

[← Zum Hauptmenü](#)

Mail-Filter

Der mp-Mailserver verfügt über zwei leistungsstarke Mailfilter zur sicheren und effektiven Spam- und Virenfilterung der ein- und ausgehenden E-Mails. Die Mailfilter können dabei alternativ verwendet werden. Während der erste Mailfilter (amavisd-new) eine zentrale Administration über die Menüs bereitstellt, kann der zweite Mailfilter (amavisd-maia) über ein Webinterface benutzerindividuell zur Filterung eingesetzt werden.

Um Änderungen an den Mailfilter-Einstellungen vorzunehmen melden Sie sich bitte als Benutzer *config* an und wählen dann den Menüpunkt *Einstellungen>Mail-Filter* aus. Sie haben folgende Konfigurationsmöglichkeiten:

Menüpunkt	Beschreibung
Ende	Verlassen des Menüs.

Max.Anzahl Empfangs-Prozesse	Anzahl der Postfix-Prozesse die maximal gleichzeitig E-Mails empfangen sollen. Der Standard sind 50 Prozesse.
Greylisting verwenden	Greylisting bezeichnet eine Form der Spam-Bekämpfung bei E-Mails, bei dem die erste E-Mail von unbekanntem Absendern temporär abgewiesen und erst nach einem zweiten Zustellversuch angenommen wird. Bitte diese Einstellung nur aktivieren, wenn Sie sich vorher über die Vor- und Nachteile von Greylisting genau informiert haben.
Pause (Tarpit) verwenden	Tarpit ist eine weitere Form der Spam-Bekämpfung im E-Mailverkehr. Hierbei wird eine Pause vor der Annahme der E-Mail erzwungen.
Verzögerung in Sekunden	Die Zeitverzögerung für Tarpit, der Standard ist 65 Sekunden.
Nach Pause kein Greylisting	Soll nach Abwarten der Zwangspause auf Greylisting verzichtet werden?
Greylisting-Empfänger-Ausnahmen	Angabe, welcher Empfänger sollen Mails sofort ohne Greylisting empfangen.
Greylisting-Sender-Ausnahmen	Angabe, welche DNS- oder IP- (Teil-) Adressen sollen ohne Greylisting-Sperre senden dürfen.
Sender Policy Framework (SPF)	Blocken falscher Absenderadressen.
Relay Blocking Lists (RBL) verwenden	Auswahl, ob RBLs verwendet werden sollen, um entsprechende Mails sofort abzuweisen. Das auf Blocking-Listen basierende Konzept greift auf so genannte "Schwarze Listen" (Blocking-Listen) zurück. In diesen Listen befinden sich IP-Adressen und Internet-Adressen (URLs) von Absendern, von denen keine E-Mail erwünscht ist, da diese bekanntermaßen nur Viren oder Werbung verschicken.
Relay Blocking List Server	Eintragung der RBL Server als Name oder IP-Adresse. Mehrere Einträge sind möglich und durch Leerzeichen zu trennen.
Verbotene Mail-Absender	Angabe, welche Absender-Adressen direkt abgewiesen werden. Die Eintragung erfolgt als name@ für beliebige Domänen oder name@domäne für eine bestimmte Domäne.

