wird der Status **„Maximaler Schutz“**angezeigt.

3.3 Terminalserver

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

3.4 ESET AV Remover

Zum Entfernen/Deinstallieren von Virenschutz-Software eines Drittanbieters in Ihrem System empfehlen wir die Verwendung des ESET AV Remover. Führen Sie dazu die folgenden Schritte aus:

1. Laden Sie den ESET AV Remover von der Downloadseite für Hilfsprogramme auf der ESET-Webseite herunter.
2. Klicken Sie auf **Ich stimme zu, Suche starten**, um die EULA zu akzeptieren und das System durchsuchen zu lassen.
3. Klicken Sie auf **Deinstallationsprogramm starten**, um die installierte Virenschutz-Software zu entfernen.

Eine Liste der Virenschutz-Software von Drittanbietern, die mit dem ESET AV Remover entfernt werden können, finden Sie in diesem KB-Artikel.

3.5 Auf neuere Version aktualisieren

Neuere Versionen von ESET Mail Security werden veröffentlicht, um Verbesserungen oder Patches bereitzustellen, die nicht durch ein automatisches Update der Programmmodule geliefert werden können. ESET Mail Security kann auch von früheren Versionen (4.5 oder früher) aufgerüstet werden, obwohl dies eine Aufrüstung auf eine andere Architektur darstellt. Sie können um eine neuere Version zu installieren:

- Manuelle Aufrüstung durch Herunterladen und Installieren der aktuelleren Version (ohne Deinstallation der vorhandenen Version). Führen Sie einfach das Installationsprogramm und die übliche Installation aus. ESET Mail Security überträgt die vorhandene Konfiguration bis auf einige Ausnahmen (siehe nachstehende Hinweise) automatisch.

WICHTIGER HINWEIS: Beim Aufrüsten sind einige Ausnahmen zu beachten. Einige Einstellungen, insbesondere Regeln, werden nicht beibehalten. Dies liegt daran, dass die Regelfunktion in ESET Mail Security 6 vollständig überarbeitet wurde. Regeln aus früheren Versionen von ESET Mail Security sind nicht mit den Regeln in ESET Mail Security Version 6 kompatibel. Wir empfehlen, Regeln manuall zu konfigurieren.

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.
  - Positivlisten und Negativlisten.

HINWEIS: Nach der Aufrüstung von ESET Mail Security sollten Sie die Einstellungen überprüfen, um sicherzustellen, dass sie richtig und wie gewünscht konfiguriert sind.

3.6 Exchange Server-Rollen – Edge und Hub

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

Vorzugsweise sollte die Spamschutzprüfung auf dem Edge-Server ausgeführt werden, weil ESET Mail Security so Spam-Nachrichten früher zurückweisen kann. Dies verhindert eine unnötige Last auf den Vermittlungsschichten. 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.

Wenn Ihre Organisation keinen Edge-Transport-Server, sondern nur einen Hub-Transport-Server verwendet, sollten Sie die Spamschutzfunktionen auf dem Hub-Transport-Server aktivieren, der die eingehenden Nachrichten über SMTP aus dem Internet empfängt.

3.7 Rollen in Exchange Server 2013

Die Architektur von Exchange Server 2013 unterscheidet sich von anderen Versionen von Microsoft Exchange. Seit der Einführung von Exchange 2013 CU4 (SP1 für Exchange 2013) wurde die Edge-Transportserverrolle wieder eingeführt.

Wenn Sie Microsoft Exchange 2013 mit ESET Mail Security schützen möchten, müssen Sie ESET Mail Security auf einem Microsoft Exchange 2013-Server mit Postfachserverrolle oder Edge-Transportserverrolle installieren.

Allerdings gibt es eine Ausnahme, wenn Sie ESET Mail Security auf Windows SBS (Small Business Server) installieren oder Microsoft Exchange 2013 mit mehreren Rollen auf einem einzigen Server verwenden. In diesem Fall existieren alle Exchange-Rollen auf demselben Server, und ESET Mail Security bietet den kompletten Schutz, inklusive Schutz für E-Mail-Server.

Wenn Sie ESET Mail Security auf einem System installieren, das mit der Clientzugriffsserverrolle ausgeführt wird, werden wichtige Features von ESET Mail Security deaktiviert, insbesondere Features für E-Mail-Server. In diesem Fall sind nur der Echtzeit-Dateischutz und bestimmte Komponenten des Computerschutzes aktiv, und E-Mail-Server werden nicht geschützt. Aus diesem Grund sollte ESET Mail Security möglichst nicht auf einem Server mit der Clientzugriffsserverrolle installiert werden. Dies gilt nicht für Windows SBS (Small Business Server) und Microsoft Exchange mit mehreren Rollen auf demselben Computer, wie oben beschrieben.

HINWEIS: Aufgrund technischer Einschränkungen wird die Clientzugriffsserverrolle (CAS) in Microsoft Exchange 2013 von ESET Mail Security nicht unterstützt. Dies gilt nicht für Windows SBS oder Microsoft Exchange 2013 auf einem einzigen Server mit allen Serverrollen. In diesem Fall können Sie ESET Mail Security mit der CAS-Rolle auf dem Server ausführen, da der E-Mail-Server und der Edge-Transportserver geschützt sind.

3.8 POP3-Connector und Spam-Schutz

Microsoft Windows Small Business Server (SBS)-Versionen enthalten einen nativen, integrierten POP3-Connector, mit dem der Server E-Mail-Nachrichten von externen POP3-Servern abrufen kann. Die Implementierung dieses nativen POP3-Connectors von Microsoft variiert je nach SBS-Version.

ESET Mail Security unterstützt den Microsoft SBS POP3-Connector, sofern er richtig konfiguriert ist. Nachrichten, die über den Microsoft POP3-Connector heruntergeladen werden, werden auf das Vorhandensein von Spam gescannt. Der Spam-Schutz für diese Nachrichten ist möglich, weil der POP3-Connector die E-Mail-Nachrichten von einem POP3-Konto über SMTP an einen Microsoft Exchange Server weiterleitet.

ESET Mail Security wurde mit häufig genutzten E-Mail-Diensten wie **Gmail.com**, **Outlook.com**, **Yahoo.com**, **Yandex.com** und **gmx.de** auf folgenden SBS-Systemen getestet:

- Microsoft Windows Small Business Server 2003 R2
- Microsoft Windows Small Business Server 2008
- Microsoft Windows Small Business Server 2011

WICHTIGER HINWEIS: Wenn Sie den integrierten Microsoft SBS POP3-Connector verwenden und alle E-Mail-Nachrichten auf Spam scannen, wählen Sie in den erweiterten Einstellungen unter **Server** > **E-Mail-Transportschutz** > Erweiterte Einstellungen für die Option **Auch Nachrichten prüfen, die über authentifizierte oder interne Verbindungen eingehen** die Einstellung **Mit Viren- und Spyware-Schutz scannen** aus der Dropdown-Liste aus. Dies gewährleistet, dass der Spam-Schutz für E-Mails angewendet wird, die über ein POP3-Konto abgerufen werden.

Sie können auch einen POP3-Connector eines Drittanbieters wie P3SS (anstelle des integrierten Microsoft SBS POP3-Connectors) verwenden. ESET Mail Security wurde auf den folgenden Systemem (mit dem P3SS-Connector zum Abrufen von Nachrichten von **Gmail.com**, **Outlook.com**, **Yahoo.com**, **Yandex.com** und **gmx.de**) getestet:

- Microsoft Windows Small Business Server 2003 R2
- Microsoft Windows Server 2008 mit Exchange Server 2007
- Microsoft Windows Server 2008 R2 mit Exchange Server 2010
- Microsoft Windows Server 2012 R2 mit Exchange Server 2013

4. Erste Schritte

Dieses Kapitel enthält eine Übersicht über ESET Mail Security, die Hauptelemente des Menüs, die Funktionen und die grundlegenden Einstellungen.

4.1 Die Benutzeroberfläche

Das Hauptprogrammfenster von ESET Mail Security ist in zwei Abschnitte unterteilt. Das primäre Fenster (rechts) zeigt Informationen zu den im Hauptmenü (links) ausgewählten Optionen an.

Nachfolgend finden Sie eine Beschreibung der verschiedenen Bereiche des Hauptmenüs:

Überwachung - Enthält Informationen zum Schutzstatus von ESET Mail Security, zur Lizenzgültigkeit, zum letzten Update der Signaturdatenbank, zu grundlegenden Statistiken und Systeminformationen.

Log-Dateien - Zugriff auf Log-Dateien mit Informationen zu allen aufgetretenen wichtigen Programmereignissen. Diese Dateien bieten einen Überblick über die erkannten Bedrohungen und über andere sicherheitsrelevante Ereignisse.

Scan - In diesem Abschnitt können Sie einen Speicher-Scan, einen Smart-Scan, einen benutzerdefinierten Scan oder ein Wechselmedien-Scan konfigurieren. Außerdem können Sie den zuletzt durchgeführten Scan wiederholen.

E-Mail-Quarantäne - Bietet eine einfache Möglichkeit zur Verwaltung der E-Mails in der Quarantäne. Mit diesem E-Mail-Quarantäne-Manager können alle drei Typen verwaltet werden: lokale Quarantäne, Quarantäne-Postfach und MS Exchange-Quarantäne.

Update - Zeigt Informationen zur Signaturdatenbank an und benachrichtigt Sie, wenn ein Update verfügbar ist. In diesem Bereich können Sie auch die Produktaktivierung vornehmen.

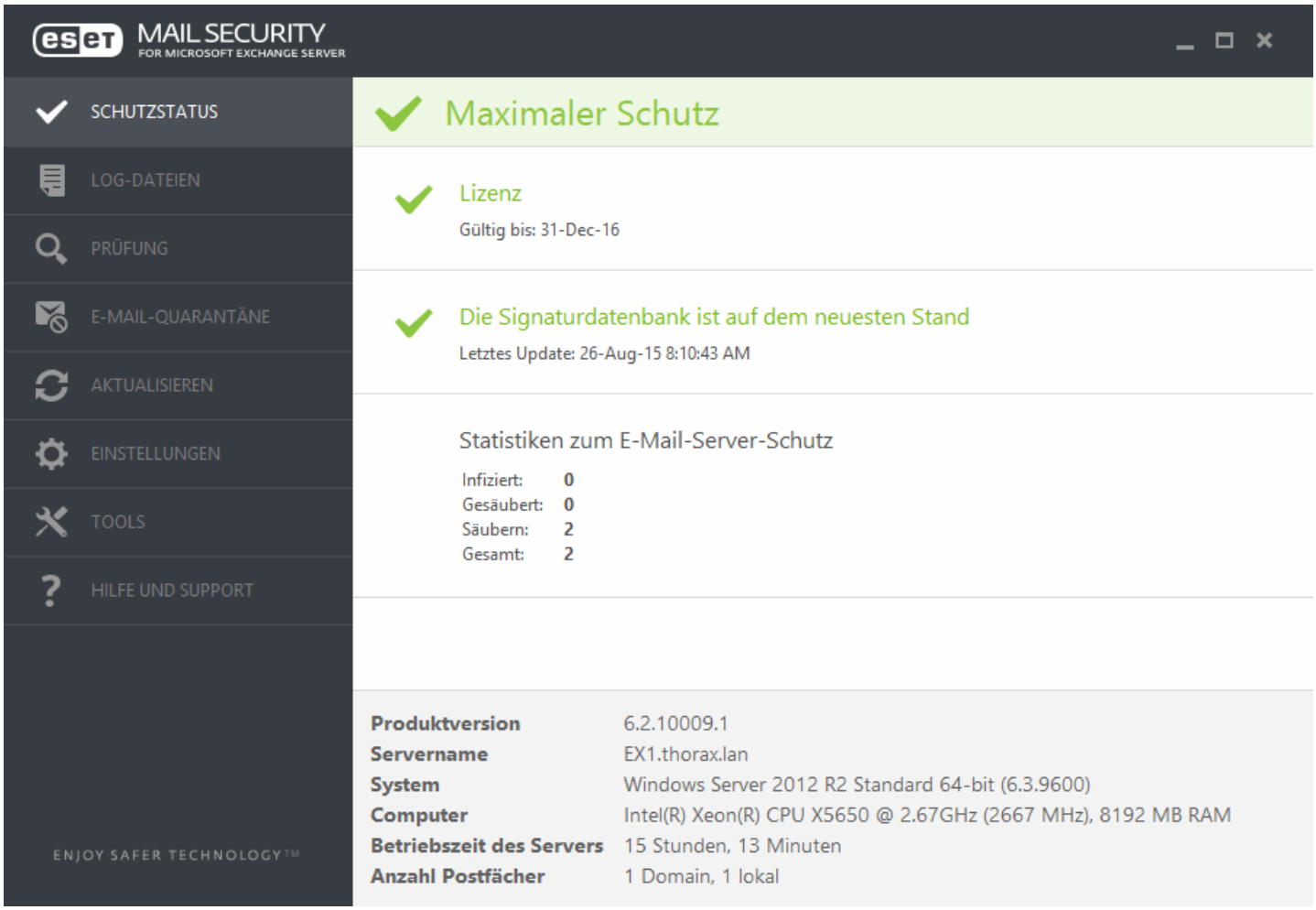
Einstellungen - Hier können Sie die Sicherheitseinstellungen Ihres Servers oder Computers anzupassen.

Tools - Enthält zusätzliche Informationen zum System und zum Schutz und Tools zur weiteren Verwaltung der Sicherheit. Der Tools-Bereich enthält folgende Elemente: Ausgeführte Prozesse, Aktivität beobachten, ESET Log Collector, Schutzstatistik, Cluster, ESET-Shell, ESET SysInspector, ESET SysRescue Live zum Erstellen einer Rettungs-CD bzw. eines USB-Rettungsmediums und Taskplaner. Sie können auch eine Probe zur Analyse einreichen oder die Quarantäne überprüfen.

Hilfe und Support - Bietet Zugriff auf Hilfeseiten, die ESET-Knowledgebase und weitere Support-Tools. Des Weiteren stehen Links zum Öffnen einer Supportanfrage und Informationen zur Produktaktivierung zur Verfügung.

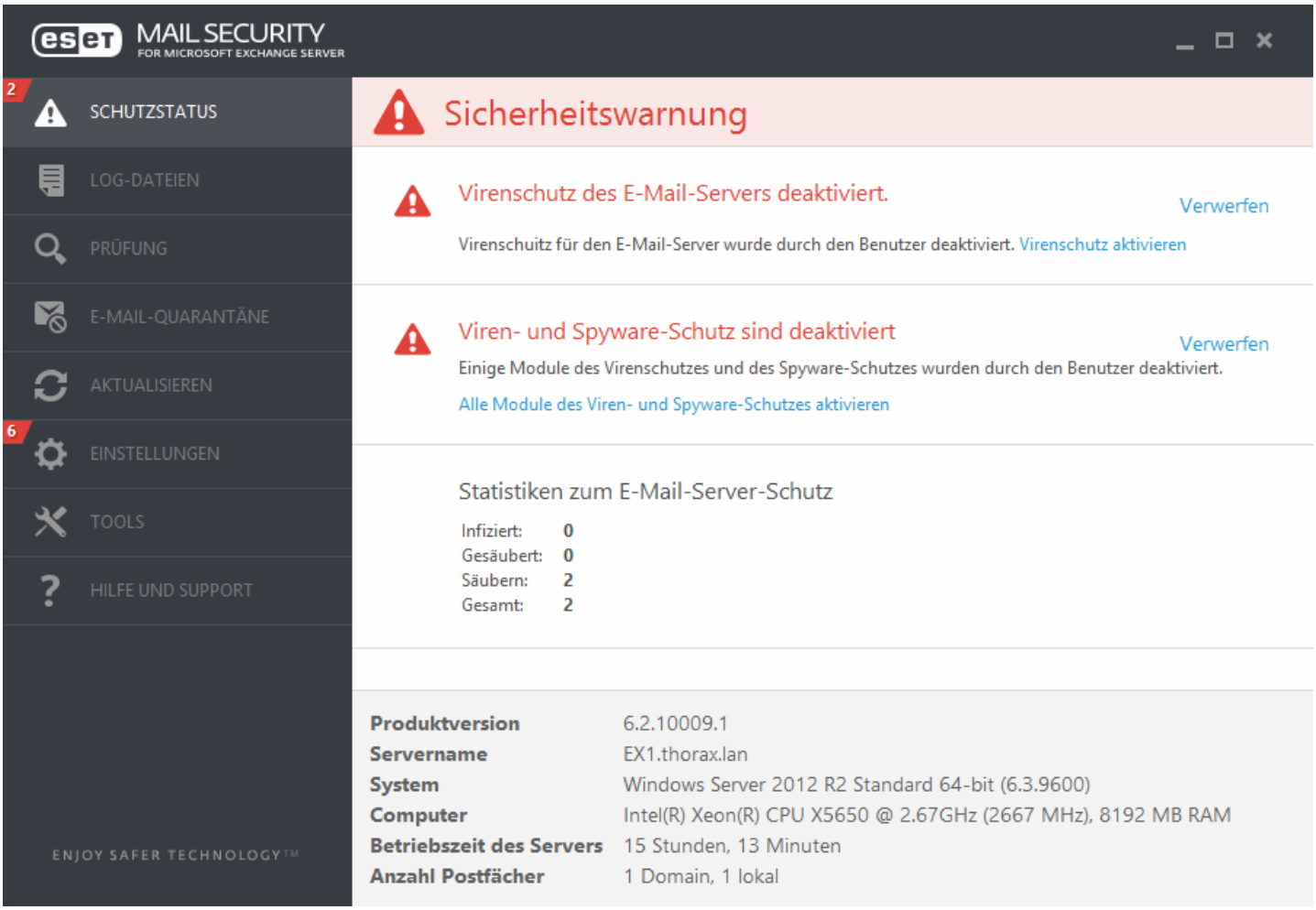
Der Bildschirm **Schutzstatus** enthält Informationen über die aktuelle Schutzstufe Ihres Computers. Das grüne Schutzstatussymbol zeigt an, dass **Maximaler Schutz** gewährleistet ist.

Das Statusfenster enthält außerdem Quicklinks zu häufig in ESET Mail Security verwendeten Funktionen sowie Informationen zum neuesten Update.



Vorgehensweise bei fehlerhafter Ausführung des Programms

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.



Das rote Symbol weist auf kritische Probleme hin. Der maximale Schutz Ihres Computers ist nicht gewährleistet. Dieser Status wird in folgenden Fällen angezeigt:

- **Viren- und Spyware-Schutz deaktiviert** - Sie können den Viren- und Spyware-Schutz erneut aktivieren, indem Sie im Hauptfenster im Bereich **Schutzstatus** auf **Echtzeitschutz aktivieren** oder im Bereich **Einstellungen** auf **Viren- und Spyware-Schutz aktivieren klicken**.
- Die Signaturdatenbank ist veraltet.
- Das Produkt ist nicht aktiviert.
- **Ihre Lizenz ist abgelaufen** - Bei diesem Zustand ist das Schutzstatussymbol rot. Bei abgelaufener Lizenz kann das Programm keine Updates mehr durchführen. Wir empfehlen Ihnen, die in der Warnung angezeigten Anweisungen zur Verlängerung Ihrer Lizenz auszuführen.

Das orangefarbene Symbol weist darauf hin, dass Ihr ESET-Produkt der Aufmerksamkeit bei einem nicht-kritischen Problem bedarf. Mögliche Gründe dafür sind:

- **Web-Schutz ist deaktiviert** - Sie können den Web-Schutz erneut aktivieren, indem Sie auf den Sicherheitshinweis und anschließend auf **Web-Schutz aktivieren** klicken.
- **Lizenz läuft bald ab** - Das Schutzstatussymbol weist mit einem Ausrufezeichen auf dieses Problem hin. Nach dem Ablaufen der Lizenz ist kein Programm-Update mehr möglich und das Schutzstatussymbol ist rot.

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

Zum Anzeigen des **Schutzstatus** klicken Sie auf die oberste Option im Hauptmenü. Im Hauptfenster wird daraufhin eine Statusmeldung über die Funktionsfähigkeit von ESET Mail Security und ein Untermenü mit zwei Optionen angezeigt: **Aktivität beobachten** und **Statistik**. Über diese beiden Optionen können Sie sich weitere Informationen

zu Ihrem System anzeigen lassen.

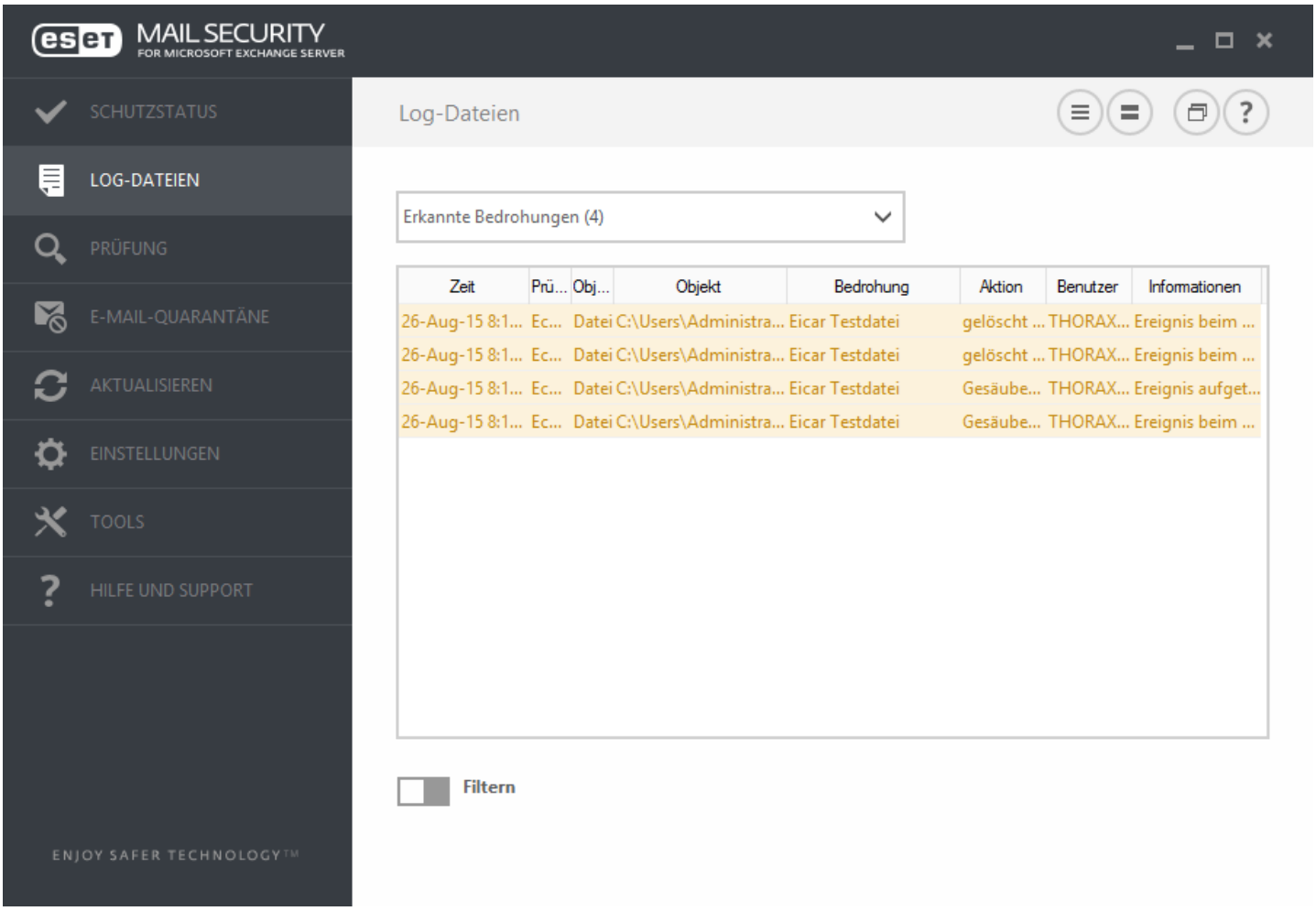
Ist ESET Mail Security voll funktionsfähig, ist das Symbol für den **Schutzstatus** grün. Wenn Ihre Aufmerksamkeit erfordert wird, ist das Symbol orange oder rot.

Klicken Sie auf **Aktivität beobachten**, um eine Echtzeit-Grafik zur Dateisystemaktivität (horizontale Achse) anzuzeigen. Die y-Achse zeigt die Menge der gelesenen Daten (blaue Linie) und die Menge der geschriebenen Daten (rote Linie) an.

Im Untermenü Statistik wird die Anzahl der infizierten, gesäuberten und sauberen Objekte für ein bestimmtes Schutzmodul angezeigt. Für welches Schutzmodul die Werte angezeigt werden sollen, können Sie über die Dropdown-Liste festlegen.

4.2 Log-Dateien

Die Log-Dateien enthalten Informationen zu wichtigen aufgetretenen Programmereignissen und bieten einen Überblick über erkannte Bedrohungen. Logs sind unabdingbar für die Systemanalyse, die Erkennung von Bedrohungen und für die Fehlerbehebung. Die Logs werden im Hintergrund ohne Eingriffe des Benutzers erstellt. Die aufgezeichneten Informationen hängen vom eingestellten Informationsumfang in den Logs ab. Textnachrichten und Logs können direkt in ESET Mail Security angezeigt oder für andere Anzeigeprogramme exportiert werden.



Sie können die Log-Dateien abrufen, indem Sie im Hatuptprogrammfenster auf **Log-Dateien** klicken. Wählen Sie im Dropdown-Menü Log den gewünschten Log-Typ aus. Folgende Logs sind verfügbar:

- **Erkannte Bedrohungen** - Das Bedrohungs-Log enthält detaillierte Informationen über Angriffe, die von ESET Mail Security entdeckt 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.

- **Ereignisse** - 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.
- **Scannen des Computers** - Alle Prüfergebnisse 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.
- **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.
- **Gefilterte Websites** - Diese Liste enthält die vom Web-Schutz gesperrten Websites. Die Logs enthalten die Uhrzeit, die URL, den Benutzer und die Anwendung, die eine Verbindung zur gegebenen Website hergestellt hat.
- **Medienkontrolle** - 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.
- **Datenbank-Prüfung** - Enthält die Version der Signaturdatenbank sowie Datum, geprüfter Ort, Anzahl geprüfter Objekte, Anzahl erkannter Bedrohungen, Anzahl Regeltreffer und Abschlusszeitpunkt.
- **E-Mail-Server-Schutz –** Aufzeichnung aller Nachrichten, die von ESET Mail Security als Spam oder wahrscheinlich Spam eingestuft werden. Diese Logs gelten für die folgenden Schutztypen: Spam-Schutz, Regeln und Virenschutz.
- **Greylisting** - Dieses Log enthält alle Nachrichten, die mit der Greylisting-Methode geprüft wurden.

In den einzelnen Abschnitten können Sie die angezeigten Informationen in die Zwischenablage kopieren (Strg+C). Wählen Sie dazu die gewünschten Einträge aus und klicken Sie auf **Kopieren**. Zur Auswahl mehrerer Einträge verwenden Sie die Strg- und die Umschalttaste.

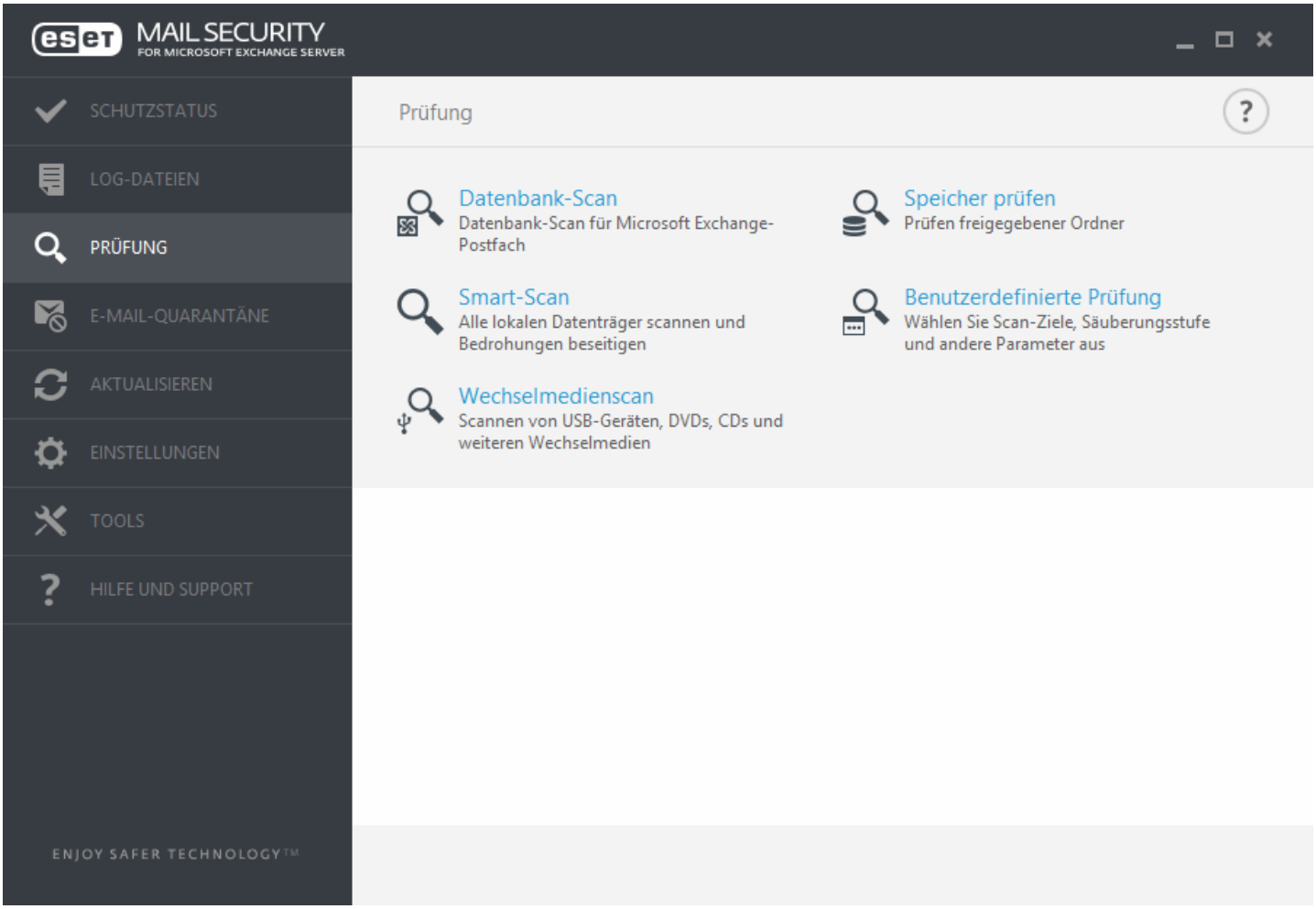
Klicken Sie auf das Schaltersymbol **Filter**, um das Fenster **Log-Filter** zu öffnen, in dem Sie Filterkriterien definieren können.

Das Kontextmenü können Sie über einen Rechtsklick auf einen Eintrag öffnen. Im Kontextmenü stehen folgende Optionen zur Verfügung:

- **Anzeigen** - Zeigt weitere Detailinformationen zum ausgewählten Log in einem neuen Fenster an (gleiche Aktion wie bei Doppelklick).
- **Gleiche Datensätze filtern** - Diese Option aktiviert die Log-Filterung, sodass nur Einträge vom Typ des ausgewählten Eintrags angezeigt werden.
- **Filter ...** – Wenn Sie auf diese Option klicken, können Sie im Fenster Log-Filterung Filterkriterien zu bestimmten Log-Einträgen festlegen.
- **Filter aktivieren** - Aktiviert die Filtereinstellungen. Bei der ersten Verwendung müssen Sie Filterkriterien festlegen. Nach der Erstellung bleiben die Filter so lange erhalten, bis Sie diese ändern.
- **Kopieren** - Kopiert die Informationen der ausgewählten Datensätze in die Zwischenablage.
- **Alles kopieren** - Kopiert die Informationen aller im Fenster angezeigten Einträge.
- **Löschen** - Löscht die ausgewählten Datensätze. Für diese Aktion sind Administratorberechtigungen erforderlich.
- **Alle löschen** - Löscht alle Datensätze im Fenster. Für diese Aktion sind Administratorberechtigungen erforderlich.
- **Exportieren...** – Exportiert die Informationen der ausgewählten Datensätze in eine XML-Datei.
- Alle exportieren ... - Exportiert sämtliche Informationen im aus dem Fenster in eine XML-Datei.
- **Suchen ...** – Öffnet das Fenster Im Log suchen, wo Sie Suchkriterien festlegen können. Kann auf bereits gefilterte Inhalte angewendet werden, um Suchergebnisse weiter einzugrenzen.
- **Weitersuchen** - Sucht den nächsten Eintrag für die zuvor definierten Suchkriterien (siehe oben).
- **Rückwärts weitersuchen** - Sucht den vorherigen Eintrag für die zuvor definierten Suchkriterien (siehe oben).
- **Diagnosedaten löschen** - Löscht alle Diagnoseeinträge im Fenster.
- **Bildlauf für Log** - Wenn diese Option aktiv ist, wandern alte Logs automatisch aus der Anzeige, sodass im Fenster **Log-Dateien** die neuesten Einträge sichtbar sind.

4.3 Prüfung

Die On-Demand-Prüfung ist ein wichtiger Teil von ESET Mail Security. Sie dient zur Prüfung von Dateien und Ordnern auf dem Computer. Aus Sicherheitsgründen ist es dringend erforderlich, dass Sie Ihren Computer nicht nur bei Infektionsverdacht prüfen, sondern diese Prüfung in die allgemeinen Sicherheitsroutinen integrieren. Es wird empfohlen, regelmäßig eine gründliche Prüfung des Computers vorzunehmen, um mögliche Viren zu entdecken, die nicht vom Echtzeit-Dateischutz erfasst wurden. Dies kommt z. B. vor, wenn der Echtzeit-Dateischutz zu diesem Zeitpunkt deaktiviert oder die Signaturdatenbank nicht auf dem neuesten Stand war oder die Datei nicht als Virus erkannt wurde, als sie auf dem Datenträger gespeichert wurde.



Die hierfür vorgesehene Funktion **Scannen des Computers** hat zwei Unterbefehle. Bei der **Smart-Scan** wird das System schnell überprüft, ohne dass Sie dafür weitere Prüfparameter konfigurieren müssen. Bei der Methode **Benutzerdefinierter Scan** können Sie ein vordefiniertes Prüfprofil und die zu prüfenden Objekte auswählen.

Weitere Informationen zum Prüfprozess finden Sie im Abschnitt Stand der Prüfung.

Prüfung der Datenbank

Ausführung der On-Demand-Datenbankprüfung. Sie können **öffentliche Ordner, E-Mail-Server und Postfächer** für die Prüfung auswählen.

HINWEIS: Falls Sie Microsoft Exchange Server 2007 oder 2010 verwenden, können Sie zwischen Postfach-Datenbankschutz und On-Demand-Datenbankprüfung wählen. Es kann jedoch nur eine dieser beiden Schutzarten gleichzeitig aktiv sein. 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.

Speicher prüfen

Prüft alle freigegebenen Ordner auf dem lokalen Server. Wenn die Option **Speicher-Scan** nicht verfügbar ist, bedeutet dies, dass auf dem Server keine freigegebenen Ordner vorhanden sind.

Hyper-V-Scan

Diese Option ist nur sichtbar, wenn Hyper-V Manager auf dem Server installiert ist, auf dem ESET Mail Security ausgeführt wird. Mit der Hyper-V-Prüfung können virtuelle Computerlaufwerke auf Microsoft Hyper-V Servern geprüft werden, ohne auf der jeweiligen VM einen "Agenten" installieren zu müssen. Weitere Informationen finden Sie unter Hyper-V-Scan (inklusive einer Liste unterstützter Hostbetriebssysteme und Einschränkungen).

Smart-Scan

Mit dem Smart-Scan können Sie schnell den Computer scannen und infizierte Dateien entfernen, ohne eingreifen zu müssen. Ihr Vorteil ist die einfache Bedienung, bei der Sie keine detaillierten Prüfeinstellungen festlegen müssen. Beim Smart-Scan werden alle Dateien auf lokalen Laufwerken geprüft, und erkannte eingedrungene Schadsoftware wird automatisch entfernt. Als Säuberungsstufe wird automatisch der Standardwert festgelegt. Weitere Informationen zu den Säuberungstypen finden Sie unter Säubern.

Benutzerdefinierter Scan

Über die Option „Prüfen mit speziellen Einstellungen“ können Sie Prüfparameter wie die zu prüfenden Objekte oder Prüfmethoden angeben. Der Vorteil dieser Methode ist die Möglichkeit zur genauen Parameterkonfiguration. Verschiedene Konfigurationen können in benutzerdefinierten Prüfprofilen gespeichert werden. Das ist sinnvoll, wenn Prüfungen wiederholt mit denselben Parametern ausgeführt werden.

Mit der Option **Scannen des Computers** > **Benutzerdefinierter Scan** können Sie **Zu prüfende Objekte** aus der Liste oder in der Baumstruktur auswählen. Sie können ein zu prüfendes Objekt auch bestimmen, indem Sie den Pfad zum Ordner oder zu den Dateien eingeben, die geprüft werden sollen. Wenn Sie nur das System ohne zusätzliche Säuberung prüfen möchten, wählen Sie die Option **Nur prüfen, keine Aktion**. Sie können bei der Prüfung zwischen drei Säuberungsebenen wählen. Klicken Sie hierfür auf **Einstellungen** > **ThreatSense-Parameter** > **Säubern**.

Benutzerdefinierte Computer-Scans sollten nur von fortgeschrittenen Benutzern ausgeführt werden, die Erfahrung im Umgang mit Virenschutzprogrammen haben.

Wechselmedien prüfen

Dieser Scan ähnelt dem Smart-Scan und ermöglicht ein schnelles Scannen der aktuell an den Computer angeschlossenen Wechselmedien (wie CD/DVD/USB). Diese Prüfung ist hilfreich, wenn Sie beispielsweise ein USB-Speichergerät an den Computer anschließen und den Inhalt auf Schadcode und sonstige mögliche Bedrohungen untersuchen 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.

Letzte Prüfung wiederholen

Führt den zuletzt ausgeführten Scan (Speicher-Scan, Smart-Scan, benutzerdefinierter Scan usw.) mit genau den gleichen Einstellungen erneut aus.

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

HINWEIS: Sie sollten mindestens einmal im Monat eine Prüfung des Computers vornehmen. Sie können die Prüfung als geplanten Task unter **Tools** > **Taskplaner** konfigurieren.

4.3.1 Hyper-V-Scan

Mit der Hyper-V-Virenprüfung können Laufwerke auf Microsoft Hyper-V-Servern geprüft werden, ohne auf der jeweiligen VM einen Agenten installieren zu müssen. Der Virenschutz wird mit Administratorberechtigungen auf dem Hyper-V-Server installiert.

Die Hyper-V-Prüfung basiert auf dem Modul für On-Demand-Scans, wobei manche Features nicht implementiert wurden (Prüfung der Bootsektoren - wird später implementiert, Prüfung des Arbeitsspeichers).

Unterstützte Hostbetriebssysteme

- Windows Server 2008 R2 - Virtuelle Computer können nur im Offlinebetrieb geprüft werden
- Windows Server 2012
- Windows Server 2012 R2

Hardwareanforderungen

Der Server darf keine Performanceprobleme bei der Ausführung virtueller Computer haben. Die Prüfung selbst nutzt hauptsächlich die CPU-Ressourcen.
Für die Prüfung 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 wird aufgrund der Funktionsweise dynamischer Datenträger nicht unterstützt. Daher sollten Sie den Einsatz dynamischer Datenträger in Ihren VMs nach Möglichkeit vermeiden.
- Die Prüfung erfolgt immer ausschließlich für die aktuelle virtuelle Maschine, Checkpoints/Snapshots sind nicht betroffen.
- Hyper-V auf Hosts in einem Cluster wird momentan von ESET Mail Security nicht unterstützt.
- Virtuelle Computer auf Hyper-V-Hosts unter Windows Server 2008 R2 können nur im schreibgeschützten Modus geprüft werden (**keine Säuberung**), unabhängig von der in den ThreatSense-Parametern ausgewählten Säuberungsstufe.

HINWEIS: ESET Mail Security unterstützt die Prüfung des MBR für virtuelle Datenträger, jedoch nur im schreibgeschützten Modus. Die MBR-Prüfung wird standardmäßig ausgeführt. Sie finden diese Einstellung unter **Erweiterte Einstellungen** > **Virenschutz** > **Hyper-V-Prüfung** > ThreatSense-Parameter > **Bootsektoren**.

Zu prüfender virtueller Computer ist offline - (**ausgeschaltet**)

ESET Mail Security verwendet den Hyper-V-Manager, um virtuelle Datenträger von virtuellen Computern zu erkennen und zu verbinden. Auf diese Weise hat ESET Mail Security denselben Zugriff auf den Inhalt der Laufwerke wie beim Zugriff auf Daten und Dateien herkömmlicher Laufwerke.

Zu prüfender virtueller Computer ist online - (**in Betrieb**, **angehalten**, **gespeichert**)

ESET Mail Security verwendet den Hyper-V-Manager, um virtuelle Datenträger von virtuellen Computern 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 eigentliche virtuelle Maschine nicht betroffen ist. Auf diese Weise können Sie feststellen, ob die virtuellen Computer Infektionen enthalten und ggf. Details zu den Infektionen herausfinden.

Die Erstellung von Checkpoint/Snapshot ist ein langsamer Vorgang und kann bis zu eine Minute dauern. Berücksichtigen Sie dies, wenn Sie Hyper-V-Prüfungen für eine große Anzahl virtueller Computer planen.

Namenskonvention

Das Modul für die Hyper-V-Prüfung verwendet die folgende Namenskonvention:
`VirtualMachineName\DiskX\VolumeY`

Wobei X die Nummer des Laufwerks und Y die Nummer des Volumes ist.
Z. B.: `"Computer\Disk0\Volume1"`.

Die Zahlen werden in der Reihenfolge der Erkennung angefügt. Diese Reihenfolge stimmt mit der Reihenfolge im Manager für virtuelle Datenträger überein.
Die Namenskonvention wird in der Baumstruktur der Prüfziele, in der Fortschrittsleiste und in den Log-Dateien verwendet.

Ausführung einer Prüfung

Prüfungen können auf drei Arten ausgeführt werden:

- On-Demand - Klicken Sie auf die Option Hyper-V-Prüfung im Menü von ESET Mail Security, um eine Liste der für die Prüfung verfügbaren virtuellen Computer anzuzeigen. Die unterste Ebene in dieser Baumstruktur sind Volumes, d. h. es ist nicht möglich, Verzeichnisse oder Dateien für die Prüfung auszuwählen. Stattdessen muss immer das gesamte Volume geprüft werden.
  Um die verfügbaren Volumes auflisten zu können, müssen wir die entsprechenden virtuellen Laufwerke verbinden, was jeweils einige Sekunden dauern kann. Daher ist es oft schneller, einen virtuellen Computer bzw. dessen Laufwerke für die Prüfung zu markieren.
  Markieren Sie die zu prüfenden virtuellen Computer, Laufwerke bzw. Volumes, und klicken Sie auf die Schaltfläche "Prüfen".
- Über den Taskplaner
- Über ERA in Form eines Clienttasks mit dem Namen "Serverscan". Laufwerke von virtuellen Computern sind die niedrigste mögliche Prüfebene.

Es können mehrere Hyper-V-Prüfungen parallel ausgeführt werden.

Nach Abschluss der Prüfung wird eine Benachrichtigung mit einem Link für die Loganzeige geöffnet, in der Sie Details zur abgeschlossenen Prüfung nachlesen können. Sämtliche Prüf-Logs sind auch im Bereich "Log-Dateien" von ESET Mail Security verfügbar. Sie müssen jedoch "Hyper-V-Prüfung" im Dropdownmenü auswählen, um die entsprechenden Logs anzuzeigen.

Mögliche Probleme

- Für die Prüfung eines aktiven virtuellen Computers wird ein Checkpoint/Snapshot des jeweiligen virtuellen Computers erstellt. Während der Erstellung von Checkpoint/Snapshot werden möglicherweise einige allgemeine Aktionen des virtuellen Computers eingeschränkt oder deaktiviert.
- Inaktive virtuelle Computer können nicht eingeschaltet werden, solange eine Prüfung ausgeführt wird.
- Im Hyper-V Manager ist es möglich, zwei virtuelle Computer mit identischem Namen anzulegen. Dies kann zu Problemen bei der Unterscheidung der Computer in den Prüf-Logs führen.

4.4 E-Mail-Quarantäne

Der E-Mail-Quarantäne-Manager ist für alle drei Quarantänetypen verfügbar:

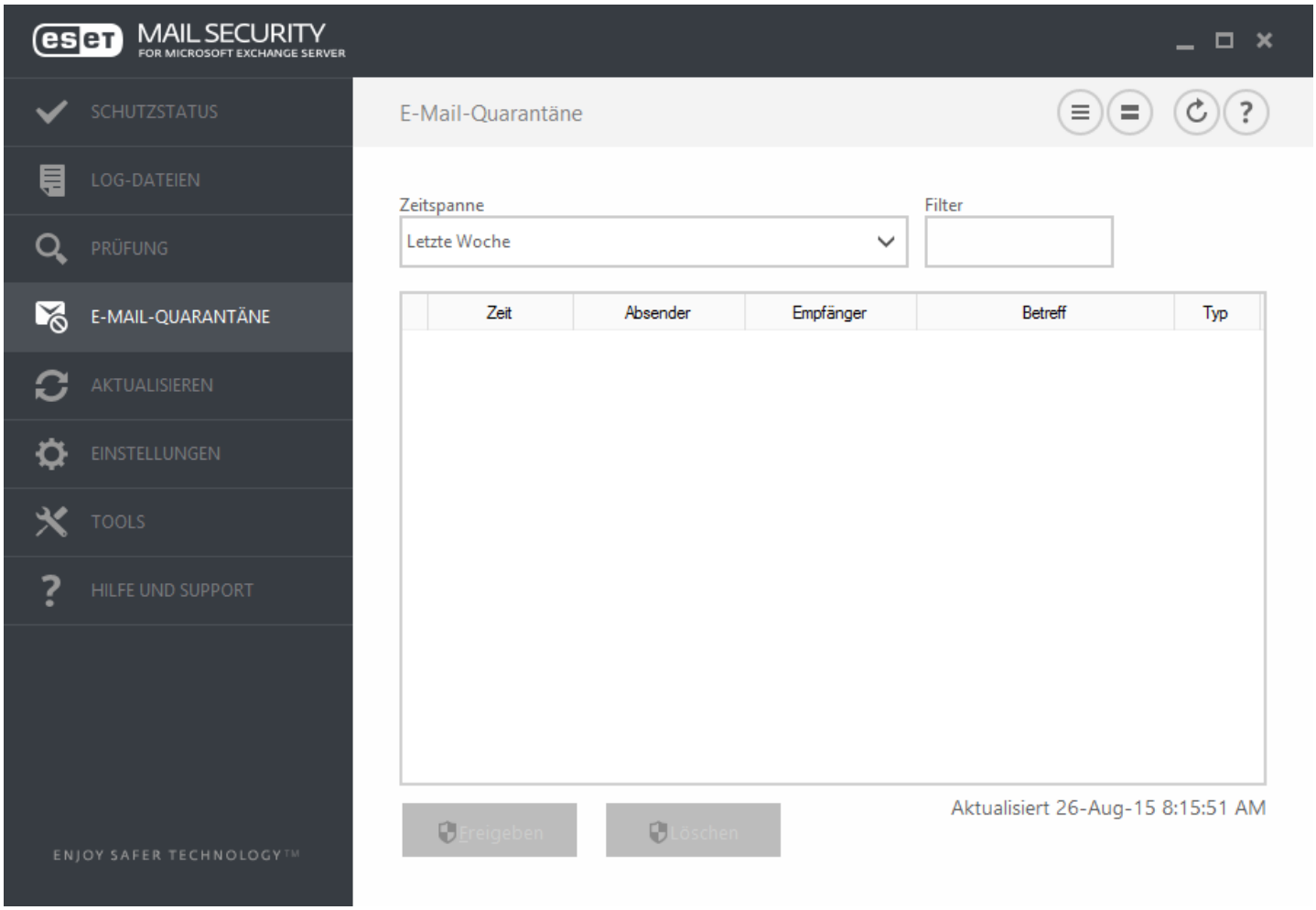
- Lokale Quarantäne
- Quarantäne-Postfach
- MS Exchange-Quarantäne

HINWEIS: Die Web-Oberfläche für die E-Mail-Quarantäne ist eine Alternative zum E-Mail-Quarantäne-Manager für die Verwaltung der E-Mail-Objekte in der Quarantäne.

Filterung

- **Zeitspanne** - Wählen Sie aus, für welche Zeitspanne die E-Mails angezeigt werden sollen (standardmäßig 1 Woche). Wenn Sie die Zeitspanne ändern, werden die E-Mails in der Quarantäne automatisch neu geladen.
- **Filter** - Verwenden Sie dieses Textfeld, um die angezeigten E-Mails zu filtern (alle Spalten werden durchsucht).

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

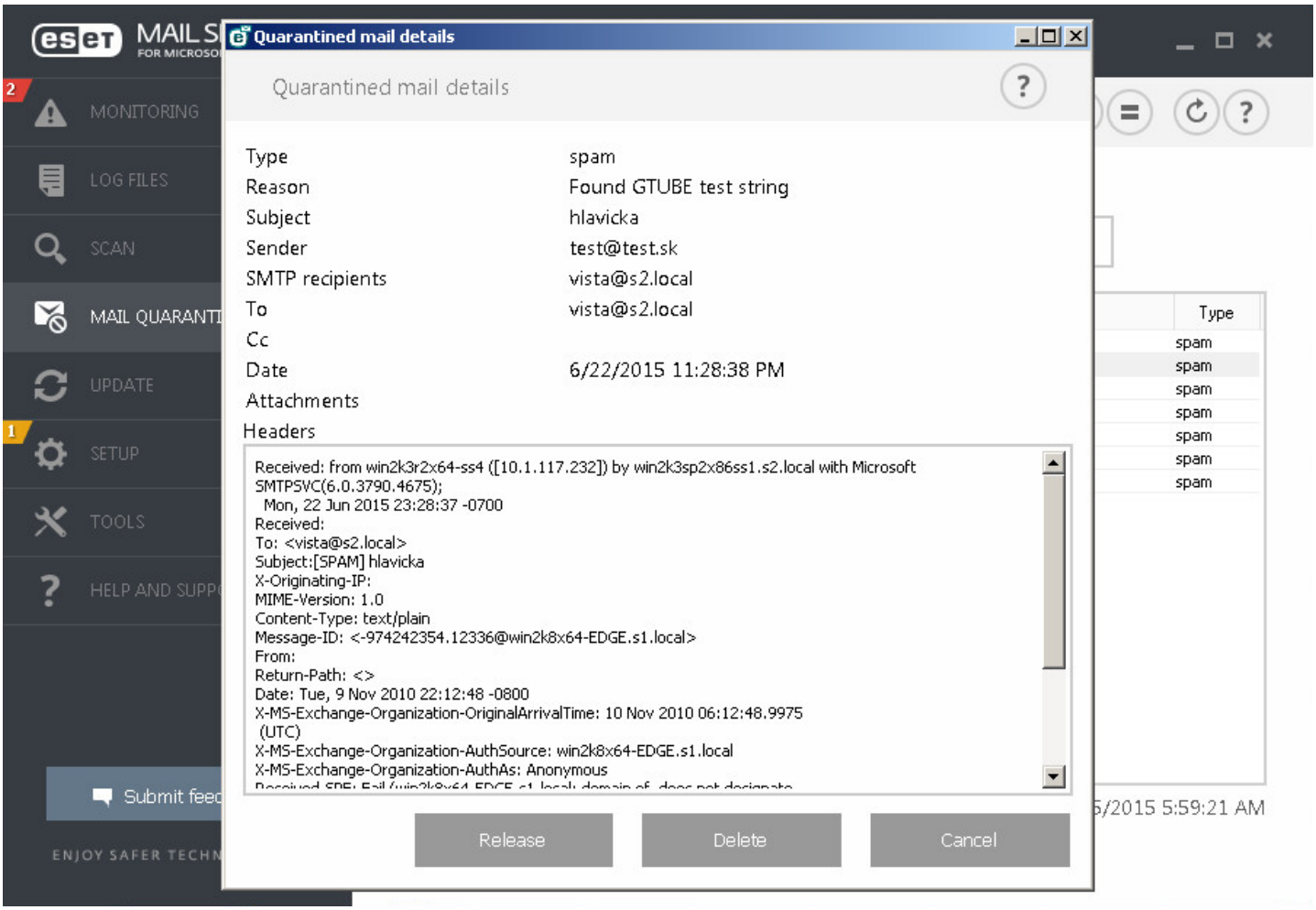


Aktion

- **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.
- **Löschen** - Löscht ein Element aus der Quarantäne. Klicken Sie auf **Ja**, um den Vorgang zu bestätigen.

Details zur E-Mail in Quarantäne – Doppelklicken Sie auf eine E-Mail in der Quarantäne oder klicken Sie mit der rechten Maustaste darauf und wählen **Details** aus. Ein Popup-Fenster mit Details zur E-Mail in der Quarantäne wird angezeigt. Im RFC-E-Mail-Header finden Sie einige zusätzliche Informationen zur E-Mail.

Im Kontextmenü sind verschiedene Aktionen verfügbar. Klicken Sie ggf. 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.



4.4.1 Details zur E-Mail in Quarantäne

Dieses Fenster enthält Informationen zur E-Mail in der Quarantäne, wie **Typ**, **Grund**, **Betreff**, **Absender**, **SMTP-Empfänger**, **An**, **Cc**, **Datum**, **Anlagen** und **Header**. Bei Bedarf können Sie die Header auswählen, kopieren und einfügen.

Über die Schaltflächen können Sie bestimmte Aktionen für die E-Mails in der Quarantäne ausführen:

- **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.
- **Löschen** - Löscht ein Element aus der Quarantäne. Klicken Sie auf **Ja**, um den Vorgang zu bestätigen.

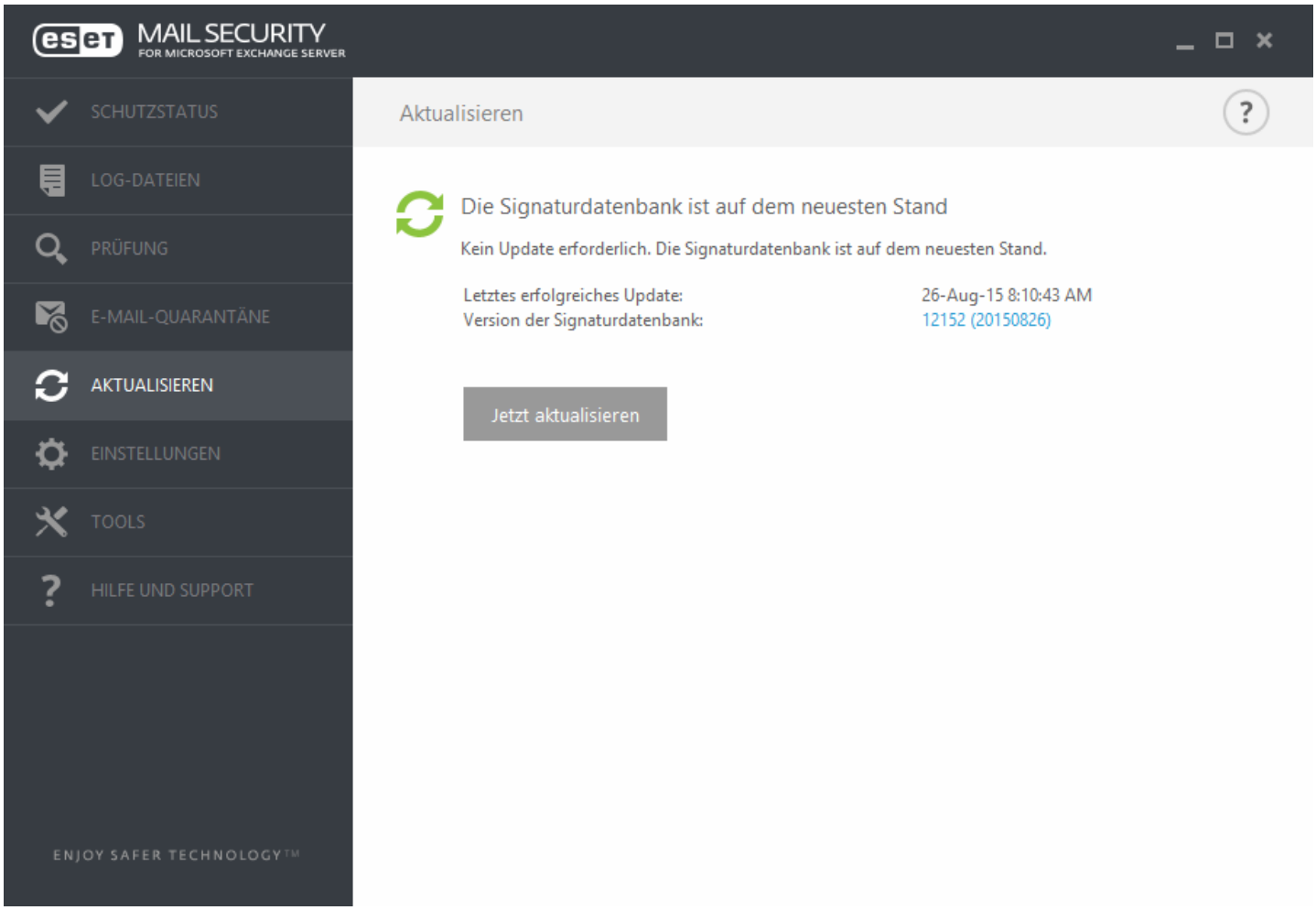
Um das Fenster mit den Details zur E-Mail in Quarantäne zu schließen, klicken Sie auf die Schaltfläche **Abbrechen**.

4.5 Update

Den optimalen Schutz Ihres Computers gewährleisten Sie, indem Sie ESET Mail Security regelmäßig aktualisieren. Die Updates halten das Programm fortlaufend auf dem neuesten Stand, indem die Signaturdatenbank und die Programmkomponenten aktualisiert werden.

Über den Punkt **Update** im Hauptprogrammfenster können Sie sich den aktuellen Update-Status anzeigen. Sie sehen hier Datum und Uhrzeit des letzten Updates und können feststellen, ob ein Update erforderlich ist. Die Versionsnummer der Signaturdatenbank wird ebenfalls in diesem Fenster angezeigt. Diese Nummer ist ein aktiver Link zur ESET-Website, auf der alle Signaturen aufgeführt werden, die bei dem entsprechenden Update hinzugefügt wurden.

Klicken Sie auf **Jetzt aktualisieren**, um den Update-Vorgang zu starten. Updates der Signaturdatenbank und Updates von Programmkomponenten sind wichtige Bestandteile der Maßnahmen für einen möglichst umfassenden Schutz vor Schadcode.



Letztes erfolgreiches Update - Das Datum des letzten Updates. Hier sollte ein neueres Datum angezeigt werden, was auf eine erst kürzlich vorgenommene Aktualisierung der Signaturdatenbank hinweist.

Version der Signaturdatenbank - Die Nummer der Signaturdatenbank. Diese Nummer ist gleichzeitig ein aktiver Link zur Website von ESET. Klicken Sie darauf, um eine Liste aller Signaturen anzuzeigen, die bei dem entsprechenden Update hinzugefügt wurden.

Update-Vorgang

Nachdem Sie auf **Jetzt aktualisieren** geklickt haben, beginnt der Downloadvorgang und es wird der Update-Fortschritt angezeigt. Um den Update-Vorgang abzubrechen, klicken Sie auf **Update abbrechen**.

WICHTIGER HINWEIS: Wenn keine Zwischenfälle beim Update-Download auftreten, wird im **Update**-Fenster der Hinweis **Update nicht erforderlich - die Signaturdatenbank ist auf dem neuesten Stand** angezeigt. Andernfalls ist

das Programm nicht auf dem neuesten Stand und anfälliger für Infektionen. Aktualisieren Sie die Signaturdatenbank so schnell wie möglich. In allen anderen Fällen erhalten Sie eine der folgenden Fehlermeldungen:

Signaturdatenbank nicht mehr aktuell - Dieser Fehler wird angezeigt, wenn die Signaturdatenbank trotz wiederholter Versuche nicht aktualisiert werden konnte. Sie sollten in diesem Fall die Update-Einstellungen überprüfen. Die häufigste Fehlerursache sind falsch eingegebene Lizenzdaten oder fehlerhaft konfigurierte Verbindungseinstellungen.

Der eben erwähnte Hinweis steht im Zusammenhang mit den folgenden beiden Meldungen (**Update der Signaturdatenbank fehlgeschlagen**) über nicht erfolgreiche Updates:

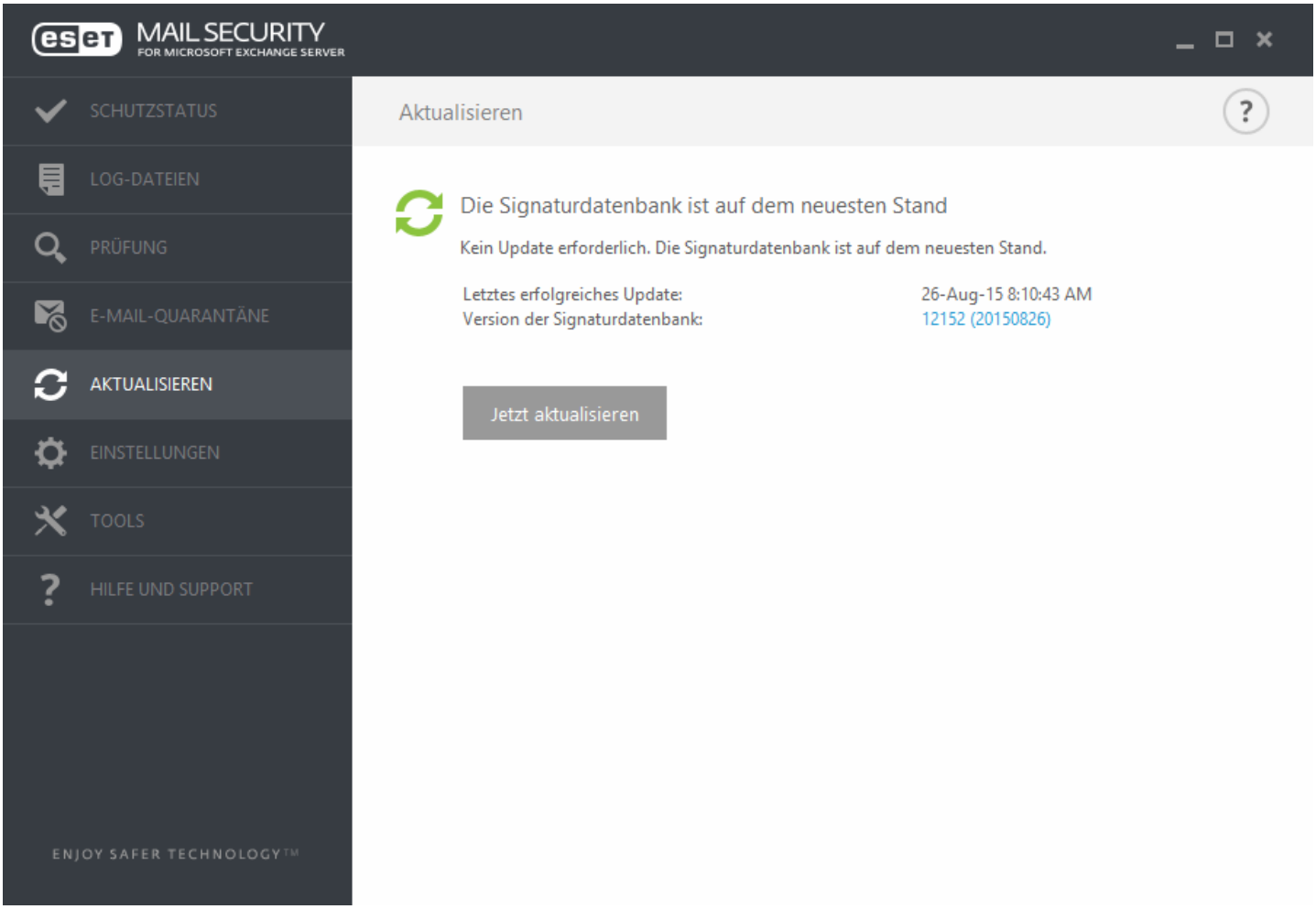
Ungültige Lizenz - Der Lizenzschlüssel wurde falsch in den Update-Einstellungen eingegeben. Wir empfehlen eine Überprüfung Ihrer Lizenzdaten. Das Fenster für die erweiterten Einstellungen enthält zusätzliche Update-Optionen (drücken Sie zum Öffnen des Fensters auf der Tastatur die Taste F5). Klicken Sie im Hauptmenü auf **Hilfe und Support** > **Lizenzen verwalten**, um einen neuen Lizenzschlüssel einzugeben.

Fehler beim Herunterladen der Update-Dateien - Ein Grund für den Fehler könnten falsche Einstellungen der Internetverbindung sein. 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. Falls dies der Fall ist, wenden Sie sich an Ihren Internetdienstanbieter.

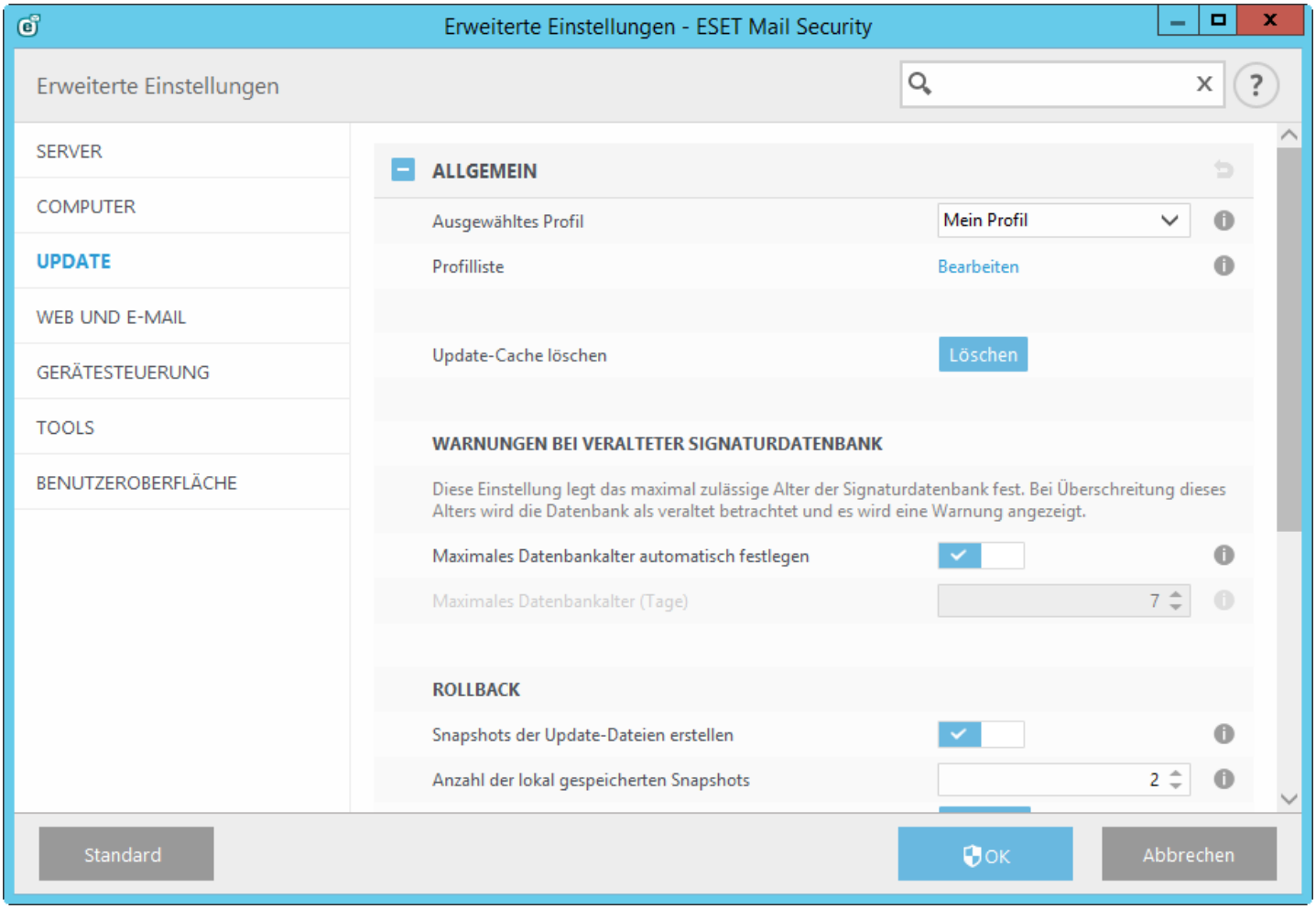
HINWEIS: Weitere Informationen finden Sie in diesem Artikel in der ESET-Knowledgebase.

4.5.1 Einrichten der Signaturdatenbank

Updates der Signaturdatenbank und von Programmkomponenten sind ein wichtiger Bestandteil der Maßnahmen für einen möglichst umfassenden Schutz vor Schadcode. Seien Sie deshalb bei Konfiguration und Ausführung besonders sorgfältig. Wechseln Sie im Hauptmenü zu **Update** und klicken Sie auf **Jetzt aktualisieren**, um nach einem aktuellen Update für die Signaturdatenbank zu suchen.



Sie können die Update-Einstellungen über das Fenster der erweiterten Einstellungen konfigurieren (drücken Sie auf der Tastatur die Taste F5). Um erweiterte Update-Optionen wie den Update-Modus, den Proxyserverzugang, die LAN-Verbindungen und Einstellungen für Kopien der Virussignaturen (Mirror) zu konfigurieren, klicken Sie links in den **erweiterten Einstellungen** auf **Update**. Wenn Probleme mit einem Update auftreten, klicken Sie auf **Cache leeren**, um temporäre Update-Dateien zu löschen. Die Option **Update-Server** ist standardmäßig auf **AUTOSELECT** eingestellt. **AUTOSELECT** bedeutet, dass der Update-Server, von dem die Updates für die Signaturdatenbank heruntergeladen werden, automatisch ausgewählt wird. Wir empfehlen, die standardmäßige Option ausgewählt zu lassen. Wenn die Hinweise im Infobereich der Taskleiste in der unteren rechten Ecke nicht angezeigt werden sollen, aktivieren Sie die Option **Benachrichtigungen über erfolgreiche Updates deaktivieren**.

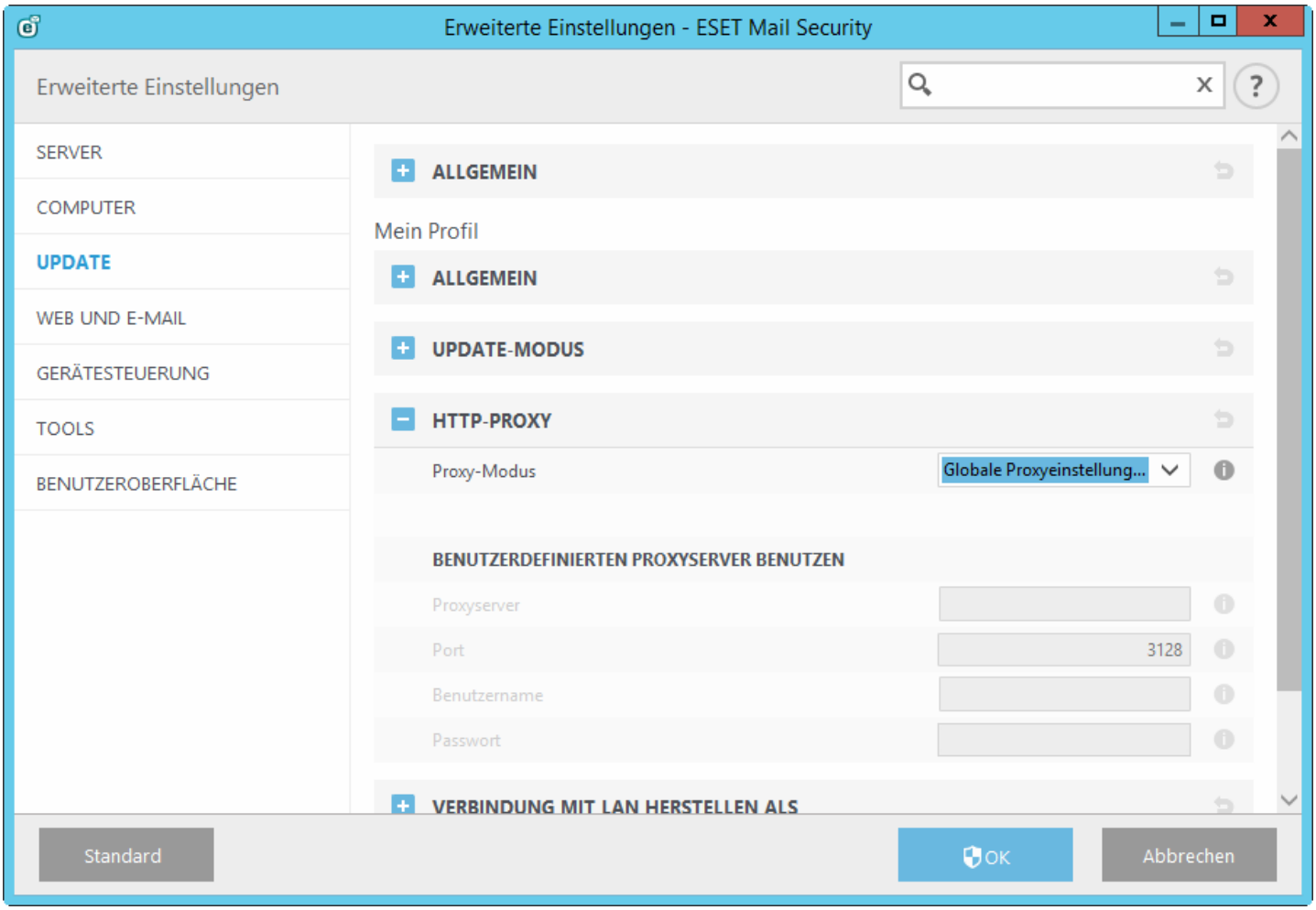


Damit alle Funktionen optimal genutzt werden können, sollte das Programm automatisch aktualisiert werden. Dies ist nur möglich, wenn der richtige **Lizenzschlüssel** unter **Hilfe und Support** > **Lizenz aktivieren** eingegeben wurde.

Wenn Sie das Produkt nicht nach der Installation aktiviert haben, können Sie dies jederzeit nachholen. Weitere Informationen zur Aktivierung finden Sie unter So aktivieren Sie ESET Mail Security. Geben Sie hier die Lizenzdaten ein, die Sie für Ihr ESET-Sicherheitsprodukt erhalten haben.

4.5.2 Proxyserver für Updates konfigurieren

Wenn Sie auf einem System, auf dem ESET Mail Security installiert ist, einen Proxyserver für die Internetverbindungen verwenden, müssen Sie die Proxy-Einstellungen in den erweiterten Einstellungen konfigurieren. Zum Öffnen des Konfigurationsfensters für den Proxyserver drücken Sie zunächst F5, um das Fenster „Erweiterte Einstellungen“ zu öffnen, und klicken dort auf **Update** > **HTTP-Proxyserver**. Wählen Sie im Dropdown-Menü **Proxy-Modus** die Option **Verbindung über Proxyserver** aus und geben Sie die Details für den Proxyserver an: **Proxyserver** (IP-Adresse), **Port**-Nummer und **Benutzername** und **Passwort** (sofern zutreffend).



Wenn Sie sich bei den Angaben nicht sicher sind, können Sie versuchen, die Einstellungen für den Proxyserver automatisch erkennen zu lassen. Wählen Sie hierzu in der Dropdown-Liste den Eintrag **In Systemsteuerung eingestellten Proxy verwenden** aus.

HINWEIS: Die Proxyserver-Optionen können für verschiedene Update-Profile abweichen. Konfigurieren Sie in diesem Fall die verschiedenen Update-Profile in den erweiterten Einstellungen. Klicken Sie dazu in der Baumstruktur der erweiterten Einstellungen auf **Update** > **Profil**.

4.6 Einstellungen

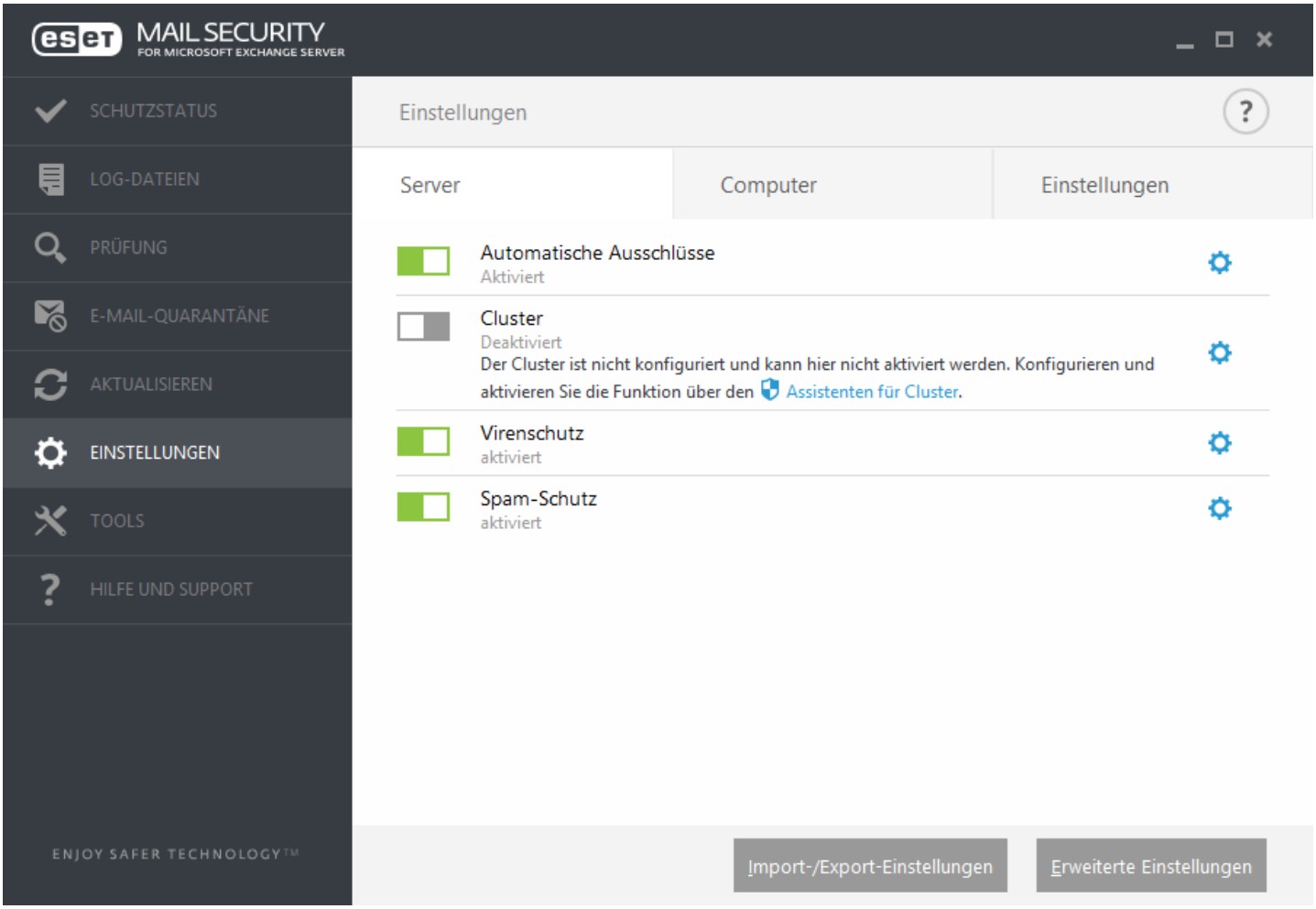
Das Setup-Menü enthält drei Registerkarten:

- Server
- Computer
- Tools

4.6.1 Server

ESET Mail Security schützt Ihren Server mit einer Reihe von leistungsstarken Funktionen: Viren- und Spyware-Schutz, Hintergrundwächter (Echtzeit-Schutz), Web-Schutz und E-Mail-Schutz. Ausführliche Informationen zu den einzelnen Schutzmodulen finden Sie unter ESET Mail Security - Computer.

- Automatische Ausschlüsse: Diese Funktion identifiziert Anwendungen und Betriebssystemdateien, die für den Serverbetrieb benötigt werden und übernimmt sie automatisch in die Liste Ausschlüsse. Auf diese Weise wird das Risiko von Konflikten durch die Virenschutz-Software minimiert und die Gesamtleistung des Servers gesteigert.
- Klicken Sie auf **Clusterassistent**, *um den ESET-Cluster einzurichten.* Ausführliche Informationen zum Einrichten des ESET-Clusters mit dem Assistenten finden Sie hier.
- **Virenschutzlösungen** - bieten durch Überwachung der Daten-, E-Mail- und Internet-Kommunikation Schutz vor bösartigen Systemangriffen.
- **Spamschutzlösungen** - verwenden verschiedenen Technologien (RBL, DNSBL, Fingerprint-Datenbanken, Reputations-Prüfung, Inhaltsanalyse, Bayesscher Filter, Regeln, manuell geführte Whitelists/Blacklists usw.), um E-Mail-Bedrohungen wirksam zu erkennen.



Wenn Sie weitere Optionen festlegen möchten, klicken Sie auf **Erweiterte Einstellungen** oder drücken Sie die Taste **F5**.

Am unteren Rand des Fensters „Einstellungen“ finden Sie weitere Optionen. Verwenden Sie die Option **Einstellungen importieren/exportieren**, um die Einstellungen aus einer *.xml*-Konfigurationsdatei zu laden oder die aktuellen Einstellungen in einer Konfigurationsdatei zu speichern. Ausführliche Informationen hierzu finden Sie unter Einstellungen importieren/exportieren.

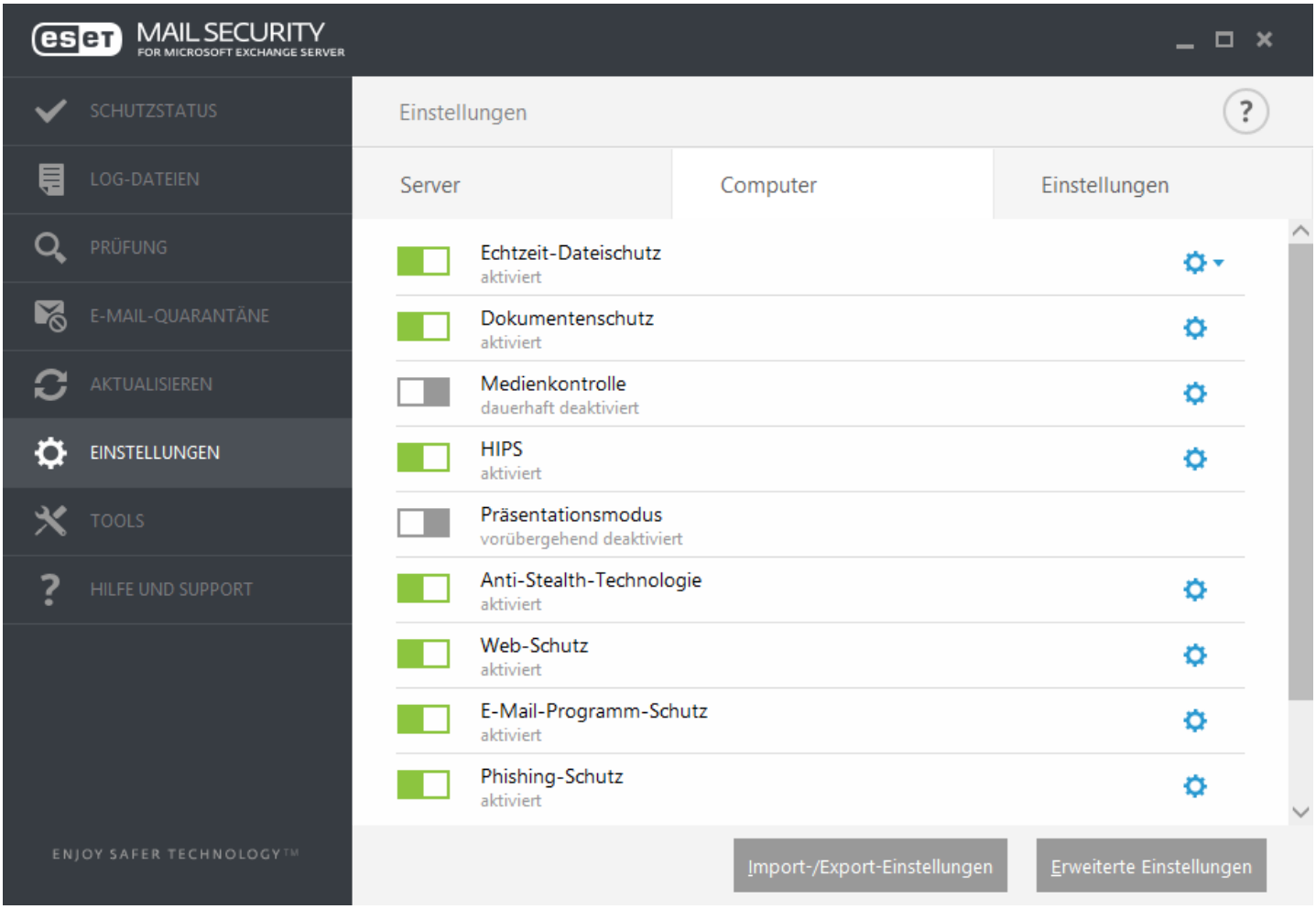
4.6.2 Computer

ESET Mail Security enthält alle erforderlichen Komponenten, um den Server als Computer zu schützen. Jede Komponente bietet eine bestimmte Schutzart: Viren- und Spyware-Schutz, Echtzeit-Dateischutz, Web-Schutz, E-Mail-Schutz, Phishing-Schutz usw.

Der Bereich **Computer** befindet sich unter **Einstellungen** > **Computer**. Hier wird eine Liste der Komponenten angezeigt, die Sie über den Schalter aktivieren/deaktivieren können. Um die Einstellungen für ein bestimmtes Element zu konfigurieren, klicken Sie auf das Zahnradsymbol. Für den **Echtzeit-Dateischutz** steht die Option **Ausschlüsse bearbeiten** zur Verfügung. Über diese Option können Sie das Fenster zum Einrichten der Ausschlüsse öffnen, wo Sie Dateien und Ordner vom Scan ausnehmen können.

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. Durch Klicken auf **Viren- und Spyware-Schutz aktivieren** wird der Schutz wieder aktiviert.

Im **Computer**-Modul können Sie folgende Komponenten aktivieren oder deaktivieren:



- **Echtzeit-Dateischutz** - Alle Dateien werden beim Öffnen, Erstellen oder Ausführen auf Ihrem Computer auf Schadcode geprüft.
- **Dokumentenschutz** - Die Dokumentenschutzfunktion überprüft Microsoft Office-Dokumente vor dem Öffnen sowie automatisch von Internet Explorer heruntergeladene Dateien wie Microsoft ActiveX-Elemente.
- **Medienkontrolle -** Mit diesem Modul können Sie Medien bzw. Geräte scannen oder sperren oder erweiterte Filter- und Berechtigungseinstellungen anpassen und definieren, wie ein Benutzer auf diese Geräte zugreifen und mit ihnen arbeiten kann.
- **HIPS** - Das HIPS-System überwacht Ereignisse auf Betriebssystemebene und führt Aktionen gemäß individueller Regeln aus.
- **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 orange.
- **Anti-Stealth-Technologie** - System zur Erkennung von gefährlichen Programmen, beispielsweise Rootkits, die sich vor dem Betriebssystem verbergen können. Aus diesem Grund ist es nahezu unmöglich, sie mit herkömmlichen Prüfmethoden zu erkennen.
- **Web-Schutz** - Wenn diese Option aktiviert ist, werden alle Daten geprüft, die über HTTP oder HTTPS übertragen werden.
- **E-Mail-Schutz** - Überwacht eingehende E-Mails, die mit dem POP3- oder dem IMAP-Protokoll 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.

