

Avira **AntiVir** Exchange 8

Support

Januar 2010

www.avira.de

Irrtümer und technische Änderungen vorbehalten

© Avira GmbH

Inhaltsverzeichnis

1. Installation AntiVir für Exchange	3
2. Lizenzierung	5
3. Anlegen neuer Email Filter	7
4. Konfiguration der Email Filter	9
5. Aktivieren des Informationsspeicher-Jobs	13
6. Quarantänen.....	14
7. Sammelbenachrichtigungen (Quarantäne).....	15
8. Update-Einstellungen	18
8.1 Update via Proxy Server	19
9. Jobvorschläge	22
9.1 Zusatz im Betreff entfernen	22
9.2 Unerwünschte Dateianhänge blocken.....	23
9.3 Advanced Spamfiltering mit separaten Quarantänen	24
9.4 Empfänger automatisch zur Whitelist hinzufügen.....	26
9.5 Passwort geschützte Archive	28

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

<http://www.avira.de> (<http://www.avira.com/de/download/index.html>)

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.

1. Installation AntiVir für Exchange

Nachdem Sie das Installationspaket von AntiVir für Exchange heruntergeladen haben, starten Sie dieses bitte auf Ihrem Microsoft Exchange Mailserver.

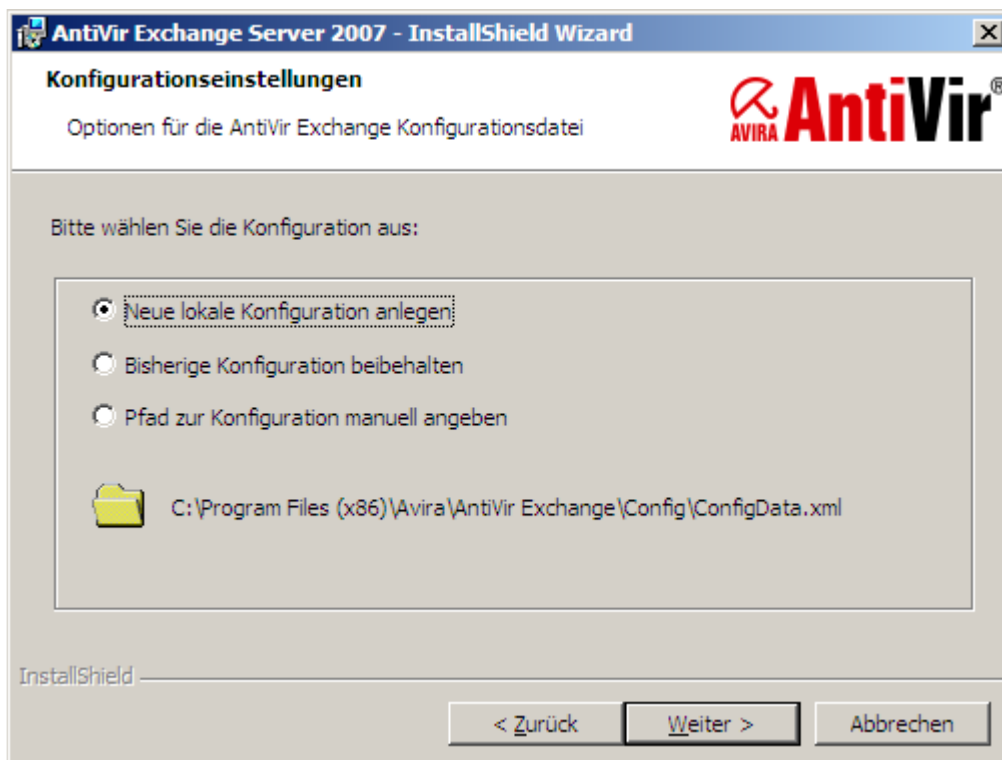
Im Laufe der Installation erscheint ein Fenster, in welchem Sie, die zu installierenden Komponenten auswählen können.

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 AntiVir Exchange befinden.
- **Pfad zur Konfiguration manuell angeben**
Sollte sich die Konfiguration in einem anderen Verzeichnis befinden, kann hier der genaue Pfad mit angegeben werden.
Wichtig: Der hier hinterlegte Pfad kann im Anschluss nicht mehr geändert werden!

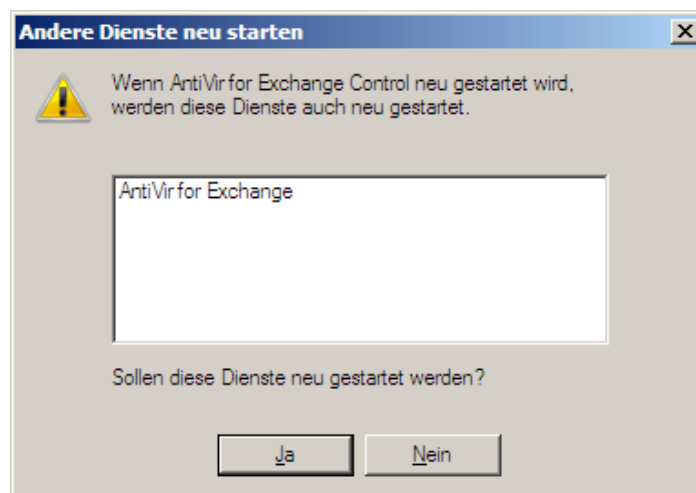


In den weiteren Schritten werden Sie nun gebeten einige administrative Voreinstellungen festzulegen. Diese beinhalten eine Emailadresse des zuständigen Administrators und einen eventuell vorhandenen Proxy Server für das Internet Update. Diese Einstellungen werden während der Installation im Programm hinterlegt, können aber auch im Anschluss in der Konfigurationsdatei „savapi.ini“ angepasst werden.

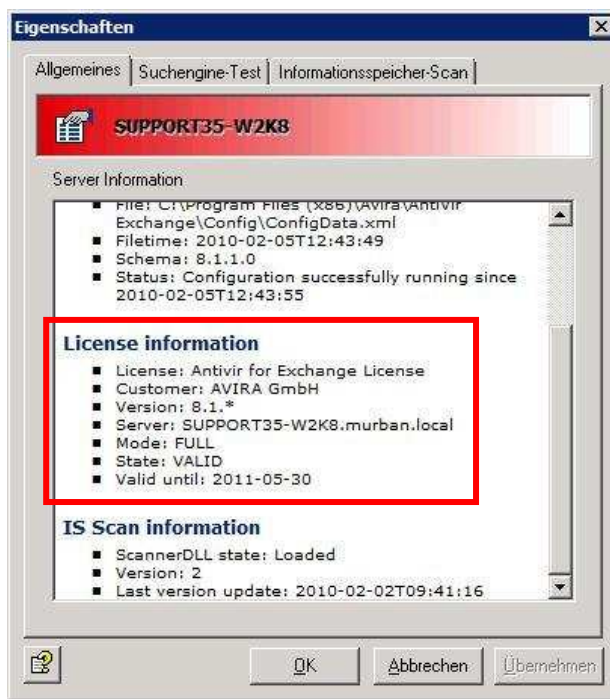
2. Lizenzierung

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 AntiVir 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 „**AntiVir for Exchange Control**“ erforderlich. Während des Neustarts erhalten Sie einen Hinweis, dass der Dienst „AntiVir for Exchange“ ebenfalls neu gestartet wird, bitte bestätigen Sie dies mit „**Ja**“.



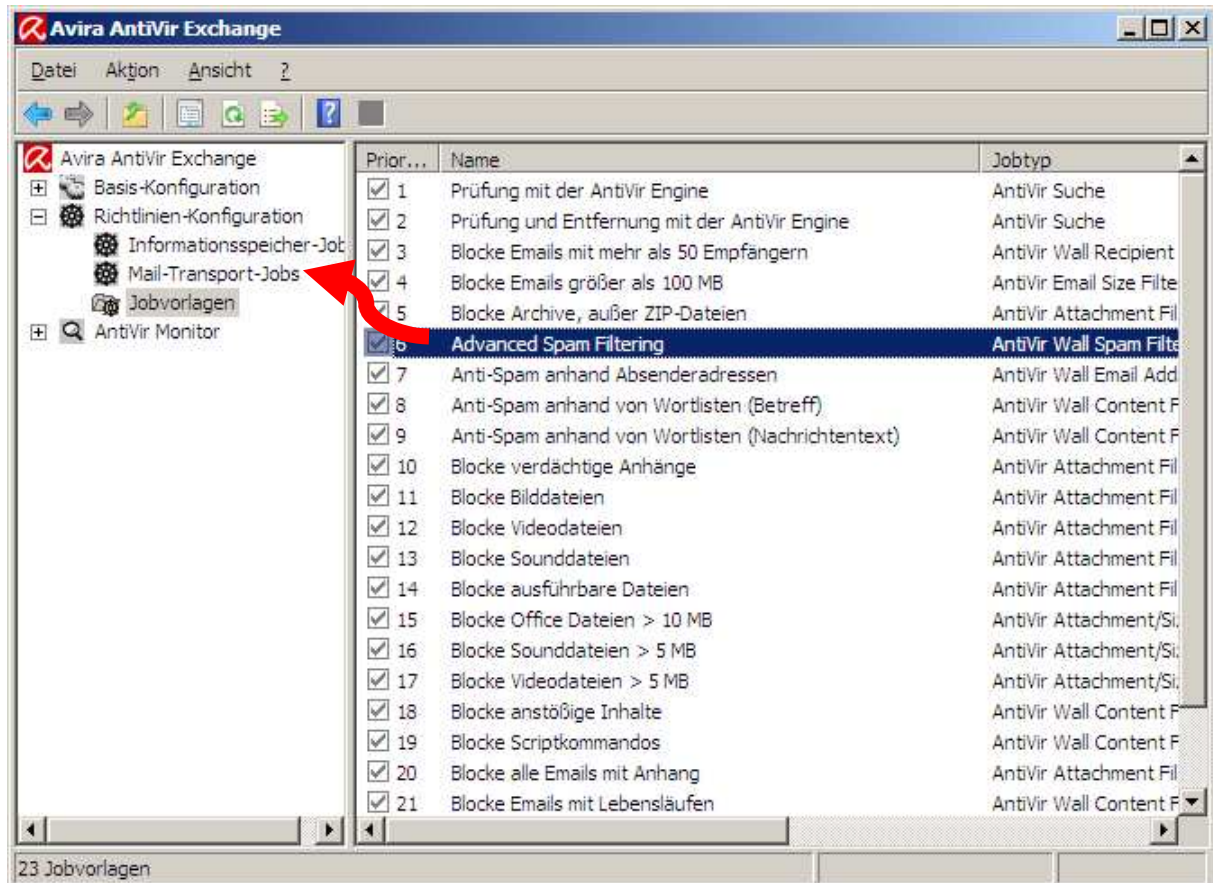
Um zu prüfen ob die Lizenzdatei richtig eingespielt wurde, starten Sie die AntiVir Exchange Management Konsole und öffnen dort den Bereich: „**AntiVir Monitor**“. Öffnen Sie nun die Eigenschaften Ihres Servers um im folgenden Fenster die Lizenzinformationen zu prüfen:



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 (support@avira.com) und senden Sie uns die Lizenzdatei zur Kontrolle zu.

3. Anlegen neuer Email Filter

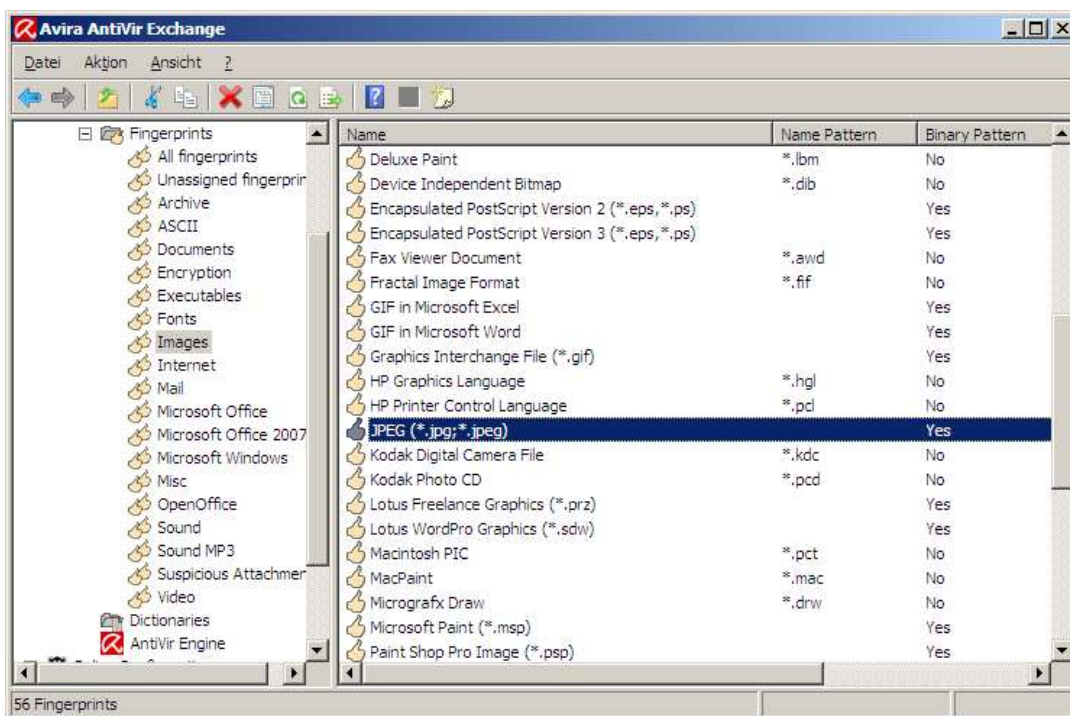
Direkt nach der Installation ist das Produkt bereits vorkonfiguriert. Eingehende Emails werden schon auf Viren geprüft und bei einem Fund in die Quarantäne verschoben. Um die Email Filterung zu erweitern und weitere Jobs einzubinden, können Sie die bereits mitgelieferten Jobvorlagen verwenden. Hier finden Sie vorkonfigurierte Jobs die den bereits aktiven Virenschanner um eine Spamfilterung, oder einen Content- / Attachment-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 Filtermethoden 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.



„Basis-Konfiguration“ → „Utility-Einstellungen“ → „Fingerprints“

Die einzelnen Dateimuster sind in Gruppen sortiert, so enthält z.B. die Gruppe Images eine Vielzahl bekannter Dateiendungen und Binärmuster.

Die Fingerprint-Gruppe (z.B. Images) wird nun einem Job zugeteilt. Dieser Job filtert eingehende Emails und überprüft, ob diese einen der genannten Fingerprints enthält.

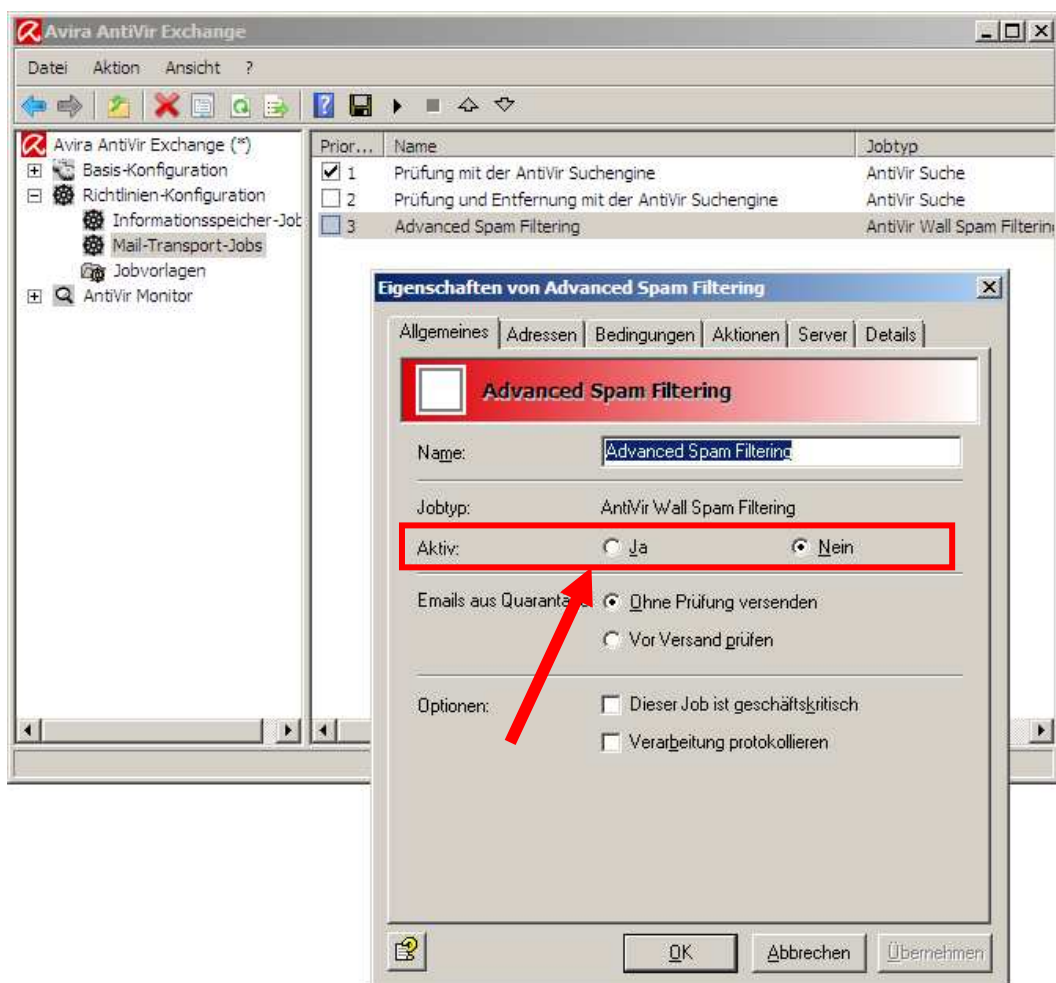
Job Beispiel:	Funktion:
Blocke Bilddateien	Dieser Job greift auf die Fingerprint-Gruppe „Images“ zu. Hier bekommt er die Information, was eine Bilddatei ist und woran er diese erkennen kann.
Blocke Videodateien	Das Prinzip der Fingerprints ist hier dasselbe wie bei den Bilddateien, lediglich die Gruppe 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

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

Um die Eigenschaften für die Konfiguration zu öffnen reicht ein normaler Doppelklick auf den gewünschten Job, das Fenster mit den Eigenschaften öffnet sich im Anschluss automatisch.

