DMARC Policy Selectors & Tags Quick Reference

Your domain's DMARC policy can be configured with different Policy Selectors, sometimes referred to as "Tags", Various tags are used to instruct remote email servers handle email from your domain name. You can start off by instructing remote email servers to *ignore* emails that fail DMARC authentication and proceed with their normal handling of email. Later, you can move a more strict policy which will instruct remote mail servers to *quarantine* emails that fail DMARC authentication and to move that email into the recipients junk mail or spam folder. Finally, you can instruct remote email recipient servers to completely *reject* a percentage or all emails that you have not implicitly authorized to send email on behalf of your domain's email addresses. The *reject* option being the most strict of all policies, caution should be used before moving to a reject policy.

DMARC None or Ignore

"**p=ignore**"

In DMARC, there is no official "**p=ignore**" policy.

"**p=none**"

To adhere to the DMARC1 Technical Specification, The correct syntax to use is "**p=none**".

The "**p=none**" policy instructs receiving mail servers to take no action based on the DMARC evaluation results. This means that the DMARC policy is set to *monitor and report mode* only; it tells recipient mail servers to neither quarantine or reject emails that fail DMARC authentication. Instead, domain owners may receive **aggregate (RUA)** and **forensic (RUF)** reports about DMARC authentication results if the "rua" and "ruf" tags are selected in the domain's DMARC policy.

The recipient mail servers are requested to go ahead and proceed with their usual mail-handling procedures. The recipient server may place the email in the inbox or junk mail folder, or any other folder depending on how the recipient's mail server is configured to deal with email, in general. "**p=none**" is typically what you would set your DMARC policy to when first starting out. This allows you to make sure that email is being handled "as usual" before adding any restrictive DMARC instructions to your domain.

DMARC Quarantine

"**p=quarantine**"

Under this policy, you are instructing the recipient's mail server that any emails failing DMARC authentication should be sent to the recipient's quarantine area, (generally the spam, junk mail or quarantine folder), rather than being delivered to the recipient's inbox. or being rejected completely. This provides an intermediate level of protection against potentially malicious emails while still allowing for delivery of legitimate email. So why do this? This policy can help protect your recipients' against phishing, spoofing, malware and other common email attacks while minimizing the risks of false positives. Once you are comfortable that the great majority or preferably, the entirety of emails that have been quarantined are legitimately "bad" emails, the next step is to move towards a p="reject" DMARC policy.

DMARC Reject

"**p=reject**"

The most stringent DMARC policy, this policy instructs receiving mail servers to outright reject emails that fail DMARC authentication. These emails are not delivered to the recipient's inbox and are rejected during the SMTP transaction. Typically, they are returned to the sender as a bounce message, or are discarded entirely. p="reject" offers the highest levels of protection against email spoofing, phishing, malware and other fraudulent email attacks. It also ensures that only emails that pass DKIM and SPF authentication arrive in the recipient's inbox. That being said, extreme caution should be used when implementing a p="reject" policy because otherwise legitimate emails that fail DMARC authentication will ultimately be rejected. An example of an otherwise legitimate email might fail to be delivered is if you use a third-party email service to deliver emails from addresses @your-domain.com. For example, a third party newsletter, calendar, or survey email service provider who sends emails on your behalf.

DMARC Policy Percentages

"**pct=n"**

You can also define a percentage policy to slowly increase the percentage of action taken on your specified policy. Setting a percentage instructs the recipient mail server to apply the desired enforcement policy to a specified percentage of emails that it receives. For example, if you have a DMARC policy of "p=reject" and "pct=40", it means that only 40% of the emails that fail DMARC authentication should be subjected to being rejected, and that the recipient server should determine how to deal with the remaining 60% of emails using it's own pre-defined rules. The purpose of the policy percentage in this example is to gradually move towards a 100% rejection policy if an email fails DMARC authentication. The values available range from 0 to 100. In this example, the DMARC record would look like this: **v=DMARC1; p=reject; pct=40;**

- Note that he "pct" tag is optional, and if a value is not specified here, then the default value of 100% will be assumed to be your intended policy by the recipient's mail server.
- Policy percentages do not have any effect when the DMARC policy is set to "p=ignore".

DMARC RUA Address

"rua=mailto:something@somedomain.com"

The "rua" tag specifies the email address to which aggregate reports should be sent. Aggregate reports provide information about email traffic, authentication results, and sending sources.

DMARC RUF Address

"**ruf=mailto:something@somedomain.com**"

The "ruf" tag specifies the email address to which forensic reports should be sent. Forensic reports provide detailed information about individual email messages that failed DMARC authentication.

DMARC SP

The "sp" tag stands for "Subdomain policy." It specifies the policy to be applied to subdomains that do not have their own DMARC record. It can have the same values as the "p" tag. For example:

- "**sp=none**"
- "**sp=quarantine**"
- "**sp=reject**"

When a subdomain of your domain does not have its own DMARC record published, the "sp" tag specifies the policy to be applied to emails specifically sent from that subdomain. This allows you to enforce a unique DMARC policy across each subdomains of a domain. If the "sp" tag is not explicitly set in the DMARC record, the DMARC policy specified by the "p" tag (the organizational domain's policy) is applied to emails sent from subdomains without their own DMARC records.

DMARC ADKIM

The "adkim" tag stands for "Alignment Mode for DKIM." It specifies how the **DKIM** mail signatures should align with the email's From domain, and can have two values:

- "**r**": Relaxed alignment. DKIM signatures must only partially match the email's From domain.
- "**s**": Strict alignment. The DKIM signature must exactly match the email's From domain.

DMARC ASPF

The "aspf" tag stands for "Alignment Mode for SPF." It specifies how the **SPF** authentication results should be aligned with the email's From domain, and can have two values:

- "**r**": Relaxed alignment. SPF authentication results must only partially match the email's "Return-Path" (or "MAIL FROM") address and the email's From domain.
- "**s**": Strict alignment. Requires a strict alignment between the domain specified in the "Return-Path" (or "MAIL FROM") address and the email's From domain.

When these tags are combined within a DMARC record, it allows domain owners to request that recipient mail servers handle email originating from their domain in a specific way.

In summary, each DMARC policy tag offers varying levels of protection against email spoofing and phishing attacks. They allow domain owners to specify their desired DMARC policies, control enforcement actions, and receive reporting information to monitor and manage email authentication for their domain. Organizations should assess their email security needs, evaluate the potential impact on legitimate email delivery, and implement DMARC policies accordingly. By deploying a successful DMARC enforcement policy, organizations not only improve email security, but add trust and visibility to their brand.

Related Topics:

- What is DMARC?
- DMARC None or Ignore Policy
- DMARC Quarantine Policy
- DMARC Reject Policy
- DMARC Policy Percentages
- 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 DMARC for you. Check out Managed DMARC Services by GlowHost.