

JamSoftware

SmartPOP2Exchange

©2003-2023 by Joachim Marder e.K.

1. Copyright & Kontakt	4
2. Systemvoraussetzungen	4
3. Was ist neu?	5
4. FAQ - Häufig gestellte Fragen	5
4.1 Knowledge Base	6
5. Einführung	6
5.1 Quickstart	7
5.2 Starthilfe für Exchange Server Anbindung	9
5.2.1 Starthilfe für Exchange Server 2000/2003	9
5.2.2 Starthilfe für Exchange Server 2007/2010	14
5.2.3 Starthilfe für Exchange Server 2013/2016	18
6. Menüs	23
6.1 Datei-Menü	23
6.2 Bearbeiten-Menü	25
6.3 Tools-Menü	28
6.4 Hilfe-Menü	29
7. Navigationsbereich	31
7.1 Einstellungen	31
7.1.1 Zeitplan	33
7.1.2 Globale Regeln	34
7.1.3 Antivirus	35
7.1.4 Spam Filter	37
7.1.5 E-Mail Sicherung	41
7.1.6 Log Einstellungen	42
7.2 Konten	44
7.2.1 Import von POP3/IMAP Konto Daten	45
7.2.2 Konto	47
7.2.3 SMTP	49
7.2.4 POP3	50
7.2.5 IMAP	54
7.2.6 PickupFolder	59
7.3 Ereignisanzeige	61
8. Regeln	63
8.1 Bedingungen	65
8.2 Die Spam-Bedingung	67
8.3 Aktionen	68

8.4	Beispiele	72
8.5	SMTP Fehler Regeln	73
9.	Spam Filter (SpamAssassin)	74
9.1	Bayes Filter mit POP3 Konten trainieren	76
10.	Antivirus Software	78
11.	Deutsche Gesetzeslage	82
12.	Gesetzeslage im Ausland	84
	Index	85

1 Copyright & Kontakt

Copyright ©2003-2023 by Joachim Marder e.K.

JAM Software GmbH
Am Wissenschaftspark 26
54296 Trier

WWW: <https://www.jam-software.de>

Support: <https://customers.jam-software.de/contact.php>

E-Mail: SmartPOP2Exchange@jam-software.de

Handelsregister: HRB: 4920 beim Amtsgericht Wittlich

Umsatzsteuer ID: DE234825349

Geschäftsführer: Joachim Marder

2 Systemvoraussetzungen

SmartPOP2Exchange kann auf folgenden Windows Betriebssystemen eingesetzt werden:

- Windows 11
- Windows 10
- Windows 8.1
- Windows 7 / 8
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2008 R2

Da SmartPOP2Exchange unabhängig vom empfangenden SMTP Server installiert werden kann, muss SmartPOP2Exchange nicht zwingend auf dem selben Server wie der SMTP Server installiert werden.

SmartPOP2Exchange arbeitet mit jedem beliebigen SMTP Server zusammen.

Dies schließt unter anderem die gängigen E-Mail Server ein:

- Microsoft Exchange Server 2003
- Microsoft Exchange Server 2007
- Microsoft Exchange Server 2010
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019
- Tobit
- Lotus Notes
- Exim
- Postfix
- SendMail
- uvm.....

Das .Net Framework 4.8 oder neuer wird benötigt.

Arbeitsspeicher:

Der Systemdienst von SmartPOP2Exchange (SmartPOP2SMTP.exe) benötigt ca. 20-50MB Arbeitsspeicher abhängig von:

- den verwendeten Optionen
- der Anzahl und
- der Größe der zu verarbeiteten Nachrichten

Der integrierte [SpamAssassin](#) läuft als separater Dienst und benötigt etwa 150-300 MB, je nachdem, wie viele E-Mails gerade verarbeitet werden.

Der Systemdienst von SmartPOP2Exchange kann also bis zu 200-300 MB Arbeitsspeicher benötigen.

Daher empfehlen wir SmartPOP2Exchange auf System mit mindestens 1GB Arbeitsspeicher einzusetzen.

3 Was ist neu?

Siehe ["Was ist neu?" online](#)

4 FAQ - Häufig gestellte Fragen

FAQ - Inhalt:

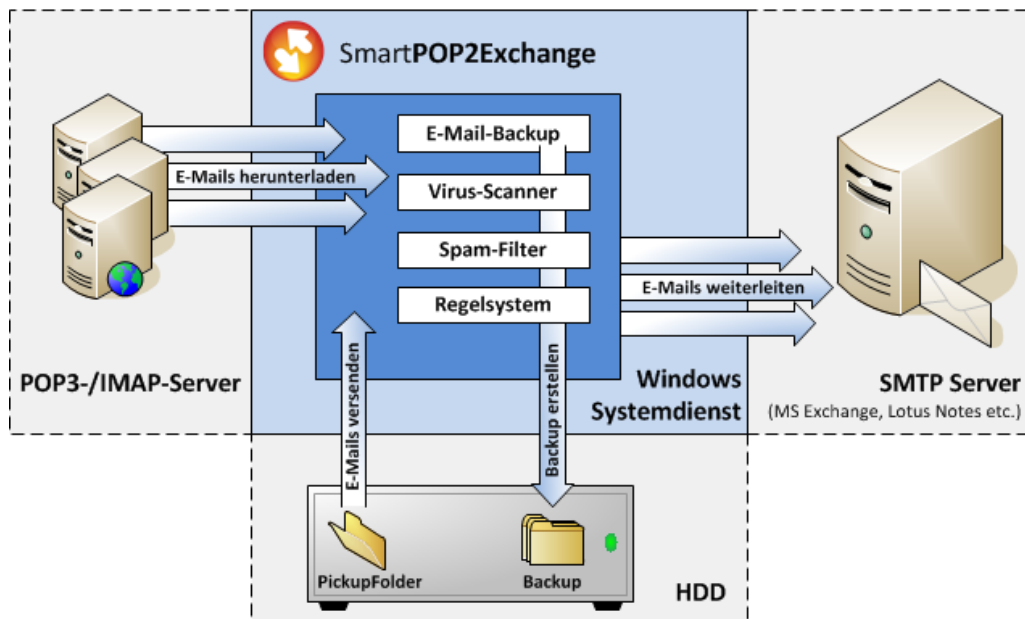
Der FAQ-Inhalt wurde in die [Knowledge Base](#) auf unserer Website verschoben. Suchen Sie dort einfach nach Ihrer Frage.

4.1 Knowledge Base

Siehe "[Knowledge Base](#)" online.

5 Einführung

SmartPOP2Exchange bindet bestehende [POP3](#)- und [IMAP](#)-Konten an einen MS Exchange-Server oder jeden anderen [SMTP](#)-Server an. Es arbeitet im Hintergrund, lädt alle E-Mails von verschiedenen Postfächern herunter und leitet sie an Ihren Exchange oder SMTP-Server weiter. Zudem werden [PickupFolder](#) unterstützt. Eine einfach zu bedienende und übersichtliche [Konfigurationsoberfläche](#) erlaubt das Einstellen üblicher Optionen wie Intervall, Timeout, Ereignisanzeige etc. sowie das Hinzufügen, Löschen und Editieren von Exchange-/SMTP und POP3-/IMAP-Konten. Der enthaltene [Spam-Filter](#) kennzeichnet oder löscht auf Wunsch E-Mails, die als Spam identifiziert wurden. Die bekannte Software [SpamAssassin](#) wird zur Identifikation von Spam herangezogen und ist bereits vorkonfiguriert in der Installation enthalten. Außerdem enthält SmartPOP2Exchange ein leistungsfähiges und flexibles [Regelsystem](#), mit dem zusätzliche Aktionen für bestimmte Mails definiert werden können. Nahezu alle installierten [Virens Scanner](#) können von SmartPOP2Exchange verwendet werden, um infizierte E-Mails zu erkennen.



5.1 Quickstart

In diesem Kapitel erhalten Sie einen kleinen Einstieg in das Arbeiten mit SmartPOP2Exchange.

Wenn SmartPOP2Exchange das erste Mal startet und Sie keine Konten angelegt haben, wird automatisch der Konto-Assistent geöffnet.

Kontoassistent
Kontenname und Typ
Bitte geben Sie den Namen und den Konto-Typ an, den Sie erstellen möchten.

Bitte geben Sie den Namen für das Konto an:

Wählen Sie einen Konto-Typ:

Bei Verwendung des IMAP-Protokolls werden alle Ihre E-Mails von E-Mailserver auf den lokalen SMTP-Server heruntergeladen, in Gegensatz zu POP3, werden die E-Mails auf dem IMAP-Server nicht gelöscht.

Kontoassistent
IMAP Konto
Bitte geben Sie die Anmeldeinformationen für den IMAP-Server an, von dem die E-Mails abgeholt werden sollen.

Server (IMAP):

Server-Port:

Sicherheits-Modus:

Benutzername:

Passwort:

☐ Sende E-Mails an die in E-Mail-Header gefundene Adresse (Sammelkonto). Wenn Sie sich nicht sicher sind, ob Sie ein solches Konto verwenden, lassen Sie diese Option deaktiviert.

Kontoassistent
SMTP Server
Bitte geben Sie die Einstellungen für den Exchange (SMTP) Server an, zu dem die E-Mails weitergeleitet werden (Zielseite).

E-Mail-Adresse:

Server (SMTP):

Server-Port:

☒ Der Server benötigt Authentifizierung

Sicherheits-Modus:

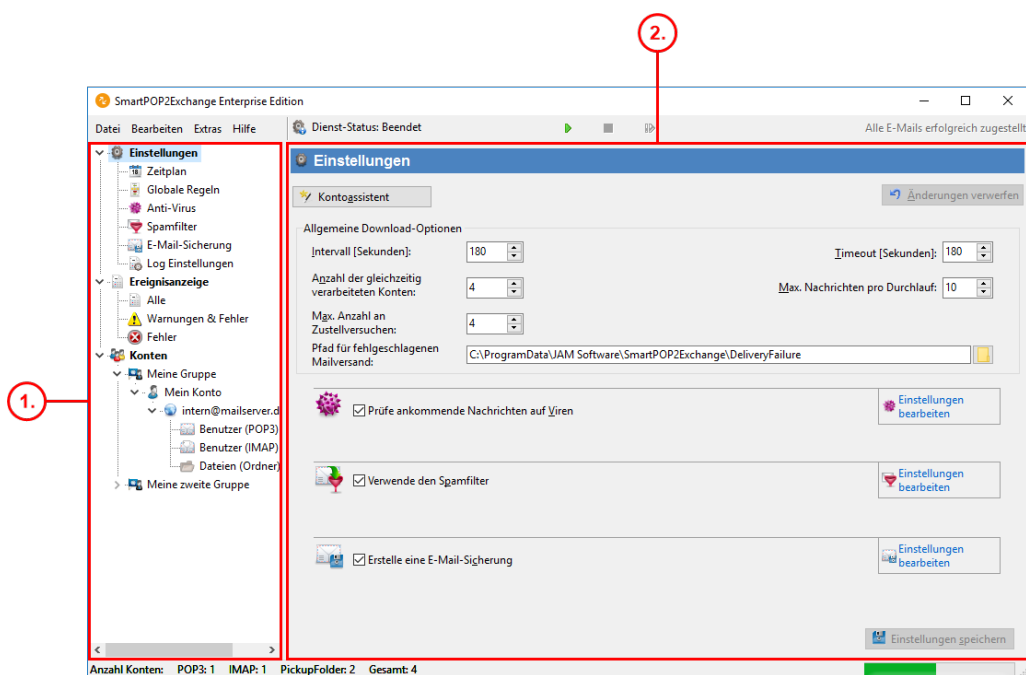
Benutzername:

Passwort:

Mit dem Konto-Assistenten können Sie bequem Schritt für Schritt Ihre Konten einrichten. Sie können den Assistenten auch später aufrufen. Benutzen Sie dafür die Schaltfläche **Kontoassistent** auf dem [Einstellungen](#) Knoten des Baumes.

Sie können auch SMTP Konten und POP3/IMAP/PickupFolder Konten manuell zu bestehenden Konten hinzufügen. Dies können Sie mit Hilfe des Menüs [Bearbeiten](#) erreichen, bzw. durch einen Rechtsklick mit der Maus auf dem entsprechenden Konto.

Das folgende Bild zeigt das Hauptfenster von SmartPOP2Exchange. Zu Beginn wird hier das [Einstellungen](#) angezeigt.



Über die Dienst-Symbolleiste erfahren Sie den Status des Dienstes. Sie können den Dienst von hier aus starten, pausieren, stoppen und neustarten, indem Sie auf den jeweiligen Knopf in der Symbolleiste klicken.

(1) Wählen Sie aus diesem Baum aus, welche Einstellungen Sie vornehmen möchten.

Einstellungen und die Unterpunkte *Logeinstellungen*, *Zeitplan*, *Globale Regeln* und *Spam Filter* ermöglichen es Ihnen, den Dienst Ihren Wünschen entsprechend zu konfigurieren sowie Spam-Filter und andere Funktionen zu (de)aktivieren.

Unter dem Punkt *Konten* finden Sie zuerst eine Aufstellung aller eingerichteten Konten. Zu jedem Konto gehört mindestens ein SMTP-Konto. Dieses wird als Unterpunkt des jeweiligen Kontos aufgelistet. Jedem SMTP-Konto können wiederum mehrere POP3-/IMAP-/PickupFolder-Konten zugeordnet werden. Diese POP3-/IMAP-Konten werden als Unterpunkte des jeweiligen SMTP-Kontos dargestellt.

Die Ereignisanzeige können Sie durch Auswählen des Ereignisanzeige-Knotens auswählen.

(2) Nachdem Sie ein Konto im Baum ausgewählt haben, können Sie hier alle Einstellungen vornehmen.

5.2 Starthilfe für Exchange Server Anbindung

Bitte beachten Sie die empfohlenen Einstellungen und für die Anbindung von Exchange Servern.

Sie finden in diesen Kapiteln auch hilfreiche Hinweise zur Einrichtung Ihres Exchange Servers:

[Starthilfe für Exchange Server 2000/2003](#)

[Starthilfe für Exchange Server 2007/2010](#)

[Starthilfe für Exchange Server 2013 - 2019](#)

5.2.1 Starthilfe für Exchange Server 2000/2003

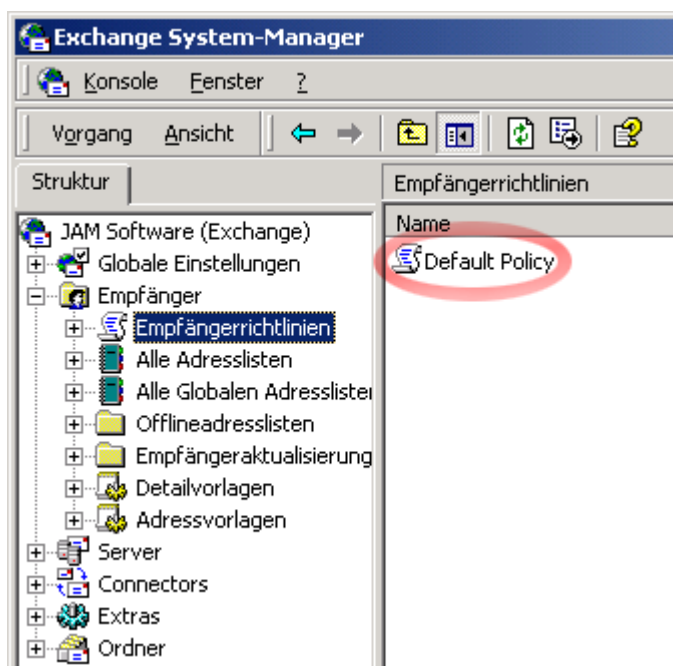
Im Folgenden wird kurz eine typische Konfiguration des MS Exchange-Server 2000/2003 und SmartPOP2Exchange beschrieben.

1. System-Manager starten

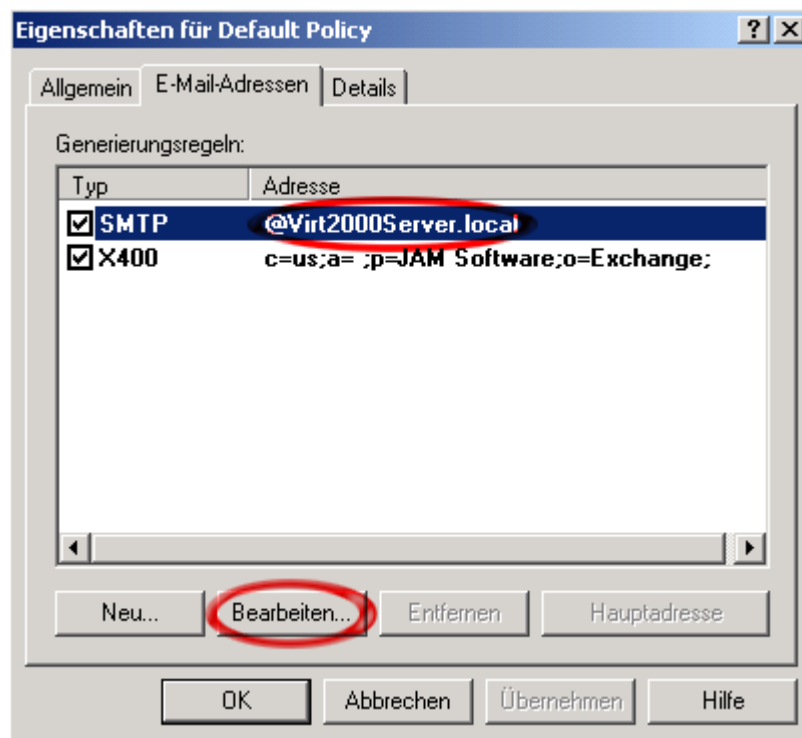
Wählen Sie aus dem Windows-Startmenü: **Start | Programme | Microsoft Exchange | System-Manager**

2. Einrichten des SMTP Standardempfängers

In Exchange haben alle Benutzer eine SMTP-Adresse, die mit Ihren Internet-Adressen übereinstimmt. Sie müssen ggf. die Standard-SMTP-Adresse ändern, damit der virtuelle SMTP-Server Nachrichten für Ihre Domäne akzeptiert.

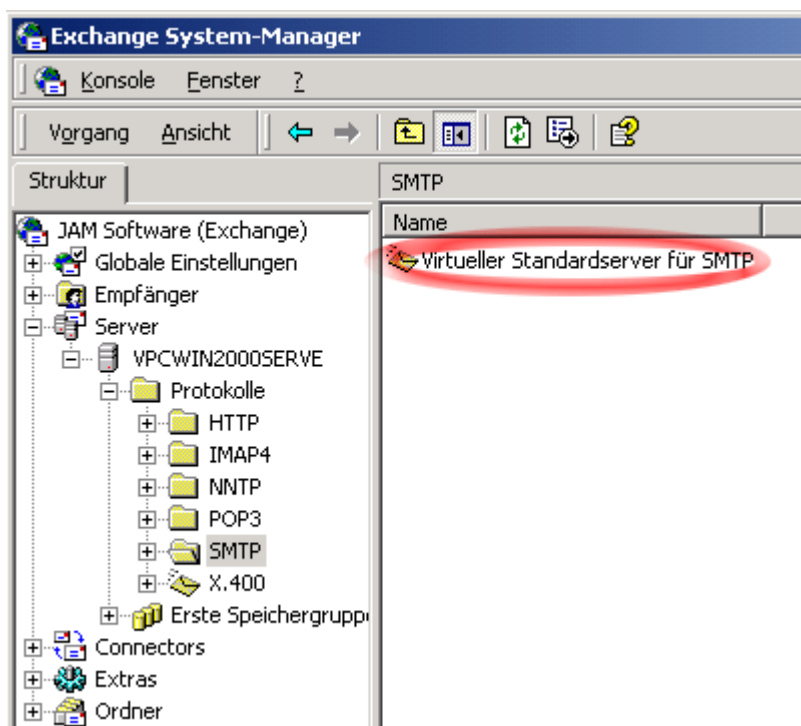


- Wählen Sie (im System-Manager) **Empfänger | Empfängerrichtlinien** aus.
- Klicken Sie mit der rechten Maustaste auf **Default Policy** und öffnen Sie die **Eigenschaften**.

