

DKIM Email Authentication

Last Modified on 07/08/2025 2:05 pm MST

This article applies to:

[Max Classic](#)

DKIM (DomainKeys Identified Mail) is an essential email authentication protocol that helps verify that your emails are truly coming from you. It protects against spoofing and email fraud by allowing recipient servers to validate that a message hasn't been tampered with and is authorized by your domain. DKIM plays a significant role in improving your email deliverability and inbox placement, as it builds trust with email providers and helps ensure your messages are delivered successfully. If you haven't set it up yet, follow the steps below to get started.

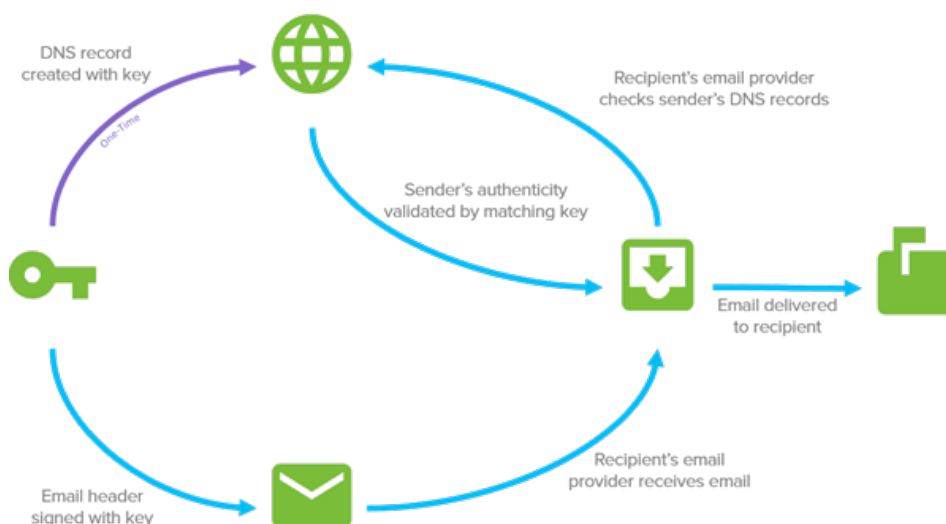
How does DKIM work?

DKIM (DomainKeys Identified Mail) works by using cryptographic authentication to verify that your email is truly coming from your domain and hasn't been tampered with.

Here's how it works:

- A **public key** is published in your DNS records.
- A **matching private key** is used by the sender (Keap) to digitally sign the header of every email you send.
- When your recipient's email provider receives the message, it checks your DNS for the public key and verifies that it matches the signature in the email.

If everything checks out, the message is delivered with a higher level of trust, improving your chances of landing in the inbox instead of the spam folder.



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

Normally, setting up DKIM requires domain owners to manually generate and manage cryptographic keys—a process that can be technical and time-consuming. Keap simplifies this for you.

We automatically generate the required public/private key pair and handle the signing process on your behalf. All you need to do is:

- Add **three CNAME records** to your DNS settings that point to Keap.
- Turn on DKIM in your Keap account.

