Avira Exchange Security 11

Kurzanleitung

AVIRA

Inhaltsverzeichnis

Allgemeine Informationen

Alle für die Installation erforderlichen Installationspakete sowie die Produkthandbücher im PDF-Format finden Sie zum Download auf unserer Internetseite.

Hinweis
Für die unterschiedlichen MS Exchange Systeme werden unterschiedliche Installationspakete angeboten! Bitte achten Sie darauf, dass Sie das richtige Installationspaket (Exchange 2000/2003 oder 2007) verwenden.
Für Informationen über die Cluster-Installation wenden Sie sich bitte an den Avira-Support.

Systemvoraussetzungen

Es ist zu beachten, dass vor jeglicher Installation von „Avira Exchange Security 11“, die Mindestsystemvoraussetzungen erfüllt sein müssen.

Betriebssysteme (32-Bit / 64-Bit)

- Windows Server 2003 (einschließlich der aktuellen Service Packs und Patches)
- Windows Server 2008 (einschließlich der aktuellen Service Packs und Patches)
- Windows Server 2008 R2 (einschließlich der aktuellen Service Packs und Patches)

MS Exchange Server

- MS Exchange Server 2003 (oder höher, d.h. SP1/SP2 inkl. alle aktuellen Security Updates)
- MS Exchange Server 2007 SP1 Update Rollup 4 (64-Bit) (oder höher, d.h. SP2/SP3 inkl. aller aktuellen Rollups)
- MS Exchange Server 2010 (64 Bit) (oder höher, d.h. SP1/SP2 inkl. aller aktuellen Rollups)

RAM

- Exchange Empfehlung & zusätzlich 64 MB

Festplatte

- Mindestens 400 MB für die Installation

Sonstiges

- CD-ROM-Laufwerk oder Netzwerkzugriff
- Microsoft .NET Framework 3.5
- 100 MB für Ereignisprotokollierung empfohlen
- Internetzugang, für das Update von Engines (Scan- und Antispam-Engine)

- Benutzerberechtigungen: Im Active Directory angemeldeter Benutzer mit vollem Lesezugriff auf das Active Directory.

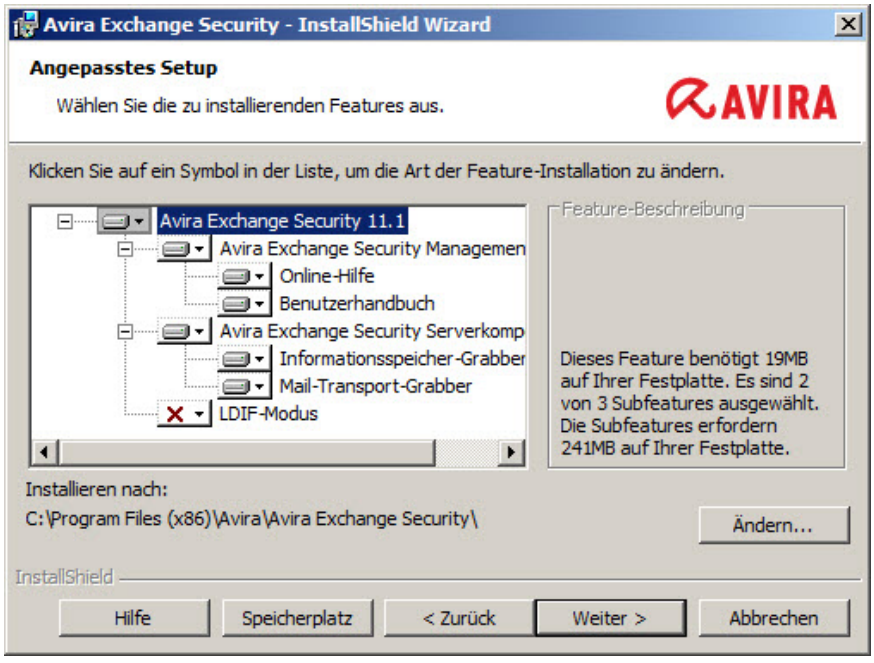
Betriebssysteme für Avira Exchange Management Konsole

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows XP Professional
- Windows Vista
- Windows 7

1. Installation der „Avira Exchange Security“

Nachdem Sie das Installationspaket von „Avira Exchange Security“ heruntergeladen haben, starten Sie dieses bitte auf Ihrem „Microsoft Exchange Mailserver“.

Im Laufe der Installation erscheint ein Fenster, in dem Sie die zu installierenden Komponenten auswählen können. Achten Sie darauf, dass hier sowohl die Management-Konsole als auch die Serverkomponenten ausgewählt sind.



Nach Auswahl der zu installierenden Komponenten werden Sie nach einer bestehenden Konfiguration gefragt.

Dieses Fenster ist nur dann interessant, wenn bereits eine ältere Installation von „AntiVir Exchange“ im Einsatz war und nun ersetzt wurde.

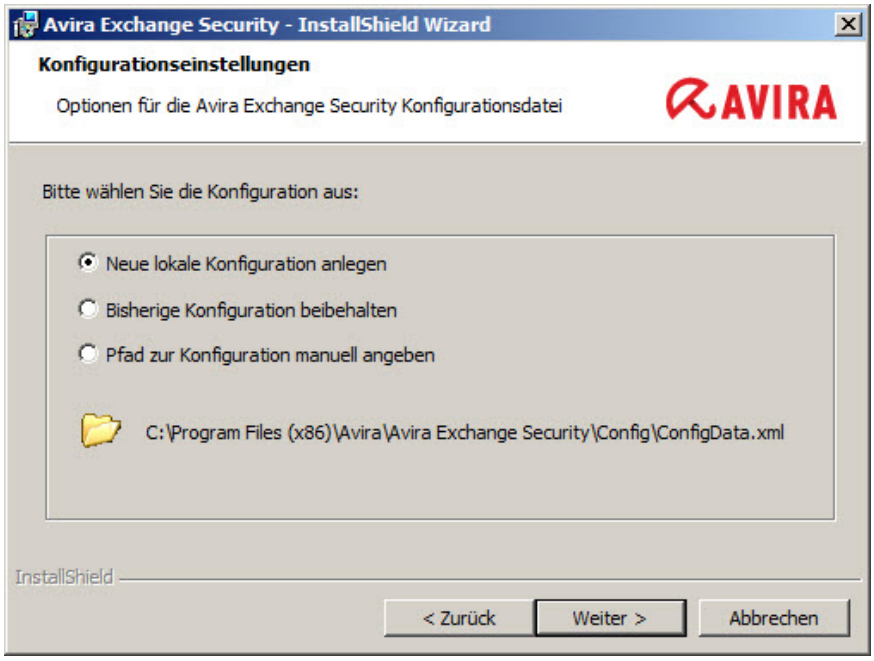
Zur Auswahl stehen hier drei mögliche Auswahlfelder:

- **Neue lokale Konfiguration anlegen**
  Diesen Punkt wählen Sie dann, wenn keine bisherige Konfiguration besteht, oder es sich um eine Erstinstallation handelt.

- **Bisherige Konfiguration beibehalten**
  Hier legen Sie bei einer erneuten Installation fest, dass die bereits hinterlegten Konfigurationen beibehalten werden sollen. Die Datei *ConfigData.xml* muss sich hierfür im Installationsverzeichnis von Avira Exchange Security befinden.

- **Pfad zur Konfiguration manuell angeben**
  Sollte sich die Konfiguration in einem anderen Verzeichnis befinden, kann hier der genaue Pfad mit angegeben werden.

Hinweis:
Der hier hinterlegte Pfad kann im Anschluss nicht mehr geändert werden!



In den weiteren Schritten werden Sie nun gebeten einige administrative Voreinstellungen festzulegen. Diese beinhalten eine Emailadresse des zuständigen Administrators und einen eventuell vorhandenen Proxyserver für das Internet Update.

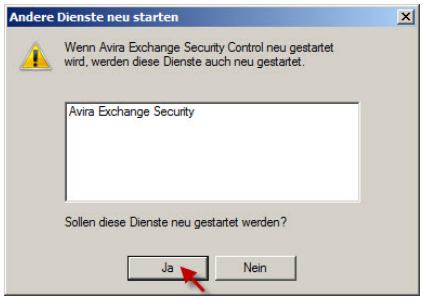
Diese Einstellungen werden während der Installation im Programm hinterlegt, können aber auch im Anschluss in der Konfigurationsdatei *savapi.ini* angepasst werden.

2. Lizenzierung

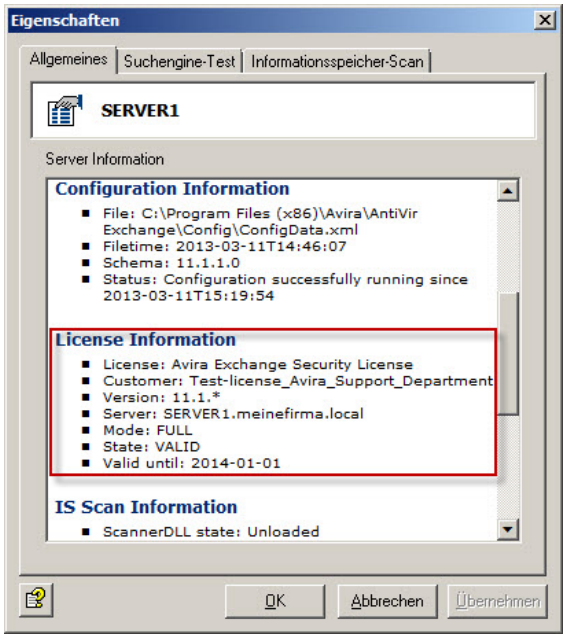
Während der Installation wird die Lizenzdatei abgefragt und korrekt eingebunden. Bei einem späteren Lizenzwechsel gehen Sie bitte wie folgt vor:

- Kopieren Sie die Datei *HBEDV.key*, welche Sie per Email erhalten haben, in das Installationsverzeichnis von Avira Exchange. Hier wurde bereits ein Verzeichnis mit dem Namen „License“ angelegt, in welchem die Datei abgelegt werden muss. Das Verzeichnis „License“ enthält bereits eine Datei mit dem Namen *oem.lic*, welche sich auch weiterhin dort befinden muss

- Nachdem Sie die Lizenzdatei in das entsprechende Verzeichnis kopiert haben, ist ein Neustart des Dienstes „Avira Exchange Security Control“ erforderlich. Während des Neustarts erhalten Sie einen Hinweis, dass der Dienst „Avira Exchange Security“ ebenfalls neu gestartet wird, bitte bestätigen Sie dies mit **Ja**



