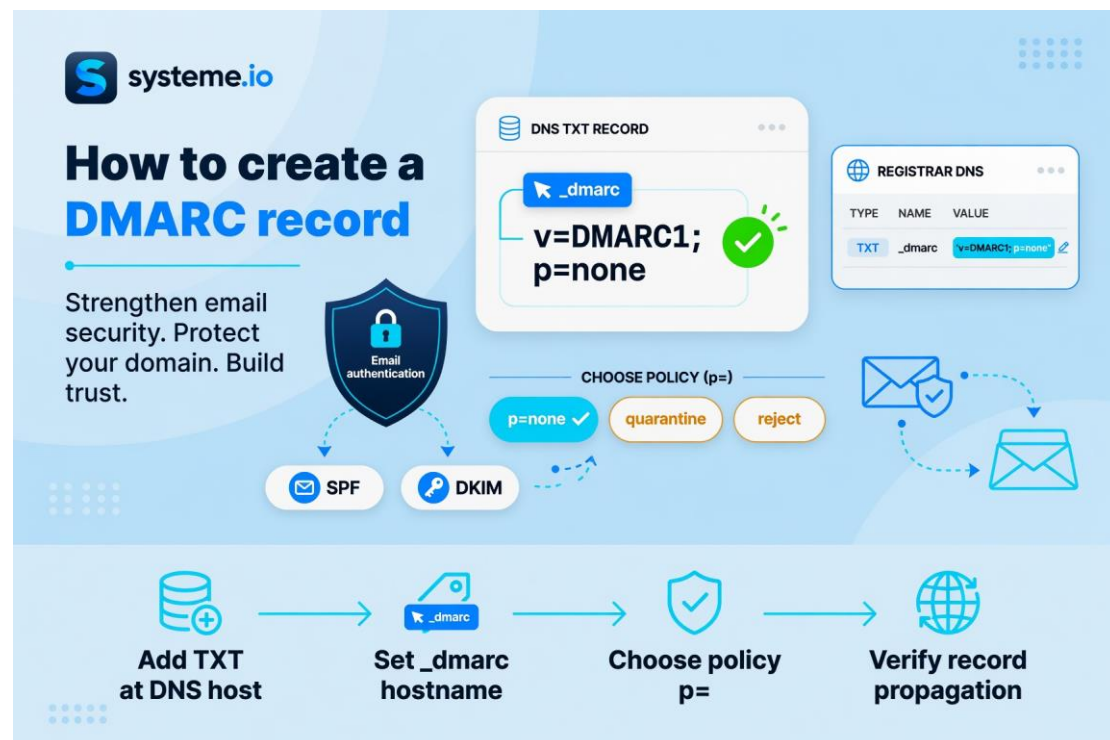


How to Create a DMARC Record

Introduction

SPF and DKIM prove who may send mail for your domain—but **DMARC** ties them together and tells inbox providers what to do when authentication fails. For marketers on systeme.io, a correct DMARC record is part of **domain authentication** alongside the three CNAME records generated in Settings → Emails.

This guide explains what DMARC does, how to create a **TEXT** record at `_dmarc`, which policy to start with (`p=none`), and how to verify propagation before your domain moves from Pending to authenticated.



What Is DMARC?

DMARC (Domain-based Message Authentication, Reporting, and Conformance) is published as a single **TEXT** DNS record. Receiving servers use it to:

- Check whether incoming mail **aligns** with your SPF and DKIM policies.
- Apply a **policy** (`p=`) when messages fail—monitor only, quarantine, or reject.

- Send **aggregate reports** (rua=) so you can see who sends on behalf of your domain.

For systeme.io senders, DMARC is not an optional “nice to have”—it completes the authentication stack expected when you authenticate your domain for email sending.

Where DMARC Fits in systeme.io Setup

Typical order of operations:

1. Add your domain in **Settings** → **Emails** and save to generate DNS values.
2. Add **three CNAME records** at your DNS host.
3. Add **one DMARC TXT record** (this article).
4. Wait for verification; confirm your **sender email address**.

systeme.io may show a DMARC TXT value in the DNS list (eye icon). You can copy that value or build a standard p=none record as described below. Full CNAME steps are in [How to Authenticate Your Domain Name for Email Sending](#).

Important

You must have **only one DMARC record** in your DNS zone. Multiple DMARC TXT entries cause validation failures.

