EasyDMARC Frequently Asked Questions

FAQ's

Here are the most common questions our Customers and DMARC users ask when using the EasyDMARC product. If you have any additional questions please contact our support team!

- **What does the activation of EasyDMARC look like?**

Most importantly, in order for EasyDMARC to fully operate, it requires adding a CNAME or TXT record to your domain’s DNS zone. Depending on the way you purchase EasyDMARC from us, CNAME will be added automatically or you have to do it manually (more information below).

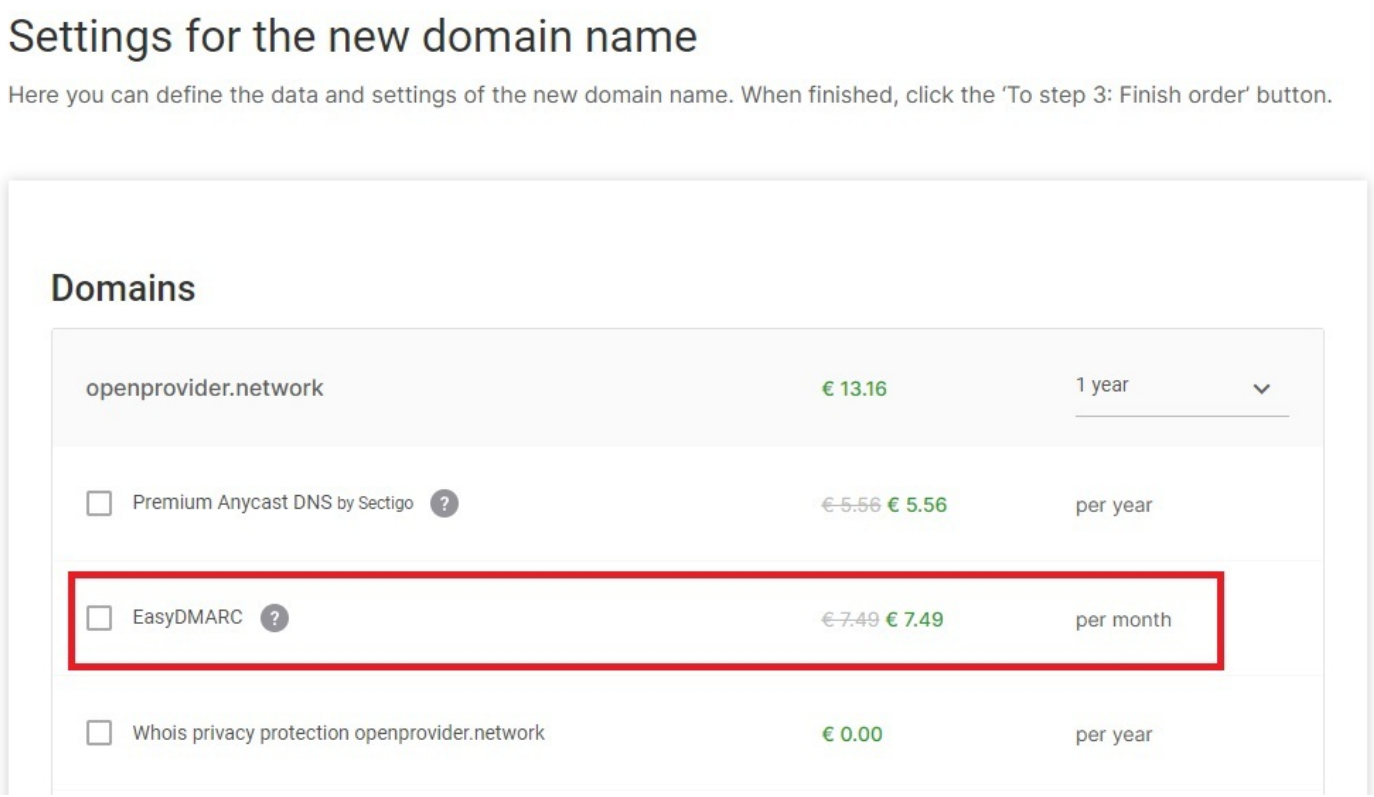
We strongly recommend using CNAME record as it allows you to manage all the settings comfortably from the EasyDMARC panel without a need to adjust your DNS zone settings every time.

