[REDACT]LABS

RESOURCE / 01

EMAIL AUTHENTICATION

DMARC Configuration Guide for Canadian SMBs

A practical setup walkthrough for Microsoft 365 and Google Workspace, covering SPF, DKIM, and DMARC alignment with deliverability in mind.

TORONTO, ON / 2026

redactlabs.ca

Why DMARC matters

If your organization sends email — and every organization does — your domain is being abused for phishing whether you know it or not. Attackers spoof your sending address to attack your customers, your suppliers, your donors, and your staff.

DMARC (Domain-based Message Authentication, Reporting, and Conformance) is the email-authentication standard that lets you tell receiving mail servers what to do with messages that claim to be from your domain but cannot be cryptographically verified. Properly configured, DMARC blocks domain spoofing at the recipient's mail server before the message reaches an inbox.

DMARC works with two older standards:

- SPF (Sender Policy Framework) publishes which IP addresses are authorized to send email for your domain.
- DKIM (DomainKeys Identified Mail) cryptographically signs outgoing messages with a private key, allowing receivers to verify authenticity using the public key in your DNS.
- DMARC ties SPF and DKIM together via "alignment" rules and tells receivers what to do when a message fails: do nothing, quarantine to spam, or reject outright.

> PLAIN ENGLISH
>
> SPF says "these servers can send for me." DKIM says "I signed this message." DMARC says "if neither matches the From: domain, here is what to do — and email me a daily report."

Deployment order

The most common DMARC mistake is publishing a strict policy before authentication is solid. This breaks legitimate mail. The correct order is:

1. Inventory every system that sends mail as your domain. Microsoft 365 / Google Workspace, marketing platforms (Mailchimp, Kit), CRMs (Salesforce, HubSpot), payroll, ticketing, e-signature tools, monitoring alerts, custom applications.
2. Configure SPF to authorize all those senders.
3. Configure DKIM for your primary mail provider and any third-party senders that support it.
4. Publish DMARC at `p=none` with reporting enabled. Collect data for 4 to 8 weeks. This is monitoring mode — no email is blocked.
5. Analyze the DMARC reports. Identify any legitimate sender failing authentication. Fix configurations.
6. Move to `p=quarantine` with a small percentage (`pct=10`), then ramp to 100%.
7. Move to `p=reject` once every legitimate sender is properly authenticated.

Typical timeline

For a 50-person organization with a few third-party senders, expect 8 to 12 weeks from first SPF record to `p=reject` . Rushing this process is the single biggest cause of email-deliverability incidents.

Step 1: SPF configuration

Your SPF record is a TXT record at the root of your domain listing which mail servers are authorized to send mail as your domain.

Microsoft 365

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

Google Workspace

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

Multiple senders

```
v=spf1 include:spf.protection.outlook.com include:servers.mcsv.net include:mail.kit.com
-all
```

The 10 lookup limit

SPF has a hard 10-DNS-lookup limit per evaluation. Each `include:` typically counts as one lookup, but those records may themselves contain includes. Exceeding the limit causes SPF to return permerror, which fails authentication.

Tools like dmarcian.com/spf-survey count your effective lookups. If you are over 10, options include consolidating senders, using SPF flattening services, or accepting that SPF fails for some senders if DKIM is solid.

> ALL VS. SOFTFAIL
>
> The trailing mechanism — `-all` (hard fail) or `~all` (soft fail) — tells receivers what to do with unauthorized IPs. For DMARC, both work; receivers use DMARC policy to decide action. Use `~all` during deployment.

Step 2: DKIM configuration

DKIM signs each outbound message with a cryptographic signature. The receiving server fetches your public key from DNS and verifies.

Microsoft 365

Microsoft 365 publishes two CNAME records pointing to Microsoft's DKIM infrastructure. After both CNAMEs resolve, enable DKIM signing in Microsoft Defender → Email & collaboration → Policies & rules → Threat policies → Email authentication settings → DKIM.

Google Workspace

In the Admin Console: Apps → Google Workspace → Gmail → Authenticate email. Generate a 2048-bit DKIM key. Google provides a TXT record to publish at `google._domainkey.yourdomain.com`. After publishing, return to the console and click "Start authentication."

