

# Avira AntiVir Exchange

Handbuch für Anwender

# Inhaltsverzeichnis

<b>1 Quickstart</b> .....	<b>5</b>
1.1 Installation auf einem Exchange-Server .....	5
1.2 Starten der AntiVir Exchange Management Konsole .....	5
1.3 Konfiguration in der AntiVir Exchange Management Konsole .....	6
1.3.1 Notwendige Schritte in der Basis-Konfiguration .....	6
1.3.2 Notwendige Schritte in der Richtlinien-Konfiguration .....	6
1.3.3 Empfehlenswerte Schritte in der Basis-Konfiguration .....	7
1.3.4 Virenprüfung der Exchange Datenbanken.....	7
1.4 Beobachtung der Daten im AntiVir Monitor .....	7
<b>2 Installation</b> .....	<b>8</b>
2.1 Systemvoraussetzungen.....	8
2.2 Installation der Avira AntiVir Exchange auf einem Exchange Server .....	8
2.3 Deinstallation der Avira AntiVir Exchange.....	13
<b>3 Technische Beschreibung</b> .....	<b>14</b>
3.1 Der Avira AntiVir Exchange Server .....	15
3.1.1 Der Transport Agent .....	15
3.1.2 Der Avira AntiVir Exchange Service = Enterprise Message Handler (EMH) .....	15
3.1.3 Die Avira AntiVir Exchange Quarantäne .....	16
3.1.4 Das Active Directory/LDIF.....	17
3.1.5 Komprimierte Dateien/Archive: Der Avira AntiVir Exchange Entpacker .....	17
3.2 Die Avira AntiVir Exchange Konfiguration.....	18
<b>4 Details zur Avira AntiVir Exchange Management Konsole</b> .....	<b>19</b>
4.1 Die Symbolleiste .....	19
4.2 Bedeutung der Icons .....	20
4.3 Basis-Konfiguration.....	22
4.3.1 Überblick durch Konfigurationsreports.....	22
4.3.2 Konfiguration importieren .....	23
4.3.3 AntiVir Server-Einstellungen .....	23
4.3.4 Einstellungen für einen einzelnen Avira AntiVir Exchange Server.....	27
4.3.5 Adresslisten .....	33
4.3.6 Benachrichtigungsvorlagen.....	40
4.3.7 Datenbankverbindung zu einem SQL-Server anlegen .....	48
4.3.8 Ordner-Einstellungen.....	53
4.3.9 Utility-Einstellungen .....	62
4.4 Richtlinien-Konfiguration .....	63
4.4.1 Beispiel einer Unternehmensrichtlinie .....	63

---

4.4.2	Bedingungen .....	63
4.4.3	Jobtypen .....	64
4.4.4	Aktionen .....	66
4.4.5	Verarbeitungsreihenfolge der Jobs .....	66
4.5	AntiVir Monitor .....	67
4.5.1	Quarantänen .....	67
4.5.2	Avira AntiVir Exchange Reports .....	75
<b>5</b>	<b>AntiVir Such Engine .....</b>	<b>76</b>
5.1	Übersicht .....	76
5.1.1	Jobtypen .....	76
5.2	AntiVir Suche .....	76
5.3	Informationsspeicher-Scan .....	77
5.3.1	Status des Informationsspeichers .....	80
5.3.2	Virenprüfung im Informationsspeicher - Jobbeispiel .....	81
5.4	AntiVir Such Engine konfigurieren und aktivieren .....	88
5.5	Virenprüfung einschalten - Jobbeispiel .....	91
5.5.1	Allgemeine Einstellungen .....	91
5.5.2	Dieser Job ist geschäftskritisch .....	92
5.5.3	Verarbeitung protokollieren .....	92
5.6	Virenprüfung von passwortgeschützten Archiven .....	98
5.6.1	Jobbeispiel .....	98
5.7	Dateieinschränkungen für den Anhang .....	99
5.7.1	nach Typ .....	99
5.7.2	nach Email-Größe .....	100
5.7.3	nach Anhangtyp und/oder -Größe .....	100
5.7.4	Fingerprints konfigurieren .....	101
5.7.5	Dateianhänge nach Typ verbieten - Jobbeispiel .....	101
5.7.6	Email-Größe einschränken - Jobbeispiel .....	105
5.7.7	Anhangtypen und -größen verbieten - Jobbeispiel .....	108
<b>6</b>	<b>AntiVir Wall .....</b>	<b>114</b>
6.1	Jobtypen .....	114
6.2	Adressprüfung .....	114
6.2.1	Absender und/oder Empfänger verbieten - Jobbeispiel .....	115
6.3	Inhaltsprüfung mit Wortlisten .....	118
6.3.1	Wortlisten einrichten .....	118
6.3.2	Textinhalte prüfen und verbieten - Jobbeispiel .....	121
6.4	Limitieren der Anzahl der Empfänger .....	125
6.4.1	Empfängeranzahl begrenzen - Jobbeispiel .....	125

<b>7 Anti-Spam</b> .....	<b>129</b>
7.1 Avira AntiSpam Engine .....	129
7.1.1 AntiSpam Engine konfigurieren.....	129
7.2 Wall Spam Filtering Jobs .....	132
7.2.1 Definitive Kein-Spam-Kriterien .....	134
7.2.2 Definitive Spam-Kriterien .....	135
7.2.3 Praxistipps .....	136
7.3 Anti-Spam für Experten .....	137
7.3.1 Kombinierte Kriterien - Beispiel .....	138
7.3.2 Kombination der Hinweise zur Spam-Wahrscheinlichkeit .....	139
7.3.3 AntiSpam-Prüfung - Jobbeispiel .....	141
7.3.4 Advanced Spam Filtering Job konfigurieren.....	151
7.3.5 Manuelle AntiSpam-Konfiguration .....	152

# 1 Quickstart

- [Installation auf einem Exchange-Server](#)
- [Starten der AntiVir Exchange Management Konsole](#)
- [Konfiguration in der AntiVir Exchange Management Konsole](#)
- [Beobachtung der Daten im AntiVir Monitor](#)

## 1.1 Installation auf einem Exchange-Server

1. Zur Installation von Avira AntiVir Exchange führen Sie bitte einen Doppelklick auf die Installationsdatei aus:
  - Für Microsoft Exchange 2003: *avira\_antivir\_exchange\_2k\_32bit.exe*
  - Für Microsoft Exchange 2007/2010 (64-bit):  
*avira\_antivir\_exchange\_2k7\_64bit.exe*
2. Wählen Sie Ihre Sprache aus und befolgen Sie die weiteren Anweisungen des Setups, bis die Installation abgeschlossen ist.

Falls Sie kein anderes Installationsverzeichnis angeben, wird Avira AntiVir Exchange im folgendem Standardverzeichnis installiert:

*C:\Programme\Avira\AntiVir Exchange\ (deutsch)*

*C:\Program Files\Avira\AntiVir Exchange\ (englisch)*

oder

*C:\Programme(x86)\Avira\AntiVir Exchange\ (deutsch)*

*C:\Program Files(x86)\Avira\AntiVir Exchange\ (englisch)*


bei 64 bit-Versionen

**Warnung:** Deaktivieren Sie unbedingt eventuelle Real-Time bzw. On-Access Scan Funktionen der eingesetzten Virens Scanner für das Verzeichnis ... \Avira\AntiVir Exchange\AntiVirData\

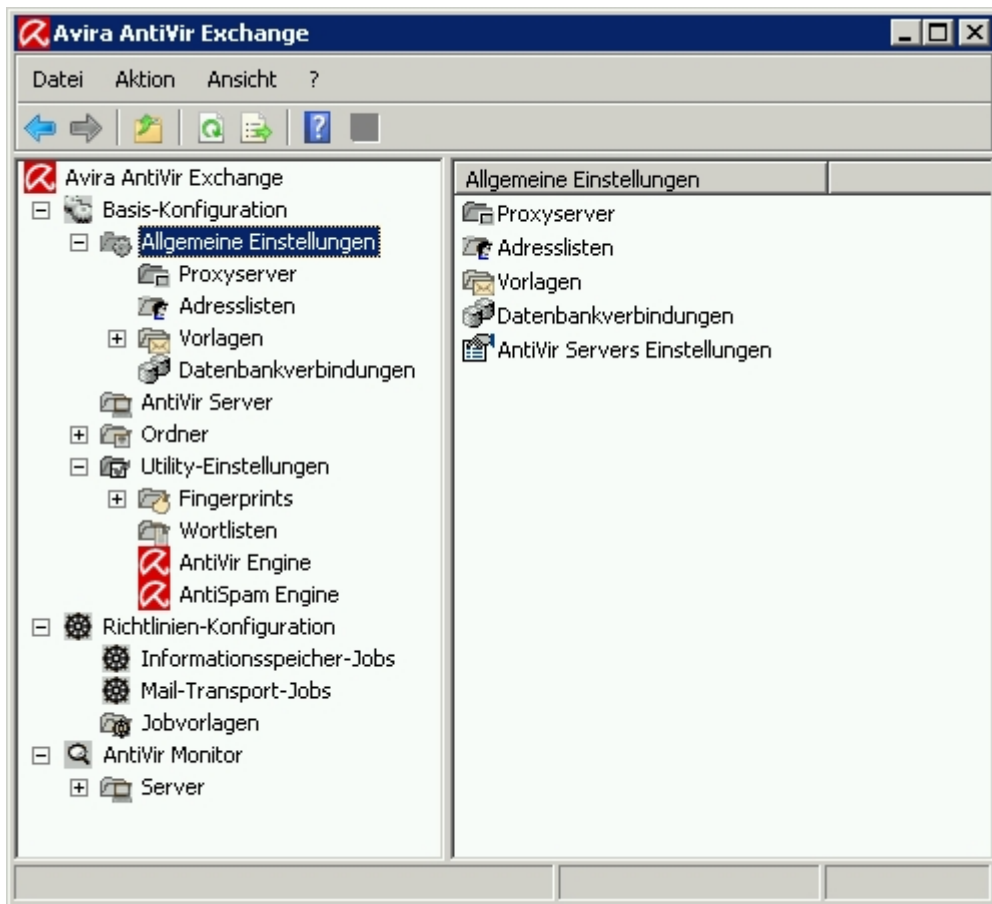
## 1.2 Starten der AntiVir Exchange Management Konsole

Avira AntiVir Exchange ist ein Serverprodukt, das durch die AntiVir Exchange Management Konsole konfiguriert wird. Damit Avira AntiVir Exchange funktioniert, muss der AntiVir für Exchange Service gestartet sein. Siehe dazu auch [Der Avira AntiVir Exchange Service = Enterprise Message Handler \(EMH\)](#)

1. Sie starten die Konsole über **Start - Programme - Avira - AntiVir Exchange - AntiVir Exchange Management Konsole**.  
Beim Schließen der AntiVir Exchange Management Konsole werden Sie gefragt, ob Sie eventuelle Änderungen speichern wollen.

**Hinweis:** Offene Änderungen werden durch (\*) am obersten Knoten angezeigt. Wenn Sie Ihre Änderungen an der Konfiguration speichern wollen, drücken Sie die **Speichern**  Schaltfläche. Die Konfiguration wird in der Datei *ConfigData.xml* gespeichert, die im Verzeichnis \Avira\AntiVir Exchange\Config\ abgelegt ist.

## 1.3 Konfiguration in der AntiVir Exchange Management Konsole



Im Anschluss an die Installation nehmen Sie in der AntiVir Exchange Management Konsole die nachfolgend beschriebenen Einstellungen vor.

### 1.3.1 Notwendige Schritte in der Basis-Konfiguration

In der **Basis-Konfiguration** definieren Sie die gültigen Server, E-Mail-Adressen, gemeinsamen Vorlagen und Utility-Einstellungen.

Überprüfen Sie unter **Basis-Konfiguration - Allgemeine Einstellungen - AntiVir Servers Einstellungen** auf der Registerkarte **Email-Adressen** die Einträge für die Administratoren und die internen Domänen. Siehe hierzu [AntiVir Servers-Einstellungen](#).

### 1.3.2 Notwendige Schritte in der Richtlinien-Konfiguration

In der **Richtlinien-Konfiguration** definieren und aktivieren Sie die gewünschten Jobs gemäß Ihren Firmenrichtlinien. D.h. Jobs sind nichts anderes als regelbasierte Maßnahmen oder Aktionen, die auf den Mailverkehr angewandt werden.

Um einen Job neu anzulegen, führen sie folgende Schritte aus:

1. Suchen Sie sich unter **Jobvorlagen** die gewünschte Vorlage aus.

2. Markieren Sie die Vorlage und ziehen Sie diese in den Ordner **Mail-Transport-Jobs**. Konfigurieren Sie den Namen und die Eigenschaften dieses Jobs und schalten Sie den Job unter Eigenschaften aktiv. (*aktiv: ja*).
3. Achten Sie auf die Reihenfolge des Abarbeitens der Jobs (siehe [Verarbeitungsreihenfolge der Jobs](#)).
4. **Speichern** Sie Ihre Änderungen. Siehe auch [Starten der AntiVir Exchange Management Konsole](#).

Es ist wichtig, zwischen zwei Kategorien für Jobs zu unterscheiden.

Jobs für die AntiVir Such Engine, die z.B. nach Viren, Malware oder schädlichen Skripten suchen oder Emails nach Größe und/oder Typ des Dateianhanges filtern, und Jobs für die AntiVir Wall, anhand derer Emails nach einer Reihe von Kriterien (z.B. Adressen, Wörter) gefiltert werden können.

### 1.3.3 Empfehlenswerte Schritte in der Basis-Konfiguration

Es ist empfehlenswert, in der Basis-Konfiguration individuelle Einstellungen für Adresslisten, Vorlagen usw. vorzunehmen. Diese Einstellungen sind für einen Testbetrieb aber nicht zwingend erforderlich.

1. Konfigurieren Sie die **Adresslisten** (für die Auswahl in den Job-Regeln) unter **Allgemeine Einstellungen**.
2. Ändern Sie ggf. die Standard-Vorlagen unter **Allgemeine Einstellungen**.
3. Konfigurieren Sie unter **Utility-Einstellungen** das benötigte Zubehör wie Wortlisten, Fingerprints und Virens Scanner.

### 1.3.4 Virenprüfung der Exchange Datenbanken

In der **Richtlinien-Konfiguration - Informationsspeicher-Jobs** können Sie für jeden AntiVir Server getrennt die entsprechenden Einstellungen vornehmen.

Informationsspeicher-Jobs können nicht selbst angelegt werden. Sobald Sie einen neuen Server hinzugefügt haben, steht automatisch ein entsprechender Informationsspeicher-Job zur Verfügung.

Wenn Sie den Server wieder entfernen, wird auch der Informationsspeicher-Job gelöscht.

Weitere Informationen über Informationsspeicher-Jobs finden Sie unter [Informationsspeicher-Scan](#).

## 1.4 Beobachtung der Daten im AntiVir Monitor

Nach dem Speichern Ihrer Einstellungen überwachen Sie den laufenden Betrieb der Avira AntiVir Exchange mit dem **AntiVir Monitor**.

Im **AntiVir Monitor** können Sie die aktuellen "Live-Daten" beobachten und zum Beispiel die **Quarantänen** der konfigurierten Server administrieren.

Nähere Informationen finden Sie unter [AntiVir Monitor](#).

## 2 Installation

- [Systemvoraussetzungen](#)
- [Installation der Avira AntiVir Exchange auf einem Exchange Server](#)
- [Deinstallation der Avira AntiVir Exchange](#)

### 2.1 Systemvoraussetzungen

Für die Installation der Avira AntiVir Exchange sind folgende Voraussetzungen erforderlich:

- CD-ROM-Laufwerk oder Netzwerkzugang
- RAM: Exchange Empfehlung + zusätzlich 64 MB
- Festplatte: mindestens 400 MB für die Installation
- Microsoft .NET Framework 2.x
- Betriebssysteme (sowohl 32 bit als auch 64 bit):
  - Windows Server 2003
  - Windows Server 2008
- Exchange Server:
  - MS Exchange Server 2003
  - MS Exchange Server 2007 SP1 Update Rollup 4  
Hier werden folgende Rollen unterstützt:
    - Hub Transport Server
    - Mailbox Server
  - MS Exchange Server 2010

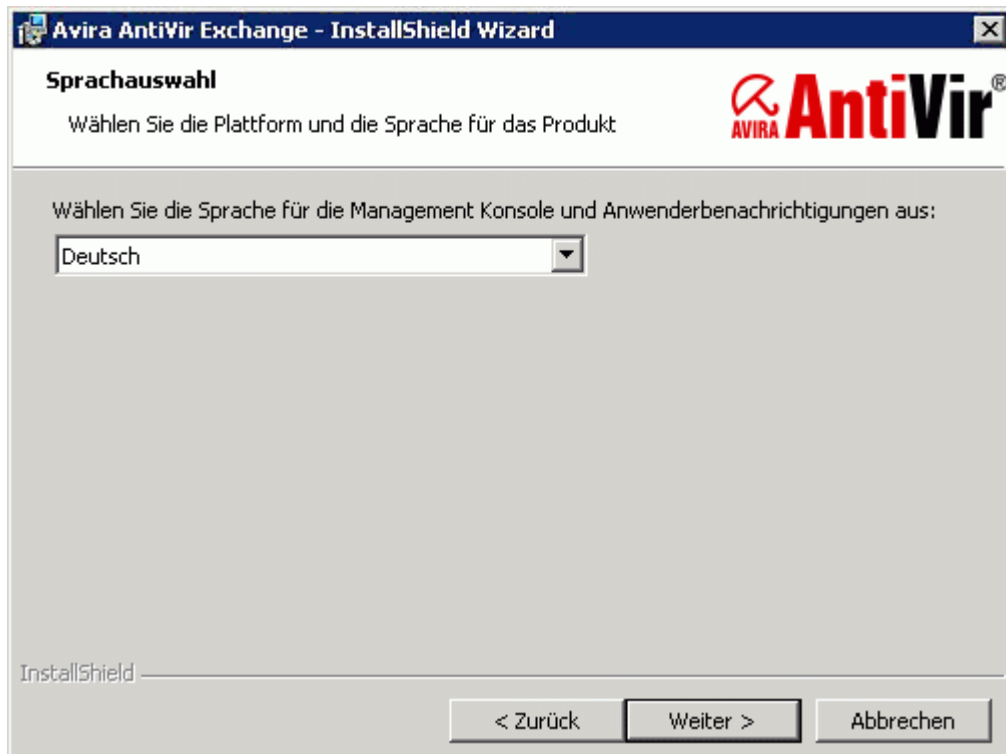
**Hinweis:** Für Informationen über Cluster-Installation wenden Sie sich bitte an den Support.

**Warnung:** Deaktivieren Sie unbedingt eventuelle Real-Time bzw. On-Access Scan Funktionen der eingesetzten Virens Scanner für das Verzeichnis ... \Avira\AntiVir Exchange\AntiVirData\

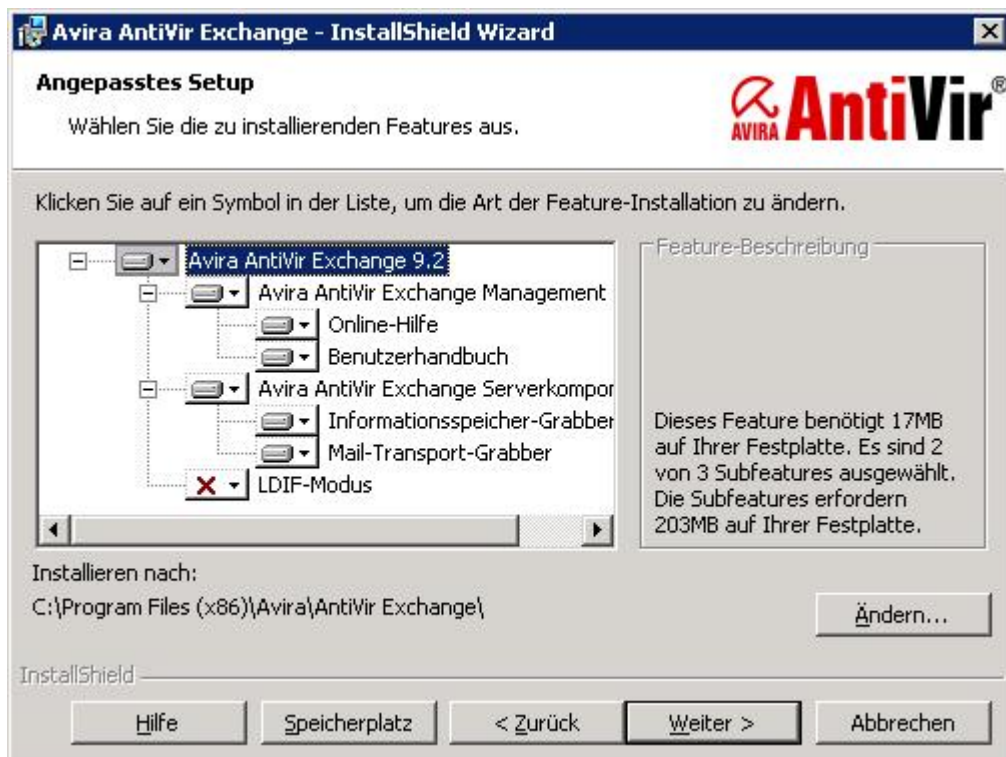
### 2.2 Installation der Avira AntiVir Exchange auf einem Exchange Server

1. Zur Installation von Avira AntiVir Exchange führen Sie bitte einen Doppelklick auf die Installationsdatei aus, wie z.B. :  
*avira\_antivir\_exchange\_2k\_32bit.exe*
2. Wählen Sie zunächst die **Setup-Sprache**. Danach wählen Sie die Plattform und die Sprache für das Produkt.  
Die ausgewählte Produktsprache gilt für die Produktoberfläche und für die Anwenderbenachrichtigungen, die von der Avira AntiVir Exchange an die Benutzer verschickt werden.



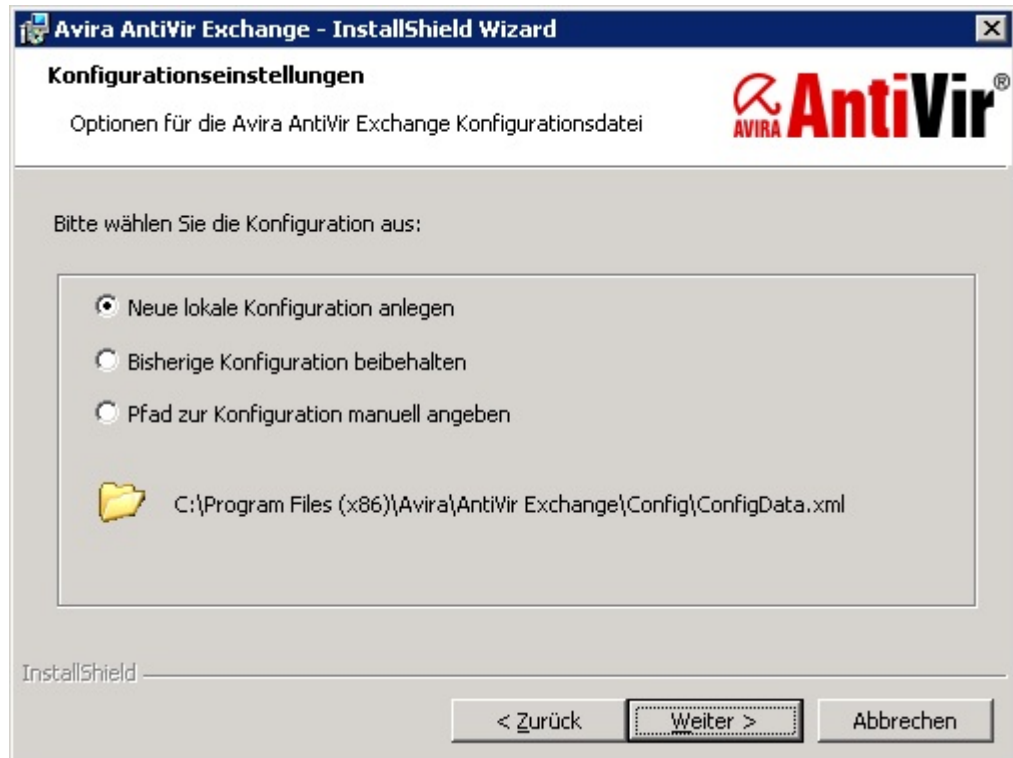


3. Akzeptieren Sie im nächsten Dialogfenster die *Lizenzvereinbarung*, um fortfahren zu können und klicken Sie **Weiter**.
4. Im nächsten Dialogfenster wählen Sie die Features aus, die Sie installieren möchten. Mit dieser Auswahl werden alle Serverkomponenten und die AntiVir Exchange Management Konsole installiert:



Sollte sich eine andere aktive Information Store Scan Anwendung, ausgenommen Avira AntiVir Exchange, auf dem Server befinden, ist die Informationsspeicher Scan Funktion inaktiv. Wenn Sie den Information Store Scan benutzen wollen, müssen Sie zuerst die andere Anwendung deinstallieren.

5. Klicken Sie **Weiter**.
6. Im nächsten Dialogfenster werden Sie nach dem Ablageort der Konfigurationsdatei gefragt:



Wenn Sie Avira AntiVir Exchange nicht auf mehreren Servern betreiben und dabei zentral mit einer Konfiguration administrieren möchten, bestätigen Sie die Voreinstellung und klicken Sie **Weiter**.

7. Im nächsten Dialog legen Sie die *Email-Adresse des Administrators* fest.

**Avira AntiVir Exchange - InstallShield Wizard**

**Konfiguration der E-Mail Adresse**

Geben Sie die E-Mail Adresse des Avira AntiVir Exchange Administrators ein.

E-Mail Adresse des Avira AntiVir Exchange Administrators:

Die E-Mail-Adresse des Administrators wird für das Versenden von Avira AntiVir Exchange Benachrichtigungen benötigt. Sie können die E-Mail-Adresse des Administrators später noch unter Basis-Konfiguration / Avira AntiVir Exchange Servers ändern. Weitere Informationen finden Sie im Handbuch oder in der Online-Hilfe.

InstallShield

< Zurück Weiter > Abbrechen

8. Wenn Sie einen Proxy-Server für das AntiVir-Update verwenden, aktivieren Sie das Kontrollkästchen und nehmen Sie die Proxy-Einstellungen zu IP-Adresse, Port, Benutzer und Passwort vor. Das Passwort wird im Klartext abgespeichert!

**Avira AntiVir Exchange - InstallShield Wizard**

**Proxy Server Einstellungen**

Geben Sie die Informationen Ihres Proxy Servers ein

Folgende Proxy-Einstellungen werden zur Aktualisierung der in Avira AntiVir Exchange integrierten Antivirus und Antispam Engines verwendet. Die Einstellungen können hier angegeben werden, oder Sie können dies später in der Administrations-Konsole nachholen.

Proxy Server verwenden

Proxy Adresse:

Port:

Benutzer:

Passwort:

InstallShield

< Zurück Weiter > Abbrechen

9. Im nächsten Dialogfenster werden Sie nach der Lizenzdatei gefragt:



Aktivieren Sie die Option **Lizenzdatei verwenden** und benutzen Sie **Browse**, um den Pfad zur Lizenzdatei festzustellen.

10. Sie erhalten nun eine Zusammenfassung Ihrer Einstellungen:



11. Deaktivieren Sie jetzt die On-Access-Scanner für das Verzeichnis ...\*AntiVirData*, falls Sie das noch nicht getan haben.

12. Überprüfen Sie Ihre Konfigurationseinstellungen.  
Diese Einstellungen werden als Standardeinträge in die Konfiguration des Avira AntiVir Exchange Servers übernommen. Näheres dazu ab [AntiVir Exchange Servers-Einstellungen](#).
13. Folgen Sie weiter den Anweisungen und klicken Sie auf Installieren.  
Avira AntiVir Exchange wird anschließend in folgendes Verzeichnis installiert:  
<LW>:\<std.progr.verzeichnis>\Avira\AntiVir Exchange\
14. Mit dem **Fertigstellen** der letzten Dialogbox haben Sie Avira AntiVir Exchange erfolgreich installiert.

Der AntiVir Virenschanner ist fertig konfiguriert und sofort einsatzfähig. Dazu stellen wir einen Job für die Virenprüfung mit AntiVir zur Verfügung, den Sie einfach aktivieren können.

Siehe auch [AntiVir Virenschanner konfigurieren und aktivieren](#).

**Warnung:** Deaktivieren Sie unbedingt eventuelle Real-Time bzw. On-Access Scan Funktionen der eingesetzten Virenschanner für das Verzeichnis ... \Avira\AntiVir Exchange\AntiVirData\

## 2.3 Deinstallation der Avira AntiVir Exchange

1. Klicken Sie auf **Start - Systemsteuerung - Programme und Funktionen**
2. Wählen Sie **Avira AntiVir Exchange** aus
3. Klicken Sie auf **Fortsetzen**. Das Setup wird aufgerufen und deinstalliert Avira AntiVir Exchange.

## 3 Technische Beschreibung

Avira AntiVir Exchange gliedert sich in drei Hauptbestandteile:

- [die Avira AntiVir Exchange Konsole](#)
- [der Avira AntiVir Exchange Server](#)
- [die Avira AntiVir Exchange Konfiguration](#)

Die Avira AntiVir Exchange Konsole ist die Benutzeroberfläche, über die Avira AntiVir Exchange konfiguriert und administriert wird. Es handelt sich hierbei um ein so genanntes "Snap-In" für die MMC.

Mit der Avira AntiVir Exchange Konsole können sowohl einzelne Exchange-Server mit installierter Avira AntiVir Exchange administriert werden als auch ganze "Avira AntiVir Exchange Serverfarmen". Dies erleichtert speziell in einer Multi-Server-Umgebung die tägliche Administration.

Mit der Avira AntiVir Exchange Konsole erhält der Administrator Zugriff auf alle erforderlichen Konfigurationsinformationen und den AntiVir Monitor (enthält u.a. einen Überblick über die Quarantänen) der Avira AntiVir Exchange Server. Für die Konfiguration und die Zugriffe auf die Quarantänen werden zwei unterschiedliche Zugriffsmethoden verwendet.

1. Standard Windows Dateizugriff  
Für den Zugriff auf die Avira AntiVir Exchange Konfiguration, um beispielsweise Sicherheitseinstellungen zu administrieren, ist ein Windows Dateizugriff erforderlich. Hierbei kann die Avira AntiVir Exchange Konfiguration lokal zur Verfügung stehen.
2. SOAP und SSL  
Der Zugriff auf den [AntiVir Monitor](#) erfolgt über SOAP und SSL. Dabei wird über einen festgelegten Kommunikationsport kommuniziert.

Die Avira AntiVir Exchange Konsole unterstützt zwei Betriebsmodi.

1. Lokale Administration  
Hierbei wird die Avira AntiVir Exchange Konsole direkt auf dem Exchange-Server betrieben, auf welchem alle Komponenten der Avira AntiVir Exchange installiert wurden. Dieser Modus eignet sich für kleinere Umgebungen und die Administration am Server vor Ort.
2. Remote Administration  
In diesem Fall wird die Avira AntiVir Exchange Konsole nicht auf dem Exchange-Server, sondern auf einem Client installiert.

Die Avira AntiVir Exchange Konsole ist auf folgenden Betriebssystemen lauffähig:

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

Die Remote Administration eignet sich für die zentrale Administration in Multi-Server-Umgebungen. Die Avira AntiVir Exchange Konsole greift dabei auf einen oder mehrere Exchange-Server zu, um die Avira AntiVir Exchange zu konfigurieren und zu administrieren.

## 3.1 Der Avira AntiVir Exchange Server

Mit Avira AntiVir Exchange Server werden die Funktionen und Prozesse der Avira AntiVir Exchange bezeichnet, die ausschließlich auf dem Exchange-Server laufen.

Hierbei kann der Avira AntiVir Exchange Server sowohl in einfachen Umgebungen als auch in Front-End/Back-End-Umgebungen installiert werden.

Der Avira AntiVir Exchange Server unterteilt sich wiederum in verschiedene Bereiche.

### 3.1.1 Der Transport Agent

Der Transport Agent ist ein Prozess, der dafür zuständig ist, dass alle E-Mails, Terminanfragen, etc., die der Exchange-Server versendet, empfängt oder routet, "abgegriffen" (englisch: to grab) werden.

Für den gesamten Transport von Emails, Terminanfragen, etc. wird das SMTP-Transportprotokoll verwendet. Ein Bestandteil des SMTP-Transportprotokolls ist der "Microsoft SMTP Transportstapel" (englisch: "MS SMTP Transport Stack"). Durch diesen Transport Stack wird der komplette E-Mail-Verkehr geleitet. Dabei ist es unerheblich, ob es sich um Emails handelt, die zwischen Postfächern auf dem gleichen Postfachspeicher oder Server gesendet werden oder um ein- und ausgehende Emails.

In allen Fällen müssen Emails den Transport Stack durchlaufen. Der Transport Agent ist in diesem Transportstapel "eingeklinkt". Als registrierte Ereignissenke (englisch: Event Sink) überwacht der Transport Agent dort den E-Mail-Verkehr und leitet alle relevanten Informationen an den Avira AntiVir Exchange Service – die zweite Komponente des Avira AntiVir Exchange Server – weiter. Die Email wird so lange aufgehalten, bis die gesamte Verarbeitung durch den Avira AntiVir Exchange Server erfolgreich beendet ist.

**Hinweis:** Exchange-interne Informationen, wie beispielsweise Replikationsnachrichten, werden vom Transport Agenten als solche erkannt und unverändert im Exchange-System belassen.

### 3.1.2 Der Avira AntiVir Exchange Service = Enterprise Message Handler (EMH)

Der Avira AntiVir Exchange Service ist als Windows Dienst permanent gestartet und übernimmt alle Informationen vom Transport Agent. Die gesamte Weiterverarbeitung durch Avira AntiVir Exchange wird ab diesem Zeitpunkt vom Avira AntiVir Exchange Service überwacht und gesteuert. Wird der Avira AntiVir Exchange Service gestoppt, werden die Sicherheitsfunktionen der Avira AntiVir Exchange abgeschaltet.

Der Avira AntiVir Exchange Service hat Zugriff auf alle notwendigen Informationen:

- Die konfigurierten Avira AntiVir Exchange Jobs
- Die installierte Avira AntiVir Exchange Lizenz
- Das Active Directory
- Die Avira AntiVir Exchange Quarantäne

Mit Hilfe all dieser Informationen werden die Emails nun beispielsweise nach Viren überprüft, Spam Emails identifiziert und unter Quarantäne gestellt.

Nach der Bearbeitung übergibt der Avira AntiVir Exchange Service die Emails wieder an den SMTP-Server.

### 3.1.3 Die Avira AntiVir Exchange Quarantäne

Als eine mögliche Option können virenverseuchte Emails oder andere unerwünschte Emails auf dem Server gestoppt werden. Damit wird verhindert, dass diese E-Mails bei den entsprechenden Empfängern ankommen. Diese Emails werden stattdessen in der Avira AntiVir Exchange Quarantäne abgelegt. Auf jedem Avira AntiVir Exchange Server stehen nach der Installation einige Quarantänen zur Verfügung. Weitere Quarantänen können vom Administrator angelegt werden.

Eine Avira AntiVir Exchange Quarantäne besteht aus:

- einem Quarantäneverzeichnis auf dem Exchange-Server (...\*AntiVirData*\*Quarantine*\*Standard-Quarantaene*)
- den E-Mails, die in die Quarantäne kopiert wurden
- einer Quarantäne Datenbank (*LocIdxDB.mdb*).

Für jede unter Quarantäne gestellte Email erzeugt Avira AntiVir Exchange automatisch einen Eintrag in der Quarantänedatenbank. Bei dieser Datenbank handelt es sich um eine Microsoft Access Datei.

In dieser Datenbank werden folgende Informationen abgelegt:

- Email Betreff
- Datum/Uhrzeit
- Email Sender
- Email Empfänger
- Email Sender (SMTP)
- Email Empfänger (SMTP)
- Kurzbeschreibung der entdeckten Restriktion
- Email-Größe
- Name des Avira AntiVir Exchange Jobs, der diese Email in Quarantäne stellte
- Name des Exchange-Servers
- Name der Emailedatei
- Bearbeitungshistorie

Beim Anzeigen einer Avira AntiVir Exchange Quarantäne mit der Avira AntiVir Exchange Konsole werden zunächst die Informationen aus der Quarantänedatenbank angezeigt.

Beim Öffnen eines Quarantäneeintrags werden weitere Informationen aus der Emailedatei geladen.

Die Kommunikation mit der Avira AntiVir Exchange Quarantäne erfolgt mit Hilfe von SOAP (Simple Object Access Protocol) + SSL (Secure Socket Layer). Dies gilt sowohl für den "lokalen" Zugriff auf dem Server direkt als auch für den Zugriff von einer entfernten Windows Workstation. Dabei wird für die Kommunikation standardmäßig der Port 8008 verwendet. Dieser Port kann in der Avira AntiVir Exchange Konsole (Knoten **AntiVir Server**) verändert werden. Wird dieser Port für den Server verändert, so muss diese Änderung auch auf allen zugreifenden Avira AntiVir Exchange Konsole angepasst werden. Alle Rechner müssen den gleichen Port verwenden. Mit Hilfe von SSL wird der SOAP Kommunikationskanal verschlüsselt. Während der Installation werden hierfür alle notwendigen Komponenten bereitgestellt.



### 3.1.4 Das Active Directory/LDIF

Avira AntiVir Exchange nimmt keine Veränderungen oder Erweiterungen im Active Directory (AD) vor. Informationen aus dem Active Directory werden jedoch an verschiedenen Stellen von der Avira AntiVir Exchange ausgelesen.

Beim Starten ermittelt der Avira AntiVir Exchange Service den verfügbaren Global Catalog Server. Dieser wird zum Beispiel bei der Adressauflösung von Verteilerlisten während der E-Mail-Verarbeitung verwendet.

Die Avira AntiVir Exchange Konsole verwendet das Active Directory bei der Auswahl von Sender/ Empfänger Bedingungen.

Steht kein Active Directory zur Verfügung, da z. B. die entsprechenden Ports nicht offen sind, kann mit einer LDIF-Datei gearbeitet werden. Diese kann beispielsweise durch einen LDAP Export aus einem Active Directory, Exchange Benutzerverzeichnis oder einem Notes Name- and Addressbook (Namens- und Adressbuch -NAB) erzeugt werden.

### 3.1.5 Komprimierte Dateien/Archive: Der Avira AntiVir Exchange Entpacker

Wenn Dateien per E-Mail verschickt werden, geschieht dieses häufig in komprimierter Form. Damit der Virenskan und alle Prüfungen auch bei Archiven funktionieren, benutzt Avira AntiVir Exchange einen Entpacker, um Dateien innerhalb der Archive prüfen zu können. Avira AntiVir Exchange beinhaltet einen Entpacker, der nach der Installation automatisch zur Verfügung steht.

Der Entpacker unterstützt die folgenden Archivformate:

- ACE
- CAB
- ZIP
- Selfextracting ZIP
- ARJ
- Selfextracting ARJ
- TAR
- GZIP
- TGZ (Tape archive)
- UUE (Executable compressed ASCII archive)
- LZH (LH ARC)
- RAR
- Selfextracting RAR
- Java Archive (.jar)
- BZIP2
- 7-ZIP

**Hinweis:** Innerhalb eines Archivs können sich wiederum Archive befinden. Diese Archive (rekursiv gepackte Dateien) werden standardmäßig bis zu einer Entpackungstiefe von 5 entpackt. Alle Archive, die dieses Limit überschreiten, werden in den Bad-Mail-Bereich überführt.

Die Standard-Obergrenze für eine Email inkl. entpackte Dateien beträgt 300 MB. Insbesondere bei so genannten "ZIP of Death"-Attacken ist eine solche Limitierung wichtig.

Die Entpackungstiefe und die Größenlimitierung können in der Konsole unter **Basis-Konfiguration - AntiVir Server - Eigenschaften - Allgemeines** geändert werden.

### 3.2 Die Avira AntiVir Exchange Konfiguration

Alle Informationen, die zum Betreiben der Avira AntiVir Exchange erforderlich sind, werden in der Avira AntiVir Exchange Konfiguration gespeichert. Die Avira AntiVir Exchange Konfiguration liegt in Form einer XML-Datei (*ConfigData.xml*) vor.

Die *ConfigData.xml* ist ähnlich einer Datenbank angelegt. Für jeden Konfigurationsbereich sind verschiedene Einträge vorhanden. Da es sich bei der Konfiguration um eine einzelne Datei handelt, ist es sehr einfach, die Konfiguration zu verteilen und zu sichern. Für die Unterstützung bei Konfigurationsproblemen kann die *ConfigData.xml* zur Analyse an das Avira Support Team gesendet werden.

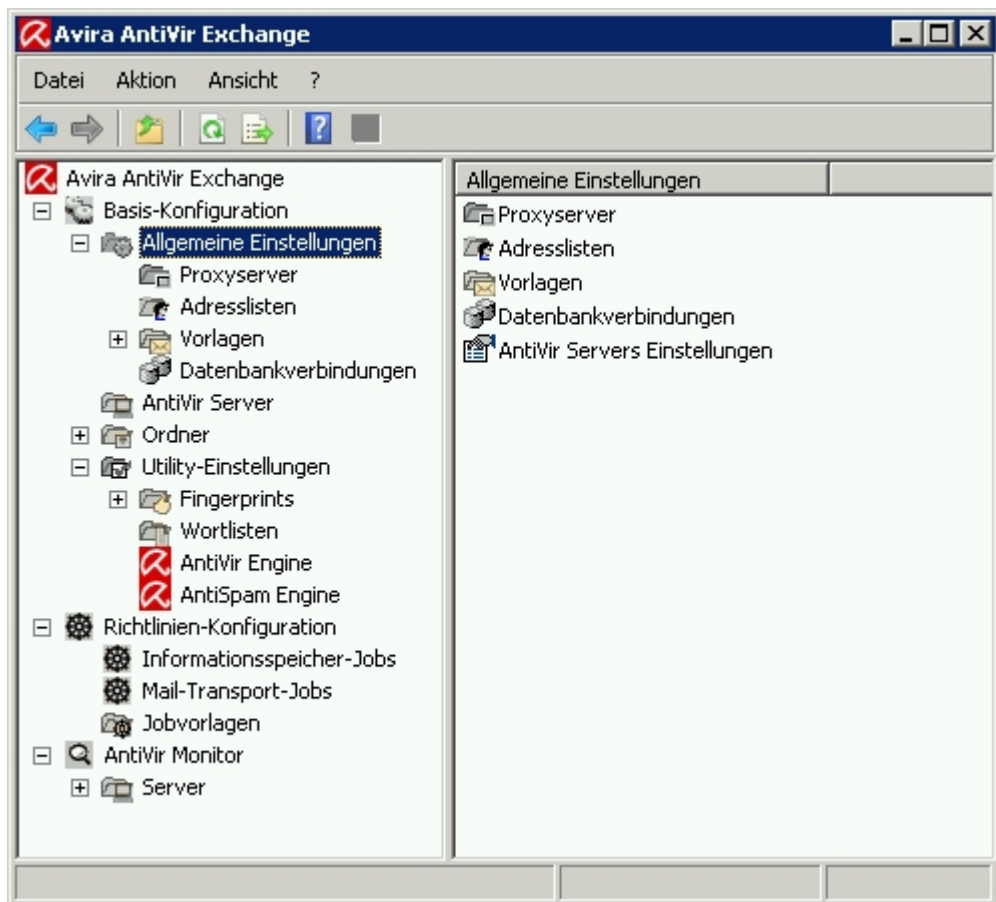
Die Konfigurationsinformationen werden sowohl vom Avira AntiVir Exchange Server als auch von der Avira AntiVir Exchange Konsole benötigt. Der Avira AntiVir Exchange Server erhält daraus z. B. die Daten über die auszuführenden Avira AntiVir Exchange Jobs. Um mit der Avira AntiVir Exchange Konsole Veränderungen in der Konfiguration vornehmen zu können, benötigt auch diese Zugriff auf die *ConfigData.xml*. Die Avira AntiVir Exchange Konfiguration kann sowohl in einem lokalen Verzeichnis als auch auf einem Netzwerkshare gespeichert werden. Welche Avira AntiVir Exchange Konfiguration die Avira AntiVir Exchange Konsole bzw. der Avira AntiVir Exchange Server verwendet, wird durch einen Eintrag in der Registry festgelegt. Der Pfad zur Avira AntiVir Exchange Konfiguration kann im Format `C:\.....` oder als UNC Pfad `\\Servername\Share\ConfigData.xml` angegeben werden. Falls die angegebene Avira AntiVir Exchange Konfiguration nicht verfügbar ist, verwendet Avira AntiVir Exchange die so genannte "Last-Known-Good"-Konfiguration. Dies wird in der Windows Ereignisanzeige protokolliert.

Die "Last-Known-Good"-Konfiguration ist pro Server lokal gespeichert und wird immer dann aktualisiert, wenn Veränderungen an der Avira AntiVir Exchange Konfiguration vorgenommen wurden und der Zugriff von der Avira AntiVir Exchange Konfiguration auf die "Last-Known-Good"-Konfiguration möglich ist.

**Hinweis:** Um eine vom Standard abweichende Konfiguration mit der Konsole öffnen zu können, steht ein Parameter zur Verfügung. Starten Sie die Avira.msc Datei mit dem Parameter `config` und der gewünschten Konfigurationsdatei, beispielsweise so:  
`"C:\Programme\Avira\AntiVir Exchange\Avira.msc" config`  
`"C:\AndererOrdner\Directory\ConfigData.xml"`  
Sie können auch hier einen UNC-Pfad angeben.





## 4 Details zur Avira AntiVir Exchange Management Konsole

1. Öffnen Sie AntiVir Exchange Management Konsole.
2. Wählen Sie in der linken Spalte die **Basis-Konfiguration, Richtlinien-Konfiguration** oder **AntiVir Monitor**.  
Im rechten Fenster erscheinen die entsprechenden Unterordner.















3. Klicken Sie für den Aufruf der **Online-Hilfe** oben in der Symbolleiste auf , oder im Menü Vorgang auf **Hilfdatei anzeigen**.

### 4.1 Die Symbolleiste

	Zurück
	Vorwärts
	Eine Ebene höher
	Eigenschaften des ausgewählten Objekts

	Ansicht aktualisieren
	Exportliste
	Hilfe
	Speichern
	Position/Rangfolge um eins hochsetzen
	Position/Rangfolge um eins runtersetzen
	Job aktivieren
	Job deaktivieren
	Neues Objekt
	Filter in Quarantäne/Badmail setzen

## 4.2 Bedeutung der Icons

	Avira AntiVir Exchange Konsole Einstieg und Logo.
	<b>Basis-Konfiguration</b> für die allgemeinen Einstellungen aller Module.
	Knoten für <b>Allgemeine Einstellungen</b>
	Der Ordner für die <b>Adresslisten</b>
	Eine einzelne <b>Avira AntiVir Exchange Adressliste</b> (Kragen rot), die mit der Avira AntiVir Exchange ausgeliefert wird und nicht geändert werden kann.
	Eine einzelne <b>eigene Adressliste</b> (Kragen gelb), selbst anlegbar und unter <b>Eigenschaften</b> konfigurierbar
	Der Ordner für <b>Benachrichtigungsvorlagen</b> , der die einzelnen Vorlagen für jeden Jobtyp und Empfänger enthält.
	Eine <b>einzelne Benachrichtigungsvorlagen</b> , unter <b>Eigenschaften</b> konfigurierbar
	Der Ordner für die einzelnen <b>Datenbankverbindungen</b> .
	Das Symbol für eine einzelne <b>Datenbankverbindung</b> , unter <b>Eigenschaften</b> konfigurierbar.
	Eine Liste aller Avira AntiVir Exchange Server. Es lassen sich Server hinzufügen, entfernen und konfigurieren. Die gemeinsamen Eigenschaften aller Server werden unter <b>Allgemeine Einstellungen - AntiVir Servers-Einstellungen</b> konfiguriert, alternativ mit der rechten Maustaste auf <b>AntiVir Server - Eigenschaften</b> . Dazu gehören die Standard-Email-Adressen und die interne(n) Domäne(n).
	Allgemeine <b>AntiVir Server-Einstellungen</b> unter dem Knoten <b>Allgemeine Einstellungen</b> im rechten Fenster.

	Ein einzelner Server, unter <b>Eigenschaften</b> konfigurierbar.
	<b>Ordner-Einstellungen</b> und <b>Utility-Einstellungen</b> . Unter Ordner-Einstellungen finden Sie die <b>Quarantänen</b> , unter Utility-Einstellungen befinden sich alle zu konfigurierenden Zusätze wie Virens Scanner, Fingerprints, Wortlisten.
	Die Quarantäne-Ordner-Struktur. Darunter befinden sich alle Quarantäne-Ordner.
	Ein einzelner Quarantäne-Ordner, unter <b>Eigenschaften</b> konfigurierbar.
	Der Ordner für Fingerprint-Gruppen.
	Eine logisch zusammengehörende Fingerprint-Gruppe.
	Ein einzelner Fingerprint, unter Eigenschaften konfigurierbar.
	Der Ordner für die Wortlisten, mit denen die Inhaltsprüfung durchgeführt wird.
	Eine einzelne Wortliste, unter Eigenschaften konfigurierbar.
	Der AntiVir Virens Scanner, unter Eigenschaften konfigurierbar.
	Richtlinien-Konfiguration für die Konfiguration von individuellen Jobs nach den eigenen Firmenrichtlinien.
	Ordner für Jobbeispiele, der die Jobs für die einzelnen Jobtypen enthält.
	Ein AntiVir-Job oder AntiVir Wall-Job, von dem es verschiedene Jobtypen gibt, unter Eigenschaften konfigurierbar.
<input checked="" type="checkbox"/>	Ein aktiver Job, unter Eigenschaften konfigurierbar.
<input type="checkbox"/>	Ein inaktiver Job, unter Eigenschaften konfigurierbar.
	Der AntiVir Monitor zur Einsicht in alle Quarantäne-Ordner auf jedem verfügbaren Server. Die Quarantäne-Ordner enthalten die Kopien der Original-E-mails inklusive der Anhänge.
	Die Quarantäne-Ordner mit Originalmails zur Einsicht. Für jede Email können detaillierte Informationen abgerufen werden.
	Ein einzelnes Quarantäneobjekt.
	Ungültiges Quarantäneobjekt.
	Erneut gesendetes Quarantäneobjekt.
	Information Store Quarantäneobjekt.
	Uhrzeit und Wochentag einer Quarantänewartung
	Ordner für verschiedene, mit der Avira AntiVir Exchange ausgelieferte AntiVir Reports.
	Einzelner AntiVir-Report.

Die Ansicht der Avira AntiVir Exchange Konsole besteht aus drei Bereichen:

- [Basis-Konfiguration](#)
- [Richtlinien-Konfiguration](#)
- [AntiVir Exchange Monitor](#)

### 4.3 Basis-Konfiguration

In der Basis-Konfiguration nehmen Sie allgemeine Einstellungen und die wesentlichen Grundeinstellungen für die Module vor.

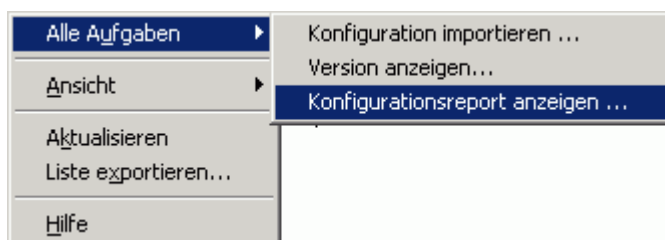
In der Basis-Konfiguration verwalten Sie:

- Allgemeine Einstellungen wie:
  - Proxyserver
  - Adresslisten
  - die Benachrichtigungsvorlagen (Vorlagen)
  - Datenbankverbindungen
  - AntiVir Server
- alle Ordner (z.B. die Quarantänen)
- und die Utilities:
  - Wortlisten für die Inhaltsprüfung
  - Fingerprints für das Blocken von Anhängen
  - AntiVir Engine
  - AntiSpam Engine

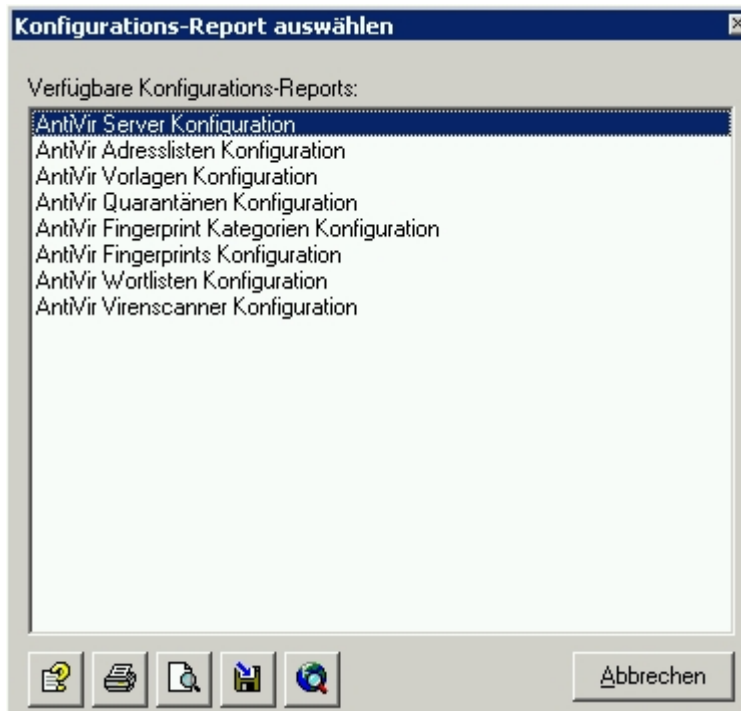
#### 4.3.1 Überblick durch Konfigurationsreports




Ein Konfigurationsreport gibt einen Überblick über die aktuelle Konfiguration:

1. Klicken Sie mit der rechten Maustaste auf *Basis-Konfiguration* und wählen Sie *Alle Aufgaben - Konfigurationsreport anzeigen*.



2. Klicken Sie auf den gewünschten Report:



3. Klicken Sie auf *Report anzeigen*:  Jetzt wird der Report als HTML-Datei im Browser geöffnet.
4. Mit der *Report-Vorschau*  erhalten Sie eine Druckvorschau.
5. Mit *Report sichern*  speichern Sie den ausgewählten Report als HTML-Datei.

### 4.3.2 Konfiguration importieren

**Warnung:** Bevor Sie eine Änderung eines Objektes der Basis-Konfiguration durchführen, empfiehlt es sich, eine Kopie des alten gleichnamigen Objekts zu erstellen und umzubenennen. Die neue Version ersetzt die alte, so dass anschließend Ihre eigenen Änderungen des Objektes verloren sind!

Wenn eine geänderte Version verfügbar ist:

1. Wählen Sie **Basis-Konfiguration - Alle Aufgaben - Konfiguration importieren**, um alle Elemente/Objekte wie z.B. Wortlisten oder Fingerprints neu einzuspielen.
2. Wählen Sie dazu die entsprechende XML-Datei, die Avira zur Verfügung stellt.

**Warnung:** Diese Funktion importiert nicht die vollständige Konfiguration (ConfigData.xml) inklusive der Jobs, sondern nur einzelne Basis-Objekte!

### 4.3.3 AntiVir Server-Einstellungen

Unter AntiVir Server-Einstellungen konfigurieren Sie die Standardeinstellungen für alle Avira AntiVir Exchange Server. Jeder Server kann zusätzlich individuell konfiguriert werden. Näheres unter [Einstellungen für einen einzelnen AntiVir Server](#).

