How to set up SPF for Mautic

SPF (Sender Policy Framework) is a DNS record that lists the servers allowed to send email for your domain. When your Mautic email arrives, the receiving mail server checks that list, and if the server that sent it isn't on there, your email looks suspicious. It's usually the first thing to get right, and the thing we see broken most often in our community!

This guide walks you through setting it up for the domain you send Mautic email from. If you want the full technical detail, SPF is defined in RFC 7208.

Before you start

You'll need these.

- Access to the DNS settings for your sending domain (your domain registrar, Cloudflare, or whoever hosts your DNS)
- Admin access to the email service Mautic sends through (Amazon SES, SendGrid, Mailgun, Brevo, your own SMTP server and so on)
- Admin access to Mautic

Step 1. Find out who sends email for your domain

Mautic doesn't send email itself. It hands each message to the email service set up under **Settings > Configuration > Email Settings**, and it's that service whose servers need to be in your SPF record.

Make a list of *everything* that sends email using your domain, not just Mautic. Think about your staff mailboxes (Google Workspace or Microsoft 365), your CRM, helpdesk, invoicing tool and website contact forms. Anything you leave off may start failing.

Step 2. Get the SPF value from your email service

Every email service publishes the bit you need to add, usually an include. Look in their domain authentication or sender setup pages. Some examples look like this.

```
include:amazonses.cominclude:sendgrid.netinclude:mailgun.org
```

Many services also offer a **custom MAIL FROM** or **custom return path** domain (something like bounce.yourdomain.com). Set this up if you can, because it means SPF passes on your own domain, which you'll need for DMARC later.

Step 3. Check whether you already have an SPF record

You can only have **one** SPF record per domain. Two records break SPF completely. Look in your DNS for a TXT record on your domain that starts with v=spf1.

Step 4. Create or update the record

If you don't have one yet, create a TXT record on your domain (the host or name is usually @) with a value like this.

```
v=spf1 include:_spf.google.com include:amazonses.com ~all
```

If you already have one, **add** your email service's include to the existing record, before the ~all or -all at the end. Don't create a second record.

The ending matters.

- ~all says anything not listed probably isn't allowed (known as a soft fail). This is the safest choice for most senders, especially once you have DMARC set up, because DMARC then decides what happens to failing email.
- -all says anything not listed definitely isn't allowed (known as a hard fail). It's stricter, but some mail servers reject on it before checking DKIM and DMARC, which can block legitimate forwarded email. Use it with care.
- **Never** use +all, which lets the whole internet send as you!

Step 5. Check it worked

1. Wait for DNS to update (usually within minutes, but it can take up to 48 hours).
2. Run your domain through an SPF checker, such as the free ones from MXToolbox or dmarcian, and make sure it shows no errors.
3. Send a test email from Mautic to a Gmail address, open the message, choose **Show original** from the three-dot menu and check that SPF shows **PASS**.

For a closer look at the results, see *How to check your email authentication in message headers*.

Common problems

"Too many DNS lookups" or permerror. SPF allows a maximum of ten lookups, and every include counts, including the includes inside other includes (Kitterman, 2014). Remove services you no longer use, or move some of them onto a subdomain such as news.yourdomain.com, which gets its own SPF record.

SPF passes, but for the wrong domain. In Gmail's "Show original", look at

which domain SPF passed for. If it's your email service's domain (like amazonses.com) and not yours, set up the custom return path from Step 2.

Two SPF records. Merge them into one.

Forwarded emails fail SPF. That's normal, because the forwarding server isn't in your record. It's one reason DKIM matters so much (see *How to set up DKIM for Mautic*).

Protect domains that don't send email

For domains you own but never send email from (parked domains, old brands), publish this record so nobody can pretend to send from them.

```
v=spf1 -all
```

Quick checklist

- Only one SPF record on the domain
- Every service that sends as your domain is included, including Mautic's email service
- Ten lookups or fewer
- Ends with ~all or -all
- Custom return path set up at your email service
- Gmail test shows SPF PASS

Over to you

How many includes are hiding in your SPF record right now? I'd love to hear the record-breaking counts people find in the wild, and how you tidied them up, over on the Mautic forum or in Slack.

References

Kitterman, S. (2014) *Sender Policy Framework (SPF) for authorizing use of domains in email, version 1*. RFC 7208. Internet Engineering Task Force. Available at https://www.rfc-editor.org/rfc/rfc7208.html (Accessed 26 October 2026).

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