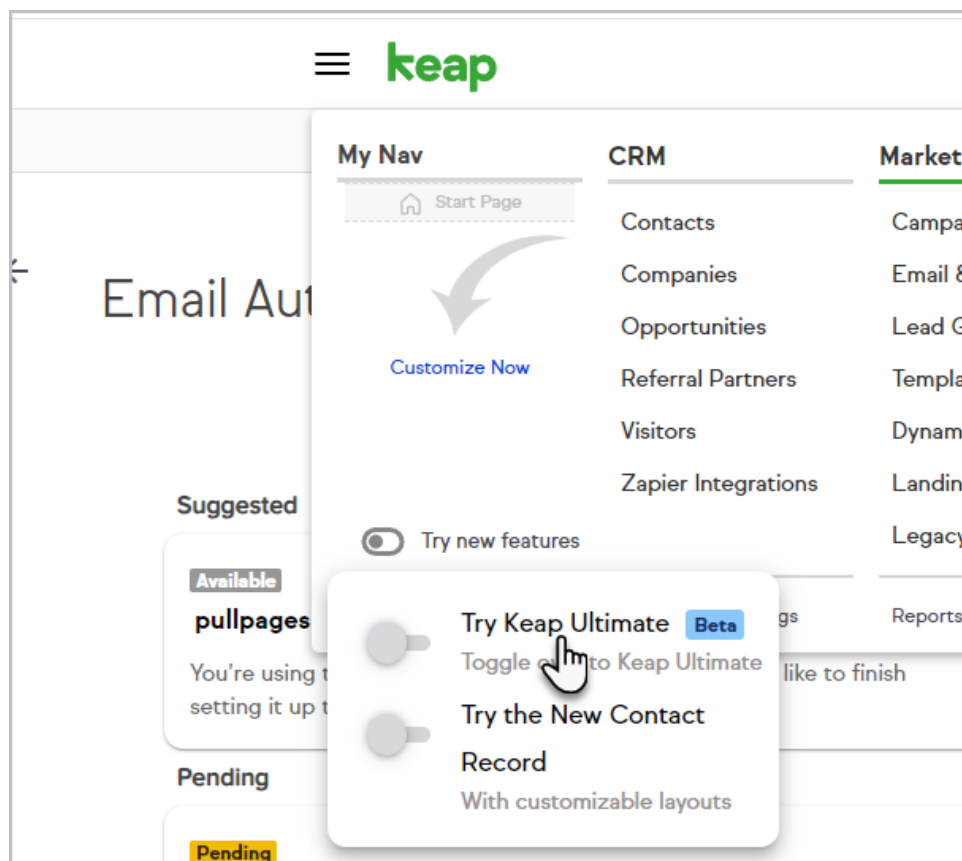
That's it—no need to manage any keys yourself.

Additionally, we offer a simple way to set up **DMARC**, which can otherwise be complex due to policy configurations and interpreting authentication reports. Keap's tools streamline this for better email security with less hassle.

We also provide easy, step-by-step instructions directly in your Keap account to guide you through setup.

Note for Keap Classic users:

To access DKIM setup via Keap Ultimate, click the menu icon next to the Keap logo, then select **"Try new features"** and enable the **"Try Keap Ultimate"** switch.



If Ultimate access isn't available, you can still manage email authentication by going to **Marketing > Settings** and searching for **Email Authentication**.

How do I set it up?

Setting up DKIM requires you to add **three CNAME records** to your domain's DNS settings.

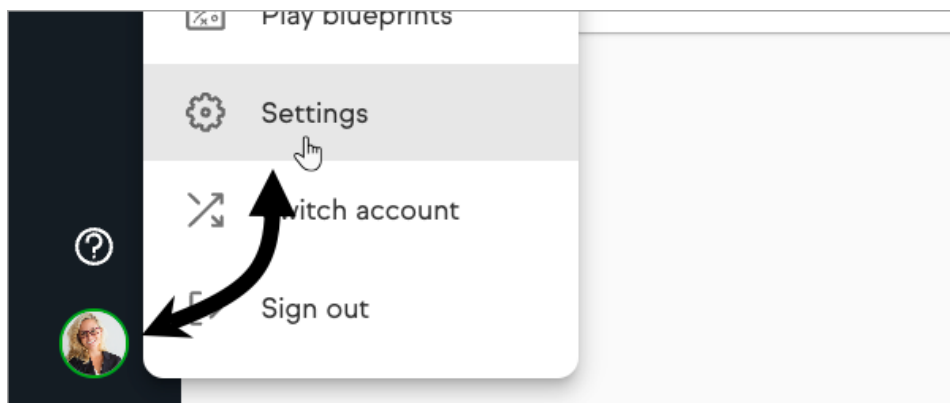
Because every DNS provider has a slightly different interface, we recommend checking with your provider's support

resources if you're unsure how to do this.

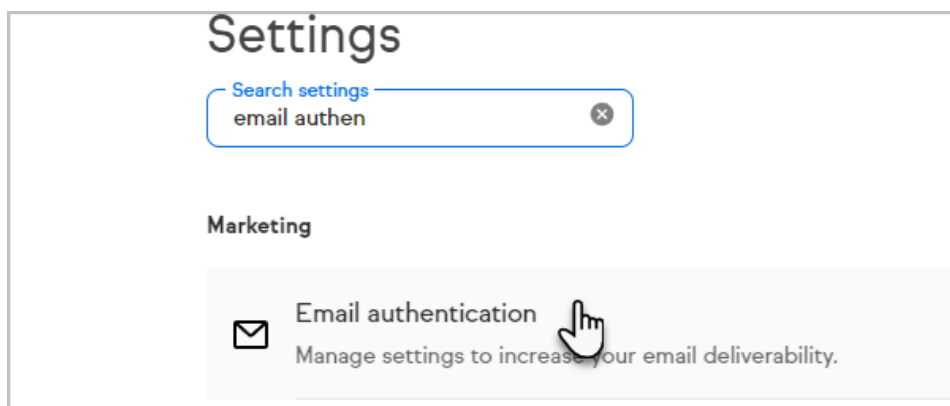
We've included links below to help guides for several common DNS providers to assist you.

