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.

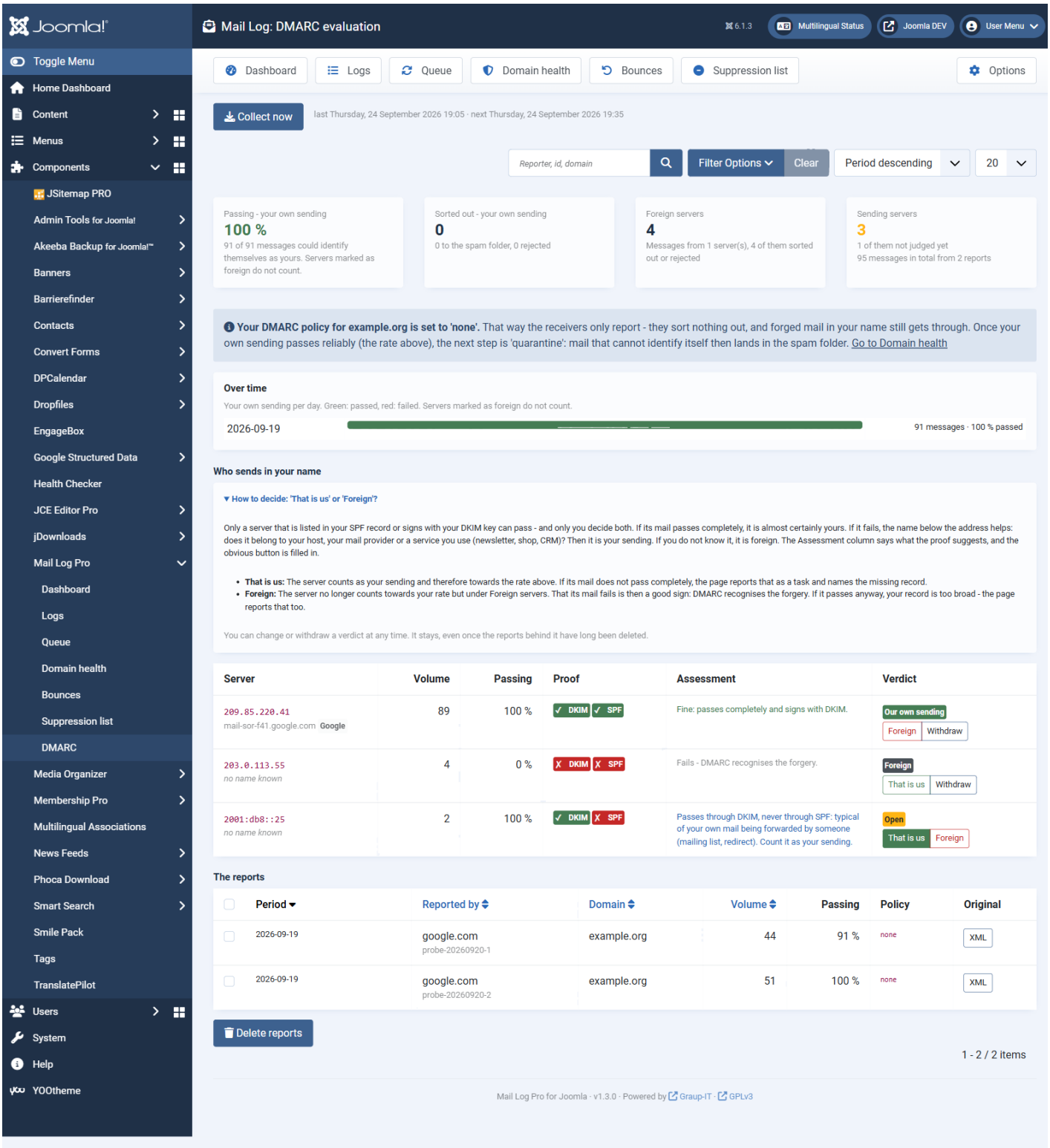
Setting it up: three steps

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. At the very top it says when the mailbox was last collected and when that happens next. **Collect now** picks up new reports straight away, without waiting for the next scheduled run; the page then reloads. The same button is on the *Bounces* screen and in the options: both read the same mailbox in one run.

The figures

Figure	What it says
Passing - your own sending	The share of your own messages that could identify themselves. This is the one number to keep an eye on. Servers you have marked as *foreign* do not count — a forger should not drag your share down.
Sorted out - your own sending	What the receiver put in the spam folder or rejected of your own mail. This should be zero.
Foreign servers	How many messages came from servers you have marked as foreign, and how many of them the receiver sorted out. If that is most of them, your policy is working.
Sending servers	How many different servers sent in your name during the period, how many of them are still unjudged, and how many messages the reports describe in total.

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.

If your policy is still set to `none`, the screen says so in a notice of its own: the receivers then only report and sort nothing out. Once your own sending passes reliably, `quarantine` is the next step — *Domain health* shows the finished record.

Over time shows your own sending per day: green for what passed, red for what did not, with volume and share next to 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. The *Proof* column shows a tick or a cross for DKIM and SPF: passed or not.

Every row gets a verdict from you. **How to tell:** only a server that is listed in your SPF record or signs with your DKIM key can pass — and only you decide both. If its mail passes completely, it is almost certainly yours. If it fails, the name helps: does it belong to your host, your mail provider or a service you use (newsletter, shop, CRM)? Then it is your sending. If you do not know it, it is foreign.

The **Assessment** column does the reading for you: for every server it says what the proof suggests, and the obvious button is filled in. The decision stays with you.

Verdict	What it does
That is us	The server counts as your sending and therefore towards the share. If its mail does not pass completely, a notice appears at the top, and the assessment names the missing record — SPF, DKIM or both.
Foreign	The server no longer counts towards your share but under *Foreign servers*. That its mail fails is then a good sign: DMARC recognises the forgery. If it passes anyway, the screen reports it — your SPF record or your key admits this server, and the record is too broad.
Withdraw	Open again. Open servers count as your sending until you say otherwise — a failing one should stand out, not disappear.

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. Mark it with *That is us*; the assessment then says what is missing, and *Domain health* shows the finished record to copy.

Servers as CSV in the toolbar downloads this list — every server in the chosen period, not just the first fifty the screen shows. Per row: address, reverse name, recognised service, volume, passed, share in per cent, passed via DKIM and via SPF, verdict (`own`, `foreign`, `open`), assessment and last seen (UTC). One row per server, not per report line: the same source appears again in every daily report.

The reports

Last comes the list of reports that came in: period, reporter, domain, volume, share and the published policy — point at it to read what it does. *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.
- The dashboard and the report calculate the share exactly like the screen: over your own sending only, without the servers marked as foreign.

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 #3
Created 2026-09-24 15:31:27 UTC by Norbert Graup
Updated 2026-10-04 10:20:01 UTC by Norbert Graup