1. Wählen Sie *Basis-Konfiguration - Allgemeine Einstellungen*
2. Öffnen Sie *Eigenschaften*:

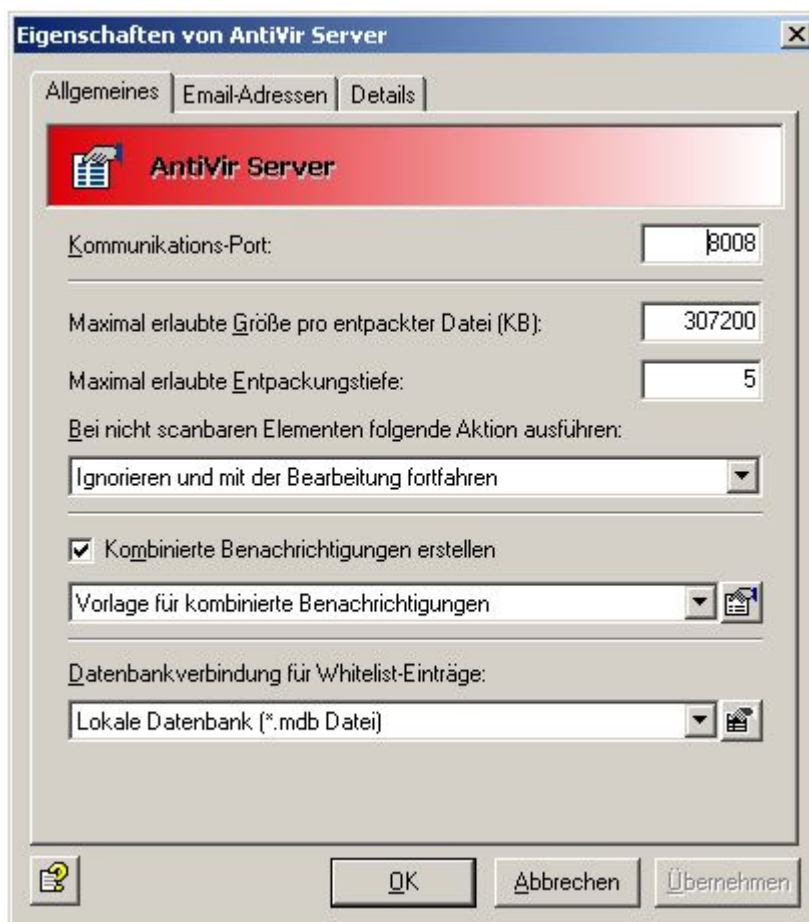
1. Klicken Sie im rechten Fensterbereich auf *AntiVir Server Einstellungen* und wählen Sie mit der rechten Maustaste *Eigenschaften*.
2. Oder öffnen Sie die Eigenschaften per Doppelklick auf *AntiVir Server Einstellungen*.
3. Alternativ können Sie im linken Fensterbereich unter *Basis-Konfiguration* mit einem rechten Mausklick auf *AntiVir Server* die Eigenschaften aufrufen.

## Gepackte Dateien und AntiVir Monitor

Die Einstellungen auf der Registerkarte *Allgemeines* legen die maximal erlaubte Größe entpackter Dateien auf der Festplatte und die maximal erlaubte Entpackungstiefe bei Archiven fest. Emails, die diese Werte überschreiten, werden in den *Bad-Mail*-Bereich überführt.

**Warnung:** Achten Sie auf die korrekte Einstellung Ihres Kommunikationsports für den AntiVir Monitor. Die Kommunikation mit den Servern ist sonst nicht möglich.

Als Standardwert wird bei der Installation der Port 8008 eingetragen. Die hier eingetragenen Werte gelten für alle Server.



Lesen Sie in diesem Zusammenhang auch die Beschreibung zur Rechtevergabe und Sicherheitseinstellungen unter [AntiVir Monitor](#).

## Aktionen bei nicht scanbaren Elementen

Für Elemente, die nicht scanbar sind, z.B. Emails mit einem verschlüsselten Anhang, kann eine serverübergreifende Aktion festgelegt werden. Diese wird automatisch ausgeführt, sobald das Programm ein Element als nicht scanbar erkennt.



Im Dropdown-Menü stehen zwei Aktionen zur Auswahl. Entweder kann die Tatsache, dass das Element nicht scanbar ist, ignoriert und das Element direkt dem nächsten vorgesehenen Job übergeben werden oder es wird automatisch in die Bad-Mails Quarantäne verschoben.

### Kombinierte Benachrichtigung

Jeder Job kann generell so konfiguriert werden, dass beim Eintreten eines bestimmten Ereignisses die Empfänger, Absender und/oder die Administratoren über dieses Ereignis benachrichtigt werden (Registerkarte *Aktionen* in Job-Eigenschaften).

Treten für eine bearbeitete Email mehrere solche Ereignisse ein, sind die Avira AntiVir Exchange-Email standardmäßig so eingestellt, dass sie nicht für jedes Ereignis eine separate Benachrichtigung versenden, sondern alle Benachrichtigungen als eine Kombinierte Benachrichtigung verschicken. Die Empfänger dieser Kombinierten Benachrichtigung erhalten also nur eine Email, die alle eingetroffenen Ereignisse gelistet anführt.

Die Empfänger dieser *Kombinierten Benachrichtigung* erhalten also nur eine Email, die alle eingetroffenen Ereignisse gelistet anführt. Als Vorlage wird dazu *Kombinierte Benachrichtigungen* verwendet. Sie können diese Vorlage modifizieren oder neue Vorlagen anlegen (über *Basis-Konfiguration - Allgemeine Einstellungen - Vorlagen - Kombinierte Benachrichtigungen*).

**Hinweis:** Falls Sie den Versand von Kombinierten Benachrichtigungen unterdrücken und stattdessen über jedes eingetretene Ereignis eine Email-Benachrichtigung versenden möchten, deaktivieren Sie unter *Allgemeine Einstellungen - AntiVir Servers Einstellungen - Registerkarte Allgemeines* das Feld *Kombinierte Benachrichtigungen erstellen*.

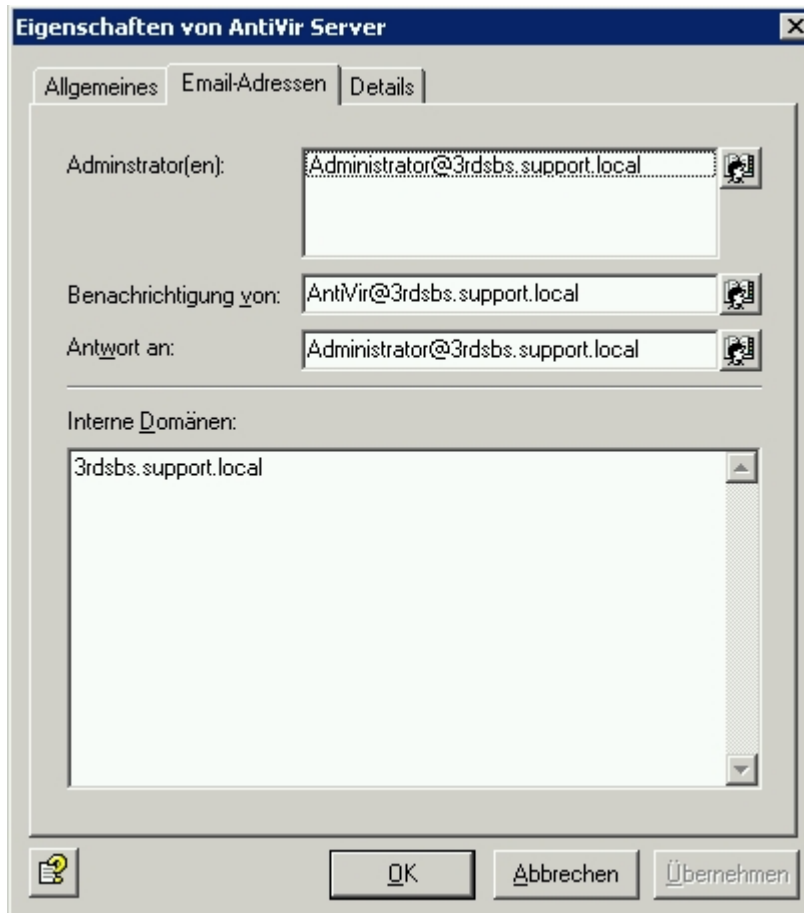
### Zentrale Whitelists

In Multi-Email-Umgebungen erzeugt jeder beteiligte Server seine eigenen Benutzer Whitelists. Ohne Email-Synchronisation erhält folglich jeder Benutzer für jeden der Server eine separate Whitelist, die einzeln gepflegt werden müssen. Um diese Whitelists zentral zu verwalten und damit die Administration zu vereinfachen, können Sie anstelle der regulären lokalen Datenbank auf Basis der Microsoft Jet-Engine auch eine Microsoft SQL-Server einrichten, die die Daten für alle beteiligten Avira AntiVir Exchange Server in eine zentrale SQL-Datenbank schreibt.

Um zentrale Benutzer Whitelists anzulegen, muss zunächst eine Datenbankverbindung zwischen dem SQL-Server und dem Avira AntiVir Exchange Server konfiguriert werden (*Basis-Konfiguration - Datenbankverbindungen*). Sobald diese Verbindung besteht, wählen Sie hier im Feld *Datenbankverbindung für Whitelist-Einträge* die entsprechende Konfiguration aus.

### Definition der Email-Adressen und internen Domänen

Die Avira AntiVir Exchange benötigt einige Basiseinstellungen zur Maildomäne der zu bearbeitenden Emails. Während der Installation wird die Email-Adresse des angegebenen Avira AntiVir Exchange Administrators verwendet, um folgende Basis-Einstellungen der Avira AntiVir Exchange einzutragen:



- *Adminstrator(en)*: Die hier eingetragenen Avira AntiVir Exchange Administratoradressen erhalten wichtige Status-Benachrichtigungen der Avira AntiVir Exchange Installation sowie die konfigurierten Administrator-Benachrichtigungen. Als Standardwert trägt die Installation die abgefragte Administratoradresse ein.
- *Benachrichtigung von*: Der in den Avira AntiVir Exchange Benachrichtigungen angezeigte Absender. Als Standardwert trägt die Installation Avira AntiVir Exchange mit der Maildomäne der abgefragten Administrator-Adresse ein.
- *Antwort an*: Der in den Avira AntiVir Exchange Benachrichtigungen hinterlegte Empfänger von Antworten auf diese Benachrichtigungen. Als Standardwert trägt die Installation die abgefragte Administratoradresse ein.

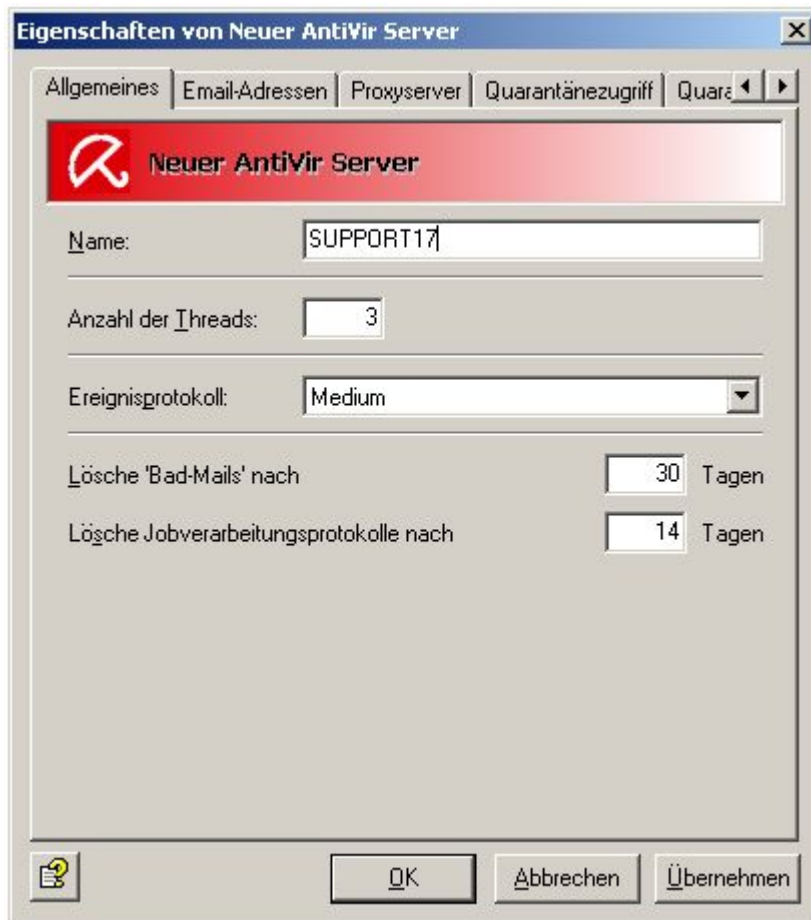
- *Interne Domänen:* Die hier angegebenen Maildomänen werden als interne Maildomänen angesehen, alle übrigen als externe Maildomänen. Diese Einstellung wird verwendet, um im Regelwerk der Avira AntiVir Exchange anhand der Absender- und Empfängeradressen einer Email zu unterscheiden, ob es sich um eine eingehende oder eine ausgehende Email handelt. Ein Spamfilter-Job wird z.B. nur eingehende Emails bearbeiten, während AntiVir an eingehende Emails nicht angehängt werden soll. Mehrere Domänen werden mit Return getrennt. Subdomänen werden automatisch eingebunden, wenn vor die Hauptdomäne als Wildcard der Präfix "\*" gestellt wird, z.B. \*.domain.com. Als Standardwert trägt die Installation die Maildomäne der abgefragten Administratoradresse ein.

Diese Einträge gelten für alle Avira AntiVir Exchange Server. Die Einstellungen können an dieser Stelle jederzeit geändert werden.

### 4.3.4 Einstellungen für einen einzelnen Avira AntiVir Exchange Server

Wählen Sie **Basis-Konfiguration**, klicken Sie im linken Fenster auf AntiVir Server und wählen Sie den gewünschten Server im rechten Fenster mit einem Doppelklick aus. Einen neuen Server erstellen Sie mit der rechten Maustaste auf **AntiVir Server - Neu - AntiVir Server**. Klicken Sie mit der rechten Maustaste auf **Eigenschaften** und konfigurieren sie die Einstellungen des neuen Servers.

## Allgemeine Servereinstellungen



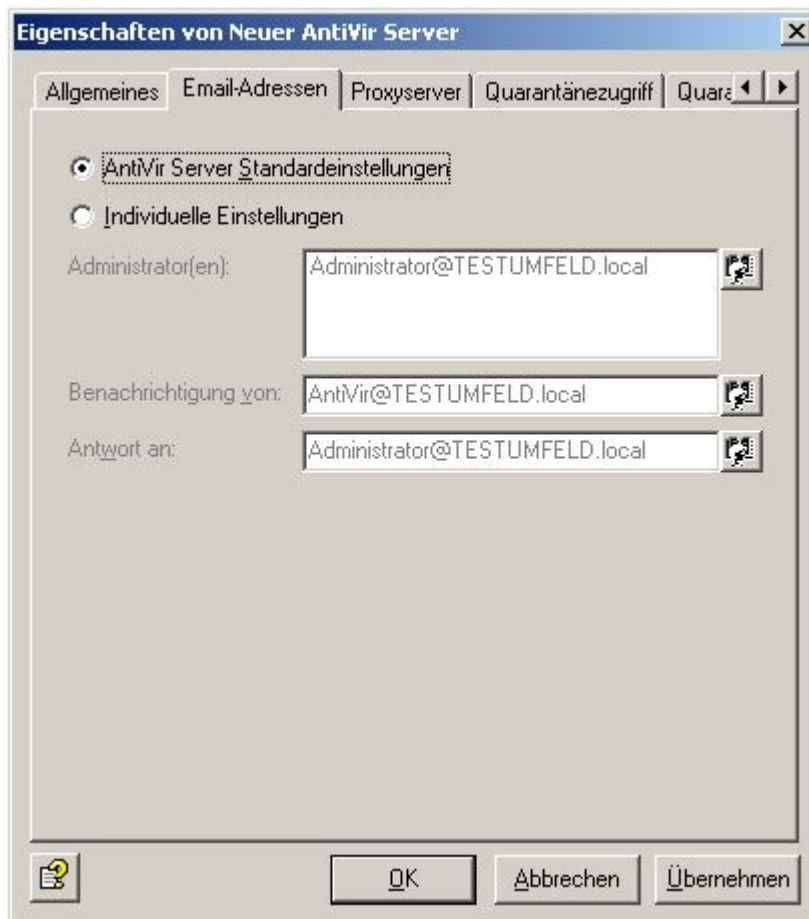
1. Tragen Sie den **Namen** des Exchange-Servers ein.  
Während der Installation wird der aktuelle Exchange-Servername automatisch eingetragen.
2. Bestimmen Sie die maximale Anzahl der gleichzeitig bearbeiteten Emails im Feld **Anzahl der Threads**.  
Wie viele Emails sinnvollerweise parallel durch die AntiVir bearbeitet werden können, hängt von der Ausstattung und Performance Ihres Servers ab.
3. Wählen Sie die **Protokollstufe für das Ereignisprotokoll**, welches Sie mit dem Event Viewer/ Ereignisanzeige einsehen können (Windows Event Log).  
Die Abstufungen reichen von **Kein** bis **Maximum**.
4. Bestimmen Sie die Anzahl der Tage, die die Emails in der Badmail-Quarantäne verbleiben sollen.  
Nach Ablauf dieser Tage werden die Emails automatisch gelöscht.
5. Legen Sie die Anzahl der Tage fest, nach denen ein Jobverarbeitungsprotokoll im Ordner Log gelöscht werden soll.

**Hinweis:** Um auf einen neu angelegten Server im AntiVir Monitor sofort zugreifen zu können, aktualisieren Sie die Ansicht im AntiVir Monitor (Rechte Maustaste auf AntiVir Monitor - Aktualisieren, oder über den Icon in der Symbolleiste).

### Individuelle Email-Adressen für einen AntiVir Server

Für jeden einzelnen Server werden die Einstellungen aus den Eigenschaften aller AntiVir Servers übernommen, die während der Installation automatisch gesetzt werden oder von Ihnen individuell eingetragen worden sind. Diese Einstellungen gelten als **AntiVir Server Standardeinstellungen**.

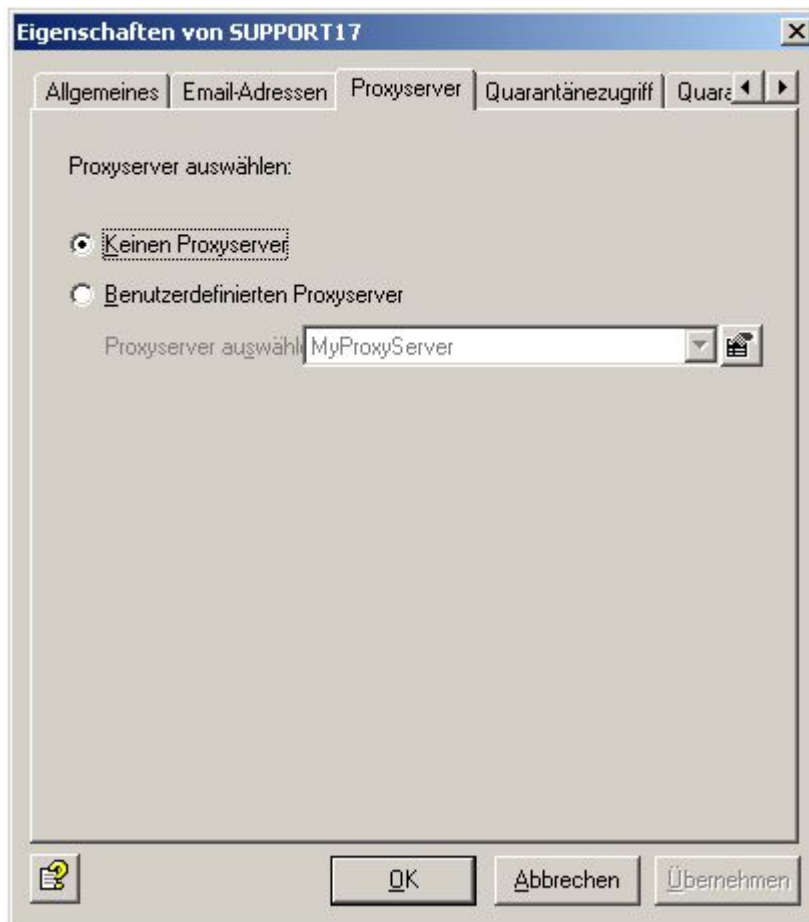
Sollten Sie für einen Server individuelle Einstellungen benötigen, aktivieren Sie die Option **Individuelle Einstellungen** und tragen Sie die Adressen in die entsprechenden Felder ein.



### Proxyserver verwenden

Wenn in Ihrer Netzwerkumgebung für Internetverbindungen ein Proxyserver erforderlich ist, können Sie für jeden AntiVir Server den passenden Proxyserver auswählen. Beispielsweise für den Download von Updates aus dem Internet.

Klicken Sie auf die Registerkarte **Proxyserver**:



Wenn Sie Ihren AntiVir Server mit einem Proxyserver verbinden möchten, wählen Sie Ihren benutzerdefinierten Proxyserver aus der Liste.

### Proxyserver-Einstellungen

Wenn Sie bereits im Verlauf der Avira AntiVir Exchange-Installation die Verbindungsdaten zum Proxyserver angegeben haben, werden Ihnen diese Proxyserver-Einstellungen bei **Basis-Konfiguration - Allgemeine Einstellungen - Proxyserver** angezeigt.

Anderenfalls geben Sie die Proxyserver-Einstellungen dort ein:

- **Name/IP-Adresse:** Vollständiger Name oder IP-Adresse des Proxyservers.  
Beispiel 1: proxy.mydomain.de  
Beispiel 2: 127.0.0.1
- **Port:** Portnummer des Proxyservers. Der angegebene Port wird für die Kommunikation mit dem Proxyserver verwendet.  
Beispiel: 8000
- **Benutzer und Passwort** (optional): Authentifizierungsdaten, unter dem sich der Updatedienst am Proxyserver anmeldet.  
Beispiel: proxy\_benutzer

Einen Proxyserver löschen Sie, indem Sie mit der Maus einen Rechtsklick ausführen und **Löschen** wählen. Beachten Sie, dass Sie keinen Proxyserver löschen können, der bereits von einem Objekt verwendet wird.

Wenn die Aktionen des Virenschanners und der AntiSpam Engine über einen Proxyserver ausgeführt werden sollen, nehmen Sie jeweils in der Registerkarte **Proxyserver** die entsprechenden Einstellungen vor.

### Benutzerspezifischer Zugriff auf die Quarantäne

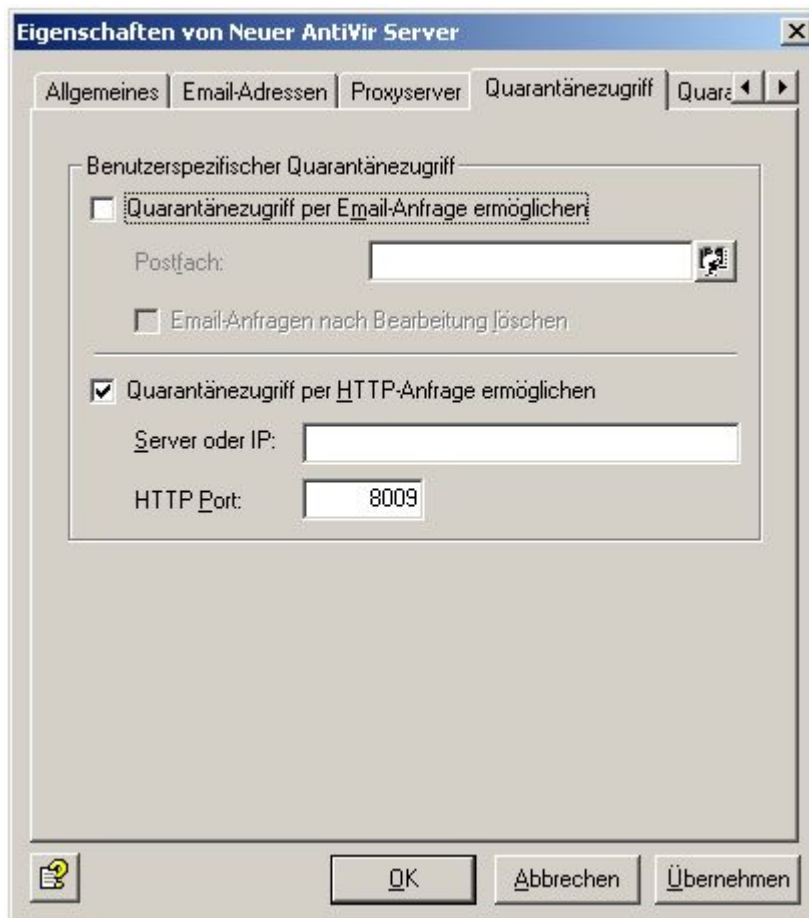
Mit der Avira AntiVir Exchange kann der Anwender selbst auf seine Quarantäne-E-mails zugreifen.

Welche Emails das sein sollen und welche Benutzer zugreifen dürfen, kann individuell für jede Quarantäne konfiguriert werden. Besonders interessant ist diese Funktion bei der Spam-Prüfung, also für die Spam-Quarantänen. Zusätzlich wird der Administrator entlastet, da sich die Benutzer die einzelnen Quarantäne-E-Mails selbst zustellen können.

Sie können für jeden Server definieren, ob und auf welche Art ein Anwender auf seine Quarantäne-E-mails zugreifen darf. Der Anwender wird durch eine Quarantäne-Sammelbenachrichtigung über die Quarantäne-E-mails informiert, klickt auf die entsprechende Aktion für die gewünschte Email und stellt damit eine Anfrage.

Diese Aktionen werden für jede Quarantäne einzeln konfiguriert und können **Anfordern** (Zustellung an Empfänger der Sammelbenachrichtigung), **Freigeben** (Zustellung an alle Empfänger) und/oder **Entfernen** (Email in der Quarantäne zum Löschen vormerken) sein. Der Zugriff durch den Anwender erfolgt über eine Email-Anfrage oder über eine HTTP-Anfrage.

Klicken Sie auf die Registerkarte Quarantänezugriff:



**Quarantänezugriff per Mail-Anfrage ermöglichen:** Die Anfrage an die Quarantäne(n) wird über eine Email-Anfrage gestartet. Wenn der Anwender in seiner Quarantäne-Sammelbenachrichtigung auf den Aktionslink für die gewünschte Email klickt, wird die Emailanfrage automatisch erzeugt und an die Email-Adresse gesendet, die Sie auf dieser Registerkarte im Feld **Postfach** definieren.

Voraussetzung ist, dass die hier angegebene Email-Adresse existiert und dass die Email über den Server gesendet wird, auf dem Avira AntiVir Exchange (und die entsprechenden Quarantäne(n)!) installiert ist.

Wir empfehlen, das Postfach auf dem jeweiligen Server anzulegen. Der Inhalt der Email wird ausgelesen und dadurch die vom Anwender gewünschte Aktion durchgeführt. Die AntiVir erkennt Anfrage-Emails der Anwender durch:

1. die Email-Adresse (Angabe im Feld **Postfach**)
2. das Schlüsselwort für eine Benutzeranfrage in der Email (User Request)

Letztlich wird die Anforderungsmail im angegebenen Postfach abgelegt.

Setzen Sie den Haken bei der Option **Email-Anfragen nach Bearbeitung löschen**, wenn die Anfrage-Emails nach Abarbeitung aus dem angegebenen Postfach gelöscht werden sollen.

**Quarantänezugriff per HTTP-Anfrage ermöglichen:** Die Anfrage an die Quarantäne wird über HTTP gestartet. Sobald der Benutzer auf die gewünschte Aktion geklickt hat, öffnet sich der Standardbrowser. Der Benutzer erhält eine Meldung, dass seine Anfrage bearbeitet wird. Voraussetzung für diese Anfrage ist ein freier Port. Der Standardeintrag ist der Port 8009.

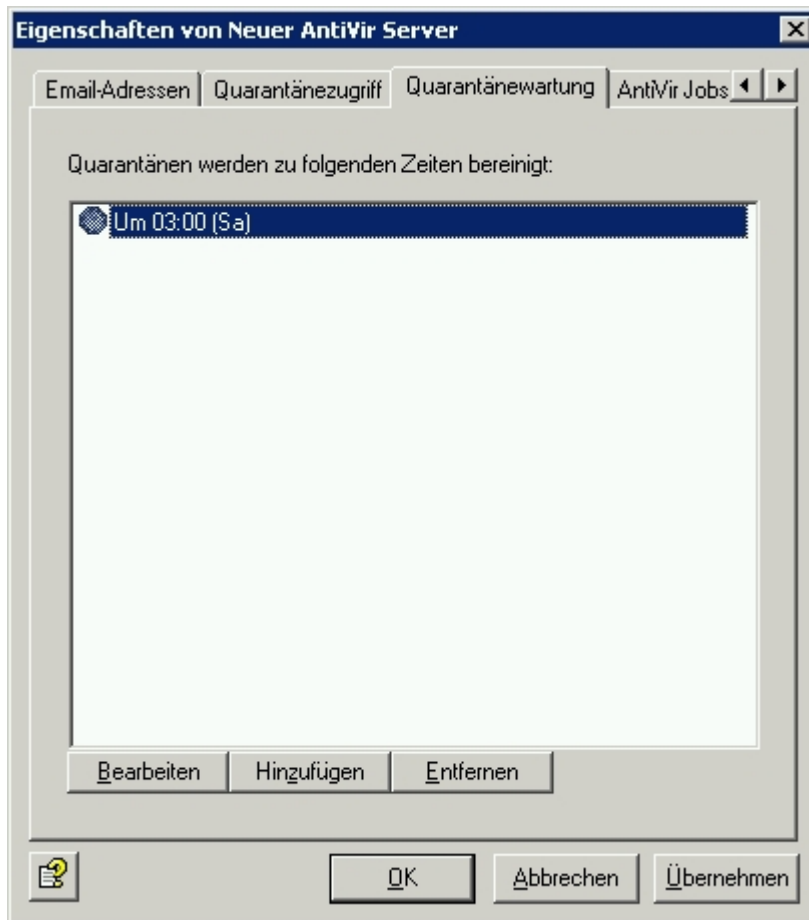
**Warnung:** Die Rückmeldung für den Anwender, die durch den Browser angezeigt wird, ist immer gleichlautend (*OK\_Response.html* im Verzeichnis *AntiVir\App-Data*). Sollte die angeforderte Email also nicht mehr existieren, da sie beispielsweise in der Quarantäne bereits gelöscht wurde, so erhält der Benutzer darüber keinerlei Benachrichtigung.

### Quarantänewartung

Legen Sie in dieser Registerkarte den Zeitpunkt fest, zu dem die Quarantänen des Servers bereinigt werden sollen. Durch die Bereinigung werden alle zum Löschen markierten Emails in allen Quarantänen physisch gelöscht und der entsprechende Platz wieder freigegeben.

Die Standardeinstellung für die Bereinigung ist jeden Samstag um 3 Uhr nachts. Falls Sie den Zeitpunkt oder die Häufigkeit der Bereinigung ändern möchten, klicken Sie auf **Bearbeiten** und legen Sie die gewünschten Zeiten fest.





**Hinweis:** Sie können eine Quarantäne bei Bedarf auch manuell bereinigen, indem Sie auf der entsprechenden Quarantäne im AntiVir Monitor mit der rechten Maustaste den Befehl **Alle Aufgaben - Quarantäne bereinigen** wählen.

### Liste aller Jobs ansehen


In der Registerkarte **AntiVir Jobs** erhalten Sie eine Liste aller Jobs, die auf diesem Server definiert sind.

Wenn Sie einen Job auf dem Server bearbeiten wollen, rufen Sie dazu direkt die Job-Eigenschaften auf.


### 4.3.5 Adresslisten

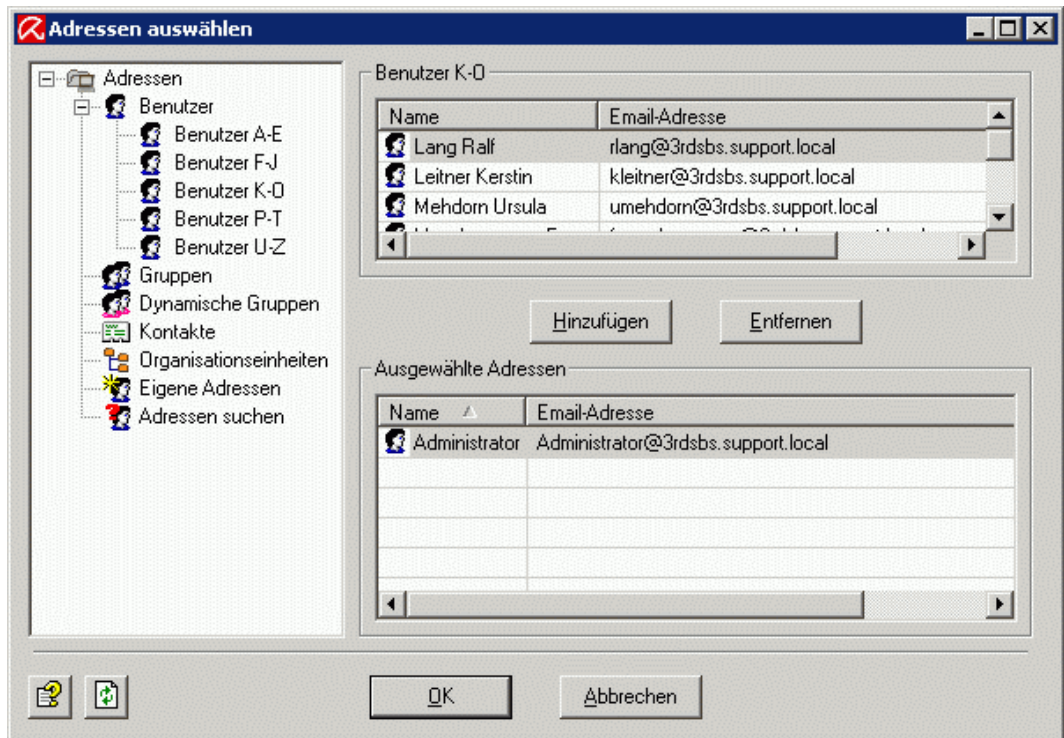
In der **Basis-Konfiguration - Allgemeine Einstellungen** unter **Adresslisten** können Sie eigene Adresslisten anlegen, die Sie im Job auswählen. Die zur Verfügung stehenden Adressen werden aus dem Active Directory entnommen.

#### Adresslisten anlegen, bearbeiten und löschen

1. Öffnen Sie **Basis-Konfiguration - Allgemeine Einstellungen**
2. Klicken Sie mit der rechten Maustaste auf **Adresslisten** und wählen Sie den Eintrag **Neu - Adressliste**.
3. Geben Sie der Adressliste einen sprechenden Namen.
4. Klicken Sie auf das Symbol für **Adressen auswählen:** .

5. Im folgenden Fenster wählen Sie aus den einzelnen Rubriken die gewünschten Adressen mit **Hinzufügen** aus.

Eigene Adressen können Sie in das Eingabefeld eintragen und ebenfalls zur Adressliste hinzufügen. Dabei sind die Wildcards \* (Stern) und ? (Fragezeichen) möglich. Es ist ebenfalls möglich, formal ungültige Email-Adressen wie z.B. info@domain einzugeben. Trennen Sie die einzelnen Einträge durch einen Absatz (Enter-Taste). Sollten Sie eine umfangreiche Liste von eigenen Adressen angelegt haben, so können Sie nach dort enthaltenem Text suchen, indem Sie auf das Symbol klicken: . Die Textsuche steht Ihnen auch in den Wortlisten zur Verfügung. Um einen Eintrag wieder aus der Liste zu löschen, markieren Sie diesen und klicken Sie auf **Entfernen**.



6. Klicken Sie **OK**.  
Ihre Adressliste müsste nun etwa so aussehen:



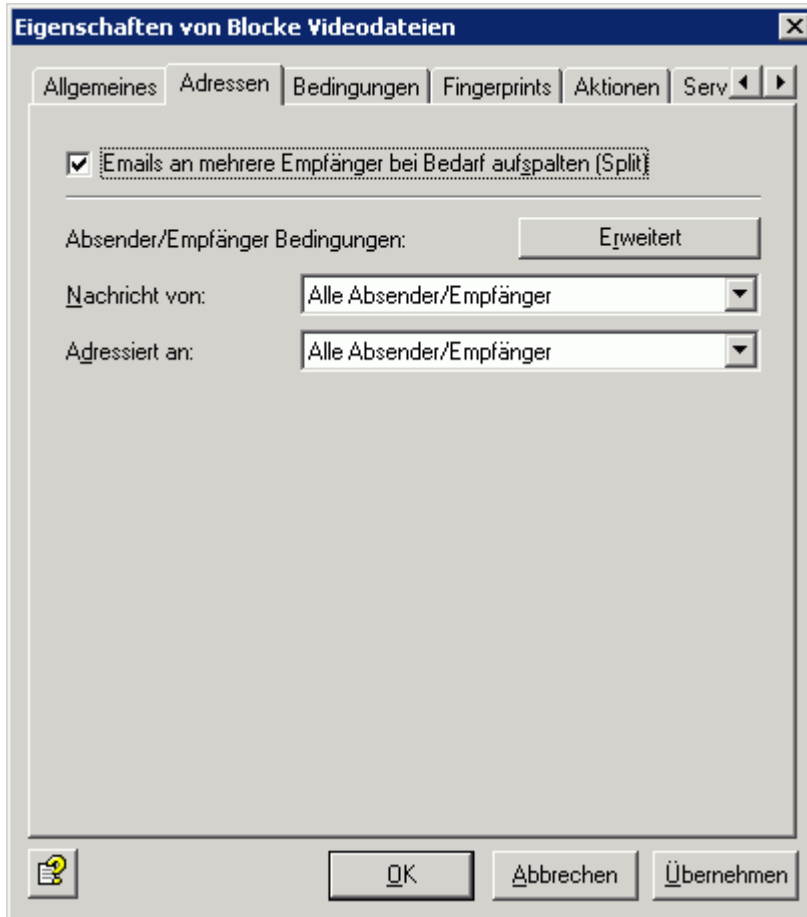
7. **Adressen dürfen aus Quarantäne hinzugefügt werden:**

Legen Sie hier fest, ob für diese Adressliste der direkte Zugriff aus einer Quarantäne-Email heraus freigegeben ist. Wenn Sie sich im [AntiVir Monitor](#) in einer Quarantäne eine Email ansehen, können Sie durch die Schaltfläche **Hinzufügen** die Absenderadresse der Quarantäne-Email zu verschiedenen Adresslisten hinzufügen. Im Auslieferungsstandard sind folgende Adresslisten für den direkten Zugriff freigegeben:

  - Anti-Spam: Blacklist
  - Anti-Spam: Newsletter Blacklist
  - Anti-Spam: Newsletter Whitelist
  - Anti-Spam: Whitelist
8. Klicken Sie noch einmal **OK**.
9. Zum Löschen markieren Sie die Adressliste mit der rechten Maustaste und wählen Sie Löschen aus dem Kontextmenü.

### Einsatz und Handhabung in einem Job

In jedem Job können Sie unter der Registerkarte Adressen bestimmen, für welche Benutzer ein Job gültig ist. Die gängigsten Anwendungsfälle können Sie mit der zunächst sichtbaren Registerkarte einstellen:



Wählen Sie hier aus, ob der Job für alle Benutzer gültig ist oder auf interne bzw. externe Benutzer beschränkt sein soll. Diese Auswahl können Sie für die Absender und für die Empfänger treffen.

**Hinweis:** Beide Bedingungen in den Feldern **Nachricht von** und **Adressiert an** müssen zutreffen, damit eine Aktion ausgelöst wird (UND-Verknüpfung).

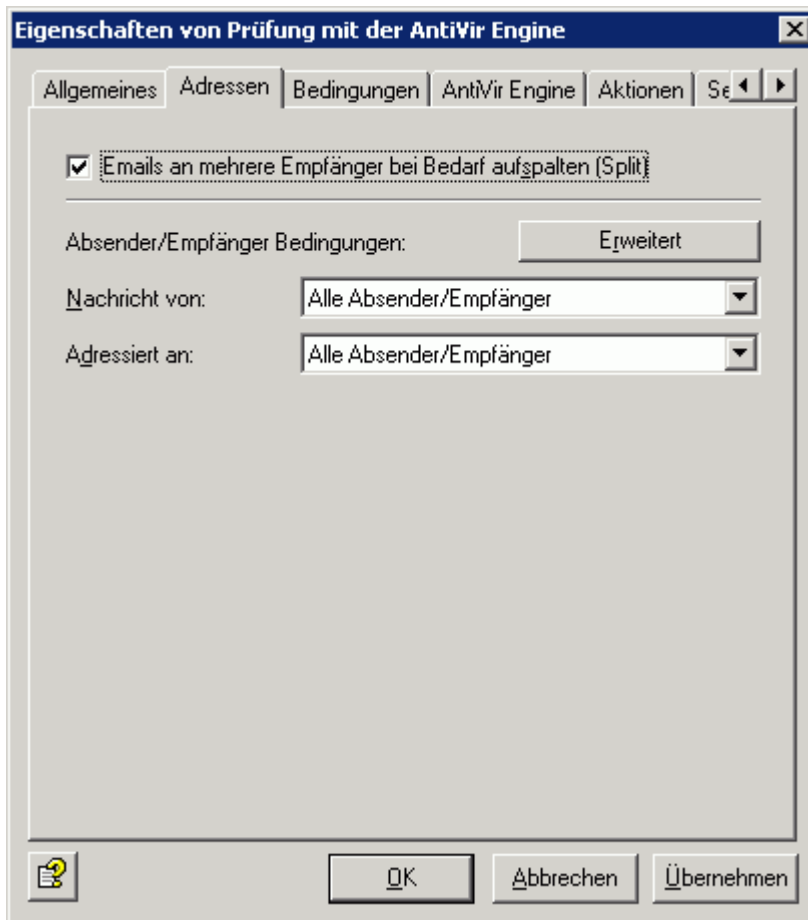
**Emails an mehrere Empfänger bei Bedarf aufspalten (Split):** Wenn eine Email an mehrere Empfänger adressiert ist, und einer oder mehrere davon in einem Job in der Adressprüfung eingetragen sind, wird diese eine Email in zwei Emails aufgesplittet: eine Email für die definierten Empfänger der Adressprüfung und eine für die nicht definierten Empfänger. Der Job behandelt dann nur die Email mit den Empfängern, die definiert sind. Es wird nicht gesplittet, wenn Sie keine Adressprüfung für Empfänger definiert haben! Das Splitten der Emails hat Auswirkungen auf die Performance Ihres Servers.

## Viren prüfen

Unternehmensrichtlinie: Es sollen alle Emails auf Viren geprüft werden. In diesem Fall kann es nicht genügen, die Emails nur von externen Absendern zu prüfen. Es muss auch sichergestellt werden, dass keine infizierte Email das Unternehmen verlässt. Die definierten Aktionen (Prüfen auf Viren, ggf. Reinigen der Datei und Kopieren in die Quarantäne) müssen also unabhängig von Absender oder Empfänger durchgeführt werden.

Umsetzung: Aktion wird ausgeführt bei **Nachricht von:** <Alle Absender/Empfänger> und bei **Adressiert an:** <Alle Absender/Empfänger>. Es gibt keinerlei Ausnahmen. Jede Email von jedem Absender an jeden Empfänger wird auf Viren geprüft.

Die Darstellung der Adresseinstellungen im Job:



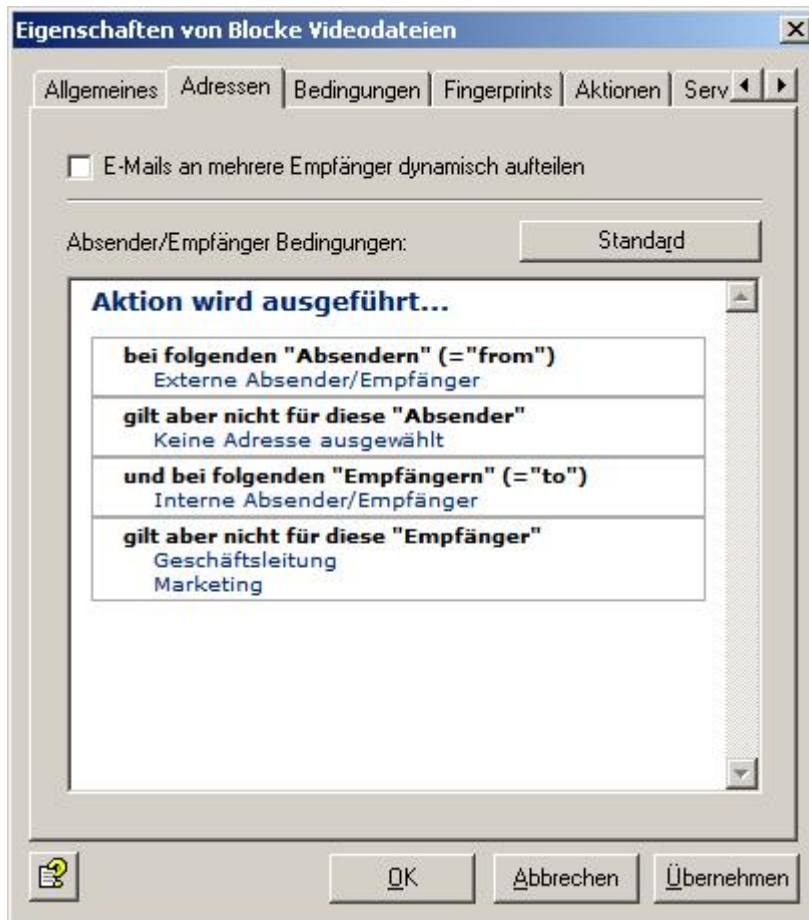
Mit der erweiterten Prüfung lassen sich komplexere Unternehmensrichtlinien einfach verwirklichen. Klicken Sie dazu auf die Schaltfläche **Erweitert**. Klicken Sie danach auf die Schaltfläche **Standard**, um zu der einfachen Auswahl zurückzukehren.

### Ein Beispiel für einen Job, der Dateianhänge blockt

Unternehmensrichtlinie: Es sollen keine Emails über das Internet ins Unternehmen gelangen, die Videoanhänge enthalten. Eine Ausnahme dieser Regel soll aber für das Marketing und die Geschäftsleitung definiert werden.

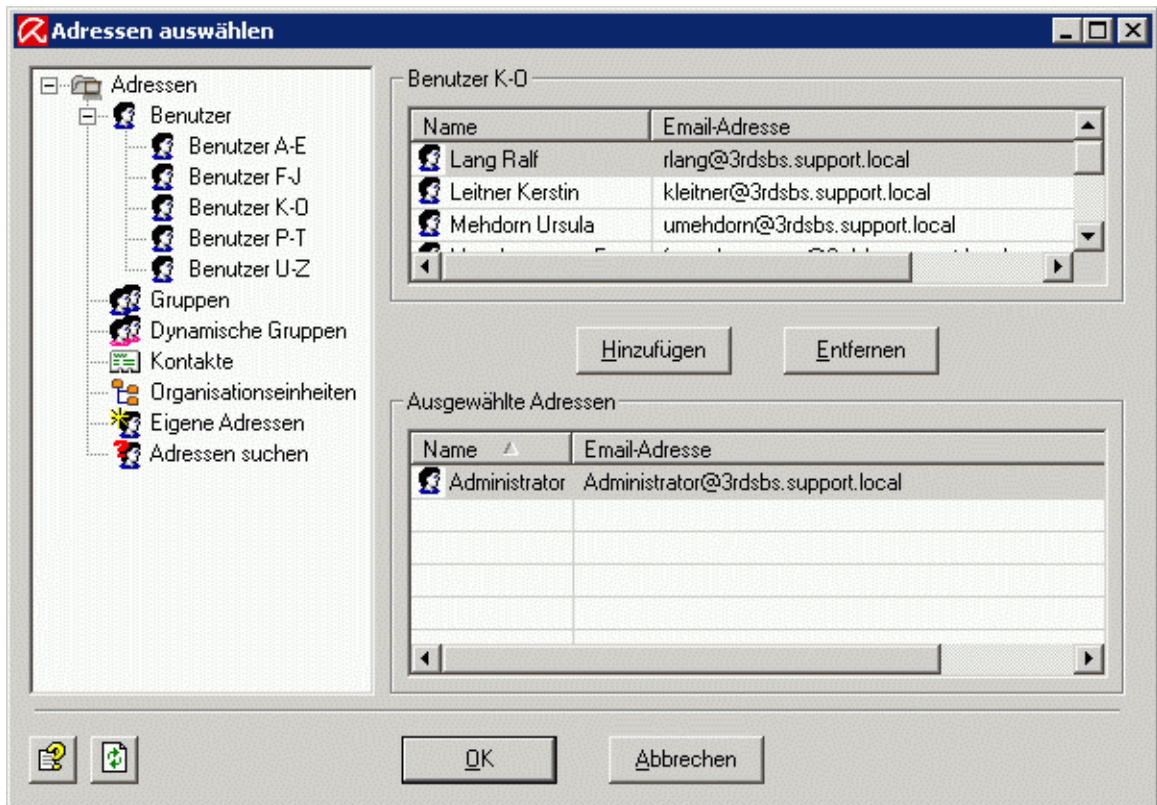
- **Bei folgenden Absendern** prüft den/die Absender. Die Ausnahme **Gilt aber nicht für diese Absender** ebenfalls.
- und **bei folgenden Empfängern** prüft den/die Empfänger. Die Ausnahme **Gilt aber nicht für diese Empfänger** ebenfalls.

Umsetzung: Die Adresseinstellungen im Job müssen wie folgt aussehen: Die definierte Aktion im Job (also das Blocken der Anhänge) wird ausgeführt **bei folgenden Absendern**: <Externe Absender / Empfänger> und soll unter und **bei folgenden Empfängern** an <Interne Absender / Empfänger> gesendet werden. Unter **Gilt aber nicht für diese Empfänger** definieren Sie als Ausnahme die Abteilungen Marketing und Geschäftsleitung, die Sie entweder bereits im Active Directory (AD) als Gruppe eingetragen haben oder die Sie separat als eigene Adressliste anlegen können. Damit werden alle Videoanhänge abgefangen, die von externen Absendern an interne Empfänger gesendet werden, es sei denn, der Empfänger ist ein Mitarbeiter des Marketing oder ein Mitglied der Geschäftsleitung. Die Darstellung der Adresseinstellungen im Job:

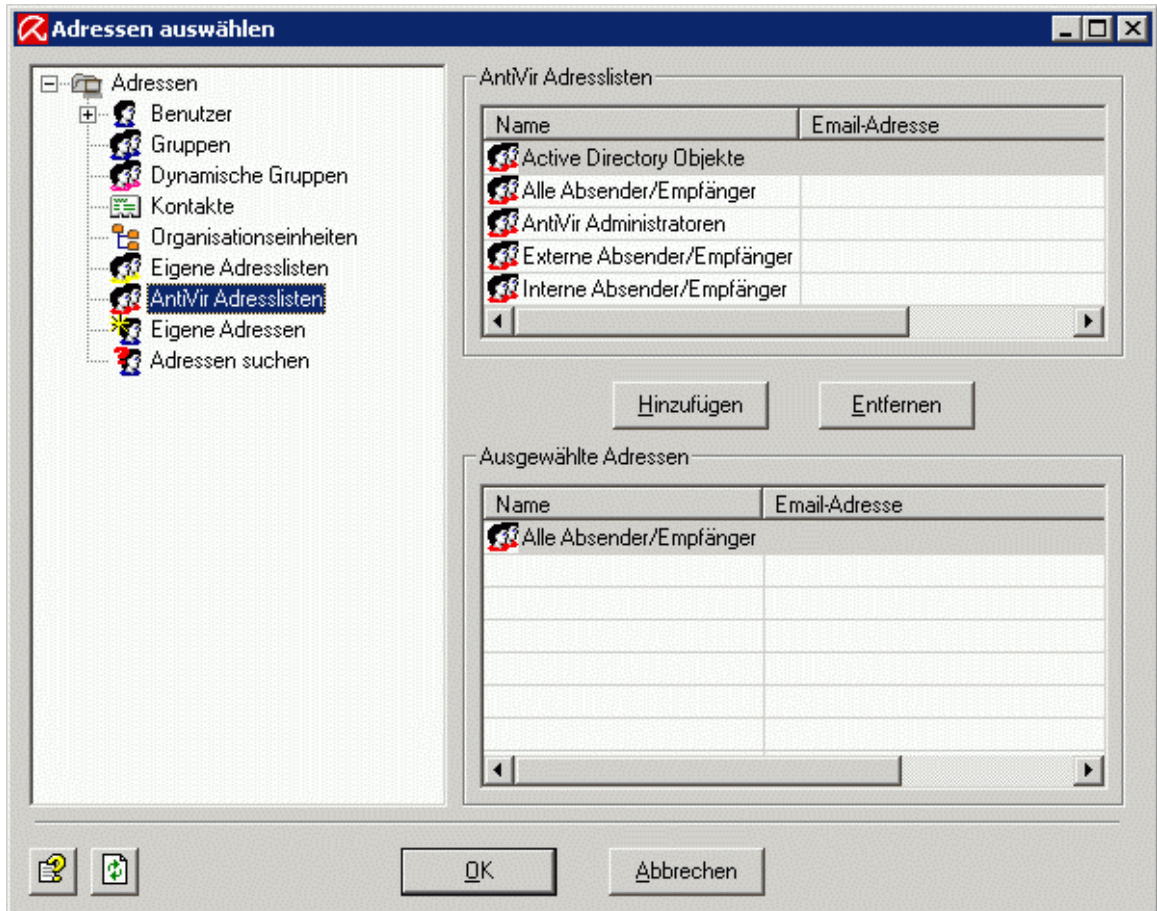


**Hinweis:** Grundsätzlich müssen alle angegebenen Bedingungen in den Feldern **bei folgenden Absendern** und **bei folgenden Empfängern** zutreffen, damit eine Aktion ausgelöst wird (UND-Verknüpfung). Wenn mehrere Adressen innerhalb der gleichen Bedingung (z.B. **bei folgenden Absendern**) eingetragen sind, muss nur eine zutreffen, um die Aktion auszulösen. Die Ausnahmen (**gilt aber nicht für ...**) sind für die grundsätzliche Aktionsauslösung irrelevant. Emails für oder von diesen Ausnahmeadressen werden nur weitergereicht, ohne dass die definierten Aktionen ausgeführt werden.

Klicken Sie auf **Interne Absender/Empfänger, Keine Adresse ausgewählt** oder einen entsprechenden Eintrag in den Ausnahmen, um das Adressauswahlfenster aufzurufen und die Adressen für genau diese Bedingung zu definieren:



Die AntiVir Adresslisten stehen Ihnen ebenfalls zur Verfügung:



Die Avira AntiVir Exchange Adresslisten sind feststehende Listen, aus den Einstellungen der übergreifenden Avira AntiVir Exchange Servers generiert, die bei der Installation abgefragt und eingetragen werden oder die Sie manuell konfiguriert haben. Siehe dazu [AntiVir Exchange Servers-Einstellungen](#).

**Hinweis: Eigene Adresslisten** und **AntiVir Adresslisten** werden nur bei der Adressauswahl für einen Job angezeigt. **Eigene Adresslisten** können Sie jederzeit ändern, **AntiVir Adresslisten** können nicht geändert werden.

### 4.3.6 Benachrichtigungsvorlagen


In jedem Job können Sie unter **Aktionen** bestimmen, wer eine Benachrichtigung erhalten soll, wenn Avira AntiVir Exchange eine verbotene Email entdeckt hat.

Beim Anlegen eines neuen Jobs können Sie die entsprechende Vorlage für den Jobtyp auswählen. Nähere Informationen zu den einzelnen Jobtypen erhalten Sie unter [Richtlinien-Konfiguration](#).


Die Benachrichtigungsvorlagen für die einzelnen Jobs (Inhaltsprüfung, Virenprüfung usw.) erstellen Sie in der **Basis-Konfiguration**.

### Benachrichtigungsvorlagen erstellen

Vorkonfigurierte Benachrichtigungsvorlagen für die einzelnen Module finden Sie unter **Basis-Konfiguration - Allgemeine Einstellungen - Vorlagen**.

1. Klicken Sie auf Vorlagen und wählen Sie den Vorlagentyp.
2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf die gewünschte Vorlage und wählen Sie **Eigenschaften**.
3. Geben Sie den Betreff ein.
4. Klicken Sie auf die Registerkarte **Benachrichtigungstext - Bearbeiten** für den Text der Benachrichtigung. Zur Gestaltung des Textes können Sie die Menüleiste für formatierten Text verwenden, die intern in HTML-Befehle umgewandelt werden. Wenn Sie den Quelltext mit der Schaltfläche  aufrufen, können Sie die HTML-Befehle auch direkt eingeben.
5. Unter der Registerkarte **Jobs** sehen Sie, in welchen Jobs die Benachrichtigungsvorlage verwendet wird.
6. Klicken Sie **OK**.

### Liste der Benachrichtigungsvariablen

Folgende Variablen, die Sie auch direkt mit dem Pfeil neben der  Schaltfläche einfügen können, sind in den Benachrichtigungstexten und in den Betreffzeilen der Benachrichtigungen möglich. Bitte beachten Sie, dass die Tokens [VAR] und [/VAR] case-sensitiv sind und immer in Großbuchstaben geschrieben werden müssen.



