Why isn’t DKIM enabled automatically?

Email · https://kyzoe.be/en/docs/why-is-dkim-not-enabled-automatically/

Why DKIM cannot always be activated automatically

The control panel can always generate the DKIM key, but it cannot always publish the corresponding DNS record itself. And without that publication, DKIM does nothing. The difference lies in who controls the DNS zone and the outgoing mail flow.

1. The DNS zone is managed externally

DKIM lives in DNS, not on the mail server. The control panel can only write records in zones it manages itself. If your domain's nameservers point to Cloudflare, to your registrar (e.g. Openprovider, Combell, GoDaddy) or to a third-party DNS server, Enhance has no write access there. The key is created and displayed, but you have to copy the record over manually.

This is the most common reason. The hosting is with us, the DNS is not.

2. Email runs through an external provider

If your mail is not sent via our servers but via, for example:

- Microsoft 365 / Exchange Online
- Google Workspace
- Amazon SES
- Mailchimp, Brevo, Mailjet, ActiveCampaign
- a CRM or ERP package that sends mail itself

… then **that** provider signs the emails, not our server. Each provider has its own key pair and its own selector (e.g. `selector1._domainkey` for Microsoft 365, or `s1._domainkey` and `s2._domainkey` in an SES configuration). The DKIM key that our control panel generates is completely separate from this and would verify nothing on those emails.

The panel cannot possibly guess which external services you use, which selectors they use or which keys they expect. Those records must come from that provider's dashboard.

3. Mixed mail flows

In practice, many domains send mail from several sources at once: the contact form on the website via the hosting server, day-to-day correspondence via Microsoft 365, and the newsletter via Mailchimp. Each of those three needs its own DKIM record.

Several DKIM records side by side are not a problem — as long as the selectors differ. But automatic activation cannot assess that situation and would cover at most one of the three. A half-configured setup gives a false sense of security and still results in `dkim=fail` for two of the three mail flows.

4. Existing records and risk of conflict

Some domains already have a DKIM record in place, from an earlier migration or a previous host. Overwriting it automatically could break existing mail flows. For that reason, publication deliberately involves a human check.

5. Delegation and registrar limitations

Some registrars and DNS panels do not allow long TXT values, truncate them above 255 characters, or offer no API that lets an external system create records. Even if the control panel wanted to publish the record, it technically cannot.

When it does happen automatically

DKIM is published automatically when all of the following conditions are met:

- The domain's DNS zone runs on our nameservers and is managed within Enhance;
- Outgoing mail for the domain runs through our mail servers;
- There is no conflicting `_domainkey` record in the zone yet.

In all other cases, the panel generates the key, but you publish the record yourself — or obtain it from the external mail provider.

Rule of thumb

> DKIM belongs to the **sender**, not the **host**.

For each mail flow, ask yourself: *which server actually puts this email onto the internet?* That party supplies the DKIM record. If you send from three systems, you need three records.