Once a CNAME record is added to your DNS zone, you will be able to manage EasyDMARC settings from the Hosted DMARC tab in the EasyDMARC control panel:

You can find more information about setting up the records in our KN article - https://openprovider.help/books/new-products/page/how-to-manage-your-dmarc-record-using-easydmarc

- **How can I enable the EasyDMARC service for a new domain registration using the Reseller Control Panel?**

It’s simple! When ordering a new domain directly from RCP, you can choose various additional products that will enhance your domain security. Simply tick the checkbox for EasyDMARC and a new subscription will be added to your order (***Please ensure that you have signed the EasyDMARC contract, https://cp.openprovider.eu/documentation/contracts.php --> EasyDMARC***).



NOTE: When ordering EasyDMARC together with the new domain, we will automatically add the required CNAME record to your domain DNS zone once it is created (if you choose yo use Openprovider nameservers). No additional action is required from your side at this time. Also, we will use Handle ID of a customer / domain owner to add new subscription in EasyDMARC dashboard.

The CNAME record we will add is:

HOST: _dmarc.*example.com*

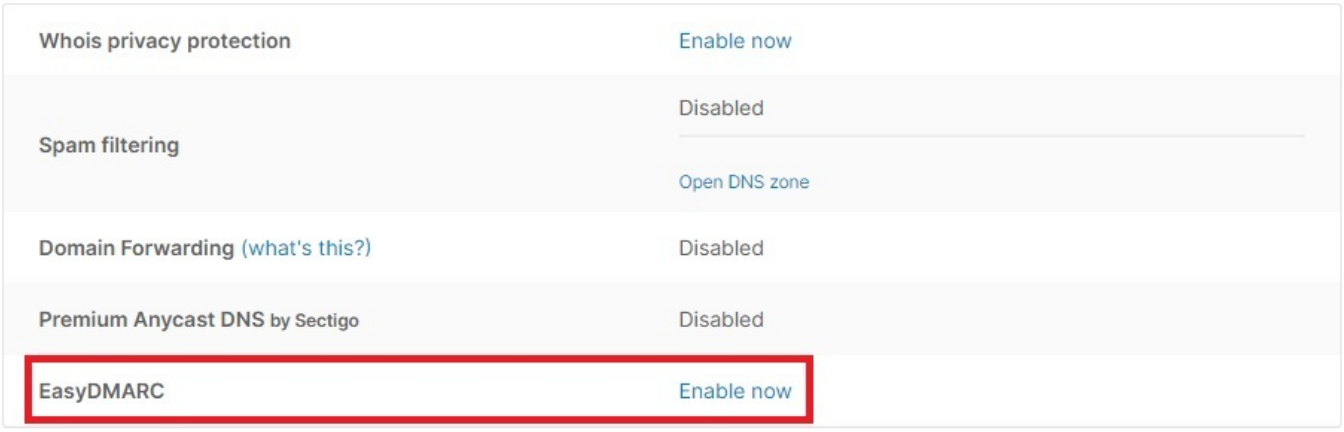
Type: CNAME

Value: _dmarc.*example_com*._d.dmarcprotect.me

Important: *If you are not using Openprovider nameservers, you have to add the above CNAME manually to your DNS zone.*

