

Email-provider change checklist

Use this when adding, replacing or removing an email service. Keep a copy with your current DNS settings and list of sending services.

Print and complete this checklist. Keep it with your DNS settings and sending-service list.

Domain or sending subdomain	Email service
Person making the change	Planned date, time and time zone

Before the change

- ☐ List what the service sends and who manages its account. Include existing services that must keep working, such as mailboxes, invoices and website forms.
- ☐ Check the provider's instructions for the From, envelope-sender (MAIL FROM) and DKIM signing domains used by your account.
- ☐ Save the DNS names, record types, values and TTLs you will change. If you use Emailmetry, also note your current provider selection.
- ☐ Check the proposed SPF record, its includes and lookup count. Keep services still in use authorised and use one SPF TXT record per DNS name.
- ☐ Check DKIM and DMARC settings. DMARC needs a passing SPF or DKIM result that aligns with the domain in the From address.
- ☐ In Emailmetry, update the sending services selected for your domain. Follow any additional DNS instructions from the provider; Emailmetry handles its ongoing SPF address updates.

Be ready to restore the previous settings

- ☐ Confirm you can restore the saved DNS values and provider selection. Decide which problems would require you to reverse the change.
- ☐ Allow for DNS caching when changing or restoring a record. Lowering its TTL does not clear answers already cached under the old TTL.

Where the previous settings are saved

Test your email

After the change

- ☐ Check the published DNS names and values. Note when you checked them and allow for cached answers.
- ☐ Send a test from the new service. Inspect the received message's SPF, DKIM and DMARC results, including which domains they refer to.
- ☐ Test the services you already use, such as your mailbox, invoicing software and website forms.
- ☐ Test any forwarding or mailing lists you use. Check authentication results and where messages arrive; a pass does not guarantee inbox delivery.
- ☐ Check for new failures and review available DMARC reports. If you need to restore the previous settings, test again afterwards.

When removing a service

- ☐ Confirm the service has stopped sending. Check scheduled campaigns, integrations, queued messages and occasional jobs such as monthly statements.
- ☐ Allow for messages still in transit and cached DNS answers before removing the service from SPF. Note when sending stopped.
- ☐ Update your list of services with the final settings, test results and date of the change. Keep a copy of the previous values.

Test results and anything left to check

Reviewed by

Completed date / time / time zone

Reference guidance

[RFC 7208: SPF transitions and authorisation](#)

[RFC 9989: DMARC domain-owner actions](#)

[Cloudflare: DNS time to live \(TTL\)](#)

[Emailmetry: guide to provider changes](#)