What is DMARC record and how to manage it with EasyDMARC

DMARC

What is the DMARC record?

DMARC, which stands for “Domain-based Message Authentication, Reporting & Conformance”, is an email authentication, policy, and reporting protocol. It is implemented as a DNS TXT Record and lets admins receive reports on their outgoing email infrastructure and set policies (p=none, p=quarantine, or p=reject) to tell receiving servers how to handle unauthorized email usage on their domain’s behalf.

Why test your DMARC record?

By performing DMARC Lookup, admins can make sure that their DMARC Record is published and deployed correctly on their domain. Additionally, admins can verify that there are no underlying errors with the Record syntax, validation, and other key issues.

Why are DMARC reports important?

DMARC reports are one of the key factors to have a successful DMARC enforcement (reaching to p=reject) journey. With DMARC reports, you will be able to analyze your outgoing email ecosystem, authenticate your legitimate email sources, and proceed with DMARC enforcement to let the ISPs (such as Google, Comcast, and Yahoo) block the fraudulent and unauthorized email usage on your domain’s behalf.

What does DMARC compliant mean?

As DMARC is an additional security layer that works upon SPF & DKIM, DMARC Compliance means that your outgoing email server is authenticated and aligned with either SPF or DKIM authentication protocols.

How does DMARC work?

To put it simply, here's how it works:

- First, admin implements DMARC TXT Record in their DNS provider
- After that, for every email sent from the domain, receiving servers will start to check the domain's DMARC Record
- Receiving servers will check SPF and DKIM authentication and alignment checks to verify the sender of the domain (if it is actually coming from a legitimate source)
- With both SPF and DKIM results, the receiving server will apply rules based on the admin's stated policy (p= tag) in DMARC Record. For example, if the domain's policy is set to Reject (p=reject) and the emails didn't pass SPF and DKIM results, the receiving server will Reject the message completely.

- Lastly, the receiving server will send DMARC reports to the admin (to an email address(es) specified in DMARC Record's RUA and RUF addresses). These reports contain all the necessary information that you can read more here.

What does DMARC domain alignment mean?

Domain Alignment is the core concept of DMARC. That is, verifying that the email address in the From header is the actual sender of the message. Practically, this means that the domain SPF check (which is based on Envelope From: or Return-Path address) and the DKIM signing domain (d=example.net) are in alignment with the message From: address.

You can read more about DMARC domain alignment here.

How does a DMARC work with subdomains?

By default, DMARC Record or policy implemented on the root domain level will automatically apply on all subdomain(s) levels, unless admins implement explicit DMARC Record on the subdomain(s) level.

Can I Add a DMARC Record Without DKIM?

Technically, you can. But, for DMARC to pass, you need to have either SPF or DKIM authentication & alignment in place.

At EasyDMARC, we always advise our customers to start their DMARC journey with Monitoring mode (p=none). That way, receiving servers will not apply any rules on the unauthenticated email flow on the domain’s behalf. But, it is important that every email source is properly configured and authenticated with SPF and DKIM during the Monitoring stage so that the admins start with their DMARC enforcement journey (heading to p=quarantine or p=reject). This will help them avoid false-positive cases and make sure that they don’t lose or block any legitimate mail flow due to DMARC reject policy.

What is DMARC Record Generator?

The DMARC Record Generator allows you to create your DMARC Record ready to be published on your DNS so that you’re able to gain valuable insights on who is abusing your domain.

EasyDMARC’s DMARC Generator guides you through each step of the process, including explanation.

Use DMARC Record Generator, if you want to:

- Create DMARC TXT record and publish it in DNS
- Read about all DMARC's terms to easily configure DMARC Record
- Validate if DMARC record's text corresponds to the specification before publishing it in DNS

Why does DKIM lookup matter?

- Select the policy that you’d like to be applied to you domain (More about policies here)
- Select the Failure reporting option (Fo) (More on that here)
- Other optional steps:
  - You can add other email addresses to receive DMARC reports in the "Reports send to" fields.(Optional)
  - Set your SPF or DKIM identifier alignment to strict
  - Chose a percentage for the applied policy
- Generate a DMARC record and update it in your DNS zone

How to use the DMARC Record Generator?

Head to EasyDMARC and click on DMARC from the tools section then DMARC generator and follow our guide.

How to implement a DMARC record on your domain?

Once the record has been generated, copy it and head to the DNS zone of your domain. Add a new TXT or CNAME record and paste the provided record. Note: With the majority of DNS providers

(ex. GoDaddy) the domain part will be added automatically in the Host/Name field so adding only _dmarc is enough.

DMARC record format

The format for the DMARC record is TXT or CNAME (for Hosted DMARC)

DMARC record tags

DMARC has some required tags which are:

Version ("v"): Must take the value DMARC1.

Policy ("p"): Policy for receiving messages, DMARC has three policies none which is used for monitoring, quarantine that lets you quarantine non-compliant emails and reject that lets you reject all the non-compliant emails.

DMARC also has some optional tags:

Like the Rua and Ruf address tags, the Percentage (pct) tag that gives you decide the percentage of the applied policy for the non-compliant emails, subdomain policy (sp), adkim, and aspf tags that can be set to either relaxed (r) or strict (s), you can read more about DMARC tags here.

Revision #2
Created 2026-08-07 14:59:02 UTC by Sarath
Updated 2026-08-07 16:05:11 UTC by Sarath