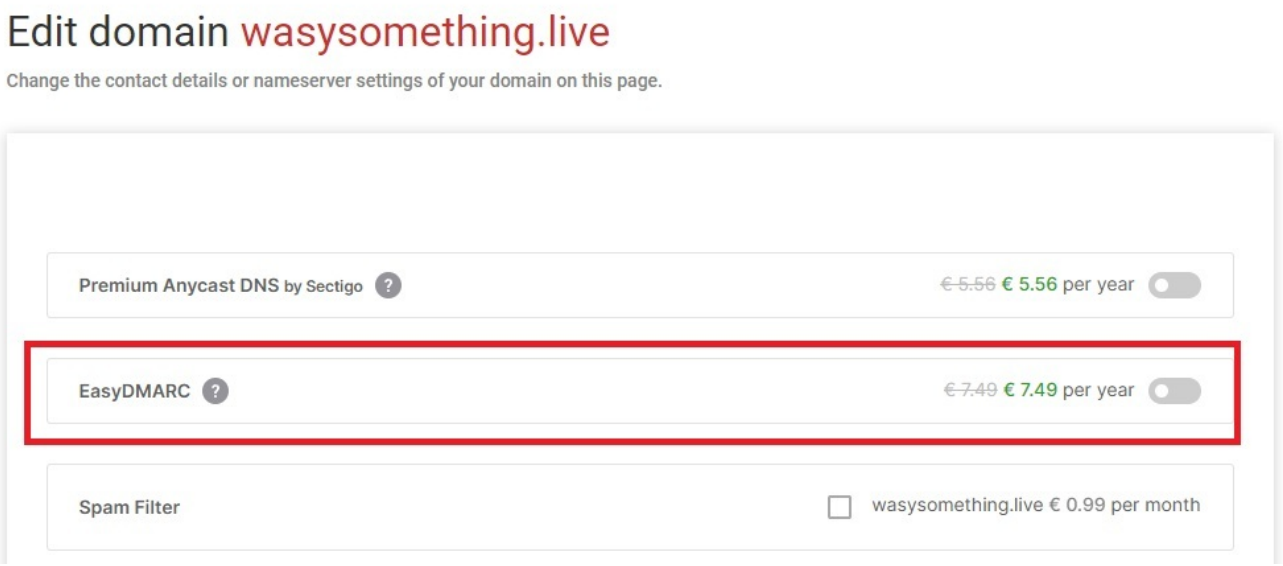
- **How can I enable the EasyDMARC service for an existing domain using the Reseller Control Panel?**

If you want to activate EasyDMARC for a domain hosted at Openprovider, then head to the selected domain details view and click the Edit button. You will be presented with several options for activating additional add-ons.



Click “Enable now” for EasyDMARC, you will be redirected to the domain edit page with a toggle for EasyDMARC (***Please ensure that you have signed the EasyDMARC contract,*** ***https://cp.openprovider.eu/documentation/contracts.php*** ***--> EasyDMARC***).

Important: *If you are not using Openprovider nameservers, you have to add the above CNAME manually to your DNS zone.*



- **Can I enable the EasyDMARC service when transferring a domain to Openprovider or when trading a domain?**

At this moment we are not supporting EasyDMARC activation when transferring a domain to Openprovider. This feature will be added in the future. However, once your domain is fully transferred to Openprovider, you can activate EasyDMARC in the domain details view.

- **Can I transfer my EasyDMARC subscription from one domain to another?**

No. If you wish to disable EasyDMARC for your domain, you can do that in the domain details view or in the EasyDMARC subscription overview page. For a new domain, simply purchase a new EasyDMARC subscription.

- **How do I disable the EasyDMARC service for a given domain using the Reseller Control Panel?**

Simply find the domain you want to stop protection with EasyDMARC, open the domain details view, find EasyDMARC on the list of activated add-ons and click the “Deactivate” button.

- **What DNS record types are supported by the EasyDMARC service?**

The main record to actually activate EasyDMARC is a CNAME or TXT record. If you are buying EasyDMARC together with a domain in RCP, the CNAME record will be added automatically to your DNS zone. Otherwise you have to add it manually once the EasyDMARC subscription is fully provisioned.

When you use the CNAME record, there is no need to adjust the DNS zone anytime you wish to change DMARC settings or policies. However, if using a TXT record, depending on what policies you want to set for DMARC, you will have to generate new records in the EasyDMARC control panel and publish them in your DNS zone.

