

<b>Policies</b> .....	1
<b>Amavis</b> .....	2
Settings.....	2
Tag-Level .....	3
<b>Rspamd</b> .....	5
<b>Default values for spam classification with Amavis</b> .....	6
<b>Default values for spam classification with Rspamd</b> .....	6

## Policies

The policies are used to classify a mail as spam, if necessary. A policy can be used in an **E-Mail Domain** or in an **E-Mail Mailbox** under "Spam filter".

You can set a general spam filter for an email domain and use a different one for individual mailboxes or none at all. The policy of an email account is always used with priority.

In the **Email** section, you can adjust the **policies** under **Spamfilter** or create a new one:

### Spamfilter Policy

Add Policy record

Name	Virus lover	Spam lover	Banned Files lover	Bad Header lover	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Non-paying	No	No	No	No	
Uncensored	Yes	Yes	Yes	Yes	
Wants all spam	No	Yes	No	No	
Wants viruses	Yes	No	Yes	Yes	
Normal	No	No	No	No	

In the following we will take a closer look at the "Normal" policy. The default spam classification values for all policies can be found at the end.

### Spamfilter policy

Policy Amavis Rspamd

Policy Name:

Virus lover:

SPAM lover:

Save Cancel

- **Virus Lover** – defines whether emails with viruses should be delivered or not. The emails will still be scanned for viruses, but the result will be ignored if you set this value to "Yes".
- **SPAM Lover** – determines whether emails detected as spam should be delivered to a mailbox or not. A spam check is always performed, but the result is ignored if you select "Yes" here.

Depending on which **content filter** (Rspamd or Amavis) is used on your server (see System / Server Configuration), the information from the respective tab is used. If you have only one filter active (one server or the same filter on all servers), you will only see the corresponding tab.

## Amavis

The **Settings** and the **Tag-Level** are relevant.

### Settings

Spamfilter policy

Policy
Amavis
Rspamd

Settings

Banned files lover: No
Bad header lover: No
Bypass virus checks: No
Bypass banned checks: No
Bypass header checks: No

Tag-Level

- **Banned files lover** – determines whether certain file types (e.g. .exe) are allowed.
- **Bad header lover** – determines whether emails with false / negative values in the mail header are allowed or not.
- **Bypass virus checks** – Similar to the concept of **Virus Lover**. When this value is active, the virus scan is bypassed completely.
- **Bypass banned checks** – Similar to the concept of **Banned Files Lover**. When this value is active, the check for banned file types is bypassed.
- **Bypass header checks** – Similar to the concept of **Bad Header Lover**. When this value is active, the header check is bypassed.

## Tag-Level

Under **Tag-Level** you define the spam value from which a mail should be classified:

### Spamfilter policy

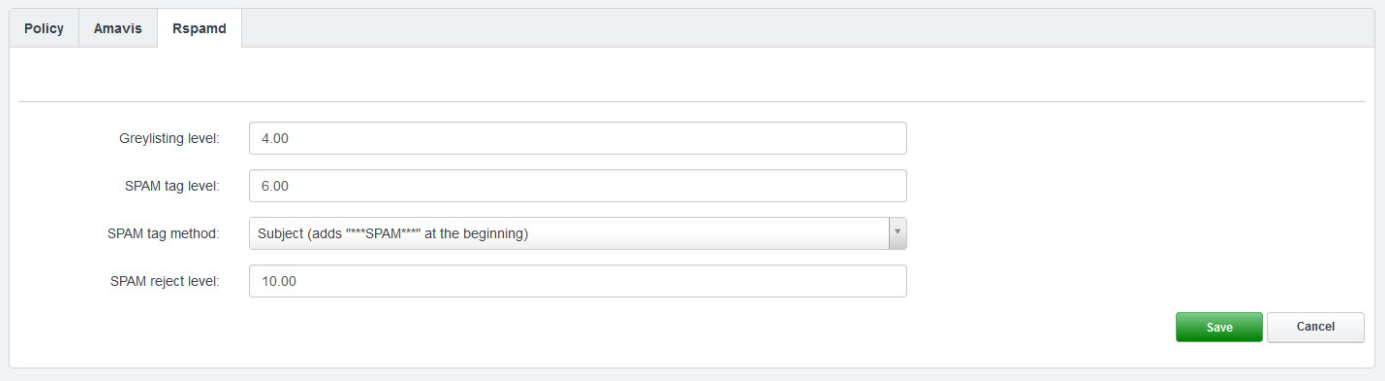
- **SPAM tag level** – The spam check adds spam information headers to the mail when this level is reached or exceeded. The value should be > 0 so that not every mail contains this information. Decimal numbers like 2.4 are possible.
- **SPAM tag2 level** - the system will add the "Spam detected" header at this level. This value should be > than the **SPAM tag level**. Decimal numbers are allowed.
- **SPAM kill level** - from this value the server triggers spam prevention measures (e.g. blocking emails). The value should be >= the **SPAM tag2 level**. Decimal numbers are allowed.  
If the **SPAM kill level** = **SPAM tag2 level**, spam will be blocked and not delivered to the user's mailbox, so in this case it makes no sense to specify a value for **SPAM tag2 level** (see below).
- **SPAM dsn cutoff level** – This is the spam value above which a DSN (Delivery Status Notification) is not sent. Since almost all spam emails have a spoofed sender address, it is questionable whether a DSN should be sent at all. To not send a DSN, enter a low value like 0.
- **SPAM quarantine cutoff level** – the value above which quarantine is disabled. Use a low one such as 0 if you do not want quarantine.
- **SPAM modifies subject** – Select whether the system should add a spam tag to the subject line of the e-mail if it is classified as spam. The spam tag can be entered in the two fields **SPAM subject tag** and **SPAM subject tag2**.

