Manuals

mail2easy PRO

Domain Settings

Basic implementation instructions

SPF ✓

DKIM ✓

CNAME ✓

In order to optimize your email deliverability, we recommend you perform the validation settings in your domain.

DINAMIZE

Contents

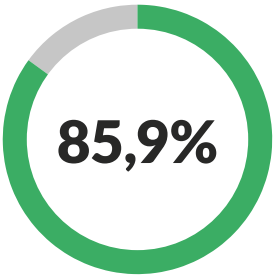
Why are they important?.....3
The positive impact in taking these settings.....3
What is CNAME?.....4
What is DKIM?.....4
What is SPF?.....4
How to configure these settings?.....5
Checking.....5

Why are they important?

The SPF, CNAME and DKIM settings are essential to make sure your email marketing is recognized as valid and trustworthy. These settings guarantee your subscribers ISP that it is really you sending your email. After setting them, the ISPs understand your campaigns as safe, decreasing the chance of blocking or scoring as spam at the time of delivery.

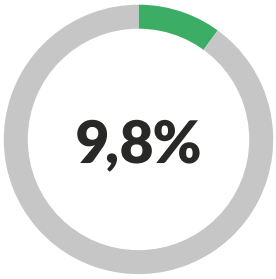
The positive impact in taking these settings

SPF and DKIM are slowly taking their place in the market, increasing ever since 2013. According to the benchmark report on Deliverability in 2016, from Return Path and Google Security Blog, the deliverability rate was of 86%, against 74% from 2015 and 60% in 2014. Check below the complete outlook:



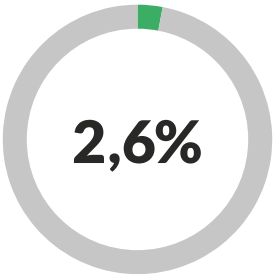
SPF & DKIM

Emails successfully delivered in the mailbox, using SPF and DKIM



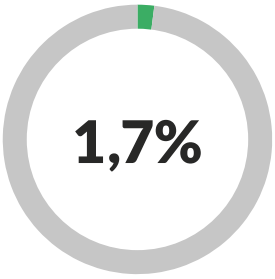
SPF Only

SPF Only - Delivered emails authenticated only by SPF



Not authenticated

Not authenticated - Unauthenticated emails, discarded as spam



DKIM Only

DKIM Only - Delivered emails authenticated only by DKIM

What is SPF?

SPF - Sender Policy Framework is a technology that aims to stop unauthorized message sending.

It states who may send emails from your domain, therefore authenticating the sender. To sum up: when the ISP receives your email, it will check if the infrastructure that sent it is authorized to use your domain. If it isn't, the email might be rejected.

For that reason it is very important that the settings are valid, optimizing the deliverability of your campaigns sent from Mail2Easy.

What is CNAME?

CNAME - Canonical Name settings are responsible for the redirections required for the operation of the tool, such as the links from the platform and the data and statistics of your reports.

Through the use of images in your email, with redirection, external view and unsubscribe links, it is much harder to score on anti-spam tools.

The whole process of unsubscribing, opening count and click mapping is made easier after having these settings done. Since there will be records pointing straight to the tool, it is possible to gather data and present them in a more efficient way.

What is DKIM?

DKIM - DomainKeys Identified Mail consists in signing the messages with a public key, to ensure the authenticity of the sender.

It performs functions similar to those of SPF, since it prevents the falsification of the domain, but it is more complex. While SPF certifies **who** is sending, DKIM certifies **what** is being sent, as it ensures that the contents of the email have not been changed in any way during the sending.

When you have a valid DKIM, the ISP will compare the content of your message (certified by the public key) with the settings configured in your domain. By verifying that the entry is the same, it will be understood that the message is authentic and unmodified, improving its deliverability and, therefore, its reputation.

How to configure these settings?

These three settings (SPF, CNAME and DKIM) are configured in the DNS zone of your domain, from the information sent by our Support team.

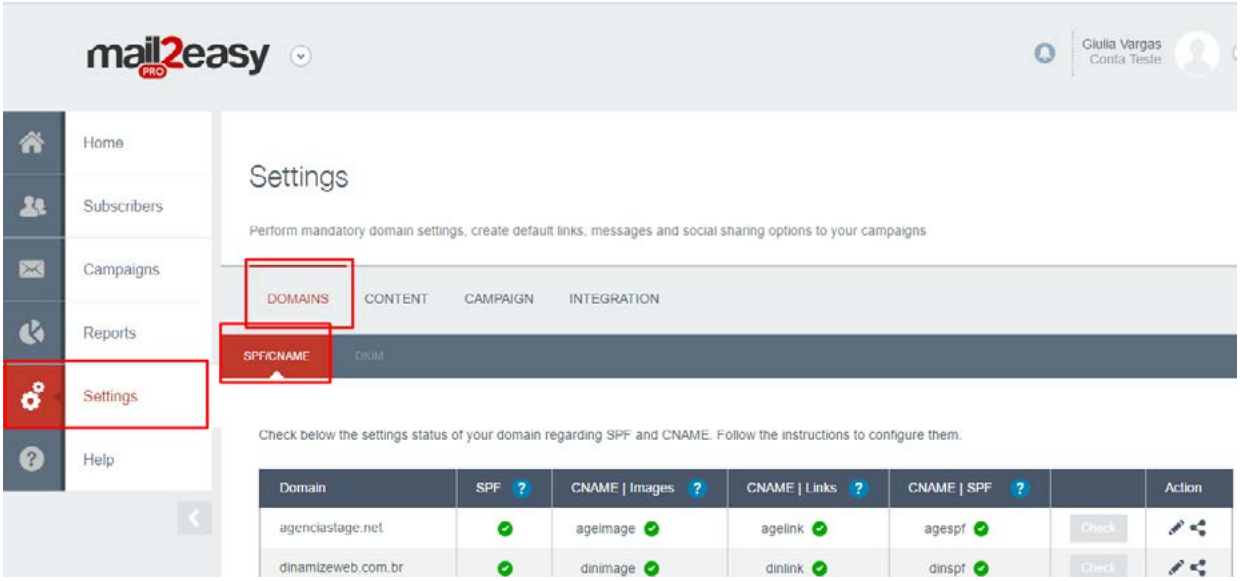
In your domain's host, you must look for the DNS zone configuration tool. There, you can manage and edit the DNS entries of your website, email and other domain services.