Um zu prüfen, ob die Lizenzdatei richtig eingespielt wurde, starten Sie die „Avira Exchange Security Management Konsole“ und öffnen dort den Bereich: „Avira Monitor“. Öffnen Sie nun die Eigenschaften Ihres Servers, um im folgenden Fenster die Lizenzinformationen zu prüfen:

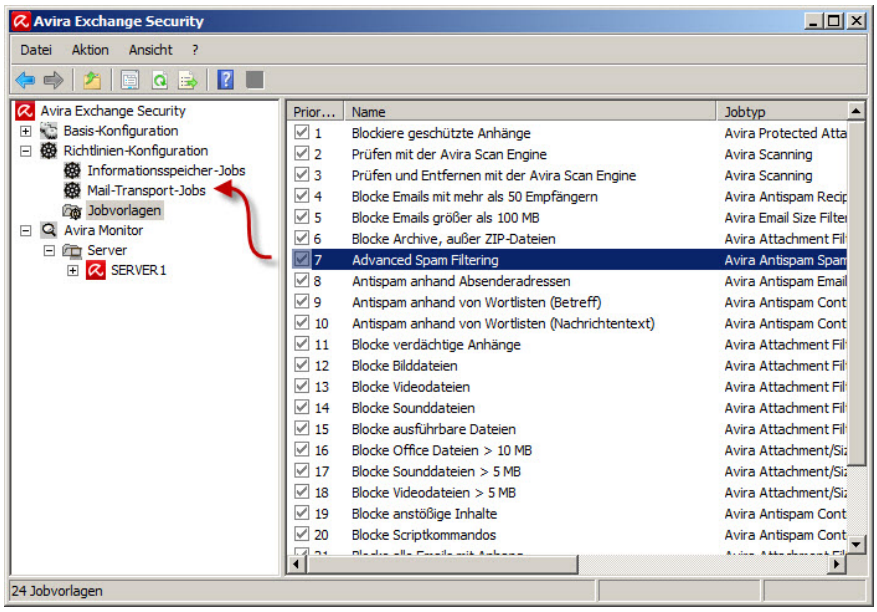


Hier sehen Sie nun Ihre Lizenzinformationen, die Werte *Mode: FULL* und *State: VALID* zeigen, dass die Lizenz richtig ausgelesen wurde und gültig ist. Sollte dies nicht der Fall sein, kontrollieren Sie bitte mit Hilfe der Textdatei *lic_info.txt*, ob Sie die richtige Lizenzdatei verwendet haben. Wenden Sie sich bitte ggf. an den Avira Support und senden Sie uns die Lizenzdatei zur Kontrolle zu.

3. Anlegen neuer Email Filter

Direkt nach der Installation ist das Produkt bereits vorkonfiguriert. Eingehende Emails werden schon auf Viren geprüft und bei einem Fund in die Quarantäne verschoben. Um die Email-Filterung zu erweitern und weitere Jobs einzubinden, können Sie die bereits mitgelieferten Jobvorlagen verwenden.

Hier finden Sie vorkonfigurierte Jobs, die den bereits aktiven Virenscanner um eine Spamfilterung, oder einen Content- / Attachement-Filter erweitern.

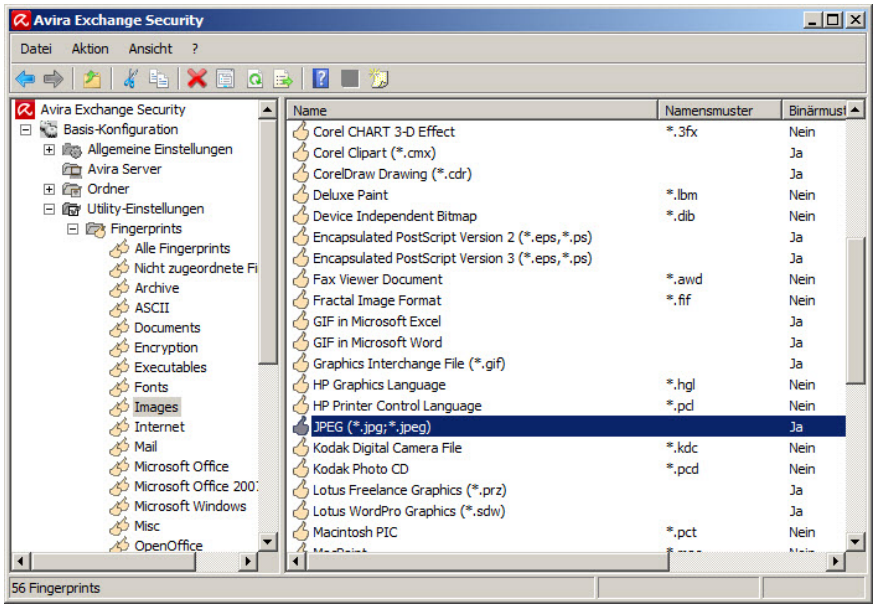


Um einen Job Ihrer Wahl für die Filterung zu aktivieren, ziehen Sie diesen einfach per *Drag&Drop* in die „Mail-Transport-Jobs“. Dort kann dieser dann aktiviert bzw. konfiguriert werden.

Hinweis:
Sollten Sie nicht sicher sein, welcher Filter für Sie der Richtige ist, empfehlen wir Ihnen den „Advanced Spam Filtering“ Job, welcher bereits mehrere Filter-methoden beinhaltet und daher eine gute Erkennungsrate liefert.

Andere Jobs filtern den Inhalt der Emails z.B. anhand von Fingerprints. Als Fingerprint bezeichnen wir das Muster der jeweiligen Datei. Diese Muster werden entweder über die Dateiendung oder über ein Binärmuster der entsprechenden Datei klassifiziert.

Zum Beispiel: *Basis-Konfiguration > Utility-Einstellungen > Fingerprints > Images*



Die einzelnen Dateimuster sind in Gruppen sortiert, so enthält z.B. die Gruppe Images eine Vielzahl bekannter Dateiendungen und Binärmuster.
Die Fingerprint-Gruppe „Images“ wird nun einem Job zugeteilt. Dieser Job filtert eingehende Emails und überprüft, ob diese einen der genannten Fingerprints enthält.

Job Beispiel	**Funktion**
Blocke Bilddateien	Dieser Job greift auf die Fingerprint-Gruppe „Images“ zu. Hier bekommt er die Information, was eine Bilddatei ist und woran er diese erkennen kann.
Blocke Videodateien	Das Prinzip der Fingerprints ist hier dasselbe wie bei den Bilddateien, lediglich die Gruppe ist eine andere und damit sind auch die Dateimuster anders. Verwendete Gruppe: „Video“
Blocke Archive, außer ZIP-Dateien	Hier kommen zwei Filterrichtlinien zum Einsatz: die Fingerprint-Gruppe „Archive“, diese enthält alle bekannten Archivtypen und dient dem Job als Dateizuordnung. Der Fingerprint „Zip-Archive“ ist jedoch in den Einstellungen dieses Jobs als Ausnahme deklariert.

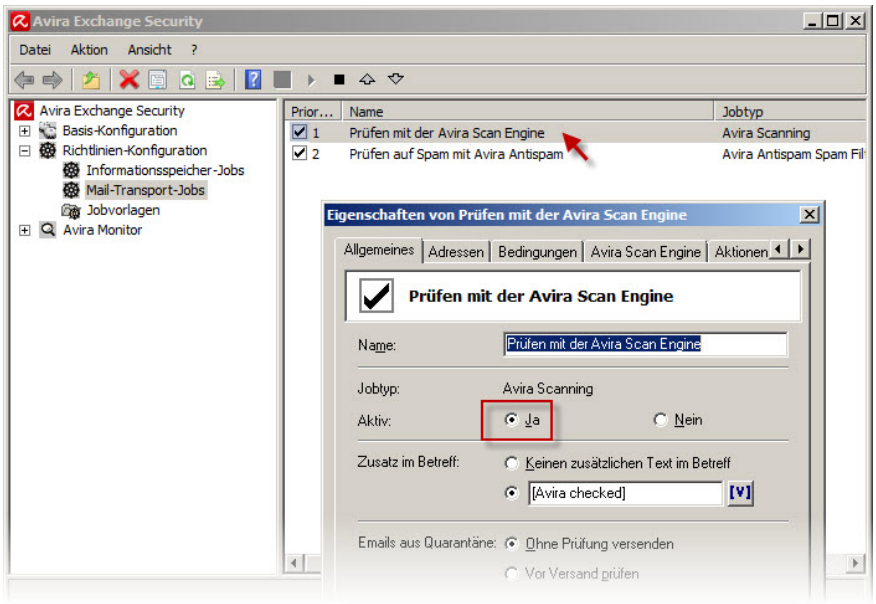
4. Konfiguration der Email Filter

In Anbetracht dessen, dass die meisten Filter bereits vorkonfiguriert sind, ist eine Anpassung nicht zwingend erforderlich. Sollten Sie diese Standardeinstellungen nicht verwenden, können die Filter individuell angepasst werden.

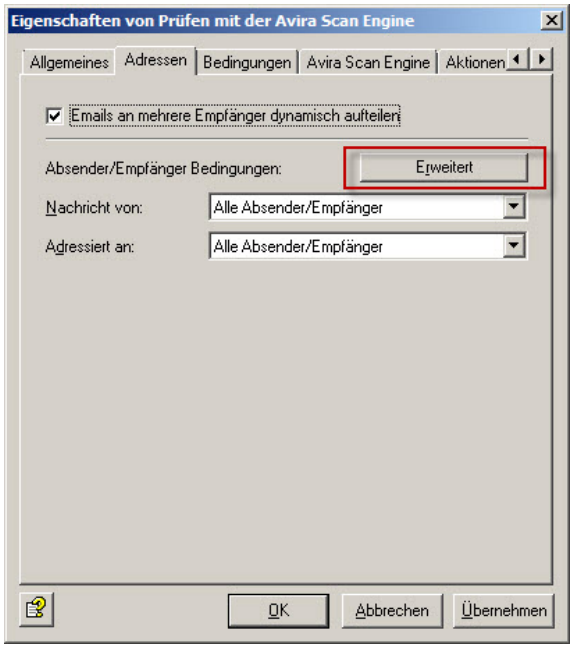
Die Eigenschaften für die Konfiguration lassen sich mit einem Doppelklick auf den gewünschten Job öffnen.

