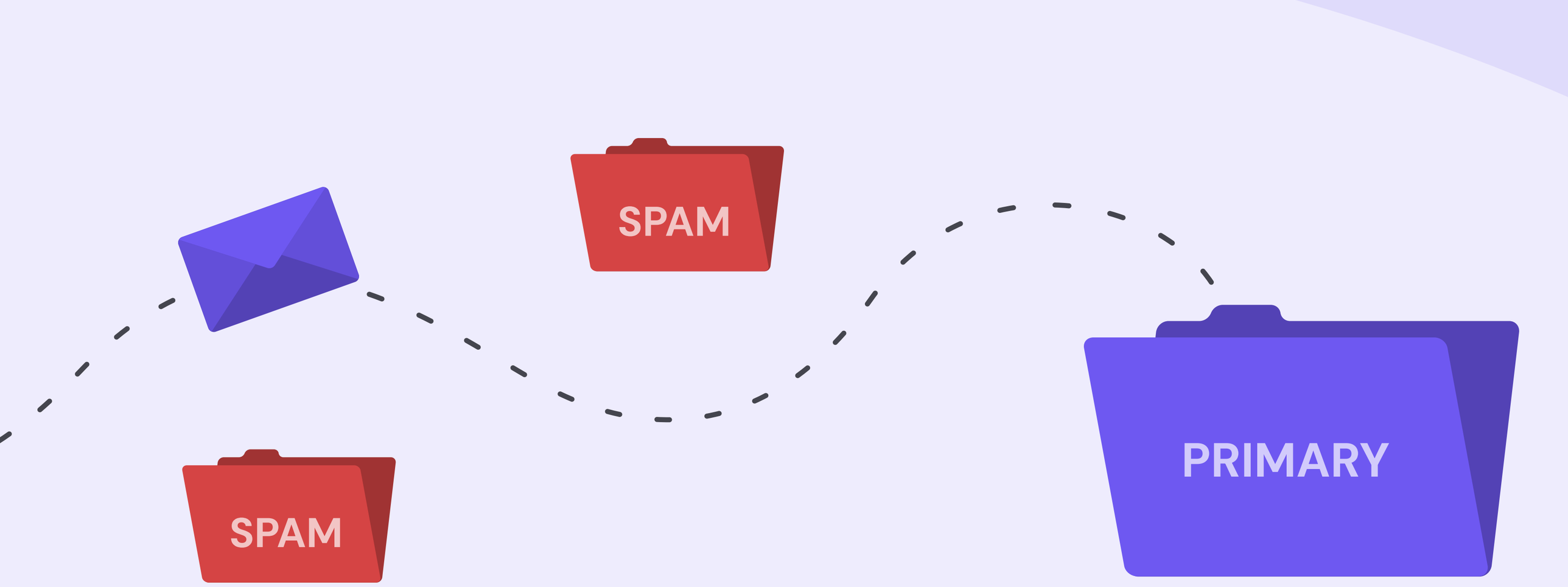
Smartlead's Email Deliverability Guide:

From Sending to Inbox



Smartlead.ai

Table of contents

Introduction

Have you ever crafted the perfect email campaign, only to have it vanish into the dreaded spam folder?

As an email marketer, that's your worst nightmare. You pour your heart (and resources) into creating compelling content, but it never reaches the intended audience. The result? Poor campaign performance and frustrated you.

Email remains a powerful marketing tool. Despite the rise of new channels, email marketing continues to thrive. ***In fact, billions of emails are sent daily, with the average person receiving over 100! The reason? It's a direct and personalized way to connect with your customers.***

However, navigating the challenges of email deliverability can be tricky. Spam filters constantly search for unwanted messages, and a staggering percentage of emails never reach inboxes.

But as a leader in email deliverability solutions, Smartlead can help you navigate these challenges with ease. More than 26.5M emails are sent from our tool per day, and many of our customers see a deliverability rate higher than 95%.

Built on our experience of working with top agencies and cold marketers, this ebook is designed to equip you with a one-stop guide for nailing email deliverability.

Here's what you'll learn:

- The fundamentals of email deliverability and why it matters.
- Key technical aspects that impact email deliverability.
- How to set a campaign in Smartlead to improve deliverability.

- Sneak peek into our new feature - email deliverability suite and other free tools that can help you solve your deliverability woes.

By the end of this guide, you'll be well on your way to landing your emails in inboxes, not spam folders.

1 Basics of Email Deliverability

1.1 What is Email Deliverability

Email deliverability refers to the ability of your email messages to successfully land in the intended recipient's inbox rather than being filtered out and sent to spam or junk folders. Yes, it is that simple. But when it comes to execution, that’s where the real challenge lies.

