MailMarketing
SEND UNLIMITED EMAIL AT A FIXED COST

IMPLEMENT SPF AND DKIM AUTHENTICATION

*After verifying the sender,
you can proceed to a series of activities
to improve the delivery rates
of your emails.*

guide

1. IMPLEMENT SPF/DKIM

After verifying the sender, you can proceed to a series of activities to improve the delivery rates of your emails. One of these activities is the implementation of SPF and DKIM authentication.

SPF and DKIM are authentication protocols, both based on the domain's DNS, that allow the owner of the site to specify which email server people will use when they will send emails from that domain and thus avoid fraudulent activities of third parties.

The implementation of SPF and DKIM allows you to increase the reliability at Email Service Providers (such as Gmail, Hotmail, Yahoo!) , improve the security of mailings and ensure the highest possible deliverability, both on shared and dedicated IPs.

For a correct implementation of SPF and DKIM it is advisable to ask for support from your domain manager or hosting service provider.

2. SPF

An SPF (Sender Policy Framework) register is a standard of email authentication that compares the actual IP address of the sender of the email with a list of IP addresses authorized to send mail from that domain.

An SPF (Sender Policy Framework) registry is an email authentication standard which compares the actual IP address of the email sender with a list of IP addresses authorized to send mail from that domain.

Basically an SPF record lists the mail servers authorized to send email on behalf of of your domain and is used to prevent spammers from using your domain for sending unauthorized emails using a fraudulent technique called spoofing.

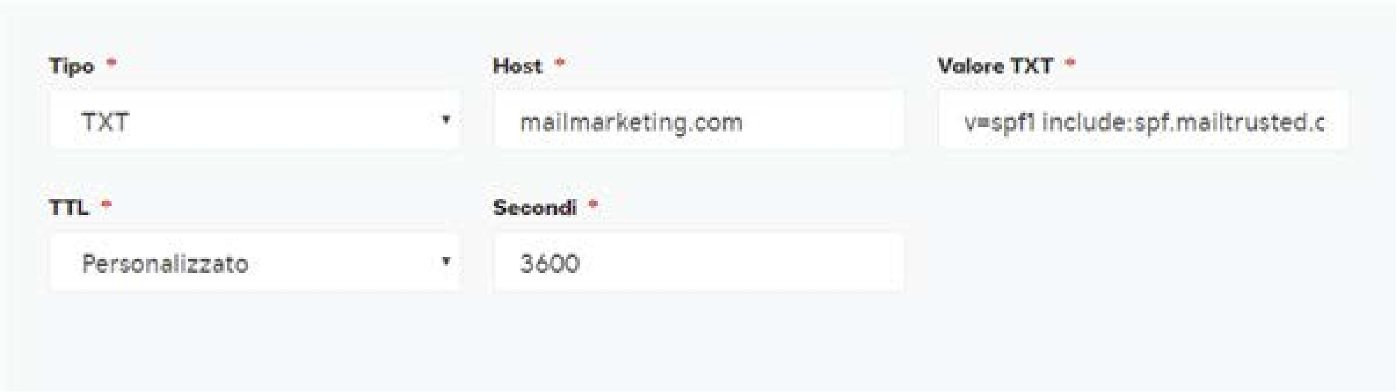
Some mail recipients require an SPF record. In these cases, if you do not add one to your domain, your messages can be marked as spam or even be rejected.

HOW TO CONFIGURE SPF

To configure SPF it must be added/modified the dedicated record in the DNS of the domain.

1. Login to your Web Hosting
2. Go to the section dedicated to DNS
3. Add a new SPF record with the following information:
   - RECORD TYPE: TXT
   - HOST: your domain name (e.g. mailmarketing.com)
   - VALUE: v=spf1 includes:spf.mailtrusted.org ~all

View the example



Tipo *	Host *	Valore TXT *
TXT ▾	mailmarketing.com	v=spf1 include:spf.mailtrusted.c
TTL *	Secondi *	
Personalizzato ▾	3600	

The SPF code is available in the section Senders Management in Enabled Senders - Configurations by clicking on the red icon in the column "Record spf".

To add a TXT record, you need to log in to your domain host, which in general corresponds to the service from which you purchased the domain name. If you are not sure which is your host, you can identify it through your billing data or through the systems of whois.

For more information on creating TXT records, please contact the support team of the host.

Once you have entered the new SPF record into the DNS of your domain, go back to the Senders Management page, update it and the color of the SPF record icon will change from red to green.