Hinweis:
Der Zusatz [Avira checked], welcher im Betreff einer Email erscheint, wird durch den Job „Prüfen mit der Avira Scan Engine“ hinzugefügt. Sollte dieser Zusatz nicht gewünscht sein, lässt er sich über die Eigenschaften des Jobs entfernen.

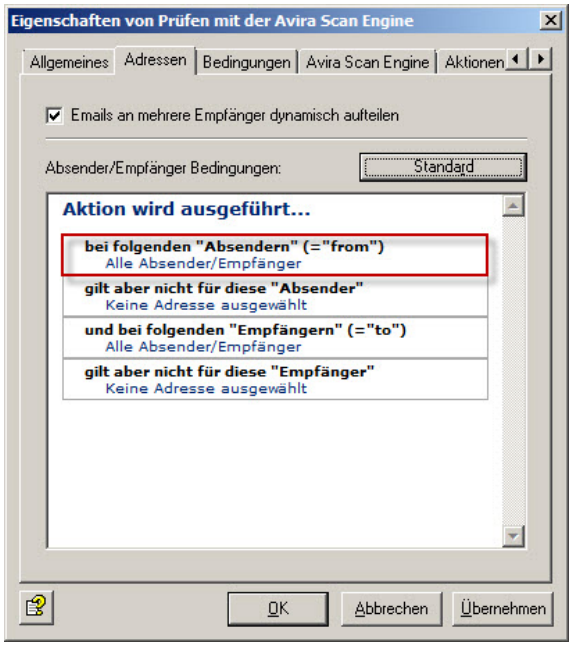
Zunächst ist jeder neue Job deaktiviert. Damit sie einen Job aktivieren, ändern Sie bitte die Einstellung im Reiter „Allgemeines“ auf „Aktiv: **Ja“**.

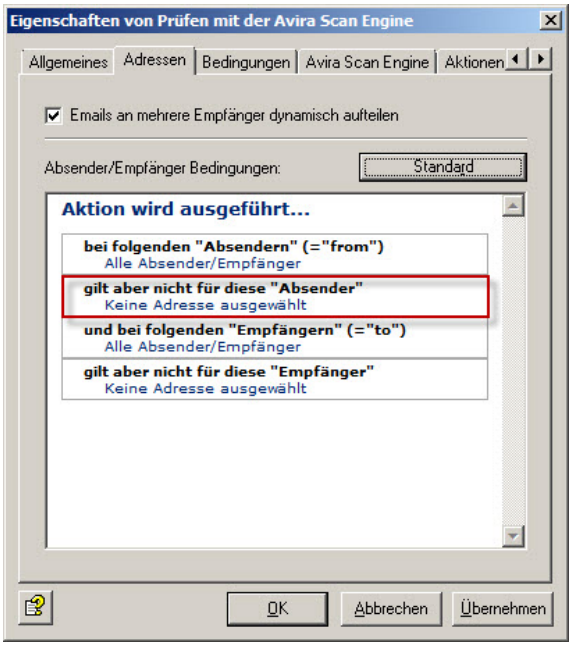


Von der Grundeinstellung her wird jeder Job auf alle ein- und ausgehenden Emails angewandt. Um dies zu ändern und gegebenenfalls Black- / Whitelisten zu verwenden, wechseln Sie bitte in den Reiter „Adressen“.



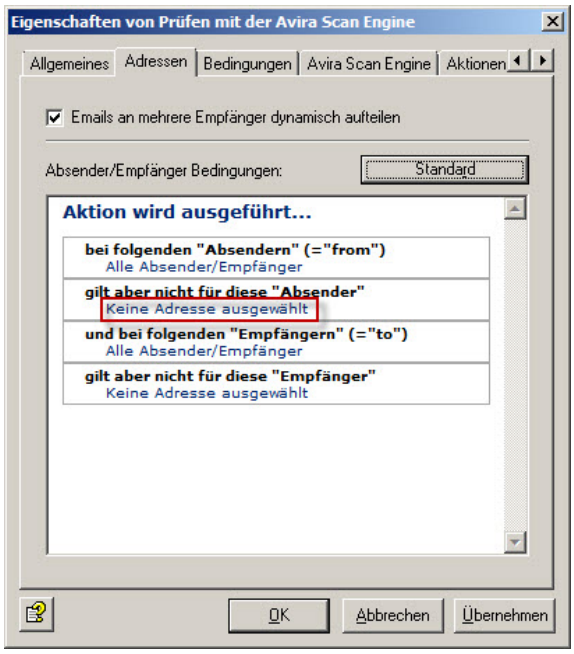
Über den Menüpunkt **Erweitert** ändert sich die Ansicht des Fensters und Sie haben nun die Möglichkeit, Adressen / Adresslisten als Ausnahme zu hinterlegen.



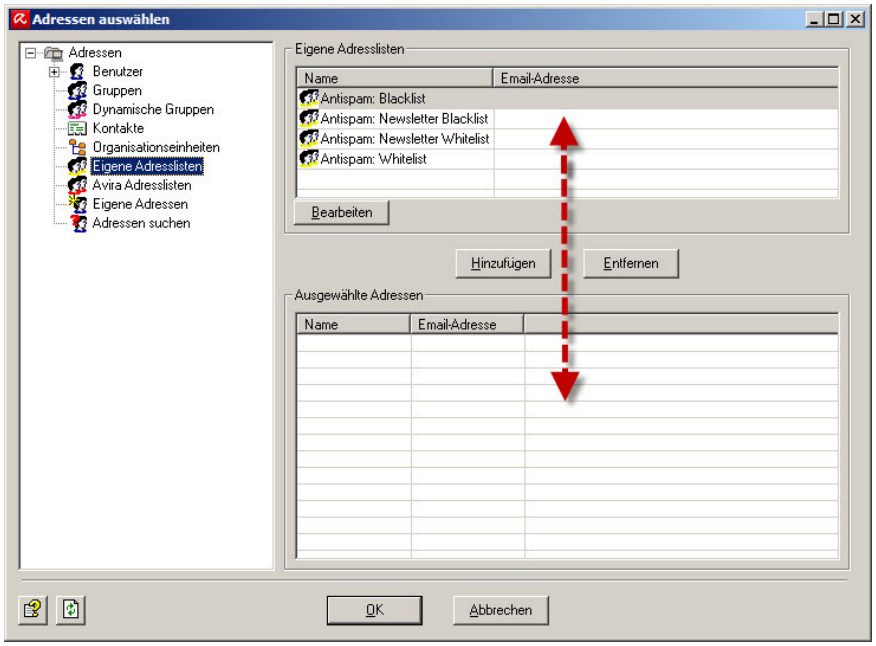


Jede Email von extern oder an extern wird durch diesen Job überprüft.	Hier können Sie jedoch eigene Adressen oder Adresslisten hinzufügen, für welche der Job nicht gilt (z.B. eine Whitelist).

Wie bereits in der Bildbeschreibung zu erkennen ist, lassen sich die Adressbereiche anpassen. Durch einen einfachen Mausklick auf „Keine Adresse ausgewählt“, im Bereich „gilt aber nicht für diese Absender“, können Sie eine Adressliste hinzufügen.

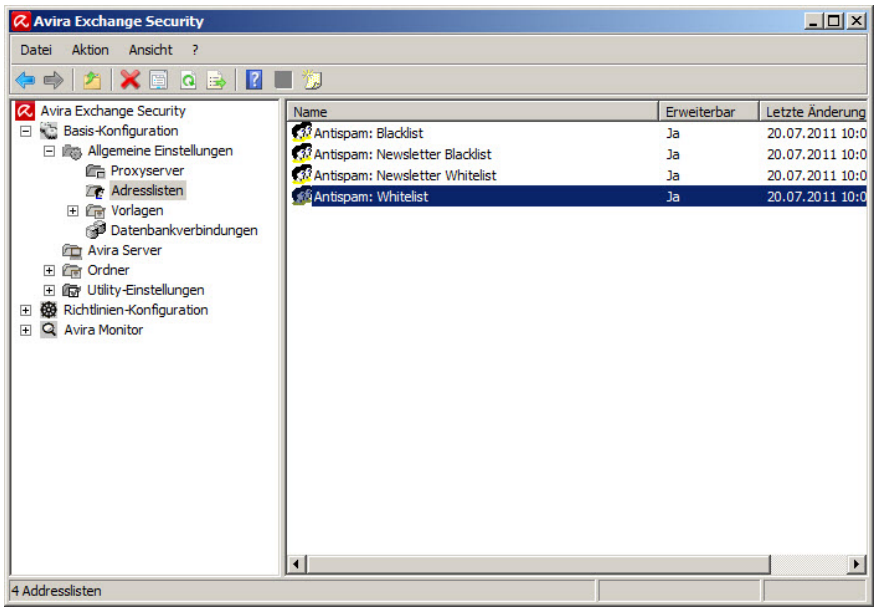


Alle in dieser Adressliste hinterlegten Absender werden dann nicht mehr von diesem Job berücksichtigt, die Nachrichten kommen dann also in jedem Fall beim Empfänger an.

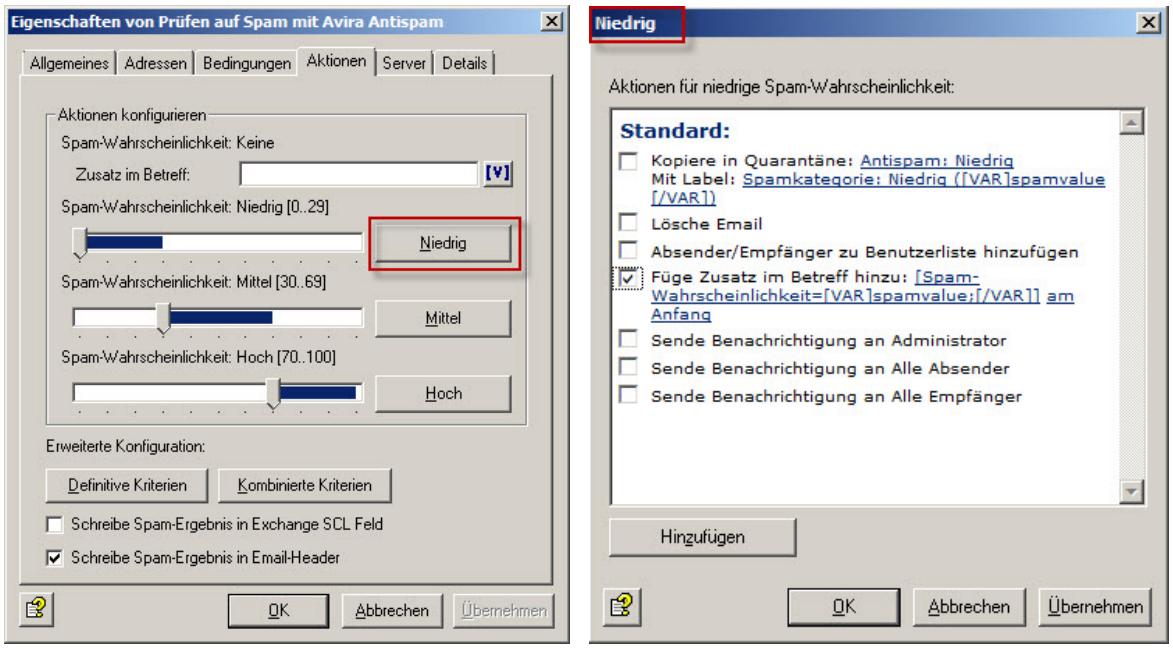


Falls Sie sich für eine der hier hinterlegten Listen entscheiden, ist unter Umständen eine Anpassung der Inhalte erforderlich.