DMARC Record Structure

A beginner-friendly DMARC record includes three essential tags:

- **v=DMARC1** — version; must appear first.
- **p=none** — policy “none” (monitor only; do not quarantine or reject failing mail yet).
- **rua=mailto:youraddress@yourdomain.com** — where aggregate reports are sent (use an address you monitor on your domain).

Example value:

v=DMARC1; p=none; rua=mailto:youraddress@yourdomain.com

If your mailbox is example@example.com, use:

v=DMARC1; p=none; rua=mailto:example@example.com

Use **semicolons** between tags, not colons. Typos in `v=DMARC1` or tag order are a common reason external checkers report “no DMARC found.”

Step-by-Step: Create the TXT Record

1. **Log in** to your domain registrar or DNS provider (Namecheap, GoDaddy, Cloudflare, Hostinger, IONOS, LWS, etc.).
2. Open **DNS settings** or the **DNS zone** for your domain.
3. Start **Add record** and choose type **TXT**.
4. In **Host** or **Name**, enter **_dmarc**. Many hosts append your domain automatically so the full name becomes `_dmarc.yourdomain.com`. If not, enter `_dmarc.yourdomain.com` explicitly.
5. In **Value** or **TXT value**, paste your DMARC string (from systeme.io or the example above with your real mailbox).
6. **Save** the record.

On Cloudflare, email-related records should use **DNS only** (gray cloud) when applicable—proxied records can interfere with mail authentication.

Understanding Policy: none, quarantine, reject

| Policy | Behavior | |-----|-----| | **p=none** | Monitoring only—failed mail is not blocked by DMARC policy. Recommended when starting and when completing systeme.io authentication. | | **p=quarantine** | Failed mail may be sent to spam/junk. Use only after reviewing reports and confirming all legitimate senders pass SPF/DKIM. | | **p=reject** | Failed mail may be rejected. Strongest; risky if marketing tools or forwarders are not aligned. |

systeme.io’s help material for creating a DMARC record focuses on **p=none** so you can authenticate and send while collecting data. Moving to quarantine or reject is an advanced step after weeks of clean reports—not required on day one.

Tip

A “yellow” or warning indicator in some checkers often simply means you use `p=none` rather than quarantine/reject—that is normal for monitoring mode.

Verify Your DMARC Record

DNS changes can take minutes to 48 hours to propagate globally.

- Return to **Settings** → **Emails** on systeme.io and check whether domain status leaves **Pending**.
- Use a public **DMARC lookup** tool (for example MXToolbox DMARC checker) and search your root domain.
- Confirm exactly **one** TXT answer at `_dmarc.yourdomain.com`.

If CNAMEs verify but DMARC does not, re-open your DNS zone and remove duplicate or conflicting TXT records at `_dmarc`.

Troubleshooting

Issue	Possible Cause	Recommended Solution
No DMARC record found	Record not saved or wrong host	Use <code>_dmarc</code> or full <code>_dmarc.domain.com</code> per host rules; wait for propagation.
Multiple DMARC records	Old TXT left in zone	Delete duplicates; keep a single TXT at <code>_dmarc</code> .
Invalid syntax	Colons instead of semicolons	Rewrite as <code>v=DMARC1; p=none; rua=mailto:...</code>
Domain still Pending	CNAME or DMARC mismatch	Re-copy all four records from systeme.io eye icon.
Reports not received	Wrong rua address or typo	Use a real mailbox on your domain; check spam.
Authentication OK but mail in spam	List/content reputation	See deliverability guides; DMARC alone does not guarantee inbox placement.

Frequently Asked Questions

What is DMARC?

A DNS TXT policy at `_dmarc` for SPF/DKIM alignment and reporting.

What value should I use first?

`v=DMARC1; p=none; rua=mailto:you@yourdomain.com`

Where is the record added?

DNS zone at your registrar—TXT type, name `_dmarc`.

More than one DMARC?

No—only one DMARC TXT per domain.

Is it required for systeme.io?

Yes, as part of full domain authentication with CNAMEs and sender verification.

Related Resources

- [How to Authenticate Your Domain Name for Email Sending](#)
- [Why Aren't My Emails Being Sent?](#)
- [How the systeme.io Affiliate Program Works](#)

Authenticate your domain, add DMARC, and run email marketing on [systeme.io](#).

Last updated: July 2, 2026