- [GoDaddy](#)
- [BlueHost](#)
- [Host Gator](#)
- [DreamHost](#)
- [Liquid Web](#)
- [In-Motion](#)
- [Amazon CloudFront](#)
- [Google Cloud](#)

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

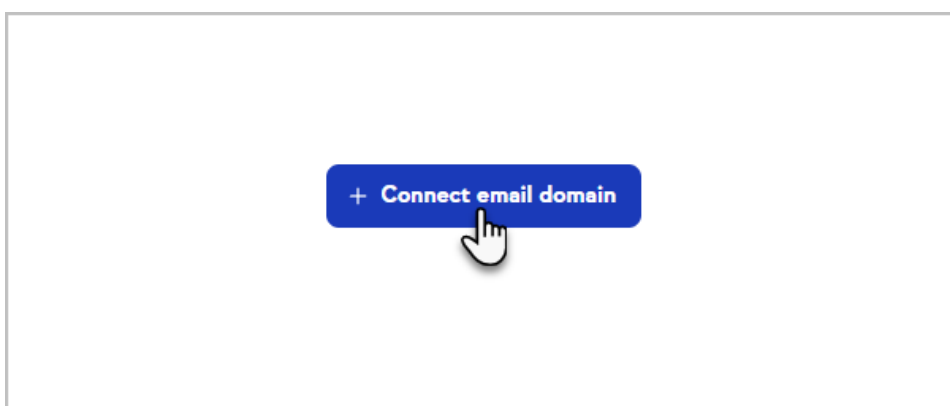
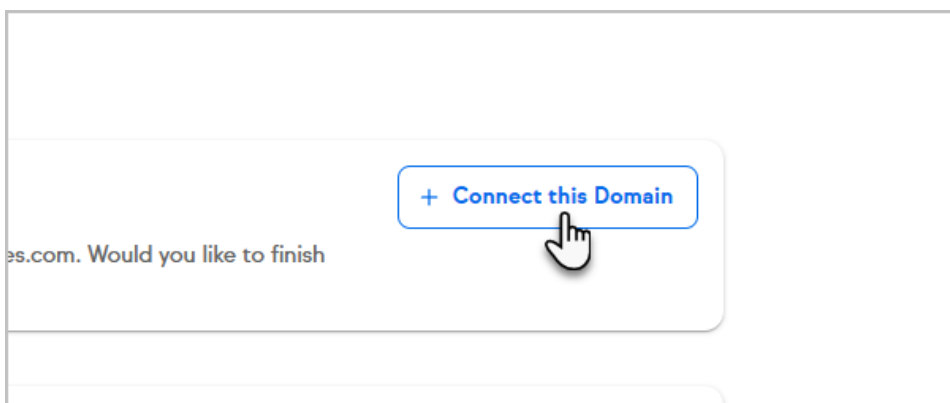


2. Search for **Email Authentication** to bring up the setting and click to open.

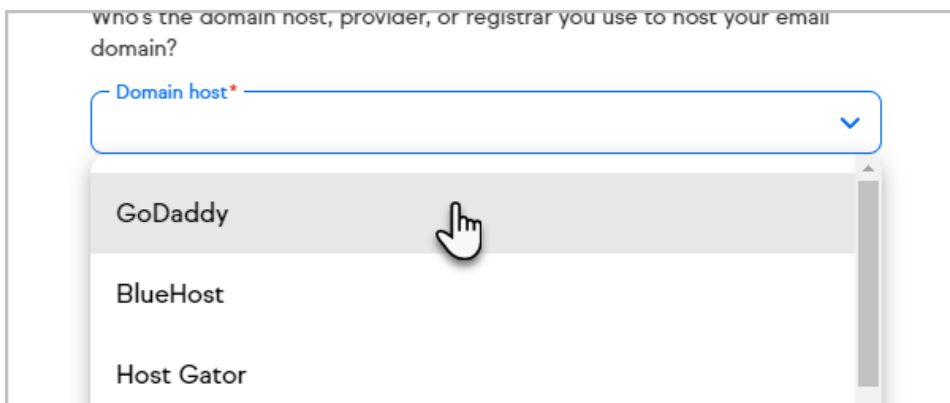


3. Under **Email**, if you have an unverified business email address domain associated with your app it will be

listed under the **Suggested** section of the page. Click on **+ Connect this domain** to begin the process. Or you can add a different email domain by clicking the stand alone **+ Connect email domain** at the top of the page