Diese Anpassung kann im Anschluss über den Programmpunkt *Basis-Konfiguration > Allgemeine Einstellungen > Adresslisten > Antispam: Whitelist* durchgeführt werden.



Um festzulegen, was im Falle einer Klassifizierung als Spam/Virus durchgeführt werden soll, können Sie die Einstellungen im Bereich „Aktionen“ anpassen. (*Richtlinien-Konfiguration > Mail-Transport-Jobs*) Hier haben Sie je nach Spam-Wahrscheinlichkeit unterschiedliche Möglichkeiten.



Der Reiter „Aktionen“ ist für jeden Job separat zu konfigurieren. Änderungen sind immer nur für diesen einen Job wirksam.

Nachdem die Konfiguration abgeschlossen wurde, bestätigen Sie diese bitte zum Abschluss mit einem Klick auf **OK** und speichern Sie danach die Änderungen im Avira Exchange Security durch einen Klick auf das Diskettensymbol.

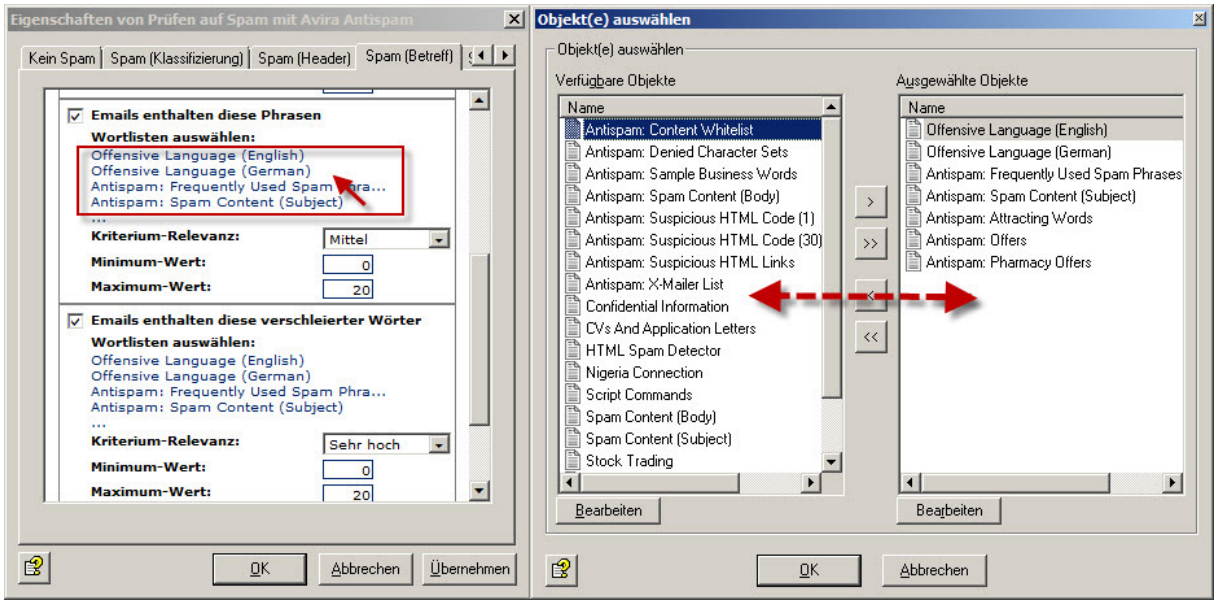
Hinweis:
Ohne das Speichern der Änderungen werden diese nicht übernommen und sind daher wirkungslos. Dies gilt für alle Änderungen im Programm.

- **Definitive „Kein Spam“ -Kriterien (Whitelist):**
  Beinhaltet Adressen aller bekannten Absender, die immer erlaubt sind und die eindeutig keinen Spam versenden. Dies sind im Prinzip alle regelmäßigen Kommunikationspartner und die Domänen von Kunden und Lieferanten. Je vollständiger diese Liste gehalten wird, desto weniger wird Ihr System mit unnötigen Prüfungen belastet.

- **Definitive „Spam-Kriterien“ (Blacklist):**
  Beinhaltet Adressen aller Absender, die immer als Spam-Absender identifiziert werden. Die Standardkonfiguration enthält bereits eine Liste von bekannten Adressen. Sie können eigene zusätzliche Adressen definieren.

- **Kombinierte „Kein Spam“ -Kriterien:**
  Die kombinierten Kriterien werden nur dann angewandt, wenn die definitiven Kriterien nicht zutreffend waren. Für die eigentliche Spam-Erkennung mit kombinierten Kriterien werden mehrere Analyse-Mechanismen (Kriterien-Untersuchungen) parallel durchgeführt und anschließend nach der Analyse der Email miteinander „verrechnet“.

  Zusätzlich ist hier eine Wortlistenerkennung für den Betreff und den Nachrichtentext hinterlegt. Die Wortlisten sind statisch, werden also nicht automatisch aktualisiert. Sie können diese Listen jedoch manuell anpassen. (*Richtlinien-Konfiguration > Mail-Transport-Jobs > Prüfen auf Spam mit Avira Antispam > Eigenschaften > Aktionen > Kombinierte Kriterien > Spam [Betreff]*)



5. Informationsspeicher-Scan-Job

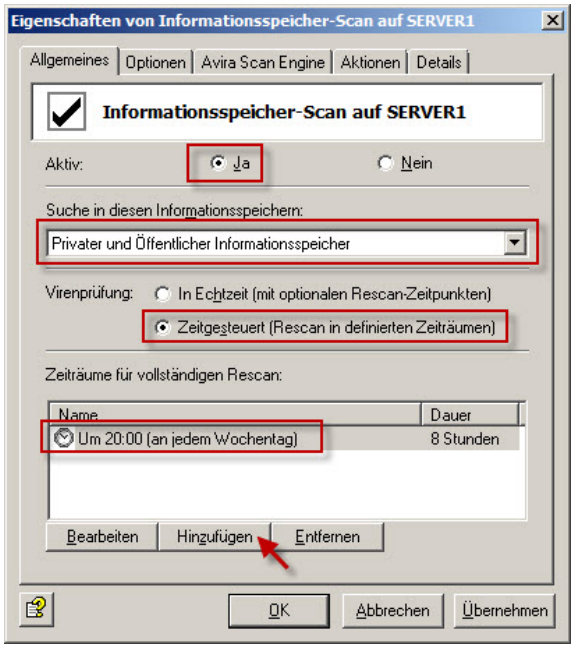
Neben der Virenprüfung auf Transportebene (Email-Verkehr) ist Avira Exchange Security auch in der Lage, Daten im öffentlichen oder privaten Informationsspeicher von MS Exchange zu prüfen (z.B. Entwürfe). Dadurch dass der Informationsspeicher-Scan eine Servereinstellung ist, steht für jeden Server nur ein Informationsspeicher-Scan-Job zur Verfügung.

Grundsätzlich ist dieser Filter deaktiviert, er kann jedoch auf Wunsch aktiviert werden.

Hinweis:
Nach dem Aktivieren/Deaktivieren des Informationsspeicher-Scan-Jobs kann es bis zu zwei Minuten dauern, bis der Exchange Store die Änderung registriert.

5.1 Aktivierung des Informationsspeicher-Scan-Jobs

Den Informationsspeicher-Scan-Job können Sie über folgenden Menüpunkt aktivieren: *Avira Exchange Security* > *Richtlinien-Konfiguration* > *Informationsspeicher-Jobs* > Doppelklick auf *Informationsspeicher auf Server.*



In der Registerkarte „Allgemeines“ aktivieren Sie mit **Ja** den Informationsspeicher-Scan. Mit Hilfe des Dropdown-Menüs können Sie auswählen, welcher der drei Informationsspeicher geprüft werden soll. (Privater Informationsspeicher/ Öffentlicher Informationsspeicher/Privater und Öffentlicher Informationsspeicher).

Zusätzlich haben Sie die Möglichkeit, den Suchlauf **In Echtzeit** oder **Zeitgesteuert** durchführen zu lassen. Bei der Auswahl einer zeitgesteuerte Virenprüfung, können Sie Zeiträume für die Virenprüfung festlegen.

Über die Registerkarten „Optionen“, „Avira Scan Engine“, „Aktionen“ und „Details“ können weitere Konfigurationen vorgenommen werden. Bestätigen Sie die Konfiguration mit einem Mausklick auf **Übernehmen** und anschließend auf **OK.**

5.2 Informationsspeicher-Scan manuell starten

Bei einen Start des Informationsspeicher-Scans werden sämtliche Elemente im Informationsspeicher erneut gescannt. Folglich kann die Prüfung zeit- und ressourcenintensiv sein. Es ist zu empfehlen einen manuellen Informationsspeicher-Scan zu Tagesrandzeiten durchzuführen.

Einen manuellen Scan können Sie im Menü *Avia Exchange Security* > *Avira Monitor* > *Server* > rechte Maustaste auf *„Servername“* > *Eigenschaften* > *Informationsspeicher-Scan* > *Jetzt scannen* durchführen.