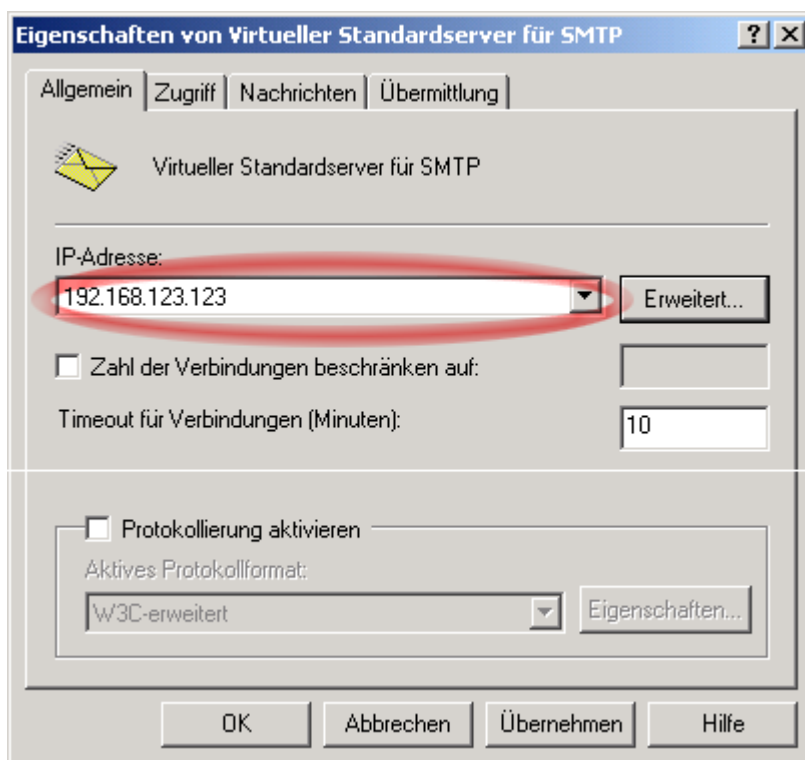


- Klicken Sie auf den Reiter **E-Mail-Adressen**.
- Markieren Sie **SMTP** in der Liste und klicken Sie auf **Bearbeiten**.
- Tragen Sie nun die Standard **SMTP-Adresse** ein (z.B. "@meinedomain.de") und drücken Sie **OK**.
- Nochmals mit **OK** bestätigen.

3. Die IP Adresse des virtuellen Standardservers für SMTP auslesen



- Wählen Sie unter **Server | <Ihr Exchange-Server> / Protokolle | SMTP** bitte **Virtueller Standardserver für SMTP** aus.
- Öffnen Sie, durch Anwahl mit der rechten Maustaste, die **Eigenschaften** des virtuellen Standardservers.



- Im Feld **IP-Adresse** sollten Sie jetzt Ihre IP finden. Bitte merken Sie sich diese.

4. Ausgehenden E-Mail-Verkehr konfigurieren

Standardmäßig ist ein MS Exchange-Server so konfiguriert, dass er E-Mails direkt via DNS-Lookup an den E-Mail Server des Empfängers sendet, was in den meisten Fällen auch korrekt ist. Sie können den Exchange-Server aber auch anweisen, alle E-Mails über den Mail-Server Ihres Providers zu senden, der in diesem Szenario dann "Smarthost" genannt wird. Diese Einstellungen können in den Eigenschaften von **Administrative Gruppen | <Ihre Gruppe> | Routinggruppen | <Ihre Routinggruppe> | Connectors | SMTP Connector** konfiguriert werden. Falls Ihr Provider zum Senden eine SMTP-Authentifizierung fordert, kann dies auf dem Reiter **Erweitert** mit der Schaltfläche **Ausgehende Sicherheit** konfiguriert werden.

5. SmartPOP2Exchange einrichten

Um SmartPOP2Exchange auf Ihrem Computer zu installieren, starten Sie bitte die Installationsdatei und befolgen Sie die weiteren Instruktionen. Sie können SmartPOP2Exchange über **Systemsteuerung | Software** wieder von Ihrem System entfernen.

Starten Sie nun SmartPOP2Exchange. Wenn Sie noch kein Konto erstellt haben, erscheint automatisch der Konto-Assistent. Sollte der Konto-Assistent nicht zu sehen sein, öffnen Sie ihn bitte über die Schaltfläche "Konto-Assistent" auf der Seite "Optionen".

- Drücken Sie **Weiter**
- Geben Sie einen **Namen** für Ihr Konto ein (z.B. "Mein Konto") und drücken Sie **Weiter**
- Geben Sie nun die **E-Mail Adresse** ein, an welche SmartPOP2Exchange ankommende Nachrichten weiterleiten soll
- Geben Sie nun die **IP-Adresse** von Schritt 3 in das Feld **Server (SMTP)** ein und drücken Sie **Weiter**
- Geben Sie nun den Namen des **POP3-Servers** und Ihren **Benutzernamen** bzw. **Passwort** in die entsprechenden Felder ein
- Drücken Sie **Fertig**

Weitere Konten können in gleicher Weise angelegt werden.

6. Automatische Antworten oder Weiterleitungen benutzen

Abwesenheitsantworten sind standardmäßig im Microsoft Exchange-Server deaktiviert. Viele Administratoren deaktivieren absichtlich die Option, Abwesenheitsantworten an Benutzer außerhalb der Exchange-Organisation zu senden, um zu verhindern, dass Außenstehende erfahren, wann Büros besetzt oder verlassen sind.

So aktivieren Sie Abwesenheitsantworten:

1. Starten Sie den Exchange-Systemmanager.
2. Doppelklicken Sie auf *Globale Einstellungen*, und klicken Sie dann auf *Internethinrichtenformat*.
3. Klicken Sie mit der rechten Maustaste in dem Detailbereich auf Domäne-Namen, und klicken Sie dann auf *Eigenschaft*. Dort finden Sie die Einstellungen für die Standard-SMTP-Domäne.
4. Klicken Sie in dem Feld *Eigenschaften* auf die Registerkarte **Erweitert**, und aktivieren Sie "Out of office responses" (*Abwesenheitsbenachrichtigungen*), dann das *Kontrolle*-Kästchen.

Es werden nun Abwesenheitsnachrichten für die gewählte Domäne versandt.

5.2.2 Starthilfe für Exchange Server 2007/2010

Im Folgenden wird kurz eine typische Konfiguration des MS Exchange-Server 2007/2010 und SmartPOP2Exchange beschrieben.

1. Den Exchange System-Manager einer MMC-Konsole hinzufügen

Öffnen Sie eine bestehende MMC-Konsole (*.msc Datei) oder erstellen Sie eine neue, indem Sie unter **Start | Ausführen**: "mmc.exe" eingeben.

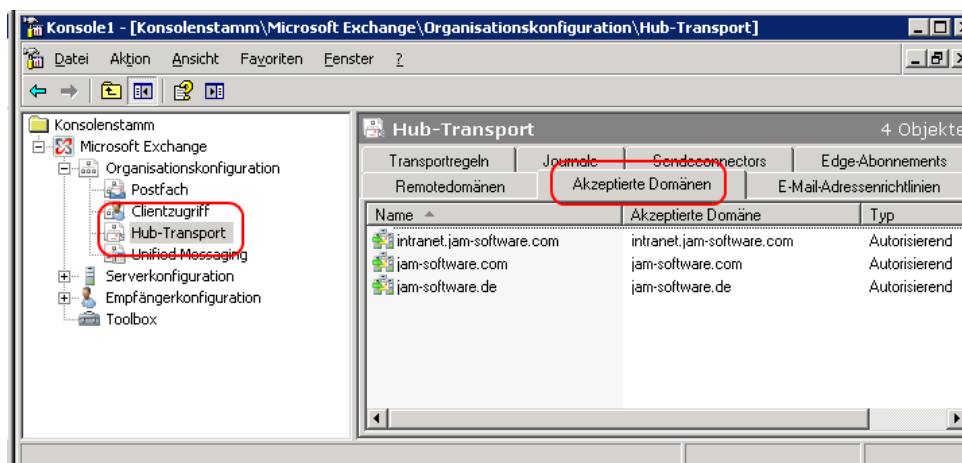
Wählen **Datei | Snap-In hinzufügen/entfernen** aus dem Menü der Konsole. Selektieren Sie **Microsoft Exchange** und fügen Sie dieses hinzu.

2. Einrichten akzeptierten Domänen

Sie müssen dem Exchange Server angeben, für welche E-Mail-Domänen er zuständig ist.

Wählen Sie Karteireiter **Akzeptierte Domänen** in den **Hub-Transport** Einstellungen der **Organisationskonfiguration**.

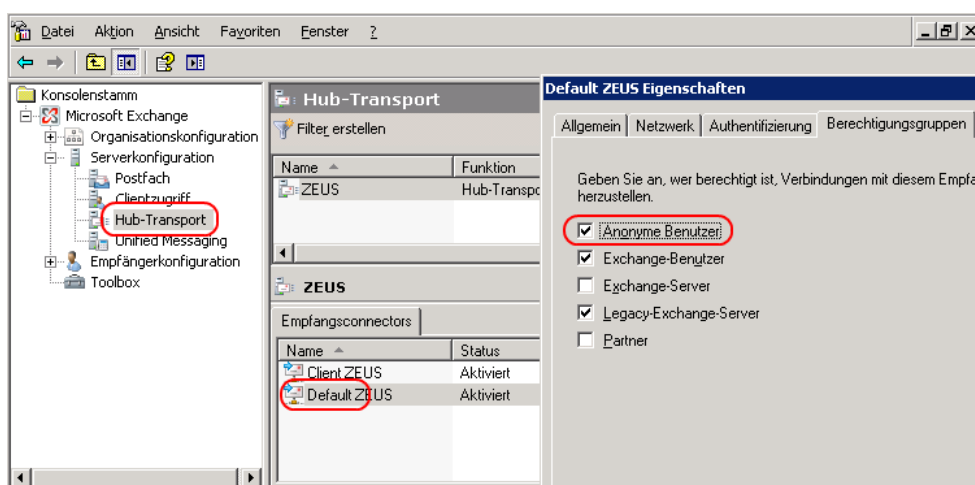
Sie können einen Eintrag für jede Domäne, die von Benutzer genutzt wird, erstellen, oder lediglich eine einzige, die alle Nachrichten akzeptiert (*). Letzteres ist nur empfohlen, wenn Ihr Exchange Server nicht direkt von Internet aus zugänglich ist.



3. Anonymen Zugriff für den empfangenden SMTP erlauben

Im Gegensatz zum Exchange 2003 ist die Option "Anonyme Benutzer" für eintreffende E-Mails nicht standardmäßig aktiviert.

Wir empfehlen, diese zu aktivieren, damit Sie in SmartPOP2Exchange keine SMTP-Anmeldeinformationen benötigen.



4. Ausgehenden E-Mail-Verkehr konfigurieren

Standardmäßig ist im Exchange-Server 2007 kein Sendecconnector eingerichtet. Sie müssen also selbst einen erstellen.

Wählen Sie dazu den Karteireiter **Sendecconnectors** in den **Hub Transport** Einstellungen der **Organisationskonfiguration** und fügen Sie einen neuen Sendecconnector für ausgehende E-Mails mit folgenden Einstellungen hinzu.

- Name: <beliebig>
- vorgesehene Verwendung: Internet
- Adressraum: *
- Netzwerkeinstellungen:

- Wählen Sie die erste Option (DNS)

wenn Ihr Exchange direkt mit dem Internet verbunden ist und eine fixe IP-Adresse besitzt.

- Nutzen Sie die zweite Option (smart host)

wenn Sie Ihre E-Mails durch den SMTP Server Ihres Providers schicken möchten/müssen;

fügen diesen Server hinzu und geben Sie Benutzernamen und Passwort auf der folgenden Setup-Seite an

auf der Sie auch **Standardauthentifizierung** aktivieren.

5. SmartPOP2Exchange einrichten

Um SmartPOP2Exchange auf Ihrem Computer zu installieren, starten Sie bitte die Installationsdatei und befolgen Sie die weiteren Instruktionen. Sie können SmartPOP2Exchange über **Systemsteuerung** | **Software** wieder von Ihrem System entfernen.

Starten Sie nun SmartPOP2Exchange. Wenn Sie noch kein Konto erstellt haben, erscheint automatisch der Konto-Assistent. Sollte der Konto-Assistent nicht zu sehen sein, öffnen Sie ihn bitte über die Schaltfläche "Konto-Assistent" auf der Seite "Optionen".

- Drücken Sie **Weiter**
- Geben Sie einen **Namen** für Ihr Konto ein (z.B. "Mein Konto") und drücken Sie **Weiter**
- Geben Sie nun die **E-Mail Adresse** ein, an welche SmartPOP2Exchange ankommende Nachrichten weiterleiten soll
- Geben Sie nun die **IP Adresse** von Schritt 3 in das Feld **Server (SMTP)** ein und drücken Sie **Weiter**
- Geben Sie nun den Namen des **POP3-Servers** und Ihren **Benutzernamen** bzw. **Passwort** in die entsprechenden Felder ein
- Drücken Sie **Fertig**

Weitere Konten können in gleicher Weise angelegt werden.

6. Message rejected as spam by Content Filtering

Das ist eine Meldung/Verhalten des Exchange Servers, nicht von SmartPOP2Exchange.

Der Exchange Server selbst hat auch einen Spamfilter integriert.

Dieser schlägt hier zu und nimmt die mail von SmartPOP2Exchange nicht an.

SmartPOP2Exchange verschickt dann stattdessen diese Benachrichtigung, damit kein Mail-Verlust entsteht.

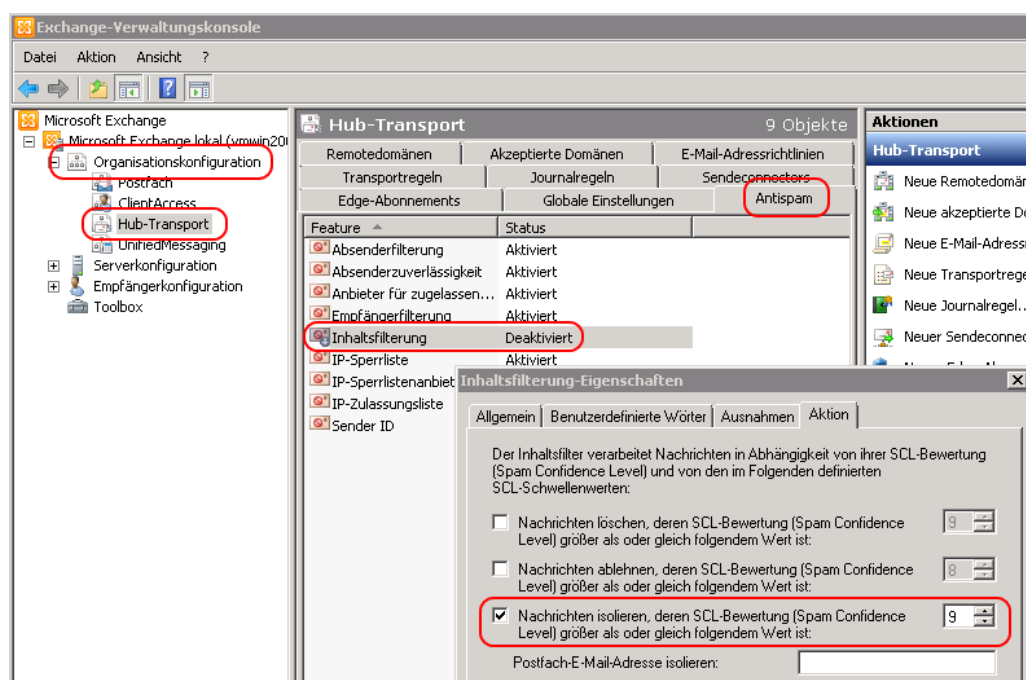
Alle E-Mails, die in einem POP3-Konto landen, sind final zugestellt.

Diese müssen z.B. auch **alle** archiviert werden. (siehe: **Exchange Server Toolbox Archiv**)

Somit ist das Ablehnen einer Mail, die von SmartPOP2Exchange an den Exchange Server gesendet wird, egal aus welchem Grund, ein undefiniertes Fehlverhalten. Weder Absender noch Empfänger erfahren etwas darüber.

Dies sollte also keinesfalls eine gewünschte Einstellung sein/bleiben.

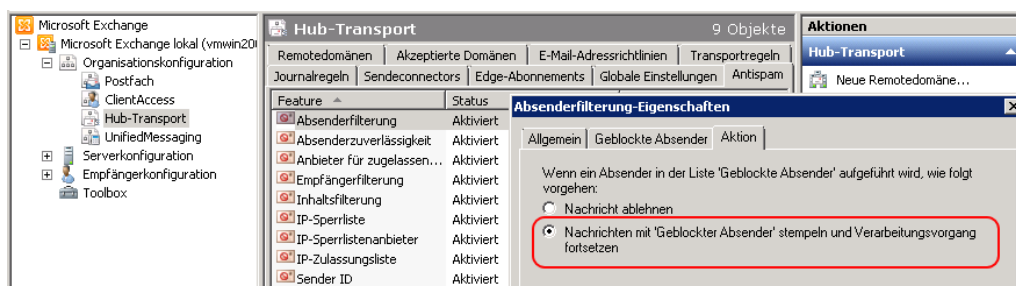
Bitte ändern Sie das Verhalten des der Inhaltsfilterung (Content-Filter) des Exchange Server und setzen Sie dessen Aktion auf "isolieren" oder schalten Sie diesen gleich ganz ab (der in SmartPOP2Exchange und der Exchange Server Toolbox enthaltene SpamAssassin ist leistungsfähiger).



Konfigurieren des Absender- und IP-Filters

Sofern der Absenderfilter nicht deaktiviert wird, sollte dieser so konfiguriert werden, dass die Nachricht markiert (stamped) und weitergeleitet wird, anstatt sie zurückzuweisen.

Dies geschieht mit einem Rechtsklick auf "Absenderfilterung". In dem Fenster unter dem Kartei-Reiter "Aktion" stellen Sie die Aktion von Zurückweisen auf "... mit 'Geblockter Absender' stempeln ..." um.



Sie sollten den Exchange Server in jedem Fall keine Mail ablehnen lassen!

Was soll SmartPOP2Exchange mit einer abgelehnten Mail tun?

Wegwerfen? --> Dann lassen Sie dies besser gleich den Exchange Server tun, das reduziert den Kommunikationsaufwand.

Beachten Sie, dass der Exchange Server auch standardmäßig eine Größenbeschränkung auf 10MB hat.

[http://technet.microsoft.com/en-us/library/aa996835\(v=exchg.80\).aspx](http://technet.microsoft.com/en-us/library/aa996835(v=exchg.80).aspx) oder <http://technet.microsoft.com/en-us/library/bb124345.aspx>

1. Starten Sie die Exchange Management Shell.
2. Geben Sie folgende Kommandos ein, um das Limit z.B. auf 100MB zu erhöhen:

```
Set-TransportConfig -MaxReceiveSize 100MB.
```

```
Get-ReceiveConnector | Set-ReceiveConnector -MaxmessageSize 100MB
```

```
(Get-MailBox | Set-Mailbox -MaxReceiveSize 100MB)
```

[Zum Abfragen der Werte z.B.: "Get-SendConnector | ft Name, MaxMessageSize"]

5.2.3 Starthilfe für Exchange Server 2013/2016

Im Folgenden wird kurz eine typische Konfiguration des MS Exchange-Server 2013 bis 2019 und SmartPOP2Exchange beschrieben.

1. Die Exchange-Verwaltungskonsole öffnen

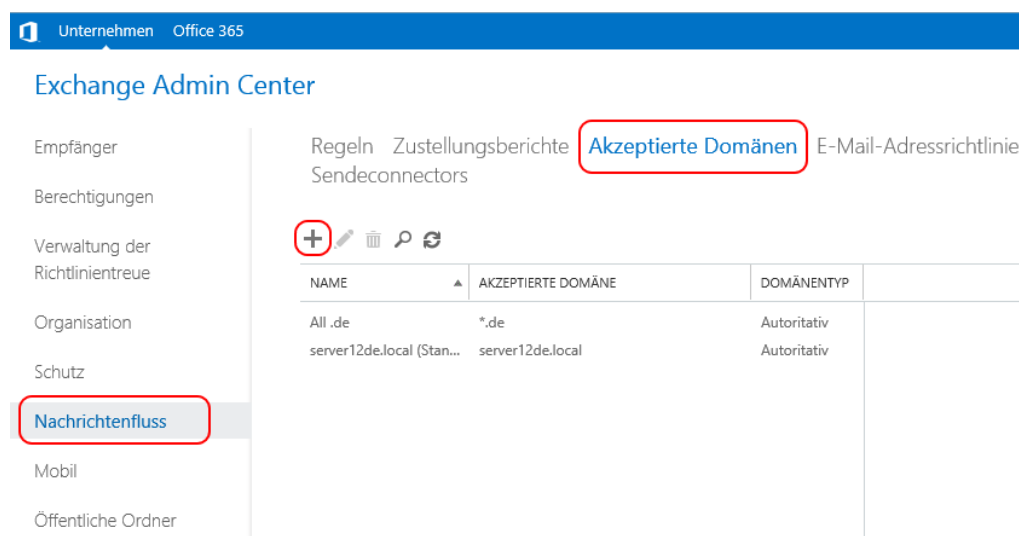
Öffnen Sie über die Taskleiste die Exchange-Verwaltungskonsole.

