EasyDMARC

- EasyDMARC Frequently Asked Questions
- DMARC failure reports
- EasyDMARC - Product overview
- EasyDMARC - SPF Record Check and Lookup
- EasyDMARC DNS Records Lookup
- EasyDMARC Email Investigation
- How to manage your DMARC record using EasyDMARC
- Phishing URL Check feature in EasyDMARC
- What is BIMI and how to manage it with EasyDMARC
- What is DKIM and how to manage it with EasyDMARC
- What is DMARC record and how to manage it with EasyDMARC

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).

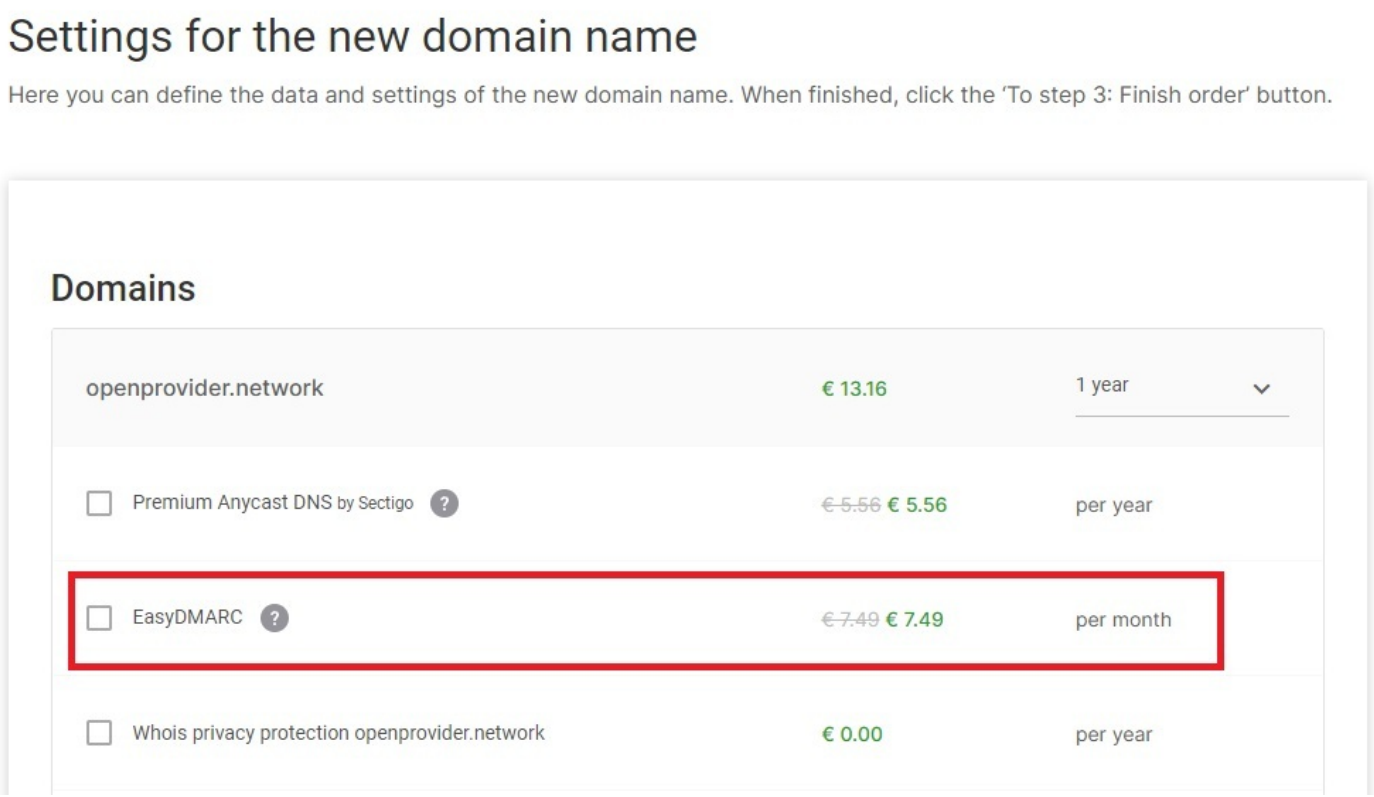
We strongly recommend using CNAME record as it allows you to manage all the settings comfortably from the EasyDMARC panel without a need to adjust your DNS zone settings every time.