3. DKIM

DKIM (Domain Keys Identified Mail) is another authentication method and it is used by email service providers to determine the identity and for establish the reputation and reliability of a sender.

An SPF (Sender Policy Framework) registry is an email authentication standard which compares the actual IP address of the email sender with a list of IP addresses authorized to send mail from that domain.

Basically an SPF record lists the mail servers authorized to send email on behalf of of your domain and it is used to prevent spammers from using your domain for sending unauthorized emails using a fraudulent technique called spoofing.

Some mail recipients require an SPF record.

In these cases, if you do not add one to your domain, your messages may be marked as spam or even be rejected.

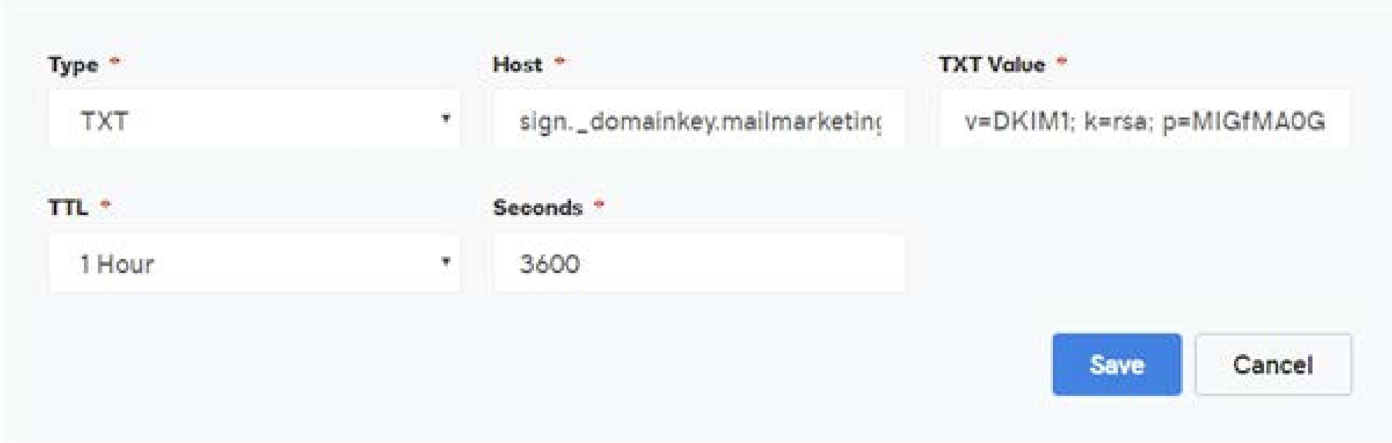
HOW TO CONFIGURE DKIM

Add a record in your DNS configuration with the following values

- **TYPE**: TXT
- **HOST**: sign._domainkey. name_domain (example sign._domainkey.mailmarketing.com)
- **DATA**: v=DKIM1; k=rsa;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDXEbvzRtmqiOfbmkxvjxt2YTVMgC1Q5qtiNbdCOnkPQFDEYh5noE/mEhRVpfpdKRJshEHXZ9U3vms3YwBg1hhMtoLsucILzyzTV6gj7IaY9UIYHsHIXVmTtiNmiTYs99JZCXiWQGcKz0BwhHx0Ifwam+U7SNIW+2o+bJnd2Y+ZYwIDAQAB

For the subdomain ‘sign._domainkey.