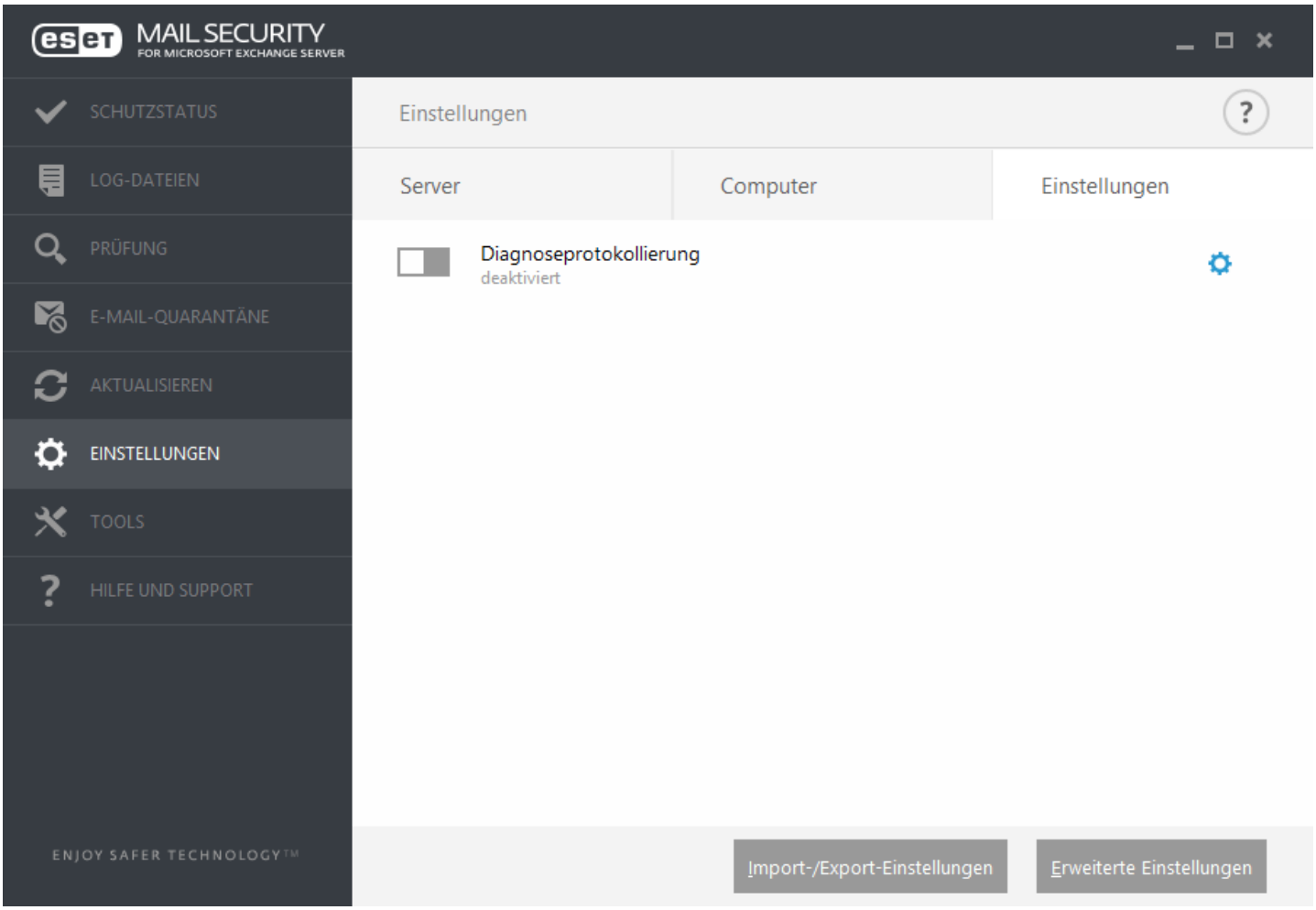
HINWEIS: Der Dokumentenschutz ist standardmäßig deaktiviert. Sie können den Schutz je nach Wunsch einfach über Klicken auf das Schaltersymbol aktivieren.

Am unteren Rand des Fensters „Einstellungen“ finden Sie weitere Optionen. Verwenden Sie die Option **Einstellungen importieren/exportieren**, um die Einstellungen aus einer *.xml*-Konfigurationsdatei zu laden oder die aktuellen Einstellungen in einer Konfigurationsdatei zu speichern. Ausführliche Informationen hierzu finden Sie unter Einstellungen importieren/exportieren.

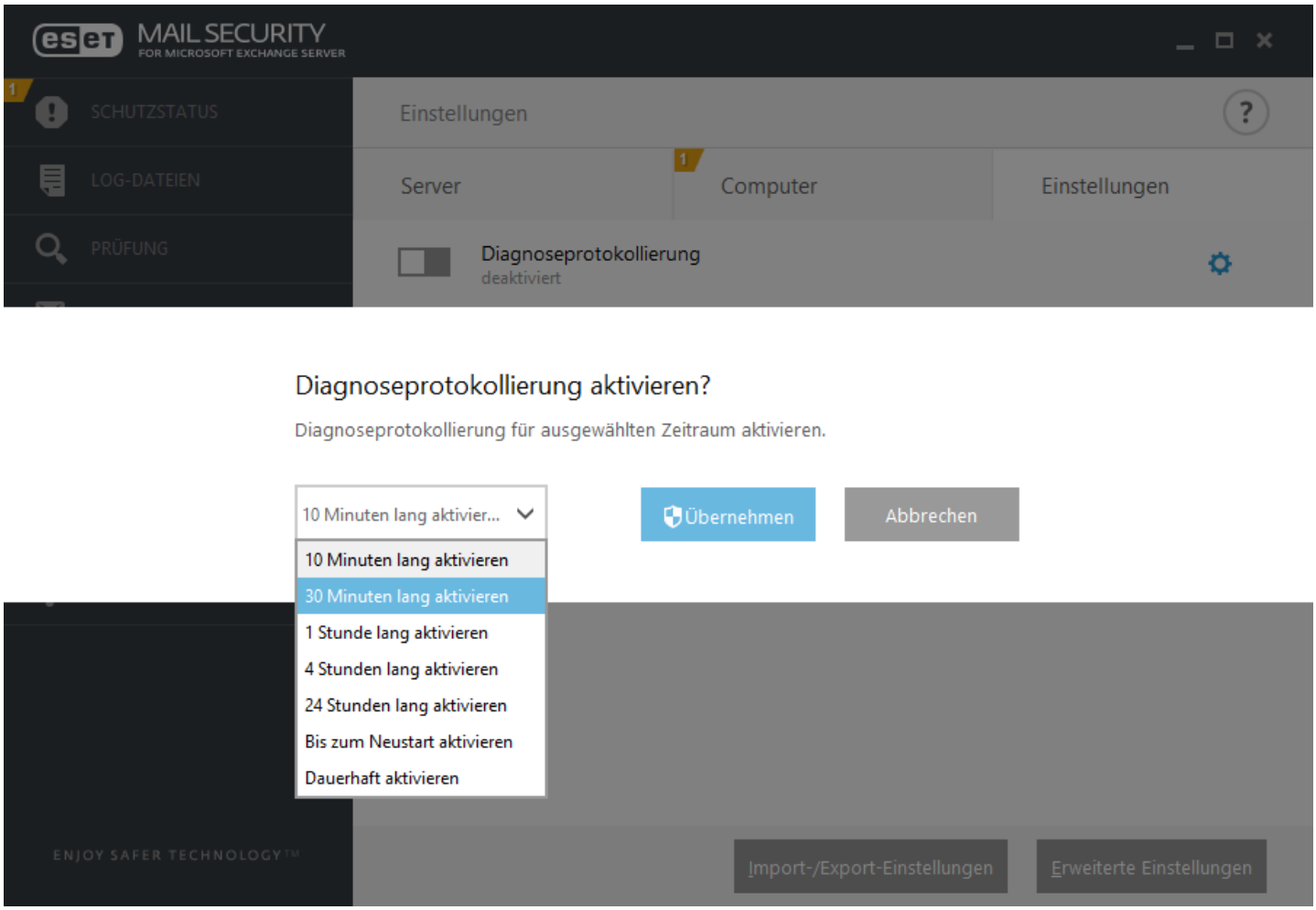
Wenn Sie weitere Optionen festlegen möchten, klicken Sie auf **Erweiterte Einstellungen** oder drücken Sie die Taste **F5**.

4.6.3 Tools

Diagnose-Logging - Konfigurieren Sie, welche Komponenten Diagnose-Logs erstellen, wenn Diagnose-Logging aktiviert ist. Wenn Sie das Diagnose-Logging aktivieren, können Sie auswählen, für welchen Zeitraum dieses Feature aktiviert werden soll (10 Minuten, 30 Minuten, 1 Stunde, 4 Stunden, 24 Stunden, bis zum nächsten Serverneustart oder permanent). Die nicht in dieser Registerkarte angezeigten Komponenten erstellen generell Diagnose-Logs.



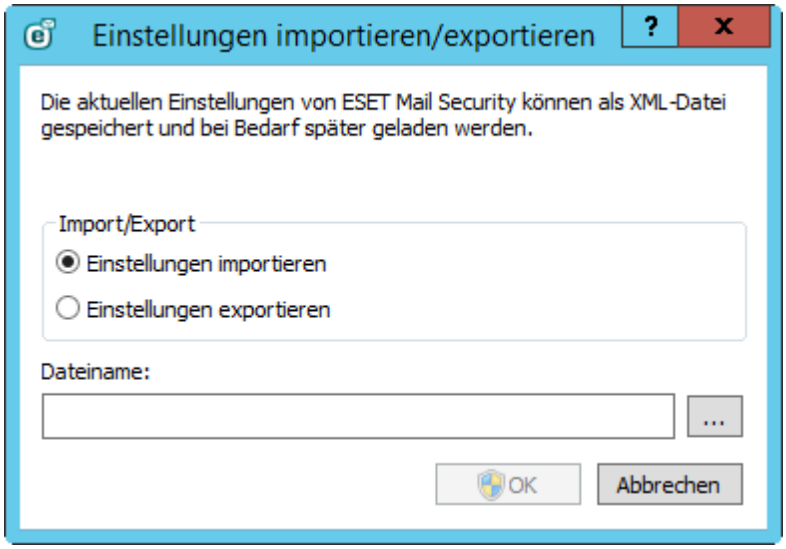
- **Diagnoseprotokollierung** für ausgewählten Zeitraum aktivieren.



4.6.4 Einstellungen importieren/exportieren

Um die Konfiguration von ESET Mail Security zu importieren oder exportieren, klicken Sie unter **Einstellungen** auf **Einstellungen importieren/exportieren**.

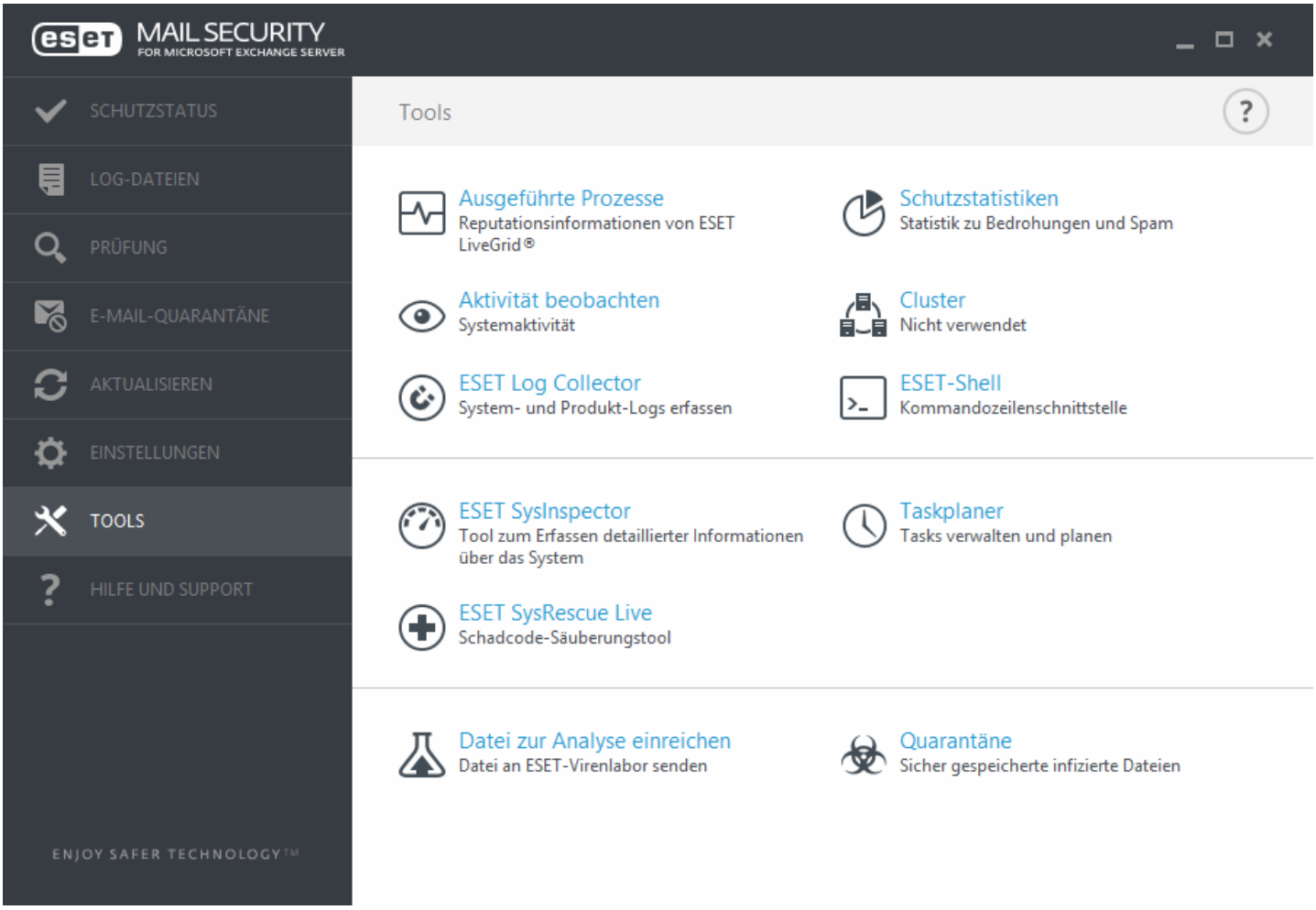
Für das Importieren und Exportieren wird das XML-Dateiformat verwendet. Die Import- und Exportfunktionen sind hilfreich, wenn Sie die aktuelle Konfiguration von ESET Mail Security sichern möchten. Sie können die exportierten Einstellungen dann später auf anderen Computern importieren, um sie dort anzuwenden.



4.7 Tools

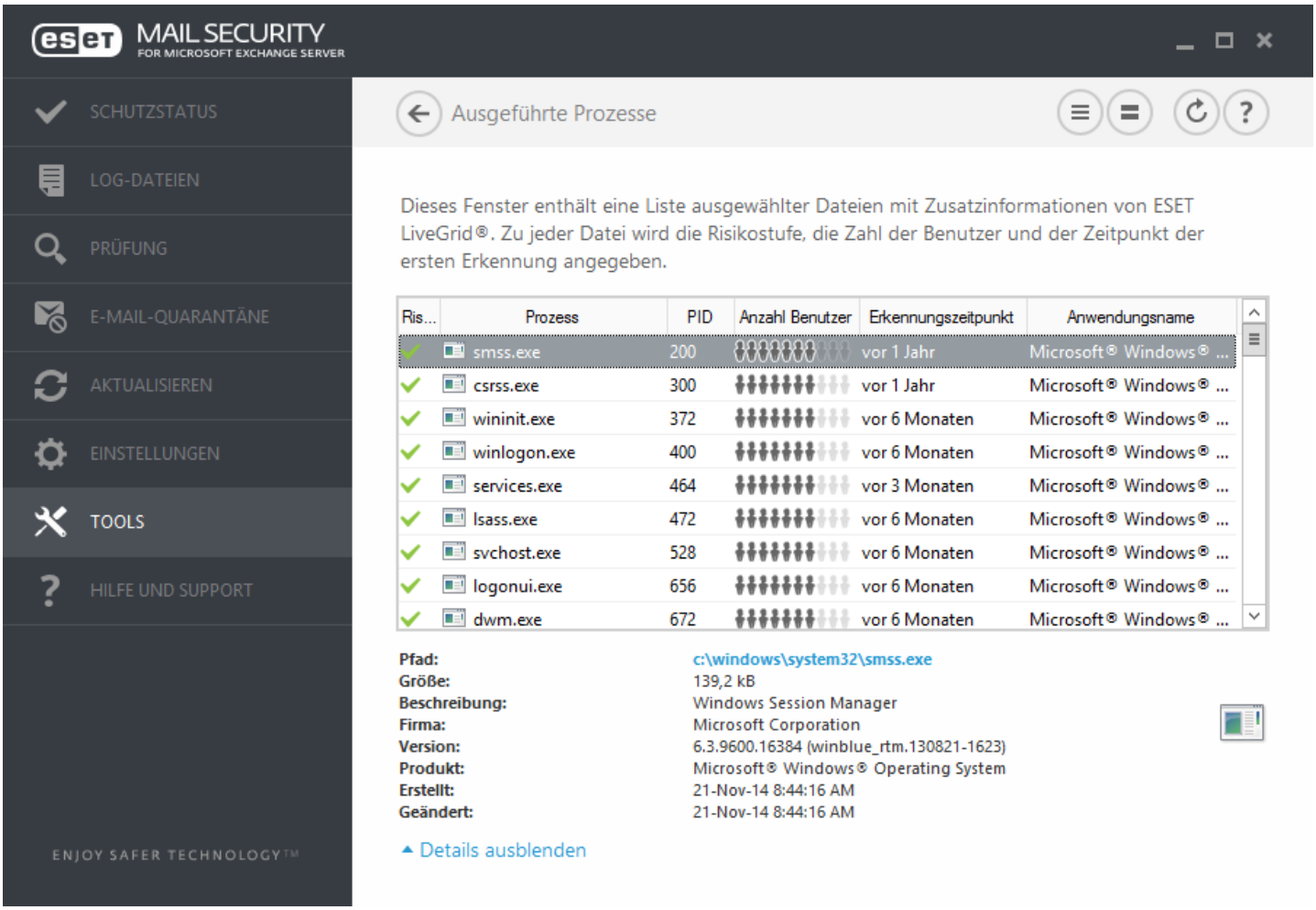
Das Tools-Menü enthält Module, die die Verwaltung des Programms vereinfachen und zusätzliche Optionen bereitstellen. Es umfasst folgende Tools:

- Ausgeführte Prozesse
- Aktivität beobachten
- ESET Log Collector
- Schutzstatistiken
- Cluster
- ESET-Shell
- ESET SysInspector
- ESET SysRescue Live
- Taskplaner
- Datei zur Analyse einreichen
- Quarantäne



4.7.1 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 Live Grid-Technologie zu bieten.



Risikostufe - Um Objekten wie Dateien, Prozessen, Registrierungsschlüsseln usw. eine Risikostufe zuzuordnen, verwenden ESET Mail Security und die ESET Live Grid-Technologie in der Regel einen Satz heuristischer Regeln, mit denen die Merkmale des Objekts untersucht werden, um anschließend nach entsprechender Gewichtung das Potenzial für schädliche Aktivitäten abzuschätzen. Basierend auf dieser Heuristik wird Objekten dann eine Risikostufe zugewiesen, von 1 - In Ordnung (grün) bis 9 - Risikoreich(rot).

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 - Stellt eine ID der in Windows-Betriebssystemen ausgeführten Prozessen dar.

HINWEIS: Bekannte Anwendungen, die als In Ordnung (grün) markiert sind, sind in jedem Fall sauber (Positivliste) und werden vom Scan ausgenommen. Dadurch wird die Geschwindigkeit des On-Demand-Scans bzw. des Echtzeit-Dateischutzes auf Ihrem Computer erhöht.

Anzahl Benutzer - gibt die Anzahl der Benutzer an, die eine bestimmte Anwendung verwenden. Diese Informationen werden von der ESET Live Grid-Technologie gesammelt.

Erkennungszeitpunkt - Zeitspanne seit der Erkennung der Anwendung durch die ESET Live Grid-Technologie.

HINWEIS: Wenn eine Anwendung als Unbekannt (orange) eingestuft wurde, muss es sich nicht zwangsläufig um Schadsoftware handeln. In der Regel ist es einfach eine neuere Anwendung. Wenn Sie sich bei einer Datei unsicher

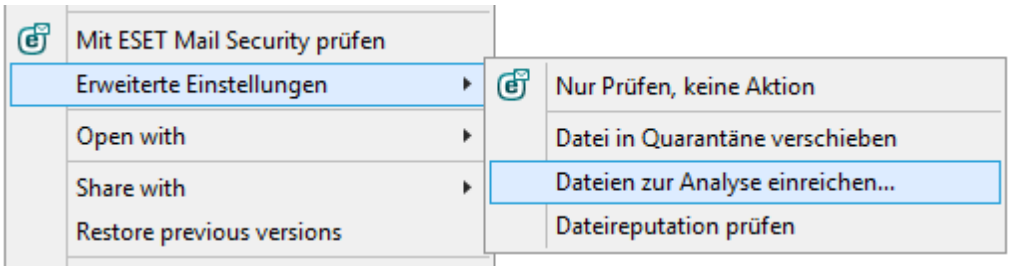
sind, können Sie diese über die Funktion Datei zur Analyse einreichen an ESET übermitteln. Wenn sich herausstellt, dass die Datei Schadcode enthält, werden entsprechende Erkennungsfunktionen in zukünftigen Updates der Signaturdatenbank berücksichtigt.

Anwendungsname - Der festgelegte Name des Programms, zu dem der Prozess gehört.

Wenn Sie unten auf eine Anwendung klicken, werden unten im Fenster die folgenden Informationen angezeigt:

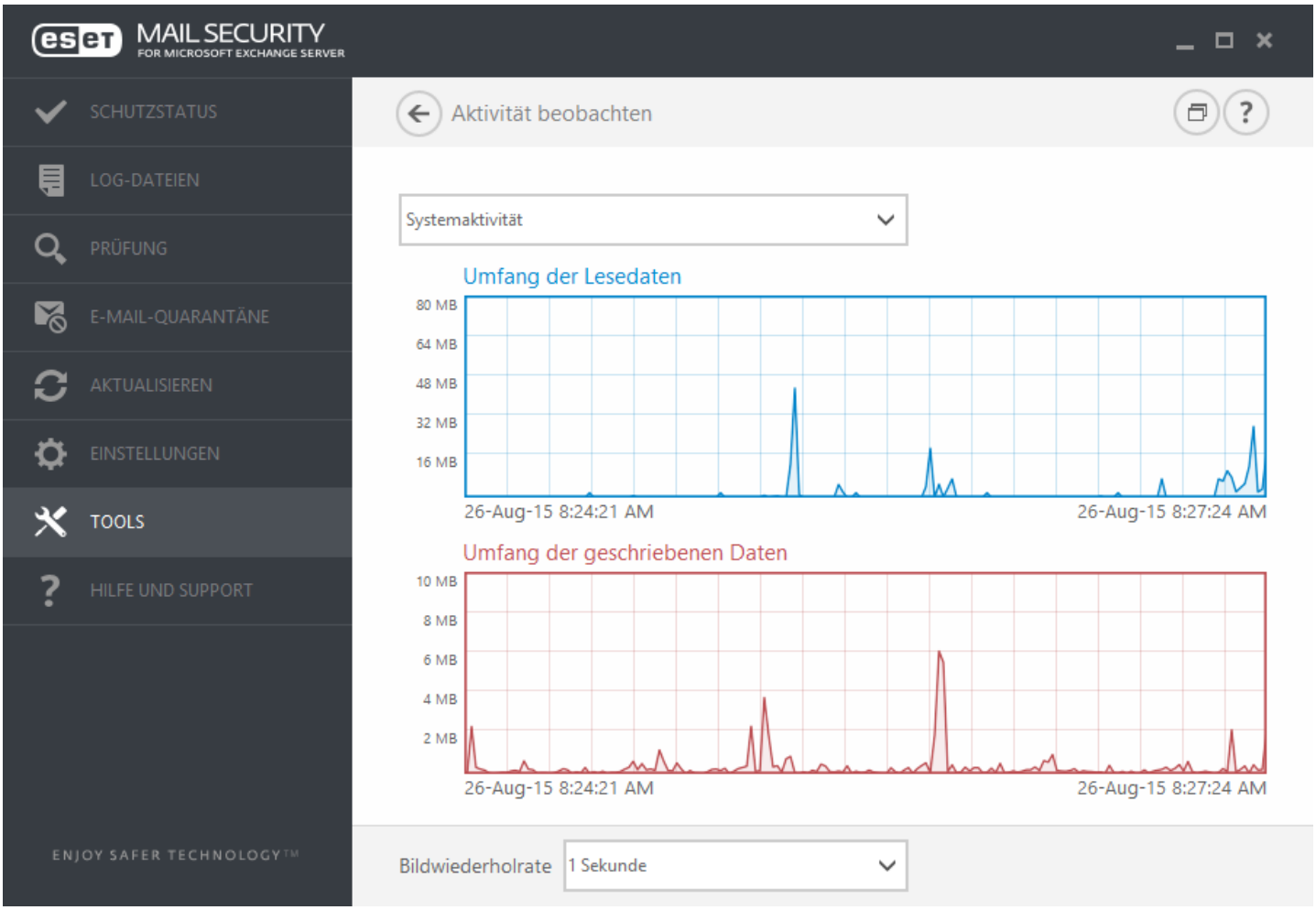
- **Pfad** - Speicherort einer Anwendung auf Ihrem Computer.
- **Größe** - Dateigröße entweder in KB (Kilobyte) oder MB (Megabyte).
- **Beschreibung** - Dateieigenschaften auf Basis der Beschreibung des Betriebssystems.
- **Firma** - Name des Herstellers oder des Anwendungsprozesses.
- **Version** - 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 Erstellung einer Anwendung.

HINWEIS: Der Reputations-Check kann auch auf Dateien angewendet werden, die nicht als Programme/Prozesse ausgeführt werden. - Markieren Sie die Dateien, die Sie überprüfen möchten, klicken Sie die Dateien mit der rechten Maustaste an und wählen Sie im Kontextmenü **Erweiterte Einstellungen** > **Dateireputation mit ESET Live Grid überprüfen** aus.



4.7.2 Aktivität beobachten

Um die aktuelle **Dateisystemaktivität** und **E-Mail-Serveraktivität** als Diagramm anzuzeigen, klicken Sie auf **Tools** > **Aktivität beobachten**. Stellt die Menge der gelesenen und geschriebenen Daten im System in zwei Grafiken dar. Im unteren Bereich des Diagramms befindet sich eine Zeitleiste, welche die Systemaktivität in Echtzeit innerhalb des gewählten Zeitraums aufzeichnet. Um die Zeitleiste zu ändern, wählen Sie im Dropdown-Menü **Bildwiederholrate** einen Wert aus.



Die folgenden Optionen stehen zur Verfügung:

- **1 Sekunde** - Das Diagramm wird jede Sekunde aktualisiert, und die Zeitleiste umfasst die letzten 10 Minuten.
- **1 Minute (letzte 24 Stunden)** - Das Diagramm wird jede Minute aktualisiert. Die Zeitleiste deckt die letzten 24 Stunden.
- **1 Stunde (letzter Monat)** - Das Diagramm wird jede Stunde aktualisiert. Die Zeitleiste deckt den letzten Monat.
- **Schritt: 1 Stunde (ausgewählter Monat)** - Das Diagramm wird jede Stunde aktualisiert. Die Zeitleiste deckt den ausgewählten Monat. Klicken Sie auf **Monat ändern**, um Ihre Auswahl zu ändern.

Die vertikale Achse im **Systemaktivitätsdiagramm** bildet die Menge an gelesenen (blau) und geschriebenen Daten (rot) ab. Beide Werte werde in KB (Kilobyte)/MB/GB angegeben. Wenn Sie mit dem Mauszeiger über die gelesenen oder geschriebenen Daten in der Legende unterhalb des Diagramms fahren, werden im Diagramm nur die Daten für diesen Aktivitätstyp angezeigt.

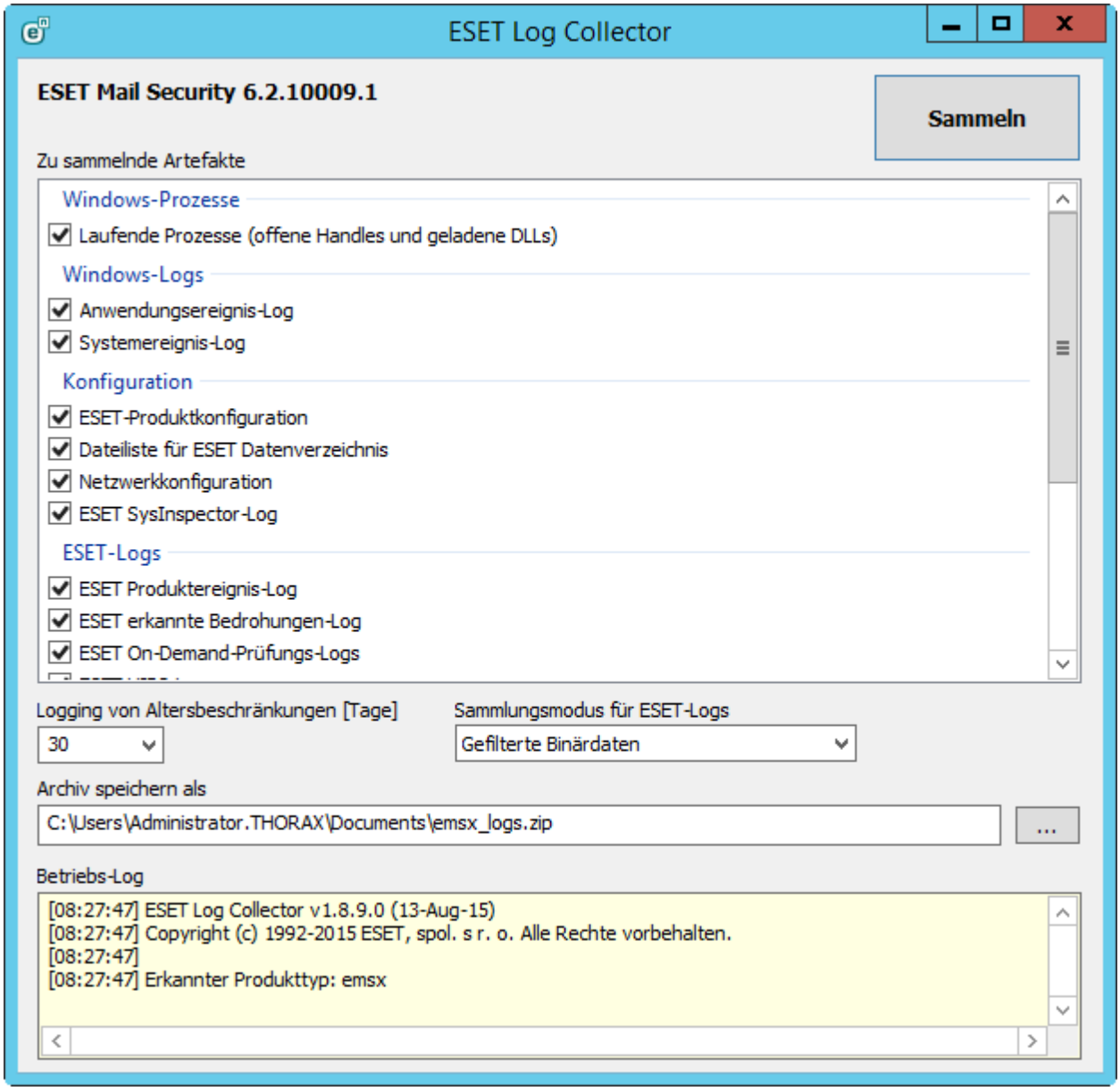
4.7.2.1 Zeitraum auswählen

Wählen Sie einen Monat (und ein Jahr) aus, für das Sie die **Dateisystemaktivität** bzw. die **Aktivität des E-Mail-Servers** in der Grafik anzeigen möchten.

4.7.3 ESET Log Collector

ESET Log Collector ist eine Anwendung zum automatischen Erfassen von Informationen wie Konfigurationsdetails und Logs eines Computers, die zur schnelleren Fehlerbehebung eingesetzt werden können. Wenn Sie die Unterstützung des ESET-Supports anfordern, werden Sie unter Umständen aufgefordert, Logs von Ihrem Computer bereitzustellen. Mit dem ESET Log Collector können Sie die benötigten Informationen ganz einfach sammeln.

Der ESET Log Collector kann über das Hauptmenü aufgerufen werden, indem Sie auf **Tools** > **ESET Log Collector** klicken.



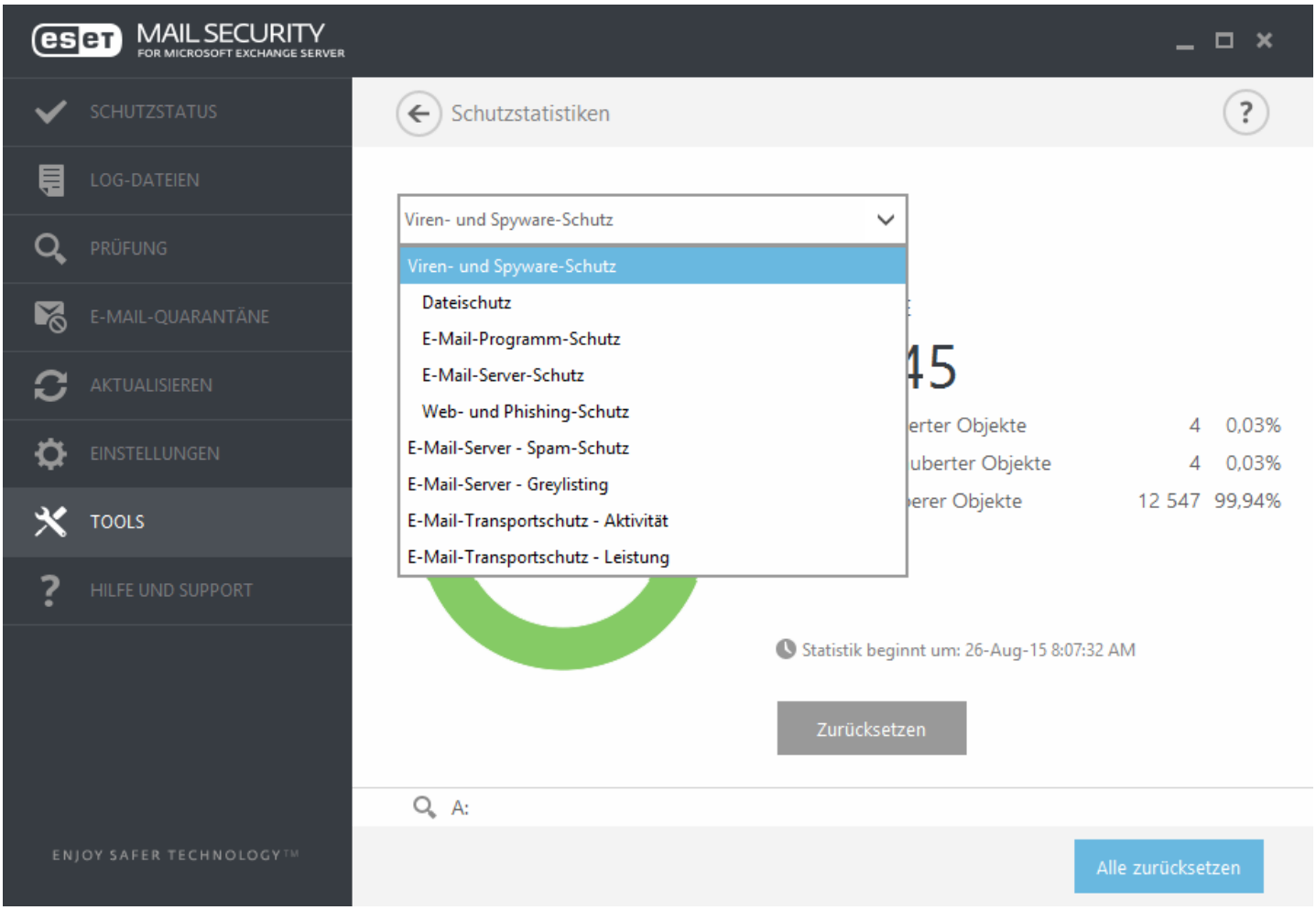
Aktivieren Sie die entsprechenden Kontrollkästchen der Logs, die Sie erfassen möchten. Wenn Sie sich nicht sicher sind, welche Logs erfasst werden sollen, lassen Sie alle Kontrollkästchen aktiviert (Standardeinstellung). Geben Sie den Speicherort für die Archivdateien an und klicken Sie auf **Speichern**. Der Archivdateiname ist bereits vordefiniert. Klicken Sie auf **Erfassen**.

Während des Erfassens können Sie unten im Fenster des Betriebs-Logs anzeigen, welcher Vorgang gerade ausgeführt wird. Nach dem Abschluss des Vorgangs sind die Dateien erfasst und archiviert und werden angezeigt. Dies bedeutet, dass die Erfassung erfolgreich war und die Archivdatei (zum Beispiel `emsx_logs.zip`) am angegebenen Speicherort gespeichert wurde.

Weitere Informationen zu ESET Log Collector und zur Liste der Dateien, die von ESET Log Collector erfasst werden, finden Sie in der ESET-Knowledgebase.

4.7.4 Schutzstatistiken

Klicken Sie auf **Tools** > **Schutzstatistiken**, um statistische Daten zu den Schutzmodulen von ESET Mail Security in einem Diagramm anzuzeigen. Wählen Sie das gewünschte Schutzmodul im Dropdown-Menü aus, um das entsprechende Diagramm und die Legende zu öffnen. Bewegen Sie den Mauszeiger über einen bestimmten Punkt in der Legende, um im Diagramm nur die Daten für diesen Punkt anzuzeigen.



Folgende Diagramme stehen zur Auswahl:

- **Viren- und Spyware-Schutz** - Gesamtanzahl infizierter und gesäuberter Objekte.
- **Dateischutz** - Objekte, die aus dem Dateisystem gelesen oder in das Dateisystem geschrieben wurden.
- **E-Mail-Schutz** - Objekte, die von E-Mail-Programmen gesendet oder empfangen wurden.
- **E-Mail-Server-Schutz** - Statistiken zum Viren- und Spyware-Schutz für den E-Mail-Server.
- **Web- und Phishing-Schutz** - Objekte, die von einem Webbrowser heruntergeladen wurden.
- **E-Mail-Spam-Schutz** - Spam-Schutz-Statistiken seit dem letzten Systemstart.
- **E-Mail-Server - Greylisting** - Spam-Schutz-Statistiken für die Greylisting-Methode.
- **E-Mail-Server-Schutz - Aktivität** - Objekte, die vom E-Mail-Server geprüft/blockiert/gelöscht wurden.
- **Performancedaten zum E-Mail-Server-Schutz** - 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**).

Neben dem Statistik-Diagramm wird die Gesamtanzahl der geprüften, infizierten, gesäuberten und sauberen Objekte angezeigt. Klicken Sie auf **Zurücksetzen**, um die Statistikdaten zu löschen, oder auf **Alle zurücksetzen**, um alle vorhandenen Daten zu löschen und zu entfernen.

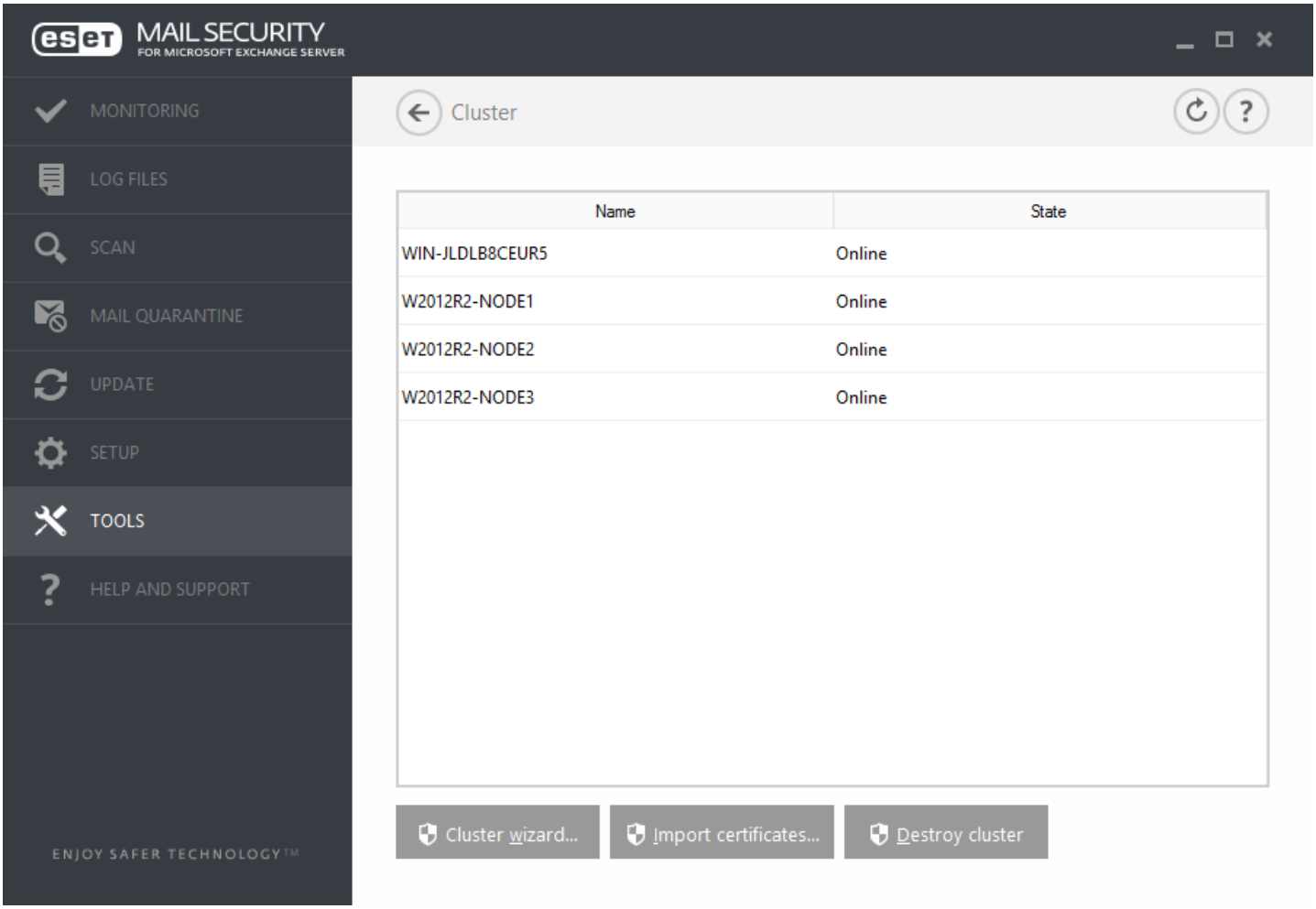
4.7.5 Cluster

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

Mit dieser Infrastruktur können ESET-Serverprodukte miteinander kommunizieren, Daten wie Konfigurationsdaten und Benachrichtigungen austauschen 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 die gleiche Konfiguration aufweisen muss. ESET-Cluster gewährleistet diese erforderliche Konsistenz der Instanzen.

HINWEIS: Die Einstellungen für die Benutzeroberfläche werden nicht zwischen ESET-Clusterknoten synchronisiert.

Die Statusseite für ESET-Cluster finden Sie im Hauptmenü unter **Tools** > **Cluster**. Richtig konfiguriert sieht die Statusseite folgendermaßen aus:



Klicken Sie auf **Clusterassistent, um den ESET-Cluster einzurichten.** Ausführliche Informationen zum Einrichten des ESET-Cluster mithilfe des Assistenten finden Sie hier.

Beim Einrichten des ESET-Cluster stehen zwei Methoden zum Hinzufügen von Knoten zur Verfügung: automatisch über einen vorhandenen Windows-Failover-Cluster/NLB-Cluster oder manuell durch Suchen nach Computern in einer Arbeitsgruppe oder Domäne.

Autom. erkennen - ermöglicht das automatische Erkennen von Knoten, die bereits Mitglied eines Windows-Failover-Cluster/NLB-Cluster sind, und fügt diese zum ESET-Cluster hinzu
Durchsuchen - Sie können Knoten manuell durch Eingeben der Servernamen hinzufügen (entweder Mitglieder der gleichen Arbeitsgruppe oder der gleichen Domäne)

HINWEIS: Zur Verwendung der ESET-Clusterfunktion müssen die Server nicht Mitglied eines Windows-Failover-

Clusters/NLB-Clusters sein. Zur Verwendung von ESET-Clustern ist in Ihrer Umgebung kein Windows-Failover-Cluster oder NLB-Cluster erforderlich.

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.

HINWEIS: Domänenknoten und Arbeitsgruppenknoten können nicht kombiniert werden.

Eine weitere Anforderung für die Verwendung eines ESET-Clusters ist, dass die **Datei- und Druckerfreigabe** in der Windows-Firewall aktiviert werden muss, bevor die ESET Mail Security-Installation auf den ESET-Knoten ausgeführt wird.

Der ESET-Cluster kann ganz einfach durch Klicken auf **Cluster zerstören** zerlegt werden. Jeder Knoten schreibt einen Eintrag in den eigenen Ereignis-Log, der auf die Zerstörung des ESET-Cluster hinweist. Anschließend werden alle ESET-Firewall-Regeln von der Windows-Firewall entfernt. Die früheren Knoten werden daraufhin in ihren vorigen Zustand zurückversetzt und können je nach Bedarf erneut in einem anderen ESET-Cluster verwendet werden.

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

Sie können jederzeit neue Knoten zu einem vorhandenen ESET-Cluster hinzufügen. Führen Sie dazu den **Clusterassistenten** wie weiter oben und hier beschrieben aus.

Weitere Informationen zur Konfiguration von ESET-Clustern finden Sie im Abschnitt Arbeits-Cluster.

4.7.6 ESET-Shell

eShell (Abkürzung für ESET Shell) ist eine Kommandozeilen-Schnittstelle für ESET Mail Security. Es handelt sich dabei um eine Alternative zur grafischen Benutzeroberfläche (GUI). 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. Des Weiteren ist eShell für jene Benutzer attraktiv, die die Kommandozeile generell der Benutzeroberfläche vorziehen.

eShell kann in den folgenden beiden Modi ausgeführt werden:

- Interaktiver Modus: Dieser Modus eignet sich, wenn Sie umfassend mit eShell arbeiten möchten (also nicht nur einen einzelnen Befehl 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.
- 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 hierzu in der Windows-Eingabeaufforderung `eshell` mit den entsprechenden Parametern ein. Beispiel:

```
eshell get status
```

oder

`eshell set antivirus status disabled`

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

HINWEIS: Um den vollständigen Funktionsumfang zu nutzen, sollten Sie eShell mit der Option **Als Administrator ausführen** starten. Dies gilt auch, wenn Sie einzelne Befehle über die Windows-Einfabeaufforderung (cmd) eingeben. Öffnen Sie die Eingabeaufforderung mit **Als Administrator ausführen**. Andernfalls können Sie nicht alle Befehle ausführen. Dies liegt daran, dass Sie nicht über ausreichende Berechtigungen verfügen, wenn Sie die Eingabeaufforderung oder eShell mit einem anderen als dem Administratorkonto öffnen.

HINWEIS: Um eShell-Befehle über die Windows-Eingabeaufforderung einzugeben oder Batch-Dateien auszuführen, müssen Sie einige Einstellungen vornehmen. Weitere Informationen zum Ausführen von Batch-Dateien finden Sie hier.

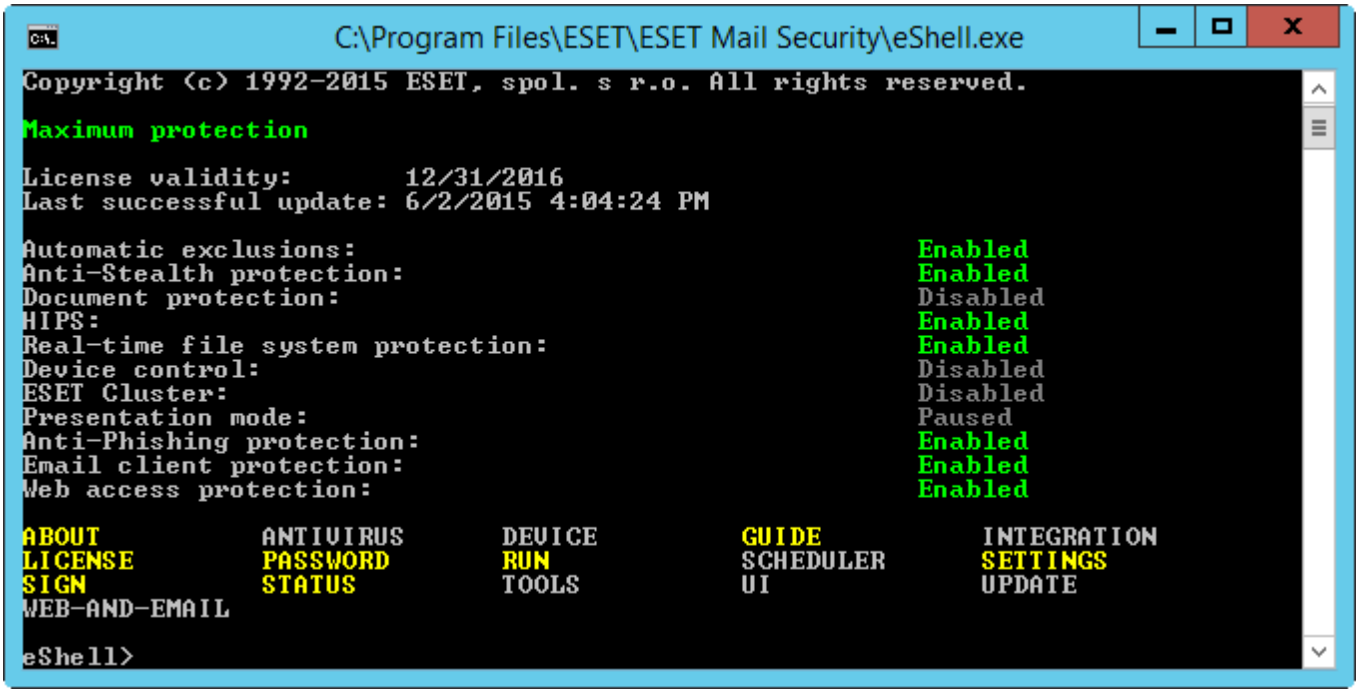
Den interaktiven eShell-Modus können Sie auf zwei Arten aktivieren:

- Über das Windows-Startmenü: **Start** > **Alle Programme** > **ESET** > **ESET File Security** > **ESET Shell**
- Über die Windows-Eingabeaufforderung: Geben Sie `eshell` ein und drücken Sie die Eingabetaste.

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

HINWEIS: Wenn Sie diesen Bildschirm später erneut aufrufen möchten, geben Sie den Befehl `guide` ein. Darin werden Ihnen ein paar einfache Beispiele für die Verwendung von eShell sowie Informationen zu Syntax, Präfixen, Befehlspfaden, Abkürzungen, Aliasnamen usw. angezeigt. Es handelt sich also um eine kurze Einführung in eShell.

Bei der nächsten Ausführung von eShell wird dieser Bildschirm angezeigt:



HINWEIS: Groß- und Kleinschreibung ist für Befehle nicht relevant. 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.

4.7.6.1 Verwendung

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 wird in eShell folgende Syntax verwendet:

[<Präfix>] [<Befehlspfad>] <Befehl> [<Argumente>]

Beispiel (aktiviert den Dokumentenschutz):
`SET ANTIVIRUS DOCUMENT STATUS ENABLED`

`SET` - Ein Präfix
`ANTIVIRUS DOCUMENT` - Pfad zu einem bestimmten Befehl, also der Kontext des Befehls
`STATUS` - Der eigentliche Befehl
`ENABLED` - Ein Argument für den Befehl

Wenn Sie `?` als Argument für einen Befehl eingeben, wird die Syntax des entsprechenden Befehls angezeigt. Zum Beispiel zeigt `STATUS ?` die Syntax des Befehls `STATUS` an:

SYNTAX:
```
[get] | status
set status enabled | disabled
```

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.

HINWEIS: 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 stellt einen Vorgang dar. Das Präfix `GET` zeigt die Konfiguration einer bestimmten ESET Mail Security-Funktion oder den Status an (z. B. zeigt `GET ANTIVIRUS STATUS` den aktuellen Schutzstatus an). Das Präfix `SET` konfiguriert die Funktion bzw. ändert ihren Status (`SET ANTIVIRUS STATUS ENABLED` aktiviert den Schutz).

Die nachfolgend genannten Präfixe stehen in eShell zur Verfügung. Je nach Befehl werden bestimmte Präfixe unterstützt.

`GET` - Aktuelle Einstellung/Status zurückgeben
`SET` - Wert/Status festlegen
`SELECT` - Element auswählen
`ADD` - Element hinzufügen
`REMOVE` - Element entfernen
`CLEAR` - Alle Elemente/Dateien entfernen
`START` - Aktion starten
`STOP` - Aktion beenden
`PAUSE` - Aktion anhalten
`RESUME` - Aktion fortsetzen
`RESTORE` - Standardeinstellungen/-objekt/-datei wiederherstellen
`SEND` - Objekt/Datei senden
`IMPORT` - Aus Datei importieren
`EXPORT` - In Datei exportieren

Präfixe wie `GET` und `SET` werden für viele, aber nicht alle Befehle verwendet. Der Befehl `EXIT` erfordert 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 entweder einen Befehl ausführen oder den Kontextnamen eingeben, um auf die entsprechende Ebene zu gelangen. 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 Punke). Nehmen wir beispielsweise an, Sie befinden sich hier:

```
antivirus startup>
```

Geben Sie `..` ein und Sie gelangen auf die nächsthöhere Ebene, nämlich:

```
eShell antivirus>
```

Wenn Sie dagegen von `antivirus startup>` 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 `..`, um zur gewünschten Ebene zu gelangen. 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 aufgerufen wird. Um zum Beispiel `GET ANTIVIRUS STATUS` auszuführen, geben Sie ein:

`GET ANTIVIRUS STATUS` - wenn Sie sich im Root-Kontext befinden (Kommandozeile zeigt an: `eShell>`)
`GET STATUS` - wenn Sie sich im Kontext `ANTIVIRUS` befinden (Kommandozeile zeigt an: `eShell antivirus>`)
`.. GET STATUS` - wenn Sie sich im Kontext `ANTIVIRUS STARTUP` befinden (Kommandozeile zeigt an: `eShell antivirus startup>`)

HINWEIS: Sie können einen einfachen `.` (Punkt) anstelle von zwei Punkten `..` verwenden, weil ein einzelner Punkt eine Abkürzung für zwei Punkte ist. Beispiel:

`. GET STATUS` - wenn Sie sich im Kontext `ANTIVIRUS STARTUP` befinden (Kommandozeile zeigt an: `eShell antivirus startup>`)

Argument
Ein Argument ist eine Aktion, die für einen bestimmten Befehl ausgeführt wird. Der Befehl `CLEAN-LEVEL` (in `ANTIVIRUS REALTIME ENGINE`) kann mit den folgenden Argumenten verwendet werden:

`no` - keine Säuberung
`normal` - Normale Säuberung
`strict` - Immer versuchen, automatisch zu entfernen

Weitere Beispiele sind die Argumente `ENABLED` oder `DISABLED` zur Aktivierung/Deaktivierung einer bestimmten Option oder Funktion.

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.

Beispiele für die Kurzform:

```
set status enabled => set stat en
add antivirus common scanner-excludes C:\path\file.ext => add ant com scann C:\path\file.ext
```

Wenn zwei Befehle oder Kontexte gleich beginnen (z. B. `ABOUT` und `ANTIVIRUS`) und Sie `A` als verkürzte Befehlsform wählen, kann eShell nicht bestimmen, welchen der beiden Befehle Sie ausführen möchten. Es werden dann eine Fehlermeldung und eine Liste der verfügbaren Befehle mit dem Anfangsbuchstaben A angezeigt:

```
eShell>a
Der folgende Befehl ist nicht eindeutig: a

In diesem Kontext sind die folgenden Befehle verfügbar:
ABOUT - Informationen über das Programm anzeigen
ANTIVIRUS - Zum Kontext antivirus wechseln
```

Das Hinzufügen von mindestens einem Buchstaben (z. B. `AB` anstelle von `A`) hat zur Folge, dass eShell den Befehl `ABOUT` ausführt, da die Abkürzung nun eindeutig ist.

HINWEIS: Um die korrekte Ausführung des Befehls sicherzustellen, wird empfohlen, Befehle, Argumente usw. nicht abzukürzen, sondern vollständig anzugeben. Auf diese Weise erfolgt die Ausführung wie von Ihnen gewünscht und unerwünschte Fehler werden vermieden. Dies betrifft vor allem Batch-Dateien und Skripte.

Automatische Vervollständigung
Ein neues Feature in eShell seit der Version 2.0. Entspricht der automatischen Vervollständigung in der Windows-Befehlszeile. Während die Windows-Befehlszeile nur Dateipfade vervollständigt, führt eShell diese Funktion ebenfalls für Befehle, Kontext- und Vorgangsnamen aus. Die Vervollständigung von Argumenten wird nicht unterstützt. Drücken Sie bei der Eingabe eines Befehls einfach die TAB-Taste, um den Befehl zu vervollständigen oder durch die möglichen Variationen zu blättern. Drücken Sie UMSCH + 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 `antivir real scan` eingeben, geschieht beim Drücken von TAB nichts. Geben Sie stattdessen `antivir` ein, drücken Sie Tab, um `antivirus`zu vervollständigen, geben Sie dann real + TAB und scan + TAB ein. Anschließend können Sie durch alle möglichen Variationen blättern: scan-create, scan-execute, scan-open, etc.

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
`antivirus on-demand log` - tools log scans

Mit „(global)“ wird angezeigt, dass der Befehl kontextunabhängig verwendet werden kann. Einem Befehl können

mehrere Aliasnamen zugewiesen werden. So hat der Befehl EXIT z. B. die Aliasnamen CLOSE, QUIT und BYE. Wenn Sie eShell beenden möchten, können Sie den Befehl EXIT oder einen seiner Aliasnamen verwenden. Das Alias 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).

Mit eShell können Sie eigene Aliasnamen festlegen. Der Befehl ALIAS existiert im Kontext UI ESHELL .

Einstellungen mit Passwort schützen
Einstellungen können mit einem Passwort geschützt werden. Sie können das Passwort in der Benutzeroberfläche oder in eShell mithilfe des Befehls `set ui access lock-password` setzen. 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 das Passwort in eShell mit dem Befehl `set password` speichern. Das Passwort wird anschließend automatisch für alle Skripts ausgefüllt, für deren Ausführung ein Passwort erforderlich ist. Das Passwort bleibt gespeichert, bis Sie eShell verlassen. Sie müssen `set password` also erneut verwenden, wenn Sie Ihr Passwort in einer neuen Sitzung von eShell erneut speichern möchten.

Guide / Help
Beim Ausführen des Befehls GUIDE oder HELP wird ein Bildschirm mit Benutzungshinweisen für eShell angezeigt. Dieser Befehl wird im Kontext ROOT aufgerufen (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 „Auf“ und „Ab“ können Sie durch den Verlauf blättern. 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 wird verwendet, um den Bildschirm zu löschen. 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).

4.7.6.2 Befehle

In diesem Abschnitt werden einige grundlegende eShell-Befehle mit einer Beschreibung aufgelistet.

HINWEIS: 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. Die Liste umfasst den Namen des installierten Produkts, die Versionsnummer, installierte Komponenten (und die jeweilige Versionsnummer) sowie grundlegende Informationen zum Server und dem Betriebssystem, auf dem ESET Mail Security ausgeführt wird.

KONTEXTPFAD:

```
root
```

PASSWORD

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 Virenschutzes zur Folge haben oder die Funktion von ESET Mail Security beeinflussen könnten. Jedes Mal, wenn ein solcher Befehl ausgeführt werden soll, muss das Passwort eingegeben werden. Um das Passwort nicht jedes Mal selbst eingeben zu müssen, können Sie es festlegen. eShell ruft das Passwort dann automatisch ab, wenn ein passwortgeschützter Befehl ausgeführt werden soll. Auf diese Weise müssen Sie das Passwort nicht jedes Mal eigenhändig eingeben.

HINWEIS: 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 ist auch bei der Ausführung von Batch-Dateien/Skripten von Nutzen. Hier ein Beispiel für eine solche Batch-Datei:

```
eshell start batch "&" set password plain <IhrPasswort> "&" set status disabled
```

Dieser verkettete Befehl startet den Batch-Modus, legt das Passwort fest und deaktiviert den Schutz.

KONTEXTPFAD:

`root`

SYNTAX:

`[get] | restore password`

`set password [plain <Passwort>]`

VORGÄNGE:

`get` - Passwort anzeigen

`set` - Passwort speichern oder löschen

`restore` - Passwort löschen

ARGUMENTE:

`plain` - Passwort als Parameter eingeben

`Passwort` - Passwort

BEISPIELE:

`set password plain <IhrPasswort>` - Legt das Passwort für passwortgeschützte Befehle fest

`restore password` - Löscht das Passwort

BEISPIELE:

`get password` - Mit diesem Befehl können Sie überprüfen, ob ein Passwort konfiguriert wurde. Es werden nur „*“ (Sternchen) angezeigt, nicht das eigentliche Passwort. Werden keine Sternchen angezeigt, so wurde auch kein Passwort festgelegt.

`set password plain <IhrPasswort>` - Festgelegtes Passwort speichern

`restore password` - Festgelegtes Passwort löschen

STATUS

Zeigt den aktuellen Schutzstatus von ESET Mail Security (wie auf der Benutzeroberfläche) an.

KONTEXTPFAD:

`root`

SYNTAX:

`[get] | restore status`

`set status disabled | enabled`

VORGÄNGE:

`get` - Status des Virenschutzes anzeigen

`set` - Virenschutz deaktivieren/aktivieren

`restore` - Standardeinstellungen wiederherstellen

ARGUMENTE:

`disabled` - Virenschutz deaktivieren

`enabled` - Virenschutz aktivieren

BEISPIELE:

`get status` - Aktuellen Schutzstatus anzeigen

`set status disabled` - Schutz deaktivieren

`restore status` - Standard-Schutzeinstellung wiederherstellen (aktiviert)

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.

