# DMARC: who sends in your name (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*.

Every day the large e-mail providers send reports about who has been sending in your name and whether that mail could identify itself as yours. These *DMARC reports* arrive as compressed XML in a mailbox — which is why in practice nobody ever reads them. Mail Log collects them, unpacks them and answers one question from them: **is this still our sending?**

# What a report answers — and what it does not

A report says: “During the day, 42 messages came from this IP address carrying your domain in the sender. 40 of them could identify themselves, 2 could not.” It does *not* say whether the mail was read, and it names no recipients and no subjects — an aggregate report contains figures, not messages.

“Identify itself” means: the message either carried a valid DKIM signature of your domain *or* came from a server your SPF record allows. One of the two is enough. That is why a forwarded message is not a problem: forwarding breaks SPF and leaves the signature intact.

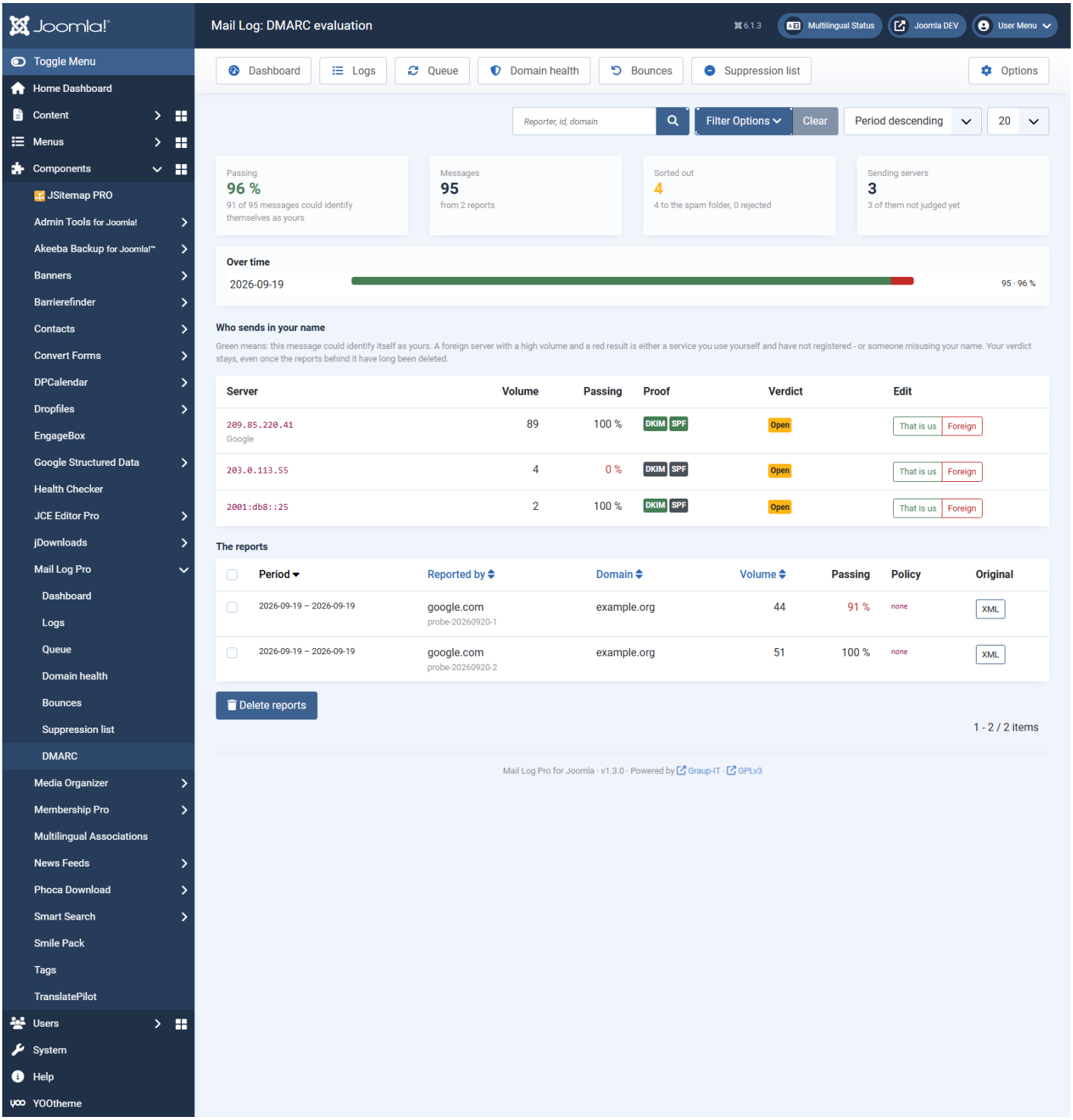
# Setting it up: three steps

1. **Set up the return channel.** The reports arrive in the *same* mailbox as the bounce messages. How to enter it is described in the chapter *Return channel*. Without the mailbox collection nothing arrives.
2. **Publish the report address in DNS.** Your DMARC record has a part for this: `rua=mailto:…`. Here *you* decide where the reports go — unlike the bounce messages, whose address is dictated by the sending path. Enter the address of the mailbox Mail Log collects from. *Domain health* shows you the finished record.

3. **Switch the evaluation on.** *Options → Return channel → DMARC reports → Evaluate reports*.

> **Patience for the first one.** Providers send once a day and report on the previous day. After publishing the DNS record it therefore takes up to two days for the first report to arrive — and only if mail was sent from your domain during that time.

# The *DMARC* screen




The screen reads from top to bottom as one answer in three stages.

# The figures

| Figure | What it says |
|---|---|
| **Passing** | The share of messages that could identify themselves. This is the one number to keep an eye on. |

| Figure | What it says |
| --- | --- |
| **Messages** | How many messages the reports describe in total — not how many reports came in. |
| **Sorted out** | What the receiver put in the spam folder or rejected. A number above zero here means your policy has already taken effect. |
| **Sending servers** | How many different servers sent in your name during the period, and how many of them are still unjudged. |

The share below which the situation counts as noteworthy is set in the options (*Warn below … per cent passing*, 95 by default). A hundred per cent is not a sensible value: one single forwarded message breaks it.

