Dokumentation Mailcluster System
Version 1.3.0

Inhaltsverzeichnis

Anmeldung Administrationsbereich

Die Anmeldung zur Administration erfolgt unter folgendem Link:

http://mail.ihrdomainname.tld

Sollten die Nameserver für Ihre Domain noch nicht auf das neue System umgestellt sein, können Sie auch folgenden Link verwenden:

http://www.clustermail.de

Drücken Sie auf Administration: Verwalten Sie Ihre Domain

Die Anmeldung muss mit der kompletten E-Mailadresse und dem zugehörigen Passwort erfolgen. Anmelden können sich Administratoren ebenso wie normale Benutzer.

Mit Administratorrechten können Sie:

- Konten anlegen/ändern/löschen
- Weiterleitungen (Aliase, Sammelpostfach) anlegen/ändern/löschen
- Verteiler anlegen/ändern/löschen
- Mailinglisten anlegen/ändern/löschen
- Einstellungen (Whitelist, Blacklisten)
- Block-Adressen anlegen/ändern/löschen
- Antispam (Training/Einstellung eigenes Postfach)

Mit Benutzerrechten können Sie:

- Konto ändern
- Blacklistverwaltung
- Antispam (Training/Einstellung eigenes Postfach)

HINWEIS: Bevor Sie sich anmelden, können Sie durch einen Klick auf eine der Landesflaggen oben rechts die gewünschte Sprache einstellen. Derzeit stehen Ihnen Deutsch und Englisch zur Auswahl.

Konten

Benutzer hinzufügen

Klicken Sie am linken Bildschirmrand auf Benutzer hinzufügen um neue POP/IMAP Accounts (E-Mailkonten) zu erstellen.

Im Feld Namen geben Sie eine Bezeichnung ein, wie das Konto in der Übersicht angezeigt werden soll (z.B. Vorname Nachname).

Im Feld Adresse geben Sie die E-Mail Adresse ein (alles VOR dem @ Zeichen).

Im Feld Passwort geben Sie ein sicheres (4 bis 16 Zeichen) Passwort ein. Dieses Passwort bestätigen Sie bitte im folgenden Feld Passwort bestätigen.

Sie haben die Möglichkeit mehreren Benutzern Administrationsrechte zu geben. Wenn Sie dem Konto Administrationsrechte geben möchten, setzen Sie bitte einen Haken bei Hat die Person Administratoren-Rechte. Achtung: vergeben Sie dieses Recht nur, wenn die Person über die entsprechenden Kenntnisse zur Mailadministration verfügt.

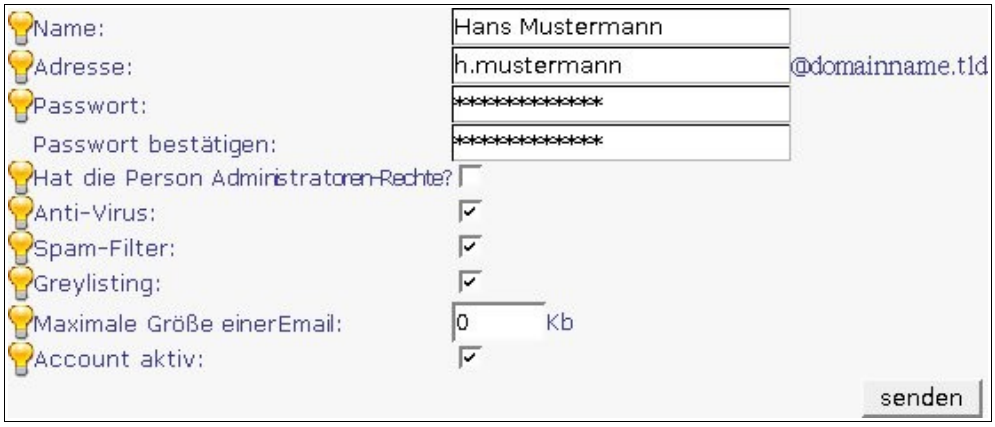
Wenn für das Konto der Anti-Virus aktiv sein soll, setzen Sie hier bitte einen Haken. Entdeckt der Virenfilter eine E-Mail mit einem Virus, wird diese vom System gelöscht. Der Versender dieser Virenmail erhält keine Benachrichtigung. Verwenden Sie zur eigenen Sicherheit dennoch einen lokalen Virenscanner auf Ihrem PC, um die Sicherheit Ihres Rechners hoch zu halten.