### Allgemein

Kategorie, Variablen-Typ	Variable	Beschreibung
Allgemein: Absender	[VAR]Mailsender[/VAR]	Absender der aktionsauslösenden E-Mail.
Allgemein: Absender (SMTP)	[VAR]From[/VAR]	Absender-SMTP der aktionsauslösenden E-Mail.
Allgemein: Betreff	[VAR]Subject[/VAR]	Betreffzeile der aktionsauslösenden E-Mail.
Allgemein: Datum und Uhrzeit	[VAR]Date[/VAR]	Datum und Uhrzeit, an dem der Job die Aktion auslöste.
Allgemein: Datum	[VAR]DateOnly[/VAR]	Datum, an dem der Job die Aktion auslöste.
Allgemein: Empfänger	[VAR]Recipients[/VAR]	Empfänger der aktionsauslösenden E-Mail.
Allgemein: Job Name	[VAR]Jobname[/VAR]	Name des Jobs, der eine Aktion auslöste.
Allgemein: Nicht zutreffende Empfänger	[VAR]UnrestrictedRecipients[/VAR]	Empfänger der aktionsauslösenden Email, die nicht in den Adress(Eingangs)-Bedingungen definiert waren.
Allgemein: Quarantäneordner	[VAR]Quarantine[/VAR]	Die Quarantäne, in die eine Email gestellt wurde.
Allgemein: ID einer quarantänierten E-Mail	[VAR]QuarantineDocRef[/VAR]	Eindeutige Kennung der Email, die in Quarantäne verschoben wurde.
Allgemein: Server	[VAR]Server[/VAR]	Server, über den die betroffene Email gesendet wurde, hier der Name, der in der Konfiguration eingetragen wurde.
Allgemein: Server (Netzwerkname)	[VAR]ServerFQDN[/VAR]	Server, über den die betroffene Email gesendet wurde, hier der Netzwerkname des Servers (Fully qualified domain name).
Allgemein: Uhrzeit	[VAR]TimeOnly[/VAR]	Uhrzeit, zu der der aktionsauslösende Job lief.

Allgemein: Avira AntiVir Exchange Report	[VAR]ToolReport[/VAR]	Kurze Zusammenfassung der Prüfungsergebnisse.
Allgemein: Avira AntiVir Exchange Report (Details)	[VAR]ToolReportDetails[/VAR]	Ergebnis der Prüfungen mit allen Details.
Allgemein: Zutreffende Empfänger	[VAR]RestrictedRecipients[/VAR]	Empfänger der aktionsauslösenden Email, die in den Adress(Eingangs)-bedingungen definiert sind.

### AntiVir Such Engine

Kategorie, Variablen-Typ	Variable	Beschreibung
AntiVir: Anhanggröße	[VAR]AttachmentSize[/VAR]	Größe des verbotenen/betroffenen Anhangs
AntiVir: Anhangtyp	[VAR]FingerprintName[/VAR]	Name des verbotenen Dateityps
AntiVir: Fingerprintkategorie	[VAR]Fingerprintcategory[/VAR]	Kategorie des verbotenen Dateityps
AntiVir: Gefundene E-Mail-Größe	[VAR]MessageSize[/VAR]	Größe der gesamten E-Mail
AntiVir: Gefundener Anhang	[VAR]AttachmentName[/VAR]	Namen der verbotenen/betroffenen Anhänge
AntiVir: Max. E-Mail-Größe	[VAR]SetSizeLimit[/VAR]	Im Job festgelegte maximale Email-Größe
AntiVir: Virusname	[VAR]Virusname[/VAR]	Namen der gefundenen Viren
AntiVir: Virens Scanner	[VAR]VirusScanner[/VAR]	Namen der fündig gewordenen Virens Scanner

### Informationsspeicher-Scan

Kategorie, Variablen-Typ	Variable	Beschreibung
IS-Scan: Datenbank	[VAR]VSAPI_Database[/VAR]	Name des Informationsspeichers, in dem sich die Nachricht zum Zeitpunkt der Virenprüfung befunden hat
IS-Scan: Datenbank URL	[VAR]VSAPI_Url[/VAR]	URL des Informationsspeichers, in dem sich die Nachricht zum Zeitpunkt der Virenprüfung befunden hat

IS-Scan: Fehlerbeschreibung	[VAR]VSAPI_ErrorText[/VAR]	Nähere Beschreibung im Fehlerfall durch den Informationsspeicher-Job
IS-Scan: Gesendet am	[VAR]VSAPI_SubmitTime[/VAR]	Sende-Datum und -Uhrzeit der Nachricht
IS-Scan: Nachrichten URL	[VAR]VSAPI_MessageUrl[/VAR]	Informationsspeicher-URL der Nachricht zum Zeitpunkt der Virenprüfung
IS-Scan: Ordner	[VAR]VSAPI_Folder[/VAR]	Name des Informationsspeicher-Ordners, in dem sich die Nachricht zum Zeitpunkt der Virenprüfung befunden hat
IS-Scan: Postfach	[VAR]VSAPI_Mailbox[/VAR]	Name des Besitzers des Postfaches, in dem sich die Nachricht zum Zeitpunkt der Virenprüfung befunden hat
IS-Scan: Server	[VAR]VSAPI_Server[/VAR]	Name der Servers, auf dem die Virenprüfung durch den Informationsspeicher-Scan durchgeführt wurde
IS-Scan: Virenschanner	[VAR]virusscanner[/VAR]	Namen des fündig gewordenen Virenschanners
IS-Scan: Virusname	[VAR]virusname[/VAR]	Name der gefundenen Viren
IS-Scan: Zugestellt am	[VAR]VSAPI_DeliveryTime[/VAR]	Zustell-Datum und -Uhrzeit der Nachricht

## AntiVir Wall

Kategorie, Variablen-Typ	Variable	Beschreibung
<b>Inhaltsprüfung</b>		
Wall: Details Inhaltsprüfung	[VAR]DeniedContentTabHTML[/VAR]	Detailinformationen über die gefundenen Wörter/Phrasen
Wall: Mailabschnitt	[VAR]DeniedMailParts[/VAR]	Betroffene aktionsauslösende Anhänge/Nachrichtentexte
Wall: Verbotene Wortlisten	[VAR]DeniedWordlists[/VAR]	Aktionsauslösende Wortlisten mit erreichtem Wert / Schwellwert
Wall: Verbotener Inhalt	[VAR]DeniedWord[/VAR]	Aktionsauslösendes Wort mit erreichtem Wert / Schwellwert

<b>Anti-Spam-Prüfung</b>		
Wall: Details Spam-Analyse	[VAR]SpamReportHTML[/VAR]	Detailinformationen der einzelnen Spam-Kriterien
Wall: Spam-Wahrscheinlichkeit	[VAR]SpamValue[/VAR]	Ermittelte Spam-Wahrscheinlichkeit in Form eines Wertes (0 - 100). Dieser Wert wird mit den individuell einzustellenden Schwellwerten im Advanced Spam Filtering Job verglichen.
Wall: Spam-Level	[VAR]SpamLevel[/VAR]	Im Email-Header jeder geprüften E-Mail wird von AntiVir Wall ein Spam-Level in Form von Sternen in 10er-Schritten eingetragen (z.B.: (X-SPAM-TAG: * bedeutet, Spam-Wahrscheinlichkeit liegt zwischen 0 und 10, X-SPAMTAG:** zwischen 20 und 30). Sie können nach diesem String im Header von Outlook suchen lassen und eine Regel formulieren, die z.B. alle Emails mit 3 und mehr Sternen mit diversen Aktionen belegt. Nähere Informationen über Regelmöglichkeiten in Outlook entnehmen Sie bitte der Outlook-Hilfe.
<b>Adressprüfung</b>		
Wall: Anzahl der Empfänger	[VAR]NumberRecipient[/VAR]	Anzahl der adressierten Empfänger
Wall: Max. Empfängeranzahl	[VAR]SetRecipientLimit[/VAR]	Im Job festgelegte Empfänger-Anzahl-Beschränkung
Wall: Verbotene Absender	[VAR]DeniedSender[/VAR]	Name der aktionsauslösenden Absender
Wall: Verbotene Empfänger	[VAR]DeniedRecipient[/VAR]	Name der aktionsauslösenden Empfänger

### Quarantäne-Sammelbenachrichtigung

Kategorie, Variablen-Typ	Variable	Beschreibung
Sammelbenachrichtigung: Absender	[VAR]From[/VAR]	Absender der Sammelbenachrichtigung
Sammelbenachrichtigung: Antwortadresse	[VAR]ReplyTo[/VAR]	Die Adresse, an die Antworten auf die Sammelbenachrichtigung geschickt werden sollen (NotificationReplyTo)
Sammelbenachrichtigung: Betreff	[VAR]Subject[/VAR]	Betreff der Sammelbenachrichtigung
Sammelbenachrichtigung: Datum aktuelle Benachrichtigung	[VAR]Nowdate[/VAR]	Datum der Generierung der aktuellen Sammelbenachrichtigung
Sammelbenachrichtigung: Datum letzte Benachrichtigung	[VAR]Lastdate[/VAR]	Datum der Generierung der letzten Sammelbenachrichtigung
Sammelbenachrichtigung: Datum und Zeit aktuelle Benachrichtigung	[VAR]Now[/VAR]	Datum und Uhrzeit der Generierung der aktuellen Sammelbenachrichtigung
Sammelbenachrichtigung: Datum und Zeit letzte Benachrichtigung	[VAR]Last[/VAR]	Datum und Uhrzeit der Generierung der letzten Sammelbenachrichtigung
Sammelbenachrichtigung: Empfänger	[VAR]RcptTo[/VAR]	Empfänger der Sammelbenachrichtigung
Sammelbenachrichtigung: Full Qualified Domain Name	[VAR]FQDN[/VAR]	Voller Netzwerkname des Servers, auf dem sich die Quarantäne befindet, für die die Sammelbenachrichtigungen erzeugt werden.
Sammelbenachrichtigung: Liste der Quarantäne E-Mails	[VAR]HtmlList[/VAR]	Komplette Liste aller Quarantäne-Objekte für den entsprechenden Empfänger mit HTML-Formatierungen (Pflichtfeld in der Quarantäne- Sammelbenachrichtigung).
Sammelbenachrichtigung: HTTP Port	[VAR]HTTPPort[/VAR]	Port des HTTP-Servers
Sammelbenachrichtigung: HTTP Server	[VAR]HTTPServer[/VAR]	HTTP-Server, um eine Benutzeranfrage per HTTP zu versenden

Sammelbenachrichtigung: Quarantäne	[VAR]Displayname[/VAR]	Name der Quarantäne, aus der die Liste der E-Mails erstellt wurde
Sammelbenachrichtigung: Server	[VAR]Server[/VAR]	Kurzname des Servers, auf dem sich die Quarantäne befindet, für die die Sammelbenachrichtigungen erzeugt werden
Sammelbenachrichtigung: Uhrzeit aktuelle Sammelbenachrichtigung	[VAR]Nowtime[/VAR]	Uhrzeit der Generierung der aktuellen Sammelbenachrichtigung
Sammelbenachrichtigung: Uhrzeit letzte Sammelbenachrichtigung	[VAR>Lasttime[/VAR]	Uhrzeit der Generierung der letzten Sammelbenachrichtigung

### Kombinierte Benachrichtigungen

Kategorie, Variablen-Typ	Variable	Beschreibung
Kombinierte Benachrichtigung: Inhaltsverzeichnis	[VAR]TOCList[/VAR]	Nummerierte HTML-Liste aller Benachrichtigungen (Subject). Jeder Listeneintrag ist per Link mit dem zugehörigen Eintrag der Benachrichtigungsliste (Variable "NotificationList") verknüpft.
Kombinierte Benachrichtigung: Benachrichtigungsliste	[VAR]NotificationList[/VAR]	HTML-Liste aller Benachrichtigungen (Body) jeweils durch einen waagerechten Trennstrich abgegrenzt.

### Whitelist

Kategorie, Variablen-Typ	Variable	Beschreibung
Userlist: Einträge	[VAR]HtmlList[/VAR]	Komplette Liste aller Einträge für den entsprechenden Empfänger mit HTML-Formatierungen (Pflichtfeld in der Whitelist Benachrichtigung)

## Details zur Avira AntiVir Exchange Management Konsole

Userlist: Fully qualified domain name	[VAR]FQDN[/VAR]	Voller Netzwerkname des Servers, auf dem sich die Whitelist befindet, für die die Sammelbenachrichtigungen erzeugt werden.
Userlist: HTTP-Port	[VAR]HTTPPort[/VAR]	Port des HTTP-Servers
Userlist: HTTP-Server	[VAR]HTTPServer[/VAR]	HTTP-Server, um eine Benutzeranfrage per HTTP zu versenden
Userlist: Name	[VAR]Displayname[/VAR]	Name der Whitelist, aus der die Liste der E-Mails erstellt wurde
Userlist: Empfänger	[VAR]RcptTo[/VAR]	Empfänger der Whitelist Benachrichtigung
Userlist: Antwortadresse	[VAR]ReplyTo[/VAR]	Die Adresse, an die Antworten auf die Whitelist Benachrichtigung geschickt werden sollen (NotificationReplyTo)
Userlist: Absender	[VAR]From[/VAR]	Absender der Whitelist Benachrichtigung
Userlist: Server	[VAR]Server[/VAR]	Kurzname des Servers, auf dem sich die Whitelist befindet, für die die Benachrichtigungen erzeugt werden
Userlist: Anzahl Einträge	[VAR]CollectedSize[/VAR]	Gesamtgröße der Whitelist Benachrichtigung
Userlist: Betreff	[VAR]Subject[/VAR]	Betreff der Benachrichtigung
Userlist: Nummer	[VAR]SummaryPart[/VAR]	Falls mehr als 3000 neue Einträge in eine Whitelist aufgeführt werden, erhält der Anwender mehrere Whitelist Benachrichtigungen. Die Variable gibt die forlaufende Nummer der Benachrichtigung zurück („1“ für die ersten 3000 Einträge, „2“ für die nächsten 3000 usw.).
Whitelist: Whitelist per HTTP versenden	[VAR]link::HTTP_SendWhitelist[/VAR]	Whitelist-Anfrage und Benachrichtigung erfolgt über HTTP
Whitelist: Whitelist per E-Mail versenden	[VAR]link::MAIL_SendWhitelist[/VAR]	Whitelist-Anfrage und Benachrichtigung erfolgt per Email
Whitelist: Whitelist per HTTP löschen	[VAR]link::HTTP_ClearWhitelis[/VAR]	Löschen der Whitelist über HTTP

Whitelist: Whitelist per E-Mail löschen	[VAR]link::MAIL_ClearWhitelist[/VAR]	Löschen der Whitelist per Email
Blacklist: Blacklist per HTTP versenden	[VAR]link::HTTP_SendBlacklist[/VAR]	Blacklist-Anfrage und Benachrichtigung erfolgt über HTTP
Blacklist: Blacklist per E-Mail versenden	[VAR]link::MAIL_SendBlacklist[/VAR]	Blacklist-Anfrage und Benachrichtigung erfolgt per E-Mail
Blacklist: Blacklist per HTTP löschen	[VAR]link::HTTP_ClearBlacklist[/VAR]	Löschen der Blacklist über HTTP
Blacklist: Blacklist per E-Mail löschen	[VAR]link::MAIL_ClearBlacklist[/VAR]	Löschen der Blacklist per E-Mail

### 4.3.7 Datenbankverbindung zu einem SQL-Server anlegen

#### Verbindung mit SQL-Servern

Mithilfe der Datenbankverbindungen können Sie externe Datenbanken an Avira AntiVir Exchange anbinden. Anstelle der regulär verwendeten lokalen Datenbank auf Basis der Microsoft Jet-Engine lässt sich so auch ein Microsoft SQL-Server verwenden, der die Avira AntiVir Exchange-Daten in eine SQL-Datenbank schreibt. Zurzeit werden MS SQL Server 2000 und MS SQL Server 2005 unterstützt, zudem kann MS SQL Server 2005 Express mit eingeschränkter CPU- und Speicherkapazität eingesetzt werden.

#### Einsatzmöglichkeiten von SQL-Servern

Um in Multi-Server-Umgebungen ohne Server-Synchronisation dafür zu sorgen, dass jeder Benutzer nur eine zentrale Whitelist für alle beteiligten Server erhält, können Sie einen Microsoft SQL-Server einsetzen.

Daneben kann der Microsoft SQL-Server auch im Zusammenhang von Quarantäne-Datenbanken eingesetzt werden.

Wenn in einer Multi-Server-Umgebung mehrere SQL-Server sowie mehrere Avira AntiVir Exchange Server installiert sind, können diese paarweise angeordnet werden. Das heißt, auf jedem Avira AntiVir Exchange Server ist ein lokaler SQL-Server installiert, wodurch nur eine Datenbankverbindung eingerichtet werden muss.

**Hinweis:** Beachten Sie, dass Avira AntiVir Exchange für den Einsatz als lokale Datenbank auf Basis der MS Jet Engine optimiert ist. Bei komplexen Serverumgebungen sind umfangreiche Konfigurationen an Avira AntiVir Exchange sowie am MS SQL Server erforderlich, die in diesem Rahmen nicht erläutert werden können. Bei konkreten Fragen konsultieren Sie bitte unseren Support.

#### Konfiguration der Datenbankverbindung

In den folgenden Abschnitten wird die Konfiguration von Datenbankverbindungen zwischen der Avira AntiVir Exchange und einem Microsoft SQL-Server beschrieben. Beachten Sie bei der Konfiguration die Unterscheidung zwischen einem zentralen MS SQL Server für zentrale Benutzer Whitelists und einem lokalen MS SQL Server für die Quarantäne.



### SQL-Server und Avira AntiVir Exchange Server

Wenn der SQL-Server und der Avira AntiVir Exchange Server auf dem selben Rechner installiert sind, müssen folgende Voraussetzungen gegeben sein:

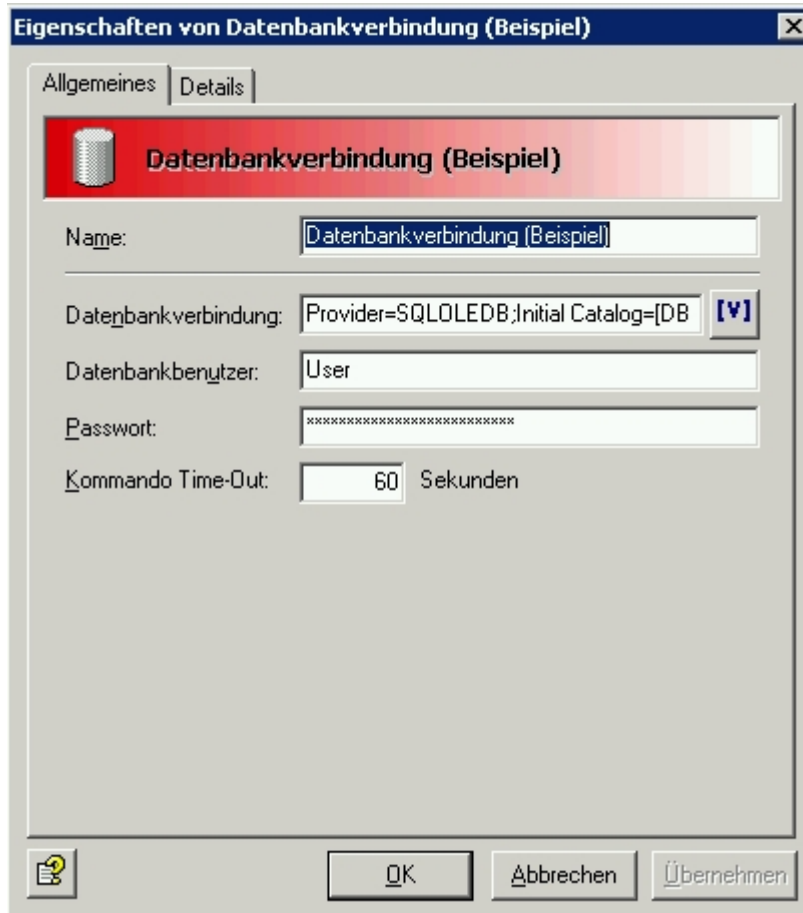
- Installationen von SQL-Server und Avira AntiVir Exchange Server sind abgeschlossen
- Datenbank(en) sind eingerichtet und die zugehörigen Tabellen angelegt
- Mindestens ein Anwender ist als Datenbank-User angelegt
- Der Datenbank-User hat entsprechende Zugriffsrechte auf die Datenbank
- Der ADO-Treiber ist auf dem Avira AntiVir Exchange Server installiert

Sind der SQL-Server und der Avira AntiVir Exchange Server auf unterschiedlichen Systemen installiert, muss zusätzlich gewährleistet sein, dass

- das auf dem SQL-Server eingestellte Protokoll den Anforderungen zum externen Serverbetrieb entspricht.
- nach der Konfiguration des SQL-Servers der Service neu gestartet wurde.

Die Datenbankverbindung zwischen der Avira AntiVir Exchange und dem SQL-Server wird über das ADO-Protokoll hergestellt.

1. Dazu legen Sie unter **Basis-Konfiguration - Allgemeine Einstellungen - Datenbankverbindungen** eine neue Datenbankverbindung an.
2. Vergeben Sie einen **Namen** für die Verbindungskonfiguration und legen Sie im Feld **Datenbankverbindung** die Angaben für den ADO-String fest.
3. Tragen Sie die benötigten Werte manuell ein oder verwenden Sie die hinterlegten Avira AntiVir Exchange-Variablen (Server, Datenbank, usw.), die zur Laufzeit durch die zugehörigen Werte ersetzt werden.



Das nachfolgende **Beispiel** ist eine von vielen Konfigurationsmöglichkeiten des ADO-Strings. Ausführliche Erklärungen zu diesen und weiteren Optionen und Konfigurationen des MS SQL ADO-Strings, entnehmen Sie bitte der entsprechenden Dokumentation von Microsoft.

Beispiel-Verbindungsstring:

```
Provider=SQLOLEDB;User
ID=[ADOUser];Password=[ADOPwd];Trusted_Connection=No;Initial
Catalog=[DBCatalog];Data Source=LOCALHOST\SQLEXPRESS;
```

- `Provider=SQLOLEDB`; Obligatorischer Parameter, der den Provider spezifiziert. Tragen Sie den Wert manuell ein (keine AntiVir-Variable verfügbar).
- `User ID=[ADOUser]; Password=[ADOPwd]`; Obligatorische Parameter; Schreiben Sie die Parameter 'User ID=' und 'Password=' manuell in den String und setzen Sie die AntiVir-Variablen **Datenbankbenutzer** und **Passwort**. Die eingefügten [ADOUser] und [ADOPwd] werden bei der Auswertung durch die Inhalte der Felder von Punkt 3 ersetzt. Die Verwendung der Variablen wird empfohlen, da so verhindert wird, dass die Werte im ADO-String in Klartext ausgegeben werden. Prinzipiell können Sie die Werte aber auch manuell eintragen. Lassen Sie in diesem Fall die beiden Felder von Punkt 3 leer.
- `Trusted_Connection=No`; Optionaler Parameter zur SQLAuthentifizierung. Damit der SQL-Server den Avira AntiVir Exchange Server als Trusted Server kennt, tragen Sie 'Trusted\_Connection=No;' manuell ein (keine Avira AntiVir Exchange-Variable verfügbar).

- `Initial Catalog=[DBCatalog]`; Obligatorischer Parameter, der die zu verwendende Datenbank angibt. Tragen Sie den Parameter 'Initial Catalog=' manuell in den String ein und setzen Sie die Avira AntiVir Exchange-Variable **Datenbank**. Wenn Sie den SQL-Server für die Quarantäne verwenden, wird die Variable [DBCatalog] durch den Namen der **Datenbank**, der unter **Quarantäne - Eigenschaften** im Feld **Ordnername** festgelegt wurde, ersetzt. Wenn Sie den SQL-Server dagegen für eine zentrale Whitelist verwenden, wird die Variable [DBCatalog] durch den festen Namen 'Whitelist' ersetzt. Mittels der Variablen [DBCatalog] können Sie eine Datenbankverbindung für mehrere Datenbanken innerhalb eines MS SQL Servers verwenden. Beachten Sie, dass die Datenbanken unter exakt diesem Namen angelegt sein müssen. Ein Verbindungsaufbau ist anderenfalls nicht möglich!
- `Data Source=LOCALHOST\SQLEXPRESS`; Obligatorischer Parameter für einen lokal installierten MS SQL Server 2005 Express. Tragen Sie in diesem Fall den Parameter 'Data Source=' manuell ein und setzen Sie bei Bedarf die Avira AntiVir Exchange-Variable **Server**. Die Variable [Server] wird zur Laufzeit durch den NetBiosNamen des Servers ersetzt. Wenn Sie in komplexen Server-Umgebungen mit Subdomains arbeiten, können Sie auch die Avira AntiVir Exchange-Variable **Server (Netzwerk)** verwenden. In diesem Fall wird die Variable [ServerFQDN] gesetzt und die FQDN (Fully Qualified Domain Name) des Servers ausgelesen. Wird der SQL-Server für zentrale Whitelists verwendet, geben Sie hier den Namen des zentralen SQL-Servers manuell an.

**Ausnahme:** Im ADO-String können im Fall eines zentralen SQL-Servers, z.B. bei Verwendung des SQL-Servers für zentrale Whitelists, die beiden Avira AntiVir Exchange Variablen **Server** bzw. **Server (Netzwerk)** nicht verwendet werden. Tragen Sie stattdessen die Bezeichnung des SQL-Servers manuell ein, also `Data-Source=Name_des_Servers`;

4. Im Feld **Datenbankbenutzer** tragen Sie den Namen des SQL-Users ein, der auf die Datenbank zugreifen darf (in der Grafik als User eingetragen). Geben Sie im Folgefild das zugehörige **Passwort** ein. Die hier eingetragenen Werte können über die Variablen [ADOUser] und [ADOPwd] im ADO-String ausgelesen werden.
5. Im Feld **Kommando Time-Out** geben Sie an, nach wievielen Sekunden die Datenbankverbindung abgebrochen wird, wenn aus der Datenbank keine Daten zurückgeliefert werden. Bei großen Datenbanken wird empfohlen mit dem Wert 60 Sekunden zu beginnen.

### Zentrale Whitelists einrichten

Findet die Emailabwicklung in Multi-Server-Umgebungen statt, erzeugt jeder Server seine eigenen Benutzer-Whitelists. Ohne Server-Synchronisation erhält folglich jeder Benutzer für jeden der beteiligten Server, eine separate Whitelist, die einzeln gepflegt werden muss. Um diese Whitelists zentral zu verwalten und damit die Administration zu vereinfachen, können Sie anstelle der regulären lokalen Datenbank auf Basis der Microsoft Jet-Engine auch einen Microsoft SQL-Server einrichten, der die Daten für alle beteiligten Avira AntiVir Exchange Server in eine zentrale SQL-Datenbank schreibt.

Um zentrale Whitelists zu konfigurieren, muss zunächst eine Datenbankverbindung zwischen dem SQL-Server und dem Avira AntiVir Exchange Server konfiguriert werden. Anschließend sind weitere Einstellungen innerhalb der Avira AntiVir Exchange erforderlich, damit Avira AntiVir Exchange die Einträge aus der Whitelist-Datenbank entnehmen kann.

Die Konfiguration der Datenbankverbindung hängt von der Server-Umgebung ab.

1. Gehen Sie je nach Betriebsumgebung, wie in den Szenarien unter [Konfiguration der Datenbankverbindung](#).
2. Unter `Data Source=` tragen Sie bitte den zentralen SQL-Server ein.

**Hinweis:** Beachten Sie, dass im ADO-String der Datenbankverbindung die Variable [DBCatalog] für die Whitelist-Datenbank durch den festen Datenbanknamen 'Whitelist' ersetzt wird.

3. Wählen Sie unter **AntiVir Servers Einstellungen- Eigenschaften** im Feld **Datenbankverbindung für Whitelist-Einträge** den SQL-Server aus. In diesem Feld stehen sämtliche Datenquellen, die unter Datenbankverbindungen eingetragen wurden, zur Auswahl.
4. Öffnen Sie den Wall-Job **Advanced Spam Filtering - Aktionen - Definitive Kriterien** und aktivieren Sie das Feld **Emails von Absendern in Benutzer Whitelist**.

### Quarantäne-Datenbank einrichten

Neben der Möglichkeit den Microsoft SQL-Server für Whitelists zu verwenden, kann er auch lokal im Zusammenhang von Quarantäne-Datenbanken eingesetzt werden. Regulär wird der Index einer Quarantäne in der lokalen Datenbank (Microsoft Jet-Engine) geführt. Wenn die Kapazität einer Jet-Datenbank nicht ausreicht, können Sie diese Einträge auch in einen lokal installierten SQL-Server schreiben lassen. Hierfür müssen Sie MS SQL auf dem Email-Server installiert haben.

Die Konfiguration der Datenbankverbindung hängt von der Server-Umgebung ab.

1. Gehen Sie je nach Betriebsumgebung, wie in den Szenarien unter [Konfiguration der Datenbankverbindung](#).
2. Tragen Sie bei `Data Source=` auf jedem Server LOCALHOST ein, um den lokal installierten SQL-Server anzusprechen.

**Hinweis:** Beachten Sie, dass im ADO-String der Datenbankverbindung die Variable [DBCatalog] für den Namen der Quarantäne-Datenbank, durch den Ordernamen unter **Quarantäne - Eigenschaften - Ordnername** ersetzt wird. Dadurch kann eine Datenbankverbindung für mehrere Quarantäne-Datenbanken verwendet werden.

Bei SQL-Datenbanken ist es mitunter möglich, dass der Datenbank-Service ausfällt oder nicht erreichbar ist. Als Folge ist auch die Quarantäne-Datenbank während dieser Ausfallzeit nicht erreichbar, wodurch Emails, die in diesem Zeitraum in Quarantäne gestellt werden sollten, nicht ordnungsgemäß abgelegt werden können. Um die Behandlung der Email im Quarantäne-Fehlerfall zu steuern, steht ihnen analog zur Option **geschäftskritisch** im Job, die selbe Option auch für die Quarantäne zur Verfügung (**Quarantäne - rechte Maustaste: Eigenschaften - Diese Quarantäne ist geschäftskritisch** aktivieren).

Ist eine Quarantäne auf 'geschäftskritisch' gesetzt, wird ein aufgetretener Quarantänefehler an den Job gemeldet. Daraufhin wird der Job abgebrochen und die Fehleroutine dieses Jobs gestartet. Wie mit der Email verfahren wird, ob der Job ignoriert oder die Email in das Verzeichnis Badmail verschoben wird, ist abhängig von der Einstellung 'geschäftskritisch' im Job selbst.

### Problembehandlung mit SQL-Servern

Treten bei der Installation bzw. Konfiguration der SQL-Server Probleme auf, kann das auf zahlreiche unterschiedliche Ursachen zurückzuführen sein. Daher können an dieser Stelle lediglich Hilfestellungen zur Fehleranalyse gegeben werden:

- Stellen Sie sicher, dass der SQL Server Browser aktiv ist.
- Prüfen Sie den Port (Standard: 1433) oder passen Sie ihn an Ihre Server-Umgebung.
- Pfad bei *Microsoft SQL Server 2005*: **Configuration Tools - SQL Server Configuration Manager** unter **SQL Native Client Configuration - Client Protocols - TCP/IP** doppelklicken.
- Pfad bei *Microsoft SQL Server 2005*: **Configuration Tools - SQL Server Configuration Manager - SQL Server 2005 Services - SQL Server Browser** (Status: Running).

Wenn ein zentraler SQL-Server installiert ist, der auf einem anderen Rechner als der AntiVir-Server läuft, müssen auch folgende Voraussetzungen gegeben sein:

- Wenn Sie den *Microsoft SQL Server 2005* verwenden, wählen Sie **Configuration Tools - SQL Server Surface Area Configuration - Surface Area Configuration for Services and Connections** an. Selektieren Sie bei **MSSQLSERVER - Database Engine - Remote Connections** die Option **Using both TCP/IP and named pipes**, um die im ADO-String konfigurierte Verbindung auf dem SQL-Server zuzulassen.
- Nach der Konfiguration muss der Service des SQL-Servers neu gestartet werden.

**Hinweis:** Beachten Sie auch die Konfigurationsmöglichkeiten der Quarantäne (**geschäftskritisch**) bei Ausfall des Datenbank-Services.

### 4.3.8 Ordner-Einstellungen

#### Quarantäne konfigurieren

Eine Quarantäne ist ein Ordner, in dem alle von den Bedingungen betroffenen Emails abgelegt werden, falls Sie dieses durch die Aktion **Kopie in Quarantäne** definiert haben. Bei der Installation der Avira AntiVir Exchange wird im Datenverzeichnis ein Ordner namens Quarantine angelegt, in dem sich zunächst einige Standard-Quarantänen und später alle weiteren neu angelegten Quarantänen befinden.

1. Unter dem Menüpunkt **Basis-Konfiguration - Ordner - Quarantänen** können Sie die vorhandenen Quarantänen konfigurieren und neue einrichten. Klicken Sie auf **Quarantänen**.

Im rechten Fenster werden alle verfügbaren Quarantänen angezeigt.

Anlegen einer neuen Quarantäne:

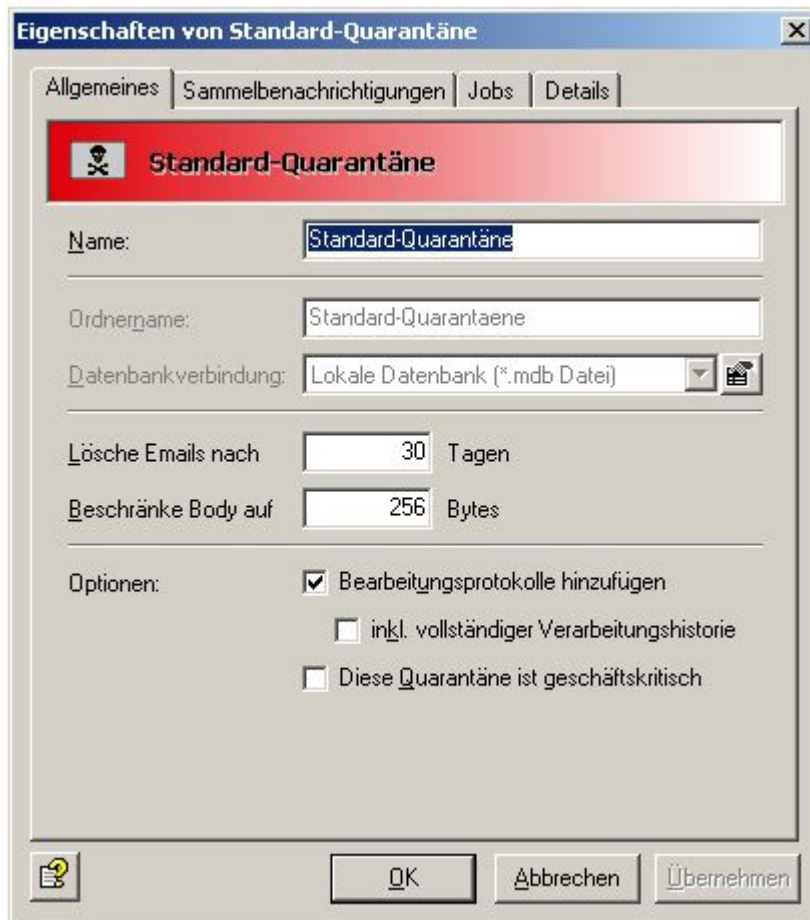
- Klicken Sie mit der rechten Maustaste auf **Quarantänen** und wählen Sie **Neu - Quarantäne**.
- Jetzt wird der **Ordnername** aus der Beschreibung übernommen. Dabei werden nur die Zeichen von A-Z und von 0-9 umgesetzt, alle anderen Zeichen werden in Unterstriche umgewandelt.
- Der vorgeschlagene **Ordnername** kann überschrieben werden.

**Hinweis:** Geben Sie hier keinen absoluten Pfad ein, sondern nur den Ordnernamen!

- Nach dem Speichern der Konfiguration wird die neue Quarantäne automatisch vom EMH angelegt und werden anschließend auch im AntiVir Monitor angezeigt (aktualisieren Sie die Ansicht!)

**Warnung:** Die Größe einer Quarantäne ist auf 1 GB beschränkt!

2. Klicken Sie mit der rechten Maustaste auf eine vorhandene Quarantäne im rechten Fenster und wählen Sie **Eigenschaften**.



3. Sie können unter **Name** die Quarantäne mit einem aussagekräftigen Namen beschreiben.  
Der **Ordnername** der Quarantäne bleibt aber unverändert. Die Eingabe im Feld Ordnername steht nur bei eigenen, neu angelegten Quarantänen zur Verfügung.
4. Legen Sie fest nach wie vielen Tagen eine Email, die in Quarantäne gestellt wurde, vorgehalten werden soll bis sie automatisch gelöscht wird.
5. Mit **Beschränke Body auf** können Sie bestimmen, ob und wie viel Text aus dem Body der Email (Nachrichtentext) in die Datenbank geschrieben wird.  
Beachten Sie bei diesem Wert die Datenschutzaspekte und den benötigten Platzbedarf in der Datenbank.

**Warnung:** Die Größe einer Quarantäne ist auf 1 GB beschränkt!

6. Mit **Bearbeitungsprotokolle hinzufügen** können Sie die Verarbeitung der Emails, die in diese Quarantäne gestellt werden, protokollieren.  
So lassen sich zum Beispiel die Gründe für eine in Quarantäne gestellten Email zurückverfolgen. Im AntiVir Monitor können Sie die jeweilige Email aufrufen und über die Registerkarte **Verarbeitung** das Verarbeitungsprotokoll einschließlich der Detailinformationen einsehen.
7. **Diese Quarantäne** ist geschäftskritisch:

Ist dieses Feld aktiviert, wird ein aufgetretener Quarantänefehler an den Job gemeldet. Daraufhin wird der Job abgebrochen und die Fehleroutine dieses Jobs gestartet. Wie mit der Email verfahren wird, ob der Job ignoriert oder die Email in das Verzeichnis Badmail verschoben wird, ist abhängig von der Einstellung 'geschäftskritisch' im Job selbst. Für Informationen zu 'geschäftskritisch' im Job, siehe [Dieser Job ist geschäftskritisch](#).

**Beispiel:** Ein Job, der auf Viren prüft, findet in einer eingehenden Email einen Virus. Der Job ist so konfiguriert, dass die Email in die Standard-Quarantäne aber nicht dem Empfänger zugestellt werden soll. Aufgrund eines Quarantänefehlers steht die Quarantäne nicht zur Verfügung. Die Email kann also nicht in Quarantäne gestellt werden. Folgende Einstellungen sind für Quarantäne und Job denkbar:

- Quarantäne + Job sind beide NICHT 'geschäftskritisch':  
Ergebnis: Der Quarantänefehler wird ignoriert. Die E-Mail kann zwar nicht in die Quarantäne kopiert werden, sie wird jedoch auch nicht zugestellt.
- Quarantäne ist NICHT 'geschäftskritisch' + Job IST 'geschäftskritisch':  
Ergebnis: siehe oben.
- Quarantäne IST 'geschäftskritisch' + Job ist NICHT 'geschäftskritisch':  
Ergebnis: Die Jobverarbeitung wird abgebrochen und die virulente(!) Email an den nächsten Job der Verarbeitungskette unbearbeitet übergeben.
- Quarantäne + Job sind beide 'geschäftskritisch':  
Ergebnis: Die Email wird in die Badmail-Quarantäne verschoben und dort vorgehalten. Die Email wird nicht zugestellt.

**Warnung:** Solange der Quarantänefehler nicht behoben ist, wird bei aktivierter Option 'geschäftskritisch' (in der Quarantäne) immer wieder ein Fehler an den Job gemeldet.

Ist der Job selbst nicht 'geschäftskritisch', schaltet er sich nach einiger Zeit ab und bearbeitet keine weiteren Emails.

Ist der Job dagegen ebenfalls 'geschäftskritisch' wird jede Email solange in den Badmail-Bereich überführt und nicht zugestellt bis der Fehler behoben ist!

Die Administratoren der Avira AntiVir Exchange werden bei häufig auftretenden Fehlern in der Quarantäne oder im Job auch unabhängig von der Einstellung 'geschäftskritisch' per Email informiert.

8. Unter der Registerkarte **Sammelbenachrichtigungen** können Sie nun für diese Quarantäne eine Quarantäne-Sammelbenachrichtigung konfigurieren.

**Hinweis:** Wenn Sie den Usern den Zugriff und die Bearbeitung der Whitelists zulassen, wählen Sie unter Vorlage Quarantäne-Sammelbenachrichtigung mit Whitelist Unterstützung aus.

### Quarantäne-Sammelbenachrichtigungen einrichten

Eine **Quarantäne-Sammelbenachrichtigung** informiert über die Emails, die von der Avira AntiVir Exchange in die Quarantäne gestellt worden sind.

Sammelbenachrichtigungen können an verschiedenste Empfänger(-gruppen) gesendet werden und eine Liste verschiedenster Quarantäne-Emails enthalten. Welche Emails das sind, welche Aktion der Empfänger der Sammelbenachrichtigung für diese Emails starten kann und welche Zusatzinformationen die Sammelbenachrichtigung enthält, wird in jeder Sammelbenachrichtigung separat konfiguriert.

Jede Art der Benachrichtigungen besteht aus zwei Teilen:

- Aus der Vorlage, in der die Form der Sammelbenachrichtigung definiert wird. Die Vorlagen der Sammelbenachrichtigungen können unter **Basis-Einstellungen - Allgemeine Einstellungen - Vorlagen - Quarantäne Sammelbenachrichtigungen** bearbeitet werden. Die hier zu Verfügung stehenden Variablen sind ausschließlich an den Sammelbenachrichtigungen und deren Form related. Konfigurieren Sie die Quarantänen-Sammelbenachrichtigungsvorlage wie unter [Benachrichtigungsvorlagen erstellen](#) beschrieben.
- Aus einer Liste der in Quarantäne gestellten Emails (der eigentliche Inhalt der Sammelbenachrichtigung), in der mit Feldern definiert wird, welche Emails und Email-Felder in der erstellten Sammelbenachrichtigung aufgeführt werden sollen. Der Inhalt der Sammelbenachrichtigung wird durch die Variable **Sammelbenachrichtigung: Liste der Quarantäne-Mails** (`[VAR]HTMLList[/VAR]`) definiert, die in jeder Sammelbenachrichtigung ein Pflichteintrag ist. Welche Einträge diese Liste enthält, wird unter **Basis Einstellungen - Ordner - Quarantänen - Eigenschaften einer Quarantäne - Sammelbenachrichtigungen - Hinzufügen - Felder** definiert.

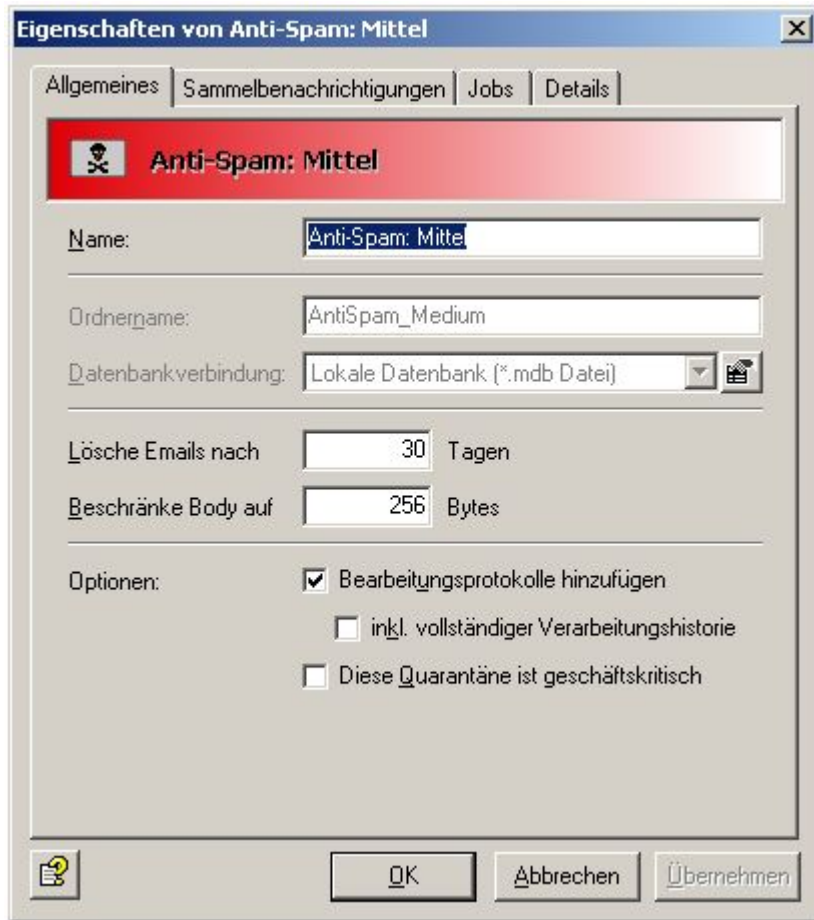
Die Variable **Sammelbenachrichtigung: Absender** unter **Vorlagen** bezeichnet den Absender der Sammelbenachrichtigung (der gleiche Absender wie für alle Avira AntiVir Exchange Benachrichtigungen und wird unter AntiVir Server-Einstellungen definiert). Die Checkbox für den **Absender** in der Registerkarte Felder in einer Quarantäne bezeichnet den Absender der in Quarantäne gestellten Emails, welcher innerhalb der Liste der Emails aufgeführt wird.

Sammelbenachrichtigungen sind insbesondere für Spam-Quarantänen und die Empfänger dieser Spam-Mails gedacht. Der Standardfall wird sein, dass die Anwender eine Liste aller neuen Spam-Mails erhalten, die an sie adressiert waren und die in einer bestimmten Spam-Quarantäne liegen. Dieser Standardfall wird wie folgt konfiguriert:

1. Öffnen Sie **Basis-Konfiguration - Ordner - Quarantänen**.



- Öffnen Sie im rechten Fenster die Spam-Quarantäne **Anti-Spam: Mittel** mit Doppelklick.



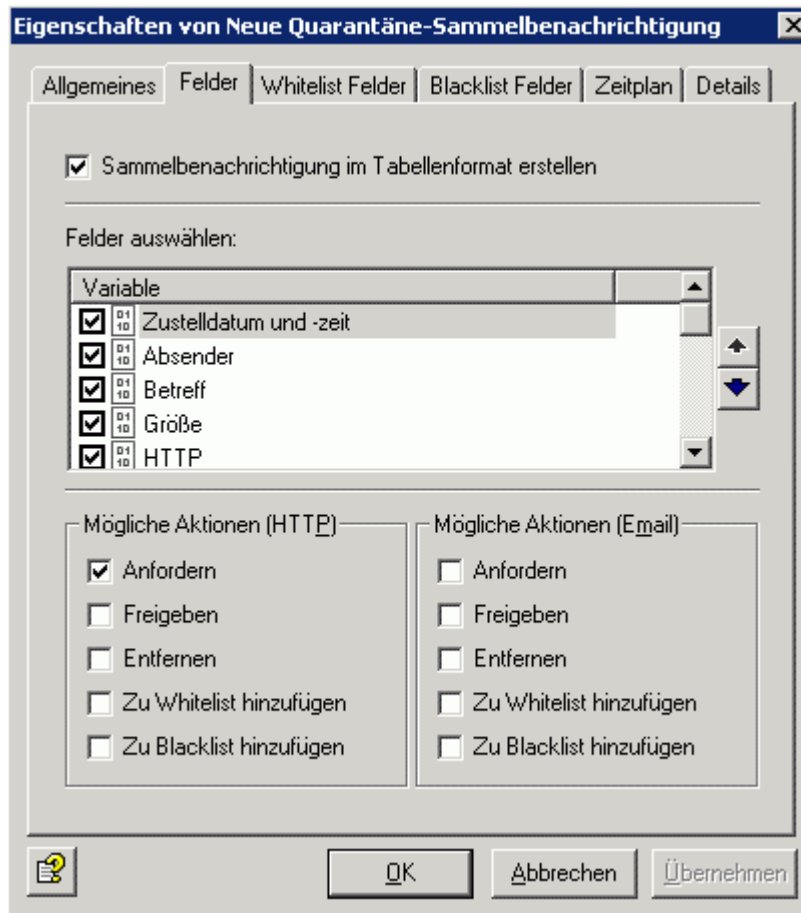
- Klicken Sie auf die Registerkarte **Sammelbenachrichtigungen**.
- Klicken Sie auf **Hinzufügen**.

5. Vergeben Sie auf der Registerkarte **Allgemeines** einen Namen für die Sammelbenachrichtigung.



6. Wählen Sie im Feld **Empfänger** den Eintrag **Alle Empfänger** aus. Empfänger der Sammelbenachrichtigung sind die ursprünglichen Empfänger der Quarantäne-E-mails. Wählen Sie **Benutzerdefinierte Empfänger** aus, wenn Sie z. B. die Gruppe von Empfängern einer Sammelbenachrichtigung einschränken wollen. Die ausgewählten Empfänger, Absender, Gruppen oder andere Adressmuster sind dann im unteren Textfeld aufgelistet.
7. Als **Vorlage** können Sie eine Sammelbenachrichtigung wählen, die Sie unter **Allgemeine Einstellungen - Vorlagen - Quarantäne-Sammelbenachrichtigungen** selbst definiert haben. Im Auslieferungszustand der Avira AntiVir Exchange ist die Vorlage **Quarantäne-Sammelbenachrichtigung** vorhanden, die bereits vorkonfigurierte Einstellungen enthält. Wenn Sie ihren Anwendern ermöglichen möchten, dass Sie aus der Sammelberechtigung heraus einen Absender auf seine Benutzer Whitelist setzen kann, verwenden Sie die Vorlage **Quarantäne-Sammelbenachrichtigung mit Whitelist-Unterstützung**.
8. Für die **Inhalte der Sammelbenachrichtigung** wählen Sie **Neue Mails**. Dadurch erhält der Empfänger der Sammelbenachrichtigung nur diejenigen Emails, die seit der letzten Sammelbenachrichtigung in der Quarantäne eingetroffen sind.
9. **Bearbeitung: nicht durch AntiVir Jobs** bearbeiten bedeutet, dass die erneut gesendete Email, die der Benutzer angefordert oder freigegeben hat, nicht mehr durch die aktiven AntiVir Jobs geprüft wird. Jede angeforderte oder freigegebene Email wird ungeprüft an die Empfänger zugestellt. Siehe hierzu auch die nächste Registerkarte **Felder**.

10. In der Registerkarte **Felder** wählen Sie aus, welche Felder aus den Quarantäne-E-mails in die Liste der Quarantäne-E-mails der Sammelbenachrichtigung geschrieben werden sollen. Markieren Sie hier beispielsweise die Checkbox **Betreff**, so wird der Betreff der Quarantäne-Email in der Email-Liste der Sammelbenachrichtigung aufgeführt. Für den Standardfall sind die entsprechenden Checkboxes bereits markiert.



Durch einen Klick auf die Links in der Benachrichtigung kann der Empfänger der Sammelbenachrichtigung eine Aktion mit der aufgeführten Email durchführen. Markieren Sie hier die Aktion, die der Anwender durchführen darf:

**Anfordern:** Die Email wird aus der Quarantäne an den Empfänger der Sammelbenachrichtigung zugestellt.

**Freigeben:** Die Email wird an alle ursprünglichen Empfänger der Email zugestellt.

**Entfernen:** Die Email wird in der Quarantäne zum Löschen vorgemerkt.

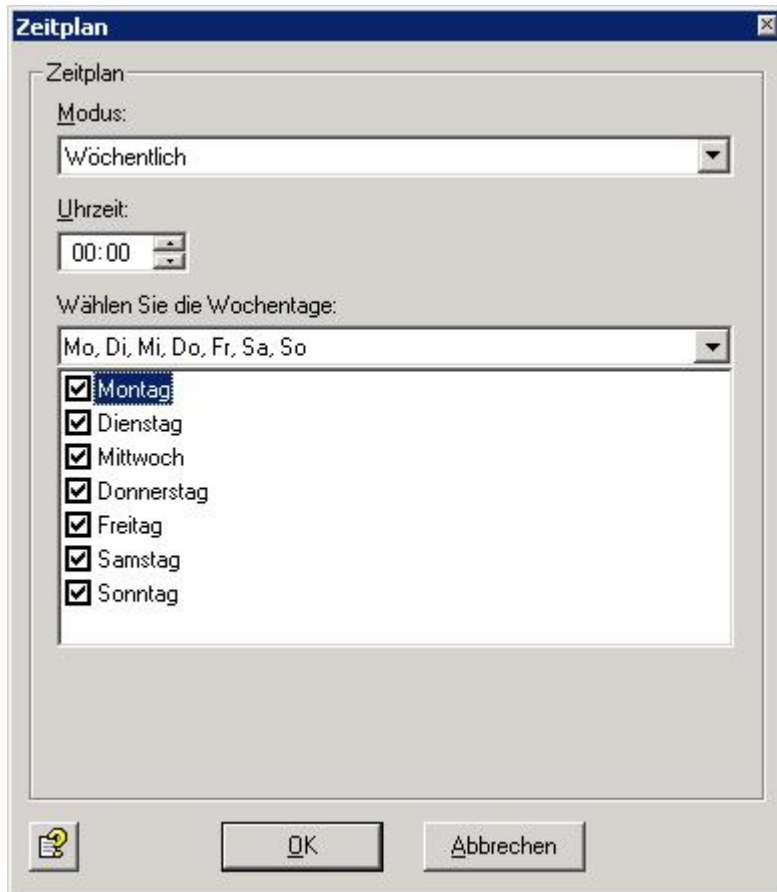
**Zu Whitelist hinzufügen:** Der Absender der Email wird in die Benutzer-Whitelist hinzugefügt.

**Zu Blacklist hinzufügen:** Der Absender der Email wird in die Benutzer-Blacklist hinzugefügt.

**Hinweis:** Wenn Sie mehrere Checkboxes aktiv setzen, so erscheinen in der Sammelbenachrichtigung mehrere Links an einer Email.

11. In der Registerkarte **Whitelist Felder** bzw. **Blacklist Felder** wählen Sie aus, welche Felder aus den Quarantäne-E-mails in die Whitelist bzw. Blacklist Benachrichtigung erscheinen sollen.

12. Klicken Sie auf die Registerkarte **Zeitplan** und dort auf **Hinzufügen**. Sie erhalten ein Zeitplan-Fenster, in dem Sie den Start der Sammelbenachrichtigungserstellung definieren. In diesem Fall wird jeden Tag um 0 Uhr eine Quarantäne-Sammelbenachrichtigung an die Empfänger der Spam-Mails erzeugt und gesendet.



13. Klicken Sie auf **OK**.

14. In der Registerkarte **Zeitplan** wird Ihre neue Quarantäne-Sammelbenachrichtigung jetzt angezeigt. Mit **Bearbeiten** ändern Sie die Zeit oder die Wochentage, mit **Entfernen** löschen Sie die Sammelbenachrichtigung:



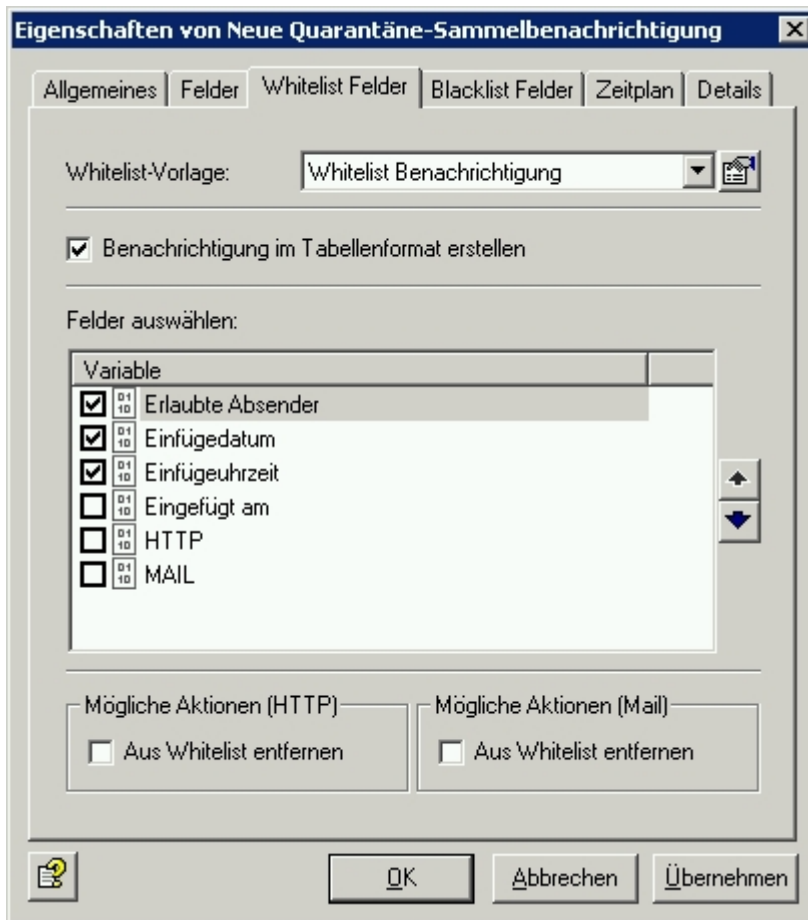
Ab sofort wird täglich um 0 Uhr eine Sammelbenachrichtigung an die Empfänger von Spam-Mails der **Quarantäne Anti-Spam: Mittel** gesendet.