# Who sends in your name

The second list is the actual work. It shows every server that sent mail carrying your domain, with volume, passing share and — where it can be resolved — its name. Mail Log recognises well known sending services and labels them.

Every row gets a verdict from you:

- **That is us** — a server sending on your behalf: your host, your newsletter service, your ticket system.
- **Foreign** — someone using your name without being entitled to.
- **Withdraw** — open again, if you got it wrong.

The verdict is yours and it stays, even once the reports the address came from have long fallen to the retention period.

> **One of your own services with a red share is the most common find.** It almost never means an attack; it means a missing record: the newsletter service is not in your SPF record, or its DKIM key is not published. *Domain health* shows you both, with the finished record to copy.

# The reports

Last comes the list of reports that came in: period, reporter, domain, volume, share and the published policy. *XML* downloads the original document — for the case where a number looks odd

and somebody wants to see what the provider actually wrote.

# What else Mail Log does with the reports

- **Takes over selectors.** A report names the DKIM selector your sending path signs with. Mail Log remembers the ones that demonstrably work and checks them in domain health on its own — you do not have to enter them.
- **In the periodic report.** The share and the number of unjudged sources appear in the weekly or monthly report, if you have switched it on.
- **On the dashboard.** A strip with the share and the open sources.

# Retention

Two periods, because these are two different things: the evaluated *figures* stay for a year by default — that makes the question “was it like this last summer?” answerable. The *original document* stays for three months; it is rarely needed and only for a short while. After that the report stays in the list, only without its attachment. The clean-up is done by the maintenance routine *Clean up old log entries*, which runs anyway.

# When nothing arrives

The screen tells you why — it distinguishes four cases: the evaluation is off, the mailbox collection is off, there is no scheduled task, or the site's task scheduler never runs at all. If no notice is shown and the screen is still empty, check the `rua=` part of your DMARC record: does it really point at the mailbox Mail Log collects from?

> **Reports for other domains.** Mail Log stores every report it finds and names the domain it is about in the list. If a domain appears there that is not yours, somebody has entered your address as their report address — annoying, but harmless. The domain filter hides them.

Deutsche Fassung

---

Revision #2
Created 2026-09-24 15:31:27 UTC by Norbert Graup
Updated 2026-09-24 15:31:28 UTC by Norbert Graup