Wenn für das Konto das Greylisting aktiv sein soll, setzen Sie hier bitte einen Haken. Greylisting ist eine Form der SPAM-Bekämpfung bei E-Mails. Typische SPAM-Software versucht nicht eine E-Mail ein zweites Mal zu zustellen. Solche E-Mails werden im Regelfall erfolgreich gefiltert. Dadurch kommt es bei Greylisting anfänglich leider zu durchschnittlich 15 Minuten Verzögerung bei der Zustellung, reduziert den SPAM aber um mehr als 50%.

Wenn Sie die Maximale Größe einer eingehenden E-Mail festlegen möchten, tragen Sie den gewünschten Wert bitte hier ein. Mit dieser Option können Sie festlegen, wie groß eine eingehende E-Mail maximal sein darf. Serverseitig sind 50 MB eingestellt. Dieser Wert kann auch nicht durch diese Einstellung überschritten werden. Der Wert NULL besagt, dass die serverseitige Bregrenzung (50MB) eingestellt ist.

Wenn der Account aktiv sein soll, hier bitte ein Haken setzen.

Klicken Sie auf senden, um die Einstellungen zu speichern!



HINWEIS: Wenn Sie auf eines der gelben Lämpchen klicken erhalten Sie eine Onlinehilfe!

Weiterleitungen

Alias hinzufügen

Ein Alias bezeichnet einen Verweis auf eine E-Mailadresse.

In das Feld Bezeichnung des Alias geben Sie eine sinnvolle Bezeichnung für den Alias an. Dieser Name ist **nicht** die E-Mailadresse unter der der Alias erreichbar ist.

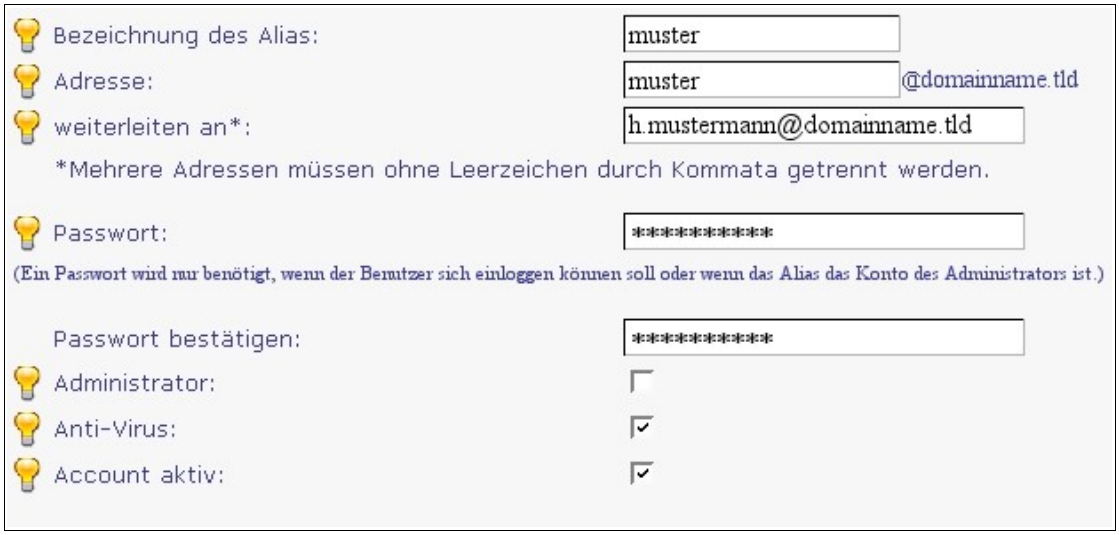
In das Feld Adresse geben Sie den Namen an, unter dem der Alias per E-Mail erreichbar sein soll.

