# Spamtitan User Guide

Spamtitan ist unsere verwendete Anti-Spam Lösung. Der Zugriff auf das Webinterface erfolgt über https://spamtitan.media-data.at/

## Quarantäne

Hier werden Mails mit Verdacht auf Spam (unerwünschte Nachrichten) festgehalten. Falls eine Mail dabei ist, die jedoch durchgehen sollte kann, man entweder auf „Release“ oder „Allow“ drücken.

„Release“ lässt nur die gewählte(n) Mail(s) durch.

„Allow“ lässt die gewählte(n) Mail(s) und alle zukünftigen Mails von dem Absender durch.
Diese Senderadressen werden dann automatisch in den „Filter Rules“ eingetragen.

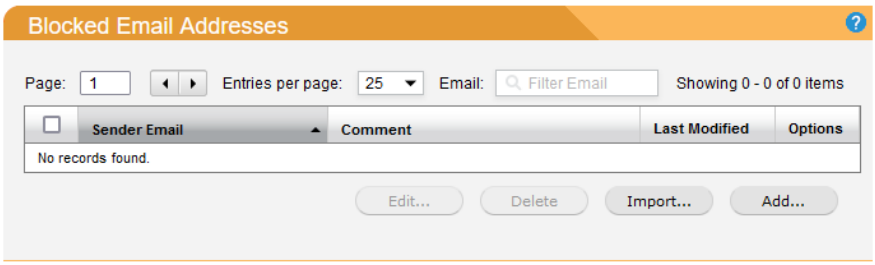
## Filter Rules

### User Block List

HINWEIS: Diese Funktion mit Bedacht verwenden!

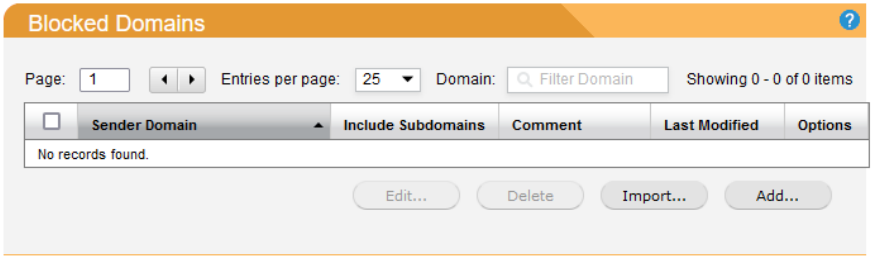
*Jede E-Mail, die blockiert wird, wird weder in der Mailbox noch im Spamtitan angezeigt.*
*Es könnten unbewusst wichtige Mails verloren gehen!*

In den „Blocked Email Addresses“ kann man mit „Add…“ eine Adresse (z.B.: spammer@mail.com) hinzufügen. Von Mailadressen, die dort eingetragen sind, kommen keine Mails mehr.




„User Blocked Domains“ funktioniert genau gleich, nur dass statt einer Senderadresse eine ganze Domain eingetragen und gesperrt wird (z.B.: mail.com -> Alle Mailadressen von dort sind gesperrt)

Beim Eintragen einer Domain kann man Subdomains inkludieren. Das bedeutet nur, dass im Falle eines Blocks von mail.com auch Mails von der Domain kunden.mail.com blockiert werden.




### User Allow List

Alle E-Mails, die von hinterlegten Senderadressen oder Domains gesendet werden, kommen nicht in Quarantäne, sondern sofort in die Mailbox. Diese Option lässt nur Spam-Verdachtsfälle durch, Viren werden regulär abgefangen.

## Settings

### User Management

Hier kann man sein Kennwort ändern und/oder Two-Factor Authentication einstellen.

### Quarantine Report Settings

Hier kann man die Mail-Reports anpassen, die von Spamtitan kommen.

Sollten Sie noch weitere Fragen haben oder Hilfe benötigen, kontaktieren Sie uns einfach: https://www.media-data.at/