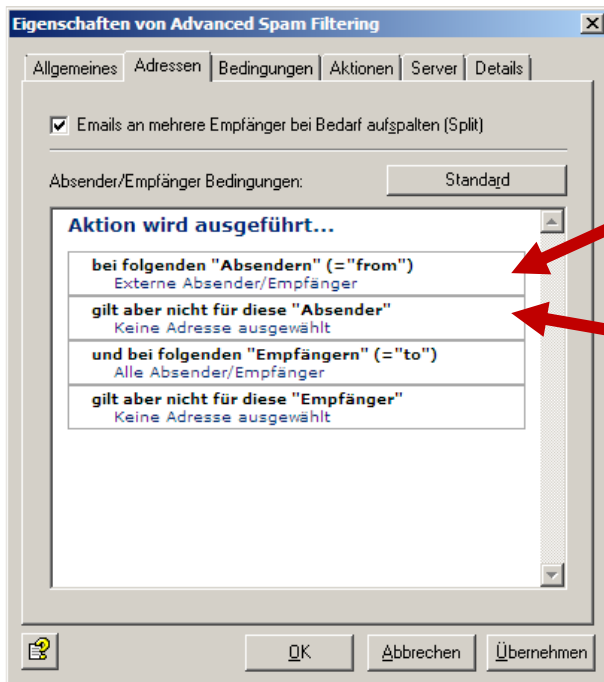
Hinweis: Der Zusatz [AntiVir checked], welcher im Betreff einer Email erscheint, wird durch den Job „**Prüfung mit der AntiVir Suchengine**“ hinzugefügt. Sollte dieser Zusatz nicht gewünscht sein, lässt er sich über die Eigenschaften des Jobs entfernen.



Zunächst ist jeder neue Job deaktiviert Um diesen zu aktivieren, verändern Sie bitte die Einstellungen 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“.

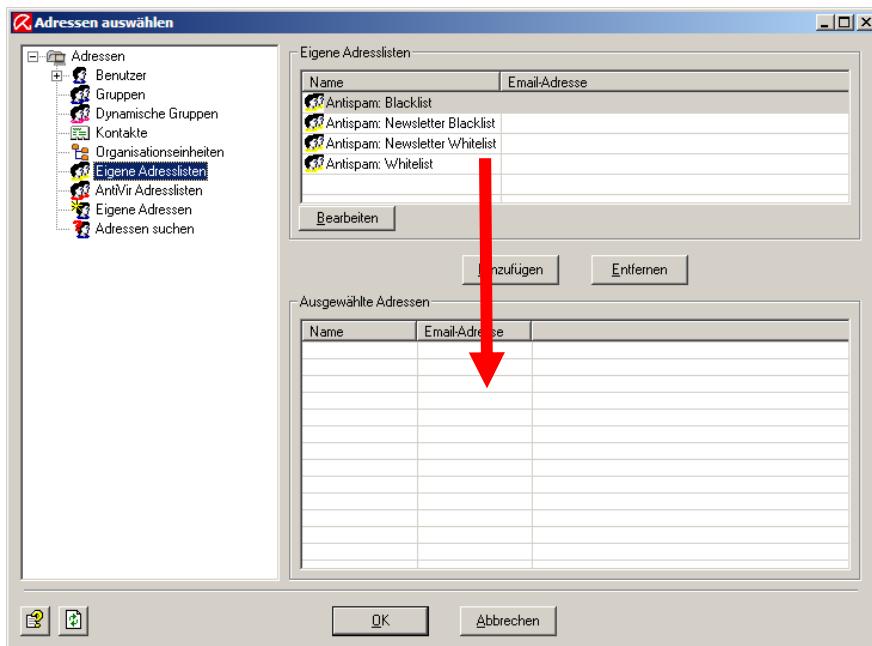
Über den Menüpunkt **Erweitert** ändert sich die Ansicht des Fensters und Sie haben nun die Möglichkeit, Adressen / Adresslisten als Ausnahme zu hinterlegen.



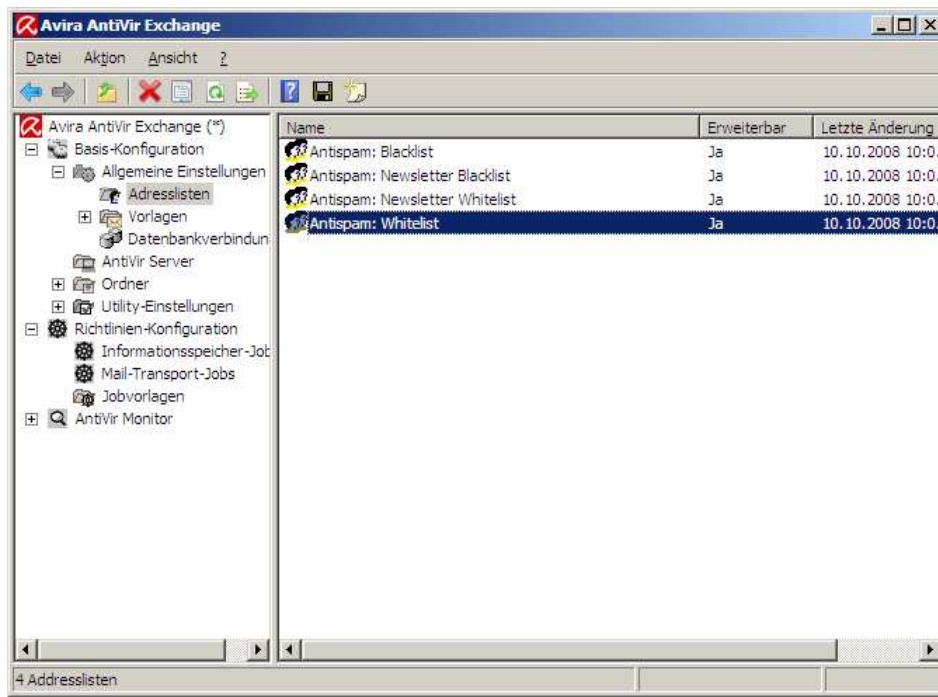
Jede Email von extern oder an extern wird durch diesen Job überprüft.

Hier können Sie jedoch eigene Adressen oder Adresslisten hinzufügen, für welche der Job nicht gilt (z.B. eine Whitelist).

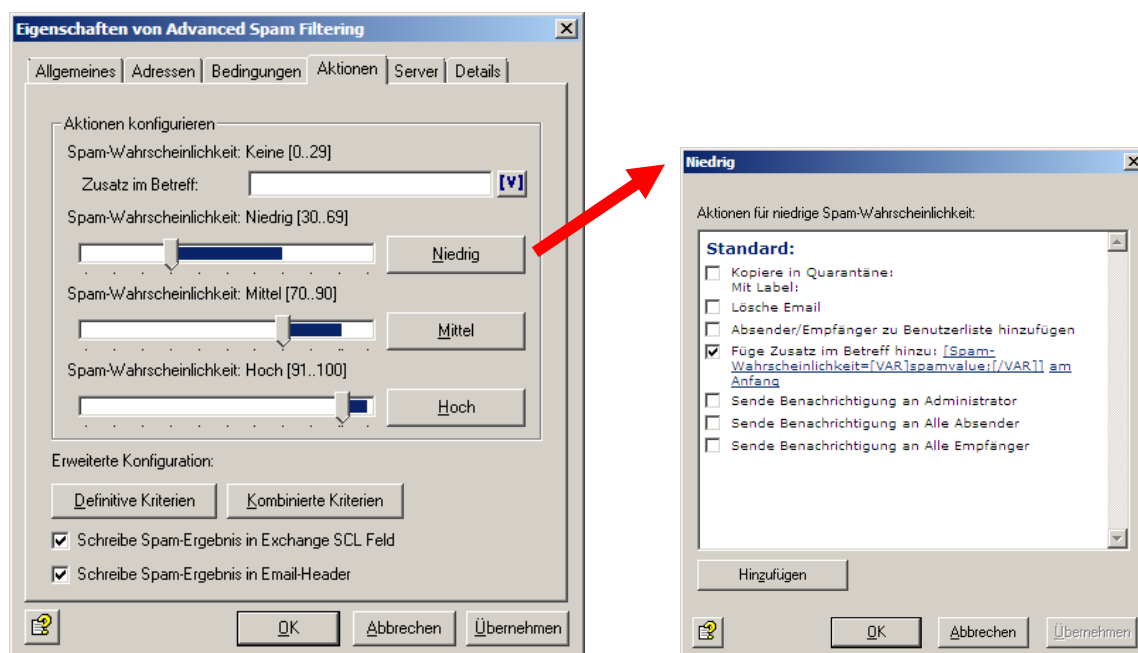
Wie bereits in der Bildbeschreibung zu erkennen ist, lassen sich die Adressbereiche anpassen. Durch einen einfachen Mausklick auf „Keine Adresse ausgewählt“, im Bereich „gilt aber nicht für diese Absender“, können Sie eine Adressliste hinzufügen. Alle in dieser Adressliste hinterlegten Absender werden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



Um festzulegen, was im Falle einer Klassifizierung als Spam / Virus durchgeführt werden soll, können Sie die Einstellungen im Bereich „**Aktionen**“ anpassen. 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 AntiVir Exchange, 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 Kriterien:

Hier sind Kriterien hinterlegt, die eine Email definitiv als „**SPAM**“ oder „**kein SPAM**“ klassifizieren.

Hinterlegt sind hier Werte wie z.B.

„**Emails von Active Directory Benutzern = kein SPAM**“

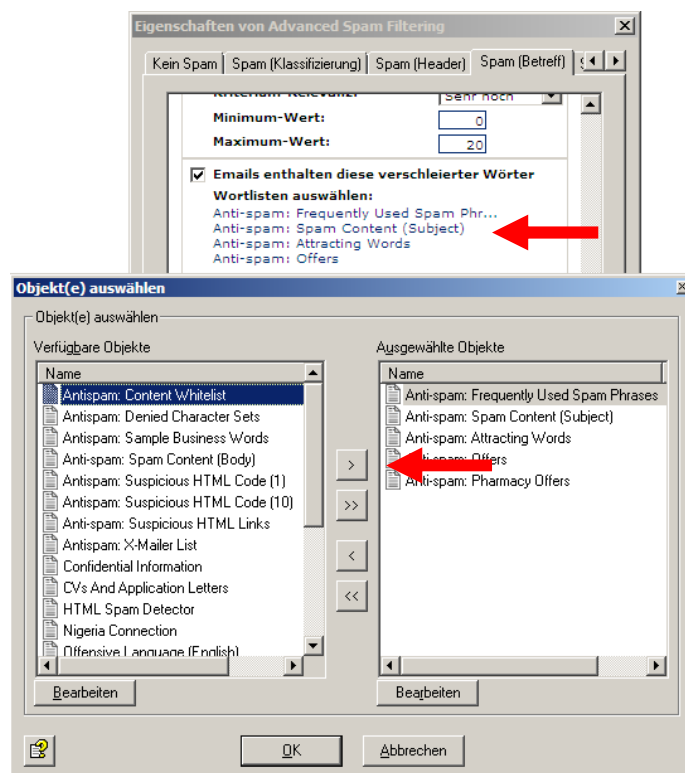
„**Emails von Absendern in Benutzer Blacklist = SPAM**“.