**Hinweis:** Sie können für eine Quarantäne mehrere verschiedene Sammelbenachrichtigungen mit unterschiedlichem Inhalt erstellen. Die E-Mails werden für jede Sammelbenachrichtigung separat aus der Quarantäne "zusammengesucht", auch wenn der Zeitplan für diese Sammelbenachrichtigungen identisch ist.

**Hinweis:** Unter **Basis Einstellungen - Ordner - Quarantänen** erhalten Sie eine Liste aller Quarantänen. Anhand der Spalte Sammelbenachrichtigung erkennen Sie sofort, für welche Quarantänen eine Sammelbenachrichtigung konfiguriert ist (ja/nein).

### Whitelist Benachrichtigung

Wählen Sie für die Quarantäne-Sammelbenachrichtigung die Vorlage mit **Whitelist Unterstützung**, damit der Empfänger der Quarantäne-Sammelbenachrichtigung die Einträge in seine Whitelist verwalten und eine Whitelist Benachrichtigung anfordern kann.



Unter **Whitelist Felder** legen Sie die zu erscheinenden Felder fest.

Über **Whitelist-Vorlage** bearbeiten Sie die vorhandene Whitelist Vorlage oder legen Sie eine neue an. Konfigurieren Sie die Whitelist-Vorlage mit den Variablen wie unter [Liste der Benachrichtigungsvariablen](#) beschrieben.

### 4.3.9 Utility-Einstellungen

#### Fingerprints

Fingerprints werden von AntiVir zur Dateityperkennung benutzt. Wir liefern eine umfangreiche Liste von Fingerprints in der Avira AntiVir Exchange mit aus, die in Kategorien eingeteilt sind. Im Regelfall ist es zunächst nicht nötig, Veränderungen vorzunehmen. Nähere Informationen über die Konfiguration von Fingerprints finden Sie in [Fingerprints konfigurieren](#).

#### Wortlisten

Hier können Sie Wortlisten erstellen, die Textfolgen enthalten, die Sie bei der Inhalts- und Spamprüfung mit AntiVir Wall verbieten möchten. Wir liefern einige Wortlistenkategorien aus, die Sie an Ihre Bedürfnisse anpassen können. Die genaue Konfiguration der Wortlisten finden Sie in [Wortlisten einrichten](#).

#### AntiVir Such Engine

Nähere Informationen zur Konfiguration der Virens Scanner entnehmen Sie dem Kapitel [AntiVir Such Engine konfigurieren und aktivieren](#).

### 4.4 Richtlinien-Konfiguration

In der Richtlinien-Konfiguration definieren Sie Ihre AntiVir Jobs basierend auf firmeneigenen Richtlinien.

Anhand unterschiedlicher Bedingungen (oder auch Filter) können Sie festlegen, welche Emails überhaupt betroffen sind, wann welche Aktion ausgeführt werden soll und in welcher Reihenfolge die Jobs abgearbeitet werden sollen (Priorität). Alle Bedingungen können innerhalb der Jobs konfiguriert werden. Die Summe der AntiVir Jobs ergibt die Unternehmensrichtlinien (Policy).

#### 4.4.1 Beispiel einer Unternehmensrichtlinie

Jede eingehende Spam-Mail soll erkannt, gelöscht oder in die Quarantäne verschoben werden.

Die Spam-Mails sollen den Empfänger zwar nicht erreichen, er soll aber darüber informiert werden, dass und welche Spams für ihn eingegangen sind, damit er selbst entscheiden kann, welche dieser Emails ihm doch zugestellt werden sollen.

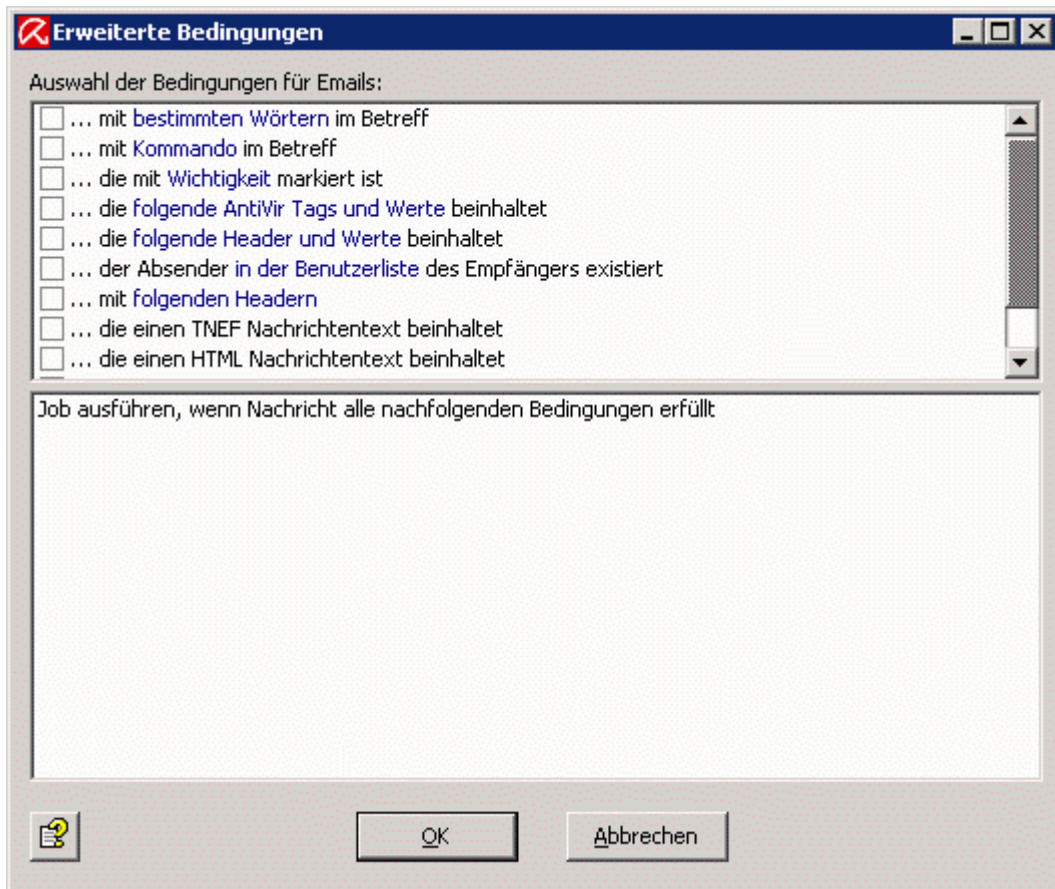
Dies sollte mittels einer Zusammenfassung geschehen, die einmal täglich versendet werden soll.

Das alles können Sie in den **Wall Spam Filtering** Jobs einrichten.

#### 4.4.2 Bedingungen

In jedem Job können Sie Voraussetzungen festlegen, die Emails aufweisen müssen, damit ein Job ausgeführt wird. Die Bedingungsparameter legen Sie gemäß Ihren Anforderungen selbst fest:

Nur wenn alle Voraussetzungen für eine versendete oder eintreffende Email gültig sind, wird eine Job-Verarbeitung initiiert, z.B. auf Viren geprüft.



**Warnung:** Die inhaltlichen Bedingungen müssen gleichzeitig mit den definierten Adressbedingungen in der Registerkarte **Adressen** zutreffen, damit der Job ausgeführt wird (UND-Verknüpfung).

Über den Wert von vorhandenen X-Headern kann die Email-Verarbeitung gesteuert werden. Externe Applikationen, welche die Emails vor der Verarbeitung durch Avira AntiVir Exchange verarbeiten, können z.B. bestimmte X-Header-Felder mit definierten Werten in die Emails schreiben. Nachfolgende AntiVir-Jobs können mithilfe der Bedingung ... **die folgenden Header und Werte beinhalten** so konfiguriert werden, dass in Abhängigkeit des Wertes eines X-Header-Feldes eine Job-Verarbeitung initiiert wird.

#### 4.4.3 Jobtypen

Es gibt 9 unterschiedliche Jobtypen, die Sie unter **Richtlinien-Konfiguration - Mail Transport Jobs - rechte Maustaste - Neu** finden können:

Jobtyp	Bedeutung
AntiVir Suche	Job prüft die Emails auf Viren.
AntiVir E-Mail Size Filtering	Job prüft die Emails auf eine maximal zugelassene Größe (Angabe pro E-Mail).



AntiVir Attachment Filtering	Job prüft die Emails auf verbotene Dateianhänge. Die verschiedenen Dateiformate werden durch Fingerprints identifiziert.
AntiVir Attachment/Size Filtering	Job prüft die Emails auf verbotene Dateianhänge. Gleichzeitig kann die maximal zugelassene Größe eines Anhangs angegeben werden.
AntiVir Protected Attachment Detection	Der Job reagiert auf Emails mit passwortgeschützten Archiven und führt die in der Registerkarte Aktionen konfigurierten Jobaktionen aus. Dadurch können passwortgeschützte Archive regelbasiert behandelt werden.
AntiVir Wall Content Filtering	Job prüft Emails und Anhänge auf verbotenen Textinhalt.
AntiVir Wall Email Address Filtering	Job prüft die Emails auf Adresseinschränkungen
AntiVir Wall Recipient Limit Filtering	Job prüft die Emails auf eine maximal zulässige Anzahl der Empfänger pro Email (Gezählt werden die Empfänger im „to“-Feld einer Email).
AntiVir Wall Spam Filtering	Job prüft Emails mittels verschiedener Kriterien auf Spam.

Für jeden Jobtyp können Sie eigene Bedingungen definieren, die alle zutreffen müssen, bevor eine definierte Aktion ausgeführt wird. Adressenfilter können bei allen Jobtypen konfiguriert werden. Sie können z.B. einen Job mit den Bedingungen erstellen, alle Emails, die von den Domänen *\*@gmx.net* und *\*@hotmail.com* gesendet werden, größer als 500 KB sind, in welchen der Betreff das Wort "Look" enthält und der Fingerprintkategorie Sound angehören, zu löschen (und damit dem Empfänger nicht zuzustellen!) und eine Kopie davon in die Quarantäne zu stellen. Dieser Fall wäre ein **AntiVir Attachment/Size Filtering** Job.

Im Lieferumfang der Avira AntiVir Exchange ist eine Reihe von Standardjobs enthalten, die Sie für Ihre Bedürfnisse ändern können. Selbstverständlich sind auch eigene möglich. Sie finden die vorkonfigurierten Jobs unter **Richtlinien-Konfiguration - Jobvorlagen**. Ziehen Sie den gewünschten Job mit der Maus in **Mail Transport Jobs**. Es lassen sich beliebig viele Jobs anlegen. Die Reihenfolge der Abarbeitung entnehmen Sie in **Mail Transport Jobs** aus der Anordnung in der Liste aller Jobs. Nähere Informationen erhalten Sie unter [Verarbeitungsreihenfolge der Jobs](#).

Ein Job kann aktiv oder inaktiv sein. Ein inaktiver Job ist zwar in der Konfiguration vorhanden, kommt aber nicht zur Ausführung. Sie müssen also Ihre Jobs nicht endgültig aus der Konfiguration löschen, wenn Sie diese deaktivieren wollen.

In jedem Job können Sie unter der Registerkarte **Aktionen** einstellen, welche Aktionen zur Ausführung kommen sollen, wenn eine Email unter die definierten Bedingungen fällt oder mit einem Virus verseucht ist.



#### 4.4.4 Aktionen

Zusätzlich zu den Aktionen, die zur Funktion eines Jobs gehören, stehen Ihnen folgende Standard-Aktionen zur Verfügung:

Aktion	Bedeutung
Kopiere in Quarantäne	Eine Kopie der Email wird in den von Ihnen angegebenen Quarantäne-Ordner gestellt, wo sie jederzeit eingesehen werden kann.
Lösche Email	Die infizierte/verbotene Original-Email wird endgültig vom Server gelöscht (die Kopie befindet sich in der Quarantäne, wenn die Option gesetzt ist).
Lösche Anhang	Die infizierten Anhänge werden endgültig vom Server gelöscht.
Zusatz im Betreff	Die Betreffzeile wird durch einen konfigurierbaren Zusatz ergänzt. Damit kann der Empfänger diese Email als bearbeitet identifizieren.
Sende Benachrichtigungen an	Benachrichtigungen können an folgende Personenkreise gesendet werden: <ul style="list-style-type: none"> <li>• Administratoren</li> <li>• Absender</li> <li>• Empfänger</li> <li>• Andere Personen</li> </ul>
Starte externe Anwendung	Eine externe, frei wählbare Anwendung wird ausgeführt.
X-Header Feld hinzufügen	Es wird im Header der Email ein Feld hinzugefügt, welches mit einem Wert aus den Variablen gefüllt werden kann.
Email umleiten	Die Email wird an die angegebenen Empfänger umgeleitet. Option: Original-Empfänger erhalten die E-Mail zusätzlich.

#### 4.4.5 Verarbeitungsreihenfolge der Jobs

Die Verarbeitungsreihenfolge eines Jobs wird in der Ansicht aller Jobs in der **Richtlinien-Konfiguration - Mail Transport Jobs** angezeigt.

Neue Jobs werden am Ende der Liste hinzugefügt und können mit den Pfeiltasten  und  in der Symbolleiste oder mit rechter Maustaste (**Alle Aufgaben - Nach oben/Nach unten**) in die gewünschte Position gebracht werden.

### 4.5 AntiVir Monitor

Mit dem AntiVir Monitor können Sie die Quarantäne-Bereiche auf jedem verfügbaren Server einsehen und erhalten detaillierte Informationen über die dort enthaltenen Emails.

Im AntiVir Monitor beobachten Sie alle **Avira AntiVir Exchange Server, Quarantänen** und **Bad-Mails**. Außerdem haben Sie hier Zugriff auf die **Statistik Auswertungen**.

Im AntiVir Monitor werden alle Server aufgeführt, die unter **Basis-Konfiguration - AntiVir Server** konfiguriert sind. Der AntiVir Monitor greift mit SOAP/SSLVerschlüsselung über das Netzwerk auf die Server zu.

Um auf einen Server zugreifen zu können, tragen Sie ihn zunächst unter **Basis-Konfiguration - AntiVir Server** ein und aktualisieren Sie den **AntiVir Monitor** in der Ansicht.



Die Vorgehensweise für das Hinzufügen eines Servers entnehmen Sie bitte der Beschreibung [Einstellungen für einen einzelnen AntiVir Server](#). Außerdem sollte die Konfiguration der Quarantäne gemäß der Beschreibung des Kapitels [Quarantäne konfigurieren](#) entsprechen.

Für jeden Server können Sie sich u.a. umfassende Informationen über die AntiVir Version, die Konfiguration anzeigen lassen. Klicken Sie im **AntiVir Monitor** mit der rechten Maustaste auf den gewünschten Server und wählen Sie **Eigenschaften**.

Der AntiVir Monitor erfordert eine Anmeldung als autorisierter Benutzer. Sollten Sie nicht lokal auf dem Server angemeldet sein, erscheint ein Anmeldedialog, in dem Sie Ihren Benutzernamen und das Passwort für die entsprechende Domäne angeben. Die Berechtigung für den AntiVir Monitor-Zugriff wird in den Eigenschaften der Datei access.acl im Ordner ...\*Avira*\Avira *AntiVir Exchange*\AppData\ eingetragen.

Klicken Sie auf die Registerkarte **Sicherheit** und geben Sie den gewünschten Benutzern mindestens einen Lesezugriff.

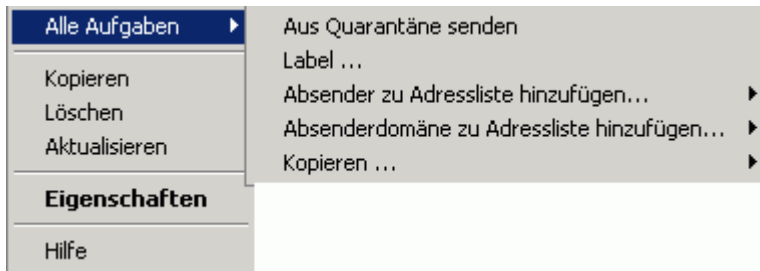
Beobachtung der Daten im AntiVir Monitor:

1. Klicken Sie auf den gewünschten Server.
2. Authentifizieren Sie sich mit einem Benutzernamen und Passwort, der auf dem Dateisystem des Servers Berechtigungen für die AntiVir Daten besitzt.
3. Klicken Sie in den Bereich, den Sie einsehen wollen, also beispielsweise auf Standard-Quarantäne oder Badmail. Alle vorhandenen Emails werden angezeigt (Anzeigegrenze 10.000 Emails).
4. Filtern Sie die gewünschten Emails mit dem **Filteroptionen-Icon**  **aus**.
5. Öffnen Sie eine Email mit einem Doppelklick.
6. Versenden Sie die Email mit  bei Bedarf erneut.

#### 4.5.1 Quarantänen


Wenn Sie im Job die Aktion **Kopie in Quarantäne** aktiviert haben, befinden sich alle betroffenen Emails in einer Quarantäne und Sie erhalten im AntiVir Monitor alle verfügbaren Informationen über die einzelnen Emails.

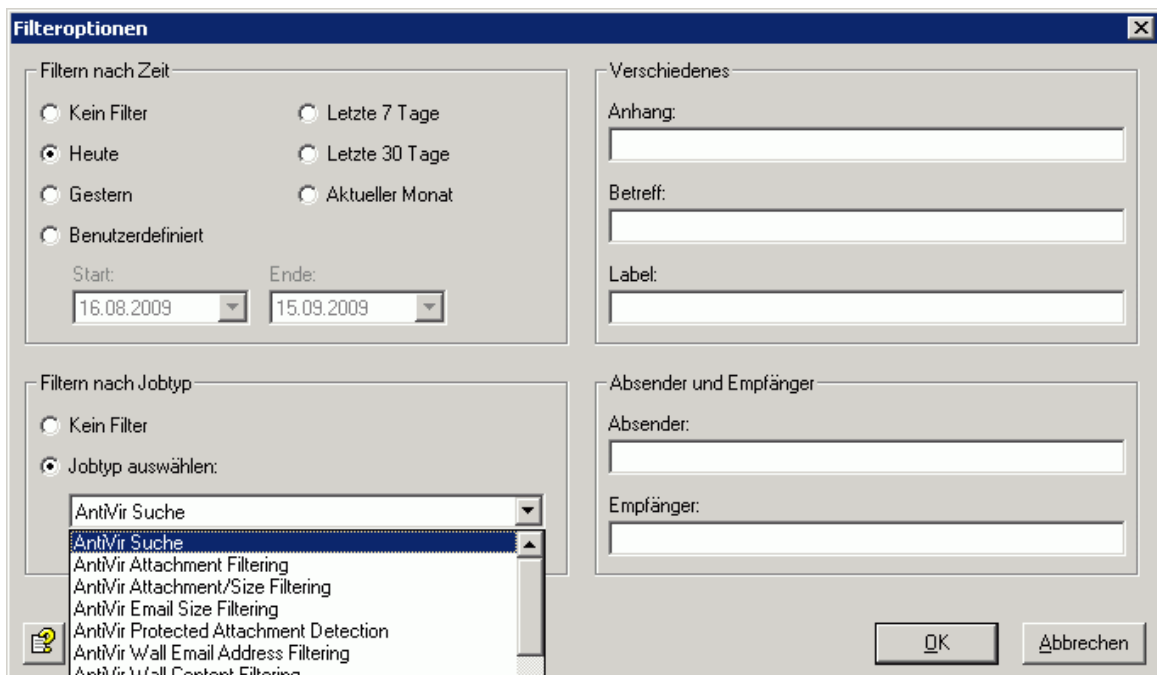
Klicken Sie auf eine Quarantäne. Wenn Sie mit der rechten Maustaste eine Email auswählen, stehen Ihnen in der Ansicht folgende Aktionen zur Verfügung:




Kopieren ist auch per Drag-and-Drop möglich. Ziehen Sie die ausgewählte Email mit der Maus in eine andere Quarantäne.

Innerhalb einer Quarantäne ist es möglich, die Emails nach etlichen Auswahlkriterien zu filtern.

Klicken Sie dazu mit der rechten Maustaste auf **Ansicht - Filteroptionen** oder auf das Icon . Sie erhalten folgenden Dialog:



Wollen Sie die Optionen wieder zurücksetzen, haben Sie drei Möglichkeiten:

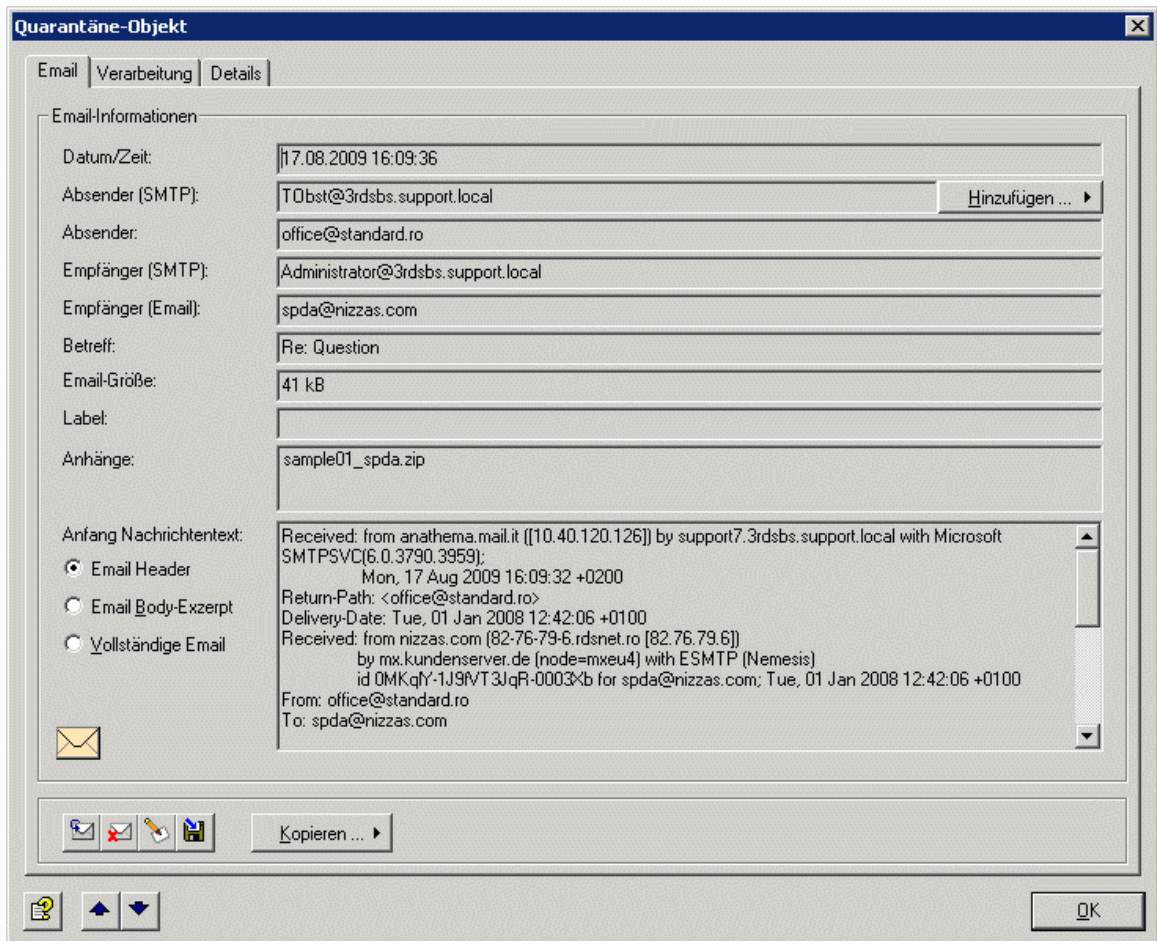
1. Aktivieren Sie die Option **Kein Filter** in Filteroptionen.
2. Klicken Sie mit der rechten Maustaste auf **Ansicht - Alle Objekte anzeigen**.
3. Benutzen Sie das Icon  in der Symbolleiste.

In der Ansicht im AntiVir Monitor werden maximal 10.000 Emails auf einmal angezeigt (die neuesten). Ältere Emails, die nicht mehr mit aufgeführt werden, erhalten Sie durch einschränken der Ansicht mit einer entsprechenden Filteroption.








## Beispiel einer Email in der Quarantäne

Diese Informationen erhalten Sie, wenn Sie mit einem Doppelklick oder der rechten Maustaste die Eigenschaften der Email in der Quarantäne aufrufen.

Unter der Registerkarte Email finden Sie das Wichtigste auf einen Blick:



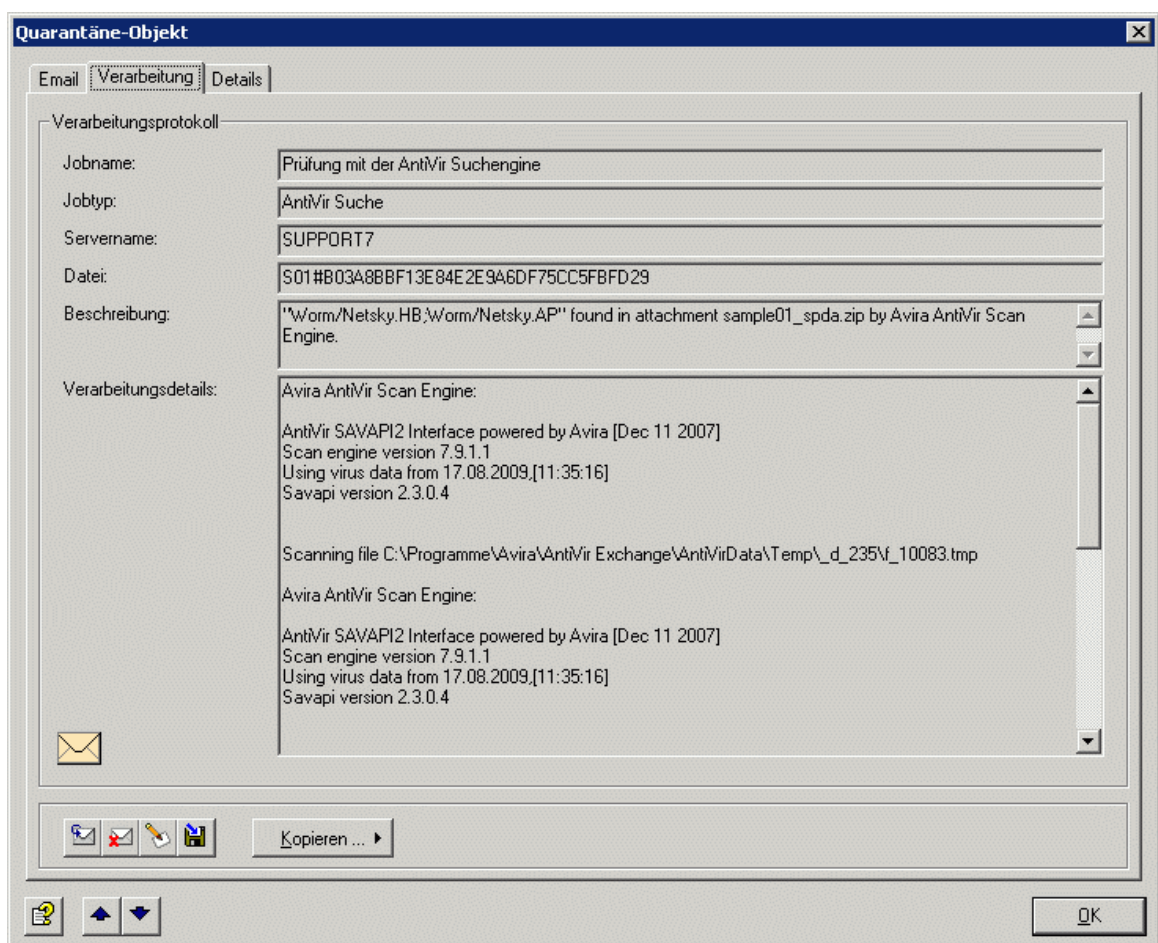
Die auf diesen Registerkarten verwendeten Icons:

	Email aus Quarantäne senden
	Email in Quarantäne löschen
	Label für die Email festlegen, ändern, löschen
	Email speichern unter
	Online-Hilfe öffnen
	Nächste Email in der Quarantäne/Badmail
	Vorherige Email in der Quarantäne/Badmail

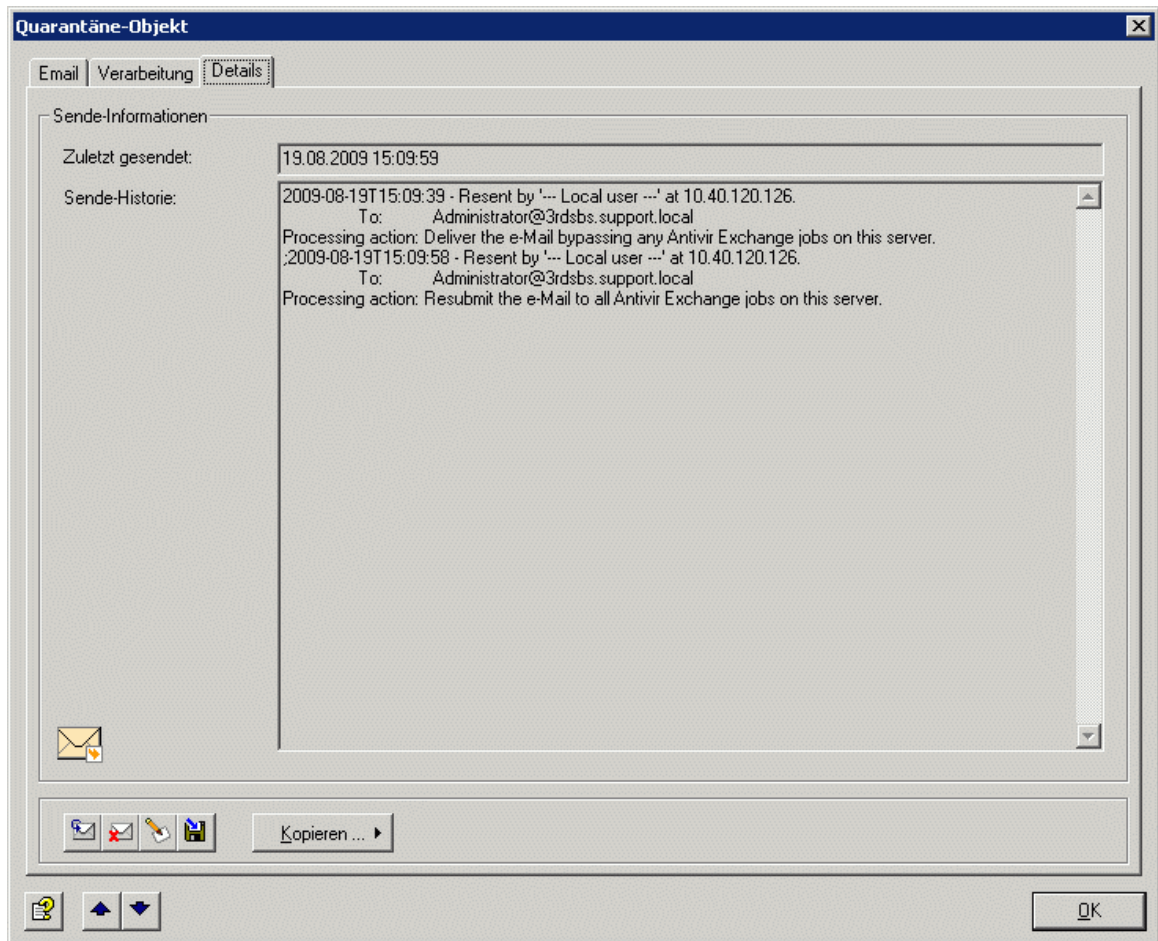
Die Schaltfläche **Hinzufügen** ermöglicht es, den SMTP-Absender der Email zur Spam-Abwehr einer bestimmten Adressliste hinzuzufügen. Welche Adresslisten unter dieser Schaltfläche angezeigt werden, definieren Sie für jede einzelne Adressliste. Siehe hierzu [Adresslisten](#). Sobald die Absenderadresse der Adressliste hinzugefügt worden ist, erhalten Sie eine Meldung:



Unter **Verarbeitung** erfahren Sie den Namen des Jobs, der die Email in die Quarantäne abgelegt hat, den Jobtyp, den Server, warum die Email unter die Einschränkungen fiel und in die Quarantäne gestellt wurde und weitere Verarbeitungsdetails:



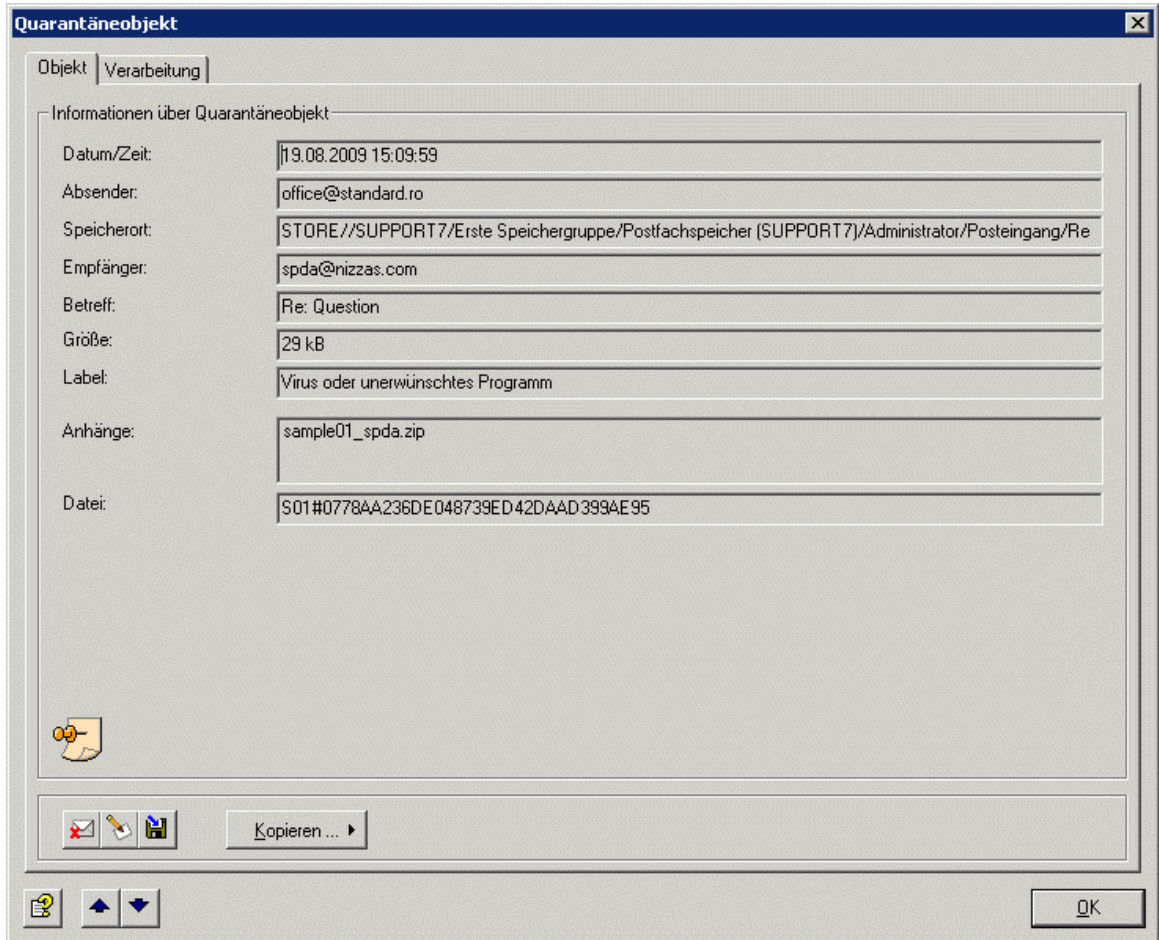
Unter **Details** erhalten Sie den Verlauf des erneuten Sendens aus der Quarantäne.



### Beispiel einer Email in der Informationsspeicher-Quarantäne

Diese Informationen erhalten Sie, wenn Sie mit einem Doppelklick oder der rechten Maustaste die **Eigenschaften** der Mail in der Informationsspeicher-Quarantäne aufrufen.

Unter der Registerkarte **Objekt** finden Sie das Wichtigste auf einen Blick:



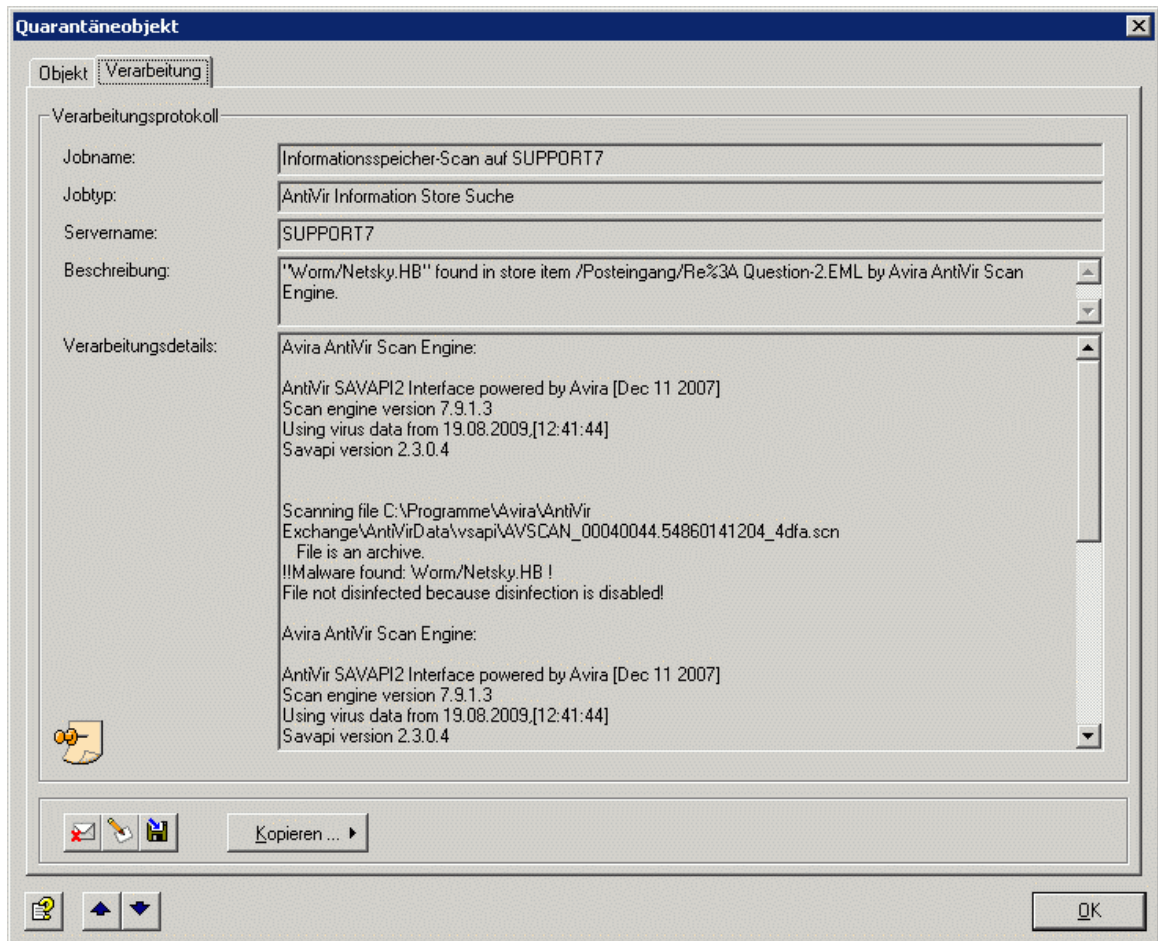
Die auf diesen Registerkarten verwendeten Icons:

	Objekt in Quarantäne löschen
	Label für das Objekt festlegen, ändern, löschen
	Objekt im Dateisystem speichern
	Nächstes Objekt in der Quarantäne
	Vorheriges Objekt in der Quarantäne

Die Schaltfläche **Kopieren** ermöglicht es, das Objekt in eine andere auf diesem Server vorhandene Quarantäne zu kopieren.

Die nächste Registerkarte **Verarbeitung** zeigt den Namen des Jobs, der die Email in die Quarantäne abgelegt hat, den Jobtyp, den Server, warum das Objekt unter die Einschränkungen fiel und in die Quarantäne gestellt wurde und weitere Verarbeitungsdetails:






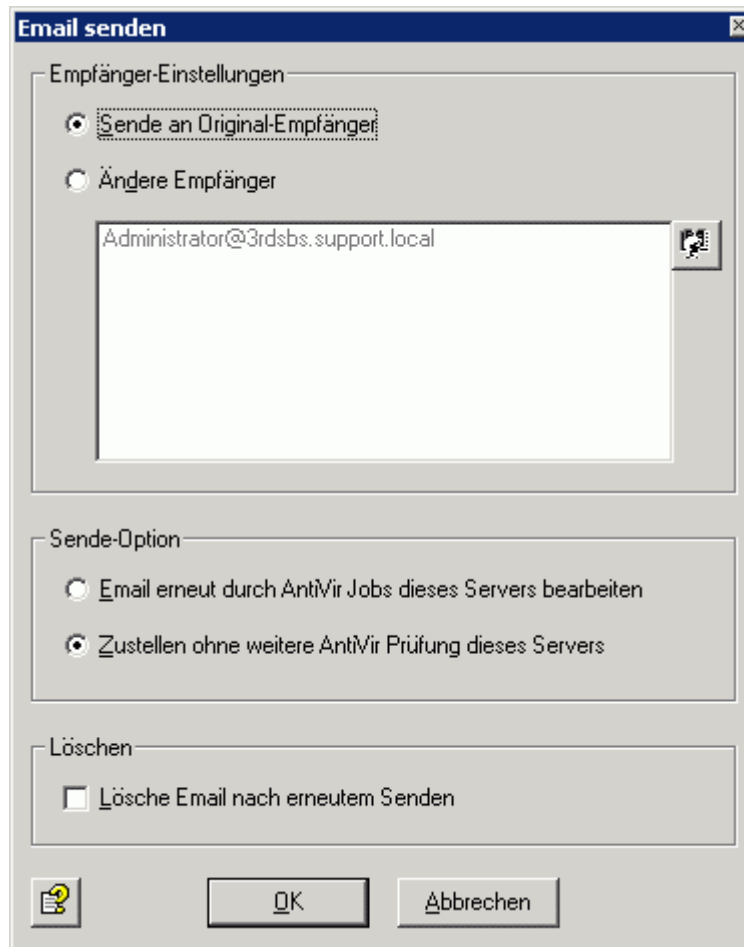
### Aus Quarantäne senden

Wenn Sie eine Email aus der Quarantäne wieder seinem ursprünglichen oder einem weiteren Empfänger zukommen lassen möchten, können Sie diese direkt aus der Quarantäne versenden, ohne dass sie erneut von einem Avira AntiVir Exchange Job geprüft wird:


1. Öffnen Sie eine Liste von Emails einer Quarantäne im AntiVir Monitor.
2. Wählen Sie die gewünschte Email mit der rechten Maustaste aus und aktivieren Sie nun **Alle Aufgaben - Aus Quarantäne senden**.

**Hinweis:** Alternativ können Sie die Email auch direkt aus dem Eigenschaften-Fenster versenden, indem Sie auf das Icon  klicken.

Sie erhalten folgenden Dialog:



Der Empfänger sieht im "Von"-Feld den Original-Absender der Email (keine Weiterleitungsmail).

3. Sie können den Empfänger ändern, indem Sie die Option **Ändere Empfänger** aktivieren und dann auf das Symbol für **Adresse auswählen** klicken: .

**Hinweis:** Bei der Auswahl der Adressen für das erneute Versenden aus der Quarantäne stehen keine Adresslisten zur Verfügung. Näheres zu Adresslisten siehe [Adresslisten](#).

4. Wenn Sie die Email nicht mehr durch die Jobs bearbeiten lassen möchten, so aktivieren Sie die Option **Zustellen ohne weitere AntiVir Prüfung dieses Servers**.

Das wird der Regelfall sein, wenn Sie eine Email aus der Quarantäne wieder zustellen lassen, weil ein Benutzer diese Email trotz z.B. verbotener Wörter oder Anhängen dringend braucht.

**Hinweis:** Es handelt sich hier um eine übergreifende Einstellung. Sollten Sie Jobs aktiviert haben, die auch erneut gesendete Emails aus der Quarantäne prüfen sollen, so setzen Sie diese Einstellung auf **Email erneut durch AntiVir Jobs bearbeiten lassen**, ansonsten greift die Jobeinstellung **Vor Versand prüfen** nicht und es werden alle Emails unbearbeitet weitergesendet.

**Hinweis:** Die Anweisung **Email erneut durch AntiVir Jobs bearbeiten lassen** gilt auch nur für diejenigen Jobs, bei denen die Option **Mails aus Quarantäne: Vor Versand prüfen** aktiviert worden ist! Selbst wenn Sie also die Quarantäne-Emails erneut bearbeiten lassen wollen, werden alle Jobs ausgeklammert, bei denen **Ohne Prüfung versenden** aktiviert ist.

### Absender einer Adressliste hinzufügen

Wenn die Email eines Absenders in Quarantäne gestellt wurde, dessen Emails aber zukünftig als erwünscht erkannt werden sollen, können Sie den Absender auf eine ihrer Adresslisten setzen, z.B. Anti-Spam: Whitelist:

1. Öffnen Sie im AntiVir Monitor die Quarantäne, welche die erwünschte Email enthält.
2. Wählen Sie die Email mit der rechten Maustaste aus und aktivieren Sie nun **Alle Tasks - Absender zu Adressliste hinzufügen**.
3. Selektieren Sie die Adressliste in die der Absender aufgenommen werden soll.

Wenn Sie dafür sorgen möchten, dass zukünftig alle Absender einer bestimmten Domäne als erwünscht erkannt werden und regulär in das Email-Postfach der Anwender gelangen, gehen Sie nach dem selben Prinzip vor, selektieren aber die Option **Maildomäne zu Adressliste hinzufügen**. So müssen bei mehreren Email-Absendern einer Maildomäne, z.B. bei einem Kundenunternehmen, nicht alle Absenderadressen einzeln in die Adressliste eingetragen werden. Die Adresse wird in Form von \*@beispielunternehmen.com in die Liste eingetragen.

**Hinweis:** In beiden Fällen muss innerhalb der Adressliste das Feld **Adressen dürfen aus Quarantäne hinzugefügt werden** aktiviert sein. Anderenfalls kann die gewünschte Absenderadresse der Liste nicht hinzugefügt werden!

### Bad-Mails

Bad-Mails sind alle Emails, die durch die AntiVir Jobs nicht bearbeitet werden konnten, wie beispielsweise Emails mit nicht verarbeitbaren Formaten. Über Bad-Mails existieren sehr wenig Informationen, da die AntiVir keine Einsicht in diese Emails nehmen konnte. Diese Emails können also auch einen unentdeckten Virus enthalten.

Für Bad-Mails existiert auf jedem Server nur ein Ordner. Es können auch keine weiteren Ordner angelegt werden. Ansonsten gelten für Bad-Mails die gleichen Funktionen und Optionen wie für Quarantäne-Mails.

### 4.5.2 Avira AntiVir Exchange Reports


Mit Hilfe der Report- und Statistik-Funktion der Avira AntiVir Exchange können detaillierte Informationen über die Email-Verarbeitung abgerufen werden.

Es stehen sieben vordefinierte und ein erweiterter Statistik Report zur Verfügung.

Der erweiterte Statistik Report kann individuell definiert werden. Die Reports sind über den AntiVir Monitor erreichbar. Die einzelnen Reports beinhalten sowohl die graphische Darstellung von erkannten Richtlinienverletzungen (z.B. Viren, unerwünschte Dateianhänge) als auch tabellarische Informationen. Zu den gängigsten Fragestellungen steht ein eigener Report bereit. Darüber hinaus werden Daten zu AntiVir Quarantänen dargestellt.

Die Reports können für frei definierbare Zeiträume erstellt werden. Umfangreiche Druck- und Exportfunktionalitäten ermöglichen die einfache Weiterverwendung der Report-Daten.

Die Report-Daten werden während der Verarbeitung zwischengespeichert und zwei Mal pro Stunde in die Auswertungsdatenbank geschrieben. Bearbeitete Emails erscheinen daher in der Regel nicht sofort in den Reports.

Klicken Sie auf **AntiVir Reports** und öffnen Sie den gewünschten Report im rechten Fenster mit einem Doppelklick. Im nun erscheinenden neuen Fenster geben Sie den gewünschten Zeitraum für den Report ein. Mit  exportieren Sie die Auswertung für den Import in eine andere Anwendung, wobei Sie unter verschiedenen Formaten wählen können.

# 5 AntiVir Such Engine

## 5.1 Übersicht

Mit AntiVir überprüfen Sie die Emails auf Viren, auf Typ und Größe eines Anhangs und auf die Gesamt-Email-Größe.

### 5.1.1 Jobtypen

- Virenprüfung ein- und ausgehender Emails  
Typ: **AntiVir Suche**
- Virus scanning in MS Exchange databases (on access & proactive/background)  
Typ: **Informationsspeicher-Scan**
- Sperren von bestimmten Dateitypen im Anhang  
Typ: **AntiVir Attachment Filtering**
- Beschränkung der Email-Größe  
Typ: **AntiVir Email Size Filtering**
- Beschränkung von Typ und/oder Größe der Anhänge  
Typ: **AntiVir Attachment/ Size Filtering**

**Hinweis:** Legen Sie für jeden Einschränkungstyp einen separaten Job an! Die Jobtypen lassen sich später nicht mehr ändern.

Die genaue Vorgehensweise entnehmen Sie bitte den Beschreibungen [Virenprüfung einschalten - Jobbeispiel](#).

## 5.2 AntiVir Suche

Den Virenschanner können Sie unter **Basis-Konfiguration - Utility-Einstellungen - AntiVir Engine - Avira AntiVir Scan Engine - Eigenschaften** konfigurieren.

Der **AntiVir Suche** Job startet gemäß der konfigurierten Bedingungen den Virenschanner. Die Bedingungen bestimmen, für welche E-Mails ein Job ausgeführt wird.

Folgendes Beispiel illustriert die Vorgehensweise eines Jobs für die Virenprüfung: Der Job prüft eine Email mit dem Ergebnis: Virus gefunden. Daraufhin wird Virenalarm ausgelöst und eine Reihe von Aktionen in Gang gesetzt, die Sie selbst unter **Aktionen** definieren können.

Sie können z. B. Folgendes festlegen:

1. Wenn ein Virus gefunden wird, soll die Originalmail gereinigt und dann dem Empfänger zugestellt werden.
2. Wenn die Originalmail nicht gereinigt werden kann, wird die betroffene Email in den von Ihnen gewählten Ordner (Quarantäne) kopiert, das Original gelöscht und nicht zugestellt.
3. In diesem Fall werden Nachrichten an Administrator, Absender und Empfänger erstellt, die mit den relevanten Informationen des Virenschanners und AntiVir Job versehen sind.

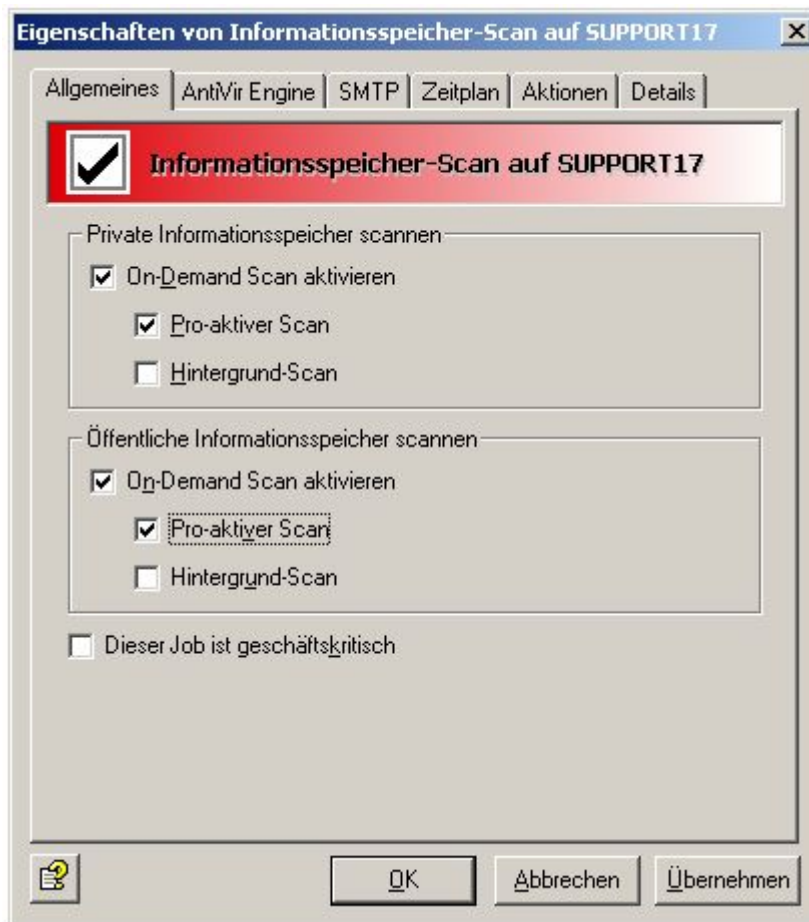
Diese Aktionen sind möglich:

- Auf Viren prüfen
- Von Viren reinigen
- Zusatz im Betreff
- Gesamte Email in Quarantäne kopieren
- Betroffene Anhänge aus Email entfernen
- Betroffene Email löschen und nicht zustellen
- Ausführen einer externen Anwendung
- Administrator, Absender, und/oder Empfänger benachrichtigen
- Andere, frei wählbare Personen benachrichtigen
- X-Header-Feld hinzufügen
- Email umleiten

### 5.3 Informationsspeicher-Scan

Neben der Virenprüfung auf Transportebene ist Avira AntiVir Exchange auch in der Lage, Daten im öffentlichen oder privaten Informationsspeicher von MS Exchange zu prüfen. Diese Prüfung bezieht nicht auf den ein- oder ausgehenden Mailverkehr, sondern auf die auf dem Server vorhandenen Maildateien bzw. solche, die nicht mit dem Transport Agent in Berührung kommen oder gekommen sind, z.B. Entwürfe.

Mit dem Informationsspeicher-Scan werden 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 Virens Scanner übermittelt. Der On-Demand Scan ist die am häufigsten gewählte Option des Informationsspeicher-Scans.
- **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 Virens Scanner-Signaturdatei noch nicht geprüft wurden.

Neben der zeitgesteuerten Überprüfung wird der Hintergrund-Scan auch immer beim Laden der Datenbanken (z. B. Start des Servers) ausgeführt.

Beim Informationsspeicher-Scan handelt es sich um eine serverweite Einstellung. Daher steht für jeden Server immer nur ein Informationsspeicher-Scan Job zur Verfügung, und nicht beliebig viele wie beim AntiVir Scanning.

Wird in einer Nachricht ein Virus gefunden, lassen sich verschiedene Aktionen durchführen, die speziell auf den Informationsspeicher-Scan abgestimmt sind:

- **Objekt blocken:** Das Blockieren verbietet den Zugriff auf das gesamte Nachrichtenobjekt. Bei aktuellen Microsoft Email Clients wird beim Versuch, eine solche Nachricht zu öffnen, eine entsprechende Meldung generiert. Bei anderen/älteren Email-Clients kann es zu unterschiedlichen Rückmeldungen kommen. Die blockierten Nachrichten können allerdings jederzeit über den Client gelöscht werden.
- **Ersetzen durch:** Das Ersetzen tauscht das virulente Element der Nachricht (z. B. Dateianhang) durch einen Textvermerk aus. Das virulente Element wird gelöscht.
- **Markiere als nicht betroffen:** In Ausnahmefällen kann entschieden werden, dass bei einem gefundenen Virus das entsprechende Element nicht als virulent markiert wird. Nachfolgende Virenprüfungen werden das Element dann wiederum als virulent erkennen. Diese Aktion ist nur in Testumgebungen sinnvoll, da hier kein Schutz des Anwenders gewährleistet ist.

---

**Hinweis:** Die Virenprüfung des MS Exchange Informationsspeichers erfolgt über die Microsoft Virus Scanning API 2.0/2.5. Weitere Informationen hierzu finden Sie unter <http://support.microsoft.com/kb/285667/DE/>

---

---

**Warnung:** Bei Nachrichten, die durch den Informationsspeicher-Scan blockiert werden, kann es zu Fehlermeldungen bei Datensicherungen des Informationsspeichers kommen.