4.7.6.3 Batchdateien / Skripts

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

```
eshell get antivirus 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 Meldung "Kein Task ausgewählt oder ausgewählter Task ist nicht mehr vorhanden" fehl.

Aus Sicherheitsgründen ist die Ausführungsrichtlinie standardmäßig auf "Eingeschränktes Skripting" beschränkt. Damit können Sie eShell als Überwachungstool verwenden, jedoch keine Konfigurationsänderungen an ESET Mail Security vornehmen. Bei sicherheitsrelevanten Befehlen, z. B. beim Deaktivieren des Schutzes, erhalten Sie die Nachricht **Zugriff verweigert**. Um Befehle mit Konfigurationsänderungen auszuführen, empfehlen wir die Verwendung von signierten Batchdateien.

Falls Sie aus irgendeinem Grund die Konfiguration mit einzelnen Befehlen in der Windows-Befehlszeile ändern möchten, 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. Alternativ können Sie dies in der Benutzeroberfläche unter **Erweiterte Einstellungen** > **Benutzeroberfläche** > ESET-Shell konfigurieren.

Mit signierten Batchdateien
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. Sie können dies entweder in der Benutzeroberfläche oder in eShell mithilfe des Befehls `set ui access lock-password` konfigurieren. Sobald Sie das Passwort für den Schutz der Einstellungen eingerichtet haben, können Sie Batchdateien signieren.

Um eine Batchdatei zu signieren, führen Sie `sign <script.bat>` 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 dem 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 Signatur durch die neue Signatur ersetzt.

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

HINWEIS: Wenn Sie das Passwort für den Schutz der Einstellungen ändern, müssen Sie alle Skripte erneut signieren, da diese andernfalls fehlschlagen werden, sobald Sie das Passwort ändern. Dies liegt daran, dass das beim Signieren der Skripte eingegebene Passwort mit dem Passwort für den Schutz der Einstellungen auf dem Zielsystem übereinstimmen muss.

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

4.7.7 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.

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:

- **Öffnen** - Öffnet das erstellte Log. Sie können ein Log auch öffnen, indem Sie mit der rechten Maustaste auf das erstellte Log klicken und im Kontextmenü **Anzeigen** auswählen.
- **Vergleichen** - Vergleich zweier vorhandener Logs.
- **Erstellen** - Erstellt ein neues Log. Warten Sie, bis das ESET SysInspector-Log erstellt wurde (**Status** ist „Erstellt“).
- **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).
- **Vergleichen** - Vergleich zweier vorhandener Logs.
- **Erstellen -** Erstellt ein neues Log. Warten Sie, bis das ESET SysInspector-Log erstellt wurde (**Status** ist Erstellt).
- **Löschen** - Entfernt die ausgewählten Logs aus der Liste.
- **Alle löschen** - Löschen aller Logs.
- **Export** - Exportieren des Logs in eine *.xml*-Datei oder komprimierte *.xml*-Datei.

4.7.7.1 Snapshot des Computerstatus erstellen

Geben Sie einen kurzen Kommentar ein, der das zu erstellende Log beschreibt, und klicken Sie auf die Schaltfläche **Hinzufügen**. Warten Sie, bis das ESET SysInspector-Log erstellt wurde (Status „Erstellt“). Je nach Hardwarekonfiguration und Systemdaten kann die Log-Erstellung eine gewisse Zeit in Anspruch nehmen.

4.7.7.2 ESET SysInspector

4.7.7.2.1 Einführung in ESET SysInspector

ESET SysInspector ist eine Anwendung, die den Computer gründlich durchsucht und die gesammelten Daten ausführlich anzeigt. Informationen wie installierte Treiber und Anwendungen, Netzwerkverbindungen und wichtige Einträge in der Registrierung helfen Ihnen, verdächtiges Systemverhalten, sei es auf Grund von Software- oder Hardwareinkompatibilität oder einer Infektion mit Schadsoftware, zu untersuchen.

Sie können auf zwei Arten auf ESET SysInspector zugreifen: über die in ESET Security-Produkte integrierte Version oder indem Sie die eigenständige Version (SysInspector.exe) kostenlos von der ESET-Website herunterladen. Die Funktionen und Steuerelemente beider Programmversionen sind identisch. Die Versionen unterscheiden sich nur in der Ausgabe der Informationen. Sowohl mit der eigenständigen als auch der integrierten Version können Snapshots des Systems in einer *.xml*-Datei ausgegeben und auf einem Datenträger gespeichert werden. Mit der integrierten Version können Sie Systemsnapshots außerdem direkt unter **Tools** > **ESET SysInspector** speichern (Ausnahme: ESET Remote Administrator). Weitere Informationen finden Sie im Abschnitt ESET SysInspector als Teil von ESET Mail Security.

Bitte gedulden Sie sich ein wenig, während ESET SysInspector Ihren Computer prüft. Je nach aktueller Hardware-Konfiguration, Betriebssystem und Anzahl der installierten Anwendungen kann die Prüfung zwischen 10 Sekunden und einigen Minuten dauern.

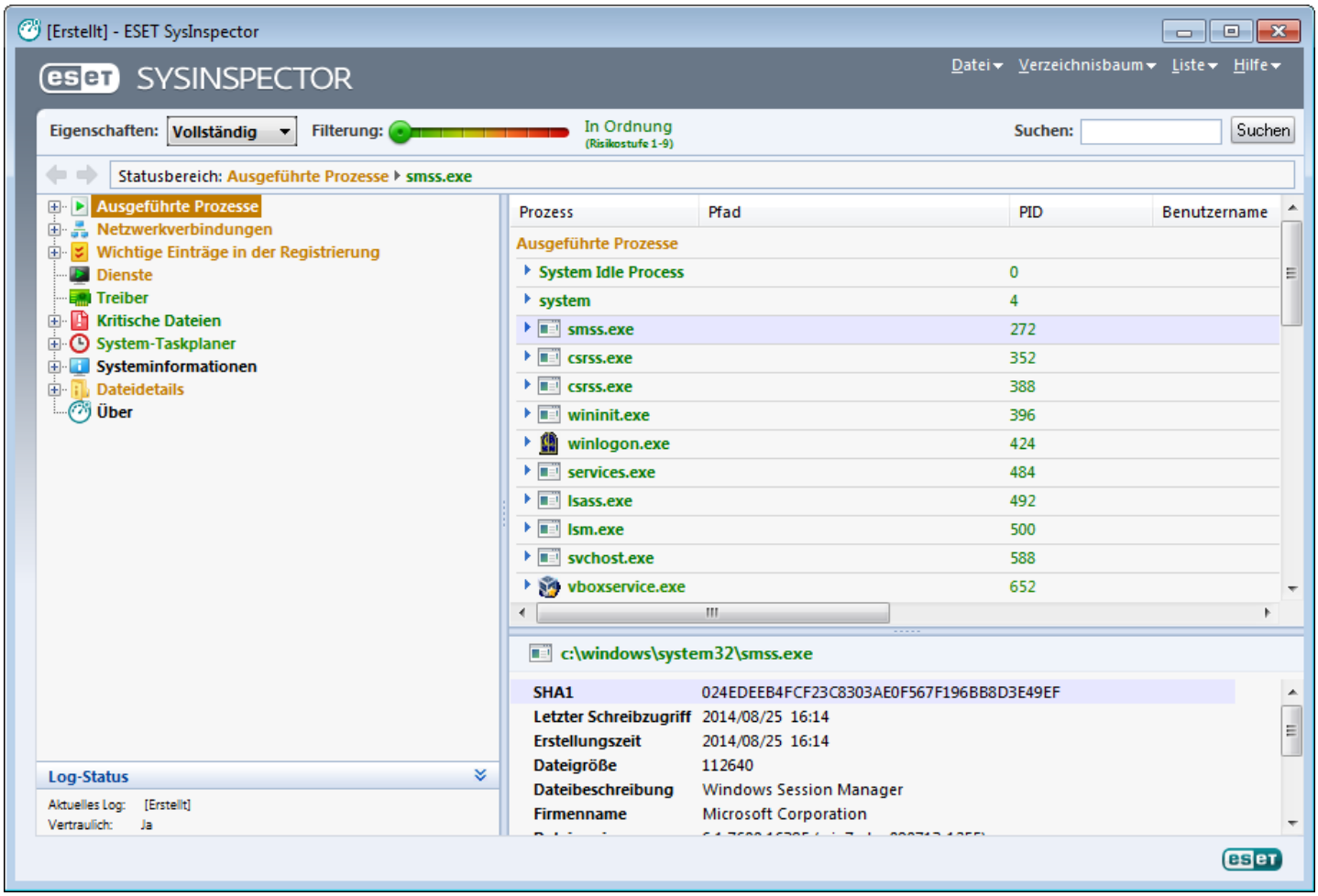
4.7.7.2.1.1 Starten von ESET SysInspector

Zum Starten von ESET SysInspector führen Sie einfach die von der ESET-Website heruntergeladene Programmdatei *SysInspector.exe* aus. Wenn bereits ein ESET Security-Produkt installiert ist, können Sie ESET SysInspector direkt aus dem Startmenü starten (**Programme** > **ESET** > **ESET Mail Security**).

Warten Sie, während die Anwendung das System überprüft. Dies kann einige Minuten in Anspruch nehmen.

4.7.7.2.2 Benutzeroberfläche und Verwenden der Anwendung

Zur besseren Übersicht ist das Hauptprogrammfenster in vier größere Bereiche unterteilt: die Steuerelemente des Programms oben, das Navigationsfenster links, das Beschreibungsfenster rechts und das Detailfenster unten im Hauptfenster. Im Bereich „Log-Status“ werden die grundlegenden Parameter eines Logs aufgeführt: Filterverwendung, Filtertyp, ob das Log Ergebnis eines Vergleichs ist usw.



4.7.7.2.2.1 Steuerelemente des Programms

Dieser Abschnitt beschreibt die Menüs und sonstigen Bedienelemente in ESET SysInspector.

Datei

Über das Menü **Datei** können Sie die aktuellen Systeminformationen zur späteren Untersuchung speichern oder ein zuvor gespeichertes Log wieder öffnen. Falls ein Log weitergegeben werden soll, sollten Sie es über die Funktion **Zum Senden geeignet** erstellen. Sicherheitsrelevante Daten (Name und Berechtigungen des aktuellen Benutzers, Computername, Domänenname, Umgebungsvariablen usw.) werden dann nicht in das Log aufgenommen.

HINWEIS: Gespeicherte ESET SysInspector-Logs können Sie schnell wieder öffnen, indem Sie sie auf das Hauptprogrammfenster ziehen und dort ablegen.

Verzeichnisbaum

Hiermit können Sie alle Knoten erweitern oder schließen sowie die ausgewählten Bereiche in ein Dienste-Skript exportieren.

Liste

Dieses Menü enthält Funktionen zur einfacheren Navigation im Programm sowie eine Reihe von Zusatzfunktionen, etwa für die Online-Informationssuche.

Hilfe

Über dieses Menü finden Sie Informationen zur Anwendung und ihren Funktionen.

Eigenschaften

Dieses Menü beeinflusst die Informationen, die im Hauptprogrammfenster dargestellt werden und vereinfacht somit ihre Verwendung. Im Modus „Einfach“ haben Sie Zugang zu Informationen, die Hilfestellung bei gewöhnlichen Problemen im System liefern. Im Modus „Mittel“ sehen Sie weniger häufig benötigte Informationen. Im Modus „Vollständig“ zeigt ESET SysInspector alle verfügbaren Informationen an, sodass Sie auch sehr spezielle Probleme beheben können.

Filterung

Mit der Filterfunktion können Sie schnell verdächtige Dateien oder Registrierungseinträge auf Ihrem System finden. Durch Verschieben des Schiebereglers legen Sie fest, ab welcher Risikostufe Objekte angezeigt werden. Befindet sich der Schieberegler ganz links (Risikostufe 1), werden alle Einträge angezeigt. Steht der Schieberegler hingegen weiter rechts, werden alle Objekte unterhalb der eingestellten Risikostufe ausgeblendet, sodass Sie nur die Objekte ab einer bestimmten Risikostufe sehen. Steht der Schieberegler ganz rechts, zeigt das Programm nur die als schädlich bekannten Einträge an.

Alle Objekte der Risikostufen 6 bis 9 stellen unter Umständen ein Sicherheitsrisiko dar. Falls solche Objekte auf Ihrem System gefunden werden und Sie keine ESET Security-Lösung einsetzen, empfiehlt sich eine Überprüfung Ihres Systems mit dem kostenlosen ESET Online Scanner.

HINWEIS: Die Risikostufe eines Eintrags können Sie leicht erkennen, indem Sie dessen Farbe mit der Farbe auf der Risikostufenskala vergleichen.

Vergleichen

Beim Vergleich zweier Log-Dateien können Sie angeben, ob alle Elemente, nur hinzugefügte Elemente, nur entfernte Elemente oder nur ersetzte Elemente angezeigt werden sollen.

Suchen

Mit der Suche können Sie ein bestimmtes Objekt schnell über seinen Namen (oder einen Teil des Namens) finden. Die Suchergebnisse werden im Beschreibungsfenster angezeigt.

Zurück

Über die Schaltflächen mit den Pfeilen nach links und rechts können Sie zwischen den bisherigen Anzeigeinhalten des Beschreibungsbereichs wechseln. Anstatt auf „Vor“ und „Zurück“ zu klicken, können Sie auch die Leertaste bzw. Rücktaste (Backspace) verwenden.

Statusbereich

Hier sehen Sie, welcher Knoten im Navigationsbereich gerade ausgewählt ist.

Wichtig: Rot hervorgehobene Objekte sind unbekannt und werden daher als potenziell gefährlich markiert. Falls ein Eintrag rot gefärbt ist, heißt das jedoch nicht zwingend, dass Sie die Datei löschen können. Stellen Sie vor dem Löschen sicher, dass die Dateien wirklich gefährlich oder unnötig sind.

4.7.7.2.2.2 Navigation in ESET SysInspector

In ESET SysInspector gliedern sich die unterschiedlichen Systeminformationen in eine Reihe von Hauptabschnitten, die so genannten „Knoten“. Falls zusätzliche Informationen verfügbar sind, erreichen Sie diese, indem Sie einen Knoten um seine Unterknoten erweitern. Um einen Knoten zu öffnen oder zu reduzieren, doppelklicken Sie auf den Knotennamen oder klicken Sie neben dem Knotennamen auf + bzw. −. Soweit vorhanden, werden im Beschreibungsbereich Detailinhalte zum gerade im Navigationsbereich ausgewählten Knoten angezeigt. Diese Einträge im Beschreibungsbereich können Sie dann wiederum auswählen, um (soweit vorhanden) im Detailbereich weitere Detailinformationen dazu anzuzeigen.

Im Folgenden sind die Hauptknoten im Navigationsbereich sowie die dazugehörigen Informationen im Beschreibungs- und Detailbereich beschrieben.

Ausgeführte Prozesse

Dieser Knoten enthält Informationen zu den Anwendungen und Prozessen, die zum Zeitpunkt der Log-Erstellung ausgeführt wurden. Das Beschreibungsfenster zeigt weitere Details zu jedem Prozess, etwa die verwendeten dynamischen Bibliotheken samt Speicherort, den Namen des Programmherstellers und die Risikostufe der Dateien.

Wenn Sie einen Eintrag im Beschreibungsfenster auswählen, erscheinen im Detailfenster weitere Informationen wie z. B. die Größe oder der Hashwert der betreffenden Datei.

HINWEIS: Ein Betriebssystem enthält verschiedene durchgängig laufende Kernelkomponenten, die grundlegende und wichtige Funktionen für andere Benutzeranwendungen bereitstellen. In bestimmten Fällen wird für solche Prozesse in ESET SysInspector ein Dateipfad angezeigt, der mit \??\ beginnt. Diese Symbole stellen eine vor dem Start liegende Optimierung für derartige Prozesse dar. Sie sind für das System ungefährlich.

Netzwerkverbindungen

Wenn Sie im Navigationsbereich ein Protokoll (TCP oder UDP) auswählen, erscheint im Beschreibungsbereich eine Liste der Prozesse und Anwendungen, die über das betreffende Protokoll im Netzwerk kommunizieren, samt der jeweiligen Remoteadresse. Außerdem können Sie hier die IP-Adressen der DNS-Server überprüfen.

Wenn Sie einen Eintrag im Beschreibungsfenster auswählen, erscheinen im Detailfenster weitere Informationen wie z. B. die Größe oder der Hashwert der betreffenden Datei.

Wichtige Einträge in der Registrierung

Hier finden Sie eine Liste ausgewählter Registrierungseinträge, die oft im Zusammenhang mit Systemproblemen stehen. Dies betrifft beispielsweise die Registrierungseinträge für Autostart-Programme, Browser-Hilfsobjekte (BHO) usw.

Im Beschreibungsbereich werden die mit dem jeweiligen Registrierungseintrag verbundenen Dateien angezeigt. Das Detailfenster zeigt zusätzliche Informationen an.

Dienste

Bei diesem Knoten enthält der Beschreibungsbereich eine Liste der Dateien, die als Windows-Dienste registriert sind. Das Detailfenster informiert über spezifische Details und darüber, auf welche Art ein Dienst gestartet wird.

Treiber

Dieser Knoten enthält eine Liste der im System installierten Treiber.

Kritische Dateien

Unter diesem Knoten können Sie sich im Beschreibungsbereich den Inhalt wichtiger Konfigurationsdateien von Microsoft Windows anzeigen lassen.

System-Taskplaner

Enthält eine Liste der Tasks, die der Windows-Taskplaner (in neueren Windows-Versionen „Aufgabenplanung“ genannt) zu einem festgelegten Zeitpunkt/in festgelegten Intervallen auslöst.

Systeminformationen

Hier finden Sie ausführliche Informationen zu Hardware und Software, den gesetzten Umgebungsvariablen, den Benutzerberechtigungen und den Systemereignis-Logs.

Dateidetails

Dieser Knoten enthält eine Liste der wichtigen Systemdateien sowie der Dateien im Ordner „Programme“. Zusätzliche Informationen speziell für diese Dateien werden im Beschreibungs- und Detailfenster angezeigt.

Über

Angaben zur Version von ESET SysInspector und eine Liste der Programmmodule.

Für die Arbeit mit ESET SysInspector stehen Ihnen die folgenden Tastaturbefehle zur Verfügung:

Datei

Strg+O	bestehendes Log öffnen
Strg+S	erstelltes Log speichern

Erstellen

Strg+G	erstellt einen Snapshot des Computerstatus
Strg+H	erstellt einen Snapshot des Computerstatus, der auch sicherheitsrelevante Informationen im Log enthalten kann

Filterung der Elemente

1, O	in Ordnung, Einträge der Risikostufen 1-9 werden angezeigt
2	in Ordnung, Einträge der Risikostufen 2-9 werden angezeigt
3	in Ordnung, Einträge der Risikostufen 3-9 werden angezeigt
4, U	unbekannt, Einträge der Risikostufen 4-9 werden angezeigt
5	unbekannt, Einträge der Risikostufen 5-9 werden angezeigt
6	unbekannt, Einträge der Risikostufen 6-9 werden angezeigt
7, B	risikoreich, Einträge der Risikostufen 7-9 werden angezeigt
8	risikoreich, Einträge der Risikostufen 8-9 werden angezeigt
9	risikoreich, Einträge der Risikostufe 9 werden angezeigt
-	verringert Risikostufe
+	erhöht Risikostufe
Strg+9	Filtermodus, gleiche oder höhere Stufe
Strg+0	Filtermodus, nur gleiche Stufe

Ansicht

Strg+5	Anzeige nach Anbieter, alle Anbieter
Strg+6	Anzeige nach Anbieter, nur Microsoft
Strg+7	Anzeige nach Anbieter, alle anderen Anbieter
Strg+3	zeigt vollen Detailmodus an
Strg+2	zeigt mittleren Detailmodus an
Strg+1	einfache Darstellung
Rücktaste	geht einen Schritt zurück
Leertaste	geht einen Schritt vor
Strg+W	erweitert die Baumstruktur
Strg+Q	reduziert die Baumstruktur

Sonstige Steuerelemente

Strg+T	kehrt nach der Auswahl von Suchergebnissen zum Ursprung des Eintrags zurück
Strg+P	zeigt grundlegende Informationen zu einem Eintrag an
Strg+A	zeigt alle Informationen zu einem Eintrag an
Strg+C	kopiert die Baumstruktur des aktuellen Eintrags

Strg+X	kopiert Einträge
Strg+B	sucht im Internet nach Informationen zu den ausgewählten Dateien
Strg+L	öffnet den Ordner, in dem sich die ausgewählte Datei befindet
Strg+R	öffnet den dazugehörigen Eintrag im Registrierungs-Editor
Strg+Z	kopiert den Pfad in eine Datei (falls der Eintrag mit einer Datei zusammenhängt)
Strg+F	zum Suchfeld wechseln
Strg+D	schließt die Suchergebnisse
Strg+E	startet ein Dienste-Skript

Vergleichen

Strg+Alt+O	öffnet das Original-/Vergleichs-Log
Strg+Alt+R	bricht das Vergleichen ab
Strg+Alt+1	zeigt alle Einträge an
Strg+Alt+2	zeigt nur hinzugekommene Einträge an, das Log listet die aktuellen Einträge auf
Strg+Alt+3	zeigt nur entfernte Einträge an, das Log listet die Einträge des vorherigen Logs auf
Strg+Alt+4	zeigt nur ersetzte Einträge an (Dateien eingeschlossen)
Strg+Alt+5	führt lediglich Unterschiede zwischen den Logs auf
Strg+Alt+C	Vergleich anzeigen
Strg+Alt+N	zeigt das aktuelle Log an
Strg+Alt+P	öffnet das vorherige Log

Allgemein

F1	ruft die Hilfe auf
Alt+F4	schließt das Programm
Alt+Umschalt+F4	schließt das Programm ohne Nachfrage
Strg+I	Log-Statistiken

4.7.7.2.2.3 Vergleichsfunktion

Mit der „Vergleichen“-Funktion ist es möglich, zwei bestehende Log-Dateien miteinander zu vergleichen. Auf diese Weise erlangen Sie Informationen, die aus den beiden einzelnen Log-Dateien für sich genommen nicht hervorgehen. Diese Funktion ist geeignet, um Änderungen am System zu erkennen, und hilft so, Schadprogramme zu entdecken.

Nach dem Start erzeugt die Anwendung ein neues Log, das in einem neuen Fenster angezeigt wird. Um das Log zu speichern, klicken Sie auf **Datei** > **Log speichern**. Gespeicherte Log-Dateien können Sie später wieder öffnen, um sie einzusehen. Ein bestehendes Log öffnen Sie über **Datei** > **Log öffnen**. Im Hauptfenster von ESET SysInspector wird immer nur jeweils ein Log angezeigt.

Die Vergleichsfunktion hat den Vorteil, dass Sie sich eine aktive und eine gespeicherte Log-Datei anzeigen lassen können. Hierzu klicken Sie auf **Datei** > **Logs vergleichen** und wählen dann **Datei auswählen**. Das gewählte Log wird mit dem gerade aktiven im Hauptprogrammfenster verglichen. Das Vergleichs-Log führt lediglich Unterschiede zwischen diesen beiden Logs auf.

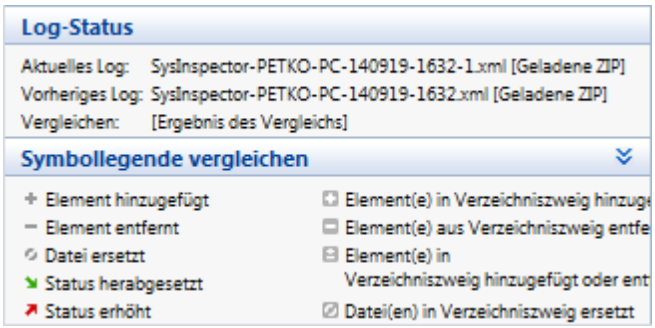
HINWEIS: Wenn Sie nach dem Vergleich zweier Logs auf **Datei** > **Log speichern** klicken und das Ergebnis als ZIP-Datei speichern, werden beide Log-Dateien gespeichert. Wenn Sie die so entstandene Datei später öffnen, werden die enthaltenen Logs automatisch verglichen.

Neben den einzelnen Einträgen erscheinen Symbole, die angeben, um was für eine Art von Unterschied es sich handelt.

Beschreibung aller Symbole, die neben den Einträgen angezeigt werden können:

- Neuer Wert, nicht im vorherigen Log enthalten
- Betreffender Zweig der Baumstruktur enthält neue Werte
- Gelöschter Wert, nur im vorherigen Log enthalten
- Betreffender Zweig der Baumstruktur enthält gelöschte Werte
- Wert/Datei wurde geändert
- Betreffender Zweig der Baumstruktur enthält geänderte Werte/Dateien
- Risiko ist gesunken (war im vorherigen Log höher)
- Risiko ist gestiegen (war im vorherigen Log niedriger)

Der Erklärungsbereich in der linken unteren Ecke beschreibt alle Symbole und zeigt auch die Namen der Log-Dateien an, die verglichen werden.



Jedes Vergleichs-Log kann als Datei gespeichert und später wieder geöffnet werden.

Beispiel

Erstellen und speichern Sie ein Log, das die ursprünglichen Informationen über das System enthält, als vorher.xml. Nachdem Sie Änderungen am System vorgenommen haben, öffnen Sie ESET SysInspector und erstellen Sie ein neues Log. Speichern Sie dieses unter dem Namen *neu.xml*.

Um die Unterschiede zwischen diesen beiden Logs zu sehen, klicken Sie auf **Datei** > **Logs vergleichen**. Das Programm erstellt nun ein Vergleichs-Log, das die Unterschiede beider Log-Dateien anzeigt.

Mithilfe des folgenden Befehls in der Kommandozeile kann das gleiche Resultat erzielt werden:

SysInspector.exe aktuell.xml vorher.xml

4.7.7.2.3 Kommandozeilenparameter

Mit ESET SysInspector können Sie auch von der Kommandozeile aus Berichte erzeugen. Hierzu stehen die folgenden Parameter zur Verfügung:

/gen	Log direkt über die Kommandozeile erstellen, ohne die Benutzeroberfläche zu starten
/privacy	Log ohne vertrauliche Daten erstellen
/zip	Log in komprimiertem Zip-Archiv speichern
/silent	Fortschrittsanzeige unterdrücken, wenn Log von der Kommandozeile aus erstellt wird
/blank	ESET-SysInspector starten, ohne Log zu erstellen/laden

Beispiele

Verwendung:
```
Sysinspector.exe [load.xml] [/gen=save.xml] [/privacy] [/zip] [compareto.xml]
```

Spezielles Log direkt im Browser öffnen: *SysInspector.exe .\clientlog.xml*
Log über die Kommandozeile erstellen: *SysInspector.exe /gen=.\mynewlog.xml*
Log ohne vertrauliche Informationen direkt in einer komprimierten Datei erstellen: *SysInspector.exe /gen=.\mynewlog.zip /privacy /zip*
Zwei Log-Dateien vergleichen und Unterschiede durchsuchen: *SysInspector.exe new.xml old.xml*

HINWEIS: Datei- und Ordnernamen mit Leerzeichen sollten in Hochkommata gesetzt werden.

4.7.7.2.4 Dienste-Skript

Ein Dienste-Skript ist ein Hilfsmittel für Benutzer von ESET SysInspector zur einfachen Entfernung unerwünschter Objekte aus dem System.

Das Dienste-Skript ermöglicht den Export des gesamten ESET SysInspector-Logs oder ausgewählten Teilen davon. Nach dem Export können Sie unerwünschte Objekte zum Löschen markieren. Anschließend können Sie das so bearbeitete Log ausführen, um die markierten Objekte zu löschen.

Das Dienste-Skript ist für fortgeschrittene Benutzer geeignet, die bereits Erfahrung mit der Diagnose von Systemproblemen haben. Unqualifizierte Änderungen können das Betriebssystem beschädigen.

Beispiel

Wenn Sie vermuten, dass Ihr Computer mit einem Virus infiziert ist, den Ihr Antivirusprogramm nicht erkennt, gehen Sie wie folgt vor:

1. Führen Sie ESET SysInspector aus, um einen neuen System-Snapshot zu erstellen.
2. Wählen Sie den ersten Menüpunkt im Bereich auf der linken Seite (in der Baumstruktur). Halten Sie die Umschalttaste gedrückt und wählen Sie den letzten Menüpunkt, um alle Menüpunkte zu markieren.
3. Klicken Sie mit der rechten Maustaste auf die ausgewählten Objekte und wählen Sie **Ausgewählte Bereiche in das Entfernen-Skript exportieren** aus.
4. Die ausgewählten Objekte werden in ein neues Log exportiert.
5. Es folgt der wichtigste Schritt des gesamten Vorgangs: Öffnen Sie das neue Log und ändern Sie das Zeichen „-“ vor allen Objekten, die gelöscht werden sollen, auf „+“. Stellen Sie sicher, dass Sie keine wichtige Betriebssystemdateien oder -objekte markieren.
6. Öffnen Sie ESET SysInspector, klicken Sie auf **Datei** > **Dienste-Skript ausführen** und geben Sie den Pfad zum Skript ein.
7. Klicken Sie auf **OK**, um das Skript auszuführen.

4.7.7.2.4.1 Erstellen eines Dienste-Skripts

Um ein Skript zu erstellen, klicken Sie im ESET SysInspector-Hauptfenster mit der rechten Maustaste auf ein beliebiges Element im Navigationsbereich auf der linken Seite des Fensters. Wählen Sie im Kontextmenü dann entweder **Alle Bereiche in das Dienste-Skript exportieren** oder **Ausgewählte Bereiche in das Dienste-Skript exportieren**.

HINWEIS: Wenn Sie gerade zwei Logs miteinander vergleichen, ist kein Export in ein Dienste-Skript möglich.

4.7.7.2.4.2 Aufbau des Dienste-Skripts

In der ersten Zeile des Skriptheaders finden Sie Angaben zur Engine-Version (ev), zur Version der Benutzeroberfläche (gv) sowie zur Log-Version (lv). Über diese Angaben können Sie mögliche Änderungen an der XML-Datei verfolgen, über die das Skript erzeugt wird, und dadurch Inkonsistenzen bei der Ausführung vermeiden. An diesem Teil des Skripts sollten keine Änderungen vorgenommen werden.

Der Rest der Datei gliedert sich in mehrere Abschnitte, deren Einträge Sie bearbeiten können, um festzulegen, welche davon bei der Ausführung verarbeitet werden sollen. Um einen Eintrag für die Verarbeitung zu markieren, ersetzen Sie das davor stehende Zeichen „-“ durch ein „+“. Die einzelnen Skriptabschnitte sind jeweils durch eine Leerzeile voneinander getrennt. Jeder Abschnitt hat eine Nummer und eine Überschrift.

01) Running processes (Ausgeführte Prozesse)

Dieser Abschnitt enthält eine Liste mit allen Prozessen, die auf dem System ausgeführt werden. Für jeden Prozess ist der UNC-Pfad gefolgt vom CRC16-Hashwert in Sternchen (*) aufgeführt.

Beispiel:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

In diesem Beispiel wurde der Prozess module32.exe ausgewählt, indem er mit dem Zeichen „+“ markiert wurde. Beim Ausführen des Skripts wird dieser Prozess beendet.

02) Loaded modules (Geladene Module)

Dieser Abschnitt enthält eine Liste der momentan verwendeten Systemmodule.

Beispiel:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

In diesem Beispiel wurde das Modul khbekhb.dll mit einem „+“ markiert. Beim Ausführen des Skripts werden alle Prozesse, die dieses Modul verwenden, ermittelt und anschließend beendet.

03) TCP connections (TCP-Verbindungen)

Dieser Abschnitt enthält Informationen zu den aktiven TCP-Verbindungen.

Beispiel:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

Beim Ausführen des Skripts wird der Eigentümer des Sockets der markierten TCP-Verbindungen ermittelt. Anschließend wird der Socket beendet, wodurch Systemressourcen wieder frei werden.

04) UDP endpoints (UDP-Endpunkte)

Dieser Abschnitt enthält Informationen zu den aktiven UDP-Endpunkten.

Beispiel:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Beim Ausführen des Skripts wird der Eigentümer des Sockets der markierten UDP-Verbindungen ermittelt. Anschließend wird der Socket beendet.

05) DNS server entries (DNS-Servereinträge)

Dieser Abschnitt enthält Angaben zur aktuellen DNS-Serverkonfiguration.

Beispiel:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Beim Ausführen des Skripts werden die markierten DNS-Servereinträge entfernt.

06) Important registry entries (Wichtige Registrierungseinträge)

Dieser Abschnitt enthält Informationen zu wichtigen Registrierungseinträgen.

Beispiel:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

Beim Ausführen des Skripts werden die markierten Einträge gelöscht, auf eine Länge von 0 Byte abgeschnitten oder auf die Standardwerte zurückgesetzt. Was davon im Einzelfall geschieht, hängt von der Art des Eintrags und dem Wert des Schlüssels ab.

07) Services (Dienste)

Dieser Abschnitt enthält eine Liste der auf dem System registrierten Dienste.

Beispiel:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

Beim Ausführen des Skripts werden die markierten Dienste samt davon abhängiger Dienste beendet und deinstalliert.

08) Drivers (Treiber)

Dieser Abschnitt enthält eine Liste der installierten Treiber.

Beispiel:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Beim Ausführen des Skripts werden die ausgewählten Treiber angehalten. Beachten Sie, dass einige Treiber nicht zulassen, angehalten zu werden.

09) Critical files (Kritische Dateien)

Dieser Abschnitt enthält Angaben zu Dateien, die für eine korrekte Funktion des Betriebssystems wesentlich sind.

Beispiel:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Die ausgewählten Objekte werden entweder gelöscht oder auf ihren ursprünglichen Wert zurückgesetzt.

4.7.7.2.4.3 Ausführen von Dienste-Skripten

Markieren Sie die gewünschten Elemente, speichern und schließen Sie das Skript. Führen Sie das fertige Skript dann direkt aus dem ESET SysInspector-Hauptfenster aus, indem Sie im Menü „Datei“ auf **Dienste-Skript ausführen** klicken. Beim Öffnen eines Skripts wird die folgende Bestätigungsabfrage angezeigt: **Möchten Sie das Dienste-Skript „%Skriptname%“ wirklich ausführen?** Nachdem Sie diese Abfrage bestätigt haben, erscheint unter Umständen eine weitere Warnmeldung, dass das auszuführende Dienste-Skript nicht signiert wurde. Klicken Sie auf **Starten**, um das Skript auszuführen.

Ein Dialogfenster mit der Bestätigung über die erfolgreiche Ausführung des Skripts wird angezeigt.

Wenn das Skript nur teilweise verarbeitet werden konnte, wird ein Dialogfenster mit der folgenden Meldung angezeigt: **Das Dienste-Skript wurde teilweise ausgeführt. Möchten Sie den Fehlerbericht anzeigen?** Wählen Sie **Ja**, um einen ausführlichen Fehlerbericht mit Informationen zu den nicht ausgeführten Aktionen anzuzeigen.

Wenn das Skript nicht erkannt wurde, wird ein Dialogfenster mit der folgenden Meldung angezeigt: **Das ausgewählte Dienste-Skript trägt keine Signatur. Wenn Sie unbekannte Skripte und Skripte ohne Signatur ausführen, können die Daten Ihres Computers beschädigt werden. Möchten Sie das Skript und die Aktionen wirklich ausführen?** Eine solche Meldung kann durch Inkonsistenzen im Skript verursacht werden (beschädigter Header, beschädigte Abschnittsüberschrift, fehlende Leerzeile zwischen Bereichen usw.). Sie können dann entweder die Skriptdatei öffnen und die Fehler beheben oder ein neues Dienste-Skript erstellen.

4.7.7.2.5 Häufig gestellte Fragen (FAQ)

Muss ESET SysInspector mit Administratorrechten ausgeführt werden?

ESET SysInspector muss zwar nicht unbedingt mit Administratorrechten ausgeführt werden, einige Informationen können jedoch nur über ein Administratorkonto erfasst werden. Führt ein Standardbenutzer oder ein Benutzer mit eingeschränkten Rechten das Programm aus, werden weniger Informationen über die Arbeitsumgebung zusammengestellt.

Erstellt ESET SysInspector eine Log-Datei?

ESET SysInspector kann eine Log-Datei mit der Konfiguration Ihres Computers erstellen. Um diese zu speichern, wählen Sie im Hauptprogrammfenster **Datei** > **Log speichern**. Logs werden im XML-Format gespeichert. Standardmäßig erfolgt dies im Verzeichnis *%USERPROFILE%\Eigene Dateien* und unter einem Namen nach dem Muster „SysInspector-%COMPUTERNAME%-JJMMTT-HHMM.XML“. Falls Sie es vorziehen, können Sie Speicherort und -namen vor dem Speichern ändern.

Wie zeige ich eine ESET SysInspector-Log-Datei an?

Um eine von ESET SysInspector erstellte Log-Datei anzuzeigen, führen Sie das Programm aus und klicken Sie im Hauptprogrammfenster auf **Datei** > **Log öffnen**. Sie können Log-Dateien auch auf ESET SysInspector ziehen und dort ablegen. Wenn Sie häufig Log-Dateien aus ESET SysInspector anzeigen müssen, empfiehlt es sich, auf dem Desktop

eine Verknüpfung zur Datei SYSINSPECTOR.EXE anzulegen. So können Sie Log-Dateien einfach auf dieses Symbol ziehen, um sie zu öffnen. Aus Sicherheitsgründen ist es unter Windows Vista und Windows 7 ggf. nicht möglich, Dateien per Drag and Drop zwischen Fenstern mit unterschiedlichen Sicherheitsberechtigungen zu verschieben.

Ist eine Spezifikation für das Format der Log-Dateien verfügbar? Wie steht es um ein Software Development Kit (SDK)?

Zum gegenwärtigen Zeitpunkt sind weder eine Spezifikation noch ein SDK verfügbar, da sich das Programm noch in der Entwicklung befindet. Nach Veröffentlichung des Programms bieten wir diese möglicherweise an, abhängig von Kundenfeedback und Nachfrage.

Wie bewertet ESET SysInspector das Risiko, das von einem bestimmten Objekt ausgeht?

Um Objekten wie Dateien, Prozessen, Registrierungsschlüsseln usw. eine Risikostufe zuzuordnen, verwendet ESET SysInspector in der Regel einen Satz heuristischer Regeln, mit denen die Merkmale des Objekts untersucht werden, um anschließend nach entsprechender Gewichtung das Potenzial für schädliche Aktivitäten abzuschätzen. Basierend auf dieser Heuristik wird Objekten dann eine Risikostufe zugewiesen, von 1 - In Ordnung (grün) bis 9 - Risikoreich(rot). In der linken Navigationsanzeige sind Bereiche auf Grundlage der jeweils höchsten Risikostufe der Objekte in ihnen eingefärbt.

Bedeutet eine Risikostufe von „6 - Unbekannt (rot)“, dass ein Objekt gefährlich ist?

Die Einschätzung von ESET SysInspector legt nicht endgültig fest, ob eine Gefahr von einem Objekt ausgeht. Diese Entscheidung muss ein Sicherheitsexperte treffen. ESET SysInspector kann hierbei helfen, indem es dem Experten schnell zeigt, welche Objekte eventuell gründlicher untersucht werden müssen.

Warum stellt ESET SysInspector beim Start eine Verbindung ins Internet her?

Wie viele Anwendungen ist auch ESET SysInspector mit einem digitalen Zertifikat signiert, mit dem überprüft werden kann, dass die Software tatsächlich von ESET stammt und nicht verändert wurde. Um das Zertifikat zu verifizieren, kontaktiert das Betriebssystem eine Zertifizierungsstelle, welche die Identität des Softwareherstellers verifiziert. Dies ist ein normaler Vorgang für alle digital unterschriebenen Programme unter Microsoft Windows.

Was ist Anti-Stealth-Technologie?

Die Anti-Stealth-Technologie ermöglicht eine effektive Erkennung von Rootkits.

Wenn ein System von Schadcode angegriffen wird, das sich wie ein Rootkit verhält, ist der Benutzer möglicherweise dem Risiko von Schaden an seinen Daten oder deren Diebstahl ausgesetzt. Ohne ein spezielles Anti-Rootkit-Tool ist es beinahe unmöglich, ein Rootkit aufzuspüren.

Warum ist bei Dateien manchmal Microsoft als Unterzeichner angegeben, wenn gleichzeitig aber ein anderer Firmenname angezeigt wird?

Beim Versuch, die digitale Signatur einer ausführbaren Datei zu ermitteln, überprüft ESET SysInspector zuerst, ob in der Datei eine eingebettete Signatur vorhanden ist. Wenn eine digitale Signatur erkannt wird, wird die Datei mit den Informationen aus der Signatur validiert. Falls die zu überprüfende Datei keine digitale Signatur enthält, sucht ESI nach einer zugehörigen CAT-Datei (Sicherheitskatalog - *%systemroot%\system32\catroot*), die Informationen über die ausführbare Datei enthält. Falls eine entsprechende CAT-Datei existiert, wird deren digitale Signatur beim Überprüfungsprozess für die ausführbare Datei übernommen.

Aus diesem Grund sind einige Dateien mit „Signatur MS“ markiert, obwohl unter „Firmenname“ ein anderer Eintrag vorhanden ist.

4.7.7.2.6 ESET SysInspector als Teil von ESET Mail Security

Um den ESET SysInspector-Bereich in ESET Mail Security zu öffnen, klicken Sie auf **Tools** > **ESET SysInspector**. Das Verwaltungssystem im ESET SysInspector-Fenster ähnelt dem von Prüfungslogs oder geplanten Tasks. Alle Vorgänge mit Systemsnapshots - Erstellen, Anzeigen, Vergleichen, Entfernen und Exportieren - sind mit einem oder zwei Klicks zugänglich.

Das ESET SysInspector-Fenster enthält Basisinformationen zum erstellten Snapshot wie z. B. Erstellungszeitpunkt, kurzer Kommentar, Name des Benutzers, der den Snapshot erstellt hat, sowie den Status des Snapshots.

Zum Vergleichen, Erstellen oder Löschen von Snapshots verwenden Sie die entsprechenden Schaltflächen unter der Snapshot-Liste im ESET SysInspector-Fenster. Diese Optionen sind ebenfalls im Kontextmenü verfügbar. Um den gewählten Systemsnapshot anzuzeigen, wählen Sie im Kontextmenü die Option **Anzeigen** aus. Um den gewünschten Snapshot in eine Datei zu exportieren, klicken Sie mit der rechten Maustaste darauf, und wählen Sie **Exportieren...**.

Die einzelnen Befehle sind nachstehend noch einmal ausführlicher beschrieben:

- **Vergleichen** - Hiermit können Sie zwei vorhandene Logs vergleichen. Diese Funktion eignet sich dafür, alle Unterschiede zwischen dem aktuellen und einem älteren Log zu ermitteln. Um sie zu nutzen, müssen Sie zwei Snapshots zum Vergleich auswählen.
- **Erstellen...** - Erstellen eines neuen Eintrags. Hierzu müssen Sie zunächst einen kurzen Kommentar zum Snapshot eingeben. Der Erstellungsfortschritt (des aktuell erstellten Snapshots) wird in der Spalte **Status** angezeigt. Fertige Snapshots haben den Status **Erstellt**.
- **Löschen/Alle löschen** - Entfernt Einträge aus der Liste.
- **Exportieren...** - Speichert den ausgewählten Eintrag als XML-Datei (wahlweise auch komprimiert als ZIP-Datei).

4.7.8 ESET SysRescue Live

ist ein Dienstprogramm, mit dem Sie einen bootfähigen Datenträger mit einer ESET Security-Lösung erstellen können, wie z. B. ESET NOD32 Antivirus, ESET Smart Security oder bestimmte serverorientierte Produkte. Der große Vorteil von ESET SysRescue Live ist, dass ESET Security damit unabhängig vom Betriebssystem auf dem jeweiligen Rechner ausgeführt werden kann, aber direkten Zugriff auf die Festplatte und das gesamte Dateisystem hat. Auf diese Weise lässt sich auch Schadsoftware entfernen, bei der dies normalerweise (bei laufendem Betriebssystem usw.) nicht möglich wäre.

4.7.9 Taskplaner

Der Taskplaner verwaltet und startet geplante Tasks mit vordefinierter Konfiguration und voreingestellten Eigenschaften. Konfiguration und Eigenschaften enthalten Informationen wie Datum und Uhrzeit und Profile, die bei Ausführung des Tasks verwendet werden.

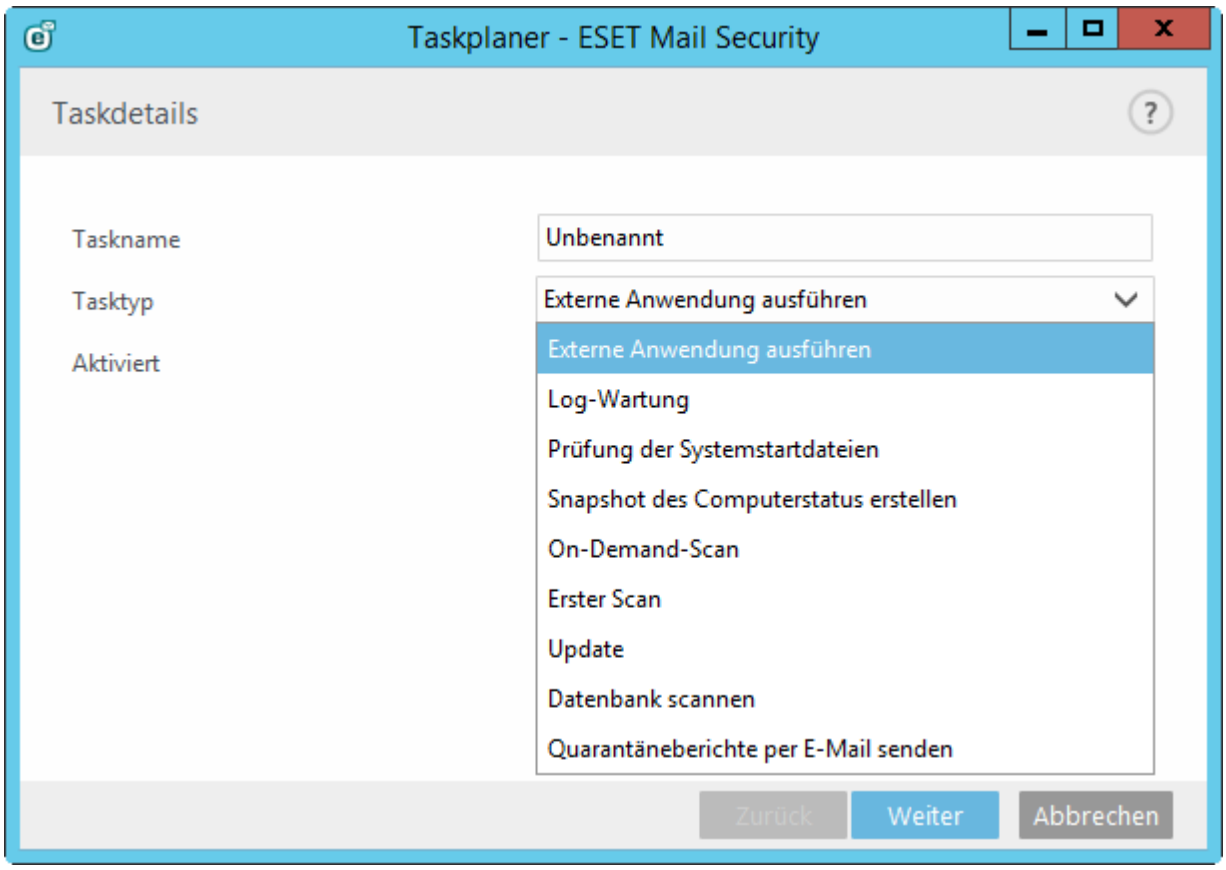
Um ihn zu öffnen, klicken Sie im Hauptprogrammfenster von ESET Mail Security unter **Tools** auf **Taskplaner**. Der **Taskplaner** umfasst eine Liste aller geplanten Tasks sowie deren Konfigurationseigenschaften, inklusive des vordefinierten Datums, der Uhrzeit und des verwendeten Prüfprofils.

Er dient zur Planung der folgenden Vorgänge: Update der Signaturdatenbank, Prüftask, Prüfung Systemstartdateien und Log-Wartung. Tasks können direkt über das Fenster „Taskplaner“ hinzugefügt oder gelöscht werden. (Klicken Sie dazu auf **Hinzufügen** oder **Löschen**.) Klicken Sie an einer beliebigen Stelle mit der rechten Maustaste in das Fenster „Taskplaner“, um folgende Aktionen auszuführen: Anzeigen ausführlicher Informationen, sofortige Ausführung des Tasks, Hinzufügen eines neuen Tasks oder Löschen eines vorhandenen Tasks. Verwenden Sie die Kontrollkästchen vor den einzelnen Einträgen zum Aktivieren oder Deaktivieren der jeweiligen Tasks.

Standardmäßig werden im **Taskplaner** die folgenden Tasks angezeigt:

- **Log-Wartung**
- **Automatische Updates in festen Zeitabständen**
- **Automatische Updates beim Herstellen von DFÜ-Verbindungen**
- **Automatische Updates beim Anmelden des Benutzers**
- **Prüfung Systemstartdateien** (nach Ameldung des Benutzers)
- **Prüfung Systemstartdateien** (nach Update der Signaturdatenbank)
- **Automatischer erster Scan**

Um die Konfiguration eines vorhandenen Standardtasks oder eines benutzerdefinierten Tasks zu ändern, klicken Sie mit der rechten Maustaste auf den Task und dann auf **Bearbeiten**, oder wählen Sie den Task aus, den Sie ändern möchten, und klicken Sie auf **Bearbeiten**.



Hinzufügen eines neuen Tasks

1. Klicken Sie am unteren Fensterrand auf **Task hinzufügen**.
2. Geben Sie einen Namen für den Task ein.

3. Wählen Sie dann den gewünschten Task aus der Liste.

- **Start externer Anwendung** - Planen der Ausführung einer externen Anwendung.
- **Log-Wartung** - Log-Dateien enthalten auch unbenutzte leere Einträge von gelöschten Datensätzen. Dieser Task optimiert regelmäßig die Einträge in Log-Dateien.
- **Prüfung Systemstartdateien** - Prüft Dateien, die während des Systemstarts oder der Anmeldung ausgeführt werden.
- **Snapshot des Computerstatus erstellen** - Erstellt einen ESET SysInspector-Snapshot und eine genaue Risikostufenanalyse Ihrer Systemkomponenten (z. B. Treiber und Anwendungen).
- **On-Demand-Scan** - Prüft die Dateien und Ordner auf Ihrem Computer.
- **Erster Scan** - Standardmäßig wird 20 Minuten nach Installation oder Neustart eine Prüfung als Task mit geringer Priorität ausgeführt.
- **Update** - Erstellt einen Update-Task. Dieser besteht aus der Aktualisierung der Signaturdatenbank und der Aktualisierung der Programmmodule.
- **Datenbankprüfung** - Plant eine Datenbankprüfung. Sie können Prüfziele (öffentliche Ordner, Datenbanken und Postfächer) auf dieselbe Weise wie bei der On-Demand-Datenbankprüfung auswählen.
- **Quarantäneberichte senden** - Gilt nur für die lokale Quarantäne. Verschickt Berichte zu Status und Inhalt der Quarantäne mit Links zur Web-Oberfläche für die E-Mail-Quarantäne, in der Sie die E-Mail-Objekte in der Quarantäne schnell und einfach verwalten können. Sie können die E-Mail-Adresse des Empfängers für die Quarantäneberichte eingeben.

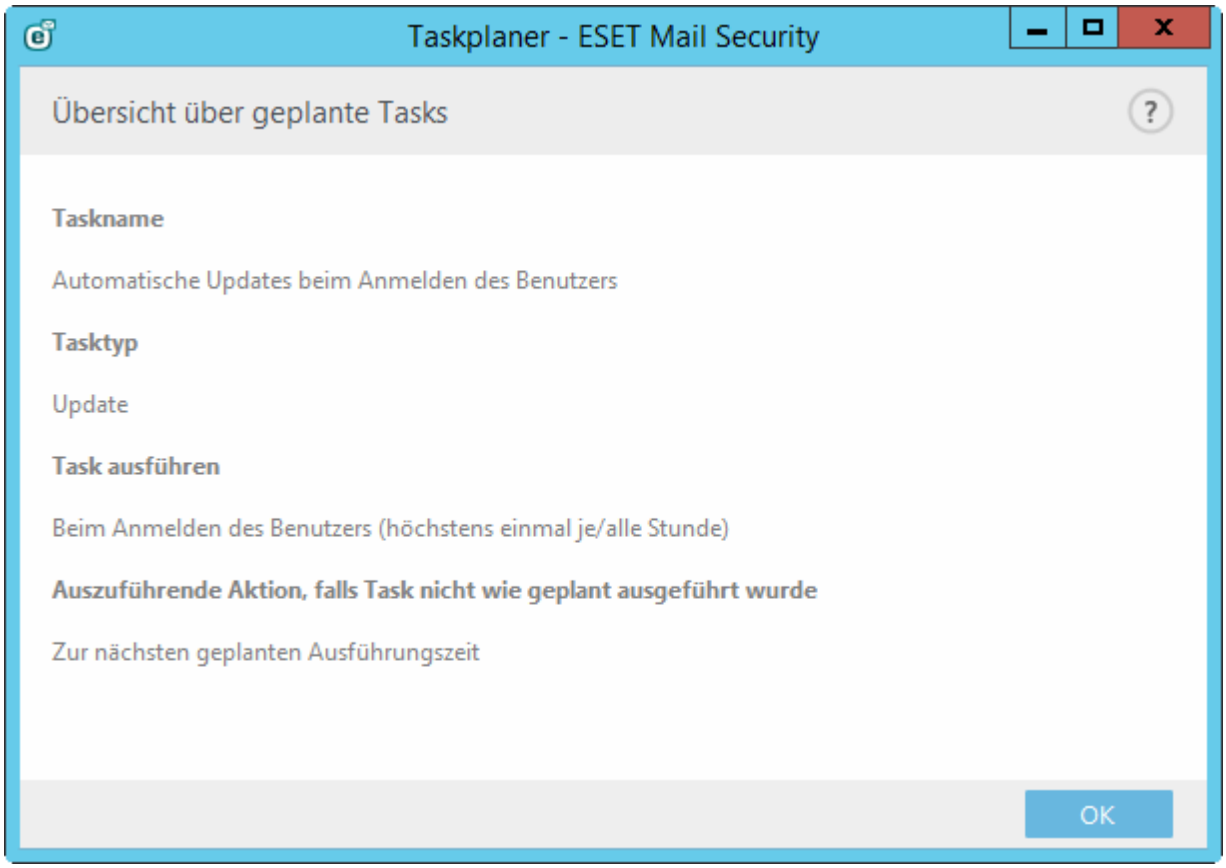
4. Aktivieren Sie den Task über den Schalter **Aktiviert** (Sie können den Task auch später über das Kontrollkästchen in der Liste der geplanten Tasks aktivieren/deaktivieren), klicken Sie auf **Weiter** und wählen Sie eine Zeitangabe aus:

- **Einmalig** - Der Task wird nur einmalig zu einem festgelegten Zeitpunkt ausgeführt.
- **Wiederholt** - Der Task wird in dem angegebenen Zeitabstand ausgeführt.
- **Täglich** - Der Task wird wiederholt täglich zur festgelegten Uhrzeit ausgeführt.
- **Wöchentlich** - Der Task wird am festgelegten Wochentag zur angegebenen Uhrzeit ausgeführt.
- **Bei Ereignis** - Der Task wird ausgeführt, wenn ein bestimmtes Ereignis eintritt.

5. Wählen Sie **Task im Akkubetrieb überspringen** aus, um die Systembelastung für einen Laptop während des Akkubetriebs möglichst gering zu halten. Der angegebene Task wird zum in den Feldern **Taskausführung** angegeben Zeitpunkt ausgeführt. Wenn der Vorgang nicht zur festgelegten Zeit ausgeführt werden konnte, können Sie einen Zeitpunkt für die nächste Ausführung angeben:

- **Zur nächsten geplanten Ausführungszeit**
- **Baldmöglichst**
- **Sofort ausführen, wenn Intervall seit letzter Ausführung überschritten** (das Intervall kann über das Feld **Zeit seit letzter Ausführung (Stunden)** festgelegt werden)

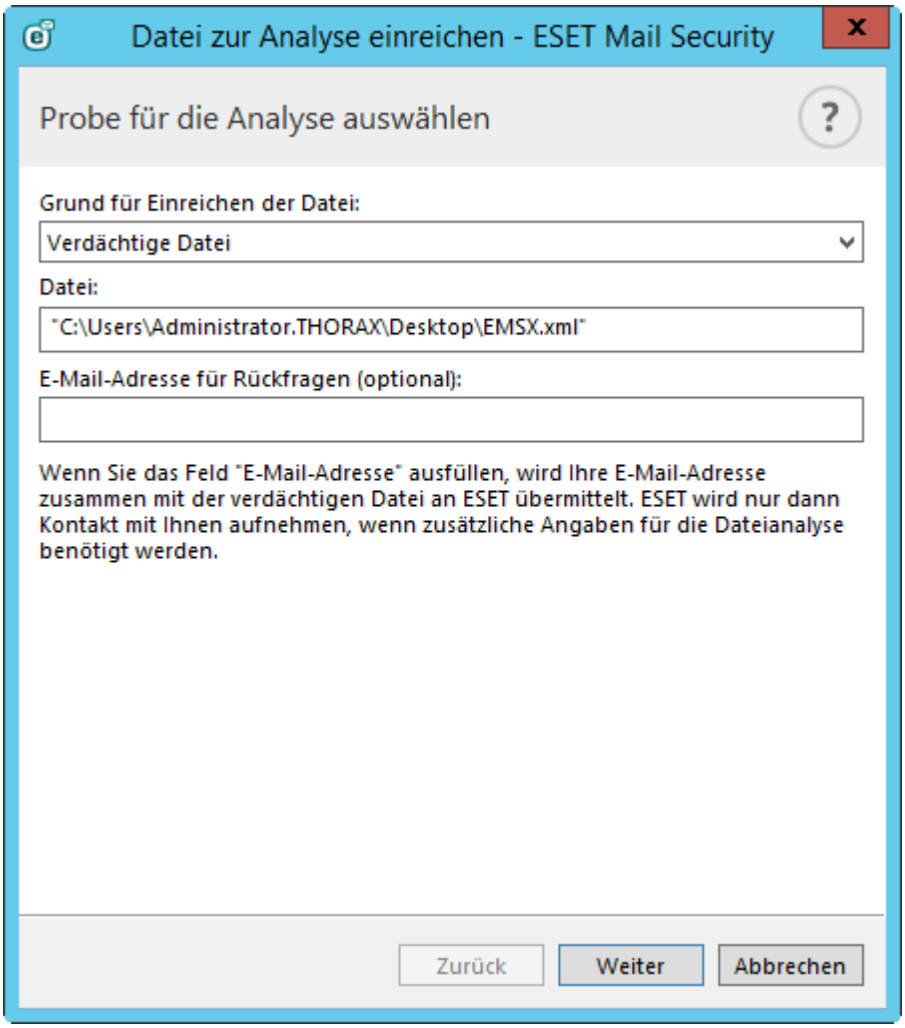
Klicken Sie mit der rechten Maustaste auf einen Task und klicken Sie dann im Kontextmenü auf **Taskdetails anzeigen**, um Informationen zum Task anzuzeigen.



4.7.10 Probe zur Analyse einreichen

Über das Dialogfenster zum Probenversand können Sie Dateien bei ESET zur Analyse einreichen. Sie öffnen es unter **Tools** > **Probe zur Analyse einreichen**. 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.

Sie können Dateien auch per E-Mail einsenden. Komprimieren Sie hierzu die Datei(en) 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).



HINWEIS: Auf Proben, die Sie an ESET senden, sollte mindestens eines der folgenden Kriterien zutreffen:

- Die Datei oder Website wird nicht als Bedrohung erkannt
- Die Datei oder Website wird als Bedrohung erkannt, obwohl sie keinen Schadcode enthält

ESET wird nur dann Kontakt mit Ihnen aufnehmen, wenn zusätzliche Angaben für die Dateianalyse benötigt werden.

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

- **Verdächtige Datei**
- **Verdächtige Website** (Website mit Schadsoftware)
- **Fehlalarm-Datei** (als Bedrohung erkannte Datei, die jedoch nicht infiziert ist)
- **Fehlalarm Webseite**
- **Sonstige**

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

E-Mail-Adresse - 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 werden nur im Ausnahmefall eine Antwort von ESET erhalten, da täglich mehrere Zehntausend Dateien auf unseren Servern eingehen und wir nicht jede Meldung individuell beantworten können.

4.7.10.1 Verdächtige Datei

Beobachtete Anzeichen und Symptome einer Malware-Infektion - Beschreiben Sie, wie sich die verdächtige Datei auf Ihrem Computer verhält.

Herkunft der Datei (URL oder Hersteller) - Bitte 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, die die Identifizierung und Auswertung der verdächtigen Datei erleichtern.

HINWEIS: 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.

4.7.10.2 Verdächtige Webseite

Wählen Sie eine der folgenden Optionen aus der Auswahlliste **Was stimmt mit der Site nicht** aus:

- **Infiziert** - Eine Webseite, die Viren oder sonstige Schadsoftware enthält, die auf verschiedenen Wegen verbreitet werden.
- **Phishing** - Oft eingesetzt, um Zugriff auf vertrauliche Daten zu erlangen, wie Kontonummern oder PIN-Codes. Weitere Informationen zu diesem Angriffstyp finden Sie im Glossar.
- **Scam** - Betrügerische Webseite.
- Wählen Sie **Sonstige** aus, wenn keine der vorherigen Optionen für die Webseite zutrifft, die Sie übermitteln.

Hinweise und Zusatzangaben - Hier können Sie zusätzliche Informationen oder eine Beschreibung eingeben, die die Analyse der verdächtigen Webseite erleichtern.

4.7.10.3 Fehlalarm Datei

Wenn eine Datei als eingedrungene Schadsoftware erkannt wird, tatsächlich aber nicht infiziert ist, bitten wir Sie, diese Datei an uns einzureichen, um unseren Viren- und Spyware-Schutz zu verbessern und andere Benutzer zu schützen. Fehlalarme können auftreten, wenn das Muster einer Datei einem Muster entspricht, das in einer Signaturdatenbank gespeichert ist.

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.

HINWEIS: Die 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.

4.7.10.4 Fehlalarm Webseite

Wir bitten Sie, Webseiten, die fälschlicherweise als infiziert, Betrug oder Phishing erkannt werden, an uns einzureichen. Fehlalarme können auftreten, wenn das Muster einer Datei einem Muster entspricht, das in einer Signaturdatenbank gespeichert ist. Wenn Sie solche Webseiten an uns einreichen, unterstützen Sie uns dabei, unseren Viren- und Spyware-Schutz zu verbessern und andere Benutzer zu schützen.

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

4.7.10.5 Sonstige

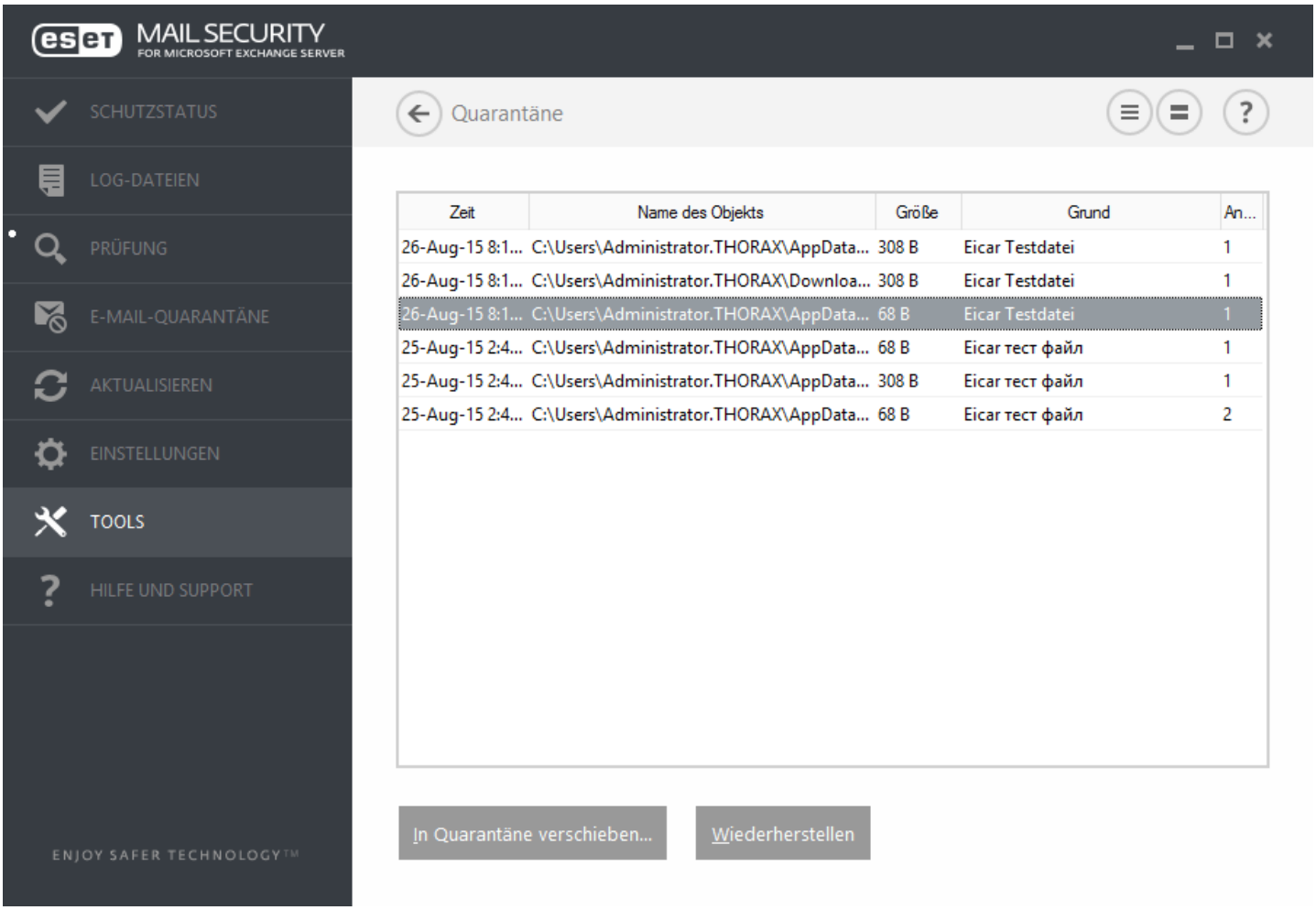
Verwenden Sie diese Auswahlmöglichkeit, wenn die Datei keine **Verdächtige Datei** und kein **Fehlalarm** ist.

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

4.7.11 Quarantäne

Die Hauptfunktion der Quarantäne ist die sichere Verwahrung infizierter Dateien. 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 worden sind.

Sie können beliebige Dateien gezielt in die Quarantäne verschieben. Geschehen sollte dies bei Dateien, die sich verdächtig verhalten, bei der Virenprüfung jedoch 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.

Quarantäne für Dateien

ESET Mail Security verschiebt gelöschte Dateien automatisch in den Quarantäneordner (sofern diese Option nicht im Warnfenster deaktiviert wurde). Auf Wunsch können Sie beliebige verdächtige Dateien manuell in die Quarantäne verschieben, indem Sie auf **Quarantäne** klicken. In die Quarantäne verschobene Dateien werden von ihrem ursprünglichen Speicherort entfernt. Alternativ kann auch das Kontextmenü zu diesem Zweck verwendet werden: Klicken Sie mit der rechten Maustaste in das Fenster **Quarantäne**, und wählen Sie **Quarantäne** aus.

Wiederherstellen aus der Quarantäne

Dateien aus der Quarantäne können auch an ihrem ursprünglichen Speicherort wiederhergestellt werden. Verwenden Sie hierzu die Funktion **Wiederherstellen** aus dem Kontextmenü, das Sie über einen 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 Scans ausschließen** verfügbar. Weitere Informationen zu diesem Anwendungstyp finden Sie im Glossar. Das Kontextmenü enthält außerdem die Option **Wiederherstellen nach ...**, mit der Dateien an einem anderen als ihrem ursprünglichen Speicherort wiederhergestellt werden können.

HINWEIS: 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 darauf und wählen im angezeigten Kontextmenü die Option **Datei zur Analyse einreichen** aus.

4.8 Hilfe und Support

ESET Mail Security enthält Tools für die Fehlerbehebung und Support-Informationen, die Ihnen bei der Lösung von möglichen Problemen behilflich sind.

Hilfe

- **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.
- **Hilfe öffnen** - Klicken Sie auf diesen Link, um die ESET Mail Security-Hilfeseiten zu öffnen.
- **Schnell eine Lösung finden** - Wählen Sie diese Option, um Lösungen für die häufigsten Probleme zu finden. Bevor Sie sich an den Support wenden, sollten Sie diesen Abschnitt unbedingt lesen.

Support

- **Supportanfrage senden** - Wenn Sie Ihr Problem nicht lösen konnten, können Sie sich auch über das Formular auf der ESET-Website schnell mit dem Support in Verbindung setzen.

Support-Tools

- **Virenenzyklopädie –** Öffnet die ESET-Virenenzyklopädie mit Informationen zu den Gefahren und Symptomen verschiedener Infiltrationsarten.
- **Signaturdatenbankverlauf** - Öffnet den ESET-Virusradar, der Informationen zu Versionen der ESET-Signaturdatenbank enthält.
- **Spezielle ESET-Säuberung** - Dieses Säuberungsprogramm identifiziert und entfernt bekannte Schadsoftware-Infektionen. Weitere Informationen finden Sie in diesem Artikel in der ESET-Knowledgebase.

Produkt- und Lizenzinformationen

- **Über ESET Mail Security –** Informationen zu Ihrer Kopie von ESET Mail Security.
- Lizenz verwalten - Klicken Sie hier, um das Produktaktivierungsfenster zu öffnen. Aktivieren Sie ESET Mail Security mit einer der verfügbaren Methoden. Weitere Informationen finden Sie unter So aktivieren Sie ESET Mail Security.

4.8.1 Lösungen für gängige Aufgaben und Probleme

In diesem Kapitel werden einige der häufigsten Fragen und Probleme behandelt. Klicken Sie auf die jeweilige Themenüberschrift, um Hilfestellung bei der Lösung Ihres Problems zu erhalten:

So aktualisieren Sie ESET Mail Security

So aktivieren Sie ESET Mail Security

So planen Sie regelmäßige Prüfungen (im 24-Stunden-Takt)

So entfernen Sie einen Virus von Ihrem Server

So funktionieren automatische Ausschlüsse

Wenn Ihr Problem nicht in der oben aufgeführten Liste der Hilfeseiten aufgeführt ist, suchen Sie es auf den ESET Mail Security-Hilfeseiten über ein Schlagwort oder eine Formulierung, das/die Ihr Problem beschreibt.

Wenn Sie die Lösung für Ihr Problem bzw. die Antwort auf Ihre Frage nicht auf den Hilfeseiten finden können, steht Ihnen auch unsere regelmäßig aktualisierte Online-Knowledgebase zur Verfügung.

Falls erforderlich, können Sie sich mit Ihren Fragen und Problemen auch direkt an die Online-Supportzentrale wenden. Sie finden das Kontaktformular auf der Registerkarte "Hilfe und Support" Ihrer ESET-Anwendung.

4.8.1.1 So aktualisieren Sie ESET Mail Security

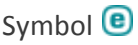
Die Aktualisierung von ESET Mail Security kann manuell oder automatisch erfolgen. Klicken Sie auf **Signaturdatenbank aktualisieren**, um die Aktualisierung zu starten. Sie finden diese Funktion im Bereich **Update** des Programms.

Bei der Standardinstallation wird stündlich ein automatisches Update ausgeführt. Wenn Sie diesen Zeitabstand ändern möchten, navigieren Sie zum **Taskplaner**. (Weitere Informationen zum Taskplaner finden Sie hier).

4.8.1.2 So aktivieren Sie ESET Mail Security

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

Zur Aktivierung des Produkts stehen verschiedene Methoden zur Verfügung. Die Verfügbarkeit einer bestimmten Aktivierungsmöglichkeit im Aktivierungsfenster hängt vom Land und von der Vertriebsart (CD/DVD, ESET-Webseite usw.) ab.

Sie können Ihre Kopie von ESET Mail Security direkt im Programm aktivieren. Klicken Sie hierfür auf das Symbol  im Infobereich der Taskleiste und wählen Sie **Produktlizenz aktivieren** aus dem Menü. Sie können das Produkt auch im Hauptmenü unter **Hilfe und Support** > **Lizenz aktivieren** oder **Schutzstatus** > **Produktlizenz aktivieren** aktivieren.

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

- **Lizenzschlüssel** - Eine eindeutige Zeichenfolge im Format XXXX-XXXX-XXXX-XXXX-XXXX zur Identifizierung des Lizenzinhabers und der Aktivierung der Lizenz.
- **Sicherheitsadministrator Konto** - Ein im ESET License Administrator-Portal erstelltes Konto mit Anmeldedaten (E-Mail-Adresse und Passwort). Mit dieser Methode können Sie mehrere Lizenzen von einem Standort aus verwalten.
- **Offline-Lizenzdatei** - Eine automatisch erzeugte Datei, die zum Zwecke der Bereitstellung von Lizenzinformationen in das ESET-Produkt übertragen wird. Die Offline-Lizenzdatei wird im Lizenzportal erzeugt und in Umgebungen verwendet, in denen die Anwendung keine Verbindung zur Lizenzierungsstelle herstellen

kann.

Klicken Sie auf **Später mit RA aktivieren**, wenn Ihr Computer Teil eines verwalteten Netzwerks ist. Anschließend führt der Administrator die Remote-Aktivierung über ESET Remote Administrator aus. Sie können diese Option auch verwenden, wenn Sie diesen Client zu einem späteren Zeitpunkt aktivieren möchten.

Sie können jederzeit im Hauptprogrammfenster auf **Hilfe und Support** > **Lizenz verwalten** klicken, um Ihre Lizenzinformationen zu verwalten. Hier wird die öffentliche Lizenz-ID angezeigt, mit der Ihr Produkt von ESET identifiziert werden kann und die Lizenzinformationen enthält. Ihr Benutzername, unter dem der Computer im Lizenzierungssystem gespeichert ist, befindet sich im Bereich **Über**. Zugriff darauf erhalten Sie, indem Sie mit der rechten Maustaste auf das Symbol im Infobereich der Taskleiste klicken.

HINWEIS: ESET Remote Administrator kann Clientcomputer mithilfe von Lizenzen, die der Administrator bereitstellt, im Hintergrund aktivieren.

4.8.1.3 So zählt ESET Mail Security die Postfächer

Weitere Informationen finden Sie in unserem Knowledgebase-Artikel.

4.8.1.4 So erstellen Sie einen neuen Task im Taskplaner

Um einen neuen Task zu erstellen, klicken Sie unter **Tools** > **Taskplaner** auf **Task hinzufügen** oder klicken mit der rechten Maustaste und wählen im Kontextmenü **Hinzufügen** aus. Es gibt fünf Arten von Tasks:

- **Start externer Anwendung** - Planen der Ausführung einer externen Anwendung.
- **Log-Wartung** - Log-Dateien enthalten auch unbenutzte leere Einträge von gelöschten Datensätzen. Dieser Task optimiert regelmäßig die Einträge in Log-Dateien.
- **Prüfung Systemstartdateien** - Prüft Dateien, die während des Systemstarts oder 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-Scan** - Prüft die Dateien und Ordner auf Ihrem Computer.
- **Erstprüfung** - Standardmäßig wird 20 Minuten nach Installation oder Neustart eine Prüfung als Task mit geringer Priorität ausgeführt.
- **Update** - Erstellt einen Update-Task. Dieser besteht aus der Aktualisierung der Signaturdatenbank und der Aktualisierung der Programmmodule.

Da **Update**-Tasks zu den meistverwendeten Tasks gehören, wird im Folgenden das Hinzufügen eines neuen Update-Tasks beschrieben:

Wählen Sie in der Liste **Geplanter Task** den Task **Update**. Geben Sie den Namen des Tasks in das Feld **Taskname** ein und klicken Sie auf **Weiter**. Wählen Sie das gewünschte Ausführungsintervall. Die folgenden Optionen stehen zur Verfügung: **Einmalig**, **Wiederholt**, **Täglich**, **Wöchentlich** und **Bei Ereignis.** Wählen Sie **Task im Akkubetrieb überspringen** aus, um die Systembelastung für einen Laptop während des Akkubetriebs möglichst gering zu halten. Der angegebene Task wird zum in den Feldern **Taskausführung** angegeben Zeitpunkt ausgeführt. Im nächsten Schritt können Sie eine Aktion festlegen für den Fall, dass der Task zur geplanten Zeit nicht ausgeführt oder abgeschlossen werden kann. Die folgenden Optionen stehen zur Verfügung:

- **Zur nächsten geplanten Ausführungszeit**
- **Baldmöglichst**
- **Sofort ausführen, wenn Intervall seit letzter Ausführung überschritten** (das Intervall kann über das Feld Zeit seit letzter Ausführung festgelegt werden)

Anschließend wird ein Fenster mit einer vollständigen Zusammenfassung des aktuellen Tasks angezeigt. Klicken Sie auf **Fertig stellen**, wenn Sie Ihre Änderungen abgeschlossen haben.

Es wird ein Dialogfenster angezeigt, in dem Sie die Profile für den Task auswählen können. Hier können Sie das primäre und das alternative Profil festlegen. Das alternative Profil wird verwendet, wenn der Task mit dem primären Profil nicht abgeschlossen werden kann. Bestätigen Sie Ihre Auswahl durch Klicken auf **Fertig stellen**. Der

neue Task wird der Liste der aktuellen Tasks hinzugefügt.

4.8.1.5 So planen Sie regelmäßige Prüfungen (im 24-Stunden-Takt)

Um einen regelmäßigen Task einzurichten, wählen Sie **ESET Mail Security** > **Tools** > **Taskplaner**. Im Folgenden finden Sie einen kurzen Überblick zum Planen eines Tasks, mit dem alle 24 Stunden eine Prüfung der lokalen Laufwerke durchgeführt wird.

So planen Sie eine regelmäßige Prüfung:

1. Klicken Sie im Hauptfenster des Taskplaners auf **Hinzufügen**.
2. Wählen Sie im Dropdown-Menü die Option **On-Demand-Scan** aus.
3. Geben Sie einen Namen für den Task an, und wählen Sie **Wiederholt**.
4. Wählen Sie die Wiederholung im 24-Stunden-Takt (alle 1440 Minuten) aus.
5. Wählen Sie aus, welche Aktion stattfinden soll, falls der Task nicht ausgeführt werden kann.
6. Überprüfen Sie die Zusammenfassung zum geplanten Task, und klicken Sie auf **Fertig stellen**.
7. Wählen Sie im Dropdown-Menü **Zu prüfende Objekte** die Option „Lokale Laufwerke“.
8. Klicken Sie auf **Fertig stellen**, um den Task zu übernehmen.

4.8.1.6 So entfernen Sie einen Virus von Ihrem Server

Wenn Ihr Computer die Symptome einer Infektion mit Schadsoftware aufweist, beispielsweise langsamer reagiert oder oft hängt, sollten Sie folgendermaßen vorgehen:

1. Klicken Sie im Hauptfenster von ESET Mail Security auf **Computer prüfen**.

2. Klicken Sie auf **Smart-Prüfung**, um die Systemprüfung zu starten.

3. Nachdem die Prüfung abgeschlossen ist, überprüfen Sie die Anzahl der geprüften, infizierten und wiederhergestellten Dateien im Log.

4. Wenn Sie nur einen Teil Ihrer Festplatte scannen möchten, wählen Sie **Benutzerdefinierter Scan**, und wählen Sie die Objekte aus, die auf Viren gescannt werden sollen.

4.8.2 Senden einer Supportanfrage

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.

Wenn Sie das Webformular einreichen, werden Ihre Systemkonfigurationsdaten an ESET gesendet. Wählen Sie **Diese Informationen immer senden** aus, wenn Sie diese Aktion für den Prozess speichern möchten. Um das Formular ohne das Senden von Daten einzureichen, klicken Sie auf **Keine Daten senden**. Sie können den ESET-Support über das Online-Supportformular erreichen.

Sie finden diese Einstellung auch unter **Erweiterte Einstellungen** > **Tools** > **Diagnose** > **Support**.

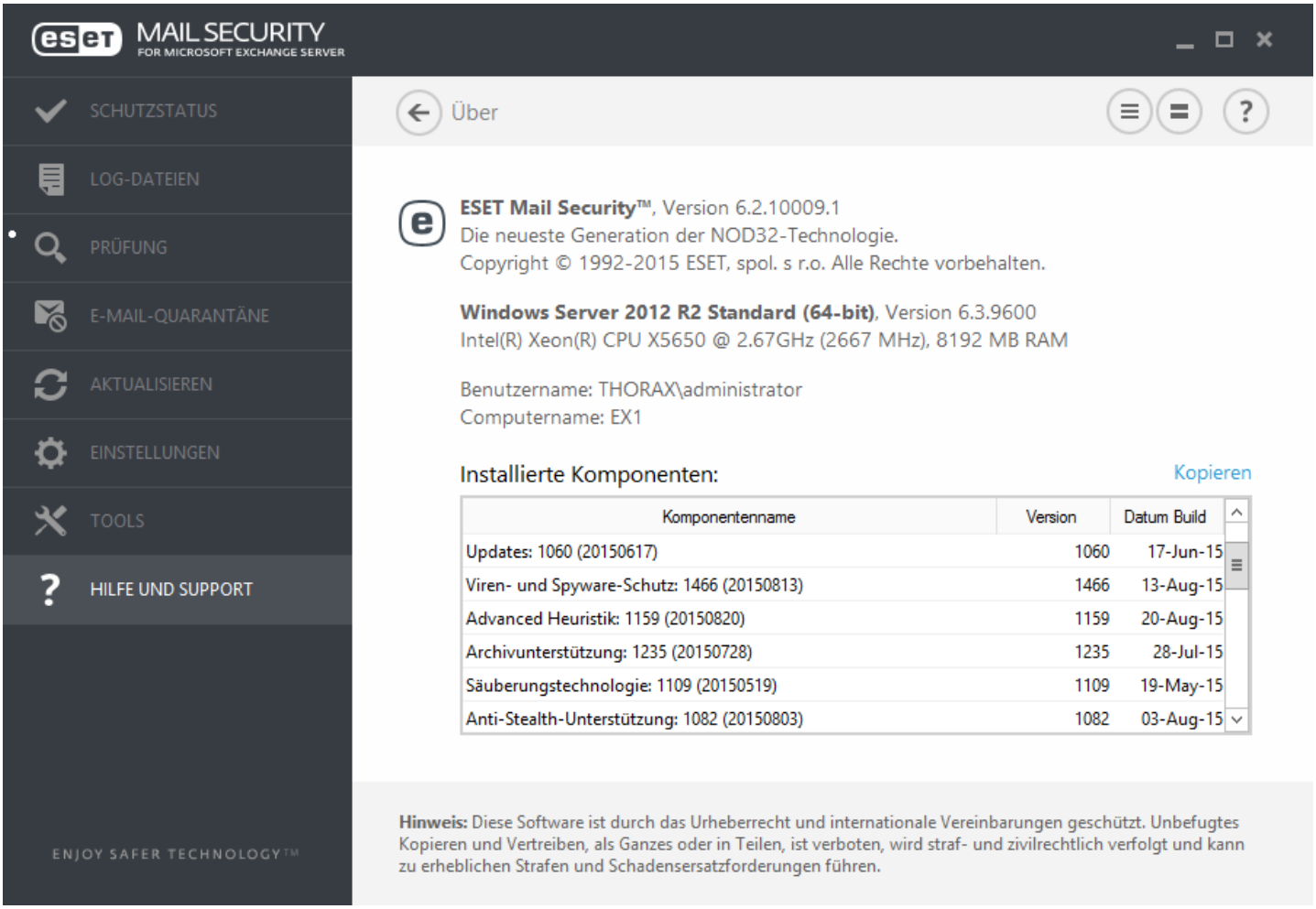
HINWEIS: Wenn Sie Systemdaten einreichen möchten, müssen Sie das Webformular ausfüllen und einreichen. Andernfalls wird kein Ticket erstellt und die Systemdaten werden nicht übermittelt.

4.8.3 Spezielles ESET-Säuberungsprogramm

Das spezielle ESET-Säuberungsprogramm ist ein Entfernungstool für bekannte Schadsoftware-Infektionen wie Conficker, Sirefef oder Necurs. Weitere Informationen finden Sie in diesem Artikel in der ESET Knowledgebase.

4.8.4 Über ESET Mail Security

In diesem Fenster werden Informationen zur installierten Version von ESET Mail Security und die Liste der installierten Programmmodule angezeigt. Der obere Teil des Fensters enthält Informationen zum Betriebssystem und zu den Systemressourcen.



Durch Klicken auf **Kopieren** können Sie Informationen zu den Modulen (**Installierte Komponenten**) in die Zwischenablage kopieren. Dies kann bei der Fehlerbehebung oder beim Kontakt zum Support hilfreich sein.

4.8.5 Produktaktivierung

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

Zur Aktivierung des Produkts stehen verschiedene Methoden zur Verfügung. Die Verfügbarkeit einer bestimmten Aktivierungsmöglichkeit im Aktivierungsfenster hängt vom Land und von der Vertriebsart (CD/DVD, ESET-Webseite usw.) ab.

Sie können Ihre Kopie von ESET Mail Security direkt im Programm aktivieren. Klicken Sie hierfür auf das Symbol im Infobereich der Taskleiste und wählen Sie **Produktlizenz aktivieren** aus dem Menü. Sie können das Produkt auch im Hauptmenü unter **Hilfe und Support** > **Lizenz aktivieren** oder **Schutzstatus** > **Produktlizenz aktivieren** aktivieren.

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

- **Lizenzschlüssel** - Eine eindeutige Zeichenfolge im Format XXXX-XXXX-XXXX-XXXX-XXXX zur Identifizierung des Lizenzinhabers und der Aktivierung der Lizenz.
- **Sicherheitsadministrator Konto** - Ein im ESET License Administrator-Portal erstelltes Konto mit Anmeldedaten (E-Mail-Adresse und Passwort). Mit dieser Methode können Sie mehrere Lizenzen von einem Standort aus verwalten.
- **Offline-Lizenzdatei** - Eine automatisch erzeugte Datei, die zum Zwecke der Bereitstellung von Lizenzinformationen in das ESET-Produkt übertragen wird. Die Offline-Lizenzdatei wird im Lizenzportal erzeugt und in Umgebungen verwendet, in denen die Anwendung keine Verbindung zur Lizenzierungsstelle herstellen kann.

Klicken Sie auf **Später mit RA aktivieren**, wenn Ihr Computer Teil eines verwalteten Netzwerks ist. Anschließend führt der Administrator die Remote-Aktivierung über ESET Remote Administrator aus. Sie können diese Option auch verwenden, wenn Sie diesen Client zu einem späteren Zeitpunkt aktivieren möchten.

Sie können jederzeit im Hauptprogrammfenster auf **Hilfe und Support** > **Lizenz verwalten** klicken, um Ihre Lizenzinformationen zu verwalten. Hier wird die öffentliche Lizenz-ID angezeigt, mit der Ihr Produkt von ESET identifiziert werden kann und die Lizenzinformationen enthält. Ihr Benutzername, unter dem der Computer im Lizenzierungssystem gespeichert ist, befindet sich im Bereich **Über**. Zugriff darauf erhalten Sie, indem Sie mit der rechten Maustaste auf das Symbol im Infobereich der Taskleiste klicken.

HINWEIS: ESET Remote Administrator kann Clientcomputer mithilfe von Lizenzen, die der Administrator bereitstellt, im Hintergrund aktivieren.

4.8.5.1 Registrierung

Registrieren Sie Ihre Lizenz, indem Sie die Felder im Registrierungsformular ausfüllen und auf **Weiter** klicken. Bei den Feldern, neben denen in Klammern „erforderlich“ steht, handelt es sich um Pflichtfelder. Diese Informationen werden nur in Bezug auf Ihre ESET-Lizenz verwendet.

4.8.5.2 Security Admin-Aktivierung

Das Sicherheitsadministratorkonto wird im Lizenzportal mit Ihrer **E-Mail-Adresse** und Ihrem **Passwort** erstellt und ermöglicht es, die Genehmigungen für alle Plätze anzuzeigen.

Mit einem **Sicherheitsadministratorkonto** können Sie mehrere Lizenzen verwalten. Wenn Sie noch kein Sicherheitsadministratorkonto haben, klicken Sie auf **Konto erstellen**. Anschließend werden Sie zur ESET License Administrator-Webseite weitergeleitet, wo Sie sich mit Ihren Daten anmelden können.

Falls Sie Ihr Passwort vergessen haben, klicken Sie auf **Passwort vergessen?**. Anschließend werden Sie zum ESET-Unternehmensportal weitergeleitet. Geben Sie Ihre E-Mail-Adresse ein und klicken Sie auf **Senden**. Sie erhalten in Kürze eine Nachricht mit Anweisungen dazu, wie Sie Ihr Passwort zurücksetzen.

HINWEIS: Weitere Informationen zum ESET License Administrator finden Sie im ESET License Administrator-Benutzerhandbuch.

4.8.5.3 Aktivierungsfehler

Die Aktivierung von ESET Mail Security war nicht erfolgreich. Vergewissern Sie sich, dass Sie den richtigen **Lizenzschlüssel** eingegeben oder eine **Offline-Lizenz** angehängt haben. Wenn Sie über eine andere **Offline-Lizenz** verfügen, geben Sie sie erneut ein. Um den eingegebenen Lizenzschlüssel zu überprüfen, klicken Sie auf **Lizenzschlüssel erneut prüfen**. Wenn Sie auf **neue Lizenz kaufen** klicken, werden Sie zur ESET-Webseite weitergeleitet, wo Sie eine neue Lizenz kaufen können.

4.8.5.4 Lizenz

Wenn Sie die Aktivierungsoption „Sicherheitsadministrator“ wählen, werden Sie zur Auswahl einer mit Ihrem Konto verknüpften Lizenz aufgefordert, die für ESET Mail Security verwendet wird. Klicken Sie auf **Aktivieren**, um fortzufahren.

4.8.5.5 Aktivierungsfortschritt

ESET Mail Security wird jetzt aktiviert, bitte haben Sie Geduld. Dies kann einige Minuten dauern.

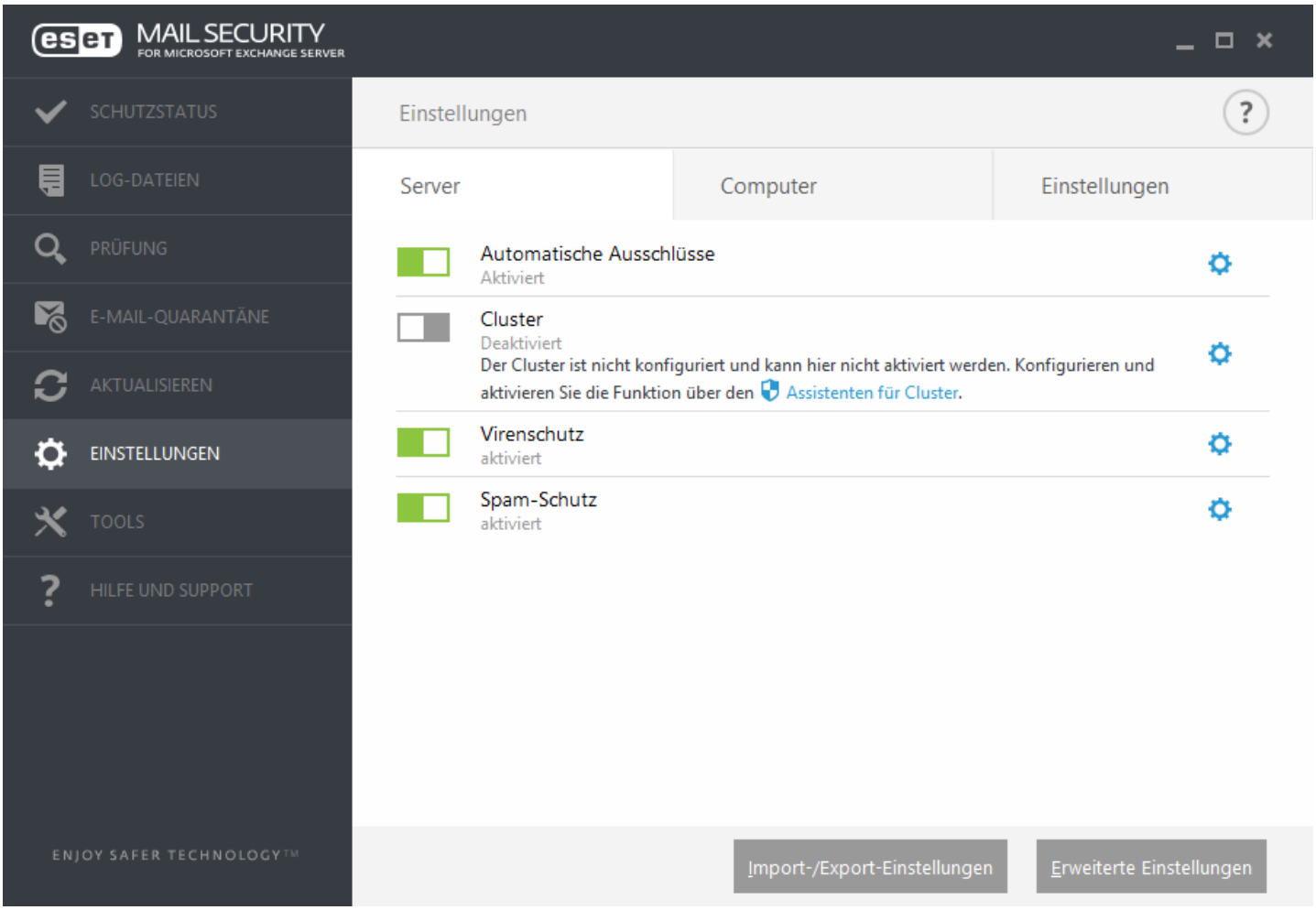
4.8.5.6 Erfolgreiche Aktivierung

Die Aktivierung erfolgreich und ESET Mail Security ist nun 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.

5. Arbeiten mit ESET Mail Security

Das Menü **Einstellungen** enthält die folgenden Bereiche, die Sie über die einzelnen Registerkarten erreichen:

- Server
- Computer
- Tools



Zur vorübergehenden Deaktivierung einzelner Module klicken Sie auf den grünen Schalter neben dem gewünschten Modul. Beachten Sie, dass dies den Schutz Ihres Computers beeinträchtigen kann.
Klicken Sie auf den roten Schalter, um eine deaktivierte Komponente erneut zu aktivieren.
Zugriff auf detaillierte Einstellungen zu einer bestimmten Sicherheitskomponente erhalten Sie, indem Sie auf das Zahnradsymbol **klicken.**

Klicken Sie auf **Erweiterte Einstellungen** oder drücken Sie **F5**, um zusätzliche Einstellungen und Optionen für Komponenten zu öffnen.

Am unteren Rand des Fensters "Einstellungen" finden Sie weitere Optionen. Unter **Einstellungen importieren/exportieren** können Sie Einstellungen aus einer *XML*-Konfigurationsdatei laden oder die aktuellen Einstellungen in einer Konfigurationsdatei speichern. Weitere Informationen hierzu finden Sie unter Einstellungen importieren/exportieren.

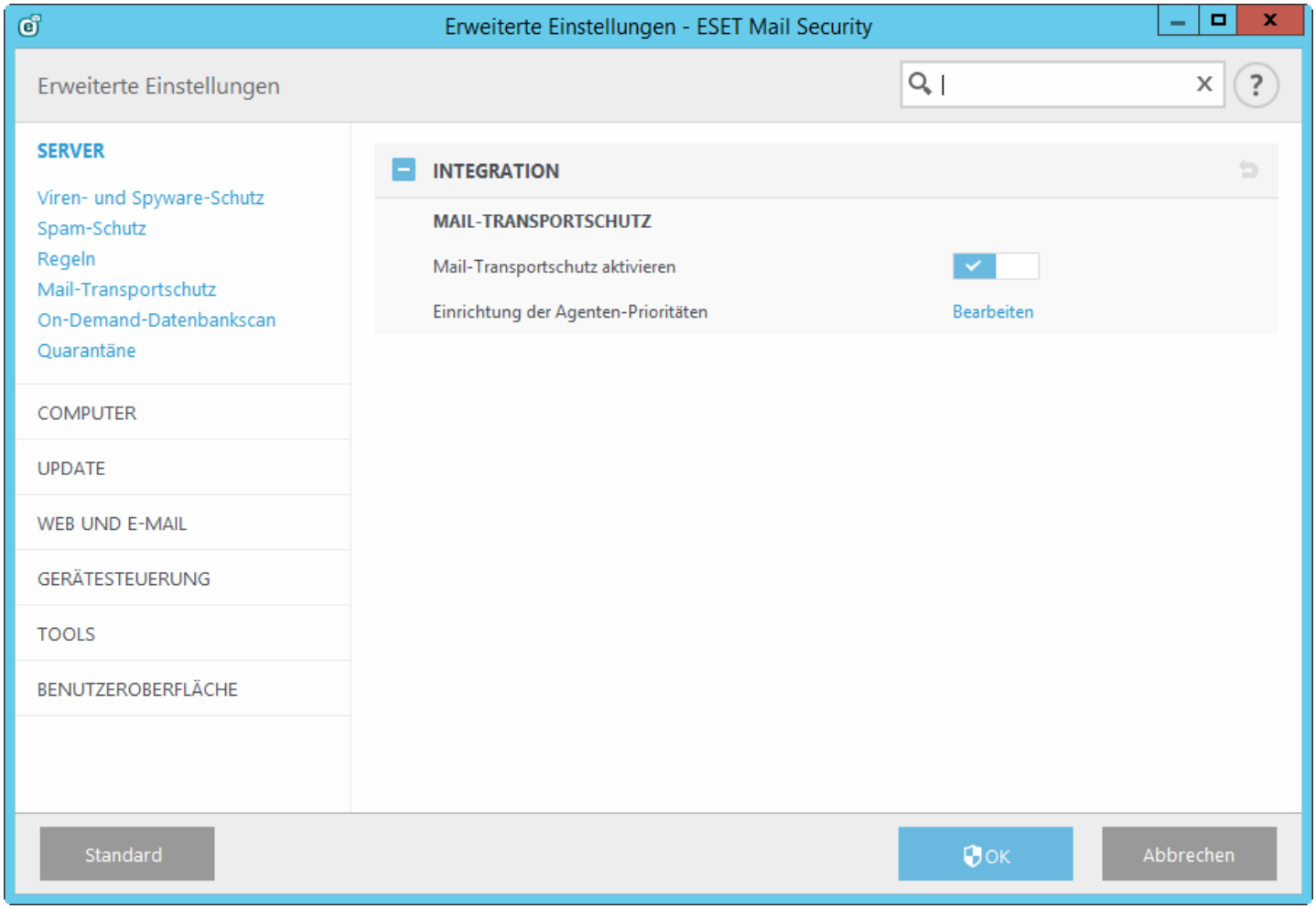
5.1 Server

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

- Viren- und Spyware-Schutz
- Spam-Schutz
- Regeln
- E-Mail-Transportschutz (Exchange Server 2007, 2010, 2013)
- Postfach-Datenbankschutz (Exchange Server 2003, 2007, 2010)
- On-Demand-Datenbankprüfung (Exchange Server 2007, 2010, 2013)
- Quarantäne (Einstellungen für E-Mail-Quarantäne)

Im Bereich für erweiterte Einstellungen können Sie die Funktionen Postfach-Datenbankschutz und E-Mail-Transportschutz aktiveren/deaktivieren und die Agenten-Priorität bearbeiten.

HINWEIS: Falls Sie Microsoft Exchange Server 2007 oder 2010 verwenden, können Sie zwischen Postfach-Datenbankschutz und On-Demand-Datenbankprüfung wählen. Es kann jedoch nur eine dieser beiden Schutzarten gleichzeitig aktiv sein. Wenn Sie sich für die On-Demand-Datenbankprüfung entscheiden, müssen Sie die Integration für den Postfach-Datenbankschutz deaktivieren. Andernfalls ist die On-Demand-Datenbankprüfung nicht verfügbar.



5.1.1 Einstellungen für Agentenpriorität

Im Menü **Agentenpriorität einrichten** können Sie konfigurieren, mit welcher Priorität die ESET Mail Security-Agenten nach dem Start von Microsoft Exchange Server aktiviert werden. Der numerische Wert definiert die Priorität. Je kleiner die Zahl, desto höher die Priorität. Dies gilt für Microsoft Exchange 2003.

Klicken Sie auf **Bearbeiten**, um ein Fenster zu öffnen, in dem Sie die Priorität für die Aktivierung von ESET Mail Security-Agenten nach dem Start von Microsoft Exchange Server festlegen können.

- **Bearbeiten** - Weisen Sie einem ausgewählten Agenten manuell eine neue Priorität zu.
- **Nach oben** - Sie können die Priorität eines ausgewählten Agenten erhöhen, indem Sie ihn auf eine höhere Listenposition verschieben.
- **Nach unten** - Sie können die Priorität eines ausgewählten Agenten verringern, indem Sie ihn auf eine niedrigere Listenposition verschieben.

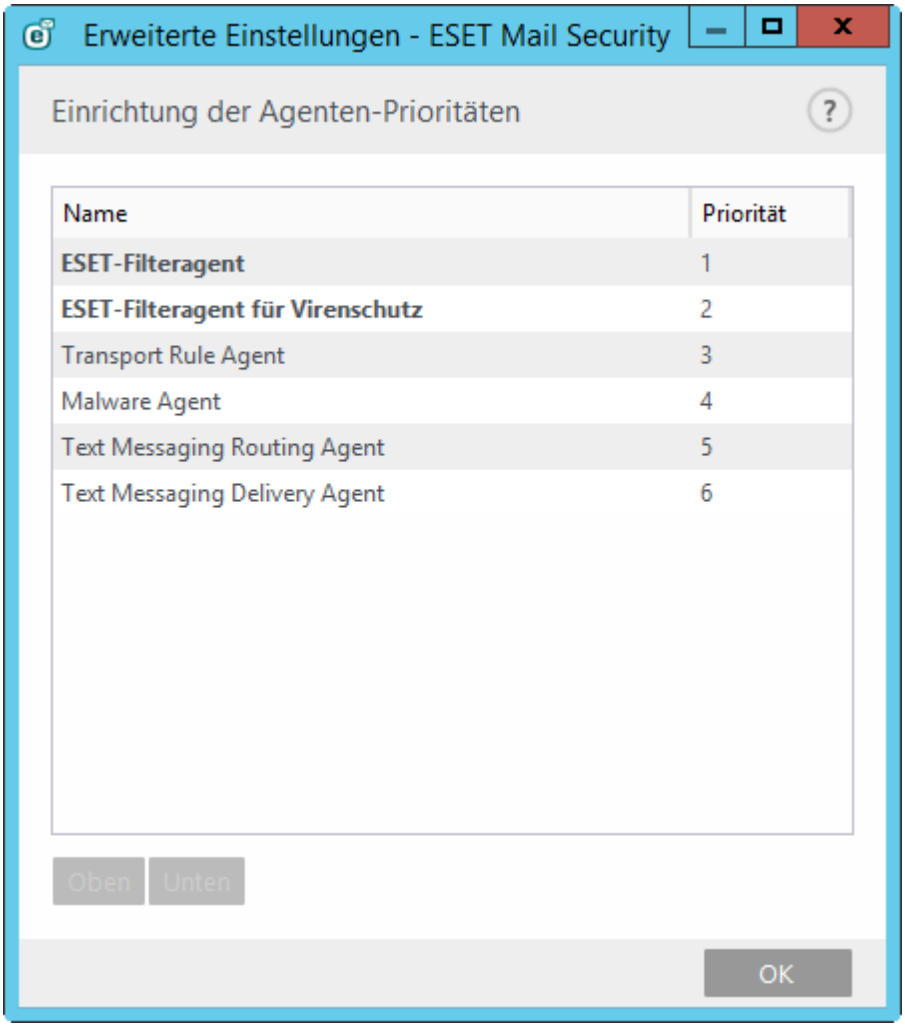
In Microsoft Exchange Server 2003 können Sie die Priorität einzelner Agenten unabhängig voneinander in den Registerkarten für EOD (End of Data) und RCPT (Empfänger) konfigurieren.

5.1.1.1 Priorität bearbeiten

Falls Sie Microsoft Exchange Server 2003 verwenden, können Sie die **Priorität des Transport-Agenten** manuell definieren. Geben Sie eine Zahl in das Textfeld ein oder verwenden Sie die Pfeile nach oben und unten, um die Priorität zu ändern. Je kleiner die Zahl, desto höher die Priorität.

5.1.2 Einstellungen für Agentenpriorität

Im Menü **Agentenpriorität einrichten** können Sie konfigurieren, mit welcher Priorität die ESET Mail Security-Agenten nach dem Start von Microsoft Exchange Server aktiviert werden. Dies gilt ab Microsoft Exchange 2007.



- **Nach oben** - Sie können die Priorität eines ausgewählten Agenten erhöhen, indem Sie ihn auf eine höhere Listenposition verschieben.
- **Nach unten -** Sie können die Priorität eines ausgewählten Agenten verringern, indem Sie ihn auf eine niedrigere Listenposition verschieben.

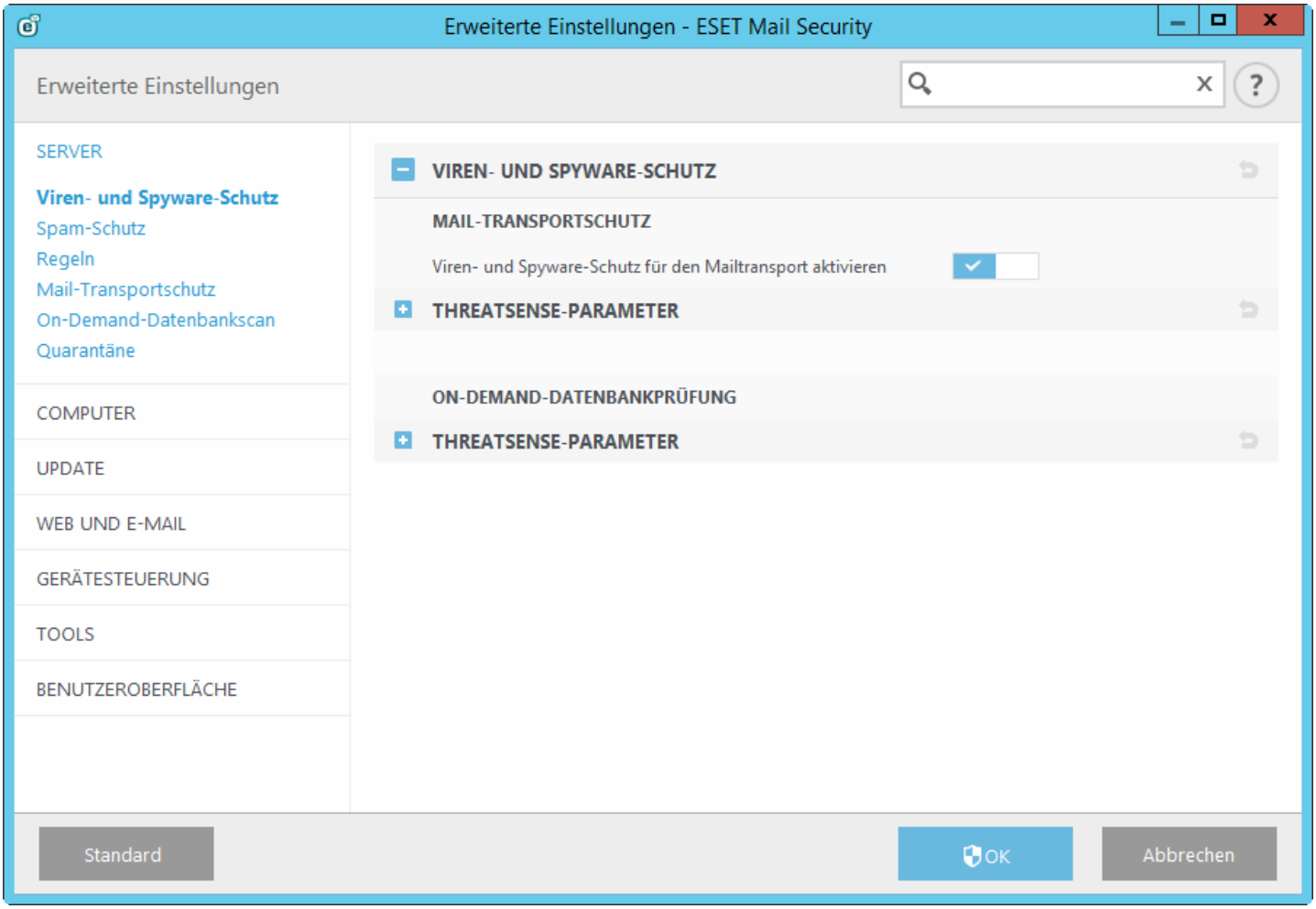
5.1.3 Viren- und Spyware-Schutz

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

WICHTIGER HINWEIS: Der E-Mail-Transportschutz wird vom Transportagenten bereitgestellt und ist nur für Microsoft Exchange Server 2007 oder neuere Versionen verfügbar, wenn Ihr 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).

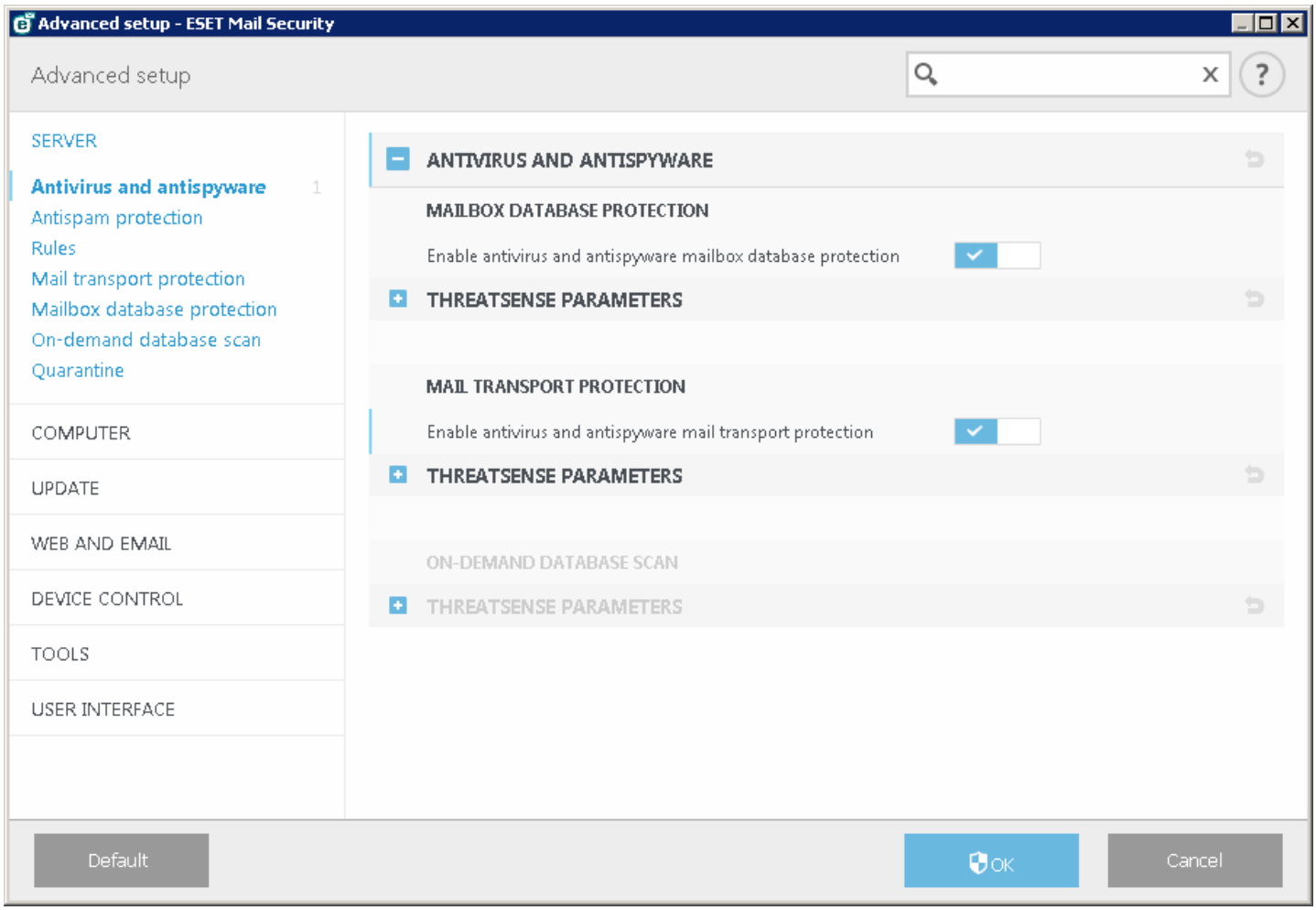
Mail-Transportschutz:

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.



Postfach-Datenbankschutz:

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.



5.1.4 Spam-Schutz

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

Über die Funktion **Spam-Schutz mit Exchange Server-Positivlisten automatisch umgehen** können Sie angeben, dass 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.

Die Option **Markierung der SMTP-Sitzung zur Umgehung des Spam-Schutzes zulassen** ist hilfreich, wenn authentifizierte SMTP-Sitzungen zwischen Exchange-Servern auftreten, 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.

HINWEIS: Die Spamschutz-Datenbank muss regelmäßig aktualisiert werden, um einen optimalen Schutz durch das Spamschutz-Modul sicherzustellen. Stellen Sie sicher, dass ESET Mail Security auf die korrekten IP-Adressen und

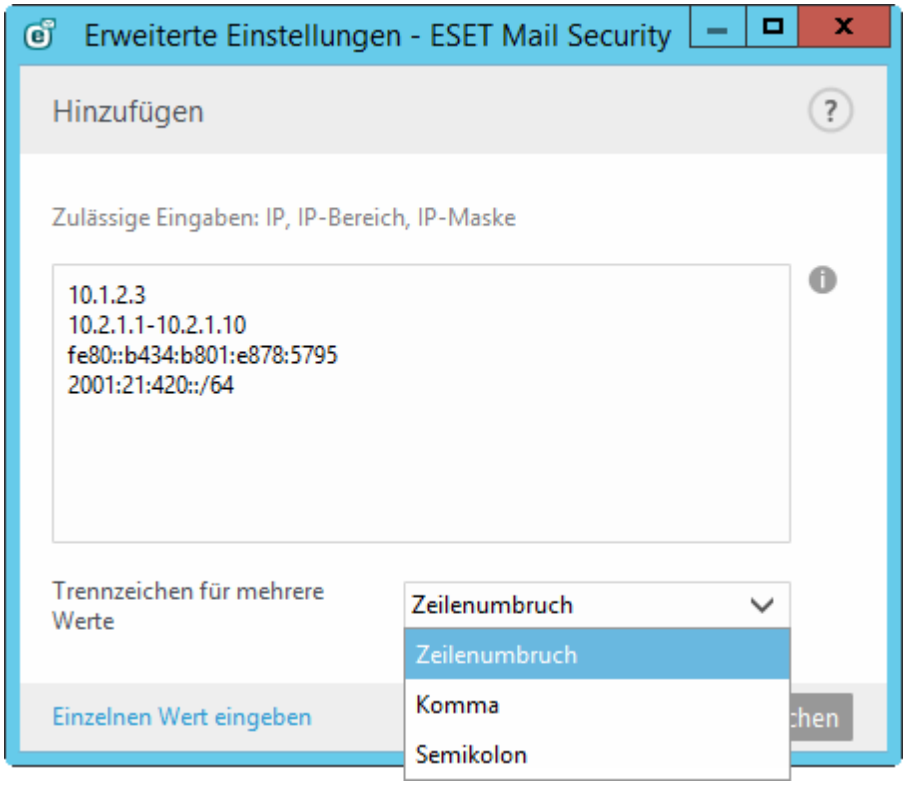
die entsprechenden Ports zugreifen kann, um regelmäßige Updates der Spamschutz-Datenbank zu ermöglichen. Weitere Informationen zu den IP-Adressen und Ports, die dafür in Ihrer Firewall aktiviert werden müssen, finden Sie in unserem KB-Artikel.

5.1.4.1 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**.

- **Liste genehmigter IP-Adressen** – E-Mails von den angegebenen IP-Adressen werden automatisch zur Positivliste hinzugefügt.
- **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.
- **Liste blockierter Körper-Domains** – E-Mails, die bestimmte Domains im Nachrichtenkörper enthalten, werden blockiert.
- **Liste ignorierter Körper-Domains** – Die angegebenen Domains im Nachrichtenkörper werden bei der Klassifizierung ignoriert.
- **Liste blockierter Körper-IP-Adressen** – E-Mails, die bestimmte IP-Adressen im Nachrichtenkörper enthalten, werden blockiert.
- **Liste ignorierter Körper-IP-Adressen** – Die angegebenen IP-Adresse im Nachrichtenkörper werden bei der Klassifizierung ignoriert.
- **Liste genehmigter Absender** – E-Mails von den angegebenen Absendern werden automatisch zur Positivliste hinzugefügt.
- **Liste blockierter Absender** – E-Mails von den angegebenen Absendern werden blockiert.
- **Liste genehmigte Domäne zu IP** – E-Mails von IP-Adressen, die über Domänen in dieser Liste aufgelöst wurden, werden automatisch zur Positivliste hinzugefügt.
- **Liste blockierte Domäne zu IP** – E-Mails von IP-Adressen, die über Domänen in dieser Liste aufgelöst wurden, werden blockiert.
- **Liste ignorierte Domäne zu IP** – Eine Liste mit Domänen, deren entsprechende IP-Adressen bei der Klassifizierung nicht überprüft werden.
- **Liste blockierter Zeichensätze** – E-Mails mit bestimmten Zeichensätzen werden blockiert.
- **Liste blockierter Länder** – E-Mails aus bestimmten Ländern werden blockiert.

HINWEIS: Klicken Sie im Popupfenster auf **Mehrere Werte eingeben**, um mehrere Einträge gleichzeitig anzulegen. Wählen Sie anschließend das gewünschte Trennzeichen aus: **Neue Zeile**, **Komma** oder **Semikolon**. Beispiel:



5.1.4.2 Erweiterte Einstellungen

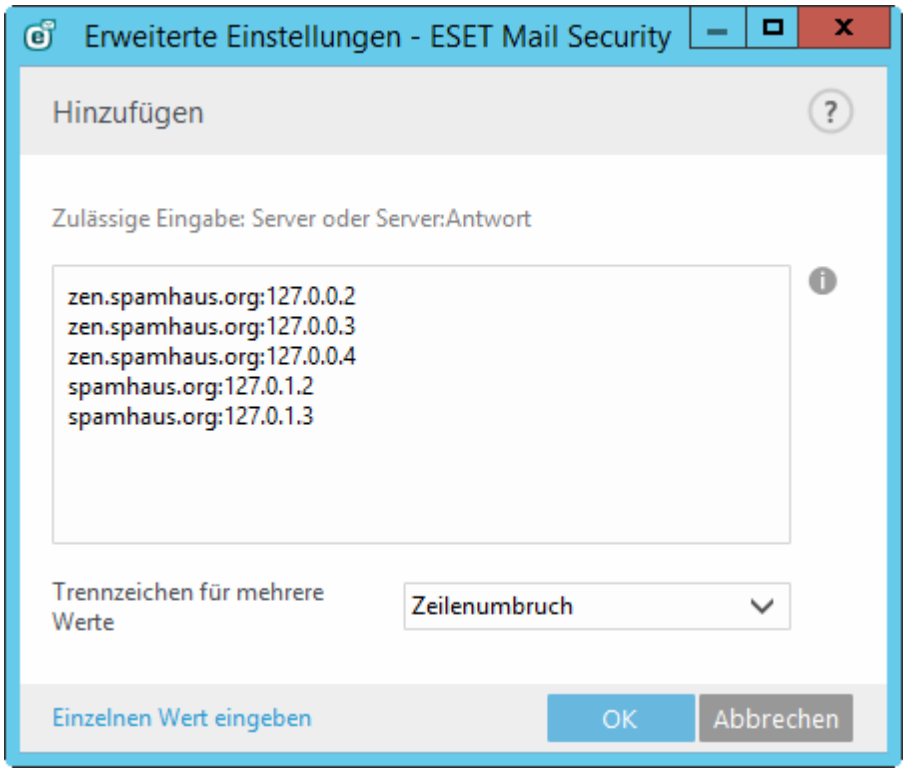
Mit diesen Einstellungen können E-Mails anhand definierter Kriterien von externen Servern geprüft werden (**RBL** - Realtime Blackhole List, **DNSBL** - DNS Blocklist).

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 werden IP-Adressen unbegrenzt 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.

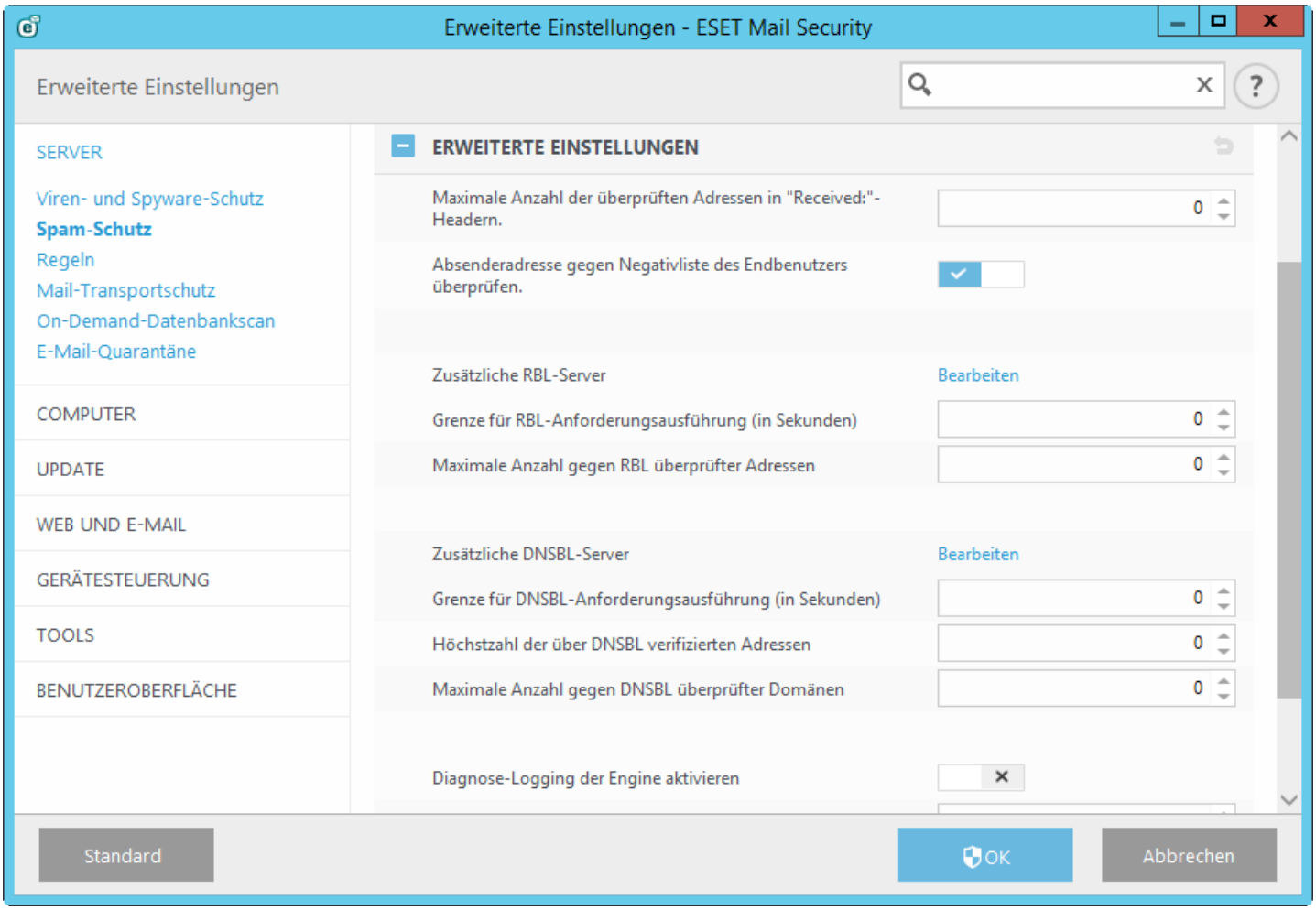
Zusätzliche RBL-Server – Liste der RBL (Realtime Blackhole List)-Server, die bei der E-Mail-Analyse abgefragt werden.

HINWEIS: Geben Sie beim Hinzufügen zusätzlicher RBL-Server den Domänennamen der Server mit einem Rückgabecode im Format `Server:Antwort` (z. B. `zen.spamhaus.org:127.0.0.4`) ein. Fügen Sie außerdem Servernamen und Rückgabecodes separat hinzu, um eine komplette Liste zu erhalten. Klicken Sie im Popupfenster 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:



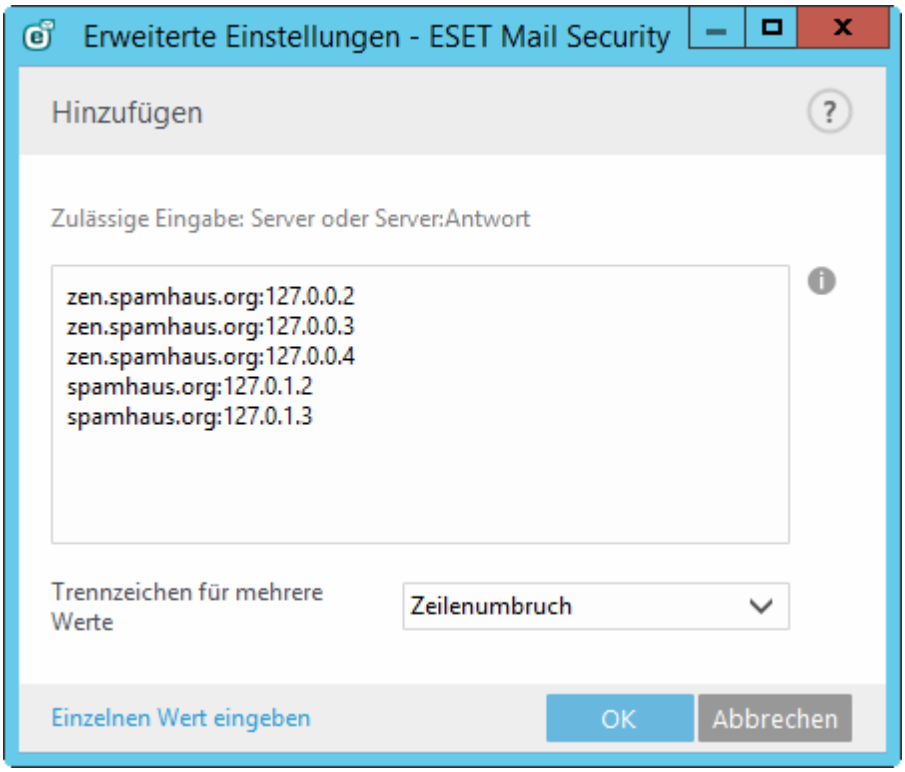
Zeitlimit für die Ausführung der RBL-Anfrage (in Sekunden) – Ermöglicht das Festlegen eines Zeitlimits für RBL-Abfragen. Nur die RBL-Antworten von den RBL-Servern, die rechtzeitig geantwortet haben, werden verwendet. Wenn der Wert auf "0" festgelegt ist, wird kein Zeitlimit verwendet.

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, mit Domänen und IP-Adressen aus dem Nachrichteninhalt abgefragt werden sollen.

HINWEIS: Geben Sie beim Hinzufügen zusätzlicher DNSBL-Server den Domänennamen der Server mit einem Rückgabecode im Format `Server:Antwort` (z. B. `zen.spamhaus.org:127.0.0.4`) ein. Fügen Sie außerdem Servernamen und Rückgabecodes separat hinzu, um eine komplette Liste zu erhalten. Klicken Sie im Popupfenster 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:



Zeitlimit für die Ausführung der DNSBL-Anfrage (in Sekunden) – Ermöglicht das Festlegen eines Zeitlimits für DNSBL-Abfragen.

Maximale Anzahl gegen DNSBL überprüfter 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 Domänen begrenzen, die auf dem DNSBL-Server abgerufen werden.

Diagnose-Logging für Modul aktivieren - Schreibt ausführliche Informationen über das Spamschutzmodul zu Diagnosezwecken in die Log-Dateien.

Max. Größe zu scannender Nachrichten (KB) - Schränkt die Spamschutzprüfung für Nachrichten ein, die größer als der angegebene Wert sind. Diese Nachrichten werden nicht vom Spamschutzmodul geprüft. Aktion:

Max. Größe zu scannender Nachrichten: 0 = unbegrenzt prüfen
Max. Größe zu scannender Nachrichten: 1 - 12288 = 12288
Max. Größe zu scannender Nachrichten: mehr als 12288 = Wert festlegen
Der empfohlene Mindestwert ist 100 kB.

5.1.4.3 Einstellungen für die Grauliste

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 nicht erkannten 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.

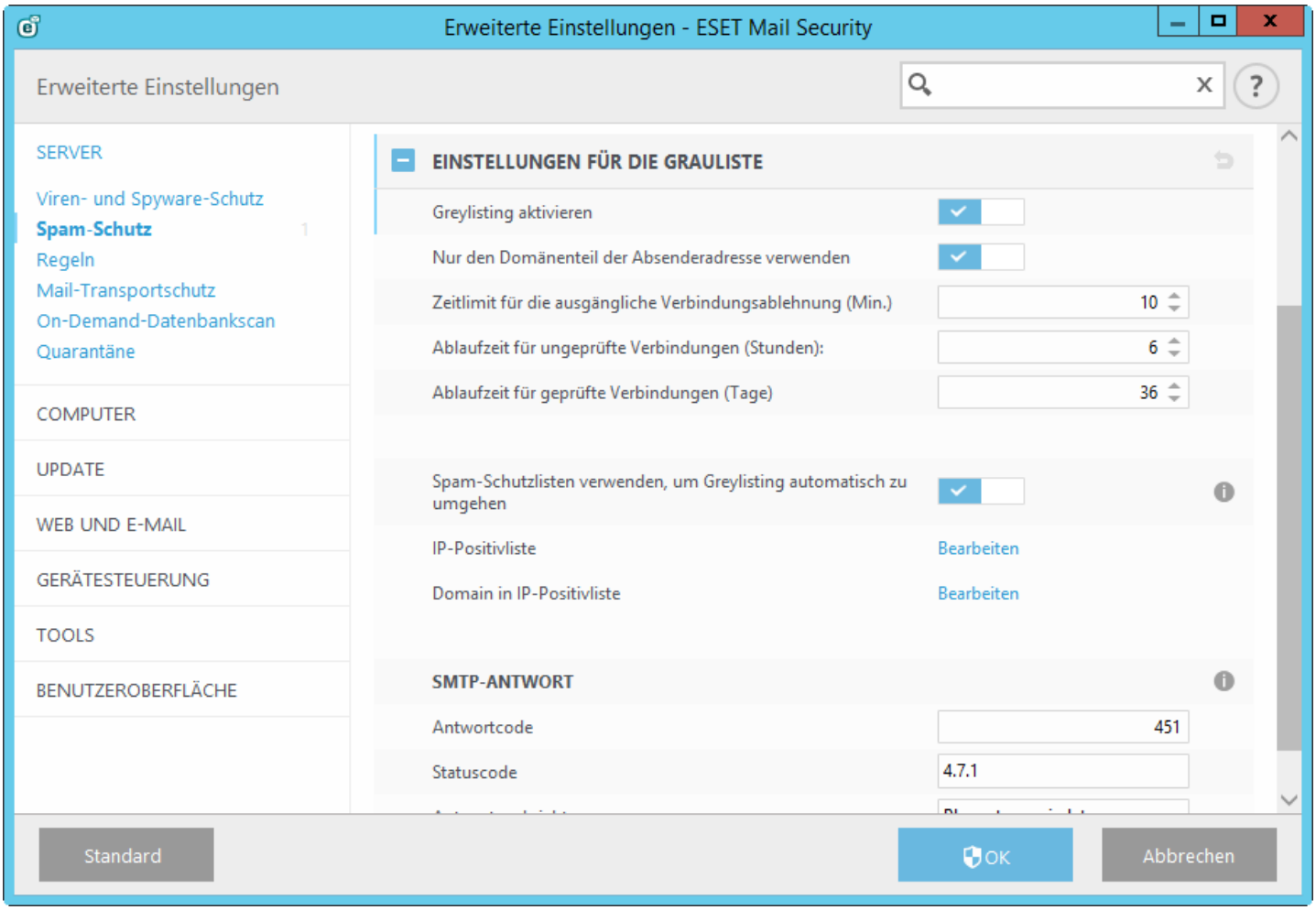
Beim Prüfen des Absenders berücksichtigt die Greylisting-Technik neben den AntispamBypass-Einstellungen für das Postfach des Empfängers auch die Einstellungen für die folgenden Listen auf dem Exchange-Server: **Freigegebene IP-Adressen**, **Ignorierte IP-Adressen**, **Sichere Absender** und **IP-Adressen 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 - Der Name des Absenders in der E-Mail-Adresse wird ignoriert, nur die Domäne wird berücksichtigt.

Zeitlimit für Abweisen des ersten Zustellversuchs (Min.) – Legt die Zeitspanne fest, in der die E-Mail, die beim ersten Sendeversuch vorübergehend abgelehnt wurde, immer abgelehnt wird (gemessen ab der ersten Ablehnung). Ist diese Zeitspanne vorüber, kann die E-Mail erfolgreich gesendet werden. Der Mindestwert beträgt 1 Minute.

Ablauf nicht verifizierter Verbindungen nach (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**.

Ablauf verifizierter Verbindungen nach (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) - Sie können **Antwortcode**, **Statuscode** und **Antwortnachricht** an den SMTP-Server für die Ablehnung einer E-Mail festlegen.

Beispiel für eine SMTP Reject-Antwort:

Antwortcode	Statuscode	Antwortnachricht
451	4.7.1	Angeforderte Aktion abgebrochen: lokaler Fehler bei der Verarbeitung

ACHTUNG: 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.

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

5.1.5 Regeln

Mit den **Regeln** können Administratoren manuell Filterbedingungen für E-Mails definieren und Aktionen mit gefilterten E-Mails verknüpfen.

Es gibt drei grundsätzliche Arten von Regeln. Die für Ihr System verfügbaren Regeln hängen davon ab, welche Version von Microsoft Exchange Server auf dem Server mit ESET Mail Security installiert ist:

- Postfach-Datenbankschutz - Dieser Schutz ist nur für Microsoft Exchange Server 2010, 2007 und 2003 verfügbar, wenn diese in der Rolle als Postfachserver (Microsoft Exchange 2010 und 2007) bzw. Backend-Server (Microsoft Exchange 2003) ausgeführt werden. 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).
- E-Mail-Transportschutz - Dieser Schutz wird vom Transportagenten bereitgestellt und ist nur für Microsoft Exchange Server 2007 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).
- On-Demand-Datenbankprüfung - ermöglicht die Planung und Ausführung von Prüfungen für Exchange-Postfächer. Dieses Feature ist nur für Microsoft Exchange Server 2007 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). Unter Rollen in Exchange Server 2013 finden Sie weitere Informationen zu Rollen in Exchange 2013.

5.1.5.1 Regelliste

Eine Regel besteht aus **Bedingungen** und **Aktionen**. Wenn alle Bedingungen für eine E-Mail erfüllt sind, werden die entsprechenden Aktionen für diese E-Mail ausgeführt. Regeln werden also anhand einer Kombination von Bedingungen angewendet. Wenn eine Regel mehrere Bedingungen enthält, werden diese durch ein logisches UND verknüpft, und die Regel wird nur angewendet, wenn alle Bedingungen erfüllt sind.

In der **Regelliste** werden die vorhandenen Regeln angezeigt. Regeln sind in drei Stufen unterteilt, und werden in der folgenden Reihenfolge ausgewertet:

- **Filterregeln (1)**
- **Regeln für Anhänge (2)**
- **Regeln für Ergebnisse (3)**

Regeln derselben Ebene werden in der Reihenfolge ausgewertet, in der sie in der Regelliste angezeigt werden. Sie können die Reihenfolge nur für Regeln innerhalb derselben Ebene ändern. Wenn Sie z. B. mehrere Filterregeln haben, können Sie deren Reihenfolge festlegen. Sie können dagegen keine Regeln für Anhänge 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.

- **Hinzufügen...** - Neue Regel hinzufügen
- **Bearbeiten...** - Bestehende Regel bearbeiten
- **Entfernen** - Ausgewählte Regel entfernen
- **Nach oben** - Ausgewählte Regel in der Liste nach oben verschieben
- **Nach unten** - Ausgewählte Regel in der Liste nach unten verschieben
- **Zurücksetzen** - Zähler für die ausgewählte Regel zurücksetzen (Spalte "Treffer")

HINWEIS: Wenn eine neue Regel hinzugefügt oder eine bestehende Regel bearbeitet wird, beginnt automatisch eine erneute E-Mail-Prüfung nach den neuen/geänderten Regeln.

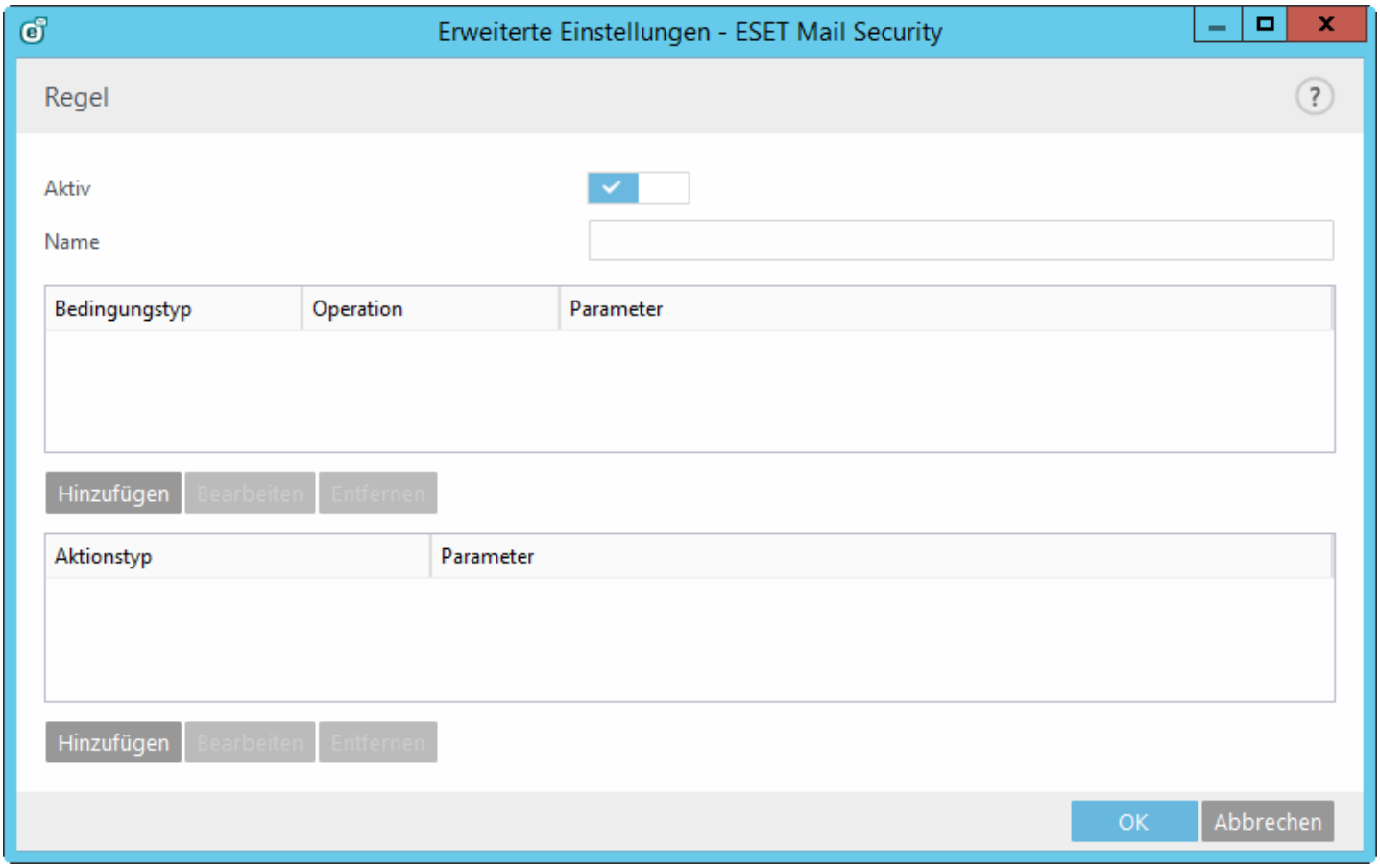
Die Überprüfung der Nachrichten mit Anwendung der Regeln erfolgt durch den Transport-Agenten (TA) oder VSAPI. Sind sowohl TA als auch VSAPI aktiviert und die E-Mail erfüllt die Regelbedingungen, kann sich der Regel-Zähler um 2 oder mehr erhöhen. VSAPI greift auf Text und Anhänge einer E-Mail separat zu, und daher werden die Regeln für die verschiedenen Komponenten einzeln angewendet. Die Regeln werden auch bei der Hintergrundprüfung (z. B. wenn ESET Mail Security nach dem Download einer neuen Signaturdatenbank eine Postfachprüfung ausführt) verwendet, wodurch der Regel-Zähler steigen kann.

5.1.5.1.1 Regelassistent

Sie können **Bedingungen** und **Aktionen** im **Regelassistenten** definieren. Definieren Sie zunächst Bedingungen, und anschließend Aktionen. Klicken Sie auf **Hinzufügen**, um ein Fenster für Regelbedingungen zu öffnen, in dem Sie Bedingungstyp, Vorgang und Wert festlegen können. In diesem Fenster können Sie außerdem eine Regelaktion hinzufügen. Definieren Sie Bedingungen und Regeln, und geben Sie anschließend einen **Namen** ein, mit dem Sie die Regel wiedererkennen. Dieser Name wird anschließend in der Regelliste angezeigt. 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, markieren Sie das Kontrollkästchen neben der entsprechenden Regeln in der Regellliste.

HINWEIS: **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 den Regelnamen eingegeben haben, sondern erst, wenn Sie auf **OK** klicken.

Manche **Bedingungen** und **Aktionen** haben unterschiedliche Funktionsweisen für **E-Mail-Transportschutz**, **Postfach-Datenbankschutz** und **On-Demand-Datenbankprüfung**. Dies liegt daran, dass diese Schutztypen unterschiedliche Ansätze bei der Verarbeitung von E-Mails verwenden, insbesondere der **E-Mail-Transportschutz**.



HINWEIS: 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:

IP-Adresse - Wird von **On-Demand-Datenbankprüfung** und **Postfach-Datenbankschutz ignoriert**
Postfach - wird vom **E-Mail-Transportschutz ignoriert**

5.1.5.1.1.1 Regelbedingung

Mit diesem Assistenten können Sie Bedingungen für eine Regel anlegen. Wählen Sie **Typ** > **Vorgang** in der Dropdownliste aus (die Liste ändert sich je nach ausgewähltem Regeltyp) und klicken Sie auf **Parameter**. Die Parameterfelder ändern sich je nach ausgewähltem Regeltyp und Vorgang.

Wählen Sie zum Beispiel **Größe des Anhangs** > **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 der Regelaktion verarbeitet, die Sie ausgewählt haben. Wählen Sie daher die gewünschte Aktion beim Auslösen dieser Regel aus, falls Sie dies beim Einstellen der Parameter für die Regel noch nicht getan haben.

HINWEIS: Sie können mehrere Bedingungen für eine Regel anlegen. Wenn Sie mehrere Bedingungen hinzufügen, werden alle Bedingungen, die sich gegenseitig aufheben, ausgeblendet.

Die folgenden **Bedingungen** sind für den **E-Mail-Transportschutz** verfügbar (je nach zuvor ausgewählten Bedingungen werden möglicherweise nicht alle Optionen angezeigt):

- **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
- **Empfänger** - gilt für Nachrichten an einen bestimmten Empfänger
- **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
- **Typ des Anhangs** - gilt für Nachrichten mit einem bestimmten Dateityp als Anhang. Dateitypen sind zur einfachen Auswahl in Gruppen geordnet. Sie können mehrere Typen oder ganze Kategorien auswählen.
- **Größe der Nachricht** - gilt für Nachrichten mit Anhängen, die eine bestimmte Größe nicht erfüllen, in einem angegebenen Bereich zwischen zwei Größen liegen oder eine bestimmte Größe überschreiten
- **Ergebnis des Spam-Schutzes** - gilt für Nachrichten, die als Ham oder Spam markiert bzw. nicht markiert wurden
- **Ergebnis des Virenschutzes** - gilt für Nachrichten, die bösartig bzw. nicht bösartig markiert wurden
- **Interne Nachricht** - gilt für interne bzw. nicht interne Nachrichten
- **Empfangszeit** - gilt für Nachrichten, die vor oder nach einem bestimmten Zeitpunkt oder während eines angegebenen Zeitintervalls empfangen wurden
- **Nachrichtenheader** - gilt für Nachrichten mit bestimmten Daten im Nachrichtenheader
- **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)
- **IP-Adresse des Absenders** - gilt für Nachrichten von einer bestimmten IP-Adresse
- **Domäne des Absenders** - gilt für Nachrichten von Absendern mit einer bestimmten Domäne in der E-Mail-Adresse

- **Organisationseinheiten des Empfängers** - gilt für Nachrichten an Empfänger in einer bestimmten Organisationseinheit

Liste der verfügbaren Bedingungen für Postfach-Datenbankschutz und On-Demand-Datenbankprüfung (je nach zuvor ausgewählten Bedingungen werden möglicherweise nicht alle Optionen angezeigt):

- **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
- **Empfänger** - gilt für Nachrichten an einen bestimmten Empfänger
- **Postfach** - gilt für Nachrichten in einem bestimmten Postfach
- **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
- **Typ des Anhangs** - gilt für Nachrichten mit einem bestimmten Dateityp als Anhang. Dateitypen sind zur einfachen Auswahl in Gruppen geordnet. Sie können mehrere Typen oder ganze Kategorien auswählen.
- **Ergebnis des Virenschutzes** -**Ergebnis des Virenschutzes** - gilt für Nachrichten, die bösartig bzw. nicht bösartig markiert wurden
- **Empfangszeit** - gilt für Nachrichten, die vor oder nach einem bestimmten Zeitpunkt oder während eines angegebenen Zeitintervalls empfangen wurden
- **Nachrichtenheader** - gilt für Nachrichten mit bestimmten Daten im Nachrichtenheader
- **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)
- **IP-Adresse des Absenders** - gilt für Nachrichten von einer bestimmten IP-Adresse
- **Domäne des Absenders** - gilt für Nachrichten von Absendern mit einer bestimmten Domäne in der E-Mail-Adresse

5.1.5.1.1.2 Regelaktionen

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

HINWEIS: Sie können mehrere Bedingungen für eine Regel anlegen. Wenn Sie mehrere Bedingungen hinzufügen, werden alle Bedingungen, die sich gegenseitig aufheben, ausgeblendet.

Die Liste der verfügbaren **Aktionen** für den **E-Mail-Transportschutz** verfügbar (je nach zuvor ausgewählten Bedingungen werden möglicherweise nicht alle Optionen angezeigt):

- **E-Mail in Quarantäne verschieben** - Die Nachricht wird nicht an den Empfänger zugestellt, sondern stattdessen in die E-Mail-Quarantäne verschoben
- **Anhang löschen -** Löscht einen Nachrichtenanhang. Die Nachricht wird ohne Anhang an den Empfänger zugestellt
- **Nachricht ablehnen** - Die Nachricht wird nicht zugestellt, und der Absender erhält einen Unzustellbarkeitsbericht
- **Nachricht automatisch löschen** - Die Nachricht wird ohne Unzustellbarkeitsbericht gelöscht
- **SCL-Wert festlegen** - Ändert einen bestimmten SCL-Wert bzw. legt diesen fest

- **E-Mail-Benachrichtigung verschicken -** Verschickt eine E-Mail-Benachrichtigung
- **Spamschutz-Scan überspringen** - Die Nachricht wird nicht vom Spamschutzmodul geprüft
- **Virenschutz-Scan überspringen** - Die Nachricht wird nicht vom Virenschutzmodul geprüft
- **Weitere Regeln auswerten** - Mit der Auswertung weiterer Regeln können Benutzer verschiedene Sätze von Bedingungen definieren und entsprechende Aktionen festlegen
- **Logging in Ereignissen -** Angaben zur angewendeten Regel werden in das Programm-Log geschrieben
- **Headerfeld hinzufügen** - fügt eine benutzerdefinierte Zeichenfolge zu einem Nachrichtenheader hinzu

Liste der verfügbaren **Aktionen** für **Postfach-Datenbankschutz** und **On-Demand-Datenbankprüfung** (je nach zuvor ausgewählten Bedingungen werden möglicherweise nicht alle Optionen angezeigt):

- **Anhang löschen -** Löscht einen Nachrichtenanhang. Die Nachricht wird ohne Anhang an den Empfänger zugestellt
- **Anhang in Quarantäne verschieben** - Der E-Mail-Anhang wird in die E-Mail-Quarantäne verschoben, und die Nachricht wird ohne Anhang an den Empfänger zugestellt
- **Anhang durch Aktionsinformationen ersetzen** - Entfernt einen Anhang und fügt Informationen zur ausgeführten Aktion zum E-Mail-Text hinzu
- **Nachricht löschen** - Löscht die E-Mail
- **E-Mail-Benachrichtigung verschicken -** Verschickt eine E-Mail-Benachrichtigung
- **Virenschutz-Scan überspringen** - Die Nachricht wird nicht vom Virenschutzmodul geprüft
- **Weitere Regeln auswerten** - Mit der Auswertung weiterer Regeln können Benutzer verschiedene Sätze von Bedingungen definieren und entsprechende Aktionen festlegen
- **Logging in Ereignissen -** Angaben zur angewendeten Regel werden in das Programm-Log geschrieben
- **Nachricht in Papierkorb verschieben** (nur verfügbar für **On-Demand-Datenbankprüfung**) - verschiebt eine E-Mail auf der Seite des E-Mail-Clients in den Papierkorb

5.1.6 Schutz für E-Mail-Datenbank

Unter den folgenden Betriebssystemen ist der **Postfach-Datenbankschutz** verfügbar unter **Erweiterte Einstellungen** > **Server**:

- Microsoft Exchange Server 2003 (Backend-Serverrolle)
- Microsoft Exchange Server 2003 (Installation auf einzelnem Server mit mehreren Rollen)
- Microsoft Exchange Server 2007 (Postfachserverrolle)
- Microsoft Exchange Server 2007 (Installation auf einzelnem Server mit mehreren Rollen)
- Microsoft Exchange Server 2010 (Postfachserverrolle)
- Microsoft Exchange Server 2010 (Installation auf einzelnem Server mit mehreren Rollen)
- Windows Small Business Server 2003
- Windows Small Business Server 2008
- Windows Small Business Server 2011

HINWEIS: Für Microsoft Exchange Server 2013 ist der Postfach-Datenbankschutz nicht verfügbar.

Wenn Sie die Option **Viren- und Spyware-Schutz mit VSAPI 2.6** deaktivieren, wird das ESET Mail Security-Plug-In für Exchange Server nicht aus dem Exchange-Serverprozess entfernt. Vielmehr werden die E-Mails dann lediglich weitergeleitet, ohne eine Virenprüfung vorzunehmen. Die E-Mails werden allerdings weiterhin auf Spam geprüft, und die Regeln werden angewendet.

Wenn die Option **Proaktive Prüfung** 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.

Hintergrundprüfung 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. Es findet eine Prüfung statt, bevor Sie die E-Mail in Ihrem E-Mail-Programm öffnen können. Sie können zwischen den Optionen **Nur Nachrichten mit Dateianlage überprüfen** und **Prüfstufe** (filterbasiert nach Eingangszeit) wählen:

- **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**

Da die Hintergrundprüfung das System belastet (nach jedem Update der Signaturdatenbank findet eine Prüfung statt), sollten die Prüfungen 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.

Wenn Sie die Option **E-Mail-Inhalt prüfen (Format Rich-Text)** aktivieren, werden RTF-Nachrichtentexte geprüft. E-Mail-Texte im Format Rich-Text können Makroviren enthalten.

HINWEIS: E-Mail-Inhalte im Format Nur-Text werden nicht mit VSAPI geprüft.

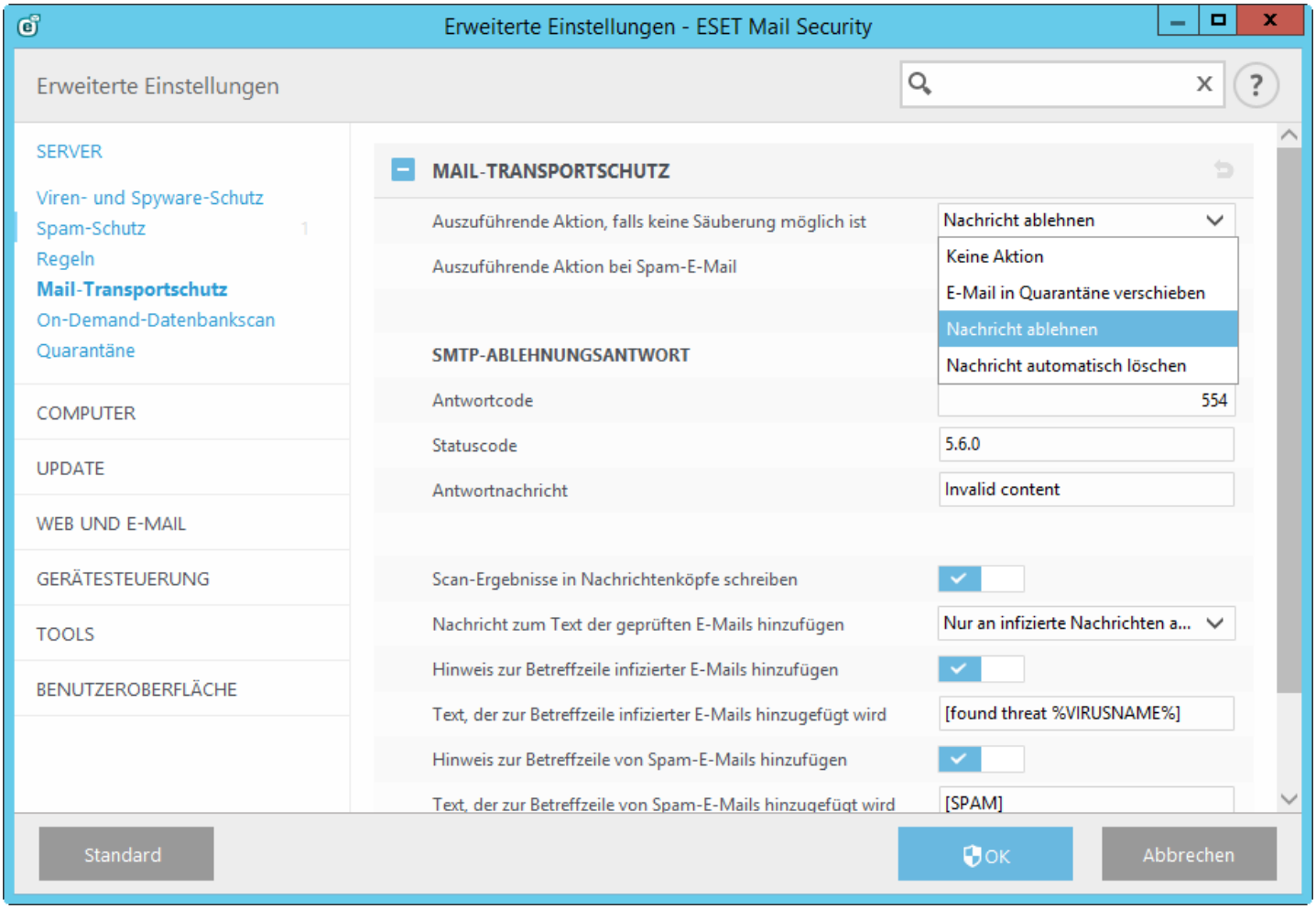
HINWEIS: Öffentliche Ordner werden auf dieselbe Weise verarbeitet wie Postfächer. Dies bedeutet, dass öffentliche Ordner ebenfalls geprüft werden.

5.1.7 Mail-Transportschutz

Unter den folgenden Betriebssystemen ist der **E-Mail-Transportschutz** verfügbar unter **Erweiterte Einstellungen** > **Server**:

- Microsoft Exchange Server 2007 (Edge-Transportserver oder Hub-Transportserver)
- Microsoft Exchange Server 2007 (Installation auf einzelnem Server mit mehreren Rollen)
- Microsoft Exchange Server 2010 (Edge-Transportserver oder Hub-Transportserver)
- Microsoft Exchange Server 2010 (Installation auf einzelnem Server mit mehreren Rollen)
- Microsoft Exchange Server 2013 (Edge-Transportserverrolle)
- Microsoft Exchange Server 2013 (Installation auf einzelnem Server mit mehreren Rollen)
- Windows Small Business Server 2008
- Windows Small Business Server 2011

Einstellungen für den E-Mail-Transportschutz:



Die Virenschutzaktion auf der Transportebene kann unter **Aktion, wenn Säubern nicht möglich ist** festgelegt werden:

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

Die Spamschutzaktion auf der Transportebene kann unter **Aktion für Spam-Mails** festgelegt werden:

- **Keine Aktion** - Erhält die Nachricht, auch wenn sie als Spam eingestuft ist
- **Nachricht in Quarantäne verschieben –** Als Spam eingestufte E-Mails werden in das Quarantäne-Postfach verschoben
- **Nachricht ablehnen –** Als Spam eingestufte E-Mails werden abgelehnt
- **Nachricht automatisch löschen** - E-Mails werden ohne Unzustellbarkeitsbericht gelöscht

SMTP Reject-Nachricht - 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

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

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`).

Nachricht zum Text der geprüften E-Mails hinzufügen bietet drei Optionen:
- Nicht an Nachrichten anhängen
- Nur an infizierte Nachrichten anhängen
- An alle geprüften Nachrichten anhängen (gilt nicht für interne Nachrichten)

Hinweis zur Betreffzeile infizierter E-Mails hinzufügen - mit dieser Option hängt <%PN%> einen Prüfhinweis 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 kann die automatische Filterung infizierter E-Mails 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.

Hinweis zur Betreffzeile von Spam-E-Mails hinzufügen - mit dieser Option hängt <%PN%> einen Prüfhinweis 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.

HINWEIS: Im Hinweistext für den Betreff können auch Systemvariablen verwendet werden.

5.1.7.1 Erweiterte Einstellungen

In diesem Bereich können Sie erweiterte Einstellungen für den Transport-Agenten festlegen:

- **Auch Nachrichten prüfen, die über authentifizierte oder interne Verbindungen eingehen** – Sie können auswählen, wie Nachrichten, die authentifizierten Quellen oder lokalen Server empfangen werden, gescannt werden sollen. Das Scannen dieser Nachrichten wird empfohlen, da es den Schutz verbessert, und ist erforderlich, wenn Sie einen integrierten Microsoft SBS POP3-Connector zum Abrufen von Nachrichten von externen POP3-Servern oder E-Mail-Diensten (wie **Gmail.com**, **Outlook.com**, **Yahoo.com** oder **gmx.de**) nutzen. Weitere Informationen finden Sie unter POP3-Connector und Spam-Schutz.

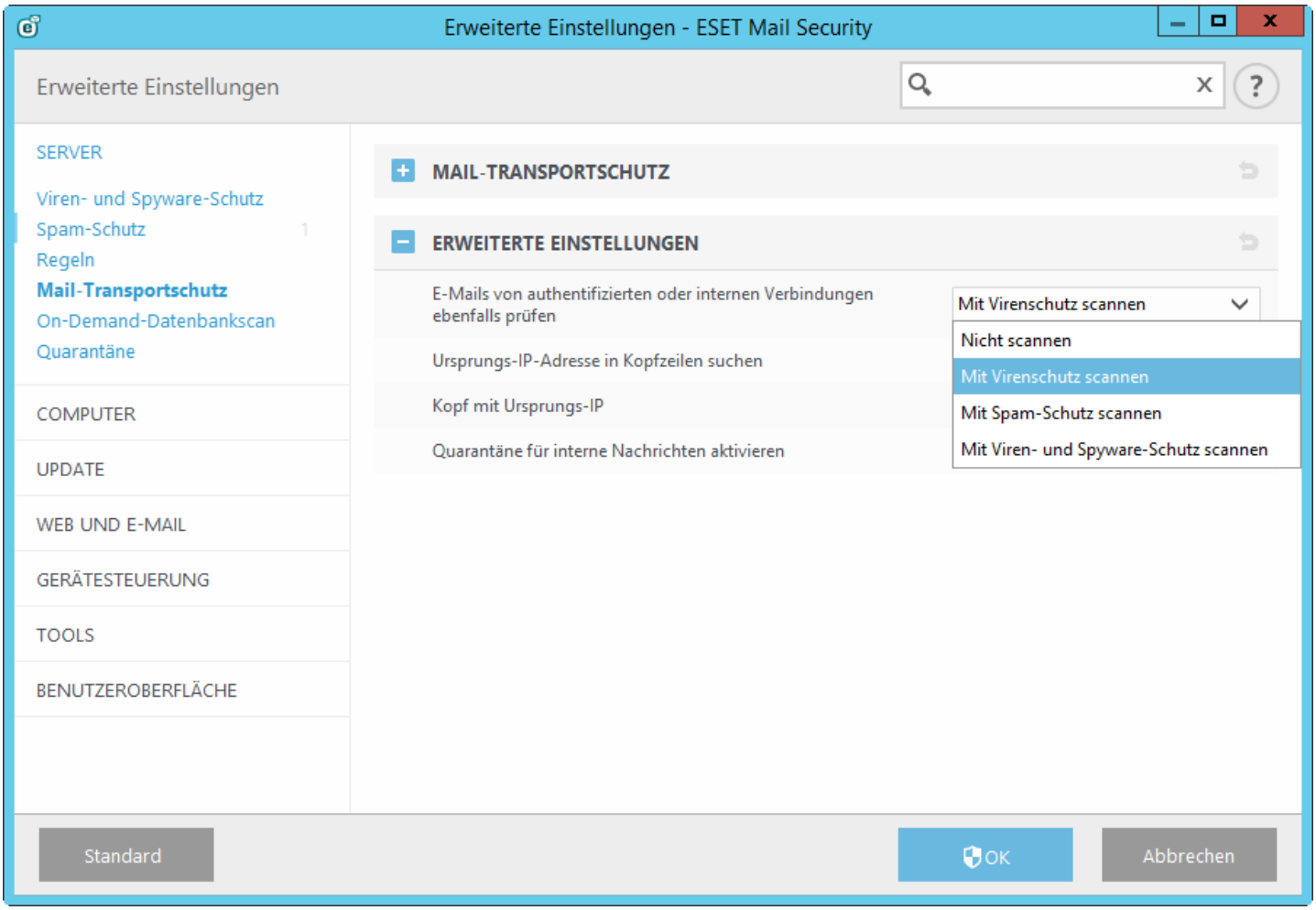
HINWEIS: Interne Outlook-E-Mails innerhalb der Organisation werden im TNEF-Format verschickt (Transport Neutral Encapsulation Format). Das TNEF-Format wird vom Spam-Schutz nicht unterstützt. Daher werden interne E-Mails im TNEF-Format nicht auf Spam geprüft, selbst wenn eine der Optionen **Mit Spam-Schutz scannen** oder **Mit Viren- und Spyware-Schutz scannen** aktiviert ist.

- **Ursprungs-IP-Adresse in Kopfzeilen suchen** – Wenn diese Option aktiviert ist, sucht ESET Mail Security im Nachrichten-Header nach der Ursprungs-IP-Adresse, damit die verschiedenen Schutzmodule (Spam-Schutz usw.) dies verwenden können. Falls Ihre Exchange-Organisation durch einen Proxyserver, ein Gateway oder eine Edge-Transportserver getrennt ist, sieht es so aus, als ob die E-Mail-Nachrichten von einer einzigen IP-Adresse (üblicherweise einer internen Adresse) empfangen werden. Üblicherweise wird auf dem außen liegenden Server (beispielsweise dem Edge-Transportserver in der DMZ), wo die IP-Adresse des Absenders bekannt ist, diese IP-Adresse in den Header der empfangen E-Mail-Nachricht geschrieben. ESET Mail Security sucht im Nachrichten-Header nach dem Wert, der im Feld **Kopf mit Ursprungs-IP** angegeben ist.

- **Kopf mit Ursprungs-IP** – Header, nach dem ESET Mail Security im Nachrichten-Header sucht. Der Standardwert ist **Ursprungs-IP**. Wenn Sie jedoch Tools von Drittanbietern oder benutzerdefinierte Tools verwenden, ändern Sie diesen Wert je nach Bedarf.

- **Quarantäne für interne Nachrichten aktivieren** – Wenn diese Option aktiviert ist, können interne Nachrichten in

die Quarantäne verschoben werden. Interne E-Mails müssen selten in die Quarantäne verschoben werden. Sie können diese Funktion jedoch bei Bedarf trotzdem aktivieren.



5.1.8 On-Demand-Datenbankprüfung

Die **On-Demand-Datenbankprüfung** ist auf den folgenden Systemen verfügbar:

- Microsoft Exchange Server 2007 (Postfachserver oder Hub-Transportserver)
- Microsoft Exchange Server 2007 (Installation auf einzelnem Server mit mehreren Rollen)
- Microsoft Exchange Server 2010 (Postfachserver oder Hub-Transportserver)
- Microsoft Exchange Server 2010 (Installation auf einzelnem Server mit mehreren Rollen)
- Microsoft Exchange Server 2013 (Postfachserverrolle)
- Microsoft Exchange Server 2013 (Installation auf einzelnem Server mit mehreren Rollen)
- Windows Small Business Server 2008
- Windows Small Business Server 2011

HINWEIS: Falls Sie Microsoft Exchange Server 2007 oder 2010 verwenden, können Sie zwischen Postfach-Datenbankschutz und On-Demand-Datenbankprüfung wählen. Es kann jedoch nur eine dieser beiden Schutzarten gleichzeitig aktiv sein. 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.

Einstellungen für On-Demand-Datenbankprüfung:

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 die Exchange-Webdienste hat.

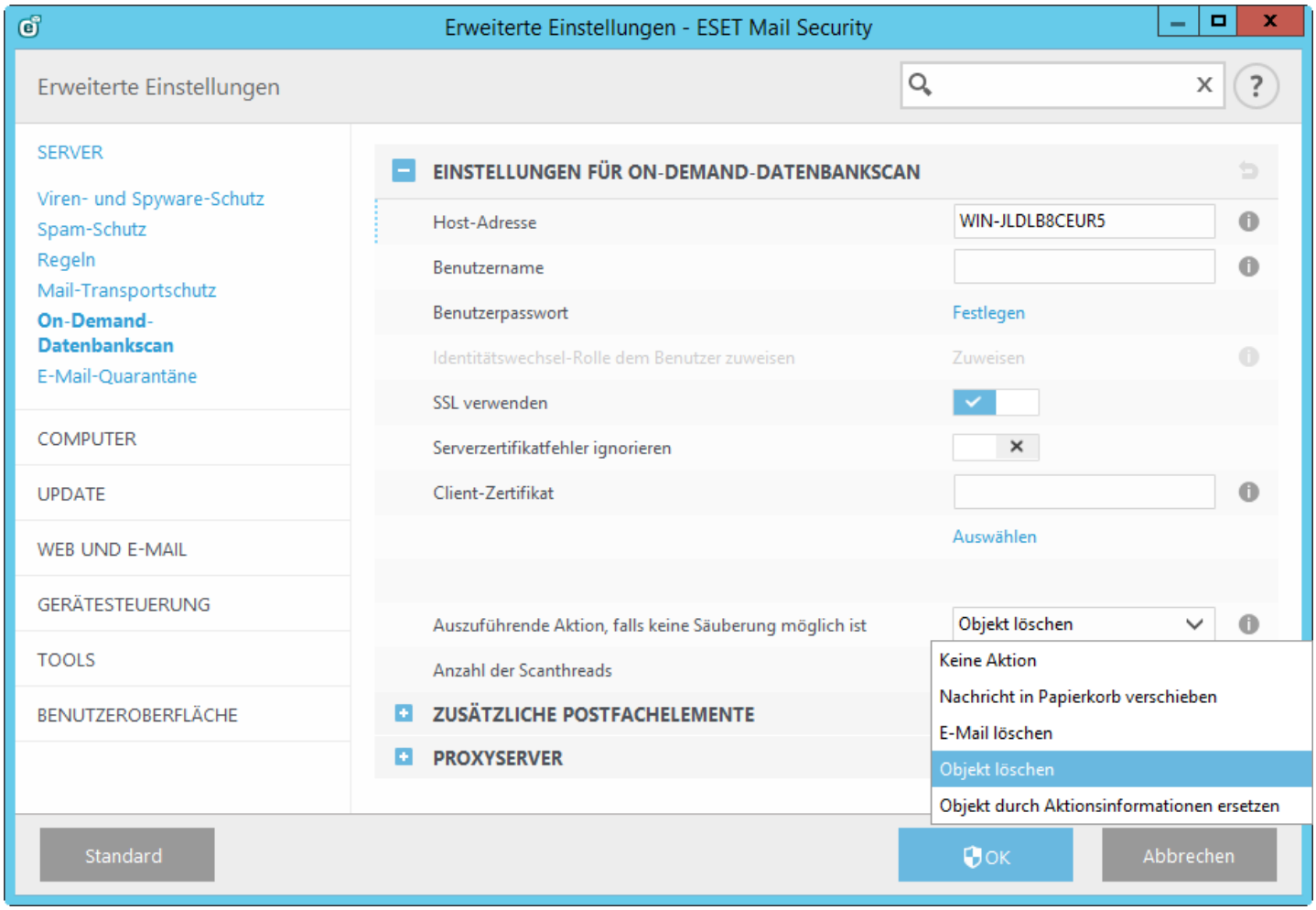
Benutzerpasswort - Klicken Sie auf **Festlegen** neben **Benutzerpasswort**, und geben Sie das Passwort für dieses Benutzerkonto ein.

ApplicationImpersonation-Rolle an Benutzer zuweisen - Wenn diese Option deaktiviert ist, müssen Sie zunächst den **Benutzernamen** angeben. Klicken Sie auf **Zuweisen**, um dem ausgewählten Benutzer automatisch die ApplicationImpersonation-Rolle zuzuweisen. Alternativ können Sie die Rolle ApplicationImpersonation manuell zuweisen. Details dazu finden Sie unter Details des Kontos für den Datenbank-Scan.

SSL verwenden - Diese Option muss aktiviert werden, wenn für die Exchange-Webdienste 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/Standardwebsite/EWS/SSL-Einstellungen*.

HINWEIS: Deaktivieren Sie die Option **SSL verwenden** nur, wenn die Exchange-Webdienste in IIS kein SSL verwenden.

Clientzertifikat - Muss nur festgelegt werden, wenn die Exchange-Webdienste Clientzertifikate verlangen. **Unter Auswählen** können Sie eines der Zertifikate auswählen.



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 - Wird für Elemente in öffentlichen Ordnern nicht unterstützt. Verwenden Sie stattdessen die Aktion **Objekt löschen**.
Objekt löschen - Der infizierte Inhalt der Nachricht wird gelöscht.
Nachricht löschen - Die gesamte Nachricht inklusive des infizierten Inhalts wird gelöscht.
Objekt durch Aktionsinformationen ersetzen - Entfernt ein Objekt und fügt Informationen zur für das Objekt ausgeführten Aktion hinzu.

5.1.8.1 Zusätzliche Postfachelemente

In den Einstellungen für On-Demand-Datenbankprüfung können Sie die Prüfung weiterer Postfachelemente aktivieren oder deaktivieren:

- Kalender scannen
- Aufgaben scannen
- Kontakte scannen
- Journal scannen

HINWEIS: Falls Leistungsprobleme auftreten, können Sie das Scannen dieser Elemente deaktivieren. Die Scans dauern länger, wenn diese Elemente aktiviert sind.

5.1.8.2 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 verbindet. Andernfalls ist die On-Demand-Datenbankprüfung nicht verfügbar.

Proxyserver - Geben Sie die IP-Adresse oder den Namen des Proxyservers ein.

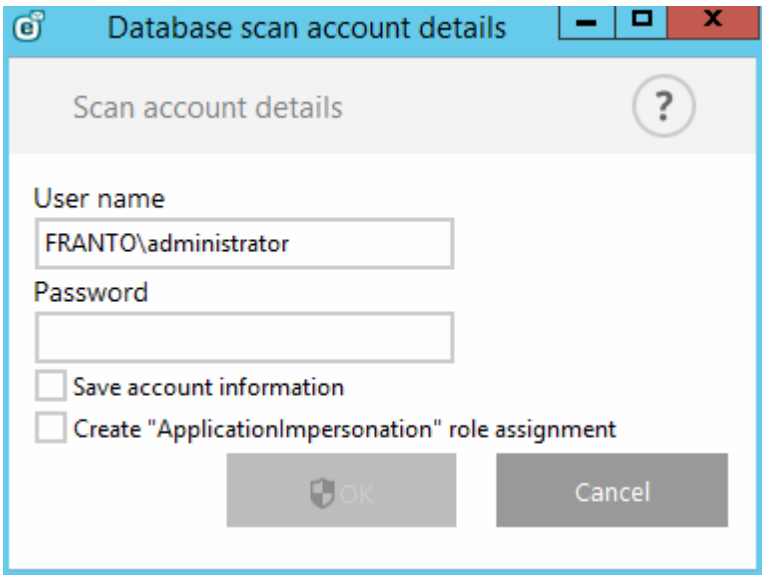
Port - Geben Sie die Portnummer des Proxyservers ein.

Benutzername, Passwort - Geben Sie die Anmeldeinformationen ein, falls Ihr Proxyserver Authentifizierung verwendet.

5.1.8.3 Details des Kontos für den Datenbank-Scan

Dieser Dialog wird angezeigt, wenn Sie keine Anmeldeinformationen für die **Datenbankprüfung** in den **erweiterten Einstellungen** eingegeben haben. Geben Sie die Anmeldeinformationen des Benutzers an, der Zugriff auf die Exchange-Webdienste (EWS, Exchange Web Services) in diesem Popupfenster ein und klicken Sie auf **OK**. Alternativ können Sie die **erweiterten Einstellungen** mit **F5** öffnen und zum Eintrag **Server** > On-Demand-Datenbankprüfung navigieren. Geben Sie Ihren **Benutzernamen** ein, klicken Sie auf **Festlegen**, geben Sie ein Passwort für das Benutzerkonto ein und klicken Sie auf OK.

- Sie können die **Kontoinformationen speichern**, um diese nicht bei jeder On-Demand-Datenbankprüfung erneut eingeben zu müssen.
- Falls ein Benutzerkonto keine ausreichenden Berechtigungen für EWS hat, können Sie **"ApplicationImpersonation" erstellen Rollenzuweisung** auswählen, um diese Rolle zu einem Konto zuzuweisen. Alternativ können Sie die Rolle ApplicationImpersonation manuell zuweisen. Details dazu finden Sie im folgenden Hinweis.



WICHTIGER HINWEIS: Das Prüfkonto benötigt die Berechtigung **ApplicationImpersonation**, um die

Benutzerpostfächer in Exchange-Postfachdatenbanken prüfen zu können. Für Exchange Server 2010 und neuere Versionen sollten Sie unbedingt eine Drosselungsrichtlinie für das Prüfkonto einrichten, um zu verhindern, dass ESET Mail Security zu viele Anfragen stellt. Andernfalls kann es passieren, dass für manche der Anfragen an Ihren Exchange Server eine Zeitüberschreitung auftritt.

HINWEIS: Sie können die folgenden Befehle verwenden, um die Rolle ApplicationImpersonation manuell zu einem Benutzerkonto zuzuweisen (ersetzen Sie `ESET-user` durch einen Kontonamen in Ihrem System):

Exchange Server 2007