In das Feld weiterleiten an geben Sie eine gütige E-Mailadresse an, an die die E-Mails dieses Alias weitergeleitet werden sollen. Mehrere Adressen müssen ohne Leerzeichen durch Kommas getrennt werden.

In das Feld Passwort geben Sie ein sicheres Passwort (4 bis 16 Zeichen) an und bestätigen dies im Feld Passwort bestätigen. Ein Passwort wird nur benötigt, wenn der Benutzer sich einloggen können soll oder wenn der Alias das Konto eines Administrators ist.

Wenn dieser Alias ein Administrator sein soll, setzen Sie hier einen Haken. Achtung: Vergeben Sie dieses Recht nur, wenn die Person über die entsprechenden Kenntnisse zur Mailadministration verfügt.

Mit der Option Anti-Virus aktivieren Sie den Virenfilter für diesen Account. E-Mails, die Viren enthalten, werden von dem System gelöscht. Verwenden Sie zur eigenen Sicherheit dennoch einen Virenscanner auf Ihrem PC, um die Sicherheit Ihres Rechners hoch zu halten.



Sammelpostfach hinzufügen

HINWEIS: Wird ein Sammelpostfach eingerichtet, und als Zieladresse ein lokaler Account angegeben, werden bei diesem Account folgende Leistungen deaktiviert: Antispam, Antivirus, Blacklistfiltering. Um diese Funktionen wieder nutzen zu können, löschen Sie bitte den Catchall-Account (Sammelpostfach)

ACHTUNG: Überlegen Sie sich gut, ob Sie auch wirklich ein Sammelpostfach einsetzen möchten. Sammelpostfach oder auch CatchAll genannte Accounts nehmen u.a. auch jeden „Müll / SPAM“ entgegen, dessen Aussortierung Ihnen wiederum Zeit kostet!

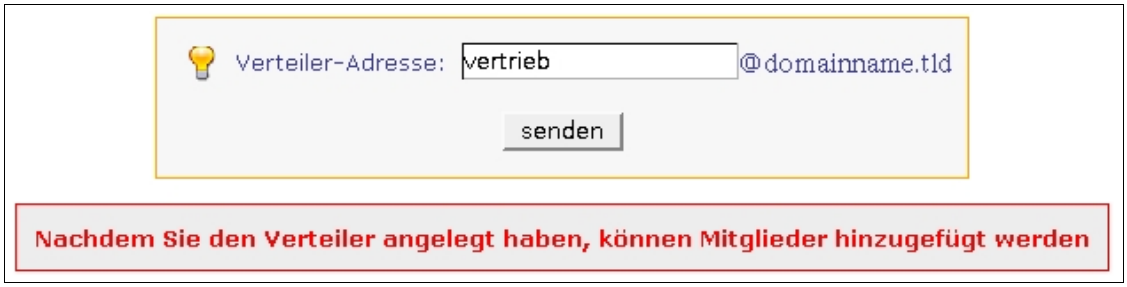
In das Feld weiterleiten der E-Mail an geben Sie die E-Mail-Adresse ein, die alle E-Mails erhalten soll, die an Ihre Domain gerichtet sind, deren E-Mail-Adresse nicht existiert.

Verteiler

Ein Verteiler ist eine Einrichtung, die eine Resource (E-Mail) an mehrere Empfänger verteilt. Zum Beispiel könnten Sie einen Verteiler vertrieb@domainname.tld generieren, der eine an vertrieb@domainname.tld gesendete E-Mail an alle Vertriebsmitarbeiter bzw. deren E-Mail-Adressen verteilt.

