SPF Records

An SPF record stands for a Sender Policy Framework, which is an open standard created to stop forgery of from email addresses by spammers. An SPF record helps mail servers distinguish forgeries from real mail by making it possible for a domain owner to say, *I only send mail from these machines.* That way, if any other machines try to spoof mail from that domain, the mail server knows that the FROM address is forged.

> For example: Let's say you send an email invite in Alchemer from You@Yoursite.com to AwesomeRespondent@yahoo.com. Yahoo would get the message and say, "OK; this email says it's from Yoursite.com... but wait, it actually came from Alchemer!" Yahoo's email server would then contact Yoursite.com and ask if Alchemer has *permission* to send messages in their name.

For more detailed information about SPF records, please refer to:

For SPF Record Testing Tools, please see: http://www.kitterman.com/spf/validate.html

When should I use one?

An SPF record is generally used when your company is trying to avoid people using your domain for SPAM. The thing you need to do if you plan to send emails from your Alchemer account, using either the Send Email Action or Email Campaigns, is to make sure that *if you do have an existing SPF record*, that we are included.

Allowlisting us will allow you to use your domain as the **From Address** field when using the Alchemer application to send out email campaigns or send email actions. You will also need to implement DKIM as part of this process.

Learn about setting up SPF and DKIM records in Alchemer by visiting our Custom Email Settings tutorial.

What should I avoid?

If you already have an SPF record or are setting one up, you'll want to make sure you don't set it to allow only Alchemer. If you do, then you won't be able to send out emails from any other servers.

If I have an SPF record and need to allowlist Alchemer, what should I use?

If you already have an SPF record set up on the domain you want to send emails from, then we recommend adding the following entry to your SPF record.

US Datacenter: v=spf1 include:_spf.alchemer.com ~all

EU Datacenter: v=spf1 include:_spf.alchemer.eu ~all

```
CA Datacenter:  v=spf1 include:_spf.alchemer-ca.com ~all
```

This will include our servers in your preferred server list, and if we ever need to change our specific IP addresses, you won't need to worry about it on your end.

You may also want to add Mandrill to your allow list, which is the email service we use to send application emails, such as, reset password emails. If you are having trouble receiving these emails, you may want add them to your allowlist. Check out Mandrill's documentation on how to allowlist:

http://help.mandrill.com/entries/39716883-How-can-my-recipients-whitelist-Mandrill-s-IP-addresses-

If I do need to set up an SPF record, how do I do so?

Here are is a great resource on setting up a valid SPF DNS record: https://support.office.com/en-us/article/Create-DNS-records-for-Office-365-at-any-DNS-hosting-provider-7b7b075d-79f9-4e37-8a9e-fb60c1d95166

Related Articles