2. Einrichten akzeptierten Domänen

Sie müssen dem Exchange Server angeben, für welche E-Mail-Domänen er zuständig ist.

Wählen Sie Karteireiter **Akzeptierte Domänen** in den **Nachrichtenfluss** Einstellungen.

Sie können einen Eintrag für jede Domäne, die von Benutzer genutzt wird, erstellen, oder lediglich eine einzige, die alle Nachrichten akzeptiert (*). Letzteres ist nur empfohlen, wenn Ihr Exchange Server nicht direkt von Internet aus zugänglich ist.

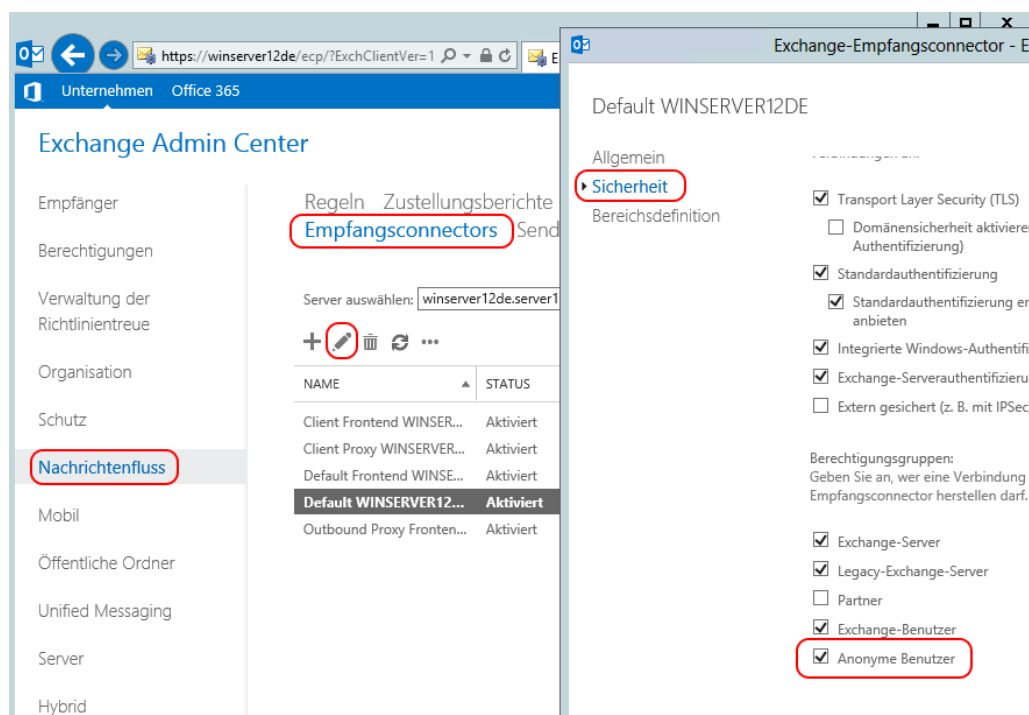


3. Anonymen Zugriff für den empfangenden SMTP erlauben

Im Gegensatz zum Exchange 2007/2010 ist die Option "Anonyme Benutzer" für eintreffende E-Mails standardmäßig über den "Default Frontend" Connector aktiviert.

Wir empfehlen, diese aktiviert zu lassen, damit Sie in SmartPOP2Exchange keine SMTP-Anmeldeinformationen benötigen.

Wenn Sie diese Einstellung dennoch ändern wollen, können Sie das unter dem Karteireiter **Empfangsconnectors** in den **Nachrichtenfluss** Einstellungen.



4. Ausgehenden E-Mail-Verkehr konfigurieren

Standardmäßig ist im Exchange-Server 2013 kein Sendecconnector eingerichtet. Sie müssen also selbst einen erstellen.

Wählen Sie dazu den Karteireiter **Sendecconnectors** in den **Nachrichtenfluss** Einstellungen und fügen Sie einen neuen Sendecconnector für ausgehende E-Mails mit folgenden Einstellungen hinzu.

- Name: <beliebig>
- vorgesehene Verwendung: Internet
- Netzwerkeinstellungen:
 - Wählen Sie die erste Option (MX-Eintrag)
 - wenn Ihr Exchange direkt mit dem Internet verbunden ist und eine fixe IP-Adresse besitzt.
 - Nutzen Sie die zweite Option (smart host)
 - wenn Sie Ihre E-Mails durch den SMTP Server Ihres Providers schicken möchten/müssen;
 - fügen Sie diesen Server hinzu und geben Sie Benutzernamen und Passwort auf der folgenden Setup-Seite an
 - auf der Sie auch **Standardauthentifizierung** aktivieren.
- Adressraum:
 - Typ: SMTP
 - FQDN: *

- Kosten: 1

- Quellserver: Als Quellserver geben Sie den eigenen Server an.

5. Message rejected as spam by Content Filtering

Das ist eine Meldung/Verhalten des Exchange Servers, nicht von SmartPOP2Exchange.

Der Exchange Server selbst hat auch einen Spamfilter integriert.

Dieser schlägt hier zu und nimmt die Mail von SmartPOP2Exchange nicht an.

SmartPOP2Exchange verschickt dann stattdessen diese Benachrichtigung, damit kein Mail-Verlust entsteht.

Alle E-Mails, die in einem POP3-Konto landen, sind final zugestellt.

Diese müssen z.B. auch **alle** archiviert werden. (siehe: **Exchange Server Toolbox Archiv**)

Somit ist das Ablehnen einer Mail, die von SmartPOP2Exchange an den Exchange Server gesendet wird, egal aus welchem Grund, ein undefiniertes Fehlverhalten. Weder Absender noch Empfänger erfahren etwas darüber.

Dies sollte also keinesfalls eine gewünschte Einstellung sein/bleiben.

Bitte ändern Sie das Verhalten der Inhaltsfilterung (Content-Filter) des Exchange Server und setzen Sie dessen Aktion auf "isolieren" oder schalten Sie diesen gleich ganz ab (der in SmartPOP2Exchange und der Exchange Server Toolbox enthaltene SpamAssassin ist leistungsfähiger).

Diese Einstellungen werden bei dem Exchange Server 2013 über die Exchange Management Shell konfiguriert.

Folgendes Kommando schaltet das Zurückweisen und das Löschen ab und das Isolieren an:

```
Set-ContentFilterConfig -SCLDeleteEnabled $false -SCLRejectEnabled $false -SCLQuarantineEnabled $true
```

Um zu prüfen, ob das Kommando funktioniert hat, können Sie das `Get-ContentFilterConfig` Kommando benutzen:

```
Get-ContentFilterConfig | Format-List SCL*
```

Sie sollten dann eine Ausgabe wie die Folgende sehen:

```
[PS] C:\>Get-ContentFilterConfig | Format-List SCL*

SCLRejectThreshold      : 7
SCLRejectEnabled        : False
SCLDeleteThreshold      : 9
SCLDeleteEnabled        : False
SCLQuarantineThreshold  : 9
SCLQuarantineEnabled    : True
```

Konfigurieren des Absender- und IP-Filters

Diese Filter sind auf ähnliche Weise wie der Inhaltsfilter zu konfigurieren.

Sofern der Absenderfilter nicht deaktiviert wird, sollte dieser so konfiguriert werden, dass die Nachricht markiert (stamped) und weitergeleitet wird, anstatt sie zurückzuweisen.

Dieses wird auf der Shell mit folgendem Befehl gemacht:

```
Set-SenderFilterConfig -Action StampStatus
```

Um zu prüfen, ob es funktioniert hat, können Sie `Get-SenderFilterConfig` benutzen und sollten dann in etwa so eine Ausgabe sehen:

```
[PS] C:\>Get-SenderFilterConfig

RunspaceId      : 5aaaabc77-a2e6-493e-9901-bf01011c3bb5
Name            : SenderFilterConfig
BlockedSenders  : {}
BlockedDomains  : {}
BlockedDomainsAndSubdomains : {}
Action          : StampStatus
BlankSenderBlockingEnabled : False
RecipientBlockedSenderAction : Reject
Enabled         : True
ExternalMailEnabled : True
InternalMailEnabled : False
```

Den IP-Filter schalten Sie mit folgendem Befehl ab:

```
Set-IPBlockListConfig -Enabled $false
```

Und zur Überprüfung kann folgender Befehl benutzt werden:

```
Get-IPBlockListConfig
```

Sie sollten den Exchange Server in jedem Fall keine Mail ablehnen lassen!

Was soll SmartPOP2Exchange mit einer abgelehnten Mail tun?

Wegwerfen? --> Dann lassen Sie dies besser gleich den Exchange Server tun, das reduziert den Kommunikationsaufwand.

6 Menüs

Menüs:

[Datei-Menü](#)

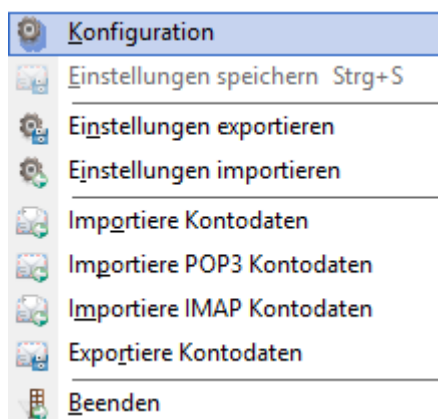
[Bearbeiten-Menü](#)

[Tools-Menü](#)

[Hilfe-Menü](#)

6.1 Datei-Menü

Das Datei-Menü erlaubt es Ihnen, Einstellungen zu im- bzw. exportieren und zu speichern.



Konfiguration Zeigt Ihnen das Konfigurations-Formular an.

Einstellungen Speichert alle Änderungen an den Einstellungen.
(Alle Änderungen an den Einstellungen werden erst wirksam, wenn sie explizit gespeichert wurden.)

Einstellungen Speichert alle ihre Konfigurationen als Zip-Archiv.
Das Zip Archiv enthält zusätzlich zu der XML Datei mit den Konto Einstellungen auch noch die Einstellungen für den Spamassassin.

Einstellungen Stellt die Einstellungen mit Hilfe der Backup-Dateien wieder her.

Importiere Ermöglicht das [Importieren von Kontendaten](#) aus CSV, Datenbank, Excel und MS Access-Dateien. Der Kontotyp wird über ein Datenfeld bestimmt.

Importiere POP3 Ermöglicht das [Importieren von POP3 Kontendaten](#) aus CSV, Datenbank, Excel und MS Access-Dateien.

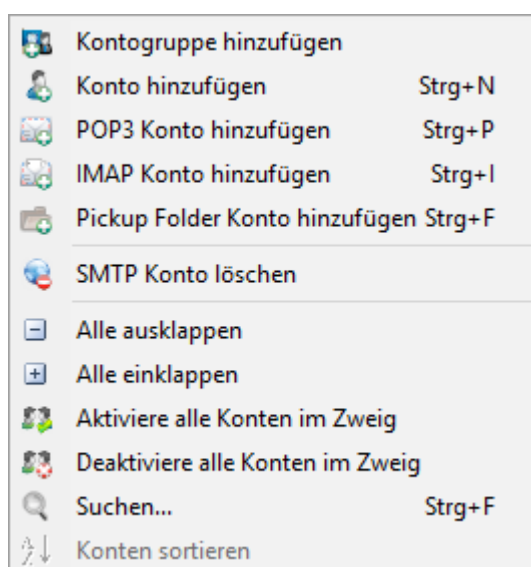
Importiere IMAP Ermöglicht das [Importieren von IMAP Kontendaten](#) aus CSV, Datenbank, Excel und MS Access-Dateien.

Exportiere Ermöglicht das Exportieren ihrer Kontendaten als CSV Datei. Diese Datei kann für einen Import benutzt werden. Es werden aus Sicherheitsgründen keine Passwörter exportiert.

Beenden Beendet das Programm

6.2 Bearbeiten-Menü

Das Bearbeiten-Menü erlaubt es Ihnen, den Konto-Assistenten aufzurufen und Konten zu sortieren. Darüberhinaus werden kontextsensitiv besonders häufig genutzte Funktionen (Konten duplizieren, SMTP-Konten oder POP3-/IMAP-Konten erstellen oder vorhandene entfernen) angezeigt, wenn Sie in der Konten-Übersicht ein Konto ausgewählt haben.



Kontoassistent Dieser Assistent hilft Ihnen bei der Erstellung eines kompletten Kontos mit einem SMTP-Konto sowie einem POP3-Konto.

Konto Fügt ein neues Konto hinzu, entfernt oder dupliziert ein bestehendes.

SMTP

Fügt ein neues SMTP-Konto hinzu oder entfernt ein bestehendes.

POP3

Fügt ein neues POP3-Konto hinzu oder entfernt ein bestehendes.

IMAP

Fügt ein neues IMAP-Konto hinzu oder entfernt ein bestehendes.

PickupFolder

Fügt ein neues PickupFolder-Konto hinzu oder entfernt ein bestehendes.

Konten sortieren

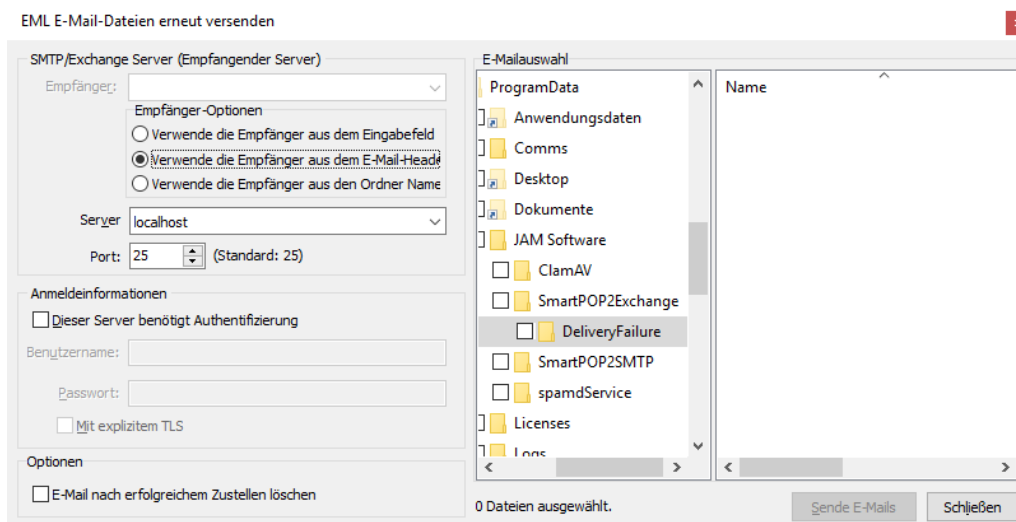
Sortiert alle bestehenden Konten in alphabetischer Reihenfolge.

6.3 Tools-Menü

Das *Tools* Menü stellt Ihnen zusätzliche nützliche kleine Programme für SmartPOP2Exchange zur Verfügung.

Sende EML E-Mail Dateien..

Zeigt einen Dialog, in dem Sie Einstellungen zum erneuten Versenden von EML E-Mails Dateien vornehmen können.



SMTP/Exch Wählen Sie den SMTP-Server, der die E-Mails empfangen soll, und stellen Sie die Empfänger E-Mail-Adresse ein.

Empfänger Wählen Sie, ob der Empfänger aus dem Eingabefeld, den E-Mail-Headern (Catch-All) oder dem übergeordneten Ordnernamen entnommen werden soll.

Anmeldeinfo Geben Sie den Benutzernamen und das Kennwort für den ausgewählte SMTP-Server ein.

Optionen: Option, die E-Mails nach dem erfolgreichen Senden zu löschen.

E- Wählen Sie die E-Mails, die wieder versendet werden sollen.

6.4 Hilfe-Menü

Über das **Hilfe** Menü können Sie diese Hilfe-Datei öffnen und weitere Informationen über SmartPOP2Exchange anzeigen lassen.

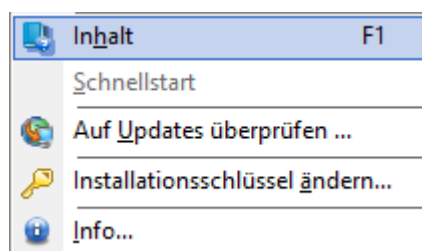
Inhalt Öffnet diese Hilfedatei.

Schnellstart Zeigt das Starthilfe Kapitel für SmartPOP2Exchange aus dieser Hilfedatei.

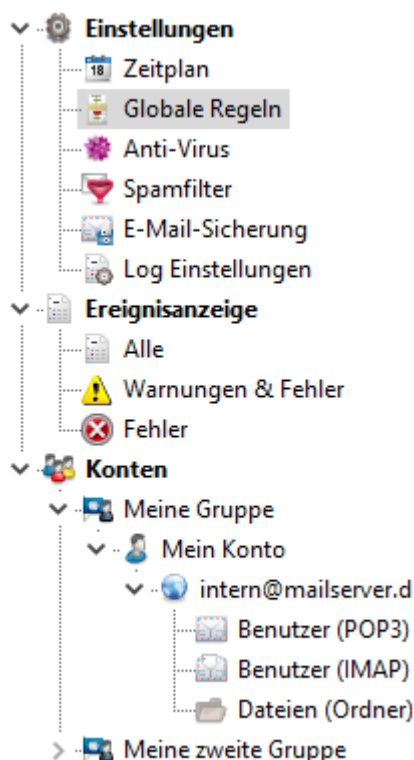
Auf Update Überprüft, ob eine neuere Version von SmartPOP2Exchange verfügbar ist.

Installationsschl Zeigt die Eingabemaske, um einen neuen Installationsschlüssel anzugeben.

Info... Zeigt den Info Dialog von SmartPOP2Exchange.



7 Navigationsbereich



Hier können Sie in einer Baumstruktur all Ihre Konten, SMTP-, POP3- und IMAP-Konten sehen. Sie erhalten außerdem Zugriff auf das Einstellungs-Formular und die Ereignisanzeige-Anzeige. Klicken Sie hierfür einfach auf das jeweilige Symbol.

Für weitere Informationen über spezifische Einstellungsmöglichkeiten der einzelnen Untereinheiten schauen Sie bitte unter : [Optionen](#), [Zeitplan-Optionen](#), [Globale Regeln](#), [Spam-Filter](#), [Logeinstellungen](#), [Konto](#), [SMTP](#), [POP3](#), [IMAP](#) , [PickupFolder](#) oder [Ereignisanzeige](#).

Ist das Symbol eines Benutzerkontos mit einem roten Kreuz versehen, so sind dessen Unterkonten (SMTP/POP3/IMAP) soweit deaktiviert, dass von diesem Konto keine E-Mails verarbeitet werden.

7.1 Einstellungen

Indem Sie im Menu [Datei](#) oder im [Navigationsbereich](#) **Einstellungen** auswählen, gelangen Sie zum **Einstellungen**-Formular.

Dieses Formular gibt Ihnen neben zentralen Optionen eine kompakte Übersicht über die Hauptfunktionen von SmartPOP2Exchange und stellt eine Schaltfläche für den Kontoassistenten bereit, den Sie ansonsten auch immer über das Kontextmenü im Navigationsbereich erreichen können.


Hier kann man folgende Einstellungen vornehmen:

Intervall	Legt die Zeit zwischen 2 Downloads desselben Kontos fest. Die Zeitspanne reicht von 1 bis 6400 Sekunden.
Timeout	Dieses Feld gibt den Zeitraum in Sekunden an, den SmartPOP2Exchange auf die Antwort eines anderen Servers (pop3, imap, smtp) wartet.
Anzahl der gleichzeitig verarbeiteten Konten	Hier können Sie festlegen, wie viele Konten gleichzeitig verarbeitet werden. Um CPU-Zeit zu sparen verkleinern Sie diesen Wert. Je mehr Konten Sie haben, desto eher sollten Sie diesen Wert erhöhen.