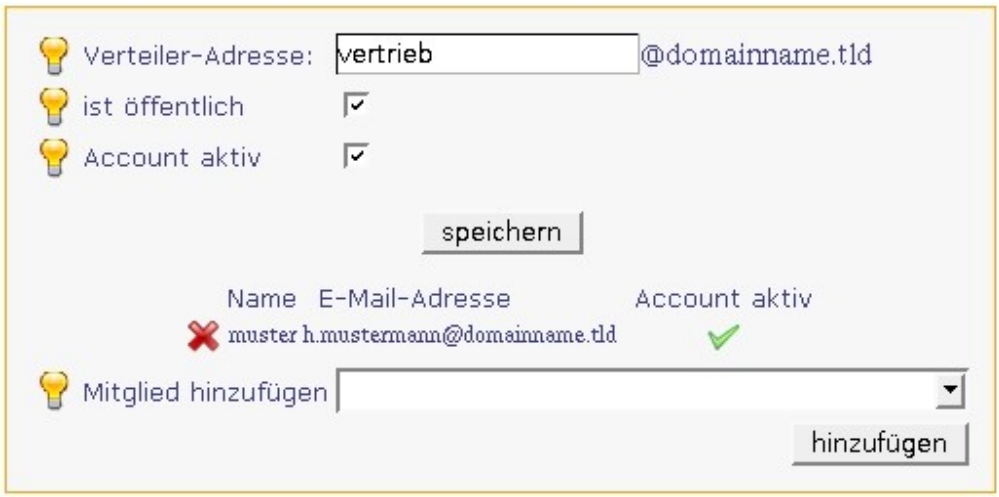
Verteiler hinzufügen

Tragen Sie im Feld Verteiler-Adresse den gewünschten Verteilernamen ein.



Um die Mitglieder für diesen Verteiler hinzuzufügen, klicken Sie auf den Verteilernamen.

Wählen Sie im Dropdown Menü Mitglied hinzufügen einen Empfänger für diesen Verteiler und klicken auf hinzufügen. Sie können beliebig viele Empfänger hinzufügen.



Mailinglisten

Dieses Modul steht im Moment leider noch nicht zur Verfügung!

Einstellungen

Hier können Sie Einstellungen vornehmen, die sich sofort auf alle Accounts in dieser Domain auswirken. z.B. Blacklisteneinstellungen für alle Benutzer der Domain aktivieren oder deaktiveren.

Whitelist

In einer Whitelist werden E-Mailadressen geführt, von denen der Mailserver für diese Domain E-Mails grundsätzlich annimmt und zustellt. Es kommen für diese Adressen keine SPAM- und Blacklisten zum Einsatz (Der Virenschutz bleibt jedoch erhalten).

In der Übersicht Inhalt der Whitelist für domainname.tld sehen Sie Ihre bereits angelegten Adressen, die whitelistet sind.

zur Whitelist hinzufügen

Im Feld Neuer Whitelisteintrag geben Sie einfach eine E-Mailadresse ein, die auf der Whitelist stehen soll.

HINWEIS: In einer der nächsten Versionen wird es möglich sein komplette Domains in die Whitelist aufzunehmen (z.B *@ebay.com, *@amazon.de).

Blacklistverwaltung

Blacklisten sind Datenbanken in denen IP-Adressen geführt werden, die von unserem Mailserver geblockt werden, wenn Sie diese Blackliste(n) aktivieren. Durch Nutzung dieser Blacklisten können Sie den Erhalt von SPAM weiter einschränken.

Hier haben Sie die Möglichkeit für Ihre Konten die Blacklistverwaltung einzustellen.

- aktivieren: für alle Konten ist die gewählte Blackliste aktiv
- deaktivieren: für alle Konten wid die ausgewählte Blackliste deaktiviert
- keine Änderung: jedes Konto kann selbst wählen welche bzw. ob eine Blackliste verwendet werden soll.

HINWEIS: Mit Änderungen können nicht mehr rückgängig gemacht werden! ist nicht gemeint, das Sie nur einmalig eine Einstellung vornehmen können!

dul.dnsbl.sorbs.net

Blockliste für Dynamische IPs (t-dsl, arcor, etc.). ('gute' Nachrichten werden im allgemeinen nicht von solchen Zugängen aus versendet.)

