

# Rspamd

Rspamd is used for AV handling, DKIM signing and SPAM handling. It's a powerful and fast filter system. For a more in-depth documentation on Rspamd please visit its [own documentation](#).

## Learn Spam & Ham

Rspamd learns mail as spam or ham when you move a message in or out of the junk folder to any mailbox besides trash. This is achieved by using the Dovecot plugin "antispam" and a simple parser script.

Rspamd also auto-learns mail when a high or low score is detected (see <https://rspamd.com/doc/configuration/statistic.html#autolearning>)

The bayes statistics are written to Redis as keys `BAYES_HAM` and `BAYES_SPAM`.

You can also use Rspamd's web UI to learn ham and / or spam or to adjust certain settings of Rspamd.

## Learn Spam or Ham from existing directory

You can use a one-liner to learn mail in plain-text (uncompressed) format:

```
# Ham
for file in /my/folder/cur/*; do docker exec -i $(docker-compose ps -q rspamd-openemail) rspamc learn_ham < $file; done
# Spam
for file in /my/folder/.Junk/cur/*; do docker exec -i $(docker-compose ps -q rspamd-openemail) rspamc learn_spam < $file; done
```

Consider attaching a local folder as new volume to `rspamd-openemail` in `docker-compose.yml` and learn given files inside the container. This can be used as workaround to parse compressed data with `zcat`. Example:

```
for file in /data/old_mail/.Junk/cur/*; do rspamc learn_spam < zcat $file; done
```

## CLI tools

```
docker-compose exec rspamd-openemail rspamc --help
docker-compose exec rspamd-openemail rspamadm --help
```

## Disable Greylisting

You can disable rspamd's greylisting server-wide by editing:

```
{mailcow-dir}/data/conf/rspamd/local.d/greylist.conf
```

Simply add the line:

```
enabled = false;
```

Save the file and then restart the rspamd container.

See [Rspamd documentation](#)