- **SPAM subject tag** – This only applies if the spam rating is  $\geq$  **SPAM tag level**, i.e. if the spam info headers have been added to the email, but it is not sure if it is really spam. Normally you leave this field empty. But you can also enter something like [POSSIBLY SPAM].  
You can also include the spam rating in the subject. For this you use `_SCORE_`, e.g. [POSSIBLY SPAM (`_SCORE_`)]. In the end this would result in something like [POSSIBLY SPAM (Score: 3.1)].
- **SPAM subject tag2** – This is the field that is normally used for tagging spam in the subject line. This value is applied when the spam value is  $\geq$  SPAM tag2 level, i.e. when this email is almost certainly spam. Common strings are [SPAM] or \*\*\*SPAM\*\*\*. The string is prefixed to the subject of the email, e.g. the subject Buy Cialis would become [SPAM] Buy Cialis. Again, you can use `_SCORE_` corresponding to SPAM subject tag. In the end, the result would be something like \*\*\*SPAM (Score: 7.5)\*\*\*.  
Important: If the SPAM tag level = SPAM tag2 level, the spam will be blocked and not delivered to the user's mailbox, so it makes no sense to specify a SPAM tag2 level then.

## Rspamd

If you use Rspamd, only a few values are required:

### Spamfilter policy



The screenshot shows the 'Spamfilter policy' configuration window. It has three tabs: 'Policy', 'Amavis', and 'Rspamd'. The 'Rspamd' tab is selected. Inside the Rspamd tab, there are four configuration fields:

- Greylisting level:** A text input field containing the value '4.00'.
- SPAM tag level:** A text input field containing the value '6.00'.
- SPAM tag method:** A dropdown menu with the selected option 'Subject (adds \*\*\*\*SPAM\*\*\*\* at the beginning)'.
- SPAM reject level:** A text input field containing the value '10.00'.

At the bottom right of the configuration area, there are two buttons: a green 'Save' button and a grey 'Cancel' button.

5

- **Greylisting level** – Rspamd and Amavis check a mail before accepting it from the mail server. If Rspamd detects a spam value that is above this value (decimal numbers like 6.2 are possible), greylisting is triggered. This instructs the delivering mail server to try delivery again later. In some cases, when spam is sent, no further delivery attempt is made.
- **SPAM tag level** – The spam check adds spam information headers to the mail when this level is reached or exceeded. The value should be > 0 so that not every mail contains this information. Decimal numbers like 2.4 are possible.
- **SPAM tag method** – Here you specify where the information with the spam value should be stored: invisibly in the header of the mail or in the subject.
- **SPAM-reject level** – above this spam value, the server refuses to accept the mail.

## Default values for spam classification with Amavis

Richtlinie	Level 1	Level 2	Kill Level	DSN Cutoff	Quarantäne Cutoff
Non-Paying	3.00	7.00	10.00	0.00	0.00
Normal	1.0	4.50	50.00	0.00	0.00
Permissive	3.00	10.00	20.00		
Trigger happy	3.00	5.00	5.00		
Uncensored	3.00	999.00	999.00		
Wants all spam	3.00	999.00	999.00		
Wants viruses	3.00	6.90	6.90		

## Default values for spam classification with Rspamd

Richtlinie	Greylisting-Level	Markierungslevel	Methode	SPAM-Reject-Level
Non-Paying	6.00	8.00	Betreff	12.00
Normal	4.00	6.00	Betreff	10.00
Permissive	7.00	10.00	Betreff	20.00
Trigger happy	2.00	4.00	Betreff	8.00
Uncensored	999.00	999.00	Betreff	999.00
Wants all spam	999.00	999.00	Betreff	999.00
Wants viruses	4.00	6.00	Betreff	10.00