Link: http://www.de.sorbs.net/faq/dul.shtml

cbl.abuseat.org

Bei CBL werden mit Viren infizierte PC-Systeme, offene Proxys und von Trojanern kompromitierte PC-Systeme, die für den SPAM-Versand genutzt werden, gelistet.

Link: http://cbl.abuseat.org

Chinablacklist

IPs, die in China verwendet werden

Link: http://www.blackholes.us

sbl-xbl.spamhaus.org

Kombinierte Liste von CBL (diese also NICHT extra auswählen), bei NJABL gelistete offene Proxys und bei Spamhaus gelistete Spammer.

Link: http://www.spamhaus.org/xbl/

Block-Adressen

E-Mails, die an eine Block-Adresse geschrieben werden, werden vom Mailserver sofort gelöscht. Der Absender erhält keine Information darüber. Die E-Mails können nicht mehr hergestellt werden!

Blockadresse hinzufügen

In das Feld Adresse zum Blocken tragen Sie die E-Mailadresse (alles vor dem @ Zeichen) ein, die keine E-Mails mehr erhalten soll.

Durch einen Klick auf das rote Kreuz kann die eingetragene Adresse wieder entfernt werden.

Antispam

Als Spam werden unerwünschte Nachrichten bezeichnet, die dem Empfänger unverlangt zugestellt werden.

Bei dem von uns eingesetzten Antispam-Filter (dspam) handelt es sich um einen statistischen Filter. Das Training des Filters erfordert anfangs zwar etwas Arbeit, bringt dafür Erfolgsquoten von bis zu 95 Prozent!

HINWEIS: Jedes E-Mailkonto muss individuel trainiert werden!

Der Filter kann wie folgt trainiert werden:

- Webinterface

Mehr über das Training via Webinterface erfahren Sie auf Seite 16 / History

- E-Mail Client (z.B. Outlook oder Mozilla Thunderbird) als E-Mail Forward oder Bounce

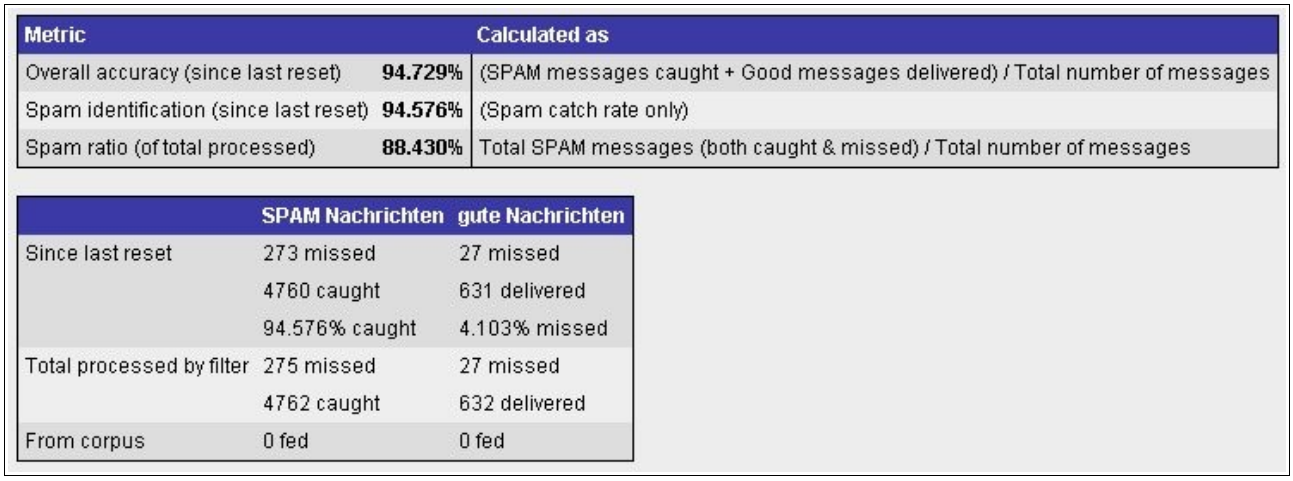
Falls Sie eine Spam-Nachricht erhalten, die nicht vom Filter erkannt wurde, leiten Sie diese einfach an '**spam+*account@ihrdomainname.tld***' weiter und schon trainieren Sie den Filter.

