Overview

Welcome to Maropost! Before you can actually start mailing from your Maropost for Marketing account, you will first need to set up several DNS and email items.

A brief list appears below, with more detailed directions for each item. If more information is needed about how to implement these items, your Maropost Customer Success Manager can schedule a conference call with you to go over them. If you would prefer that Maropost set them up for you, then we will need the site for your DNS/email hosting provider(s) and your access credentials.

Setup Items

1) A record
2) Link-branding domain
3) SPF record
4) DKIM
5) GOOGLE TXT Record
6) Yahoo Feedback Loop (FBL)
7) DMARC Record (*Optional*)

A RECORD

The A record is only required if your account is set up with new (and not existing) dedicated IP addresses. If you are sending entirely from Maropost's shared IP address pool, then disregard this section.

The A record is a type of DNS record, that tells the world what IP address your domain belongs to. It should be a subdomain of your From domain. You will need one subdomain for each dedicated IP address that Maropost has assigned to you. E.g., if your From domain is "example.com" (replace with your actual From domain in practice) and you have two dedicated IP addresses, then you will need two subdomains of "example.com", such as:

```
mta1.example.com
mta2.example.com
```
Etc.

Don't forget to replace "example.com" with your own domain when you set this up in production. Maropost will need to know exactly what subdomains you have assigned and which ones point to which IP address, so we can set up the corresponding PTR records. The A records and PTR records must match, as this is a general industry requirement for sending email.

IMPORTANT!
Notify your Customer Success Manager as soon as you have set up your A record. Be sure to specify which subdomain you have assigned to which IP Address so that Maropost can set up the proper PTR records.

LINK-BRANDING DOMAIN

This is a CNAME record which will make the links in your emails appear as your own domain instead of a redirect from our shared domain. The link-branding domain will redirect to the ultimate target URL. That way, the link-branding domain will be evaluated on the merits of your own sending practices instead of those of anyone else. To set this up, you need to choose a domain and create a CNAME record that references Maropost's link tracking server's domain name. The most common way to do this is with a subdomain of your From domain. If your From domain is "example.com", then the link-domain would be something like this:

```
links.example.com
```

Don't forget to replace "example.com" with your own domain when you set this up in production.

The Maropost link tracking server domain that your CNAME record will point to depends upon which hosted environment you log in to when you create your email campaigns.

Your Maropost for Marketing login domain	Your CNAME record points to:
app.maropost.com	api-us1.chd01.com
cloud.maropost.com	
cloud1.maropost.com	
app-ca1.maropost.com	api-ca1.chd01.com
app-eu1.maropost.com	api-eu1.chd01.com

IMPORTANT!
Notify your Customer Success Manager as soon as you have set up your CNAME record for your link branding domain so that Maropost can complete your account configuration.

If there's any reason why you can't use a subdomain, it's possible to use a different domain, but it should be one that will match your branding and not make your recipients suspicious of your email.

SPF RECORD

This uses the TXT DNS record type. It must be published by the customer for the domains set up with A records as above, to allow emails to be sent by the IP addresses assigned by Maropost for the customer's domain. In the simplest form, the value for the TXT record would be:

```
example.com descriptive text "v=spf1 include:spf.maropost.com -all"
```

(Don't forget to replace "example.com" with your actual domain.)

If the domain already has a TXT record for SPF, then you can just add "include:spf.maropost.com" to the end of it, before the "-all". This include record will automatically associate your domain with the IP addresses we will be sending your email from that is behind that include record.

After writing out a list of servers in the form of an SPF record, the right thing to do is to end an SPF record with something that says "and everything else on the Internet is NOT authorized".

The way the above is written is to use the “all” mechanism. This mechanism matches everything. By adding a prefix of “~” or “-“, the meaning of the mechanism is changed to be:

“softfail” in the case of “~”
“fail” in the case of “-“

Both mean “NOT PASS”, but there is a subtle difference. The ~all is a softfail and is usually used in testing a new SPF record out, but once you know that things are working it is recommended if you are NOT using DMARC to publish a –all after a certain time period.