---

---

**Warnung:** Das Beenden oder Deinstallieren von Avira AntiVir Exchange sowie das Anhalten des Informationsspeicher-Scan-Jobs deaktiviert nicht nur den aktiven Virenschutz des Informationsspeichers, sondern hebt auch die oben angesprochene Blockierung virulenter Inhalte auf.

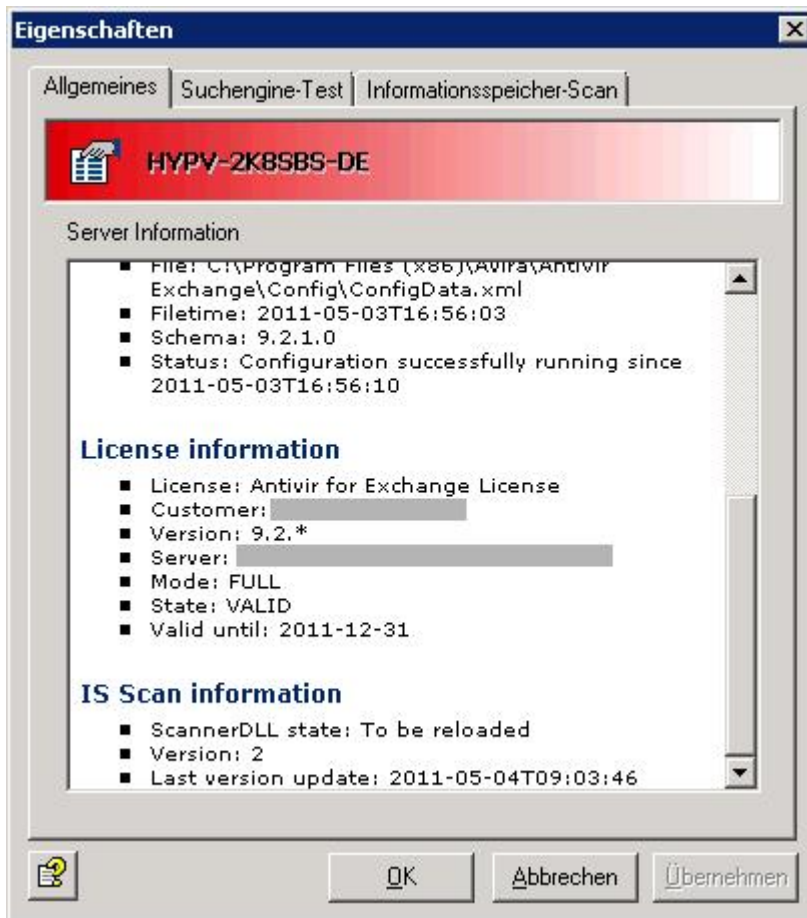
---

### 5.3.1 Status des Informationsspeichers

Klicken Sie auf **AntiVir Monitor - Server - Server Status**. Dort finden Sie sowohl den aktuellen Status des Informationsspeicher-Scans als auch die Option für einen manuellen Neustart.

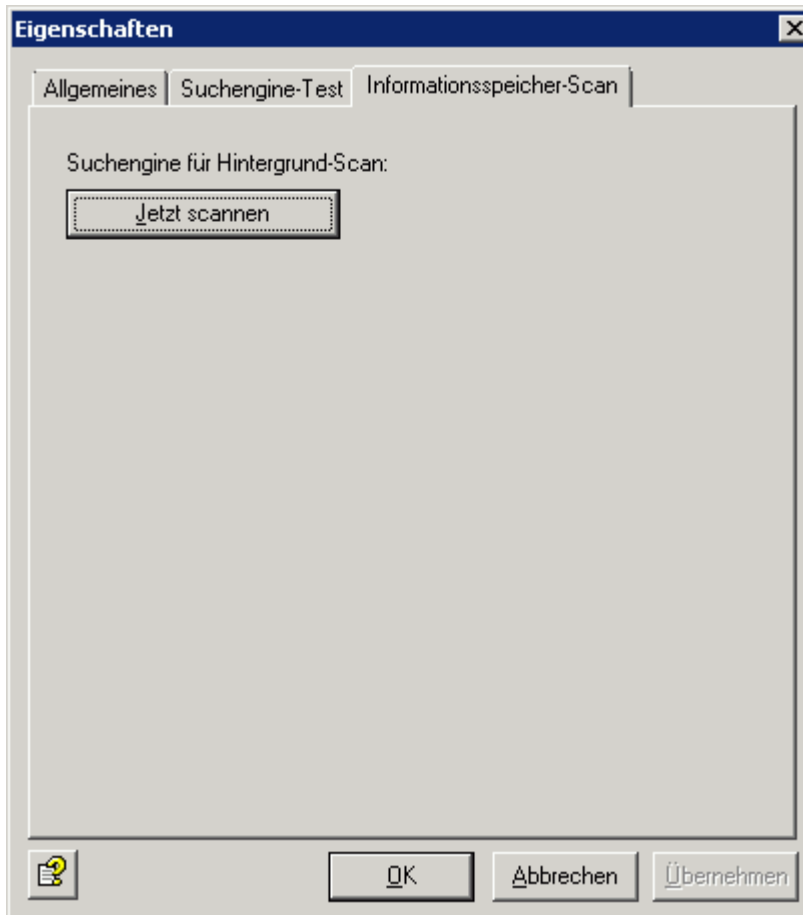
Wenn Sie auf der Registerkarte **Allgemeines** klicken, sehen Sie:

- ob die Scanner-DLL für den Informationsspeicher-Scan geladen ist. Sobald die DLL Loaded anzeigt, ist der Informationsspeicher-Scan aktiv.
- die Version des Informationsspeicher-Scans. Jeder Neustart erhöht diesen Wert.
- wann die letzte Versionsaktualisierung erfolgte und Zeit und Datum des letzten Neustarts.





Klicken Sie auf der Registerkarte **Informationsspeicher-Scan**. Dort erhalten Sie die Möglichkeit, den Hintergrund-Scan neu zu starten:



**Warnung:** Durch einen Neustart des Scans werden sämtliche Elemente im Informationsspeicher neu überprüft. Das betrifft alle drei Scanmodi. Falls Sie den Hintergrund-Scan aktiviert haben, kann diese Prüfung sehr zeit- und ressourcenintensiv sein. Es ist daher empfehlenswert, den Neustart zu Tagesrandzeiten und in Abhängigkeit der Virens Scanneraktualisierung zu starten.

### 5.3.2 Virenprüfung im Informationsspeicher - Jobbeispiel

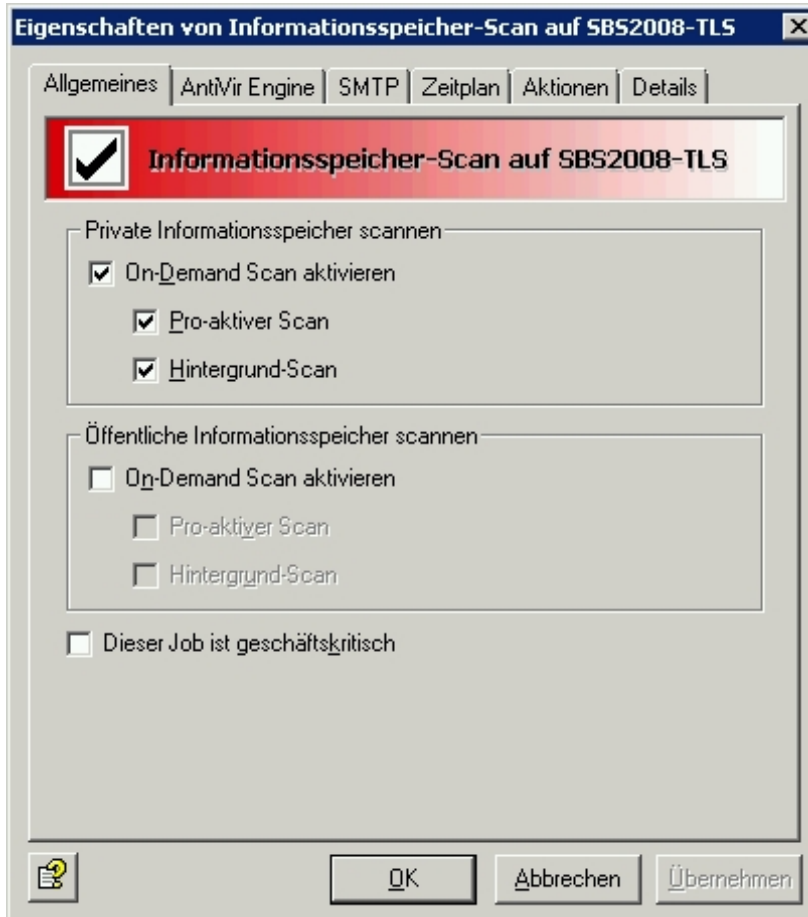
Unter **Richtlinien-Konfiguration** finden Sie im Bereich Informationsspeicher-Jobs pro Server einen **Informationsspeicher-Scan** Job. Öffnen Sie diesen mit einem Doppelklick.

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

### Allgemeine Einstellungen

Auf der Registerkarte **Allgemeines** können Sie sowohl für den Privaten als auch für den Öffentlichen Informationsspeicher den On-Demand Scan aktivieren.

Zusätzlich zum On-Demand Scan können der Proaktive Scan und der Hintergrund-Scan aktiviert werden. Nähere Informationen dazu finden Sie in [Informationsspeicher-Scan](#).

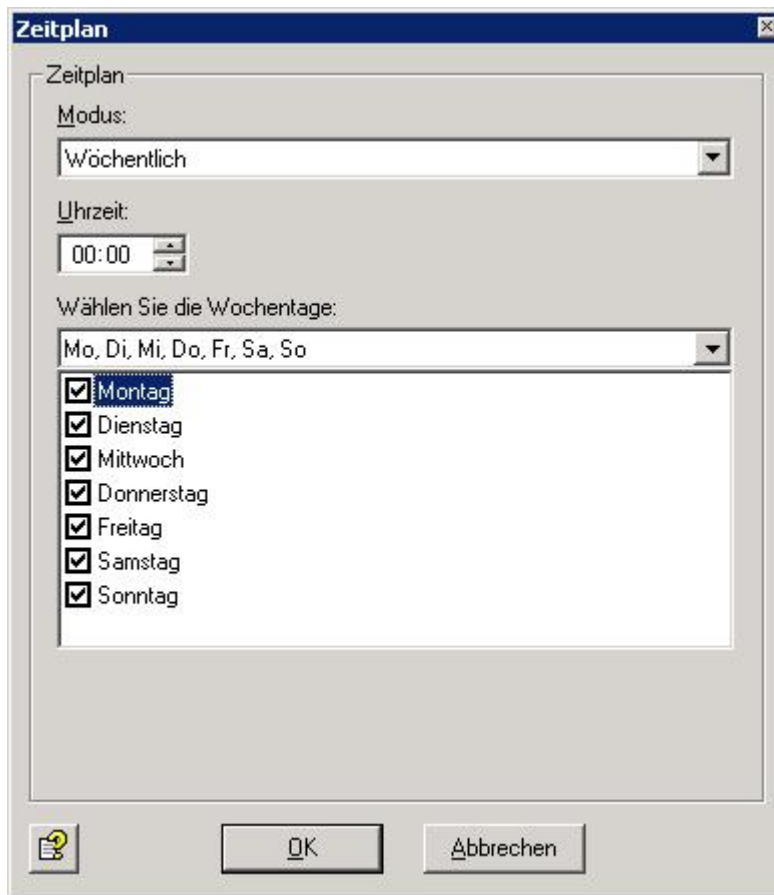


Die Option Mission Critical finden Sie unter **Dieser Job ist geschäftskritisch** näher beschrieben.

## Zeitplan festlegen

Auf der Registerkarte Zeitplan können Sie für den Neustart der Scans einen Zeitplan erstellen. Durch einen Neustart der Scans werden sämtliche Elemente im Informationsspeicher neu überprüft. Dieses betrifft alle drei Scanmodi. Falls Sie den Hintergrund-Scan aktiviert haben, kann diese Prüfung sehr zeit- und ressourcenintensiv sein. Es ist daher empfehlenswert, den Neustart zu Tagesrandzeiten und in Abhängigkeit der Virens Scanneraktualisierung zu starten.

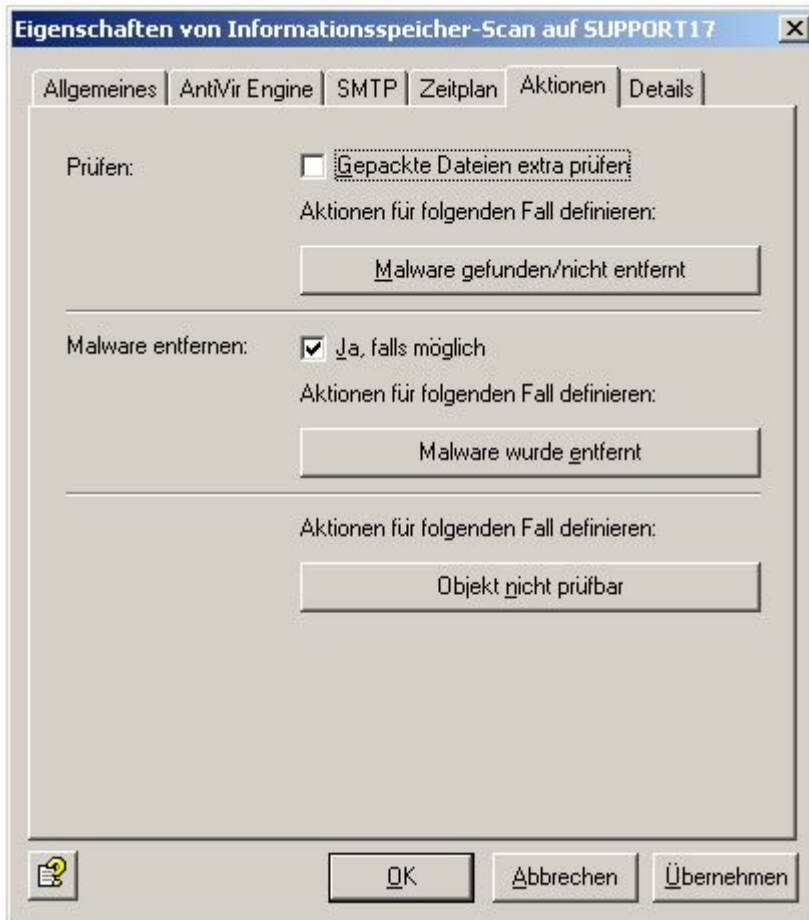
Um einen Eintrag im Zeitplan anzulegen, klicken Sie auf Hinzufügen. Wählen Sie anschließend die Startzeit und die Tage, an welchen der Neustart ausgeführt werden soll. Durch OK wird die Auswahl dem Zeitplan hinzugefügt:



## Aktionen festlegen

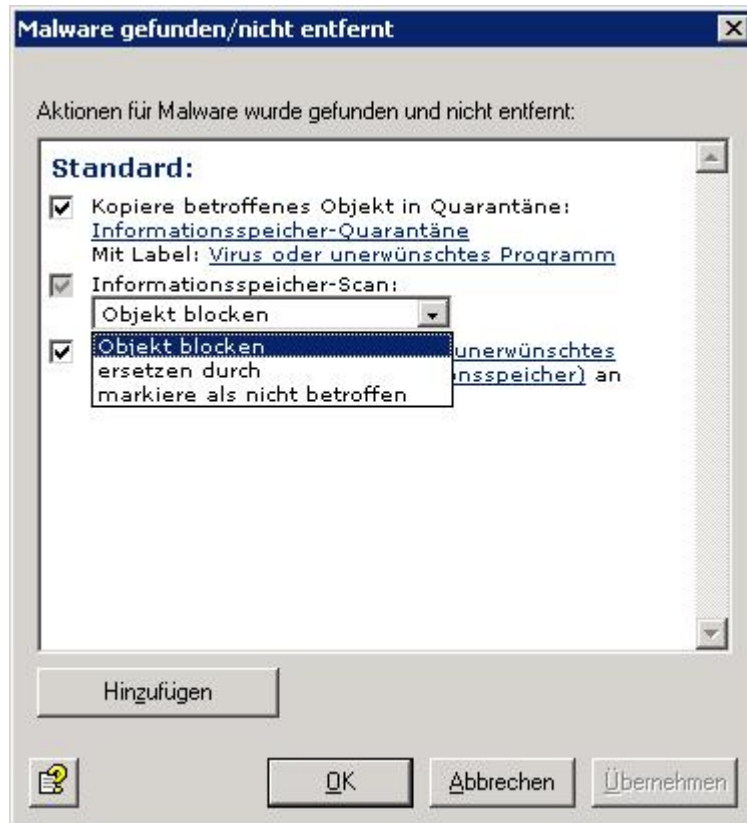
In der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn der Job eine virenverseuchte Mail gefunden hat.

**Gepackte Dateien extra prüfen:** Sollten Sie den Virenschanner eines anderen Herstellers verwenden, der im Gegensatz zu den Avira-Produkten keinen integrierten Entpacker besitzt, schalten Sie diese Option an. Damit wird ein interner Entpacker die gepackten Dateien zunächst extrahieren und danach einzeln dem Virenschanner zuführen.



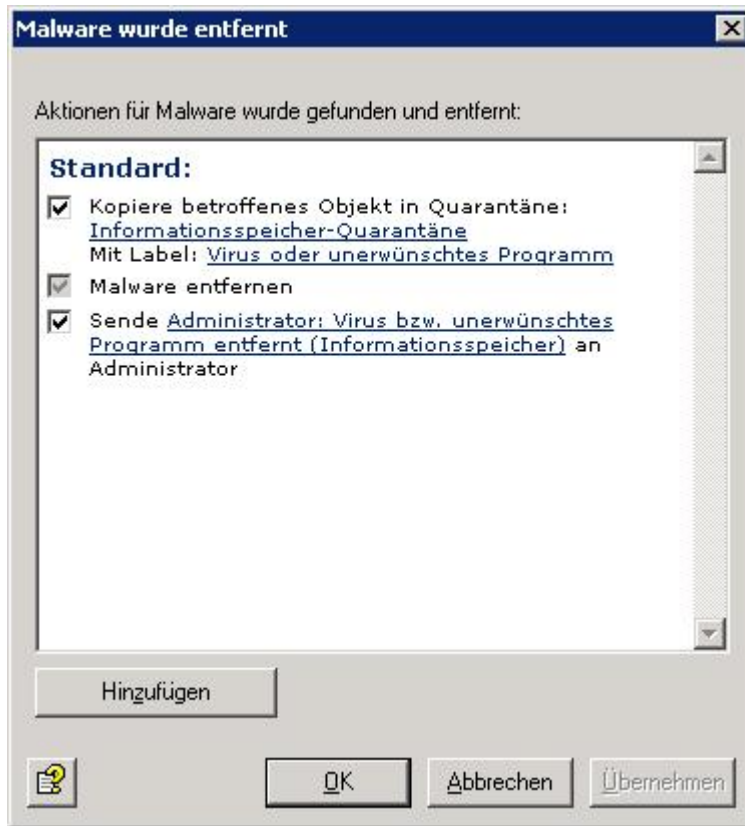
Es sind drei unterschiedliche Aktionen möglich:

- A. **Malware gefunden/ nicht entfernt:** Behandelt den Fall, dass ein Virus gefunden wurde und die Datei nicht erfolgreich gereinigt werden konnte.



- Zunächst wählen Sie, ob eine Kopie des Objektes in eine Quarantäne gestellt und mit einem Label versehen werden soll. Für den Informationsspeicher-Scan steht eine spezielle Standardquarantäne zur Verfügung.
- Das Objekt kann mit der zweiten Option wahlweise geblockt, ersetzt oder ignoriert/nicht markiert werden. Siehe auch [Informationsspeicher-Scan](#).
- Mit der letzten Standardoption wählen Sie, ob eine Benachrichtigung an den/die Administrator/en versendet werden soll.
- Über die Schaltfläche **Hinzufügen** können Sie weitere Aktionen auswählen. So ist es beispielsweise möglich, Benachrichtigungen an beliebige Empfänger zu versenden oder eine externe Anwendung zu starten.

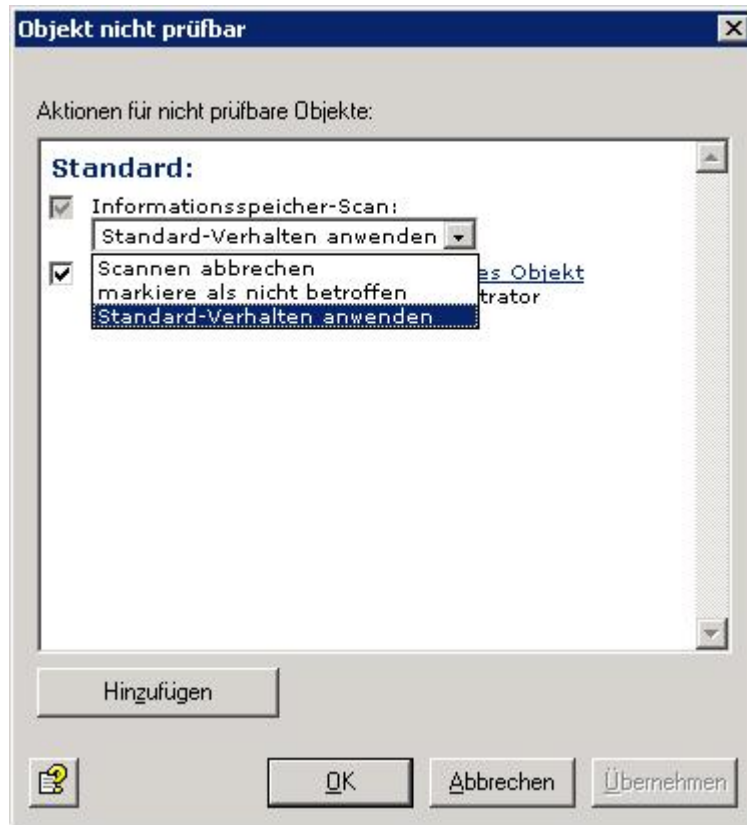
- B. **Malware wurde entfernt:** Behandelt den Fall, dass die Reinigung der Datei erfolgreich verlaufen ist und der Virus entfernt wurde.



Hier können folgende Aktionen definiert werden:

- a. Mit der ersten Option wählen Sie, ob eine Kopie des Objektes in eine Quarantäne gestellt und mit einem Label versehen werden soll. Die Kopie wird vor der Reinigung des Objektes erstellt, so dass sich das Objekt im Originalzustand in der Quarantäne befindet.
- b. Zusätzlich können Sie wählen, ob eine Benachrichtigung an den/die Administrator/en versendet werden soll.

- C. **Objekt nicht prüfbar:** Behandelt den Fall, dass die Dateien nicht geprüft werden konnten. So lässt sich beispielsweise das Verhalten von Avira AntiVir Exchange beim Auffinden verschlüsselter Objekte beeinflussen, welche naturgemäß nicht einsehbar und damit nicht auf Viren prüfbar sind.



Hier stehen Ihnen zwei Optionen zur Verfügung. Zum einen die Aktion des Informationsspeicher-Scans:

- Scannen abbrechen:** Das Objekt wird beim nächsten Scanvorgang erneut überprüft. Der Zugriff ist dabei blockiert, falls vorhergehende Scanvorgänge das Objekt nicht als virenfrei behandelt haben.
- Markiere als nicht betroffen:** Das Objekt wird behandelt, als wäre es virenfrei. Es wird erst beim nächsten Neustart der Virenprüfung erneut geprüft.
- Standard-Verhalten anwenden:** Das Objekt wird, wie unter **Basis-Konfiguration - AntiVir Server - Allgemeines** für die Option **Bei nicht scanbaren Elementen folgende Aktion ausführen** eingestellt, behandelt.

Zum anderen die Möglichkeit, eine Benachrichtigung an den Administrator zu versenden, sowie mit Hinzufügen zusätzliche Aktionen auszuführen.

## Job Details

Auf der letzten Registerkarte **Details** können Sie den Job näher beschreiben.

## 5.4 AntiVir Such Engine konfigurieren und aktivieren

Avira AntiVir Exchange ruft den Virenschanner durch das sogenannte **Avira AV Interface** - eine DLL-Datei - auf.

**Warnung:** Deaktivieren Sie unbedingt eventuelle Real-Time bzw. On-Access Scan Funktionen der eingesetzten Virenschanner für das Verzeichnis ... \Avira\AntiVir Exchange\AntiVirData\

Testen Sie, ob Ihr Virenschanner korrekt arbeitet: Markieren Sie unter **AntiVir Monitor** den gewünschten Servernamen und klicken Sie im rechten Fenster auf **Server Status**. Unter der Registerkarte **Suchengine-Test** wählen Sie **Virenschanner-Test**. Bei Erfolg erhalten Sie ein OK und die Meldung, dass ein EICAR Test Virus gefunden wurde.



Unter **Basis-Konfiguration - Utility-Einstellungen - AntiVir Engine - Avira AntiVir Scan Engine - Eigenschaften** können Sie AntiVir konfigurieren.

- Im Feld **Avira AV Interface** muss der Name der Avira Interface-DLL eingetragen sein. Diese DLL-Datei stellt die Verbindung der Avira AntiVir Exchange zum Virenschanner her. Dieser Eintrag ist für jeden Virenschanner vorkonfiguriert und darf nicht geändert werden! Im Folgefild geben Sie den **Parameter** an, der vom Virenschanner zur Virenprüfung (Scan) verwendet werden soll.
- Um den Virenschanner so einzustellen, dass Emails oder Anhänge bei einem gefundenen Virus bereinigt werden, aktivieren Sie das Feld **Alternativer Reinigungsparameter** und geben im Folgefild **Reinigungsparameter** den zugehörigen Parameter an.



---

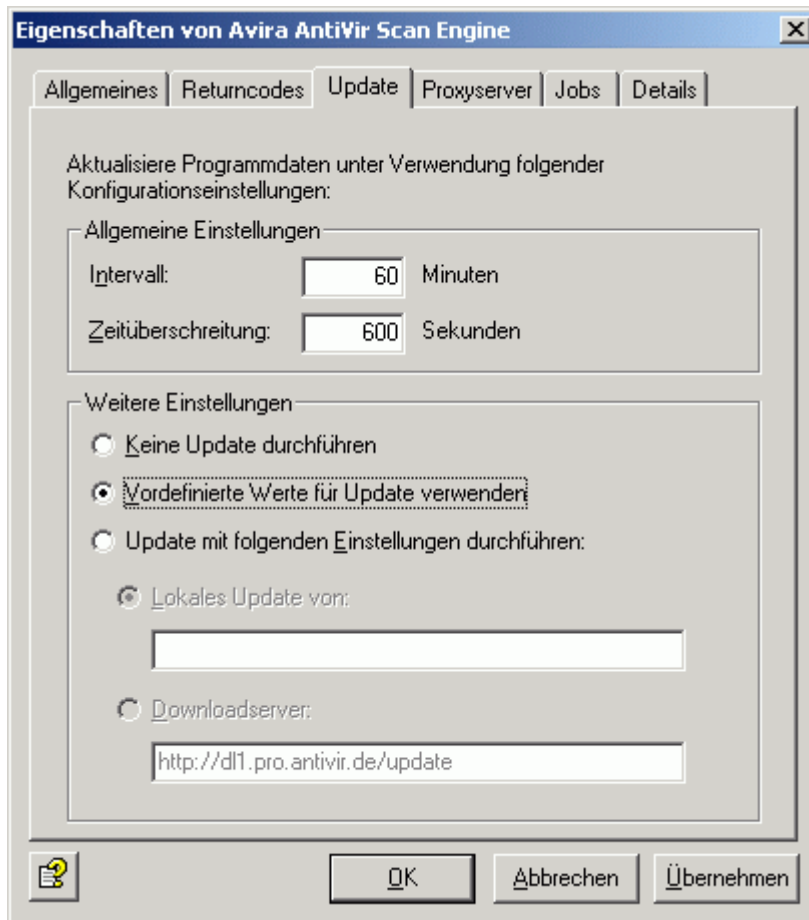
**Hinweis:** Die entsprechenden Reinigungsparameter können Sie telefonisch oder per Email beim Support erfragen.

**Hinweis:** Wenn Sie den Virenschanner nur zur Virenprüfung einsetzen möchten, verwenden Sie den AntiVir-Job **Prüfung mit AntiVir-Engine**. In der Registerkarte **Aktionen** muss das Feld **Virus entfernen** deaktiviert sein. Wenn der Virenschanner einen gefundenen Virus auch entfernen soll, verwenden Sie den AntiVir-Job **Prüfung und Entfernung mit AntiVir-Engine**. In diesem Fall muss das oben genannte Feld aktiviert und die gewünschten Aktionen im Virusfall festgelegt sein.

- **Zeitüberschreitung:**  
Geben Sie die Anzahl der Sekunden an, nach der ein Versuch, die Verbindung zum Server herzustellen, abgebrochen wird (wenn die Verbindung bis dahin noch nicht aufgebaut sein sollte). Berücksichtigen Sie bei der Zeitangabe die Performance Ihres Servers. Minimalwert: 60 Sekunden.
- **Erlaube mehrere zeitgleiche Aufrufe:**  
bestimmt, dass mehrere E-Mails gleichzeitig durch diesen Virenschanner bearbeitet werden können. Die Anzahl der Aufrufe wird in **AntiVir Server - Eigenschaften - Registerkarte Allgemeines: Anzahl der Threads** festgelegt. Siehe auch Einstellungen für einen einzelnen Avira AntiVir Exchange Server.

In der Registerkarte **Returncodes** können Sie die vorkonfigurierten Returncodes bearbeiten. Die Bedeutung der einzelnen Codes finden Sie in der Registerkarte **Details**.

Registerkarte **Update:** Der Virenschanner verfügt über einen Mechanismus, mit dem er die neuesten Pattern aus dem Internet lädt.



- **Pattern-Datenbank aktualisieren:** Aktivieren Sie diesen Schalter.
- **Parameter:** Dieses Feld gibt das Verzeichnis an, in dem die aktualisierten Virenpattern abgelegt werden und ist voreingestellt (Standardeinstellung: *Update\Extract*).
- **Intervall:** Zeitintervall in Minuten, in dem nach Pattern Updates gesucht wird. Minimalwert: 15 Min.
- **Zeitüberschreitung:** Nach Ablauf dieser Frist wird der Update-Vorgang abgebrochen. Minimalwert: 60 Sekunden.

Sie können für die Aktualisierung der Virenpattern einen **Proxyserver** verwenden. Wählen Sie den gewünschten Proxyserver in der Registerkarte Proxyserver aus. Um einen neuen Proxyserver anzulegen, siehe Kapitel "Proxyserver verwenden" unter [Einstellungen für einen einzelnen AntiVir Server](#).

Aus der Registerkarte **Jobs** ersehen Sie, in welche Jobs der Virens Scanner eingebunden ist.

**Warnung:** Bitte nutzen Sie für Aktualisierungen der Avira AntiVir Exchange nicht diese Registerkarte, sondern wählen Sie auf der Registerkarte Suchengine-Test die Option Virens Scanner/Antispam-Aktualisierung und klicken Sie auf Start. Nach dem Update bekommen Sie einen detaillierten Update- Bericht.

Auf der Registerkarte **Details** ist die Beschreibung der voreingestellten Rückgabewerte enthalten. Wenn Sie Änderungen auf der Registerkarte Returncodes vornehmen, empfehlen wir diese Änderungen auf der Registerkarte Details zu dokumentieren.

## 5.5 Virenprüfung einschalten - Jobbeispiel

Unter **Richtlinien-Konfiguration - Mail Transport Jobs** finden Sie den Job **Prüfung mit AntiVir Suchengine**. Öffnen Sie diesen mit einem Doppelklick.

### 5.5.1 Allgemeine Einstellungen

Auf der Registerkarte **Allgemeines** können Sie einen eigenen Namen für den Job vergeben. Setzen Sie den Job **Aktiv**. Sobald Sie mit OK Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert. Dass der Job aktiv ist, erkennen Sie sofort an dem Haken im Job-Symbol.



Der **Zusatz im Betreff** ist vordefiniert auf **AntiVir checked**. Dieser Zusatz wird in den Betreff jeder Email eingefügt, die der Job geprüft hat.

Dieser Job bearbeitet auch solche Emails, die aus der Quarantäne wieder versendet werden. Die Sende-Option beim **Versand aus der Quarantäne** ist jobübergreifend und hat Priorität. Wenn Sie eine Mail also mit der **Quarantäne-Sende-Option Zustellen ohne weitere AntiVir Prüfung dieses Servers** erneut versenden, wird die Mail durch keinen Job bearbeitet. Setzen Sie beim Versand aus der Quarantäne die Sende-Option deshalb auf **Email erneut durch AntiVir Jobs dieses Servers bearbeiten**.

Näheres zum erneuten Versand aus der Quarantäne finden Sie in [Aus Quarantäne senden](#).

### 5.5.2 Dieser Job ist geschäftskritisch

Ein Job ist **geschäftskritisch**, wenn die Email bei einem Verarbeitungsfehler - wie beispielsweise bei fehlendem Virenschanner - in den Bad-Mail-Bereich abgelegt werden soll. Wählen Sie diese Option für unternehmenskritische Jobs wie Virenprüfungen (Haken wird gesetzt).

**Warnung:** Solange der Verarbeitungsfehler nicht behoben ist, wird bei dieser Option **jede** Email - eingehend oder ausgehend - in den Bad-Mail-Bereich überführt!

Ein Job ist **nicht geschäftskritisch**, wenn das Ergebnis des Jobs im Falle eines Verarbeitungsfehlers bei der betreffenden Email ignoriert werden soll. Die Email wird in diesem Fall dem nächsten Job zur Bearbeitung übergeben. Jeder Verarbeitungsfehler wird im Windows Event Log eingetragen. Tritt der Verarbeitungsfehler fünf Mal hintereinander auf, wird der Job deaktiviert. Der deaktivierte Job wird nach 15 Minuten automatisch wieder gestartet. Wählen Sie diese Option für nicht unternehmenskritische Jobs.

Die Standardeinstellung für fast alle Jobs ist **nicht geschäftskritisch**. Welche Jobs als unternehmenskritisch gelten, sollte in den Firmenrichtlinien festgelegt werden.

### 5.5.3 Verarbeitung protokollieren

Mit dem Verarbeitungsprotokoll beobachten Sie die Verarbeitung der Emails durch den Job. Schalten Sie diese Funktion ein, wenn evtl. eine Nachweispflicht bestehen kann, oder wenn Sie einen Job testen wollen.

Wenn Sie den Haken dieser Option setzen, wird für jede bearbeitete Email in eine Textdatei geschrieben, ob und wie der Job die jeweilige Email bearbeitet hat. Diese Protokoll-Textdatei wird im Installationsverzeichnis der Avira AntiVir Exchange im Ordner Log abgelegt. Die Protokollierung wird pro Job definiert, die Textdatei enthält aber die Informationen aller Jobs, für die **Verarbeitung protokollieren** eingeschaltet ist. Für jeden Tag wird eine extra Textdatei angelegt.

Name der Textdatei: *Audit\_all\_<Datum der letzten Änderung>.log*, z. B. *Audit\_all\_20050909.log*

Die einzelnen Informationen über die bearbeitete Email sind mit Semikola getrennt und können daher manuell oder automatisch ausgewertet werden:

1. Datum und Uhrzeit der Bearbeitung der Email
2. Job-ID
3. Jobname
4. Message-ID
5. SMTP-Absender
6. SMTP-Empfänger
7. Ergebnis der Prüfung durch Avira AntiVir Exchange
  - Restricted - Email entspricht den definierten Restriktionen
  - Unrestricted - Email entspricht nicht den definierten Restriktionen

Empfängergruppen werden aufgelöst. Für jeden Empfänger wird eine eigene Zeile in die Datei geschrieben.

### Adressbedingungen einrichten

Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus. Wie Sie Adresslisten am besten einsetzen und eine genaue Beschreibung der Vorgehensweise finden Sie in [Adresslisten](#).

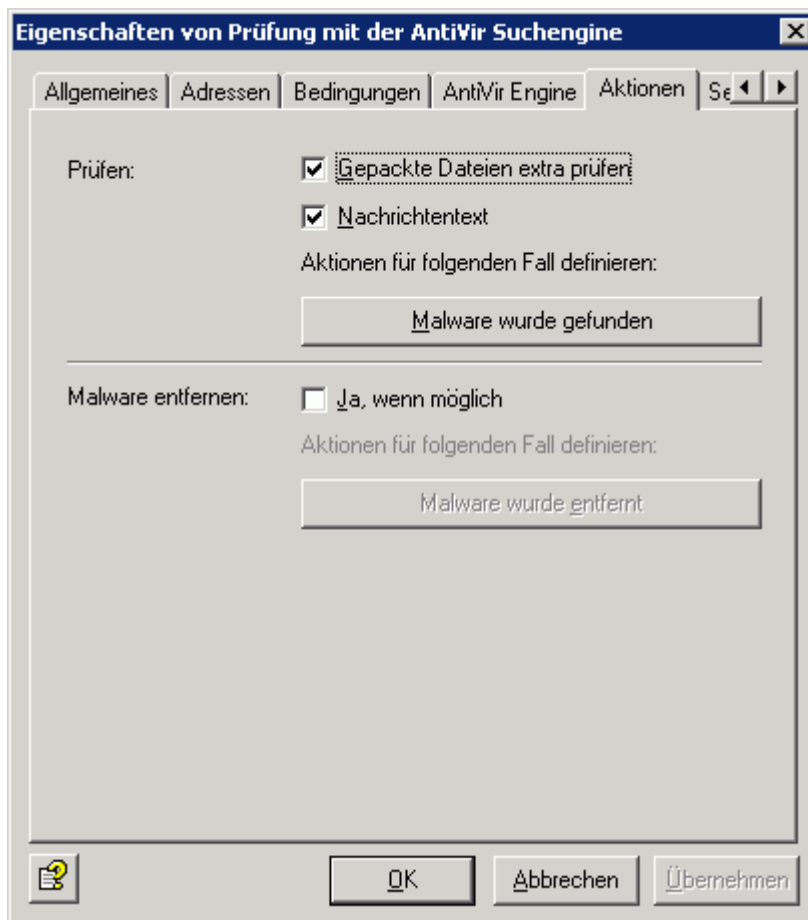
## Inhaltliche Bedingungen einrichten

Auf der Registerkarte **Bedingungen** können Sie die Ausführungsbedingungen eines Jobs festlegen. Wie Sie Bedingungen am besten einsetzen finden Sie in [Bedingungen](#).

**Warnung:** Die inhaltlichen Bedingungen müssen gleichzeitig mit den definierten Adressbedingungen in der Registerkarte **Adressen** zutreffen, damit der Job ausgeführt wird (UND-Verknüpfung).

## Aktionen festlegen

In der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, **wenn der Job eine virulente Email gefunden hat:**



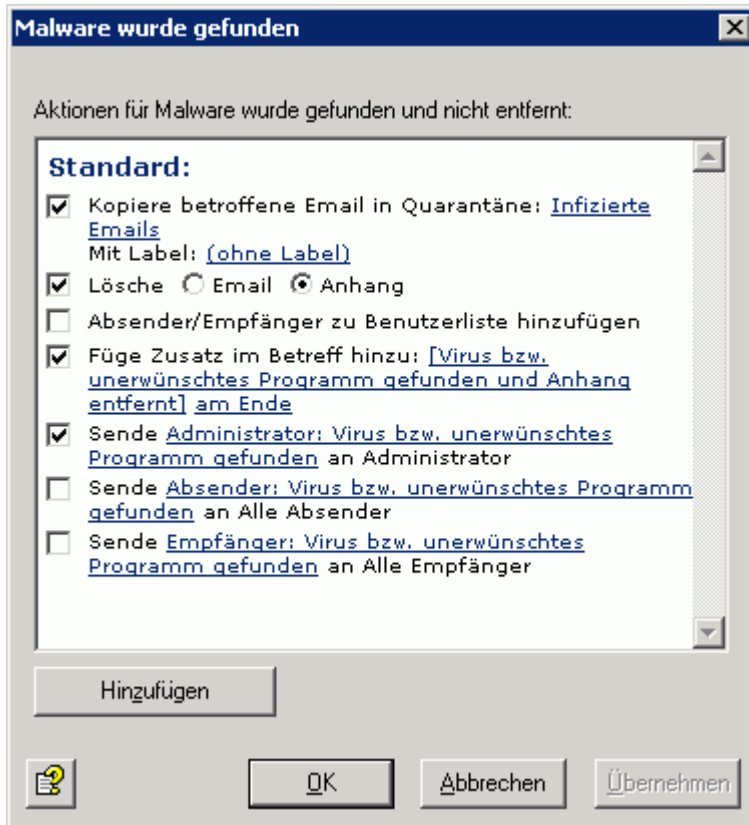
Dieser Job soll die Email auf Viren prüfen, aber nicht versuchen, die Email bzw. den Anhang von diesen Viren zu reinigen. In der Regel sind zwar alle Virens Scanner zu einer Reinigung in der Lage. Da es in der Praxis aber kaum noch vorkommt, dass Viren versehentlich von bekannten Kommunikationspartnern versendet werden, sondern es meist Spam ist, der gleichzeitig Viren enthält, ist es effektiver, virenbehaftete Anhänge sofort in die Quarantäne zu stellen.

**Hinweis:** Da der Job lediglich eine Virenprüfung durchführen soll, müssen Sie die AntiVir Engine entsprechend konfigurieren. Wählen Sie unter **Basis-Konfiguration - Utility-Einstellungen - AntiVir Engine** die gewünschte Engine aus und deaktivieren Sie das Feld **Alternativer Reinigungsparameter**. Aktivieren Sie dieses Feld dann, wenn der Job die Email bzw. den Anhang bei einem gefundenen Virus bereinigen soll.

Nachdem Sie festgelegt haben, was genau geprüft werden soll, definieren Sie zwei unterschiedliche Aktionen:

1. Für den Fall, dass ein Virus gefunden wurde und die Datei nicht erfolgreich gereinigt werden konnte,
2. für den Fall, dass die Reinigung der Datei erfolgreich verlaufen ist und der Virus entfernt wurde (falls Sie diese Option ausgewählt haben).

Die Konfiguration der Aktionen ist in beiden Fällen identisch. Das folgende Beispiel bezieht sich auf den ersten Fall:

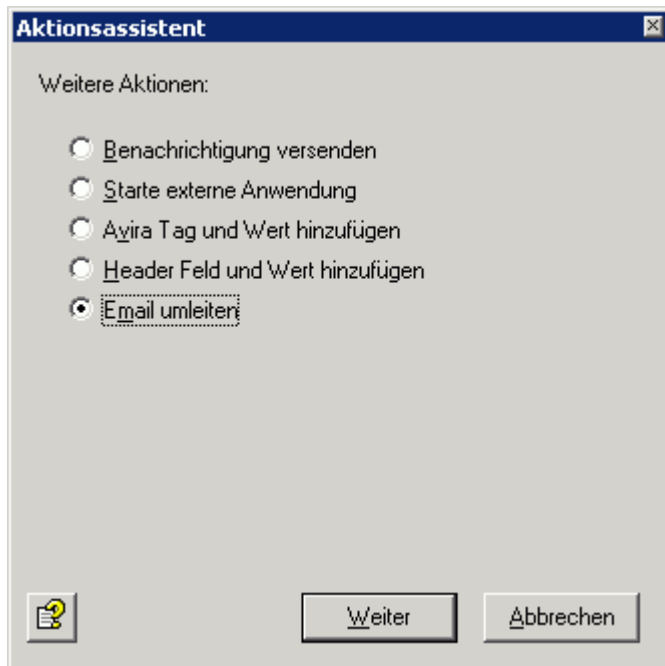


Eine Kopie der Email wird in die Quarantäne gestellt und die betroffenen Anhänge werden gelöscht. Das beinhaltet, dass die Email nur dann an den Empfänger zugestellt wird, wenn der Nachrichtentext virenfrei war und der Anhang gelöscht werden konnte. Eine Benachrichtigung über den Virus wird an den Administrator versandt. Diese Benachrichtigung wird aus dem Pull Down-Menü der verfügbaren Benachrichtigungsvorlagen ausgewählt und diese können individuell mit der HTML-Symbolleiste oder direkt mit HTML-Formatbefehlen gestaltet werden.

**Hinweis:** Prüfen Sie, ob an Ihr Unternehmen gesendeten Virenmails sehr häufig gleichzeitig Spam sind. Wenn das der Fall ist, löschen Sie am besten sofort die gesamte Email und nicht nur den Anhang. So müssen die übrig gebliebenen Nachrichtentexte nicht noch auf Spam untersucht werden.

**Hinweis:** Wenn Sie die Option **Auf Viren prüfen: Nachrichtentext** aktiviert haben und tatsächlich ein Virus im Text gefunden wird, so wird die gesamte Email inklusive der Anhänge gelöscht, wenn Sie **Lösche Anhang** gesetzt haben (es wird kein Anhang ohne Nachrichtentext zugestellt). Der betroffene Emailabschnitt wird in der Regel einzeln gelöscht. Wenn nur der Anhang virulent war, wird auch nur dieser gelöscht.

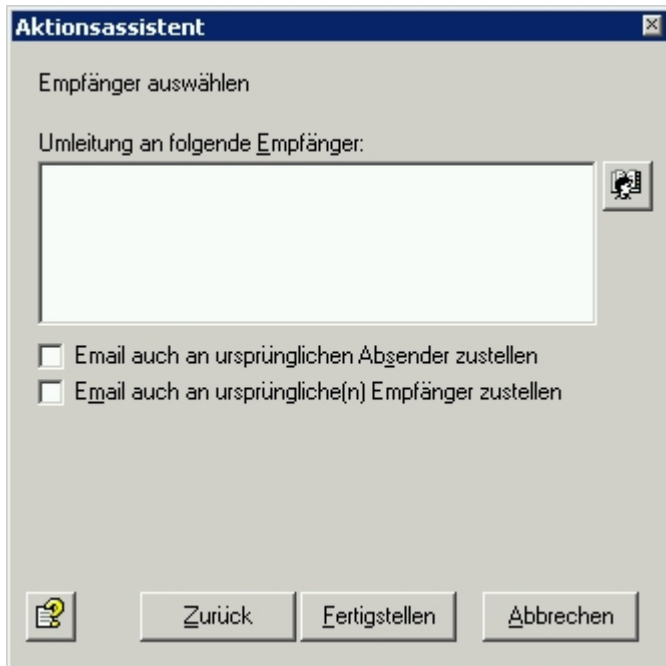
Klicken Sie auf die Schaltfläche **Hinzufügen**, falls Sie weitere Aktionen definieren wollen:




- **Benachrichtigung versenden:** Wählen Sie den Empfänger der Benachrichtigung aus dem Adressbuch aus.
- **Starte externe Anwendung:** Eine neue Anwendung / Applikation kann definiert werden, um Aktionen dieser Anwendung ausführen zu lassen. Für den Start einer externen Anwendung geben Sie den Pfad und ggf. die notwendigen Parameter an.
- **Avira Tag und Wert hinzufügen:** Mail-Header Tags können während des Verarbeitungsprozesses durch Avira AntiVir Exchange eingesetzt werden, um spezielle Avira AntiVir Exchange-Aktionen ausführen zu lassen. Beispielsweise können einer E-Mail zusätzliche Angaben hinzugefügt werden, die ein nachfolgender Job auswertet. Beim Versenden der E-Mail an die ursprünglichen Empfänger werden die Angaben des Mail-Header-Tags entfernt.
- **Header Feld und Wert hinzufügen:** Definieren Sie ein neues X-Header-Feld und wählen Sie die Variable aus, die eingefügt werden soll, z.B. um das Ergebnis einer Spam-Analyse als Wert auszugeben. Im Gegensatz zum Mail-Header-Tag bleiben diese Informationen auch beim Versand der Email an den ursprünglichen Empfänger erhalten.
- **Email umleiten:** Wählen Sie den Empfänger der umgeleiteten Email aus dem Adressbuch aus. Mail umleiten ist nicht voreingestellt, die Option wird ihnen lediglich als weitere Aktion vorgeschlagen.

**Hinweis:** Anmerkung zu **Email umleiten:** Wenn Sie eine TNEF-Mail an eine externe Adresse umleiten, erhalten Sie dort eine leere Email, evtl. mit einem *winmail.dat* Anhang. Das TNEF-Format wird von Exchange verwendet, wenn ein Outlook-Benutzer (nicht Outlook Express!) innerhalb einer Exchange-Organisation eine Email sendet. Bei der Kommunikation über das Internet bzw. bei der Verwendung von anderen Email Programmen wird dieses Format nicht verwendet.

Klicken Sie auf **Weiter** und nehmen Sie je nach ausgewählter Option weitere Konfigurationen vor. Im Falle von Email umleiten haben Sie folgende Optionen:



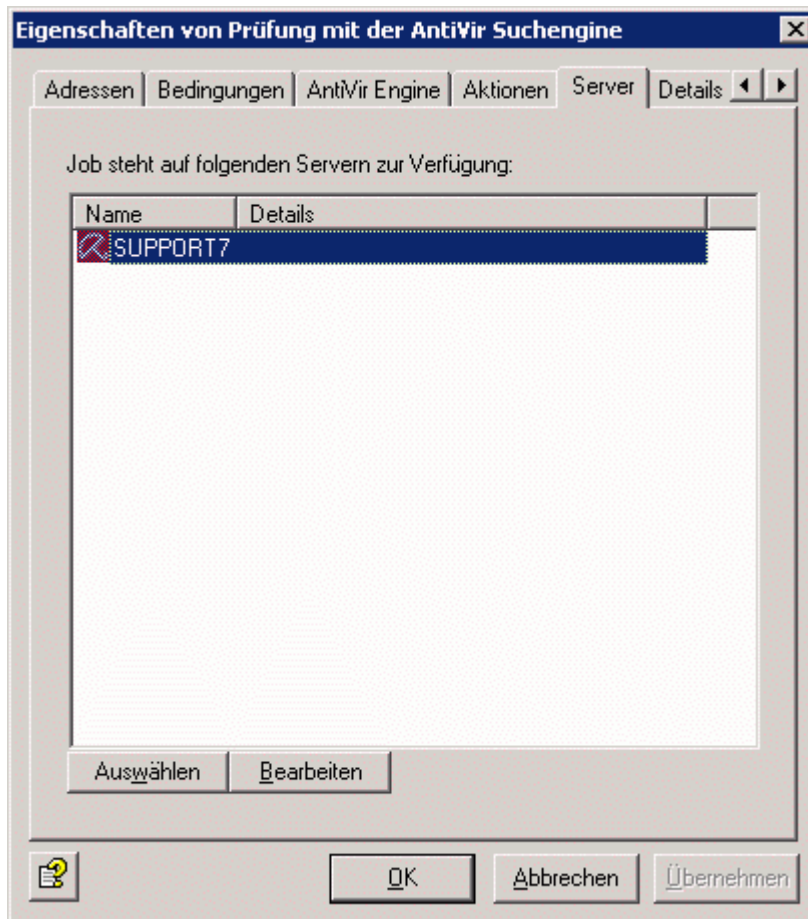
Klicken Sie auf das Symbol für das Adressbuch , um weitere Empfänger auszuwählen oder eigene Adressen zu definieren. Wenn Sie die Email zusätzlich auch dem ursprünglichen Empfänger oder dem ursprünglichen Absender zustellen möchten, aktivieren Sie jeweils das zugehörige Kontrollkästchen.

Klicken Sie auf **Fertigstellen**, wenn der Empfänger eingetragen ist.



## Server auswählen

Auf der Registerkarte **Server** wählen Sie den oder die Server aus, auf denen der Job aktiv sein soll.




Klicken Sie auf die Schaltfläche **Auswählen**. Sie erhalten einen zu der Auswahl von Virensclannern analogen Dialog.

**Hinweis:** Damit der Server in der Auswahlliste erscheint, muss er korrekt konfiguriert sein. Näheres zur Konfiguration von Avira AntiVir Exchange Servern finden Sie in [Einstellungen für einen einzelnen Avira AntiVir Exchange Server](#).

## Details zum Job eingeben

Auf der letzten Registerkarte **Details** können Sie den Job näher beschreiben.

## Konfiguration Speichern

Speichern Sie die Konfiguration der Avira AntiVir Exchange Konsole jedes Mal, wenn Sie Änderungen durchgeführt haben. Drücken Sie dafür die Schaltfläche . Die Konfiguration wird in der Datei *ConfigData.xml* gespeichert, die im Verzeichnis *Avira\AntiVir Exchange\Config* abgelegt ist. Offene Änderungen werden durch (\*) am obersten Knoten angezeigt.

## 5.6 Virenprüfung von passwortgeschützten Archiven

Damit AntiVir Jobs Emails verarbeiten können, müssen die Emails vollständig entpackt sein. Bei passwortgeschützten Archiven ist kein Entpacken möglich. Daher werden Emails mit solchen Dateianhängen defaultmäßig von einem Virensan Job als "nicht prüfbar" geblockt und in der Badmail-Quarantäne der AntiVir abgelegt.

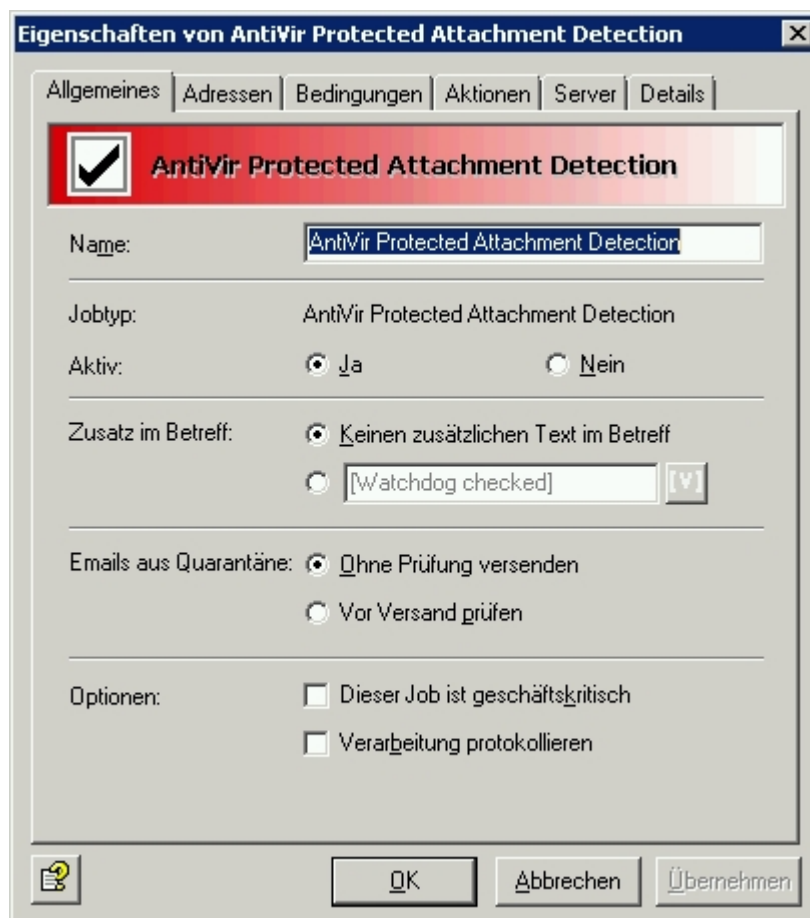
Um diese Aktion zu verhindern, verwenden Sie den Job **AntiVir Protected Attachment Detection**. Der Job reagiert auf Emails mit passwortgeschützten Archiven und führt die in der Registerkarte **Aktionen** konfigurierten Jobaktionen aus. Dadurch können passwortgeschützte Archive regelbasiert behandelt werden. Beispielsweise werden solche Emails für bestimmte Personen/ Personengruppen geblockt während sie für andere zugestellt werden.

Da die Emails im letzteren Fall ungeprüft zugestellt würden, sollten die Emails vor der Zustellung von einem Virensan Job geprüft werden. Dazu markiert der AntiVir Scanner Job die Emails, in denen passwortgeschützte Archive enthalten sind. Ein nachfolgender Virensan Job behandelt die Emails aufgrund dieser Markierung wie eine "normale" Email und kann ohne diesen Job auftretende Verarbeitungsfehler (DENIED) ignorieren.