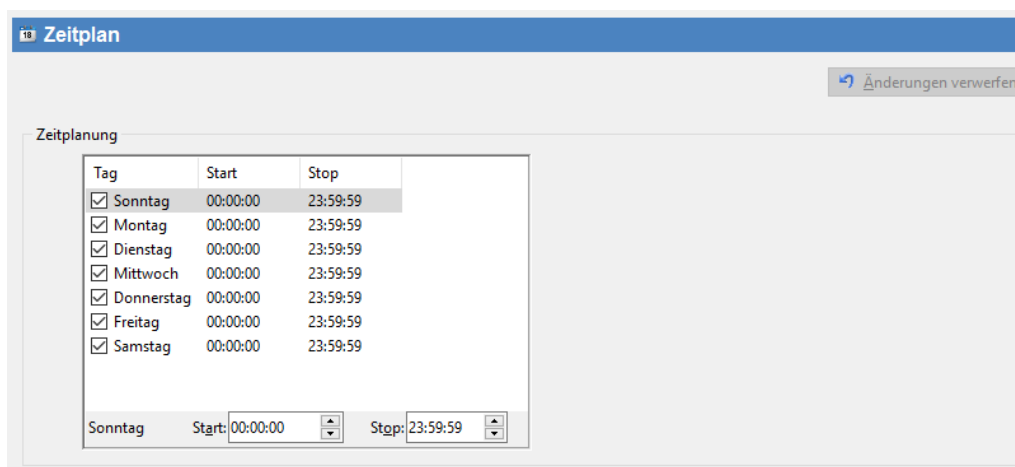
Über die Dienst-Symbolleiste (am oberen Rand des Fensters) erfahren Sie den Status des Dienstes. Sie können den Dienst von hier aus starten, stoppen und neustarten, indem Sie auf den jeweiligen Knopf in der Symbolleiste klicken.

Um Änderungen rückgängig zu machen, drücken Sie die Rückgängig-Schaltfläche.

 **Bitte beachten Sie, dass alle Änderungen nur nach dem ausdrücklichen Speichern der Einstellungen vom Dienst berücksichtigt werden.**

7.1.1 Zeitplan

Wenn Sie **Zeitplan** im [Navigationsbereich](#) auswählen, gelangen Sie zu diesem Formular. Hier können Sie folgende Einstellungen vornehmen:



Tag	Start	Stop
<input checked="" type="checkbox"/> Sonntag	00:00:00	23:59:59
<input checked="" type="checkbox"/> Montag	00:00:00	23:59:59
<input checked="" type="checkbox"/> Dienstag	00:00:00	23:59:59
<input checked="" type="checkbox"/> Mittwoch	00:00:00	23:59:59
<input checked="" type="checkbox"/> Donnerstag	00:00:00	23:59:59
<input checked="" type="checkbox"/> Freitag	00:00:00	23:59:59
<input checked="" type="checkbox"/> Samstag	00:00:00	23:59:59


Sonntag Start: 00:00:00 Stop: 23:59:59

Tag Wählen Sie hier die Wochentage aus, an denen SmartPOP2Exchange Ihre Konten auf Nachrichten überprüft.

Start Geben Sie hier den Zeitpunkt für den ausgewählten Tag an, an dem SmartPOP2Exchange beginnt, Ihre Konten regelmäßig zu überprüfen.

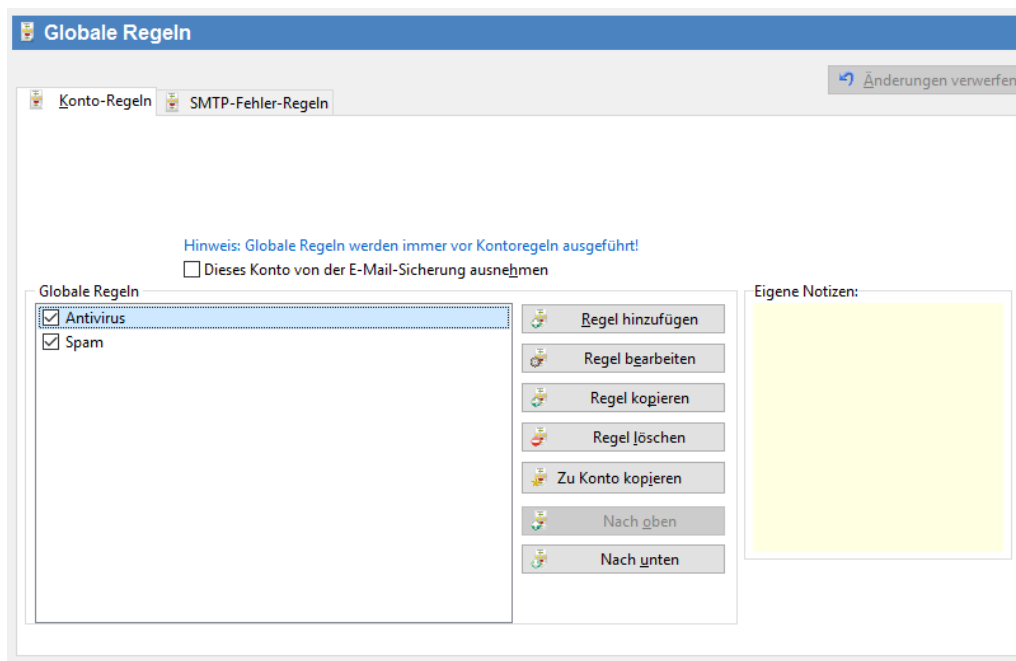
Stop Geben Sie hier den Zeitpunkt für den ausgewählten Tag an, an dem SmartPOP2Exchange Ihre Konten nicht mehr regelmäßig überprüfen soll. (Liegt dieser Zeitpunkt vor der Startzeit, dann findet keine Überprüfung statt.)

Um Änderungen rückgängig zu machen, drücken Sie die Rückgängig-Schaltfläche.

 **Bitte beachten Sie, dass alle Änderungen nur nach dem ausdrücklichen Speichern der Einstellungen vom Dienst berücksichtigt werden.**

7.1.2 Globale Regeln

Wenn Sie **Globale Regeln** im [Navigationsbereich](#) auswählen, gelangen Sie zu diesem Formular. Hier können Sie folgende Einstellungen vornehmen:



Regel Diese Schaltfläche fügt dem Konto eine neue [Regel](#) hinzu.

Regel Mit dieser Schaltfläche können Sie die ausgewählte [Regel](#) bearbeiten.


Regel Mit dieser Schaltfläche können Sie die ausgewählte [Regel](#) in das aktuelle oder ein anderes Konto kopieren.

Regel Mit dieser Schaltfläche können Sie die ausgewählte [Regel](#) löschen.

Aufwärts Hier können Sie die Reihenfolge, in der die Regeln benutzt werden, verändern. Dabei ist die oberste Regel die zuerst angewandte.

Globale Hier sind alle globalen Regeln aufgelistet. Sie können Regeln aktivieren/deaktivieren, indem Sie das Kontrollkästchen neben dem Namen anklicken. Sie können eine Regel auch durch Doppelklick bearbeiten.

Um Änderungen rückgängig zu machen, drücken Sie die Rückgängig-Schaltfläche.

 **Bitte beachten Sie, dass alle Änderungen nur nach dem ausdrücklichen Speichern der Einstellungen vom Dienst berücksichtigt werden.**

7.1.3 Antivirus

Wenn Sie **Antivirus** im [Navigationsbereich](#) auswählen, gelangen Sie zu diesem Formular. Hier können Sie folgende Einstellungen vornehmen:

Anti-Virus-Einstellungen

Änderungen verwerfen

☒ Prüfe ankommende Nachrichten auf Viren

[Das Aktivieren dieser Option erstellt eine globale "Anti-Virus"-Regel - Klicken zum Bearbeiten](#)

☐ Verwende die installierte Anti-Virus-Software Virens Scanner Testen

☒ Benutze den integrierten ClamAV

ClamAV

ClamAV version: ClamAV 0.100.2 (0.100.2) Signaturen aktualisieren

Letztes Signaturupdate: 08.11.2018 15:22

[Um in ClamAV zusätzliche Signaturen von sanesecurity zu integrieren klicken Sie diesen Link \(führt 'sanesecurity_install.bat' aus\).](#)

☐ Infizierte E-Mails vom Backup ausschließen

☐ Gefundene Viren nur als Warnung protokollieren

☐ ClamAV Update Fehler nur als Warnung protokollieren

Prüfe ankommende Nachrichten auf Viren

Hier können Sie die Antivirus-Funktion aktivieren. SmartPOP2Exchange nutzt dann den installierten [Virens Scanner](#), um eingehende Nachrichten auf Viren zu prüfen.

Virens Scanner

Klicken Sie diese Schaltfläche an, um von SmartPOP2Exchange eine Virus-Test-Datei auf Ihre Festplatten schreiben zu lassen und so festzustellen, ob Ihr Virens Scanner diese erkennt. Wenn der Test erfolgreich ist, kann SmartPOP2Exchange die installierte Anti-Viren-Software benutzen.

Benutze den

Wählen Sie diese Option, wenn Sie bereits einen [Virens Scanner](#) mit OnAccess-Funktion installiert haben.

Benutze den integrierten ClamAV	Wählen Sie diese Option, damit SmartPOP2Exchange den integrierten ClamAV nutzt
Signaturen aktualisieren	Verwenden Sie diese Schaltfläche, um eine Signaturaktualisierung des ClamAV manuell anzustoßen.
Infizierte Nachrichten vom Backup ausschließen	Wenn diese Option ausgewählt ist, wird SmartPOP2Exchange Nachrichten, die vom Virens Scanner als schädlich erkannt wurden, wieder aus dem Backup entfernen. Diese Option ist ebenfalls in den Einstellungen E-Mail Sicherung zu finden.
Gefundene Viren nur als Warnung protokollieren	Wählen Sie diese Option, damit SmartPOP2Exchange Virenfunde nur als Warnung protokolliert
ClamAV Update Fehler nur als Warnungen protokollieren	Wählen Sie diese Option, damit SmartPOP2Exchange Fehler während des Updates von ClamAV nur als Warnungen protokolliert.

7.1.4 Spam Filter

Wenn Sie **Spam Filter** im [Navigationsbereich](#) auswählen, gelangen Sie zu diesem Formular. Hier können Sie folgende Einstellungen vornehmen:

Spam-Filter aktivieren:

Globale	Wählen Sie diese Option, um eine globale Spam-Regel zu aktivieren, die für alle Konten angewendet wird.
---------	---

Spam-Filter- Hier können Sie den Spam-Filter für jedes Konto ein bzw. ausschalten. Wenn Sie eine Spam-Regel für ein Konto aktivieren, welches zuvor keine solche Regel besaß, dann wird eine neue Regel erzeugt.

Alle/Keinen Diese Knöpfe schalten alle Konto Spam-Filter ein bzw. aus.

Bearbeiten Sie können hiermit die Spam-Regel des gewählten Kontos bearbeiten. Beachten Sie bitte, dass nach der Deaktivierung der Spam-Bedingung die Regel nicht mehr in der Spamfilter Liste auftaucht. Sollte es mehr als eine Spam-Regel im ausgewählten Konto geben, dann können Sie hiermit die erste Spam-Regel bearbeiten.

The screenshot shows the 'Spamfilter-Optionen' (Spam Filter Options) window. It has three tabs: 'Spamfilter aktivieren', 'Spam Filter Listen', and 'Spamfilter-Optionen'. The 'Spamfilter-Optionen' tab is active. It contains a message: 'Der Schwellenwert für Spam kann in jeder Spamregel angepasst werden.' (The threshold for spam can be adjusted in each spam rule). Below this, there are two lists: 'Whitelist (Sender)' with the entry 'meine@freunde.de' and 'Blacklist (Sender)' with the entry 'spam@absender.de'. To the right, there is a text area for 'gutes meine interessen'. Below the text area, there is a slider for 'Spam-Wahrscheinlichkeit von E-Mails, die diese Wörter enthalten:' (Spam probability of emails containing these words). The slider is positioned between 'Manchmal' (Sometimes) and 'Eher nicht' (Probably not), with 'Nie' (Never) at the far right.

Spam-Filter Listen:

Blacklist für Fügen Sie hier die Adressen hinzu, von denen nur Spam zu erwarten ist. (Der Spam-Filter wird Nachrichten von diesen Absendern eher als Spam deklarieren als andere.)

Whitelist für Fügen Sie hier die Adressen hinzu, von denen nur Ham (kein Spam) zu erwarten ist. (Der Spam-Filter wird Nachrichten von diesen Absendern nicht so leicht als Spam deklarieren.)

Anmerkung: Sie können auch Adressen wie **@domain.com* eingeben. Dies bedeutet dann, dass alle Adressen von dieser Domäne genommen werden.

Whitelist für Fügen Sie hier Wörter oder Wortgruppen hinzu, die in Spam nicht auftauchen sollten. Dies sind z.B. Firmennamen, Produktnamen usw.

Der Spam-Filter wird Nachrichten, die diese Wörter im Betreff oder Rumpf enthalten - je nach Bewertung (s.u.) - eher als Ham (= zulässige Nachricht) deklarieren.

Bewertung Ändern Sie mit dem Schiebeelement (Slider), wie "sicher" diese Wörter Nachrichten als Spam ausweisen.

Spamfilter aktivieren Spam Filter Listen Spamfilter-Optionen

Bayes-Filter Der Schwellenwert für Spam kann in jeder Spamregel angepasst werden.

Spam trainieren Ham trainieren

[Klicken Sie hier für einen komfortablen Weg den Spamfilter mit Hilfe von POP3 Konten zu trainieren](#)

Erlaubte Zeichensätze

- ☒ Westeuropäisch
- ☒ Japanisch
- ☒ Koreanisch
- ☒ Kyrillisch
- ☒ Thai
- ☒ Chinesisch

Benutzerdefinierte SpamAssassin CF Datei

Spam-Filter Optionen:

Trainiere Benutzen Sie diese Schaltflächen, um den Bayes-Filter mit E-Mails aus Dateien zu trainieren. Dies wird die Effizienz des

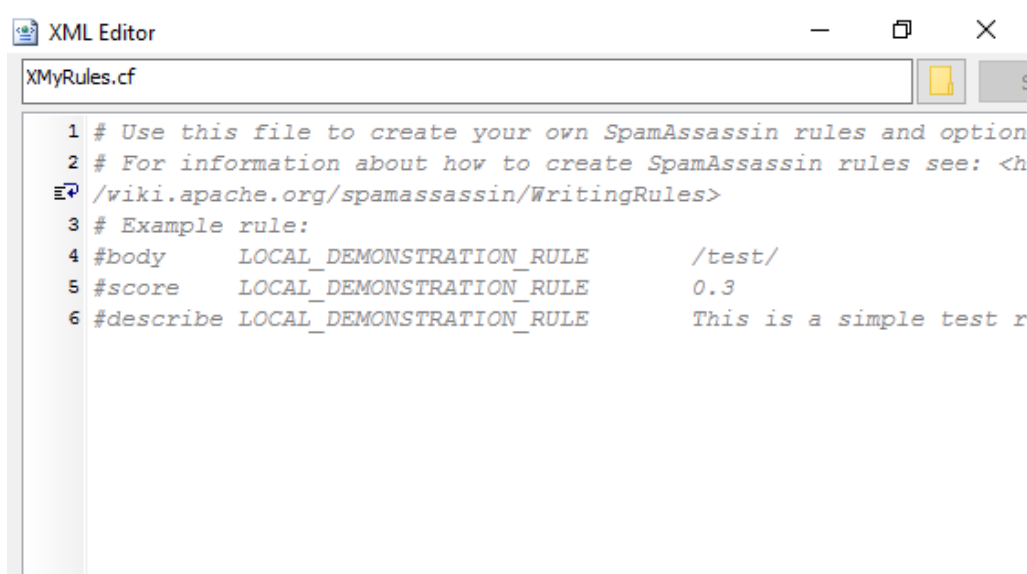
Filters verbessern. Die E-Mails müssen als txt-Dateien im MIME-Format vorliegen (wie sie z.B. von Outlook Express gespeichert werden).

Erlaubte Hier können Sie wählen, welche Zeichensätze (links) und Sprachen (rechts) erlaubt sind. Wenn keine oder alle Zeichensätze bzw. Sprachen ausgewählt sind, sind alle erlaubt.





und Sprachen

Benutzerdefini Hier können Sie eine eigene SpamAssassin Konfigurationsdatei selbst direkt editieren. Bitte beachten Sie, dass wir keine Support dafür geben. Anleitung und Hilfestellungen dafür gibt es z.B. hier: <http://wiki.apache.org/spamassassin/WritingRules>

SpamAssassi



```
1 # Use this file to create your own SpamAssassin rules and options
2 # For information about how to create SpamAssassin rules see: <http://wiki.apache.org/spamassassin/WritingRules>
3 # Example rule:
4 #body      LOCAL_DEMONSTRATION_RULE      /test/
5 #score     LOCAL_DEMONSTRATION_RULE      0.3
6 #describe  LOCAL_DEMONSTRATION_RULE      This is a simple test rule
```


-  **Wenn der Bayes-Filter aktiv ist, kann man nach einiger Zeit den Schwellwert für Spam senken.**
-  **Bitte beachten Sie, dass alle Änderungen nur nach dem ausdrücklichen Speichern der Einstellungen vom Dienst berücksichtigt werden.**
-  **Sie können die Spam-Filter Regeln genau wie jede andere Regel im Konto-Formular ändern.**
-  **Es sollte beachtet werden, dass auch bei einer Bewertung von "... niemals Spam." die ankommenden Nachrichten von [SpamAssassin](#) getestet werden und in extremen Fällen als Spam befunden werden können.**

7.1.5 E-Mail Sicherung

Wenn Sie **E-Mail Sicherung** im [Navigationsbereich](#) auswählen, gelangen Sie zu diesem Formular. Hier können Sie folgende Einstellungen vornehmen:

Speichere eine Kopie ankommender E-Mail in folgendem Pfad: SmartPOP2Exchange wird durch Aktivieren dieser Option für jede ankommende Nachricht eine Kopie auf Ihrer Festplatte speichern. Legen Sie hier fest, wo die Sicherheitskopien der Nachrichten abgelegt werden sollen.

- Erstelle einen Unterordner für jeden Empfänger** Dies Option lässt SmartPOP2Exchange die E-Mail in einen Unterordner mit der Empfänger-E-Mail-Adresse speichern.
- Lösche alte** Wählen Sie diese Funktion, um alte Backup E-Mail automatisch nach X Tagen löschen zu lassen.

- Alte E-Mail-Backup-Ordner Zippen** Wählen Sie diese Funktion, um alte Backup-Ordner automatisch Zippen zu lassen.
- Infizierte Nachrichten vom Backup ausschließen** Wenn diese Option ausgewählt ist, wird SmartPOP2Exchange Nachrichten, die vom Virenschanner als schädlich erkannt wurden, wieder aus dem Backup entfernen.
Diese Option ist ebenfalls in den Einstellungen [Antivirus](#) zu finden.

7.1.6 Log Einstellungen

Wenn Sie **Log Einstellungen** im [Navigationsbereich](#) auswählen, gelangen Sie zu diesem Formular.

Hier können Sie folgende Einstellungen vornehmen:

Wenn ein Fehler auftritt, sende ... Wählen Sie diese Option, damit SmartPOP2Exchange eine E-Mail mit der Fehlerbenachrichtigung an die unten angegebene Adresse schickt.

Absender-Adresse Geben Sie hier die E-Mail-Adresse ein, die als Absender in der E-Mail stehen soll.

Empfänger Geben Sie hier die E-Mail-Adresse ein, die die Nachricht empfangen soll.

Betreff Geben Sie hier den Betreff für die Fehlerbenachrichtigung an.


Server Geben Sie hier einen SMTP-Server ein, der die Nachricht übermitteln wird.

Port Geben Sie hier den Port des SMTP-Servers ein, Standard-Port ist 25.

Server benötigt Wählen Sie diese Option, falls der SMTP Server eine Authentifizierung benötigt.

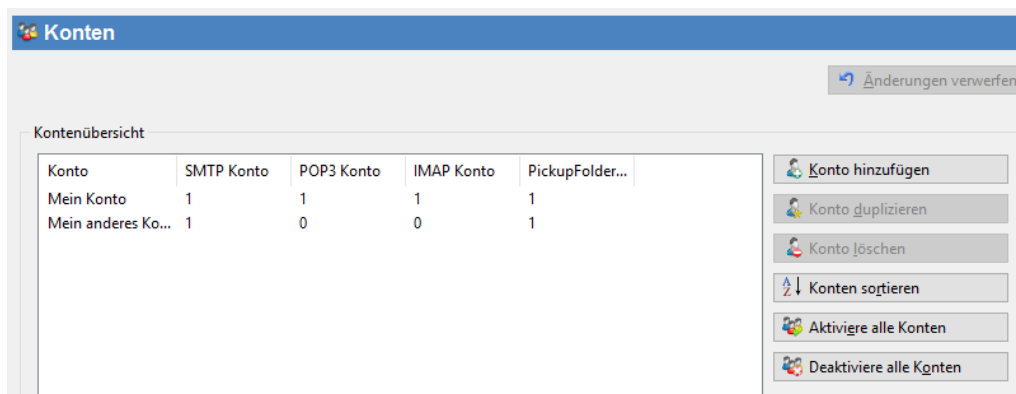
Benutzernam e	Geben Sie hier den Benutzernamen für den SMTP-Server ein.
Passwort	Geben Sie hier das Passwort für den SMTP-Server ein.
Einträge mit folgenden Wörtern ausschließen	Mit dieser Option können Sie die Fehlerbenachrichtigungen Filtern. Fehlermeldungen, die ein oder mehrere der angegebenen Wörter enthalten, werden nicht in der Fehlerbenachrichtigung aufgeführt.
Maximale Anzahl an Fehlermeldunge n	Hier können Sie die maximale Anzahl der Fehler angeben, die in einer Fehler-Benachrichtigung aufgeführt werden sollen.
Maximale Protokoll Größe	Legt die Maximale Größe des Protokolls fest.