```
Get-ClientAccessServer | Add-AdPermission -User ESET-user -ExtendedRights ms-Exch-EPI-Impersonation
```

```
Get-MailboxDatabase | Add-AdPermission -User ESET-user -ExtendedRights ms-Exch-EPI-May-Impersonate
```

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 -EWSFastSearchTimeoutInSeco
```

```
Set-ThrottlingPolicyAssociation -Identity user-ESET -ThrottlingPolicy ESET-ThrottlingPolicy
```

Exchange Server 2013

```
New-ManagementRoleAssignment -Name:ESET-ApplicationImpersonation -Role:ApplicationImpersonation
-User:ESET-user
```

Dieser Vorgang kann einige Zeit in Anspruch nehmen

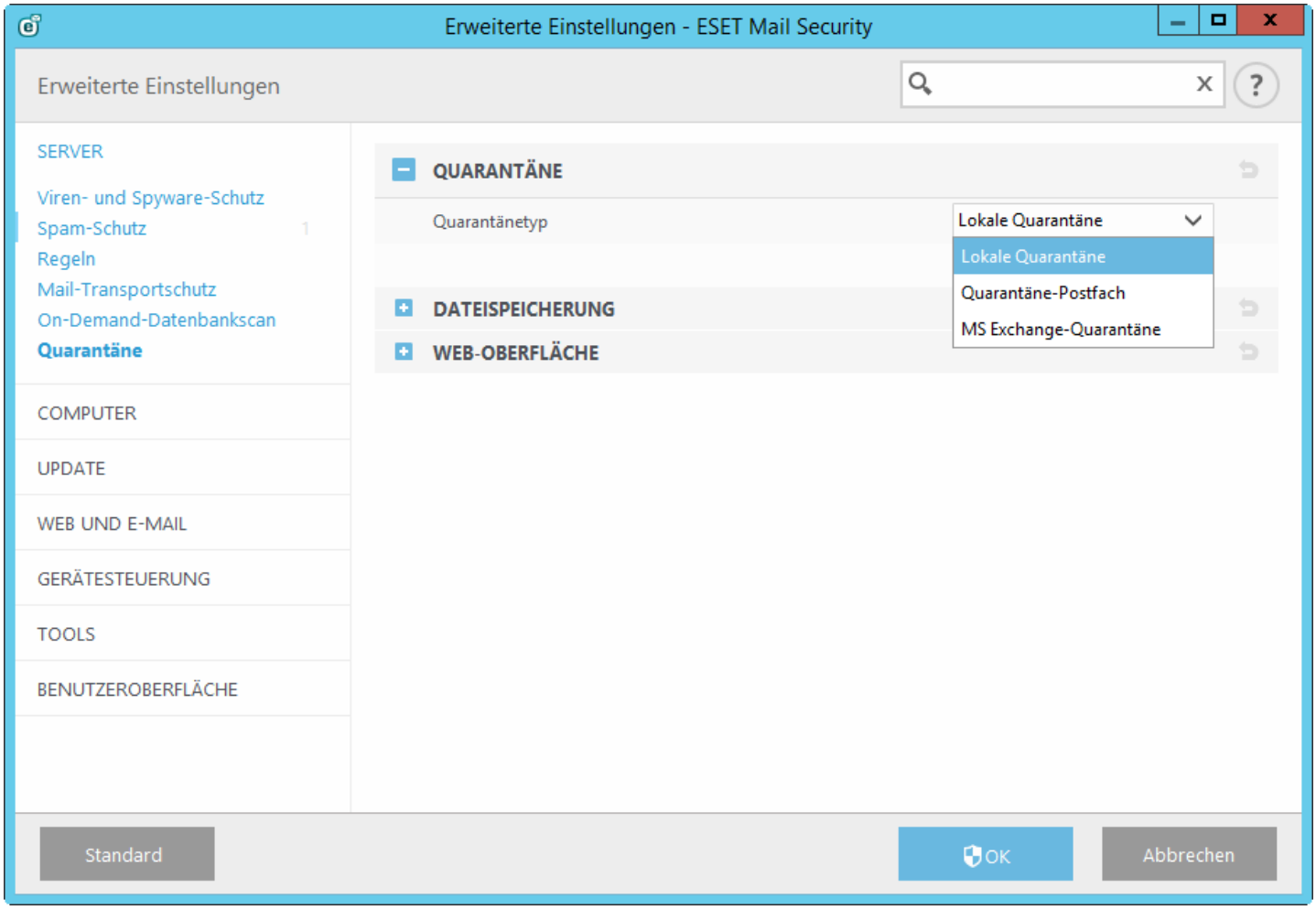
```
New-ThrottlingPolicy -Name ESET-ThrottlingPolicy -EWSMaxConcurrency Unlimited -EwsCutoffBalance Unlim
```

```
Set-ThrottlingPolicyAssociation -Identity ESET-user -ThrottlingPolicy ESET-ThrottlingPolicy
```

5.1.9 E-Mail-Quarantäne

Der E-Mail-Quarantäne-Manager ist für alle drei Quarantänetypen verfügbar:

- Lokale Quarantäne
- Quarantäne-Postfach
- MS Exchange-Quarantäne



Im E-Mail-Quarantäne-Manager können Sie den Inhalt der E-Mail-Quarantäne für alle Quarantänetypen anzeigen. Die lokale Quarantäne kann außerdem in der Web-Oberfläche für die E-Mail-Quarantäne angezeigt werden.

5.1.9.1 Lokale Quarantäne

Die lokale Quarantäne verwendet das lokale Dateisystem als Speicher für die E-Mail-Quarantäne und eine SQLite-Datenbank als Index. Die in der Quarantäne gespeicherten E-Mail-Dateien und die Datenbankdatei werden aus Sicherheitsgründen verschlüsselt. Diese Dateien befinden sich unter `C:\ProgramData\ESET\ESET Mail Security\MailQuarantine` (Windows Server 2008 und 2012) oder unter `C:\Documents and Settings\All Users\Application Data\ESET\ESET Mail Security\MailQuarantine` (Windows Server 2003).

HINWEIS: Wenn Sie die Quarantänedateien auf einem anderen Datenträger als dem normalen `C:`-Laufwerk speichern möchten, müssen Sie den **Datenordner** bei der Installation von ESET Mail Security auf den gewünschten Ordner festlegen.

Merkmale der lokalen Quarantäne:

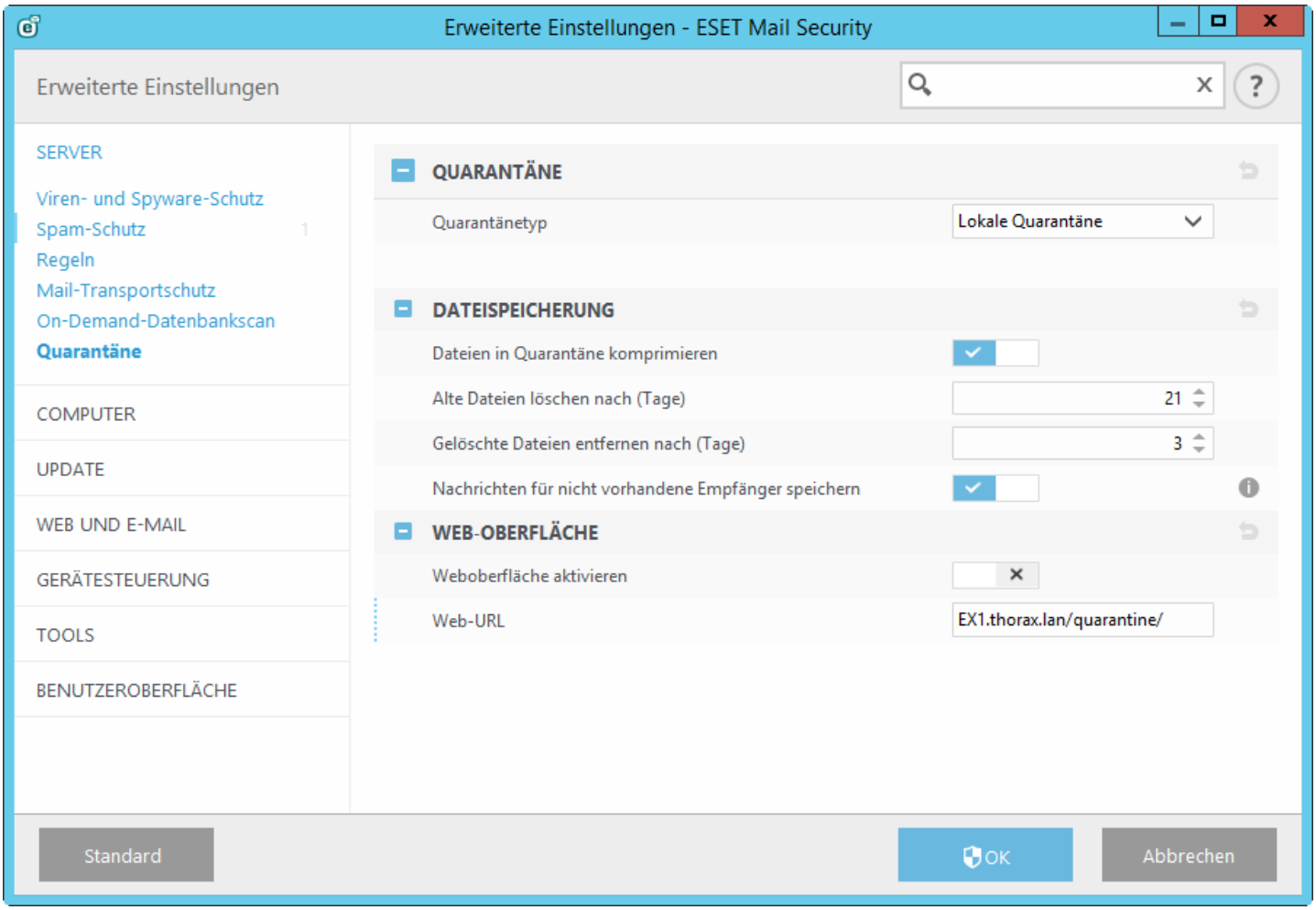
- SPAM- und Quarantäne-E-Mails werden im lokalen Dateisystem gespeichert und sind daher nicht in der Exchange-Postfachdatenbank enthalten.
- Lokal gespeicherte E-Mail-Dateien in der Quarantäne werden verschlüsselt und komprimiert.
- Web-Oberfläche für die E-Mail-Quarantäne als webbasierte Alternative zum E-Mail-Quarantäne-Manager.
- Quarantäneberichte können mit einem geplanten Task an eine angegebene E-Mail-Adresse geschickt werden.
- Die aus demQuarantänefenster entfernten E-Mail-Dateien (standardmäßig nach 21 Tagen) bleiben im Dateisystem erhalten (bis zur automatischen Löschung nach einer festgelegten Anzahl von Tagen)
- Automatische Löschung alter E-Mail-Dateien (standardmäßig nach 3 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).

HINWEIS: Mit der lokalen Quarantäne haben Sie den Nachteil, dass Sie die lokale Quarantäne unterschiedlicher Server einzeln verwalten müssen, falls Sie mehrere ESET Mail Security-Server mit der Hub-Transport-Serverrolle betreiben. Je mehr Server Sie betreiben, desto mehr Quarantäneorder müssen Sie verwalten.

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 entweder mit dem E-Mail-Quarantäne-Manager in der Hauptanwendung oder mit der Web-Oberfläche für die E-Mail-Quarantäne verwalten.

5.1.9.1.1 Dateispeicherung

In diesem Bereich können Sie Einstellungen für den Dateispeicher vornehmen, den die lokale Quarantäne verwendet.



Dateien in Quarantäne komprimieren - Die Dateien in der Quarantäne werden komprimiert, um Speicherplatz zu sparen. Deaktivieren Sie den Schalter, um die Komprimierung zu deaktivieren.

Alte Dateien löschen nach (Tage) - Dateien werden nach einer bestimmten Anzahl von Tagen aus dem Quarantänefenster entfernt. Die Dateien werden jedoch erst nach Ablauf der unter **Gelöschte Dateien entfernen**

nach (Tage) angegebenen Zeitdauer von der Festplatte gelöscht. Die Dateien werden nicht aus dem Dateisystem gelöscht und können z. B. mit eShell wiederhergestellt werden.

Gelöschte Dateien entfernen nach (Tage) - Dateien werden nach einer bestimmten Anzahl von Tagen von der Festplatte gelöscht und können nicht wiederhergestellt werden (es sei denn, Sie verwenden eine Sicherungslösung).

Nachrichten für nicht vorhandene Empfänger speichern - Spam-E-Mails werden oft an unbekannte Empfänger für bestimmte Domänen verschickt in der Hoffnung, dass diese zugestellt werden. E-Mails an unbekannte Benutzer im Aktive Directory werden standardmäßig in der lokalen Quarantäne gespeichert. Sie können diese Option deaktivieren, um Nachrichten an unbekannte Empfänger nicht zu speichern und zu verhindern, dass Ihre lokale Quarantäne mit Spam-E-Mails dieser Art überläuft. Außerdem sparen Sie auf diese Weise Speicherplatz.

5.1.9.1.2 Web-Oberfläche

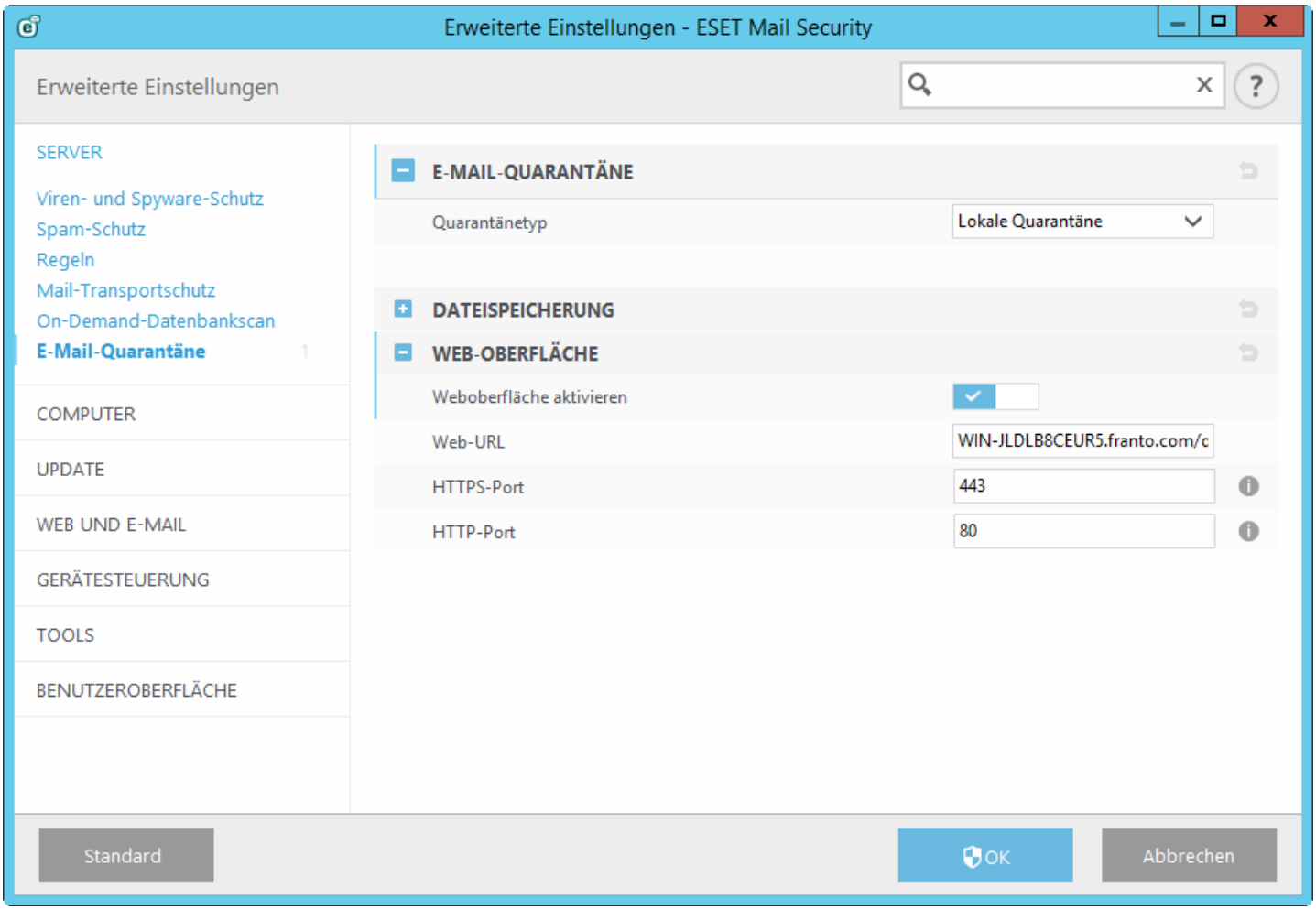
Die Web-Oberfläche für die E-Mail-Quarantäne ist eine Alternative zum E-Mail-Quarantäne-Manager, ist jedoch nur für die lokale Quarantäne verfügbar.

HINWEIS: Die Web-Oberfläche für die E-Mail-Quarantäne ist auf Servern mit der Rolle „Edge-Transportserver“ nicht verfügbar. Dies liegt daran, dass hier kein Zugriff auf Active Directory für die Authentifizierung möglich ist.

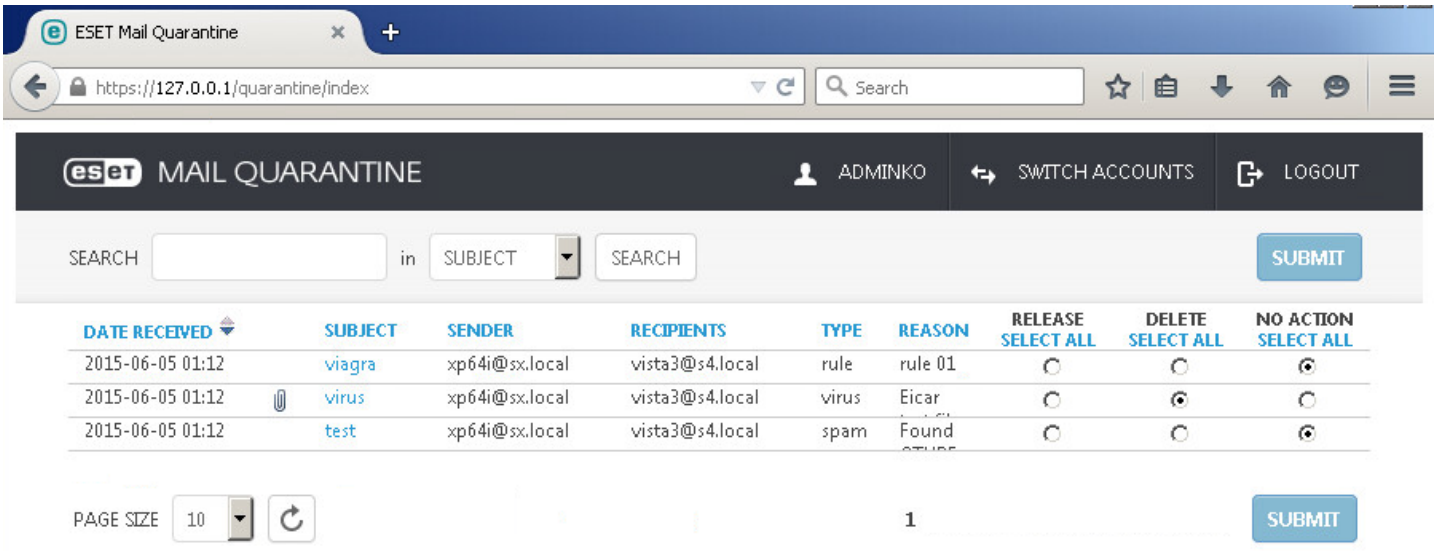
In der Web-Oberfläche für die E-Mail-Quarantäne können Sie den Status der E-Mail-Quarantäne abrufen. Außerdem können Sie die E-Mail-Objekte in der Quarantäne verwalten. Sie erreichen diese Web-Oberfläche über Links in den Quarantäne-Berichten, oder indem Sie die URL direkt in Ihren Webbrowser eingeben. Sie müssen sich mit Domänenanmeldeinformationen anmelden, um die Web-Oberfläche für die E-Mail-Quarantäne zu öffnen. Internet Explorer authentifiziert Domänenbenutzer automatisch. Dafür muss die Webseite ein gültiges Zertifikat enthalten, die automatische Anmeldung muss in IE aktiviert sein, und Sie müssen die Web-Oberfläche für die E-Mail-Quarantäne zu den lokalen Intranet-Sites hinzufügen.

Mit dem Schalter **Web-Oberfläche aktivieren** können Sie die Web-Oberfläche aktivieren bzw. deaktivieren.

Web-URL - Unter dieser URL ist die Web-Oberfläche für die E-Mail-Quarantäne erreichbar. Standardmäßig ist dies der FQDN des Servers mit `/quarantine` (z. B. `mailserver.company.com/quarantine`).
HTTPS-Port - Der Standardport ist 443. Sie können die Portnummer bei Bedarf ändern.
HTTP-Port - Der Standardport ist 80. Sie können die Portnummer bei Bedarf ändern.

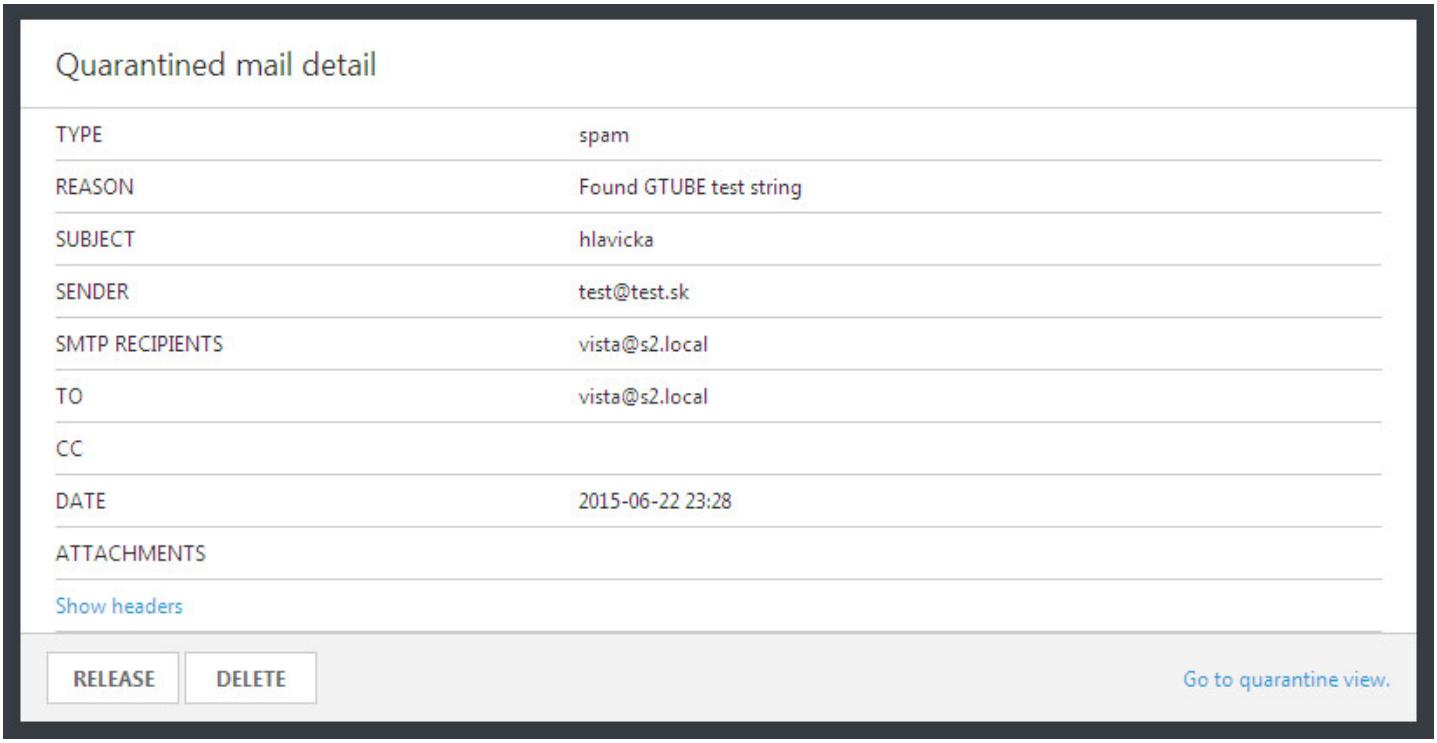


Um die Web-Oberfläche der E-Mail-Quarantäne zu erreichen, öffnen Sie Ihren Webbrowser und verwenden Sie die URL, die unter **Erweiterte Einstellungen** > **Server** > **E-Mail-Quarantäne** > **Web-Oberfläche** > **Web-URL** festgelegt wurde.

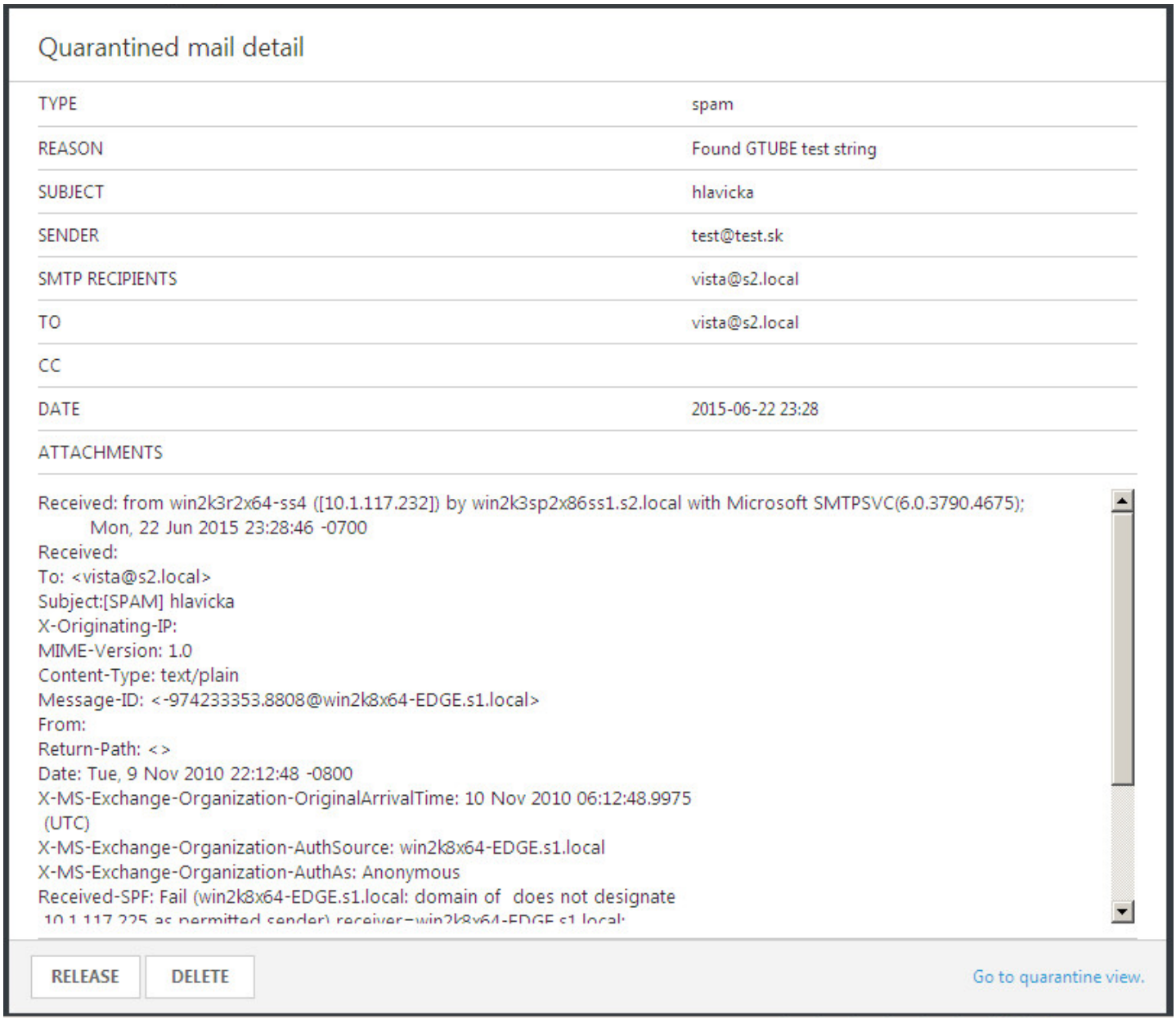


Freigeben - Gibt die E-Mail über das Replay-Verzeichnis an den bzw. die Originalempfänger frei, und löscht sie aus der Quarantäne. Klicken Sie auf **Senden**, um den Vorgang zu bestätigen.
Löschen - Löscht ein Element aus der Quarantäne. Klicken Sie auf **Senden**, um den Vorgang zu bestätigen.

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 E-Mail zu öffnen.



Klicken Sie ggf. auf **Freigeben** oder auf **Löschen**, um die entsprechende Aktion für die E-Mail in der Quarantäne auszuführen.

HINWEIS: 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.

WICHTIGER HINWEIS: 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.

5.1.9.2 Quarantäne-Postfach und MS 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 Postfach anlegen (zum Beispiel quarantäne@firma.de), das anschließend für die Speicherung der E-Mails in Quarantäne verwendet wird. Der E-Mail-Quarantäne-Manager verwendet diesen Benutzer, um die Elemente in der Quarantäne anzuzeigen und zu verwalten. Geben Sie die Anmeldeinformationen dieses Benutzers in den Einstellungen für den Quarantäne-Manager an.

WICHTIGER HINWEIS: Das Administrator-Benutzerkonto sollte nicht als Quarantäne-Postfach verwendet werden.

HINWEIS: **MS Exchange-Quarantäne** ist nicht für Microsoft Exchange 2003 verfügbar, nur **lokale Quarantäne** und **Quarantäne-Postfach**.

- Wenn Sie **MS Exchange-Quarantäne** auswählen, verwendet ESET Mail Security das **Microsoft Exchange-Quarantänesystem** (gilt ab Microsoft Exchange Server 2007). Eine interne Funktion des Servers speichert dabei potenziell infizierte Nachrichten und Spam.

HINWEIS: Die interne Quarantäne ist in Exchange standardmäßig deaktiviert. Führen Sie den folgenden Befehl in der Exchange-Verwaltungsshell aus, um die Funktion zu aktivieren (ersetzen Sie `name@domain.com` durch die tatsächliche Adresse Ihres Quarantäne-Postfachs):

```
Set-ContentFilterConfig -QuarantineMailbox name@domain.com
```

- Wenn Sie **Quarantäne-Postfach** auswählen, müssen Sie die Adresse des Quarantäne-Postfachs angeben (z. B. quarantäne@firma.de).

HINWEIS: Quarantäne-Postfach und MS 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. Quarantäne-Postfach und MS Exchange-Quarantäne haben jedoch auch einen Nachteil: Spam- und Quarantäne-E-Mails werden in Exchange-Postfachdatenbanken gespeichert und können nur von Administratoren verwaltet werden.

5.1.9.2.1 Einstellungen für Quarantäne-Manager

Host-Adresse - Wird automatisch ausgefüllt, wenn Ihr Exchange Server mit CAS-Rolle lokal vorhanden ist. Falls sich die CAS-Rolle nicht auf demselben Server wie ESET Mail Security befindet, diese jedoch im AD auffindbar ist, wird die Host-Adresse ebenfalls automatisch ausgefüllt. Falls kein Wert angezeigt wird, können Sie den Hostnamen manuell eingeben. Die automatische Erkennung funktioniert nicht für die Edge-Transportserverrolle.

HINWEIS: IP-Adressen werden nicht unterstützt. Sie müssen den Hostnamen des CAS-Servers verwenden.