Menüpunkt	Beschreibung
Verbotene Mail-Empfänger	Angabe, welche Empfänger-Adressen direkt abgewiesen werden. Die Eintragung erfolgt als name@ für beliebige Domänen oder name@domäne für eine bestimmte Domäne.
Absender-Syntax prüfen	Hier könne Sie auswählen ob eine ungültige Mail-Absender-Adresse abgewiesen werden soll.
Adressprüfung von außen (Verify)	Auswahl, ob lokale Adressen mit dem verify-Kommando von außen geprüft werden können.
Adressprüfung am Zielservers	Auswahl, ob lokale Adressen an einem lokalen Zielservers mit dem verify-Kommando überprüft werden sollen, damit unbekannte Adressen gleich abgewiesen werden können.
—	
Mail-Archiv-Intervall	Auswahl, in welchem Intervall Mails in ein Mail-Archiv geschrieben werden sollen.
Signatur-Key neu	Signatur-Key für das Mail-Archiv
Mail-Archiv komprimieren	Angabe, ob und wie Mail-Archive archiviert werden sollen.
—	
Art des Viren- und Spam-Filters	Zur Auswahl stehen der amavisd-new, bei dem der Administrator maint globale Filterregeln (Black/White-Listen) für alle Benutzer setzt, oder der amavisd-maia, ein Filter, der individuell von jedem Benutzer über ein Webinterface konfiguriert werden kann. Wenn der entsprechende Filter ausgewählt wurde, öffnet sich das dazugehörige Konfigurationsmenü automatisch.
—	
1. Auswahl des amavisd-maia Filters (Maia Mailguard)	
RAM-Disk in MB	Festsetzen des für dem Spamfilter verfügbaren RAM-Speichers für temporäre Dateien. Es wird empfohlen die Standardeinstellungen von 128 MB nicht zu ändern.
Anzahl parallele Aufrufe	Anzahl der Prozesse, die maximal gleichzeitig vom Scanner bearbeitet werden dürfen. Je mehr Prozesse gleichzeitig laufen, desto mehr Rechenkapazität wird beansprucht. Der Standard ist 2.
Externe Spam-Abfragen	Auswahl, ob empfangenen E-Mail mit Spam-Listen von externen Anbietern verglichen werden sollen. Es wird zum Abgleich nicht der Inhalt der empfangenen Nachricht übermittelt, sondern ausschließlich der Header! Es stehen folgende externe Anbieter zur Verfügung: Razor, DCC, Pyzor und iX.
Verbotene Attachment-Typen	Einstellung von verbotenen Mail-Attachment-Typen. Alle Attachments, die einen verbotenen Typ haben, werden getrennt behandelt. Die Typ-Erkennung erfolgt nach dem Inhalt der Datei.
Verbotene Attachment-Namen	Einstellung von verbotenen Mail-Attachment-Namens-Endungen. Alle Attachments, die einen verbotenen Namen haben, werden getrennt behandelt.
Verschlüsselte Archive zulassen	Einstellung, ob verschlüsselte Archive (zip etc.) in E-Mail Anhängen zugelassen werden sollen. Diese Archive werden ggf. wie die anderen verbotenen Typen behandelt.
Sprache der Filtermeldungen	Einstellung der Sprache für Meldungen und E-Mails des Mail-Filter-Systems. Zur Auswahl stehen Englisch und Deutsch.

Menüpunkt	Beschreibung
Spam-Muster täglich akt.	Falls aktiviert, lädt Ihre Firewall täglich aktualisierte Muster für den Spam-Filter aus dem Internet. Achtung: Die Nutzung dieser Muster erfolgt auf eigenes Risiko!
Spam-Muster von SARE akt.	Falls aktiviert, wird zusätzlich das Muster des SARE-Projektes aktualisiert.
Viren-Administrator	E-Mail Adresse für Benachrichtigungen, die versandt werden, sobald eine mit einem Virus infizierte E-Mail empfangen wurde.
Spam-Administrator	E-Mail Adresse für Spam-Warnungen. Es wird empfohlen hier keine Adresse eintragen, da sonst für jede Spam-Nachricht eine weitere Benachrichtigung an die hier eingetragenen E-Mail-Adresse versandt wird.
Weitere-Empfänger-Domänen	Welche weiteren Empfänger-Domänen sollen Spam-Markierungen erhalten. Im Standard-Fall wird nur für E-Mails, die für die Haupt-Domäne bestimmt sind Spam-Markierungen gesetzt. Es können hier weitere Domänen eingetragen werden, die auch durch den Spam-Filter gefiltert werden sollen.
Spam-Betreff	Spam-Markierung, die erkannte Spam-E-Mails bekommen, die trotzdem zugestellt werden sollen.
Spam-Auto-Lern-Schwelle	Angabe, ab wie vielen Spam-Punkten eine Mail automatisch als Spam eingelernt und aus der Quarantäne entfernt werden soll.
Ham-Auto-Lern-Schwelle	Angabe, unter wie vielen Spam-Punkten eine Mail automatisch als Ham eingelernt und aus der Quarantäne entfernt werden soll.
MySQL Server	Name oder IP-Adresse des MySQL-Servers für die Maia-Mailverwaltung (Spam-Verwaltung). Die Einstellung sollte immer auf <i>localhost</i> stehen bleiben.
Amavis-MySQL-Passwort setzen	Passwort für die Administration der lokalen MySQL amavis-Datenbank setzen.
Maia-Authentifizierungs-Server	Server-Adresse für die Maia-Benutzer-Authentisierung. Für den integrierten Server bitte <i>localhost</i> eintragen.
Maia-Authentifizierungs-Methode	Für die Authentifizierung der Benutzer gegen den Maia-Server stehen POP3 und IMAP als Protokoll zur Verfügung. Wenn der integrierte Maia-Authentifizierungsserver verwendet wird ist die Methode POP3. Wenn die Authentifizierung gegen einen Active Directory-Server erfolgen soll, so ist IMAP als Protokoll auszuwählen.
—	
2. Auswahl des amavisd-new Filters (Interner Filter)	
RAM-Disk in MB	Festsetzen des für dem Spamfilter verfügbaren RAM-Speichers für temporäre Dateien. Es wird empfohlen die Standardeinstellungen von 128 MB nicht zu ändern.
Anzahl parallele Aufrufe	Anzahl der Prozesse, die maximal gleichzeitig vom Scanner bearbeitet werden dürfen. Je mehr Prozesse gleichzeitig laufen, desto mehr Rechenkapazität wird beansprucht. Der Standard ist 2.
Externe Spam-Abfragen	Auswahl, ob empfangenen E-Mail mit Spam-Listen von externen Anbietern verglichen werden sollen. Es wird zum Abgleich nicht der Inhalt der empfangenen Nachricht übermittelt, sondern ausschließlich der Header! Es stehen folgende externe Anbieter zur Verfügung: Razor, DCC, Pyzor und iX.