6. Quarantänen

Avira Exchange Security verfügt über eine zentrale Quarantäne, welche über den Programmpunkt *Avira Monitor* > *Server* > *„Ihr Server“* > *Quarantänen* eingesehen werden kann. Nach der Installation sind im Produkt standardmäßig die wichtigsten Quarantänen vordefiniert. Ein Spamfilter überprüft die eingehenden Emails auf Viren und verschiebt sie bei einem Fund in die festgelegten Quarantänen. Zusätzlich zu den schon bekannten Quarantänen „Standard-Quarantäne“ und „Infizierte Emails“, sind zusätzlich folgende Quarantänen vordefiniert.

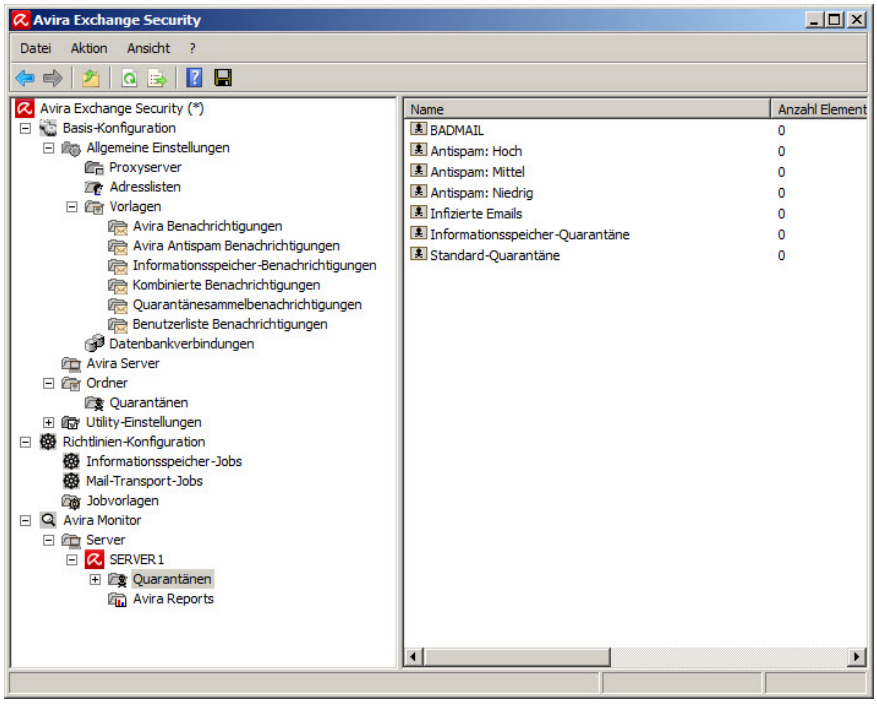
- **Informationsspeicher Quarantäne**
  Dies ist die Quarantäne des Informationsspeicher-Scanners und enthält Informationsspeicher-Dokumente. Im Allgemeinen handelt es sich bei diesen Dokumenten um Email-Anhänge oder um Elemente, die sich in öffentlichen Ordnern im Exchange befinden. In Abhängigkeit der Informationsspeicher-Job-Einstellungen sind die Dokumente
  - virulent
  - fehlerhaft (konnten nicht von der Avira Scan Engine geprüft werden)

- **Antispam: Niedrig**
  Diese Quarantäne enthält Emails der letzten Tage, die nur eine geringe Spamwahrscheinlichkeit aufweisen. Die Emails dieser Quarantäne müssen öfters überprüft werden. Bei Notwendigkeit muss der SPAM-Job angepasst werden.
  Zur Verbesserung der Klassifizierungsergebnisse, kann zum Beispiel der Spam-Absender Zur „Antispam: Blacklist“ Adressenliste hinzugefügt werden.

- **Antispam: Mittel**
  In dieser Quarantäne befinden sich Emails der letzten Tage, die nicht eindeutig als „Spam“ oder „NoSpam“ klassifiziert werden konnten. Diese Quarantäne sollte regelmäßig nach falsch zugeordneten Emails („False Positives“) überprüft werden. Verwenden Sie hierzu die Quarantäne-Sammelbenachrichtigung, damit die Empfänger selbst ihre falsch zugeordneten Emails überprüfen.

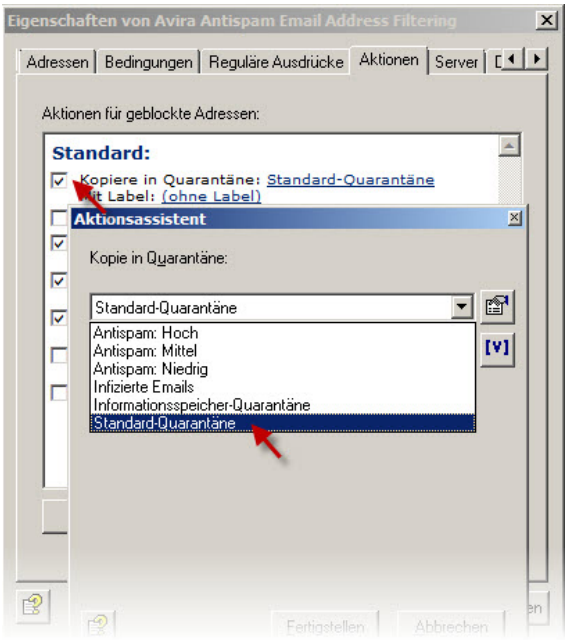
  Um die Anzahl der als „Mittel“ eingestuften Emails so gering wie möglich zu halten, sollten Sie die Analyse dieser Emails in den SPAM-Jobeinstellungen berücksichtigen.
  Zum Beispiel:
  - Gewünschte Absender von Newslettern, in die „Antispam: Whitelist Newsletter“ Adressenliste eintragen
  - Ungewünschte Absender von Newslettern, in die „Antispam: Blacklist Newsletter“ Adressenliste eintragen

- **Antispam: Hoch**
  Die Antispam Quarantäne „Hoch“ enthält Emails der letzten Tage, die eine hohe Spamwahrscheinlichkeit aufweisen.



Sollte der Bedarf bestehen, eine weitere Quarantäne anzulegen, können Sie diese im Bereich *Basis-Konfiguration* > *Ordner* > *Quarantänen* anlegen.

Beachten Sie jedoch, dass die bereits vordefinierten Quarantänen den einzelnen Jobs zugeteilt wurden und dass hier eventuell weitere Änderungen erforderlich sind.



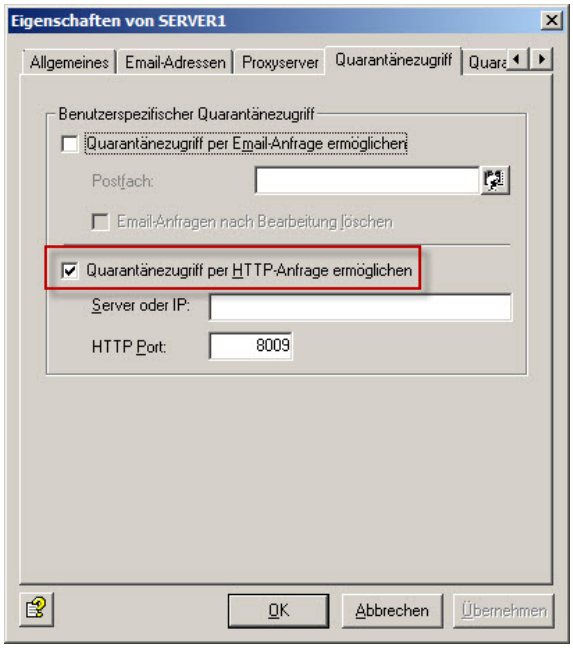
Um Ihre neu angelegte Quarantäne zu verwenden, muss diese in den gewünschten Jobs, im Reiter „Aktionen“, hinterlegt werden.

7. Quarantänesammelbenachrichtigungen

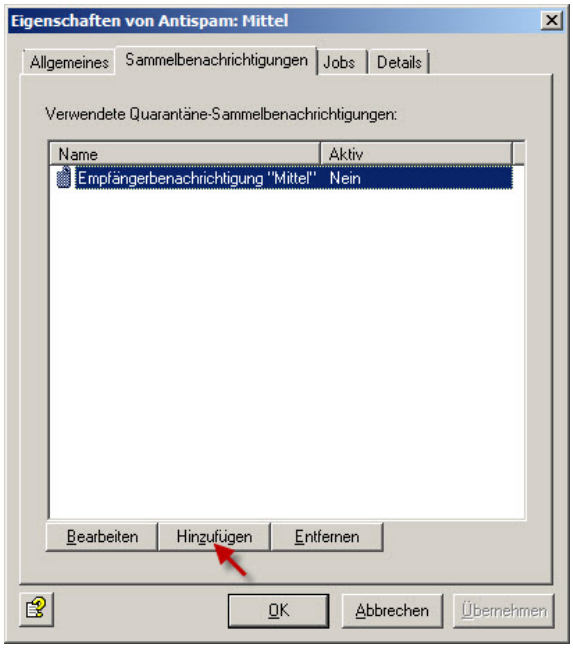
Die Sammelbenachrichtigung gibt den Empfänger oder Gruppen eine Meldung über die Emails, welche in die Quarantäne gestellt worden sind. Alle benötigten Zusatzinformationen einer Meldung können über die Sammelbenachrichtigung konfiguriert werden.

Um die Funktion der Sammelbenachrichtigung zu nutzen, gehen Sie wie folgt vor.

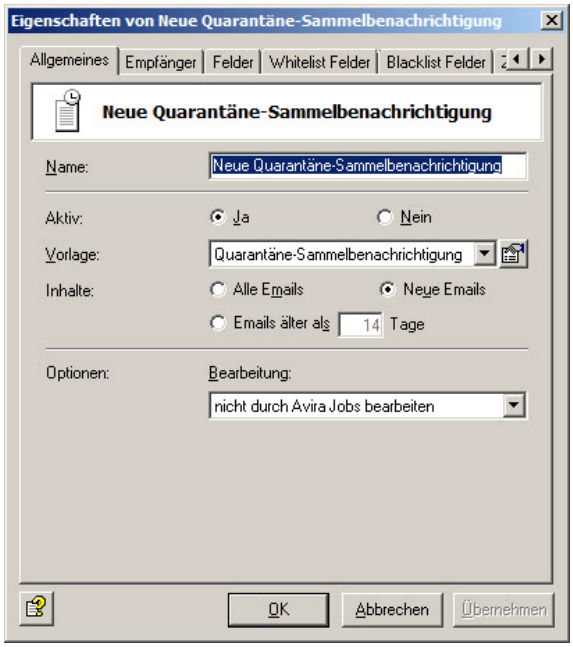
- Schalten Sie zunächst den Quarantänezugriff frei: *Basiskonfiguration > Avira Server > Doppelklick auf „Servername“ > Quarantänenzugriff > Quarantänenzugriff per HTTP-Anfrage ermöglichen*



- Wechseln Sie danach bitte wieder zu: *Basiskonfiguration > Ordner > Quarantänen.* Dort öffnen Sie die Eigenschaften der gewünschten Quarantäne mit einem Doppelklick. Im Reiter „Sammelbenachrichtigung“ klicken Sie bitte auf **Hinzufügen**.