Um eine als Spam erkannte Nachricht als erwünscht zu trainieren, leiten Sie diese einfach an '**nospam+*account@ihrdomainname.tld***' weiter. Diese 'nospam+account@ihrdomainname.tld - Funktion' funktioniert natürlich nur, wenn Sie sich den SPAM auch zustellen und nicht in den Quarantäne Ordner verschieben lassen.

HINWEIS: Wenn Sie den Filter per Forward trainieren möchten, müssen Sie in der Konfiguration den Punkt 'sende ich den Spam als forward' einstellen.

Leistung

Hier sehen Sie die Leistungsübersicht des Antispam-Filters. Im unten dargestellten Bild hat der Spamfilter eine Spam Identifikation von 94.576%. Dieses E-Mailkonto bzw. dessen Spamfilter wurde durch uns ca. 7 Tage lang trainiert bei über 5000 E-Mails.



Metric		Calculated as
Overall accuracy (since last reset)	**94.729%**	(SPAM messages caught + Good messages delivered) / Total number of messages
Spam identification (since last reset)	**94.576%**	(Spam catch rate only)
Spam ratio (of total processed)	**88.430%**	Total SPAM messages (both caught & missed) / Total number of messages

	SPAM Nachrichten	gute Nachrichten
Since last reset	273 missed	27 missed
	4760 caught	631 delivered
	94.576% caught	4.103% missed
Total processed by filter	275 missed	27 missed
	4762 caught	632 delivered
From corpus	0 fed	0 fed

Konfiguration

Das Konfigurationsmenü unterteilt sich in drei Menüpunkte:

- Training – Configure how the filter learns as it processes messages
- Message Handling – Configure how SPAM is handled
- Features – Tuning SPAM filtering

In der Regel stellt man den Filter auf jede neue Nachricht trainieren. Die Empfindlichkeit des Filters kann während der Trainingszeit so eingestellt werden, dass mehr Nachrichten als SPAM erkannt werden. Dies fördert den Trainingsprozess!

Wenn Sie den Filter per E-Mail trainieren möchten (z.B. per Outlook via Weiterleiten an '**spam+*account@ihrdomainname.tld***') müssen Sie sende ich den Spam als forward einstellen. Die Signatur des DSPAM wird dann in den Body geschrieben, was z.B. bei PGP-Verschlüsselung zu Fehlern führen kann.

In diesem Fall müssten Sie die bounce Methode, sende ich den Spam als bounce, verwenden.

Hier einige Anleitungen wie in den wichtigsten E-Mail Clients ein Bounce ausgeführt wird:

- Die Funktion heißt in **Outlook/Express** "Diese Nachricht erneut senden" und ist im Menü "Aktionen" zu finden, wenn die entsprechende E-Mail mit einem Doppelklick geöffnet wurde. Die Funktion steht nicht zur Verfügung, wenn Outlook/Express diese E-Mail lediglich im Vorschau-Fenster anzeigt.
- Bei **Netscape E-Mail** heißt diese Funktion "Nachricht als neu bearbeiten" (im Menü "Nachricht").
- Bei **Eudora** verwenden Sie bitte die "Redirect"-Funktion im Menü "Message".

Auch andere E-Mail-Programme stellen ähnliche Funktionen zum erneuten versenden von E-Mails (ohne Änderung von Text und Absender-Informationen) zur Verfügung.

