sendkit

2026

GUIDE

45

SPF, DKIM, DMARC: The 45-Minute Setup Guide

Copy-paste DNS records for cold email — 2026 edition.

WHY THIS EXISTS

Gmail and Yahoo now require this. 68% of senders still haven't complied.

In February 2024, Gmail and Yahoo announced bulk-sender requirements that, for cold email operators, are non-negotiable. SPF, DKIM, and DMARC are now the price of admission. This guide is the exact 45-minute setup we run for SendKit-connected mailboxes.

What you'll have at the end

- A working SPF record under the 10-DNS-lookup limit.
- A 2048-bit DKIM key validating from your sending domain.
- A DMARC policy that reports failures back to you, with a path to enforcement.
- A validation procedure you can run after every DNS change.
- A recovery playbook for the most common breakage modes.

> **Cost of not doing this**
>
> Senders without SPF + DKIM + DMARC at 5,000+/day get rate-shaped at Gmail. Without DMARC specifically, Gmail can drop your messages with a permerror that produces zero bounce signal — you simply do not arrive.

How long this takes

PHASE	TIME	YOU NEED
SPF publish + validate	8 min	DNS access
DKIM key gen + publish + validate	15 min	Email host admin + DNS access
DMARC publish at p=none	6 min	DNS access
DMARC progression to quarantine/reject	6–8 weeks	Aggregate report monitoring
Validation + smoke test	6 min	mxtoolbox or equivalent

SPF · PART 1 OF 3

Sender Policy Framework

SPF is the IP allowlist. It tells receivers which servers are permitted to send email "From:" your domain. It is the simplest of the three, and the easiest to break by accident.

How SPF works

When a receiver gets your email, it does a DNS TXT lookup on `yourdomain.com` for a record beginning with `v=spf1`. If the sending IP matches one of the allowed mechanisms in that record, SPF passes. If not, SPF fails — and modern receivers treat that as a strong negative signal.

The 10-DNS-lookup limit

SPF caps total DNS lookups at 10 per record. Every `include:` mechanism counts. Going over produces a `permerror`, and Gmail treats `permerror` as if SPF were failing — your messages disappear with no bounce trail. This is the most common silent SPF failure we see.

> **How to count lookups**
>
> Use a checker like `dmarcian.com/spf-survey/` or `mxtoolbox.com/spf.aspx`. Most include-chains hide nested lookups — `include:_spf.google.com` alone consumes 4 of your 10.

Pre-built SPF records

GOOGLE WORKSPACE ONLY

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

MICROSOFT 365 ONLY

```
v=spf1 include:spf.protection.outlook.com ~all
```

GOOGLE WORKSPACE + SENDKIT (SENDING SUBDOMAIN)

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

M365 + MAILGUN

```
v=spf1 include:spf.protection.outlook.com include:mailgun.org ~all
```

M365 + SENDGRID

```
v=spf1 include:spf.protection.outlook.com include:sendgrid.net ~all
```

~all vs -all

- `~all` — soft-fail. Receivers may treat unauthorized senders as suspicious but won't reject outright. **Recommended for cold email.**
- `-all` — hard-fail. Receivers should reject unauthorized senders. Use only after a clean 30-day audit window with `~all` and DMARC reporting confirms zero legitimate sources are missing from your record.

Validation

1. Run `dig TXT yourdomain.com +short` and confirm the SPF record returns.
2. Validate at `mxtoolbox.com/spf.aspx` — confirm lookup count < 10 and no syntax errors.
3. Send one test email to a Gmail account. Open the message, click "Show original," confirm `SPF: PASS`.

> **Done when**
>
> mxtoolbox shows green, and a Gmail "Show original" view of a real email displays `spf=pass`.

DKIM · PART 2 OF 3

DomainKeys Identified Mail

DKIM is the cryptographic signature. It tells receivers "this email was actually authored by someone with the private key for this domain." It is the strongest of the three signals when set up correctly.

How DKIM works

Your email host signs every outgoing message with a private key. The matching public key is published as a DNS TXT record at `<selector>._domainkey.yourdomain.com`. Receivers fetch the public key, verify the signature against the message body, and treat a passing signature as authoritative proof of origin.

2048-bit recommended, 1024-bit minimum

Google's current sender guidelines require **DKIM keys of 1024 bits or longer** for sending to personal Gmail accounts, with **2048-bit recommended** as longer keys are more secure. There is no hard 1024-bit deprecation as of writing — but if you're generating a key today, generate at 2048-bit. The DNS-record size difference is trivial; the security and forward-compatibility benefit is real.

> **If you're mid-migration to 2048-bit**
>
> Most providers (Workspace, M365, Mailgun, Sendgrid) support running 1024 and 2048-bit keys side-by-side using a different selector for each. Publish the new 2048 selector first, verify it's passing for ~48 hours, then retire the 1024 selector. Avoid the "delete then create" pattern — leaves a window with no signing key.