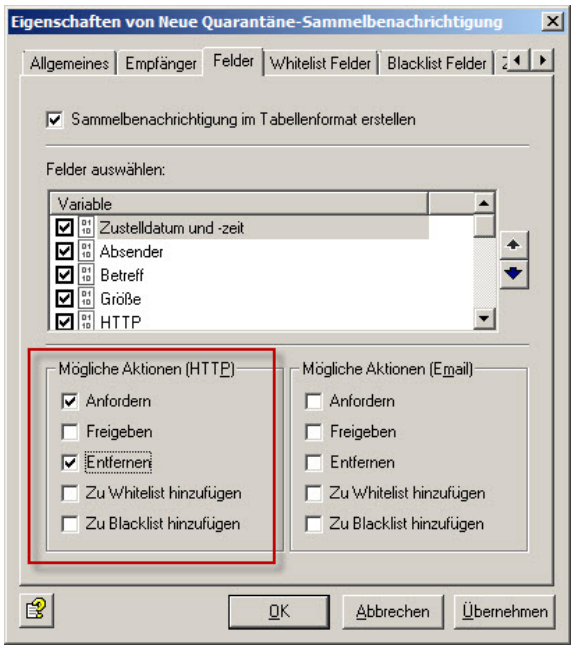


In den Eigenschaften der Sammelbenachrichtigung können Sie zunächst festlegen, wer diese Benachrichtigung erhalten soll. Zusätzlich legen Sie hier einen Namen und die Inhalte fest.



Im Reiter „Felder“ legen Sie fest, welche Möglichkeiten der Empfänger haben soll.

Hinweis:
Da der Quarantänezugriff zuvor auf HTTP eingestellt wurde, ist auch hier nur der HTTP-Zugriff möglich. Soll hier der Email-Zugriff verwendet werden, muss dies auch im Quarantänezugriff freigeschaltet werden.

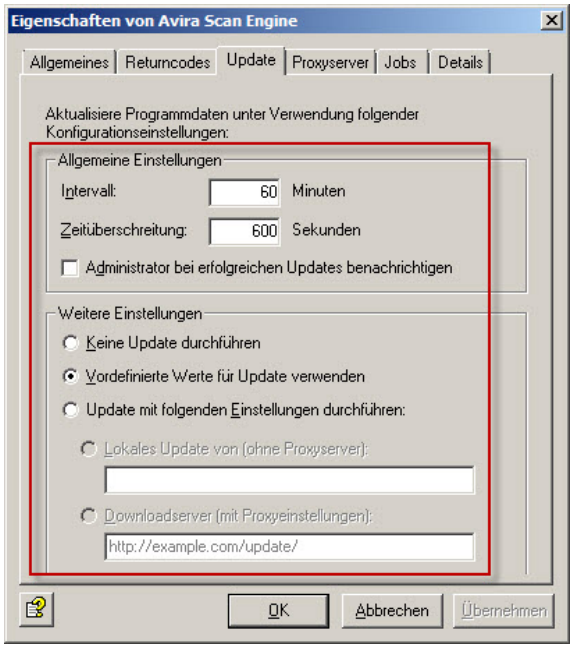


Nachdem Sie die möglichen Aktionen festgelegt haben, fehlt zum Schluss nur noch der Zeitplan, nach welchem die Sammelbenachrichtigungen versendet werden.

Die Punkte „Zu White- / Blacklist hinzufügen“, im Reiter „Felder“ beziehen sich übrigens auf separate Adresslisten. Hier sind nicht die Listen im Bereich *Basis-Konfiguration > Allgemeine Einstellungen >Adresslisten* gemeint.

8. Update-Einstellungen

Die Einstellungen für das Update kann ab der Version 8 in der Oberfläche von Avira Exchange Security vorgenommen werden. Navigieren Sie nach *Basis-Konfiguration > Utility-Einstellungen*. Rufen Sie dort die Eigenschaften von „Avira Scan Engine“ (Virensignaturen) bzw. von „Avira Spam Engine“ (AntiSpam Signaturen) auf.
Im Reiter „Update“ ist der Punkt „Vordefinierte Werte für Update verwenden“ ausgewählt. Dies bezeichnet die Avira Updateserver im Internet.



Die relevanten Logdateien finden Sie unter folgenden Verzeichnissen:

- **Avira Spam Engine:**
  C:\Programme (x86)\Avira\Avira Exchange Security\Bin\SPACE\Update\avupdate.log

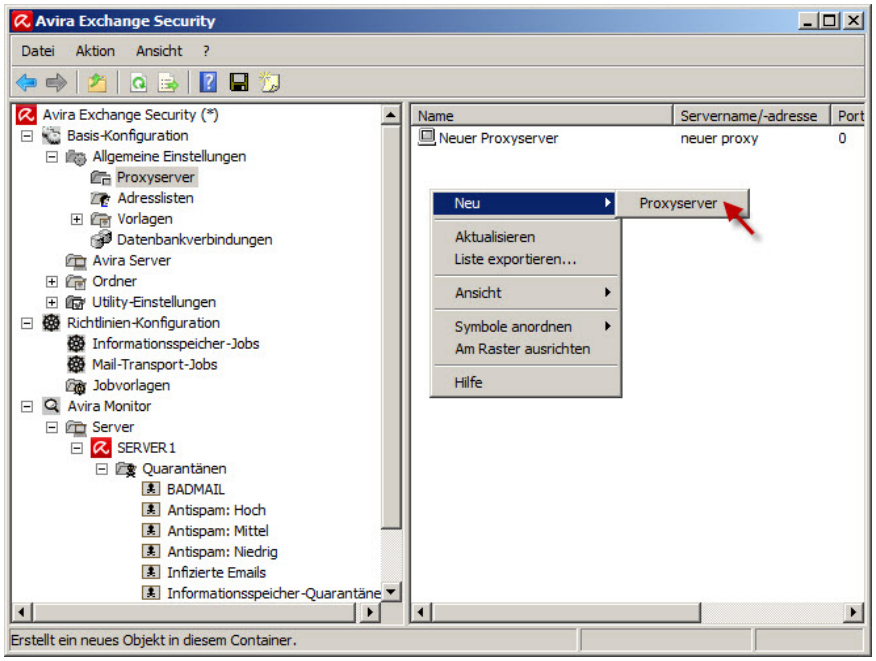
- **Avira Scan Engine:**
  C:\Programme (x86)\Avira\Avira Exchange Security\Bin\Savapi\Update\avupdate.log

8.1 Update via Proxy Server

Ebenfalls neu in der Version 8 ist die Möglichkeit, bei Bedarf einen Proxy über die Oberfläche von „Avira Exchange Security“ konfigurieren zu können.

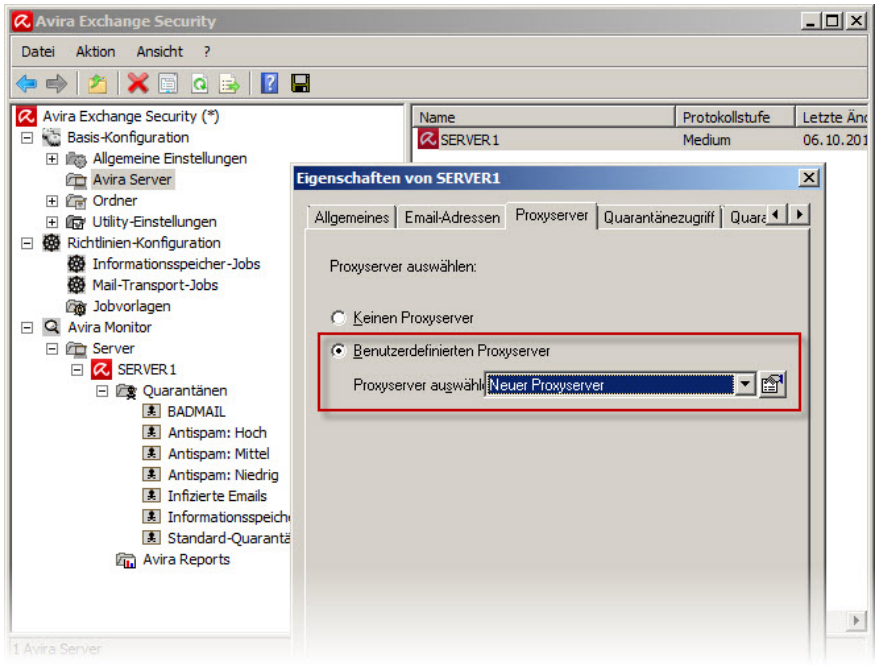
Die notwendige Konfiguration kann bzw. muss an verschiedenen Stellen vorgenommen werden.

Zuerst muss ein oder mehrere Proxy Server angeben werden. Navigieren Sie unter *Basis-Konfiguration > Allgemeine Einstellungen > Proxyserver* und erstellen einen neuen Eintrag.



Geben Sie in den Eigenschaften einen DNS-Namen bzw. IP-Adresse sowie Port und ggf. Benutzer und Passwort an.

Diesen Server geben Sie bitte unter *Basis-Konfiguration* > *Avira Server* in den Eigenschaften von ihrem Server an.