Um Änderungen rückgängig zu machen, drücken Sie die Rückgängig-Schaltfläche.

 **Bitte beachten Sie, dass alle Änderungen nur nach dem ausdrücklichen Speichern der Einstellungen vom Dienst berücksichtigt werden.**

7.2 Konten

Wenn Sie **Konten** im [Navigationsbereich](#) auswählen, gelangen Sie zu diesem Formular.



Hier bekommen Sie eine Übersicht über alle Konten.

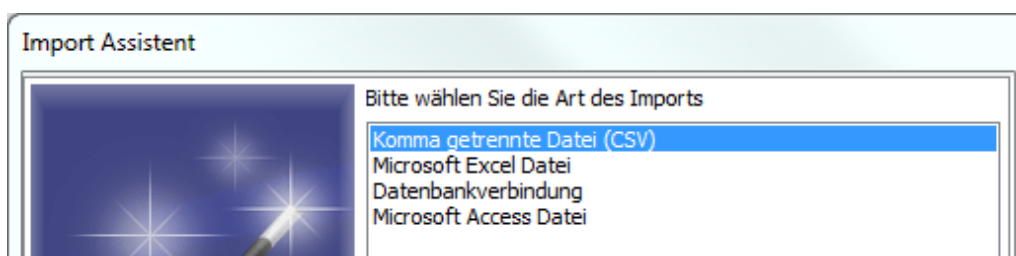
Sie können hier ebenfalls Konten hinzufügen, kopieren, löschen oder die Konten sortieren lassen.

Ist das Symbol eines Benutzerkontos mit einem roten Kreuz versehen, sind dessen Unterkonten (SMTP/POP3/IMAP) so deaktiviert, dass von diesem Konto keine E-Mails verarbeitet werden.

7.2.1 Import von POP3/IMAP Konto Daten

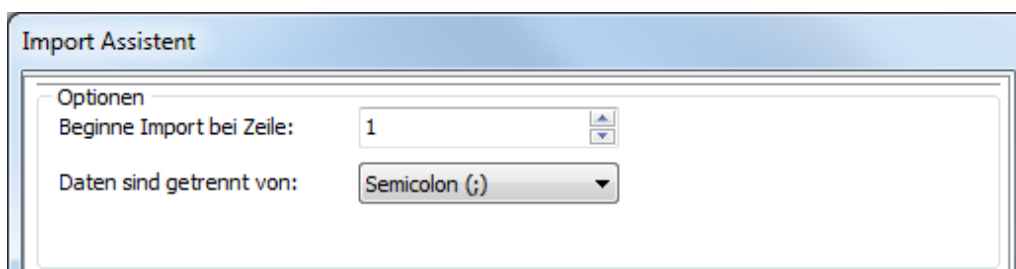
Wenn Sie **Importiere POP3 Kontendaten** im **Datei-Menü** auswählen, öffnen Sie den Import Assistent

Dort haben Sie die Wahl zwischen folgenden Datenquellen:



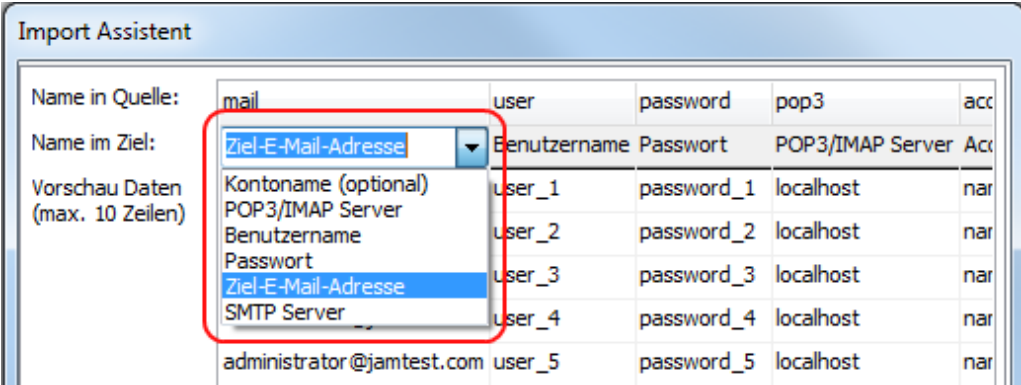
Danach folgt die Auswahl der Datei, die die Daten enthält.

Im Falle der "Komma getrennte Datei (CSV)" werden Sie nach der Auswahl der Datei aufgefordert, anzugeben, mit welchem Symbol die Werte getrennt sind.



Zum Schluss wählen Sie, welche Spalte aus der Quelle welches Attribut des Kontos darstellt.

Es sollte zumindest für jedes nicht-optionale Attribut des Kontos eine Spalte mit Daten existieren.



Die folgenden Daten werden für den Import eines Kontos benötigt (die Reihenfolge ist nicht wichtig):

Kontoname (optional) Name des Kontos innerhalb von SmartPOP2Exchange

POP3/IMAP Server Adresse des POP3/IMAP Server

Benutzername Benutzername des POP3/IMAP Kontos

Passwort Passwort des POP3/IMAP Kontos

Ziel-E-Mail-Adresse Ziel-E-Mail-Adresse in Ihrem Exchange Server

SMTP Server Adresse Ihres Exchange Server

Andere **optionale** Daten, die Importiert werden können:

Konto Gruppe Name der Konto Gruppe des Kontos

Port Port des POP3/IMAP Server

Sicherheitsmodus Sicherheitsmodus des POP3/IMAP Kontos (SSL / TLS / None)

SMTP Benutzername Benutzername Ihres Exchange Server Log-ins

SMTP Passwort Passwort Ihres Exchange Server Log-ins

SMTP Port Port Ihres Exchange Server

SMTP Sicherheitsmodus Sicherheitsmodus Ihres Exchange Server. (SSL / TLS / None)

7.2.2 Konto

Wenn Sie ein Konto im [Navigationsbereich](#) auswählen, gelangen Sie zu diesem Formular. Hier können Sie folgende Einstellungen vornehmen:


Kontoname Tragen Sie hier einen Namen für das aktuelle Konto ein.

Kontoregeln Hier sind alle Regeln des Kontos aufgelistet. Sie können Regeln aktivieren/deaktivieren, indem sie das Kontrollkästchen neben dem Namen anklicken. Sie können eine Regel auch durch Doppelklick bearbeiten.

Dieses Konto von globalen Regeln ausnehmen Wenn Sie diese Option wählen, werden die globalen Regeln nicht auf dieses Konto angewandt

-
- Regel** Diese Schaltfläche fügt dem Konto eine neue [Regel](#) hinzu.
- Regel** Mit dieser Schaltfläche können Sie die ausgewählte [Regel](#) bearbeiten.
- Regel** Mit dieser Schaltfläche können Sie die ausgewählte [Regel](#) in das aktuelle oder ein anderes Konto kopieren.
- Regel löschen** Mit dieser Schaltfläche können Sie die ausgewählte [Regel](#) löschen.
- Aufwärts** & Hier können Sie die Reihenfolge, in der die Regeln benutzt werden, verändern. Dabei ist die oberste Regel die zuerst Angewandte.

Um Änderungen rückgängig zu machen, drücken Sie die Rückgängig-Schaltfläche.

 **Bitte beachten Sie, dass alle Änderungen nur nach dem ausdrücklichen Speichern der Einstellungen vom Dienst berücksichtigt werden.**

7.2.3 SMTP

Wenn Sie ein SMTP-Konto im [Navigationsbereich](#) auswählen, gelangen Sie zu diesem Formular. Hier können Sie folgende Einstellungen vornehmen:



The screenshot shows the 'SMTP Server Einstellungen' form. It has a blue header bar with the title and a 'Änderungen verwerfen' button. The form is divided into two main sections. The first section, 'SMTP / Exchange Server (Zielserver)', contains three fields: 'E-Mail-Adresse (lokal):' with a dropdown menu showing 'intern@mailserver.de', 'SMTP/Exchange Server:' with a dropdown menu showing 'internSMTP', and 'Port:' with a numeric input field set to '465' and a note '(Standard: 25)'. The second section, 'Anmeldeinformationen', contains a checkbox 'Dieser Server benötigt Authentifizierung' which is checked, a 'Benutzername:' field with 'SMTP Nutzername', a 'Passwort:' field with 'SMTP Passwort', and a 'Sicherheits Modus:' dropdown menu set to 'SSL'. There is a 'Einstellungen testen' button in this section. At the bottom, there is a checkbox 'Konto aktiviert' which is also checked.

SMTP/Exchange Server (Empfänger Server)

E-Mail- Dieses Feld enthält die E-Mail-Adresse, an die SmartPOP2Exchange die Nachrichten vom POP3-/IMAP-Konto weiterleiten soll. (bzw. dessen Benutzernamen).

Für POP3/IMAP-Konten, die als Sammelkonten arbeiten, wird diese E-Mail-Adresse als "Fallback"-Adresse genutzt. In diesem Fall nutzt also SmartPOP2Exchange diese Adresse, wenn keine Empfänger-Adresse aus der E-Mail extrahiert werden kann oder der SMTP Server die extrahierte Adresse ablehnt.

Server Geben Sie hier den Namen des SMTP-Servers ein, auf dem das E-Mail-Konto liegt.

Port Geben Sie den Port des Servers ein.

Anmeldeinformationen

Benutzerna Geben Sie hier Ihren Benutzernamen für den SMTP-Server ein.


- Passwort** Geben Sie hier Ihr Passwort für den SMTP-Server ein.
- Sicherheits** Geben Sie hier das verwendete Sicherheitsprotokoll für den SMTP-Server ein.

Sonstiges

- Einstellung** Benutzen Sie diesen Knopf, um Ihre Einstellungen für dieses SMTP-Konto zu prüfen. SmartPOP2Exchange wird versuchen, eine Verbindung aufzubauen.

- Konto** Sie können hier das SMTP-Konto aktivieren bzw. deaktivieren.

Um Änderungen rückgängig zu machen, drücken Sie die Rückgängig-Schaltfläche.

 **Bitte beachten Sie, dass alle Änderungen nur nach dem ausdrücklichen Speichern der Einstellungen vom Dienst berücksichtigt werden.**

 **SmartPOP2Exchange unterstützt nur Login-Authentifizierung.**

7.2.4 POP3

Wenn Sie ein POP3-Konto im [Navigationsbereich](#) auswählen, gelangen Sie zu diesem Formular. Hier können Sie folgende Einstellungen vornehmen:

Allgemeine Einstellungen:

POP3-Server

- Nachrichten** Aktivieren Sie diese Option, um SmartPOP2Exchange das Arbeiten mit "catch all" Konten (Sammelkonten) zu ermöglichen. SmartPOP2Exchange durchsucht dann die Nachricht nach einer Zieladresse. Die E-Mail-Adresse in den SMTP Optionen wird als "Fallback"-Adresse genutzt. In diesem Fall nutzt SmartPOP2Exchange also jene Adresse, wenn keine Empfänger-Adresse aus der E-Mail extrahiert werden kann oder der SMTP Server die extrahierte Adresse ablehnt.

Server Geben Sie hier den Namen des POP3-Servers ein, von dem die Nachrichten herunter geladen werden sollen.

Port Geben Sie hier den Port für den POP3-Server ein.

Sammelkonto

Beforzugten Header-Eintrag editieren Hier können Sie einen Header angeben, der bei der Bestimmung des Empfängers beforzugt werden soll

Ausgeschlossene Header editieren Hier können Sie einen Header angeben, der bei der Bestimmung des Empfängers ignoriert werden soll

Gültige Domänen bearbeiten Editieren Sie hier die Liste der gültigen Domänen, an die zugestellt werden darf. Hier muss mindestens eine gültige Domäne drin stehen, damit das Sammelkonto richtig funktioniert.

Ausgeschlossene Empfänger editieren Editieren Sie hier die Liste der Empfänger-Adressen, an denen keine Zustellung stattfinden soll.

Anmeldeinformationen

Benutzername Geben Sie hier Ihren Benutzernamen für den POP3-Server ein. (Dieser ist oft gleich der E-Mail-Adresse auf dem Server.)

Passwort Geben Sie hier Ihr Passwort für den POP3-Server ein.

Sicherheits Geben Sie hier das verwendete Sicherheitsprotokoll für den POP3-Server ein.

Sonstiges

Verbindung Benutzen Sie diesen Knopf, um Ihre Einstellungen für dieses POP3-Konto zu prüfen. SmartPOP2Exchange wird versuchen, eine Verbindung aufzubauen.

Aktiviert Sie können hier das POP3-Konto aktivieren bzw. deaktivieren.

Experten-Einstellungen:

Individuelles Intervall und Timeout

Timeout Sie können hier ein individuelles Timeout für das POP3-Konto festlegen.

Standardwert Setzen Sie diese Option, um die allgemein gültige Timeout-Einstellung vom [Optionen-Formular](#) zu nutzen.

Intervall Sie können hier ein individuelles Intervall für das POP3-Konto festlegen in dem dieses von SmartPOP2Exchange bearbeitet werden soll.


Sammelkonto-Option

E-Mails für jeden Wenn Sie ein Sammelkonto verwenden und diese Option wählen, wird SmartPOP2Exchange eine E-Mail für jeden

Empfänger in TO: und CC: Empfänger in Ihrer Domäne replizieren. Verwenden Sie diese Option, falls Ihr Provider nicht für jeden Empfänger eine E-Mail im Sammelpostfach vorhält.


der Zieldomäne replizieren (für Sammelkonten)


Um Änderungen rückgängig zu machen, drücken Sie die Rückgängig-Schaltfläche.

 **Bitte beachten Sie, dass alle Änderungen nur nach dem ausdrücklichen Speichern der Einstellungen vom Dienst berücksichtigt werden.**

7.2.5 IMAP

Wenn Sie ein IMAP-Konto im [Navigationsbereich](#) auswählen, gelangen Sie zu diesem Formular. Hier können Sie folgende Einstellungen vornehmen:

 **IMAP Server Einstellungen**

 Änderungen verwerfen

Allgemeine Einstellungen Erweiterte Optionen

IMAP Server

☐
 Sende E-Mails an die im E-Mail-Header gefundene Adresse (Sammelkonto). Wenn Sie sich nicht sicher sind, ob Sie ein solches Konto verwenden, lassen Sie diese Option deaktiviert.

Wenn keine Empfängeradresse in der Nachricht gefunden wird, wird die E-Mail an die Adresse aus den SMTP Einstellungen gesendet.

Sie können zusätzlich konfigurieren, welcher Header zu der Bestimmung der E-Mail-Adresse

[Bevorzugten Header-Eintrag editieren](#) [Ausgeschlossene Header editieren](#)

[Gültige Domänen bearbeiten](#) [Ausgeschlossene Empfänger editieren](#)

Server (IMAP):

Port: (Standard: 143)


Mailbox:

Anmeldeinformationen


Benutzername:

Passwort:

Sicherheits Modus:

 Einstellungen testen

☒ Konto aktiviert

 Zeige E-Mails auf dem Server

Allgemeine Einstellungen

IMAP-Server

Sende E-Mails an die im E-Mail-Kopf gefundene Adresse (Sammelkonto) Aktivieren Sie diese Option, um SmartPOP2Exchange das Arbeiten mit "catch all" Konten (Sammelkonten) zu ermöglichen. SmartPOP2Exchange durchsucht dann die Nachricht nach einer Zieladresse. Die E-Mail-Adresse in den SMTP-Optionen wird als "Fallback"-Adresse genutzt. In diesem Fall nutzt SmartPOP2Exchange also jene Adresse, wenn keine Empfänger-Adresse aus der E-Mail extrahiert werden kann oder der SMTP Server die extrahierte Adresse ablehnt.

Server Geben Sie hier den Namen des IMAP-Servers ein, von dem die Nachrichten herunter geladen werden sollen.

Port Geben Sie hier den Port für den IMAP-Server ein.

Mailbox Geben Sie hier den Namen der IMAP Mailbox an, die von SmartPOP2Exchange abgefragt werden soll. (Standard: INBOX)

Sammelkonto

Beforzugten Header-Eintrag editieren Hier können Sie einen Header angeben, der bei der Bestimmung des Empfängers bevorzugt werden soll

Ausgeschlossene Header editieren Hier können Sie einen Header angeben, der bei der Bestimmung des Empfängers ignoriert werden soll

Gültige Domänen bearbeiten Editieren Sie hier die Liste der gültigen Domänen, an die zugestellt werden darf. Hier muss mindestens eine gültige Domäne drin stehen, damit das Sammelkonto richtig funktioniert.

Ausgeschlossene Empfänger editieren Editieren Sie hier die Liste der Empfänger-Adressen, an denen keine Zustellung stattfinden soll.

Anmeldeinformationen

Benutzernam Geben Sie hier Ihren Benutzernamen für den IMAP-Server ein. (Dieser ist oft gleich der E-Mail-Adresse auf dem Server)

Passwort Geben Sie hier Ihr Passwort für den IMAP-Server ein.

Sonstiges

Verbindung Benutzen Sie diesen Knopf, um Ihre Einstellungen für dieses IMAP-Konto zu prüfen. SmartPOP2Exchange wird versuchen, eine Verbindung aufzubauen.

Konto aktiviert Sie können hier das IMAP-Konto aktivieren bzw. deaktivieren.

Experten-Einstellungen:

Allgemeine Einstellungen
Erweiterte Optionen

Individueller Intervall und Timeout

Timeout: 299 ☒ Standardwert verwenden

Intervall: 180 Sekunden

☐ Als "gelesen" markierte Nachrichten herunterladen
☐ Nachrichten auf dem Server belassen
☐ Heruntergeladene Nachrichten als "gelesen" markieren

Lösche E-Mails, älter als 0 Tage (0 = nicht löschen)

☐ Verschiebe Nachrichten nach:

☐ E-Mails für jeden Empfänger in TO und CC der Zieldomäne replizieren (für Sammelkonten)

Den Verlauf der erfolgreich zugestellten E-Mails zurücksetzen

Zurücksetzen des OAuth2-Tokens für dieses Konto

Individuelles Intervall und Timeout

Timeout Sie können hier ein individuelles Timeout für das IMAP-Konto festlegen.

Standardwert Setzen Sie diese Option, um die allgemein gültige Timeout-Einstellung vom [Optionen-Formular](#) zu nutzen.

Intervall Sie können hier ein individuelles Intervall für das IMAP-Konto festlegen, in dem dieses von SmartPOP2Exchange bearbeitet werden soll.

Sonstiges

Als "gelesen" markierte Nachrichten herunterladen Wenn Sie diese Option wählen, wird SmartPOP2Exchange bereits als "gelesen" markierte Mails ebenfalls vom IMAP-Server herunterladen

Nachrichten auf dem Server belassen Hiermit können Sie SmartPOP2Exchange veranlassen, alle Mails auf dem IMAP-Server zu belassen. Die Mails werden somit nicht nach dem Download vom Server gelöscht.

Heruntergeladene Nachrichten als "gelesen" markieren Diese Option ist nur bei Verwendung von Sammelkonten verfügbar. Sie bewirkt, dass SmartPOP2Exchange heruntergeladene Mails auf dem IMAP-Server als "gelesen" markiert.

Lösche E-Mails, älter als... Tage Wenn Sie die Option **Nachrichten auf dem Server belassen** aktiviert haben, können Sie hier einstellen, wie lange E-Mails in Ihrem elektronischen Postfach verbleiben, bevor sie gelöscht werden. Wenn Sie diesen Wert auf "0" belassen, bleiben die Nachrichten auf ihrem Server und werden niemals gelöscht.

Verschiebe Nachrichten nach: Ermöglicht es, die E-Mails nach dem Verarbeiten auf dem IMAP-Server in Unterordner zu verschieben. Geben Sie den Namen des Unterordners an.