NOTE: By default we are adding DMARC records with policy set to “monitoring”. Once you add your domain for the first time to EasyDMARC, it takes 4-6 weeks to collect enough data to actually be able to tailor your DMARC experience better, for example changing the default policy to “quarantine”.

Apart from DMARC records, you should also configure records for SPF and DKIM in your DNS zone. You can use Generator tools in the EasyDMARC panel to generate them according to your preferences.

We strongly recommend using CNAME record as it allows you to manage all the settings comfortably from the EasyDMARC panel without a need to adjust your DNS zone settings every time.

- **Can I use the EasyDMARC service if my domain is not managed by Openprovider?**

Of course! EasyDMARC allows you to use whatever domain you want; it does not have to be managed at Openprovider. Go to the EasyDMARC dedicated menu in RCP, click on “Buy new subscription” and follow the instructions on the screen.

NOTE: Please remember that once you purchase EasyDMARC for a domain outside Openprovider, you have to either add below CNAME record to your DNS zone or use DMARC Generator tool to create TXT record which you have to add to DNS zone for your domain:

HOST: _dmarc.*example.com*

Type: CNAME

Value: _dmarc.*example_com*._d.dmarcprotect.me

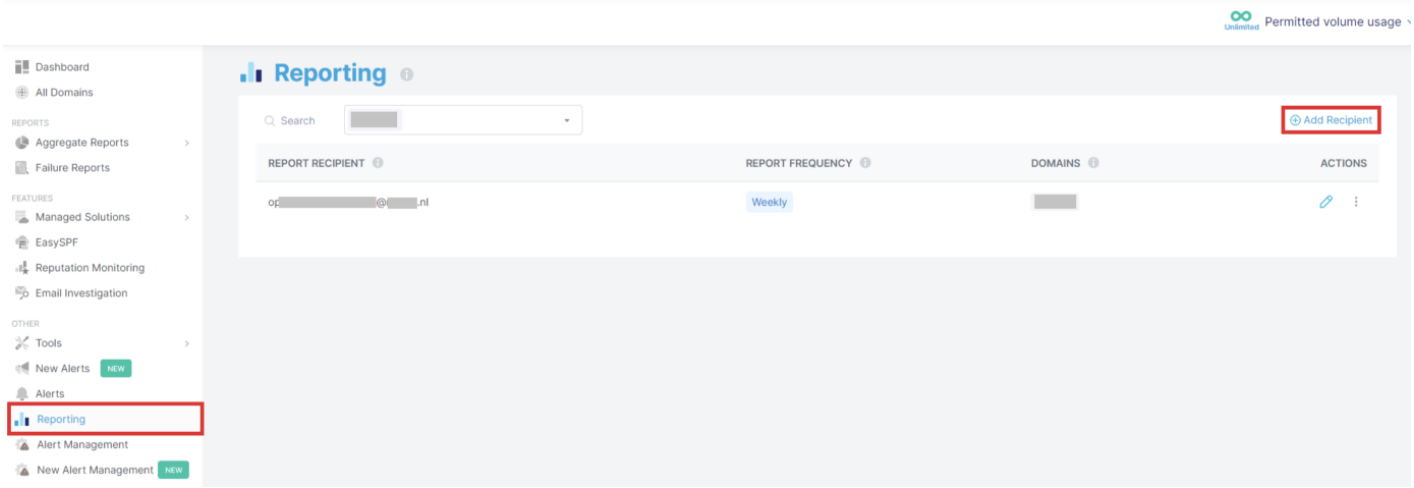
- **How do I delete the EasyDMARC and prevent further billing?**

You can do that from the domain details view in RCP. Simply find EasyDMARC in a list of active add-ons and click the “Deactivate” button. If you are doing that for a domain hosted at Openprovider, CNAME records will be automatically deleted from your DNS zone. Otherwise please remove it manually from your DNS zone.