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*

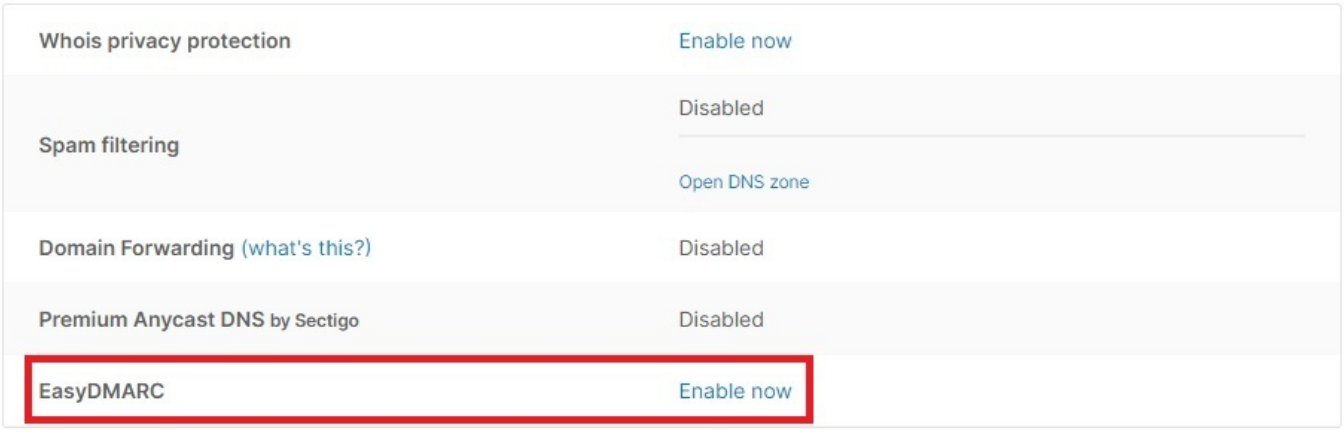
Type: CNAME

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.*

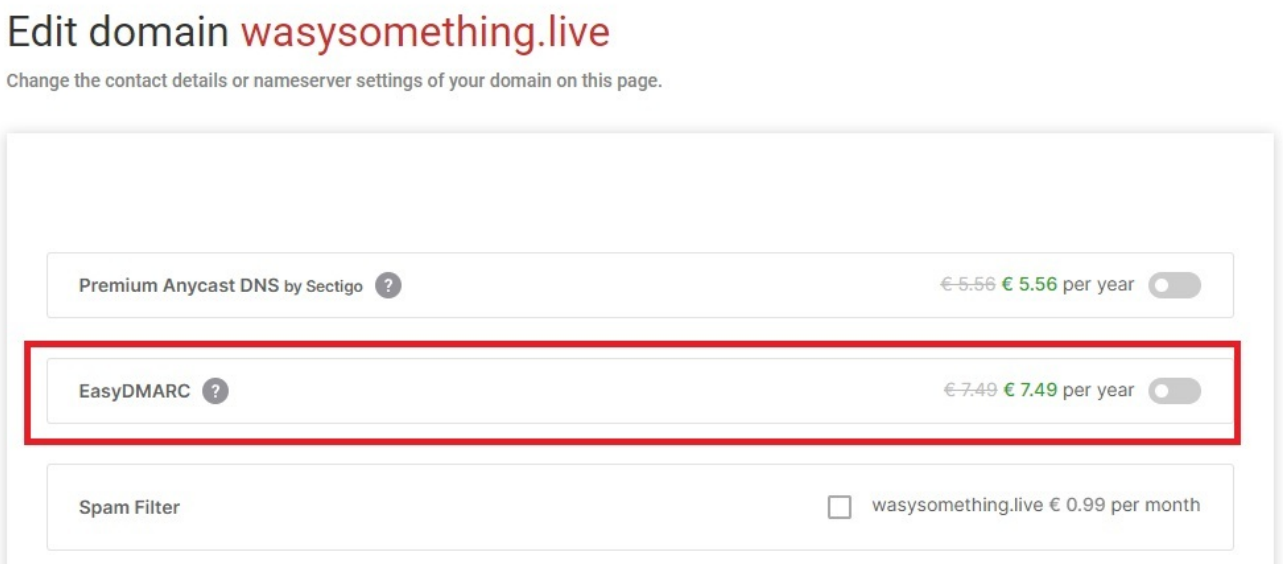
- **How can I enable the EasyDMARC service for an existing domain using the Reseller Control Panel?**