E-Mails für jeden Empfänger in TO und CC der Zieldomäne replizieren (für Sammelkonten) Wenn Sie ein Sammelkonto verwenden und diese Option wählen, wird SmartPOP2Exchange eine E-Mail für jeden Empfänger in Ihrer Domäne replizieren. Verwenden Sie diese Option, falls Ihr Provider nicht für jeden Empfänger eine E-Mail im Sammelpostfach vorhält.

Den Verlauf der erfolgreich Diese Schaltfläche setzt den Verlauf der zugestellten Mails zurück. Dies bewirkt, dass einmalig wieder alle auf IMAP-Server


Zurücksetze Setzt das OAuth2-Token des Kontos zurück.
n des
OAuth2-
Tokens für
dieses
Konto:

[illegible]

Markieren als "Zu Downloaden" / Kein Download Mit dieser Option wird die ausgewählte E-Mail bei der nächsten Verarbeitung des Kontos auf jeden Fall mit bearbeitet. Mit "Kein Download" deaktivieren Sie dies wieder. Wenn Sie die Option "Kein Download" auf eine E-Mail anwenden, die nicht schon einmal abgeholt wurde, funktioniert dies ähnlich wie ein Blockierung der E-Mail.

- Gelesen / Ungelesen** / Markiert eine E-Mail als gelesen bzw. ungelesen.
- Blockieren / Blockierung aufheben / Alle Blockierungen aufheben** / Hiermit können Sie E-Mails auf eine SmartPOP2Exchange interne Block-Liste setzen oder davon entfernen.
- Löschen / Löschen aufheben** / Markiert die selektierten E-Mails zum Löschen. Dies geschieht dann, wenn die Verbindung getrennt oder das Fenster geschlossen wird.
- E-Mail speichern** Ermöglicht es, die selektierten E-Mails als EML-Datei zu speichern.

Um Änderungen rückgängig zu machen, drücken Sie die Rückgängig-Schaltfläche.

 **Bitte beachten Sie, dass alle Änderungen nur nach dem ausdrücklichen Speichern der Einstellungen vom Dienst berücksichtigt werden.**

7.2.6 PickupFolder

Wenn Sie ein IMAP-Konto im [Navigationsbereich](#) auswählen, gelangen Sie zu diesem Formular. Hier können Sie folgende Einstellungen vornehmen:
(Nur in der Enterprise Version und Demo verfügbar)

Pickup Folder Einstellungen

Änderungen verwerfen

Pickup Folder

☐ **Sende E-Mails an die im E-Mail-Header gefundene Adresse. (Sammelkonto)**

Wenn keine Empfängeradresse in der Nachricht gefunden wird, wird die E-Mail an die Adresse aus den SMTP Einstellungen gesendet.

☐ E-Mails für jeden Empfänger in TO und CC der Zieldomäne replizieren (für Sammelkonten).

[Bevorzugten Header-Eintrag editieren](#) [Ausgeschlossene Header editieren](#)

[Gültige Domänen bearbeiten](#) [Ausgeschlossene Empfänger editieren](#)

Name:

Ordner:

Intervall: ☒ Standardwert verwenden

☐ Unterordner verarbeiten

☒ Konto aktiviert

Sende E-Mails an die im E-Mail-Kopf gefundene Adresse (Sammelkonto) Aktivieren Sie diese Option, um SmartPOP2Exchange das Arbeiten mit "catch all" Konten (Sammelkonten) zu ermöglichen. SmartPOP2Exchange durchsucht dann die Nachricht nach einer Zieladresse. Die E-Mail-Adresse in den SMTP-Optionen wird als "Fallback"-Adresse genutzt. In diesem Fall nutzt SmartPOP2Exchange also jene Adresse, wenn keine Empfänger-Adresse aus der E-Mail extrahiert werden kann oder der SMTP Server die extrahierte Adresse ablehnt.

E-Mails für jeden Empfänger in TO und CC der Zieldomäne replizieren (für Sammelkonten) Wenn Sie ein Sammelkonto verwenden und diese Option wählen, wird SmartPOP2Exchange eine E-Mail für jeden Empfänger in Ihrer Domäne replizieren. Verwenden Sie diese Option, falls Ihr Provider nicht für jeden Empfänger eine E-Mail im Sammelpostfach vorhält.

Name Hier geben Sie den Kontonamen für das PickupFolder-Konto an.

Folder Wählen Sie den Ordner, in dem SmartPOP2Exchange nach E-Mail Dateien suchen soll (*.eml*.txt)

Intervall Setzen Sie das Zeit-Intervall, nachdem SmartPOP2Exchange nach neuen E-Mail Dateien schauen soll.

Aktiviert Sie können hier das PickupFolder-Konto aktivieren bzw. deaktivieren.

Sammelkonto

Beforzugten Header-Eintrag editieren Hier können Sie einen Header angeben, der bei der Bestimmung des Empfängers bevorzugt werden soll

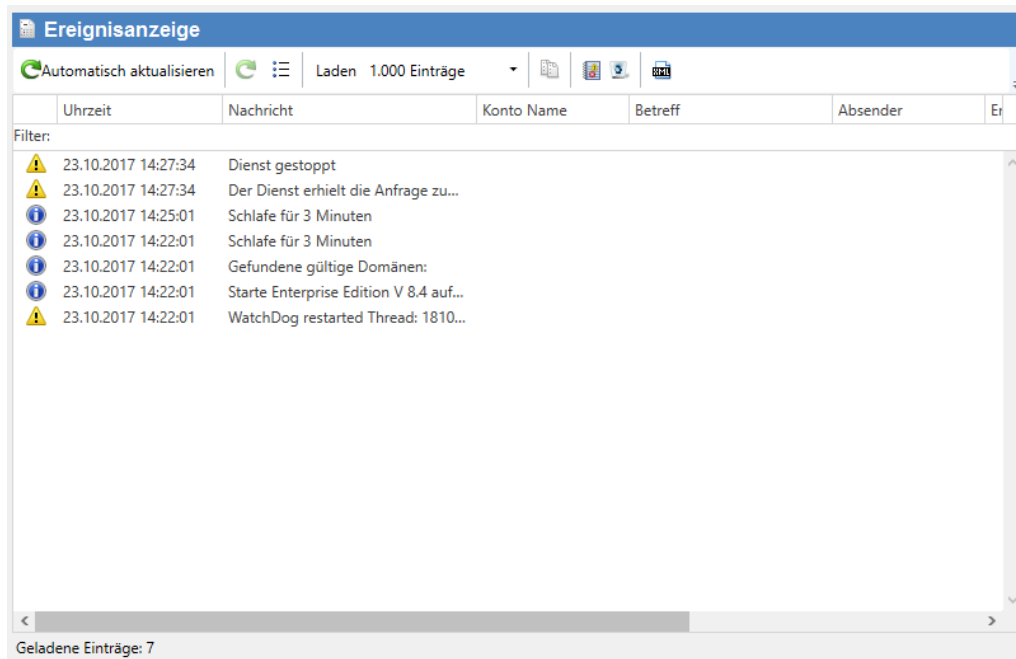
Ausgeschlossene Header editieren Hier können Sie einen Header angeben, der bei der Bestimmung des Empfängers ignoriert werden soll

Gültige Domänen bearbeiten Editieren Sie hier die Liste der gültigen Domänen, an die zugestellt werden darf. Hier muss mindestens eine gültige Domäne drin stehen, damit das Sammelkonto richtig funktioniert.

Ausgeschlossene Empfänger editieren Editieren Sie hier die Liste der Empfänger-Adressen, an die keine Zustellung stattfinden soll.

7.3 Ereignisanzeige

Wenn Sie **Ereignisanzeige** im [Navigationsbereich](#) auswählen, gelangen Sie zu diesem Formular. Hier können Sie folgende Einstellungen vornehmen:



Automatisch	Klicken Sie auf diese Schaltfläche, um die automatische Aktualisierung der Ereignisanzeige zu aktivieren oder deaktivieren.
Aktualisieren	Klicken Sie auf diese Schaltfläche, um die Ereignisanzeige zu aktualisieren.
Filter	Geben Sie hier einen Text, um die Ansicht nach Ereignisanzeige mit diesem Text in der ausgewählten Spalte zu filtern.
Filter anwenden	Wendet den Filter an oder entfernt diesen.
Öffne	Öffnet die Windows Ereignisanzeige MMC. Dort können Sie die Größe des Log einstellen und somit die Anzahl der vorgehaltenen Einträge beeinflussen.
Kopieren	Kopiert alle ausgewählten Einträge in die Zwischenablage.
Log löschen	Löscht alle Einträge. - Leert das log.
Laden X	Gibt an, wie viele Einträge geladen werden sollen.
Log als XML	Exportiert das aktuelle (gefilterte) Log in eine XML Datei.

8 Regeln

SmartPOP2Exchange erlaubt es Ihnen, Ihre Arbeit durch das Erstellen eigener Spam-Regeln erheblich zu vereinfachen. Durch diese Regeln ist es Ihnen möglich, Spam abzuwehren, Nachrichten mit bestimmten Eigenschaften direkt zu löschen oder an mehrere Personen weiterzugeben. In SmartPOP2Exchange bestehen alle Regeln aus einer oder mehreren Bedingung(en) und einer oder mehreren Aktion(en). Werden die Bedingungen von einer ankommenden Nachricht erfüllt, dann werden die mit ihr zusammenhängenden Aktionen ausgeführt.

Sie haben zwei Möglichkeiten, neue Regeln zu erstellen:

1. Wählen Sie "[Globale Regeln](#)" im [Navigationsbereich](#) und öffnen Sie den Regeldialog durch einen Klick auf die Schaltfläche "Regel hinzufügen". Dies wird eine globale Regel erstellen, welche auf alle Konten angewendet wird.
2. Wählen Sie ein Konto aus und drücken Sie den Knopf "Hinzufügen". Es wird sich dann ein Regel-Dialog öffnen, über den Sie alle nötigen Einstellungen vornehmen können.

Regeln ✕

1. Bitte geben Sie den Namen für die neue Regel an.

Spam

2. Welche Bedingungen sollen gelten?

☐ Alle Nachrichten
☐ Nachrichten mit [bestimmten Wörtern] im Betreff
☐ Nachrichten mit [bestimmten Wörtern] im Absender Feld (From)
☐ Nachrichten mit [bestimmten Wörtern] im Empfänger Feld (To)

3. Die Bedingungen verknüpfen mit: ☒ UND ☐ ODER

4. Was soll mit der Nachricht geschehen?

☒ Schreibe [bestimmten Text] an den Anfang des Betreffs
☐ Ersetze Absenderadresse durch [E-Mail Adresse]
☐ Ersetze [bestimmten Text] in der Nachricht.
☐ Ersetze [bestimmten Text] im E-Mail Header.
☐ Erstelle oder ersetze [Header-Feld].

5. Regelbeschreibung (klicken, um die Werte in zu ändern)

Als Spam erkannte Nachrichten (erforderliche Punktzahl: '45,0' [Klicken...
 Füge '*****SPAM*****' dem Anfang des Betreffs hinzu

☒ Aktiviert

Der Regel-Dialog ist in 5 Punkte aufgeteilt:


1. Der Name der Regel. Sie können hier jeden beliebigen Namen eingeben. Obwohl zwei unterschiedliche Regeln den gleichen Namen haben dürfen, ist aus Gründen der Übersichtlichkeit davon abzuraten. Der Name soll Ihnen lediglich eine Möglichkeit der schnellen Wiedererkennung bieten und wird vom Dienst nicht weiter benutzt.
2. Die Bedingungen wählen. Wählen Sie hier, welche Bedingungen eine Nachricht erfüllen soll, damit die Aktionen der Regel auf die Nachricht angewendet werden. Unsere [Bedingungen-Liste](#) zeigt Ihnen alle verfügbaren Bedingungen.
3. Verknüpfung der Bedingungen. Hier entscheiden Sie ob eine Nachricht *eine* (ODER) oder *alle* (UND) Bedingungen erfüllen muss, damit diese Regel angewendet wird.
4. Die Aktionen auswählen. Wählen Sie hier, welche Aktionen mit einer Nachricht durchgeführt werden sollen, wenn sie die

Bedingungen erfüllt. Unsere [Aktionen-Liste](#) zeigt Ihnen alle verfügbaren Aktionen.

5. Beschreibung der Regelemente. Hier sind alle von Ihnen ausgewählten Bedingungen und Aktionen aufgelistet - zuerst die Bedingungen, dann die Aktionen. Die Reihenfolge in der Liste bestimmt die Reihenfolge, in der die Bedingungen geprüft und die Aktionen ausgeführt werden. Außerdem können hier bei einigen Bedingungen bzw. Aktionen weitere Einstellungen vorgenommen werden. Durch einen Mausklick auf ein Element wird ein Eingabefenster geöffnet, über das die notwendigen Informationen eingegeben werden können, die dann die Regel vervollständigen.

Bestätigen Sie Ihre Eingabe durch einen Klick auf die Schaltfläche **Ok**, oder brechen Sie den Dialog ab, indem Sie die **Abbrechen**-Schaltfläche betätigen.

 **Bitte beachten Sie, dass die Aktionen der Regeln in derselben Reihenfolge ausgeführt werden, wie sie unter Punkt 5 aufgelistet sind.**

 **Bitte beachten Sie, dass alle Änderungen nur nach dem ausdrücklichen Speichern der Einstellungen vom Dienst berücksichtigt werden.**

8.1 Bedingungen

Bedingungen sind die Voraussetzungen, die eine Nachricht erfüllen muss, damit eine Regel angewandt wird. Es stehen Ihnen folgende Bedingungen zur Verfügung:

Alle Nachrichten

Diese Bedingung wird von jeder Nachricht erfüllt.

Nachrichten mit [bestimmten Wörtern] im Betreff

Eine Nachricht erfüllt diese Bedingung, wenn ihr Betreff (Subject) die von Ihnen bestimmten Wörter enthält.

Nachrichten mit [bestimmten Wörtern] im Absender-Feld (From)

Eine Nachricht erfüllt diese Bedingung, wenn ihr Von-Kopf (From:-Header) die von Ihnen bestimmten Wörter enthält.

Nachrichten mit [bestimmten Wörtern] im Empfänger-Feld (To)

Eine Nachricht erfüllt diese Bedingung, wenn ihr An-Kopf (To:-Header) die von Ihnen bestimmten Wörter enthält.

Nachrichten mit [bestimmten Wörtern] im Cc-Feld

Eine Nachricht erfüllt diese Bedingung, wenn ihr Cc-Kopf (Header) die von Ihnen bestimmten Wörter enthält.

Nachrichten mit einer Empfängeradresse mit Phrasen wie...

Eine Nachricht erfüllt diese Bedingung, wenn ihre SMTP Empfängeradresse die von Ihnen bestimmten Phrasen enthält.

Nachrichten mit [bestimmten Wörtern/Phrasen] im Header

Eine Nachricht erfüllt diese Bedingung, wenn ihr Header (Internetkopfzeilen) die von Ihnen bestimmten Wörter enthält.

Nachrichten mit [bestimmten Wörtern] im Inhalt (Body)

Eine Nachricht erfüllt diese Bedingung, wenn ihr Inhalt (Body) die von Ihnen bestimmten Wörter enthält.

Nachrichten ohne Betreff

Eine Nachricht erfüllt diese Bedingung, wenn ihr Betreff (Subject) leer ist.

Nachrichten, die einen Virus enthalten

Eine Nachricht erfüllt diese Bedingung, wenn ClamAV oder ihr installierter [Virens Scanner](#) einen Virus in einem E-Mail-Anhang erkennt.

([Hier](#) gibt es weitere Informationen)

Nachrichten, die als Spam erkannt wurden

Eine Nachricht erfüllt diese Bedingung, wenn [SpamAssassin](#) ihr einen Wert zuweist, der über dem von Ihnen bestimmten Schwellenwert liegt.

([Hier](#) gibt es weitere Informationen)

Nachrichten, die größer als ein [bestimmter Wert] sind

Eine Nachricht erfüllt diese Bedingung, wenn sie eine von Ihnen bestimmte Größe überschreitet.


Nachrichten mit [Anhang]


Eine Nachricht erfüllt diese Bedingung, wenn sie mindestens einen Anhang (Attachment) besitzt. Es ist möglich eine Maske für spezielle Anhänge anzugeben (z.B. *.mp3).

Die angegebene Maske gilt bei entsprechend gewählter Option auch für Dateien in zip-Archiven.

Nachricht hat einen Anhang größer als [angegeben]

Eine Nachricht erfüllt diese Bedingung, wenn sie mindestens einen Anhang (Attachment) besitzt, der die von Ihnen bestimmte Größe überschreitet.

 **Alle Bedingungen berücksichtigen nicht die Groß- und Kleinschreibung (z.B. 'JAM-Software' und 'jam-software' werden gleich behandelt)**

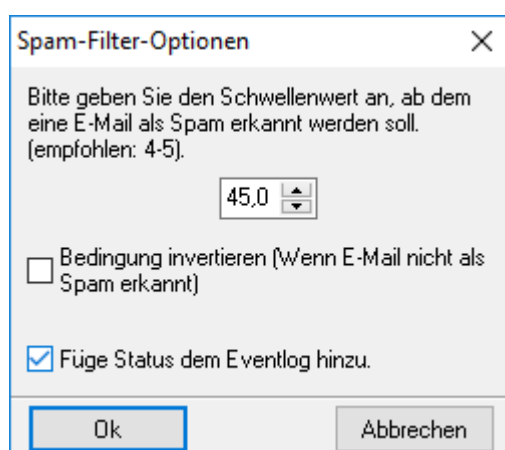
 **Alle Bedingungen, die nach bestimmten Wörtern/Phrasen suchen, können auch als regulärer Ausdruck konfiguriert werden.**

8.2 Die Spam-Bedingung

SmartPOP2Exchange benutzt [SpamAssassin](#) als Spamfilter, um unerwünschte Spam-E-Mails zu erkennen.

Um die Spam-Erkennung einzuschalten, müssen Sie eine Regel erstellen, die eine *SpamCondition* als Bedingung enthält. Mit Hilfe der Aktionen, die Sie für die Regel festlegen, bestimmen Sie dann, was mit der Spam-E-Mail geschehen soll.


([Hier](#) erfahren Sie mehr über das Einrichten von Regeln)




Einige Einstellungen des Spam-Filters lassen sich über die Anwendung einstellen.

Schwelldwert Der Schwellenwert (zwischen 0 und 100) bestimmt, welche Nachrichten als Spam gelten sollen. Dafür wird der Schwellenwert mit dem Wert von SpamAssassin verglichen. Ist der Wert größer als der Schwellenwert, wird die Nachricht als Spam behandelt. (SmartPOP2Exchange multipliziert den Wert von SpamAssassin mit 10, um auf eine sinnvolle Skala von 0 bis 100 zu kommen).

Statusbericht Hier können Sie festlegen, ob SmartPOP2Exchange einen Statusbericht in die Ereignisanzeige schreiben soll. Der Statusbericht besteht aus dem Wert, den SpamAssassin für die Nachricht ermittelt hat, und einer Liste aller erfolgreichen Tests.

 ***Es wird nicht empfohlen, Spam-Nachrichten automatisch löschen zu lassen, da dabei die Gefahr besteht, dass auch erwünschte Nachrichten gelöscht werden. Es kann durchaus vorkommen, dass erwünschte Nachrichten (auch 'Ham' genannt) fälschlicherweise als Spam erkannt werden.***

Sie sollten als Spam erkannte E-Mails mit einem Text wie [SPAM] im Betreff markieren lassen und diese dann im E-Mail-Programm (Outlook) über eine Regel aussortieren, wenn der Betreff diesen Text enthält.

 ***Es macht auch Sinn, mehrere Regeln zum Filtern von Spam für ein Konto zu erstellen. So können E-Mails, die einen hohen Schwellenwert überschreiten, direkt gelöscht werden, während E-Mails, die nur einen niedrigen Schwellenwert erreichen, nur markiert werden.***

 **Nutzen Sie die "Trainiere Bayes" Aktion nicht zusammen mit dieser Bedingung, da es keinen Sinn macht, den Bayes mit Mails zu trainieren, die ohnehin schon korrekt erkannt werden. (Dies macht SpamAssassin automatisch)**

Für ein Beispiel zur Verwendung der "Trainiere Bayes" Aktion sehen bitte unter [Spam-Filter](#) nach.

8.3 Aktionen

Aktionen geben an, was mit Nachrichten geschehen soll. Es stehen Ihnen folgende Aktionen zur Verfügung:

Schreibe einen [bestimmten] Text an den Anfang des Betreffs

Nachrichten werden mit einem neuen Text am Anfang des Betreffs weitergeleitet.