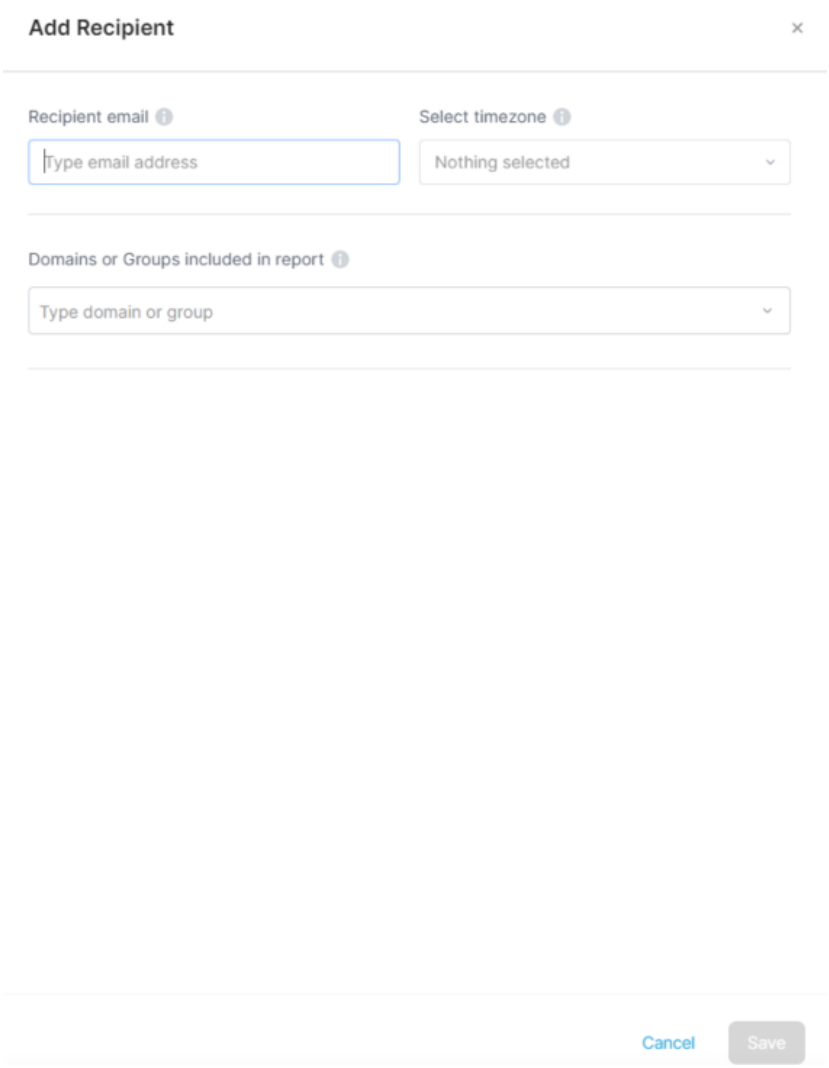
NOTE: If you cancel your EasyDMARC subscription during the monthly subscription period, you will NOT be refunded for the remaining time.

- **Can I provide access to my customer? (enduser)**

It is not possible to provide access to the EasyDMARC panel to end users. To be able to provide reporting to the client, you can add their email and domains in the following reporting screen(this will create automated reporting on a daily, weekly or monthly basis):



This will open the following screen:



Billing:

- **How does billing work for the EasyDMARC service?**

EasyDMARC subscription is billed monthly and the price is based on your current member status. The renewal happens automatically every month until you cancel the subscription.

- **What happens to my subscription if I disable the EasyDMARC service for a domain?**

If you cancel your subscription, you will lose access to the EasyDMARC control panel immediately and you will not be billed for that subscription anymore.

NOTE: If you delete your EasyDMARC before the current billing cycle has come to an end, you will not get a refund for the rest of the period you paid for as mentioned in the signed Terms and Conditions.

- **What happens to my subscription if I delete my domain, I transfer it out or my domain expires?**

Your EasyDMARC is not canceled automatically if you delete your domain. You have to manually cancel your subscription in RCP, either from a domain dashboard or EasyDMARC dashboard in the Reseller Control Panel. If however you transfer your domain and wish to use EasyDMARC with this domain, once the transfer is completed, you can again add CNAME records to the DNS zone with the new provider.