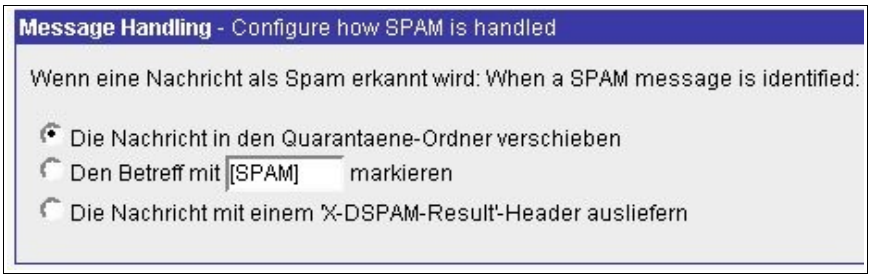
HINWEIS: In der Regel genügt es wenn Sie die forward Methode verwenden!

Wenn der Filter eine Nachricht als SPAM erkannt hat, können Sie einstellen was mit dieser passieren soll. Sie haben die Möglichkeit erkannten SPAM in den Quarantäne Ordner verschieben zu lassen, die Betreffzeile mit [SPAM] markieren zu lassen oder die Nachricht mit einem speziellen X-DSPAM-Result Headereintrag zu versehen.

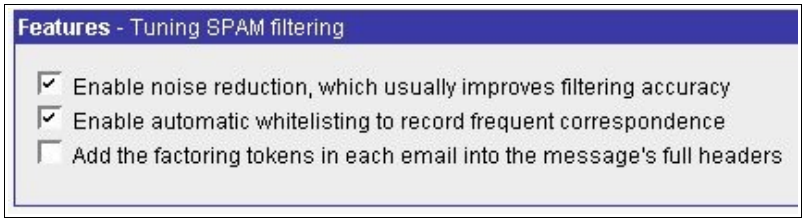
Wenn Sie den SPAM in den Quarantäne Ordner verschieben lassen, bleibt Ihr PC frei von SPAM.

Wenn Sie den Betreff mit [SPAM] markieren, bekommen Sie den SPAM zugestellt und haben die Möglichkeit selbst mit eigenen Regeln zu sortieren.

Wenn Sie den Header mit X-DSPAM-Result versehen, bekommen Sie den SPAM ebenso zugestellt und haben die Möglichkeit selbst mit eigenen Regeln zu sortieren.



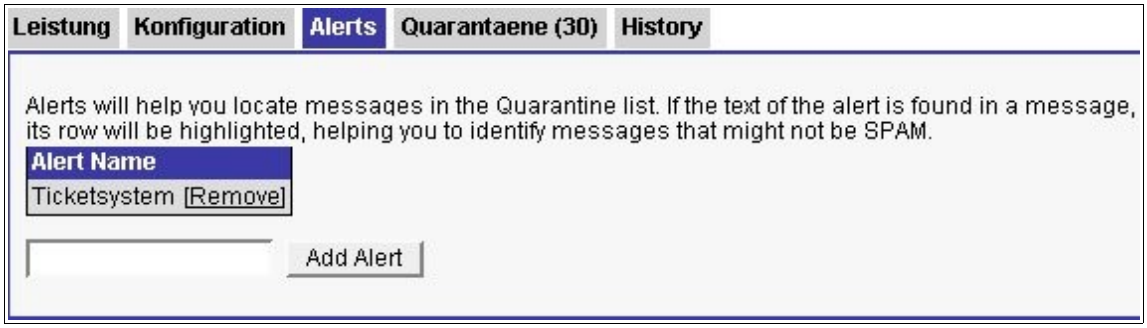
Das Tuning des Filters haben wir per Default auf die besten Werte eingestellt!



Bitte Vergessen Sie nicht Ihre Einstellungen mittels Submit Changes zu speichern!

Alerts

In Alerts eingetragene Schlagwörter werden in der Quarantäneübersicht besonders hervorgehoben.



HINWEIS: Die Nutzung dieser Funktion dient zur leichteren Identifikation von Nachrichten, die KEIN Spam sind.

Quarantäne

Im Quarantäne Ordner landen Nachrichten, die der Filter als SPAM erkannt hat. Vorraussetzung ist, dass Sie im Konfigurationsmenü des Filters „Die Nachricht in den Quarantäne-Ordner verschieben“ eingestellt haben. Sie sehen in aufsteigender Reihenfolge die Bewertung in Prozent, mit welcher der Filter die Nachrichten eingestuft hat.