Third-party senders

Every reputable third-party sender provides DKIM setup instructions. The pattern is identical: they generate a public key, you publish it as a TXT or CNAME at a vendor-specified selector under `_domainkey`, and they begin signing on your behalf.

Step 3: DMARC record

The DMARC record is a TXT record at `_dmarc.yourdomain.com`. Start in monitoring mode:

```
_dmarc.yourdomain.com IN TXT "v=DMARC1; p=none; rua=mailto:dmarc@yourdomain.com; fo=1;
adkim=r; aspf=r"
```

Tag-by-tag

- v=DMARC1 — required version identifier.
- p=none — policy. Options: `none` (monitor only), `quarantine` (send to spam), `reject` (block).
- rua — aggregate report email. Receivers send daily XML summaries.
- ruf — forensic report email. Many receivers do not send these; do not depend on them.
- fo=1 — generate forensic reports for any failure.
- adkim / aspf — alignment mode. `r` relaxed (subdomain matches parent), `s` strict.
- pct=N — apply policy to N% of failing mail. Use during ramp.
- sp= — subdomain policy override.

Aggregate reports

The `rua` address receives daily XML reports from major receivers. Reading raw XML is unpleasant. Use a DMARC aggregator (Postmark's free DMARC Digest, dmarcian, EasyDMARC, Cloudflare's Email Security Insights) to ingest reports and produce a human-readable dashboard.

Common mistakes

Publishing reject before monitoring

The most damaging mistake. Always start at `p=none`, monitor for at least 4 weeks, then ramp.

Forgetting low-volume senders

Payroll, e-signature, monitoring alerts, and one-off transactional senders often get missed during inventory and start failing once policy enforces. DMARC reports surface them — that is what monitoring mode is for.

SPF lookup overflow

Each `include:` burns lookups, and chains of includes can silently push you over 10. `permerror` means DMARC sees SPF as failing.

Forwarded mail breaks SPF

When mail is forwarded (mailing lists, alumni redirects), the forwarding server's IP is what the receiver sees — and it will not be in your SPF record. DKIM survives forwarding, which is why DKIM is the primary authentication signal for DMARC alignment in practice.

Mismatched From: domain

DMARC alignment is checked against the visible `From:` header. If you send "from" `marketing.yourdomain.com` via Mailchimp but Mailchimp signs with a Mailchimp domain, alignment fails. Fix by using a custom DKIM key tied to your domain.

Verification

Quick command-line verification

```
dig +short TXT yourdomain.com
dig +short TXT selector1._domainkey.yourdomain.com
dig +short TXT _dmarc.yourdomain.com
```

Web-based checkers

- mxtoolbox.com/SuperTool.aspx — comprehensive DNS and email diagnostics.
- dmarcian.com/dmarc-inspector — DMARC record parser.
- mail-tester.com — send a test email, get a deliverability score.
- aboutmy.email — passes a real test message through Gmail.

Ongoing monitoring

DMARC is not set-and-forget. New senders get added, vendors change infrastructure, SPF lookup counts drift. Review reports at least monthly. Add a quarterly DMARC posture check to your IT runbook.

> A STARTING CHECKLIST
>
> If you do nothing else: (1) publish SPF for your primary mail provider, (2) enable DKIM for that provider, (3) publish DMARC at `p=none` with a `rua` address pointing at a free aggregator. That setup alone catches 80% of phishing-of-your-domain attempts at the receiver.

Sources

- RFC 7208 — Sender Policy Framework (SPF), Version 1.
- RFC 6376 — DomainKeys Identified Mail (DKIM) Signatures.
- RFC 7489 — Domain-based Message Authentication, Reporting, and Conformance.
- Microsoft Learn — DKIM and DMARC documentation for Microsoft 365.
- Google Workspace Admin Help — SPF, DKIM, DMARC documentation.
- M3AAWG — Email Authentication Recommended Best Practices.

Need help? DMARC deployment is a standard fixed-fee engagement. We run the inventory, publish the records, monitor reports, and walk your domain through to `p=reject` with no deliverability incidents. Typical engagement: 6 to 10 weeks. Email contact@redactlabs.ca.