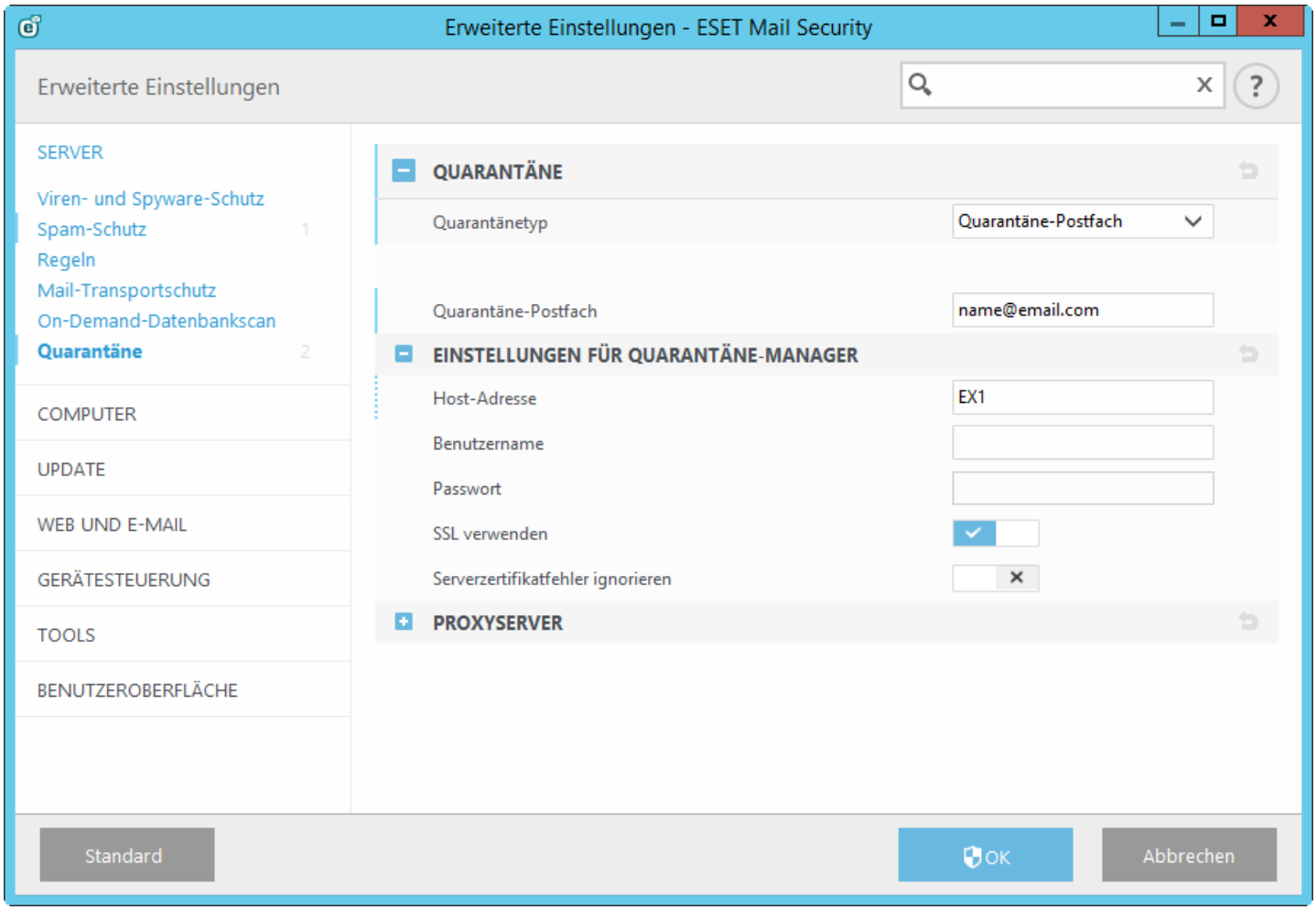
Benutzername - Ein speziell eingerichtetes Quarantäne-Benutzerkonto, das Sie für die Speicherung der E-Mails in Quarantäne angelegt haben (bzw. ein Benutzerkonto, das per Zugriffsdelegierung Zugriff auf dieses Postfach hat). Für Edge-Transportserverrollen, die sich nicht in derselben Domäne befinden, müssen Sie die komplette E-Mail-Adresse angeben (z. B. quarantäne@firma.de).

Passwort - Geben Sie das Passwort für Ihr Quarantänekonto ein.

SSL verwenden - Diese Option muss aktiviert werden, wenn für die Exchange-Webdienste 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/Standardwebsite/EWS/SSL-Einstellungen*.

HINWEIS: Deaktivieren Sie die Option **SSL verwenden** nur, wenn die Exchange-Webdienste in IIS kein SSL verwenden.

Serverzertifikatfehler ignorieren – Folgende Status werden ignoriert: eigensigniert, falscher Name im Zertifikat, falsche Verwendung, abgelaufen.



5.1.9.2.2 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 verbindet. Andernfalls funktionieren die Postfach-Quarantäne und die MS Exchange-Quarantäne nicht.

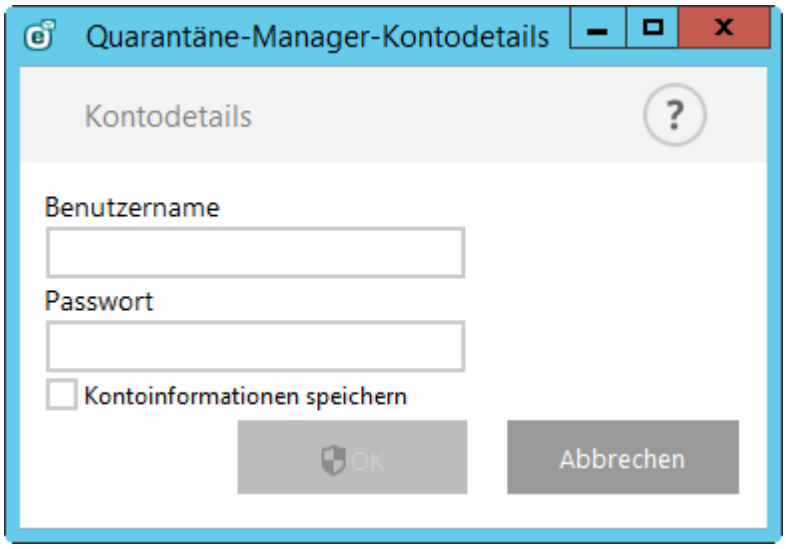
Proxyserver - Geben Sie die IP-Adresse oder den Namen des Proxyservers ein.

Port - Geben Sie die Portnummer des Proxyservers ein.

Benutzername, Passwort - Geben Sie die Anmeldeinformationen ein, falls Ihr Proxyserver Authentifizierung verwendet.

5.1.9.3 Quarantäne-Manager-Kontodetails

Dieser Dialog wird angezeigt, wenn Sie kein Konto unter **Quarantäne-Manager-Kontodetails** eingerichtet 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 bei zukünftigen Zugriffen auf den Quarantäne-Manager nicht erneut eingeben zu müssen.

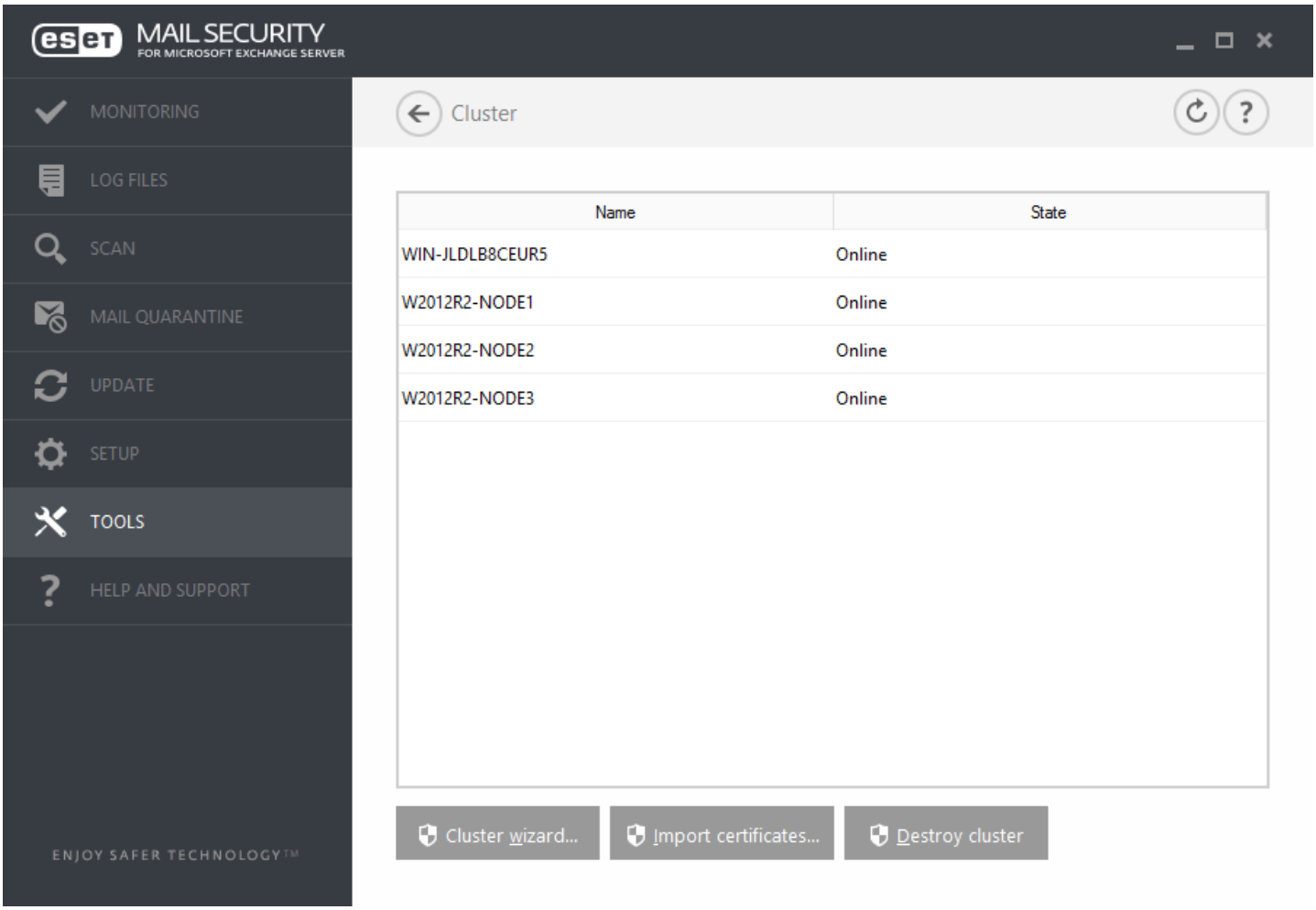
5.1.10 Cluster

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

Mit dieser Infrastruktur können ESET-Serverprodukte miteinander kommunizieren, Daten wie Konfigurationsdaten und Benachrichtigungen austauschen 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 die gleiche Konfiguration aufweisen muss. ESET-Cluster gewährleistet diese erforderliche Konsistenz der Instanzen.

HINWEIS: Die Einstellungen für die Benutzeroberfläche werden nicht zwischen ESET-Clusterknoten synchronisiert.

Die Statusseite für ESET-Cluster finden Sie im Hauptmenü unter **Tools** > **Cluster**. Richtig konfiguriert sieht die Statusseite folgendermaßen aus:



Klicken Sie auf **Clusterassistent, um den ESET-Cluster einzurichten.** Ausführliche Informationen zum Einrichten des ESET-Cluster mithilfe des Assistenten finden Sie hier.

Beim Einrichten des ESET-Cluster stehen zwei Methoden zum Hinzufügen von Knoten zur Verfügung: automatisch über einen vorhandenen Windows-Failover-Cluster/NLB-Cluster oder manuell durch Suchen nach Computern in einer Arbeitsgruppe oder Domäne.

Autom. erkennen - ermöglicht das automatische Erkennen von Knoten, die bereits Mitglied eines Windows-Failover-Cluster/NLB-Cluster sind, und fügt diese zum ESET-Cluster hinzu
Durchsuchen - Sie können Knoten manuell durch Eingeben der Servernamen hinzufügen (entweder Mitglieder der gleichen Arbeitsgruppe oder der gleichen Domäne)

HINWEIS: Zur Verwendung der ESET-Clusterfunktion müssen die Server nicht Mitglied eines Windows-Failover-Clusters/NLB-Clusters sein. Zur Verwendung von ESET-Clustern ist in Ihrer Umgebung kein Windows-Failover-Cluster oder NLB-Cluster erforderlich.

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.

HINWEIS: Domänenknoten und Arbeitsgruppenknoten können nicht kombiniert werden.

Eine weitere Anforderung für die Verwendung eines ESET-Clusters ist, dass die **Datei- und Druckerfreigabe** in der Windows-Firewall aktiviert werden muss, bevor die ESET Mail Security-Installation auf den ESET-Knoten ausgeführt wird.

Der ESET-Cluster kann ganz einfach durch Klicken auf **Cluster zerstören** zerlegt werden. Jeder Knoten schreibt einen Eintrag in den eigenen Ereignis-Log, der auf die Zerstörung des ESET-Cluster hinweist. Anschließend werden alle ESET-Firewall-Regeln von der Windows-Firewall entfernt. Die früheren Knoten werden daraufhin in ihren vorigen Zustand zurückversetzt und können je nach Bedarf erneut in einem anderen ESET-Cluster verwendet werden.

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

Sie können jederzeit neue Knoten zu einem vorhandenen ESET-Cluster hinzufügen. Führen Sie dazu den **Clusterassistenten** wie weiter oben und hier beschrieben aus.

Weitere Informationen zur Konfiguration von ESET-Clustern finden Sie im Abschnitt Arbeits-Cluster.

5.1.10.1 Clusterassistent – Seite 1

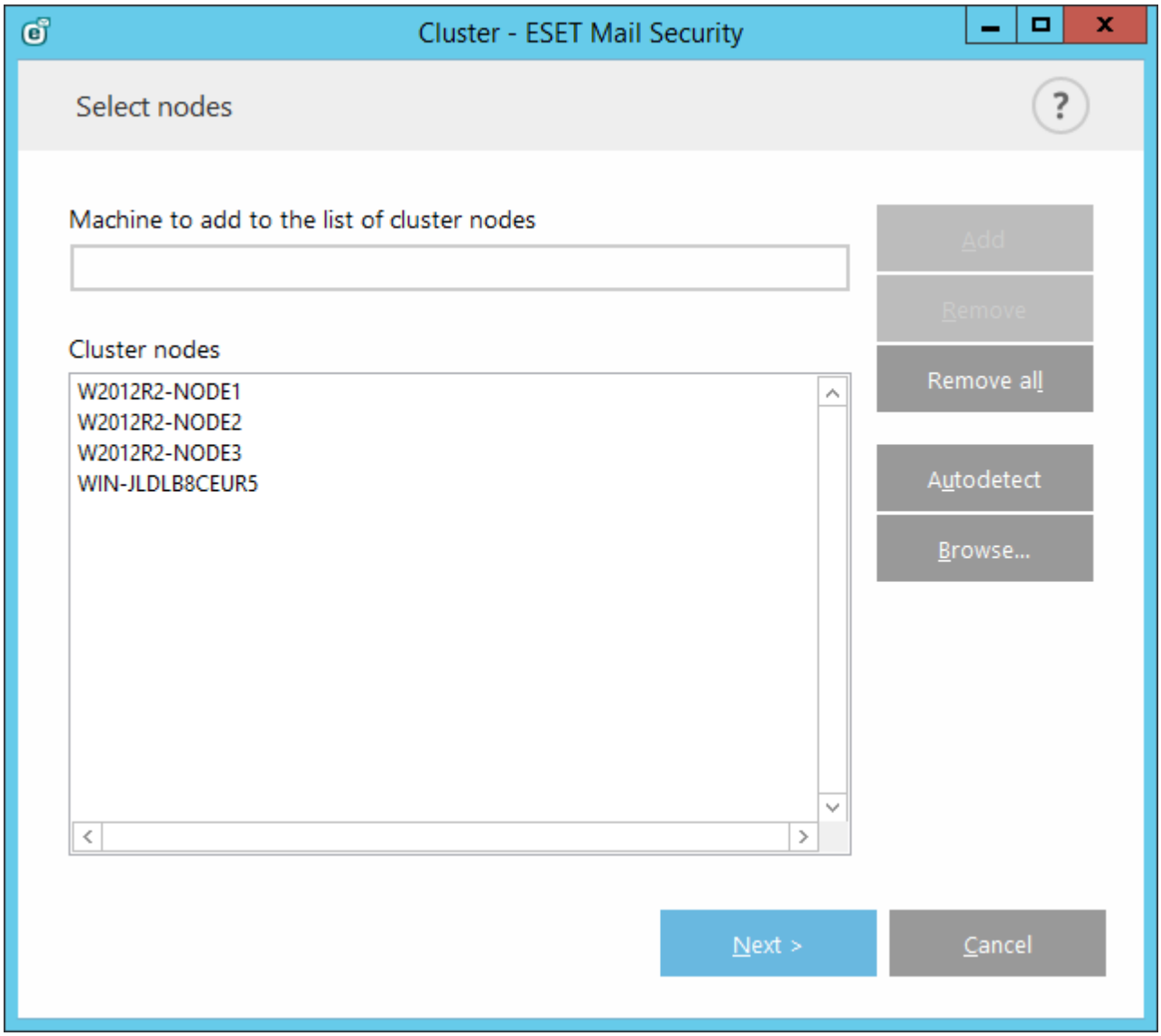
Der erste Schritt zur Einrichtung eines ESET-Clusters ist das Hinzufügen von Knoten. Verwenden Sie entweder die Option **Automatisch erkennen** oder fügen Sie die Knoten über die Funktion **Durchsuchen** manuell hinzu. Alternativ können Sie den Servernamen in das Textfeld eingeben und auf **Hinzufügen**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

Über **Automatisch ermitteln** werden Knoten eines vorhandenen Windows-Failover-Clusters/Network Load Balancing(NLB)-Clusters automatisch hinzugefügt. Der Server, über den Sie den ESET-Cluster erstellen möchten, muss Mitglied eines Windows-Failover-Clusters/NLB-Clusters sein, damit die Knoten automatisch hinzugefügt werden. Auf dem NLB-Cluster muss in den Clustereigenschaften die Option **Remotesteuerung zulassen** aktiviert sein, damit der ESET-Cluster die Knoten richtig erkennt. Nachdem die Liste der neu hinzugefügten Knoten erstellt wurde, können Sie nicht gewünschte Knoten entfernen, falls Sie nur bestimmte Knoten in den ESET-Cluster aufnehmen möchten.

Klicken Sie auf Durchsuchen, um Computer innerhalb einer Domäne oder Arbeitsgruppe 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**.

Aktuelle **Clusterknoten**, die nach dem Klicken auf **Weiter** zum ESET-Cluster hinzugefügt werden:



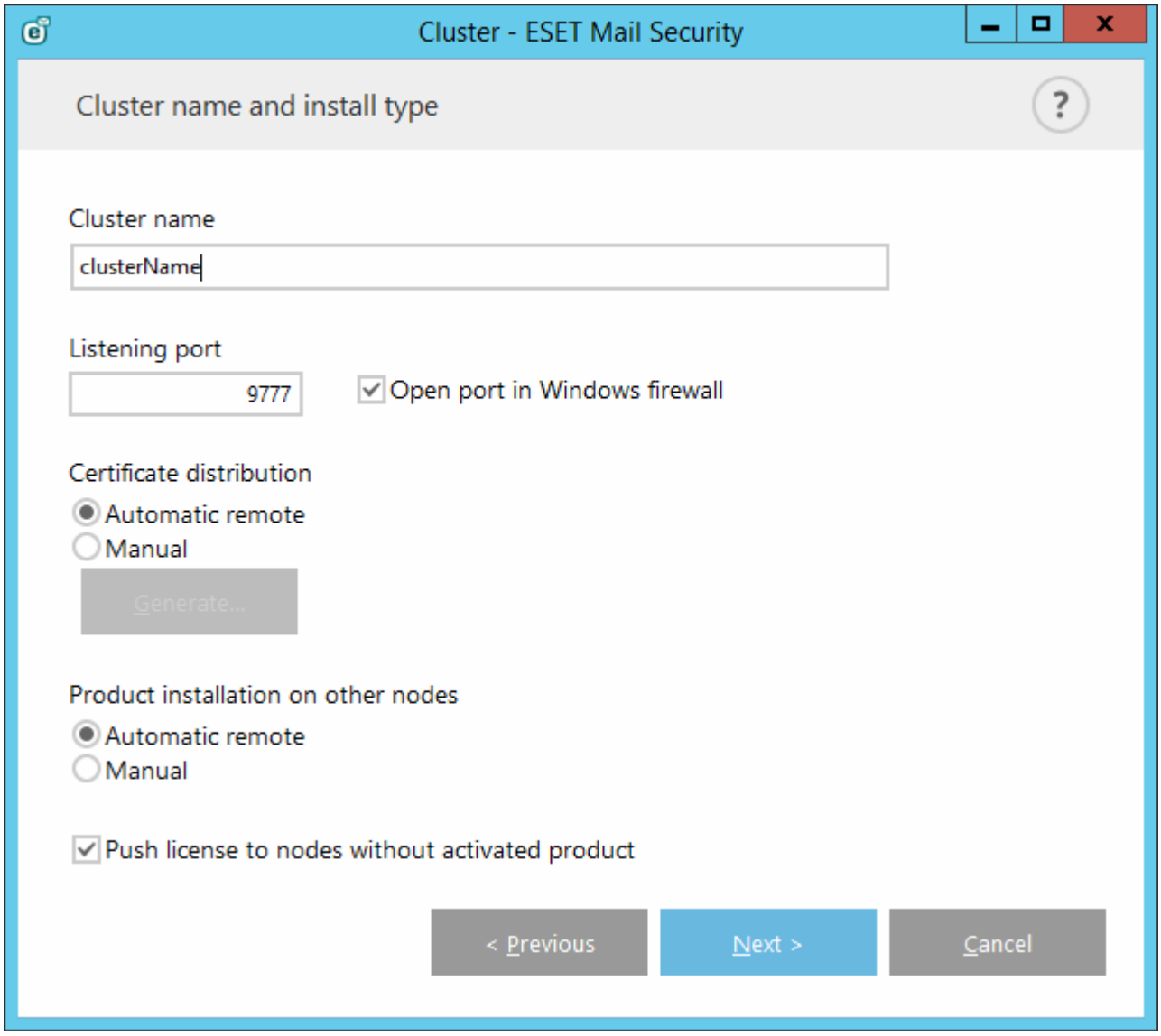
Um **Clusterknoten** in der Liste zu ändern, wählen Sie einen zu entfernenden Knoten aus und klicken Sie auf **Entfernen**. Klicken Sie alternativ auf **Alle entfernen**, um die Liste vollständig zu löschen.

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

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

5.1.10.2 Clusterassistent – Seite 2

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



Clustername - Geben Sie den Clusternamen ein.
Listening Port - (Der Standardport ist 9777.)
Port in Windows-Firewall öffnen - Wenn diese Option aktiviert ist, wird in der Windows-Firewall eine Regel erstellt.

Zertifikatverteilung:
Automatisch remote - Das Zertifikat wird automatisch installiert.
Manuell - Wenn Sie auf **Erstellen** klicken, wird ein Fenster zum Durchsuchen geöffnet. 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 die Einrichtung des ESET-Cluster ausführen. Anschließend können Sie das Zertifikat auf dem lokalen Computer registrieren, indem Sie auf **Ja** klicken. Später müssen Sie die Zertifikate manuell installieren, wie hier beschrieben.

Produktinstallation an anderen Knoten:
Automatisch remote - ESET Mail Securitywird an jedem Knoten automatisch installiert (vorausgesetzt, die Betriebssysteme der Knoten weisen die gleiche Architektur auf).
Manuell - Wählen Sie diese Option aus, wenn Sie ESET Mail Security manuell installieren möchten (beispielsweise falls einige der Knoten eine andere Betriebssystemarchitektur aufweisen).

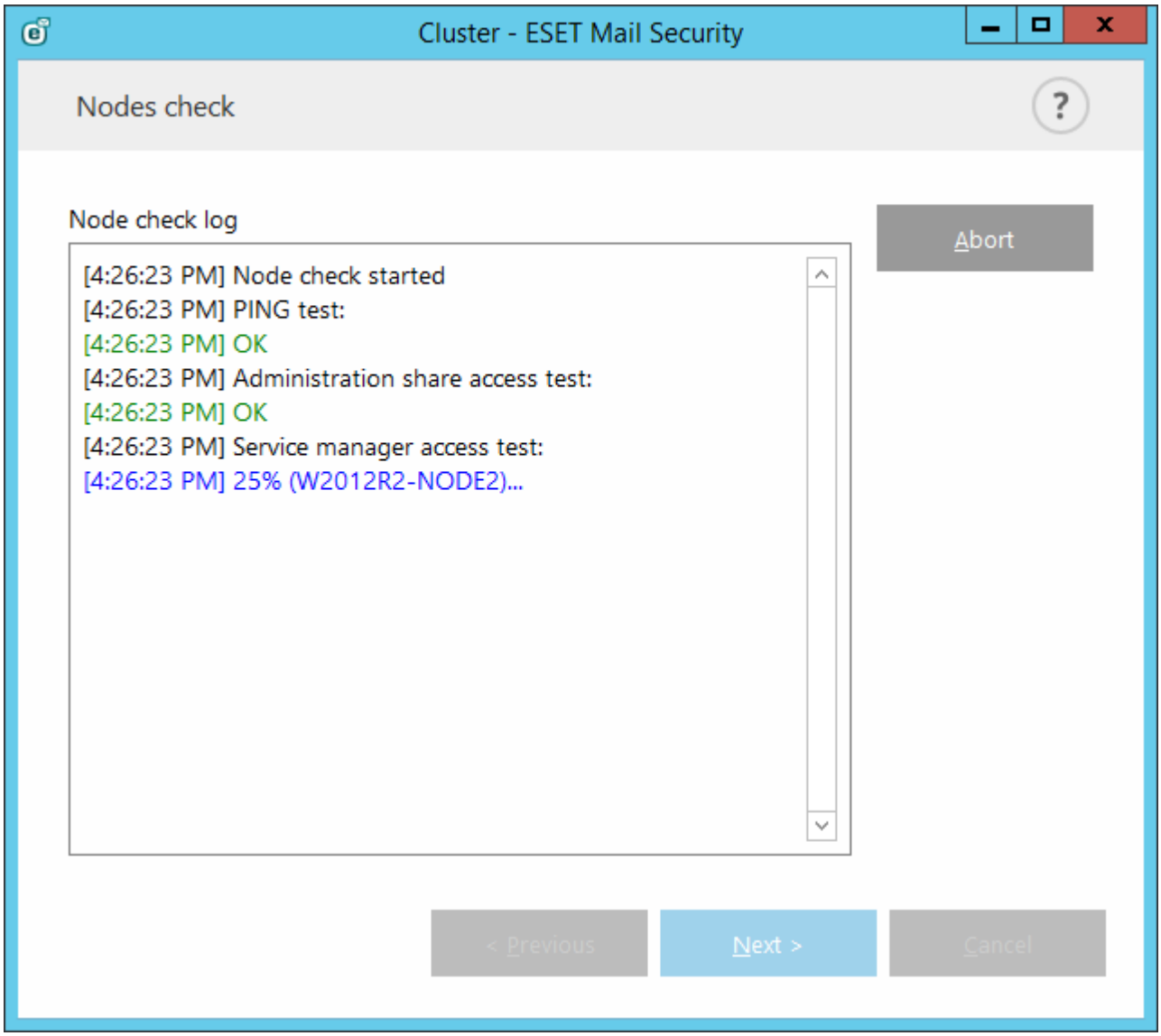
Lizenz auf Knoten ohne aktiviertes Produkt übertragen - ESET Mail Security wird auf den Knoten aktiviert, wenn diese Option markiert ist.

HINWEIS: Wenn Sie ein ESET-Cluster mit gemischten Betriebssystemarchitekturen (32-Bit und 64-Bit) erstellen möchten, müssen Sie ESET Mail Security manuell installieren. Dies wird in den nächsten Schritten ermittelt und es werden im Log-Fenster entsprechende Informationen angezeigt.

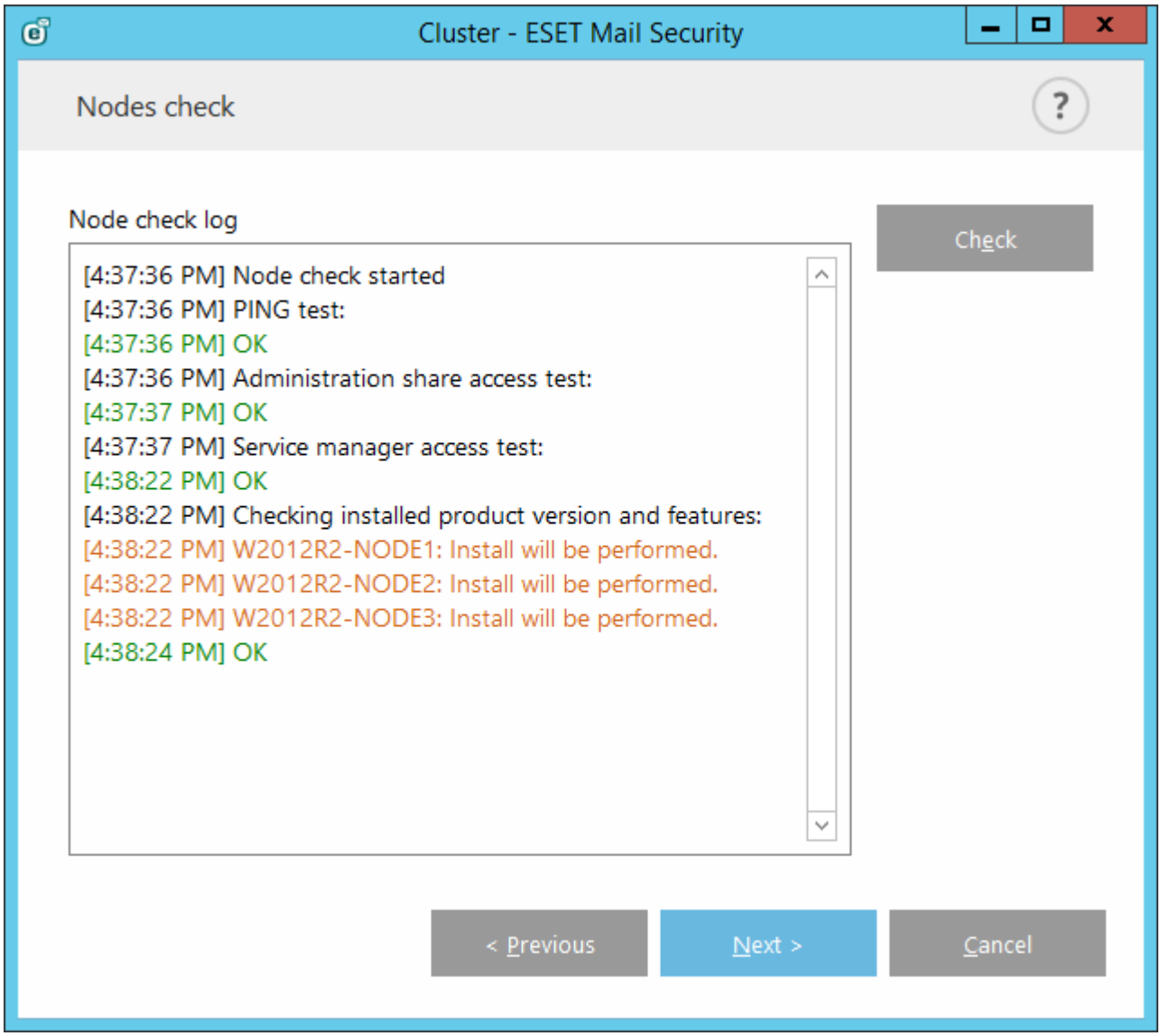
5.1.10.3 Clusterassistent – Seite 3

Nach dem Festlegen der Installationsdetails wird eine Knotenprüfung ausgeführt. Im **Knotenprüfungs-Log** werden die einzelnen geprüften Bedingungen angezeigt:

- Alle vorhandenen Knoten sind online.
- Der Zugriff auf die neuen Knoten ist möglich.
- Der Knoten ist online.
- Der Zugriff auf die administrative Freigabe ist möglich.
- Die Remote-Ausführung ist möglich.
- Die richtige Produktversion ist installiert bzw. es ist kein Produkt installiert (falls die automatische Installation ausgewählt ist).
- Die neuen Zertifikate sind vorhanden

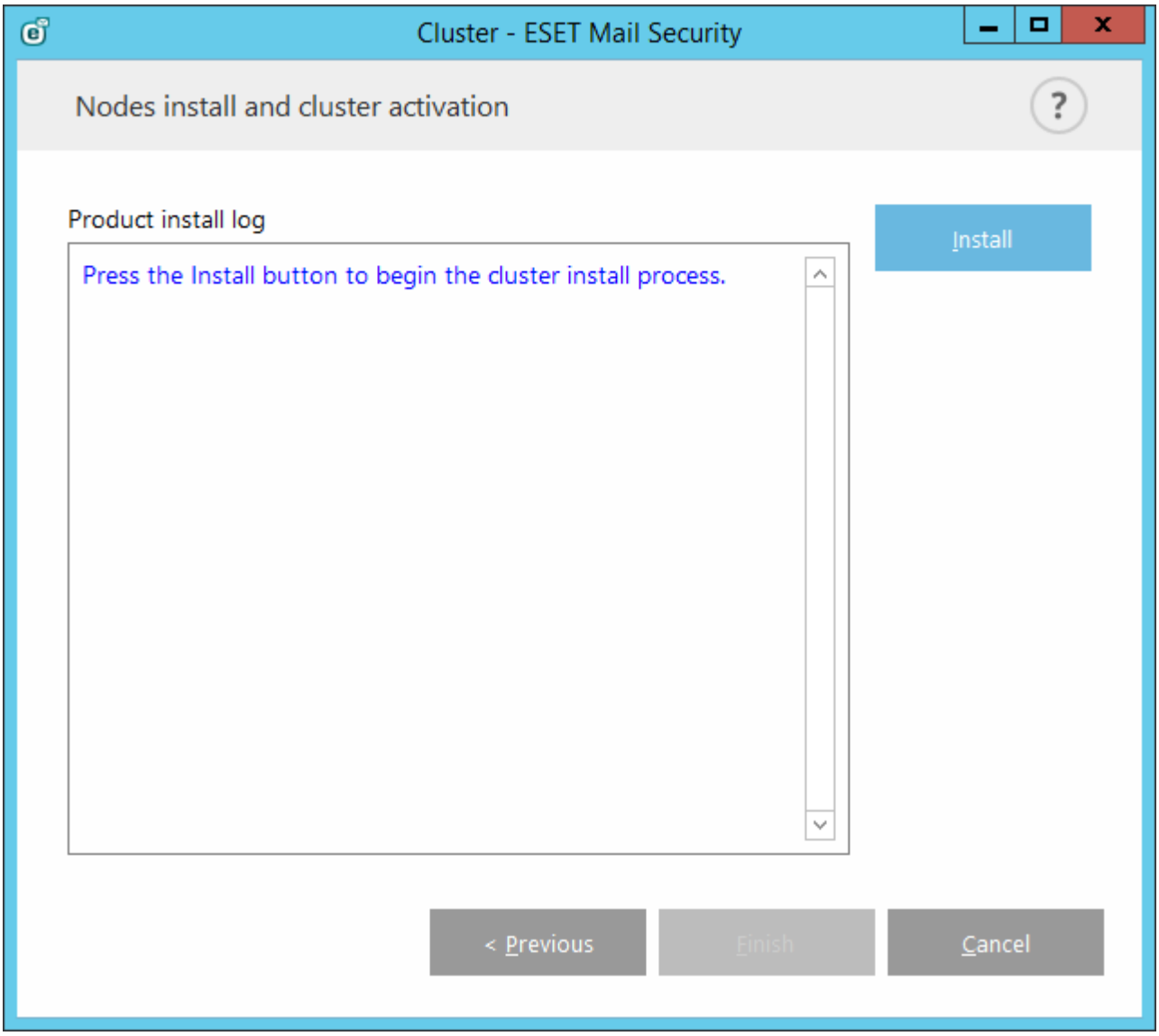


Nach dem Abschließen der Knotenprüfung wird der Bericht angezeigt:



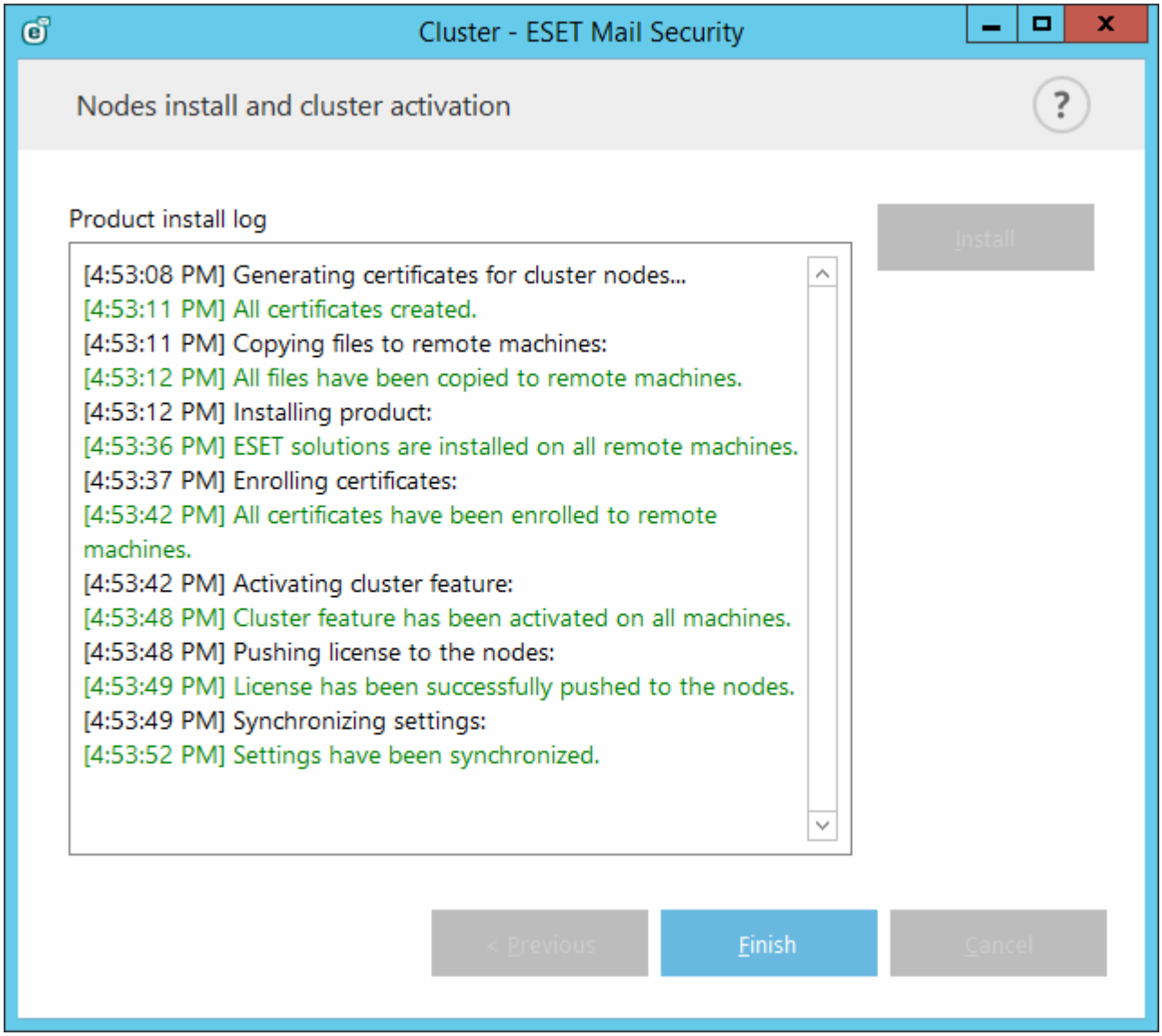
5.1.10.4 Clusterassistent – Seite 4

Wenn das Produkt während der Initialisierung des ESET-Clusters auf einem Remotecomputer installiert werden muss, sucht das Installationspaket im Verzeichnis %ProgramData%\ESET\<Produktname>\Installer nach dem Installationsprogramm. Wenn das Installationspaket dort nicht gefunden wird, wird der Benutzer aufgefordert, eines anzugeben.

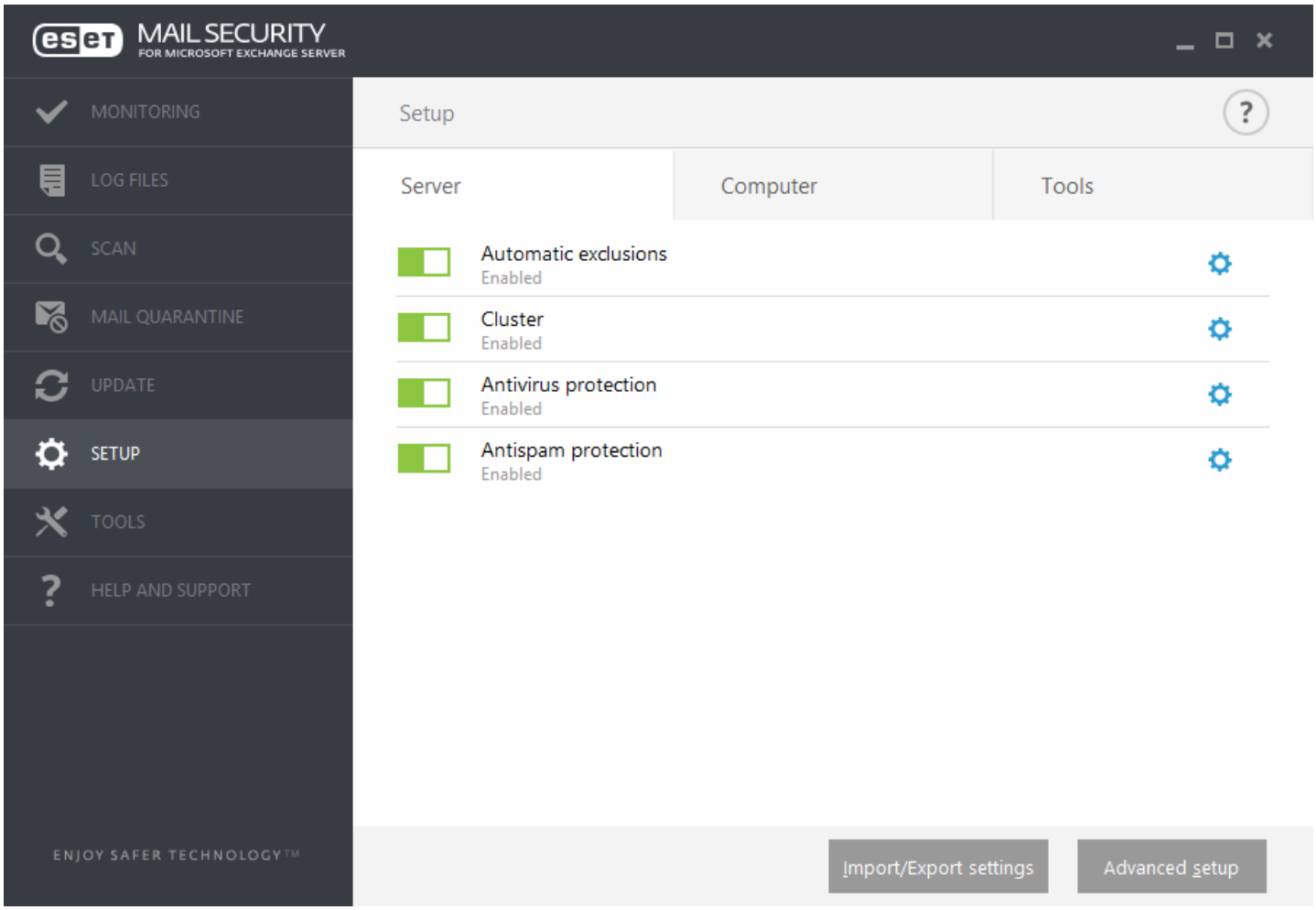


HINWEIS: Wenn versucht wird, eine automatische Remoteinstallation für einen Knoten einer anderen Plattform (32-Bit im Gegensatz zu 64-Bit) auszuführen, erkennt das Programm diese Tatsache und es wird die Empfehlung angezeigt, für den Knoten eine manuelle Installation auszuführen.

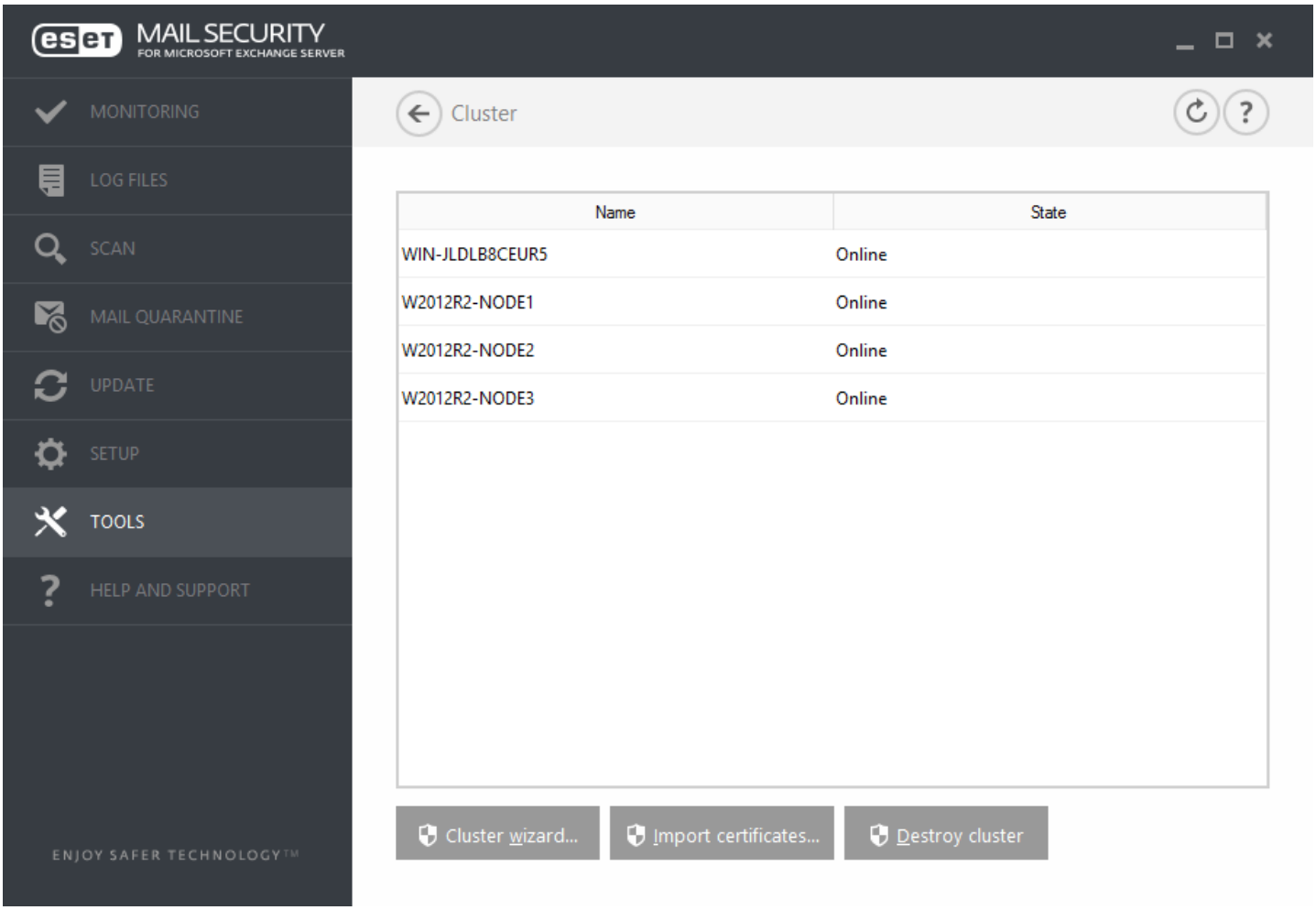
HINWEIS: Wenn Sie bereits eine ältere Version von ESET Mail Security auf manchen Knoten installiert haben, dann muss zunächst eine neuere Version von ESET Mail Security auf diesen Computern installiert werden, bevor das Cluster erstellt wird. Dies kann einen automatischen Neustart der betroffenen Computer auslösen. In diesem Fall wird ein Warnhinweis angezeigt.



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



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



Zertifikate importieren ...

- Navigieren Sie zum Ordner, der das Zertifikat enthält (im Clusterassistenten erzeugt). Wählen Sie das Zertifikat aus und klicken Sie auf **Öffnen**.

5.2 Computer

Das Modul **Computer** befindet sich unter **Einstellungen** > **Computer**. Es enthält eine Übersicht über die im vorherigen Kapitel beschriebenen Schutzmodule. In diesem Bereich stehen die folgenden Einstellungen zur Verfügung:

- Echtzeit-Dateischutz
- On-Demand-Scan
- Prüfen im Leerlaufbetrieb
- Scan der Systemstartdateien
- Wechselmedien
- Dokumentenschutz
- HIPS

Über die Scan-Einstellungen der verschiedenen Schutzmodule (Echtzeit-Dateischutz, Web-Schutz usw.) können Sie die Erkennung der folgenden Elemente aktivieren und deaktivieren:

- Eventuell unerwünschte Anwendungen sind Programme, die zwar nicht unbedingt Sicherheitsrisiken in sich bergen, sich jedoch negativ auf Leistung und Verhalten Ihres Computers auswirken können.
  Weitere Informationen zu diesen Anwendungen finden Sie im Glossar.
- Potenziell unsichere Anwendungen sind gewerbliche Programme, die zu einem böswilligen Zweck missbraucht werden können. Beispiele für potenziell unsichere Anwendungen sind Programme für das Fernsteuern von Computern (Remotedesktopverbindung), Programme zum Entschlüsseln von Passwörtern und Keylogger

(Programme, die aufzeichnen, welche Tasten vom Benutzer gedrückt werden). Standardmäßig ist diese Option deaktiviert.
Weitere Informationen zu diesen Anwendungen finden Sie im Glossar.

- **Verdächtige Anwendungen** umfassen Programme, die mit Packprogrammen oder Schutzprogrammen komprimiert wurden. Diese Schutzarten werden oft von Verfassern von Schadcode eingesetzt, um die Erkennung zu umgehen.

Die Anti-Stealth-Technologie ist ein fortschrittliches System zur Erkennung gefährlicher Programme wie Rootkits, die sich vor dem Betriebssystem verstecken können und daher nicht mit üblichen Prüfmethoden erkannt werden.

Mit den ausgeschlossenen Prozessen können Sie bestimmte Prozesse ausschließen. Wenn Sie z. B. die Prozesse Ihrer Sicherungssoftware ausschließen, werden alle Dateioperationen dieser Prozesse ignoriert und als sicher betrachtet. Auf diese Weise werden Wechselwirkungen mit dem Sicherungsprozess minimiert.

Mit dem Ausschlussfilter können Sie festlegen, welche Dateien und Ordner von Scans 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 Scannen auszuschließen, beispielsweise bei großen Datenbankeinträgen, deren Scan die Computerleistung zu stark beeinträchtigen würde, oder bei Software, die Konflikte mit dem Scan verursacht. Informationen zum Ausschließen von Objekten von den Prüfungen finden Sie unter Ausschlussfilter.

5.2.1 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-Schutz
- On-Demand-Scan

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 einem solchen Fall sollten Sie zuerst 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. Die Option „Immer versuchen, automatisch zu entfernen“ sollten Sie mit Bedacht einsetzen, da in diesem Modus alle Archive gelöscht werden, die mindestens eine infizierte Datei enthalten, und dies unabhängig vom Status der übrigen Archivdateien.
Wenn Ihr Computer die Symptome einer Malware-Infektion aufweist (Computer arbeitet langsamer als gewöhnlich, reagiert häufig nicht usw.), sollten Sie folgendermaßen vorgehen:

- Öffnen Sie ESET Mail Security und klicken Sie auf „Computer prüfen“.
- Klicken Sie auf **Smart-Scan** (weitere Informationen siehe Abschnitt Scannen des Computers).
- Nachdem die Prüfung abgeschlossen ist, überprüfen Sie im Log die Anzahl der geprüften, infizierten und wiederhergestellten Dateien.

Wenn Sie nur einen Teil Ihrer Festplatte prüfen möchten, wählen Sie **Benutzerdefinierter Scan** und anschließend die Bereiche, die auf Viren geprüft werden sollen.

5.2.2 Ausgeschlossene Prozesse

Mit diesem Feature können Sie Anwendungsprozesse von der Virenschutz-Echtzeitprüfung ausschließen. Auf diese Weise können Sie die Gefahr von Konflikten minimieren und die Leistung der ausgeschlossenen Anwendungen verbessern, was sich wiederum positiv auf die Gesamtleistung des Betriebssystems auswirkt.

Wenn ein Prozess ausgeschlossen ist, wird dessen ausführbare Datei nicht überwacht. Die Aktivität der ausgeschlossenen Prozesse wird von ESET Mail Security nicht überwacht, und die Dateivorgänge dieser Prozesse werden nicht geprüft.

Verwenden Sie die Optionen **Hinzufügen**, **Bearbeiten** und **Entfernen**, um die ausgeschlossenen Prozesse zu verwalten.

HINWEIS: Die Prozesse werden lediglich von der Virenschutz-Echtzeitprüfung ausgeschlossen. Der Web-Schutz berücksichtigt diese Liste zum Beispiel dagegen nicht. Wenn Sie also die ausführbare Datei Ihres Webbrowsers ausschließen, werden heruntergeladene Dateien dennoch überprüft. Auf diese Weise können Angriffe weiterhin erkannt werden. Dieses Szenario ist lediglich ein Beispiel und keine Empfehlung, Webbrowser auszuschließen.

HINWEIS: HIPS ist an der Auswertung der ausgeschlossenen Prozesse beteiligt. Sie sollten daher neu ausgeschlossene Prozesse mit aktiviertem HIPS testen (bzw. HIPS deaktivieren, falls Probleme auftreten). Wenn Sie HIPS deaktivieren, wirkt sich dies nicht auf die ausgeschlossenen Prozesse aus. Mit deaktiviertem HIPS werden die ausgeschlossenen Prozesse lediglich anhand des Pfads identifiziert.

5.2.3 Automatische Ausschlüsse

Die Entwickler von Server-Anwendungen und Betriebssystemen empfehlen für die meisten ihrer Produkte, kritische Arbeitsdateien und -ordner vom Virenschutz auszuschließen. Prüfungen mit einer Virenschutz-Software können die Serverleistung beeinträchtigen, zu Konflikten führen und sogar die Ausführung mancher Anwendungen auf dem Server verhindern. Ausschlussfilter können beim Anwenden von Virenschutz-Software das Konfliktrisiko minimieren und die Gesamtleistung des Servers steigern.

ESET Mail Security identifiziert Anwendungen und Betriebssystem-Dateien, die für den Server kritisch sind, und übernimmt sie automatisch in die Liste Ausgeschlossene Elemente. Unter **Zu generierende automatische Ausschlüsse** wird eine Liste der erkannten Serveranwendungen angezeigt, für die Ausschlüsse erstellt wurden. Standardmäßig sind alle automatischen Ausschlüsse aktiviert. Sie können jede Serveranwendung durch Klicken auf den Schalter deaktivieren/aktivieren. Dies verursacht Folgendes:

1. Wenn eine Anwendung bzw. eine Betriebssystemdatei weiterhin ausgeschlossen bleibt, werden alle zugehörigen kritischen Dateien und Ordner zur Liste der vom Scannen ausgeschlossenen Elemente hinzugefügt (**Erweiterte Einstellungen** > **Computer** > > **Basis** > **Ausschlüsse** > **Bearbeiten**). Bei jedem Neustart des Servers werden die Ausschlüsse automatisch überprüft und alle aus der Liste gelöschten Ausschlüsse wiederhergestellt. Diese Einstellung wird empfohlen, wenn Sie sicherstellen möchten, dass die empfohlenen automatischen Ausschlüsse immer angewendet werden.

2. Wenn der Benutzer den Ausschluss einer Anwendung bzw. eines Betriebssystems aufhebt, bleiben alle zugehörigen kritischen Dateien und Ordner in der Liste der vom Scannen ausgeschlossenen Elemente (**Erweiterte Einstellungen** > **Computer** > **Basis** > **Ausschlüsse** > **Bearbeiten**). Sie werden jedoch nicht bei jedem Neustart des Servers automatisch überprüft und in der Liste **Ausgeschlossene Elemente** aktualisiert (siehe Punkt 1 oben). Wir empfehlen diese Einstellung fortgeschrittenen Benutzern, die Standard-Ausschlüsse entfernen oder bearbeiten möchten. Wenn Sie Elemente aus der Ausschlussliste entfernen möchten, ohne den Server neu zu starten, müssen Sie manuell vorgehen (**Erweiterte Einstellungen** > **Computer** > **Einfach** > **Ausschlüsse** > **Bearbeiten**).

Manuell eingetragene benutzerdefinierte Ausschlüsse (**Erweiterte Einstellungen** > **Computer** > **Einfach** > **Ausschlüsse** > **Bearbeiten**) sind nicht von den oben beschriebenen Einstellungen betroffen.

Die automatischen Ausschlüsse für Serveranwendungen bzw. Betriebssystemdateien werden nach Microsoft-Empfehlungen ausgewählt. Weitere Informationen finden Sie in den folgenden Artikeln der Microsoft-Knowledgebase:

- Empfehlungen zum Virenscan auf Unternehmenscomputern, auf denen unterstützte Windows-Versionen ausgeführt werden
- Empfehlungen für die Problembehandlung bei einem Exchange Server-Computer mit installierter Antivirensoftware
- Antivirenscans auf Dateiebene für Exchange 2007
- Antivirensoftware im Betriebssystem auf Exchange-Servern

5.2.4 Gemeinsam genutzter lokaler Cache

Ein gemeinsam genutzter lokaler Cache steigert die Leistung in virtualisierten Umgebungen, indem er doppelte Scans im Netzwerk vermeidet. Somit wird jede Datei nur einmal gescannt und im gemeinsamen Cache gespeichert. Durch Aktivieren der **Caching-Option** werden Informationen zu Prüfungen von Dateien und Ordnern im Netzwerk im lokalen Cache gespeichert. Bei der Durchführung eines neuen Scans sucht ESET Mail Security nach gescannten Dateien im Cache. Wenn übereinstimmende Dateien gefunden werden, werden diese vom Scan ausgeschlossen.

Die Einstellungen für den **Cache-Server** umfassen Folgendes**:**

- **Hostname** - Name oder IP-Adresse des Computers, auf dem sich der Cache befindet.
- **Port** - Nummer des für die Kommunikation verwendeten Ports (mit der im gemeinsam genutzten lokalen Cache festgelegten identisch).
- **Passwort** - Bei Bedarf können Sie ein Passwort für den gemeinsamen lokalen Cache festlegen.

5.2.5 Leistung

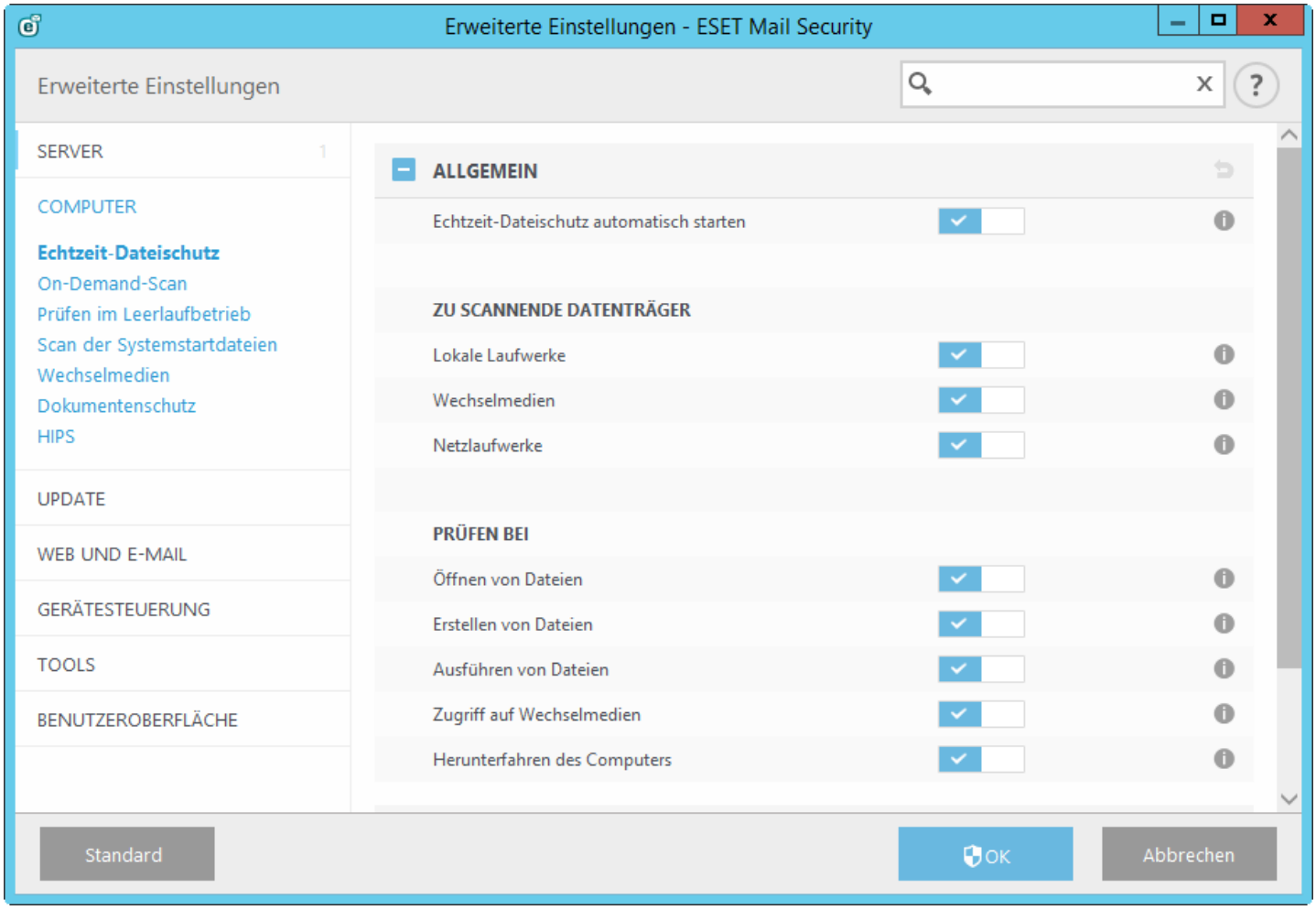
Sie können einstellen, wie viele unabhängige ThreatSense-Prüfmodule für Viren- und Spyware-Schutz gleichzeitig verwendet werden.

Nach Möglichkeit sollte die Anzahl der ThreatSense-Prüfmodule anhand der folgenden Formel erhöht werden: *Anzahl der ThreatSense-Prüfmodule = (Anzahl der physischen Prozessoren x 2) + 1*.

HINWEIS: Der zulässige Wertebereich liegt zwischen 1 und 20, d. h. Sie können maximal 20 ThreatSense-Prüfmodule verwenden.

5.2.6 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 beim Systemstart gestartet.



Der Echtzeit-Dateischutz wird standardmäßig beim Systemstart gestartet und fortlaufend ausgeführt. In Ausnahmefällen (z. B. bei einem Konflikt mit einer anderen Echtzeitprüfung) kann der Echtzeit-Dateischutz deaktiviert werden. Wählen Sie dazu die Option **Echtzeit-Dateischutz automatisch starten** im Bereich **Echtzeit-Dateischutz** > **Basis** in den erweiterten Einstellungen.

- **Zu scannende Datenträger**

In der Standardeinstellung werden alle Datenträger auf mögliche Bedrohungen geprüft:

Lokale Laufwerke - Geprüft werden alle lokalen Laufwerke
Wechselmedien - Geprüft werden /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** - Prüfen von Dateien beim Öffnen aktivieren/deaktivieren.
- **Erstellen von Dateien** - Prüfen von Dateien beim Erstellen aktivieren/deaktivieren.
- **Dateiausführung** - Prüfen von Dateien beim Ausführen aktivieren/deaktivieren.
- **Wechselmedienzugriff** - Prüfen beim Zugriff auf Wechselmedien mit Speicherplatz aktivieren/deaktivieren.
- **Computer-Abschaltung** - Prüfen beim Herunterfahren des Computers aktivieren/deaktivieren.

Der Echtzeit-Dateischutz überwacht alle Datenträger auf das Eintreten bestimmter Ereignisse wie den Zugriff auf eine Datei. Durch die Verwendung der ThreatSense-Erkennungsmethoden (siehe Abschnitt Einstellungen für ThreatSense) kann der Echtzeit-Dateischutz so konfiguriert werden, dass neu erstellte und vorhandene Dateien unterschiedlich behandelt werden. Sie können den Echtzeit-Dateischutz z. B. so konfigurieren, dass neuere Dateien genauer überwacht werden.

Bereits geprüfte Dateien werden nicht erneut geprüft (sofern sie nicht geändert wurden), um die Systembelastung durch den Echtzeit-Dateischutz möglichst gering zu halten. Nach einem Update der Signaturdatenbank werden die Dateien sofort wieder geprüft. 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 bearbeiten, öffnen Sie das Fenster mit den erweiterten Einstellungen **F5** und klicken Sie auf **Computer** > **Echtzeit-Dateischutz**. Klicken Sie auf **Einstellungen für ThreatSense**> **Sonstige** und aktivieren bzw. deaktivieren Sie die Option **Smart-Optimierung aktivieren**.

5.2.6.1 Ausschlussfilter

Nicht zu verwechseln mit **Ausgeschlossene Erweiterungen**

Mit dem Ausschlussfilter können Sie festlegen, welche Dateien und Ordner von Scans 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).

So schließen Sie ein Objekt von Prüfungen aus:

Klicken Sie auf **Hinzufügen** und geben Sie den Pfad zu einem Objekt ein oder wählen es in der Baumstruktur aus. 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“.

Beispiele

- Wenn Sie alle Dateien in einem bestimmten Ordner ausschließen möchten, geben Sie den Pfad zum Ordner mit der Maske "*.*" ein.
- Wenn Sie ein gesamtes Laufwerk einschließlich aller Dateien und Unterordner ausschließen möchten, geben Sie den Pfad mit der Maske „D:*“ ein.
- Wenn nur DOC-Dateien ausgeschlossen werden sollen, verwenden Sie die Maske „*.doc“.
- 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 (unbekannten) Zeichen.

HINWEIS: 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.

Spalten

Pfad - Pfad zu den auszuschließenden Dateien/Ordnern
Bedrohung - Steht neben einer ausgeschlossenen Datei der Name einer Bedrohung, so gilt die Ausnahme nicht generell für die Datei, sondern nur für diese bestimmte Bedrohung. Wird die Datei später durch andere Malware infiziert, erkennt der Virenschutz dies. Dieser Ausschlusstyp kann nur bei bestimmten Arten eingedrungener

Schadsoftware verwendet werden und wird entweder in dem Warnungsfenster für die Bedrohung erstellt (klicken Sie auf **Erweiterte Einstellungen anzeigen** und dann auf **Von der Erkennung ausschließen**) oder indem Sie unter **Einstellungen** > **Quarantäne** mit der rechten Maustaste auf die Datei in der Quarantäne klicken und aus dem Kontextmenü den Befehl **Wiederherstellen und von der Erkennung ausschließen** auswählen.

Steuerelemente

Hinzufügen - Objekte von der Erkennung ausnehmen
Bearbeiten - ausgewählte Einträge bearbeiten
Entfernen - ausgewählte Einträge entfernen

5.2.6.1.1 Hinzufügen oder Bearbeiten der Ausschlüsse

In diesem Dialogfenster können Sie Ausschlussfilter hinzufügen oder bearbeiten. Dazu haben Sie zwei Möglichkeiten:

- Geben Sie den Pfad zu einem Objekt ein, das ausgeschlossen werden soll, oder
- wählen Sie das Objekt in der Baumstruktur aus (klicken Sie dazu am Ende des Textfelds zum Durchsuchen auf **...**).

Bei der ersten Methode können Platzhalter verwendet werden, wie sie im Abschnitt zum Eingeben von Ausschlussfiltern beschrieben werden.

5.2.6.1.2 Eingeben von Ausschlussfiltern

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“.

Beispiele

- Wenn Sie alle Dateien in einem bestimmten Ordner ausschließen möchten, geben Sie den Pfad zum Ordner mit der Maske "*.*" ein.
- Wenn Sie ein gesamtes Laufwerk einschließlich aller Dateien und Unterordner ausschließen möchten, geben Sie den Pfad mit der Maske „D:*“ ein.
- Wenn nur DOC-Dateien ausgeschlossen werden sollen, verwenden Sie die Maske „*.doc“.
- 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 (unbekannten) Zeichen.

5.2.6.2 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.

HINWEIS: 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 Fenster für die Einstellungen zu öffnen, klicken Sie im Fenster der erweiterten Einstellungen auf **ThreatSense-Einstellungen**. Dies gilt für beliebige Module, die ThreatSense verwenden (siehe unten). Je nach Anforderung sind eventuell verschiedene Sicherheitseinstellungen erforderlich. Dies sollte bei den individuellen ThreatSense-Einstellungen für die folgenden Schutzmodule berücksichtigt werden:

- Echtzeit-Dateischutz
- Prüfen im Leerlaufbetrieb
- Scan der Systemstartdateien
- Dokumentenschutz
- E-Mail-Schutz
- Web-Schutz
- Scannen des Computers

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 Advanced 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 scannende Objekte

In diesem Bereich können Sie festlegen, welche Dateien und Komponenten Ihres Computers auf Schadcode gescannt werden sollen.

- **Arbeitsspeicher** - Scannt auf Bedrohungen für den Arbeitsspeicher des Systems.
- **Systembereiche (Boot, MBR)** - Scannt die Bootsektoren auf Viren im Master Boot Record. Im Fall von virtuellen Hyper-V-Computern wird der Laufwerks-MBR im schreibgeschützten Modus geprüft.
- **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 Starten im Arbeitsspeicher dekomprimiert. Neben statischen laufzeitkomprimierten Dateiformaten (UPX, yoda, ASPack, FSG usw.) kann die Prüfung durch Code-Emulation viele weitere SFX-Typen erkennen.

Prüfungseinstellungen

Wählen Sie die Methoden aus, mit denen das System auf Infiltrationen gescannt werden soll. Die folgenden Optionen stehen zur Verfügung:

- **Heuristik** - Als heuristische Methoden werden Verfahren bezeichnet, die (bösartige) Aktivitäten von Programmen analysieren. Auf diese Weise können auch bösartige Programme erkannt werden, die noch nicht in der Signaturdatenbank verzeichnet sind. Nachteilig ist, dass es in Einzelfällen zu Fehlalarmen kommen kann.
- **Advanced Heuristik/DNA/Smart-Signaturen** - Als Advanced Heuristik werden besondere heuristische Verfahren bezeichnet, die von ESET entwickelt wurden, um eine verbesserte Erkennung von Würmern und Trojanern zu ermöglichen und Schadprogramme zu erkennen, die in höheren Programmiersprachen geschrieben wurden. Mit Advanced Heuristik werden die Fähigkeiten von ESET-Produkten zur Erkennung von Bedrohungen beträchtlich gesteigert. Mit Hilfe von Signaturen können Viren zuverlässig erkannt werden. Mit automatischen Updates sind Signaturen für neue Bedrohungen innerhalb weniger Stunden verfügbar. Nachteilig an Signaturen ist, dass mit ihrer Hilfe nur bekannte Viren und gering modifizierte Varianten bekannter Viren erkannt werden können.
-

Säubern

Die Einstellungen zum Entfernen von Schadcode legen fest, wie beim Entfernen vorgegangen werden soll. Es gibt drei Arten der Schadcodeentfernung:

Nicht säubern - Der in infizierten Objekten erkannte Schadcode wird nicht automatisch entfernt. Eine Warnung wird

angezeigt, und der Benutzer wird aufgefordert, eine Aktion auszuwählen. Diese Stufe eignet sich für fortgeschrittene Benutzer, die wissen, wie sie im Falle eingedrungener Schadsoftware vorgehen sollen.

Normale Säuberung - Das Programm versucht, infizierte Dateien automatisch zu säubern oder zu löschen. Es wendet hierzu vordefinierte Aktionen an (je nach Art der Infiltration). Ein Hinweis am unteren rechten Bildschirmrand informiert über die Erkennung und das Löschen infizierter Dateien. Wenn es nicht möglich ist, die angemessene Aktion automatisch zu bestimmen, schlägt das Programm verschiedene Aktionen vor. Dies gilt auch für Fälle, in denen eine vordefinierte Aktion nicht erfolgreich abgeschlossen werden kann.

Immer versuchen, automatisch zu säubern - Das Programm entfernt den Schadcode aus infizierten Dateien oder löscht diese Dateien. Ausnahmen gelten nur für Systemdateien. Wenn eine Datei nicht gesäubert werden kann, wird der Benutzer zur Auswahl einer Aktion aufgefordert.

ACHTUNG: Wenn infizierte Dateien in einem Archiv gefunden werden, sind zwei Vorgehensweisen möglich. Im Standardmodus („normales Säubern“) wird die Archivdatei nur dann gelöscht, wenn alle Dateien im Archiv infiziert sind. Wenn die Option **Immer versuchen, automatisch zu entfernen** aktiviert ist, wird die Archivdatei gelöscht, sobald eine einzige Datei im Archiv infiziert ist.

WICHTIGER HINWEIS: Auf Hyper-V-Hosts mit Windows Server 2008 R2 werden die Optionen **normale Säuberung** und **Immer versuchen, automatisch zu entfernen** nicht unterstützt. Die Laufwerke der virtuellen Computer werden im schreibgeschützten Modus geprüft - **keine Säuberung**. Die Prüfung erfolgt immer im schreibgeschützten Modus, unabhängig von der ausgewählten Säuberungsstufe.

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) scannen** - Bei den von NTFS-Dateisystemen verwendeten alternativen Datenströmen (ADS) handelt es sich um Datei- und Ordnerzuordnungen, die mit herkömmlichen Scan-Techniken nicht erkannt werden können. Eingedrungene Schadsoftware tarnt sich häufig als alternativer Datenstrom, um nicht erkannt zu werden.
- **Hintergrund-Scans mit geringer Priorität ausführen** - Jeder Scan 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 aktivieren, werden alle gescannten Dateien im Log eingetragen. Es werden also auch Dateien eingetragen, bei denen keine Bedrohung erkannt wurde. Wenn beispielsweise in einem Archiv Schadcode gefunden wird, listet das Log auch die in diesem Archiv enthaltenen, nicht infizierten Dateien auf.
- **Smart-Optimierung aktivieren** - Wenn die Smart-Optimierung aktiviert ist, werden die optimalen Einstellungen verwendet, um den effizientesten Scan bei höchster Geschwindigkeit zu gewährleisten. Die verschiedenen Schutzmodule führen eine intelligente Prüfung durch. Dabei verwenden sie unterschiedliche Prüfmethoden für die jeweiligen Dateitypen. Wenn die Smart-Optimierung deaktiviert ist, werden nur die benutzerdefinierten Einstellungen im ThreatSense-Kern der entsprechenden Module für den Scan 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:

Einstellungen für Objektprüfung

Standard-Einstellungen Objektprüfung

- **Maximale Objektgröße** - Definiert die Maximalgröße der zu scannenden Elemente. Der aktuelle Virenschutz prüft dann nur die Elemente, deren Größe unter der angegebenen Maximalgröße liegt. Diese Option sollte nur von fortgeschrittenen Benutzern geändert werden, die bestimmte Gründe dafür haben, dass größere Elemente von der Prüfung ausgeschlossen werden. Der Standardwert ist *unbegrenzt*.
- **Maximale Scanzeit pro Objekt (Sek.)** - Definiert die maximale Dauer für die Prüfung eines Elements. Wenn hier ein benutzerdefinierter Wert eingegeben wurde, beendet der Virenschutz die Prüfung eines Elements, sobald diese Zeit abgelaufen ist, und zwar ungeachtet dessen, ob die Prüfung abgeschlossen ist oder nicht. Der Standardwert ist *unbegrenzt*.

Einstellungen für Archivprüfung

Verschachtelungstiefe bei Archiven - Legt die maximale Tiefe der Virenprüfung von Archiven fest. Der Standardwert ist *10*.

Maximalgröße von Dateien im Archiv - Hier können Sie die maximale Dateigröße für Dateien in (extrahierten) Archiven festlegen, die geprüft werden sollen. Der Standardwert ist *unbegrenzt*.

HINWEIS: Die Standardwerte sollten nicht geändert werden; unter normalen Umständen besteht dazu auch kein Grund.

5.2.6.2.1 Von der Prüfung ausgeschlossene Dateiendungen

Die Erweiterung ist der Teil des Dateinamens nach dem Punkt. Die Erweiterung definiert den Typ und den Inhalt einer Datei. In diesem Abschnitt der ThreatSense-Einstellungen können Sie die Dateitypen festlegen, die gescannt werden sollen.

Standardmäßig werden alle Dateien gescannt. Jede Erweiterung kann der Liste ausgeschlossener Dateien hinzugefügt werden.

Der Ausschluss bestimmter Dateien ist dann sinnvoll, wenn das Scannen bestimmter Dateitypen die Funktion eines Programms beeinträchtigt, das diese Erweiterungen verwendet. So sollten Sie z. B. die Erweiterungen EDB, EML und TMP ausschließen, wenn Sie Microsoft Exchange Server verwenden.

Über die Schaltflächen **Hinzufügen** und **Entfernen** können Sie festlegen, welche Erweiterungen gescannt werden sollen. Klicken Sie zum Hinzufügen einer neuen Erweiterung zur Liste auf „Hinzufügen“, geben Sie die Erweiterung in das Feld ein und klicken Sie anschließend auf „OK“. Mit der Option **Mehrere Werte eingeben** können Sie mehrere, durch Zeilen, Komma oder Semikolon getrennte Erweiterungen eingeben. Wenn die Mehrfachauswahl aktiviert ist, werden die Erweiterungen in der Liste angezeigt. Wählen Sie eine Erweiterung in der Liste aus und klicken Sie auf **Entfernen**, um die markierte Erweiterung aus der Liste zu entfernen. Wenn Sie eine ausgewählte Erweiterung bearbeiten möchten, klicken Sie auf **Bearbeiten**.

Sie können die Sonderzeichen „*“ (Sternchen) und „?“ (Fragezeichen) verwenden. Das Sternchen ersetzt eine beliebige Zeichenfolge, das Fragezeichen ein beliebiges Symbol.

5.2.6.2.2 Zusätzliche ThreatSense-Parameter

Zusätzliche ThreatSense-Parameter für neu erstellte und geänderte Dateien - Das Infektionsrisiko für neu erstellte oder geänderte Dateien ist vergleichsweise größer als für vorhandene Dateien. Daher prüft das Programm solche Dateien mit zusätzlichen Parametern. Zusätzlich zu den üblichen Prüfmethoden auf Signaturbasis wird die Advanced Heuristik verwendet. Diese Methode erkennt neue Bedrohungen, bevor ein Update der Signaturdatenbank veröffentlicht wird. Neben neu erstellten Dateien werden auch selbstentpackende Archive (SFX) und laufzeitkomprimierte Dateien (intern komprimierte, ausführbare Dateien) geprüft. In den Standardeinstellungen werden Archive unabhängig von ihrer eigentlichen Größe bis zur 10. Verschachtelungstiefe geprüft. Deaktivieren Sie die Option **Standardeinstellungen Archivprüfung**, um die Archivprüfeinstellungen zu ändern.

Weitere Informationen zu **laufzeitkomprimierten Dateien**, **selbstentpackenden Archiven** und **Advanced Heuristik** finden Sie unter Einstellungen für ThreatSense.

Zusätzliche ThreatSense-Einstellungen für ausführbare Dateien - Standardmäßig wird bei der Dateiausführung keine Advanced Heuristik verwendet. Wenn diese Option aktiviert ist, sollten Smart-Optimierung und ESET Live Grid unbedingt aktiviert bleiben, um die Auswirkungen auf die Systemleistung gering zu halten.

5.2.6.2.3 Säuberungsstufen

Für den Echtzeit-Dateischutz stehen drei Säuberungsstufen zur Verfügung. Zugriff darauf erhalten Sie durch Klicken auf **ThreatSense-Parameter** im Bereich **Echtzeit-Dateischutz** unter **Säubern**.

Nicht säubern - Der in infizierten Objekten erkannte Schadcode wird nicht automatisch entfernt. Eine Warnung wird angezeigt, und der Benutzer wird aufgefordert, eine Aktion auszuwählen. Diese Stufe eignet sich für fortgeschrittene Benutzer, die wissen, wie sie im Falle eingedrungener Schadsoftware vorgehen sollen.

Normale Säuberung - Das Programm versucht, infizierte Dateien automatisch zu säubern oder zu löschen. Es wendet hierzu vordefinierte Aktionen an (je nach Art der Infiltration). Ein Hinweis am unteren rechten Bildschirmrand informiert über die Erkennung und das Löschen infizierter Dateien. Wenn es nicht möglich ist, die angemessene Aktion automatisch zu bestimmen, schlägt das Programm verschiedene Aktionen vor. Dies gilt auch für Fälle, in denen eine vordefinierte Aktion nicht erfolgreich abgeschlossen werden kann.

Immer versuchen, automatisch zu säubern - Das Programm entfernt den Schadcode aus infizierten Dateien oder löscht diese Dateien. Ausnahmen gelten nur für Systemdateien. Wenn eine Datei nicht gesäubert werden kann, wird der Benutzer zur Auswahl einer Aktion aufgefordert.

ACHTUNG: Wenn infizierte Dateien in einem Archiv gefunden werden, sind zwei Vorgehensweisen möglich. Im Standardmodus („normales Säubern“) wird die Archivdatei nur dann gelöscht, wenn alle Dateien im Archiv infiziert sind. Wenn die Option **Immer versuchen, automatisch zu entfernen** aktiviert ist, wird die Archivdatei gelöscht, sobald eine einzige Datei im Archiv infiziert ist.

WICHTIGER HINWEIS: Auf Hyper-V-Hosts mit Windows Server 2008 R2 werden die Optionen **normale Säuberung** und **Immer versuchen, automatisch zu entfernen** nicht unterstützt. Die Laufwerke der virtuellen Computer werden im schreibgeschützten Modus geprüft - **keine Säuberung**. Die Prüfung erfolgt immer im schreibgeschützten Modus, unabhängig von der ausgewählten Säuberungsstufe.

5.2.6.2.4 Wann sollten die Einstellungen für den Echtzeit-Dateischutz geändert werden?

Der Echtzeit-Systemschutz ist die wichtigste Komponente für ein sicheres System. Daher sollte gründlich geprüft werden, ob eine Änderung der Einstellungen wirklich notwendig ist. Es wird empfohlen, seine Parameter nur in einzelnen Fällen zu verändern.

Bei der Installation von ESET Mail Security werden alle Einstellungen optimal eingerichtet, um dem Benutzer die größtmögliche Schutzstufe für das System zu bieten. Wenn Sie die Standardeinstellungen wiederherstellen möchten, klicken Sie auf neben den Registerkarten im Fenster (**Erweiterte Einstellungen** > **Computer** > **Echtzeit-Dateischutz**).

5.2.6.2.5 Echtzeit-Dateischutz prüfen

Um sicherzustellen, dass der Echtzeit-Dateischutz aktiv ist und Viren erkennt, verwenden Sie eine Testdatei von eicar.com. Diese Testdatei ist harmlos und wird von allen Virenschutzprogrammen erkannt. Die Datei wurde von der Firma EICAR (European Institute for Computer Antivirus Research) erstellt, um die Funktionalität von Virenschutzprogrammen zu testen. Die Datei kann unter http://www.eicar.org/download/eicar.com heruntergeladen werden.

5.2.6.2.6 Vorgehensweise bei fehlerhaftem Echtzeit-Dateischutz

In diesem Kapitel werden mögliche Probleme mit dem Echtzeit-Dateischutz sowie Lösungsstrategien beschrieben.

Echtzeit-Dateischutz ist deaktiviert

Der Echtzeit-Dateischutz wurde versehentlich von einem Benutzer deaktiviert und muss reaktiviert werden. Um den Echtzeit-Dateischutz erneut zu aktivieren, navigieren Sie im Hauptprogrammfenster zu **Einstellungen** und klicken auf **Echtzeit-Dateischutz**.

Wenn der Echtzeit-Dateischutz beim Systemstart nicht gestartet wird, ist wahrscheinlich die Option **Echtzeit-Dateischutz automatisch starten** deaktiviert. Zum Aktivieren dieser Option klicken Sie in den **Erweiterten Einstellungen** (**F5**) auf **Computer** > **Echtzeit-Dateischutz** > **Basis**. Achten Sie darauf, dass **Echtzeit-Dateischutz automatisch starten** aktiviert ist.

Echtzeit-Dateischutz erkennt und entfernt keinen Schadcode

Stellen Sie sicher, dass keine anderen Virenschutzprogramme auf Ihrem Computer installiert sind. Zwei parallel ausgeführte Schutzprogramme können miteinander in Konflikt geraten. Wir empfehlen Ihnen, vor der Installation von ESET alle anderen Virusschutzprogramme zu deinstallieren.

Echtzeit-Dateischutz startet nicht

Wenn der Echtzeit-Dateischutz beim Systemstart nicht initialisiert wird (und die Option **Echtzeit-Dateischutz automatisch starten** aktiviert ist), kann dies an Konflikten mit anderen Programmen liegen. Sollte dies der Fall sein, wenden Sie sich an den ESET-Support.

5.2.6.2.7 Einreichen

Hier legen Sie fest, wie verdächtige Dateien und statistische Daten an ESET gesendet werden. Wählen Sie **Über Remote Administrator Server oder direkt an ESET**, wenn die Dateien und Daten auf allen verfügbaren Übertragungswegen übermittelt werden sollen. Mit der Option **Über Remote Administrator** werden Dateien und Statistiken an den Remote Administration Server gesendet, der sie zur Analyse an das ESET-Virenlabor weiterleitet. Bei Auswahl der Option **Direkt an ESET** werden alle verdächtigen Dateien und statistischen Daten direkt aus dem Programm an das ESET-Virenlabor gesendet.

Wenn Dateien vorhanden sind, die noch gesendet werden müssen, ist die Schaltfläche **Jetzt einreichen** aktiviert. Klicken Sie auf diese Schaltfläche, um die Dateien und statistischen Daten direkt zu senden.

Wählen Sie **Erstellen von Logs aktivieren** aus, um eine Log-Datei zu erstellen, in der alle Informationen über das Senden von Dateien und statistischen Daten protokolliert werden.

5.2.6.2.8 Statistik

Das ThreatSense.Net-Frühwarnsystem sammelt anonyme Daten über neue Bedrohungen, die auf Ihrem Computer erkannt wurden. Erfasst werden der Name der Bedrohung, Datum und Uhrzeit der Erkennung, die Versionsnummer des ESET Security-Produkts sowie Versionsdaten und die Regionaleinstellung des Betriebssystems. Statistiken werden üblicherweise einmal oder zweimal täglich an ESET übermittelt.