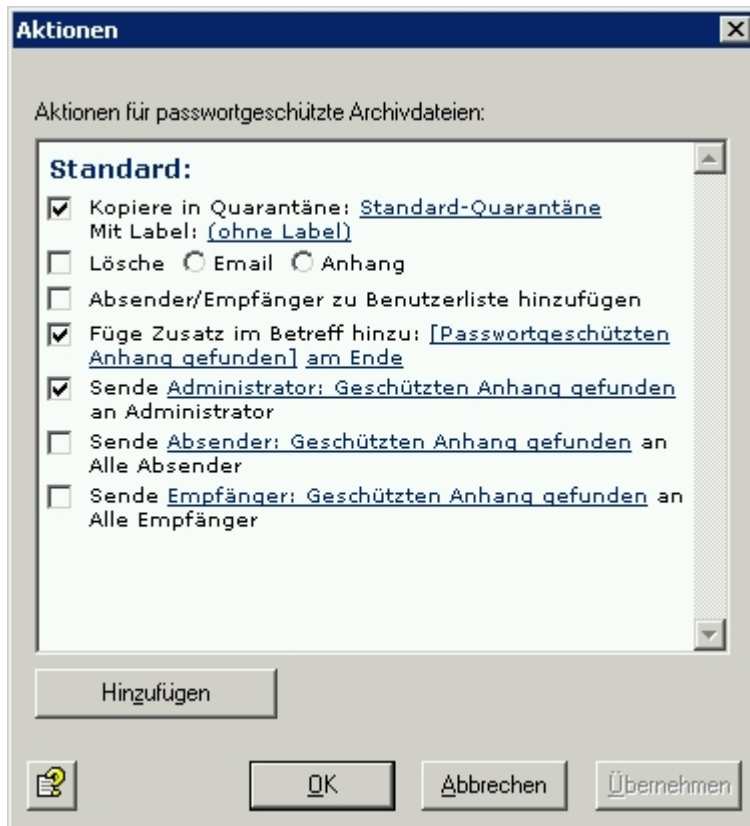
**Warnung:** Der Virensan scanner prüft nicht die in Archiven enthaltenen Dateien auf Virenbefall.

### 5.6.1 Jobbeispiel

Klicken Sie mit der rechten Maustaste auf **Mail Transport Jobs**, wählen Sie **Neu - AntiVir Protected Attachment Detection**.



Aktivieren Sie den Job. Im Beispiel werden nur die jobspezifischen Details erläutert.



Mit der Voreinstellung des Jobs wird ein Zusatz in den Betreff der Email eingefügt und dem Administrator eine Benachrichtigung zugestellt. Eine Email-Kopie wird in der Standard-Quarantäne abgelegt, die Email jedoch nicht geblockt (Option **Lösche Email** ist deaktiviert). Je nach Konfiguration wird sie an einen nachfolgenden Virensan-Job übergeben und anschließend dem Empfänger zugestellt.

Wenn Emails geblockt und nicht den Empfängern zugestellt werden sollen, aktivieren Sie die Option **Lösche Email**. Die Email verbleibt dann bis zur Prüfung und Freigabe durch den Administrator in der Standard-Quarantäne.

## 5.7 Dateieinschränkungen für den Anhang

Dateien können nach den Kriterien Typ und Größe eingeschränkt werden. Zunächst können Sie bestimmte Typen von Dateien nicht zulassen. Außerdem können Sie die maximale Größe einer Email und die maximale Größe der Anhänge von Emails festlegen. Die Größe und der Typ der Anhänge können auch in einem gemeinsamen Job geprüft werden.

### 5.7.1 nach Typ

Die Datei muss von AntiVir identifiziert werden. Dafür wird der Fingerprint der Datei geprüft, der das binäre Dateimuster, z.B. bei \*.exe-Dateien und/oder die Dateierweiterung (Extension), z.B. bei \*.vbs-Dateien, enthält.

Das Ergebnis dieser Prüfung wird mit den verbotenen/erlaubten Fingerprints unter AntiVir-Einschränkungen verglichen und entsprechend ausgegrenzt oder durchgelassen. Für abgelehnte Dateien werden dann die Aktionen aus dem Job ausgeführt, z.B. bei einer Email mit einem verbotenen Anhang:

- Der verbotene Anhang wird in die Quarantäne kopiert.
- Der Nachrichtentext wird dem Empfänger zugestellt.
- Benachrichtigungen werden an den Administrator und den Absender geschickt.

Folgende Aktionen sind bei einem **AntiVir Attachment Filtering** Job möglich:

- Gesamte Email in Quarantäne stellen
- Betroffene Anhänge aus der Email entfernen
- Betroffene Email löschen und nicht zustellen
- Absender oder Empfänger in Whitelist hinzufügen
- Zusatz im Betreff
- Administrator benachrichtigen
- Absender benachrichtigen
- Empfänger benachrichtigen
- Andere, frei wählbare Personen benachrichtigen
- Eine externe Anwendung ausführen
- Avira-Header-Feld hinzufügen
- X-Header-Feld hinzufügen
- Email umleiten

### 5.7.2 nach Email-Größe

Emails können anhand Ihrer Gesamtgröße analysiert und ggf. abgewiesen werden. Das Limit pro Email können Sie unter der Registerkarte **Email-Größe** einstellen.

Folgende Aktionen sind bei einem **AntiVir Email Size Filtering** Job möglich:

- Gesamte E-Mail in Quarantäne stellen
- Zusatz im Betreff
- Betroffene E-Mail löschen und nicht zustellen
- Absender oder Empfänger in Whitelist hinzufügen
- Administrator, Absender, Empfänger benachrichtigen
- Andere, frei wählbare Personen benachrichtigen
- Eine externe Anwendung ausführen
- Avira-Header-Feld hinzufügen
- X-Header-Feld hinzufügen
- Email umleiten

### 5.7.3 nach Anhangtyp und/oder -Größe

Emails können anhand der Größe ihres Anhangs analysiert und ebenfalls abgewiesen werden. Die maximale Größe eines Anhangs pro Email können Sie unter der Registerkarte **Fingerprint/Größe** einstellen. Es ist möglich, in diesem Job gleichzeitig den Typ des Anhangs einzuschränken.

Die Aktionsmöglichkeiten sind bei einem **AntiVir Attachment/Size Filtering** Job die gleichen wie in einem Attachment Filtering Job.

### 5.7.4 Fingerprints konfigurieren

Ein Fingerprint besteht aus einem Namensmuster und/oder einem Binärmuster.

- **Namensmuster:** Damit können Fingerprints anhand von Dateiname und -erweiterung (\*.exe, ...) konfiguriert werden.
- **Binärmuster:** Damit können Fingerprints anhand von eindeutigen binären Dateinformationen konfiguriert werden.

Mit dem Namensmuster sind natürlich auch Manipulationen möglich, da (wenn die Anwender davon wissen) einfach die Erweiterung geändert werden kann. Das Binärmuster ist eine eindeutige Zuordnung zu einem Format und lässt sich in der Datei nicht so leicht manipulieren. Somit ist der sichere Weg, ein Dateiformat zu erkennen, die Eingabe eines Binärmusters.

Mit Namensmustern ist es aber möglich, auf neue Virusattacken schnell zu reagieren:

Sobald bekannt ist, mit welchen Anhangnamen ein neuer Virus verbreitet wird (Beispiel: Nimda Virus = readme.exe) kann die Virusattacke abgewehrt werden, noch bevor ein Virus Pattern Update des Antivirus Herstellers verfügbar ist. Der Dateiname wird einfach mit dem Namensmuster als neuer Fingerprint angelegt.

Auch das Blocken individueller Dateien ist möglich:

Setzt ein Unternehmen Individualsoftware ein, welche ein eigenes Dateiformat erzeugt, kann dafür ebenfalls ein Fingerprint erstellt und somit beispielsweise verhindert werden, dass solche Dateien das Unternehmen per Email verlassen. Fingerprints können Sie organisieren und zu einer logischen Kategorie zusammenfassen.

Eine Reihe von vorgefertigten Fingerprints für Standarddateien steht mit dem Programm automatisch zur Verfügung. Zur Erstellung individueller Fingerprints setzen Sie sich bitte dem Support in Verbindung.

### 5.7.5 Dateianhänge nach Typ verbieten - Jobbeispiel

Unter **Richtlinien-Konfiguration - Jobvorlagen** finden Sie verschiedene Jobs für das Blocken diverser Dateiformate:

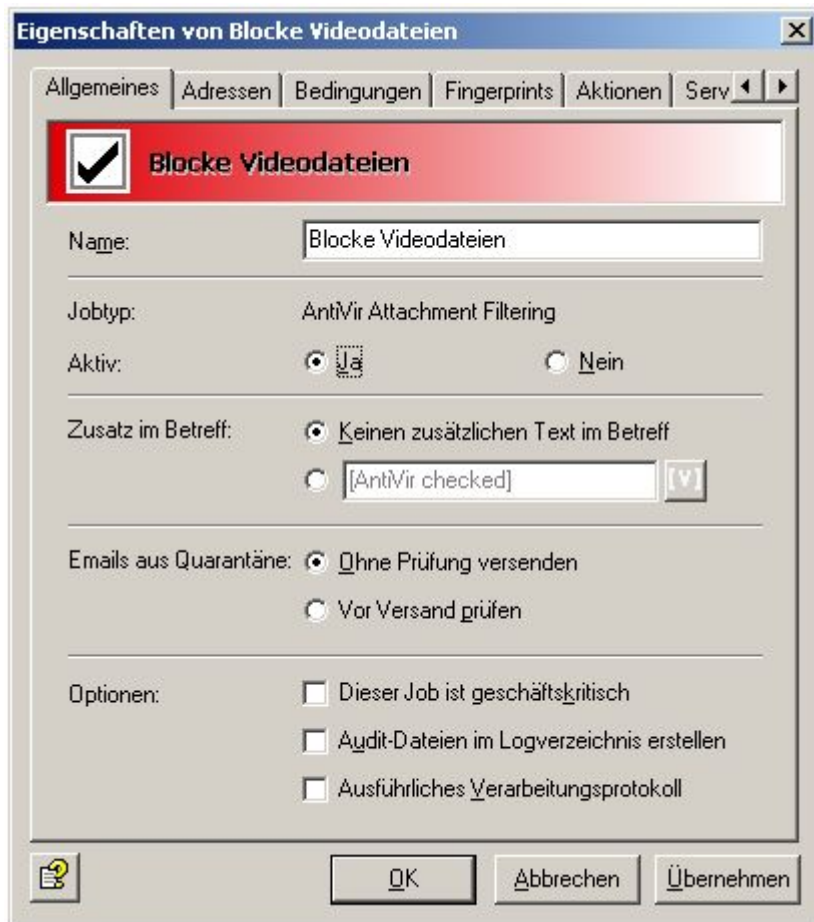
- **Bloke Archive, außer ZIP-Dateien**  
Alle komprimierten Formate außer ZIP-Dateien
- **Bloke verdächtige Anhänge**  
Bekannte gefährliche Anhänge wie Nimda etc.
- **Bloke Videodateien**  
Videoformate
- **Bloke Sounddateien**  
Soundformate
- **Bloke ausführbare Dateien**  
ausführbare Dateien (exe, com, etc.)

Als Beispiel wird hier der Job **Bloke Videodateien** behandelt. Ziehen Sie diesen Job per Drag-and-Drop in den Ordner **Mail Transport Jobs** und öffnen Sie ihn dort mit einem Doppelklick.

### Allgemeine Einstellungen

1. Auf der Registerkarte **Allgemeines** können Sie einen eigenen Namen für den Job vergeben.  
Dass der Job aktiv ist, erkennen Sie sofort an dem Hacken im Job-Symbol.
2. Setzen Sie den Job **Aktiv**.

3. Sobald Sie mit OK Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert.



Der **Zusatz im Betreff** ist vordefiniert auf **AntiVir checked**. Dieser Zusatz wird in den Betreff jeder Email eingefügt, die der Job geprüft hat.

Dieser Job bearbeitet auch solche Emails, die aus der Quarantäne wieder versendet werden. Die Send-Option beim **Versand aus der Quarantäne** ist Jobübergreifend und hat Priorität. Wenn Sie eine Mail also mit der **Quarantäne-Sende-Option Zustellen ohne weitere AntiVir Prüfung dieses Servers** erneut versenden, wird die Mail durch keinen Job bearbeitet. Setzen Sie beim Versand aus der Quarantäne die Send-Option deshalb auf **Email erneut durch AntiVir Jobs bearbeiten lassen**.

## Adressbedingungen einrichten

Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll.

Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus.

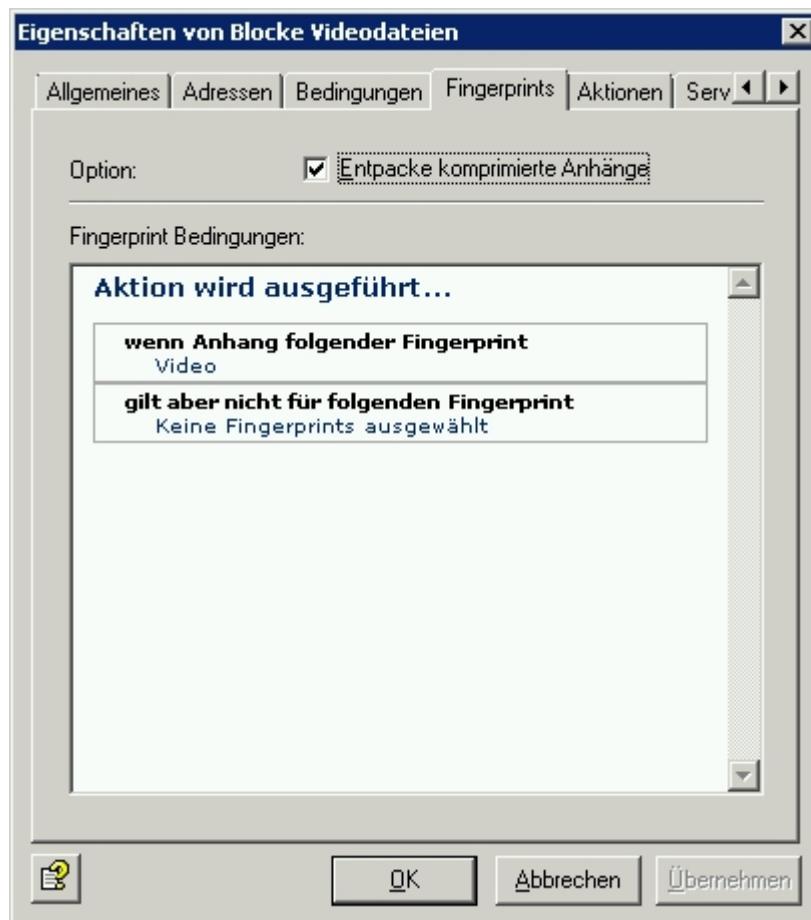
## Inhaltliche Bedingungen einrichten

Auf der Registerkarte **Bedingungen** können Sie die Ausführungsbedingungen eines Jobs festlegen.

**Warnung:** Die inhaltlichen Bedingungen müssen gleichzeitig mit den definierten Adressbedingungen in der Registerkarte **Adressen** zutreffen, damit der Job ausgeführt wird (UND-Verknüpfung).

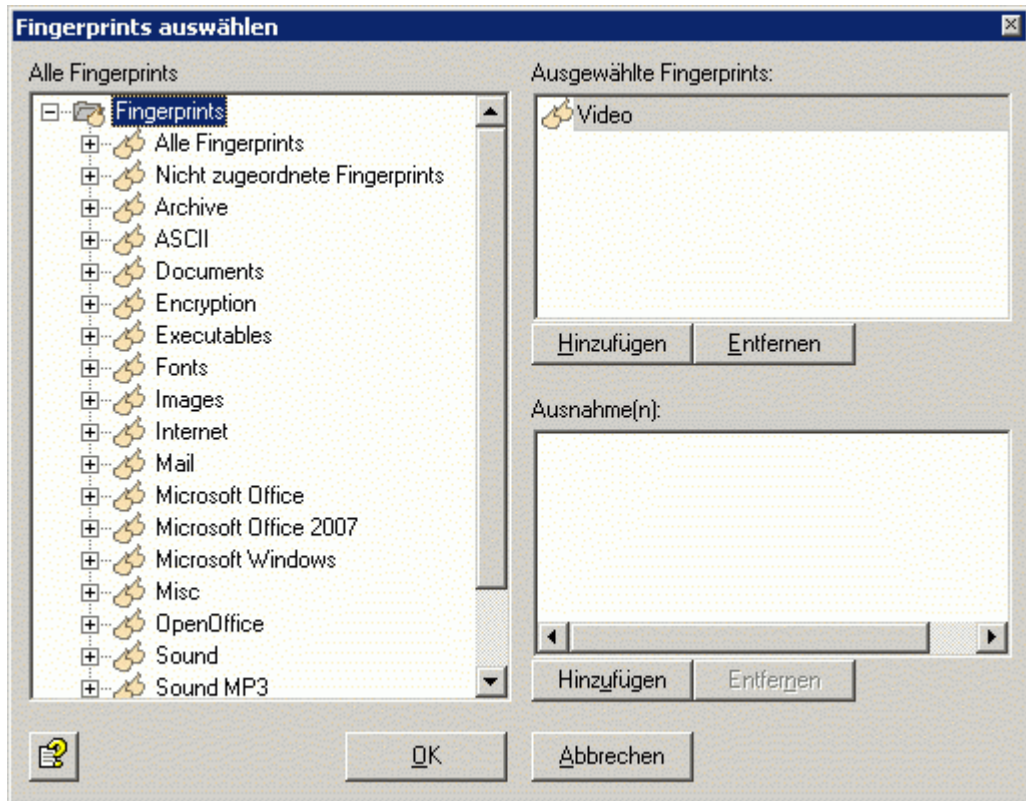
## Fingerprints auswählen

1. Wählen Sie auf der Registerkarte **Fingerprints** die verbotenen Fingerprints aus:



**Entpacke komprimierte Anhänge** bedeutet, dass der interne Entpacker die Archive aufmacht und die darin liegenden Dateien auf die angegebenen Fingerprints untersucht. Ist die Checkbox nicht aktiviert, wird nur das Archiv als oberste Datei untersucht und als gepacktes Format erkannt.

2. Fingerprint-Bedingungen: Klicken Sie auf **Video** bzw. **keine Fingerprints ausgewählt**, um aus der Liste der Fingerprints eine Fingerprintkategorie oder einen einzelnen Fingerprint zu wählen.  
Sie erhalten folgende Ansicht:



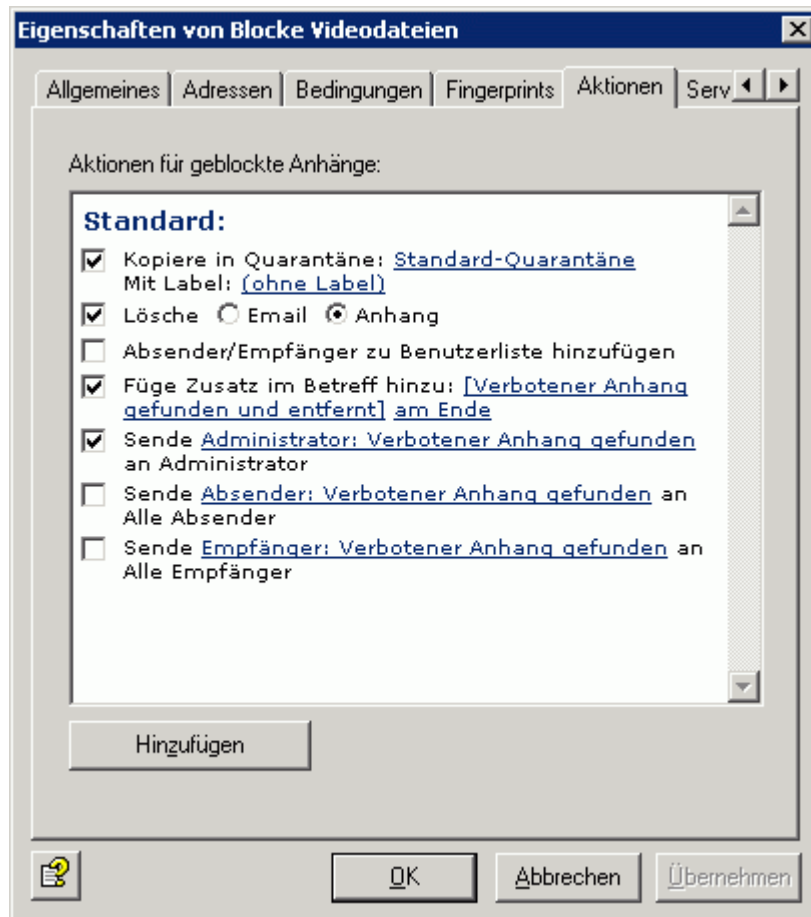
3. Mit den Schaltflächen **Hinzufügen** und **Entfernen** können Sie der Liste der verbotenen und/oder erlaubten Fingerprints ganze Kategorien oder einzelne Fingerprints zuweisen. Öffnen Sie dafür die Kategorie im linken Fenster per Doppelklick oder mit einem Klick auf das +.

**Hinweis:** Sie können eine Kategorie wie z. B. Video unter **Ausgewählte Fingerprints** und einen einzelnen oder mehrere Fingerprint(s) dieser Kategorie unter **Ausnahme(n)** eintragen. Um eine bessere Übersicht zu behalten, sollten Sie nicht zu viele Kategorien von einem Job überprüfen lassen.



## Aktionen festlegen

1. In der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, **wenn der Job einen verbotenen Fingerprint als Anhang gefunden hat**:



Eine Kopie der Email wird in Quarantäne verschoben und die betroffenen Anhänge werden gelöscht. Das beinhaltet, dass die Email zwar an den Empfänger zugestellt wird, die verbotenen Anhänge aber entfernt werden. Eine Benachrichtigung über den gefundenen Fingerprint wird an Administrator versandt. Diese Benachrichtigung wird aus dem Pull Down-Menü der verfügbaren Benachrichtigungsvorlagen ausgewählt und diese können individuell mit der HTML-Symbolleiste oder direkt mit HTML-Formatbefehlen gestaltet werden.

2. Sie können mit der Schaltfläche **Hinzufügen** weitere Aktionen definieren.

### 5.7.6 Email-Größe einschränken - Jobbeispiel

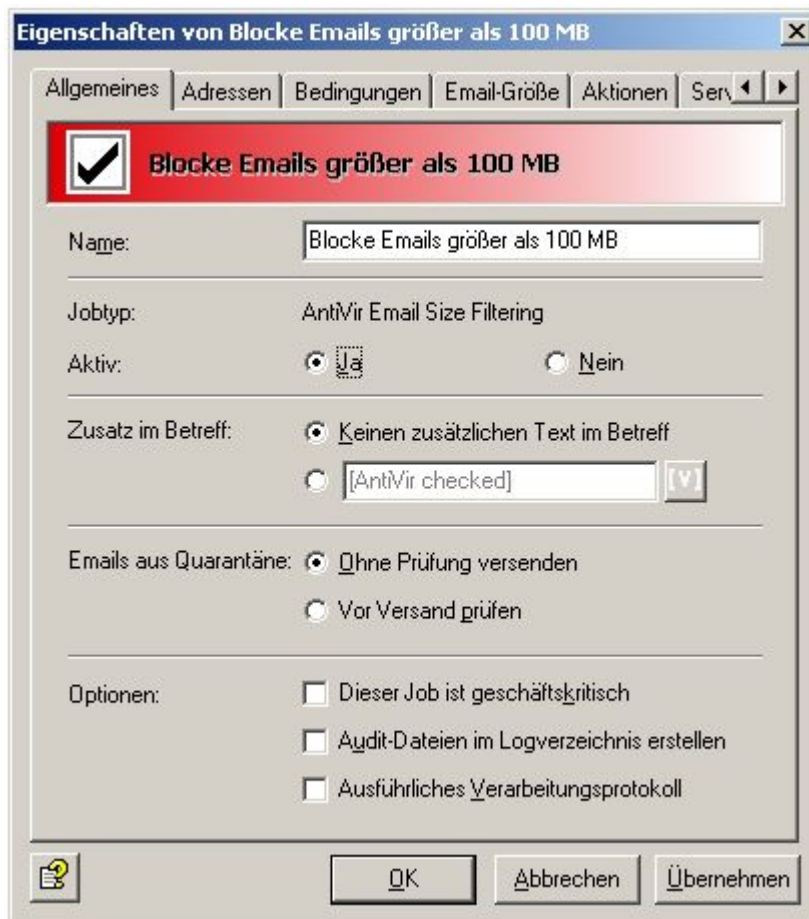
Unter **Richtlinien-Konfiguration - Jobvorlagen** finden Sie den Job **Blocke Emails größer als 100 MB**.

**Hinweis:** Die Einschränkung der Email-Größe bezieht sich auf die gesamte Email inklusive Betreff, Nachrichtentext, Header und Anhang.

Ziehen Sie diesen Job per Drag-and-Drop in den Ordner **Mail Transport Jobs** und öffnen Sie ihn dort mit einem Doppelklick.

## Allgemeine Einstellungen

Auf der Registerkarte **Allgemeines** können Sie einen eigenen Namen für den Job vergeben. Setzen Sie den Job **Aktiv**. Sobald Sie mit **OK** Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert. Dass der Job aktiv ist, erkennen Sie sofort an dem Haken im Job-Symbol.



Der **Zusatz im Betreff** ist vordefiniert auf **AntiVir checked**. Dieser Zusatz wird in den Betreff jeder Email eingefügt, die der Job geprüft hat.

Dieser Job bearbeitet auch solche Emails, die aus der Quarantäne wieder versendet werden. Die Sende-Option beim **Versand aus der Quarantäne** ist jobübergreifend und hat Priorität. Wenn Sie eine Mail also mit der **Quarantäne-Sende-Option Zustellen ohne weitere AntiVir Prüfung dieses Servers** erneut versenden, wird die Mail durch keinen Job bearbeitet. Setzen Sie beim Versand aus der Quarantäne die Sende-Option deshalb auf **Email erneut durch AntiVir Jobs bearbeiten lassen**.

## Adressbedingungen einrichten

Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus.

Wie Sie Adresslisten am besten einsetzen und eine genaue Beschreibung der Vorgehensweise finden Sie in [Adresslisten](#).

## Inhaltliche Bedingungen einrichten

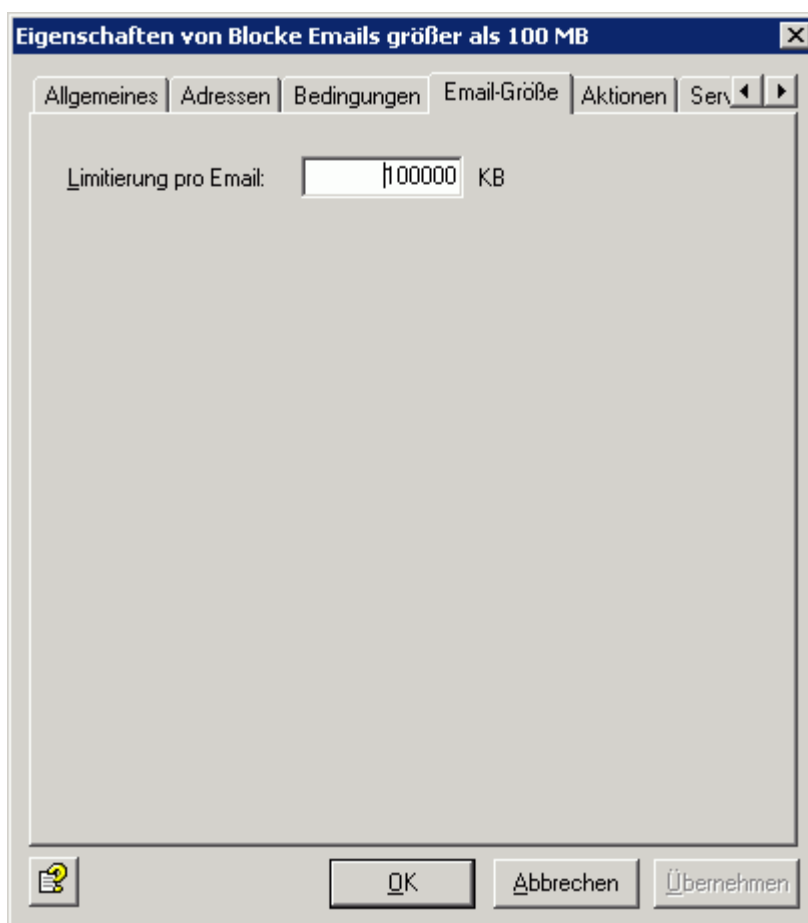
Auf der Registerkarte **Bedingungen** können Sie die Ausführungsbedingungen eines Jobs festlegen.

Wie Sie Bedingungen am besten einsetzen finden Sie in [Bedingungen](#).

**Warnung:** Die inhaltlichen Bedingungen müssen gleichzeitig mit den definierten Adressbedingungen in der Registerkarte **Adressen** zutreffen, damit der Job ausgeführt wird (UND-Verknüpfung).

## Email-Größe festlegen

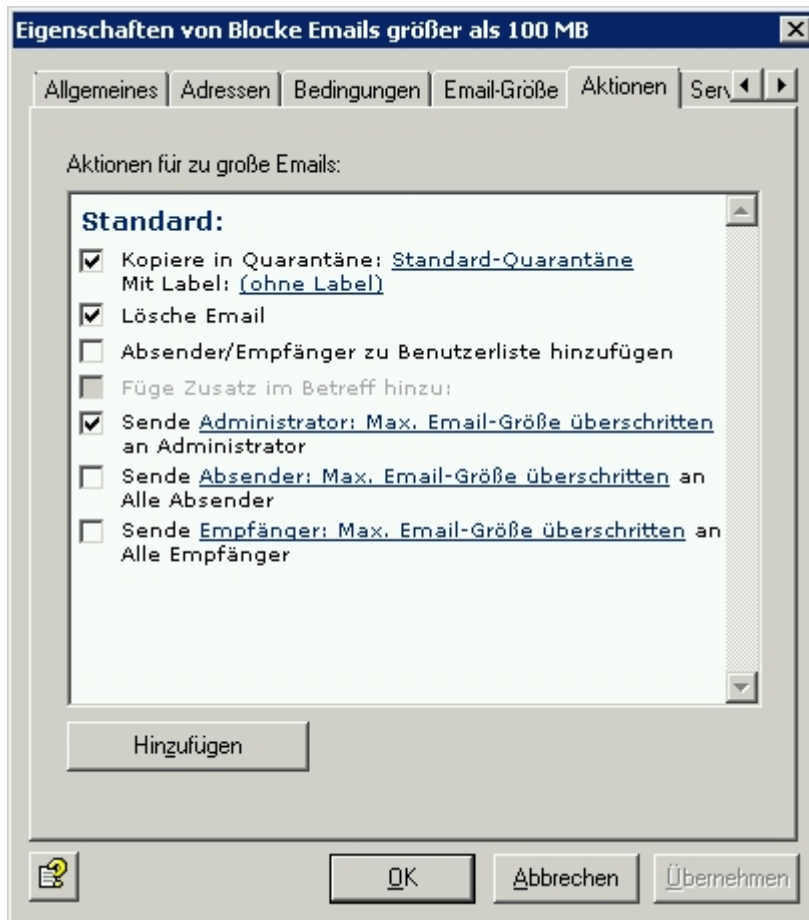
Auf der Registerkarte **Email-Größe** geben Sie die gewünschte maximale Email-Größe in Kilobyte an:



Jede ein- und ausgehende Email darf also maximal 100.000 Kilobyte groß sein.

## Aktionen festlegen

In der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn der Job eine zu große Email festgestellt hat.



Als Aktion für die Email wird eine Kopie in die Quarantäne gestellt und die betroffene Email gelöscht. Das beinhaltet, dass die Email nicht an den Empfänger zugestellt wird. Eine Benachrichtigung über die zu große Email wird als Warnung an den Administrator versandt. Die Benachrichtigung wird aus dem Pull Down-Menü der verfügbaren Benachrichtigungsvorlagen ausgewählt und diese können individuell mit der HTML-Symbolleiste oder direkt mit HTML-Formatbefehlen gestaltet werden.


Sie können mit der Schaltfläche **Hinzufügen** weitere Aktionen definieren.

Die Vorgehensweise entnehmen Sie bitte der Beschreibung in "Virenprüfung einschalten - Jobbeispiel" unter [Aktionen festlegen](#).

## Server auswählen

Die Auswahl der Server wird wie in der Beschreibung zu [Server auswählen](#) durchgeführt.

## Konfiguration Speichern

Speichern Sie die Konfiguration der AntiVir Exchange Management Konsole jedes Mal, wenn Sie Änderungen durchgeführt haben. Drücken Sie dafür die Schaltfläche . Die Konfiguration wird in der Datei `ConfigData.xml` gespeichert, die im Verzeichnis `Avira\AntiVir Exchange\Config\` abgelegt ist. Offene Änderungen werden durch (\*) am obersten Knoten angezeigt.

### 5.7.7 Anhangtypen und -größen verbieten - Jobbeispiel

Unter **Richtlinien-Konfiguration - Jobvorlagen** finden Sie verschiedene Jobs für das Blocken diverser Dateiformate und entsprechender Größen:

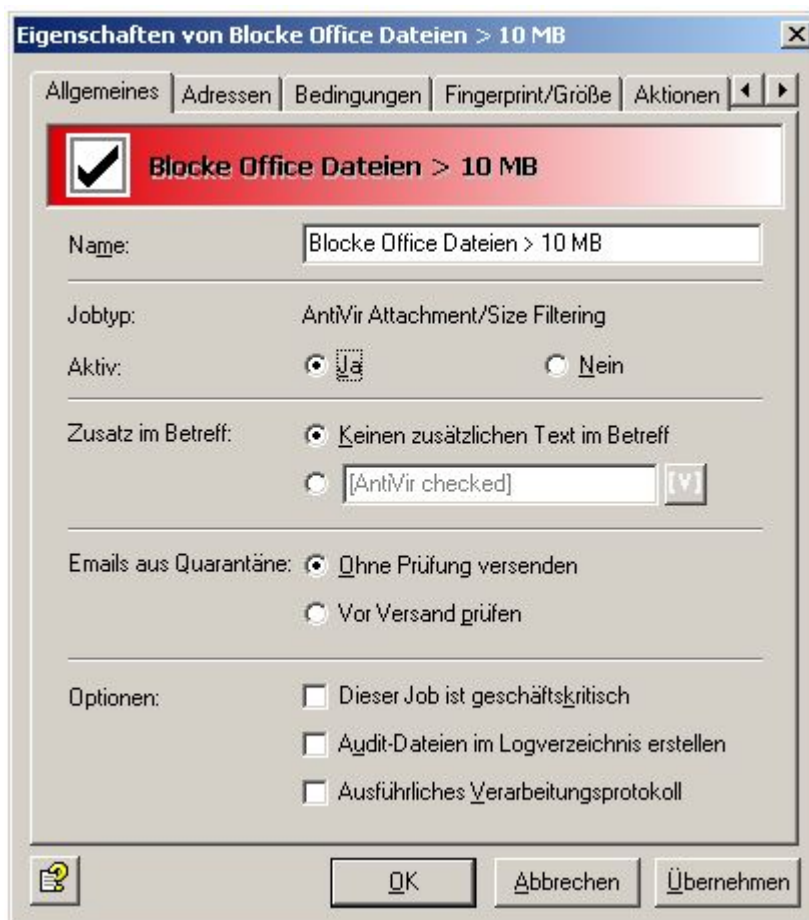
- **Blocke Office Dateien > 10 MB**  
Microsoft Office Dateien größer als 10 MB
- **Blocke Sounddateien > 5 MB**  
Sounddateien größer als 5 MB
- **Blocke Videodateien > 5 MB**  
Videodateien größer 5 MB

**Hinweis:** Die Prüfung auf Anhangformat und -größe betrifft im Gegensatz zur Prüfung der Email-Größe nur die Anhänge. Betreff, Nachrichtentext und die Kopfdaten der Email bleiben bei dieser Prüfung unberücksichtigt.

Als Beispiel wird hier der **Blocke Office Dateien > 10 MB** behandelt. Ziehen Sie diesen Job per Drag-and-Drop in den Ordner **Mail Transport Jobs** und öffnen Sie ihn dort mit einem Doppelklick.

## Allgemeine Einstellungen

Auf der Registerkarte **Allgemeines** können Sie einen eigenen Namen für den Job vergeben. Setzen Sie den Job **Aktiv**. Sobald Sie mit **OK** Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert. Dass der Job aktiv ist, erkennen Sie sofort an dem Haken im Job-Symbol.



Der **Zusatz im Betreff** ist vordefiniert auf **AntiVir checked**. Dieser Zusatz wird in den Betreff jeder Email eingefügt, die der Job geprüft hat.

Dieser Job bearbeitet auch solche Emails, die aus der Quarantäne wieder versendet werden. Die Sende-Option beim **Versand aus der Quarantäne** ist jobübergreifend und hat Priorität. Wenn Sie eine Mail also mit der **Quarantäne-Sende-Option Zustellen ohne weitere AntiVir Prüfung dieses Servers** erneut versenden, wird die Mail durch keinen Job bearbeitet. Setzen Sie beim Versand aus der Quarantäne die Sende-Option deshalb auf **Email erneut durch AntiVir Jobs bearbeiten lassen**.

### Adressbedingungen einrichten

Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus.

Wie Sie Adresslisten am besten einsetzen und eine genaue Beschreibung der Vorgehensweise finden Sie in [Adresslisten](#).

### Inhaltliche Bedingungen einrichten

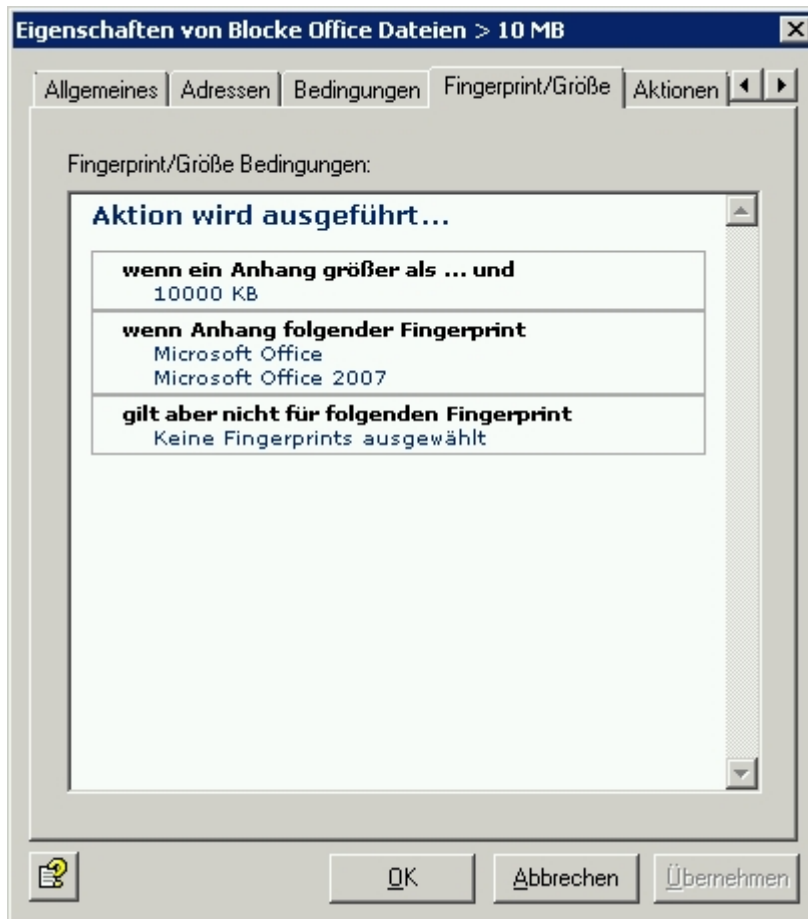
Auf der Registerkarte **Bedingungen** können Sie die Ausführungsbedingungen eines Jobs festlegen.

Wie Sie Bedingungen am besten einsetzen finden Sie in [Bedingungen](#).

**Warnung:** Die inhaltlichen Bedingungen müssen gleichzeitig mit den definierten Adressbedingungen in der Registerkarte **Adressen** zutreffen, damit der Job ausgeführt wird (UND-Verknüpfung).

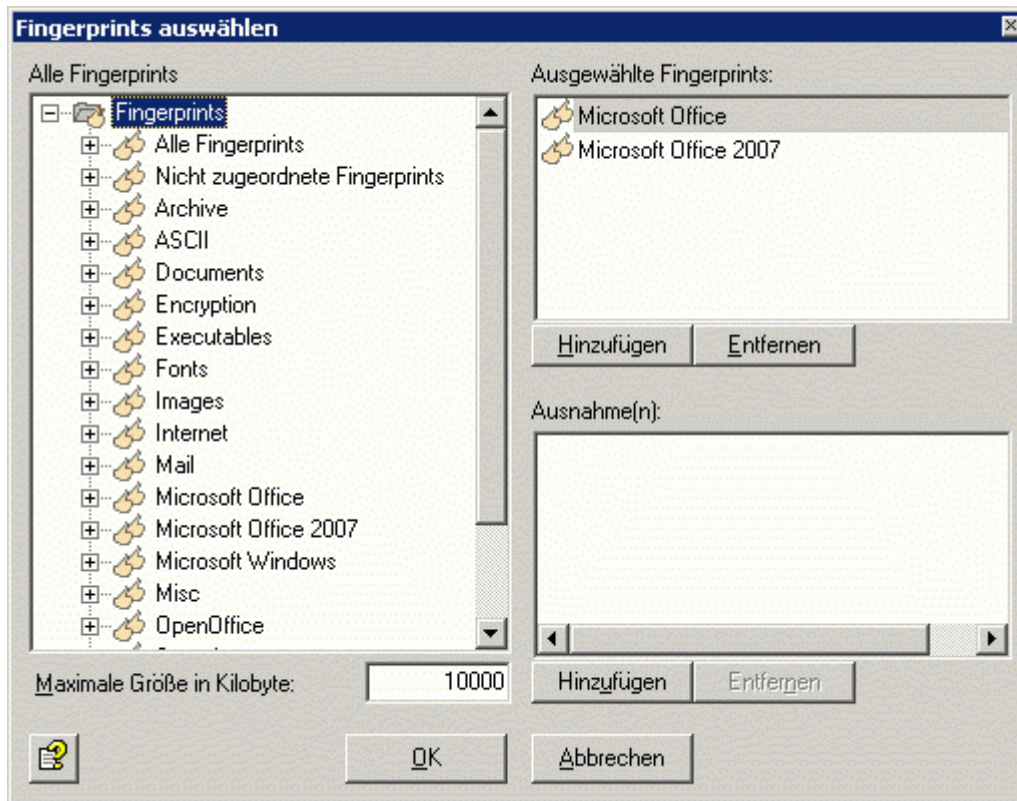
## Fingerprint/Größe bestimmen

Auf der Registerkarte **Fingerprint/Größe** geben Sie die gewünschte maximale Email-Größe und das Fingerprintformat an:



**Hinweis:** Im Gegensatz zur einfachen Fingerprint-Prüfung steht hier die Option **Entpacke komprimierte Anhänge** nicht zur Verfügung. Wenn Sie komprimierte Dateien in der Größe beschränken wollen, geben Sie diese Formate in diesem Job einfach an.

**Fingerprint/Größe-Bedingungen:** Klicken Sie auf **10.000**, um die Größe in Kilobyte festzulegen bzw. auf Microsoft Office, um aus der Liste der Fingerprints eine Fingerprintkategorie, einen einzelnen Fingerprint oder die maximale Größe zu wählen. Sie erhalten folgende Ansicht:



Mit den Schaltflächen **Hinzufügen** und **Entfernen** können Sie der Liste der verbotenen und/oder erlaubten Fingerprints ganze Kategorien oder einzelne Fingerprints zuweisen. Öffnen Sie dafür die Kategorie im linken Fenster per Doppelklick oder mit einem Klick auf das +.

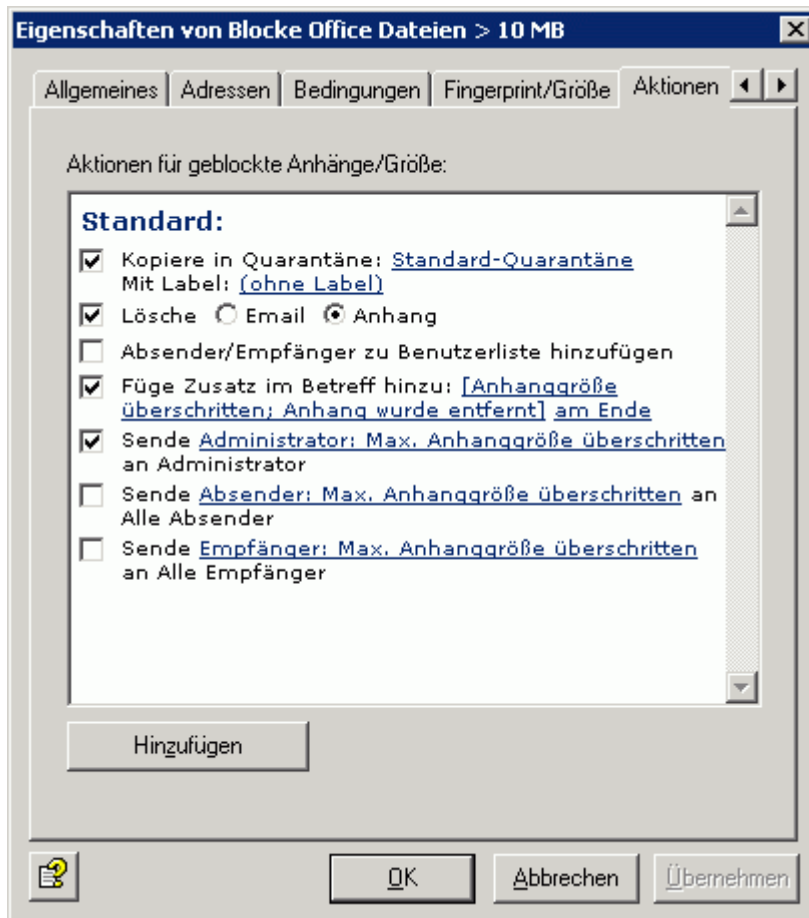
**Hinweis:** Sie können eine Kategorie wie z.B. "Microsoft Office" unter **Ausgewählte Fingerprints** und einen einzelnen oder mehrere Fingerprint(s) dieser Kategorie unter **Ausnahme(n)** eintragen. Um eine bessere Übersicht zu behalten, sollten Sie nicht zu viele Kategorien von einem Job überprüfen lassen.

Näheres über Fingerprints und über die Eingabe von Namens- und Binärmustern finden Sie unter [Fingerprints konfigurieren](#).

## Aktionen festlegen

In der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, **wenn der Job eine Email gefunden hat, die durch einen Attachment/ Size-Job verboten war**.





Eine Kopie der Email wird in die Quarantäne gestellt und die betroffenen Anhänge gelöscht. Die Email wird also ohne ihren Anhang dem Empfänger zugestellt. Eine Benachrichtigung über die gefundene Einschränkung geht an den Administrator. Diese Benachrichtigung wird aus dem Pull Down-Menü der verfügbaren Benachrichtigungsvorlagen ausgewählt und diese können individuell mit der HTML-Symbolleiste oder direkt mit HTML-Formatbefehlen gestaltet werden.

Sie können mit der Schaltfläche **Hinzufügen** weitere Aktionen definieren.

Die Vorgehensweise entnehmen Sie bitte der Beschreibung in "Virenprüfung einschalten - Jobbeispiel" unter [Aktionen festlegen](#).

## Server auswählen

Die Auswahl der Server wird wie in der Beschreibung zu [Server auswählen](#) durchgeführt.

## 6 AntiVir Wall

Mit AntiVir Wall prüfen Sie den Textinhalt der Email oder der Anhänge, klassifizieren Emails nach Inhalten, beschränken Email-Adressen im Ein-/Ausgang oder limitieren die Anzahl der Empfänger pro Email.

### 6.1 Jobtypen

- die Adressprüfung  
Job: **AntiVir Wall Email Address Filtering**
- die Inhaltsprüfung  
Job: **AntiVir Wall Content Filtering**
- die Anti-Spam-Prüfung  
Job: **AntiVir Wall Spam Filtering**
- Prüfung auf Anzahl der Empfänger  
Job: **AntiVir Wall Recipient Limit Filtering**

**Hinweis:** Legen Sie für jeden Einschränkungstyp einen separaten Job an! Die Jobtypen lassen sich später nicht mehr ändern.

Die genaue Vorgehensweise für die Job-Einrichtung entnehmen Sie bitte den Jobbeispiel-Beschreibungen, z. B. [Absender und/oder Empfänger verbieten - Jobbeispiel](#).

### 6.2 Adressprüfung

Die Adressprüfung konzentriert sich auf die Absender und die Empfänger einer Email. Dabei können Sie bestimmte Absender verbieten, so dass keine Email mehr von diesen zu Ihren Benutzern gelangt oder aber auch bestimmte Empfänger, so dass keiner Ihrer Mitarbeiter (oder nur ausgewählte) an gewisse Empfänger Emails versenden können.

Bei der Adressprüfung können folgende Objekte verwendet werden:

- Mail-Enabled Active Directory Benutzer
- Mail-Enabled Active Directory Gruppen
- Mail-Enabled Active Directory Kontakte
- Frei definierbare SMTP Adressen inkl. Wildcards
- [INTERN] = Als in der Avira AntiVir Exchange definierten internen Domänen
- [EXTERN] = Alle Adressen, die nicht [INTERN] sind
- "Administrator" = Die in der Avira AntiVir Exchange als Administrator definierten Email-Adressen.

Maßgebend für die Definition, ob es sich um einen Absender oder einen Empfänger handelt, ist immer der Eintrag in den entsprechenden Feldern der Email. Ein Absender kann also sowohl ein Mitarbeiter Ihres Unternehmens sein, der eine Email nach außen sendet, als auch eine externe Person, die einem Mitarbeiter Ihres Unternehmens eine Email schickt. Sie können sowohl Absender als auch Empfänger als Person oder als Gruppe definieren.

Bei der Adressprüfung sind generell folgende Wildcards möglich:

- Stern (\*)  
Der Stern symbolisiert den Platzhalter für ein oder mehrere beliebige Buchstaben und/oder Zahlen. Der Stern kann mehrfach mitten im Begriff eingesetzt werden.
- Fragezeichen (?)  
Das Fragezeichen dagegen ist der Platzhalter für ein einziges Zeichen. Auch das Fragezeichen kann mehrfach mitten im Begriff vorkommen.

Wenn Sie einen verbotenen Absender angeben, können Sie statt einzelner Email-Adressen auch tom\*@\*. nehmen. Das heißt, dass alle Emails, die von einem Tom mit beliebiger Erweiterung (also auch Nachnamen) von welcher Domäne auch immer gesendet werden, als Absender verboten sind. Darunter fällt dann auch Ihr eigener Mitarbeiter namens Tom Jones, der somit unter die Einschränkung und dessen Emails unter die definierten Aktionen fallen. Eine bestimmte Domäne können Sie zum Beispiel als \*@domain.com definieren. Damit gelten alle Absender bzw. Empfänger dieser Domäne als verboten. Einen Job zur Adressprüfung mit dem Verbot einer ganzen Domäne sollten Sie nur mit großer Vorsicht serverübergreifend für alle anlegen. Es ist nicht immer klar, welche Adressen privater und welche beruflicher Natur sind. Bedenken Sie, dass kleinere Geschäftspartner durchaus Email-Adressen unter der Domäne @tonline.de oder @aol.com besitzen.

Die Adressprüfung ist ein einfaches Mittel, bekannte Spamadressen auszufiltern. Die "üblichen Verdächtigen" können vom Job auf dem Server abgefangen und sofort gelöscht werden.

**Hinweis:** Da bei den Adressprüfungsjobs die Eintrittsbedingung mit der Jobrestriktionsbedingung übereinstimmt, wird ein ggf. konfigurierter **Zusatz im Betreff** im OK-Fall - im Gegensatz zu den anderen Jobtypen - auch angefügt, wenn die Eintrittsbedingung nicht zutreffend ist.

- Gesamte Email in Quarantäne kopieren
- Zusatz im Betreff
- Betroffene Email löschen und nicht zustellen
- Administrator benachrichtigen
- Absender benachrichtigen
- Empfänger benachrichtigen
- Andere, frei wählbare Personen benachrichtigen
- Ausführen einer externen Anwendung
- Avira-Header-Feld hinzufügen
- X-Header-Feld hinzufügen
- Email umleiten

### 6.2.1 Absender und/oder Empfänger verbieten - Jobbeispiel

Unter **Richtlinien-Konfiguration - Jobvorlagen** finden Sie einen vorkonfigurierten Job für die Adressprüfung. Kopieren Sie den Job **Anti-Spam anhand Emailadressen** unter **Mail-Transport Jobs** und öffnen Sie ihn mit einem Doppelklick.

## Allgemeine Einstellungen


Auf der Registerkarte **Allgemeines** können Sie einen eigenen Namen für den Job vergeben. Setzen Sie den Job **Aktiv**. Sobald Sie mit **OK** Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert.



Der **Zusatz im Betreff** ist vordefiniert auf **AntiVir Wall checked**. Dieser Zusatz wird in den Betreff jeder Email eingefügt, die der Job geprüft hat.

Dieser Job bearbeitet keine Mails, die aus der Quarantäne wieder versendet werden, selbst wenn beim Versand aus der **Quarantäne (AntiVir Monitor - <Email auswählen> - Alle Aufgaben - Aus Quarantäne senden)** die Sende-Option **Email erneut durch AntiVir Jobs bearbeiten lassen** aktiviert wurde. Die Option **Ohne Prüfung versenden** bedeutet, dass dieser Job generell bei einem Mail-Versand aus der Quarantäne übergangen wird.

Näheres zum erneuten Versand aus der Quarantäne finden Sie in [Aus Quarantäne senden](#). Im Kapitel **AntiVir** ist die Option **Dieser Job ist geschäftskritisch** näher beschrieben.

Speichern Sie die Konfiguration der Avira AntiVir Exchange Konsole jedes Mal, wenn Sie Änderungen durchgeführt haben. Drücken Sie dafür die Schaltfläche . Die Konfiguration wird in der Datei `ConfigData.xml` gespeichert, die im Verzeichnis `Avira\AntiVir Exchange\Config\` abgelegt ist. Offene Änderungen werden durch (\*) am obersten Knoten angezeigt.

## Adressbedingungen einrichten

Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus.

Wie Sie Adresslisten am besten einsetzen und eine genaue Beschreibung der Vorgehensweise finden Sie in [Adresslisten](#).

## Inhaltliche Bedingungen einrichten

Auf der Registerkarte **Bedingungen** können Sie die Ausführungsbedingungen eines Jobs festlegen.

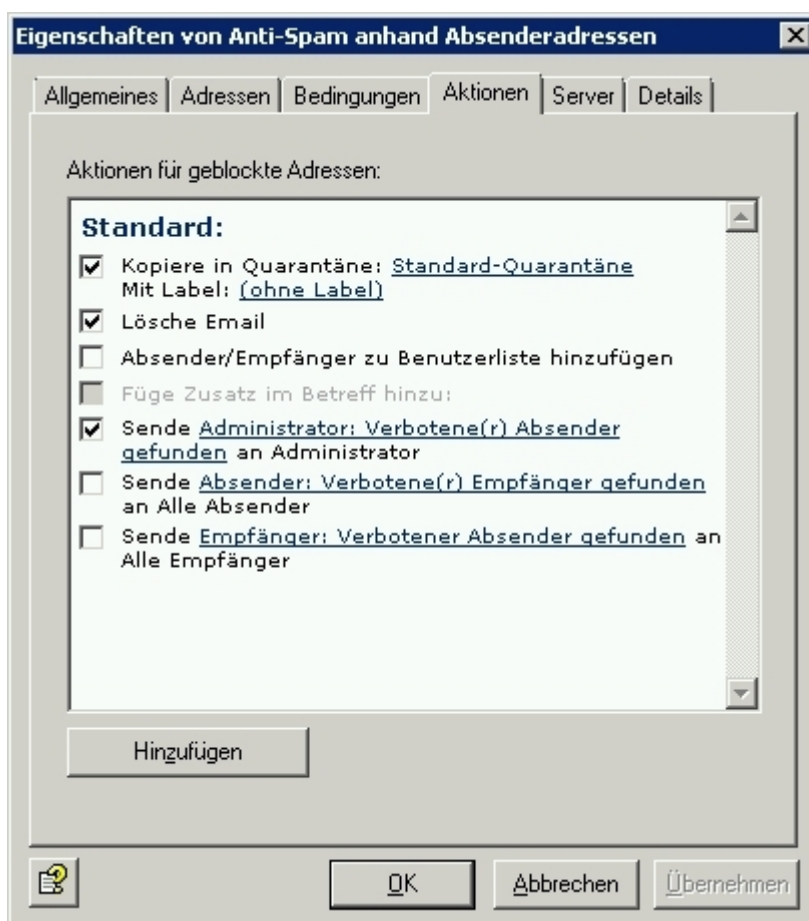
Wie Sie Bedingungen am besten einsetzen finden Sie in [Bedingungen](#).

