

DMARC Instructions:

A DMARC record instructs mail receivers on how to apply SPF and DKIM to messages purporting to be from your domain. SPF is a DNS-only solution which specifies the mail servers allowed to send on behalf of your domain, while DKIM will require both a DNS record as well as some configuration of your SMTP service. DKIM should only be configured on your SMTP server. It is only recommended to configure DKIM directly within your MyClient portal when you are using the built-in mailer. Many online tools exist to validate your DMARC, SPF and DKIM records. We recommend validating each of these after implementation.

All records should be enclosed in double quotations ("...") when applied as a DNS TXT record.

DMARC Record:

The DMARC record should be implemented after SPF and DKIM are ready, but it is useful to understand how it works before proceeding with those.

A DNS TXT record, similar to the following, must be assigned on the subdomain `_dmarc` of the domain for which you're sending messages (i.e. `_dmarc.yourdomain.com`):

```
"v=DMARC1; p=none; sp=none; rua=mailto:example@yourdomain.com;
ruf=mailto:example_two@yourdomain.com; aspf=r; adkim=r;"
```

All tags should be formatted as `tag=value;`. It's important to understand what these tags mean, particularly as the record will need to be adjusted over time. The `v` tag must appear first in the record (it is always `v=DMARC1;`), followed by the `p` tag. After these two tags, tag order is not important.

DMARC Record Tags:

Primary DMARC Record Tags:

These tags are the main tags you should configure for your DMARC record. Only `v` (version) and `p` (policy) are mandatory.

- `v` - Version (mandatory):
 - Value is always `DMARC1`.
- `p` - Policy (mandatory):
 - Possible values are 'none', 'quarantine', and 'reject'.
 - This tag dictates what should be done when mail sent on behalf of your domain fails to clear DKIM or SPF checks. 'none' will do nothing, 'quarantine' will classify messages as spam, and 'reject' will block delivery entirely.
 - New DMARC implementations should start with a policy of 'none' to give you time to ensure that genuine mail is being delivered without errors.

- **rua** - Aggregate report address (optional, but *strongly* recommended):
 - This value is an email address at which you will receive regular aggregate reports. Multiple email addresses can be specified by comma separation (e.g. `rua=mailto:one@example.com,mailto:two@example.com`;). Each email address must be prefixed with `mailto:`.
 - Audit reports help you to verify whether all genuine senders are passing DMARC correctly.
 - Ensure that you either specify email address/es belonging to the domain that you are configuring DMARC for, or that the domains of any specified addresses implement an external reporting authorization records for your domain.
 - This is done by creating a new TXT record at the destination domain, like so:
 - `yourdomain.com._report._dmarc.destinationdomain.com`
 - The value of this TXT record must be "v=DMARC1;". The subdomain must always match your full domain, followed by `._report._dmarc`.
 - Aggregate reports are sent every 24 hours by default, however you can change this by specifying the **ri** tag with a number of seconds defining the report frequency (the default 24 hours would be expressed as `ri=86400`;). 24 hours is generally the minimum frequency, although individual receivers may implement their own minimum frequency.
- **ruf** - Forensic report address (optional): This value is an email address at which you will receive forensic reports. Rules for this value are as above for the **rua** tag, except the **ri** tag does not apply. A small number of receivers support the **ruf** tag, which produces a forensic report after each message failure. This tag is optional, and could reasonably be disregarded given the small number of receivers that actually send forensic reports.

Alignment DMARC Record Tags:

These tags specify how to handle validation in consideration of the alignment of 'header from', and 'mail from' values. Header from is the address displayed in mail clients and used when replying, while mail from is primarily used for bounce notifications. MyClient uses the same address for each when sending reports - in essence, these are already aligned. Many mail services do not send in alignment however (particularly mailing list services). If you utilise other mailing list services, the safest approach is to utilise the tags detailed below, setting a 'relaxed' policy for each.