This brings us to the concept of email delivery - which is mainly confused with email deliverability.

But there's quite a bit of difference between the two terms.

Both Email Delivery and Deliverability are crucial aspects of email sending, but they should not be considered the same.

Let's break it down:

- **Email Delivery:** Once you hit "send" on your email – successful delivery means the message has physically reached its destination.

- **Email Deliverability:** This goes beyond just reaching the server. It focuses on whether your email lands in the recipient's inbox or gets filtered out and sent to spam.

The goal of your email campaign should be to reach the primary folder. This will give your emails a better chance of being opened, read, and replied to.

Now, how do you calculate the deliverability rate?

Here's how:

$$\text{Deliverability Rate} = \text{Total Sent Emails} - \frac{\text{Number of Bounces}}{\text{Total Emails Sent}} \times 100$$

For example, if you sent 1000 emails and 50 bounced, your calculation would look like this:

Deliverability Rate = (1000-50/1000) x 100

i.e.,

(950/1000) x 100 = 95%

Calculating the deliverability rate matters because it gives you more insight into your email campaign's success. You might have a 100% email delivery rate, but if the emails land in spam, they will not be useful.

But ***how do you know when your email deliverability is poor?***

According to industry benchmarks, **a good deliverability rate above 89%** indicates a healthy sender reputation. If you want to aim for excellence, shoot for over 95%.

The problem comes when your deliverability is below 80%. (we recommend to try and keep it above 95% only)

The Telltale Signs of Low Deliverability

- A sudden or sustained drop in open rates suggests your emails might be landing in spam folders or recipients are losing interest in your content.
- A significant increase in bounces can signal several issues, including an outdated email list, typos in addresses, or exceeding sending limits.
- Recipients marking your emails as spam directly affects your sender reputation and future deliverability.
- In extreme cases, internet service providers (ISPs) might block your emails if they suspect spam-like practices.

So, by now, you have a basic idea of what email deliverability is and ways to calculate it. Next, let's directly get into business and discuss how you can improve your email deliverability. We will look at the top factors that affect your deliverability and how you can optimize each one of them.

2 How To Improve Your Email Deliverability:

Key Strategies and Best Practices

2.1 Set Up The Right Email Infrastructure

2.1.1 Complete SPF, DKIM, and DMARC Setup

Authentication protocols like SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting & Conformance) are your secret weapon for improving email deliverability. These protocols work together to build trust with ESPs (Email Service Providers) and ensure your emails reach inboxes, not spam folders.

How SPF protects your email

SPF is like a bouncer for your email domain. It ensures that only approved servers can send emails on your behalf, preventing email spoofing.

