How to set up DMARC for Mautic

DMARC ties SPF and DKIM to the From address your contacts actually see, tells mailbox providers what to do with email that fails, and sends you reports about who's sending email using your domain. Gmail, Yahoo and Microsoft all expect it from bulk senders now, so if you send any volume from Mautic it's no longer optional.

The standard was updated in May 2026. RFC 9989 replaced the original RFC 7489, and existing DMARC records keep working. This guide covers what's changed where it affects you.

Before you start

Get SPF and DKIM working first, because DMARC builds on them.

- *How to set up SPF for Mautic*
- *How to set up DKIM for Mautic*

You'll also need access to your DNS, and a mailbox or a DMARC reporting service to receive reports.

How DMARC decides pass or fail

An email passes DMARC when **either** of these is true.

- DKIM passes **and** the DKIM domain matches your From domain
- SPF passes **and** the return path domain matches your From domain

"Matches" is called **alignment**. By default it's relaxed, so subdomains count. A DKIM signature for yourdomain.com aligns with a From address of news@mail.yourdomain.com.

Here's what that looks like for typical Mautic setups.

From address	SPF passed for	DKIM signed by	DMARC
news@yourdomain.com	bounce.yourdomain.com	yourdomain.com	Pass, both aligned
news@yourdomain.com	amazonses.com	yourdomain.com	Pass, DKIM aligned
news@yourdomain.com	yourdomain.com	provider.net	Pass, but fragile if forwarded

DMARC ties SPF and DKIM to the From address your contacts actually see, tells mailbox providers what to do with email that fails, and sends you reports about who's sending email using your domain. Gmail, Yahoo and Microsoft all expect it from bulk senders now, so if you send any volume from Mautic it's no longer optional.

The standard was updated in May 2026. RFC 9989 replaced the original RFC 7489, and existing DMARC records keep working. This guide covers what's changed where it affects you.

Before you start

Get SPF and DKIM working first, because DMARC builds on them.

- *How to set up SPF for Mautic*
- *How to set up DKIM for Mautic*

You'll also need access to your DNS, and a mailbox or a DMARC reporting service to receive reports.

How DMARC decides pass or fail

An email passes DMARC when **either** of these is true.

- DKIM passes **and** the DKIM domain matches your From domain
- SPF passes **and** the return path domain matches your From domain

"Matches" is called **alignment**. By default it's relaxed, so subdomains count. A DKIM signature for yourdomain.com aligns with a From address of news@mail.yourdomain.com.

Here's what that looks like for typical Mautic setups.

From address	SPF passed for	DKIM signed by	DMARC

news@yourdomain.com	bounce.yourdomain.com	yourdomain.com	Pass, both aligned
news@yourdomain.com	amazonses.com	yourdomain.com	Pass, DKIM aligned
news@yourdomain.com	yourdomain.com	provider.net	Pass, but fragile if forwarded
news@yourdomain.com	amazonses.com	provider.net	**Fail**, nothing aligned

Aim for DKIM alignment at the very least, because it survives forwarding.

Step 1. Publish a monitoring record

Create a TXT record with the host or name _dmarc on your sending domain, with this value.

```
v=DMARC1; p=none; rua=mailto:dmarc-reports@yourdomain.com
```

- p=none means "don't change how my email is handled, just send me reports". It's the safe place to start.
- rua is where daily summary reports go.

The reports arrive as zipped XML files, which aren't meant for reading by hand. A DMARC reporting service (there are free tiers and open source options) turns them into something readable. If you send reports to an address on a *different* domain, that domain has to publish a record agreeing to receive them. Reporting services set this up for you.

Step 2. Read the reports for a few weeks

The reports show every server that sent email claiming to be from your domain, and whether it passed. Use them to build a list of everything that sends as you. You'll almost always find something nobody remembered, like an old newsletter tool, the invoicing system or the office scanner!

Step 3. Fix anything legitimate that fails

For each legitimate sender that fails, set up DKIM with your own domain at that service (best), or a custom return path so SPF aligns. In Mautic, also check every From address in use, both the default in **Settings > Configuration > Email Settings** and any override on an email's **Advanced** tab. An email using a different domain will start failing once you tighten the policy.

Step 4. Tighten the policy

Once the reports are clean, move up in stages.

```
v=DMARC1; p=quarantine; rua=mailto:dmarc-reports@yourdomain.com
```

Failing email now goes to spam. Watch the reports for a couple of weeks, then move to the strongest setting.

```
v=DMARC1; p=reject; rua=mailto:dmarc-reports@yourdomain.com
```

Failing email is now refused. At this point nobody can successfully send email pretending to be your exact domain.

What changed in 2026

- **pct is gone.** You might see older guides suggest pct=10 to apply a policy to only part of your email. RFC 9989 removed it (Herr and Levine, 2026).
- **t=y is the new testing switch.** It asks receivers to apply your policy one step softer, so p=reject; t=y is treated like quarantine. Handy for a gentle move to reject.

- **np sets a policy for subdomains that don't exist**, which stops spoofers inventing subdomains like billing.yourdomain.com.

Receivers that haven't updated yet just ignore tags they don't recognise, so it's safe to use them.

Step 5. Check it worked

Send a test email from Mautic to a Gmail address, choose **Show original**, and check DMARC shows **PASS**. Repeat at Outlook.com and Yahoo if you can.

Why some of your own emails fail DMARC

Once your reports start coming in, you'll probably spot some of your own, perfectly good Mautic emails failing, sent from servers you've never heard of. Very often, that's forwarding.

When a contact forwards your email to another mailbox, or it goes out through a mailing list, the email arrives from the forwarding server. SPF fails because that server isn't in your record, and DKIM breaks too if the forwarder changes anything, like adding a footer. With both gone, DMARC fails, even though the email was fine when it left you.

Large mailbox providers use a standard called ARC to see that an email passed authentication before it was forwarded, and they factor that in. You don't need to do anything in Mautic for this.

What you can do is this.

- **Make DKIM as sturdy as possible.** Sign with your own domain and use relaxed/relaxed canonicalisation. DKIM survives simple forwarding much better than SPF.
- **Learn to spot forwarding in your reports.** It usually shows up as small numbers of messages from servers belonging to mailbox

providers, universities or mailing list services, failing SPF but sometimes still passing DKIM. Real spoofing looks different, with lots of messages from servers with no connection to you, failing both.
- **Don't add forwarding servers to your SPF record.** They're not your servers, and adding them would let them send anything as your domain.
- **Don't let forwarding keep you at p=none.** Some forwarded email will always fail, and that's expected.

Tips for Mautic users

- **Consider a subdomain for marketing**, such as news.yourdomain.com. It keeps your marketing reputation separate from staff email and you can give it its own DMARC policy with the sp tag or its own record.
- **There's nothing to switch on inside Mautic.** DMARC lives in your DNS and depends on how your email service authenticates.

Quick checklist

- SPF and DKIM working first
- _dmarc record published, starting at p=none
- Reports going to a mailbox or service you actually look at
- Every legitimate sender aligned, ideally with DKIM
- Gmail test shows DMARC PASS
- A plan for moving to quarantine then reject

Over to you

Where is your domain on the journey from p=none to p=reject? I'd love to hear what you found hiding in your reports!

References

Herr, T. and Levine, J. (eds.) (2026) *Domain-based Message Authentication, Reporting, and Conformance (DMARC)*. RFC 9989. Internet Engineering Task Force. Available at https://www.rfc-editor.org/rfc/rfc9989.html (Accessed 26 October 2026).

Online URL:
https://kb.mautic.org/article/how-to-set-up-dmarc-for-mautic.html