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

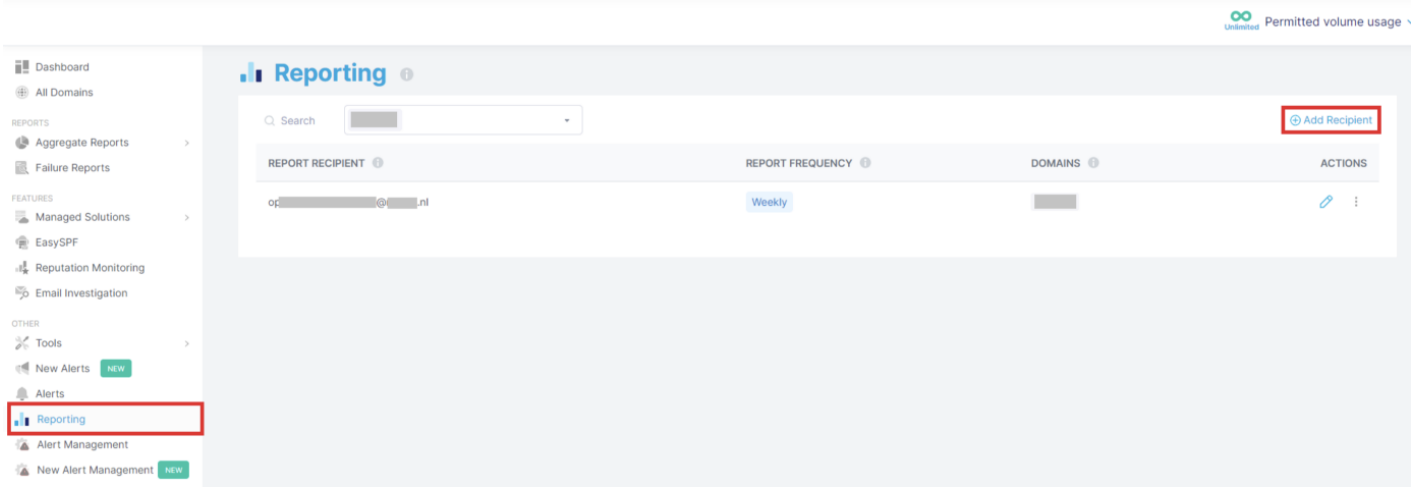
- **How do I delete the EasyDMARC and prevent further billing?**

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.

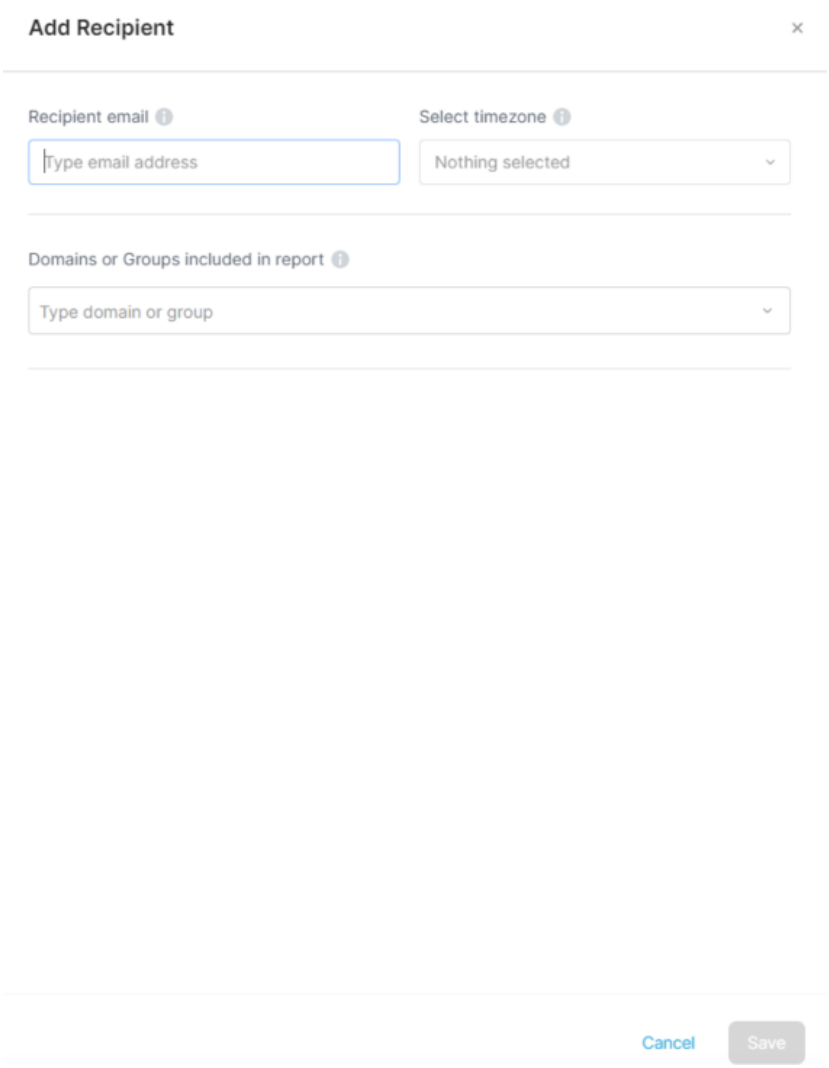
NOTE: If you cancel your EasyDMARC subscription during the monthly subscription period, you will NOT be refunded for the remaining time.

- **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.

DMARC failure reports

What is a DMARC Failure (Forensic) Report?