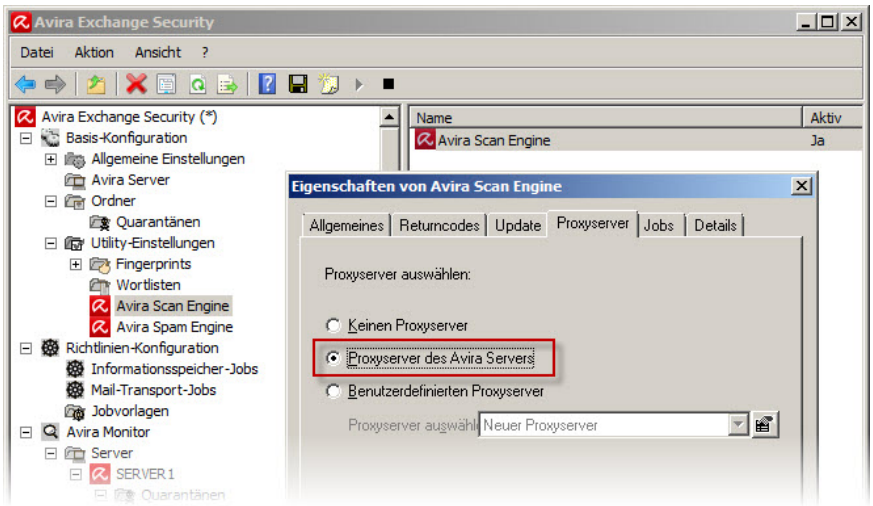
Somit haben Sie einen globalen Proxy Server definiert.

Damit ist dieser Proxy Server in den folgenden Modulen standardmäßig hinterlegt:

- Avira Scan Engine
- Avira Spam Engine

Diese Module finden Sie unter *Basis-Konfiguration > Utility-Einstellungen*.

Rufen Sie die Eigenschaften des jeweiligen Moduls auf und prüfen, ob dort die Einstellung „Proxyserver des Avira Servers“ verwendet wird.



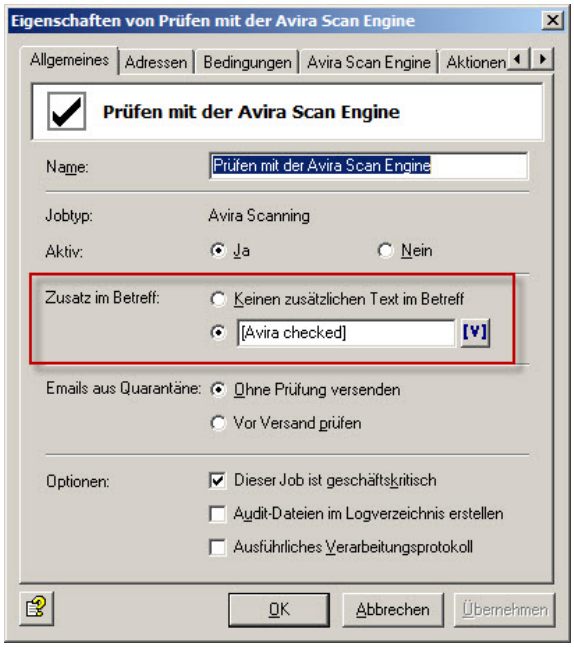
Hinweis:
Sie haben die Möglichkeit, mehrere Proxy Server einzurichten und bei jedem Modul einen separaten Server anzugeben.
Setzen Sie in dem Fall bei dem Punkt „Benutzerdefinierten Proxyserver“ einen Haken und wählen den entsprechenden Server in der Liste aus.

9. Jobvorschläge

9.1 Zusatz im Betreff entfernen

In der Standardkonfiguration fügt Avira Exchange im Betreff jeder Email den Zusatz [Avira checked] ein. Um diesen Zusatz zu ändern bzw. zu deaktivieren, muss jeder aktive Job separat konfiguriert werden (*Richtlinien-Konfiguration* > *Mail-Transport-Jobs*). Rufen Sie die Eigenschaften jedes Jobs auf und prüfen im Reiter „Allgemeines“, ob der Zusatz im Betreff aktiviert ist.

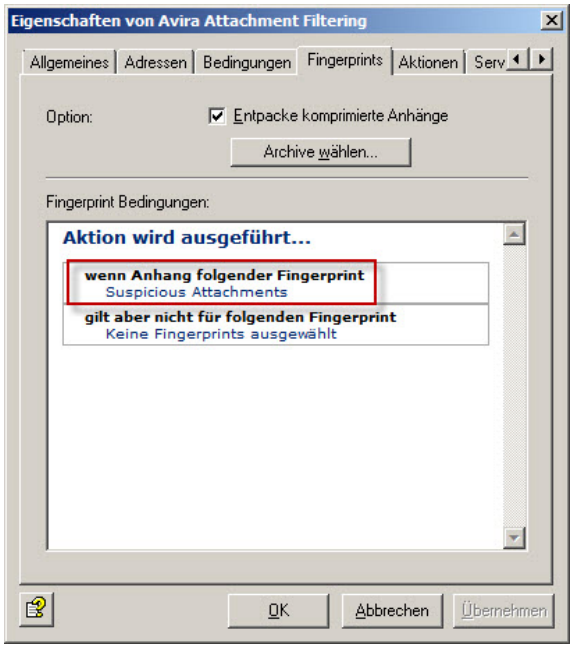
Nachfolgend anhand des Jobs „Prüfen mit der Avira Scan Engine“ gezeigt:



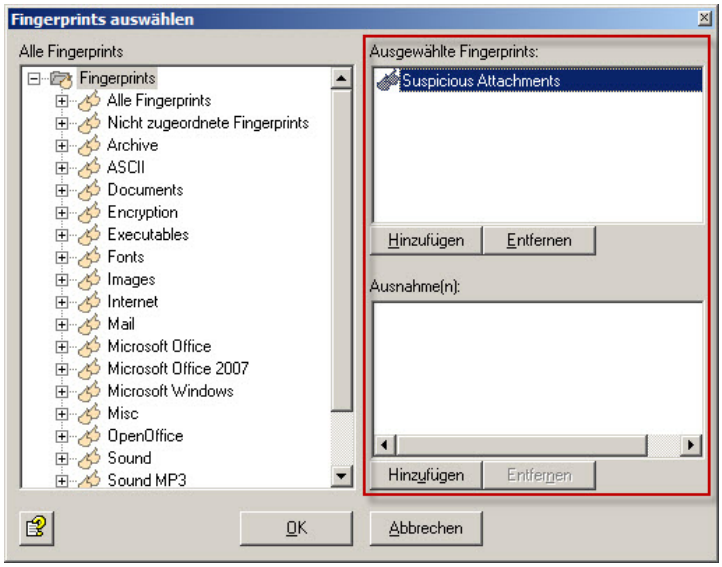
9.2 Unerwünschte Dateianhänge blocken

Um bestimmte Dateianhänge zu blocken, bietet Avira Exchange unter „Jobvorlagen“ einige vorkonfigurierte Jobs. Diese werden in der Spalte „Jobtyp“ als „Avira Attachment Filtering“ bezeichnet.
Sie können diese vordefinierten Jobs benutzen oder einen neuen Job erstellen. Dazu muss man einen neuen Job anlegen (oder einen vorhandenen konfigurieren) und entsprechende Kriterien hinzufügen. Die Klassifizierung anhand von Fingerprints ist die beste Methode um Anhänge in Mails zu erkennen.

Navigieren Sie unter *Richtlinien-Konfiguration* > *Mail-Transport-Jobs* und legen Sie dort einen neuen Job an, in dem Fall „Avira Attachment Filtering“.
Die Eigenschaften des Jobs werden geöffnet und im Reiter „Fingerprints“ können sowohl Bedingungen als auch Ausnahmen definiert werden.



Hier können Fingerprints geblockt werden (auch eine ganze Fingerprint Gruppe, z.B. Images) Zusätzlich können für bestimmt Fingerprints Ausnahmen gesetzt werden (z.B. alle Bilddateien außer JPEG)



Möchten Sie, dass der Absender über blockierte Anhänge informiert wird, aktivieren Sie bitte im Reiter „Aktionen“ den Haken bei „Sende Absender: Verbotener Inhalt gefunden“.

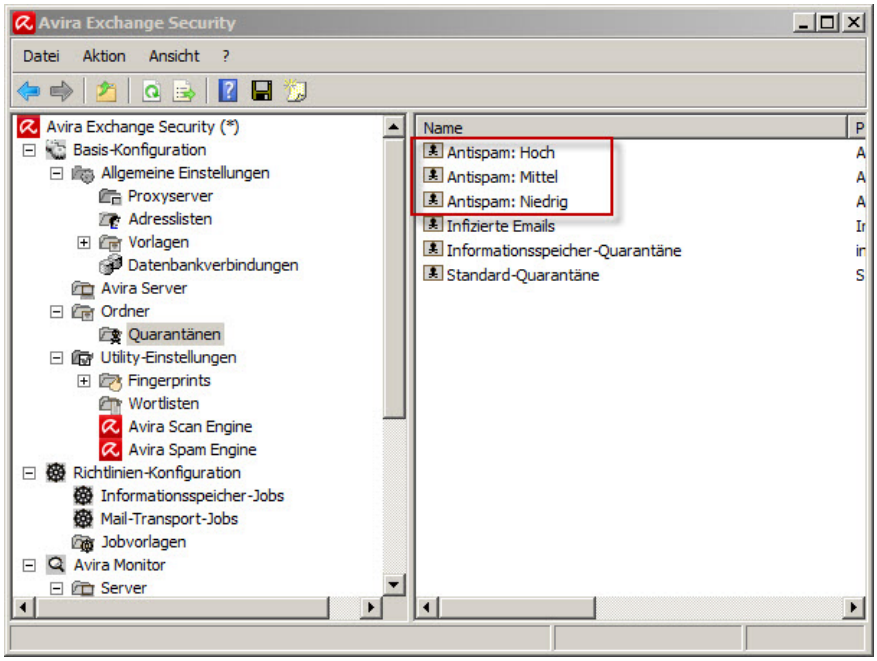
Empfehlenswert ist es auch, dass der Administrator nicht jedes Mal eine Mail bekommt wenn ein Anhang blockiert wurde. Entfernen Sie ggf. den entsprechenden Haken.

9.3 Advanced Spamfiltering mit separaten Quarantänen

Hinweis:
Bitte beachten Sie, dass nachfolgender Jobvorschlag in Avira Exchange Security als Job integriert („Advanced Spamfiltering“) und standardmäßig aktiviert ist.