Any change in the DNS zone has a propagation time, which is the period taken by the server to start transmitting the new entries and changes made by you. So remember: the changes made will not be automatic, they take, usually, 24 hours.

SPF is a TXT type entry, that will have includes (infrastructure authentications). DKIM is also a TXT type entry, with a coded key to certify your campaign. CNAME settings, on the other hand, are made through CNAME entries, with permission records to the tool.

Checking

To check the status of your SPF, CNAME and DKIM, you must go to the Settings menu on the side. By default, the first page already displays the domains.



On this page, you can see a chat with all the domains used by this account and the status of each of them.

Domain	SPF	CNAME | Images	CNAME | Links	CNAME | SPF		Action
agenciastage.net	✓	ageimage ✓	agelink ✓	agespf ✓	Check	
dinamizeweb.com.br	✓	dinimage ✓	dinlink ✓	dinspf ✓	Check	

When all the settings are OK, there will be a CHECK symbol besides each setting.

When the settings are not correct, there will be an ERROR symbol.

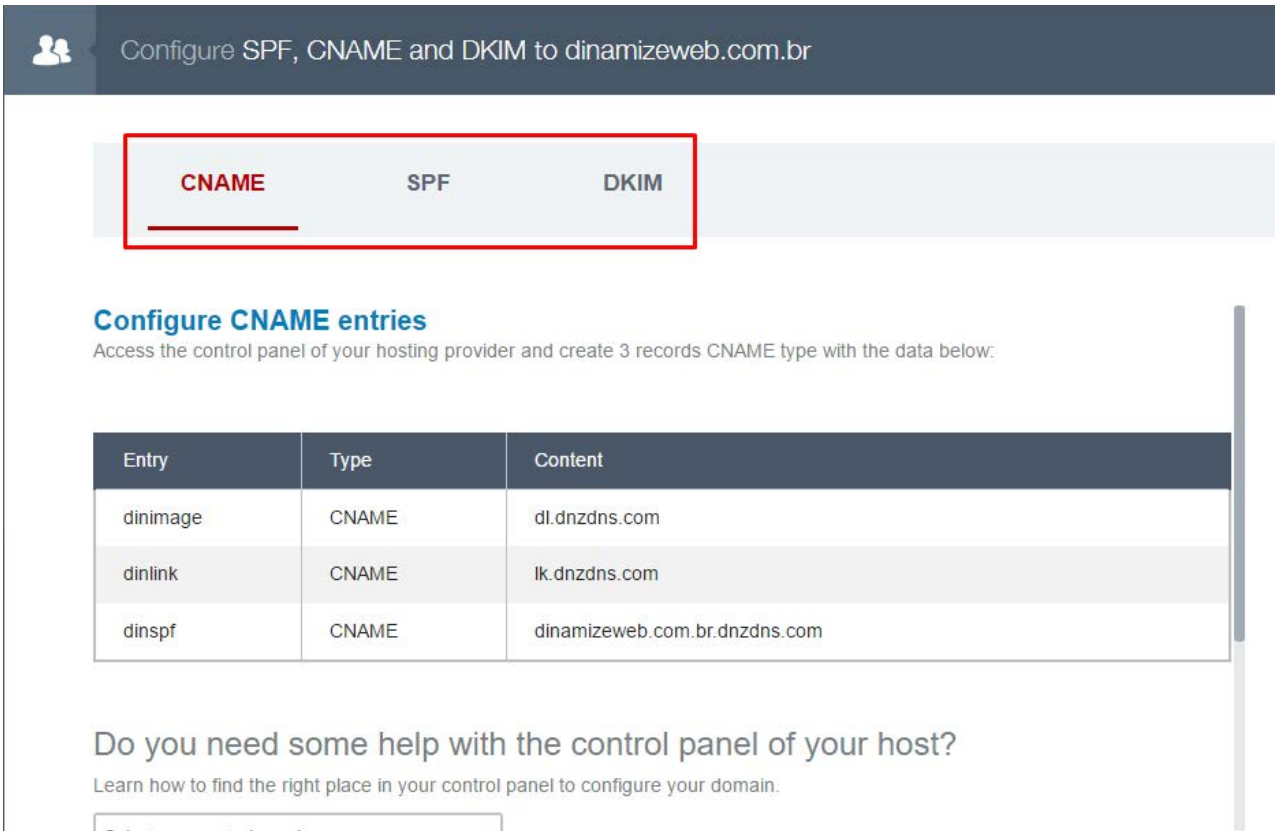
Check

In that case, you can click on the CHECK button , to check if the settings are correct and change the status.

In order to use a domain, you must ask the Support team to add it for you, as well as send you the required settings, which you can also find in your account.

Right below this chart is a settings tutorial

After choosing the domain a new window will open, with the SPF, CNAME and DKIM settings as well as the instructions on how to do so.




DINAMIZE