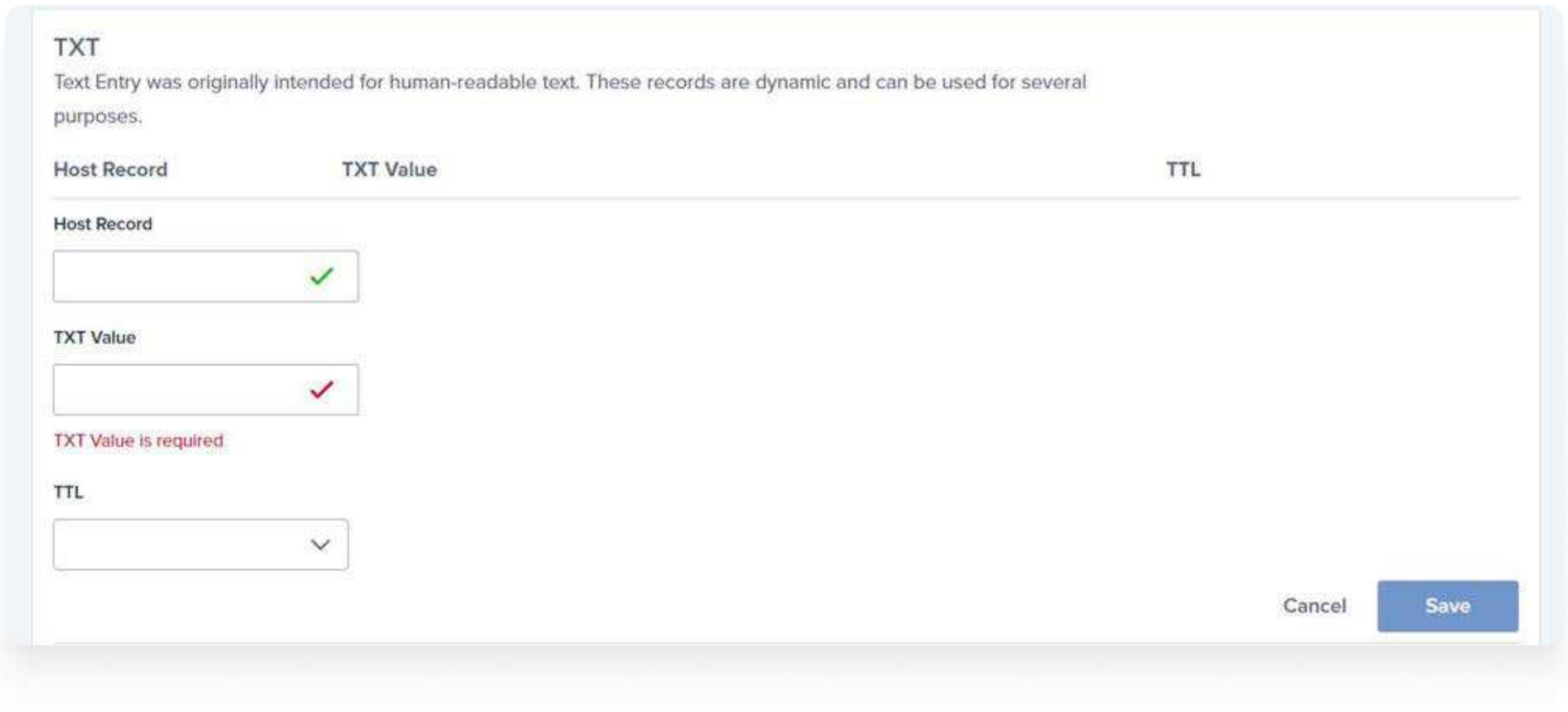
Here's how it works: You set up an SPF record in your domain's DNS settings, listing the IP addresses of the servers allowed to send emails from your domain. When you send an email, the recipient's mail server checks your SPF record to verify if the sending server is on your approved list.

If the server is listed, the email is considered legitimate and goes through. If it's not, the email might be marked as spam or rejected. For example, an SPF record might look like this: v=spf1 ip4:192.168.1.1 include:_spf.google.com -all. This means emails can only be sent from the IP address 192.168.1.1 and Google's mail servers. Any other server's email should be rejected.

Let's break down the steps to set it up:

a) SPF:

- Log in to your DNS settings from your domain registrar or hosting provider (GoDaddy, Zoho, etc.)
- Create a new record with the type "TXT."



- Name: Use "@" or a prefix like "mail," depending on where you want to place the record on your domain.
- Value: This specifies authorized email sending IP addresses (consult your provider for the exact format).
- TTL: Keep the TTL (Time To Live) at default settings.
- Save the record.

Use our free SPF Record Lookup to verify your SPF records.

How does DKIM work?

DKIM is like a secret handshake for your emails. It ensures that your emails haven't been tampered with in transit and verifies that they're truly from you.

Here's how it works: When you set up DKIM, your email server adds a special digital signature to the header of every email you send. This signature is generated using a private key that only your server knows.

On the recipient's end, their mail server looks up the public key that you've published in your domain's DNS records. It uses this public key to verify the signature. If the signature matches, it confirms that the email is legit and hasn't been altered since it was sent.

Here's how you can set up a DKIM record:

- Log in to your DNS settings again.
- Create a "TXT" or "CNAME" record based on your hosting provider's instructions.
- Paste the DKIM value provided by your hosting provider.
- Set the Hostname as instructed (e.g., s1._domainkey).
- Save the record.

Use our DKIM Record Lookup to verify if your DKIM is published correctly.

How DMARC works

DMARC is like your email's bodyguard. It helps prevent email spoofing and phishing by making sure only legitimate emails are sent from your domain. Think of it as a checkpoint that verifies both SPF and DKIM are in place before allowing emails through.

Here's the scoop: when you set up DMARC, you publish a DMARC policy in your DNS records. This policy tells receiving mail servers what to do if an email fails the SPF and DKIM checks. You can set the policy to one of three modes:

- None (p=none): This is a "monitoring" mode. It doesn't affect email delivery but helps you collect data on how your emails are being authenticated.

- Quarantine (p=quarantine): Emails that fail the checks might end up in the spam folder.
- Reject (p=reject): This is the strictest. Emails that fail the checks are outright rejected and never reach the inbox.

For cold emailing, you might think that starting with a "none" policy is usually a good idea. It may be, but you should take DMARC quite seriously to ensure that only legitimate emails reach the inbox. You can start with a quarantine policy, and once you see good results in terms of deliverability and reputation, you can fully protect your domain from misuse by switching to a "reject" policy.