Um die Liste übersichtlich zu halten empfielt es sich in gewissen Abständen den Quarantäne Ordner auf “gute“ Nachrichten zu prüfen. Es kann gerade während der Lernphase vorkommen, dass eine gute Nachricht fälschlicherweise als SPAM erkannt wird.

Sie haben die Möglichkeit eine/mehrere Nachrichten zu markieren und mittels Delete Checked (löschen, E-Mail = SPAM) oder Deliver Checked (zustellen, E-Mail = gut) zu bearbeiten.

Mit Delete All können Sie den kompletten Quarantäne Ordner löschen.

Wenn Sie sich nicht sicher sind, ob eine Nachricht auch wirklich SPAM ist, können Sie auf den Subject dieser E-Mail klicken, Sie bekommen dann den Inhalt angezeigt und können besser entscheiden. Wenn Sie nun der Meinung sind, dass es sich um keinen SPAM handelt, klicken Sie einfach auf Deliver Message und diese Nachricht wird Ihnen zugestellt. Zusätzlich lernt der Filter natürlich, dass diese Art der E-Mails in Ihren Augen kein SPAM ist.

HINWEIS: Im Quarantäne Ordner befindliche Nachrichten werden nach 90-Tagen automatisch vom System gelöscht!

History

In der History sehen Sie die 800 zuletzt eingegangenen E-Mails in statistischer Form, d.h. dass Sie nur Datum, From und Subject sehen, nicht jedoch den Body der E-Mails. Im Historybereich können Sie das Training Ihres Filter vornehmen indem Sie eingegangene E-Mails auf die Reaktion des Filters trainieren. Bitte beachten Sie, dass jedes POP3 Konto separat trainiert werden muss!

E-Mail wurde als gut erkannt und dem POP3 Konto zugestellt. Sie können den Filter mit einem Klick auf As Spam dahingehend trainieren, dass diese E-Mail in Ihren Augen SPAM ist.

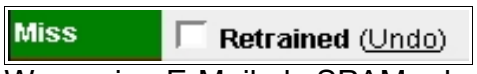
E-Mail wurde als SPAM erkannt und je nach Einstellung behandelt (Quarantäneordner, Tag im Subject oder X-DSPAM-Result Headereintrag). Sie können den Filter mit einem Klick auf As Innocent dahingehend trainieren, dass diese E-Mail in Ihren Augen kein SPAM ist.

E-Mail ist whitelisted. Wenn viele E-Mails von einem Empfänger eingegangen und niemals von Ihnen beanstandet worden sind, macht der Filter ein Auto-Whitelist.

Resend bedeudet, dass Sie diese E-Mail (mit exakt dem gleichen Inhalt) mehr als einmal erhalten haben. Entweder stand Ihre E-Mail Adresse im To + CC/BCC Feld oder es ist irgendwo eine Weiterleitung auf diese E-Mail Adresse eingerichtet. Im vorliegenden Fall könnten Sie den Filter dahingehend trainieren, dass diese E-Mail Spam ist.

Resend bedeudet, dass Sie diese E-Mail (mit exakt dem gleichen Inhalt) mehr als einmal erhalten haben. Entweder stand Ihre E-Mail Adresse im To + CC/BCC Feld oder es ist irgendwo eine Weiterleitung auf diese E-Mail Adresse eingerichtet. Im vorliegenden Fall könnten Sie den Filter dahingehend trainieren, dass diese E-Mail **KEIN** Spam ist.

Wenn eine E-Mail als gut erkannt wurde, Sie diese jedoch als SPAM trainiert haben. Sie haben die Möglichkeit dieses wieder Rückgangig zu machen, indem Sie auf Undo klicken.



Wenn eine E-Mail als SPAM erkannt wurde, Sie diese jedoch als gut trainiert haben. Sie haben die Möglichkeit dieses wieder Rückgangig zu machen, indem Sie auf Undo klicken.