Kombinierte Kriterien:

Unter „Kombinierte Kriterien“ kommen mehrere Filter zum Einsatz.

Hinterlegt sind hier z.B. das „**Avira Space Modul**“, welches eine automatische Spamerkennung liefert. Die Erkennungsmuster der Spammails werden anhand eines Updates in bestimmten Abständen aktualisiert.

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.



5. Aktivieren des Informationsspeicher-Jobs

Neben der Virenprüfung auf Transportebene ist AntiVir Exchange auch in der Lage, Daten im öffentlichen oder privaten Informationsspeicher von MS Exchange zu prüfen.

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

Mit dem Informationsspeicher-Scan werden dann drei Hauptbereiche abgedeckt:

On-Demand Scan

Versucht ein Client eine Nachricht zu öffnen, wird ein Vergleich durchgeführt, um sicherzustellen, dass der Textkörper und der Anhang von der aktuellen Virensignaturdatei überprüft wurden. Wenn der Inhalt nicht anhand der aktuellen Virensignaturdatei überprüft wurde, wird die entsprechende Nachrichtenkomponente vor der Weiterleitung an den Client dem Virenschanner übermittelt. On-Demand Scan ist der geläufigste Bereich, für welchen der Informationsspeicher-Scan gewählt wird.

Proaktiver Scan

Der proaktive Scan überprüft neue eintreffende Nachrichten, bevor der Zugriff eines Clients über den On-Demand Scan erfolgt. Der proaktive Scan stellt eine Ergänzung zum On-Demand Scan dar, welcher für einen schnelleren Clientzugriff sorgen kann.

Hintergrund Scan

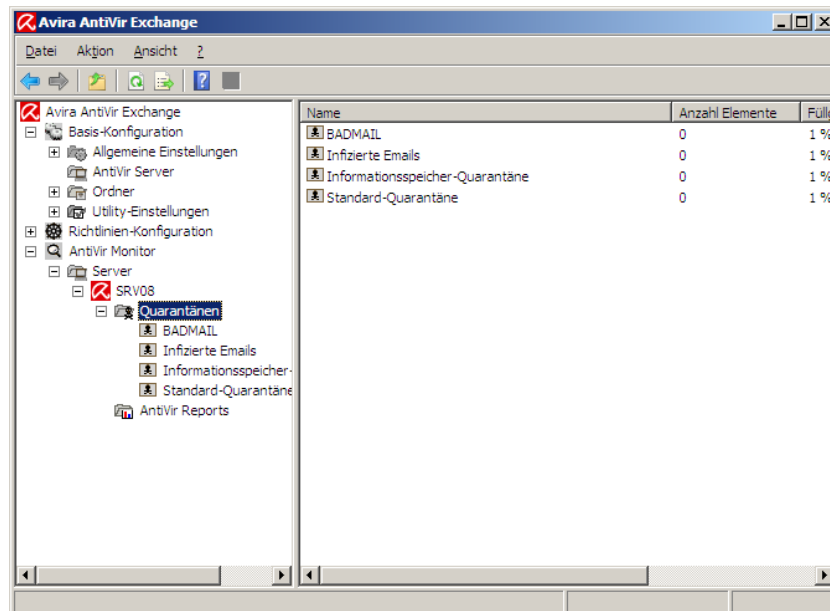
Beim Hintergrund Scan kann ein kompletter Prüflauf durch alle Elemente des Informationsspeichers angestoßen werden. Diese Überprüfung kann für den öffentlichen und privaten Informationsspeicher getrennt aktiviert werden. Es werden hierbei alle Elemente erfasst, welche mit der aktuellen Virenschannersignaturdatei noch nicht geprüft wurden.

Zusätzlich haben Sie die Möglichkeit, einen zeitgesteuerten Suchlauf durchführen zu lassen. So können Sie den Informationsspeicher z.B. am Wochenende auf Viren prüfen zu lassen.

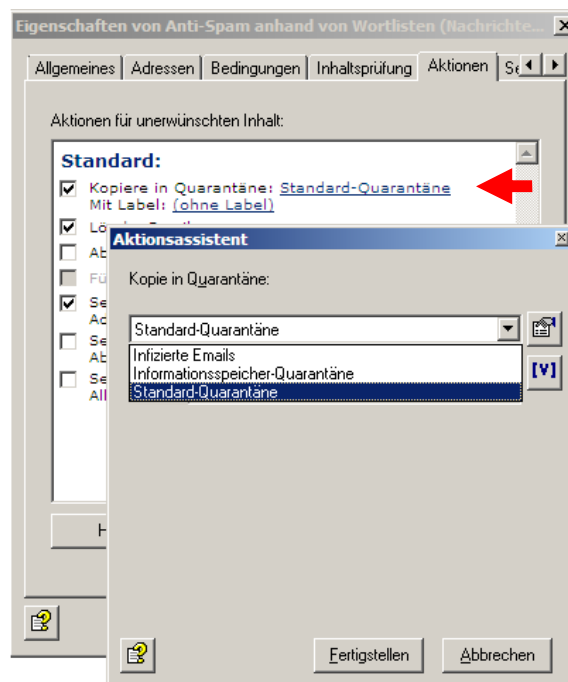
Genau wie bei den „**Mail-Transport-Jobs**“ können Sie auch hier die Aktionen festlegen, welche bei einem Fund durchgeführt werden sollen.

6. Quarantänen

AntiVir Exchange verfügt über eine zentrale Quarantäne, welche über den Programmpunkt „**AntiVir Monitor**“ → „**Server**“ → „**<Ihr Server>**“ → „**Quarantänen**“ eingesehen werden kann.



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.

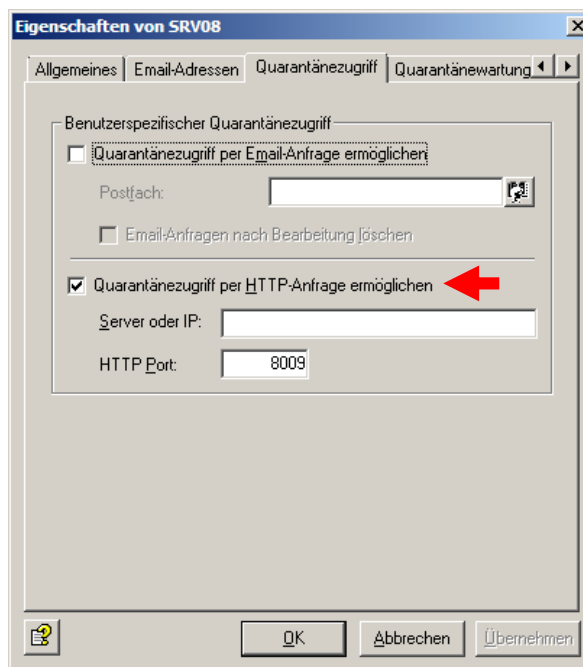


7. Sammelbenachrichtigungen (Quarantäne)

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

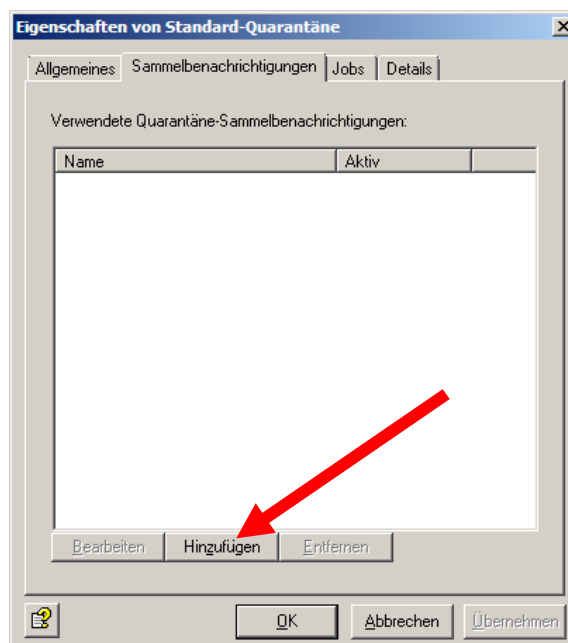
Schalten Sie zunächst den Quarantänezugriff frei:

„**Basiskonfiguration**“ → „**AntiVir Server**“ → Doppelklick auf „<Servername>“ → „**Quarantänezugriff**“ → „**Quarantänezugriff 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**“

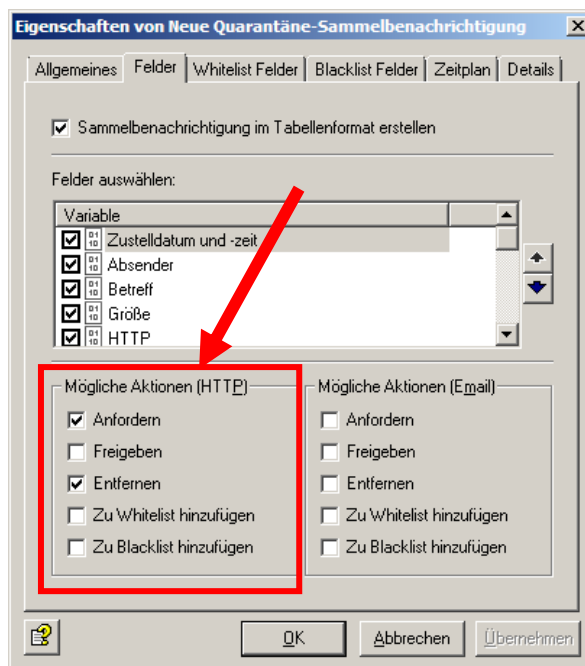


In den Eigenschaften der Sammelbenachrichtigung können Sie zunächst festlegen, wer diese Benachrichtigung erhalten soll. Zusätzlich legen Sie hier einen Namen und die Inhalte fest.