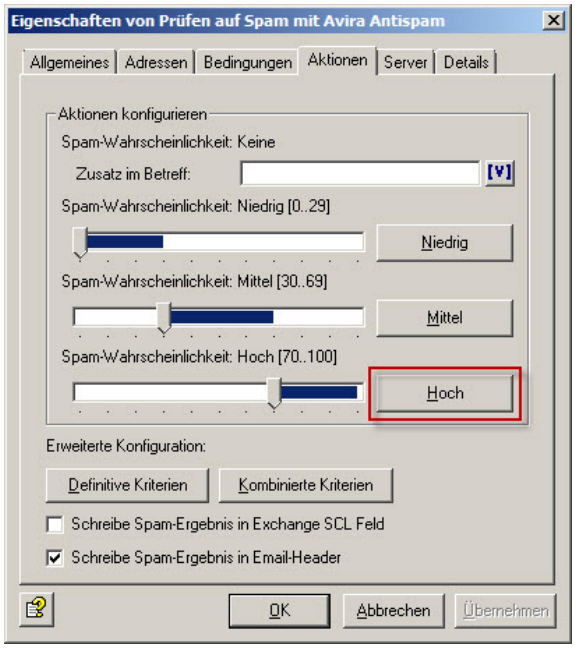
Mit dem Job „Advanced Spamfiltering“ kann man Spam in drei Kategorien unterteilen. Navigieren Sie dafür in der Avira Exchange Konsole unter *Basis-Konfiguration* > *Ordner* > *Quarantänen*.

- Antispam: Niedrig
- Antispam: Mittel
- Antispam: Hoch

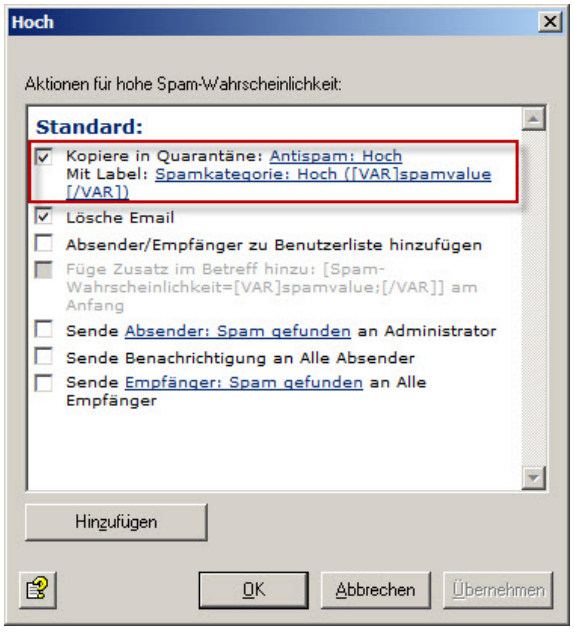


Für jede Kategorie kann man einen separaten Quarantäneordner auswählen und eingehende Mails können somit in verschiedene Quarantäneordner abgelegt werden.

Anschließend muss noch der Job „Prüfen auf Spam mit Avira Antispam“ unter *Richtlinien-Konfiguration* > *Mail-Transport-Jobs* entsprechend konfiguriert werden.
In den Eigenschaften des Jobs unter dem Reiter „Aktionen“ werden nun für alle drei Kategorien die zuvor erstellten Quarantänen festgelegt.



Jetzt konfigurieren Sie jede Kategorie (in dem Beispiel **Hoch**) und wählen den entsprechenden Quarantäneordner aus:

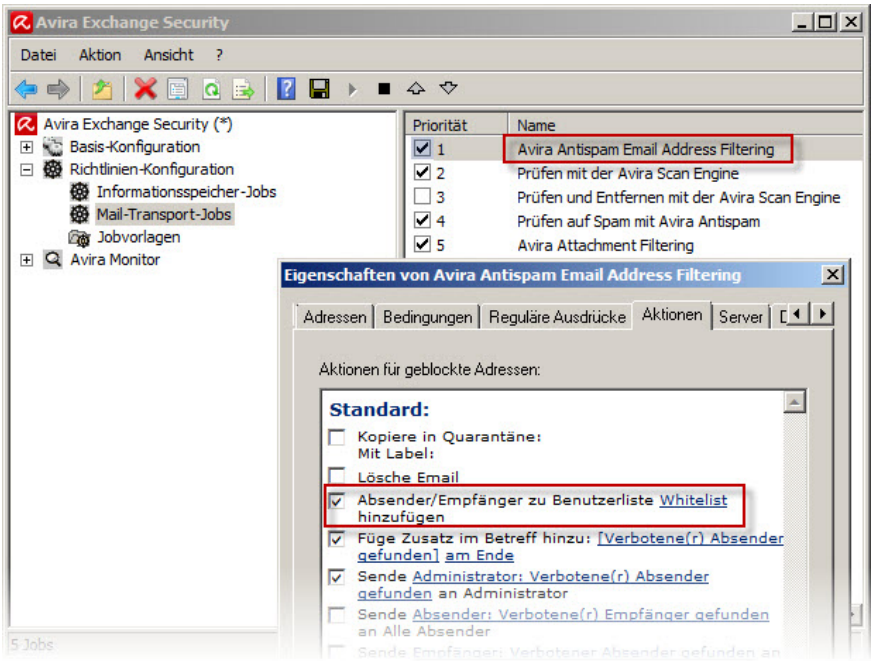


Wiederholen Sie diesen Vorgang für die Kategorie **Mittel** sowie **Niedrig**.

9.4 Empfänger automatisch zur Whitelist hinzufügen

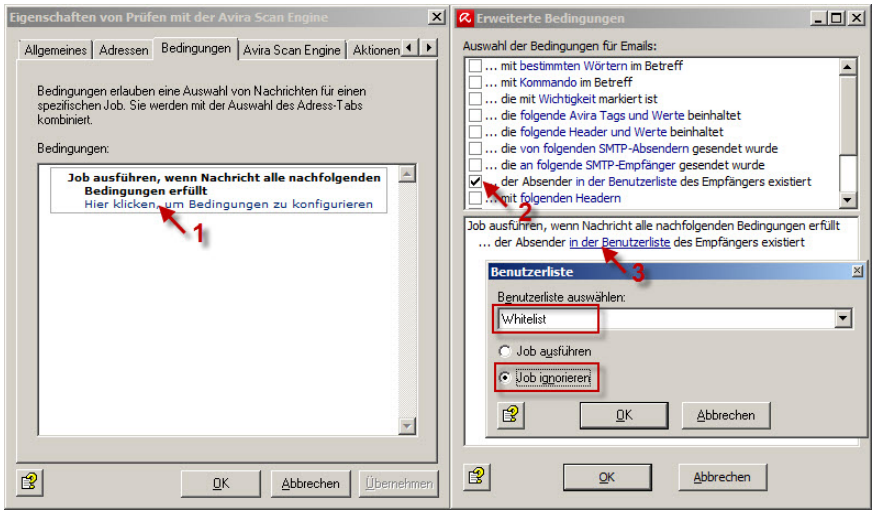
Empfänger können Sie automatisch bei Versand einer Mail, zur Whitelist hinzufügen:

- Legen Sie einen neuen Job unter „Mail-Transport-Jobs“ an:
  „Avira Antispam Email Address Filtering“
- Klicken Sie auf den Reiter „Aktionen“ und setzen den Haken *nur* bei „Absender/Empfänger zur Benutzerliste Whitelist“ hinzufügen.
- Schieben Sie den Job in „Mail-Transport-Jobs“ auf den ersten Platz (rechte Maustaste auf *Avira Antispam Email Address Filtering > Alle Aufgaben > An den Anfang)*



Nun muss jeder nachfolgende Anti-Spam-Job so konfiguriert werden, dass der Job ignoriert wird wenn ein Absender in der Whitelist steht.

- Rufen Sie die Eigenschaften des entsprechenden Jobs auf und klicken Sie auf den Reiter „Bedingungen“.
- Fügen Sie eine neue Bedingung hinzu: „...der Absender *nicht* in der Benutzerliste ‚Whitelist‘ des Empfängers existiert“

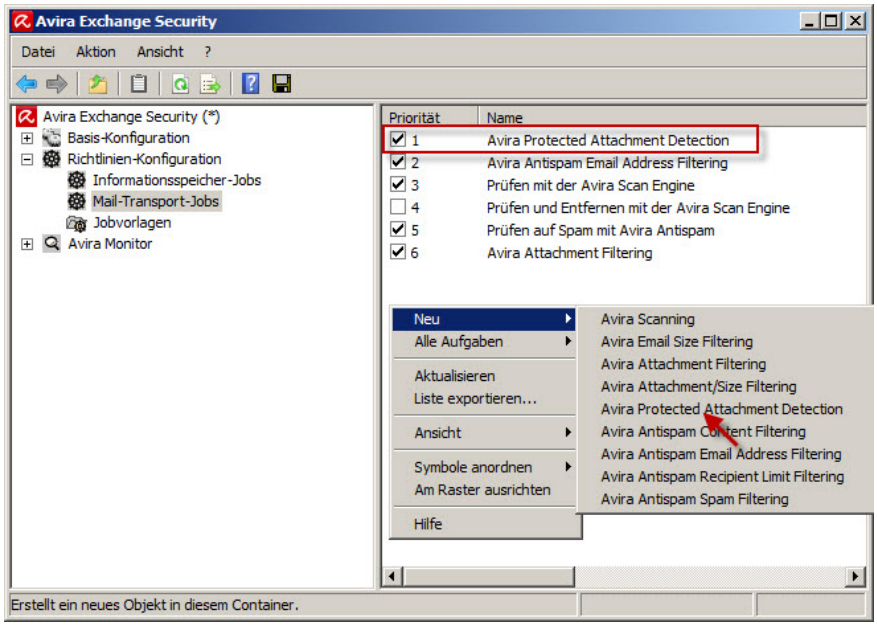


Nun werden alle Empfänger automatisch in die Whitelist hinzugefügt und in den Anti-Spam-Jobs ignoriert.

9.5 Passwortgeschützte Archive

Passwortgeschützte Archive werden standardmäßig von Avira Exchange geblockt. Seit der Version 8 gibt es jedoch einen neuen Job: „Avira Protected Attachment Detection“. Da der Job nicht automatisch aktiv ist, muss dieser erst einmal eingerichtet werden.

Richten Sie unter „Mail-Transport-Jobs“ den oben erwähnten Job ein und verschieben diesen an die erste Stelle.



Nun können Sie diesen Job nach Belieben unter dem Reiter „Aktionen“ konfigurieren und festlegen, was passieren soll, wenn eine Mail mit einem Passwort geschützten Archiv als Anhang eingeht.

Speichern Sie abschließend die durchgeführten Änderungen um diese zu aktivieren.

Ausgabe Q2-2013

AVIRA

live free.™

Avira Operations GmbH & Co. KG
Kaplaneiweg 1
88069 Tettnang
Germany

Telefon: +49 7542-500 0
Telefax: +49 7542-500 3000
www.avira.de