Here's how you can set up a DMARC record:

- You can set up DMARC records in your DNS settings.
- Add a DNS TXT record for "_dmarc.yourdomain.com"
- In the second field, enter the text for your DMARC policy (e.g., v=DMARC1; p=none; rua=mailto:dmarc-reports@example.com).

The specific policy settings will vary depending on your needs.

You can check your DMARC records for free by using our DMARC Checker.

2.1.2 Set Up Secondary Domains

While email authentication is crucial, email deliverability is a constant battle. One strategy you can employ to optimize deliverability is leveraging secondary domains. These are additional email addresses under different domain names, all managed through your primary account.

But how do secondary domains impact deliverability?

IP reputation plays a significant role in email deliverability. When you send a large volume of emails from a single domain and IP address, it can raise red flags for ESPs, especially if you're new or haven't established a positive reputation yet.

Secondary domains help you spread your email sending across multiple IPs, effectively diversifying your reputation. This can be particularly beneficial for:

- **High-Volume Senders:** If you send a large number of cold emails, using secondary domains distributes the sending load across different IPs. This reduces the risk of your primary domain's IP getting flagged for suspicious activity due to high sending volume.

- **Targeted Campaigns:** Secondary domains are excellent for sending targeted email campaigns. For example, a company with a primary domain, "companyname.com," could use a secondary domain, "[companygrowth.com]," for its welcome emails to new customers. This keeps email content specific and avoids overwhelming inboxes with a mix of emails under the same domain.

At Smartlead, we recommend setting up secondary domains before you start sending warm-up emails or running any email campaign.

2.1.3 Shared vs. dedicated IPs

When it comes to cold emailing, the choice between shared and dedicated IP addresses can significantly impact your email deliverability and overall campaign success.

A shared IP address is used by multiple senders. Your emails are sent from the same IP address as other users. Shared IPs are generally less expensive because the cost is distributed among multiple users. Your email deliverability can be affected by the actions of other users sharing the same IP. If they send spammy or low-quality emails, it can damage the IP's reputation.

A dedicated IP address is used exclusively by one sender. Your emails are sent from an IP address that only you control. This means your deliverability is solely influenced by your own email practices.

You need to gradually increase your email volume to establish and maintain a good sending reputation. This process, known as IP warming, can take time and effort (more on this later).

At Smartlead, we recommend dedicated IPs for email campaigning to help improve your deliverability.

2.1.4 Use Custom Tracking

By default, many email marketing platforms use shared tracking domains to register link clicks and email opens. This means all their users' links might point to a generic domain. This might affect your email deliverability.

Why?

Because the same "tracking" domain is employed across thousands of campaigns established by all users of the cold emailing software, ESPs can easily understand that numerous emails are being opened, and they all generate "requests" to the same "tracking URL." This could potentially result in a slight decrease in your deliverability.

So, what's the solution? It's straightforward.

