DKIM signing (Pro)

> **Pro version.** This feature belongs to the Pro version of Mail Log. What the Free version does is described under *Free version and Pro version*.

A DKIM signature is a seal on your outgoing mail: it lets the receiver check that the message really comes from your domain and was not altered on the way. Mail Log can apply that seal — for installations whose sending path does not do it itself.

> **First check whether you need this.** Most mail providers and all sending services already sign. Look at *Domain health*: if a DKIM record is found there, somebody is signing — then leave this feature off. Signing twice is allowed, but it gains nothing and makes the next key change error-prone.

The order is the actual feature

Four steps, and they belong in exactly this order:

1. **Generate the key.** *Options* → *Delivery* → *DKIM signing*. Mail Log generates an RSA key pair (2048 bits) and stores the private part encrypted, as a file below the log directory — never in the database. More on that under *Where the key lives*.
2. **Publish the DNS record.** Below it, what has to be entered appears: a name like `maillog._domainkey.your-domain.com` and a long value starting with `v=DKIM1; k=rsa; p=…`. Type: TXT. You enter that at your domain provider, or forward it to their support.
3. **Have it verified.** The button *Check publication* looks the record up and compares it with the stored key. Only when it says *“matches”* is everything ready. After publishing, this can take up to a day.
4. **Switch it on.** Only now set *Sign outgoing messages* to *Yes*.

DKIM signing

Signs outgoing messages with a key of your own. For installations whose sending path does not do it itself - plain hoster SMTP or PHP mail.

Domain

example.org

Leave empty: the domain of the sender address in the Joomla configuration is used. Fill it in only if you know it has to be a different one.

Selector

maillog

The name the public key is published under in DNS. The default does not disturb an existing selector of your provider - both may stand side by side.

Key

Key present, generated on Sunday, 20 September 2026 23:43. Length: 2048 bits.

This record belongs in DNS

`maillog._domainkey.example.org`

```
v=DKIM1; k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvLiaCxrketjSZ
f2Gdhp7aQ34Sc5H80Rk4yxpURMz9mM9dSvS38gc4RWZeyPdQsjNk5Uku
k3Q4rm8vDcQ3DML7xaFTM+o85kvYCA/foCbGE+ScYiQFvD4UtEVI5qDLD
```

Type TXT. Some interfaces want the value in quotes or split into several parts - both are fine.

Generate a new key

Check publication

The order is fixed: generate the key, publish the DNS record, have it verified - only then switch it on.

Sign outgoing messages

No

Switch this on only after the check above has confirmed the published key. A broken signature is worse than none at all. Do not switch it on if your sending provider already signs.

Why not switch it on right away? A signature whose key cannot be found in DNS is worse than none at all: the receiver then sees a *failed* check instead of no check — and a failed

check is exactly the marker spam filters use to recognise forgeries.

The two fields above

Field	What belongs there
Domain	Leave it empty. Mail Log then takes the domain of the sender address from the Joomla configuration — and that is exactly what the receiver compares against. Entering a different domain produces a valid signature that still does not count for DMARC.
Selector	The name the public key is published under in DNS. `maillog` is the default and does not disturb an existing selector of your provider — several selectors may stand side by side.

Where the key lives

As a file below your Joomla installation's log directory (`…/com_maillog/dkim/`), readable only by the web server user and **encrypted** — with the same method as your stored credentials, derived from the secret in your Joomla configuration.

Why encrypted, when the file is protected anyway? Joomla's default log directory is `administrator/logs` — right inside the web directory. Mail Log puts blocking files there, but those only work on Apache; on an nginx server they do nothing. While checking this version, the key really was retrievable that way on the test instance. Encrypted, it still is — but the content is worthless: without your `configuration.php`, which no web server hands out, it cannot be deciphered.

If your host allows a log directory outside the web directory, that is still the better setting (*System → Global Configuration → Server → Path to Log Folder*).

If your Joomla secret is renewed, the DKIM key can no longer be deciphered. Mail Log then stops signing — silently, and without disturbing the sending. Generate a new key in that case and publish the new DNS record.

> **When moving to another server** the file does not travel automatically if you only transfer the database and the web directory. Either generate a new key in the new place and publish the new record — or copy the file along.

Generating a new key

The button is then called *Generate a new key*, and that is exactly what it does: the old one is gone afterwards. Until the new record is published, every signature fails. The sensible way is therefore a second selector: change the selector (to `maillog2`, say), generate the key, publish the new record, have it verified — and only then delete the old record.

How you can tell it works

- **Domain health** finds the selector and reports the key length.
- In the **DMARC reports** the share of messages that identified themselves via DKIM rises — visible in the *Proof* column of the source list.
- The source of a received message carries a `DKIM-Signature:` header with your domain.

> **What happens if something is missing?** If the key, the domain or the selector is missing, Mail Log does not sign — silently, and the mail goes out as before. A logger must not prevent sending, and that holds for the one feature that reaches into the sending path too.

Deutsche Fassung

Revision #2
Created 2026-09-24 15:31:30 UTC by Norbert Graup
Updated 2026-09-24 15:31:31 UTC by Norbert Graup