EMAIL SETTINGS

1 Introduction

The FL3XX application sends emails on behalf of your business. To do so, the FL3XX email servers send on behalf of your own email servers. Correctly (but unfortunately for us), such activity is categorized as SPAM. For your customers and partners to receive your emails from FL3XX servers, you must set FL3XX's email servers as authorized email servers.

The way this works, in simple terms, is you will put a flag in the public record of your domain (e.g. mycompany.com). When someone receives an email, their server will check that the sending service is authorized for that domain and if they find the flag will determine the message is legitimate. Of course, setting up flags in your domain is protected and only you (or your IT manager) can access the record. If you remove the flag, immediately the emails sent by the FL3XX servers will be detected as SPAM.

This document helps the users to setup all the necessary configuration to allow FL3XX's email servers to send on your behalf.

The email protocol relies on DNS to send and receive emails. For a server to be authenticated as not a SPAM server, it's important for your business to add or update 3 specific DNS records with your DNS provider.

SPF

The SPF is a special record that allow a list of authorized servers that can send email on behalf of your business. It's important to add FL3XX's email server into this record or to create one in case you don't have one.

DKIM

The DKIM is like an encryption key that says yes this email is really coming from this email address. It's important to add FL3XX's public DKIM key into your dns to ensure that your clients properly receive the emails from the FL3XX application..

DMARC

The DMARC allows the owner of a domain to publish a policy on which mechanism (DKIM, SPF or both) is employed when sending email from that domain and how the receiver should deal with failures. Additionally, it provides a reporting mechanism of actions performed under those policies. It thus coordinates the results of DKIM and SPF and specifies under which circumstances the email should be considered legitimate.

2 How to Configure SPF?

There are 2 options available to you for this procedure to work. The 2 options are:

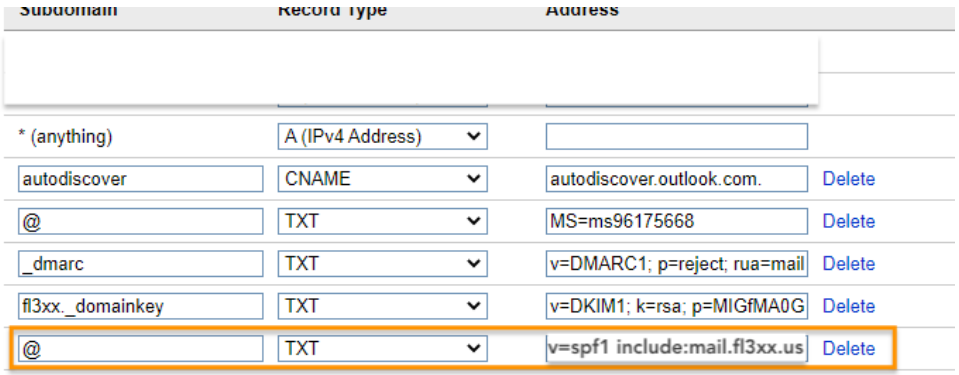
- You don't have an already configure TXT record for our domain
- You already have a TXT record for our domain

1a. We don't have a TXT record yet

Simply add a new TXT record. There are 4 fields that are important to configure.

1. **Type**: You need to choose the type **TXT**. The list should contain other type like A, AAAA, CNAME, MX, etc
2. **Name**: The name should be the name of your domain. It usually is the last part of your email address after the @
3. **Value**: The value is a special field where we define all the authorized email servers. Add exactly this without the double-quotes "v=spf1 include:mail.fl3xx.us ~all"
    a. "v=spf1" means that the spf version is 1. It's always like this
    b. "include:mail.fl3xx.us" means that we allow fl3xx.com to send emails on our behalf.
    c. "~all" means that if the email comes from anything else, it should be flag as SPAM.

    Example:



4. **TTL**: This value specifies how long the internet servers should cache this record. If you are configuring this record for the first time; **we recommend 300 seconds or 5 minutes**.

1b. We already have a TXT record

This procedure is easier than creating a new record. For this to work properly, simply add include:mail.fl3xx.us after the v=spf1. Make sure you keep all the information in this record and do not change anything else! It should look like this “v=spf1 include:mail.fl3xx.us …”

Example:

2. Test SPF configuration

After configuration, please make sure that the SPF record is correct. Please note that changes to the DNS can take several minutes up to hours to take effect!

You can verify the SPF configuration with for example with DMARC Analyzer.

Domain to Verify = <your domain, e.g. abc.com>. You should see mail.fl3xx.us somewhere in the results.

You can also use a tool called Dig using the following command: dig +short [your domain, e.g. fl3xx.us] TXT

3 How to Configure DKIM?

You can have several DKIM entries for different providers sending email on behalf of you. Hence if you already have one, just ignore and create an additional one for FL3XX.