- **aspf** - SPF Alignment:
 - Possible values are **r** (relaxed) and **s** (strict).
 - This tag dictates whether the SPF record for this domain should apply when header from and mail from are not in alignment.
 - Strict mode will prevent the SPF record for this domain applying when the domains are not in alignment, while relaxed will allow the SPF to apply regardless.
 - Note on alignment: Domains do not need to be identical to be aligned - a domain in combination with one of its subdomains would also be considered aligned.
- **adkim** - DKIM Alignment:
 - Possible values are **r** (relaxed) and **s** (strict).
 - This tag dictates whether DKIM records for this domain should apply when header from and mail from are not in alignment.

- Strict mode will prevent the SPF record for this domain applying when the domains are not in alignment, while relaxed will allow the SPF to apply regardless.
- Note on alignment: Domains do not need to be identical to be aligned - a domain in combination with one of its subdomains would also be considered aligned.

Additional DMARC Record Tags:

- **sp** - Subdomain policy:
 - Possible values are **none**, **quarantine**, and **reject**.
 - This tag supports the same values as the **p** (policy) tag, and also functions in the same way, but applying instead to mail from child domains.
 - You can immediately set this to **quarantine** or **reject** if you do not send mail from child domains, otherwise start with **none**, as per the policy tag.
- **ri** - Report interval:
 - Possible values are numbers of seconds, at **86400** or higher.
 - This tag determines the frequency at which aggregate reports are sent.

Graduating policy:

After verifying that genuine senders are covered by your SPF configuration and are implementing DKIM signing correctly, you can graduate your record to **quarantine** (or directly to **reject**, which is the recommended policy setting if you are confident that all genuine senders will not be impacted). General advice is to gradually escalate over several weeks or even months, using another tag which has not yet been covered:

- **pct** - Percentage of messages to apply policy to:
 - Possible values are all (integral) numbers from **0** to **100**.
 - This tag determines which percentage of messages a receiver should apply the DMARC policy for this domain to. With a policy of **none**, this tag will have no effect, however it can be used at values under 100 to mitigate the effects of a transition to **quarantine** or **reject** on genuine mail which is still failing SPF or DKIM checks.

When graduating policy, you should typically move from **none** to **quarantine**, starting with a low **pct** value (e.g. **10** or **25**), and increasing this a few times to reach **100**. After reaching **100** under the **quarantine** policy, you should graduate to **reject**, starting again from a low value and increasing to **100** over time.

SPF Record:

Your SPF record specifies the mail servers which are allowed to send on behalf of your domain.

You will need to assign a TXT record like the following at the root of your domain (e.g. *yourdomain.com*):

```
"v=spf1 include:spf.someothermailprovider.com ip4:111.111.111.111
ip4:222.222.222.222 ~"
```

Unlike a DMARC record, you should not use semicolons here. The record must always begin with `v=spf1`, and should end with one of the `-`, `+` or `~` qualifiers, followed by the `all` keyword (e.g. `-all`, `+all`, or `~all`). The `all` keyword, in combination with a qualifier, determines how to handle all mail servers representing your domain which are not specified in the SPF record: `+` is a pass, `-` is a fail (reject), and `~` is a "soft fail" (this generally allows messages to be delivered but may result in categorization as spam). `-` or `~` are the generally recommended qualifiers to use with the `all` keyword.

Wherever practical, you should prefer `ip4` or `ip6` tags to allow a server, as other tags will require a DNS lookup, and SPF records allow a maximum of 10 DNS lookups (including `a` tags, as well as any lookups incurred by an `include` tag).

Primary tags:

- `v` - Version (mandatory):
 - Value is always `spf1`.
- `ip4` - IPv4 address (optional, default behaviour is a pass unless prefixed with `-` or `~`):
 - Value must be an IPv4 address for a server that you wish to allow (or deny).
- `ip6` - IPv6 address (optional, default behaviour is a pass unless prefixed with `-` or `~`):
 - Value must be an IPv6 address for a server that you wish to allow (or deny).
- `a` - DNS 'A' record reference (optional, default behaviour is a pass unless prefixed with `-` or `~`):
 - Value must be a domain name pointing to a server that you wish to allow (or deny).
- `include` - Include external SPF (optional):
 - Value must be a domain name hosting an SPF record specifying one or more servers that you wish to allow (or deny). This is commonly required by mail service providers, who manage their own SPF records which can be associated with your domain to permit sending.