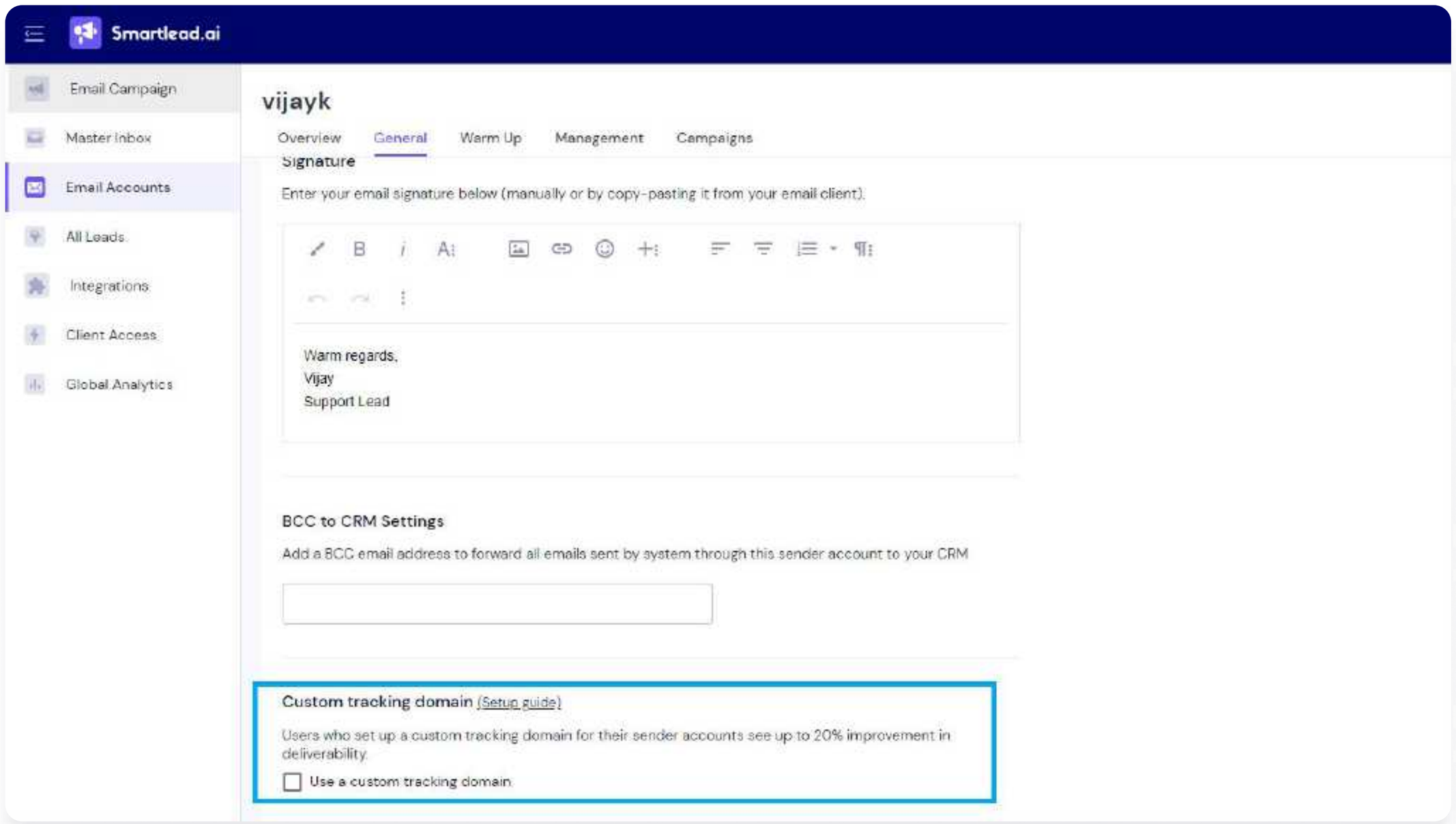
You can outsmart the ESP by "masking" the tracking URL with your own.

How to Set Up Custom Domain Tracking?

a) In Smartlead

Step 1:

- Create a new email account or access an existing one within the Smartlead app.
- Navigate to the Custom Tracking Domain section located under the 'General' tab.



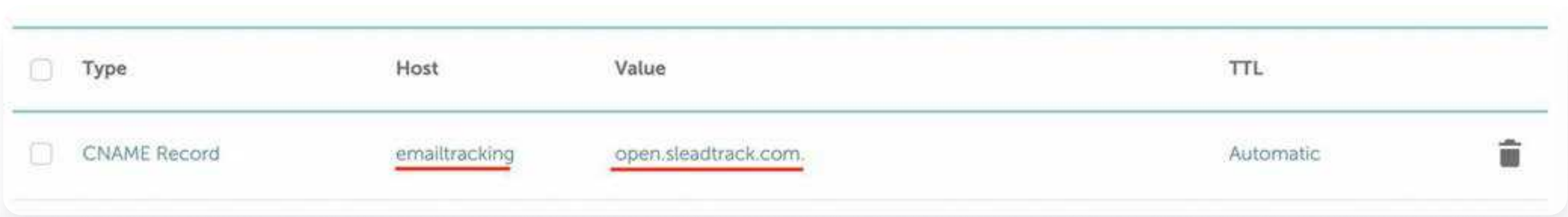
Step 2:

Open your domain management tool, e.g., Godaddy, Namecheap, Crazydomains, etc.
(Here, we have used Namecheap, for example)

Head over to the DNS management section.