- DMARC Failure Report, formerly known as DMARC Forensic Report, is another type of report, which the DMARC protocol enables you to receive.
- Failure reports are much more detailed than DMARC Aggregate reports, as they show a "sample" of an email message that failed SPF, DKIM, or DMARC tests.
- To receive a Failure report, one must set an email address in "ruf" field, like it's done for "rua" field.
- Failure reports are normally generated and sent almost immediately after the Mail Receiver detects a DMARC failure.
- Rather than waiting for an aggregate report, these reports are useful for quickly notifying the Domain Owners when there is an authentication failure.
- Whether the failure is due to an infrastructure problem or the message is inauthentic, failure reports also provide more information about the failed message than is available in an aggregate report.

EasyDMARC - Product overview

In collaboration with our Partner - EasyDMARC - Openprovider introduces a new product called EasyDMARC.

- **EasyDMARC Benefits**

EasyDMARC is a full set of features that make the tool stand out in the market.

AI-Powered Data Classification - Correct source identification is very important for DMARC deployment. It helps customers distinguish legitimate and trusted sending sources from non-trusted ones. EasyDMARC provides the Source Classification functionality, which identifies valid sending sources and reports those to the owner of the domain. This functionality dramatically decreases the time to move the domain policy from “none” to “reject”.

Anomaly Detection - AI-powered anomaly detection recognizes and informs/alerts owners about anomalies detected in their DMARC reported data. This is very useful for identifying

targeted attacks, human errors in the infrastructure, and/or third-party service changes (if the company uses third-party services).

DMARC Advanced Filtering - Precise identification of details in aggregate data helps system administrators track down any possible issues resulting in a faster, easier, and hassle-free advancement of DMARC policy. Filtering is designed based on DMARC experts’ hands-on experience and includes every single case of data filtering identified during the past 5 years.

Custom Alerts - On top of its own alerting algorithms, EasyDMARC offers customers the ability to set up custom alerts that specify the importance and the category of the metrics to be monitored. Administrators can be notified via email and stay up-to-date with any changes in their email infrastructure.

Single Pane of Glass for Domain Management - Identifying problems, reporting, and management across hundreds of domains can prove to be difficult and time-consuming.

EasyDMARC provides a single pane of glass to simplify and expedite the monitoring and control process, while decreasing the time spent on DMARC deployments. This approach provides quick access to multiple domains from a single dashboard, as well as filtering capabilities for the entire infrastructure.

Source Reputation Check - Sending source quality checks is a nightmare especially for multiple domains and their associated services and IP addresses. EasyDMARC's source reputation check automatically detects sending sources and performs checks to alert administrators of important changes. This allows checking IP address or domain name correlation against popular blacklists and delisting of blacklisted IPs to boost domain reputation.

Industry-leading BIMI Implementation Tools - BIMI allows an organization to accompany the "from" address with a brand logo. BIMI is a standard, currently supported by Google and Yahoo which reduces the chances of spam complaints while adding an important element of trust to an organization. EasyDMARC is a pioneer in the DMARC Industry providing tools for BIMI implementations including deployment, error correction, and control.

- **What is that package configuration I am purchasing at Openprovider?**

Together with our Partner EasyDMARC we tailored the configuration of the product so that it remains packed with security features but at the same time the price remains very competitive in comparison to similar products in the market. Here's the detailed specification of the package. We will be adding more features in the future and also expand our offer with additional variants to meet our Resellers' and Customers' needs! You can find more details on every feature in our EasyDMARC Knowledge Base section.

Important:

The below list contains basic set of features.
Our partner EasyDMARC is constantly working on new features and most of them will be added to EasyDMARC product. We will keep our Resellers and Customers informed about any new feature that is added to EasyDMARC package.

25.000 emails / month
1 Domain
1 User
1 month data history
Domain Scanner
Tools - SPF, DKIM, DMARC, BIMI, MTA-STS, TLS-RPT
Managed DMARC
Managed BIMI

Email investigation
Phishing URL check
DNS Record Checker
Aggregated reports (RUA) by Compliance or by Geolocation
Failure Reports (RUF)
Blacklist check / Reputation monitoring
Email Vendor Identification
Basic Daily/Weekly/Monthly email reports
Custom email Alerts for DNS Records change/Blacklist/Email Volume

EasyDMARC - SPF Record Check and Lookup

What is an SPF Record Check and Lookup?

SPF lookup checks if an SPF record is published on a domain and deployed correctly. It also features a DNS lookup counter.

What is an SPF record generator?

SPF Record Generator tool allows you to generate an SPF record. Generally, SPF provides mechanisms, qualifiers, and modifiers to allow domain administrators to specify IP addresses in a highly flexible way. SPF Record generator is particularly made to make the process easy and fast.

Use SPF Record Generator, if you want to:

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

What is an SPF record raw checker?

SPF record raw checker allows you to validate your SPF TXT record before publishing it in DNS. Email deliverability and domain protection will improve once you have a properly set up SPF record. SPF record is correctly configured when an SPF record checker finds the SPF record, the record does not exceed 10 lookups limit and the configured IP addresses are the ones from which emails are sent.