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.



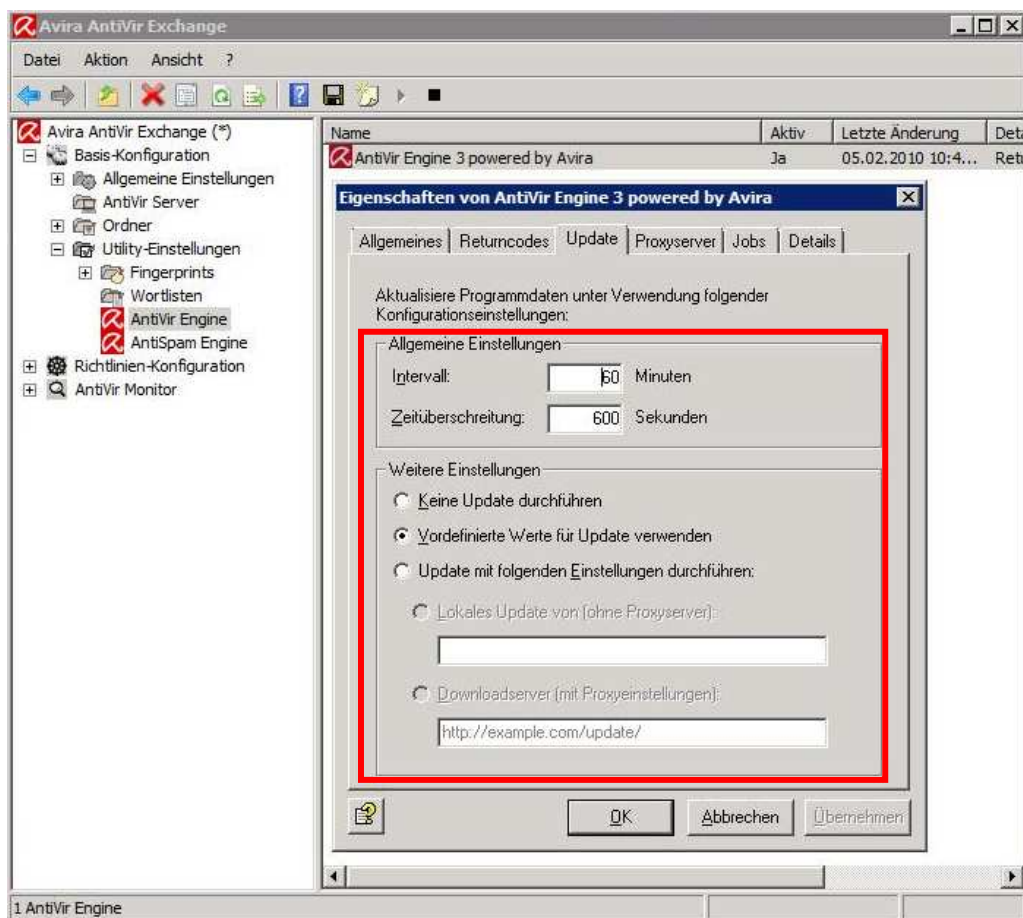


Nachdem Sie die möglichen Aktionen festgelegt haben, fehlt zum Schluss nur noch der Zeitplan, nach welchem die Sammelbenachrichtigungen versendet werden. Die Punkte „**Zu White- / Blacklist hinzufügen**“, im Reiter „**Felder**“ beziehen sich übrigens auf separate Adresslisten. Hier sind nicht die Listen 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 AntiVir Exchange vorgenommen werden.

Navigieren Sie nach „**Basis-Konfiguration**“ → „**Utility-Einstellungen**“. Rufen Sie dort die Eigenschaften von **AntiVir Engine** (Virensignaturen) bzw. von **AntiSpam 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:

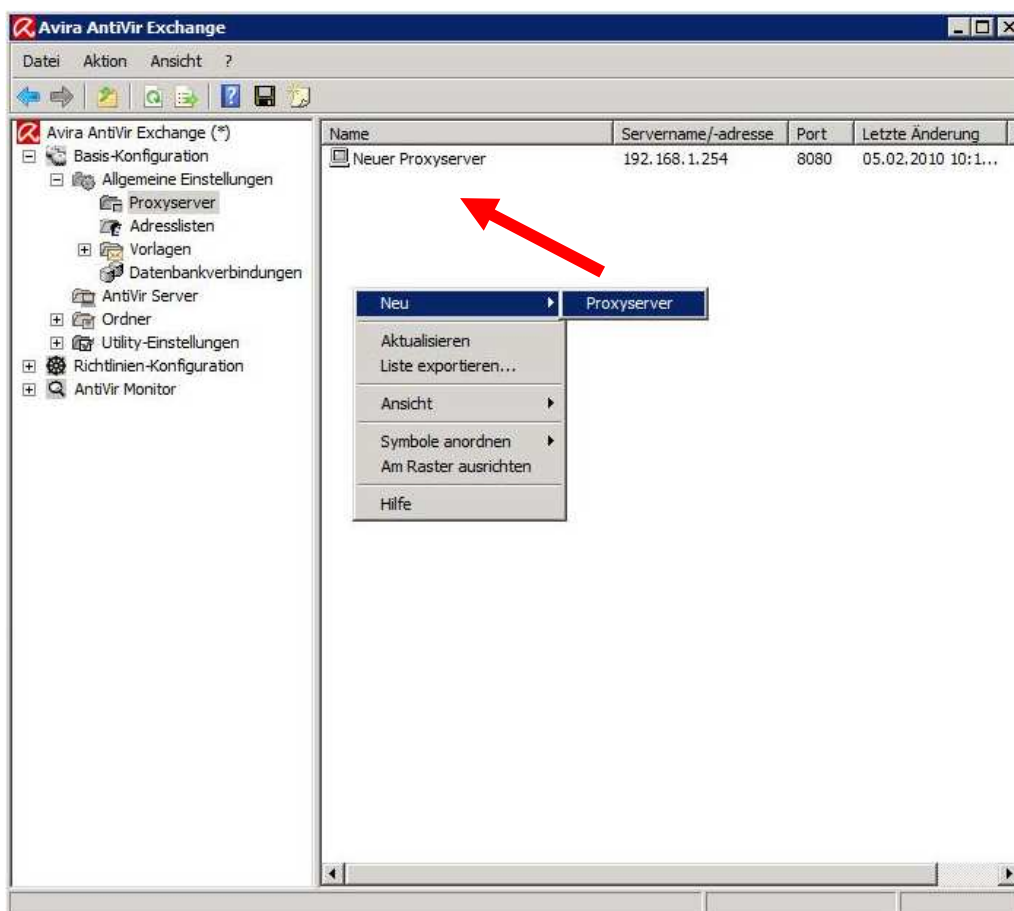
- **AntiSpam Engine:**
C:\Program Files (x86)\Avira\AntiVir Exchange\Bin\SPACE\Update\avupdate.log
- **AntiVir Engine:**
C:\Program Files (x86)\Avira\AntiVir Exchange\Bin\Savapi\Update\avupdate.log