Ersetze Absenderadresse durch [E-Mail Adresse]

Die aktuelle (POP3) E-Mail-Adresse wird als neuer Absender benutzt. Sie können "\$HeaderValue(X-Some-HeaderEntry)\$" (ohne Anführungszeichen) verwenden, um einen Wert eines Header Eintrages zu verwenden.

Ersetze [bestimmten Text] in der Nachricht

Ersetzt einen beliebigen Text in der Nachricht durch einen anderen.

Ersetze [bestimmten Text] im E-Mail Header

Ersetzt einen beliebigen Text im E-Mail Header durch einen anderen.

Erstelle oder ersetze [Header-Feld]

Erstellt ein Header-Feld mit von Ihnen festgelegtem Namen und Wert. Besteht bereits ein Feld mit dem Namen, so wird dieses mit Ihren Angaben ersetzt.

Ersetze [bestimmten Text] im Betreff

Ersetzt einen beliebigen Text im E-Mail Betreff durch einen anderen.

Setze Priorität auf [bestimmten Wert]

Nachrichten wird eine neue Priorität zugewiesen.

Kopie weiterleiten an [Empfänger]

Eine Kopie der Nachricht wird an die angegebenen E-Mail-Adressen geschickt. Wird die entsprechende Option abgewählt, wird die Nachricht an den ursprünglichen Empfänger nicht mehr zugestellt (Umleitung).

Sende eine Kopie an [einen bestimmten Server]

Eine Kopie der Nachricht wird an den angegebenen SMTP-Server geschickt. Benötigt dieser eine Authentifizierung, ist diese ebenfalls anzugeben.

Sende folgende autom. Antwort an den Absender: [Text]

Sie können dem Verfasser der E-Mail eine Antwortnachricht senden. [Achtung hier muss Ihr lokaler SMTP/Exchange Server so konfiguriert sein, dass SmartPOP2Exchange über diesen relayen darf.](#)

Speichere E-Mail unter [gewähltem Pfad]

Dies speichert die E-Mail unter dem angegebenen Pfad als *EML-Datei im MIME-Format.

Speichere Anhänge unter [gewähltem Pfad]

Dies speichert die Anhänge einer E-Mail unter dem angegebenen Pfad. Die Aktion ermöglicht es ebenfalls, automatisch ein Verzeichnis für jeden Absender oder Empfänger zu erstellen.

Trainiere Bayes mit Nachricht als [Spam/Ham]

Benutzen Sie diese Aktion für Konten, mit denen Sie den [Bayes-Filter automatisch trainieren](#) wollten, oder für ein [Honeypot-Konto](#).

Beachten Sie, dass die Nachrichten standardmäßig nach dem Trainieren nicht zugestellt (gelöscht) werden.

Es macht keinen Sinn, diese Aktion zusammen mit einer Spam-[Bedingung](#) zu verwenden. Diese Aktion ist nur für nicht korrekt erkannten Spam gedacht.

Für ein Beispiel zur Verwendung der "Trainiere Bayes" Aktion sehen bitte unter [Spam-Filter](#) nach.

Füge Absender der Black-/Whitelist hinzu

Fügt alle Absender Adressen zur Auto-Blacklist oder zur Auto-Whitelist hinzu. (Die Auto-Listen sind separate Listen. Einträge auf diesen Listen sind nicht in den Listen der Spam-Einstellungen zu sehen.)

[Datei] ausführen

Diese Aktion führt eine ausgewählte Datei aus. Diese Datei darf keine Benutzerinteraktion fordern oder eine grafische Benutzeroberfläche (GUI) zeigen. GUI's werden nicht angezeigt.

Der Pfad zur E-Mail wird immer als erster Parameter übergeben und der SMTP Empfänger als zweiter Parameter.

Der Pfad zur E-Mail ist entweder der Pfad zum letzten Speicherort der E-Mail, sofern diese zuvor von SmartPOP2Exchange gespeichert wurde. (Per Backup Einstellung oder per Regel) Ansonsten ist es der Pfad zu einer temporär erstellten Datei.

Versende ohne Anhang

Es werden alle Anhänge der Nachricht gelöscht.

Versende ohne bestimmte Anhänge

Es werden alle Anhänge der Nachricht gelöscht, deren Name eines der Schlüsselwörter enthält.

Versende folgende autom. Antwort an den Absender: [Text]

Der von Ihnen vorgegebene Text wird automatisch als Antwort an den Absender geschickt.

Entpacke Zip Archive in Nachricht

Entpackt alle ZIP-Archive in der Nachricht. Die Dateien des ZIP-Archives sind danach "normale" Anhänge.

Keine weiteren Regeln anwenden

Verhindert, dass nach der aktuellen Regel noch weitere auf die Nachricht angewandt werden.

Nachricht nicht zustellen

Diese Aktion sollte die letzte einer Regel sein. Weitere Aktionen oder Regeln nach dieser zu nutzen macht keinen Sinn, denn die Nachricht wird vom Server gelöscht, ohne zugestellt zu werden.

E-Mail aus Backup löschen

Diese Aktion löscht die E-Mail aus dem Backup.

Header bereinigen

Diese Aktion sollte vor allen anderen Aktionen sein, die Veränderungen auf dem Header ausführen. Diese Aktion "bereinigt" den Header von E-Mails, die von Office 365 verschickt wurden. Dabei ersetzt die Aktion alle fehlerhaften Name-Wert-Trennzeichen im Header.

Setze SCL Wert

Diese Aktion setzt den Spam Confidence Level (SCL)-Wert der E-Mail für Microsoft Exchange. Standardmäßig wird die E-Mail ab einem Level von 5 als Spam klassifiziert.

 **Bitte beachten Sie, dass die Aktionen der Regeln in derselben Reihenfolge ausgeführt werden, wie sie unter Punkt 5 aufgelistet sind.**

 **Bitte beachten Sie, dass die "Nachrichten nicht zustellen"-Aktion die letzte Aktion in der letzten Regel sein sollte. SmartPOP2Exchange ist es**

nicht möglich weitere Aktionen anzuwenden, wenn diese Aktion ausgeführt wurde.

8.4 Beispiele

Alle Beispiele haben folgende Voraussetzungen:

- das Konto heißt "Test-Konto"
- die SMTP Einstellungen sind:
 - E-Mail: "Mails@example.com"
 - Server: "www.example.com"
- die POP3-/IMAP-Einstellungen sind:
 - Server: "www.externaldomain.com"
 - Benutzername: "test@externaldomain.com"

Regel 1: Diese Regel überprüft das Absender-Feld. Wenn diese den Text "Info@Jam" enthält, sollen die E-Mail an "Peter@example.com" weitergeleitet, der Betreff abgeändert und die Nachricht an den ursprünglichen Empfänger "Mails@example.com" zugestellt werden.

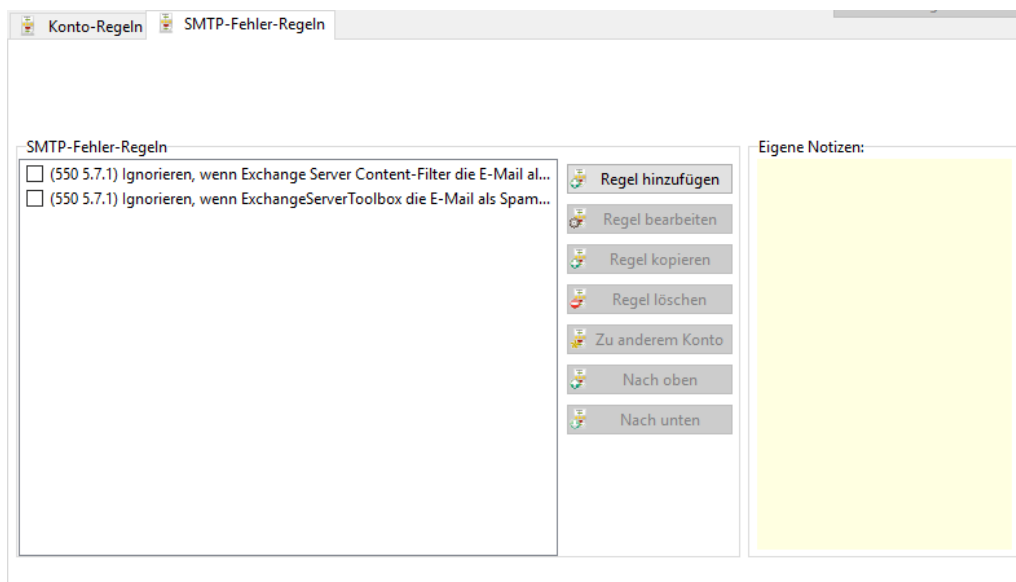
1. Benennen Sie die Regel "Weiterleiten und Markieren";
2. Wählen Sie "Nachrichten mit [bestimmten Wörtern] im Absender-Feld (From)" unter den Bedingungen aus;
3. Wählen Sie "Versende an [bestimmten] Empfänger" unter den Aktionen aus;
4. Wählen Sie "Schreibe einen [bestimmten] Text an den Anfang des Betreffs" unter den Aktionen aus;
5. Belassen Sie "Bedingungen sind verknüpft mit:" bei "UND";
6. Klicken Sie auf "Nachrichten mit "" im Absender Feld (From)" und geben Sie "Info@Jam" ein;
7. Klicken Sie auf "Versende an "" " und geben Sie "Peter@example.com" ein, dann wählen Sie die Option "Sende Kopie an SMTP-Konto-Adresse";
8. Klicken Sie auf "Schreibe "" an den Anfang des Betreffs" und geben Sie "InfoMail" ein;
9. Klicken Sie auf OK.

Regel 2: Diese Regel überprüft E-Mails auf Anhänge und löscht die E-Mail gegebenenfalls.

1. Benennen Sie die Regel "Lösche Mail mit Anhängen"
2. Wählen Sie "Nachrichten mit einem Anhang" unter den Bedingungen aus.
3. Wählen Sie "Nachricht nicht zustellen" unter den Aktionen aus.
4. Belassen Sie "Bedingungen sind verknüpft mit:" bei "UND".
8. Klicken Sie auf OK.

8.5 SMTP Fehler Regeln

Ähnlich wie bei den normalen Mail-Regeln können im SmartPOP2Exchange Regeln angelegt werden, die auf Fehlermeldungen des SMTP Servers während der Übertragung reagieren.



Spezielle Bedingungen:

Ein Fehler

Eine Nachricht erfüllt diese Bedingung, sobald ein Fehler auftritt.

Fehlermeldung enthält [bestimmte Wörter]

Eine Nachricht erfüllt diese Bedingung, wenn die erhaltene Fehlermeldung die von Ihnen bestimmten Wörter enthält.

Fehlercode stimmt mit [bestimmter Nummer] überein

Eine Nachricht erfüllt diese Bedingung, wenn der Code der erhaltenen Fehlermeldung mit der von Ihnen bestimmte Nummer übereinstimmt.

Spezielle Aktionen:

Einen [bestimmten Text] in die Ereignisanzeige schreiben

Dies schreibt den von Ihnen bestimmten Text in die Ereignisanzeige. Wenn kein eigener Text bestimmt wird, wird eine Standardnachricht, abhängig von der Fehlermeldung, in die Ereignisanzeige geschrieben.

Keine Fehlermeldung in die Ereignisanzeige schreiben

Es wird keine Fehlermeldung in die Ereignisanzeige geschrieben.

E-Mail nicht zustellen

Dies markiert die E-Mail zur Löschung, damit nicht nochmal versucht wird, sie zuzustellen.

9 Spam Filter (SpamAssassin)

Über SpamAssassin

SpamAssassin ist ein leistungsfähiger, modular aufgebauter E-Mail-Filter, der eine Vielzahl von Mechanismen wie Textanalysen, Bayes Filter, DNS-Anfragen und kollaborative Filterdatenbanken zur Erkennung von Spam-Mails verwendet. SpamAssassin ist ein Projekt der [Apache Software Foundation \(ASF\)](https://www.apache.org/) und unterliegt dessen Lizenz-Bedingungen.

SmartPOP2Exchange benutzt eine eigens von JAM Software für Windows portierte Variante des Spamfilters: [SpamAssassin in a Box](https://www.jam-software.com/spamassassin-in-a-box/). Die Portierung installiert den Spamfilter als eigenständigen Windows-Dienst, um ihn für die Spamfilterung von SmartPOP2Exchange verwendbar zu machen.

Mehr Informationen zu SpamAssassin finden Sie unter <https://www.spamassassin.org/>.

Was kann SpamAssassin?

Jedes der in SpamAssassin enthaltenen Module gibt eine Punktzahl beim Untersuchen einer E-Mail zurück. Die Summe aller Punkte der Module ergeben schließlich den "Spam-Score". Je höher diese Punktzahl, desto wahrscheinlicher ist es, dass es sich bei der untersuchten E-Mail um Spam handelt. Die Module zur Bewertung stützen sich auf unterschiedliche Methoden. Die wichtigsten Methoden sind hier aufgelistet:

- Test des E-Mail-Kopfes, wie zum Beispiel Stellen von Anfragen an die Server, über welche die E-Mail angeblich weitergeleitet wurde, um herauszufinden, ob diese wirklich existieren.
- Statische Tests: meist lexikalische Untersuchungen auf den E-Mail-Kopf und -Rumpf bis hin zur Untersuchung kompletter Phrasen des Inhalts.
- Analyse von Zeichensätzen im Zusammenhang mit lokalisierter Benutzung.
- Abfrage sogenannter RBLs (Realtime Blackhole Lists): IP-Adressen bekannter Spam-Versender werden auf diesen Servern veröffentlicht. SpamAssassin vergleicht die IP-Adressen eingehender E-Mails mit den auf den Listen veröffentlichten, bekannten Spammer-Adressen.
- Benutzung von Prüfsummen-basierten, verteilten Filternetzwerken (Razor): Hashwerte von bekannten Spam-E-Mails werden auf einem zentralen Server

gespeichert. Der Hashwert einer eingehenden E-Mail wird mit den Werten auf diesem Server verglichen.

- Abfrage von URL-Blacklists: Untersuchung, ob URLs innerhalb von E-Mails auf Internetseiten verweisen, die schon als Werbeziel von Spam-E-Mails erkannt wurden.
- Automatisches "Whitelisting": Aufnehmen von Absender-E-Mail-Adressen auf die Whitelist, falls die Gesamtpunktzahl einen bestimmten Wert nicht erreicht hat.
- Nutzung eines Bayes Filters: Ein Filter, der mit Hilfe von komplexen statistischen Algorithmen die Nachrichten bewertet.

Einige dieser Methoden erzeugen negative Punktwerte, wie zum Beispiel die Whitelist. Deshalb erzielen die meisten erwünschten E-Mails oftmals eine negative Gesamtpunktzahl.

Alle Methoden, auch als Regeln bezeichnet, stehen SpamAssassin in Form von Textdateien zur Verfügung. So ist es auf einfache Weise möglich, eigene Regelsammlungen in zusätzlichen Dateien hinzuzufügen. Die Regel-Dateien werden vom SpamAssassin-Dienst selbstständig aktualisiert, um jederzeit eine möglichst effektive Spamfilterung zu garantieren.

Ob eine E-Mail als Spam eingestuft wird, entscheidet letztendlich der Benutzer selbst. In den Spam-Regeln von SmartPOP2Exchange kann man unter anderem den "required score" angeben; der Schwellwert, ab dem eine E-Mail als Spam klassifiziert wird. Das Ergebnis einer untersuchten Nachricht ist im Kopf der E-Mail wiederzufinden.

Was ist ein Bayes Filter (und warum sollte es mich interessieren)?

Ein Bayes Filter ist ein statistischer Filter, der Spam aufgrund statistisch häufig wiederkehrender Merkmale identifiziert. Das heißt ein Bayes Filter zerlegt Nachrichten in diverse einzelne Bestandteile und prüft, wie häufig welches Einzelteil in welcher Form in Spam oder in kein Spam auftaucht und legt dann eine Bewertungsskala fest, die mit jeder angebotenen und analysierten Spam-Nachricht / kein Spam-Nachricht genauer definiert wird. Je mehr eine gegebene Nachricht dem bisher erhobenen Merkmalsprofil für Spam oder kein Spam entspricht, desto eher wird sie in die entsprechende Kategorie eingereiht.

Deshalb ist es auch unabdingbar, dass ein Bayes Filter entsprechend trainiert werden muss, um gute Dienste zu leisten. Ein statistischer Filter kann nur dann "gut" trainiert werden, wenn man ihm die Möglichkeit gibt, Erwünschtes als Erwünschtes und Unerwünschtes als Unerwünschtes kennen zu lernen. Das heißt es muss dem Filter nicht nur beigebracht werden, was Spam ist, sondern auch, was kein Spam ist. Dem Filter nur Spam-Nachrichten als Trainingsmaterial anzubieten verfehlt dabei dieses Ziel, weil es verhindert, dass der Filter neben unerwünschter auch die erwünschten Eigenschaften einer E-Mail kennenlernt.

Richtig trainiert kann ein Bayes Filter ein wertvolles Mittel zur Spam-Erkennung sein. Je kleiner die Masse an E-Mails, desto weniger Vorteile kann der Bayes

Filter bieten, allein weil ihm nicht genügend Trainingsmaterial zur Verfügung steht. Wir empfehlen deshalb, den mitgelieferten und vortrainierten Bayes Filter zu verwenden, den die SpamAssassin-Version von SmartPOP2Exchange nutzt.

Was kann man tun, um die Effizienz des Filters zu erhöhen?

Schwellenwert erniedrigen:

Eine einfache Möglichkeit zur Erhöhung der Filter-Rate ist die Anpassung des Spam-Schwellenwertes. Hierdurch wird strenggenommen allerdings nicht die Effektivität des Filters erhöht, stattdessen kann hierdurch erreicht werden, dass eine E-Mail bereits bei geringerer Spam-Punktzahl als Spam markiert wird. Die Funktion sollte daher mit Bedacht verwendet werden, da möglicherweise erwünschte E-Mails als Spam markiert werden könnten.

Bayes Filter trainieren

Falls SpamAssassin eine E-Mail falsch klassifiziert, können Sie den Spamfilter mit dieser E-Mail trainieren. Dazu sammeln Sie Spam- und kein Spam-E-Mails im MIME-Format in einem Ordner und lassen den Bayes Filter diese dann manuell über die Schaltflächen **"Spam trainieren"** bzw. **"Kein Spam trainieren"** lernen. Da der Bayes Filter mit eingeschalteter "autolearn" Funktion schon alle Nachrichten mit einer Punktzahl von über 120 als Spam und unter 0 als kein Spam qualifiziert, ist dies vor allem für nicht erkannten Spam wichtig. Der Bayes Filter arbeitet mit Wörtern, Phrasen und Strukturen, die in Spam-/kein Spam-E-Mails immer wieder auftreten. Daher kann er von erkanntem Spam fast genau soviel lernen wie von nicht erkanntem Spam (bzw. kein Spam).

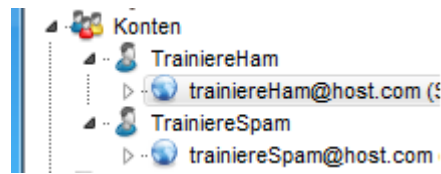
Regeln hinzufügen

SpamAssassin verwendet eine Reihe von Dateien mit Anti-Spam-Regeln (meist in Form von regulären Ausdrücken). Diese Dateien befinden sich in den Ordnern "share" und "etc" im Installationsordner des Spamfilters und werden bei aktivierter Spamfilterung von SmartPOP2Exchange automatisch genutzt. Die Regeln im "share" Ordner sollten nicht verändert werden, da sie beim automatischen Update der Filter-Regeln ersetzt werden. Im "etc" Ordner dagegen können eigene Regel-Dateien erstellt werden. Mehr Informationen zum Erstellen eigener Regeln finden Sie unter der folgenden Adresse: <https://cwiki.apache.org/confluence/display/SPAMASSASSIN/WritingRules> (englischsprachig).

9.1 Bayes Filter mit POP3 Konten trainieren

Es ist möglich, den Bayes-Filter über E-Mails an bestimmte POP3-Konten und Anwenden von Regeln zu trainieren.

Dazu werden zwei zusätzliche POP3-Konten erforderlich, wie im folgenden Bild zu sehen ist:



Ein Konto um als "Ham" und eines um als "Spam" zu trainieren. Sie können die Konten benennen, wie Sie wollen, aber für eine bessere Benutzbarkeit sollten die Namen verständlich sein. Dasselbe zählt für die Mail Adresse, die zum jeweiligen Konto gehört.

Jedes der Konten sollte wie in der folgenden Abbildung konfiguriert werden.



Eine SMTP-Server-Adresse ist nicht erforderlich, da Sie von diesen Konten keine E-Mails weiterleiten werden.