To allow MyClient to send on behalf of your domain when using its built-in mailer, you need an SPF record with either an `include:servermanagerpro.com` entry, or an `ip4:xxx.xxx.xxx.xxx` entry (where `xxx.xxx.xxx.xxx` is replaced with your portal's IP, as specified at the bottom of the Manage Servers page). The `servermanagerpro.com` SPF record does not contain DNS lookups, and so will not contribute to your SPF's DNS lookup limit. If you're configuring your own domain for usage with MyClient, it's likely that you already have an SPF record, in which case you can simply add the `include:...` or `ip4:...` tag to your existing record. If you're creating a new record, do keep in mind that any other mail services being used on behalf of your domain may be impacted, and should also be allowed in your SPF record as per their own documentation.

DKIM Record:

DKIM records specify public keys which correspond to private keys used by mail servers to sign messages which are sent on behalf of your domain.

Generally, each mail service that you use with your domain should have its own public/private keypair. These are assigned to 'selectors' on your domain, which point to TXT records containing a public key.

You can generate a new DKIM key pair in MyClient by visiting **System Settings** -> **System Behaviour** -> **Gateways**. Locate the **Email > Signing** -> **DKIM** area and click **generate new..** to create a new public private key pair.

After generating your key pair, decide on a selector that you wish to use for MyClient (e.g. **portal**, **myclient**, **default**, etc). Selectors can only contain letters, numbers and hyphens (and a hyphen can not be the first character), and input this in the **Selector** field. Finally, enter the email address you'll be using in the **Email** field, and click **Save Changes**.

Copy the public key value that was generated in the previous step to a text editor, and remove the prefix/suffix sections (-----BEGIN PUBLIC KEY----- and -----END PUBLIC KEY-----), then remove all line breaks.

You should start with something like this:

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1GExoSeLjg49J8nPe/Tx
nKNHyR6d0JZykLtcz99JDeB0puukthi+Zhn32gG6JpPHie0lc2qTtamDCI7WP4r1
fdXsXlisDkzthjFEsU3oH5hVhDZ7xZT39leXfN7z0I1C32M0cTlQEV0WVK7ZohXi
/BuEXFlyQf7xoqpljkPNk4bB70/eQtEaQRdZq0gN50CCs2rdUFR0JY0yz/OvRgwI
8rY6ii22oAq0lg1Mn+kodY3JgGyOutIaph/1JD8qg4hGLL4FoYvvuim2i6vMGyLB
GapnDu2UxhWPhL1lVP+m23ciCW9l21u+CuEiQ504nNET3C5lBHsokJ3FDC3saADD
hQIDAQAB
-----END PUBLIC KEY-----
```

And end up with something like this:

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1GExoSeLjg49J8nPe/TxnKNHyR6d0JZykLtcz9
9JDeB0puukthi+Zhn32gG6JpPHie0lc2qTtamDCI7WP4r1fdXsXlisDkzthjFEsU3oH5hVhDZ7xZT39leX
fN7z0I1C32M0cTlQEV0WVK7ZohXi/BuEXFlyQf7xoqpljkPNk4bB70/eQtEaQRdZq0gN50CCs2rdUFR0JY
0yz/OvRgwI8rY6ii22oAq0lg1Mn+kodY3JgGyOutIaph/1JD8qg4hGLL4FoYvvuim2i6vMGyLBGapnDu2U
xhWPhL1lVP+m23ciCW9l21u+CuEiQ504nNET3C5lBHsokJ3FDC3saADDhQIDAQAB
```

Take care not to accidentally delete any other characters while removing the line breaks.