8.1 Update via Proxy Server

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

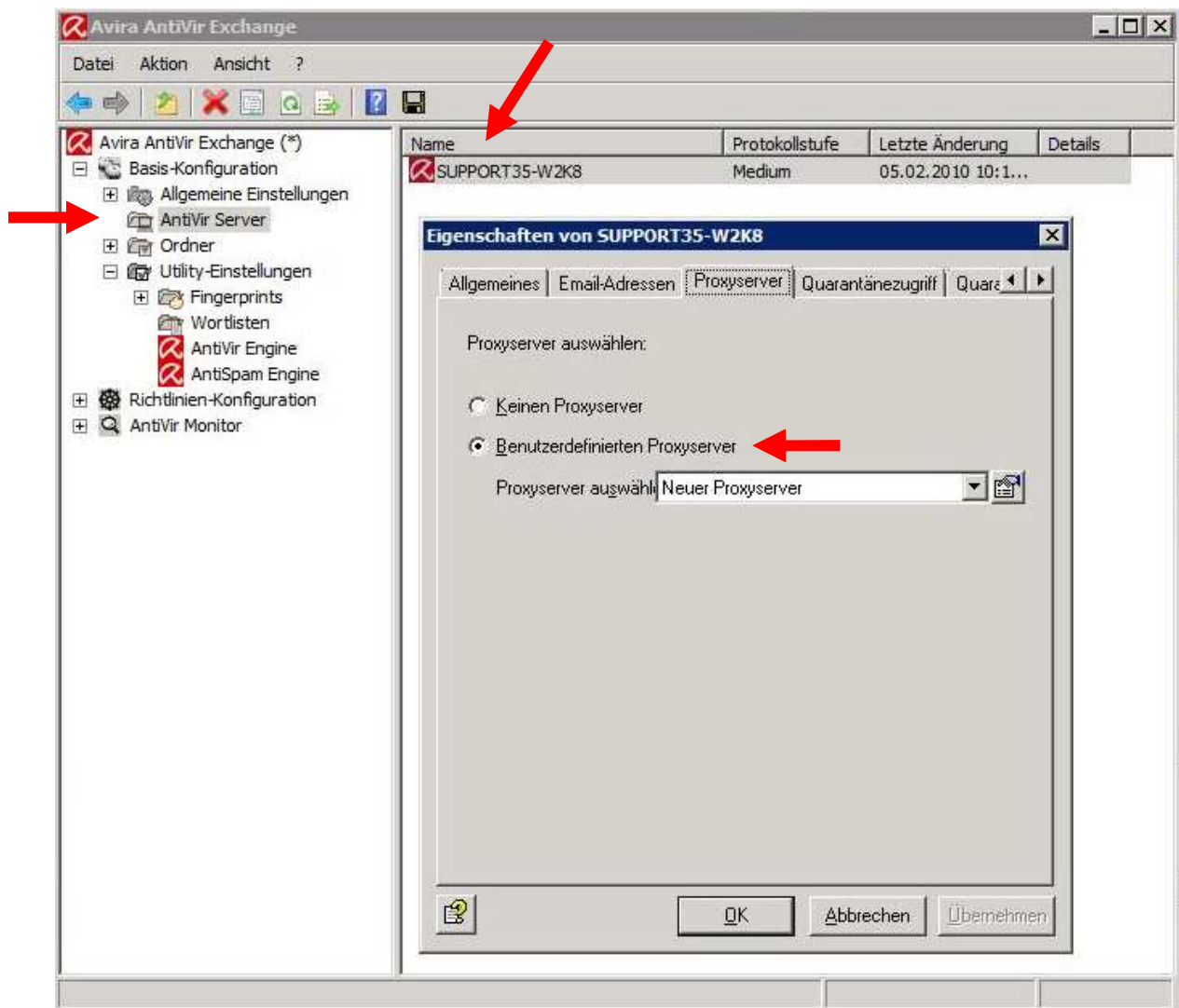
Die notwendige Konfiguration kann bzw. muss an verschiedenen Stellen vorgenommen werden.

Zuerst muss ein oder mehrere Proxy Server angegeben 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“** → **„AntiVir Server“** in den Eigenschaften von ihrem Server an.



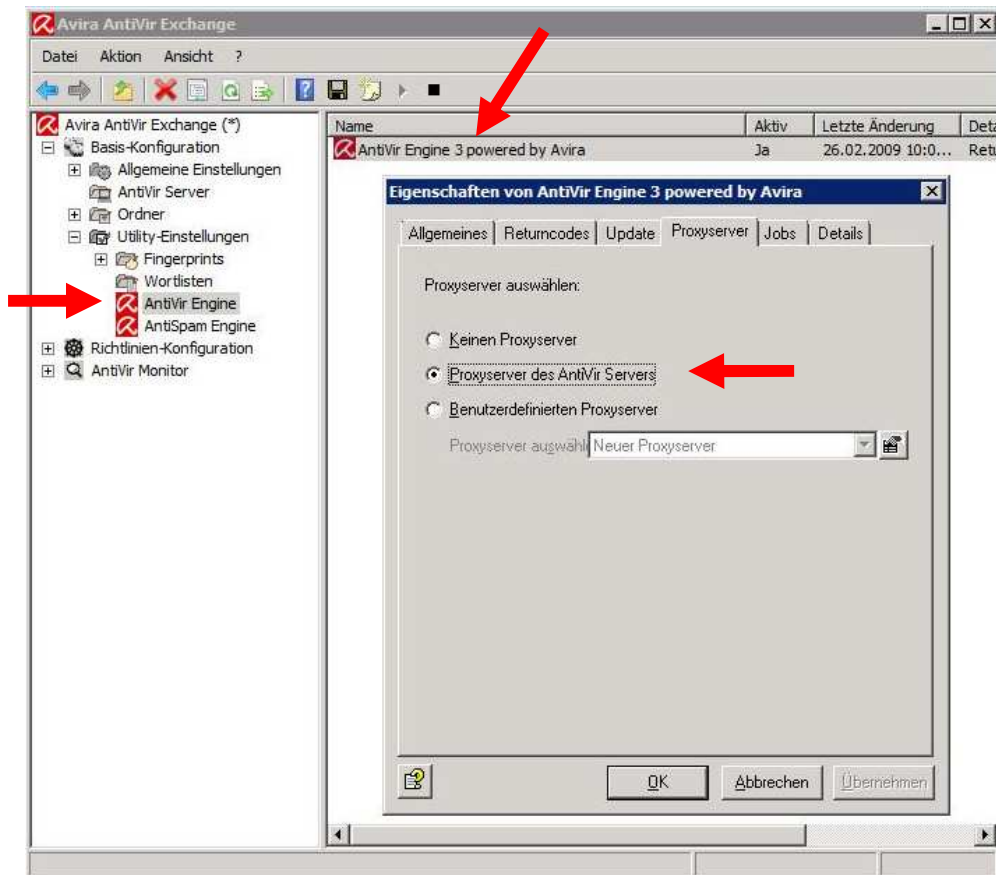
Somit haben Sie einen globalen Proxy Server definiert.

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

- *AntiVir Engine*
- *AntiSpam 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 AntiVir Servers**“ verwendet wird.



Hinweis:

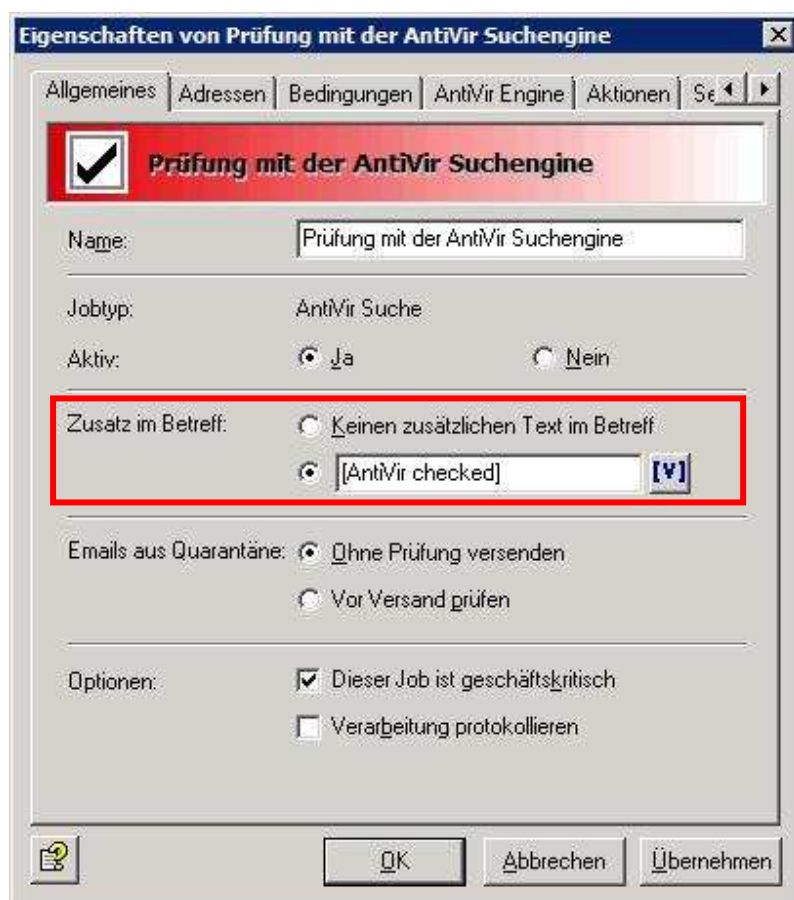
Sie haben die Möglichkeit, mehrere Proxy Server einzurichten und jedem Modul einen separaten Server anzugeben. Haken Sie in dem Fall den Punkt „**Benutzerdefinierten Proxyserver**“ an und wählen den entsprechenden Server in der Liste aus.

9. Jobvorschläge

9.1 Zusatz im Betreff entfernen

In der Standardkonfiguration fügt AntiVir Exchange im Betreff jeder Email den Zusatz [AntiVir checked] ein. Um diesen Zusatz zu ändern bzw. zu deaktivieren, muss jeder aktive Job separat konfiguriert werden. Rufen Sie die Eigenschaften jedes Jobs auf und Prüfen im Reiter „**Allgemeines**“, ob der Zusatz im Betreff aktiviert ist.

