eTrigue Corporation
6399 San Ignacio Avenue
San Jose, CA 95119

www.etrigue.com

800.858.8500 toll-free
408.490.2901 fax

eTrigue Support Article ID: 115001028231 - Setup DKIM

Background

When campaign emails are sent from DemandCenter, the emails will originate from eTrigue's servers, but your recipients will see the FROM address displayed as coming from a sender from your domain.

Since the originating source is coming from eTrigue, but the actual sender (the "from") appears to be from your own domain, recipient mail servers may find that suspicious. This perceived suspicious behavior is due to the fact that email spammers can forge the "From" address on emails so that the spam appears to come from a user in your domain.

To help prevent this type of abuse, eTrigue recommends that users implement Sender Policy Framework (SPF). This mechanism makes the forging of emails much more difficult for spammers and improves the deliverability of your emails.

How does SPF help my deliverability?

SPF is an industry standard that deals with email authenticity. Major ISPs and many corporate spam/security filters perform SPF checks by default, so establishing SPF records in your domain's DNS records will allow you to pass these common checks.

SPF is established through Domain Name System (DNS) records and is important to setup for a number of reasons, including:

- If you do not have DKIM and/or SPF in place, it will make it tougher for your emails to reach your audiences because they may be marked as spam by corporate spam filters or personal junk folders.
- Recipient mail servers can verify the sender of an email.
- Confidence is increased everywhere. Recipients will know that their emails is from a legitimate source and not a spammer. Other organizations will know that you took the time to configure these widely industry standards.
- Messages that pass SPF checks will have a higher deliverability probability than messages without SPF, as they build "Trust" between the sending and receiving domains.

eTrigue Corporation
6399 San Ignacio Avenue
San Jose, CA 95119

www.etrigue.com

800.858.8500 toll-free
408.490.2901 fax

How to Setup SPF

Add the following to your existing SPF record before the "all" statement:

```
include:etrgmail.com
```

For example, if your existing SPF record looks like this:

```
v=spf1 mx ip4:67.108.8.192/26 -all
```

...then the updated SPF record to include eTrigue would look like this:

```
v=spf1 mx ip4:67.108.8.192/26 include:etrgmail.com -all
```

How can I check that I have SPF configured?

Use one of OpenSPF's referenced validator tools: http://www.kitterman.com/spf/validate.html

If your SPF has been updated correctly, the DNS information should proprograte publically (typically within 24-48 hours).

eTrigue Corporation
6399 San Ignacio Avenue
San Jose, CA 95119

www.etrigue.com

800.858.8500 toll-free
408.490.2901 fax

Frequently Asked Questions

Will SPF negatively affect corporate emails sent directly from my company's servers?

SPF may affect your corporate email delivery only if your organization does not set up proper SPF entries. Many times, we see that organizations forget to list all possible entities that may send emails on their domains' behalf.

When configuring your SPF entries, be sure to include ALL entities that are allowed to send emails on behalf your domain, including your own mail servers and any other indirect parties that will be sending emails on your behalf.

I already have an SPF entry. Should I create a new entry for eTrigue?

We do not recommend creating an additional SPF record. In fact, OpenSPF recommends that organizations combine multiple SPF entries into a single entry.

For example, if an organization had three SPF entries...

```
v=spf1 mx ip4:67.108.8.192/26 -all

v=spf1 include:_spf.etrigue1.com -all

v=spf1 include:_spf.etrigue2.com -all
```

...then a combined SPF entry would look something like this:

```
v=spf1 mx ip4:67.108.8.192/26 include:_spf.etrigue1.com include:_spf.etrigue2.com -all
```