Why Am I Receiving DMARC Report Emails?

After transitioning to Muse, you may notice a surge of automated emails arriving daily with XML file attachments and subjects like "Report Domain" or "DMARC Aggregate Report." **These emails are safe and expected.** This article explains what they are, why they appeared, and how to get them out of your inbox.

> **Note:** *These emails do not contain spam, phishing attempts, or any personal or member data. No action is required on your part beyond redirecting where the reports are delivered.*

What Are DMARC Reports?

DMARC (Domain-based Message Authentication, Reporting & Conformance) is an email security standard that helps protect your domain from being spoofed — meaning it prevents bad actors from sending fake emails that appear to come from your organization.

As part of how DMARC works, major email providers — including Google, Yahoo, and Microsoft — automatically send daily "report cards" to a designated address on your domain. Each report summarizes:

- What email traffic those providers saw using your domain name
- Whether that traffic passed authentication checks (SPF and DKIM)
- Any suspicious or failed attempts to use your domain

The reports arrive as XML file attachments. They are not meant to be opened or read directly — they are machine-readable data files intended for security monitoring tools, not a personal inbox.

Why Did This Start After Switching to Muse?

When your organization transitioned to Muse, your domain's email settings (DNS records) were reconfigured as part of the platform setup. During that process, an email address — likely yours or a general staff address — was set as the recipient for these automated DMARC reports.

Because each major mail provider sends its own report independently, a single domain can receive dozens of these emails per day. The volume is normal and reflects how widely your domain's email is monitored across the internet.

> **Why so many?** *Every large mail provider (Gmail, Yahoo, Outlook, etc.) sends a separate daily report. If your domain sends email to a wide audience, you may receive reports from 20+ providers every day.*

What Should I Do?

You do not need to read or act on these reports day-to-day. The best solution is to redirect them away from your personal inbox. There are two recommended approaches:

Option 1: Redirect to a Dedicated Email Address

Have your IT team or domain administrator update the DMARC record in your DNS settings to point the report delivery (the "rua" tag) to a dedicated mailbox — such as dmarc-reports@yourorganization.org — that doesn't clutter an active inbox.

Option 2: Use a DMARC Monitoring Tool

Several free and low-cost tools can receive, parse, and visualize these reports in a useful dashboard rather than raw XML files. Options include:

- **Postmark's DMARC Digests** (free) — dmarc.postmarkapp.com
- **Dmarcian** — dmarcian.com
- **Google Postmaster Tools** (if your organization uses Google Workspace) — postmaster.google.com

Is There Anything to Worry About?

No. To recap:

- **These emails are safe** — not spam, not phishing.
- **The attachments are harmless XML data files** — they contain no personal or member information.
- **The volume is normal** — each mail provider sends its own report separately.
- **No day-to-day action is needed** — the reports only become useful when reviewed in aggregate by a monitoring tool.

Still have questions? *Reach out to your Muse support representative or submit a ticket through the Help Center.*