**Warnung:** Die inhaltlichen Bedingungen müssen gleichzeitig mit den definierten Adressbedingungen in der Registerkarte **Adressen** zutreffen, damit der Job ausgeführt wird (UND-Verknüpfung).

## Aktionen festlegen

In der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn der Job eine Email mit verbotenen Adressen gefunden hat.

Als Aktion wird eine Kopie in die Quarantäne gestellt und die betroffene Email gelöscht. Das beinhaltet, dass die Email dem Empfänger nicht zugestellt wird. Eine Benachrichtigung über die Verletzung der Adress-Richtlinien wird als Warnung an den Administrator versandt. Die Benachrichtigung wird aus dem Pull Down-Menü der verfügbaren Benachrichtigungsvorlagen ausgewählt und diese können individuell mit der HTML-Symboleiste oder direkt mit HTML-Formatbefehlen gestaltet werden.



Sie können mit der Schaltfläche **Hinzufügen** weitere Aktionen definieren.

Die Vorgehensweise entnehmen Sie bitte der Beschreibung in "Virenprüfung einschalten - Jobbeispiel" unter [Aktionen festlegen](#).

## Server auswählen

Die Auswahl der Server wird wie in der Beschreibung zu [Server auswählen](#) durchgeführt.

## 6.3 Inhaltsprüfung mit Wortlisten

AntiVir Wall verwendet vordefinierte Wortlisten, um nach unerwünschten Textinhalten zu suchen.

Dabei können folgende Bestandteile der Email geprüft werden:

- Betreff
- Nachrichtentext
- Anhänge

Die Inhaltssuche kann auf bestimmte Absender bzw. Empfänger eingeschränkt werden. Damit können z. B. nur von außen eintreffende Emails auf Pornographie, Rassismus etc. untersucht werden. Bei Emails von internen Absendern nach außen könnten Sie hingegen die Emails nach Firmeninterna durchsuchen lassen. Die Emails werden anhand der zu verwendenden Wortliste durchsucht und die von Ihnen angegebenen Wörter oder Sätze innerhalb der Email gelten ab einem bestimmten Schwellwert als verboten, sobald diese Wortliste im Job aktiviert ist. Auch die Zeichenumsetzung wird im Job festgelegt. Bei erreichtem Schwellwert setzt der Job die Aktionen in Gang, die Sie vorher in der Registerkarte **Aktionen** festgelegt haben.

Hier ein Beispiel für die Arbeitsweise eines Jobs für die Inhaltsprüfung:

Der Job prüft eine Email mit dem Ergebnis: Verbotener Inhalt gefunden. Daraufhin wird ein Alarm ausgelöst und eine Reihe von Aktionen in Gang gesetzt, die Sie selbst im Job unter Aktionen definieren können. Wir nehmen an, dass Sie Folgendes festgelegt haben:

1. Die Email wird in den von Ihnen gewählten Ordner (Quarantäne) verschoben und dem Empfänger nicht zugestellt.
2. Es werden Nachrichten an Administrator, Absender und Empfänger erstellt, die mit den relevanten Informationen des Wall-Jobs versehen sind.

Die möglichen Aktionen sind die gleichen wie bei der Adressprüfung.

### 6.3.1 Wortlisten einrichten

1. Klicken Sie auf **Basis Konfiguration - Utility-Einstellungen - Wortlisten**.
2. Öffnen Sie mit einem Doppelklick eine Wortliste im rechten Fenster.
3. Vergeben Sie auf der Registerkarte **Allgemeines** einen Namen für die Wortliste.
4. Geben Sie der Wortliste eine **Wertigkeit** von 1 bis 200.

Diese Wertigkeit gilt pro Wort oder Phrase und bestimmt sowohl das Verhältnis zu anderen Wortlisten als auch, wie stark die Wortliste im Job berücksichtigt wird.

Näheres zu Wertigkeiten finden Sie in [Textinhalte prüfen und verbieten - Jobbeispiel](#).



5. Klicken Sie in das Eingabefeld für die Worte und fügen Sie die Wörter/ Phrasen hinzu, die Sie verbieten wollen.

Die einzelnen Wörter/Phrasen werden mit einem Absatz (Enter-Taste) voneinander getrennt.

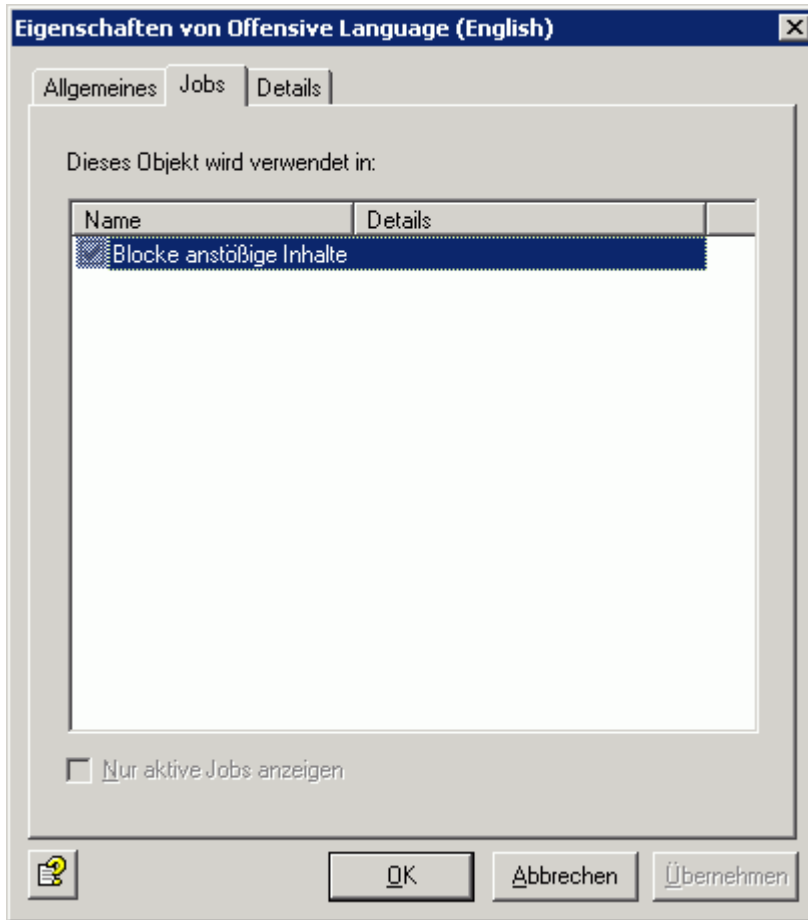
Folgende Wildcards sind in Wortlisten möglich:

- Stern (\*)  
Der Stern bedeutet, dass das gesuchte Wort/Phrase auch ein Teil größeren Wortes sein kann, aber nicht muss. Beispiele:  
\*check\* findet das einzelne Wort "check" genauso wie das Wort "checkpoint", "intercheck" oder "intercheckpoint".  
check\* findet "check" genauso wie "checkpoint".  
Der Stern muss entweder am Anfang eines Wortes/ Phrase oder am Ende eingesetzt werden.
- Pluszeichen (+)  
Das Pluszeichen bedeutet das Gleiche wie der Stern mit dem Unterschied, dass das gesuchte Wort **ein Teil** eines größeren Wortes sein muss. Beispiele:  
+check+ findet nur "checkpoint", "intercheck" oder "intercheckpoint", aber nicht "check".  
check+ findet nur "checkpoint".  
Das Pluszeichen muss ebenfalls am Anfang oder am Ende eines Wortes/Phrase eingesetzt werden.

**Hinweis:** Wenn Sie weder einen Stern noch ein Pluszeichen in Ihren Wörtern/Phrasen der Wortliste einsetzen, so muss genau dieses eingegebene Wort exakt gefunden werden. Also: Wenn Sie check eingeben, so wird auch nur das einzelne Wort "check" gefunden.


6. Sortieren Sie die Wortliste nach Wunsch aufsteigend oder absteigend, indem Sie auf  für aufsteigend und  für absteigend klicken.
7. Eine neue Wortliste erstellen Sie, indem Sie mit der rechten Maustaste auf **Wortlisten** klicken und **Neu - Wortliste** wählen.

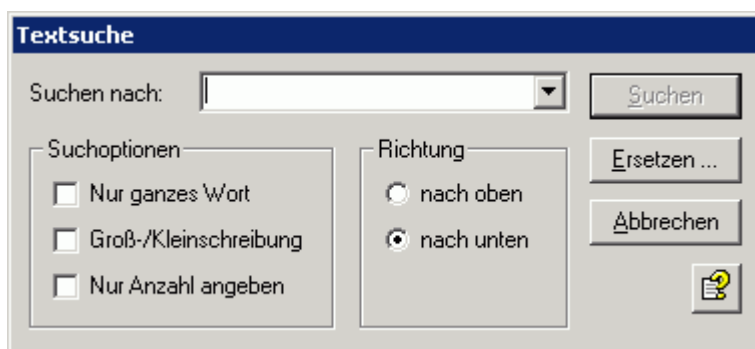
In welche Jobs die Wortliste eingebunden ist, ersehen Sie aus der Registerkarte **Jobs**:



**Hinweis:** Um die Wortlisten im Job einzusetzen, wählen Sie in der Richtlinien-Konfiguration einen Content-Filtering Job aus, aktivieren die entsprechende Wortliste und bestimmen einen Gesamt-Schwellwert (von 1 bis 10.000). Sobald dieser Schwellwert durch das Addieren aller Wertigkeiten (gefundene Wörter) der aktiven Wortlisten erreicht wurde, treten die definierten Aktionen in Kraft. Nähere Informationen erhalten Sie unter [Textinhalte prüfen und verbieten - Jobbeispiel](#).

## Textsuche in Wortlisten

1. Sie können in Wortlisten nach Begriffen suchen und sie ggf. ersetzen. Öffnen Sie die Wortliste mit einem Doppelklick und klicken Sie auf das Symbol für Textsuche .



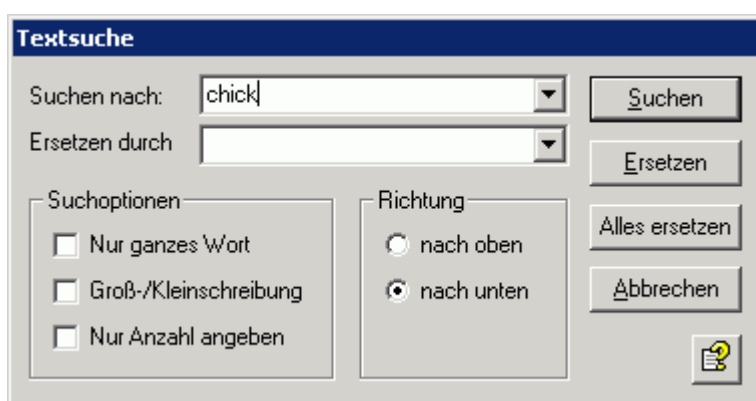


Wenn Sie keine Zusatzoption angeben, wird die Zeichenfolge überall gefunden, also auch in Teilen eines Wortes oder einer Phrase.

- **Nur ganzes Wort:**  
Als Trennzeichen zwischen Wörtern gelten alle nicht-alphanumerischen Zeichen inklusive eines Absatz- bzw. Zeilenwechsels.
- **Groß-/Kleinschreibung:**  
Berücksichtigt die Groß- und Kleinschreibung bei der Suche.
- **Nur Anzahl angeben:**  
Die Treffer werden nicht direkt "angesprungen", sondern durchgezählt und das Ergebnis in Form einer Mitteilung ausgegeben:



2. Klicken Sie auf die Schaltfläche **Ersetzen**, wenn Sie einen bestimmten Begriff durch einen anderen ersetzen möchten:



Die Textsuche können Sie auch für das Suchen und Ersetzen in eigenen Adressen verwenden. Siehe dazu [Adresslisten](#).

### 6.3.2 Textinhalte prüfen und verbieten - Jobbeispiel

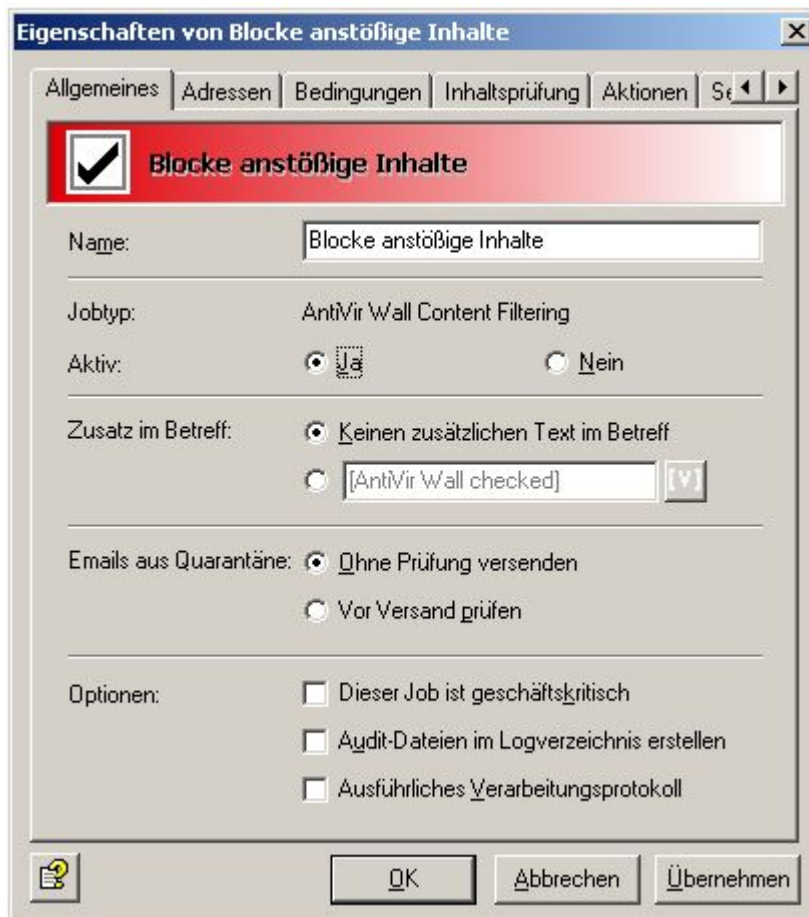
Unter **Richtlinien-Konfiguration - Jobvorlagen** finden Sie verschiedene Jobs für die Inhaltsprüfung mit Wortlisten:

- **Blocke anstößige Inhalte**  
Suchen Email ordinärer und pornografischer Sprache
- **Blocke Scriptkommandos**  
Suchen Email Script-Befehlen, die Schaden anrichten können
- **Blocke E-Mails mit Lebensläufen**  
Suchen Email Begriffen aus Lebensläufen
- **Blocke E-Mails von "Nigeria-Connection"**  
Suchen Email speziellen Begriffen in den "Nigeria"-Emails

Als Beispiel wird hier **Blocke anstößige Inhalte** behandelt. Ziehen Sie diesen Job per Drag-and-Drop in den Ordner **Mail Transport Jobs** und öffnen Sie ihn dort mit einem Doppelklick.

## Allgemeine Einstellungen

Auf der Registerkarte **Allgemeines** können Sie einen eigenen Namen für den Job vergeben. Setzen Sie den Job **Aktiv**. Sobald Sie mit **OK** Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert. Dass der Job aktiv ist, erkennen Sie sofort an dem Hacken im Job-Symbol.



Der **Zusatz im Betreff** ist vordefiniert auf **AntiVir Wall checked**. Dieser Zusatz wird in den Betreff jeder Email eingefügt, die der Job geprüft hat.

Dieser Job bearbeitet keine Mails, die aus der Quarantäne wieder versendet werden, selbst wenn beim Versand aus der **Quarantäne (AntiVir Monitor - <Email auswählen> - Alle Aufgaben - Aus Quarantäne senden)** die Sende-Option **Email erneut durch AntiVir Jobs bearbeiten lassen** aktiviert wurde. Die Option **Ohne Prüfung versenden** bedeutet, dass dieser Job generell bei einem Mail-Versand aus der Quarantäne übergangen wird.

Näheres zum erneuten Versand aus der Quarantäne finden Sie in [Aus Quarantäne senden](#). Im Kapitel **AntiVir** ist die Option [Dieser Job ist geschäftskritisch](#) näher beschrieben.

## Adressbedingungen einrichten

Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus.

Wie Sie Adresslisten am besten einsetzen und eine genaue Beschreibung der Vorgehensweise finden Sie in [Adresslisten](#).

## Inhaltliche Bedingungen einrichten

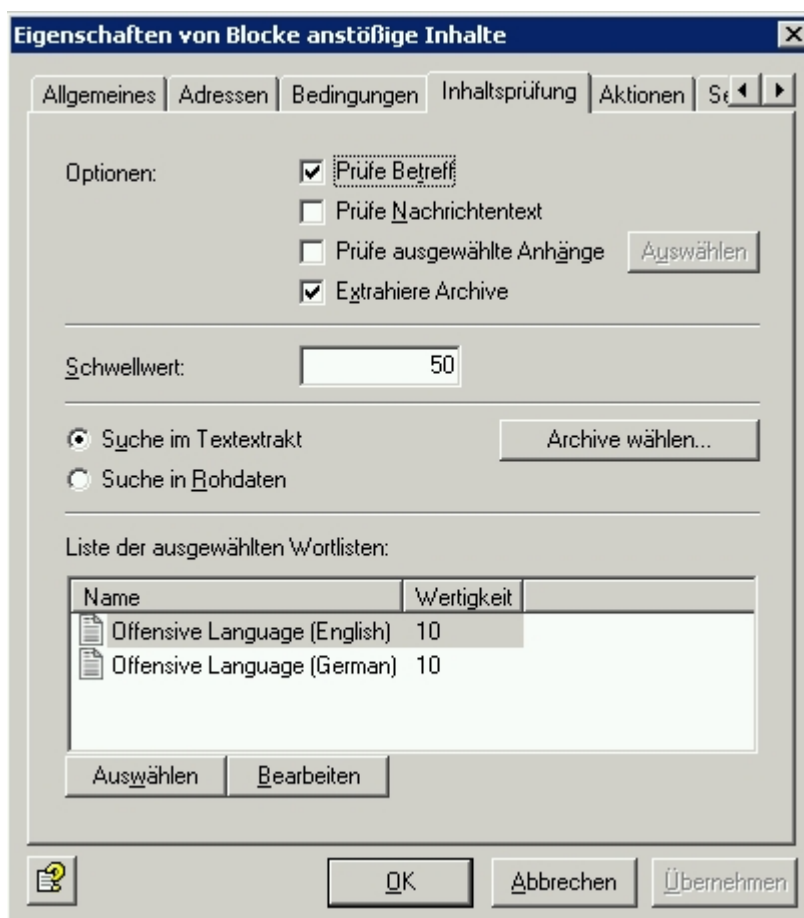
Auf der Registerkarte **Bedingungen** können Sie die Ausführungsbedingungen eines Jobs festlegen.

Wie Sie Bedingungen am besten einsetzen finden Sie in [Bedingungen](#).

**Warnung:** Die inhaltlichen Bedingungen müssen gleichzeitig mit den definierten Adressbedingungen in der Registerkarte **Adressen** zutreffen, damit der Job ausgeführt wird (UND-Verknüpfung).

## Wortlisten auswählen

In der Registerkarte **Inhaltsprüfung** stellen Sie ein, welche Wortlisten mit diesem Job aufgerufen werden sollen.



Dieser Job prüft den Betreff. Der Gesamt-Schwellwert ist auf 50 festgelegt. Damit wird bei 5 gefundenen Wörtern/Phrasen aus der Wortliste **Offensive Language (English)** oder **Offensive Language (German)** die definierten Aktionen ausgeführt.

**Die Rechnung:** Jedes Wort oder jede Phrase der Liste **Offensive Language** ist mit der Wertigkeit 10 belegt. Damit werden bei mindestens 5 gefundenen Wörtern/ Phrasen aus diesen Listen die Aktionen ausgeführt.

**Erklärung:** Jedes Wort oder jede Phrase der Liste **Offensive Language** ist mit der Wertigkeit 10 belegt. Jedes gefundene Wort/Phrase aus dieser Liste wird gezählt, die Anzahl der Wörter/Phrasen aus dieser Liste werden mit der Wertigkeit multipliziert, und die Email mit dem Schwellwert verglichen.

**In diesem Fall also:** 5 Wörter, die auf der Liste stehen, wurden in der Email gefunden. Es ergibt sich einen Wert von 5 Wörter x 10 (Wertigkeit):  $5 \times 10 = 50$ . Verglichen mit dem Schwellwert 50 = Aktion wird ausgelöst. Werden nur 4 Wörter in der Email entdeckt, beträgt der Gesamtwert nur 40 ( $4 \times 10$ ), der Schwellwert ist nicht erreicht und es wird keine Aktion in Gang gesetzt.

Ein anderes Beispiel:

Sie prüfen **mit zwei verschiedenen Wortlisten** den Betreff und den Nachrichtentext einer Email auf verbotenen Inhalt.

Der **Gesamt-Schwellwert** ist im Job auf 20 festgelegt und die erste im Job angegebene Wortliste (A) hat eine Wertigkeit von 20. Die zweite in diesem Job angegebene Wortliste (B) hat eine Wertigkeit von 1. Damit werden bei 1 gefundenen Wort/Phrase aus der Wortliste A oder alternativ bei 20 gefundenen Begriffen aus der Wortliste B die definierten Aktionen ausgeführt.

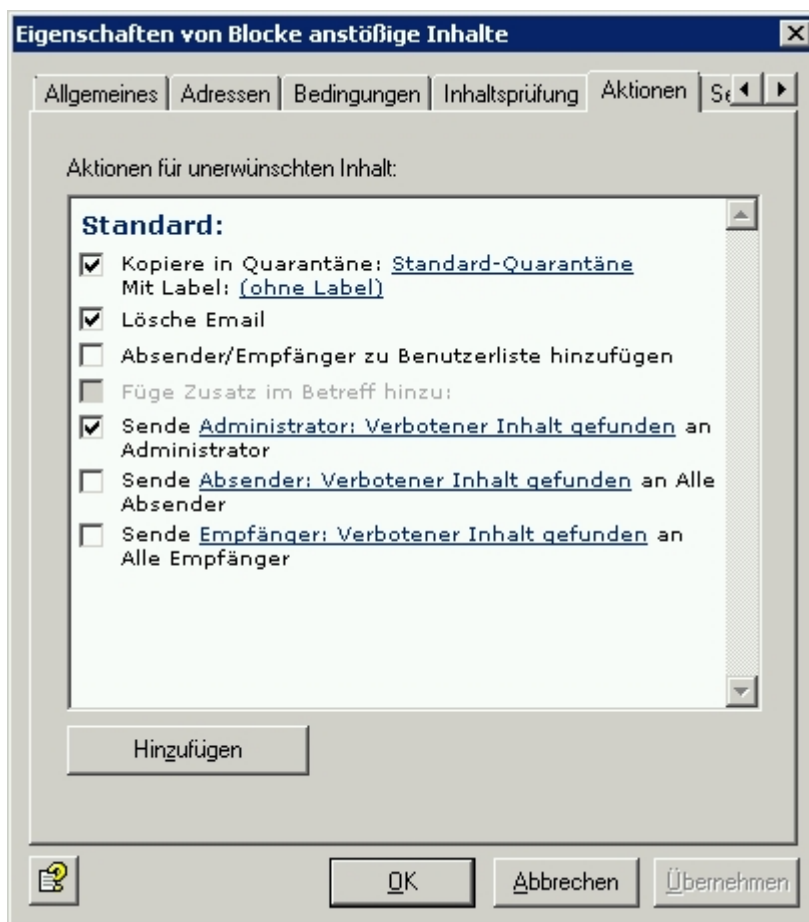
**Die Rechnung:** Jedes Wort oder jede Phrase der Wortliste A ist mit der Wertigkeit 20 belegt. Damit ist bei einer einzigen gefundenen Phrase aus dieser Liste der Job-Schwellwert bereits erreicht und die Aktion wird durchgeführt.

Jedes Wort oder jede Phrase der Wortliste B ist mit der Wertigkeit 1 belegt. Jedes gefundene Wort/Phrase aus dieser Liste wird gezählt, die Gesamtanzahl der Wörter/Phrasen mit der Wertigkeit multipliziert und mit dem Schwellwert verglichen. Wenn hier also 21 Wörter, die auf der Liste B stehen, in der Email gefunden werden, werden diese mit der Wertigkeit 1 multipliziert:  $21 \times 1 = 21$ . Verglichen mit dem Job-Schwellwert 20 = Aktion wird ausgelöst.


**Hinweis:** Wenn Sie Inhalte aus verschiedenen Sprachen erkennen wollen, legen Sie die entsprechenden Wortlisten an und richten Sie pro Sprache einen Job ein. Definieren Sie bei Sprachen wie Französisch und Spanisch eine benutzerdefinierte Zeichenumsetzung. Bitte wenden Sie sich für diese Konfiguration an unseren Support.

### Aktionen festlegen

In der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, **wenn der Job eine Email mit verbotenen Inhalt gefunden hat.**



Als Aktion wird eine Kopie in die Quarantäne gestellt und die betroffene Email gelöscht. Das beinhaltet, dass die Email dem Empfänger nicht zugestellt wird. Eine Benachrichtigung über die Verletzung der Unternehmensrichtlinien wird als Warnung an Administrator versandt. Die Benachrichtigung wird aus dem Pull Down-Menü der verfügbaren Benachrichtigungsvorlagen ausgewählt und diese können individuell über die HTML-Symboleiste oder direkt mit HTML-Formatbefehlen gestaltet werden.

Speichern Sie die Konfiguration der Avira AntiVir Exchange Konsole jedes Mal, wenn Sie Änderungen durchgeführt haben. Drücken Sie dafür die Schaltfläche . Die Konfiguration wird in der Datei *ConfigData.xml* gespeichert, die im Verzeichnis *Avira\AntiVir Exchange\Config\* abgelegt ist. Offene Änderungen werden durch (\*) am obersten Knoten angezeigt.

## 6.4 Limitieren der Anzahl der Empfänger

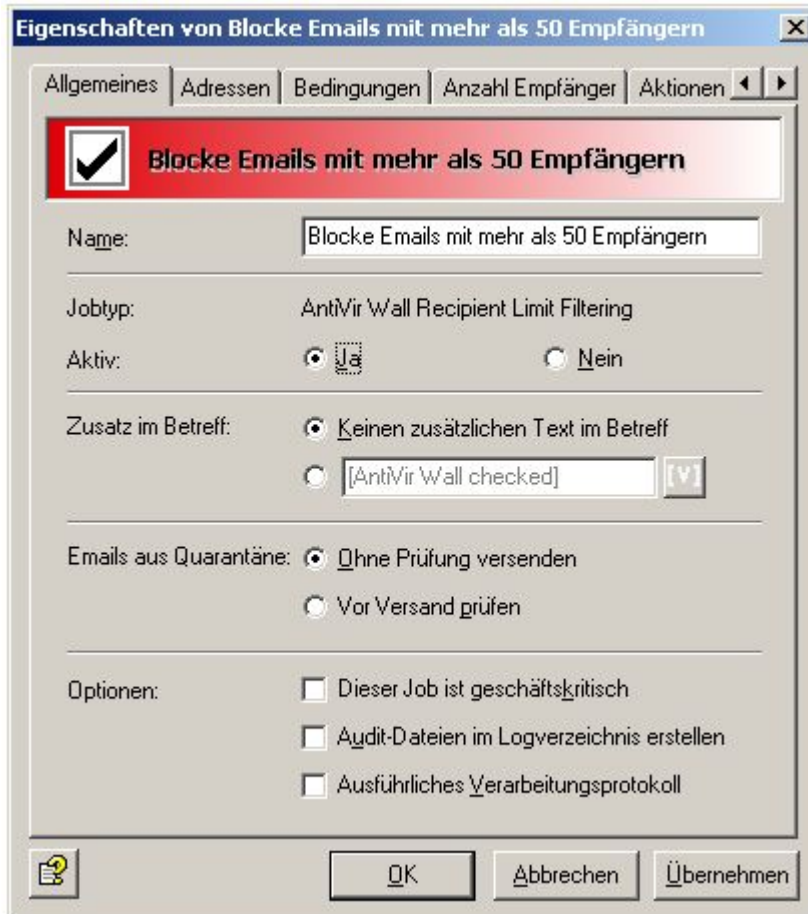
Dieser Jobtyp ermöglicht die Begrenzung auf eine gewisse Anzahl von Empfängern pro Email. Ist dieser Job aktiv, ist es nicht möglich, unnötige Massenmails an alle Mitarbeiter des Unternehmens zu versenden.

### 6.4.1 Empfängeranzahl begrenzen - Jobbeispiel

Unter **Richtlinien-Konfiguration - Jobvorlagen** finden Sie den Job **Blocke Emails mit mehr als 50 Empfängern**. Ziehen Sie diesen Job per Drag-and-Drop in den Ordner **Mail Transport Jobs** und öffnen Sie ihn dort mit einem Doppelklick.

## Allgemeine Einstellungen

Auf der Registerkarte **Allgemeines** können Sie einen eigenen Namen für den Job vergeben. Setzen Sie den Job **Aktiv**. Sobald Sie mit **OK** Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert.



Der **Zusatz im Betreff** ist vordefiniert auf **AntiVir Wall checked**. Dieser Zusatz wird in den Betreff jeder Email eingefügt, die der Job geprüft hat.

Dieser Job bearbeitet keine Mails, die aus der Quarantäne wieder versendet werden, selbst wenn beim Versand aus der **Quarantäne (AntiVir Monitor - <Email auswählen> - Alle Tasks - Aus Quarantäne senden)** die Sende-Option **Email erneut durch AntiVir Jobs bearbeiten lassen** aktiviert wurde. Die Option **Ohne Prüfung versenden** bedeutet, dass dieser Job generell bei einem Mail-Versand aus der Quarantäne übergangen wird.

Näheres zum erneuten Versand aus der Quarantäne finden Sie in [Aus Quarantäne senden](#).

## Adressbedingungen einrichten

Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus.

Wie Sie Adresslisten am besten einsetzen und eine genaue Beschreibung der Vorgehensweise finden Sie in [Adresslisten](#).

## Inhaltliche Bedingungen einrichten

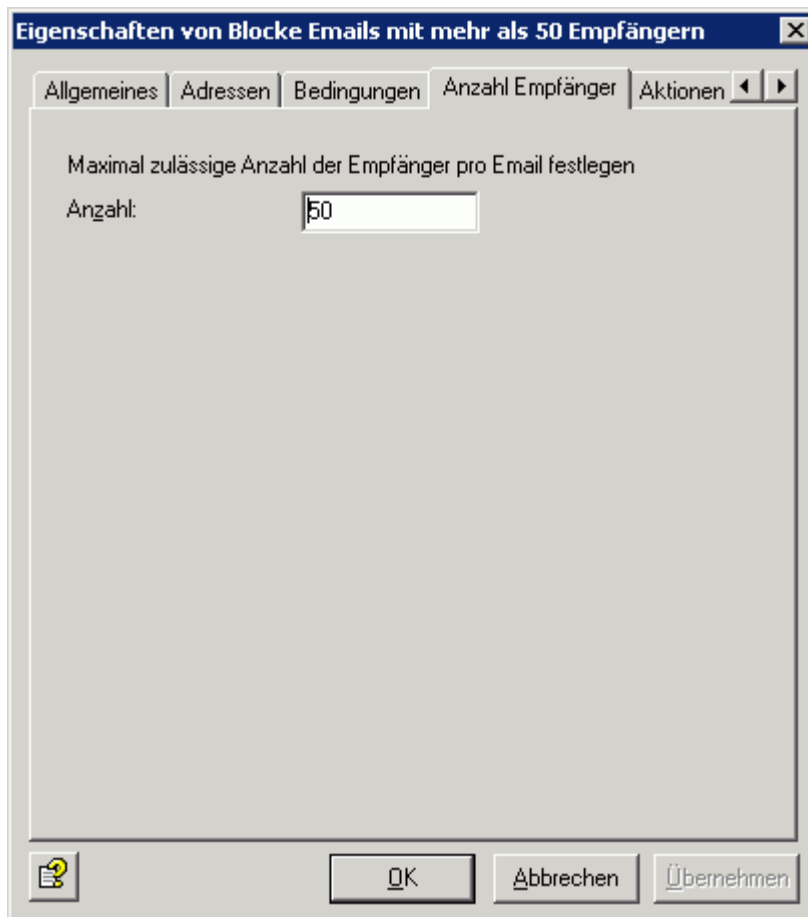
Auf der Registerkarte **Bedingungen** können Sie die Ausführungsbedingungen eines Jobs festlegen.

Wie Sie Bedingungen am besten einsetzen finden Sie in [Bedingungen](#).

**Warnung:** Die inhaltlichen Bedingungen müssen gleichzeitig mit den definierten Adressbedingungen in der Registerkarte **Adressen** zutreffen, damit der Job ausgeführt wird (UND-Verküpfung).

## Anzahl Empfänger festlegen

In der Registerkarte **Anzahl Empfänger** geben Sie die maximale Anzahl von Empfängern pro Email an:

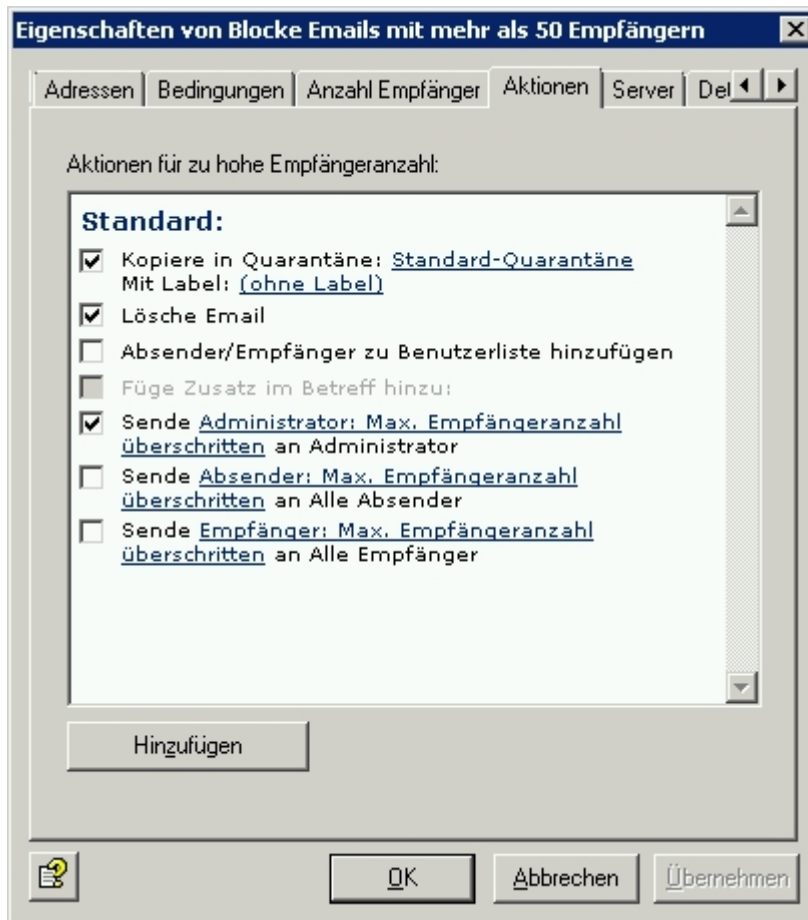


Jede ein- und ausgehende Email darf also an maximal 50 Empfänger adressiert sein. Sobald eine Email an 51 Empfänger adressiert ist, wird die definierte Aktion ausgelöst.

**Hinweis:** Sollten die Emails an eine Liste von Empfängern adressiert sein, die in einer einzigen Adresse zusammengefasst sind, so muss der Exchange-Server die Liste in die verschiedenen Empfänger auflösen können, um die Anzahl der Empfänger zu erkennen. Eine Adresse, die eigentlich eine Mailingliste ist, gilt als ein einziger Empfänger, wenn sie außerhalb der Reichweite des Exchange-Servers liegt.

## Aktionen festlegen

In der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn der Job eine Email mit zu vielen Empfängern gefunden hat.



Als Aktion wird eine Kopie der Email in die Quarantäne gestellt und die betroffene Email gelöscht. Das beinhaltet, dass die Email den Empfängern **nicht** zugestellt wird. Eine Benachrichtigung über die Anzahl der Empfänger wird als Warnung an den Administrator versandt. Die Benachrichtigung wird aus dem Pull Down-Menü der verfügbaren Benachrichtigungsvorlagen ausgewählt und diese können individuell mit der HTML-Symbolleiste oder mit HTML-Formatbefehlen gestaltet werden.

Sie können mit der Schaltfläche **Hinzufügen** weitere Aktionen definieren. Die Vorgehensweise entnehmen Sie bitte der Beschreibung in "Virenprüfung einschalten - Jobbeispiel" unter [Aktionen festlegen](#).

## Server auswählen

Die Auswahl der Server wird wie in der Beschreibung zu [Server auswählen](#) durchgeführt.

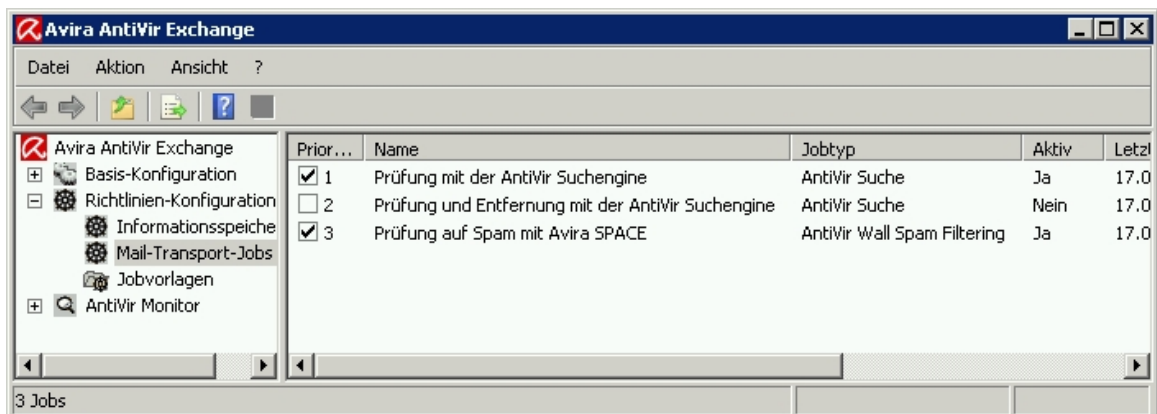


## 7 Anti-Spam

Die Anti-Spam Prüfung sucht in Emails nach speziellen Merkmalen, die auf Spam hinweisen. Nun ist Spam, im Gegensatz zu Viren, nicht immer eindeutig als solches erkennbar. Spammer versenden ganz unterschiedliche Inhalte in den unterschiedlichsten Formen, immer darauf bedacht, ihre Emails nicht als das erkennen zu lassen, was sie sind: Nämlich Spam. Dazu benutzen Spammer immer neue Tricks, um an der Erkennung durch Spam-Filter vorbei zu kommen.

So muss auch ein Anti-Spam-Job berücksichtigen, dass eine Email mitunter nicht eindeutig als Spam identifizierbar sein kann. Daher arbeitet der Spam-Filtering Job mit den unterschiedlichsten Spam-Kriterien, die in definitive und kombinierte Kriterien aufgeteilt sind.

Für Ihre Sicherheit, wurde der Job **Prüfung auf Spam mit Avira AntiSpam** vorkonfiguriert und voraktiviert. Sie finden den Job unter **Mail-Transport-Jobs**.



### 7.1 Avira AntiSpam Engine

AntiSpam ist ein Typ von AntiSpam Engine, welcher zur Erkennung von Spam und Phishing Emails verwendet wird. AntiSpam ist Bestandteil von AntiVir Wall Spam Filtering Jobs und als Standard AntiSpam Engine voreingestellt.

Die **Avira AntiSpam Engine** verwendet zur Analyse der Emails die Informationen aus einer lokalen Datenbank, die periodisch aktualisiert wird, und verschiedene RBL DNS Servers (Realtime Black Lists).

Das Ergebnis dieser Prüfung ist ein Wert, der im Rahmen des erweiterten Spam-Filter Jobs in die Berechnung des Spam-Wahrscheinlichkeitswertes einfließt.

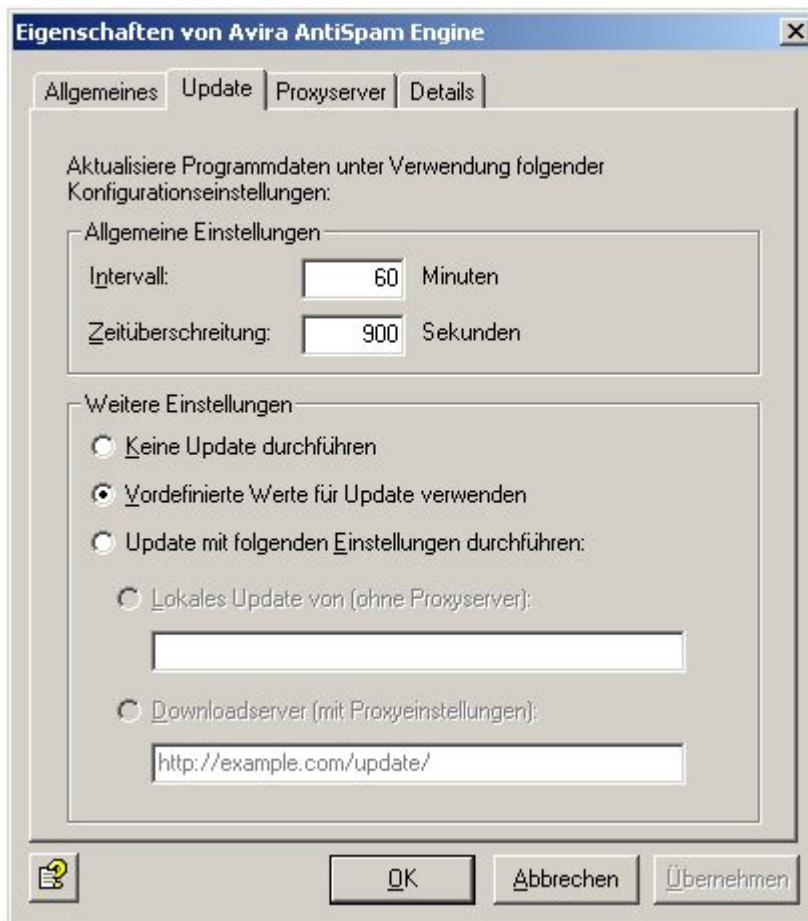
#### 7.1.1 AntiSpam Engine konfigurieren

Wenn Sie AntiSpam zur Spam-Bekämpfung verwenden, konfigurieren Sie zunächst die AntiSpam Engine für regelmäßige Pattern-Updates. Die konfigurierte Engine wird automatisch verwendet, sobald ein Spam-Filtering Job mit aktiviertem AntiSpam-Kriterium aktiviert wird.

Öffnen Sie die **Basis-Konfiguration - Utility-Einstellungen** und klicken Sie auf **AntiSpam Engine**. Wählen Sie mit einem Doppelklick **Avira AntiSpam Engine** aus oder klicken Sie mit der rechten Maustaste auf **Eigenschaften**.

Es ist möglich, AntiSpam zu duplizieren, z.B. wenn Sie unterschiedliche Konfigurationen oder Intervalle nutzen möchten.

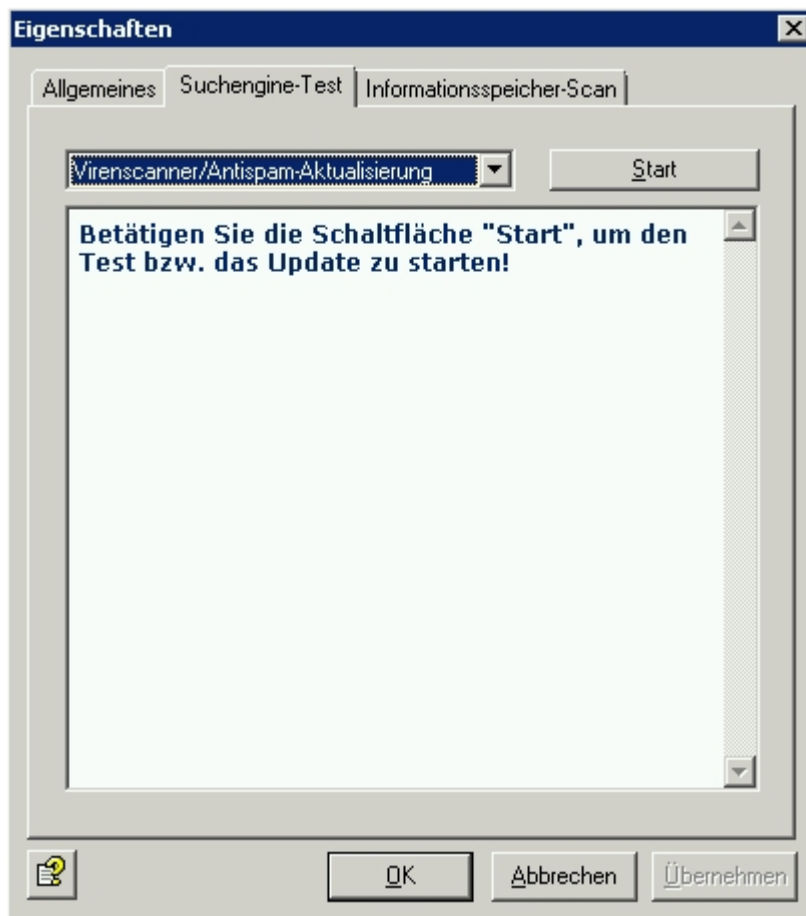
### Aktualisierung (AntiSpam Update) einstellen



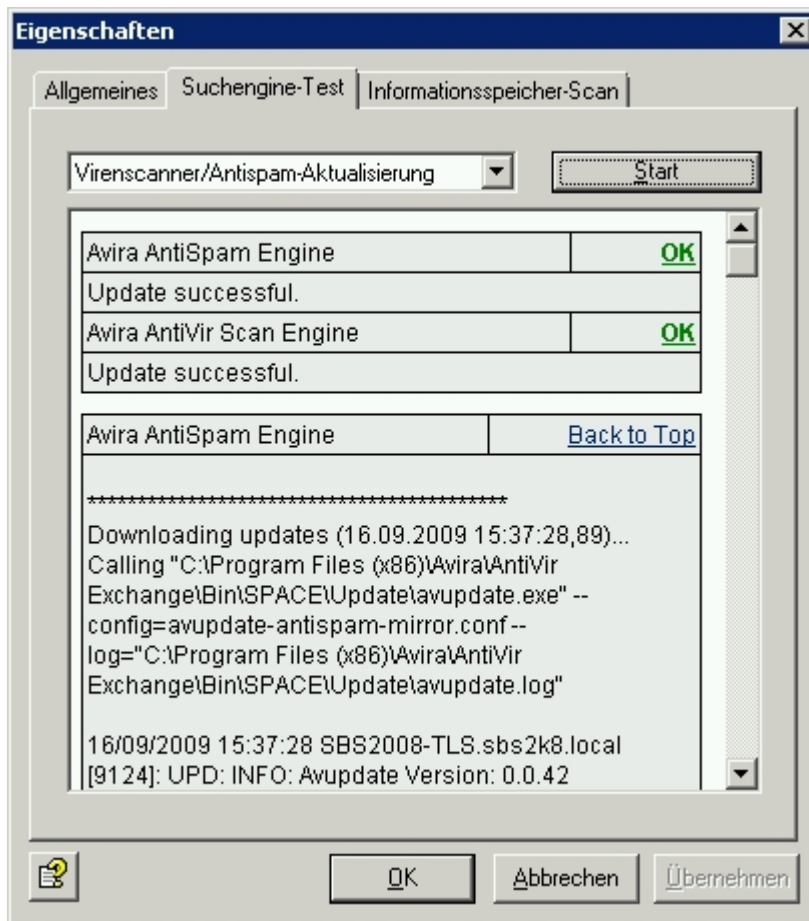
Für den Standardfall genügt es, wenn Sie in dieser Registerkarte nur noch das Intervall für das Pattern-Update eintragen:

- **Parameter:** Dieses Feld gibt das Verzeichnis an, in dem die aktualisierten Patterns abgelegt werden. Verändern Sie die Angaben nur dann, wenn Sie bei der Einrichtung von AntiSpam andere Verzeichnisse gewählt haben.
- **Intervall:** Zeitintervall in Minuten, in dem nach Pattern Updates gesucht wird. Minimalwert: 15 min.
- **Zeitüberschreitung:** Bei Zugriff auf den Server in Sekunden. Nach Ablauf dieser Frist wird der Update-Vorgang abgebrochen.

Wenn Sie einen Proxyserver für die Updates benutzen, klicken Sie auf der Registerkarte **Proxyserver** und wählen Sie den Server aus. Um AntiSpam manuell zu aktualisieren, klicken Sie im Navigationsbereich auf **AntiVir Monitor - Server - <server> - Server Status**:



Auf der Registerkarte **Suchengine-Test** wählen Sie **Virenschanner/AntiSpam-Aktualisierung** und klicken Sie auf **Start**. Nach dem Update bekommen Sie einen detaillierten Update-Report:



## 7.2 Wall Spam Filtering Jobs

Der Job untersucht die Email anhand der definitiven Kriterien auf absolut eindeutige Spam-Merkmale und urteilt nach der Prüfung: 100% Spam oder 100% Nicht-Spam. Anhand der kombinierten Kriterien wird die "Grauzone" untersucht, um zu errechnen, mit welcher Wahrscheinlichkeit die geprüfte Email Spam ist (= Spam-Wahrscheinlichkeit). Dabei ist die Spam-Wahrscheinlichkeit der definitiven Kriterien immer 0% oder 100%, die der kombinierten Kriterien kann von 1 bis 99 reichen. Einen vorkonfigurierten **Wall Spam Filtering Job** finden Sie in der **Richtlinien-Konfiguration**. Der Job enthält eine Reihe von Analysen und prüft folgende Bestandteile der Email:

- Email-Kopfzeilen (Header)
- Betreff
- Nachrichtentext

Auch hier werden - wie in der normalen Inhaltsprüfung - vordefinierte Wortlisten unterschiedlichsten Inhalts verwendet, um nach Spam-Textinhalten zu suchen.

In der "Grauzone" treten einige der kombinierten Kriterien bei Spam-Mails gehäuft auf und andere Kriterien sind eher ein Hinweis für Nicht-Spam-Mails. Jedes kombinierte Kriterium für sich allein ist normalerweise nur ein Hinweis darauf, ob eine Email bestimmte Merkmale aufweist, die auf Spam hindeuten. Je mehr Kriterien einen hohen Wert für Spam in einer Email ausweisen, desto sicherer kann man davon ausgehen, dass es sich in der Tat um eine Spam-Mail handelt. Durch die Kombination der Einzelergebnisse dieser Kriterien (daher: kombinierte Kriterien) ergibt sich im Job eine Maßzahl, die den Grad der Überzeugung ausdrückt, dass es sich bei dieser Email um Spam handelt (= Spam-Wahrscheinlichkeit).

Der vorkonfigurierte Job ist so eingestellt, dass eine Email eine hohe **Spam-Wahrscheinlichkeit** von z. B. über 91% nur erreichen kann, wenn für mehrere kombinierte Kriterien deutliche Hinweise auf Spam gefunden wird.

Im Job werden bis zu vier Bereiche dieser Spam-Wahrscheinlichkeit unterschieden. Sie können die Grenzen zwischen vier Bereichen (Spam-Wahrscheinlichkeit = Schwellwerte) per Schieberegler selbst festlegen und für jeden festgelegten Bereich die Aktionen definieren, die der Job mit den Emails ausführen soll, deren Spam-Wahrscheinlichkeit im entsprechenden Bereich liegt. So könnten Sie z. B. konfigurieren, dass

- definitiver "Nicht-Spam" mit einer Spam-Wahrscheinlichkeit von 0% normal zugestellt wird,
- unter einer Spam-Wahrscheinlichkeit von 10% die Email ebenfalls normal zugestellt wird. Eine Option könnte sein, diese Emails für die Klassifizierung in die Quarantäne **Email: Low** zu stellen,
- zwischen 10% und 50% Spam-Wahrscheinlichkeit das **SCL-Feld** in Exchange 2003 ausgewertet wird, so dass die Email automatisch in den Junk-Mail-Ordner des Empfängers verschoben wird oder die Emails in die Quarantäne **Email: Medium** gestellt werden, die Empfänger eine Sammelbenachrichtigung der in Quarantäne gestellten Emails und sie ggf. anfordern können,
- Emails über 50% Spam-Wahrscheinlichkeit gleich gelöscht werden. Auch hier können Sie die Emails für die Klassifizierung in die Quarantäne der in Quarantäne gestellten E-Mails **Email: High** stellen.

Folgende Aktionen sind möglich:

- Gesamte Email in Quarantäne kopieren
- Zusatz im Betreff
- Betroffene Email löschen und nicht zustellen
- Absender oder Empfänger ins Whitelist hinzufügen
- Administrator benachrichtigen
- Absender benachrichtigen
- Empfänger benachrichtigen
- Andere, frei wählbare Personen benachrichtigen
- Ausführen einer externen Anwendung
- Avira-Header-Feld hinzufügen
- X-Header-Feld hinzufügen
- Email umleiten

Die einzelnen Schwellwertbereiche:

1. **Spam-Wahrscheinlichkeit: Keine.** Vorkonfiguriert: 0
2. **Spam-Wahrscheinlichkeit: Niedrig.** Vorkonfiguriert: 0- 19.
3. **Spam-Wahrscheinlichkeit: Mittel.** Vorkonfiguriert: 20 - 74.

4. **Spam-Wahrscheinlichkeit: Hoch.** Vorkonfiguriert: 75-100.

Die Bereiche **Niedrig, Mittel und Hoch** können per Regler definiert und dazugehörige Aktionen eingerichtet werden. Je nachdem, in welchen Bereich die Email nach der Prüfung einsortiert wurde, wird die für diesen Schwellwertbereich definierte Aktion ausgelöst. Für die Spam-Wahrscheinlichkeit **Keine** können Sie einen Zusatz im Betreff konfigurieren.

Wichtig für eine gute Email-Lösung ist auch die effektive Vermeidung von falsch klassifizierten Emails (False Positives) und die effiziente Verwendung der für die Spam-Prüfung zur Verfügung stehenden Rechenleistung im Produktivbetrieb. Die **definitiven Ausschlusskriterien** (= Definitive Kriterien) sind daher den kombinierten Kriterien so vorgeschaltet, dass bei deren Eintreten die weitere Untersuchung der Email auf Spam-Merkmale unterbleiben kann. Die Ausschlusskriterien dienen dazu, die durchzuführenden Spam-Untersuchungen auf solche Emails zu beschränken, für die nicht bereits z. B. aufgrund des Absenders ausgeschlossen werden kann, dass es sich um Spam handelt.

**Hinweis:** Bei Zutreffen eines definitiven Kriteriums beträgt die Spam-Wahrscheinlichkeit immer 0% oder 100% und fällt damit in den Wahrscheinlichkeitsbereich **Keine** oder **Hoch** mit den entsprechenden Aktionen.

**Hinweis:** Selbstverständlich beeinflussen diese Kriterien nicht die Prüfung durch die anderen konfigurierten und aktiven Email wie z. B. die Prüfung auf Dateianhänge durch AntiVir. Wenn Sie also das definitive "Kein-Spam"-Kriterium **Emails mit Anhängen** aktiviert und den Schwellwert (**Minimum-Anzahl**) auf 2 eingestellt haben, bedeutet das nur, dass der Spam-Filtering Job diese Emails sofort in den Spam-Wahrscheinlichkeitsbereich **Keine** einsortiert und nicht, dass ein Watchdog Job diese 2 Anhänge plötzlich völlig ungeprüft in Ihr Netzwerk gelangen lässt.

**Hinweis:** Normalerweise ist es nicht nötig, die kombinierten Kriterien anzupassen. Versuchen Sie bei nicht zufrieden stellenden Spam-Erkennungsraten, zunächst die definitiven Spam-Kriterien (Ausschlusskriterien) zu optimieren (siehe unten).

### 7.2.1 Definitive Kein-Spam-Kriterien

Im Job können die folgenden Kriterien konfiguriert werden, aufgrund derer Emails automatisch als nicht bedrohlich oder kein Spam angesehen werden:

Kriterium	Beschreibung
Emails der folgenden Absender (Whitelist)	Whitelist: 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.
Emails von Active Directory Benutzern	Weitere vertrauenswürdige Adressen sind alle im Active Directory eingetragenen Benutzer und Kontakte.
Emails von Absendern in Benutzer Whitelist	Die in der Benutzer-Whitelist eingetragenen Email Adressen werden ohne Prüfung auf Spam durchgelassen.

