Email: sending domain configuration

SPF configuration

Sender Policy Framework (SPF) technology allows to verify that sender domain has not been faked. To make it work you need to add a special TXT record to your sending domain. It will allow only specified hosts to send messages using your domain.

We recommend to add records for different SPF versions:

Domain	Record type	Contents
example.com.	TXT	v=spf1 include:spf.aksend.net -all
example.com.	TXT	spf2.0/pra include:spf.aksend.net -all

The domain spf.aksend.net here contains the list of IP addresses Altkraft Cloud MTA uses.

If you have already used your domain for email, add to the existing SPF records "include:spf.aksend.net".

Note that we recommend to use restricting rules where only the enlisted resources are allowed!

DKIM configuration

DomainKeys Identified Mail (DKIM) technology adds to your message a digital signature of your from-domain. The signature is automatically verified on the recipient side and hen it is used to manage sender reputation. The signature is technically an RSA key pair: the private part is built in sender infrastructure and the public part should be added to your domain as a special subdomain TXT record:

Domain	Record type	Contents
ak._domainkey.example.com.	TXT	v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCldFYh3Rfrmeov+WqYYpwfW2bVUzxXPy9dSVoUCGLKCn+vgY/pdKIIBFitkvZJXGLnHqreqwGzoriEWf9ZRd+cL2LdA4UrDKheMeorBd2NSIqihkTaKz8PA+SIBFxFGm2Z0Krh5ZDF2NtFVhtD4YvqmrFqk2muzZ0tFEko8zP30wIDAQAB
_domainkey.example.com.	TXT	o=-;

To get a personal DKIM for Altkraft Marketing contact team@altkraft.com and provide us with your domain name.

DMARC settings

DMARC technology allows mailing servers to decide what to do if SPF or DKIM verification fails.

Here we recommend to restrict messages sent from unknown IP addresses or signed incorrectly.

Domain	Record type	Contents
_dmarc.example.com.	TXT	v=DMARC1; p=reject; sp=reject; mailto:report@example.com

BIMI settings

BIMI technology (Brand Indicators for Message Identification) is used along with SPF, DKIM and DMARC or identifying email sender by company brand logo, placed near the message subject in recipient's inbox. Email providers thus can additionally verify the sender.

To start using BIMI you will need an **svg** image, that is rectangular and has no extra layers.

Add the following record to your domain settings, specifying the svg file path:

Domain	Record type	Contents
default._bimi.example.com	TXT	v=BIMI1; l=https://example.com/bimi/bimi.svg

You can also use BIMI record generator at https://bimigroup.org/bimi-generator/

Tracking domain settings

Tracking domains are used to collect your customers' behavior information. For any subdomain you use add this record:

Domain	Record type	Contents
trk.example.com.	CNAME	trk.aksend.net

You can use this record for all of your tracking domains.