2. Auswahl des amavisd-new Filters (Interner Filter)	
Verbotene Attachment-Typen	Einstellung von verbotenen Mail-Attachment-Typen. Alle Attachments, die einen verbotenen Typ haben, werden als Viren behandelt.
Verbotene Attachment-Namen	Einstellung von verbotenen Mail-Attachment-Namens-Endungen. Alle Attachments, die einen verbotenen Namen haben, werden als Viren behandelt.
Verschlüsselte Archive zulassen	Einstellung, ob verschlüsselte Archive (zip etc.) in E-Mail Anhängen zugelassen werden sollen.
Sprache der Filtermeldungen	Einstellung der Sprache für Meldungen und E-Mails des Mail-Filter-Systems. Zur Auswahl stehen Englisch und Deutsch.
Spam-Muster täglich akt.	Falls aktiviert, lädt Ihre Firewall täglich aktualisierte Muster für den Spam-Filter aus dem Internet. Achtung: Die Nutzung dieser Muster erfolgt auf eigenes Risiko!
Spam-Muster von SARE akt.	Falls aktiviert, wird zusätzlich das Muster des SARE-Projektes aktualisiert.
Viren-Behandlung	Behandlung von E-Mails, die mit bekannten Viren infiziert sind. Zusätzlich zu dieser Auswahl wird eine E-Mail mit einer Warnung an den Viren-Administrator geschickt. Für die Behandlung stehen folgende Möglichkeiten zur Auswahl: REJECT » E-Mail direkt zurückweisen BOUNCE » Eine Fehler-E-Mail mit Erklärungen an den Absender schicken PASS » E-Mail trotzdem an den Empfänger zustellen DISCARD » E-Mail löschen
Viren-Administrator	E-Mail Adresse für Viren-Warnungen.
Viren-Quarantäne	E-Mail Adresse für die Zustellung von E-Mails, die Viren enthalten. Falls leer, werden die Mails in einem lokalen Verzeichnis auf der Festplatte abgelegt.
Spam-Behandlung	Behandlung von E-Mails, die als Spam erkannt worden ist. Für die Behandlung stehen folgende Möglichkeiten zur Auswahl: REJECT » E-Mail direkt zurückweisen BOUNCE » Eine Fehler-E-Mail mit Erklärungen an den Absender schicken PASS » E-Mail trotzdem an den Empfänger zustellen DISCARD » E-Mail löschen
Spam-Administrator	E-Mail Adresse für Spam-Warnungen.
Spam-Quarantäne	E-Mail-Adresse für die Zustellung von Spam-E-Mails. Falls leer, werden die Mails in einem lokalen Verzeichnis auf der Festplatte abgelegt.
Banned-Behandlung	Behandlung von Attachments, die nicht erlaubt sind. Für die Behandlung stehen folgende Möglichkeiten zur Auswahl: REJECT » E-Mail direkt zurückweisen BOUNCE » Eine Fehler-E-Mail mit Erklärungen an den Absender schicken PASS » E-Mail trotzdem an den Empfänger zustellen DISCARD » E-Mail löschen
Banned-Administrator	E-Mail Adresse für Warnungen bei verbotenen Attachments.
Banned-Quarantäne	E-Mail Adresse für die Zustellung von verbotenen Attachments. Falls leer, werden die Mails in einem lokalen Verzeichnis auf der Festplatte abgelegt.