EasyDMARC DNS Records Lookup

DNS Records Lookup

What is the DNS Records Lookup tool?

The DNS Records lookup tool retrieves the DNS records of your domain and show them in a list. You can run DNS lookup against well known DNS servers such as Google, Cloudflare, Quad9, or the domain's authoritative name server (SOA). Use the DNS lookup tool to verify that you have configured correct DNS records for your domain, so you can avoid any downtime. DNS records types you can check include A, AAAA, MX, CNAME, TXT, PTR, NS, SOA.

Description of DNS Records types

A record:

This DNS record category points a fully qualified domain name (FQDN) to an IPv4 address and acts as a translator by converting domain names to IP addresses. It could be used for pointing to both the main domain and subdomains.

AAAA record:

This is similar to A record but points to an IPv6 address. IPv6 has been created due to the shortage of IPv4.

MX record:

This record type points to the mail server(s) and specifies their priority for receiving email for a domain. It should point to a mail server name and not an IP address.

CNAME record:

It’s an alias that points domain or subdomain to another hostname, but never an IP address. The aliased domain gets all DNS records or target hostname and is commonly used to associate subdomains with the existing main domain.

TXT record:

Administrators can add limited human and machine-readable notes via this record type. It can also be used for email validation, site ownership verification, SPF, DKIM, DMARC, MTA-STS, policies, etc.

PTR record:

This record points the IPv4 or IPv6 address to a domain name. It provides a reverse DNS record (also known as rDNS record) pointing an IP address to the domain hostname. These records require domain authority and can’t exist in the same zone as other DNS record types.

NS record:

It points to the name servers which have authority in managing and publishing DNS records of a given domain. These are the authoritative DNS servers that handle any query related to that domain.

SOA record:

This record provides essential information about the domain. It contains data on the master node of the domain authoritative nameserver, domain administrator’s email, DNS zone’s serial number, etc. It’s used to direct how a DNS zone propagates to secondary name servers.

EasyDMARC Email Investigation

Email Investigation

What is Email Investigate and how can it help?

When adding a DMARC record into your DNS, it takes some time for the first report to arrive. Instead of waiting, you can get your first aggregate report instantly and check if your particular sending source is configured properly.
Speed up your DMARC policy enforcement journey and check your email sending source's compliance with our new feature.
Email Investigate helps you detect and troubleshoot any potential issues with delivery. It also gives you a configuration overview with email authentication from any of your email sending services.

How Email Investigate works?

Email Investigate provides a unique inbox address to which you can send an email from the specific service.
It analyzes the results and provides you with detailed information about SPF, DKIM, and DMARC records. It also reveals the DMARC policy that will be applied to your email and retrieves the configuration guide for source authentication setup.

Here are the steps to follow:

1. Send an email to Investigate inbox address from the email sending source you want to check;
2. Open the email for a more detailed breakdown of each email sending source and its current status;

3. The email will appear in Investigator's inbox labeled as 'Compliant' or 'Non-compliant';
4. Adjust your domain setup where necessary by following the instructions provided to you.

How to manage your DMARC record using EasyDMARC

EasyDMARC provides intuitive and easy to use ways to manage your DMARC record, its settings and policy. There are actually 2 ways to do it using EasyDMARC control panel by adding one of the below records to your DNS zone:

1. CNAME - preferred and the easier way to set up and manage DMARC
2. TXT - requires more manual work when you want to adjust the settings

Using CNAME record allows you automate DMARC management without a need to manually change records in the DNS zone whenever you wish to adjust DMARC policy.

Important:

When you buy EasyDMARC together with a new domain in RCP or activate it for existing domain and decide to use our nameservers, we will automatically add the below DMARC CNAME record to your DNS zone. Otherwise you have to add CNAME manually to your DNS zone.

Here’s the step by step instruction on how to set up EasyDMARC using both ways.

Setting up EasyDMARC using CNAME record (for domains not using Openprovider nameservers)

Just before you purchase and activate EasyDMARC with a selected domain, you will be presented with a popup screen with brief information on how to set up your DNS zone with DMARC CNAME record:

Important:

- You need to remove existing DMARC TXT record from DNS zone before adding this smart CNAME record.
- If you use CDN (e.g. Cloudflare), make sure that added CNAME record is not proxied.

Publish DNS record

To allow EasyDMARC manage DMARC policy for this domain please create the following record in your domain DNS. This is a one time action, after which all changes to DMARC, you made in our platform, will be automatically reflected in DNS.

