DMARC Reports: How to Read and Use Them

Introduction

DMARC (Domain-based Message Authentication, Reporting & Conformance) tells mailbox providers how to treat mail that claims to be from your domain. After you publish a DMARC DNS record with an **rua** reporting address, **receiving mail servers** send **daily aggregate reports**—usually as **XML attachments**. Help article **10240** explains how to interpret those reports and put them to work when you send from systeme.io.

Note: When you **authenticate your domain** on systeme.io, the required **SPF** and **DKIM** records are set up for sending through the platform. DMARC reports then confirm that Gmail, Yahoo, Microsoft, and other receivers see your legitimate mail as **authenticated**—and highlight abuse or misconfiguration when something fails.

Prerequisites

- A published **TXT** record at _dmarc.yourdomain.com with rua=mailto:… (How to Create a DMARC Record, 2241).

- Domain authentication (316) completed on systeme.io —including DMARC if prompted during DNS setup.
- An inbox that receives **rua** reports (ideally a **dedicated address** on the same domain, e.g. dmarc@yourdomain.com).

What Lands in Your Inbox

- **Frequency:** Roughly every **24 hours** per reporting organization (Google, Yahoo, etc.)—so multiple emails per day is normal.
- **Format:** Email with a **.xml** file inside a **.zip** or **.gz** attachment; subject lines often look like Report Domain: yourdomain.com Submitter: google.com.
- **Content:** No message bodies from your subscribers—only **metadata**: IPs, volumes, SPF/DKIM results, and policy disposition.
- **Spam folder:** Automated attachments sometimes land in junk—check there if reports stop appearing.

Receiving a report **does not automatically mean** your domain is broken; it means a provider is sharing visibility, as described in article 10240.

Key Parts of an Aggregate (RUA) Report

Article 10240 walks through a sample XML structure. These fields matter most:

- report_metadata **/** org_name**:** Who sent the report (e.g. google.com, emailsrvr.com).
- report_id**:** Unique ID for that file.
- date_range**: Reporting period** (start/end timestamps) the summary covers.
- policy_published**:** Your DMARC policy as seen by the receiver—often p=none, aspf/adkim alignment mode, pct.
- row **/** source_ip **+** count**:** Which server sent how many messages using your domain.
- policy_evaluated**: Authentication status**—dkim and spf **pass** or **fail**, plus disposition (e.g. none under p=none).
- auth_results**:** Detail per protocol—for systeme.io sends you may see DKIM like inbound.systeme.io with result=pass when configuration is correct.

Example pattern from 10240 when mail is healthy:

```
<policy_evaluated>
  <disposition>none</disposition>
  <dkim>pass</dkim>
  <spf>pass</spf>
</policy_evaluated>
```

How to Read a Report: Manual Analysis (10240)

1. Locate the DMARC email and **download the attachment**; unzip if needed and open the **.xml** in a text editor.
2. Identify the **reporting ISP** (org_name) and **report_id.**
3. **Note the date range (reporting period).**
4. **Read policy_published for your domain and current** p= **policy.**
5. **For each record, check source_ip and count—do you recognize the sender (your ESP, Google Workspace, etc.)?**
6. **Inspect policy_evaluated: both SPF and DKIM should pass for legitimate** systeme.io **campaign traffic.**
7. **Drill into auth_results if one check fails—misaligned domains or missing DNS often show up here.**

Optional helpers (not required by 10240): upload XML to MXToolbox DMARC Report Analyzer or dmarcian XML-to-Human Converter for a readable summary.

How to Read a Report: AI Assistance (10240)

1. **Open the email with the XML attachment.**
2. **Extract and open the XML file.**
3. **Paste the XML into an AI tool such as ChatGPT and ask it to analyze and interpret the DMARC report: list each** source_ip**, message counts, SPF/DKIM pass/fail, and flag unknown high-volume sources.**
4. **Cross-check anything critical (especially unknown IPs) against your known sending stack before changing DNS or policy.**

AI is useful for dense XML; for compliance and policy changes, still validate against your live DNS and authentication status in systeme.io.

How to Use Reports (Action Framework)

What you see	What to do
Known systeme.io paths, **SPF + DKIM pass**, healthy volume	**No action**—monitoring confirms deliverability signals are aligned.
Known sender (you), **SPF or DKIM fail**	Fix DNS: re-check registrar-specific auth, DMARC TXT, and domain status **Verified** in Settings → Emails.
Unknown IP, mail claiming	Possible **spoofing** or shadow IT—track volume;

your domain	investigate sender; keep p=none until all legitimate sources pass, then consider stricter policy with provider guidance.
disposition=none with p=none and failures	Expected during **monitoring**—failures are visible but not blocked yet; use data to fix auth before moving to quarantine or reject.
Flood of XML in main inbox	Point rua=mailto: to a **dedicated mailbox** and filter/forward as needed.

Goal: ensure **all legitimate emails** from your domain are **identified and pass authentication** (2241 / 10240)—the same foundation as improving deliverability and how spam filters work (10452).

systeme.io-Specific Context

- **Marketing mail sent through the built-in autoresponder should authenticate via records created during domain authentication—reports are your third-party proof receivers agree.**
- **If you send through your own SendGrid instead, DMARC rows reflect SendGrid's IPs and DKIM selectors—not only** inbound.systeme.io**.**
- **Yellow "monitoring" indicators in some checkers often mean** p=none**—that is normal for the monitoring phase, not necessarily a misconfiguration.**
- **Do not publish multiple conflicting _dmarc TXT records; keep one record with one** rua **address.**

Troubleshooting

Issue	Fix
No reports after a week	Confirm rua=mailto: in DNS; verify with MXToolbox DMARC lookup; wait for mail volume to trigger reports.
Reports in spam	Whitelist report senders; use dedicated rua inbox.
All fails from your campaigns	Re-authenticate domain on systeme.io; confirm CNAME/DMARC at host.
Cannot open XML	Decompress .zip/.gz first; open plain .xml in any editor or analyzer tool.

Frequently Asked Questions

Does a report mean something is wrong?

No—reports are routine aggregate summaries for monitoring.

Who sends them?

Mailbox providers to your **rua** address, typically daily.

What should pass for systeme.io?

SPF and DKIM pass for legitimate sends; DKIM details may reference **inbound.systeme.io**.

Dedicated rua inbox?

Recommended to avoid inbox overload.

What is p=none?

Monitor-only policy—collect data without enforcing reject/quarantine yet.

Related Resources

- How to Create a DMARC Record
- How to Authenticate Your Domain Name for Email Sending
- How to Add a DMARC Record on LWS
- How to Improve Your Email Deliverability

Use **DMARC aggregate reports** as a daily health check: legitimate systeme.io mail should trend toward **SPF/DKIM pass**; investigate failures and unknown IPs before tightening policy beyond p=none.

Last updated: July 4, 2026