In your Host Records section, add a CNAME with the following:

- Type: CNAME Record
- Host: emailtracking
- Value: open.sleadtrack.com
- TTL: Automatic

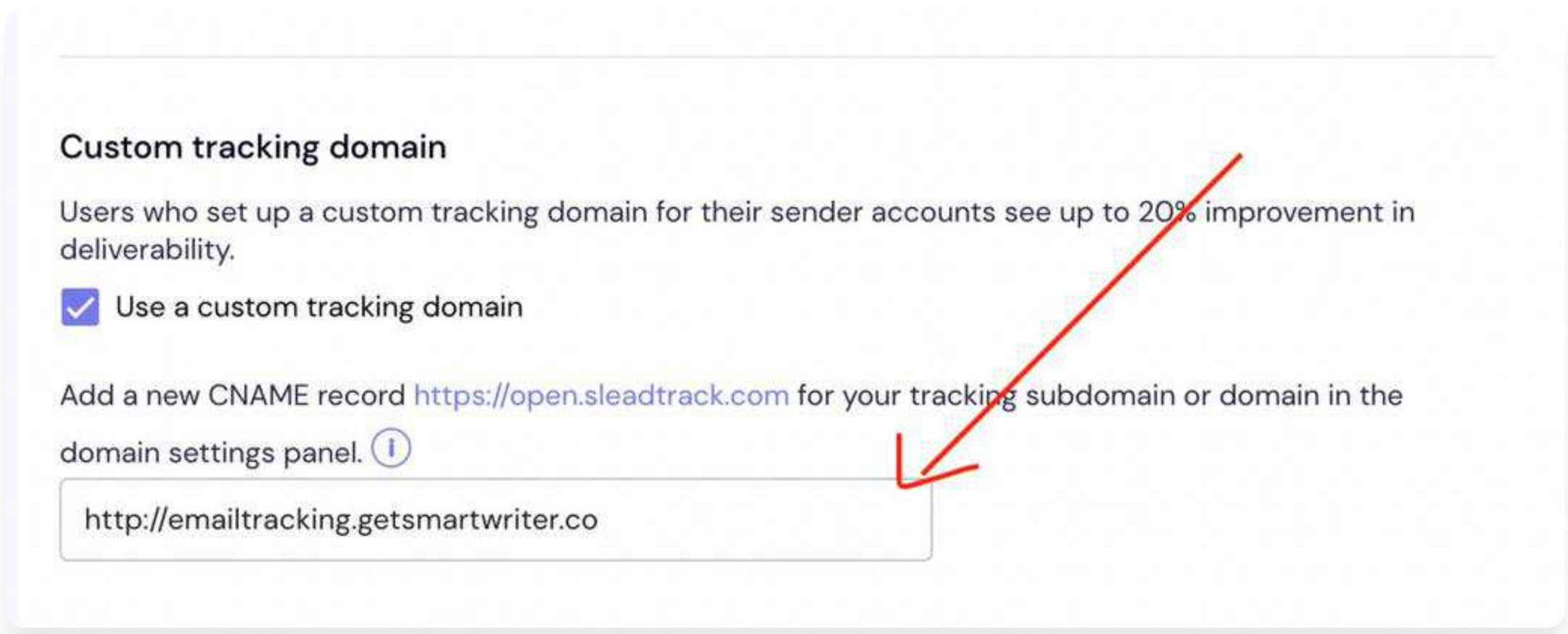


After completing this step, allow 30 minutes to 24 hours for the changes to take effect in your account.

Next, proceed to your Smartlead dashboard and paste the full URL into the text field following the format shown below.

http://{host}.{yourdomain}

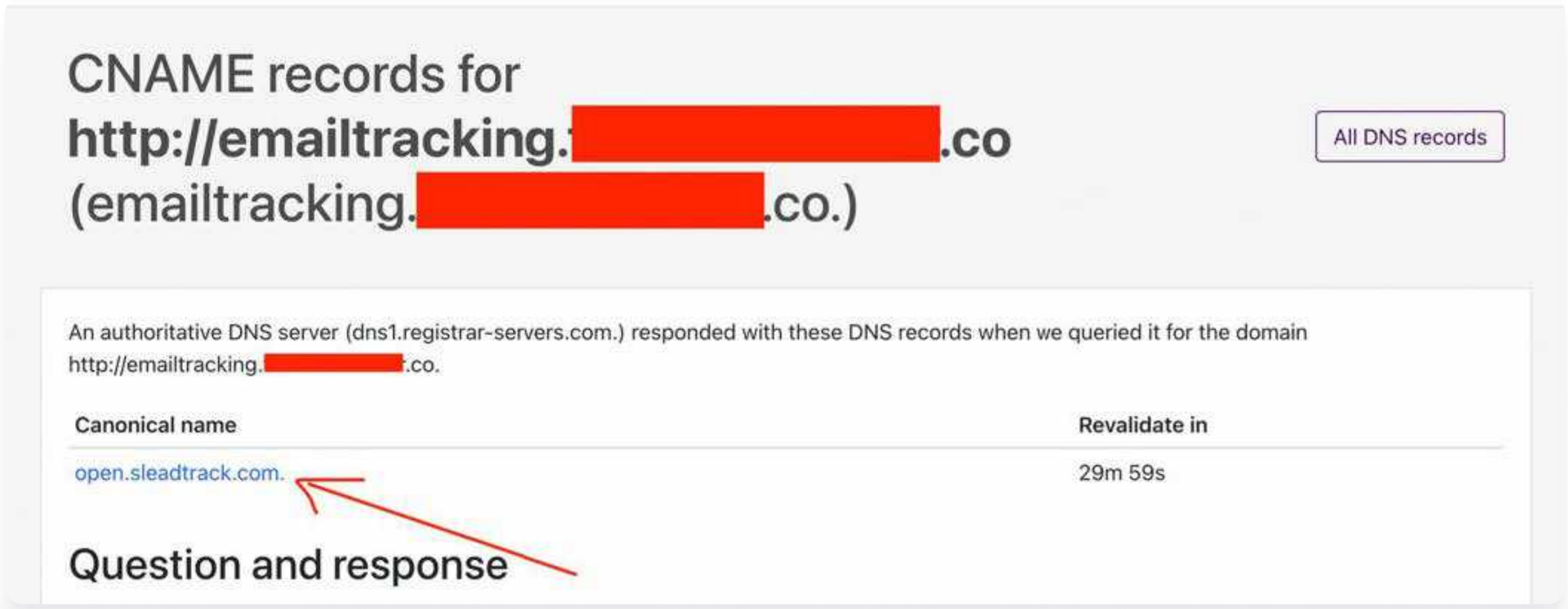
In my case, the domain is *getsmartwriter.co*, and my host is *emailtracking*