Beispiel für ein typisches Statistikpaket:

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\C14J8
```

Wann einreichen - Sie können festlegen, wann die statistischen Daten übermittelt werden sollen. Wenn Sie die Option **Baldmöglichst** auswählen, werden die statistischen Daten direkt nach ihrer Erstellung gesendet. Diese Einstellung eignet sich, wenn eine dauerhafte Internetverbindung besteht. Bei der Option **Beim nächsten Update** werden die statistischen Daten gespeichert und beim nächsten Update gesammelt gesendet.

5.2.6.2.9 Verdächtige Dateien

In der Registerkarte **Verdächtige Dateien** können Sie konfigurieren, wie Bedrohungen zur Analyse an das ESET-Virenlabor gesendet werden.

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 der Signaturdatenbank berücksichtigt.

Das Einreichen von Dateien kann automatisch erfolgen. Wenn Sie dies nicht wünschen und stattdessen wissen möchten, welche Dateien eingereicht werden, aktivieren Sie die Option **Vor dem Einreichen fragen**, die Sie zu einer Bestätigung des Vorgangs auffordert.

Wenn keine Dateien gesendet werden sollen, wählen Sie die Option **Nicht einreichen**. Die Übermittlung statistischer Daten wird separat konfiguriert und daher durch diese Einstellung nicht beeinflusst (siehe Abschnitt Statistik).

Wann einreichen - Standardmäßig ist **Baldmöglichst** für das Einreichen verdächtiger Dateien an ESET festgelegt. Diese Einstellung wird empfohlen, wenn eine dauerhafte Internetverbindung besteht und die verdächtigen Dateien ohne Verzögerung übermittelt werden können. Aktiveren Sie die Option **Beim nächsten Update**, um verdächtige Dateien bei der nächsten Aktualisierung an ThreatSense.Net zu übertragen.

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. Einige typische Dateitypen sind bereits in der Standardeinstellung in die Liste eingetragen (.doc usw.). Sie können der Ausschlussliste weitere Dateien hinzufügen.

E-Mail-Adresse - Sie können mit den verdächtigen Dateien eine **E-Mail [optional]** 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.

5.2.7 On-demand-Scan und Hyper-V-Scan

Dieser Bereich enthält Optionen zur Auswahl von Scan-Parametern.

HINWEIS: Diese Scanprofil-Auswahl gilt für On-demand- und für Hyper-V-Scans.

Ausgewähltes Profil - Eine bestimmte Reihe von Parametern, die beim On-Demand-Scan verwendet werden. Wenn Sie einen neuen erstellen möchten, klicken Sie neben der **Profilliste** auf **Bearbeiten**.

Wenn nur ein bestimmtes Objekt gescannt werden soll, können Sie neben **Zu scannende Objekte** auf **Bearbeiten** klicken und eine Option aus dem Dropdown-Menü oder bestimmte Objekte aus der Ordnerstruktur auswählen.

Im Fenster mit den zu scannenden Objekten können Sie definieren, welche Objekte (Arbeitsspeicher, Laufwerke, Dateien und Ordner) auf Schadcode gescannt werden. Wählen Sie die zu scannenden Objekte aus der Baumstruktur aus, in der alle auf dem Computer verfügbaren Ordner aufgelistet werden. Im Dropdown-Menü **Zu scannende Objekte** können Sie vordefinierte Optionen für die zu scannenden Objekte auswählen.

- **Nach Profileinstellungen** - Im Scan-Profil festgelegte Ziele
- **Wechselmedien** - Disketten, USB-Speichergeräte, CDs/DVDs
- **Lokale Laufwerke** - Alle lokalen Systemlaufwerke
- **Netzlaufwerke** - Alle zugeordneten Netzlaufwerke
- **Freigegebene Ordner** - Alle freigegebenen Ordner auf dem lokalen Server
- **Keine Auswahl** - Bricht die Zielauswahl ab

Klicken Sie auf Einstellungen für ThreatSense, um die Einstellungen (z. B. die Erkennungsmethoden) für den On-Demand-Scanner zu ändern.

5.2.7.1 Benutzerdefinierter Scan und Hyper-V-Scan

Wenn Sie nur bestimmte Objekte prüfen möchten, klicken Sie auf **Scannen des Computers** > **Benutzerdefinierter Scan**. Wählen Sie die zu prüfenden Objekte aus dem Dropdown-Menü **Zu prüfende Objekte** oder in der Ordnerstruktur (Baumstruktur) aus.

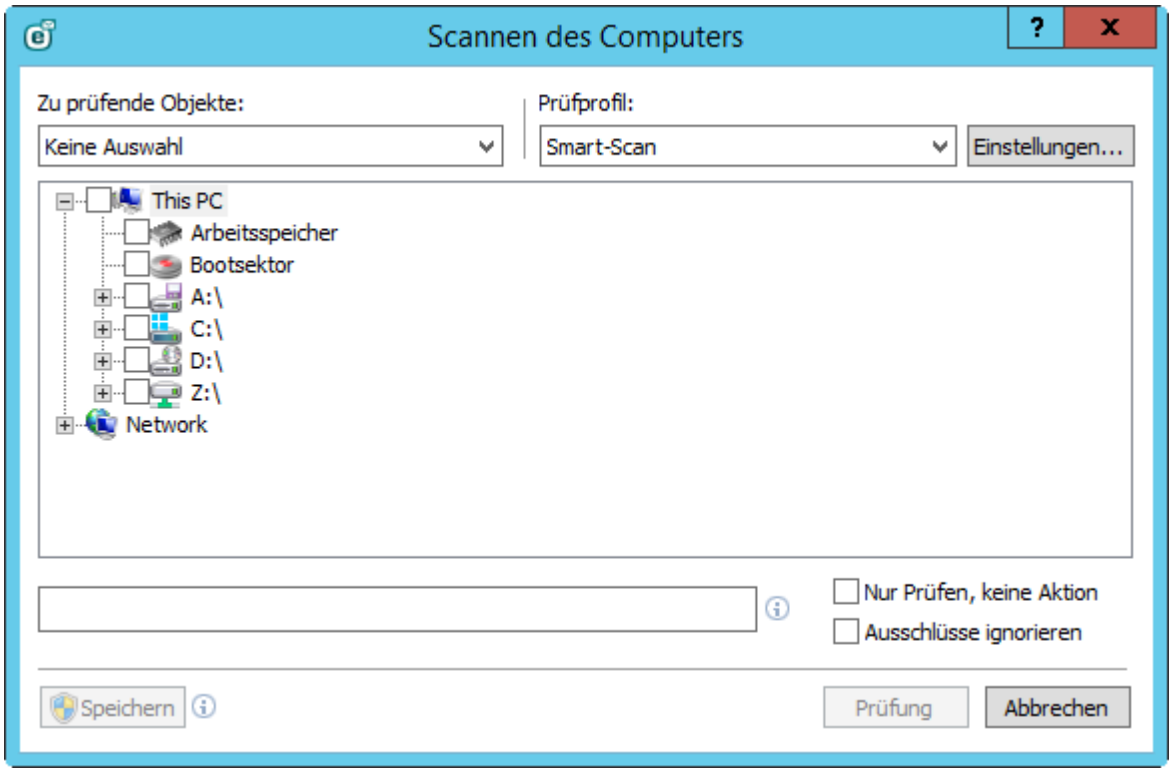
HINWEIS: Diese Scanziel-Auswahl gilt für benutzerdefinierte und für Hyper-V-Scans.

Im Fenster mit den zu scannenden Objekten können Sie definieren, welche Objekte (Arbeitsspeicher, Laufwerke, Dateien und Ordner) auf Schadcode gescannt werden. Wählen Sie die zu scannenden Objekte aus der Baumstruktur aus, in der alle auf dem Computer verfügbaren Ordner aufgelistet werden. Im Dropdown-Menü **Zu scannende Objekte** können Sie vordefinierte Optionen für die zu scannenden Objekte auswählen.

- **Nach Profileinstellungen** - Im Scan-Profil festgelegte Ziele
- **Wechselmedien** - Disketten, USB-Speichergeräte, CDs/DVDs
- **Lokale Laufwerke** - Alle lokalen Systemlaufwerke
- **Netzlaufwerke** - Alle zugeordneten Netzlaufwerke
- **Freigegebene Ordner** - Alle freigegebenen Ordner auf dem lokalen Server
- **Keine Auswahl** - Bricht die Zielauswahl ab

Um schnell zu einem zu prüfenden Objekt zu navigieren oder um ein gewünschtes Objekt (Ordner oder Datei(ein)) direkt 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 **Zu prüfende Objekte** die Option **Keine Auswahl** festgelegt ist.

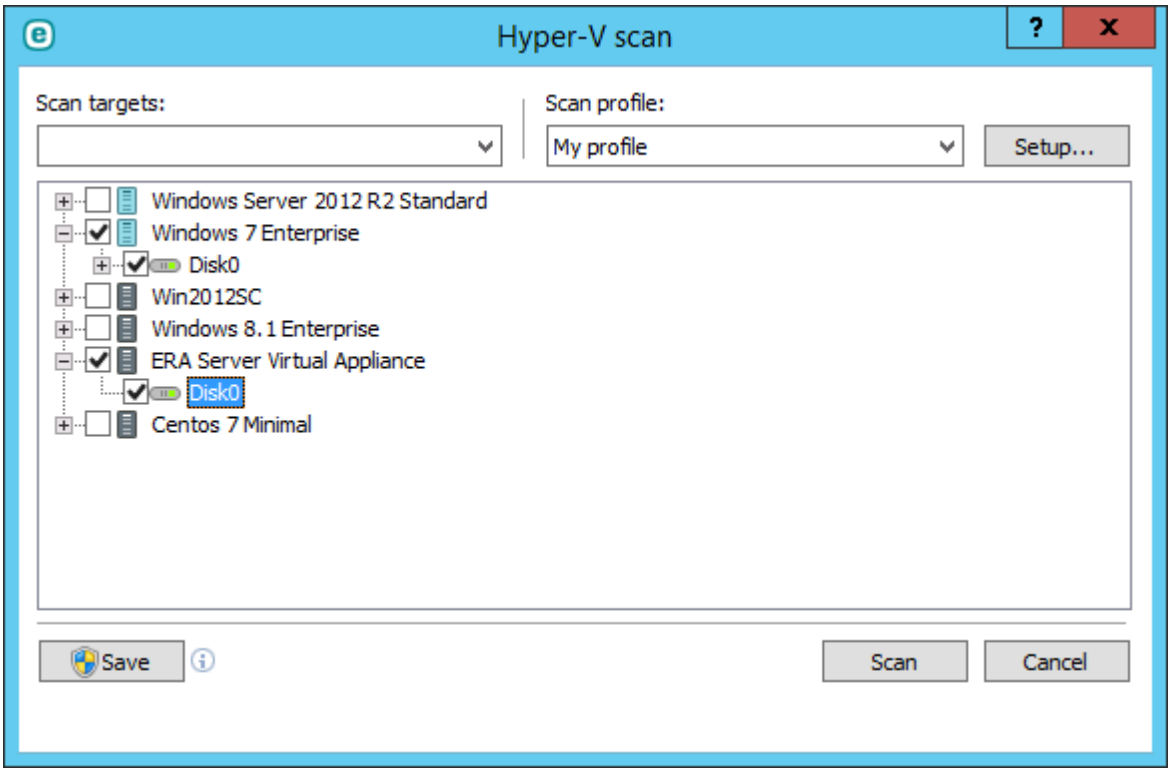
Benutzerdefinierter Scan Popupfenster:



Wenn Sie nur das System ohne zusätzliche Säuberung prüfen möchten, wählen Sie die Option **Nur prüfen, keine Aktion**. 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.

Wenn Sie **Ausschlüsse ignorieren** auswählen, können Sie einen Scan ohne die Ausschlüsse durchführen, die normalerweise gelten würden.

Hyper-V-Scan Popupfenster (siehe Hyper-V-Scan für weitere Informationen):



Aus dem Dropdown-Menü **Prüfprofil** können Sie ein Profil auswählen, um ausgewählte Objekte zu prüfen. Das Standardprofil ist **Smart-Scan**. Es stehen außerdem zwei weitere vordefinierte Prüfprofile zur Verfügung: **Tiefenprüfung** und **Kontextmenü-Prüfung**. Diese Prüfprofile verwenden unterschiedliche ThreatSense-Einstellungen. Klicken Sie auf **Einstellungen ...**, um ein ausgewähltes Prüfprofil detailliert zu konfigurieren. Die verfügbaren Optionen sind im Abschnitt **Sonstige** in Einstellungen für ThreatSense beschrieben.

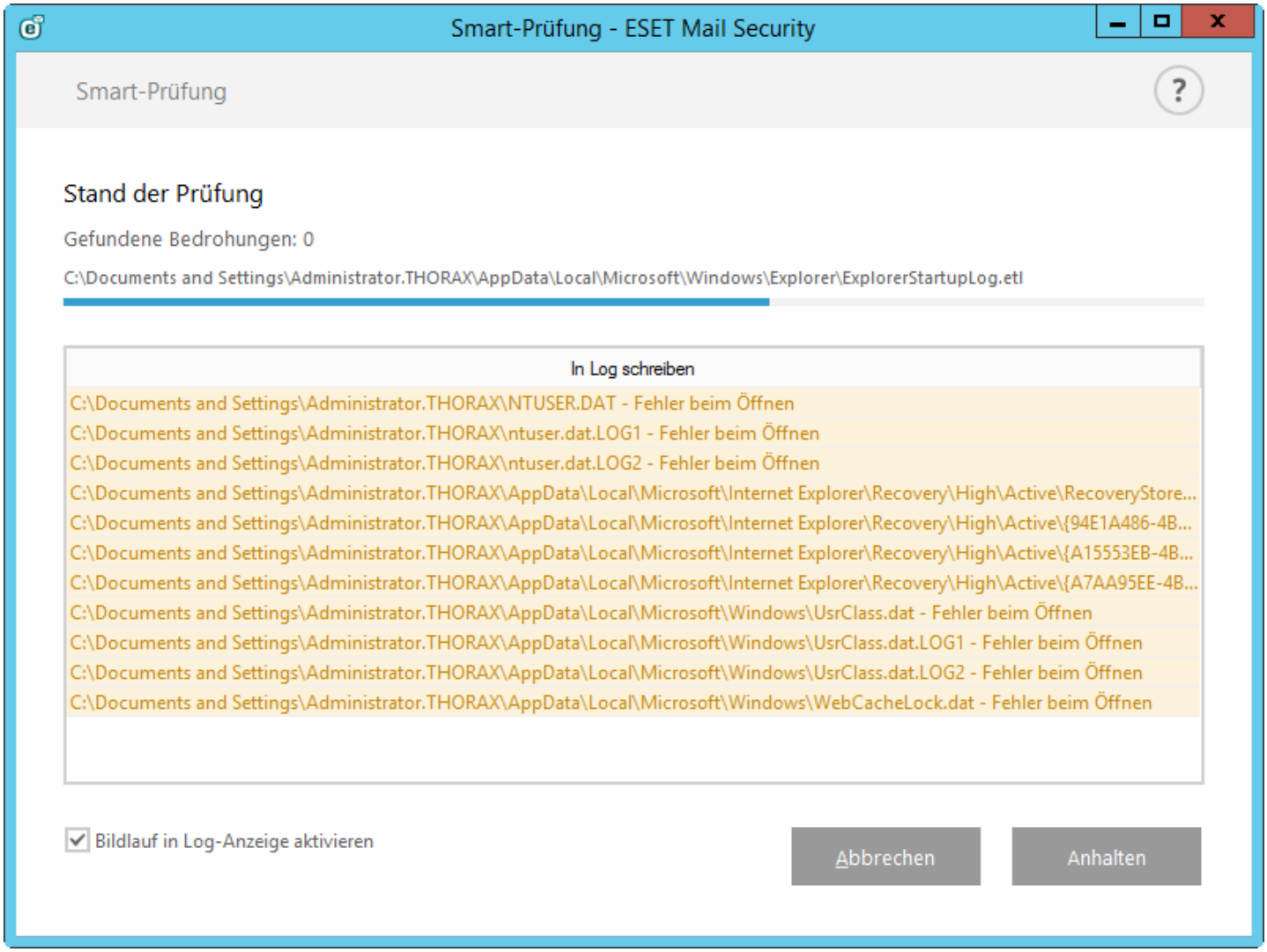
Klicken Sie auf **Speichern**, um die an den zu prüfenden Objekten vorgenommenen Änderungen zu speichern, einschließlich der Auswahl in der Baumstruktur.

Klicken Sie auf **Prüfen**, um die Prüfung mit den von Ihnen festgelegten Parametern auszuführen.

Mit der Schaltfläche **Als Administrator prüfen** können Sie die Prüfung mit dem Administratorkonto ausführen. Wählen Sie diese Option, wenn der aktuell angemeldete Benutzer keine ausreichenden Zugriffsrechte auf die zu prüfenden Dateien hat. Diese Schaltfläche ist nur verfügbar, wenn der aktuell angemeldete Benutzer UAC-Vorgänge als Administrator aufrufen kann.

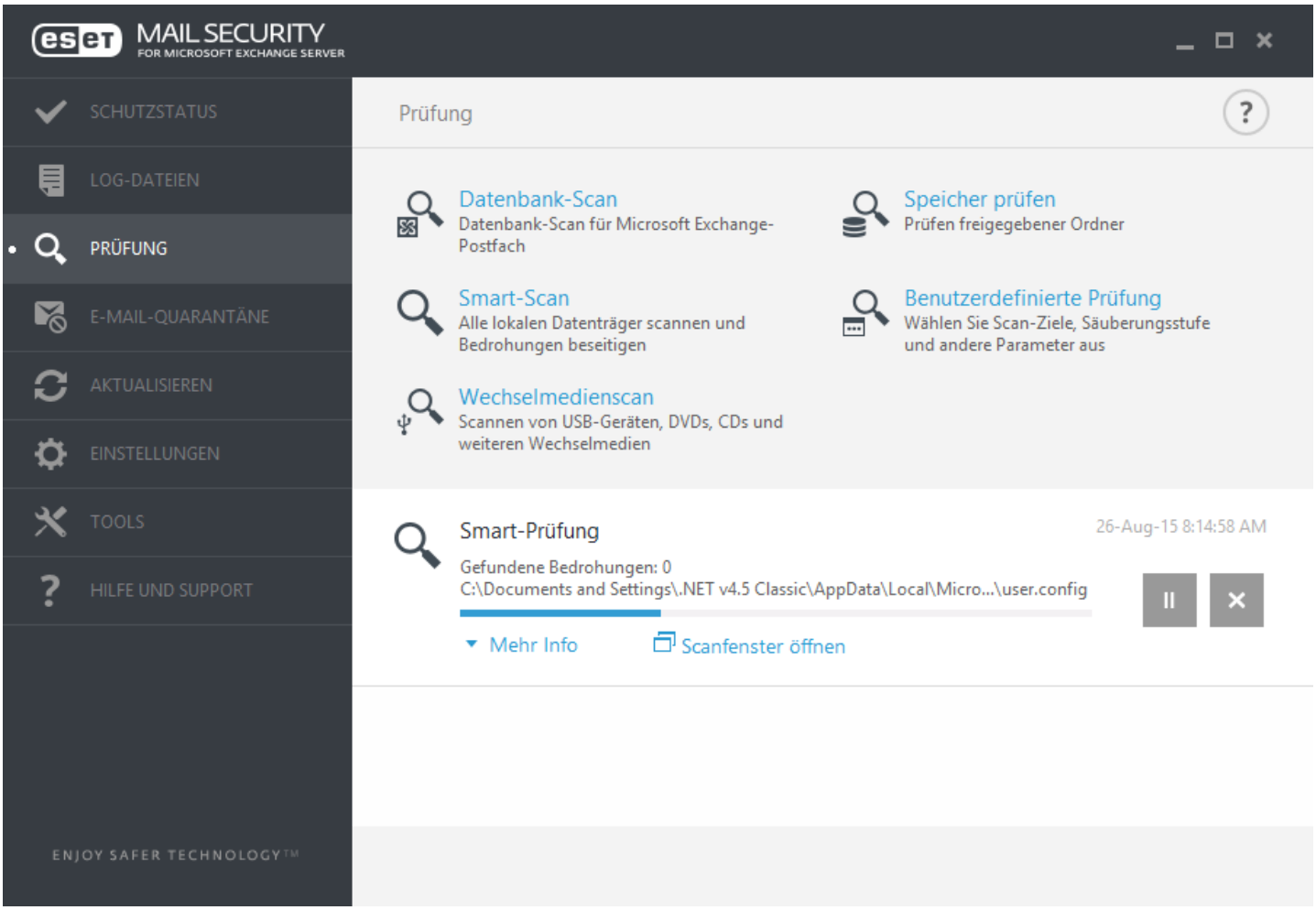
5.2.7.2 Stand der Prüfung

Die Fortschrittsanzeige enthält den aktuellen Stand der Prüfung und die Anzahl der bisher gefundenen infizierten Dateien.



HINWEIS: 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.

Stand der Prüfung - Die Fortschrittsanzeige zeigt den Status der bereits geprüften Objekte in Bezug auf die noch zu prüfenden Objekte an. Der Status für den Stand der Prüfung ergibt sich aus der Gesamtzahl der Objekte, die in die Prüfung einbezogen werden.
Zu prüfende Objekte - Der Name und Speicherort des aktuell geprüften Objekts werden angezeigt.
Bedrohungen erkannt - Die Gesamtzahl der Bedrohungen, die während einer Prüfung erkannt wurden, wird angezeigt.
Anhalten - Unterbrechen der Prüfung.
Fortsetzen - Diese Option ist wählbar, wenn die Prüfung angehalten wurde. Klicken Sie auf „Fortsetzen“, um mit der Prüfung fortzufahren.
Beenden - Beenden der Prüfung.
Bildlauf in Log-Anzeige aktivieren - Wenn diese Option aktiviert ist, fährt der Bildlauf automatisch nach unten, um die neuesten Einträge der sich verlängernden Liste anzuzeigen.



5.2.7.3 Profilmanager

An zwei Stellen von ESET Mail Security wird der Profilmanager verwendet: in den Bereichen **On-Demand-Scan** und **Update**.

On-Demand-Scan

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).

Um ein neues Profil zu erstellen, öffnen Sie das Fenster mit den erweiterten Einstellungen (F5) und klicken Sie auf **Computer** > > **On-Demand-Scan** und anschließend auf **Bearbeiten** neben der **Liste der Profile**. Das daraufhin geöffnete Dropdown-Menü **Ausgewähltes Profil** enthält die vorhandenen Prüfprofile. Eine Beschreibung der einzelnen Prüfeinstellungen finden Sie im Abschnitt Einstellungen für ThreatSense. So können Sie ein Prüfprofil erstellen, das auf Ihre Anforderungen zugeschnitten ist.

Beispiel: Nehmen wir an, Sie möchten Ihr eigenes Prüfprofil erstellen. Die Standardprüfung eignet sich in gewissem Maße, aber Sie möchten nicht die laufzeitkomprimierten Dateien oder potenziell unsichere Anwendungen prüfen. Außerdem möchten Sie die Option **Immer versuchen, automatisch zu entfernen** anwenden. Geben Sie den Namen des neuen Profils in das Fenster **Profilmanager** ein und klicken Sie auf **Hinzufügen**. Wählen Sie das neue Profil aus der Dropdown-Liste **Ausgewähltes Profil** aus, passen Sie die verbleibenden Parameter entsprechend Ihren Anforderungen an und klicken Sie auf **OK**, um das neue Profil zu speichern.

Update

Mit dem Profil-Editor unter „Einstellungen für Updates“ können Benutzer neue Update-Profile erstellen. Das Erstellen und Verwenden eigener benutzerdefinierter Profile (d. h. anderer Profile als das standardmäßige **Mein Profil**) ist nur sinnvoll, wenn Ihr Computer auf mehrere Verbindungsarten zurückgreifen muss, um eine Verbindung zu den Update-Servern herzustellen.

Nehmen wir als Beispiel einen Laptop, dessen Updates normalerweise über einen lokalen Server (einen sogenannten Mirror) im lokalen Netzwerk erfolgen, der aber seine Updates direkt von den ESET-Update-Servern bezieht, wenn keine Verbindung zum lokalen Netzwerk hergestellt werden kann (z. B. auf einer Geschäftsreise). Dieser Laptop kann zwei Profile haben: das erste Profil für die Verbindung zum lokalen Server, das zweite Profil für die Verbindung zu den ESET-Servern. Sobald diese Profile eingerichtet sind, wählen Sie **Tools** > **Taskplaner** und bearbeiten Sie die Update-Task-Einstellungen. Legen Sie eines der Profile als primäres Profil fest, das andere als sekundäres Profil.

Ausgewähltes Profil - Das momentan verwendete Update-Profil. Um es zu ändern, wählen Sie ein Profil aus dem Dropdown-Menü aus.

Profilliste - Dient der Erstellung neuer oder der Bearbeitung von aktualisierten Profilen.

5.2.7.4 Zu prüfende Objekte

Im Fenster mit den zu scannenden Objekten können Sie definieren, welche Objekte (Arbeitsspeicher, Laufwerke, Dateien und Ordner) auf Schadcode gescannt werden. Wählen Sie die zu scannenden Objekte aus der Baumstruktur aus, in der alle auf dem Computer verfügbaren Ordner aufgelistet werden. Im Dropdown-Menü **Zu scannende Objekte** können Sie vordefinierte Optionen für die zu scannenden Objekte auswählen.

- **Nach Profileinstellungen** - Im Scan-Profil festgelegte Ziele
- **Wechselmedien** - Disketten, USB-Speichergeräte, CDs/DVDs
- **Lokale Laufwerke** - Alle lokalen Systemlaufwerke
- **Netzlaufwerke** - Alle zugeordneten Netzlaufwerke
- **Freigegebene Ordner** - Alle freigegebenen Ordner auf dem lokalen Server
- **Keine Auswahl** - Bricht die Zielauswahl ab

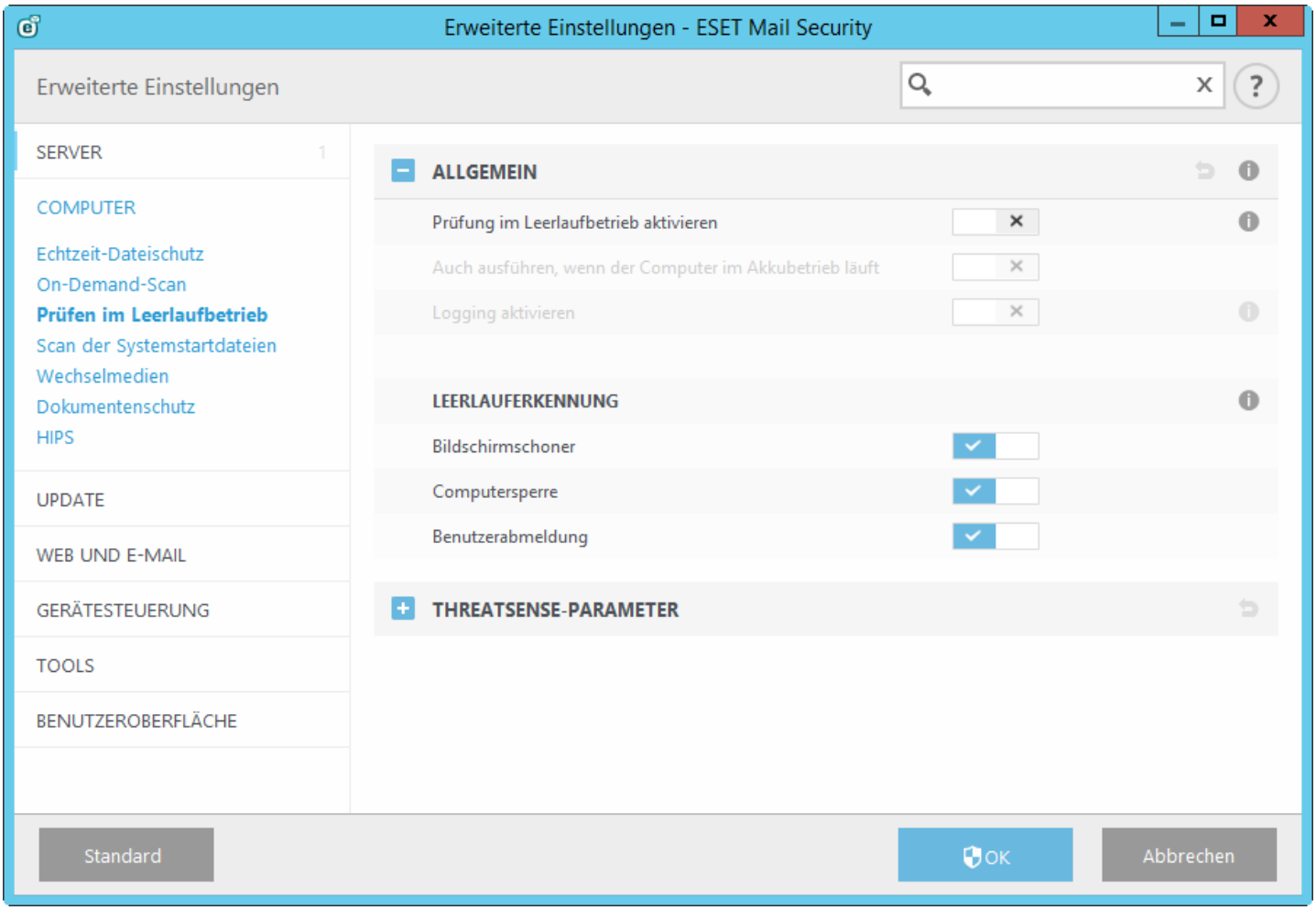
5.2.7.5 Geplanten Scan anhalten

Sie können einen geplanten Scan verschieben. Wenn Sie den Scan des Computers verschieben möchten, legen Sie die Option **Geplanten Scan beenden in (Minuten)** fest.

5.2.8 Prüfen im Leerlaufbetrieb

Sie können die Prüfung im Leerlaufbetrieb in den **Erweiterten Einstellungen** unter **Computer** > **Prüfen im Leerlaufbetrieb** > **Einfach**. Stellen Sie den Schalter neben **Prüfung im Leerlaufbetrieb aktivieren** auf „Ein“, um diese Funktion zu aktivieren. Wenn der Computer im Leerlauf ist, wird auf allen lokalen Festplatten eine Prüfung ausgeführt.

Diese Prüfung wird nicht ausgeführt, wenn sich der Computer (Notebook) im Batteriebetrieb befindet. Sie können diese Einstellung überschreiben, indem Sie das Kontrollkästchen neben **Auch ausführen, wenn der Computer im Batteriebetrieb ausgeführt wird** in den erweiterten Einstellungen aktivieren.



Aktivieren Sie **Erstellen von Logs aktivieren** in den erweiterten Einstellungen, um die Ausgabe einer Computerprüfung in den Log-Dateien abzulegen (Klicken Sie im Hauptprogrammfenster auf **Tools** > **Log-Dateien** und wählen Sie **Scannen des Computers** im Dropdown-Menü **Log** aus).

Die Prüfung im Leerlaufbetrieb erfolgt, wenn sich der Computer im folgenden Zustand befindet:

- Bildschirm ausgeschaltet oder Bildschirmschoner
- Computersperre
- Benutzerabmeldung

Klicken Sie auf Einstellungen für ThreatSense, um die Einstellungen (z. B. die Erkennungsmethoden) für das Scannen im Leerlaufbetrieb zu ändern.

5.2.9 Scan der Systemstartdateien

Die automatische Prüfung der Systemstartdateien wird standardmäßig beim Systemstart und beim Update der Signaturdatenbank ausgeführt. Die Ausführung des Scans ist abhängig davon, wie der Taskplaner konfiguriert ist und welche Tasks eingerichtet wurden.

Die Optionen der Systemstartprüfung sind Bestandteil des Task **Scan der Systemstartdateien** im Taskplaner. Navigieren Sie zum Ändern der Einstellungen für den Systemstart-Scan zu **Tools** > **Taskplaner** und klicken Sie auf **Scan Systemstartdateien** und anschließend auf **Bearbeiten**. Nach dem letzten Schritt wird das Fenster Prüfung Systemstartdateien angezeigt. (Weitere Informationen finden Sie im nächsten Kapitel.)

Detaillierte Anweisungen zum Erstellen und Verwalten von Tasks im Taskplaner finden Sie unter Erstellen neuer Tasks.

5.2.9.1 Prüfung Systemstartdateien

Beim Erstellen eines geplanten Tasks für die Prüfung der Systemstartdateien stehen Optionen zum Anpassen der folgenden Parameter zur Verfügung:

Im Dropdown-Menü **Scan-Stufe** können Sie die Scan-Tiefe für Dateien festlegen, die beim Systemstart ausgeführt werden. Die Dateien werden auf Grundlage der folgenden Kriterien in aufsteigender Reihenfolge sortiert:

- **Nur die am häufigsten verwendeten Dateien** (kleinste Anzahl gescannter Dateien)
- **Häufig verwendete Dateien**
- **Regelmäßig verwendete Dateien**
- **Selten verwendete Dateien**
- **Alle registrierten Dateien** (größte Anzahl gescannter Dateien)

Außerdem stehen zwei besondere Gruppen für die **Scan-Stufe** zur Verfügung:

- **Dateien, die vor der Benutzeranmeldung gestartet werden** - Enthält Dateien von Standorten, auf die ohne Benutzeranmeldung zugegriffen werden kann (umfasst nahezu alle Systemstartstandorte wie Dienste, Browserhilfsobjekte, Windows-Anmeldungshinweise, Einträge im Windows-Taskplaner, bekannte DLL-Dateien usw.).
- **Dateien, die nach der Benutzeranmeldung gestartet werden** - 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.

5.2.10 Wechselmedien

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.

Aktion nach Einlegen von Wechselmedien - Wählen Sie die Aktion, die standardmäßig ausgeführt werden soll, wenn ein Wechselmedium in den Computer eingelegt wird (CD/DVD/USB). Wenn die Option **Scanoptionen anzeigen** aktiviert ist, wird ein Hinweisfenster angezeigt, in dem Sie eine Aktion wählen können:

- **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.
- **Scanoptionen anzeigen** - Öffnet die Einstellungen für Wechselmedien.

Beim Einlegen eines Wechselmediums wird folgender Dialog angezeigt:

- **Jetzt scannen** - Dies löst den Wechselmedien-Scan aus.
- **Später scannen** - Der Wechselmedien-Scan wird auf einen späteren Zeitpunkt verschoben.
- **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.

Zusätzlich bietet ESET Mail Security die Funktion der Medienkontrolle, mit der Sie Regeln für die Nutzung externer Geräte mit einem bestimmten Computer festlegen können. Weitere Informationen zur Medienkontrolle finden Sie im Abschnitt Medienkontrolle.

5.2.11 Dokumentenschutz

Die Dokumentenschutzfunktion überprüft Microsoft Office-Dokumente vor dem Öffnen und 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.

- Die Option **Systemintegration** aktiviert das Schutzmodul. Um diese Option zu bearbeiten, öffnen Sie das Fenster mit den erweiterten Einstellungen (F5) und klicken Sie auf **Computer** > **Dokumentenschutz** in den Erweiterten Einstellungen.

- Weitere Informationen zu den Einstellungen des Dokumentenschutzes finden Sie unter Threatsense-Parameter.

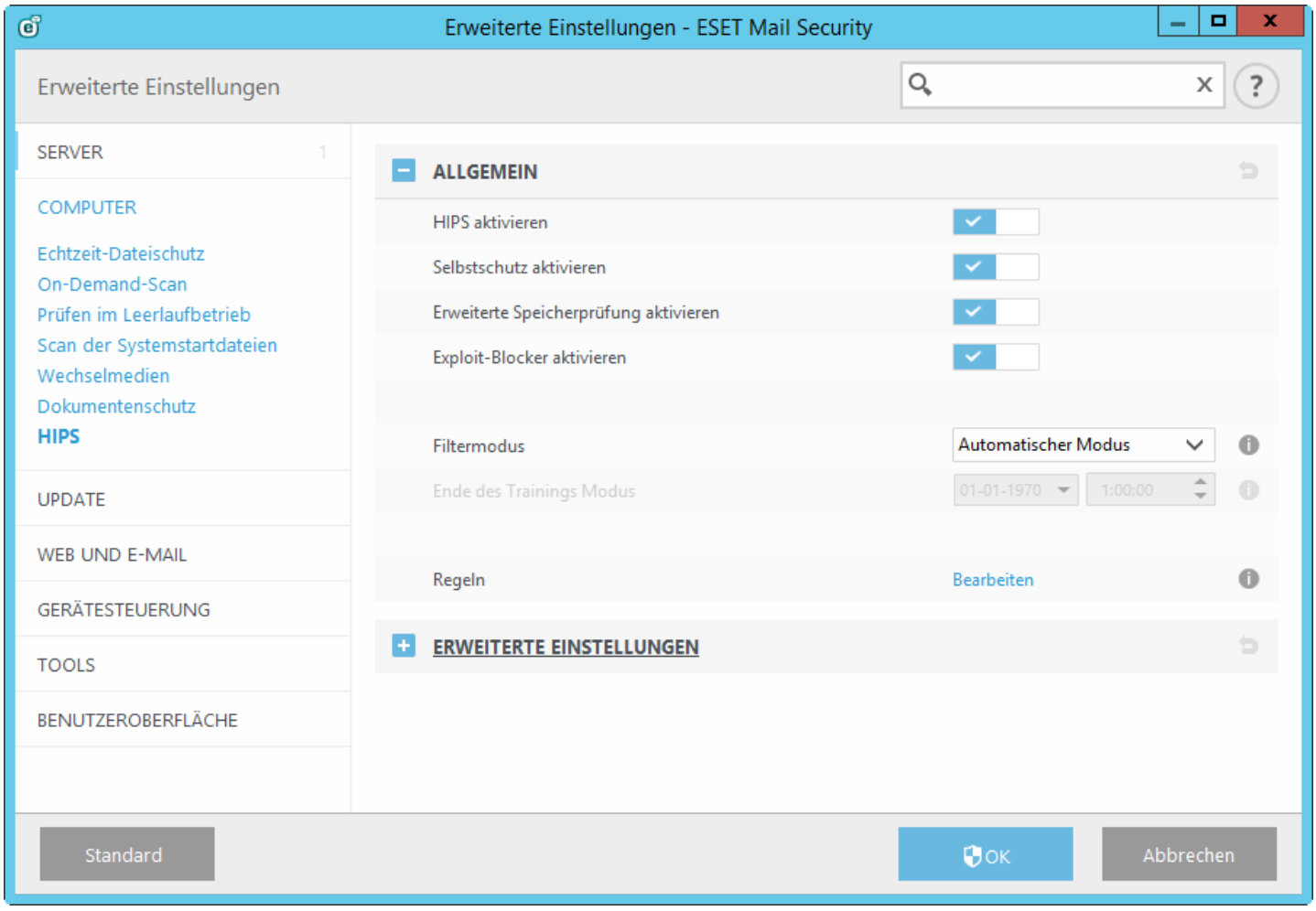
Die Funktion wird von Anwendungen aktiviert, die Microsoft Antivirus API verwenden (beispielsweise Microsoft Office 2000 und höher oder Microsoft Internet Explorer 5.0 und höher).

5.2.12 HIPS

Nur erfahrene Benutzer sollten die Einstellungen von HIPS ändern. Eine falsche Konfiguration der HIPS-Einstellungen kann zur Instabilität des Systems führen.

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.

Sie finden die HIPS-Einstellungen unter **Erweiterte Einstellungen** (F5) > **Computer** > **HIPS**. Der Status von HIPS (aktiviert/deaktiviert) wird im Hauptfenster von ESET Mail Security angezeigt, im Bereich **Einstellungen** rechts vom Bereich **Computer**.



ESET Mail Security bietet die integrierte *Selbstschutz*-Technologie, die Beschädigungen oder eine Deaktivierung Ihres Viren- und Spyware-Schutzes durch Schadsoftware verhindert. So ist Ihr System nie ungeschützt. Änderungen an den Optionen **HIPS aktivieren** und **Selbstschutz aktivieren** werden nach einem Neustart des Windows-Betriebssystems wirksam. Auch das Abschalten von **HIPS** erfordert einen Computer-Neustart.

Die Erweiterte Speicherprüfung bietet im Zusammenspiel mit dem Exploit-Blocker einen 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 dieser Art des Schutzes finden Sie in unserem Glossar.

Der **Exploit-Blocker** sichert besonders anfällige Anwendungstypen wie Webbrowser, PDF-Leseprogramme, E-Mail-Programme und MS Office-Komponenten ab. Der Exploit-Blocker ist standardmäßig aktiviert. Weitere Informationen zu dieser Art des Schutzes finden Sie in unserem Glossar.

Folgende vier Modi stehen für das Filtern zur Verfügung:

- **Automatischer Modus** - Vorgänge werden ausgeführt, mit Ausnahme der Vorgänge, die durch vorab definierte Regeln zum Schutz Ihres Systems blockiert wurden.
- **Smart-Modus** - Der Benutzer wird nur über sehr verdächtige Ereignisse benachrichtigt.
- **Interaktiver Modus** - Der Benutzer wird zur Bestätigung von Vorgängen aufgefordert.
- **Policy-basierter Modus** - Vorgänge werden blockiert.
- **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 Dropdown-Menü 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.

HIPS überwacht Ereignisse auf Betriebssystemebene und führt Aktionen gemäß Regeln aus, die den Regeln für die Personal Firewall ähneln. Klicken Sie auf **Bearbeiten**, um das Fenster zur HIPS-Regelverwaltung zu öffnen. Hier können Sie Regeln auswählen, erstellen, bearbeiten und löschen. Weitere Informationen zur Erstellung von Regeln und zu HIPS-Vorgängen finden Sie im Kapitel Regel bearbeiten.

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.

Über das 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. Die Einstellungen der einzelnen Parameter erfolgt unter **Optionen anzeigen**. 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 die Anzeige desselben Fenster auslösen.

Mit **Diese Aktion für Prozess vorübergehend anwenden** wird die Aktion (**Zulassen/Blockieren**) so lange angewendet, bis die Regeln oder der Filtermodus geändert werden, ein Update des HIPS-Moduls ausgeführt wird oder das System neu gestartet wird. Wenn eine dieser drei Aktionen (Regel- oder Filtermodusänderung, Update des HIPS-Moduls oder Neustart des Systems) ausgeführt wird, wird die vorübergehende Regel gelöscht.

5.2.12.1 HIPS-Regeln

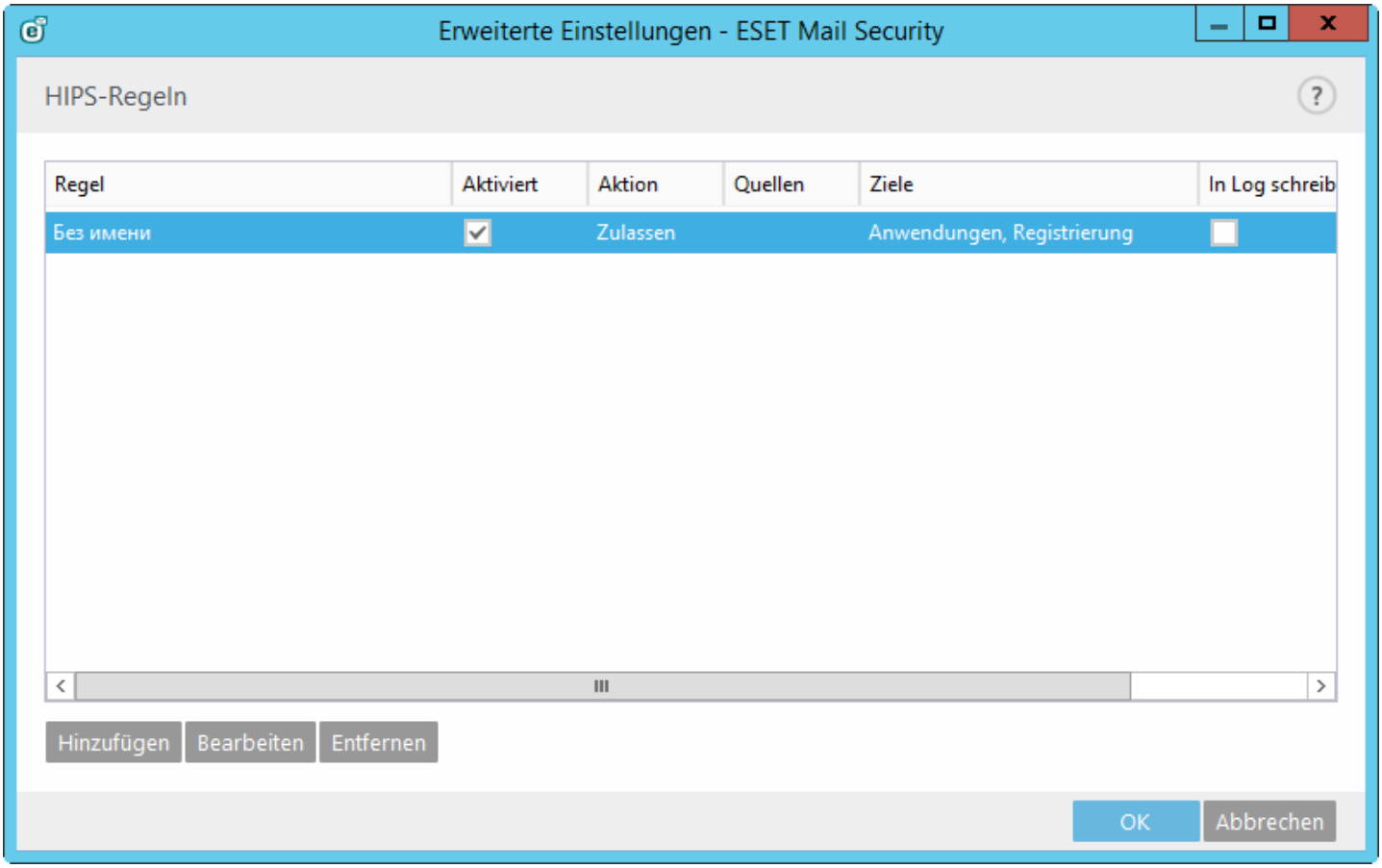
Dieses Fenster enthält eine Übersicht vorhandener HIPS-Regeln.

Spalten

Regel - Benutzerdefinierter oder automatisch ausgewählter Regelname.
Aktiviert - Deaktivieren Sie diesen Schalter, wenn Sie die Regel nicht verwenden, jedoch nicht aus der Liste löschen möchten.
Aktion - Mit der Regel wird eine Aktion festgelegt (**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 - Wenn Sie diese Option aktivieren, werden Informationen zu dieser Regel im HIPS-Log gespeichert.
Benachrichtigen - In der rechten unteren Ecke wird ein kleines Fenster angezeigt, wenn ein Ereignis ausgelöst wird.

Steuerelemente

Hinzufügen - Neue Regel erstellen
Bearbeiten - Ausgewählte Einträge bearbeiten
Entfernen - Ausgewählte Einträge entfernen



5.2.12.1.1 HIPS-Regeleinstellungen

- **Regelname** - Benutzerdefinierter oder automatisch ausgewählter Regelname.
- **Aktion** - Die Regel definiert eine Aktion (**Zulassen**, **Blockieren** oder **Fragen**), die ausgeführt wird, wenn die Bedingungen der Regel erfüllt sind.

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.

- **Dateien** - Die Regel wird nur angewendet, wenn sich der Vorgang auf eines dieser Ziele bezieht. Wählen Sie Bestimmte Dateien aus dem Dropdown-Menü aus und klicken Sie auf Hinzufügen, um neue Dateien oder Ordner hinzuzufügen. Sie können auch den Eintrag Alle Dateien aus dem Dropdown-Menü auswählen, um alle Anwendungen hinzuzufügen.
- **Anwendungen** - Die Regel wird nur angewendet, wenn das Ereignis von dieser/diesen Anwendung(en) ausgelöst wird. Wählen Sie Bestimmte Anwendungen aus dem Dropdown-Menü aus und klicken Sie auf Hinzufügen, um neue Dateien oder Ordner hinzuzufügen. Sie können auch den Eintrag Alle Anwendungen aus dem Dropdown-Menü auswählen, um alle Anwendungen hinzuzufügen.
- **Registrierungseinträge** - Die Regel wird nur angewendet, wenn sich der Vorgang auf eines dieser Ziele bezieht. Wählen Sie Bestimmte Einträge aus dem Dropdown-Menü aus und klicken Sie auf Hinzufügen, um neue Dateien oder Ordner hinzuzufügen. Sie können auch die Option Alle Einträge aus dem Dropdown-Menü auswählen, um alle Anwendungen hinzuzufügen.
- **Aktiviert** - Deaktivieren Sie diesen Schalter, wenn Sie die Regel nicht verwenden, jedoch nicht aus der Liste löschen möchten.
- **Log** - Wenn Sie diese Option aktivieren, werden Informationen zu dieser Regel im HIPS-Log gespeichert.
- **Benutzer benachrichtigen** - In der rechten unteren Ecke wird ein Popup-Fenster angezeigt, wenn ein Ereignis ausgelöst wird.

Die Regel besteht aus mehreren Teilen, mit denen die Auslösebedingungen der Regel beschrieben werden:

Quellanwendungen - Die Regel wird nur angewendet, wenn das Ereignis von einer dieser Anwendungen ausgelöst wird. Wählen Sie **Bestimmte Anwendungen** aus dem Dropdown-Menü aus und klicken Sie auf **Hinzufügen**, um neue Dateien oder Ordner hinzuzufügen. Mit dem Eintrag **Alle Anwendungen** im Dropdown-Menü können Sie alle Anwendungen hinzufügen.
Dateien - Die Regel wird nur angewendet, wenn sich der Vorgang auf eines dieser Ziele bezieht. Wählen Sie **Bestimmte Dateien** aus dem Dropdown-Menü aus und klicken Sie auf **Hinzufügen**, um neue Dateien oder Ordner hinzuzufügen. Mit dem Eintrag **Alle Dateien** im Dropdown-Menü können Sie alle Anwendungen hinzufügen.
Anwendungen - Die Regel wird nur angewendet, wenn sich der Vorgang auf eines dieser Ziele bezieht. Wählen Sie **Bestimmte Anwendungen** aus dem Dropdown-Menü aus und klicken Sie auf **Hinzufügen**, um neue Dateien oder Ordner hinzuzufügen. Mit dem Eintrag **Alle Anwendungen** im Dropdown-Menü können Sie alle Anwendungen hinzufügen.
Registrierungseinträge - Die Regel wird nur angewendet, wenn sich der Vorgang auf eines dieser Ziele bezieht. Wählen Sie **Bestimmte Einträge** aus dem Dropdown-Menü aus und klicken Sie auf **Hinzufügen**, um neue Dateien oder Ordner hinzuzufügen. Sie können auch die Option **Alle Einträge** aus dem Dropdown-Menü auswählen, um alle Anwendungen hinzufügen.

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.
- **Globalen Hook installieren** - Bezieht sich auf das Aufrufen der Funktion SetWindowsHookEx aus der MSDN-Bibliothek.
- **Treiber laden** - Installieren und Laden von Treibern im System.

Anwendungsbezogene Vorgänge

- **Andere Anwendung debuggen** - Verknüpfen eines Debuggers mit dem Prozess. Beim Debuggen einer Anwendung können Informationen zu deren Verhalten angezeigt und verändert werden. Ebenso ist der Zugriff auf die Daten der Anwendung möglich.
- **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 bzw. setzt ihn fort oder beendet ihn (direkter Zugriff aus dem Process Explorer oder im Bereich „Prozesse“ möglich).
- **Neue Anwendung starten** - Starten neuer Anwendungen oder Prozesse.
- **Zustand anderer Anwendung ändern** - Die Quellanwendung versucht, in den Speicher der Zielanwendung zu schreiben oder in ihrem Namen bestimmten Code auszuführen. Diese Funktion ist geeignet, um wichtige Anwendungen zu schützen, indem sie in einer Regel zum Blockieren des Vorgangs als Zielanwendungen konfiguriert werden.

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.
- **Registrierungsinhalte löschen** - Registrierungsschlüssel oder seinen 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.

HINWEIS: 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* kann zum Beispiel *HKEY_USERS\.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. Enthält ein Registrierungspfad *, bedeutet dies „dieser Pfad oder jeder untergeordnete Pfad nach diesem Symbol“. Platzhalter können nur auf diese Weise für Zieldateien verwendet werden. Erst wird der angegebene Teil des Pfades überprüft, dann der Pfad nach dem Platzhalter (*).


Wenn Sie eine sehr allgemeine Regel erstellen, wird eine Warnung zu dieser Art Regel angezeigt.

5.2.12.2 Erweiterte 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.

Alle blockierten Vorgänge in Log aufnehmen - Alle blockierten Vorgänge werden in den HIPS-Log geschrieben.

Änderungen an Autostart-Einträgen melden - Zeigt eine Desktopbenachrichtigung an, wenn eine Anwendung vom Systemstart entfernt bzw. zum Systemstart hinzugefügt wird.

Eine aktualisierte Version dieser Hilfeseite finden Sie im unserem Knowledgebase-Artikel.

5.2.12.2.1 Treiber dürfen immer geladen werden

In dieser Liste angezeigte Treiber werden unabhängig vom HIPS-Filtermodus immer zugelassen, sofern sie nicht ausdrücklich durch eine Benutzerregel blockiert werden.

Hinzufügen - Neuen Treiber hinzufügen.
Bearbeiten - Pfad eines ausgewählten Treibers bearbeiten.
Entfernen - Treiber aus der Liste entfernen.
Zurücksetzen - Systemtreiber werden erneut geladen.

HINWEIS: 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.

5.3 Update

Sie finden die Optionen für die Update-Einstellungen im Fenster **Erweiterte Einstellungen** (F5) unter **Update** > **Allgemein**. In diesem Bereich finden Sie Informationen zum Abruf von Updates, z. B. die Liste der Update-Server und die Anmeldedaten für diese Server.

Allgemein

Das aktuell verwendete Update-Profil wird im Dropdown-Menü **Ausgewähltes Profil** angezeigt. Zum Erstellen eines neuen Profils klicken Sie neben **Profilliste** auf **Bearbeiten**. Geben Sie den **Namen des Profils** ein und klicken Sie auf **Hinzufügen**.

Wenn Probleme mit einem Update auftreten, klicken Sie auf **Löschen**, um den temporären Update-Cache zu leeren.

Veraltete Signaturdatenbank

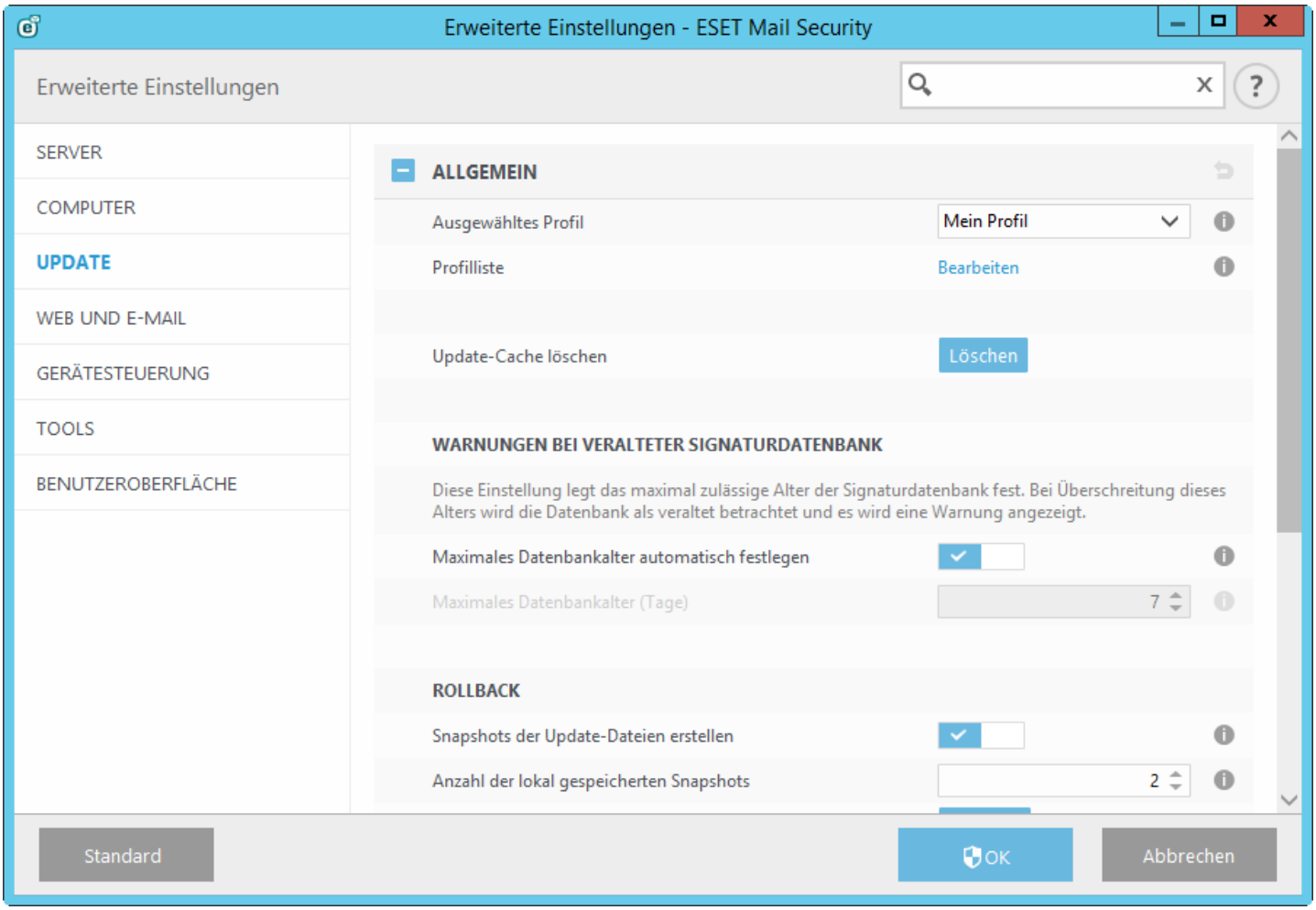
Maximales Datenbankalter automatisch festlegen - Hier können Sie eine Zeitdauer (in Tagen) festlegen, nach der die Signaturdatenbank spätestens als veraltet gemeldet wird. Der Standardwert ist 7.

Rollback

Wenn Sie befürchten, dass ein neues Update der Signaturdatenbank oder eines Programmmoduls korrupt 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 Signaturdatenbank und der Programmmodule zur späteren Verwendung mit der *Rollback*-Funktion auf. Um Snapshots der Signaturdatenbank zu erstellen, lassen Sie das Kontrollkästchen **Snapshots der Update-Dateien erstellen** aktiviert. Das Feld **Zahl der lokal gespeicherten Snapshots** legt fest, wie viele vorige Snapshots der Signaturdatenbank gespeichert werden.

Wenn Sie auf **Rollback ausführen** (**Erweiterte Einstellungen** (F5) > **Update** > **Allgemein**) klicken, müssen Sie im Dropdownmenü einen Zeitraum auswählen. Dieser Wert legt fest, wie lange die Updates der Signaturdatenbank und der Programmkomponenten ausgesetzt werden.



Damit Updates fehlerfrei heruntergeladen werden können, müssen Sie alle Uptdate-Einstellungen ordnungsgemäß eingeben. Falls Sie eine Firewall verwenden, stellen Sie sicher, dass das ESET-Programm Verbindungen mit dem Internet herstellen darf (zum Beispiel HTTP-Verbindungen).

Standardmäßig ist der **Update-Typ** (unter **Basis**) auf **Reguläres Update** eingestellt. So werden Updates automatisch von dem ESET-Server heruntergeladen, der am wenigsten belastet ist.

Basis

Benachrichtigungen über erfolgreiche Updates deaktivieren - Deaktiviert die Benachrichtigungen im Infobereich der Taskleiste rechts unten auf dem Bildschirm. Diese Option ist sinnvoll, wenn eine Anwendung im Vollbildmodus oder ein Spiel ausgeführt wird. Beachten Sie, dass die Anzeige von Benachrichtigungen im Präsentationsmodus deaktiviert ist.

Die Option **Update-Server** ist standardmäßig auf AUTOSELECT eingestellt. Der Update-Server dient als Speicher für die Updates. Es wird empfohlen, die Standardoption bei Verwendung eines ESET-Servers beizubehalten. Wenn Sie einen benutzerdefinierten Update-Server verwendet haben und wieder die Standardwerte einstellen möchten, geben Sie **AUTOSELECT** ein. ESET Mail Security Daraufhin wird der ESET-Updateserver automatisch ausgewählt.

Wenn Sie einen lokalen HTTP-Server (auch als „Update-Mirror“ bezeichnet) verwenden, konfigurieren Sie den Server wie folgt:
http://computername_oder_IP_adresse:2221

Wenn Sie einen lokalen HTTP-Server mit SSL verwenden, konfigurieren Sie den Server wie folgt:
https://computername_oder_IP_adresse:2221

Wenn Sie einen lokalen freigegebenen Ordner verwenden, konfigurieren Sie den Server wie folgt:
\\computername_oder_IP_adresse\freigegebener_ordner

Aktualisieren über einen Mirror

Zur Anmeldung beim Update-Server verwenden Sie den **Lizenzierungsschlüssel**, der beim Kauf erzeugt und Ihnen zugestellt wurde. Mit einem Mirror-Server können Sie Anmeldedaten festlegen, mit denen sich Clients beim Mirror-Server anmelden müssen, bevor sie Updates erhalten. Standardmäßig wird keine Anmeldung verlangt und die Felder **Benutzername** und **Passwort** bleiben leer.

5.3.1 Update-Rollback

Wenn Sie auf **Rollback ausführen** (**Erweiterte Einstellungen** (F5) > **Update** > **Profil**) klicken, müssen Sie im Dropdown-Menü einen Zeitraum auswählen. Dieser Wert legt fest, wie lange die Updates der Signaturdatenbank und der Programmkomponenten ausgesetzt werden.

Wählen Sie **Bis zur Aufhebung**, um keine regelmäßigen Updates auszuführen, bis die Update-Funktion manuell wieder aktiviert wird. Das Aktivieren dieser Option ist mit einem Sicherheitsrisiko verbunden und daher nicht empfehlenswert.

Die Version der Signaturdatenbank wird auf die älteste verfügbare Version herabgestuft und als Snapshot im lokalen Dateisystem des Computers gespeichert.

Beispiel: Die aktuellste Version der Signaturdatenbank ist beispielsweise 10646. Die Versionen 10645 und 10643 sind als Snapshots der Signaturdatenbank gespeichert. Die Version 10644 ist nicht verfügbar, weil der Computer beispielsweise eine Zeit lang heruntergefahren war und ein aktuelleres Update verfügbar war, bevor Version 10644 heruntergeladen wurde. Wenn Sie in das Feld **Zahl der lokal gespeicherten Snapshots** den Wert „2“ (zwei) eingegeben haben und auf **Rollback ausführen** klicken, wird die Version 10643 der Signaturdatenbank (und Programmmodule) wiederhergestellt. Dieser Vorgang kann einige Zeit in Anspruch nehmen. Überprüfen Sie, ob die Version der Signaturdatenbank im Hauptprogrammfenster von ESET Mail Security im Abschnitt Update herabgestuft wurde.

5.3.2 Update-Modus

Auf der Registerkarte **Update-Modus** finden Sie Optionen zum Aktualisieren der Programmkomponenten. Sie können festlegen, wie das Programm reagieren soll, wenn neue Updates für Programmkomponenten verfügbar sind.

Mit Updates für Programmkomponenten können neue Funktionen in das Programm integriert oder bestehende Funktionen modifiziert werden. Updates für Programmkomponenten können automatisch oder nach Bestätigung durch den Benutzer gestartet werden. Nach der Installation von Updates der Programmkomponenten muss der Computer möglicherweise neu gestartet werden. Im Abschnitt **Updates für Programmkomponenten** stehen drei Optionen zur Verfügung:

- **Benutzer fragen** - Dies ist die Standardoption. Stehen Updates für Programmkomponenten zur Verfügung, werden Sie aufgefordert, sie zu bestätigen oder abzulehnen.
- **Immer ausführen** - Updates zu Programmkomponenten werden heruntergeladen und automatisch installiert. Beachten Sie, dass nach der Installation von Programmkomponenten möglicherweise der Computer neu gestartet werden muss.
- **Niemals ausführen** - Es werden keine Updates für Programmkomponenten ausgeführt. Diese Option wird für Server empfohlen, da Server normalerweise nur im Rahmen geplanter Wartungsarbeiten neu gestartet werden dürfen.

HINWEIS: Die Auswahl der geeigneten Option hängt vom jeweiligen Computer ab, auf dem die Einstellungen ausgeführt werden. Beachten Sie die unterschiedliche Funktion von Arbeitsplatzcomputern und Servern. Das automatische Neustarten eines Servers nach einem Update kann beispielsweise schwerwiegende Folgen haben.

Wenn die Option **Vor dem Herunterladen von Updates fragen** aktiviert ist, wird eine Benachrichtigung angezeigt, wenn ein neues Update verfügbar ist.

Übersteigt die Größe des Updates den unter **Fragen, falls Update größer ist als (KB)** angegebene Wert, wird eine Benachrichtigung angezeigt.

5.3.3 HTTP-Proxy

Um auf die Optionen der Proxyserver-Einstellungen zuzugreifen, klicken Sie auf **Update** unter **Erweiterte Einstellungen** (F5). Klicken Sie dann auf **HTTP-Proxy**. Klicken Sie auf das Dropdown-Menü **Proxy-Modus** und wählen Sie eine der drei folgenden Optionen aus:

- Keinen Proxyserver verwenden
- Verbindung über Proxyserver
- In Systemsteuerung eingestellten Proxy verwenden

Mit dem Aktivieren der Option **In Systemsteuerung eingestellten Proxy verwenden** wird die in den erweiterten Einstellungen unter **Tools** > **Proxyserver** festgelegte Proxyserver-Konfiguration übernommen.

Mit der Option **Keinen Proxyserver verwenden** legen Sie fest, dass kein Proxyserver für Updates von ESET Mail Security genutzt wird.

Die Option **Verbindung über Proxyserver** sollten Sie wählen, wenn:

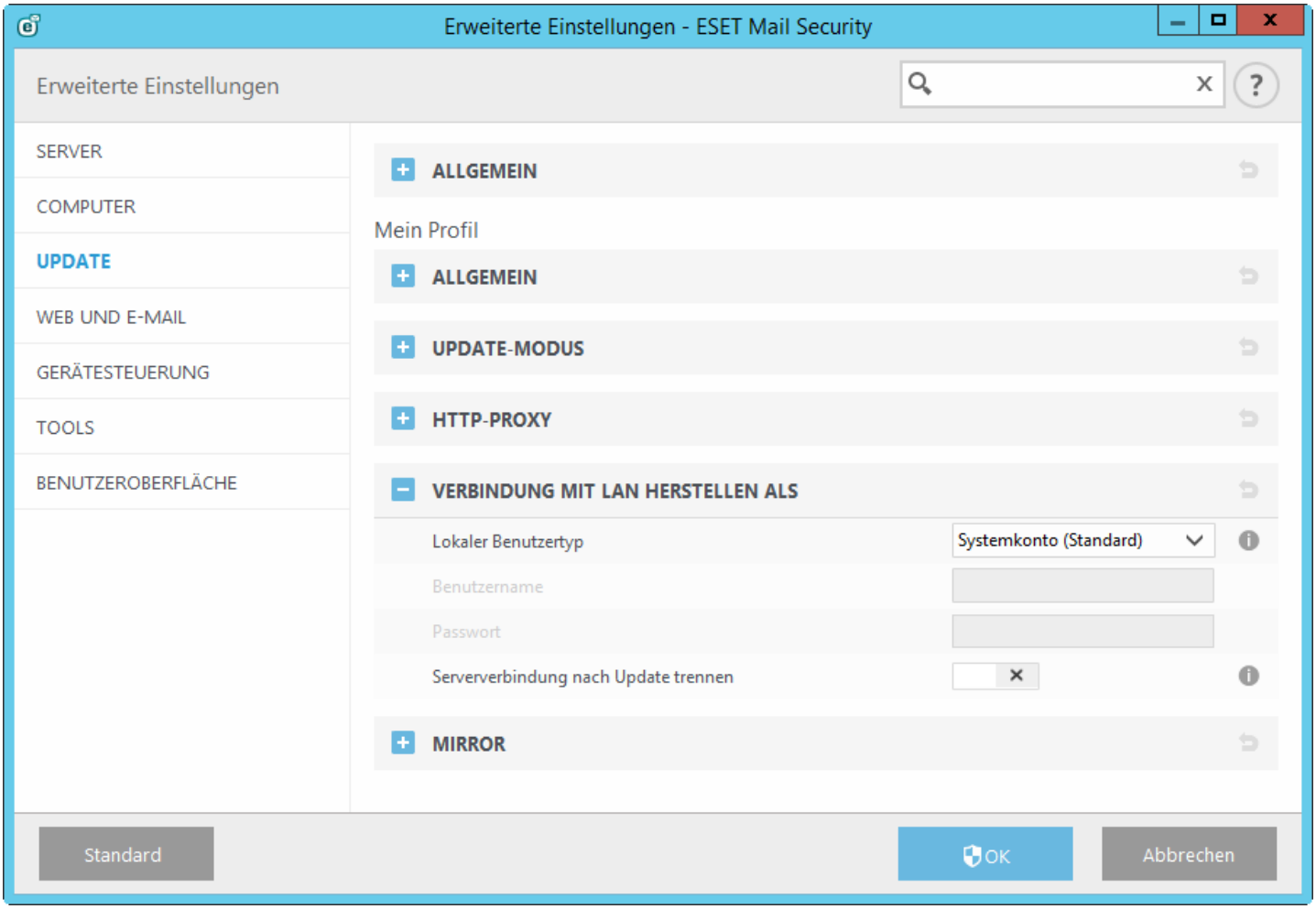
- Ein Proxyserver für Updates von ESET Mail Security benötigt wird, bei dem es sich nicht um den in den allgemeinen Einstellungen festgelegten Proxyserver handelt (**Tools** > **Proxyserver**). In diesem Fall sind an dieser Stelle Einstellungen erforderlich: **Proxyserver**-Adresse, Kommunikations-**Port** (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 über einen Proxyserver mit dem Internet verbunden ist. 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 Standardeinstellung für den Proxyserver ist **In Systemsteuerung eingestellten Proxy verwenden**.

HINWEIS: 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.

5.3.4 Verbindung mit LAN herstellen als

Beim Aktualisieren von einem lokalen Server mit einem Windows NT-Betriebssystem ist standardmäßig eine Authentifizierung für jede Netzwerkverbindung erforderlich.



Um ein entsprechendes Konto zu konfigurieren, treffen Sie im Dropdownmenü **Lokaler Benutzertyp** eine Auswahl:

- **Systemkonto (Standard)**
- **Aktueller Benutzer**
- **Folgender Benutzer**

Wählen Sie **Systemkonto (Standard)**, um das Systemkonto für die Authentifizierung zu verwenden. Normalerweise findet keine Authentifizierung statt, wenn in den Haupteinstellungen für Updates keine Anmeldedaten angegeben sind.

Wenn sich das Programm mit dem Konto des aktuell angemeldeten Benutzers anmelden soll, wählen Sie **Aktueller Benutzer**. Nachteil dieser Lösung ist, dass das Programm keine Verbindung zum Update-Server herstellen kann, wenn kein Benutzer angemeldet ist.

Wählen Sie **Folgender Benutzer**, wenn das Programm ein spezielles Benutzerkonto für die Authentifizierung verwenden soll. Verwenden Sie diese Option, wenn eine Anmeldung mit dem standardmäßigen Systemkonto nicht möglich ist. Beachten Sie, dass für das ausgewählte Benutzerkonto Zugriffsrechte auf den Ordner mit den Update-Dateien definiert sein müssen. Wenn keine Zugriffsrechte definiert sind, kann das Programm keine Updates abrufen.

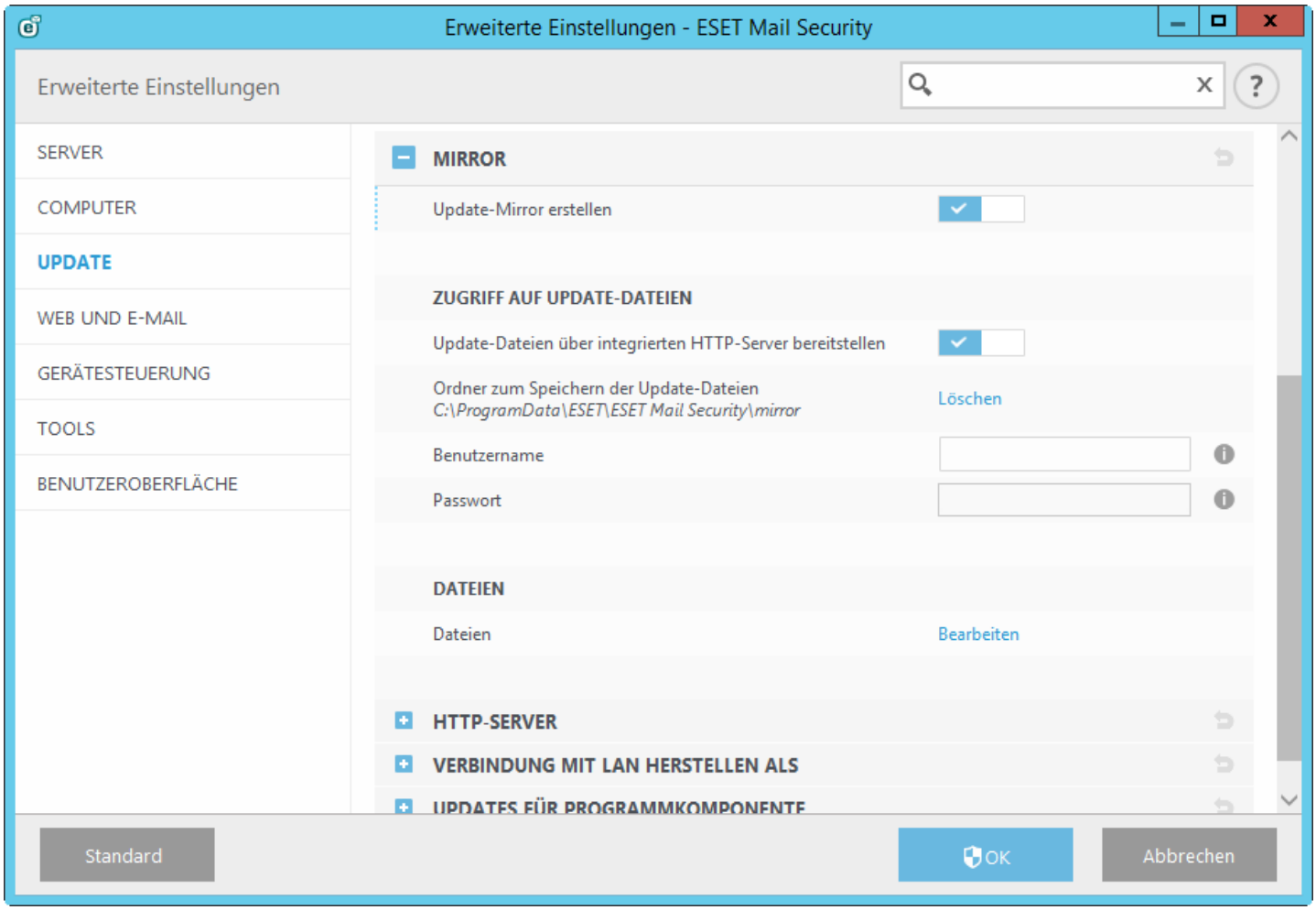
ACHTUNG: Wenn entweder **Aktueller Benutzer** oder **Folgender Benutzer** aktiviert ist, kann ein Fehler beim Wechsel der Identität zum gewünschten Benutzer auftreten. Aus diesem Grund wird empfohlen, die LAN-Anmeldedaten in den Haupteinstellungen für Updates einzugeben. In diesen Update-Einstellungen geben Sie die Anmeldedaten wie folgt ein: *Domänenname\Benutzer* (bei einer Arbeitsgruppe geben Sie *Arbeitsgruppenname\Name* ein) und das Passwort. Bei Aktualisierung von der HTTP-Version des lokalen Servers ist keine Authentifizierung erforderlich.

Aktivieren Sie die Option **Nach Update Verbindung zum Server trennen**, um das Trennen der Verbindung zu erzwingen, wenn die Verbindung zum Server nach dem Abrufen von Update-Dateien aktiv bleibt.

5.3.5 Update-Mirror

ESET Mail Security bietet Ihnen die Möglichkeit, Kopien der Update-Dateien zu erstellen. Diese können Sie dann zur Aktualisierung anderer Arbeitsstationen 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.

Konfigurationsoptionen für den lokalen Mirror-Server stehen in den erweiterten Einstellungen unter **Update** zur Verfügung. Zugriff auf diesen Bereich erhalten Sie, indem Sie die Taste **F5** drücken, auf Update klicken und die Registerkarte Mirror auswählen.



Um einen Mirror auf einem Clientcomputer zu erstellen, aktivieren Sie **Update-Mirror erstellen**. Durch Aktivieren dieser Option stehen weitere Konfigurationsoptionen für Update-Mirrors zur Verfügung, die beispielsweise die Art des Zugriffs auf Update-Dateien und den Pfad zu den Kopien der Update-Dateien betreffen.

Zugriff auf Update-Dateien

Dateien bereitstellen über integrierten HTTP-Server - Wenn dieses Kontrollkästchen aktiviert ist, können Update-Dateien über HTTP abgerufen werden. Hierzu sind keine Anmeldedaten erforderlich.

HINWEIS: Für Windows XP ist Service Pack 2 oder höher erforderlich, um den HTTP-Server zu verwenden.

Die Zugriffsmethoden auf den Mirror-Server sind unter Aktualisieren über Update-Mirror ausführlich beschrieben. Es gibt zwei Grundvarianten des Zugriffs auf einen Update-Mirror: Der Ordner mit den Update-Dateien kann eine Netzwerkfreigabe sein, oder der Zugriff auf den Update-Mirror auf einem HTTP-Server kann über Clients erfolgen.

Der für die Update-Dateien vorgesehene Ordner wird unter **Ordner zum Speichern der Update-Dateien** festgelegt. Klicken Sie auf **Ordner**, um den gewünschten Ordner auf dem lokalen Computer oder eine Netzwerkfreigabe auszuwählen. Wenn für den angegebenen Ordner eine Authentifizierung erforderlich ist, müssen die Anmeldedaten in die Felder **Benutzername** und **Passwort** eingegeben werden. Wenn sich der Speicherordner auf einem Windows NT/2000/XP-Netzlaufwerk befindet, wird ein Benutzerkonto mit Schreibzugriff auf den Ordner benötigt. Der Benutzername muss im Format *Domäne/Benutzer* oder *Arbeitsgruppe/Benutzer* eingegeben werden. Denken Sie daran, auch die entsprechenden Passwörter einzugeben.

Dateien - Bei der Konfiguration des Mirrors können Sie die Sprachversionen der herunterzuladenden Updates festlegen. Die ausgewählte Sprache muss vom konfigurierten Mirror-Server unterstützt werden.

HTTP-Server

Server-Port - Standardmäßig ist „2221“ als Server-Port festgelegt.

Authentifizierung - Dient zur Festlegung der Authentifizierungsmethode für den Zugriff auf die Update-Dateien. Die folgenden Optionen stehen zur Verfügung: **Keine**, **Basis** und **NTLM**. Wählen Sie **Basis** für Base64-Verschlüsselung und einfache Authentifizierung mit Benutzername und Passwort. 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.

Hängen Sie die **Zertifikatskettendatei** an oder generieren Sie ein eigensigniertes Zertifikat, wenn Sie den HTTP-Server mit HTTPS (SSL)-Unterstützung ausführen möchten. Folgende Zertifikattypen stehen zur Verfügung: ASN, PEM und PFX. 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.

Verbindung mit LAN herstellen als

Lokaler Benutzertyp - Die Einstellungen zu **Systemkonto (Standard)**, **Aktueller Benutzer** und **Folgender Benutzer** werden in den entsprechenden Dropdown-Menüs angezeigt. **Benutzername** und **Passwort** sind optional. Siehe auch Verbindung mit LAN herstellen als.

Aktivieren Sie die Option **Nach Update Verbindung zum Server trennen**, um das Trennen der Verbindung zu erzwingen, wenn die Verbindung zum Server nach dem Abrufen von Update-Dateien aktiv bleibt.

Update für Programmkomponente

Komponenten automatisch aktualisieren - Ermöglicht das Installieren neuer Funktionen sowie Updates zu bestehenden Funktionen. Updates für Programmkomponenten können automatisch oder nach Bestätigung durch den Benutzer gestartet werden. Nach der Installation von Updates der Programmkomponenten muss der Computer möglicherweise neu gestartet werden.

Komponenten jetzt aktualisieren - Hiermit werden die Programmkomponenten auf die neueste Version aktualisiert.

5.3.5.1 Aktualisieren über Update-Mirror

Es gibt zwei grundlegende Methoden zum Konfigurieren eines Mirrors. Ein Mirror ist im Grunde ein Repository, aus dem Clients Update-Dateien herunterladen können. Der Ordner mit den Update-Dateien kann als Netzwerkfreigabe oder als HTTP-Server dargestellt werden.

Zugriff auf den Update-Mirror über internen HTTP-Server

Diese Variante wird automatisch verwendet, da es sich um die Standardeinstellung des Programms handelt. Um Zugriff auf den Update-Mirror über den HTTP-Server zu ermöglichen, wechseln Sie zu **Erweiterte Einstellungen** > **Update** > **Mirror** und wählen Sie **Update-Mirror erstellen** aus.

Im Bereich **HTTP-Server** der Registerkarte **Update-Mirror** können Sie den **Server-Port** angeben, auf dem der HTTP-Server Anfragen empfängt, und den Typ der **Authentifizierung** festlegen, die vom HTTP-Server verwendet wird. Standardmäßig ist **2221** als Server-Port festgelegt. Unter **Authentifizierung** wird die Authentifizierungsmethode für den Zugriff auf die Update-Dateien festgelegt. Die folgenden Optionen stehen zur Verfügung: **Keine**, **Basis** und **NTLM**.

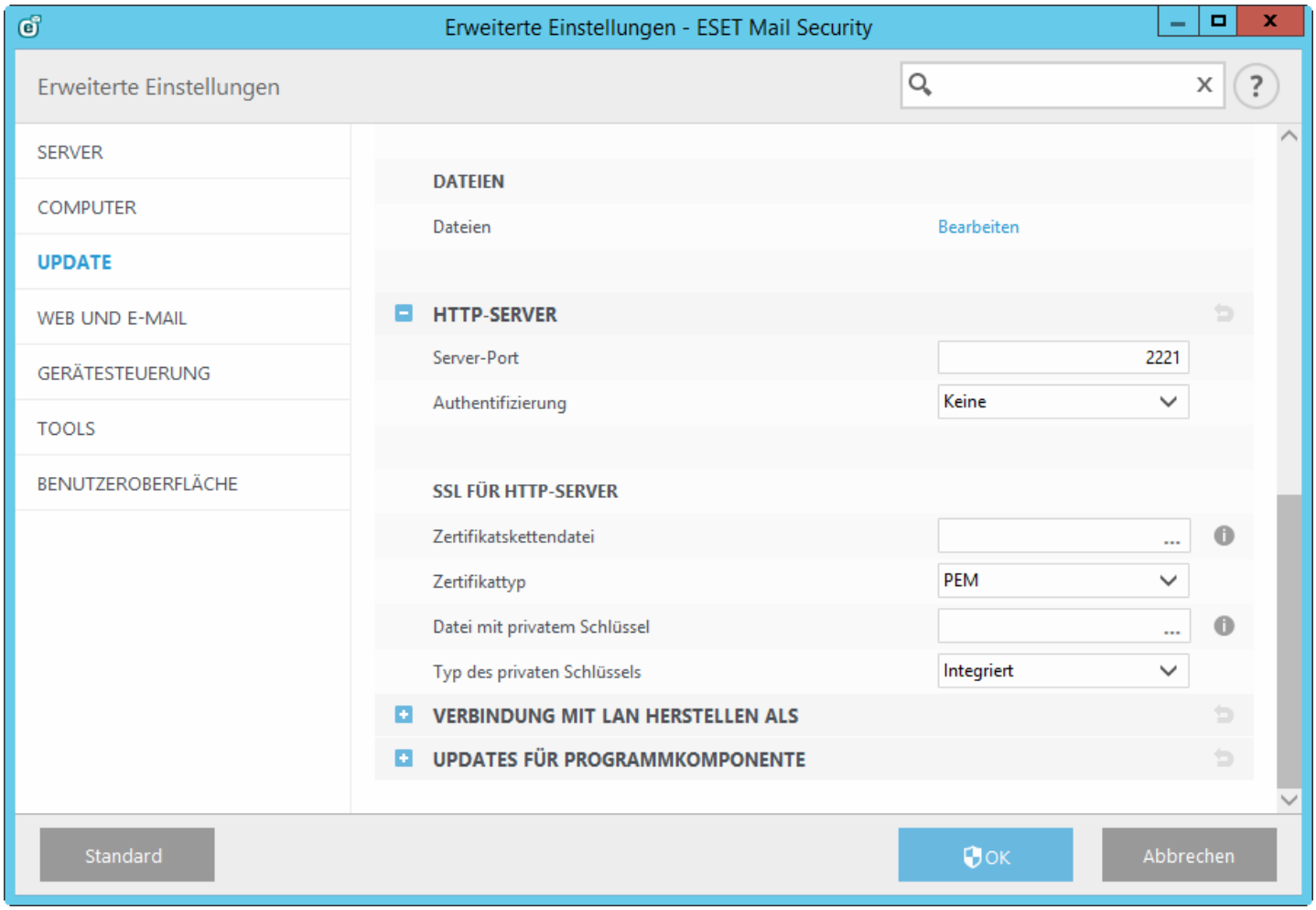
- Wählen Sie **Basis** für Base64-Verschlüsselung und einfache Authentifizierung mit Benutzername und Passwort.
- Bei Auswahl von **NTLM** wird eine sichere Verschlüsselungsmethode verwendet. Zur Authentifizierung wird der auf dem Computer erstellte Benutzer verwendet, der die Update-Dateien freigegeben hat.
- Die Standardeinstellung ist **Keine**, sodass für den Zugriff auf die Update-Dateien keine Authentifizierung erforderlich ist.

ACHTUNG: 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 eigensigniertes 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. **Typ des privaten Schlüssels** ist standardmäßig auf **Integriert** festgelegt, was bedeutet, dass der private Schlüssel Bestandteil der ausgewählten Zertifikatskettendatei ist.

HINWEIS: Nach mehreren erfolglosen Versuchen, die Signaturdatenbank über den Update-Mirror zu aktualisieren, wird im Update-Bereich im Hauptmenü der Fehler **Ungültiger Benutzername und/oder ungültiges Passwort** angezeigt. Navigieren Sie in diesem Fall zu **Erweiterte Einstellungen** > **Update** > **Mirror** und überprüfen Sie den Benutzernamen und das Passwort. Die häufigste Ursache für diesen Fehler sind falsch eingegebene Authentifizierungsdaten.



Nach Abschluss der Konfiguration des Mirror-Servers müssen Sie den neuen Update-Server auf Clientcomputern hinzufügen. Führen Sie dazu die folgenden Schritte aus:

- Klicken Sie unter **Erweiterte Einstellungen** (F5) auf **Update** > **Basis**.
- Deaktivieren Sie **Automatisch auswählen** und fügen Sie im Feld **Update-Server** einen neuen Server in einem der folgenden Formate hinzu:
  http://IP-Adresse_Ihres_Servers:2221
  https://IP_adresse_des_servers:2221 (bei Verwendung von SSL)

Zugriff auf den Update-Mirror über Systemfreigaben

Zunächst muss ein freigegebener Ordner auf einem lokalen Laufwerk oder auf einem Netzlaufwerk erstellt werden. Beim Erstellen des Ordners für den Update-Mirror ist Folgendes zu beachten: Der Benutzer, der Update-Dateien im Ordner speichert, benötigt Schreibzugriff (*„write“*), während die Benutzer, die ESET Mail Security über diesen Ordner aktualisieren, eine Leseberechtigung (*„read“*) benötigen.

Konfigurieren Sie als Nächstes den Zugriff auf den Update-Mirror im Bereich **Erweiterte Einstellungen** > **Update** > Registerkarte **Update-Mirror**, indem Sie die Option **Dateien über integrierten HTTP-Server bereitstellen** deaktivieren. Diese Option ist in der Standardeinstellung des Programms aktiviert.

Wenn der freigegebene Ordner sich auf einem anderen Computer im Netzwerk befindet, ist für den Zugriff auf den anderen Computer eine Authentifizierung erforderlich. Um die Anmeldedaten anzugeben, öffnen Sie **Erweiterte Einstellungen** (F5) von ESET Mail Security und klicken Sie auf **Update** > **Verbindung mit LAN herstellen als**. Diese Einstellung entspricht der Einstellung für Updates, wie im Kapitel Verbindung mit LAN herstellen als beschrieben.

Nach Abschluss der Konfiguration des Update-Mirrors geben Sie auf den Client-Arbeitsstationen jeweils *UNC**PFAD* als Update-Server ein. Gehen Sie hierbei folgendermaßen vor:

1. Klicken Sie in ESET Mail Security unter Erweiterte Einstellungen auf **Update** > **Basis**.
2. Klicken Sie auf **Update-Server** und fügen Sie unter Verwendung des Formats *UNC**PATH* einen neuen Server hinzu.

HINWEIS: Damit Updates fehlerfrei funktionieren, muss der Pfad zum Ordner mit den Kopien der Update-Dateien als UNC-Pfad angegeben werden. Updates über zugeordnete Netzlaufwerke können möglicherweise nicht ausgeführt werden.

Der letzte Bereich dient der Steuerung der Programmkomponenten (PCUs). Standardmäßig werden heruntergeladene Programmkomponenten zur Kopie auf den lokalen Update-Mirror vorbereitet. Wenn die Option **Updates für Programmkomponenten** aktiviert ist, ist es nicht erforderlich, auf **Update** zu klicken, da die Dateien bei ihrer Verfügbarkeit automatisch zum lokalen Update-Mirror kopiert werden. Weitere Informationen zu Updates von Programmkomponenten finden Sie unter Update-Modus.

5.3.5.2 Mirror-Dateien

Liste der verfügbaren und lokalisierten Programmkomponentendateien.

5.3.5.3 Fehlerbehebung bei Problemen mit Updates über Update-Mirror

Die meisten Probleme bei Updates von einem Update-Mirror haben eine oder mehrere der folgenden Ursachen: falsche Einstellungen für den Mirror-Ordner, falsche Anmeldedaten für den Mirror-Ordner, falsche Konfiguration auf lokalen Computern, die versuchen, Update-Dateien vom Update-Mirror herunterzuladen, oder eine Kombination der angegebenen Gründe. Hier erhalten Sie einen Überblick über die am häufigsten auftretenden Probleme bei Updates von einem Update-Mirror:

- **ESET Mail Security meldet einen Fehler bei der Verbindung mit dem Mirror-Server** - Wahrscheinlich wird dieser Fehler durch falsche Angaben zum Update-Server (Netzwerkpfad zum Mirror-Ordner) verursacht, von dem die lokalen Computer Updates herunterladen. Um den Ordner zu überprüfen, klicken Sie auf das Windows-Menü **Start** > **Ausführen**, geben Sie den Ordnernamen ein und klicken Sie auf **OK**. Daraufhin sollte der Inhalt des Ordners angezeigt werden.
- **ESET Mail Security verlangt einen Benutzernamen und ein Passwort** - Es wurden wahrscheinlich falsche Anmeldedaten (Benutzername und Passwort) im Bereich „Update“ angegeben. Benutzername und Passwort werden für den Zugriff auf den Update-Server verwendet, über den das Programm aktualisiert wird. Vergewissern Sie sich, dass die Anmeldedaten korrekt und im richtigen Format eingegeben sind. Verwenden Sie das Format *Domäne/Benutzername* bzw. *Arbeitsgruppe/Benutzername* und die entsprechenden Passwörter. Auch wenn der Zugriff auf den Mirror-Server für die Gruppe „Jeder“ gestattet wurde, sollten Sie bedenken, dass deshalb nicht jedem beliebigen Benutzer der Zugriff gewährt wird. „Jeder“ umfasst keine nicht autorisierten Benutzer, sondern bedeutet, dass alle Benutzer der Domäne auf den Ordner zugreifen können. Daher müssen, auch wenn die Gruppe „Jeder“ auf den Ordner zugreifen kann, in den Update-Einstellungen ein Domänen-Benutzername und -Passwort eingegeben werden.
- **ESET Mail Security meldet einen Fehler bei der Verbindung mit dem Mirror-Server** - Der für den Zugriff auf die HTTP-Version des Update-Mirrors angegebene Port ist blockiert.

5.3.6 So erstellen Sie Update-Tasks

Mit der Option **Update der Signaturdatenbank** können Updates manuell ausgeführt werden. Klicken Sie dazu im Hauptmenü auf **Update** und wählen Sie im daraufhin angezeigten Dialogfenster die entsprechende Option aus.

Darüber hinaus können Sie Updates auch als geplante Tasks einrichten. Um einen Task zu konfigurieren, klicken Sie auf **Tools** > **Taskplaner**. Standardmäßig sind in ESET Mail Security folgende Tasks aktiviert:

- **Automatische Updates in festen Zeitabständen**
- **Automatische Updates beim Herstellen von DFÜ-Verbindungen**
- **Automatische Updates beim Anmelden des Benutzers**

Jeder Update-Task kann bei Bedarf angepasst werden. Neben den standardmäßig ausgeführten Update-Tasks können zusätzliche Update-Tasks mit benutzerdefinierten Einstellungen erstellt werden. Weitere Informationen zum Erstellen und Konfigurieren von Update-Tasks finden Sie im Abschnitt Taskplaner in diesem Handbuch.

5.4 Web und E-Mail

Im Bereich **Web und E-Mail** können Sie den E-Mail-Schutz konfigurieren, Ihre Internetverbindung mittels Web-Schutz schützen und durch Konfiguration der Option Prüfen von Anwendungsprotokollen die entsprechenden Internetprotokolle wählen. Dies sind grundlegende Funktionen für den Schutz Ihres Computers, wenn Sie damit im Internet arbeiten.

Der **E-Mail-Schutz** überwacht den gesamten E-Mail-Verkehr, schützt vor Schadsoftware und bietet Ihnen eine Auswahl an Handlungsmöglichkeiten, wenn eine Infektion erkannt wurde.

Der **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.

Das **Prüfen von Anwendungsprotokollen** durch das ThreatSense-Modul bietet erweiterten Schutz für die verwendeten Anwendungsprotokolle. Die Prüfung findet automatisch statt, egal, ob ein Webbrowser oder ein E-Mail-Programm verwendet wird. Auch verschlüsselte Verbindungen (SSL/TLS) werden geprüft.

HINWEIS: Unter Windows Server 2008 und Windows Server 2008 R2 ist die Installation der Komponente **Web und E-Mail** standardmäßig deaktiviert. Wählen Sie den **Installationstyp** Benutzerdefiniert aus, um diese Funktion zu installieren. Falls Sie <%PN%> bereits installiert haben, können Sie das Installationsprogramm erneut ausführen, um Ihre Installation zu ändern und die Komponente Web und E-Mail hinzuzufügen.

5.4.1 Prüfen von Anwendungsprotokollen

Protokollprüfung

Das ThreatSense-Modul, in dem alle erweiterten Scan-Methoden integriert sind, bietet Virenschutz für Anwendungsprotokolle. Die Protokollprüfung ist unabhängig vom eingesetzten E-Mail-Programm oder Webbrowser. Sie können die Verschlüsselungs-Einstellungen (SSL) unter **Web und E-Mail** > **SSL/TLS** bearbeiten.

Prüfen von anwendungsspezifischen Protokollen aktivieren - Hiermit kann die Protokollprüfung deaktiviert werden. Bedenken Sie jedoch, dass zahlreiche Komponenten von ESET Mail Security wie Web-Schutz, E-Mail-Schutz und Phishing-Schutz von dieser Option abhängen und ohne sie nicht ordnungsgemäß funktionieren.

Ausgeschlossene Anwendungen - Ermöglicht das Ausschließen bestimmter Remoteadressen von der Protokollprüfung. Diese Option ist nützlich, wenn es aufgrund der Protokollprüfung zu Kompatibilitätsproblemen kommt.

Ausgeschlossene IP-Adressen - Ermöglicht das Ausschließen bestimmter Anwendungen von der Protokollprüfung. Diese Option ist nützlich, wenn es aufgrund der Protokollprüfung zu Kompatibilitätsproblemen kommt.

Web und E-Mail-Programme - Ermöglicht die Auswahl von Anwendungen, deren gesamter Datenverkehr unabhängig von den verwendeten Ports durch die Protokollprüfung geprüft wird (nur Windows-Betriebssysteme).

Aufzeichnung von Informationen für den ESET-Support zur Diagnose von Protokollfilterungsproblemen - Aktiviert die erweiterte Protokollierung von Diagnosedaten. Verwenden Sie diese Option nur, wenn Sie vom ESET-Support dazu aufgefordert werden.

5.4.1.1 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. Wir empfehlen, diese Option nur für Anwendungen zu aktivieren, deren Datenkommunikation nicht ordnungsgemäß funktioniert, wenn die Prüfung aktiviert ist.

Anwendungen und Dienste, die von der Protokollprüfung bereits betroffen waren, werden nach dem Klicken auf **Hinzufügen** automatisch angezeigt.

Bearbeiten - Bearbeiten von ausgewählten Einträgen in der Liste.

Entfernen - Entfernt ausgewählte Einträge aus der Liste.

5.4.1.2 Ausgeschlossene IP-Adressen

Die IP-Adressen in dieser Liste werden von der Prüfung von Protokollen ausgenommen. Die HTTP/POP3/IMAP-Datenkommunikation von/an die ausgewählten Adressen wird nicht auf Bedrohungen geprüft. Wir empfehlen, diese Option nur für Adressen zu aktivieren, die als vertrauenswürdig bekannt sind.

Hinzufügen - Hier können Sie eine IP-Adresse, einen Bereich von Adressen oder ein Subnetz für die Gegenstelle festlegen, die von der Regel erfasst wird.

Bearbeiten - Bearbeiten von ausgewählten Einträgen in der Liste.

Entfernen - Entfernt ausgewählte Einträge aus der Liste.

5.4.1.3 Webbrowser und E-Mail-Programme

HINWEIS: Ab Windows Vista Service Pack 1 und Windows Server 2008 wird zur Prüfung der Netzwerkkommunikation die neue Architektur der Windows-Filterplattform (WFP) verwendet. Da bei der WFP-Technologie spezielle Überwachungstechniken verwendet werden, steht hier der Abschnitt **Webbrowser und E-Mail-Programme** nicht zur Verfügung.

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.

5.4.2 SSL/TLS

ESET Mail Security kann Verbindungen, die das SSL/TLS-Protokoll verwenden, auf Bedrohungen untersuchen. Für die Untersuchung von durch 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 der Protokollfilter deaktiviert ist, werden SSL/TLS-Verbindungen nicht geprüft.

Für den SSL/TLS-Protokollfiltermodus sind folgende 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.

Verschlüsselte Kommunikation sperren, die das obsolete Protokoll SSL v2 verwendet - Verbindungen, die die frühere Version des SSL-Protokolls verwenden, werden automatisch blockiert.

Stammzertifikat

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 den Speicher der VSZS 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. Sie können die Option **Kommunikation blockieren, die das Zertifikat verwendet** aktivieren, um verschlüsselte Verbindungen zu der Site, die nicht verifizierte Zertifikate verwendet, immer zu beenden.

Wenn das Zertifikat ungültig oder beschädigt ist - Dies bedeutet, dass es entweder abgelaufen ist oder wurde fehlerhaft signiert wurde. In diesem Fall wird empfohlen, die Option **Kommunikation blockieren, die das Zertifikat verwendet** aktiviert zu lassen.

Mit der **Liste bekannter Zertifikate** können Sie das Verhalten von ESET Mail Security für bestimmte SSL-Zertifikate anpassen.

5.4.2.1 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 aufgefordert, die Option **Zulassen** oder **Blockieren** für die Verbindung auszuwählen.

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.

5.4.2.2 Liste bekannter Zertifikate

Mit der Liste bekannter Zertifikate können Sie das Verhalten von ESET Mail Security bei bestimmten SSL-Zertifikaten anpassen und gewählte Aktionen speichern, wenn der Modus „Interaktiv“ im Filtermodus für SSL-Protokoll ausgewählt ist. Sie können die Liste unter **Erweiterte Einstellungen** (F5) > **Web und E-Mail** > **SSL-Protokollprüfung** > **Liste bekannter Zertifikate** anzeigen und bearbeiten.

Das Fenster **Liste bekannter Zertifikate** besteht aus folgendem Inhalt:

Spalten

- **Name** - - 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.
- **Zugriff** - Wählen Sie **Zulassen** oder **Blockieren** als **Zugriffsaktion** aus, um die von diesem Zertifikat gesicherte Verbindung unabhängig von ihrer Vertrauenswürdigkeit zuzulassen oder zu blockieren. Wählen Sie **Autom.** aus, wennvertrauenswürdige Zertifikate zugelassen werden sollen und bei nicht vertrauenswürdigen nachgefragt werden soll. Wählen Sie **Nachfragen** aus, wenn der Benutzer immer gefragt werden soll, welche Maßnahme ergriffen werden soll.
- **Scannen** - Wählen Sie **Scannen** oder **Ignorieren** als **Scan-Aktion** aus, um die von diesem Zertifikat gesicherte Verbindung zu scannen oder zu ignorieren. Wählen Sie **Autom.**, wenn im automatischen Modus geprüft und im interaktiven Modus nachgefragt werden soll. Wählen Sie **Nachfragen** aus, wenn der Benutzer immer gefragt werden soll, welche Maßnahme ergriffen werden soll.

Steuerelemente

- **Bearbeiten** - Wählen Sie das zu konfigurierende Zertifikat aus und klicken Sie auf **Bearbeiten**.
- **Entfernen** - Wählen Sie das zu löschende Zertifikat aus und klicken Sie auf **Entfernen**.
- **OK/Abbrechen** - Klicken Sie auf **OK**, um die Änderungen zu speichern, oder auf **Abbrechen**, um den Vorgang ohne Speichern zu beenden.

5.4.3 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). Die Integrationseinstellungen befinden sich unter **Einstellungen** > **Erweiterte Einstellungen** > **Web und E-Mail** > **E-Mail-Schutz** > **E-Mail-Programme**.

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. Eine vollständige Liste der unterstützten E-Mail-Programme und Versionen finden Sie im entsprechenden ESET-Knowledgebase-Artikel.

Auch bei nicht aktivierter Integration ist die E-Mail-Kommunikation durch den E-Mail-Client-Schutz (POP3, IMAP) weiterhin geschützt.

Aktivieren Sie die Option **Prüfen neuer Elemente im Posteingang deaktivieren**, falls Sie während der Arbeit mit Ihrem E-Mail-Programm eine Systemverlangsamung bemerken (nur MS Outlook). Dies kann der Fall sein, wenn Sie E-Mails vom Kerio Outlook Connector Store abrufen.

Zu scannende E-Mails

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).

5.4.3.1 E-Mail-Protokolle

IMAP und POP3 sind die gängigsten Protokolle für den Empfang von E-Mail-Kommunikation in einer E-Mail-Clientanwendung. ESET Mail Security bietet Schutz für diese Protokolle, ganz gleich, welcher E-Mail-Client verwendet wird. Dieser braucht auch nicht neu konfiguriert zu werden.

Die IMAP/IMAPS- und POP3/POP3S-Protokollprüfung kann in den erweiterten Einstellungen konfiguriert werden. Zugriff auf diese Einstellung erhalten Sie über **Web und E-Mail** > **E-Mail-Schutz** > **E-Mail-Protokolle**.

ESET Mail Security unterstützt außerdem das Scannen 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.

Verschlüsselter Datenverkehr wird mit den Standardeinstellungen nicht gescannt. Sie können das Scannen von verschlüsseltem Datenverkehr in den erweiterten Einstellungen unter SSL/TLS-Protokollprüfung aktivieren. Klicken Sie dazu auf **Web und E-Mail** > **SSL/TLS** und wählen Sie **SSL-Protokollfilterung aktivieren** aus.

5.4.3.2 Warnungen und Hinweise

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 Signaturdatenbank statt. Das Scannen der POP3-Kommunikation erfolgt unabhängig vom verwendeten E-Mail-Programm.

Die Optionen für diese Funktion finden Sie unter **Erweiterte Einstellungen** unter **Web und E-Mail** > **E-Mail-Client-Schutz** > **Warnungen und Benachrichtigungen**.

Einstellungen für ThreatSense - In diesem Bereich finden Sie erweiterte Einstellungen für den Virenschutz. Hier können Sie Einstellungen für zu scannende Objekte, Erkennungsmethoden usw. festlegen. Klicken Sie, um die erweiterten Einstellungen für den Virenschutz anzeigen.

Nach erfolgter Prüfung kann ein Prüfhinweis mit dem Scan-Ergebnis zu der E-Mail-Nachricht hinzugefügt werden. Sie haben folgende Optionen: **Prüfhinweis zu eingehenden/gelesenen E-Mails hinzufügen, Prüfhinweis an den Betreff empfangener und gelesener infizierter E-Mails anhängen** oder **Prüfhinweis zu ausgehenden E-Mails hinzufügen**. 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. Folgende Optionen stehen zur Verfügung:

- **Nie** - Es werden keine Prüfhinweise zu E-Mails hinzugefügt.
- **Nur an infizierte E-Mails** - Prüfhinweise werden nur E-Mails hinzugefügt, in denen Schadcode erkannt wurde (Standardeinstellung).
- **Bei allen geprüften E-Mails** - Alle geprüften E-Mails werden mit Prüfhinweisen versehen.

Prüfhinweis an den Betreff gesendeter infizierter E-Mails anhängen - Deaktivieren Sie dieses Kontrollkästchen, wenn Prüfhinweise zu den Betreffzeilen infizierter E-Mails hinzugefügt werden sollen. Ohne großen Aufwand können Sie in Ihrem E-Mail-Programm eine Filterregel erstellen, die diesen Prüfhinweis erkennt (falls Ihr E-Mail-Programm Filterregeln unterstützt). Diese Funktion erhöht beim Empfänger auch die Glaubwürdigkeit von Nachrichten. Bei der Erkennung von eingedrungener Schadsoftware stehen wertvolle Informationen zur Verfügung, um den Bedrohungsgrad durch die Nachricht oder den Absender einzuschätzen.

Text, der zur Betreffzeile infizierter E-Mails hinzugefügt wird - Geben Sie hier den Text ein, der das Präfix in der Betreffzeile einer infizierten E-Mail ersetzen soll. Mit dieser Funktion wird der Nachrichtenbetreff *„Hallo“* mit dem voreingestellten Präfix *„[virus]“* folgendermaßen gekoppelt: *„[virus] Hallo“*. Dabei repräsentiert die Variable *%VIRUSNAME%* die erkannte Bedrohung.

5.4.3.3 Symbolleiste für MS Outlook

Die Sicherheitslösung für Microsoft Outlook ist ein Plug-In. Nach der Installation von ESET Mail Security wird Outlook Express um diese Symbolleiste mit den Virenschutz-Optionen erweitert:

ESET Mail Security - Mit einem Klick auf das Symbol wird das Hauptprogrammfenster von ESET Mail Security geöffnet.

E-Mails erneut scannen - Ermöglicht es Ihnen, den E-Mail-Scan manuell zu starten. Sie können E-Mails festlegen, die geprüft werden sollen. Außerdem können Sie das erneute Prüfen empfangener E-Mails aktivieren. Weitere Informationen hierzu finden Sie unter E-Mail-Schutz.

Scanner-Einstellungen - Anzeige der Optionen für den E-Mail-Schutz.

5.4.3.4 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 Outlook Express bzw. Windows Mail um diese Symbolleiste mit den Virenschutz-Optionen erweitert:

ESET Mail Security - Mit einem Klick auf das Symbol wird das Hauptprogrammfenster von ESET Mail Security geöffnet.

E-Mails erneut scannen - Ermöglicht es Ihnen, den E-Mail-Scan manuell zu starten. Sie können E-Mails festlegen, die geprüft werden sollen. Außerdem können Sie das erneute Prüfen empfangener E-Mails aktivieren. Weitere Informationen hierzu finden Sie unter E-Mail-Schutz.

Scanner-Einstellungen - Anzeige der Optionen für den E-Mail-Schutz.

Benutzeroberfläche

Anzeige anpassen - Die Anzeige der Symbolleiste kann für Ihr E-Mail-Programm geändert werden. Deaktivieren Sie die Option für die Anpassung der Anzeige unabhängig von den Parametern des E-Mail-Programms.

Symboltitel anzeigen - Anzeige der Beschreibung für Symbole.

Symboltitel rechts - Die Beschreibungen werden vom unteren zum seitlichen Bereich der Symbole verschoben.

Große Symbole - Anzeige großer Symbole für Menüeinstellungen.

5.4.3.5 Bestätigungsfenster

Mit dieser Benachrichtigung wird geprüft, ob die ausgewählte Aktion wirklich ausgeführt werden soll. Dadurch sollen mögliche Fehler vermieden werden.

Darüber hinaus bietet das Fenster die Option, die Anzeige von Bestätigungsfenstern zu deaktivieren.

5.4.3.6 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 scannen** bietet zwei Scan-Modi:

Alle E-Mails im aktuellen Ordner - Alle E-Mails im aktuell angezeigten Ordner werden gescannt.

Nur markierte E-Mails - Nur markierte E-Mails werden gescannt.

Das Kontrollkästchen **Bereits gescannte E-Mails erneut scannen** bietet dem Benutzer die Option eines erneuten Scans von bereits geprüften E-Mails.

5.4.4 Web-Schutz

Der Internetzugang ist eine Standardfunktion der meisten Computer. Leider ist diese technische Möglichkeit mittlerweile auch der wichtigste Weg zur Verbreitung von Schadsoftware. Der Web-Schutz besteht in der Überwachung der Kommunikation zwischen Webbrowsern und Remoteservern und entspricht den Regeln für HTTP (Hypertext Transfer Protocol) und HTTPS (verschlüsselte Kommunikation).

Der Zugriff auf Webseiten, die bekanntermaßen Schadcode enthalten, wird vor dem Herunterladen von Inhalt 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.

Es wird dringend empfohlen, den Web-Schutz stets aktiviert zu lassen. Sie finden diese Option im Hauptfenster von ESET Mail Security unter **Einstellungen** > **Computer** > **Web-Schutz**.

In **Erweiterte Einstellungen** (F5) > **Web und E-Mail** > **Web-Schutz** stehen die folgenden Optionen zur Verfügung:

- **Einfach** - Hier können Sie den gesamten Web-Schutz aktivieren oder deaktivieren. Bei deaktiviertem Web-Schutz werden die folgenden Optionen deaktiviert.

- **Web-Protokolle** - Hier können Sie die Überwachung dieser von den meisten Internetbrowsern verwendeten Standardprotokolle konfigurieren.
- **URL-Adressverwaltung** - Hier können Sie festlegen, welche HTTP-Adressen blockiert, zugelassen oder von der Prüfung ausgeschlossen werden sollen.
- **Einstellungen für ThreatSense** - In diesem Bereich finden Sie erweiterte Einstellungen für den Virenschutz. Hier können Sie Einstellungen für zu prüfende Objekte (E-Mails, Archive usw.), Erkennungsmethoden für den Web-Schutz usw. festlegen.

Webprotokolle

ESET Mail Security ist standardmäßig so konfiguriert, dass das von den meisten Internetbrowsern verwendete HTTP-Protokoll überwacht wird.

Unter Windows Vista und neuer werden HTTP-Verbindungen immer an allen Ports in allen Anwendungen überwacht. Unter Windows XP/2003 können Sie die vom HTTP-Protokoll verwendeten Ports in **Erweiterte Einstellungen** (F5) > **Web und E-Mail** > **Web-Schutz** > **Web-Protokolle** > **Einstellungen für den HTTP-Scanner** ändern. HTTP-Verbindungen werden an den angegebenen Ports in allen Anwendungen sowie an allen Ports zu Anwendungen überwacht, die als Web- und E-Mail-Clients markiert sind.

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 von verschlüsseltem Datenverkehr in den erweiterten Einstellungen unter SSL-Protokollprüfung aktivieren. Klicken Sie hierzu auf **Web und E-Mail** > **SSL-Protokollprüfung** und wählen Sie **SSL-Protokollfilterung aktivieren**.

5.4.4.1 Einfach

Hier können Sie den **Web-Schutz** aktivieren (Standard) oder deaktivieren. Bei deaktiviertem Web-Schutz werden die folgenden Optionen deaktiviert.

HINWEIS: Es wird dringend empfohlen, den Web-Schutz stets aktiviert zu lassen. Sie finden diese Option auch im Hauptfenster von ESET Mail Security unter **Einstellungen** > **Computer** > **Web-Schutz**.

5.4.4.2 URL-Adressverwaltung

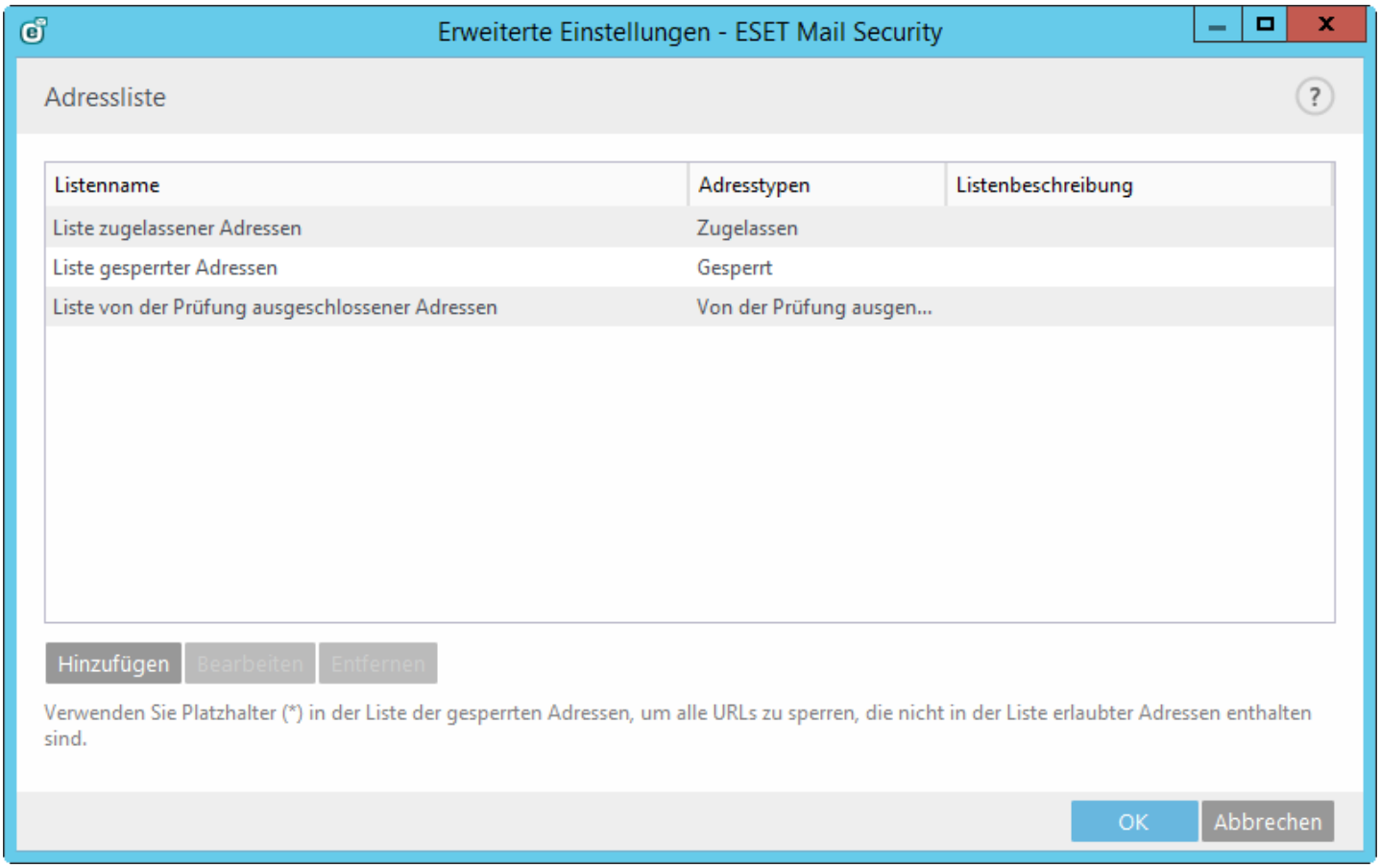
Im Bereich URL-Adressverwaltung können Sie festlegen, welche HTTP-Adressen blockiert, zugelassen oder von der Prüfung ausgeschlossen werden sollen.

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, muss die Option SSL/TLS-Protokollfilterung aktivieren aktiviert sein. Andernfalls werden nur die Domänen besuchter HTTPS-Sites hinzugefügt, nicht aber die URL.

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.



Hinzufügen - Erstellen einer neuen Liste zusätzlich zu den vordefinierten. Dies kann nützlich sein, wenn Sie verschiedene Gruppen und Adressen auf logische Art und Weise aufteilen möchten. So kann eine Liste blockierter Adressen beispielsweise Adressen aus einer externen öffentlichen Negativliste und eine zweite Ihre eigene Negativliste enthalten. Auf diese Weise lässt sich die externe Liste einfacher aktualisieren, während Ihre Liste intakt bleibt.
Bearbeiten - Bearbeiten bestehender Listen. Hiermit können Sie Adressen zu den Listen hinzufügen oder daraus entfernen.
Entfernen - Löschen einer bestehenden Liste. Es können nur Listen entfernt werden, die mit „Hinzufügen“ erstellt wurden; nicht Standardlisten.

5.4.4.2.1 Neue Liste erstellen

In diesem Bereich können Sie festlegen, welche URL-Adressen/Masken blockiert, zugelassen oder von der Prüfung ausgeschlossen werden sollen.

Für die Erstellung einer neuen Liste stehen die folgenden Optionen zur Verfügung:

Typ der Adressliste - Es stehen drei Listentypen zur Verfügung:

- **Liste von der Prüfung ausgeschlossener Adressen** - Für Adressen, die in dieser Liste enthalten sind, wird keine Prüfung auf Schadcode ausgeführt.
- **Liste blockierter Adressen** - Der Benutzer darf nicht auf die in dieser Liste genannten Adressen zugreifen. Dies gilt nur für das HTTP-Protokoll. Andere Protokolle als das HTTP-Protokoll werden nicht blockiert.
- **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.

Listenname - Geben Sie den Namen der Liste ein. Bei der Bearbeitung einer der drei vordefinierten Listen wird dieses Feld grau dargestellt.

Listenbeschreibung - Geben Sie eine kurze Beschreibung für die Liste ein (optional). Wird bei der Bearbeitung einer der drei vordefinierten Listen grau dargestellt.

Um eine Liste zu aktivieren, wählen Sie **Liste aktiv** neben der gewünschten Liste. Wenn Sie benachrichtigt werden möchten, wenn eine bestimmte Liste bei der Prüfung einer von Ihnen besuchten HTTP-Site verwendet wird, aktivieren Sie die Option **Bei Anwendung benachrichtigen**. So wird beispielsweise eine Benachrichtigung ausgegeben, wenn eine Website blockiert oder zugelassen wird, da sie in der Liste der blockierten oder zugelassenen Adressen enthalten ist. Die Benachrichtigung enthält den Namen der Liste mit der angegebenen Website.

Hinzufügen - Hinzufügen einer neuen URL-Adresse zur Liste (geben Sie mehrere Werte mit einem Trennzeichen ein).

Bearbeiten - Bearbeiten einer bestehenden Adresse in der Liste. Nur bei Adressen möglich, die mit „Hinzufügen“ erstellt wurden.

Entfernen - Entfernen einer bestehenden Adresse aus der Liste. Nur bei Adressen möglich, die mit „Hinzufügen“ erstellt wurden.

Importieren - Importieren einer Datei mit URL-Adressen (trennen Sie die Werte mit einem Zeilenumbruch, z. B. *.txt mit der Codierung UTF-8).

5.4.4.2.2 HTTP-Adressen

In diesem Bereich können Sie festlegen, welche HTTP-Adressen blockiert, zugelassen oder von der Prüfung ausgeschlossen werden sollen.

Standardmäßig stehen die drei folgenden Listen zur Verfügung:

- **Liste von der Prüfung ausgeschlossener Adressen** - Für Adressen, die in dieser Liste enthalten sind, 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.

Klicken Sie auf **Hinzufügen**, um eine neue Liste zu erstellen. Klicken Sie auf **Entfernen**, um ausgewählte Listen zu löschen.

5.4.5 Phishing-Schutz

<%PN%> bietet außerdem Schutz vor Phishing-Angriffen. Der Phishing-Schutz ist im Web und E-Mail-Modul enthalten. Wenn Sie <%PN%> mit dem Installationstyp **Vollständig** installiert haben, ist das Web und E-Mail-Modul mit aktiviertem Phishing-Schutz automatisch enthalten. Dies gilt jedoch nicht für Systeme mit dem Betriebssystem Microsoft Windows Server 2008.

HINWEIS: Die Web und E-Mail-Komponente ist nicht im Installationstyp **Vollständig** <%PN%> auf Systemen mit dem Betriebssystem Windows Server 2008 oder Windows Server 2008 R2 enthalten. Sie können bei Bedarf Ihre vorhandene Installation ändern und die Web und E-Mail-Komponente hinzufügen, um den Phishing-Schutz zu nutzen.

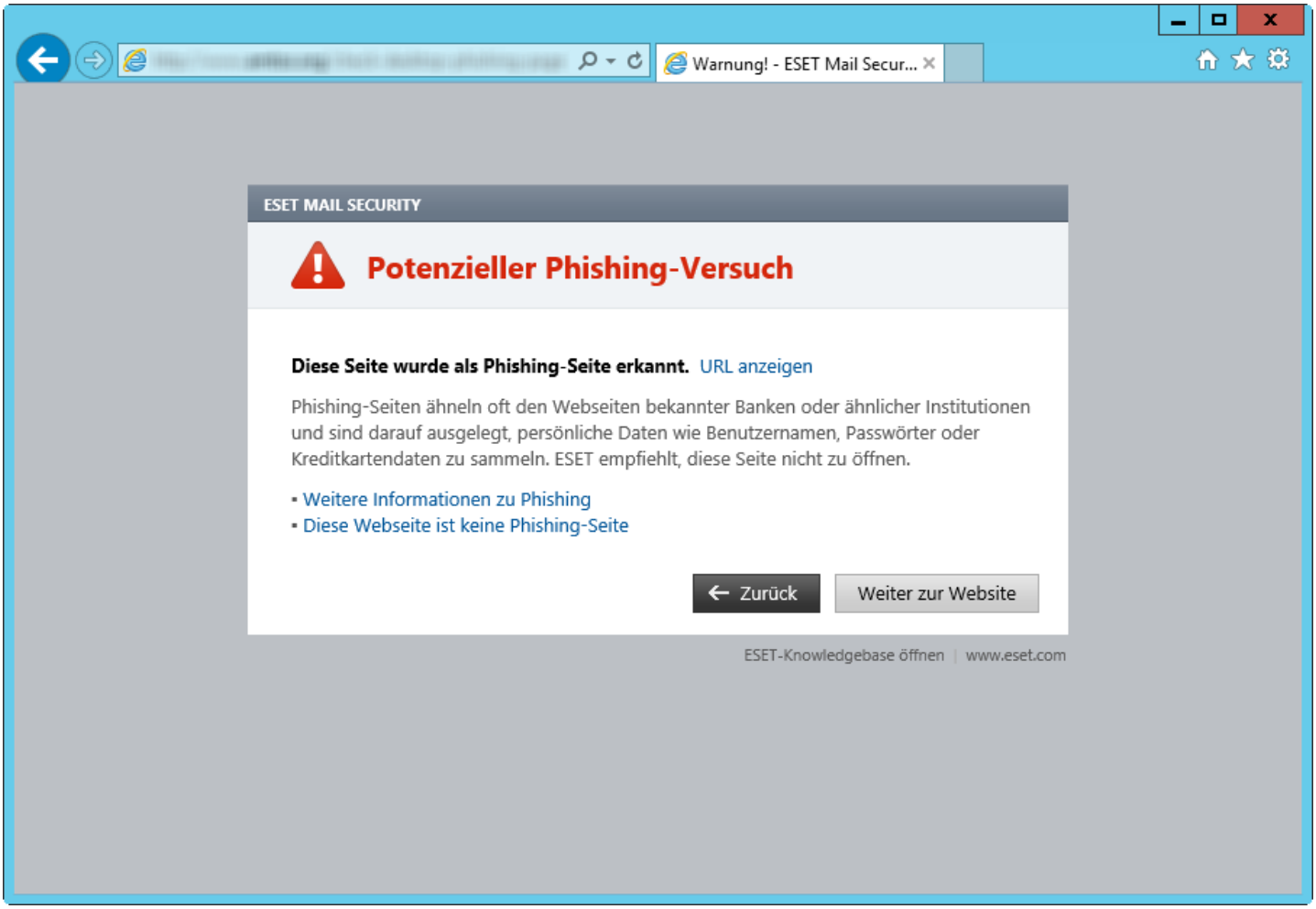
Der Begriff „Phishing“ bezeichnet eine kriminelle Vorgehensweise, die sich Techniken des Social Engineering (Manipulation von Benutzern zur Erlangung vertraulicher Informationen) zunutze macht. Phishing wird oft eingesetzt, um Zugriff auf vertrauliche Daten zu erlangen, wie Kontonummern oder PIN-Codes. Weitere Informationen zu dieser Aktivität finden Sie im Glossar. ESET Mail Security enthält einen Phishing-Schutz: Webseiten, die dafür bekannt sind, Phishing-Inhalte zu enthalten, können gesperrt werden.

Wir empfehlen, den Phishing-Schutz in ESET Mail Security zu aktivieren. Diese Option finden Sie im Bereich **Erweiterte Einstellungen** (F5) unter **Web und E-Mail** > **Phishing-Schutz**.

In unserem Knowledgebase-Artikel finden Sie weitere Informationen zum Phishing-Schutz von ESET Mail Security.

Zugriff auf eine Phishing-Website

Wenn Sie auf eine erkannte Phishing-Website zugreifen, wird das folgende Dialogfenster im Webbrowser angezeigt. Wenn Sie trotzdem auf die Website zugreifen möchten, klicken Sie auf **Weiter zur Website** (nicht empfohlen).



HINWEIS: 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. Klicken Sie unter **Erweiterte Einstellungen** (F5) auf **Web und E-Mail** > **Web-Schutz** > **URL-Adressverwaltung** > **Adressliste**. Klicken Sie anschließend auf **Bearbeiten** und fügen Sie die Website, die Sie bearbeiten möchten, zu dieser Liste hinzu.

Melden einer Phishing-Website

Über den Link Melden können Sie eine Website mit vermutetem Phishing-Inhalt oder anderem Schadcode bei ESET melden.

HINWEIS: 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.).

5.5 Medienkontrolle

ESET Mail Security bietet Methoden zur automatischen Prüfung von Geräten (CD/DVD/USB/...). Mit diesem Modul können Sie Medien bzw. Geräte scannen oder sperren oder erweiterte Filter- und Berechtigungseinstellungen anpassen und definieren, wie ein Benutzer auf diese Geräte zugreifen und mit ihnen arbeiten kann. Dies ist sinnvoll, wenn der Administrator verhindern möchte, dass Benutzer Geräte mit unerwünschten Inhalten verwenden.

Unterstützte externe Geräte:

- Datenträgerspeicher (Festplatten, USB-Wechselmedien)
- CD/DVD
- USB-Drucker
- FireWire-Speicher
- Bluetooth-Gerät
- Smartcard-Leser
- Bildverarbeitungsgerät
- Modem
- LPT/COM-Port
- Tragbares Gerät
- Alle Gerätetypen

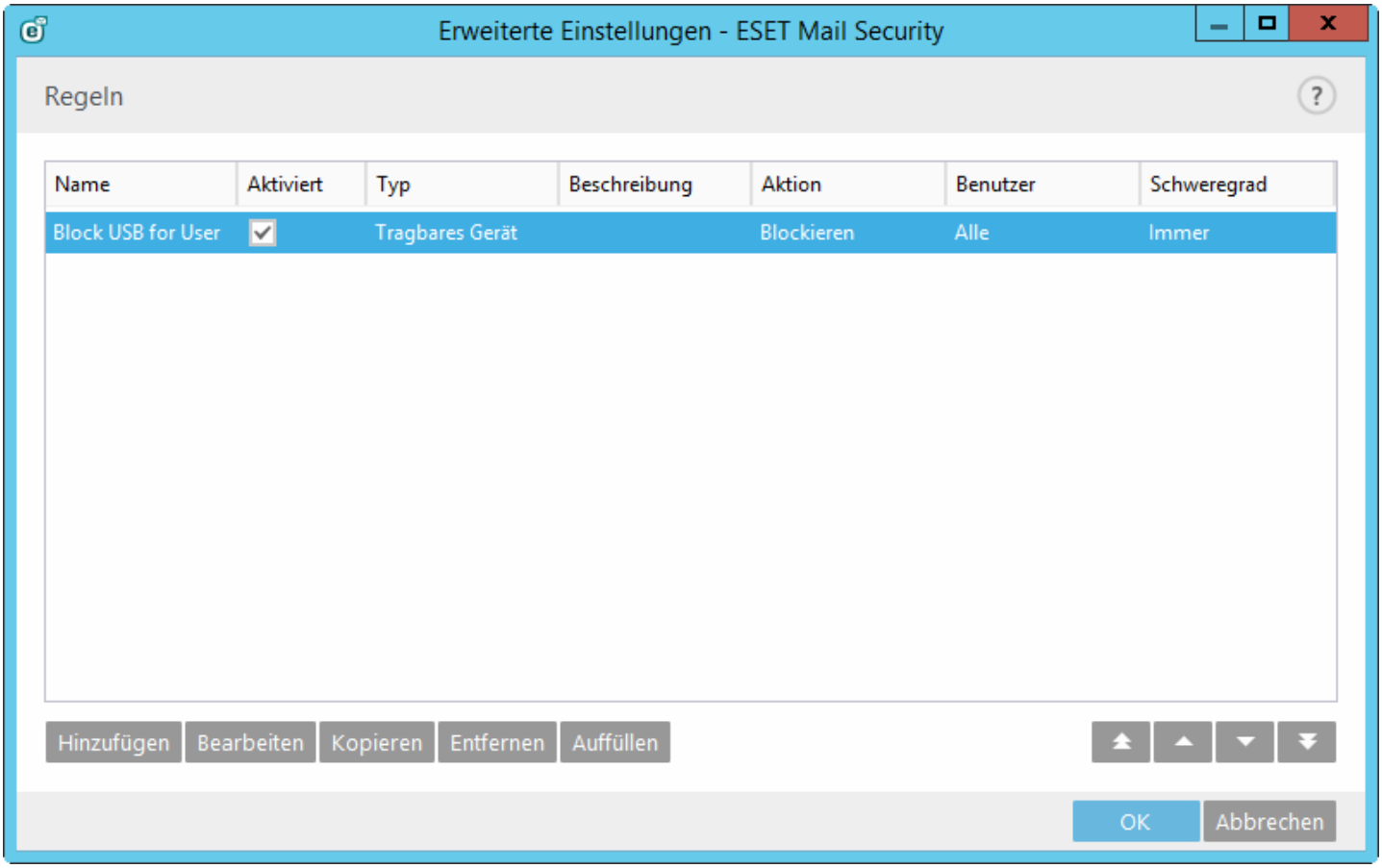
Die Einstellungen für die Medienkontrolle können unter **Erweiterte Einstellungen** (F5) > **Medienkontrolle** geändert werden.

Über das Kontrollkästchen **Systemintegration** aktivieren Sie die Medienkontrolle in ESET Mail Security. Sie müssen Ihren Computer neu starten, um die Änderungen zu übernehmen. Wenn die Medienkontrolle aktiviert ist, wird die Option **Regel-Editor** verfügbar, über die Sie das Fenster Regel-Editor öffnen können.

Wenn ein von einer bestehenden Regel blockiertes Gerät eingefügt wird, wird ein Benachrichtigungsfenster angezeigt und es wird kein Zugriff auf das Gerät gewährt.

5.5.1 Regeln für die Medienkontrolle

Im Fenster **Regel-Editor für die Medienkontrolle** können Sie bestehende Regeln anzeigen und präzise Regeln für Geräte erstellen, die Benutzer an den Computer anschließen.



Bestimmte Gerätetypen können für Benutzer oder Benutzergruppen oder auf Grundlage weiterer, in der Regelkonfiguration festgelegter Parameter zugelassen oder gesperrt werden. Die Liste der Regeln enthält verschiedene Angaben wie Regelname, Art des externen Geräts, auszuführende Aktion beim Anschließen eines externen Geräts und Log-Schweregrad.

Klicken Sie zum Bearbeiten von Regeln auf **Hinzufügen** oder **Bearbeiten**. Klicken Sie auf **Entfernen**, wenn Sie die ausgewählte Regel löschen möchten, oder entfernen Sie die Markierung aus dem Kontrollkästchen **Aktiviert** neben einer Regel, um diese zu 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.

Kopieren - Erstellt eine neue Regel mit den Parametern der ausgewählten Regel.

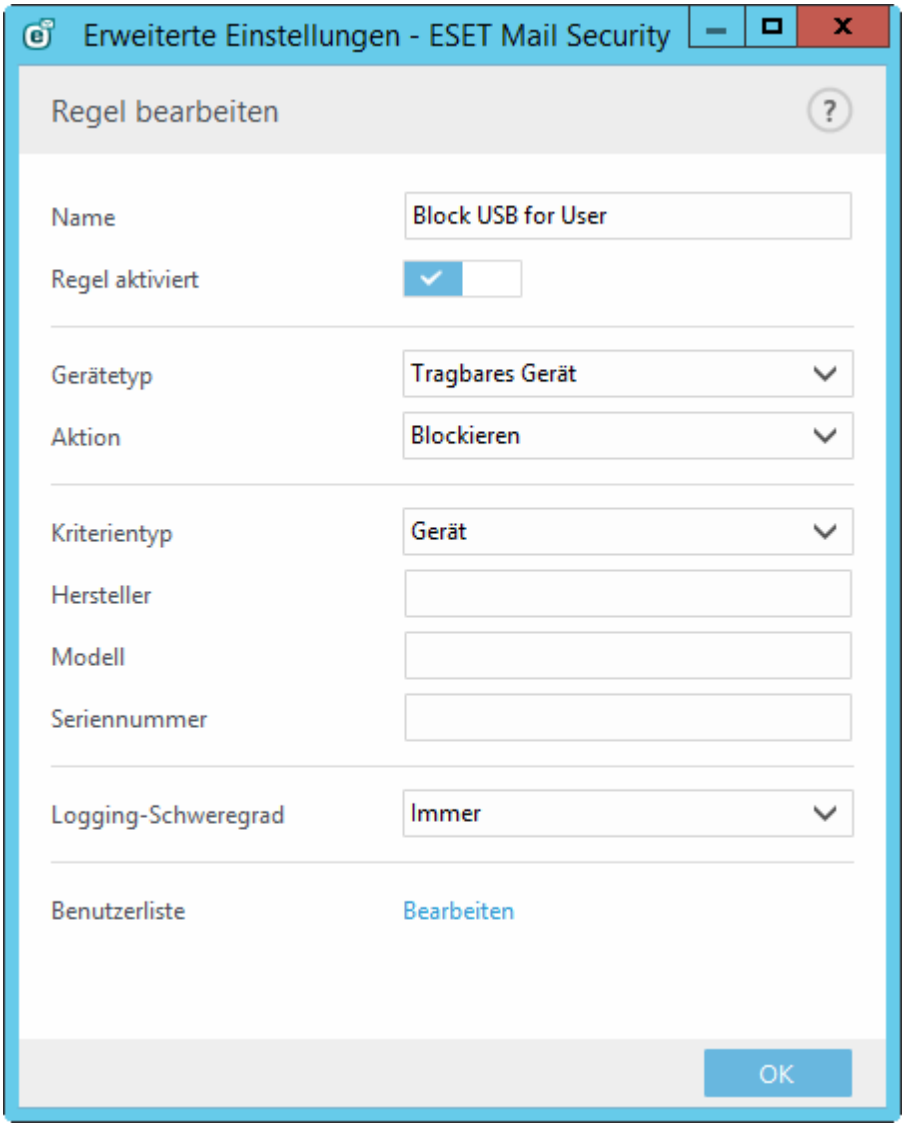
Klicken Sie auf die Option **Auffüllen**, um automatisch die Parameter für am Computer angeschlossene Wechselmedien zu übernehmen.

Die Regeln sind nach absteigender Priorität geordnet (Regeln mit höchster Priorität werden an oberster Stelle angezeigt). Sie können mehrere Regeln auswählen und Aktionen auf die Mehrfachauswahl anwenden, beispielsweise die ausgewählten Regeln löschen oder mit den Pfeiltasten **Oben/Nach oben/Nach unten/Unten** nach oben oder nach unten in der Liste verschieben.

Um Log-Einträge anzuzeigen, klicken Sie im Hauptfenster von ESET Mail Security auf **Tools** > Log-Dateien.

5.5.2 Hinzufügen von Regeln für die Medienkontrolle

Eine Regel für die Medienkontrolle definiert die Aktion, die ausgeführt wird, wenn ein Gerät, das die Regelkriterien erfüllt, an den Computer angeschlossen wird.



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 beispielsweise nützlich, wenn Sie eine Regel deaktivieren, jedoch nicht dauerhaft löschen möchten.

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. Speichergeräte umfassen externe Datenträger oder herkömmliche Kartenlesegeräte, die über den USB- oder FireWire-Anschluss an den Computer 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.

Beachten Sie, dass bestimmte Rechte (Aktionen) nur für bestimmte Gerätetypen verfügbar sind. Wenn das Gerät über Speicherplatz verfügt, 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).

Weitere Parameter zur Feinanpassung der Regeln und Anpassung an bestimmte Geräte. (die Groß-/Kleinschreibung muss nicht beachtet werden):

- **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.

HINWEIS: Wenn diese drei Bezeichner leer sind, ignoriert die Regel diese Felder bei der Zuordnung. Bei Filterparametern mit Textfeldern braucht die Groß-/Kleinschreibung nicht beachtet zu werden. Platzhalter (*, ?) werden nicht unterstützt.

Tipp: 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 Medienkontrolle-Log.

Schweregrad

- **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:

- **Hinzufügen** - Öffnet das Dialogfenster **Objekttypen: Benutzer oder Gruppen**, in dem Sie bestimmte Benutzer auswählen können.
- **Entfernen** - Entfernt den ausgewählten Benutzer aus dem Filter.

HINWEIS: Nicht alle Geräte können über Benutzerregeln eingeschränkt werden (Bildverarbeitungsgeräte liefern beispielsweise keine Informationen über Benutzer, sondern nur über aufgerufene Aktionen).

5.5.3 Erkannte Geräte

Die Schaltfläche **Auffüllen** 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).

5.5.4 Gerätegruppen

 Ein Gerät, das an den Computer angeschlossen wird, kann ein Sicherheitsrisiko darstellen.

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.

Wenn Sie das Gerätegruppenfenster öffnen und eine Gruppe auswählen, können Sie Geräte zur Liste hinzufügen oder aus der Liste entfernen. Sie können Geräte auch über eine Datei importieren, um sie zur Gruppe hinzuzufügen. Alternativ können Sie auf **Auffüllen** klicken. Alle an den Computer angeschlossenen Geräte werden im Fenster **Erkannte Geräte** angezeigt. Wählen Sie ein Gerät aus der aufgefüllten Liste aus und klicken Sie auf **OK**, um es zur Gruppe hinzuzufügen.

Steuerelemente

Hinzufügen - Sie können eine Gruppe hinzufügen, indem Sie einen Namen eingeben, oder ein Gerät zu einer vorhandenen Gruppe hinzufügen, je nachdem, in welchem Bereich des Fensters Sie auf die Schaltfläche klicken. Geben Sie optional weitere Details wie den Herstellernamen, das Modell und die Seriennummer ein.

Bearbeiten - Mit dieser Option können Sie den Namen der ausgewählten Gruppe oder die Parameter der in der Gruppe enthaltenen Geräte (Hersteller, Modell, Seriennummer) ändern.

Entfernen - Löscht die ausgewählte Gruppe bzw. das ausgewählte Gerät, je nachdem, in welchem Bereich des Fensters Sie auf die Schaltfläche klicken.

Importieren - Importiert eine Geräteliste aus einer Datei.

Die Schaltfläche **Auffüllen** bietet einen Überblick über alle aktuell angeschlossenen Geräte nebst Informationen zu Gerätetyp, Gerätehersteller, Modell und Seriennummer (sofern verfügbar).

Klicken Sie auf **OK**, wenn Sie die Bearbeitung abgeschlossen haben. Klicken Sie auf **Abbrechen**, wenn Sie das Fenster **Gerätegruppen** schließen möchten, ohne die Änderungen zu speichern.

TIPP: Sie können unterschiedliche Gerätegruppen für Geräte erstellen, auf die jeweils unterschiedliche Regeln angewendet werden sollen. Sie können auch nur eine einzige Gerätegruppe erstellen, auf die die Regel mit der Aktion **Lesen/Schreiben** oder **Schreibgeschützt** angewendet wird. So werden nicht erkannte Geräte durch die Medienkontrolle gesperrt, wenn sie an den Computer angeschlossen werden.

Beachten Sie, dass bestimmte Aktionen (Berechtigungen) nur für bestimmte Gerätetypen verfügbar sind. Für Speichergeräte sind alle vier Aktionen verfügbar. Bei anderen Geräten als Speichergeräten sind nur drei Aktionen verfügbar. (Die Aktion **Schreibgeschützt** ist beispielsweise für Bluetooth-Geräte nicht verfügbar. Bluetooth-Geräte können daher nur entweder gesperrt oder zugelassen werden oder eine Warnung auslösen.)

5.6 Tools

Dieser Abschnitt beschreibt die erweiterten Einstellungen der Tools, die in ESET Mail Security auf der Registerkarte **Tools** im Hauptprogrammfenster zur Verfügung stehen.

5.6.1 ESET Live Grid

ESET Live Grid ist ein modernes Frühwarnsystem, das mehrere Cloud-basierte Technologien umfasst. 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 Live Grid weitere Informationen verfügbar. Wählen Sie bei der Installation von ESET Mail Security eine der folgenden Optionen aus:

1. Sie haben die Möglichkeit, ESET Live Grid 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 Signaturdatenbank.
2. Sie können ESET Live Grid 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 Live Grid 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 genauen Analyse beim ESET-Virenlabor eingereicht werden. Dateien mit bestimmten Erweiterungen (z. B. *.doc* oder *.xls*) sind immer von der Übermittlung ausgeschlossen. Sie können andere Dateierweiterungen hinzufügen, wenn es bestimmte Dateitypen gibt, die Sie oder Ihr Unternehmen nicht übermitteln möchten.

Das Reputationssystem von ESET Live Grid arbeitet mit Cloud-basierten Positiv- und Negativlisten. Zugriff auf die Einstellungen von ESET Live Grid erhalten Sie, indem Sie die Taste F5 drücken, um die Erweiterten Einstellungen zu öffnen und anschließend **Tools** > **ESET Live Grid** wählen.

Am ESET Live Grid-Reputationssystem teilnehmen (empfohlen) - Das ESET Live Grid-Reputationssystem erhöht die Wirksamkeit der ESET-Sicherheitslösungen, indem es gescannte Dateien mit Positiv- und Negativlisten in einer Datenbank in der Cloud vergleicht.

Anonyme Statistiken senden- Zulassen, dass ESET Informationen über neu erkannte Bedrohungen erfasst, wie den Bedrohungsnamen, das Datum und die Uhrzeit der Erkennung, die Erkennungsmethode und verknüpften Metadaten oder die Produktversion und -konfiguration, einschließlich Daten zum System.

Dateien einreichen - Verdächtige Dateien, die auf eine Bedrohung hinweisen, und/oder Dateien mit ungewöhnlichen Eigenschaften oder ungewöhnlichem Verhalten werden zur Analyse an ESET gesendet.

Wählen Sie die Option **Erstellen von Logs aktivieren** aus, um einen Ereignis-Log zu erstellen, in dem alle Informationen über das Einreichen von Dateien und statistischen Daten protokolliert werden. Dadurch werden Einträge im Ereignis-Log erstellt, wenn Dateien oder statistische Daten eingereicht werden.

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.

Ausschlussfilter - Mit dem Ausschlussfilter können Sie bestimmte Dateien/Ordner von der Übermittlung ausschließen. So kann es beispielsweise nützlich sein, Dateien mit vertraulichen Informationen wie Dokumente oder Tabellenkalkulationen auszuschließen. Hier eingetragene Dateien werden nicht an ESET übermittelt, auch wenn sie verdächtigen Code enthalten. Einige typische Dateitypen sind bereits in der Standardeinstellung in die Liste eingetragen (.doc usw.). Sie können der Ausschlussliste weitere Dateien hinzufügen.

Wenn Sie ESET Live Grid 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.

5.6.1.1 Ausschlussfilter

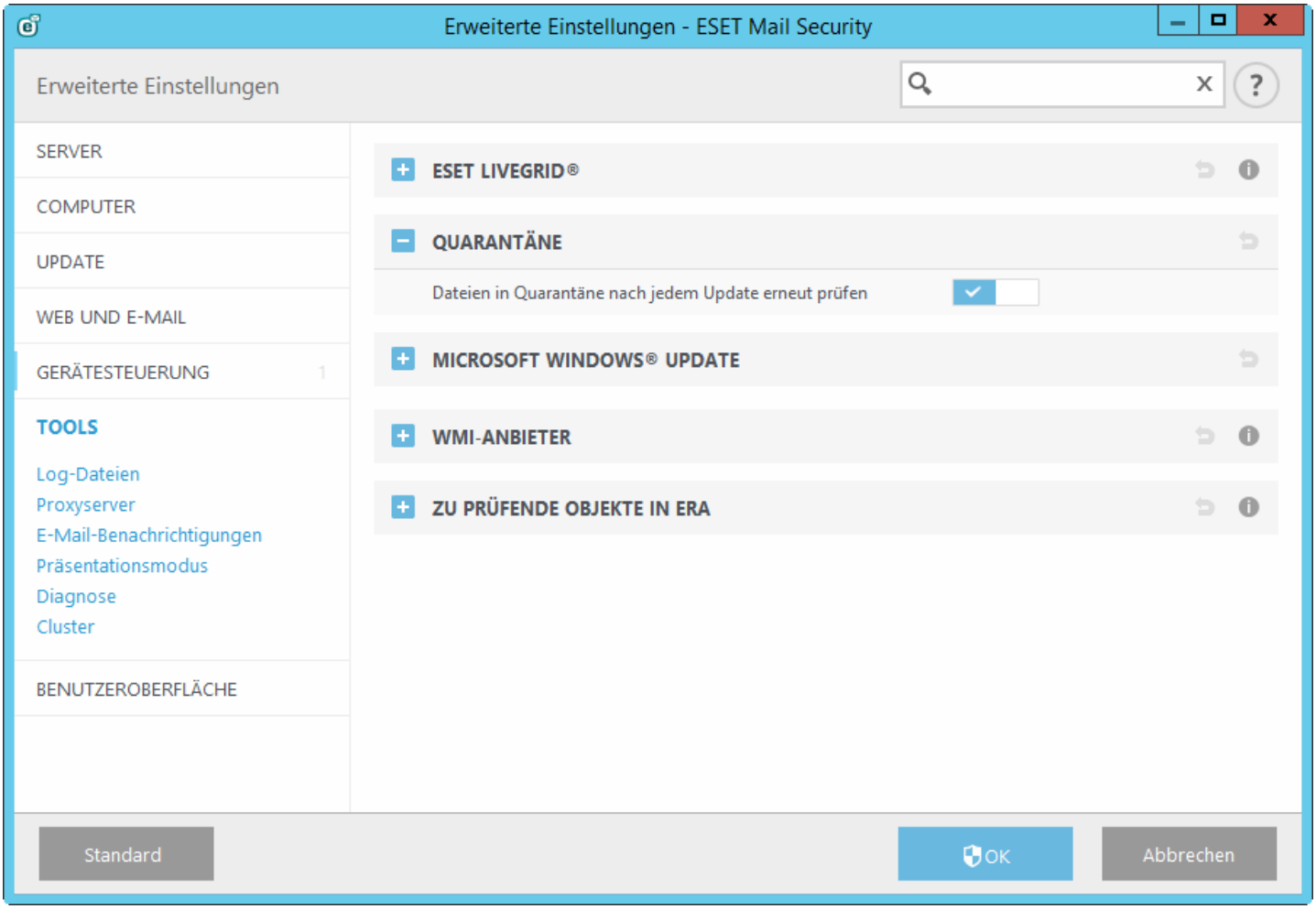
Mit der Option **Bearbeiten** neben „Ausschlussfilter“ in ESET Live Grid können Sie konfigurieren, wie Bedrohungen zur Analyse an ESET gesendet werden.

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 der Signaturdatenbank berücksichtigt.

5.6.2 Quarantäne

Im Quarantäneordner werden infizierte oder verdächtige Dateien gespeichert, ohne dass sie Schaden anrichten können. Vom Echtzeit-Dateischutz werden neu erstellte verdächtige Dateien standardmäßig im Quarantäneordner gespeichert, um Infektionen zu verhindern.

Dateien in Quarantäne nach jedem Update erneut scannen - Nach jedem Update der Signaturdatenbank werden alle Objekte im Quarantäneordner erneut gescannt. Dies ist besonders dann hilfreich, wenn eine Datei nach einem Fehlalarm in die Quarantäne verschoben wurde. Wenn diese Option aktiviert ist, können bestimmte Dateitypen automatisch an ihrem ursprünglichen Speicherort wiederhergestellt werden.



5.6.3 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 wichtig, 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.

5.6.4 WMI Provider

WMI

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.

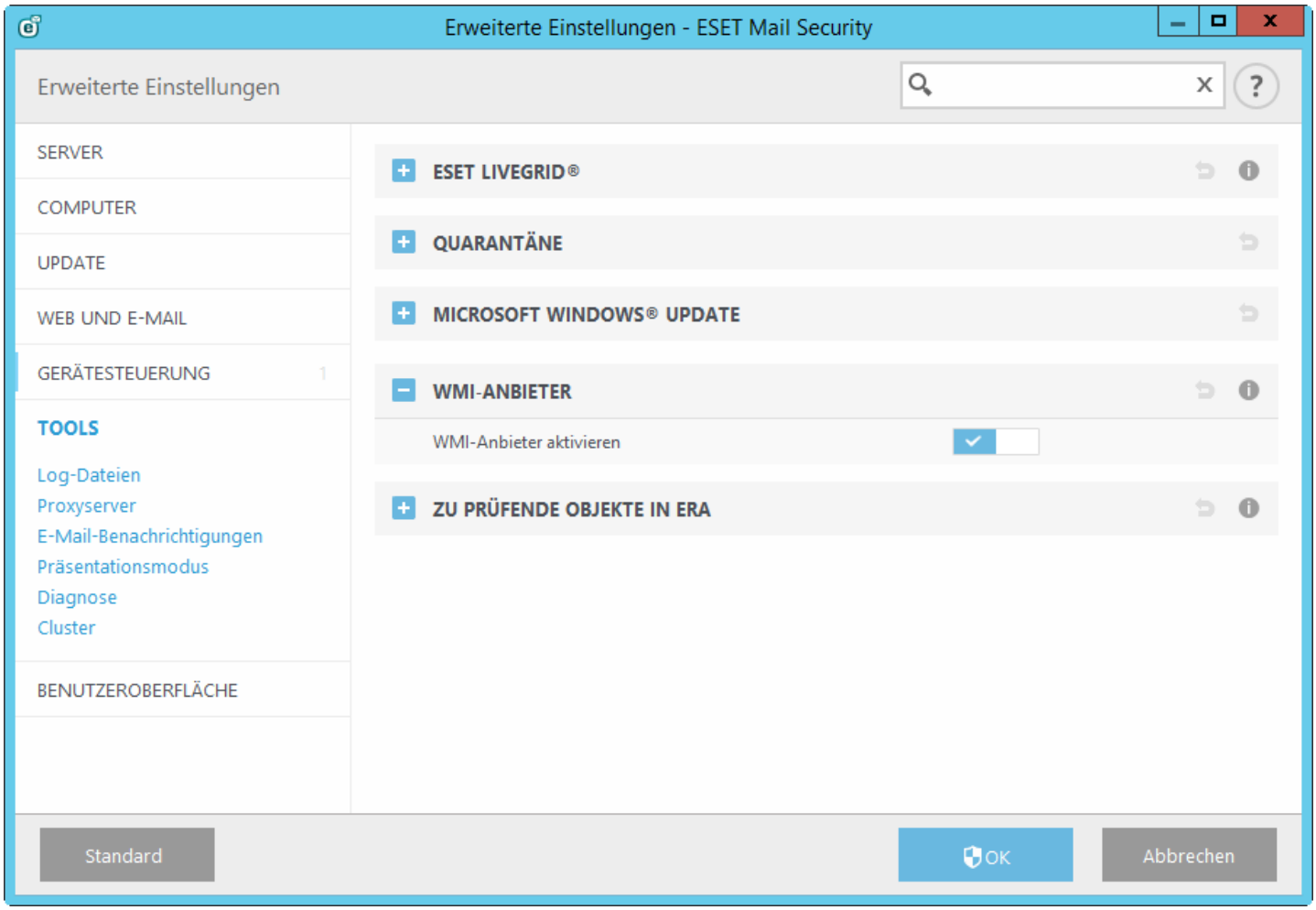
Weitere Informationen zu WMI finden Sie bei http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642(v=vs.85).aspx

ESET WMI Provider

Mit dem ESET WMI Provider 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 Provider können Sie Sie die Windows WMI-Standardinfrastruktur und -Tools verwenden, um den Status von Produkt und Produkt-Logs auszulesen.



5.6.4.1 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_GreylistLog
- ESET_SpamLog

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 „essbe“
- **Name** - Produktbezeichnung, zum Beispiel „ESET Security“
- **Edition** - Produktausgabe, zum Beispiel „Microsoft SharePoint Server“
- **Version** - Produktversion, zum Beispiel „4.5.15013.0“
- **VirusDBVersion** - Version der Signaturdatenbank, zum Beispiel „7868 (20130107)“
- **VirusDBLastUpdate** - Zeitstempel des letzten Update der Signaturdatenbank. Die Zeichenkette enthält den Zeitstempel im WMI-Format für Datum und Uhrzeit, zum Beispiel „20130118115511.000000+060“
- **LicenseExpiration** - Lizenzablaufzeitpunkt. Die Zeichenkette enthält den Zeitstempel im WMI-Format für Datum und Uhrzeit, zum Beispiel „20130118115511.000000+060“
- **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 bei ESET Mail Security Dateien in der SharePoint-Inhaltsdatenbank
- **SERVER_EMAIL_AV** - Virenschutz für E-Mails auf dem geschützten Serverprodukt, zum Beispiel E-Mails in MS Exchange oder IBM Lotus Domino
- **SERVER_EMAIL_AS** - Spam-Schutz für E-Mails auf dem geschützten Serverprodukt, zum Beispiel E-Mails in MS Exchange oder IBM Lotus 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 bestimmten 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 stellt einen Log-Eintrag aus dem Log „Erkannte Bedrohungen“ dar. Jede Instanz enthält Folgendes:

- **ID** - eindeutige ID dieses Log-Eintrags
- **Timestamp** - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- **LogLevel** - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8 ausgedrückt. 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

ESET_EventLog

Die ESET_EventLog-Klasse hat mehrere Instanzen. Jede stellt einen Log-Eintrag aus dem Log „Ereignisse“ dar. Jede Instanz enthält Folgendes:

- **ID** - eindeutige ID dieses Log-Eintrags
- **Timestamp** - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- **LogLevel** - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8 ausgedrückt. 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“ der Benutzeroberfläche. Jede Instanz enthält Folgendes:

- **ID** - eindeutige ID dieses On-Demand-Log-Eintrags
- **Timestamp** - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- **Targets** - Zielordner/-objekte des Scans
- **TotalScanned** - Gesamtzahl der gescannten 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 Scan-Logs 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 Scan-Logs benötigt wird, 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_ODFileScanLogs-Klasse)
- **ID** - eindeutige ID dieses Scan-Log-Eintrags
- **Timestamp** - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- **LogLevel** - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8 ausgedrückt. 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 On-Demand-Log-Eintrags
- **Timestamp** - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- **Targets** - Zielordner/-objekte des Scans
- **TotalScanned** - Gesamtzahl der gescannten 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 Scan-Logs 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 Scan-Logs benötigt wird, 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_ODServerScanLogs-Klasse)
- **ID** - eindeutige ID dieses Scan-Log-Eintrags
- **Timestamp** - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- **LogLevel** - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8 ausgedrückt. 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_GreylistLog

Die ESET_GreylistLog-Klasse hat mehrere Instanzen. Jede stellt einen Log-Eintrag aus dem Log „Greylist“ dar. Jede Instanz enthält Folgendes:

- **ID** - eindeutige ID dieses Log-Eintrags
- **Timestamp** - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- **LogLevel** - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8 ausgedrückt. 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
- **Action** - ausgeführte Aktion
- **TimeToAccept** - Anzahl der Minuten, nach der die E-Mail akzeptiert wird

ESET_SpamLog

Die ESET_SpamLog-Klasse hat mehrere Instanzen. Jede stellt einen Log-Eintrag aus dem Log „Spamlog“ dar. Jede Instanz enthält Folgendes:

- **ID** - eindeutige ID dieses Log-Eintrags
- **Timestamp** - Zeitstempel der Log-Erstellung (im WMI-Format für Datum/Uhrzeit)
- **LogLevel** - Schweregrad des Log-Eintrags, als Zahl zwischen 0 und 8 ausgedrückt. Die Werte entsprechen folgenden Schweregradstufen: Debug-Meldung, Information/Fußnote, Information, wichtige Information, Warnung, Fehler, Sicherheitswarnung, kritischer Fehler, kritische Sicherheitswarnung
- **Sender** - Absender der E-Mail
- **Recipients** - Empfänger der E-Mail
- **Subject** - Betreff der E-Mail
- **Received** - Uhrzeit des Empfangs
- **Score** - Spam-Score in Prozent [0-100]
- **Reason** - Grund für das Kennzeichnen der E-Mail als Spam
- **Action** - ausgeführte Aktion
- **DiagInfo** - zusätzliche Diagnoseinformationen

5.6.4.2 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. Es stehen jedoch mit anderen Skriptsprachen und Tools zahlreiche weitere Möglichkeiten für den Zugriff auf die Daten zur Verfügung.

Befehlszeile ohne Skripts

Mit dem Befehlszeilen-Tool `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            # fordert den Benutzer zur Eingabe der Anmeldedaten auf und speichert dies
Get-WmiObject ESET_Product -namespace 'root\ESET' -computername '10.1.118.180' -cred $cred
```