IMPORTANT!
Notify your Customer Success Manager as soon as you have set up your TXT record for SPF.

DKIM RECORD

This also uses the TXT record type, and should be for your From domain. The entry for it would be like this:

```
default._domainkey.example.com
```

Don't forget to replace "example.com" with your actual domain.

Copy and paste the value for the DKIM record:

```
v=DKIM1; g=*; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDV37ViPSDKA47nSZwc+gVo/X
aLKiZeiwNSJMzyLtOie7VKjFxT/jMM7WTX2Mq//NV5ezSVWxSJh7fvdBKQJB7MWL
1XK2YtCYu19fb5hS1vrd9/oyihSc0PHBplnJmeXoc4+S9nAFoKS6IUt5VF/R+IJC
03xTtBnXpdtUDvCcpnaQIDAQAB
```

(All on one line, with no line breaks.)

When the DKIM record is visible in DNS, you can do a lookup on it here:

http://xnnd.com/dns.cgi?t=txt&d=default._domainkey.example.com

(Again, replace "example.com" with your actual DKIM domain.)

You can tell if you have the right value set in your DNS by seeing if it matches this one:

http://xnnd.com/dns.cgi?t=txt&d=default._domainkey.mp2200.com

IMPORTANT!
Notify your Customer Success Manager as soon as you have set up your TXT record for DKIM so that Maropost can complete your account configuration.

GOOGLE TXT RECORD

In order to set up your domain on the Gmail delivery dashboard offered by Google, you will need to create another TXT record in your DNS. The TXT value for this record will be shared by Maropost to you once you tell us what your From domain is. The value is unique per domain and we cannot share that value in this document.

IMPORTANT!
Tell your Customer Success Manager what From domain you intend to use for your email campaigns. Maropost will provide you with the TXT value that you need to add in your DNS server where your domain is hosted.

YAHOO FEEDBACK LOOP

Spam complaint feedback loops (FBLs) are an automated way to get reports about who makes spam reports about your messages so you can keep track of your complaint rates and automatically suppress the complainers. Most FBLs are IP-based, but Yahoo's is based on your DKIM domain. Maropost will ask Yahoo to set up an FBL for your DKIM domain, but Yahoo requires that a confirmation email be sent to the below email address at the DKIM domain:

postmaster@*yourdkimdomain.com*

IMPORTANT!
Notify your Customer Success Manager when your "postmaster@*yourdkimdomain.com*" email address has been set up. The Maropost Deliverability Team will trigger the sending of the confirmation to this email address.

IMPORTANT!
Notify your Customer Success Manager when you have received the Yahoo Feedback Loop confirmation email, including the login credentials provided in that email. Maropost needs the one-time password in order to complete your Yahoo FBL configuration.

DMARC TXT RECORD (*OPTIONAL*)

Domain-based Message Authentication, Reporting & Conformance (DMARC) is a policy that a domain (or website) publishes to let a receiving Internet Service Provider (ISP) know which email authentication methods (DKIM or SPF) are used by the sending domain. A published DMARC record basically serves two purposes:

1. Tell the recipient server to either: Quarantine the message or Reject the message or Allow the message to continue delivery.
2. Sends reports to an email address or addresses with data about all the messages seen from the domain.

Those two benefits alone drive home the huge value of setting up DMARC! Once published, a DMARC record is used by receiving mail servers (think Gmail or Yahoo! Mail) to determine what to do with a failed message. The receiving mail server at Gmail looks at the DMARC record for the policy to follow from the following choices:

- Do Nothing to the message
- Quarantine the message.
- Reject the message.

IMPORTANT!
Notify your Customer Success Manager as soon as you have set up your TXT record for DMARC

Final Check

Your Customer Success Manager will confirm with you that all steps included in this document are completed. Maropost will activate your custom authentication and link branding, and your account will be ready to start sending.