

Configuring Sending Emails from a Customer's Domain Using SPF

Last Modified on 03/23/2022 3:42 pm IST

Sender Policy Framework (*SPF*) is an email authentication method designed to detect forging sender addresses during the delivery of the email.

The setup requires the customer to perform actions in their DNS configuration, and also requires Kaltura to perform tasks to complete the process. This article goes through the steps an admin must perform to set up a *Kaltura* Account ID (Partner Id, PID) that allows Kaltura to send email notifications on-behalf of an email address in the customer's domain.

Sender Policy Framework (*SPF*) is an email authentication method designed to detect forging sender addresses during the delivery of the email.

Kaltura's solution is based on [SPF DNS records](#) in which the customer basically whitelists the Kaltura's mail server as an approved server for sending emails on behalf of their domain.

The SPF record is **a DNS record that has to be added to the DNS zone of your domain**. In the SPF record you can specify which IP addresses and/or hostnames are authorized to send email from the specific domain.

Other techniques (such as DKIM) are currently **not** supported by Kaltura. An SPF-based solution aims to protect both Kaltura's mail server as well as the customer's domain from being added to spam black-lists. An SPF-based solution is a common practice used by many other SaaS providers.

Customer Instructions

You will need to either create or update your domain's SPF DNS record to include the Kaltura's mail server.

Be certain that you have the following in your SPF record:

```
include:mailer.kaltura.com
```

If you do not have an SPF record already, you will need to add one with the following value:

```
v=spf1 include:mailer.kaltura.com
```

For example, the Kaltura domain allows emails to be sent from [outlook.com](#) on behalf of Kaltura by using the following SPF record:



```
1v=spf1 ip4:38.74.192.64/27 ip4:38.122.106.8/30 ip4:38.102.153.129/27 ip4:38.122.152.32/29  
ip4:159.63.54.50/30 ip4:64.215.193.192/27 include:spf.protection.outlook.com  
include:outlook.com a mx -all
```

The `include:outlook.com` in the record is what allows outlook.com to send on Kaltura's behalf.

After you have performed these actions Kaltura will be able to add your domain to the list of email notifications' domains only **after verifying** that you have completed the configurations in your DNS.