5.6.5 Zu scannende Objekte in ERA

Mit dieser Funktion können für ESET Remote Administrator geeignete Scan-Ziele für den On-Demand-Datenbank-Scan definiert werden, die beim Ausführen des Client-Tasks **Server-Scan** auf einem Server mit ESET Mail Security berücksichtigt werden.

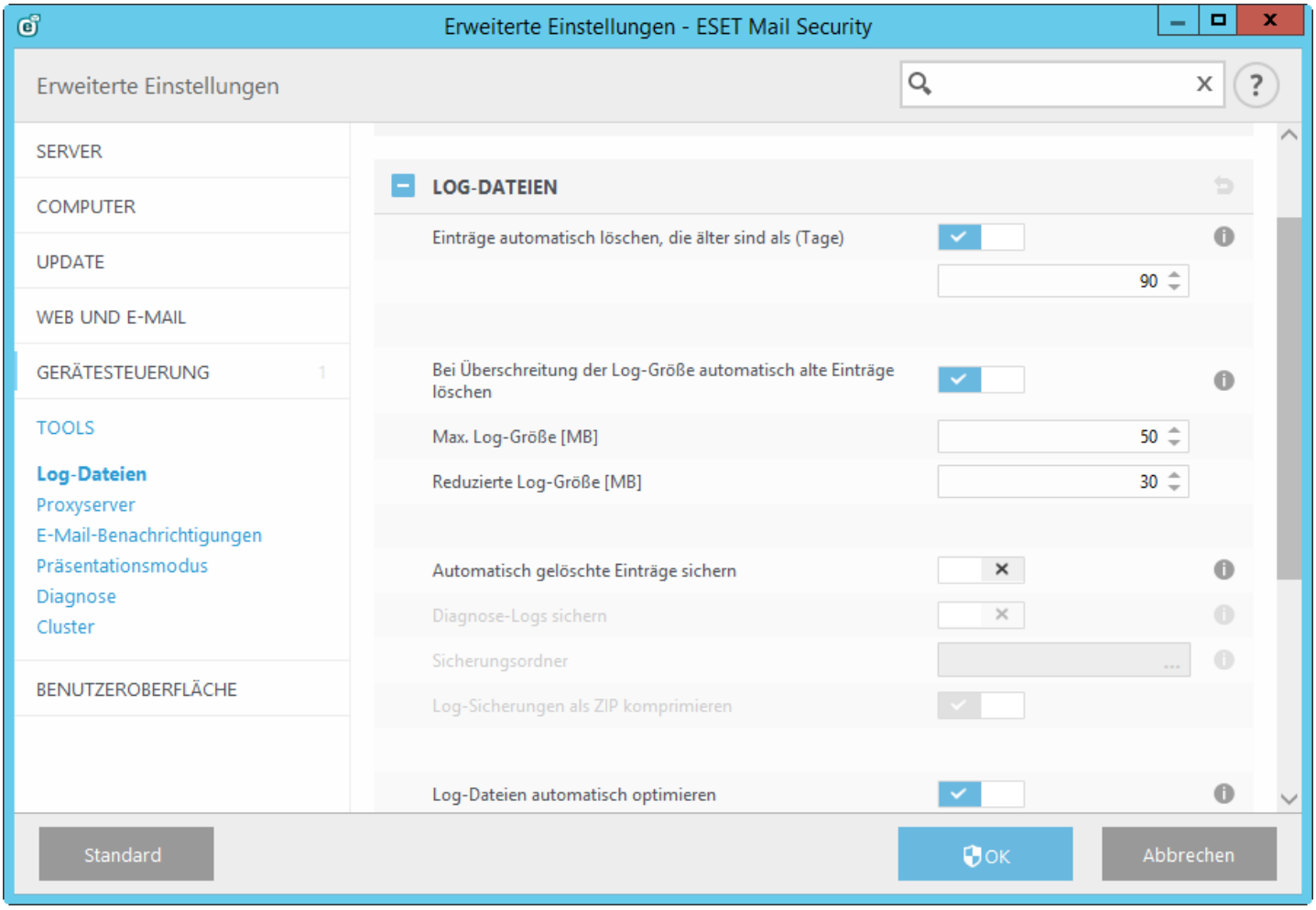
Wenn Sie die Funktion **Liste der Ziele generieren** aktivieren, erstellt ESET Mail Security eine Liste der aktuell verfügbaren Ziele für den Datenbank-Scan. Diese Liste wird periodisch gemäß dem in Minuten festgelegten **Updateintervall** erzeugt. Wenn ERA den Client-Task **Server-Scan** ausführt, erfasst es diese Liste und fordert Sie auf, Scan-Ziele für den On-Demand-Datenbank-Scan auf dem betroffenen Server auszuwählen.

5.6.6 Log-Dateien

Sie können die Option Cluster-**Diagnose-Logging** bei Bedarf aktivieren oder deaktivieren. Die Option ist standardmäßig aktiviert. Dies bedeutet, dass das Cluster-Logging in den allgemeinen Diagnose-Logs enthalten ist. Um das allgemeine Logging zu aktivieren, müssen Sie die Diagnose-Logs unter Hauptmenü > Einstellungen > Tools aktivieren. Anschließend werden in den Diagnose-Logs auch ausführliche Logs vom ESET-Cluster gesammelt.

Im Bereich Log-Dateien können Sie die Logging-Konfiguration von ESET Mail Security ändern.

Hier können Sie Einstellungen für Logs festlegen. Um den Speicherbedarf zu reduzieren, werden ältere Logs automatisch gelöscht.



5.6.6.1 Log-Filter

In den Logs werden Informationen über wichtige Systemereignisse gespeichert. Mit dem Log-Filter können Sie sich Einträge zu einer bestimmten Ereignisart anzeigen lassen.

Geben Sie das Suchwort im Feld **Suchen nach** ein. Über das Dropdown-Menü **In Spalten** können Sie Ihre Suche verfeinern.

Eintragstypen - Wählen Sie einen oder mehrere Log-Eintragstypen aus dem Dropdown-Menü aus:

- **Diagnose** - 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.
- **Kritische Warnungen** - Nur kritische Warnungen (z. B. bei einem Fehler beim Start des Virenschutz-Moduls) werden protokolliert.

Zeitraum - Legen Sie fest, aus welchem Zeitraum die Suchergebnisse stammen sollen.

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.

5.6.6.2 In Log suchen

Zusätzlich zum Log-Filter können Sie die Suchfunktion in den Log-Dateien verwenden. Die Suchfunktion kann aber auch unabhängig vom Log-Filter verwendet werden. Diese Funktion ist sinnvoll, wenn Sie nach bestimmten Log-Einträgen suchen. Wie der Log-Filter hilft auch sie Ihnen beim Auffinden von Informationen, besonders bei einer unüberschaubaren Anzahl von Einträgen.

Für die Suche in den Logs stehen Ihnen die Funktion **Suchen nach:** zum Suchen nach einer bestimmten Zeichenkette, das Dropdown-Menü **In Spalten** zum Filtern nach Spalten, die Auswahl bestimmter **Eintragstypen** und eine Funktion zum Festlegen des **Zeitraums** zum Einschränken der Suchergebnisse zur Verfügung. Die Angabe bestimmter Suchoptionen hat zur Folge, dass nur Einträge, die diesen Angaben entsprechen, im Log-Dateien-Hauptfenster durchsucht werden.

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. Standardmäßig sind alle Spalten ausgewählt:

- **Zeit**
- **Gescannter Ordner**
- **Ereignis**
- **Benutzer**

Eintragstypen: Wählen Sie einen oder mehrere Log-Eintragstypen aus dem Dropdown-Menü aus:

- **Diagnose** - 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.
- **Kritische Warnungen** - Nur kritische Warnungen (z. B. bei einem Fehler beim Start des Virenschutz-Moduls) werden protokolliert.

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

- **Keine Angabe** (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 (Datum und Uhrzeit), um nur Einträge aus diesem Zeitraum zu suchen.

Nur ganze Wörter - Sucht nur nach Einträgen, die eine im **Nach**-Textfeld eingegebene Zeichenfolge als vollständiges Wort enthalten.

Groß-/Kleinschreibung beachten - Sucht nur nach Einträgen, die eine im **Nach**-Textfeld eingegebene Zeichenfolge mit gleicher Groß- und Kleinschreibung enthalten.

Rückwärts suchen - Sucht von der aktuellen Position aus rückwärts.

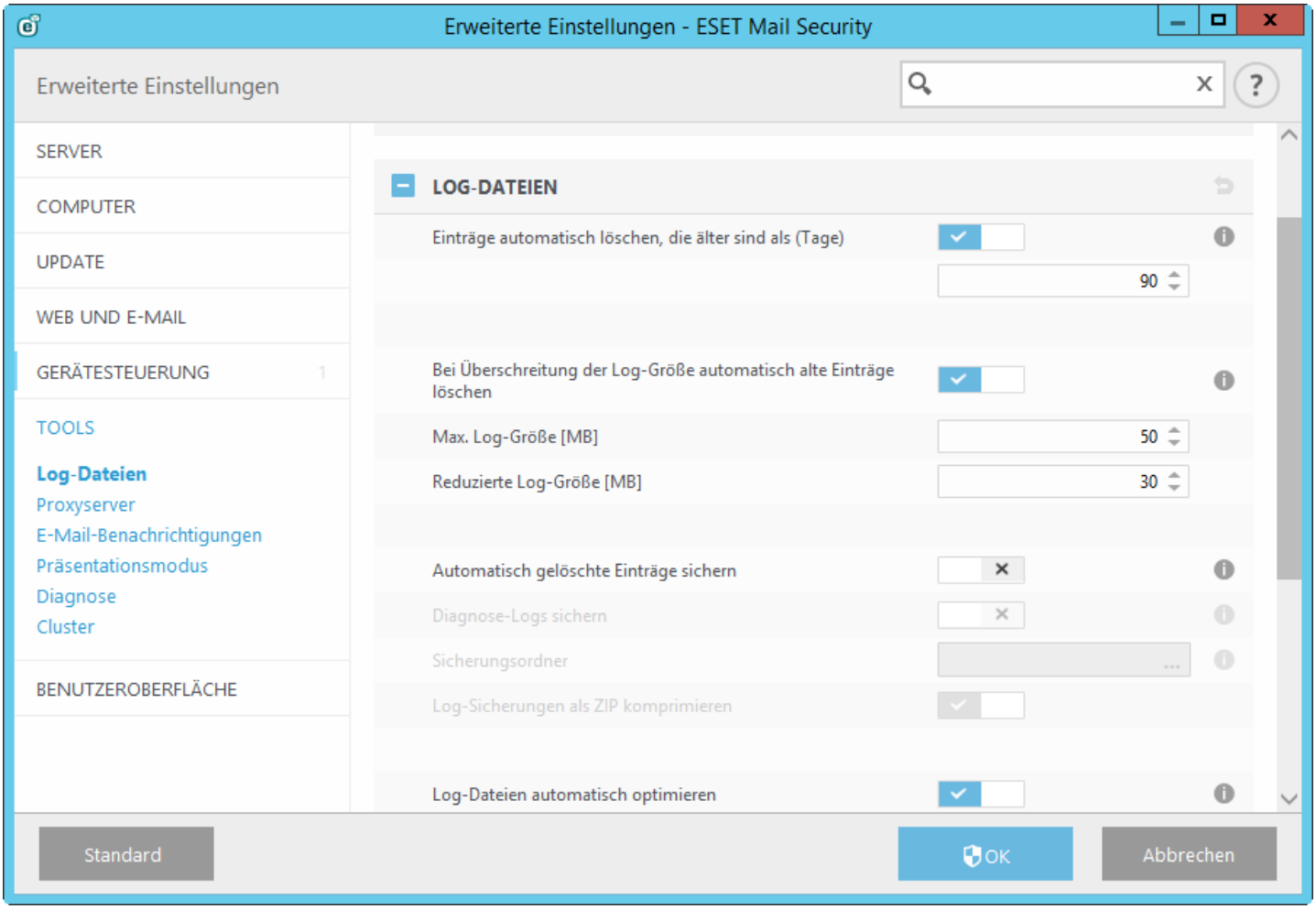
Wenn Sie die Suchoptionen konfiguriert haben, klicken Sie auf **Suchen**, um die Suche zu starten. Die Suche wird gestoppt, sobald der erste Eintrag gefunden wurde, der den Suchkriterien entspricht. Klicken Sie erneut auf **Suchen**, um weitere Einträge anzuzeigen. Von der aktuellen (hervorgehobenen) Position aus werden die Log-Dateien von oben nach unten durchsucht.

5.6.6.3 Log-Wartung

Sie können die Option Cluster-**Diagnose-Logging** bei Bedarf aktivieren oder deaktivieren. Die Option ist standardmäßig aktiviert. Dies bedeutet, dass das Cluster-Logging in den allgemeinen Diagnose-Logs enthalten ist. Um das allgemeine Logging zu aktivieren, müssen Sie die Diagnose-Logs unter Hauptmenü > Einstellungen > Tools aktivieren. Anschließend werden in den Diagnose-Logs auch ausführliche Logs vom ESET-Cluster gesammelt.

Im Bereich Log-Dateien können Sie die Logging-Konfiguration von ESET Mail Security ändern.

Hier können Sie Einstellungen für Logs festlegen. Um den Speicherbedarf zu reduzieren, werden ältere Logs automatisch gelöscht.



- **Einträge automatisch löschen**: Log-Einträge, die älter als die angegebene Anzahl von Tagen sind, werden automatisch gelöscht.
- **Log-Dateien automatisch optimieren**: Log-Dateien werden automatisch defragmentiert, wenn der festgelegte Prozentsatz an nicht verwendeten Einträgen überschritten wird
- **Mindestinformation in Logs**: Hier können Sie festlegen, welche Informationen in den Logs enthalten sein sollen. Verfügbare Optionen:
  - **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** - Nur Fehler wie "Fehler beim Herunterladen einer Datei" und kritische Fehler werden protokolliert
  - **Kritische Warnungen** - Nur kritische Warnungen (z. B. bei einem Fehler beim Start des Virenschutz-Moduls) werden protokolliert

5.6.7 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. Wenn die Einstellungen nicht vorgenommen werden, ist es möglicherweise nicht möglich, automatisch Updates über das Internet zu beziehen. ESET Mail Security bietet Optionen für die Proxyserver-Einstellungen in zwei verschiedenen Bereichen der erweiterten Einstellungen.

Die Einstellungen für den Proxyserver können zum einen in **Erweiterte Einstellungen** unter **Tools** > **Proxyserver** konfiguriert werden. So legen Sie die allgemeinen Proxyserver-Einstellungen für alle Funktionen von ESET Mail Security fest. Diese Parameter werden von allen Modulen verwendet, die eine Verbindung zum Internet benötigen.

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.

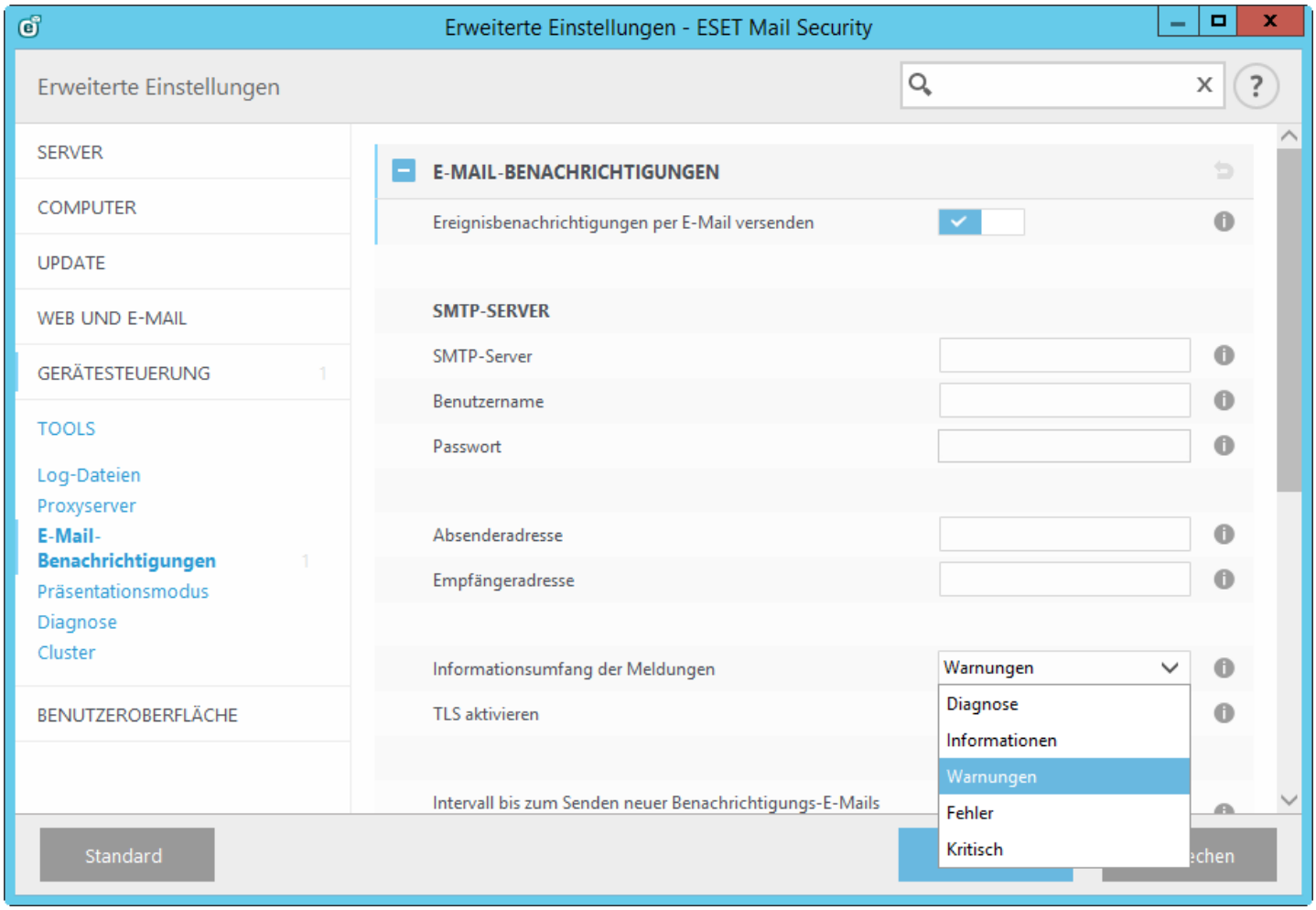
Wenn der Proxyserver eine Authentifizierung benötigt, aktivieren Sie das Kontrollkästchen **Proxyserver erfordert Authentifizierung** und geben einen gültigen **Benutzernamen** sowie das entsprechende **Passwort** ein. Klicken Sie auf **Erkennen**, wenn die Einstellungen des Proxyservers automatisch erkannt und ausgefüllt werden sollen. Die in Internet Explorer festgelegten Einstellungen werden kopiert.

HINWEIS: Diese Funktion ruft keine Anmeldedaten (Benutzername und Passwort) ab; Sie müssen diese Informationen eingeben.

Die Proxyserver-Einstellungen können auch in den erweiterten Einstellungen für Updates festgelegt werden (**Erweiterte Einstellungen**> **Update** > **HTTP-Proxy**, Option **Verbindung über Proxyserver** im Dropdown-Menü **Proxy-Modus**). Die Einstellungen gelten dann für das entsprechende Update-Profil. Diese Methode wird für Laptops empfohlen, da diese die Updates der Signaturdatenbank oft von verschiedenen Quellen beziehen. Weitere Informationen zu diesen Einstellungen finden Sie im Abschnitt Erweiterte Einstellungen für Updates.

5.6.8 E-Mail-Benachrichtigungen

ESET Mail Security kann automatisch Ereignismeldungen senden, wenn ein Ereignis mit dem ausgewählten Informationsumfang auftritt. Aktivieren Sie **Ereignismeldungen per E-Mail versenden**, damit Ereignismeldungen versendet werden.



HINWEIS: ESET Mail Security unterstützt keine SMTP-Server mit TLS-Verschlüsselung.

- **SMTP-Server** - Der SMTP-Server, über den Meldungen per E-Mail verschickt werden sollen.
- **Benutzername und Passwort** - Falls für den SMTP-Server Zugangsdaten zur Authentifizierung erforderlich sind, geben Sie hier einen gültigen Benutzernamen und das Passwort ein.

- **Absenderadresse** - Dieses Feld enthält die Adresse, die in Ereignismeldungen als Absender verzeichnet sein soll.
- **Empfängeradresse** - Dieses Feld enthält die Adresse, die in Ereignismeldungen als Empfänger verzeichnet sein soll.

- **Informationsumfang der Meldungen** - Hier können Sie festlegen, welche Ereignistypen das Versenden von Meldungen auslösen sollen.
- **TLS aktivieren** - Hiermit werden von der TLS-Verschlüsselung unterstützte Warnungen und Benachrichtigungen versendet.

- **Intervall bis zum Senden neuer Benachrichtigungs-E-Mails (Min.)** - Intervall in Minuten, nach dem neue Benachrichtigungen per E-Mail gesendet werden. Legen Sie für diese Einstellung den Wert "0" fest, wenn die Benachrichtigungen sofort gesendet werden sollen.
- **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 empfangen werden.

Format von Meldungen

- **Format der Meldungen bei Ereignissen** - Format der Meldungen bei auf Remotecomputern angezeigten Ereignissen. Siehe auch Format bearbeiten.
- **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. Siehe auch Format bearbeiten.

- **Lokalen Zeichensatz verwenden** - Konvertiert eine E-Mail-Nachricht anhand der Ländereinstellungen in Windows in eine ANSI-Zeichenkodierung (z. B. Windows-1250). Wenn Sie diese Option deaktiviert lassen, werden Nachrichten in 7-Bit-ACSII kodiert (dabei wird z. B. „à“ zu „a“ geändert und ein unbekanntes Symbol durch ein Fragezeichen ersetzt).
- **Lokale Zeichenkodierung verwenden** - Die E-Mail-Nachrichtenquelle wird in das QP-Format konvertiert, das ASCII-Zeichen verwendet und besondere regionale Zeichen in der E-Mail korrekt im 8-Bit-Format überträgt (áéíóú).

5.6.8.1 Format von Meldungen

Ereignismeldungen werden an Remotebenutzer/Administratoren als E-Mails oder LAN-Nachrichten (Windows®-Messaging-Dienst) weitergeleitet. Das Standard-Nachrichtenformat ist für die meisten Einsatzfälle ausreichend. Sie können das Format der Meldungen bei Ereignissen jedoch auch anpassen.

Schlüsselwörter (durch %-Zeichen abgetrennte 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
- **%InfectedObject%** - Name der infizierten Datei, Nachricht usw.
- **%VirusName%** - Angabe des Infektionsverursachers
- **%ErrorDescription%** - Beschreibung eines nicht durch Viruscode ausgelösten Ereignisses

Die Schlüsselwörter **%InfectedObject%** und **%VirusName%** werden nur in Warnmeldungen bei Bedrohungen verwendet, **%ErrorDescription%** nur in Ereignismeldungen.

5.6.9 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 während Präsentationen verwendet werden, die nicht durch eine Aktion des Virenschutzes unterbrochen werden dürfen. Wenn er aktiviert ist, werden alle Popup-Fenster deaktiviert und geplante Tasks werden nicht ausgeführt. Der Systemschutz läuft weiter im Hintergrund, doch es sind keine Eingaben durch Benutzer erforderlich.