Nun müssen Sie für jedes der beiden Konten eine Regel erstellen, welche dafür sorgt, dass alle E-Mails, die an eins dieser Konten geschickt werden, benutzt werden, um den Bayes-Filter entweder als "Ham" oder als "Spam" zu trainieren.

Ein Beispiel ist im folgenden Bild zu sehen.

Regeln

1. Bitte geben Sie den Namen für die neue Regel an.
Trainiere Spam

2. Welche Bedingungen sollen gelten?

- ☒ Alle Nachrichten
- ☐ Nachrichten mit [bestimmten Wörtern] im Betreff
- ☐ Nachrichten mit [bestimmten Wörtern] im Absender Feld (From)
- ☐ Nachrichten mit [bestimmten Wörtern] im Empfänger Feld (To)

3. Die Bedingungen verknüpfen mit: ☒ UND ☐ ODER

4. Was soll mit der Nachricht geschehen?

- ☐ Kopie weiterleiten an [Empfänger]
- ☐ Sende eine Kopie an [einen bestimmten Server]
- ☐ Speichere E-Mail unter [gewähltem Pfad]
- ☐ Speichere Anhänge unter [gewähltem Pfad]
- ☒ Trainiere Bayes mit Nachricht als [Spam/Ham]

5. Regelbeschreibung (klicken, um die Werte in zu ändern)

Alle Nachrichten
Trainiere Bayes mit Nachricht als [Spam]

☒ Aktiviert

Ok Abbrechen

Wenn Sie einen existierenden SMTP Server verwenden, müssen Sie zusätzlich die "Nachricht nicht zustellen"-Aktion aktivieren.

10 Antivirus Software

Mit SmartPOP2Exchange können Sie eingehende Nachrichten durch den integrierten ClamAV oder einen von Ihnen installierten Virens Scanner testen lassen.

ClamAV

Der integrierte Virens Scanner ist die Windows-Version von [ClamAV](https://www.clamwin.com): ClamWin (<https://www.clamwin.com>)

"Clam AntiVirus ist ein Antivirus-Toolkit für Unix das unter der GPL Lizenz steht. Es wurde speziell für das Scannen von E-Mails auf Mailgateways design. [...] Das Herzstück des Paketes ist eine Antivirus-Einheit in Form einer gemeinsam genutzten Bibliothek.

Hier ist eine Liste mit den wichtigsten Funktionen:

* ...

* Komplexes Update-Programm für die Datenbank mit Unterstützung für scripted Updates und digitale Signaturen

* Virus Scanner Bibliothek in C

* Mehrmals tägliche Updates der Virusdatenbank (siehe Homepage für die gesamte Anzahl von Signaturen)

* Eingebaute Unterstützung für verschieden Archiv-Formate wie Zip, RAR, Tar, Gzip, Bzip2, OLE2, Cabinet, CHM, BinHex, SIS und andere

* Eingebaute Unterstützung für nahezu alle Mail Dateien Formate

* Eingebaute Unterstützung für ELF executables und Portable Executable Dateien komprimiert mit UPX, FSG, Petite, NsPack, wwpack32, MEW, Upack und verschleiert mit SUE, Y0da Cryptor und anderen

* Eingebaute Unterstützung für populäre Dokumentenformate wie MS Office und MacOffice Dateien, HTML, RTF und PDF

(Quelle: <https://www.clamav.net/>)

Installierte Antivirus-Software

Mit der SmartPOP2Exchange können Sie eingehende Nachrichten durch den von Ihnen installierten Virens scanner testen lassen. Wird ein Virus gefunden, wird die Nachricht automatisch gelöscht. Das genaue Verhalten wird dabei jedoch von Ihrem Virens scanner bestimmt. Die SmartPOP2Exchange arbeitet mit einer Reihe von Antivirus-Software zusammen und versucht so elegant wie möglich deren Vorteile zu nutzen.

Allgemeine Einstellungen für jeden Virens scanner, den Sie mit der SmartPOP2Exchange benutzen möchten sind:

- Wenn ein Virus gefunden wird (Dateien und Archive), darf keine Benutzerinteraktion (Nachfragen) verlangt werden. Wählen Sie "Datei löschen" oder "Datei umbenennen/verschieben".
- Deaktivieren Sie jedes Scannen von POP3-/IMAP- und SMTP-Protokollen. Diese Option wird zumeist als "Scannen von eingehenden/ausgehenden E-Mails" beschrieben.

Wählen Sie bitte Ihren Virens scanner aus folgender Liste aus, um weitere Informationen zu erhalten.

- [GData](#)
- [BitDefender](#)
- [Kaspersky](#)
- [Sophos](#)

G Data

Achtung: Es ist notwendig, dass die E-Mail-Scanner deaktiviert werden, da sie sonst die Arbeit der SmartPOP2Exchange behindern!

Virens Scanner vom Typ G Data besitzen einen so genannten "On Access Scanner", welcher Dateien beim Lesen und Schreiben auf der Festplatte auf Viren testet. Da der "On Access Scanner" etwas Zeit benötigt bis er die Anhänge getestet hat, dauert das Herunterladen von Nachrichten länger.

Damit die SmartPOP2Exchange mit dem G Data-Scanner zusammenarbeiten kann, müssen Sie den "AVK Wächter" aktiviert haben und ggf. einige Einstellungen daran verändern.

Folgende Einstellungen sind notwendig:

- "Im Fall einer Infektion:" sollte die Datei ohne Nachfragen behandelt werden
- Gleiches gilt für "Infizierte Archive"
- "Beim Schreiben prüfen" muss aktiviert sein

Folgende Einstellungen werden empfohlen:

- Es sollten auch komprimierte Dateien gescannt werden, weil Viren oft in Archiven (z.B. *.zip-Dateien) verschickt werden.

BitDefender

Virens Scanner vom Typ BitDefender unterstützen von sich aus die Funktion eingehende Nachrichten auf Viren zu testen.

Versucht die SmartPOP2Exchange, eine Nachricht mit einem Virus weiterzuleiten, wird die BitDefender Antiviren Software aktiv und ersetzt die Nachricht durch eine Statusnachricht.

Kaspersky

Virens Scanner vom Typ Kaspersky besitzen einen so genannten "On Access Scanner", welcher Dateien beim Lesen und Schreiben auf der Festplatte auf Viren testet. Da der "On Access Scanner" etwas Zeit benötigt bis er die Anhänge getestet hat, dauert das Herunterladen von Nachrichten länger.

Damit die SmartPOP2Exchange mit dem Kaspersky-Scanner zusammenarbeiten kann, müssen Sie ggf. einige Einstellungen des "Antivirus-Monitor" verändern.

Folgende Einstellungen sind notwendig:

- Gefundene Viren müssen gelöscht oder umbenannt werden.
- Alle Warnhinweise sollten ausgeschaltet werden.

Folgende Einstellungen werden empfohlen:

- Es sollten auch Archive gescannt werden, weil Viren oft in Archiven (z.B. *.zip-Dateien) verschickt werden.
- Sie sollten Dateien jeder Art scannen lassen (nicht nur infizierbare Dateien) um ein besseres Ergebnis zu bekommen.
- Lassen Sie Kaspersky eine Report-Datei erstellen, da Sie sonst keine Rückmeldung über eventuelle Virenfunde haben.

Sophos

Virens Scanner vom Typ Sophos besitzen einen so genannten "On Access Scanner", welcher Dateien beim Lesen und Schreiben auf der Festplatte auf Viren testet. Da der "On Access Scanner" etwas Zeit benötigt bis er die Anhänge getestet hat, dauert das Herunterladen von Nachrichten länger.

Damit die SmartPOP2Exchange mit dem Sophos-Scanner zusammenarbeiten kann, müssen Sie den "InterCheck - Client" mit installiert haben und ggf. einige Einstellungen daran verändern.

Folgende Einstellungen sind notwendig:

- Infizierte Dateien müssen umbenannt, verschoben oder gelöscht werden.
- Dateien müssen beim Schreiben überprüft werden.

Folgende Einstellungen werden empfohlen:

- Es sollten auch komprimierte Dateien gescannt werden, weil Viren oft in Archiven (z.B. *.zip-Dateien) verschickt werden.

- Dateien sollten auch beim Lesen und Umbenennen überprüft werden.

Diese Bilder zeigen alle wichtigen Einstellungen des "InterCheck - Client" von Sophos.

11 Deutsche Gesetzeslage

[§ 257 \(HGB\) Aufbewahrung von Unterlagen / Aufbewahrungsfristen](#)

(1) Jeder Kaufmann ist verpflichtet, die folgenden Unterlagen geordnet aufzubewahren:

1. Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, Einzelabschlüsse nach § 325 Abs. 2a, Lageberichte, Konzernabschlüsse, Konzernlageberichte sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen,
2. die empfangenen Handelsbriefe,
3. Wiedergaben der abgesandten Handelsbriefe,
4. Belege für Buchungen in den von ihm nach § 238 Abs. 1 zu führenden Büchern (Buchungsbelege).

(2) Handelsbriefe sind nur Schriftstücke, die ein Handelsgeschäft betreffen.

(3) Mit Ausnahme der Eröffnungsbilanzen und Abschlüsse können die in Absatz 1 aufgeführten Unterlagen auch als Wiedergabe auf einem Bildträger oder auf anderen Datenträgern aufbewahrt werden, wenn dies den Grundsätzen ordnungsmäßiger Buchführung entspricht und sichergestellt ist, dass die Wiedergabe oder die Daten

1. mit den empfangenen Handelsbriefen und den Buchungsbelegen bildlich und mit den anderen Unterlagen inhaltlich übereinstimmen, wenn sie lesbar gemacht werden,
2. während der Dauer der Aufbewahrungsfrist verfügbar sind und jederzeit innerhalb angemessener Frist lesbar gemacht werden können.

Sind Unterlagen auf Grund des § 239 Abs. 4 Satz 1 auf Datenträgern hergestellt worden, können statt des Datenträgers die Daten auch ausgedruckt aufbewahrt werden; die ausgedruckten Unterlagen können auch nach Satz 1 aufbewahrt werden.

(4) Die in Absatz 1 Nr. 1 und 4 aufgeführten Unterlagen sind zehn Jahre, die sonstigen in Absatz 1 aufgeführten Unterlagen sechs Jahre aufzubewahren.

(5) Die Aufbewahrungsfrist beginnt mit dem Schluss des Kalenderjahrs, in dem die letzte Eintragung in das Handelsbuch gemacht, das Inventar aufgestellt, die Eröffnungsbilanz oder der Jahresabschluss festgestellt, der Einzelabschluss nach § 325 Abs. 2a oder der Konzernabschluss aufgestellt,

der Handelsbrief empfangen oder abgesandt worden oder der Buchungsbeleg entstanden ist.

SmartPOP2Exchange kann dies leider nicht erfüllen, da dieser ausgehende E-Mails nicht verarbeitet. Aber schauen Sie sich doch unser Produkt [Exchange Server Toolbox](#) an.

Insbesondere sind folgende Gesetze bei Verwendung von Spamfiltern zu beachten, jedoch nur für Unternehmen zutreffend, die im Sinne des Telekommunikationsgesetzes (TDG) agieren:

§ 206 (StGB) Verletzung des Post- oder Fernmeldegeheimnisses

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt

1. eine Sendung, die einem solchen Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,

2. eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt oder

3. eine der in Absatz 1 oder in Nummer 1 oder 2 bezeichneten Handlungen gestattet oder fördert.

(3) Die Absätze 1 und 2 gelten auch für Personen, die

1. Aufgaben der Aufsicht über ein in Absatz 1 bezeichnetes Unternehmen wahrnehmen,

2. von einem solchen Unternehmen oder mit dessen Ermächtigung mit dem Erbringen von Post- oder Telekommunikationsdiensten betraut sind oder

3. mit der Herstellung einer dem Betrieb eines solchen Unternehmens dienenden Anlage oder mit Arbeiten daran betraut sind.

(4) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die ihm als außerhalb des Post- oder Telekommunikationsbereichs tätigem Amtsträger auf Grund eines befugten oder unbefugten Eingriffs in

das Post- oder Fernmeldegeheimnis bekanntgeworden sind, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(5) Dem Postgeheimnis unterliegen die näheren Umstände des Postverkehrs bestimmter Personen sowie der Inhalt von Postsendungen. Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

§ 303a (StGB) Datenveränderung

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

12 Gesetzeslage im Ausland

Für Nutzer, deren E-Mail-Service-Provider mit in den U.S.A. registrierten Servern arbeiten, sind zu den deutschen auch die U.S.-amerikanischen Gesetze von Belang.

Sowohl der "E-mail Privacy Act of 2004" als auch der "Stored Communications Act of 2007" ([18 U.S.C. § 2701](#)) weichen in ihrer Herangehensweise von den deutschen Konzept des Fernmeldegeheimnisses ab.

Ein Nutzer eines E-Mail-Services kann nur dann erwarten, dass seine E-Mails vertraulich bleiben (***expectation of privacy***), wenn er dem Service-Provider keine oder nur genau definierte Zugriffsrechte gewährt (z.B. nur Scan auf Spam / Viren, ohne verdächtige Mails eigenmächtig zu löschen oder abzulehnen). Für jedes Zugriffsrecht, das der Nutzer dem Service-Anbieter gemäß Nutzungsvertrag einräumt, verliert der Nutzer auch seine gesetzlich verankerte ***expectation of privacy*** und er wird danach nur noch durch die firmeneigene *Privacy policy* des Service-Anbieters geschützt.

Fernerhin erlischt nach dem Gesetz ein Anspruch auf Privatsphäre grundsätzlich, wenn eine gelesene (d.h. zugestellte) E-Mail für mehr als 180 Tage auf dem Server des Diensteanbieters verbleibt. Der Zugriff Fremder auf solche Mails ist dann ohne Rechtsbruch möglich und kann durch den Diensteanbieter erfolgen bzw. gewährt werden, auch ohne den ursprünglichen Eigentümer der Mail darüber zu informieren.

- 2 -

2007 14
2010 14
2013 18

- A -

abwesenheitsnachricht 9
account data 45
AccountView 31
Add rule 34
adjust virus scanner 78
Aktionen 68
Alle Nachrichten 65
Alle/Keinen auswählen 37
ändern 29
Änderungen 5
ani-virus 31
anti virus 35, 78
Antivirus 31, 65
archivieren 41
Assistent 31
Ausland 84
Ausnahmen für Absender 37
Ausnahmen für Nachrichteninhalte 37
ausschließen 41
Auto-lernen 37
automatische Antworten 9

- B -

backup 31, 41
backup e-mail 31
Baumstruktur 31
bayes 37, 74, 76
Bearbeiten Menu 25
Bedingungen 65
Beenden 23
Beispiele 72
Benutzername 49, 50
Bestellen 4
Bewertung 37
Blacklist 37
Buildnummer 29

- C -

ClamAV 35, 65, 78

ClamWin 35, 78
Clear Log Datei 61
Content Filtering 18
Contents 6
Copyright 4
CSV 45

- D -

Datei 23, 59
Datei Menü 23
Datenbank 45
Delete rule 34
dienst start stop neustart 31
Dienstag 33
Donnerstag 33
DSGVO 82, 84
Duplizieren 25

- E -

Edit rule 34
Einstellungen 31, 33
Einstellungen speichern 23
EMail 49
eml 59
erneut versenden 28
error 61
Ersetze Absenderadresse durch [E-Mail Adresse] 68
erstelle Regel 72
ersten schritte 7
every account 34
excel 23, 45
Exchange Server 9, 14, 49
Exchange server 2000 9
Exchange server 2003 9
Exchange Server 2007 9, 14
Exchange Server 2010 9, 14
Exchange Server 2013 9
Exim 4
Export 23

- F -

F.A.Q. 5
FAQ 5, 6
Fehler 61
Fehler E-Mail 42
Fehlerbenachrichtigung 42
Feritag 33
filter 61, 67, 76

first steps 7
 Formular Einstellungen 31
 Fragen 5, 6
 funktioniert 6

- G -

Ganzer Tag 33
 Gesetz 82, 84
 Global 34

- H -

ham 76
 Hilfe 29
 History 5
 honey pot 74
 how it works 6

- I -

IMAP 25, 54
 IMAP account 54
 IMAP hinzufügen 25
 IMAP löschen 25
 IMAPport 54
 IMAPServer 54
 import 23, 45
 importieren 45
 Info 29
 Inhalts Filter 14
 Installationsschlüssel 29
 Intervall 31, 33

- J -

JAM Software 4

- K -

Kaufen 4
 Keine weiteren Regeln anwenden 68
 Knowledge base 6
 konfiguration 9, 14, 78
 Kontakt 4
 Konten 25
 Konten Anzeige 31
 Konten hinzufügen 25
 Konten Liste 44
 Konten löschen 25

Konten Wizard 25
 Konto 25, 31, 47, 76
 Konto Daten 45
 Konto hinzufügen 44
 Konto löschen 44
 Konto Name 47

- L -

Liste aller Aktionen 68
 Liste aller Bedingungen 65
 Log 61
 Log Datei 61
 Log Einstellungen 42
 Logeintrag 42
 Logeintrag löschen 42
 lösche Logeintrag nach X Tagen 42
 Löschen Nachricht ohne Download 68
 Lotus Notes 4

- M -

maximale Nachrichten 31
 Memory 4
 Menü 23
 Menüs 23
 Microsoft Exchange Server 2003 4
 Microsoft Exchange Server 2007 4
 Microsoft Exchange Server 2010 4
 Mittwoch 33
 Montag 33

- N -

Nachrichten die größer als ein [bestimmter Wert] sind 65
 Nachrichten die SpamAssassin als Spam erkennt 65
 Nachrichten mit [bestimmten Wörtern] im Body 65
 Nachrichten mit [bestimmten Wörtern] im Cc header 65
 Nachrichten mit [bestimmten Wörtern] im From header 65
 Nachrichten mit [bestimmten Wörtern] im Subject 65
 Nachrichten mit [bestimmten Wörtern] im To header 65
 Nachrichten mit einem Attachment 65
 Nachrichten mit ungültiger Mailadresse 65
 Nachrichten ohne Subject 65
 Nachrichtenzahl 31
 neu 5

- O -

Optionen 33
Ordner 59
Overview 6

- P -

Password 54
Passwort 49, 50
Periode 33
pickup folder 59
pickup Ordner 59
pickupfolder 59
pop3 25, 50, 76
POP3 hinzufügen 25
POP3 Konto 50
POP3 löschen 25
Port 49, 50
Postfix 4
Punkte 67
Punktzahl 67

- Q -

quickstart 7

- R -

regel 34
Regel bearbeiten 47
Regel hinzufügen 47
Regel kopieren 47
Regel löschen 47
Regelliste 47
Regeln 34, 47, 63, 72, 74
Regeln Inhalt 63
Registrierung 4
Requirements 4
rules 34

- S -

Samstag 33
SBS 9, 14, 49
Scanner 35, 78
Schnellstart 7
Schreibt einen [bestimmten] Text an den Anfang des
Subjects 68

Schwellwert 67
sende EML Dateien 28
SendMail 4
Server 4, 9, 14, 49, 50
Setze Priorität auf [bestimmten Wert] 68
sicherung 31, 41
signaturen 35
SMTP 4, 9, 14, 25, 49
SMTP Fehler 73
SMTP Fehler Regeln 73
SMTP hinzufügen 25
SMTP Konto 49
SMTP löschen 25
Sonabend 33
Sonntag 33
sortieren 44
spam 67, 74, 76
Spam Filter 31, 67, 74
Spam Filter aktivieren/Deaktivieren 37
SpamAssassin 67
Spamfilter 74
SpamfilterChecklist 37
speichern 41
SSL 54
start 7
Startzeit 33
status 31
Stopzeit 33
Systemvoraussetzungen 4

- T -

Timeout 31
Tobit 4
trainieren 74, 76
tree 31

- U -

Überblick 6
Username 54

- V -

Versende an [bestimmten] Empfänger 68
Versende ohne Anhang 68
Version 29
viren scanner 78
viren scanner anpassen 78
Virus 35, 78

- W -

Warnungen 61
Was ist neu 5
Was ist SmartPOP2Exchange 6
Was sind Regeln? 63
Weiterleitungen 9, 14
Whitelist 37
wie arbeitet 6
Windows 2003 Server (x86 / x64) 4
Windows 7 (x86 / x64) 4
Windows Server 2008 (x86 / x64) 4
Windows Server 2008 R2 (x86 / x64) 4
Windows Vista (x64 / x64) 4
Windows Vista (x86 / x64) 4
Windows XP (x86 / x64) 4
Wochentag 33
Wörter 37

- X -

xml 61

- Z -

Zeitplan 33