HOST: _dmarc.*example.com*
Type: CNAME
Value: _dmarc.*example_com*._d.dmarcprotect.me

Simply go to your DNS management portal and create a new CNAME record, that will contain:

- **HOST**: _dmarc.<*your domain name*>
- **Type**: CNAME
- **Value**: _dmarc.yourdomain_extension._d.pro.dmarcprotect.me (for example _dmarc.openprovider_com._d.pro.dmarcprotect.me

Important: ***The above value is just given as an example. Always use the value shown in the control panel to create CNAME record.***

After you add CNAME, you can log in to EasyDMARC control panel then go to section **Hosted DMARC** where you will be able to manage various settings related to your DMARC:

Here you can decide about:

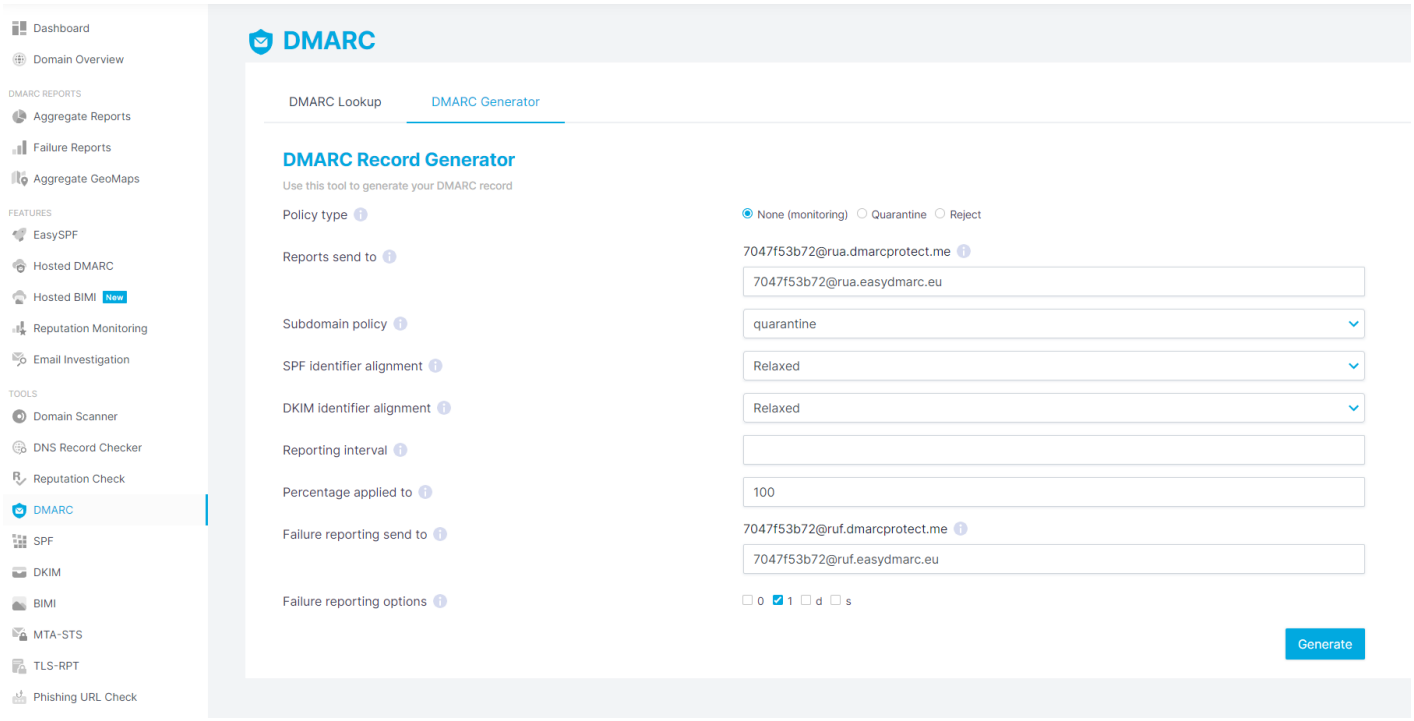
- The DMARC policy: **NONE, Quarantine, Reject.**
- Alignment modes for SPF and DKIM.
- How often you wish to receive reports.
- How the failure reports should be handled.

Important: Every change you will make in the EasyDMARC will be automatically applied - there is no need to change anything in the DNS zone of your domain!

Setting up EasyDMARC using TXT record

By default we encourage you to use CNAME records to set up DMARC. However for various reasons you may want to handle DMARC more manually by using a TXT record.

After you purchase EasyDMARC for a selected domain, please log in to EasyDMARC control panel and go to **DMARC** section and then **DMARC Generator**



This tool allows you to specify various settings for DMARC. Once you provide all necessary details, please click **Generate** and you will be provided with a TXT record that you have to add to your domain's DNS zone.

Important: Whenever you wish to adjust for example the policy type for DMARC, you have to generate a new TXT record in the EasyDMARC tool and then update it in your domain's DNS zone.

Once the DMARC is configured and the CNAME or TXT record is added to the DNS zone, the EasyDMARC tool will start collecting the data in the panel. Usually it takes 4 to 6 weeks to have relevant information in the panel and based on it you can start tailoring the policies for DMARC.

