DKIM and SPF Setup Example

This article applies to:
Pro
Max

An SPF record is a type of Domain Name Service (DNS) record that identifies which mail servers are permitted to send email on behalf of your domain. The purpose of an SPF record is to prevent spammers from sending messages with forged From addresses at your domain.

Example of SPF record using Gmail
v=spf1 include:_spf.google.com include:infusionmail.com ~all

1. In your domain add a TXT record
2. Enter @ into the "Name" or "Host" field
3. Points to would be the v=spf1 include:_spf.google.com include:infusionmail.com ~all

Note: This is only an example and does not mean it's exactly how you would set up the SPF record in your OWN Domain. Please contact your domain provider to verify their process.

DKIM (Domain Keys Identified Mail) is a complex email protocol that allows a sender's identity to be authenticated by the recipient to help combat email fraud.

To setup:

1. Navigate to your Keap settings by clicking your avatar located in the bottom left followed by "Settings"
2. Click **Domains**

3. Under "Email domains" if you have a business email address domain it will be listed with a "Set up email domain" or you can add a different domain by clicking "Add a different domain". Note: To add a different email domain, a user containing that email domain must be Active under Settings > Users.

4. Select your domain provider from the drop-down

5. Click the "Continue" button

6. Add the information provided to your domain in the steps shown below.
   1. Create a new NAME record in Other
2. Copy paste text into **Name** or **Host** field

3. Copy paste text into **Value** or **Points to** field

   1. Create a new CNAME record in Other

   2. Copy paste text into **Name** or **Host** field

      ![Key Image]

      7bcefe-3e94-4dbb-a6bb-7dcb494a0c7c_domainkey

5. Click **Confirm** after the information has been saved in your domain provider.

8. These instructions require you to create a CNAME entry in your DNS records. If you need assistance with this step, we recommend you contact your DNS provider for assistance because the steps may vary depending on your provider. Below are links to help articles of several common DNS providers to help you.

   1. GoDaddy
   2. BlueHost
   3. Host Gator
   4. DreamHost
   5. Liquid Web
   6. In-Motion
   7. Amazon CloudFront
   8. Google Cloud

**Important Note!** Some DNS providers are not compatible with this method of DKIM.

7. Once the domain has been verified, Keap will begin using DKIM when sending emails on your behalf.
DKIM Re-validation Steps

You may need to follow these steps to ensure DKIM is signed properly for mail from your Keap application. The changes require you to update your CNAME record that you added to your domain and then to re-validate your domain. There are 2 steps to complete:

1. Update Your CNAME record - These instructions require you to edit a CNAME entry in your DNS records. If you need assistance with this step, we recommend you contact your DNS provider because the steps may vary depending on your provider.
   - Locate the CNAME entry in your DNS records where you previously entered `infusionmail.com` and replace it with `dkim.infusionmail.com`, then save the record.
   - If you have multiple domains that were previously verified, you will need to do this for each CNAME record on each domain.

2. Re-Validate Your DKIM record
   1. Login to your Keap application, navigate to the Marketing module and click on `Settings`.
   2. On this page, look at the navigation bar on the left and click on `Email Authentication`.
   3. Now you should see your domain(s). Click on the hyperlink `Retry Validation`.
   4. This will open up a Retry Domain Verification pop-up window. Click on the **Verify Button** to complete the update. If this fails to validate, please wait and try again (it can take hours, depending on your DNS provider). If you have multiple domains that were previously verified, you will need to repeat these steps for each Domain.