Next, you'll need to use your condensed public key to create a new TXT record on your domain. The record will need to look like the following:

```
"v=DKIM1; k=rsa; p=yourpublickeyhere;"
```

Like the DMARC record, all entries must be capped with a semicolon. DKIM TXT records must always begin with **v=DKIM1;**.

This record must be added to the subdomain `yourselector._domainkey` (i.e. `yourselector._domainkey.yourdomain.com`), where *yourselector* is replaced with the selector that you assigned to the key pair in MyClient earlier.

Primary tags:

- **v** - Version (mandatory):
 - Value is always **DKIM1**.
- **k** - Key type (mandatory):
 - Value should always be **rsa** when using keys generated by MyClient.
- **p** - Public key (mandatory):
 - The public key generated earlier.

The key generated by MyClient may be too long to fit in a single TXT record, depending on your DNS provider. If this is the case, identify an arbitrary point at approximately halfway through the record, and split the record cleanly there using an extra pair of double quotation marks; this will result in two values. If your DNS provider allows it, save these two values to the same TXT record field on the **same line**, with no separation. If you cannot save these to the same field, assign the separate halves to two new adjacent TXT records (these must be adjacent to ensure that they are joined correctly by mail services validating the record).

- Long record example:

```
"v=DKIM1; k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1GExoSeLjg49J8nPe/TxnKNHyR6d0J
ZykLtcz99JDeB0puukthi+Zhn32gG6JpPHie0lc2qTtamDCI7WP4r1fdXsXlisdKzthjFEsU3oH5
hVhDZ7xZT39leXfN7z0I1C32M0cTlQEVOVVK7ZohXi/BuEXFlyQf7xoqp1jkPNk4bB70/eQtEaQR
dZq0gN50CCs2rdUFROJY0yz/OvRgwI8rY6ii22oAqOlglMn+kodY3JgGyOutIaph/lJD8qg4hGLL
4FoYvvuim2i6vMGyLBGapnDu2UxhWPhLl1VP+m23ciCW9l21u+CuEiQ504nNET3C5lBHsokJ3FDC
3saADDhQIDAQAB;"
```

- Split single-line record example:

```
"v=DKIM1; k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1GExoSeLjg49J8nPe/TxnKNHyR6d0J
ZykLtcz99JDeB0puukthi+Zhn32gG6JpPHie0lc2qTtamDCI7WP4r1fdXsXlisdKzthjFEsU3oH5
hVhDZ7xZT39leXfN7z0I1C32M0cT""lQEVOVVK7ZohXi/BuEXFlyQf7xoqp1jkPNk4bB70/eQtEa
QRdZq0gN50CCs2rdUFROJY0yz/OvRgwI8rY6ii22oAqOlglMn+kodY3JgGyOutIaph/lJD8qg4hG
LL4FoYvvuim2i6vMGyLBGapnDu2UxhWPhLl1VP+m23ciCW9l21u+CuEiQ504nNET3C5lBHsokJ3F
DC3saADDhQIDAQAB;"
```

- Separate records example:

```
"v=DKIM1; k=rsa;  
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1GExoSeLjg49J8nPe/TxnKNHyR6d0J  
ZykLtcz99JDeB0puukthi+Zhn32gG6JpPHie0lc2qTtamDCI7WP4r1fdXsXlisDkzthjFEsU3oH5  
hVhDZ7xZT39leXfN7z0I1C32M0cT"
```

```
"lQEV0WVK7ZohXi/BuEXFlyQf7xoqpljkPNk4bB70/eQtEaQRdZq0gN50CCs2rdUFR0JY0yz/OvR  
gwI8rY6ii22oAq0lg1Mn+kodY3JgGyOutIaph/1JD8qg4hGLL4FoYvvuim2i6vMGyLBGapnDu2Ux  
hWPhL1lVP+m23ciCW9l21u+CuEiQ504nNET3C5lBHsokJ3FDC3saADDhQIDAQAB;"
```