NOTE: Until you cancel your EasyDMARC subscription, the domain will remain active in the EasyDMARC control panel, no matter if it’s active or moved outside Openprovider.

Pricing:

- You can find the actual price for EasyDMARC in your Reseller Control Panel under pricing.

API:

- **Is the Openprovider API compatible with EasyDMARC?**

Unfortunately not at this moment. We are working on adding EasyDMARC to Openprovider’s public API and as soon as it is available, we will let you know in a separate email.

- **Can the EasyDMARC service also be used via Plugins, like WHMCS, Blesta or Hostbill?**

We are planning to release the WHMCS support module for EasyDMARC in the near future. Please stay tuned for more information coming from Openprovider.

SPF

- **How do you handle SPF flattening? Do we need to give you access to our DNS settings for that?**

No, you don't need to give us your DNS settings or any other access. With our EasySPF, we will provide you with a single include: mechanism that you will apply in your DNS, and every update/change in your SPF Record will be managed from your EasyDMARC account portal.

- **What does "Too many DNS lookups'" mean?**

SPF specification has a limit on the number of DNS lookups (10) required to fully resolve an SPF record. This is a highly critical limitation to prevent Denial of Service (DoS) attacks. If you are using multiple Third-Party services for your various email strategies, it can be easy to exceed this limitation. Check our EasySPF solution on how to overcome this limitation.

- **Since there can be only one SPF Record, how can I add or whitelist multiple servers in a single TXT Record?**

For adding two SPF includes in your single SPF record, you need to include the two include: mechanisms next to each other for example: v=spf1 include:example.com include:example2.com ~all.

- **I have an issue with my SPF record length. I got "Record is too long. It must be no more than 450 characters"!**

If your SPF record has more than 450 characters, this may lead to SPF record validation errors. To solve this issue, you need to adjust your SPF Record or check our EasySPF solution.

- **Why is SPF failing even by having the server or source IP whitelisted in SPF Record?**

SPF checks against the Return-Path: or MailFrom: address domain for verification. If the address domain doesn't match with your From: domain, then SPF will fail due to misalignment. Check out Why is DMARC Failing article for more information.

DKIM

- **What are DKIM selectors?**

DKIM selector is part of the DKIM record and it allows publishing multiple DKIM keys for a domain. Check our article for more information.

- **How should I implement DKIM?**

DKIM works with Private and Public keys. Private keys are stored in email servers, while Public keys are implemented in domain's DNS. There are multiple use-cases for DKIM implementation:

1. If you are using Third-Party ESPs (Google, Microsoft365, Mailchimp, etc.) DKIM Public keys are obtained from their portals. ESPs won't share their Private Keys for privacy and security concerns.
2. For dedicated servers, EasyDMARC's DKIM Generator tool can be used. You will securely store the Private key in your own server, while implementing the Public key in your DNS.

- **What is the recommended key size for DKIM?**

Senders should use 1024 to 4096-bit keys. Google and some other receivers consider keys smaller than 1024-bits insecure, and will not use them for authentication.

DMARC

- **I created a DMARC record, but I am still getting an error.**

There can be multiple cases for this. Most common cases include:

1. Syntax issue with subdomain added in the "Host" or "Name" section. DMARC needs to be implemented on _dmarc.yourdomain.com subdomain. Make sure you got that right.
2. Some DNS Zones (e.g GoDaddy) will not inherit but overwrite the subdomain name once added in the "Host" section. (For e,g, when you input your whole subdomain "_dmarc.yourdomain.com", GoDaddy will read that as "_dmarc.yourdomain.com.yourdomain.com" which invalidates your DMARC Record. To fix this, simply remove your domain name and just keep "_dmarc".
3. You have multiple DMARC Records implemented in your DNS. Make sure you have only one DMARC TXT Record on per your root/subdomain level.
4. You are still with DMARC None policy (Monitoring mode) and you are getting an error indicating "DMARC record is valid, but you are not protected against email spoofing and phishing". This is a warning sign from our side that your DMARC Policy is not enforced, and your domain is still open to any spoofing attempts.