Klicken Sie auf **Einstellungen** > **Computer** und anschließend auf den Schalter neben **Präsentationsmodus**, um den Präsentationsmodus manuell zu aktivieren. Klicken Sie in **Erweiterte Einstellungen** (F5) auf **Tools** > **Präsentationsmodus** und anschließend auf den Schalter neben **Präsentationsmodus automatisch aktivieren, wenn Anwendungen im Vollbildmodus ausgeführt werden**, damit ESET Mail Security automatisch in den Präsentationsmodus wechselt, wenn Anwendungen im Vollbildmodus ausgeführt werden. Im Präsentationsmodus besteht ein erhöhtes Risiko. Daher wird das Schutzstatus-Symbol in der Taskleiste orange und mit einer Warnung angezeigt. Diese Warnung wird auch im Hauptprogrammfenster angezeigt (**Präsentationsmodus aktiviert** wird orangefarben dargestellt).

Mit der Option **Präsentationsmodus automatisch aktivieren, wenn Anwendungen im Vollbildmodus ausgeführt werden** wird der Präsentationsmodus gestartet, sobald Sie eine Anwendung im Vollbildmodus ausführen. Der Präsentationsmodus wird beendet, sobald Sie die Anwendung beenden. Dies ist besonders hilfreich, um den Präsentationsmodus direkt nach dem Start eines Computerspiels, einer Anwendung im Vollbildmodus oder einer Präsentation automatisch zu starten.

Mit der Option **Präsentationsmodus automatisch deaktivieren nach** können Sie außerdem die Zeit in Minuten festlegen, nach der der Präsentationsmodus automatisch deaktiviert wird.

5.6.10 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 kann Entwicklern helfen, Fehler im Code zu finden und verschiedene Probleme von ESET Mail Security zu lösen. Klicken Sie auf das Dropdown-Menü neben **Typ des Speicherabbilds** und wählen Sie eine von drei Optionen:

- Mit**Deaktivieren** (Standardoption) wird diese Funktion deaktiviert.
- **Mini** - Protokolliert die kleinste Menge an Daten, die helfen könnten, die Ursache für den Absturz der Anwendung herauszufinden. Dieser Dateityp 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 auch 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 Fenster von *Windows Explorer* zu öffnen.

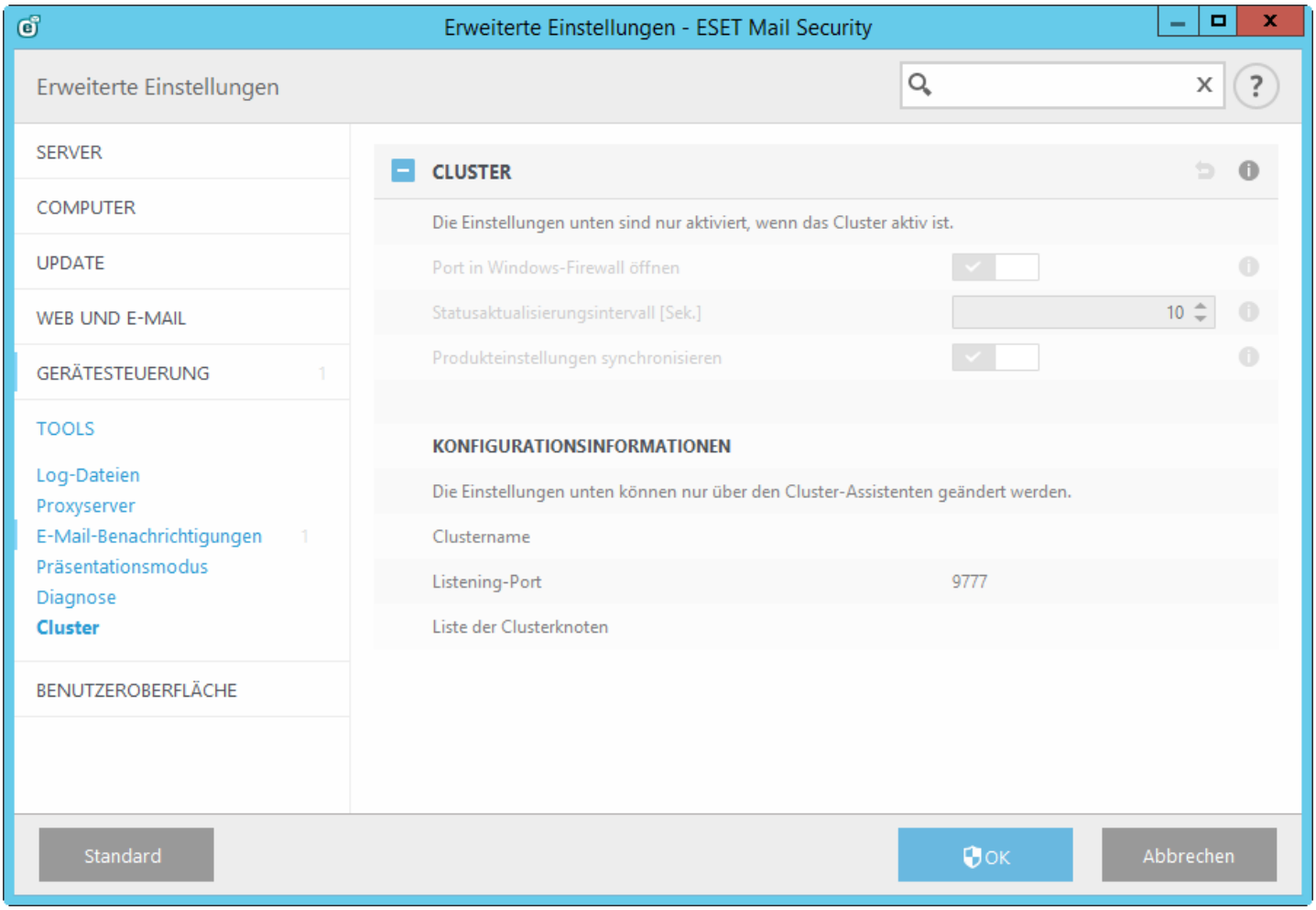
5.6.11 Support

Systemkonfigurationsdaten senden - Wählen Sie im Dropdownmenü **Immer senden** aus oder **Vor dem Senden nachfragen**, wenn Sie zum Senden aufgefordert werden möchten.

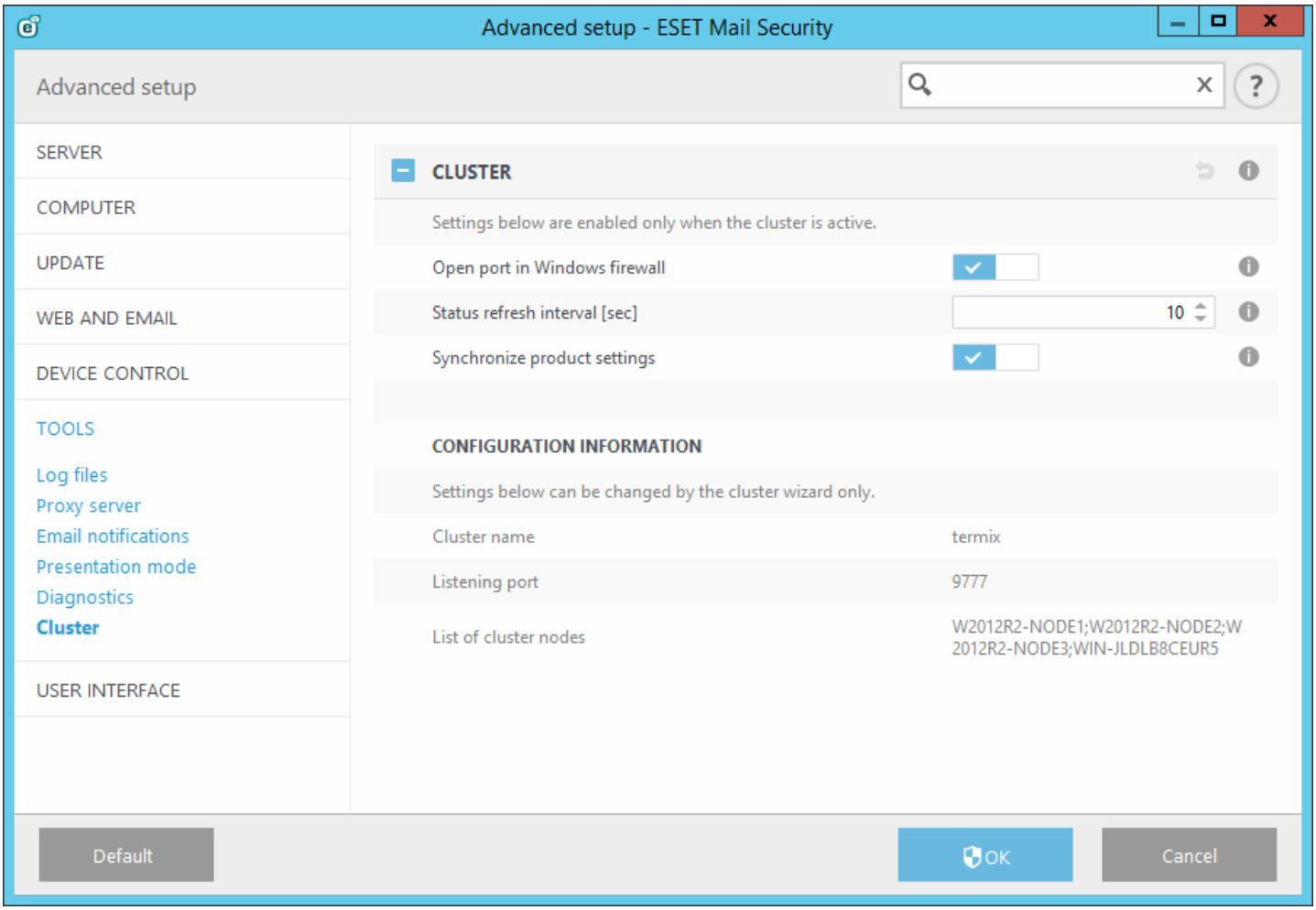
5.6.12 Cluster

Cluster aktivieren wird automatisch aktiviert, wenn der ESET-Cluster konfiguriert wird. Sie können den Cluster manuell im Fenster „Erweiterte Einstellungen“ deaktivieren, indem Sie auf das Schaltersymbol klicken (dies ist beispielsweise hilfreich, wenn Sie 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** des Hauptprogrammfensters.

ESET-Cluster nicht konfiguriert und deaktiviert:



ESET-Cluster richtig mit Details und Optionen konfiguriert:



Weitere Informationen zum ESET-Cluster finden Sie hier.

5.7 Benutzeroberfläche

Im Abschnitt **Benutzeroberfläche** können Sie das Verhalten der grafischen Benutzeroberfläche (GUI) des Programms konfigurieren. Sie können die optische Gestaltung und visuellen Effekte des Programms anpassen.

Um die maximale Sicherheit Ihrer Sicherheitssoftware zu gewährleisten, können Sie unbefugte Änderungen mit dem Tool Einstellungen für den Zugriff verhindern.

Konfigurieren Sie Warnungen und Benachrichtigungen, um festzulegen, wie Warnungen bei erkannten Bedrohungen und Systembenachrichtigungen angezeigt werden sollen. So können Sie diese Funktion Ihren Anforderungen anpassen.

Wenn Sie festlegen, dass bestimmte Benachrichtigungen nicht angezeigt werden sollen, werden diese in die Liste Deaktivierte Nachrichten und Statusmeldungen aufgenommen. Hier können Sie den Status der Hinweise einsehen, sie detaillierter anzeigen lassen oder sie aus dem Fenster entfernen.

Integration in Kontextmenüs wird angezeigt, wenn Sie mit der rechten Maustaste auf ein ausgewähltes Element klicken. Mit diesem Tool können ESET Mail Security-Steuerelemente in das Kontextmenü integriert werden.

Der Präsentationsmodus ist für Benutzer geeignet, die ohne störende Popup-Fenster, ohne geplante Tasks und ohne Komponenten, die die Systemressourcen stark beanspruchen könnten, mit einer Anwendung arbeiten möchten.

Elemente der Benutzeroberfläche

Über die Konfigurationsoptionen für die Benutzeroberfläche von ESET Mail Security können Sie die Arbeitsumgebung an Ihre Anforderungen anpassen. Zugriff auf diese Optionen erhalten Sie unter **Benutzeroberfläche** > **Elemente der Benutzeroberfläche** in den erweiterten Einstellungen von ESET Mail Security.

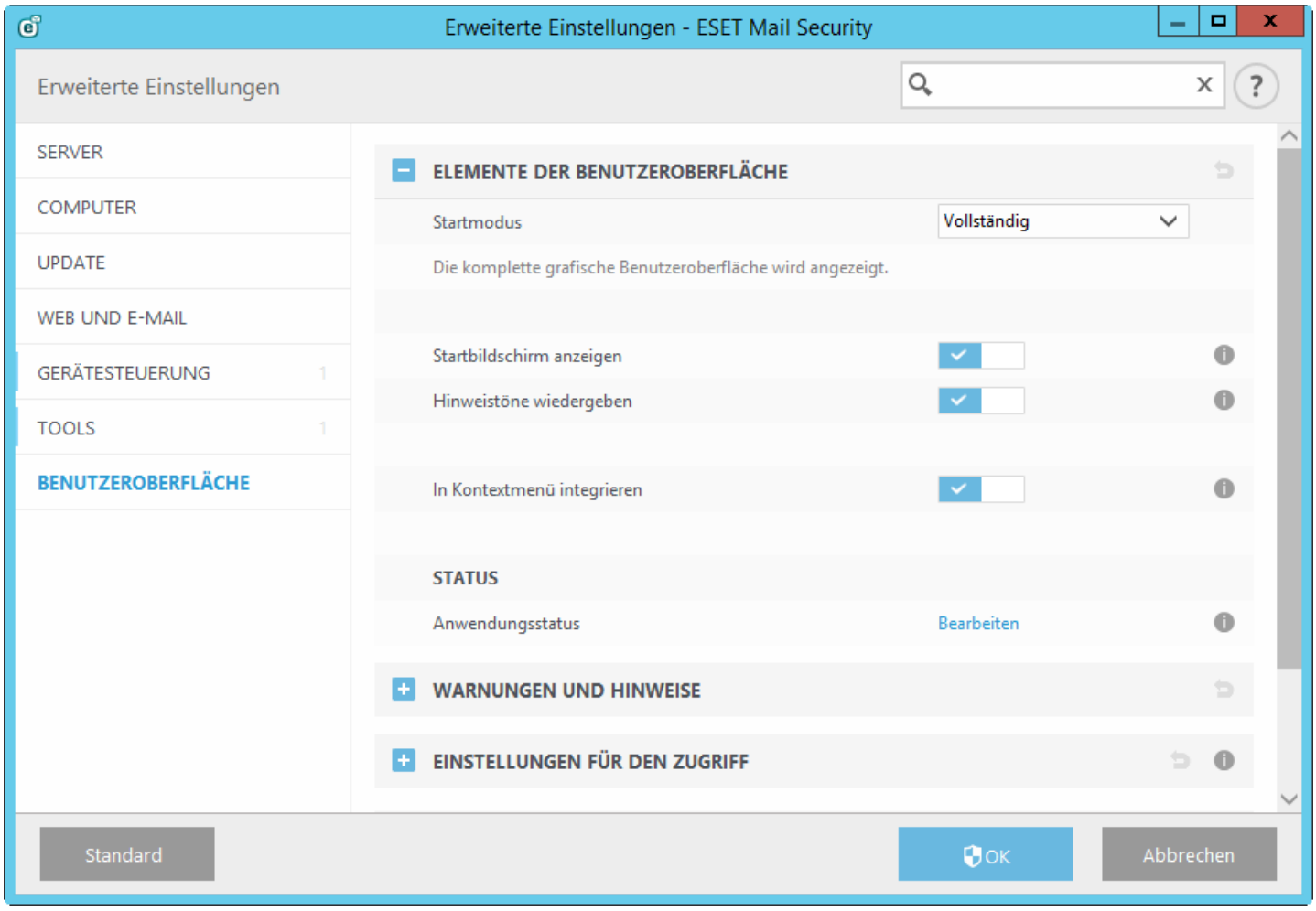
Im Bereich **Elemente der Benutzeroberfläche** können Sie die Arbeitsumgebung anpassen. Die Benutzeroberfläche sollte auf **Terminal** eingestellt werden, wenn durch die grafischen Elemente die Leistung des Computers beeinträchtigt wird oder andere Probleme auftreten. Außerdem können Sie die grafische Benutzeroberfläche für Terminalserver deaktivieren. Weitere Informationen zur Installation von ESET Mail Security auf einem Terminalserver finden Sie im Thema Deaktivieren der Benutzeroberfläche auf Terminalserver.

Klicken Sie auf das Dropdownmenü **Startmodus**, um einen der folgenden Startmodi auszuwählen:
Vollständig - Die komplette Benutzeroberfläche wird angezeigt.
Terminal - Es werden keine Warnungen und Benachrichtigungen angezeigt. Die grafische Benutzeroberfläche kann nur vom Administrator gestartet werden.

Wenn ESET Mail Security ohne Anzeige des Startbilds gestartet werden soll, deaktivieren Sie die Option **Startbild anzeigen**.

Wenn ESET Mail Security bei wichtigen Ereignissen, z. B. bei der Erkennung einer Bedrohung oder wenn eine Prüfung abgeschlossen wird, einen Warnton ausgeben soll, aktivieren Sie die Option **Hinweistöne wiedergeben**.

In Kontextmenü integrieren - ESET Mail Security kann in das Kontextmenü integriert werden.



Status - Klicken Sie auf Bearbeiten, um Status, die im Hauptmenü im Bereich Überwachung angezeigt werden, zu verwalten (zu aktivieren oder zu deaktivieren). **Anwendungstatus** - Mit dieser Option können Sie die Statusanzeige unter **Schutzstatus** im Hauptmenü aktivieren/deaktivieren.

Lizenzinformationen - Mit dieser Option können Sie Lizenzinformationen, Nachrichten und Benachrichtigungen anzeigen.

5.7.1 Warnungen und Hinweise

Im Bereich **Warnungen und Benachrichtigung** unter **Benutzeroberfläche** können Sie festlegen, wie ESET Mail Security mit Bedrohungswarnungen und Systembenachrichtigungen (z. B. über erfolgreiche Updates) umgehen soll. Außerdem können Sie Anzeigedauer und Transparenz von Meldungen in der Taskleiste festlegen (nur bei Systemen, die Meldungen in der Taskleiste unterstützen).

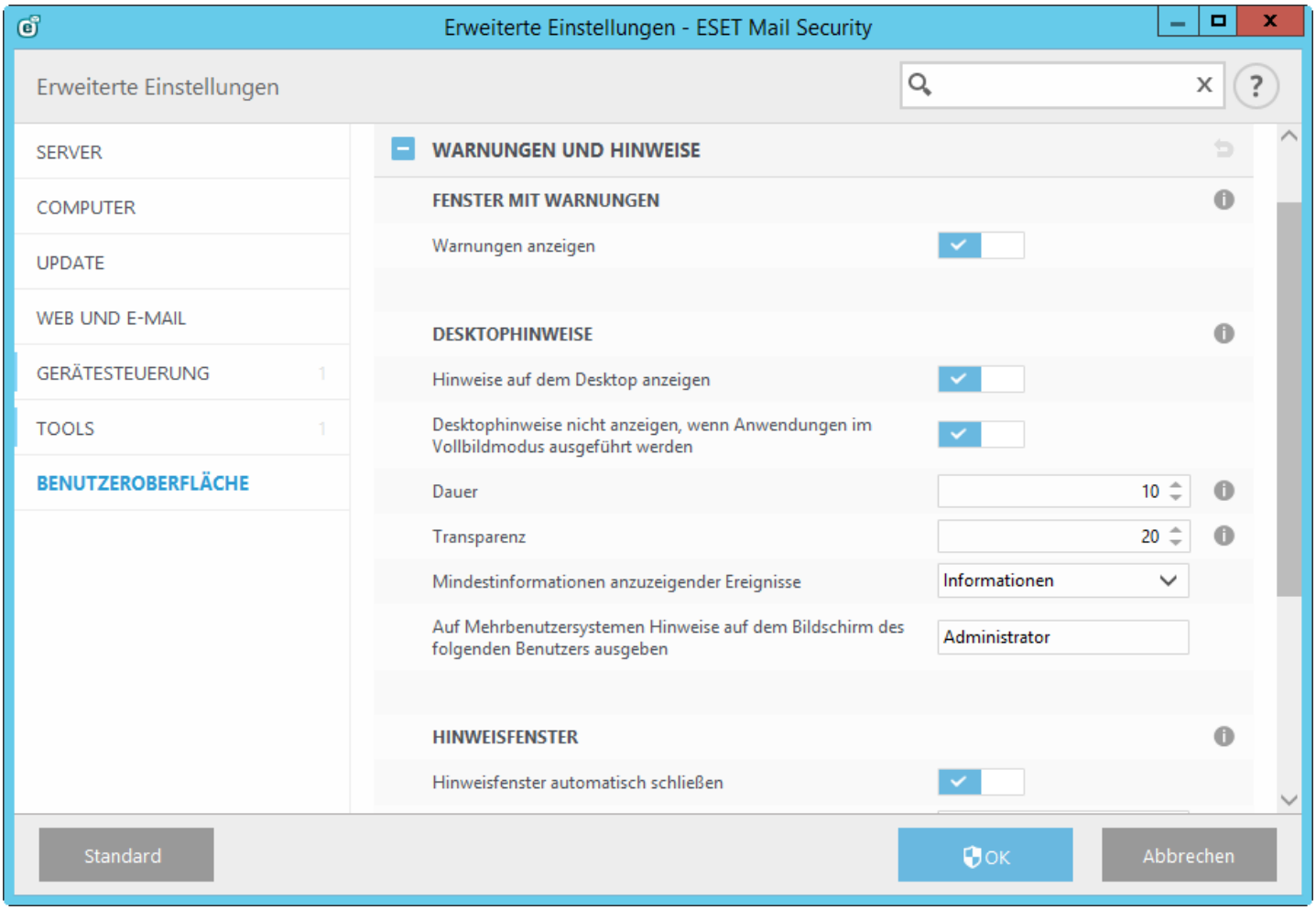
Fenster mit Warnungen

Bei Deaktivieren der Option **Warnungen anzeigen** werden keine Warnmeldungen mehr angezeigt. Diese Einstellung eignet sich nur in einigen speziellen Situationen. Für die meisten Benutzer empfiehlt es sich, die Standardeinstellung (aktiviert) beizubehalten.

Desktopbenachrichtigungen

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. Zum Aktivieren von Desktopbenachrichtigungen aktivieren Sie die Option **Benachrichtigungen auf dem Desktop anzeigen**. Weitere Optionen, wie Anzeigedauer und Transparenzkönnen unten geändert werden.

Aktivieren Sie **Desktopbenachrichtigungen nicht anzeigen, wenn Anwendungen im Vollbildmodus ausgeführt werden**, wenn keine nicht-interaktiven Benachrichtigungen angezeigt werden sollen.



Aus der Liste **Mindestinformationen anzuzeigender Ereignisse** können Sie den niedrigsten Schweregrad der anzuzeigenden Warnungen und Benachrichtigungen wählen. Die folgenden Optionen stehen zur Verfügung:

- **Diagnose** - 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.
- **Kritische Warnungen** - Nur kritische Warnungen (z. B. bei einem Fehler beim Start des Virenschutz-Moduls) werden protokolliert.

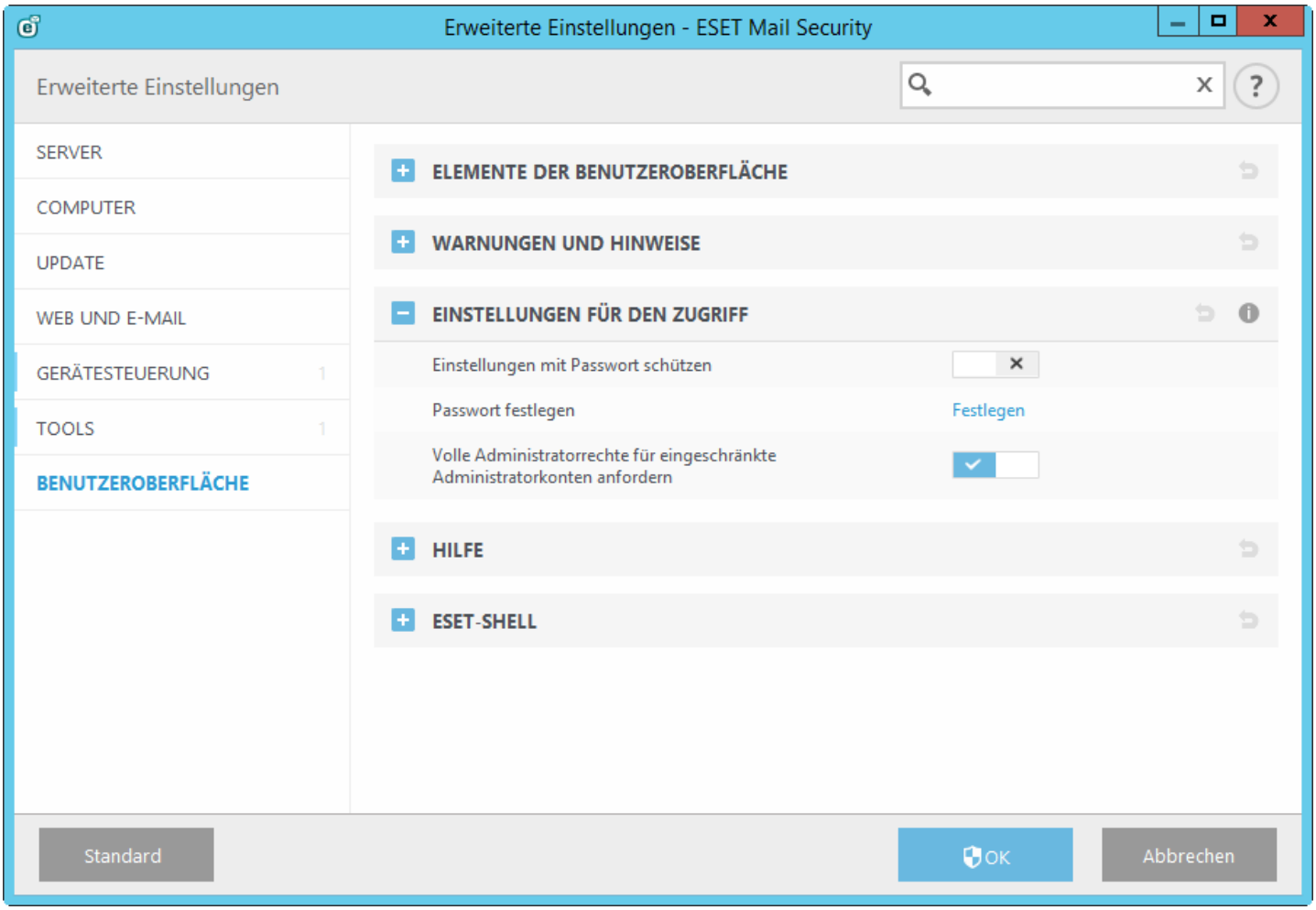
Der letzte Eintrag in diesem Bereich gibt Ihnen die Möglichkeit, die Ausgabe für Meldungen in einer Mehrbenutzerumgebung zu konfigurieren. Mit dem Feld **Auf Mehrbenutzersystemen Benachrichtigungen auf dem Bildschirm des folgenden Benutzers ausgeben** können Sie festlegen, bei welchem Benutzer Warnungen 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, vorausgesetzt alle Systemmeldungen werden an den Administrator gesendet.

Hinweisfenster

Wenn Popup-Fenster nach einer bestimmten Zeit automatisch geschlossen werden sollen, aktivieren Sie die Option **Fenster mit Hinweisen schließen**. Die Hinweise werden nach Ablauf der festgelegten Zeit automatisch geschlossen, sofern sie nicht bereits vom Benutzer geschlossen wurden.

5.7.2 Einstellungen für den Zugriff

Maßgeblich für einen wirksamen Schutz Ihres Systems ist die ordnungsgemäße Konfiguration von ESET Mail Security. Bei unbedachten Änderungen können wichtige Daten verlorengehen. Um unberechtigte Änderungen zu verhindern, können Sie die Einstellungen von ESET Mail Security mit einem Passwort schützen. Die Einstellungen für den Passwortschutz befinden sich in der Baumstruktur der erweiterten Einstellungen im Untermenü **Einstellungen für den Zugriff** im Bereich **Benutzeroberfläche**.



Einstellungen mit Passwort schützen - Sperrt/entsperrt die Programmeinstellungen. Durch Klicken hierauf wird das

Passwortfenster geöffnet.

Klicken Sie auf **Passwort festlegen**, um ein Passwort für den Schutz der Einstellungen anzugeben oder um es zu ändern.

Volle Administratorrechte für eingeschränkte Administratorkonten anfordern - Aktivieren Sie diese Option, damit Benutzer ohne Administratorrechte zur Eingabe eines Administratorbenutzernamens und -passworts aufgefordert werden, wenn sie bestimmte Systemeinstellungen ändern möchten (ähnlich der Benutzerkontensteuerung/UAC in Windows Vista). Dazu gehört das Deaktivieren von Schutzmodulen.

5.7.2.1 Passwort

Um unberechtigte Änderungen zu verhindern, können Sie die Einstellungen von ESET Mail Security mit einem Passwort schützen.

5.7.2.2 Festlegen des Passworts

Zum Schutz der Einstellungsparameter von ESET Mail Security vor unbefugter Änderung 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.

5.7.3 Hilfe

Wenn Sie die Taste **F1** drücken oder auf die Schaltfläche **?** klicken, wird ein Fenster mit der Onlinehilfe geöffnet. Die Onlinehilfe ist die primäre Quelle für Hilfeinhalte. Mit dem Programm wird jedoch auch eine Offlinekopie der Hilfe installiert. Die Offlinehilfe wird geöffnet, wenn keine Internetverbindung vorhanden ist.

Bei funktionierender Internetverbindung wird automatisch die neueste Version der Onlinehilfe angezeigt.

5.7.4 ESET-Shell

Sie können die Zugriffsrechte auf Produkteinstellungen, Funktionen und Daten in eShell konfigurieren, indem Sie die Einstellung **ESET-Shell-Ausführungsrichtlinie** ändern. Die Standardeinstellung ist **Eingeschränktes Scripting**. Sie können dies jedoch bei Bedarf ändern, indem Sie **Deaktiviert**, **Nur Lesezugriff** oder **Vollzugriff** aktivieren.

- **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. 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.

5.7.5 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` 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 terminal
```

Führen Sie den Befehl `get ui ui gui-start-mode` aus, um den aktuellen Modus herauszufinden.

HINWEIS: Falls Sie ESET Mail Security auf einem Citrix-Server installiert haben, sollten Sie die in unserem KB-Artikel empfohlenen Einstellungen verwenden.

5.7.6 Deaktivierte Nachrichten und Statusmeldungen

Bestätigungsmeldungen - Zeigt eine Liste von Bestätigungsmeldungen an, die Sie zur Anzeige oder zur Nicht-Anzeige auswählen können.

Deaktivierte Anwendungs-Statusmeldungen - Mit dieser Option können Sie die Statusanzeige im **Schutzstatusbereich** im Hauptmenü aktivieren/deaktivieren.

5.7.6.1 Bestätigungsnachrichten

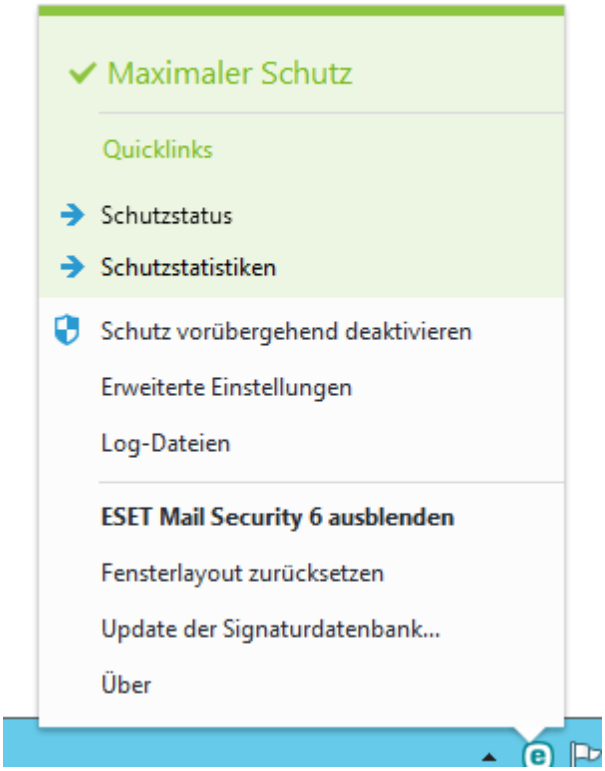
In diesem Dialogfeld werden Bestätigungsmeldungen angezeigt, die von ESET Mail Security vor der Durchführung von Aktionen angezeigt werden. Aktivieren oder deaktivieren Sie die gewünschten Bestätigungsmeldungen, indem Sie das jeweilige Kontrollkästchen markieren oder die Markierung daraus entfernen.

5.7.6.2 Deaktivierte Anwendungs-Statusmeldungen

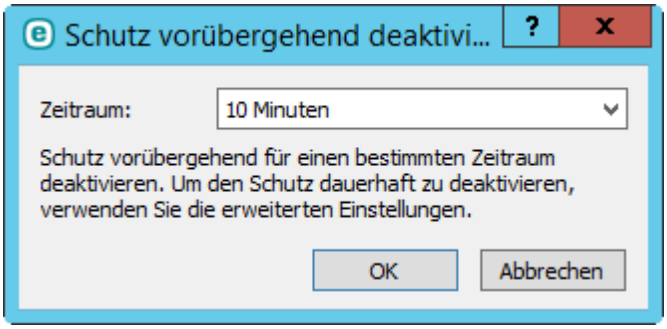
in diesem Fenster können Sie wählen, welche Anwendungs-Statusmeldungen angezeigt werden sollen und welche nicht. Hier können Sie beispielsweise den Viren- und Spyware-Schutz anhalten oder den Präsentationsmodus aktivieren. Wenn Ihr Produkt nicht aktiviert oder Ihre Lizenz abgelaufen ist, wird ebenfalls eine Anwendungs-Statusmeldung angezeigt.

5.7.7 Symbol im Infobereich der Taskleiste

Einige der wichtigsten Einstellungsoptionen und -funktionen können durch Klicken mit der rechten Maustaste auf das Symbol im Infobereich der Taskleiste geöffnet werden.



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.



Über das Dropdown-Menü **Zeitraum** können Sie festlegen, wie lange der Viren- und Spyware-Schutz deaktiviert sein soll.

Erweiterte Einstellungen - Öffnet die Baumstruktur **Erweiterte Einstellungen**. Zugriff auf die erweiterten Einstellungen erhalten Sie auch durch Drücken der Taste F5 oder über **Einstellungen** > **Erweiterte Einstellungen**.

Log-Dateien - Log-Dateien enthalten Informationen zu allen wichtigen aufgetretenen Programmereignissen und geben einen Überblick über erkannte Bedrohungen.

ESET Mail Security minimieren - Blendet das ESET Mail Security-Fenster auf dem Bildschirm aus.

Fensterlayout zurücksetzen - Stellt die standardmäßige Fenstergröße von ESET Mail Security und deren Standardposition auf dem Bildschirm wieder her.

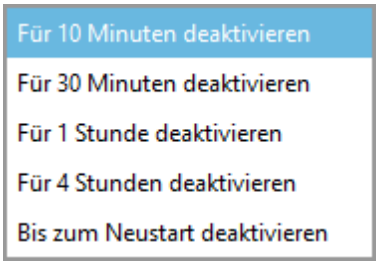
Update der Signaturdatenbank - Beginnt mit der Aktualisierung der Signaturdatenbank, um den Schutz vor Schadcode zu gewährleisten.

Über - Bietet 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.

5.7.7.1 Schutz vorübergehend deaktivieren

Wenn Sie den Viren- und Spyware-Schutz vorübergehend über das Symbol im Infobereich der Taskleiste deaktivieren, wird das Dialogfenster **Vorübergehende Deaktivierung des Schutzes** angezeigt. Der Malware-Schutz wird für die ausgewählte Dauer deaktiviert. Eine dauerhafte Deaktivierung des Schutzes ist nur über die erweiterten Einstellungen möglich. Verwenden Sie diese Möglichkeit mit Vorsicht, da sie Ihr System Bedrohungen aussetzen kann.

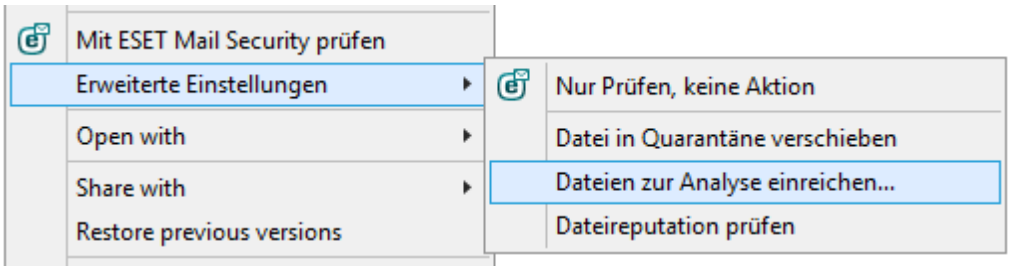


5.7.8 Kontextmenü

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.

Bestimmte Steuerungselemente von ESET Mail Security können in das Kontextmenü integriert werden. Die Einstellungsoptionen für diese Funktion sind unter „Erweiterte Einstellungen“ in **Benutzeroberfläche** > **Elemente der Benutzeroberfläche** verfügbar.

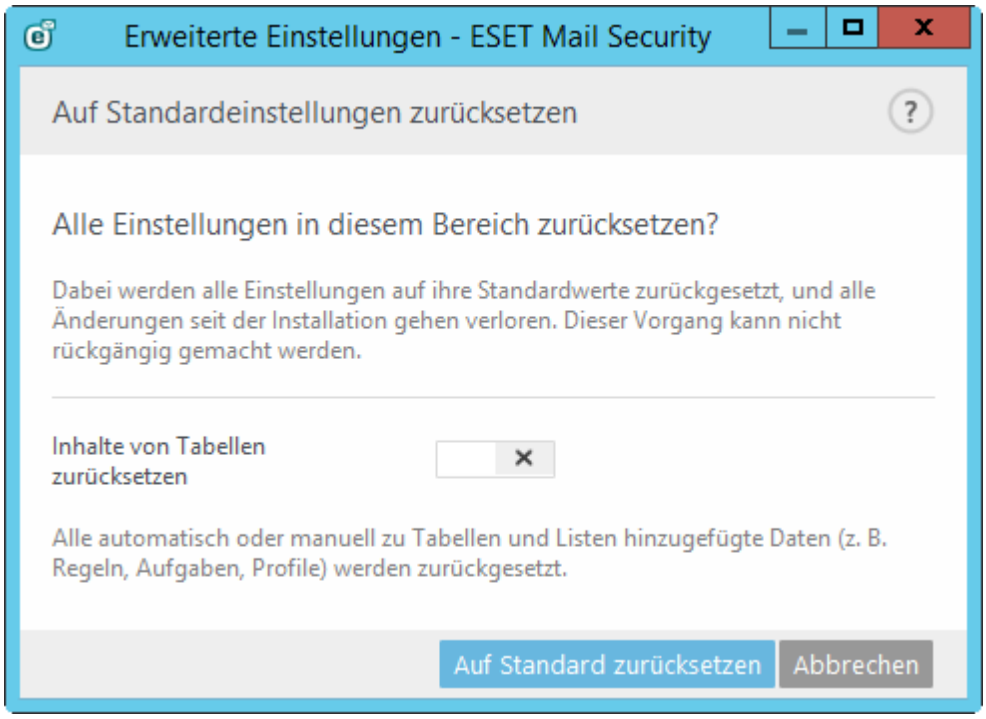
In Kontextmenü integrieren - Integriert die Steuerelemente von ESET Mail Security in das Kontextmenü.



5.8 Alle Einstellungen in diesem Bereich zurücksetzen

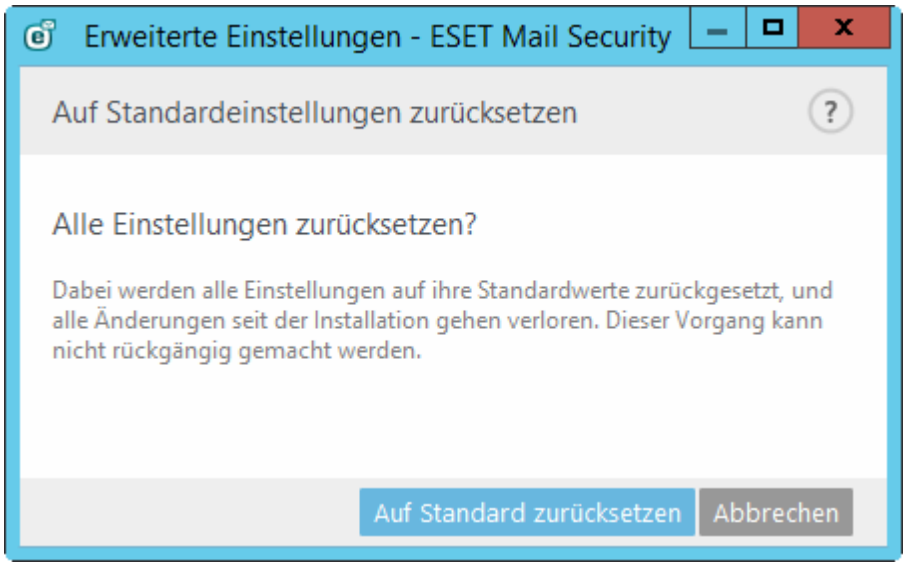
Die Einstellungen des Moduls werden auf die Standardeinstellungen zurückgesetzt. Beachten Sie, dass alle vorgenommenen Änderungen nach dem Klicken auf **Auf Standard zurücksetzen** verloren gehen.

Inhalte von Tabellen zurücksetzen - Wenn diese Option aktiviert ist, gehen manuell oder automatisch hinzugefügte Regeln, Tasks oder Profile verloren.



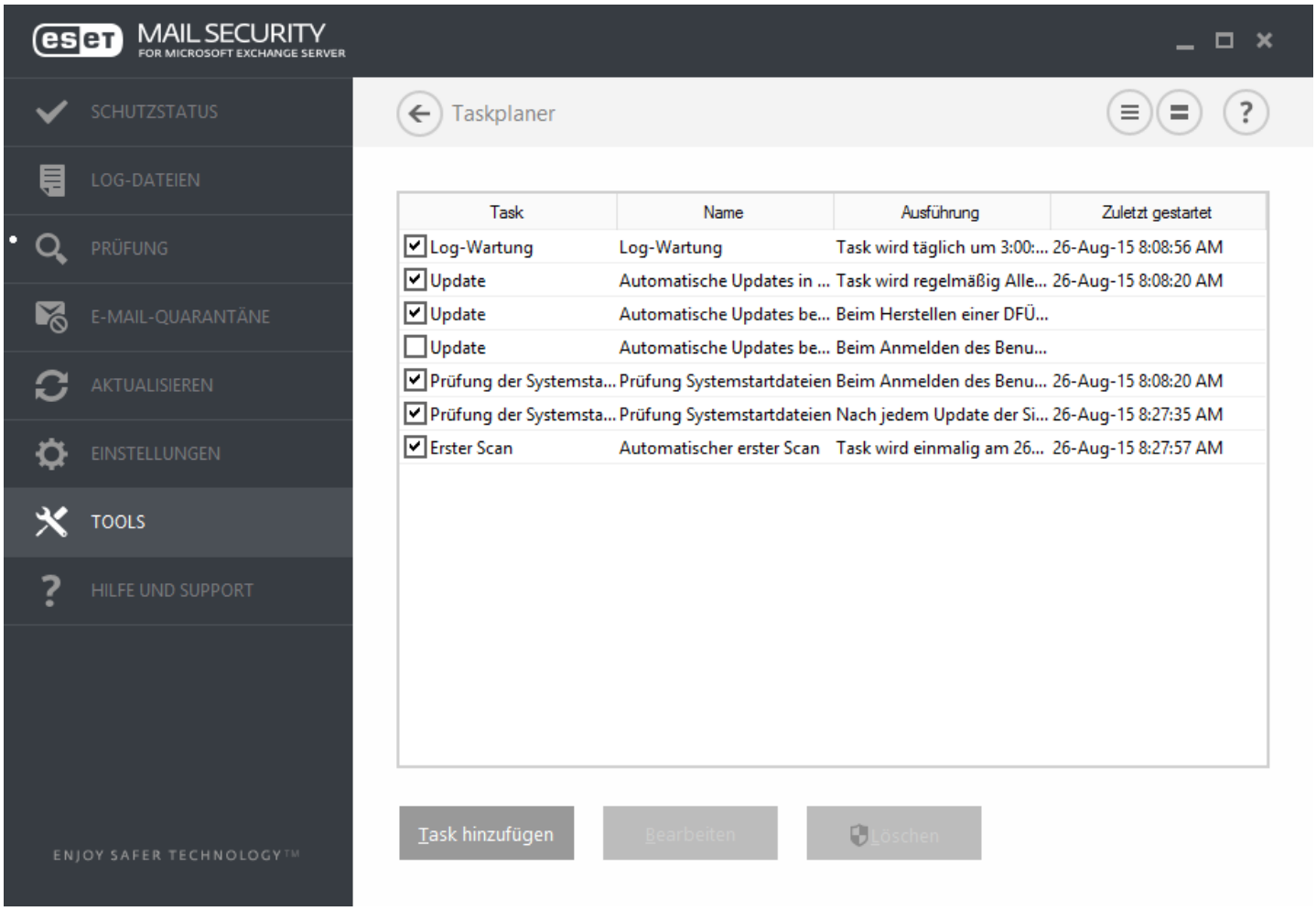
5.9 Auf Standardeinstellungen zurücksetzen

Alle Einstellungen des Programms werden auf die herstellerseitigen Standardwerte zurückgesetzt.



5.10 Taskplaner

Um ihn zu öffnen, klicken Sie im Hauptmenü von ESET Mail Security unter **Tools** auf **Taskplaner**. Der Taskplaner umfasst eine Liste aller geplanten Tasks sowie deren Konfigurationseigenschaften, inklusive des vordefinierten Datums, der Uhrzeit und des verwendeten Prüfprofils.



Standardmäßig werden im **Taskplaner** die folgenden Tasks angezeigt:

- **Log-Wartung**
- **Automatische Updates in festen Zeitabständen**
- **Automatische Updates beim Herstellen von DFÜ-Verbindungen**
- **Automatische Updates beim Anmelden des Benutzers**
- **Prüfung Systemstartdateien (nach Anmeldung des Benutzers)**
- **Prüfung Systemstartdateien (nach Update der Signaturdatenbank)**
- **Automatischer erster Scan**

Um die Konfiguration eines vorhandenen Standardtasks oder eines benutzerdefinierten Tasks zu ändern, klicken Sie mit der rechten Maustaste auf den Task und dann auf **Bearbeiten**, oder wählen Sie den Task aus, den Sie ändern möchten, und klicken Sie auf **Bearbeiten**.

5.10.1 Taskdetails

Geben Sie den Namen des Task ein, wählen Sie einen **Tasktyp** aus und klicken Sie auf **Weiter**:

- **Start externer Anwendung**
- **Log-Wartung**
- **Prüfung Systemstartdateien**
- **Snapshot des Computerstatus erstellen**
- **On-Demand-Scan**
- **Erster Scan**
- **Update**
- **Prüfung der Datenbank**
- **Quarantäneberichte per E-Mail senden -** Verschickt Berichte zur E-Mail-Quarantäne (nur für die lokale Quarantäne) gemäß des geplanten Tasks an ausgewählte E-Mail-Adressen. Falls Sie keine lokale E-Mail-Quarantäne verwenden, werden keine Quarantäne-Berichte verschickt.

Taskausführung- Der angegebene Task wird zum angegeben Zeitpunkt einmalig ausgeführt.

Tasks können übersprungen werden, wenn der Computer ausgeschaltet ist oder im Akkubetrieb läuft. Wählen Sie aus, wann der Task ausgeführt werden soll und klicken Sie auf **Weiter**:

- Zur nächsten geplanten Ausführungszeit
- Baldmöglichst
- Sofort, wenn seit der letzten Ausführung eine bestimmte Zeitdauer (Stunden) überschritten wurde

5.10.2 Taskausführung – einmalig

Taskausführung - Der angegebene Task wird zum angegeben Zeitpunkt einmalig ausgeführt.

5.10.3 Task-Zeitplanung

Der Task wird in dem angegebenen Zeitabstand wiederholt ausgeführt. Wählen Sie eine Zeitangabe aus:

- **Einmalig** - Der Task wird nur einmalig zu einem festgelegten Zeitpunkt ausgeführt.
- **Wiederholt** - Der Task wird in den (in Stunden) angegebenen Zeitabständen ausgeführt.
- **Täglich** - Der Task wird täglich zur festgelegten Uhrzeit ausgeführt.
- **Wöchentlich** - Der Task wird an einem oder mehreren Wochentagen zur festgelegten Uhrzeit ausgeführt.
- **Bei Ereignis** - Der Task wird ausgeführt, wenn ein bestimmtes Ereignis eintritt.

Task im Akkubetrieb überspringen - Wenn sich der Computer zum geplanten Startzeitpunkt des Task im Akkubetrieb befindet, wird der Task nicht gestartet. Dies gilt auch für Computer, die ihren Strom über eine USV (unterbrechungsfreie Stromversorgung) beziehen.

5.10.4 Taskausführung – täglich

Der Task wird täglich zur festgelegten Uhrzeit ausgeführt.

5.10.5 Taskausführung – wöchentlich

Der Task wird am festgelegten Wochentag zur angegebenen Uhrzeit ausgeführt.

5.10.6 Taskausführung – durch Ereignis ausgelöst

Der Task wird durch eines der folgenden Ereignisse ausgelöst:

- **Bei jedem Computerstart**
- **Jeden Tag beim ersten Start des Computers**
- **Wählverbindung zum Internet/VPN**
- **Update der Signaturdatenbank abgeschlossen**
- **Update der Programmkomponenten abgeschlossen**
- **Benutzeranmeldung**
- **Erkennung von Bedrohungen**

Beim Planen eines Vorgangs, der durch ein Ereignis ausgelöst wird, können Sie einen Mindestzeitraum zwischen Ausführungen des Tasks angeben. Wenn Sie sich z. B. mehrmals täglich auf Ihrem Computer anmelden, können Sie „24 Stunden“ auswählen, damit der Task nur bei der ersten Anmeldung des Tages und dann erst wieder am nächsten Tag ausgeführt wird.

5.10.7 Taskdetails – Anwendung ausführen

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 **...** 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).

Klicken Sie auf **Fertig stellen**, um den Task zu übernehmen.

5.10.8 Taskdetails - Quarantäneberichte per E-Mail senden

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

- **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. Sie können mehrere Empfänger angeben.

Klicken Sie auf **Fertig stellen**, um den geplanten Task zu erstellen.

5.10.9 Übersprungener Task

Wenn der Task nicht zur festgelegten Zeit ausgeführt werden konnte, können Sie einen Zeitpunkt für die nächste 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 behinderten, nicht länger gegeben 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.

5.10.10 Task-Eigenschaften

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

5.10.11 Update-Profile

Um das Programm von zwei Update-Servern aus 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.

Weitere Informationen finden Sie im Kapitel Update.

5.10.12 Erstellen von Tasks

Zum Erstellen eines neuen Tasks im Taskplaner klicken Sie auf **Task hinzufügen** oder klicken mit der rechten Maustaste und wählen dann im Kontextmenü **Hinzufügen** aus. Es gibt fünf Arten von Tasks:

- **Start externer Anwendung** - Planen der Ausführung einer externen Anwendung.
- **Log-Wartung** - Log-Dateien enthalten auch unbenutzte leere Einträge von gelöschten Datensätzen. Dieser Task optimiert regelmäßig die Einträge in Log-Dateien.
- **Prüfung Systemstartdateien** - Prüft Dateien, die während des Systemstarts oder 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-Scan** - Scannt die Dateien und Ordner auf Ihrem Computer.
- **Erster Scan** - Standardmäßig wird 20 Minuten nach Installation oder Neustart ein Scan als Task mit geringer Priorität ausgeführt.
- **Update** - Erstellt einen Update-Task. Dieser besteht aus der Aktualisierung der Signaturdatenbank und der Aktualisierung der Programmmodule.

Da **Update**-Tasks zu den meistverwendeten Tasks gehören, wird im Folgenden das Hinzufügen eines neuen Update-Tasks beschrieben.

Geben Sie im Feld **Taskname einen Namen für den Task** ein. Wählen Sie in der Dropdownloste **Tasktyp** den Eintrag **Update** aus und klicken Sie auf **Weiter**.
Aktivieren Sie den Task über den Schalter **Aktiviert** (Sie können den Task auch später über das Kontrollkästchen in der Liste der geplanten Tasks aktivieren/deaktivieren), klicken Sie auf **Weiter** und wählen Sie eine Zeitangabe aus: **Einmalig**, **Wiederholt**, **Täglich**, **Wöchentlich** und **Bei Ereignis**. Je nach ausgewähltem Intervall werden Ihnen verschiedene Update-Parameter angezeigt. Im nächsten Schritt können Sie eine Aktion festlegen für den Fall, dass der Task zur geplanten Zeit nicht ausgeführt oder abgeschlossen werden kann. Folgende Optionen stehen zur Verfügung:

- **Zur nächsten geplanten Ausführungszeit**
- **Baldmöglichst**
- **Sofort ausführen, wenn Intervall seit letzter Ausführung überschritten** (das Intervall kann über das entsprechende Feld festgelegt werden)

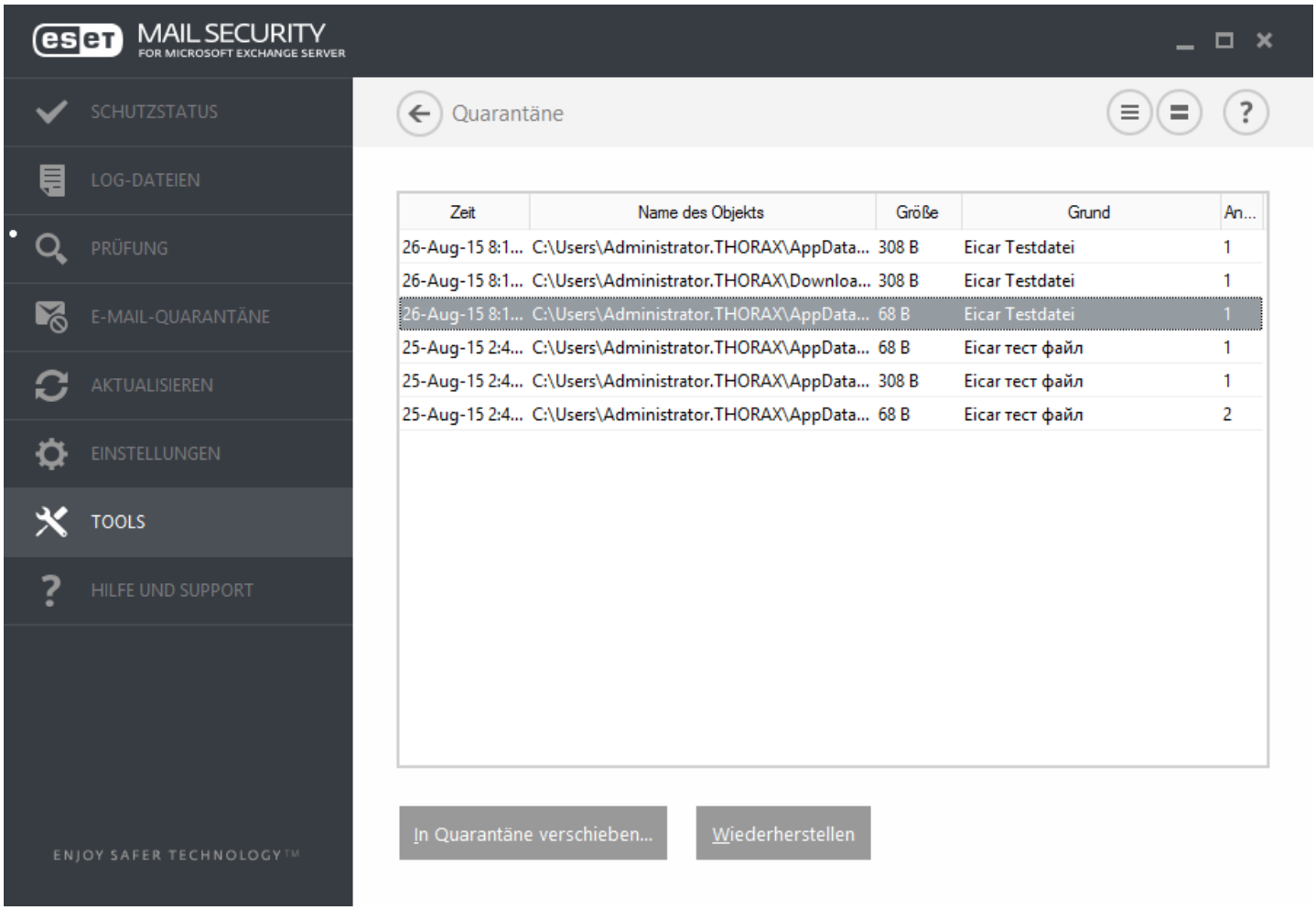
Anschließend wird ein Fenster mit einer vollständigen Zusammenfassung des aktuellen Tasks angezeigt. Klicken Sie auf **Fertig stellen**, wenn Sie Ihre Änderungen abgeschlossen haben.

Es wird ein Dialogfenster angezeigt, in dem Sie die Profile für den Task auswählen können. Hier können Sie das primäre und das alternative Profil festlegen. Das alternative Profil wird verwendet, wenn der Task mit dem primären Profil nicht abgeschlossen werden kann. Bestätigen Sie Ihre Auswahl durch Klicken auf **Fertig stellen**. Der neue geplante Task wird der Liste der geplanten Tasks hinzugefügt.

5.11 Quarantäne

Die Hauptfunktion der Quarantäne ist die sichere Verwahrung infizierter Dateien. 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 worden sind.

Sie können beliebige Dateien gezielt in die Quarantäne verschieben. Geschehen sollte dies bei Dateien, die sich verdächtig verhalten, bei der Virenprüfung jedoch 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.

Quarantäne für Dateien

ESET Mail Security verschiebt gelöschte Dateien automatisch in den Quarantäneordner (sofern diese Option nicht im Warnfenster deaktiviert wurde). Auf Wunsch können Sie beliebige verdächtige Dateien manuell in die Quarantäne verschieben, indem Sie auf **Quarantäne** klicken. In die Quarantäne verschobene Dateien werden von ihrem ursprünglichen Speicherort entfernt. Alternativ kann auch das Kontextmenü zu diesem Zweck verwendet werden: Klicken Sie mit der rechten Maustaste in das Fenster **Quarantäne**, und wählen Sie **Quarantäne** aus.

Wiederherstellen aus der Quarantäne

Dateien aus der Quarantäne können auch an ihrem ursprünglichen Speicherort wiederhergestellt werden. Verwenden Sie hierzu die Funktion **Wiederherstellen** aus dem Kontextmenü, das Sie über einen 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 Scans ausschließen** verfügbar. Weitere Informationen zu diesem Anwendungstyp finden Sie im Glossar. Das Kontextmenü enthält außerdem die Option **Wiederherstellen nach ...**, mit der Dateien an einem anderen als ihrem ursprünglichen Speicherort wiederhergestellt werden können.

HINWEIS: 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 darauf und wählen im angezeigten Kontextmenü die Option **Datei zur Analyse einreichen** aus.

5.11.1 Quarantäne für Dateien

ESET Mail Security verschiebt gelöschte Dateien automatisch in den Quarantäneordner (sofern diese Option nicht im Warnfenster deaktiviert wurde). Auf Wunsch können Sie beliebige verdächtige Dateien manuell in die Quarantäne verschieben, indem Sie auf **Quarantäne** klicken. In diesem Fall wird die Originaldatei nicht 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.

5.11.2 Wiederherstellen aus Quarantäne

Dateien aus der Quarantäne können auch an ihrem ursprünglichen Speicherort wiederhergestellt werden. Um eine Datei aus der Quarantäne wiederherzustellen, klicken Sie mit der rechten Maustaste in das Quarantänefenster und wählen Sie im Kontextmenü **Wiederherstellen** aus. Wenn eine Datei als Eventuell unerwünschte Anwendung gekennzeichnet ist, wird die Funktion **Wiederherstellen und von Scans ausschließen** verfügbar. Das Kontextmenü enthält außerdem die Option **Wiederherstellen nach ...**, mit der Dateien an einem anderen als ihrem ursprünglichen Speicherort wiederhergestellt werden können.

Löschen aus der Quarantäne - Klicken Sie mit der rechten Maustaste auf ein Element und wählen Sie **Aus Quarantäne löschen** aus. Alternativ können Sie das zu löschende Element auswählen und auf der Tastatur die Entf-Taste drücken. Sie können auch mehrere Einträge gleichzeitig auswählen und gesammelt löschen.

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

5.11.3 Einreichen von Dateien 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 darauf und wählen im angezeigten Kontextmenü die Option **Datei zur Analyse einreichen**.

5.12 Betriebssystem-Updates

Das Fenster „System-Updates“ listet verfügbare Updates auf, die heruntergeladen und installiert werden können. Neben dem Namen des Updates wird die Update-Priorität angezeigt.

Klicken Sie auf **System-Update durchführen**, um mit dem Herunterladen und Installieren zu beginnen.

Klicken Sie mit der rechten Maustaste auf ein beliebiges Update und klicken Sie dann auf **Information anzeigen**, um ein Fenster mit zusätzlichen Informationen anzuzeigen.

6. Glossar

6.1 Schadsoftwaretypen

Bei Schadsoftware handelt es sich um bösartige Software, die versucht, in einen Computer einzudringen und/oder auf einem Computer Schaden anzurichten.

6.1.1 Viren

Bei einem Computervirus handelt es sich um eingedrungene Schadsoftware, die Dateien auf Ihrem Computer beschädigt. Ihren Namen haben sie nicht umsonst mit den Viren aus der Biologie gemein. Schließlich verwenden sie ähnliche Techniken, um sich von einem zum anderen Computer auszubreiten.

Computerviren greifen hauptsächlich ausführbare Dateien und Dokumente an. Um sich zu vermehren, hängt sich ein Virus mit seinem "Körper" an das Ende einer Zieldatei. Und so funktioniert ein Computervirus: Durch Ausführung der infizierten Datei wird der Virus aktiviert (noch bevor die eigentliche Anwendung gestartet wird) und führt seine vordefinierte Aufgabe aus. Erst dann wird die eigentliche Anwendung gestartet. Ein Virus kann einen Computer also nur dann infizieren, wenn der Benutzer selbst (versehentlich oder absichtlich) das bösartige Programm ausführt oder öffnet.

Computerviren unterscheiden sich nach Art und Schweregrad der durch sie verursachten Schäden. Einige von ihnen sind aufgrund ihrer Fähigkeit, Dateien von der Festplatte gezielt zu löschen, äußerst gefährlich. Andererseits gibt es aber auch Viren, die keinen Schaden verursachen. Ihr einziger Zweck besteht darin, den Benutzer zu verärgern und die technischen Fähigkeiten ihrer Urheber unter Beweis zu stellen.

Viren werden (im Vergleich zu Trojanern oder Spyware) immer seltener, da sie keinen kommerziellen Nutzen für ihre Urheber haben. Außerdem wird der Begriff "Virus" oft fälschlicherweise für alle Arten von Schadsoftware verwendet. Heute setzt sich mehr und mehr der neue, treffendere Ausdruck "Malware" (engl. bösartige Software) durch.

Wenn Ihr Computer mit einem Virus infiziert wurde, ist es notwendig, den Originalzustand der infizierten Dateien wiederherzustellen, das heißt, den Schadcode mithilfe eines Virenschutzprogrammes daraus zu entfernen.

Beispiele für Viren sind: OneHalf, Tenga und Yankee Doodle.

6.1.2 Würmer

Bei einem Computerwurm handelt es sich um ein Programm, das bösartigen Code enthält, der Hostcomputer angreift und sich über Netzwerke verbreitet. Der grundlegende Unterschied zwischen Viren und Würmern besteht darin, dass Würmer in der Lage sind, sich selbstständig zu vermehren und zu verbreiten. Sie sind unabhängig von Hostdateien (oder Bootsektoren). Würmer verbreiten sich über die E-Mail-Adressen in Ihrer Kontaktliste oder nutzen Sicherheitslücken von Anwendungen in Netzwerken.

Daher sind Würmer wesentlich funktionsfähiger als Computerviren. Aufgrund der enormen Ausdehnung des Internets können sich Würmer innerhalb weniger Stunden und sogar Minuten über den gesamten Globus verbreiten. Da sich Würmer unabhängig und rasant vermehren können, sind sie gefährlicher als andere Arten von Schadsoftware.

Ein innerhalb eines Systems aktivierter Wurm kann eine Reihe von Unannehmlichkeiten verursachen: Er kann Dateien löschen, die Systemleistung beeinträchtigen oder Programme deaktivieren. Aufgrund ihrer Beschaffenheit können Würmer als Transportmedium für andere Arten von Schadcode fungieren.

Wurde Ihr Computer mit einem Wurm infiziert, empfiehlt es sich, alle betroffenen Dateien zu löschen, da sie höchstwahrscheinlich Schadcode enthalten.

Zu den bekanntesten Würmern zählen: Lovsan/Blaster, Stration/Warezov, Bagle und Netsky.

6.1.3 Trojaner

Trojaner galten früher als eine Klasse von Schadprogrammen, die sich als nützliche Anwendungen tarnen, um den Benutzer zur Ausführung zu verleiten. Dies gilt jedoch nur für die Trojaner von damals. Heutzutage müssen sich Trojaner nicht mehr tarnen. Ihr einzige Absicht besteht darin, sich möglichst leicht Zugang zu einem System zu verschaffen, um dort den gewünschten Schaden anzurichten. Der Ausdruck "Trojaner" ist zu einem sehr allgemeinen Begriff geworden, der jegliche Form von Schadsoftware beschreibt, die nicht einer bestimmten Kategorie zugeordnet werden kann.

Aus diesem Grund wird die Kategorie "Trojaner" oft in mehrere Gruppen unterteilt:

- **Downloader** - Ein bösartiges Programm zum Herunterladen von Schadsoftware aus dem Internet
- **Dropper** - Trojaner, der auf angegriffenen Computern weitere Schadsoftware absetzt ("droppt")
- **Backdoor** - Anwendung, die Angreifern Zugriff auf ein System verschafft, um es zu kontrollieren
- **Keylogger** - Programm, das die Tastenanschläge eines Benutzers aufzeichnet und die Informationen an Angreifer sendet
- **Dialer** - Dialer sind Programme, die Verbindungen zu teuren Einwahlnummern herstellen. Dass eine neue Verbindung erstellt wurde, ist für den Benutzer nahezu unmöglich festzustellen. Dialer sind nur eine Gefahr für Benutzer von Einwahlmodems. Diese werden allerdings nur noch selten eingesetzt

Trojaner sind in der Regel ausführbare Dateien mit der Erweiterung EXE. Wenn auf Ihrem Computer eine Datei als Trojaner identifiziert wird, sollte diese gelöscht werden, da sie mit hoher Wahrscheinlichkeit Schadcode enthält.

Zu den bekanntesten Trojanern zählen: NetBus, Trojandownloader. Small.ZL, Slapper.

6.1.4 Rootkits

Rootkits sind bösartige Programme, die Hackern unbegrenzten und verdeckten Zugriff auf ein System verschaffen. Nach dem Zugriff auf ein System (in der Regel unter Ausnutzung einer Sicherheitslücke) greifen Rootkits auf Funktionen des Betriebssystems zurück, um nicht von der Virenschutz-Software erkannt zu werden: Prozesse, Dateien und Windows-Registrierungsdaten werden versteckt. Aus diesem Grund ist es nahezu unmöglich, Rootkits mithilfe der üblichen Prüfmethoden zu erkennen.

Rootkits können auf zwei verschiedenen Ebenen entdeckt werden:

1) Beim Zugriff auf ein System. Die Rootkits haben das System noch nicht befallen, sind also inaktiv. Die meisten Virenschutzsysteme können Rootkits auf dieser Ebene entfernen (vorausgesetzt, dass solche Dateien auch als infizierte Dateien erkannt werden).
2) Wenn die Rootkits sich vor den regulären Prüfmethoden verstecken. Benutzer von ESET Mail Security haben den Vorteil der Anti-Stealth-Technologie, die auch aktive Rootkits erkennen und entfernen kann.

6.1.5 Adware

Adware ist eine Abkürzung für durch Werbung (engl. Advertising) unterstützte Software. In diese Kategorie fallen Programme, die zur Anzeige von Werbung dienen. Adware-Anwendungen öffnen häufig in Internetbrowsern neue Popup-Fenster mit Werbung oder ändern die Startseite des Browsers. Adware gehört oftmals zu Freeware-Programmen, damit deren Entwickler auf diesem Weg die Entwicklungskosten ihrer (gewöhnlich nützlichen) Anwendungen decken können.

Adware selbst ist nicht gefährlich - allerdings werden die Benutzer mit Werbung belästigt. Bedenklich ist Adware, insofern sie auch dazu dienen kann, Daten zu sammeln (wie es bei Spyware der Fall ist).

Wenn Sie sich dafür entscheiden, ein Freeware-Produkt zu verwenden, sollten Sie bei der Installation besonders aufmerksam sein. Die meisten Installationsprogramme benachrichtigen Sie über die Installation eines zusätzlichen Adware-Programms. In vielen Fällen ist es möglich, diesen Teil der Installation abzubrechen und das Programm ohne Adware zu installieren.

In einigen Fällen lassen sich Programme jedoch nicht ohne die Adware installieren, oder nur mit eingeschränktem

Funktionsumfang. Das bedeutet, dass Adware häufig ganz "legal" auf das System zugreift, da sich der Benutzer damit einverstanden erklärt hat. In diesem Fall gilt: Vorsicht ist besser als Nachsicht. Wenn auf Ihrem Computer eine Datei als Adware identifiziert wird, muss diese gelöscht werden, da sie mit hoher Wahrscheinlichkeit Schadcode enthält.

6.1.6 Spyware

Der Begriff "Spyware" fasst alle Anwendungen zusammen, die vertrauliche Informationen ohne das Einverständnis/Wissen des Benutzers versenden. Diese Programme verwenden Überwachungsfunktionen, um verschiedene statistische Daten zu versenden, z. B. eine Liste der besuchten Websites, E-Mail-Adressen aus dem Adressbuch des Benutzers oder eine Auflistung von Tastatureingaben.

Die Entwickler von Spyware geben vor, auf diesem Weg die Interessen und Bedürfnisse der Benutzer erkunden zu wollen. Ziel sei es, gezieltere Werbeangebote zu entwickeln. Das Problem dabei ist, dass nicht wirklich zwischen nützlichen und bösartigen Anwendungen unterschieden werden kann. Niemand kann sicher sein, dass die gesammelten Informationen nicht missbraucht werden. Die von Spyware gesammelten Daten enthalten möglicherweise Sicherheitscodes, PINs, Kontonummern usw. Spyware wird oft im Paket mit der kostenlosen Version eines Programms angeboten, um so Einkünfte zu erzielen oder einen Anreiz für den Erwerb der kommerziellen Version zu schaffen. Oft werden die Benutzer bei der Programminstallation darüber informiert, dass Spyware eingesetzt wird, um sie damit zu einem Upgrade auf die kommerzielle, Spyware-freie Version zu bewegen.

Beispiele für bekannte Freeware-Produkte, die zusammen mit Spyware ausgeliefert werden, sind Client-Anwendungen für P2P-Netzwerke. Programme wie Spyfalcon oder Spy Sheriff gehören zur einer besonderen Kategorie von Spyware: Getarnt als Spyware-Schutzprogramme üben sie selbst Spyware-Funktionen aus.

Wenn auf Ihrem Computer eine Datei als Spyware identifiziert wird, sollte diese gelöscht werden, da sie mit hoher Wahrscheinlichkeit Schadcode enthält.

6.1.7 Packprogramme

Ein Packprogramm ist eine selbstextrahierende, ausführbare Anwendung, mit der verschiedene Arten Malware in einem einzigen Paket kombiniert werden können.

Zu den bekanntesten Packprogrammen zählen UPX, PE_Compact, PKLite und ASPack. Die Erkennung einer bestimmten Malware unterscheidet sich je nach dem verwendeten Packprogramm. Packprogramme können außerdem ihre "Signatur" verändern, sodass die Malware schwieriger zu erkennen und zu entfernen ist.

6.1.8 Exploit-Blocker

Der Exploit-Blocker sichert besonders anfällige Anwendungen wie Webbrowser, PDF-Leseprogramme, E-Mail-Programme oder MS Office-Komponenten ab. Er überwacht das Verhalten von Prozessen auf verdächtige Aktivitäten, die auf einen Exploit hinweisen könnten. Mit seiner komplett neuen Technologie, die über das bloße Fokussieren auf die Erkennung schädlicher Dateien hinausgeht, sorgt er für zusätzlichen Schutz, da er Angreifern immer einen Schritt voraus ist.

Wenn der Exploit-Blocker einen verdächtigen Prozess identifiziert, kann er ihn sofort anhalten und Daten über die Bedrohung erfassen, die dann an das ESET Live Grid-Cloudsystem gesendet werden. Diese Daten werden durch ESET analysiert und genutzt, um alle Anwender besser vor unbekannten Bedrohungen und neuesten Angriffen durch Malware, für die noch keine Erkennungssignaturen vorhanden sind, zu schützen.

6.1.9 Erweiterter Speicher-Scan

Der erweiterte Speicher-Scan bietet im Zusammenspiel mit dem Exploit-Blocker einen besseren Schutz vor Malware, die darauf ausgelegt ist, der Erkennung durch Anti-Malware-Produkte mittels Verschleierung und/oder Verschlüsselung zu entgehen. In Fällen, in denen herkömmliche Emulation oder Heuristik eine Bedrohung eventuell nicht aufspüren, kann die erweiterte Speicherprüfung verdächtiges Verhalten identifizieren und Bedrohungen erkennen, wenn sie sich im Arbeitsspeicher manifestieren. Diese Lösung kann selbst gegen stark verschleierte Malware wirkungsvoll agieren. Anders als der Exploit-Blocker sucht der erweiterte Speicher-Scan nach ausgeführter Malware. Damit ist das Risiko verbunden, dass vor der Erkennung einer Bedrohung bereits schädliche Aktivitäten durchgeführt wurden. falls jedoch andere Erkennungsmethoden versagt haben, bietet sie eine zusätzliche Schutzebene.

6.1.10 Potenziell unsichere Anwendungen

Es gibt zahlreiche seriöse Programme, die die Verwaltung miteinander vernetzter Computer vereinfachen sollen. Wenn sie aber in die falschen Hände geraten, kann mit ihnen Schaden angerichtet werden. Mit ESET Mail Security können solche Bedrohungen erkannt werden.

potenziell unsichere Anwendungen sind kommerzielle, rechtmäßige Programme. Dazu zählen beispielsweise Programme für den Remotezugriff auf Computer, Programme zum Entschlüsseln von Passwörtern und Keylogger (Programme, die Tastaturanschläge von Benutzern aufzeichnen).

Sollten Sie feststellen, dass auf Ihrem Computer eine potenziell unsichere Anwendung vorhanden ist (die Sie nicht selbst installiert haben), wenden Sie sich an Ihren Netzwerkadministrator oder entfernen Sie die Anwendung.

6.1.11 Eventuell unerwünschte Anwendungen

Eventuell unerwünschte Anwendungen sind Programme, die zwar nicht unbedingt Sicherheitsrisiken in sich bergen, aber auf Leistung und Verhalten Ihres Computers negative Auswirkungen haben können. Als Benutzer werden Sie normalerweise vor deren Installation zur Bestätigung aufgefordert. Nach erfolgter Installation ändert sich das Systemverhalten (im Vergleich zum Stand vor der Installation). Die gravierendsten Veränderungen sind:

- Neue Fenster werden angezeigt (Popup-Fenster, Werbung)
- Versteckte Prozesse werden gestartet und ausgeführt
- Prozessor und Speicher werden stärker belastet als zuvor
- Suchergebnisse ändern sich
- Die Anwendung kommuniziert mit Servern im Internet

6.2 E-Mails

Die E-Mail ("elektronische Post") ist ein modernes Kommunikationsmittel mit vielen Vorteilen. Dank ihrer Flexibilität, Schnelligkeit und Direktheit spielte die E-Mail bei der Verbreitung des Internets in den frühen 1990er Jahren eine entscheidende Rolle.

Doch aufgrund der Anonymität, die E-Mails und das Internet bieten, wird diese Kommunikationsform auch häufig für illegale Aktivitäten wie das Versenden von Spam-Mails genutzt. Als "Spam" gelten z. B. unerwünschte Werbeangebote, Hoaxes (Falschmeldungen) und E-Mails, mit denen Schadsoftware verbreitet werden soll. Die Belästigung und Gefährdung durch Spam wird zusätzlich dadurch gefördert, dass E-Mails praktisch kostenlos versendet werden können und den Verfassern von Spam-Mails verschiedenste Tools und Quellen zur Verfügung stehen, um an neue E-Mail-Adressen zu gelangen. Die große Anzahl und Vielfalt, in der Spam-Mails auftreten, erschwert die Kontrolle. Je länger Sie eine E-Mail-Adresse verwenden, desto wahrscheinlicher ist es, dass diese in einer Spam-Datenbank erfasst wird. Einige Tipps zur Vorbeugung:

- Veröffentlichen Sie Ihre E-Mail-Adresse, soweit möglich, nicht im Internet
- Geben Sie Ihre E-Mail-Adresse nur an vertrauenswürdige Personen weiter
- Benutzen Sie, wenn möglich, keine üblichen Aliasnamen - bei komplizierten Aliasnamen ist die Wahrscheinlichkeit der Verfolgung niedriger

- Antworten Sie nicht auf Spam-Mails, die sich in Ihrem Posteingang befinden
- Seien Sie vorsichtig, wenn Sie Internetformulare ausfüllen - achten Sie insbesondere auf Optionen wie "Ja, ich möchte per E-Mail informiert werden".
- Verwenden Sie separate E-Mail-Adressen - z. B. eine für Ihre Arbeit, eine für die Kommunikation mit Freunden usw.
- Ändern Sie Ihre E-Mail-Adresse von Zeit zu Zeit
- Verwenden Sie eine Spamschutz-Lösung

6.2.1 Werbung

Werbung im Internet ist eine der am schnellsten wachsenden Formen von Werbung. Die wesentlichen Vorteile für das Marketing liegen im geringen finanziellen Aufwand und dem hohen Grad von Direktheit. Davon abgesehen erreichen E-Mails die Empfänger fast ohne Zeitverzögerung. In vielen Unternehmen werden E-Mail-Marketingtools für eine effektive Kommunikation mit aktuellen und zukünftigen Kunden verwendet.

Da Sie Interesse an kommerziellen Informationen zu bestimmten Produkten haben könnten, handelt es sich dabei um rechtmäßige Werbung. Doch vielfach werden unerwünschte Massen-E-Mails mit Werbung versendet. In solchen Fällen ist die Grenze der E-Mail-Werbung überschritten, und diese E-Mails gelten als Spam.

Die Masse der unerwünschten E-Mails hat sich zu einem Problem entwickelt, ohne dass ein Nachlassen abzusehen ist. Die Verfasser unerwünschter E-Mails versuchen häufig, Spam-E-Mails wie rechtmäßige Nachrichten aussehen zu lassen.

6.2.2 Falschmeldungen (Hoaxes)

Ein Hoax ist eine Spam-Nachricht, die über das Internet verbreitet wird. Hoaxes werden im Allgemeinen per E-Mail oder über Kommunikationstools wie ICQ oder Skype versendet. Der Inhalt der Nachricht ist meist ein Scherz oder eine Falschmeldung.

Oft werden dabei Falschmeldungen zu angeblichen Computerviren verbreitet. Der Empfänger soll verunsichert werden, indem ihm mitgeteilt wird, dass sich auf seinem Computer ein "nicht identifizierbarer Virus" befindet, der Dateien zerstört, Passwörter abruft oder andere schädliche Vorgänge verursacht.

Es kommt vor, dass ein Hoax den Empfänger auffordert, die Nachricht an seine Kontakte weiterzuleiten, wodurch er sich verbreitet. Es gibt verschiedenste Arten von Hoaxes - Mobiltelefon-Hoaxes, Hilferufe, Angebote zu Geldüberweisungen aus dem Ausland usw. Häufig ist es nicht möglich, die tatsächliche Absicht des Autors zu durchschauen.

Wenn Sie eine Nachricht lesen, in der Sie aufgefordert werden, diese an alle Ihre Kontakte weiterzuleiten, so handelt es sich möglicherweise um einen Hoax. Es gibt viele Internetseiten, auf denen Sie prüfen können, ob eine E-Mail rechtmäßig ist oder nicht. Bevor Sie eine fragliche Nachricht weiterleiten, versuchen Sie über eine Internetsuche abzuklären, ob es sich um einen Hoax handelt.

6.2.3 Phishing

Der Begriff "Phishing" bezeichnet eine kriminelle Vorgehensweise, die sich Techniken des Social Engineering (Manipulation von Benutzern zur Erlangung vertraulicher Informationen) zunutze macht. Das Ziel von Phishing ist es, an vertrauliche Daten wie Kontonummern, PIN-Codes usw. heranzukommen.

Der Zugriff auf vertrauliche Informationen wird oft durch das Versenden von E-Mails erreicht, die von einer scheinbar vertrauenswürdigen Person bzw. von einem scheinbar seriösen Unternehmen (z. B. Finanzinstitution, Versicherungsunternehm) stammen. Eine solche E-Mail kann sehr echt aussehen. Grafiken und Inhalte wurden möglicherweise sogar von der Quelle entwendet, die nachgeahmt werden soll. Sie werden unter einem Vorwand (Datenprüfung, finanzielle Transaktionen usw.) aufgefordert, persönliche Daten einzugeben, wie Ihre Bankverbindung, Benutzernamen und Passwörter. Alle diese Daten, werden Sie denn übermittelt, können mühelos gestohlen oder missbraucht werden.

Banken, Versicherungen und andere rechtmäßige Unternehmen fragen nie in einer E-Mail nach Benutzername und

Passwort.

6.2.4 Erkennen von Spam-Mails

Es gibt verschiedene Anzeichen, die darauf hindeuten, dass es sich bei einer fraglichen E-Mail in Ihrem Postfach um Spam handelt. Wenn eines oder mehrere der folgenden Kriterien zutreffen, handelt es sich höchstwahrscheinlich um eine Spam-Nachricht:

- Die Adresse des Absenders steht nicht in Ihrer Kontaktliste
- Ihnen wird ein größerer Geldbetrag in Aussicht gestellt, Sie sollen jedoch zunächst eine kleinere Summe zahlen
- Sie werden unter einem Vorwand (Datenprüfung, finanzielle Transaktionen usw.) aufgefordert, persönliche Daten einzugeben, wie Ihre Bankverbindung, Benutzernamen und Passwörter.
- Die Nachricht ist in einer anderen Sprache verfasst
- Sie werden aufgefordert, ein Produkt zu erwerben, das Sie nicht bestellt haben. Falls Sie das Produkt dennoch kaufen möchten, prüfen Sie, ob die Absenderadresse eine vertrauenswürdige ID ist (fragen Sie beim Hersteller nach)
- Einige Wörter sind falsch geschrieben, um den Spamfilter zu umgehen. Z. B. "Vaigra" statt "Viagra" usw.

6.2.4.1 Regeln

Im Kontext von Spam-Schutz-Lösungen und E-Mail-Programmen dienen Regeln der Steuerung von E-Mail-Funktionen. Regeln setzen sich aus zwei logischen Teilen zusammen:

1) einer Bedingung (z. B. einer eingehenden Nachricht von einer bestimmten Adresse)

2) einer Aktion (z. B. das Löschen der Nachricht bzw. das Verschieben der Nachricht in einen angegebenen Ordner)

Je nach Virenschutzlösung gibt es unterschiedlich viele Regeln und Kombinationsmöglichkeiten. Die Regeln dienen als Maßnahme gegen Spam (unerwünschte E-Mail-Nachrichten). Typische Beispiele sind:

- 1. Bedingung: Eine eingehende E-Mail-Nachricht enthält einige der Wörter, die häufig in Spam-Nachrichten vorkommen. 2. Aktion: Nachricht löschen
- 1. Bedingung: Eine eingehende E-Mail-Nachricht enthält einen Anhang mit der Erweiterung „EXE“. 2. Aktion: Anhang löschen und Nachricht dem Postfach zustellen
- 1. Bedingung: Der Absender einer eingehenden Nachricht ist Ihr Arbeitgeber. 2. Aktion: Nachricht in den Ordner "Arbeit" verschieben

Wir empfehlen Ihnen, in Spam-Schutz-Programmen verschiedene Regeln miteinander zu kombinieren, um die Verwaltung zu vereinfachen und den Spam-Schutz noch effektiver zu gestalten.

6.2.4.2 Bayesscher Filter

Die bayessche Filtermethode ist eine effektive Form der E-Mail-Filterung, die von fast allen Spam-Schutz-Produkten verwendet wird. Ein solcher Filter kann unerwünschte E-Mails mit hohem Genauigkeitsgrad erkennen und für jeden Benutzer separat konfiguriert werden.

Bayessche Filter funktionieren nach folgendem Prinzip: In der ersten Phase findet ein Lernprozess statt. Der Benutzer kennzeichnet manuell eine ausreichende Anzahl von E-Mails als rechtmäßig oder als Spam (gewöhnlich 200/200). Der Filter analysiert beide Kategorien und lernt so zum Beispiel, dass in Spam-E-Mails häufig die Wörter "Rolex" oder "Viagra" auftreten, während rechtmäßige E-Mails von Familienmitgliedern oder von Adressen in der Kontaktliste des Benutzers gesendet werden. Sofern eine ausreichende Anzahl von Nachrichten verarbeitet wurde, kann der bayessche Filter jede E-Mail mit einem bestimmten "Spam-Index" versehen und so festlegen, ob sie als Spam gilt oder nicht.

Der größte Vorteil dieses Filters liegt in seiner Flexibilität. Ist ein Benutzer etwa Biologe, erhalten alle eingehenden E-Mails in Bezug auf Biologie oder verwandte Forschungsfelder im Allgemeinen einen geringeren Wahrscheinlichkeitsindex. Wenn eine E-Mail Wörter enthält, durch die sie normalerweise als unerwünscht

klassifiziert würde, der Absender jedoch zu den Kontakten des Benutzers gehört, wird sie als rechtmäßig eingestuft, da sich bei Absendern aus der eigenen Kontaktliste die Gesamtwahrscheinlichkeit für Spam verringert.

6.2.4.3 Positivliste

Im Allgemeinen handelt es sich bei einer Positivliste (auch "Whitelist") um eine Liste von Objekten oder Personen, die akzeptiert werden oder denen eine Berechtigung eingeräumt worden ist. Der Begriff "E-Mail-Positivliste" bezeichnet eine Liste von Kontakten, von denen der Nutzer Nachrichten erhalten möchte. Solche Positivlisten beruhen auf Stichwörtern, nach denen E-Mail-Adressen, Domain-Namen oder IP-Adressen durchsucht werden.

Ist bei einer Positivliste der "Exklusiv-Modus" aktiviert, werden Nachrichten von jeder anderen Adresse, Domain oder IP-Adresse zurückgewiesen. Ist dieser Modus jedoch nicht aktiviert, werden solche Nachrichten nicht etwa gelöscht, sondern auf andere Art und Weise geprüft.

Eine Positivliste beruht somit auf dem entgegengesetzten Prinzip einer Negativliste Blacklist. Im Vergleich zu Negativlisten sind Positivlisten relativ pflegeleicht. Es wird empfohlen, sowohl eine Positiv- als auch eine Negativliste zu verwenden, damit Spam effektiver gefiltert werden kann.

6.2.4.4 Negativliste

Eine Negativliste bezeichnet im Allgemeinen eine Liste unerwünschter oder verbotener Personen oder Dinge. In der virtuellen Welt handelt es sich um eine Technik, die das Annehmen von E-Mail-Nachrichten aller Absender erlaubt, die nicht in einer solchen Liste stehen.

Es gibt zwei Arten von Negativlisten. Solche, die vom Benutzer in seinem Spam-Schutz-Programm eingerichtet wurden, und professionelle, von spezialisierten Institutionen erstellte und regelmäßig aktualisierte Negativlisten, die im Internet verfügbar sind.

Das Verwenden von Negativlisten ist eine wesentliche Technik zur erfolgreichen Spam-Filterung, allerdings sind Negativlisten schwierig zu pflegen, da täglich neue Einträge anfallen. Für effektiven Spam-Schutz empfehlen wir Ihnen, sowohl eine Positivliste als auch eine Negativliste zu führen.

6.2.4.5 Serverseitige Kontrolle

Die serverseitige Kontrolle ist eine Technik zur Erkennung von massenweise versendeten Spam-E-Mails auf Basis der Anzahl empfangener Nachrichten und der Reaktionen von Benutzern. Jede E-Mail-Nachricht hinterlässt einen eindeutigen digitalen Footprint ("Fußabdruck"), der sich nach dem Inhalt der Nachricht richtet. Diese eindeutige ID-Nummer lässt keine Rückschlüsse über den Inhalt zu. Zwei identische Nachrichten besitzen denselben Footprint, verschiedene E-Mails auch verschiedene Footprints.

Wenn eine E-Mail als Spam eingestuft wird, wird der Footprint dieser E-Mail an den Server gesendet. Wenn der Server weitere identische Footprints empfängt (die einer bestimmten Spam-E-Mail entsprechen), wird dieser Footprint in einer Datenbank gespeichert. Beim Prüfen eingehender E-Mails sendet das Programm die Footprints der E-Mails an den Server. Der Server gibt Informationen darüber zurück, welche Footprints E-Mails entsprechen, die von Benutzern bereits als Spam eingestuft worden sind.