Phishing URL Check feature in EasyDMARC

Phishing URL Check

How Does it Work?

Wouldn’t it be magical to paste the text in a box and quickly learn whether the included links contain anything suspicious?

EasyDMARC’s Phishing URL Checker tool is a robust AI-powered analyzer that can accept a text of any kind and give you the verdict in a few seconds.

Here's how the tool works:

- Extracts all URLs from the pasted text
- Scans the links to detect any issues
- Tells you whether the links are "Good" or "Suspicious."

EasyDMARC’s phishing link checker is a proprietary machine-learning model designed to make email security just a little bit easier.

How to Identify URL Phishing?

While using our tool is a safe way to eliminate the risk of suspicious URLs, you can identify phishing attempts or malicious links with the naked eye.

Ask yourself the following questions before clicking on any URL:

Is the Message Legitimate?

When you receive a link directing you to another website, it can be potentially harmful unless proven otherwise

- Does it urge you to take action?This is a sign that you or your feelings are being exploited.

- Who’s sending you the message and what do they wantIf the request seems in any way weird, always seek verbal confirmation.

- Is the message grammatically correct? Check for any blunders in spelling or grammar. It’s not that hackers don’t know how to spell—they just misspell words to avoid spam filters.

- Does the email ask you for personal information?If you receive an email from an unidentified institution requesting sensitive information, the chances are that it’s a scam.

Does the URL Look Suspicious?

Analyze the received URL closely before engaging it. Hover your cursor on the link and check the text that displays at the bottom left of your browser. This helps identify the source, even if the display link is shortened.

Are There Any Homographs in the Domain Name?

Professional cybercriminals use letter combinations that look similar ("rn" looks like "m"), letters from foreign alphabets (Cyrillic "a" looks like Latin "a"), or numbers that look like letters ("0" looks like "O").

Is There an "S" in the HTTPS?

Websites with an SSL (Secure Socket Layer) certificate are more secure because they ensure your data is encrypted. If the link you received via email does not use HTTPS, avoid clicking it.

How to Protect Against URL Phishing

A link is not always what it looks like. Cybercriminals go to great lengths to create malicious websites resembling real ones. Stay alert!

Security Awareness

Even if you’re relying on technology to guard your organization, security awareness training is vital. Teach your employees how to check phishing URLs, avoid scams, detect malicious attachments, and deal with various attack types.

URL Filtering

Absolutely. Both SPF and DKIM play a major role in the email authentication world. In fact, unlike SPF, DKIM tends to survive the Forwarding cases.

DMARC Compliance

Absolutely. Both SPF and DKIM play a major role in the email authentication world. In fact, unlike SPF, DKIM tends to survive the Forwarding cases.

How to Check Link Safety With EasyDMARC

You can use EasyDMARC’s phishing link checker by copying and pasting the URL into the search bar and clicking "Enter". In a couple of seconds, you’ll receive information about each link separately.You can also paste text containing links into the box. The tool checks for phishing URLs, detecting and analyzing up to 20 links at a time.

What Does a "Good URL" Mean?

"Good" is one of the outcomes of our phishing link checker. It usually means the link doesn’t contain any malicious elements. Basically, it’s the legit brand link and can’t lead to a phishing site.

What Does a "Suspicious URL" Mean?

"Suspicious" is the second outcome that our phishing link checker tool can produce. It means the URL in question leads to a malicious website, and it’s better to avoid clicking it.

What is BIMI and how to manage it with EasyDMARC

BIMI

Why does BIMI Check and Lookup matter?

BIMI (Brand Indicators for Message Identification) allows Domain Owners to coordinate with Mail User Agents (MUAs) to display brand-specific Indicators next to properly authenticated messages. There are two aspects of BIMI coordination: a scalable mechanism for Domain Owners to publish their desired indicators, and a mechanism for Mail Transfer Agents (MTAs) to verify the authenticity of the indicator. The BIMI Record Checker tool checks if your BIMI record is valid and informs whether you have actions to do related to the BIMI record validation process. To run a BIMI record lookup, enter your domain in the Domain section and click the Check BIMI button.

Why does the BIMI Record Generator matter?

Our platform allows generating a BIMI record. Generally, BIMI works in conjunction with DMARC, DKIM, and SPF to enable recipient email providers to identify the company correctly and allow your messages to appear in the inbox. EasyDMARC’s BIMI Record Generator tool is particularly made to make the process easy and fast. To generate a proper BIMI record you need to:

- Input the HTTPS URL to SVG file
- Input the URL to the trust certificate

What is a BIMI Logo Converter?

The logo referenced by a Brand Indicators for Message Identification (BIMI) record must be in a specific SVG Tiny Portable/Secure (SVG P/S) format. Existing graphic design software and generator tools don't support that format yet. EasyDMARC provides a tool to fix SVG Tiny 1.2 issues and

convert SVG Tiny 1.2 images, logos to BIMI-compatible SVG P/S images..

