What is DKIM?

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.

How does it work?

A public key is used to create a DNS record. That same key is also used to digitally sign the header of emails that are sent. When the recipient's provider receives the email, they check the sender's DNS records and the sender's authenticity is validated by the matching key. The message can then be delivered to the recipient with confidence that the sender is who they claim to be.
Why is it important?

DKIM affords the greatest assurance that the sender is who they say they are and gives email providers a way to track and hold senders accountable for the messages they’re sending. As a result, deliverability of these messages is greater and inbox placement is improved.

What's special about Keap's implementation of DKIM?

Normally, implementing DKIM requires a domain owner to create public and private RSA keys which are used in the authentication process. To make it easier for you to implement DKIM, Keap has eliminated this complexity by creating these keys on your behalf. With this approach, you only need to create a CNAME record in your DNS that points back to the Keap servers, and turn on the function in your Keap account. We've tried to further simplify this process by providing simple, step-by-step instructions directly within your Keap account to help guide you.

How do I set it up?

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
7. 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.
   a. GoDaddy
   b. BlueHost
   c. Host Gator
   d. DreamHost
   e. Liquid Web
   f. In-Motion
   g. Amazon CloudFront
   h. 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.
   1. 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.
2. 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**.

3. 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.