Nachfolgend anhand des Jobs „**Prüfung mit der AntiVir Suchengine**“ gezeigt:

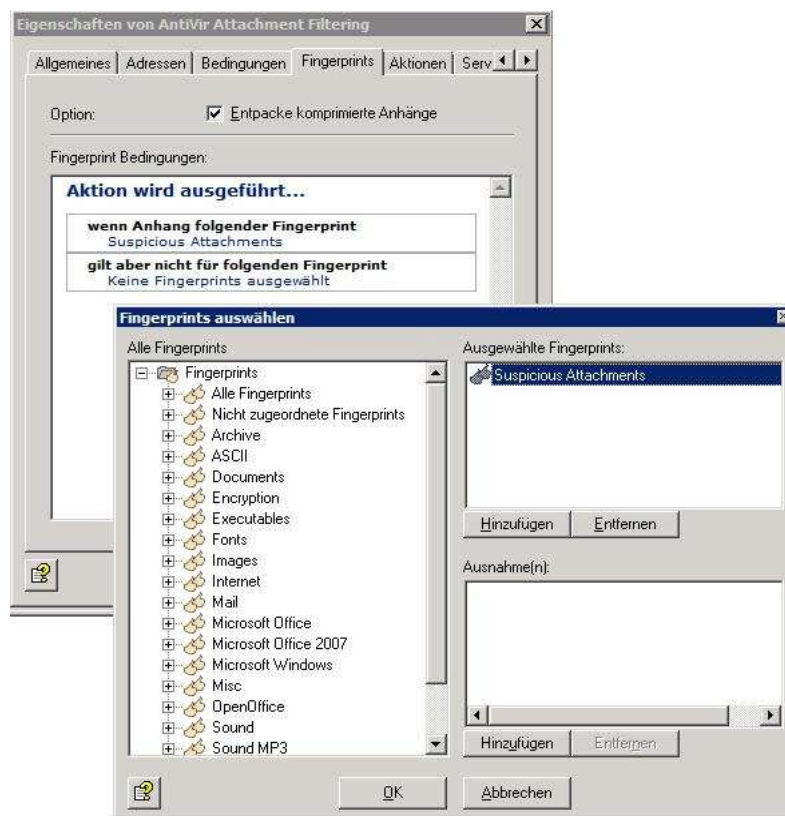


9.2 Unerwünschte Dateianhänge blocken

Um bestimmte Dateianhänge zu blocken, bietet AntiVir Exchange unter „**Jobvorlagen**“ einige vorkonfigurierte Jobs. Diese werden in der Spalte „**Jobtyp**“ als „**AntiVir 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 „**AntiVir Attachment Filtering**“. Die Eigenschaften des Jobs werden geöffnet und im Reiter „**Fingerprints**“ können Bedingungen sowie auch Ausnahmen definiert werden werden.



Fingerprints, die geblockt werden (auch eine ganze Fingerprint Gruppe, z.B. Images)

Hier kann man bestimmte Fingerprints ausnehmen (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 den entsprechenden Haken ggf.

9.3 Advanced Spamfiltering mit separaten Quarantänen

Hinweis: Bitte beachten Sie, dass nachfolgender Jobvorschlag in AntiVir Exchange 8 als Job integriert („Prüfung auf Spam mit Avira SPACE“) und standardmäßig aktiviert ist.

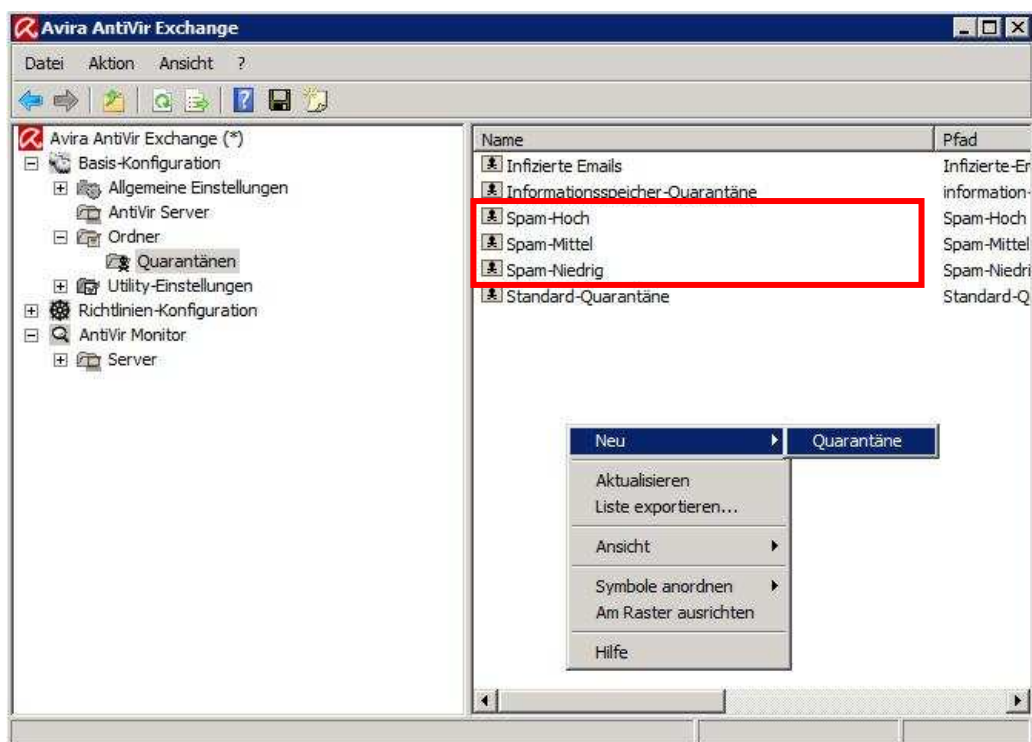
Mit dem Job „Advanced Spamfiltering“ kann man Spam in drei Kategorien unterteilen:

- Spam-Wahrscheinlichkeit: Niedrig
- Spam-Wahrscheinlichkeit: Mittel
- Spam-Wahrscheinlichkeit: Hoch

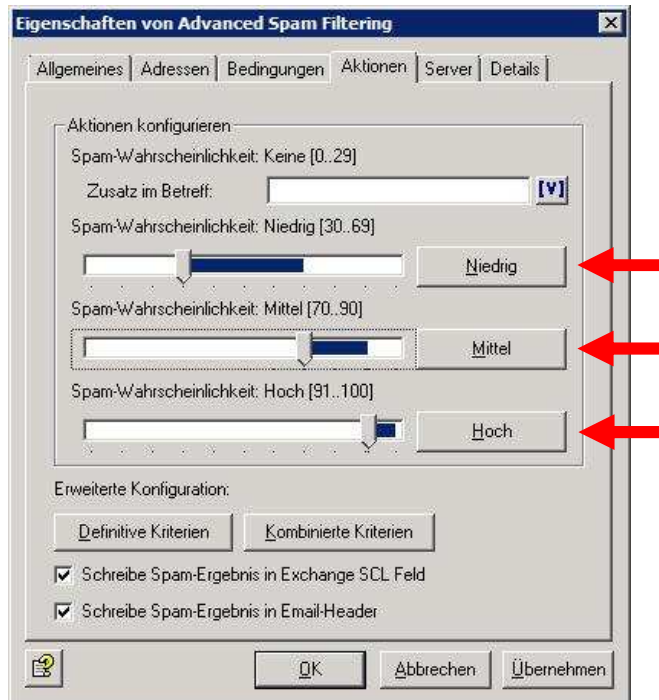
Für jede Kategorie kann man einen separaten Quarantäneordner auswählen und eingehende Mails können somit in verschiedene Quarantäneordner abgelegt werden.

Dazu müssen Sie zunächst entsprechende Quarantäneordner anlegen. Navigieren Sie dafür in der AntiVir Exchange Konsole unter „**Basis-Konfiguration**“ → „**Ordner**“ → „**Quarantänen**“. Klicken Sie mit der rechten Maustaste unter die bereits existierenden Ordner und legen folgende Quarantänen an (maximal 30 Zeichen möglich):

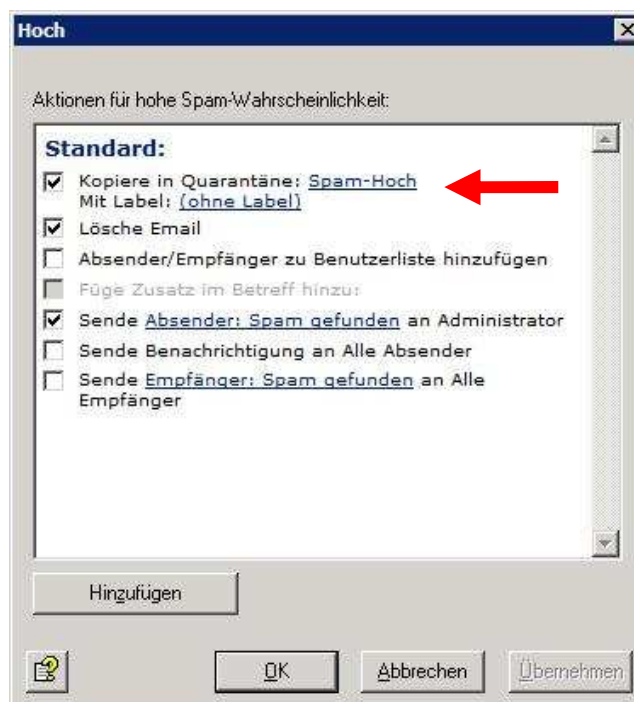
- Spam-Niedrig
- Spam-Mittel
- Spam- Hoch



Anschließend muss noch der Job „**Advanced Spam Filtering**“ unter „**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:

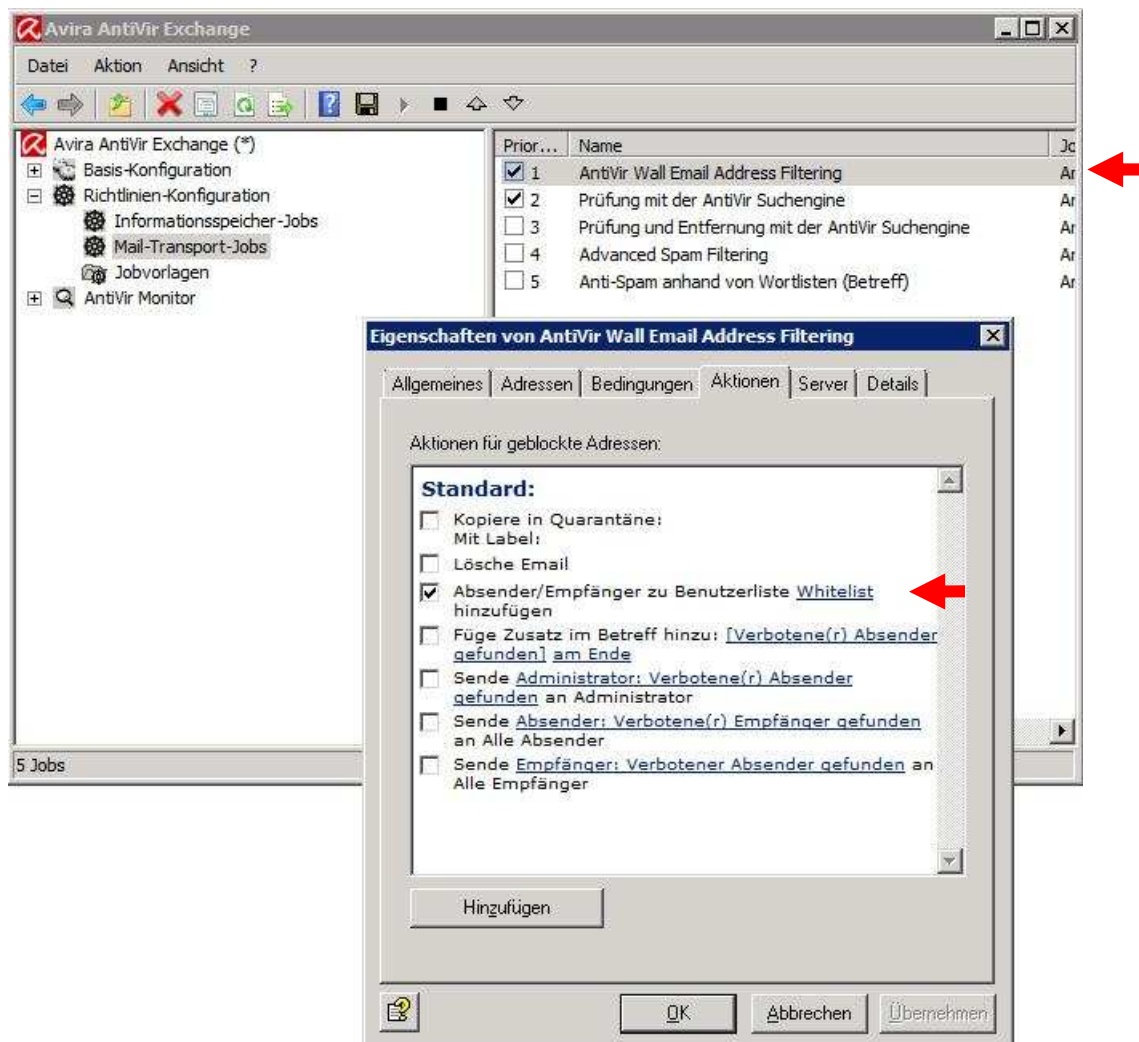


Wiederholen Sie diesen Vorgang für die Kategorie „**Mittel**“ sowie „**Niedrig**“.

9.4 Empfänger automatisch zur Whitelist hinzufügen

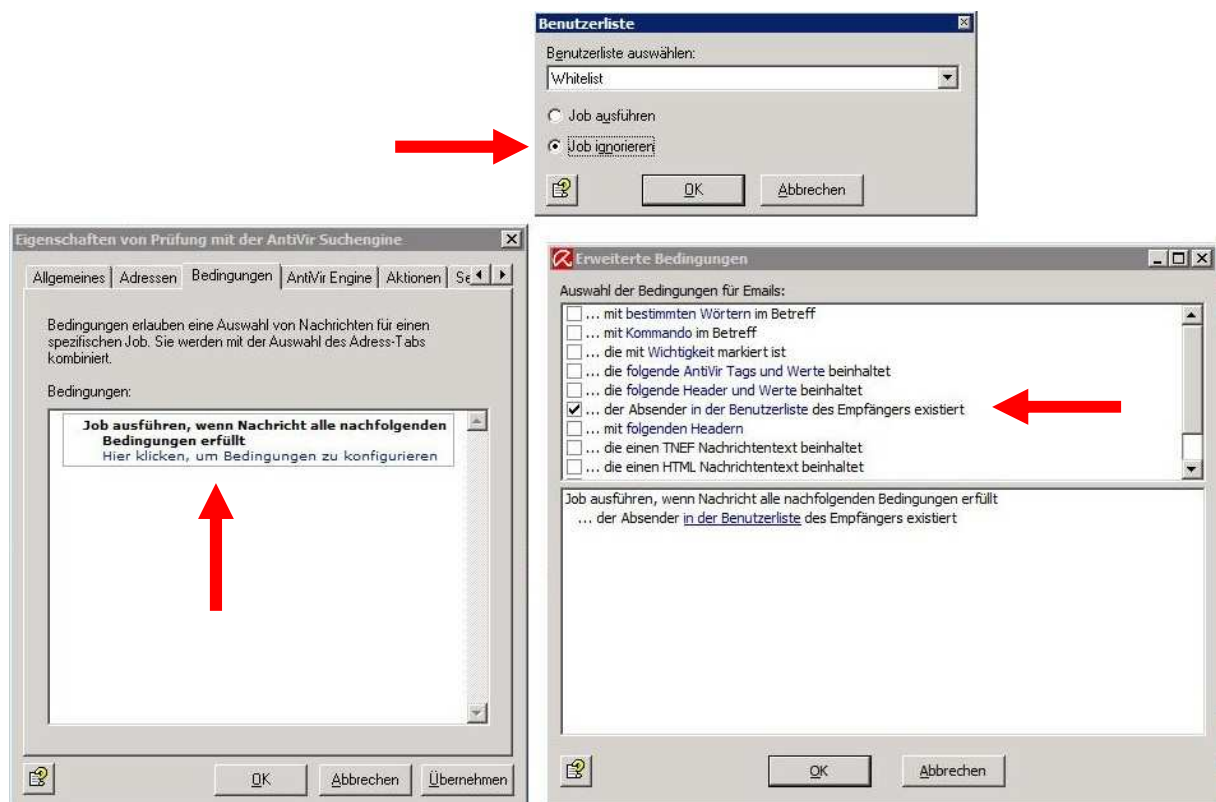
Folgendermaßen können Sie Empfänger bei Versand einer Mail automatisch zur Whitelist hinzufügen:

- Legen Sie einen neuen Job unter "**Mail-Transport-Jobs**" an:
"**AntiVir Wall 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



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 Job auf und klicken auf den Reiter "Bedingungen".
- Fügen Sie eine neue Bedingung hinzu: **"...der Absender *nicht* in der Benutzerliste 'Whitelist' des Empfängers existiert"**



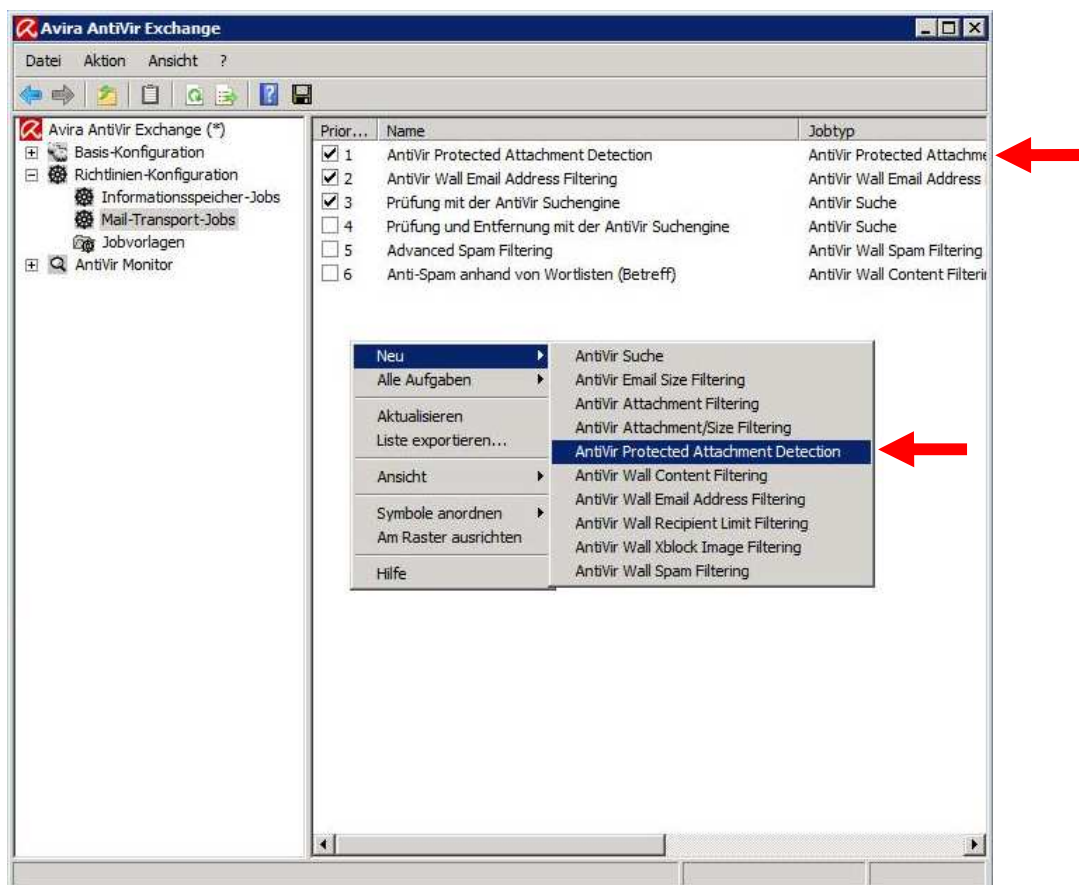
Speichern Sie anschließend die neue Konfiguration.

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

9.5 Passwort geschützte Archive

Passwort geschützte Archive werden standardmäßig von AntiVir Exchange geblockt. Seit der Version 8 gibt es jedoch einen neuen Job: "**Antivir 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.