2. Auswahl des amavisd-new Filters (Interner Filter)

Bad-Header-Behandlung	Behandlung von defekten Kopfzeilen, die erkannt worden sind. Für die Behandlung stehen folgende Möglichkeiten zur Auswahl: REJECT » E-Mail direkt zurückweisen BOUNCE » Eine Fehler-E-Mail mit Erklärungen an den Absender schicken PASS » E-Mail trotzdem an den Empfänger zustellen DISCARD » E-Mail löschen
Bad-Header-Administrator	E-Mail Adresse für Warnungen von defekten Kopfzeilen.
Bad-Header-Quarantäne	E-Mail Adresse für die Zustellung E-Mails mit defekten Kopfzeilen. Falls leer, werden die Mails in einem lokalen Verzeichnis auf der Festplatte abgelegt.
Lebensdauer Quarantäne in Tagen	Anzahl der Tage, die Viren- und Spam-E-Mails in dem lokalen Verzeichnis aufbewahrt werden sollen. Ist nur relevant, wenn die Quarantäne das lokale Verzeichnis ist.
Weitere-Empfänger-Domänen	Welche weiteren Empfänger-Domänen sollen Spam-Markierungen erhalten. Im Standard-Fall wird nur für E-Mails, die für die Haupt-Domäne bestimmt sind Spam-Markierungen gesetzt. Es können hier weitere Domänen eingetragen werden, die auch durch den Spam-Filter gefiltert werden sollen.
Spam-Betreff	Spam-Markierung, die erkannte Spam-E-Mails bekommen sollen.
Spam-Schwelle 1 / Info-Header*	Anzahl der Punkte, ab denen E-Mails einen zusätzlichen Spam-Header erhalten sollen.
Spam-Schwelle 2 / Betreff*	Anzahl der Punkte, ab denen E-Mails einen Spam-Betreff erhalten sollen.
Spam-Schwelle 3 / Behandlung*	Anzahl der Punkte, ab denen E-Mails nach der eingestellten Spam-Behandlung verwaltet werden.
Spam-Schwelle 4 / Kein Bounce*	Anzahl der Punkte, ab denen die Absender von Spam-E-Mails niemals mehr benachrichtigt werden.

*Die Anzahl der Punkte wird von dem amavisd-new Filter automatisch berechnet. Ein Anhaltspunkt, wie sich die SPAM-Punktbewertung zusammensetzt, kann unter folgender Internetadresse nachgelesen werden. http://spamassassin.apache.org/tests_3_1_x.html¹⁾

ACHTUNG: Wenn Sie alle Einstellungen vorgenommen haben verlassen Sie das Menü. Speichern Sie nun alle Änderungen über den Menüpunkt *Speichern* ab und wenden Sie diese mit dem Menüpunkt *Sanft Anwenden* an. Erst nach dem Anwenden werden die neuen Einstellungen wirksam.

[← Zum Hauptmenü](#)

1)

Die m-privacy GmbH hat auf die dort dargelegten Informationen keinen direkten Einfluss, die Angabe der URL erfolgt lediglich als Hilfe für die Benutzung.

From:
<https://help.m-privacy.de/> -

Permanent link:
https://help.m-privacy.de/doku.php/tightgate-mailserver:dienste:mail_filter

Last update: 2020/09/25 07:58