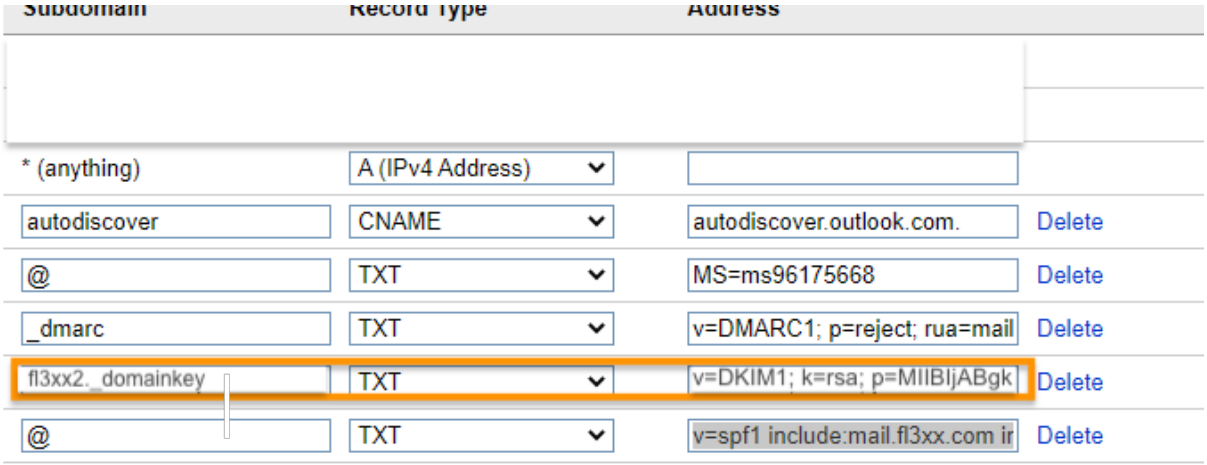
1. DKIM Configuration

The DKIM configuration is similar to the SPF. This means that we will need to add a TXT record but with different values.

1. **Type**: You need to choose the type TXT. The list should contain other type like A, AAAA, CNAME, MX, etc
2. **Name**: The name should always be this and pay attention to the underline: fl3xx2._domainkey
3. **Value**: The value contains three things: a “v-tag” specifying the version, a “k-tag” specifying the type of encryption key used and a “p-tag” containing the public key of the message signature. The exact Value you need to add is displayed below. ***NOTE: remove all line breaks and spaces. You can copy and paste the key from the separate file DKIM.txt to ensure no breaks and spaces.***

4. v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzO4/puhH+25v3T2iHQJJSxDbTmxe1mv8Z2CTF+vF70q1Qvhl0fNkLIH5BhRUKacOuql3u4paeufmL8zRqNCT8ge7w3mnJmcieKGeNRX5/o6MvO04Hfmmt7UWOjO7JFlPskTL12UINVXKyVsSjaSQH2bg3ZaS6SlGCxEf9qcB/+LlMu4SwNRQ+JFmw7GvQ4njluE+/S4H0zGDB6qu7hj2mgYLox9oH3m4E4+yKuR5a6MmOuE0pGIDCz4yp8i5p7Bq0dbnqF4wQbbYD99JoXm8iPr4DGsliaWO4xpTGr3ziH/0zn2Roxxim+aOwaQRvFLjlyPaKq8AVBtZKenKrCfGhQIDAQAB;

   Example:



5. **TTL**: This value specifies how long the internet servers should cache this record. If you are configuring this record for the first time; we recommend 300 seconds or 5 minutes.

2. Test DKIM configuration

After configuration, please make sure that the DKIM record is correct. Please note that changes to the DNS can take several minutes up to hours to take effect!

You can verify the SPF configuration with for example with DMARC Analyzer.

DKIM Selector to verify = fl3xx2. Domain to Verify = <your domain, e.g. abc.com>. The tool should say that all is good.

You can also use a tool called Dig using the following command: dig +short fl3xx2._domainkey. [your domain, e.g. fl3xx.us] TXT

4 How to Configure DMARC?

DMARC is a very powerful system, that gives you full control over how the receiving party processes your emails. You can read up more here.

In this tutorial we're not going into detail, but we show you how to initialize your DMARC entry, which for most SPAM-filters is already enough to increase your score.

1. DMARC Configuration

The DMARC configuration is similar to the SPF. This means that we will need to add a TXT record but with different values.

1. **Type**: You need to choose the type TXT. The list should contain other type like A, AAAA, CNAME, MX, etc
2. **Name**: The name should always be this and pay attention to the underline: **_dmarc**
3. **Value**: In our basic version the value contains two things: a "v-tag" specifying the version, a "p-tag" specifying the policy deployed by the receiving party. The exact Value you need to add is displayed below:
4. "v=DMARC1; p=none"
5. **TTL**: This value specifies how long the internet servers should cache this record. If you are configuring this record for the first time; **we recommend 300 seconds or 5 minutes**.

2. Test DMARC configuration

After configuration, please make sure that the DMARC record is correct. Please note that changes to the DNS can take several minutes up to hours to take effect!

You can verify the SPF configuration with for example with DMARC Analyzer. Domain to Verify = <your domain, e.g. abc.com>. Basically good if you see anything here. However, this is also more an optional thing and has way less impact than the other two (SPF and DKIM).

You can also use a tool called Dig using the following command: dig +short _dmarc.[your domain, e.g. fl3xx.us] TXT

5 SMIME Certificate

In addition to the DNS improvements described above, FL3XX offers the option to sign outgoing emails with an SMIME certificate.

6 Mail Relay

If required by the customer, FL3XX can relay outgoing emails via the mail server of the customer.

Authentication is possible based on whitelisting (Staging IP: 184.169.249.43 / 2600:1f1c:974:8700:5af9:9397:4188:c911, Production IP: 54.193.219.134 / 2600:1f1c:b07:4400:78a2:1bb:9150:3772) or login credentials.

Please contact FL3XX Support with your Mail-Server URL/IP-Address and authentication details to set this up.

7 Conclusion

After setting up the SPF, DKIM and DMARC records, FL3XX will be able to send emails on your behalf to your customer with a better reputation score. You can test the score online with MailTester. You can create a dedicated email address there and send an email directly from FL3XX to this email. Currently our score should be in the area of 9, which is an excellent result.

This will ensure that those emails won't end up in the SPAM folder. In any case, if you are not sure what you are doing, we can assist you in the configuration of those settings.

Signing emails with an SMIME Certificate aims at increasing the trustworthiness of outgoing emails.

Implementing an own mail relay is not recommended for standard users.