# DMARCsimple – DMARC Troubleshooting Guide

DMARCsimple – DMARC Troubleshooting Guide

## What DMARC aggregate reports show

DMARC aggregate reports summarize how messages claiming to be from your domain behave over a period of time: which IPs send them, which providers are involved and whether SPF, DKIM and DMARC checks pass or fail.

## SPF, DKIM and alignment

SPF or DKIM passing on their own is not enough; they must also align with the domain in the From header. A frequent pattern is SPF or DKIM passing technically but failing alignment because a different domain is used.

## Identifying legitimate vs unauthorized sources

DMARCsimple helps distinguish between legitimate services that were never properly documented and suspicious sources that consistently fail authentication. Look at volume, provider reputation, alignment behavior and consistency over time.

## Common patterns

• Marketing platforms that sign using their own domain until a custom DKIM configuration is enabled.

• Transactional services that use a different return-path domain, causing SPF alignment to fail.

• Legacy systems sending as your domain without DKIM.

• Suspicious bursts of traffic from unfamiliar IP ranges.

## A practical troubleshooting workflow

1. Identify the source by provider or IP range.

2. Check SPF authorization and lookup depth.

3. Check for DKIM signatures and signing domains.

4. Evaluate whether SPF or DKIM is aligned with the From domain.

5. Decide whether to configure, adjust or block the source.

## Prioritizing fixes

Start with high-volume legitimate senders, then address reputable providers with intermittent failures, followed by unknown sources, and finally low-volume edge cases. This order supports a smooth path toward DMARC enforcement.