- **I got the alert "DMARC record is valid, but set policy (none / quarantine) does not yet protect your domain against email spoofing and phishing." Can you guide what settings are missing?**

That is because your DMARC record policy is p=none; which is the monitoring phase to ensure all your email vendors pass the DMARC check, when you later enforce your DMARC record to higher levels then that alert will disappear. That means to change your policy from p=none; to p=quarantine; and later p=reject.

- **How do I know whether I'm ready to switch to p=reject?**

DMARC enforcement can be achieved after making sure that all your outgoing legitimate servers are properly authenticated . Contact our Support team to discuss further.

- **The RI (Reporting Interval) tag of DMARC Record is set to 3600 sec (1 Hour) but the aggregated reports are sent only 24 hours. Why?**

Major Providers like Google & Verizon Media have chosen to simplify the reporting by

sending Daily reports only (every 24 hours), even if admins have a shorter "ri" period tag included in their DMARC Record. You can check our article for a detailed overview of DMARC Tags.

BIMI

- **Do I need BIMI?**

BIMI is a fairly new protocol and not many ISPs currently support it. Also, for BIMI to work, first you need to have an enforced DMARC Policy (Quarantine or Reject). We at EasyDMARC highly recommend our users to first start with their DMARC enforcement journey, and then proceed forward with BIMI.

- **I have multiple issues in my SVG, how can I fix that?**

EasyDMARC's BIMI Converter Tool can be used to convert BIMI SVG images and logos to BIMI-compatible SVG Tiny P/S format. You can also check our article on how to convert a PNG/JPEG to BIMI-Compatible SVG format.

- **How will I obtain a Verified Mark Certificate (VMC) for our logo?**

Currently, VMCs are being issued by two BIMI-qualified Certification Authorities, DigiCert and Entrust Datacard. Contact them for more details.

Reporting

- **Is it possible to speed up the display of DMARC Aggregate reports?**

If you've just added or updated your DMARC Record, it will take up to 72 hours (3 days) until the first DMARC reports are received. After that, reports are usually updated every 24-32 hours.

- **I've modified my DMARC record to send emails to my assigned easydmarc.com email address, but reports don't show up in my dashboard**

If you've just added or updated your DMARC Record, it will take up to 72 hours (3 days) until the first DMARC reports are received. After that, reports are usually updated every 24-32 hours.

- **DMARC Aggregate vs. Failure Reports - What is the difference?**

There are 2 different types of DMARC reports: Aggregate report and Failure (formerly known as Forensic report). Check our article for more information.

- **DMARC Compliant vs. Non-Compliant vs. Threat/Unknown vs. Forwarded tabs - What do they represent?**

EasyDMARC segments DMARC Reports into 4 tabs to make your DMARC enforcement journey easier and more successful.

DMARC Compliant: Under this tab, our system discovers and shows you all the email sources that are sending DMARC Compliant emails on your domain behalf. These are your legitimate sources that are meeting compliance via SPF and/or DKIM authentication and alignment.

DMARC Non-Compliant: This tab identifies all your sending sources that are failing DMARC compliance checks. These sources are failing both SPF and DKIM authentication and alignment.

Threat/Unknown: This tab identifies all the spoofing or fraudulent attempts on your domain behalf that are being sent from Source IPs that are blacklisted in multiple RBLs (Blacklist checks) or a Source IP which doesn't resolve to a Reverse DNS (PTR). You may, at some point, discover your legitimate servers labeled under this tab, which indicates your server is either blacklisted in multiple lists or lacks Reverse DNS (PTR).

Forwarded: Forwarding happens when your receiver forwards your email to another recipient. This is usually caused by Auto-Forwarding or Routing rules that are applied in major Mailbox Providers.

Revision #3
Created 2026-08-07 14:00:07 UTC by Sarath
Updated 2026-08-19 14:32:32 UTC by Sarath