SPF / DKIM / DMARC Troubleshooting Checklist

For MDaemon Email Server administrators

When a message that failed authentication still lands in a user inbox, walk this list in order. Each step targets a specific cause — from sender policy, to MDaemon enforcement, to filter rules — so you can isolate the configuration that let the message through.

STEP 1

Pull the message from the log

Locate the SMTP session and corresponding delivery entries. Capture source IP, MAIL FROM, the visible From: header, and the SPF/DKIM/DMARC results recorded in the headers.

STEP 2

Confirm the published DMARC policy

Run a TXT lookup against the sender's DMARC record. A policy of p=none explains delivery on its own — your enforcement is working correctly.

DNS: _dmarc.<sender-domain>

STEP 3

Check the DKIM Verification Exempt list

Search by source IP. DKIM Verification has its own 'Exempt list' button, separate from the global Trusted IPs under Security Settings, so a clean Trusted IPs audit can miss it. IPs listed here are exempt from cryptographic verification specifically.

Security → Sender Authentication → DKIM Verification → Exempt list

STEP 4

Check Trusted Domains and Trusted IPs

Same search — by IP and domain. Be especially skeptical of broad CIDR ranges and legacy relay entries that may no longer be in use.

Security → Security Settings → Trusted Domains / Trusted IPs

STEP 5

Verify ARC trust configuration

If the message went through a forwarder, mailing list, or upstream gateway, an ARC seal from a trusted intermediary may explain why a failure was preserved as a pass.

Security → Sender Authentication → ARC

STEP 6

Confirm alignment, not just a component pass

A message can pass SPF or DKIM and still fail DMARC on alignment. The DMARC result is the one that matters for impersonation defense — never the underlying mechanism alone.

STEP 7

Walk the Content Filter rules

Check top to bottom for any rule whose action is Deliver, Move to, Stop processing, or similar. A single misnamed legacy rule can silently override sender authentication.

Security → Content Filter

SPF / DKIM / DMARC Troubleshooting Checklist

For MDaemon Email Server administrators

STEP 8

Check whether the session was authenticated

If the source was an authenticated SMTP session, authentication enforcement may have been bypassed by design. Investigate whether the credentials are being used legitimately.

Security → Sender Authentication → [each tab] → 'Do not apply to authenticated sessions'

STEP 9

Confirm the configured enforcement action

Walk each Sender Authentication tab and verify the action options match the policy. On SPF, '…send a 550 error code'. On DMARC, 'Honor p=reject when DMARC produces a FAIL result'. DKIM Verification has no direct fail-action option of its own — failed DKIM influences DMARC alignment and Spam Filter scoring instead.

Security → Sender Authentication → SPF / DKIM Verification / DMARC Verification

Once you've isolated the cause, run this quarterly audit to prevent the next one:

- [ ] Confirm 'Honor p=reject when DMARC produces a FAIL result' and 'Filter messages which fail the DMARC test into Junk E-Mail folders' are enabled under DMARC settings.
- [ ] Audit Trusted Domains, Trusted IPs, and the DKIM Verification Exempt list. Remove anything you can't justify.
- [ ] Walk Content Filter rules and document each delivery-related rule's purpose.
- [ ] Enable DMARC aggregate reporting on every domain you send from.