Verify Your CNAME Tracking

If you've done things right. Click on the "Verify CNAME" button. It'll take you to a nslookup.io link.

If underneath the "Canonical name," it says "open.sleadtrack.com," then you did it right.



b) In GoDaddy

Step 1: Setting up a CNAME Record on GoDaddy

Sign in to GoDaddy and navigate to your dashboard.

- Click on "My Products."
- Locate your domain.
- Select the "DNS" button.
- On the DNS Management page, click "Add."
- Choose "CNAME" as the record type.

In the "Name" field, designate the name of your subdomain. You have the flexibility to choose the name for your tracking domain, but we recommend simplicity, such as "tracking." Thus, your final subdomain would resemble this: tracking.yourdomain.com.

The "Value" field should contain your ESP's tracking domain - in Smartlead's case, it will be open.sleadtrack.com. This step redirects your subdomain to your ESP's tracking domain, eliminating the need to display suspicious URLs from your ESP in your emails.

Save your record.

Please note: It may take a couple of days for your record to become active.

Once done, you just need to integrate your custom tracking domain with Smartlead. This is similar to what we did in Namecheap. Proceed to your app and paste the full URL into the text field following the format shown below.

http://{host}.{yourdomain}

Save changes once done.

c) In Cloudflare

Step 1: Add Your Domain to Cloudflare

- Login to Cloudflare: If you don't have an account, create one and log in.
- Add a Site: Click on the "Add a Site" button.
- Enter your domain name (e.g., yourdomain.com) and click "Add Site."
- Update DNS Records: Cloudflare will scan your existing DNS records. Verify that they are correct, then continue.
- Change Nameservers: Update your domain registrar's nameservers to the ones provided by Cloudflare.

Step 2: Create a Subdomain for Tracking

- In Cloudflare, go to the DNS section of your domain.
- Add a new CNAME record.
- Name: Enter the subdomain you want to use for tracking (e.g., open if you want open.yourdomain.com).
- Target: Set this to open.sleadtrack.com.
- TTL: Set to Auto.
- Proxy Status: Set to DNS only (grey cloud).

Step 3: Configure SSL/TLS

- Go to the SSL/TLS tab in Cloudflare.
- Ensure SSL is set to Full or Full (Strict), depending on your existing SSL setup.

Step 4: Verify and Update Smartlead Settings

Once you have added a CNAME record in Cloudflare, come back to Smartlead and add this record in the designated place and format, as we did for Namecheap.

Use tools like Smartlead's CNAME Checker to verify that your new CNAME record has propagated accurately.

2.2 Build (and maintain) Your Domain Reputation

Whenever you send a cold email to somebody, your emails will first go through a reputation-check. It basically means that the recipients' email clients are ensuring that only relevant and trustworthy emails reach the inboxes, rest everything is sent to either less important folders, like social or promotions in Gmail or in spam or junk.

Your domain reputation is difficult to build and maintain but quite easy to tarnish.

There are several factors that contribute to a solid reputation. We will cover all these factors in the subsequent sections.