4. Select your domain provider from the drop-down



5. Determine if you have DMARC authenticated on your domain

1. If you already have a DMARC record on your DNS you will check the **I already have a DMARC record** box

A screenshot of a web form titled "DMARC record". Below the title is a paragraph: "This record is required by providers to verify that the email sent by Keap on your behalf isn't spam." There are two checkboxes: the first is checked and labeled "I already have a DMARC record", and the second is labeled "Unsure? Check here". A hand cursor is pointing at the checked checkbox. Below the checkboxes is a blue button labeled "Continue".

2. If you are unsure, you can use the link next to the box to check, this will bring you to the Dmarcian DMARC domain checker

NOTE: The new Yahoo and Google DMARC requirement will be enforced beginning February 2024 for higher volume senders. We've written a [guide](#) to help you prepare for the mandate and to ensure your emails won't be disrupted.

Why test your DMARC record?

- Find out if your record has been published correctly
- Prevent mistakes in the formatting of your record
- Get more information about the possible extra parameters
- Find out where your DMARC reports are being sent to

Enter domain INSPECT THE DOMAIN

3. If you do not have a DMARC record on your DNS file, you will need to select either the DMARC policy None, Quarantine, or Reject. We suggest starting off using the Quarantine policy. [To learn more check here](#)

☐ I already have a DMARC record [Unsure? Check here](#)

How do you want email that fails your DMARC record to be treated by the recipient?

None Quarantine Reject

No security **Recommended**

Observation or reporting mode. Email providers will only give statistics on your email domain.

6. Click **Continue** button

your behalf isn't spam.

☒ I already have a DMARC record [Unsure? Check here](#)

Continue

Need help? [Learn more](#) about how Keap connects to your domain.

7. Access your Domain Provider's platform and paste the provided CNAME records into your DNS settings. Please avoid highlighting and directly copying the record, as this might result in incorrect setup of your record. Instead, click on the intended record to ensure accurate configuration. If you are unsure on how to create and add CNAME records to your DNS provider, please see the links above or contact your DNS provider for assistance.

1. Create new CNAME records in your provider for each row shown
2. Copy and paste text into **Name** or **Host** field
3. Copy and paste text into **Value** or **Points to** field

Copy records to GoDaddy

1. Create a new record in GoDaddy for each row shown.
2. Copy and paste the text into each record.

Record	Type	Host	Value
1	CNAME	martyc.pullpages.com	return.infusionmail.com
2	CNAME	martyc1_domainkey.pullpages.com	s1.domainkey.infusionmail.com
3	CNAME	martyc2_domainkey.pullpages.com	s2.domainkey.infusionmail.com

Need help? We suggest contacting [GoDaddy](#) for assistance in locating your CNAME records.

8. Click **Confirm** after the CNAME records have been added in your Domain Provider DNS records

3

CNAME

martyc2_dom

Need help? We suggest contacting [GoDaddy](#) for assistance

Confirm

9. You will then be taken back to the Domains home page, and your new domain will be displayed with a **Pending** status. The verification process may take up to 48 hours to complete. Once verification is complete your domain will show **Connected**.

Pending

Pending

nhl.com

This email domain verification is pending. It can take up to 48 hours for verification to complete and the domain to connect.

Connected

Connected

all-in-poker.app

This email domain is verified and connected without a DMARC record. [Learn more.](#)

If your domain is stuck in "Pending"

If your domain status is stuck in **"Pending"** for more than 48 hours after setup, follow these steps:

- Click the **Edit** button (shown below).
- Go through the setup steps again.
 - If you've already added the correct CNAME records, simply click **Confirm** when you reach the DNS record page.
- If your records are verified, your status will change to **Connected**.
 - If not, it will remain in **Pending** until verification completes.

This can sometimes take additional time depending on your DNS provider's propagation speed.

Pending

glitteringgoldie.com

This email domain verification is pending. It can take up to 48 hours for verification to complete and the domain to connect.

