

New Email Account Setup Requirements for Mailout to Suppliers

Introduction

Outlined below are the email account setup requirements to permit Eftsurre to send the supplier emails from your domain as opposed to from the Eftsurre domain. This allows suppliers to receive emails directly from you who they are accustomed to dealing with. This significantly improves the supplier's trust and timeliness of responses as well as minimising disruption to your personnel.

Set-Up

1. Apply the requested additions to your Domain MX record as detailed in the step (Requirements to modify Domain MX record) below. [The changes to your Domain records permit Eftsurre to send emails through a specialist email program authorised to send emails from your domain and in so doing does not interfere, impede or place any burden on your email servers and services.]
2. Create an email group alias on your domain called noreply_verifications@yourdomainname.com.au (AUS), noreply_verifications@yourdomainname.co.nz (NZ) and add onboarding@eftsure.com.au as one of the group recipients. (If you are unable to do this, please contact Eftsurre for alternative options). Please ensure the distribution list is configured to allow external emails to be received and distributed to an external email address. (onboarding@eftsure.com.au)

Once the above two steps are completed the supplier will receive an email displaying the following:

From: Your Business Name noreply_verifications@yourdomainname.com.au (AUS),
noreply_verifications@yourdomainname.co.nz (NZ)

Requirements to modify Domain MX record

Please can your IT officer follow the steps below in order to accomplish the Domain MX record modifications required.

How do I add/modify relevant DNS records for my sending domains?

To add the SPF and DKIM records for your sending domains, you'll need to add records of type 'TXT' through your hosting provider, domain registrar, or DNS provider.

1. SPF record

If you don't yet have an SPF record, you'll want to add one for your domain. At a minimum, the value should be the following if you're only sending mail through Mandrill for that domain:
v=spf1 include:spf.mandrillapp.com ?all

If you already have a TXT record with SPF information, you'll need to add Mandrill's servers to that record by adding include:spf.mandrillapp.com in the record (before the last operator, which is usually ?all, ~all, or -all).

Note: Depending on the DNS registrar, some have an option to add/edit an SPF record directly rather than adding a TXT record with the SPF entry. If this is the case for your registrar rather than editing a specific SPF entry, please ensure that you add an actual TXT record with the value of:
v=spf1 include:spf.mandrillapp.com ?all

2. DKIM record

Create two CNAME records:

Step 1: one CNAME record with the name mte1._domainkey.yourdomain.com with the value dkim1.mandrillapp.com

Step 2: the second CNAME record with the name mte2._domainkey.yourdomain.com with the value dkim2.mandrillapp.com

Where yourdomain.com is your domain, for example:

mte1._domainkey.companyabc.com.au = dkim1.mandrillapp.com

mte2._domainkey.companyabc.com.au = dkim2.mandrillapp.com

3. Required DMARC setup - (Note: you can ignore this step if you already have a valid DMARC record)

There are many online references on how to set up a DMARC record and why it is important to help reduce spam emails, as well as the logistics of progressively enabling various options within DMARC whilst monitoring the impact of emails.

Good references from resources such as:

<https://mxtoolbox.com/dmarc/details/what-is-a-dmarc-record>

<https://dmarcreport.com/dmarc-record>

<https://dmarcian.com/why-dmarc>

If a DMARC record is defined, that is all required. For example, any one of the following settings is supported for DMARC:

- p=none
- p=quarantine
- p=reject

The instructions above are an extract from the [Mandrill website](#). The site includes extra information relating to Specific Domain Registrars as well as some Troubleshooting sections which include links to testing tools.