Walkthrough — Google Workspace

1. Admin Console → Apps → Google Workspace → Gmail → Authenticate email.
2. Select your sending domain (or subdomain).
3. Click **Generate New Record**. In the dialog, choose `2048-bit` and the selector `google` (or anything else, but match it on DNS).
4. Copy the TXT record name and value.
5. In your DNS, create a TXT record at `google._domainkey.yourdomain.com` with the long value.
6. Wait 5–10 minutes for propagation.
7. Back in Workspace admin, click **Start Authentication**.

Walkthrough — Microsoft 365

1. Microsoft 365 Defender → Email & collaboration → Policies → DKIM.
2. Select your domain → click **Create DKIM keys**.
3. M365 returns two CNAME records: `selector1._domainkey` and `selector2._domainkey`.
4. Publish both as CNAMEs in your DNS, pointing to the M365 targets shown.

5. Wait for propagation, then return to the DKIM page and toggle **Sign messages for this domain with DKIM signatures** to On.

Walkthrough — Mailgun

1. Mailgun → Sending → Domain settings → DNS records.
2. Mailgun shows the DKIM TXT record (selector usually `pic._domainkey` or `mailo._domainkey`).
3. Publish the TXT record exactly as shown — single string, no line breaks.
4. Click **Verify DNS Settings** in Mailgun.

Walkthrough — SendGrid

1. SendGrid → Settings → Sender Authentication → Authenticate Your Domain.
2. Choose your DNS host. SendGrid generates 3 CNAME records.
3. Publish all three CNAMEs at the names shown.
4. Click **Verify**.

Validation

1. Run `dig TXT <selector>._domainkey.yourdomain.com +short` and confirm the public key returns.
2. Send a test email to a Gmail account, click "Show original," confirm `DKIM: PASS` with `domain=yourdomain.com`.
3. Run mxtoolbox's `dkim:<selector>` lookup to confirm the key is well-formed.

> **The "domain mismatch" trap**
>
> "DKIM PASS" alone is not enough — DMARC requires DKIM **alignment**. The signing domain (`d=` in the DKIM-Signature header) must match the visible `From:` domain. If you sign with `d=mailgun.org` while sending `From: hello@yourdomain.com`, DMARC will fail. Always sign with your own domain.

DMARC · PART 3 OF 3

Domain-based Message Authentication, Reporting & Conformance

DMARC ties SPF and DKIM together. It tells receivers what to do when authentication fails, and asks them to send you reports about every message claiming to be from your domain. It is the most powerful and the most easily misconfigured of the three.

How DMARC works

DMARC is a TXT record at `_dmarc.yourdomain.com`. It contains a policy (`p=none`, `p=quarantine`, or `p=reject`) and a reporting address. Receivers send aggregate XML reports daily to that address, summarizing every message they saw claiming to be from your domain — pass or fail.

The three policy modes

POLICY	RECEIVER BEHAVIOR ON FAIL	WHEN TO USE
p=none	Deliver as normal, send report	Weeks 1–2. Establish baseline. Required starting point.
p=quarantine	Move to spam folder	Weeks 3–6. After confirming zero false-positives in reports.
p=reject	Reject outright. No bounce.	Week 7+. Only if reports show 100% legitimate alignment.

Starter record (week 1)

```
v=DMARC1; p=none; rua=mailto:dmarc-reports@yourdomain.com; ruf=mailto:dmarc-reports@yourdomain.com; fo=1; aspf=r; adkim=r
```

- `p=none` — observe only, don't enforce.
- `rua=` — daily aggregate reports (volume, pass/fail).
- `ruf=` — per-message failure reports (verbose; expect ~zero from cold email if config is right).
- `fo=1` — generate a failure report whenever any auth fails.
- `aspf=r` / `adkim=r` — relaxed alignment (allows subdomain sends).

The 8-week progression plan

1. **Week 1 — Publish.** Push the `p=none` record. Set up an inbox or DMARC service to ingest reports.
2. **Week 2 — Read reports.** Identify every IP/source claiming to send from your domain. Anything that fails alignment is either a forgotten legitimate sender (e.g. an HR tool) or spoofing.
3. **Week 3 — Fix legitimate sources.** Update SPF includes for any tool you forgot. Re-enable DKIM signing where missing.
4. **Week 4 — Confirm green reports.** Two consecutive weeks where 100% of legitimate sources align passes.
5. **Week 5 — Move to `p=quarantine`** with `pct=10` (apply the policy to 10% of failing mail).

6. **Week 6 — Ramp pct.** Move pct from 10 → 25 → 50 → 100 across the week, watching reports.
7. **Week 7 — Move to `p=reject`** with `pct=10`.
8. **Week 8 — Ramp to `p=reject; pct=100`.**

> **How SendKit handles this**
>
> SendKit publishes `p=none` automatically on connect, ingests aggregate reports, and surfaces alignment failures in your dashboard. The 8-week progression is a one-click ramp once your sources are clean.