View the example



Type * TXT

Host * sign._domainkey.mailmarketing

TXT Value * v=DKIM1; k=rsa; p=MIGfMA0G

TTL * 1 Hour

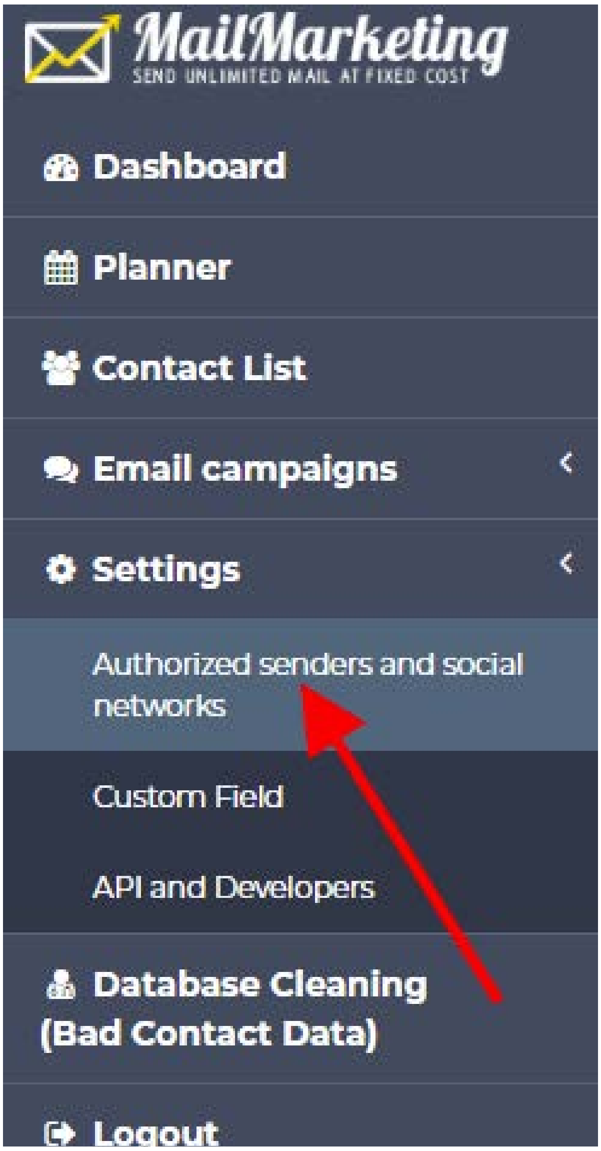
Seconds * 3600

4. VERIFY

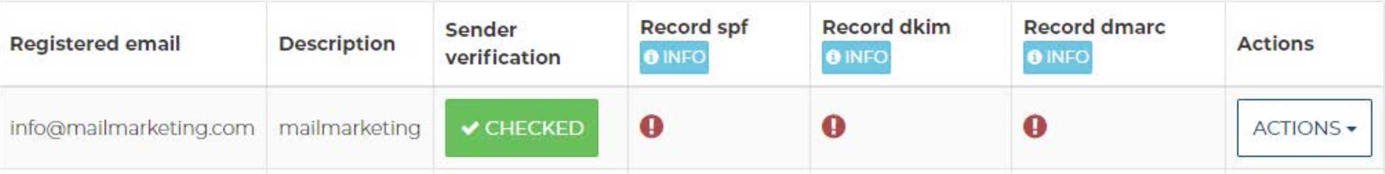
After 24 hours you will be able to verify the correct setting of the SPD Record and DKIM nen DNS

24 hours after adding the SPF record and DKIM in the DNS of your domain you can check if they have been configured successfully directly in the section of Enabled Senders and Social Networks.

In case SPF and DKIM have been configured successfully, the icons in the record SPF and DKIM will change the status from red to green

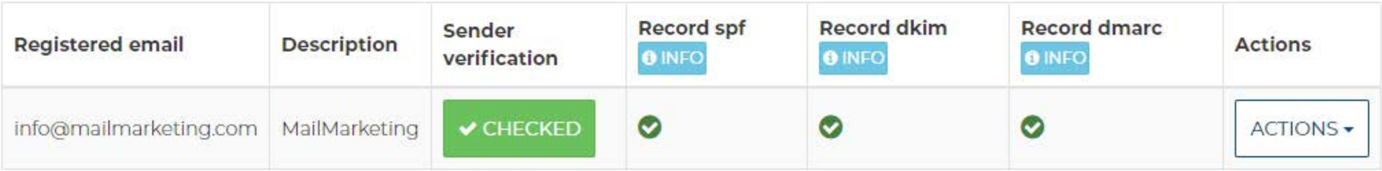

MailMarketing
SEND UNLIMITED MAIL AT FIXED COST
Dashboard
Planner
Contact List
Email campaigns
Settings
Authorized senders and social networks
Custom Field
API and Developers
Database Cleaning (Bad Contact Data)
Logout

Before implementation



Registered email	Description	Sender verification	Record spf INFO	Record dkim INFO	Record dmarc INFO	Actions
info@mailmarketing.com	mailmarketing	✓ CHECKED	!	!	!	ACTIONS ▾

Implementation successfully completed



Registered email	Description	Sender verification	Record spf INFO	Record dkim INFO	Record dmarc INFO	Actions
info@mailmarketing.com	MailMarketing	✓ CHECKED	✓	✓	✓	ACTIONS ▾

DID YOU FIND THIS GUIDE HELPFUL?

Discover how to take advantage of the potential of email thanks to a solution tailored to your needs.

www.mailmarketing.com

MailMarketing
SEND UNLIMITED EMAIL AT A FIXED COST