DMARC Policy Percentages

DMARC Policy Percentages Explained

The end goal for every DMARC policy is to check against 100% of all emails sent which use your domain. If you're not ready to fully adopt a strict DMARC policy, you should consider implementing a percentage policy and slowly increase this value over time under each policy.

When using a quarantine percentage policy selector, the sender may or may not receive a notification about any messages that were sent to quarantine, depending on the server's configuration. The remaining emails might be delivered to the recipient's inbox, placed in the spam/junk folder, or processed according to the server's usual email handling procedures. Essentially the same thing as if using the "**p=none**' selector.

Examples of quarantine polices based on percentages are below:

- **"v=DMARC1; p=quarantine; pct=10"**
  1 in 10 emails that fail DMARC authentication should be quarantined. The rest will be treated as having a "**p=none**" policy.
- **"v=DMARC1; p=quarantine; pct=50"**
  1 in 2 emails that fail DMARC authentication should be quarantined. The rest will be treated as having a "**p=none**" policy.
- **"v=DMARC1; p=quarantine; pct=100"**
  All emails that fail DMARC authentication should be quarantined.
  At this stage, you can now switch to the "**p=reject**" policy, and eliminate the "**pct=100**" value, or set it to a lower value (highly recommended).

The purpose of setting a percentage with the "**p=quarantine**" flag is to gradually implement DMARC enforcement, allowing organizations to monitor the impact of their DMARC policy before fully enforcing it. It can be helpful in scenarios where strict enforcement might risk legitimate emails being rejected erroneously. It provides a balance between security and ensuring legitimate emails are not erroneously quarantined.

⚠ !! Please use extra caution when setting up "**p=reject**" with a percentage value as it works slightly different than "**p=quarantine**" !!

As you move towards the final goal of a 100% "**p=reject**" policy, you should consider starting with a lower percentage value. When using "**p=reject**" combined with a percentage flag, a percentage of sent emails that fail DMARC authentication will be rejected at SMTP time and the sender will typically receive a bounce-back message indicating that the email was rejected. The rest will be processed by the recipient's mail server settings. This means the email might be delivered to the recipient's inbox, placed in the spam/junk/quarantine folder, or processed according to the recipient's mail server's usual email handling instructions.

Examples of reject polices based on percentages are below:

- **"v=DMARC1; p=reject; pct=10"**
  1 in 10 emails that fail DMARC authentication should be rejected at SMTP time. The rest will be processed by the recipient's mail server settings.
- **"v=DMARC1; p=reject; pct=50"**
  1 in 2 emails that fail DMARC authentication should be rejected at SMTP time. The rest will be processed by the recipient's mail server settings.
- **"v=DMARC1; p=reject; pct=100"**
  All emails that fail DMARC authentication should be rejected at SMTP time.
  At this stage, you can remove the "**pct=100**" tag entirely.

A DMARC policy using these two example selectors below mean the exact same thing, which is that they carry the same weight in the DMARC policy enforcement hierarchy.

"v=DMARC1; p=reject; pct=100"
"v=DMARC1; p=reject"

The purpose of setting a percentage with the "**p=reject**" flag is to gradually implement DMARC enforcement, allowing organizations to monitor the impact of their DMARC policy before fully enforcing it. It can be helpful in scenarios where strict enforcement might risk legitimate emails being rejected erroneously. However, eventually, the goal should be to increase the percentage or remove it altogether to fully enforce the "reject" action for better email security posture.

⚠ Please note that the percentage tag will not work with the "**p=none**" policy.

Related Topics:

- What is DMARC?
- DMARC Policy Selectors & Tags Quick Reference
- DMARC None or Ignore Policy
- DMARC Quarantine Policy
- DMARC Reject Policy
- DMARC RUA Reporting - Aggregate Reports (rua)
- DMARC RUF Reporting - Forensic Reports (ruf)
- DMARC Subdomain Policy (sp)

- DMARC DKIM Alignment (adkim)
- DMARC SPF Alignment (aspf)
- What is BIMI?
- What is a VMC?
- DMARC, DKIM, SPF and BIMI Info

Don't have the time or energy to learn, setup, monitor and maintain DMARC? What if you had a team of DMARC experts to do this for you?

Let us do the DMARC for you. Check out Managed DMARC Services by GlowHost.