Validation

1. Run `dig TXT _dmarc.yourdomain.com +short`.
2. Validate at `dmarcian.com/dmarc-inspector/`.
3. Send a test to Gmail. In "Show original," confirm `DMARC: PASS`.

VALIDATION

Smoke test in 6 minutes

After every DNS change, run this. It catches 90% of the silent failures.

1. **1. dig sweep.** `dig TXT yourdomain.com +short`, `dig TXT <selector>._domainkey.yourdomain.com +short`, `dig TXT _dmarc.yourdomain.com +short`. All three must return.
2. **2. mxtoolbox.** Run `superTool` on `yourdomain.com`. SPF green, DMARC green, no errors.
3. **3. Gmail roundtrip.** Send a real email to a Gmail account. "Show original" → all three must show PASS.
4. **4. Outlook roundtrip.** Send to an Outlook.com account. View source → confirm `Authentication-Results` header shows all three pass.
5. **5. Google Postmaster.** Add `yourdomain.com` to `postmaster.google.com`. Check the Authentication tab the next day — should show > 95% authenticated.
6. **6. Microsoft SNDS.** Add the sending IP to `sendersupport.olc.protection.outlook.com/snds/`. Within 7 days, the data tab should populate with reputation signals.

> **If SPF passes but DMARC fails**
>
> You almost certainly have an alignment problem — DMARC requires the `From:` domain to align with either the SPF `MailFrom` domain OR the DKIM `d=` domain. The most common cause is a third-party sender (Mailgun, Sendgrid) signing with their own domain. Re-configure to sign with yours.

RECOVERY

Common breakage modes

These are the issues we see most often when an existing setup goes red. Each has a fast diagnostic and a known fix.

SPF permerror — too many DNS lookups

- **Diagnose:** mxtoolbox shows lookup count > 10.
- **Fix:** Flatten the SPF record. Replace nested `include:` chains with the IPs they resolve to (use a flattening service if the source ESP changes IPs frequently). Or remove unused includes.

DKIM signature appears but DMARC fails

- **Diagnose:** `Show original` shows `dkim=pass` but `dmarc=fail`.
- **Fix:** Alignment problem. The DKIM `d=` domain doesn't match the visible `From:` domain. Re-configure your sender to sign with your domain, not the ESP's.

DMARC reports stop arriving

- **Diagnose:** No reports in the inbox after 48 hours.
- **Fix:** Verify the `rua=` mailto address actually receives mail (someone may have forgotten to provision the inbox). Confirm DMARC TXT record syntax with `dmarcian.com/dmarc-inspector/`.

New mailbox not signing with DKIM

- **Diagnose:** `Show original` shows no DKIM-Signature header.
- **Fix:** Most common cause is the email host hasn't finished provisioning the new mailbox onto the existing DKIM key. Wait 30 minutes, retest. If still missing, regenerate the DKIM key in the host admin panel.

CLOSING

Authentication is a one-time setup, then a maintenance habit.

Run the smoke test monthly. The records do not drift on their own — but DNS providers do migrate, ESPs do change includes, and someone on your team will eventually re-configure something.

Get started in SendKit

Connect a mailbox to SendKit. SPF, DKIM (2048-bit), and DMARC publish automatically. DNS drift is checked every 4 hours, and broken records get paged before sends start failing. → sendkit.ai

SOURCES

Sources & references.

Every requirement and threshold in this guide is sourced from official documentation or RFC specifications.

01 Email sender guidelines (Google Workspace Admin Help) — official Gmail bulk-sender requirements effective Feb 1, 2024
Google · 2024
https://support.google.com/a/answer/81126?hl=en

02 An Overview of Bulk Sender Changes at Yahoo / Gmail
AWS Messaging & Targeting Blog · Updated Feb 27, 2024
https://aws.amazon.com/blogs/messaging-and-targeting/an-overview-of-bulk-sender-changes-at-yahoo-gmail/

03 Enhancing email compliance: A guide to the 2024 Gmail and Yahoo changes
Mailgun (Sinch) · 2024
https://help.mailgun.com/hc/en-us/articles/20263554449179

04 February 2024 New Gmail Guidelines — operator-perspective summary
Woodpecker · 2024
https://woodpecker.co/blog/gmail-rules-changes-february-2024/

05 RFC 7208 — Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1
IETF · April 2014
https://tools.ietf.org/html/rfc7208

06 SPF PermError: Too Many DNS Lookups — explains the 10-DNS-lookup limit per RFC 7208
DMARCLY · 2024
https://dmarcly.com/blog/spf-permerror-too-many-dns-lookups-when-spf-record-exceeds-10-dns-lookup-limit

07 RFC 8058 — Signaling One-Click Functionality for List Email Headers
IETF · February 2017
https://tools.ietf.org/html/rfc8058

08 RFC 6376 — DomainKeys Identified Mail (DKIM) Signatures
IETF · September 2011
https://tools.ietf.org/html/rfc6376

09 RFC 7489 — Domain-based Message Authentication, Reporting, and Conformance (DMARC)
IETF · March 2015
https://tools.ietf.org/html/rfc7489