What is DKIM and how to manage it with EasyDMARC

DKIM Lookup

Why does DKIM lookup matter?

DKIM record lookup tool checks if your DKIM record is published for domain selector (as a subdomain) and deployed correctly. It also informs whether you need to take action regarding the DKIM record validation result. To run a DKIM check, enter your domain in the Domain section, input your selector name and click on the DKIM Lookup button.

What does DKIM lookup do?

- Check if the DKIM TXT record is published in DNS for the domain
- Check the published DKIM TXT record syntax
- Validate DKIM public key associated with selector

DKIM - How does it work?

The domain owner generates a public/private key pair to be used for signing outgoing messages. Private keys are stored on the email server, while public keys are implemented in the domain's DNS server. Upon sending emails, the server uses the stored private key to generate a digital signature of the message, which will be inserted in the message header. The receiving server, on the other hand, will retrieve the sender's Public Key from DNS to verify that the signature was generated by the matching private key. A match effectively proves that the email was truly sent from, and with the permission of, the claimed domain and that the message headers and content have not been altered during transit.

How to analyze DKIM selector from DMARC Aggregate Reports

DMARC Aggregate reports contain a specific tag with” selector name”, which helps you easily identify your DKIM signature Selector name. We also convert this data into an easy-to-read format where you can identify your DKIM Selector name under the “DKIM Auth. Results” tab of your dashboard.

How to check DKIM record in your DNS

To check your DKIM Record in your DNS, you need to find a TXT or CNAME type record with the Host / Name similar to [selector]._domainkey.yourdomain.com.

How to analyze DKIM selector from Email Headers

DKIM selector is inserted into the DKIM-Signature email header as an s= tag when the email is sent.

E.g: DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=easydmarc.com; h=content-type:from:mime-version:subject:reply-to:x-feedback-id:to: list-unsubscribe; s=s1;

How many DKIM records can I have?

There are no limitations. You can have multiple DKIM Records, since technically speaking each DKIM record can be associated with a unique selector. In fact, if your domain uses multiple email services to send emails (Marketing, Transactional, etc.), multiple DKIM selectors and private/public key pairs must be used to separate these services.

Investigating DKIM Issues

Use EasyDMARC's DKIM Lookup tool to verify if your DKIM record and Public Key are properly implemented without any syntax or other issues

Analyze DMARC Aggregate Reports that contains all the relevant information of your DKIM Signatures (If they’re passing or failing)

Investigate Email Headers to retrieve DKIM-Signature, and analyze the underlying results

If you’re using third-party ESPs and obtained DKIM Public key from them, make sure you have “Activated” DKIM Signing process from their portal

Is DKIM part of the DMARC protection?

Yes. DKIM is one of the authentication protocols (along with SPF) DMARC relies on to provide a set of instructions to receiving email servers on how to handle unauthenticated mail.

If I have an SPF do I have to implement DKIM?

Absolutely. Both SPF and DKIM play a major role in the email authentication world. In fact, unlike SPF, DKIM tends to survive the Forwarding cases.

How to generate a DKIM record?

How to generate a DKIM record? DKIM adds an encrypted signature to the header of all outgoing messages. Email servers that get signed messages use DKIM public key to decrypt the message header and verify the message was not changed after it was sent. Generally, DKIM detects forged header fields and content in emails. As DKIM works with Private and Public keys, there are multiple use-cases for DKIM implementation:

- 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.
- For dedicated servers, EasyDMARC's DKIM Generator tool is particularly made to make the process easy and fast. You will securely store the Private key in your own server while implementing the Public key in your DNS.

How does DKIM work?

DKIM uses a pair of keys, one private and one public, to verify messages. A private domain key adds an encrypted signature header to all outgoing messages sent from your email domain. A matching public key is added to the Domain Name System (DNS) record for your email domain. Email servers that get messages from your domain use the public key to decrypt the message signature and verify the signed message sources.

How to use a DKIM Record Generator?

In order to use the DKIM Record Generator, you need to specify the “selector” name, your domain name, and the Key length.

- A selector can be any given name. Use a name to clearly identify the DKIM Signature in future.
- Enter your domain name, this should match the visible “From” address domain.
- Specify the Key length. We support 1024, 2048, and 4096-bit size keys.
- Once DKIM Record is generated, store the Private Key in your mail server configurations (with .pem file), and implement the Public Key in your DNS Zone.

Do I need to generate a DKIM Record if I’m using a third-party ESP?

No. This is a common misconception. You only need to generate a DKIM Record only for your dedicated mail servers. For Third-Party ESPs such as Google Workspace, Microsoft, Mailchimp, etc. they already store the Private Key in their own mail server configurations and provide only Public Signatures for their users. The only action you need to take is to get the Public Signature from the given ESP portal and implement it in your DNS, and later turn on the “Activation” for DKIM within the ESP portal.

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.