Emails mit Anhängen	Emails mit Dateianhänge. Die meisten unerwünschten Emails enthalten keine Anhänge. Optional können Sie hier einen Schwellwert eintragen. Beispiel: Mindestwert = 2, d.h. alle Emails, die nur 2 Anhänge beinhalten, werden ohne Spamprüfung geliefert.
Emails mit Mindestgröße von	Spam-Mails sind in der Regel klein. Deshalb sind große Emails meist kein Spam. Hier kann ein Schwellwert eingestellt werden, ab dem die Emails nicht mehr durch die Spam-Prüfung laufen.
Emails sind in TNEF-Format	TNEF Emails. Dieses Exchange-spezifische Format wird bisher nicht von Spammern benutzt.
Emails sind verschlüsselt oder signiert	Verschlüsselte und/oder signierte Emails. Spammer versenden bisher keine verschlüsselten oder signierten Emails.
Microsoft Exchange "Kein Spam" SCL-Wert Siehe auch <a href="#">Schreibe Spam-Ergebnis in Exchange SCL Feld.</a>	Spam Confidence Level (SCL), Spam-Filter (Intelligent Message Filter (IMF) ab Exchange 2003. SCL kann ganzzahlige Werte zwischen -1 und 9 annehmen. -1 wird von Exchange für Emails von Absendern aus der gleichen Exchange-Organisation vergeben. Dieser Wert wird vom Wall Spam Filtering Job als definitives „Kein Spam“-Kriterium gewertet.

### 7.2.2 Definitive Spam-Kriterien

Ebenso können folgende Ausschlusskriterien definiert werden, die dafür sorgen, dass eine Email auf jeden Fall gefiltert und gegebenenfalls abgefangen wird.

Kriterium	Beschreibung
Emails der folgenden Absender (Blacklist)	Blacklist: 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.
Emails mit diesem Zeichensatz	Die Funktion prüft das Feld „charset“ in den Kopfzeilen (Header) der Email auf die Zeichensätze, die in der angegebenen Liste eingetragen sind. Emails mit einem solchen Zeichensatz werden sofort als Spam klassifiziert.
Exchange SenderIDErgebnis = "FAIL" Näheres zur SenderID finden Sie unter <a href="#">Details: SenderID</a>	Wenn Sie dieses Kriterium aktivieren, wird die Sender-ID der Email mit ausgewertet. Dadurch wird "spoofing" also das Fälschen von Absender-Mailadressdomänen verhindert. Die Auswertung erfolgt anhand von Einträgen in einem DNS. Über dieses DNS kann ermittelt werden, von welchen IP-Adressen Emails bestimmter Domänen versandt bzw. nicht

versandt werden dürfen. Das Ergebnis der Sender-ID wird mit der Email mitgeliefert. Wall prüft die SenderID der Email und wertet das Ergebnis "FAIL" als Spam aus. Um die Funktion SenderID nutzen zu können, müssen Sie einige Funktionen am Server einschalten, z.B. den zugehörigen Filter für SenderID am Server aktivieren. Die Aktivierung erfolgt unter **Server - Protokolle - SMTP - Eigenschaften** im Feld **Identifikation**. Daneben müssen sowohl Server als auch Client (Outlook) konfiguriert werden.

**Hinweis:** Sollen Emails nur dann direkt gelöscht werden, wenn diese definitiv SPAM sind, müssen Sie die **Spam-Wahrscheinlichkeit** für **Hoch** auf 100 stellen und eine entsprechende Aktion definieren. Somit wird sichergestellt, dass nur die Emails, bei denen die definitiven Kriterien (= die Blacklist oder Zeichensatz) eindeutig SPAM festgestellt haben, in diesen Bereich fallen. Bei einer Einstellung von z. B. 91 bis 100 fallen auch Emails mit einer hohen Spam-Wahrscheinlichkeit aus anderen Kriterien in diesem Bereich.

### 7.2.3 Praxistipps

Abhängig von der Einsatzumgebung kann es sein, dass der Job auch bei normalen und erwünschten Emails aufgrund der Kriterien Spam Hinweise findet, und diese somit fälschlicherweise als Spam behandelt. Sollten solche Fälle vorkommen, empfehlen wir die folgenden Konfigurationseinstellungen:

1. Liegen die betroffenen Emails immer knapp über dem Schwellwert der Spam-Wahrscheinlichkeit beginnt, sollten Sie zunächst diesen Schwellwert etwas höher einstellen, um die Falsch-Klassifikationen zukünftig zu vermeiden.
2. Stehen Sie mit dem Absender von falsch klassifizierten Email regelmäßig in Kontakt, sollten Sie ihn als Kontakt im Active Directory anlegen oder in die Whitelist (unter der Schaltfläche **Definitive Kriterien - Definitive "Kein Spam"-Kriterien**) eintragen, so dass die Untersuchung dieser Emails künftig entfallen kann.
3. Versuchen Sie für Ihre Einsatzumgebung typische Business-Begriffe in den betroffenen Email zu identifizieren und tragen Sie diese in die Business Words Wortliste ein. Der Job wird diese Wörter zukünftig über das kombinierte "Kein Spam"-Kriterium **HAM Phrasen im Nachrichtentext** berücksichtigen und Emails, die diese Wörter enthalten, weniger stark als Spam werten.
4. Wenn trotz der Anpassungen 1 - 3 sich Falsch-Klassifikationen nicht in einem akzeptablen Rahmen bewegen, sollten Sie z. B. mit Hilfe der Ursachenbeschreibung in der Quarantäne oder auch mit der Benachrichtigungs-Variable **Details Spam-Analyse** herausfinden, welche Kriterien bei den falsch klassifizierten Email Hinweise auf Spam geliefert haben. Handelt es sich wiederholt um dasselbe Kriterium, so ist dieses für Ihre Einsatzumgebung wahrscheinlich nicht aussagekräftig genug: Sie sollten dessen Bedeutung daher vermindern, indem Sie unter **Kombinierte Kriterien** die **Kriterium-Relevanz** um eine Stufe verringern. So berücksichtigt der Job dieses Kriterium nicht mehr so stark bei der Bestimmung der Spam-Wahrscheinlichkeit.



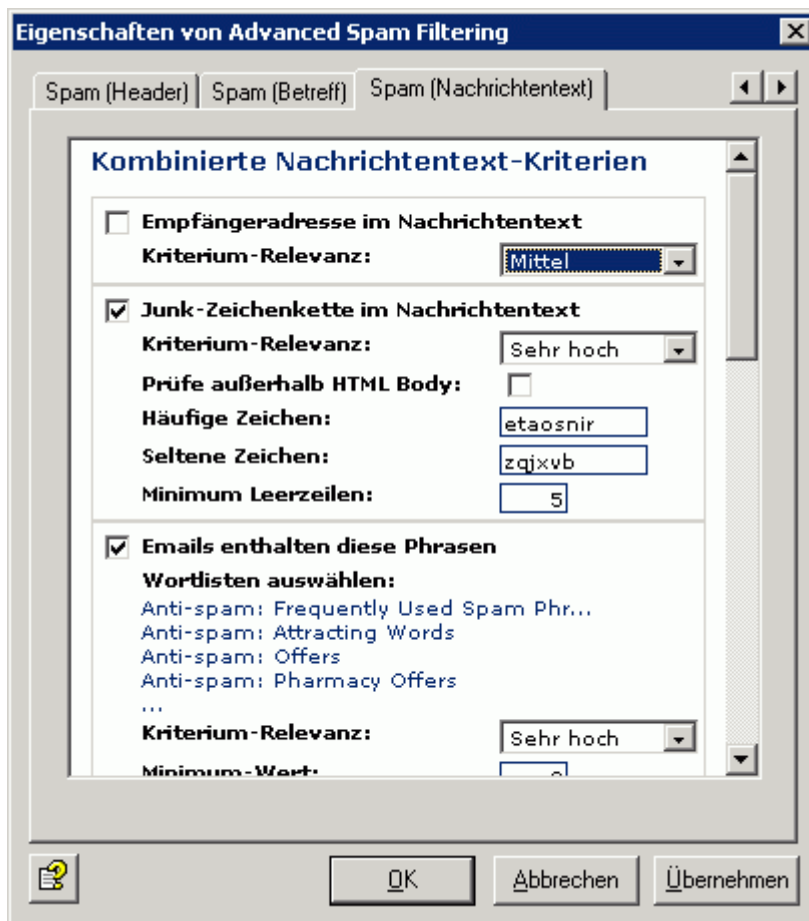
5. Wenn Sie sich sehr gut mit den Merkmalen der bei Ihnen üblichen Email (Spam und Nicht-Spam) auskennen, können Sie mit Hilfe der **kombinierten Kriterien in Erweiterte Konfiguration** auch die einzelnen Kriterien auf Ihre Einsatzumgebung hin optimieren. Dies kann vor allem dann sinnvoll sein, wenn Sie die Relevanz eines Kriteriums sehr weit verringern oder das Kriterium ganz ausschalten mussten, um Falsch-Klassifikationen auszuschließen. Die Kehrseite der Medaille kann eine spürbare Abnahme der Spam-Erkennung sein. Zu diesem Thema lesen Sie bitte das Kapitel [Anti-Spam für Experten](#).

## 7.3 Anti-Spam für Experten

Im Spam-Filtering Job lassen sich definitive und kombinierte Spam-Kriterien einstellen. Die **definitiven Kriterien** bedeuten eine sofortige Entscheidung in die eine oder andere Richtung (Spam oder Nicht-Spam) und werden sofort mit dem Etikett "Spam-Wahrscheinlichkeit ist 0% = **Keine**" oder "Spam-Wahrscheinlichkeit ist 100% = **Hoch**" belegt. Die **kombinierten Kriterien** werden nur dann angewandt, wenn die definitiven Kriterien nicht zutreffend waren. Für die eigentliche Spam-Erkennung mit kombinierten Kriterien werden mehrere Analysemechanismen (Kriterien-Untersuchungen) parallel durchgeführt und anschließend nach der Analyse der Email miteinander "verrechnet". Jedes Kriterium besitzt seine eigene Relevanz für das Gesamtergebnis (die individuelle Wertigkeit dieses Kriteriums), die von **Niedrig** bis **Sehr hoch** eingestellt werden kann. Deaktiviert wird das Kriterium per Klick in der Checkbox. Außerdem lassen sich die meisten Kriterien noch mit einem individuellen Wert für **Minimum** und **Maximum** belegen. Diese beiden Werte beziehen sich z. B. auf die Wortlisten, gegen die das Kriterium die Emails prüft. Unterhalb des Minimum-Werts wird dieses Kriterium für die entsprechende Email in der Gesamtwertung nicht berücksichtigt. Ist der Maximum-Wert erreicht, so ist **dieses Kriterium** der Meinung: "Das ist Spam!".

**Warnung:** Die Aussage "**Das ist Spam!**" gilt nur für das spezielle einzelne Kriterium, dessen Maximum-Wert durch die Analyse der Email erreicht ist. Da es sich in dieser Spam-Analyse immer um eine Analyse mit kombinierten Kriterien handelt, können die anderen Kriterien auch "ganz anderer Meinung sein" und beim gegenseitigen Verrechnen das einzelne Kriterium sozusagen "überstimmen". Näheres finden Sie auch im unten stehenden Beispiel.

## 7.3.1 Kombinierte Kriterien - Beispiel



Sie benutzen im kombinierten Kriterium **Emails enthalten diese Phrasen** in der Registerkarte **Spam (Nachrichtentext)** u.a. die Wortliste **Anti-Spam: Frequently Used Spam Phrases**, um den Nachrichtentext aller eingehenden Emails auf Spam zu prüfen. Diese Wortliste ist mit der Wertigkeit 5 belegt. Wird in einer Email nun ein Wort/Phrase dieser Wortliste gefunden, z. B. "check it out", so wird es mit 5 bewertet und gezählt. Sie geben nun an, ab wie vielen Wörtern dieses Kriterium in der Gesamtwertung berücksichtigt werden soll (**Minimum-Wert**) und wann Ihr individuelles "Spam-Maß" für dieses Kriterium voll ist (**Maximum-Wert**). Zählen Sie dazu die Wertigkeit der zu findenden Wörter zusammen. Wenn Sie hier also einen Wert von 30 angegeben (so wie in unserem vorkonfigurierten Job), so müssen in der Email 6 verschiedene Wörter dieser Wortliste gefunden werden, um für dieses Kriterium voll als Spam klassifiziert zu werden, da die Wertigkeit der Wortliste und der darin enthaltenen Wörter = 5 ist. Werden hier beispielsweise nur 3 verschiedene Wörter gefunden, so ist diese Email für dieses Kriterium noch nicht "voll" Spam, aber die Wahrscheinlichkeit schon recht hoch. Von einer anderen Wortliste mit der Wertigkeit = 10 genügen natürlich bereits 3 Treffer für den "vollen" Spam-Hinweis.

**Hinweis:** Mehrere gleiche Wörter werden nicht mehrfach, sondern nur einmal gezählt. Sollte also in diesem Beispiel in der Email drei Mal der Begriff "check it out" vorkommen, so zählt dieser Begriff insgesamt nur 5, nicht 15 (im Gegensatz zu einem normalen Wall Content Filtering Job).

Zusätzlich geben Sie die **Kriterium-Relevanz** an. Wenn Sie diese auf **Sehr hoch** eingestellt haben, wird das Kriterium in der Gesamtwertung entsprechend stark berücksichtigt.

### 7.3.2 Kombination der Hinweise zur Spam-Wahrscheinlichkeit

Die Einzelwertigkeiten aller kombinierten Kriterien werden anschließend entsprechend ihrer eingestellten Relevanz gewichtet und es wird eine Gesamtwertigkeit errechnet. Der Job vergleicht diese Gesamtwertigkeit (= Spam-Wahrscheinlichkeit der Email) am Ende der Prüfung mit den drei individuell einzustellenden Schwellwerten und ordnet die Email damit einem der vier Spam-Wahrscheinlichkeitsbereiche zu (**Keine** bis **Hoch**). Zusammen mit anderen kombinierten Kriterien kann also unsere Beispiemail mit den 3 gefundenen Wörtern aus der 5er Wortliste dann in der Gesamtrechnung doch noch in den "Das ist Spam"-Bereich fallen.

In diesem Beispiel könnte unsere Email mit den 6 gefundenen Wörtern der 5er Wortliste, die in diesem Kriterium den Stempel "Das ist voll Spam" erhalten hat, durch die Aufrechnung mit anderen Kriterien aber auch die Spam-Wahrscheinlichkeit **Keine** oder **Niedrig** erhalten haben und damit am Ende im Gesamtergebnis den Stempel "Das ist wahrscheinlich kein Spam".

Die Gesamtwertung entsteht erst aus den Kriterium-Relevanzen, den Minimum und Maximum-Werten und den individuell eingestellten Email.

Die einzelnen kombinierten Kriterien finden Sie unter **Erweiterte Konfiguration** auf vier Registerkarten.

Einen Überblick über die im Job enthaltenen kombinierten Kriterien geben die folgenden Tabellen.

**Hinweis:** Bitte wenden Sie sich für weiterführende Informationen zu kombinierten Kriterien an unseren Support.

#### Kombiniertes Kein Spam-Kriterium

Kriterium	Beschreibung
HAM-Phrasen im Nachrichtentext	Überprüft, ob sich Wörter aus dem typischen Business-Wortschatz der Anwender im Nachrichtentext der Email befinden.

#### Kombinierte Klassifizierungskriterien

Hier werden Ergebnisse von anderen Spam-Erkennungsprodukten eingerechnet, von denen jedes oftmals als alleiniges Spam-Erkennungsmerkmal eingesetzt wird. Durch die Kombination mit anderen Kriterien im Wall Spam Filtering Job werden die spezifischen Nachteile der einzelnen Produkte eliminiert.

Kriterium	Beschreibung
Exchange SCL Wert	<p>Siehe auch <a href="#">Definitive Kein-Spam-Kriterien</a> und <a href="#">Schreibe Spam-Ergebnis in Exchange SCL Feld</a></p> <p>Auch der Intelligent Message Filter (IMF) ermittelt eine Wahrscheinlichkeit dafür, ob eine E-Mail Spam ist. Das Ergebnis dieser Berechnung ist der so genannte Spam Confidence Level (SCL). Er kann ganzzahlige Werte zwischen -1 und 9 annehmen. Je größer der SCL, umso größer ist auch die Spam-Wahrscheinlichkeit. Der SCL-Wert einer Email kann über dieses Kriterium mit in die Spam-Bewertung der iQ.Suite einbezogen werden.</p> <p>Nähere Informationen siehe auch <a href="http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/Avira">http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/Avira</a></p>

Avira AntiSpam-Ergebnisse	Avira AntiSpam führt zur Spam-Erkennung einen Abgleich zwischen bekannten Pattern "Mustern" und der eingehenden Email durch.
---------------------------	--

### Kombinierte Header-Kriterien

Kriterium	Beschreibung
Suspekte Absendereigenschaften	Überprüft, ob der "From"-Header vorhanden und gefüllt ist und ob er mit dem Absender des SMTP-Protokolls übereinstimmt.
Suspekte Empfängereigenschaften	Überprüft, ob der "To"-Header vorhanden und gefüllt ist und ob sich mindestens einer der SMTP-Empfänger im "To"- oder "CC"-Header befindet.
Zahlen in Absenderadresse(n)	Überprüft, ob sich in einer der Absender-Adressen (SMTP oder Email-Header) Ziffern befinden.
Anzahl Empfänger pro Email	Überprüft die Anzahl der Empfänger einer Email.
Bekannte Spam X-Mailer	Überprüft, ob es sich beim X-Mailer-Eintrag in der Email um einen bekannten Spam-Mail-Client handelt.
Bekannte Spam-Resultate	Berücksichtigt das Ergebnis einer vorgeschalteten Spam-Analyse zur Klassifizierung von Emails als Spam oder Nicht-Spam. Das Ergebnis (Anzahl der gefundenen <b>Spam-Zeichen</b> ) wird in den <b>X-Header</b> der Email geschrieben. Avira AntiVir Exchange wertet den X-Header aus und schreibt die Anzahl an <b>Spam-Zeichen</b> in das Kriterium. Anhand der Angaben über die <b>Minimale/Maximale Anzahl</b> an möglichen Spam-Zeichen erfolgt die Auswertung. Das Ergebnis kann von einem externen System stammen oder von der Avira AntiVir Exchange eines anderen Servers ermittelt worden sein.

### Kombinierte Betreff-Kriterien

Kriterium	Beschreibung
Fehlender Betreff	Überprüft, ob das Betreff-Feld vorhanden und gefüllt ist.
Empfängeradresse im Betreff	Überprüft, ob sich der Teil vor dem @ einer Empfänger-Adresse im Betreff der Email befindet.
Junk-Zeichenkette im Betreff	Überprüft, ob lange Zeichenketten von Versteckzeichen (Leerzeichen) und sinnlose Junk-Zeichenketten im Betreff der Email vorkommen.
Phrasen im Betreff	Überprüft, ob sich Wörter aus dem typischen Spam-Wortschatz im Betreff der Email befinden.
Verschleierte Wörter im Betreff	Überprüft, ob sich verschleierte Wörter aus der angegebenen Wortliste(n) im Betreff der Email befinden.

## Kombinierte Nachrichtentext-Kriterien

Kriterium	Beschreibung
Empfängeradresse im Nachrichtentext	Überprüft, ob sich der Teil vor dem @ einer Empfänger-Adresse im Nachrichtentext der Email befindet.
Junk-Zeichenkette im Nachrichtentext	Überprüft, ob lange Zeichenketten von Versteckzeichen und sinnlose Junk-Zeichenketten im Nachrichtentext der Email vorkommen.
Phrasen im Nachrichtentext	Überprüft, ob sich Wörter aus dem typischen Spam-Wortschatz im Nachrichtentext der Email befinden.
Verschleierte Wörter im Nachrichtentext	Überprüft, ob sich verschleierte Wörter aus der angegebenen Wortliste(n) im Nachrichtentext der Email befinden.
Suspekter HTML-Code	Überprüft, ob sich HTML-Konstrukte im Nachrichtentext der Email befinden.
Suspekte HTML-Links	Überprüft, ob sich Spammer-Links im Nachrichtentext der Email befinden.
Viele HTML-Links	Überprüft, ob sich im Verhältnis zum Textumfang viele HTML-Links im Nachrichtentext der Email befinden.
Eingebettete Bilder	Spam-Inhalte, die durch eingebettete Bilder transportiert werden (interner Verweis auf Attachments), können mit diesem Kriterium erkannt werden. Beispielsweise ist es so möglich, dass (in Konfigurationen ohne AntiSpam) Emails mit eingebetteten Bildern pauschal als Spam bewertet werden, sofern eingebettete Bilder nicht auch Bestandteil der regulären Email Kommunikation der Einsatzumgebung ist.

## 7.3.3 AntiSpam-Prüfung - Jobbeispiel

**Warnung:** Für Ihre Sicherheit, wurde der Job **Prüfung auf Spam mit Avira AntiSpam** vorkonfiguriert und voraktiviert. Sie finden den Job unter **Mail-Transport-Jobs**.

Unter **Richtlinien-Konfiguration - Jobvorlagen** finden Sie noch einen Job für die AntiSpam-Prüfung. Kopieren Sie den **Advanced Spam Filtering** Job in **Mail-Transport-Jobs** und öffnen Sie ihn mit einem Doppelklick. Dieser Job untersucht die Emails auf spezielle Spam-Hinweise.

## Allgemeine AntiSpam Prüfung

Auf der Registerkarte **Allgemeines** können Sie einen eigenen Namen für den Job vergeben. Setzen Sie den Job **Aktiv**. Sobald Sie mit **OK** Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert.



Dieser Job bearbeitet keine Mails, die aus der Quarantäne wieder versendet werden, selbst wenn beim Versand aus der **Quarantäne (AntiVir Monitor - <Email auswählen> - Alle Tasks - Aus Quarantäne senden)** die Sende-Option **Email erneut durch AntiVir Jobs bearbeiten lassen** aktiviert wurde. Die Option **Ohne Prüfung versenden** bedeutet, dass dieser Job generell bei einem Mail-Versand aus der Quarantäne übergangen wird.

Näheres zum erneuten Versand aus der Quarantäne finden Sie in [Aus Quarantäne senden](#). Im Kapitel **AntiVir Such Engine** ist die Option [Dieser Job ist geschäftskritisch](#) näher beschrieben.

**Hinweis:** In diesem Job ist der **Zusatz im Betreff** auf der Registerkarte **Aktionen** zu finden.

## Adressbedingungen einrichten

Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus.

Wie Sie Adresslisten am besten einsetzen und eine genaue Beschreibung der Vorgehensweise finden Sie in [Adresslisten](#).

## Inhaltliche Bedingungen einrichten

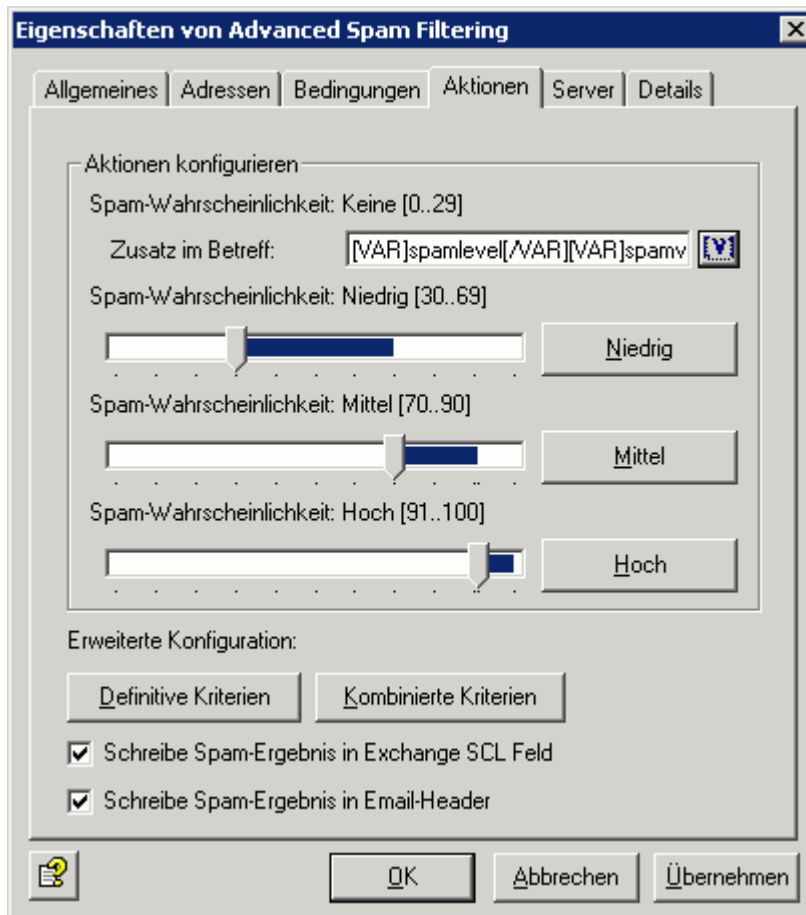
Auf der Registerkarte **Bedingungen** können Sie die Ausführungsbedingungen eines Jobs festlegen.

Wie Sie Bedingungen am besten einsetzen finden Sie in [Bedingungen](#).

**Warnung:** Die inhaltlichen Bedingungen müssen gleichzeitig mit den definierten Adressbedingungen in der Registerkarte **Adressen** zutreffen, damit der Job ausgeführt wird (UND-Verknüpfung).

## Aktionen festlegen

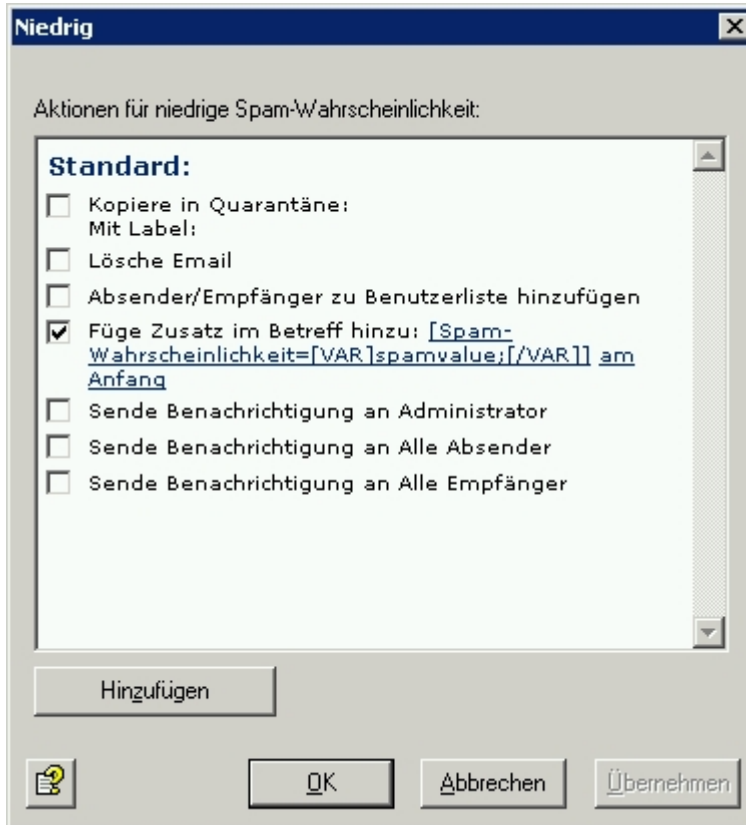
In der Registerkarte **Aktionen** legen Sie fest, wie hoch die Spam-Wahrscheinlichkeiten sein sollen und was mit dem gefundenen Spam passieren soll.



In diesem Beispiel werden folgende Spam-Wahrscheinlichkeiten festgelegt:

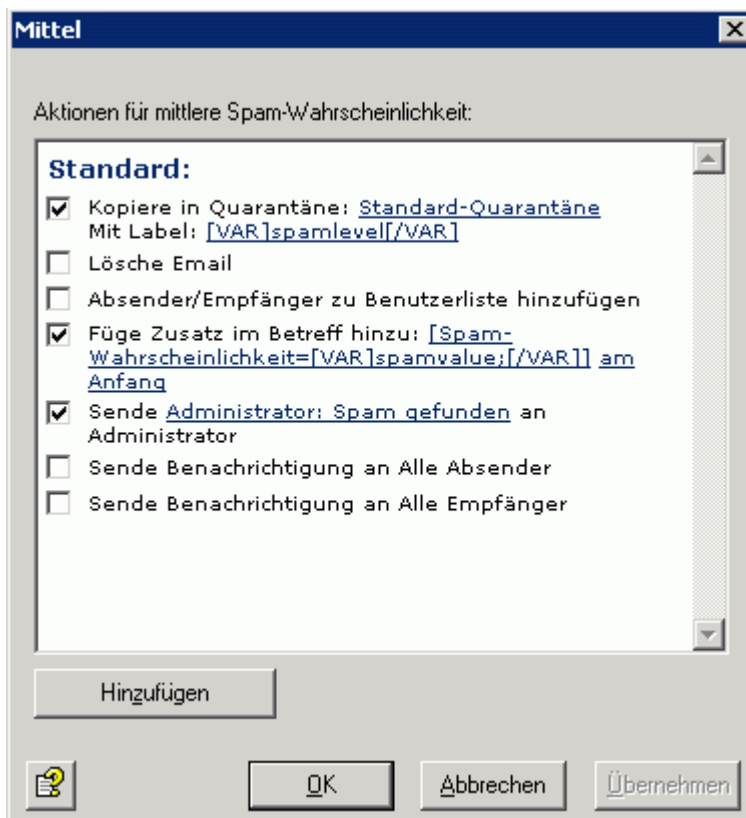
- Im Bereich **Spam-Wahrscheinlichkeit: Keine** (Wert = 0-29) werden normalerweise überhaupt keine Aktionen ausgeführt. Die einzig mögliche Aktion in diesem Wahrscheinlichkeitsbereich ist ein **Zusatz im Betreff**, den Sie direkt innerhalb dieser Registerkarte einrichten können. Denkbar wäre ein Zusatz wie AntiSpam checked o. ä.
- Für den Bereich **Spam-Wahrscheinlichkeit: Niedrig** (hier eingestellt von 30 - 69) stellen Sie die Aktionen auf einer separaten Registerkarte ein. Klicken Sie dazu auf die Schaltfläche **Niedrig**.

Sie erhalten folgenden Dialog:



Als einzige Aktion wird die Spam-Wahrscheinlichkeit im Betreff geschrieben.

Für die Konfiguration der Aktionen im Bereich **Spam-Wahrscheinlichkeit: Mittel** (hier eingestellt von 70 - 90) klicken Sie auf die Schaltfläche **Mittel**. Sie erhalten folgenden Dialog:





Als Aktion wird eine Kopie in die Quarantäne gestellt und der Administrator wird benachrichtigt. Die Original-Mail wird dem Empfänger zugestellt. Eine weitere Aktion ist der **Zusatz im Betreff**, der dem Empfänger die Spam-Wahrscheinlichkeit dieser Email mitteilt (z. B. Spam-Wahrscheinlichkeit = 75). Je höher dieser Wert ist, desto mehr kann der Empfänger davon ausgehen, dass diese Email nicht oberste Priorität hat. Die Spam-Wahrscheinlichkeit Mittel ist für die Emails gedacht, bei denen es unsicher ist, ob sie Spam sind oder nicht. Die niedrigen Werte dieser Einstellung bedeuten, dass eine mittlere Wahrscheinlichkeit für Spam angenommen wird, wenn nur einige Kriterien massive Hinweise oder aber viele Kriterien kleinere Hinweise auf Spam gefunden haben. Es ist empfehlenswert, diese Emails in einer eigenen Quarantäne (**Anti-Spam: Mittel**) zu sammeln und es den Anwendern zu überlassen, was mit diesen Emails geschehen soll.

**Hinweis:** Die Anwender können mittels Quarantäne-Sammelbenachrichtigungen über die Spam-Mails einer Quarantäne informiert werden. Sie können die Emails auch mittels des Microsoft-SCL-Wertes durch den Exchange Store direkt in die Junk-Ordner der Anwender leiten lassen (siehe dazu auch nächsten Abschnitt). Durch den konfigurierten **Zusatz im Betreff** mit der Angabe des Spam-Wahrscheinlichkeitswerts kann jeder Anwender selbst mit einem Filter in Outlook die weitere Behandlung dieser Emails einrichten.

### Schreibe Spam-Ergebnis in Exchange SCL Feld

Ab Service Pack 1 für Exchange 2003 und Outlook 2003 liefert Microsoft einen Spam-Filter aus. Dieser Intelligent Message Filter (IMF) ermittelt eine Wahrscheinlichkeit dafür, ob es sich bei einer Email um Spam handelt. Das Ergebnis dieser Berechnung ist der so genannte Spam Confidence Level (SCL). Er kann ganzzahlige Werte zwischen -1 und 9 annehmen. Je größer der SCL, umso größer ist auch die Spam-Wahrscheinlichkeit. Ein SCL von 0 bedeutet, dass höchstwahrscheinlich keine Spam-Mail vorliegt, und -1 wird für Emails vergeben, auf die der Filter überhaupt nicht angewandt wurde, beispielsweise für interne Emails von Absendern aus der gleichen Exchange-Organisation. Der Exchange-SCL-Wert kann automatisch bestimmte Aktionen auslösen wie zum Beispiel die Weiterleitung in die Junk-Mail-Ordner der Anwender in Outlook 2003, ohne dass die Anwender selbst aktiv werden müssen. Im "Exchange System Manager" können Sie zentral definieren, was bei einem bestimmten SCL-Schwellenwert mit den Emails passieren soll. Dabei muss die Aktion nicht auf dem System festgelegt werden, das die Bewertung vornimmt. Da der IMF den SCL-Wert in die Email schreibt, kann erst das Zielsystem die gewünschte Maßnahme ergreifen. Das Email-Gateway muss hierfür ebenfalls mit Exchange 2003 betrieben werden.

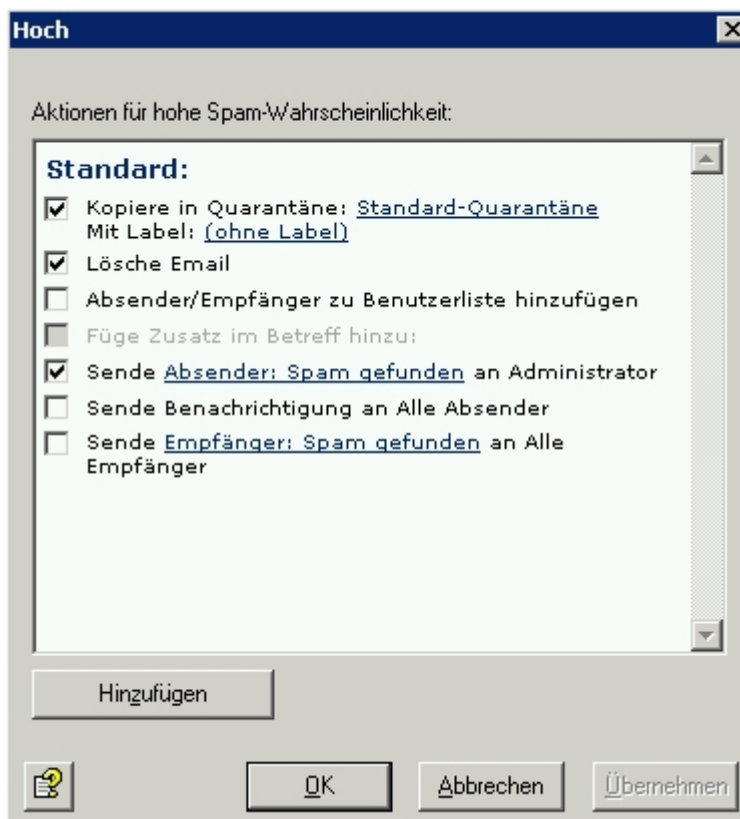
Auch wenn Sie den IMF nicht nutzen können oder möchten, können Sie mit dieser Option den Spam-Wahrscheinlichkeitswert des Spam Filtering Jobs als SCL-Ergebnis festlegen, so dass Sie die Exchange-Store-Funktionalität für die möglichen Aktionen bzw. Weiterverarbeitung nutzen können. Der Spam-Wahrscheinlichkeitswert wird intern in die SCL-Werte umgerechnet, so dass Outlook sie erkennen kann.

**Hinweis:** Wenn Sie die Quarantäne-Sammelbenachrichtigungen nutzen, werden die Anwender über alle relevanten Spam-Mails informiert. Sie können in diesem Fall auf die Verwendung der Exchange-Store-Weiterleitung in Junk-Mail-Ordner verzichten. Nähere Informationen über das Exchange-SCL-Feld erhalten Sie unter <http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/imfdeploy.mspx>

## Schreibe Spam-Ergebnis in Mail-Header

Der Spam-Wahrscheinlichkeitswert wird für alle drei Spam-Wahrscheinlichkeiten (Niedrig, Mittel und Hoch) in den Email-Header geschrieben. Dazu wird der Ergebniswert in eine Sternenkette umgerechnet (1 Stern beinhaltet einen Wert bis zu 10, 2 Sterne bis zu 20, 3 Sterne bis zu 30 ...), so dass darauf eine Outlook-Regel anwendbar ist. Sie können das Ergebnis auch für jede Spam-Wahrscheinlichkeit extra definieren, indem Sie unter der **Aktionen**-Registerkarte **Hinzufügen - X-Header-Feld hinzufügen** wählen. In diesem Fall wird das Ergebnis nicht in eine Sternenkette umgerechnet, sondern direkt als Wert ausgegeben.

Für die Konfiguration der Aktionen im Bereich **Spam-Wahrscheinlichkeit: Hoch** (hier eingestellt von 91 - 100) klicken Sie auf die Schaltfläche **Hoch**. Sie erhalten folgenden Dialog:



Die Spam-Wahrscheinlichkeit **Hoch** ist für die Emails gedacht, die wirklich Spam sind und daher nicht zugestellt werden sollen. Hier wird die Original-Mail sofort gelöscht und dem Empfänger nicht zugestellt. Eine Kopie der Email geht in die Quarantäne. Angesichts des heutigen Spamaufkommens werden keinerlei Benachrichtigungen an den Administrator versandt.

**Hinweis:** Bei hohem Email-Aufkommen können die Quarantänen schnell sehr umfangreich werden und den Email-Durchsatz belasten. Wenn Sie die Emails nicht mehr benötigen, sollten Sie die Low und High-Quarantänenkopie deaktivieren.

**Hinweis:** Es kann für Ihre Produktivumgebung durchaus vertretbar sein, die Wahrscheinlichkeiten für den **Mittel**- und **Hoch**-Bereich anders anzusetzen. Beobachten Sie aber am besten vorher einige Zeit, ob der Job mit diesen Email in Ihrer Produktivumgebung gute Ergebnisse erzielt.

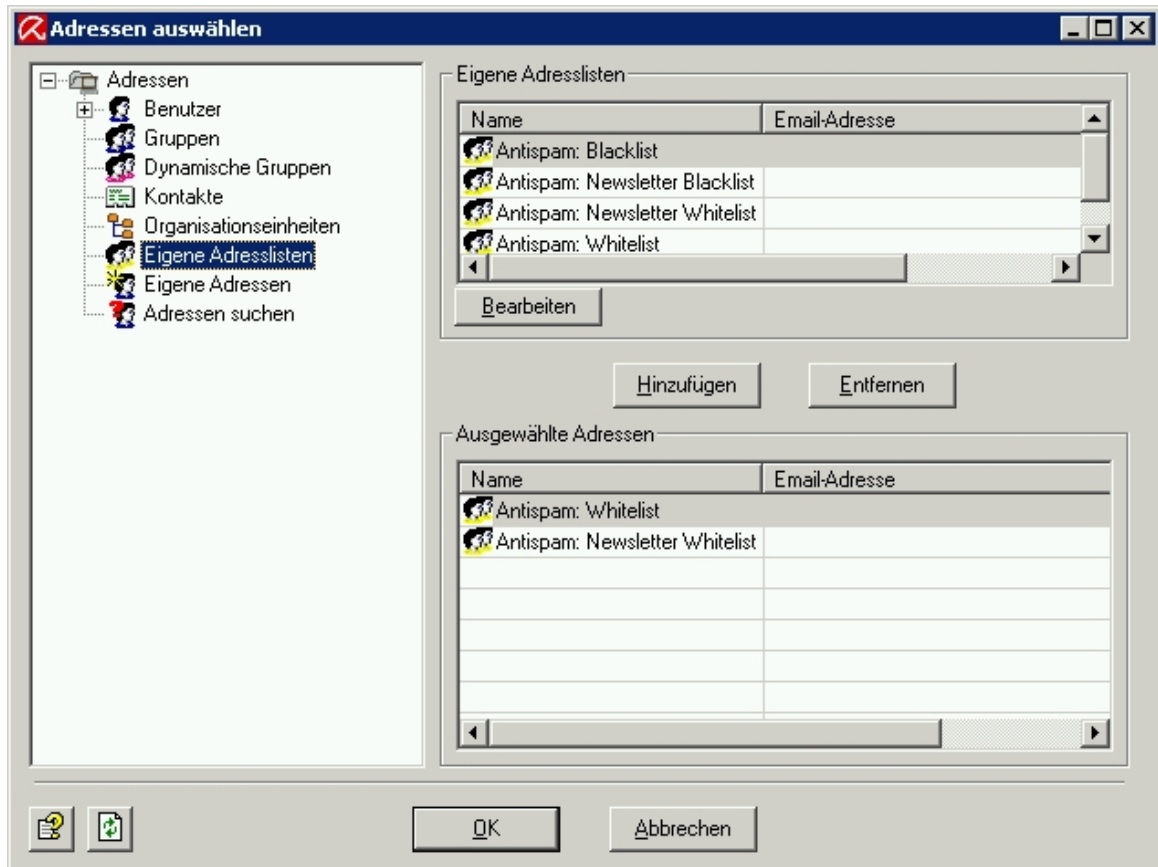
Ziel sollte sein:

- möglichst viele Spam-Mails in der **Anti-Spam: High**-Quarantäne,
- möglichst viele Ham-Mails in der **Anti-Spam: Low**-Quarantäne

- und damit möglichst wenig Emails in **Anti-Spam: Medium**

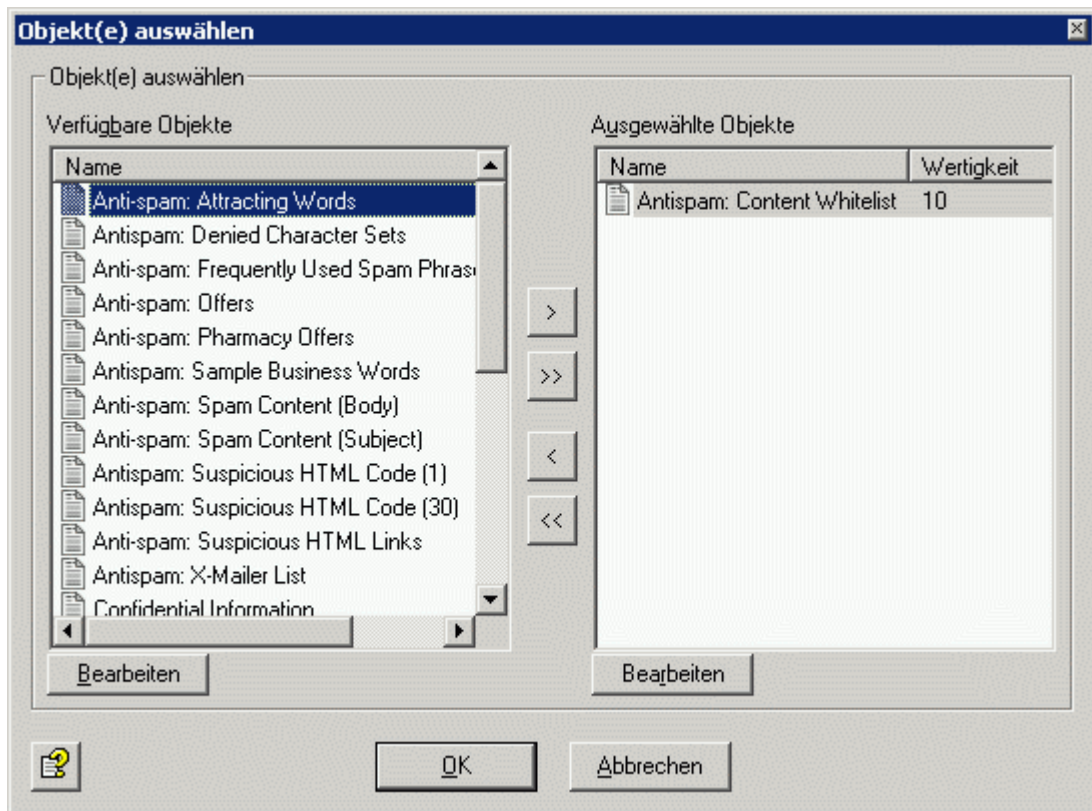
Auf der Registerkarte **Aktionen** können Sie die Spam-Kriterien anpassen. Klicken Sie auf **Definitive Kriterien**. Sie erhalten folgenden Dialog:



Wenn Sie Emails bestimmter Absender immer zulassen möchten, klicken Sie im Kriterium **Emails der folgenden Absender (Whitelist)** auf die Liste **Anti-Spam: Whitelist** und **Anti-Spam: Newsletter Whitelist**. Sie erhalten das Adressauswahlfenster:



Wählen Sie hier die Adressen aus oder geben Sie eigene Email-Adressen an, die als Absender immer zugelassen werden sollen. Als Wildcards sind der Stern (\*) und das Fragezeichen (?) zugelassen. Sie können also z. B. auch nur Domänen in der Form \*.domain.com angeben. Klicken Sie nach der Eingabe Ihrer Adressen auf **OK**.

Nun können Sie im Dialog Definitive "KeinSpam"-Kriterien das nächste Kriterium **Wörter im Betreff** anpassen. Klicken Sie auf **Anti-Spam: Content Whitelist**. Sie erhalten den Dialog zur Auswahl der Wortlisten:

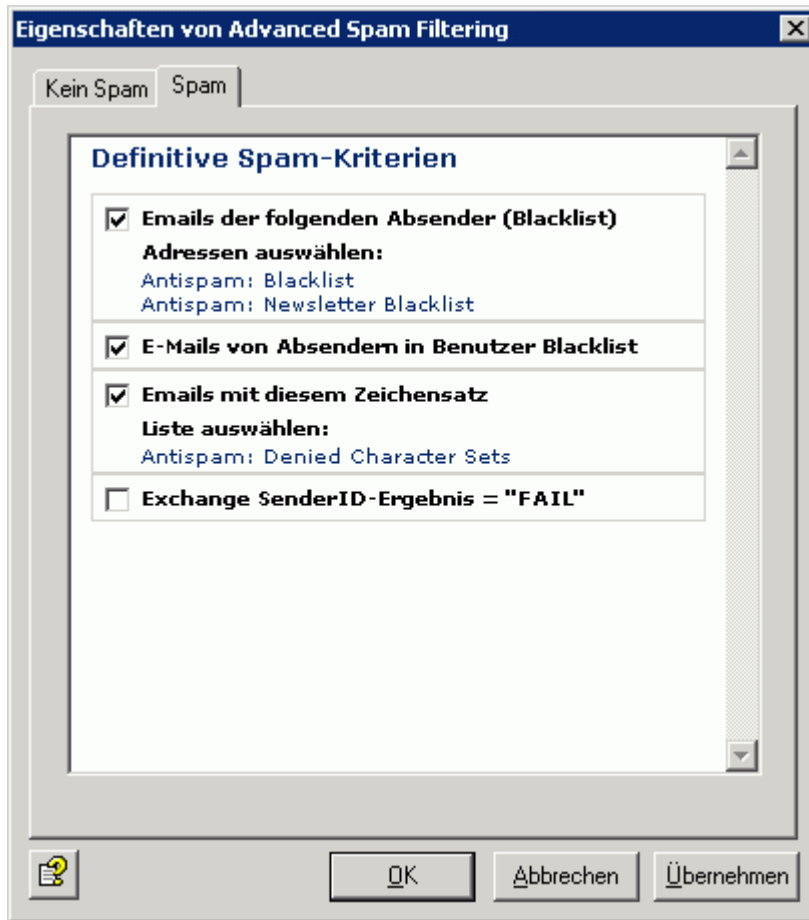


Mit den Pfeiltasten  und  können Sie der Liste Wortlisten hinzufügen und entfernen. Die Doppelpfeile fügen alle vorhandenen Wortlisten hinzu bzw. entfernen alle. Klicken Sie auf die Schaltfläche **Bearbeiten**. Sie erhalten folgenden Dialog:



Weitere Informationen zur Einrichtung von Wortlisten finden Sie in [Wortlisten einrichten](#). Eine nähere Beschreibung der weiteren Kriterien finden Sie unter [Definitive Kein-Spam-Kriterien](#).

Nachdem Sie die Wortliste gefüllt und zwei Mal mit **OK** bestätigt haben, klicken Sie nun auf die Registerkarte **Spam**:



Klicken Sie im Feld **Emails der folgenden Absender (Blacklist)** auf die Liste mit **Anti-Spam: Blacklist** und **Anti-Spam: Newsletter Blacklist**. Sie erhalten wieder ein Adressauswahlfenster und können nun eigene Email-Adressen oder Domännennamen hinzufügen.

**Hinweis:** Sowohl die Whitelist als auch die Blacklist sollte korrekt und aktuell gehalten werden!

Zusätzlich können Sie mit der Wahl eines bestimmten Zeichensatzes Emails bestimmter Regionen definitiv zum Spam erklären. Aktivieren Sie die Checkbox neben **Emails mit diesem Zeichensatz** und klicken Sie auf **Anti-Spam: Denied Character Sets** und öffnen Sie die entsprechende Liste zur Bearbeitung. Jede Zeile enthält den Code für einen Zeichensatz. Die Zuordnung der einzelnen Länder zu einem Zeichensatz können Sie der Registerkarte **Details** entnehmen. Sollten Sie Kommunikationspartner aus den Ländern haben, deren Zeichensätze in dieser Liste angegeben sind, so passen Sie die Liste folgendermaßen an:

1. Kopieren Sie die Liste **Anti-Spam: Denied Character Sets** unter **Basis-Konfiguration - Utility Einstellungen - Wortlisten**.
2. Geben Sie Ihrer Liste einen neuen Namen.
3. Löschen Sie die Zeichensätze mit den Länder Ihrer Kommunikationspartnern aus der Liste heraus.
4. Speichern Sie die Liste ab.


- Löschen Sie die Liste **Anti-Spam: Denied Character Sets** im Job **Erweitertes Spam Filtering** und setzen Sie Ihre eigene Liste unter **Definitive Spam-Kriterien - Emails mit diesem Zeichensatz** ein.

**Hinweis:** Die Funktion prüft in der Email ausschließlich das Header-Feld „charset“. Achten Sie darauf, dass Sie für diese Option nur die dafür bestimmten Zeichensatz-Liste(n) auswählen und keine andere Wortliste.

## Server auswählen

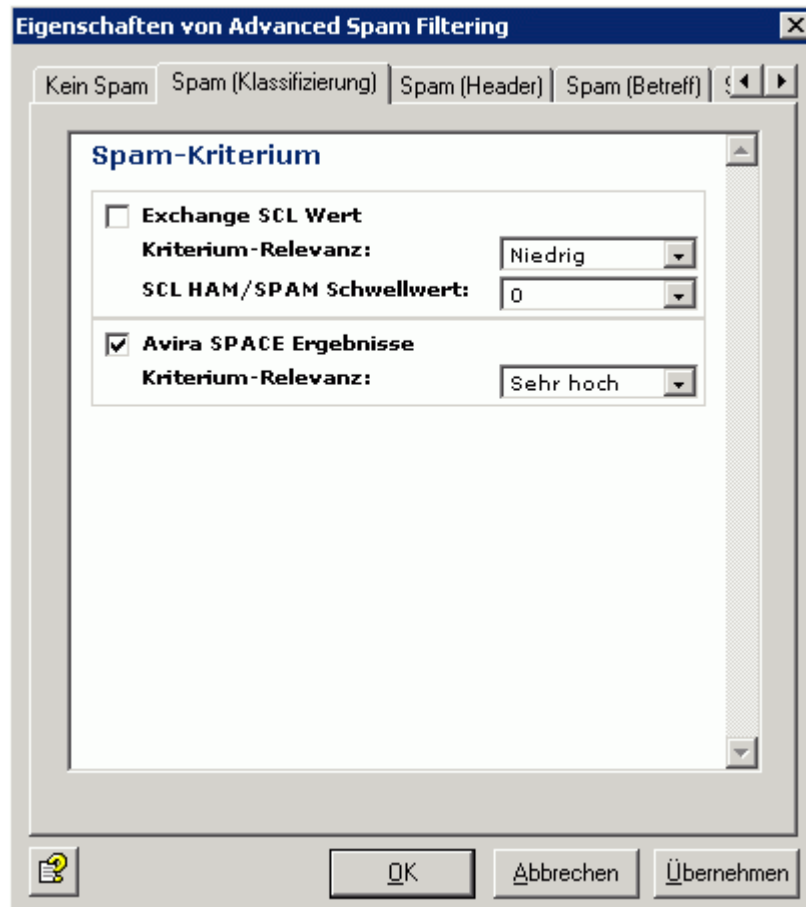
Die Auswahl der Server wird wie in der Beschreibung zu [Server auswählen](#) durchgeführt.

## Konfiguration Speichern

Speichern Sie die Konfiguration der AntiVir Exchange Management Konsole jedes Mal, wenn Sie Änderungen durchgeführt haben. Drücken Sie dafür die Schaltfläche . Die Konfiguration wird in der Datei *ConfigData.xml* gespeichert, die im Verzeichnis *Avira\AntiVir Exchange\Config* abgelegt ist. Offene Änderungen werden durch (\*) am obersten Knoten angezeigt.

### 7.3.4 Advanced Spam Filtering Job konfigurieren

- Öffnen Sie unter **Mail-Transport-Jobs** den **Advanced Spam Filtering Job**. Schalten Sie den Job aktiv und behalten Sie die Voreinstellungen bei.
- Klicken Sie in der Registerkarte **Aktionen** auf **Kombinierte Kriterien - Spam (Klassifizierung)** und aktivieren Sie das Kriterium **Avira AntiSpam-Ergebnisse**. Es wird empfohlen auch diese Einstellungen beizubehalten.



**Kriterium-Relevanz:** Legen Sie die Relevanz (Gewichtung) für das gesamte Kriterium (Bereiche von Niedrig - Sehr hoch) fest. Die Werte für die Relevanz und den Koeffizienten werden multipliziert und liefern zusammen das Ergebnis für dieses Kriterium

3. Mit dem Aktivieren dieses Jobs wird die konfigurierte AntiSpam Engine automatisch aktiviert.

### 7.3.5 Manuelle AntiSpam-Konfiguration

Wenn Sie den oben beschriebenen Wall Spam Filtering Job nicht nutzen möchten, empfiehlt es sich, für eine effektive AntiSpam-Konfiguration folgende Reihenfolge im Jobablauf einzurichten:

1. Adressprüfung auf bekannte Spam-Adressen
2. Betreffzeilenprüfung auf Text und auf Auffälligkeiten in der Formatierung, z. B. Punkte oder Leerzeichen. Siehe dazu die Wortliste **Spam Content (Subject)** in der Basis-Konfiguration unter **Wortlisten**.
3. Nachrichtentextprüfung auf Spam Links (z. B. auch auf Umleitungen und Click tracker). Siehe dazu die Wortliste **Spam-Links (Body)** in der Basis-Konfiguration unter **Wortlisten**.
4. Nachrichtentextprüfung auf Spam-Text und bekannte typische Auffälligkeiten wie z. B. HTML-Kommentare innerhalb eines HTML-Mailtextes. Siehe dazu auch die Wortliste **HTML Spam Detector** in der Basis-Konfiguration unter **Wortlisten**.

Achten Sie auf die richtigen Verarbeitungsreihenfolge der Jobs , um die Prüfungen möglichst effektiv und Performance optimiert durchzuführen.



Dieses Handbuch wurde mit äußerster Sorgfalt erstellt. Dennoch sind Fehler in Form und Inhalt nicht ausgeschlossen. Die Vervielfältigung dieser Publikation oder von Teilen dieser Publikation in jeglicher Form ist ohne vorherige schriftliche Genehmigung durch die Avira GmbH nicht gestattet. Irrtümer und technische Änderungen vorbehalten.

Ausgabe Q2-2011

AntiVir® ist ein registriertes Warenzeichen der Avira GmbH. Alle anderen Marken- und Produkt-namen sind Warenzeichen oder eingetragene Warenzeichen ihrer entsprechenden Besitzer. Geschützte Warenzeichen sind in diesem Handbuch nicht als solche gekennzeichnet. Dies bedeutet jedoch nicht, dass sie frei verwendet werden dürfen.



live free.™