If you have a new domain, reputation becomes even more critical as you are completely new and have no credibility in the email market right now. It is like when you have a low credit score and you face a difficult time getting approval for loans or credit cards. But the good news is that just like your credit score, your domain reputation can also be improved with time.

This will include steps like warming up your emails, cleaning up your email list, and following list hygiene.

2.2.1 Create a Clean Email List

A clean email list, free of inactive or invalid addresses, is essential for maximizing email deliverability. ESPs consider engagement metrics like open and click-through rates when determining where to deliver emails.

A clean list with engaged recipients translates to higher engagement metrics, increasing the likelihood of your emails reaching inboxes.

A clean list also minimizes bounce rates as the likelihood of the email addresses being invalid is less.

Here are some strategies for cleaning up your email list:

- **Identify Inactive Subscribers:** Segment your list and track engagement metrics. Consider unsubscribing or re-engaging those who haven't opened or clicked on your emails in a long time (define a specific timeframe relevant to your industry).

- **Remove Hard Bounces:** Hard bounces indicate a permanent delivery failure due to an invalid address. Remove these addresses promptly to maintain a clean list and improve bounce rates.

- **Consider Soft Bounces:** Soft bounces, like a full inbox, may be temporary. You can attempt to resend to soft bounces a few times but eventually remove them if deliveries consistently fail.

Here's a list of major bounce codes you can encounter. Remember that the codes starting from '4' are generally considered as soft bounce, while the ones starting from '5' are generally considered hard bounce.

```
5.1.1 - Bad destination mailbox address
4.2.2 - The email account is over quota
5.0.0 - Syntax error: invalid email address format
5.1.0 - Bad destination mailbox address
5.1.1 - Bad destination mailbox address
5.1.2 - Bad destination system address
5.1.3 - Bad destination mailbox address syntax
5.1.4 - Destination mailbox address ambiguous
5.1.5 - Destination mailbox address valid
5.1.6 - Mailbox has moved
```

```
5.1.7 - Bad sender's mailbox address syntax
5.1.8 - Bad sender's system address
5.1.9 - Message relayed to non-existent domain
5.2.0 - Other or undefined mailbox status
5.2.1 - Mailbox disabled, not accepting messages
5.2.2 - Recipient's mailbox is full and cannot accept new messages
5.2.3 - Message length exceeds administrative limit
5.2.4 - Mailing list expansion problem
5.3.0 - Other or undefined mail system status
5.3.2 - System not accepting network messages
5.3.3 - System not capable of selected features
5.3.4 - Message too big for system
5.3.5 - Recipient's mail system is misconfigured
5.4.0 - Other or undefined network or routing status
5.4.1 - Recipient's mail server did not respond
5.4.2 - Problem with the connection to the recipient's mail server
5.4.3 - Routing server encountered an error while delivering the message
5.4.4 - Message cannot be routed to the recipient's mail server
5.4.5 - Network congestion is preventing delivery of the message
5.4.6 - Routing loop detected while delivering the message
5.4.7 - Message delivery time expired
5.5.0 - Other or undefined protocol status
5.5.1 - SMTP command issued by the sender is invalid
5.5.2 - SMTP command syntax is incorrect
5.5.3 - Recipient count exceeds the maximum allowed by the recipient's mail system
5.5.4 - Arguments provided with the SMTP command are invalid
5.5.5 - SMTP protocol version used by the sender is not supported
5.6.0 - Other or undefined media error
5.6.1 - Recipient's mail system doesn't support the media type used by the sender.
5.6.2 - Conversion between media types is required but prohibited.
5.6.3 - Conversion between media types is required but not supported
5.6.4 - Conversion with loss performed
5.6.5 - Conversion between media types failed
5.7.0 - Other or undefined security status
5.7.1 - Delivery not authorized, message refused
5.7.2 - Mailing list expansion prohibited
5.7.3 - Security conversion required but not possible
5.7.4 - Security features not supported
```

```
5.7.5 - Cryptographic operations performed by the sender failed
5.7.6 - Cryptographic algorithm not supported
5.7.7 - Message integrity failure
```

The above are SMTP bounce codes, there are some traditional bounce codes as well:

```
420 - Network congestion or server issue
421 - Receiving server temporarily unavailable
422 - Recipient's mailbox is full
431 - Receiving server encountered an error
432 - Recipient server is not accepting messages at the moment
441 - Recipient's server is not responding
442 - Connection was dropped
446 - Maximum hop count was exceeded (internal loop)
447 - Outgoing message timed out in the incoming server
449 - A routing error occurred
450 - Mailbox unavailable
451 - Local processing error temporarily
452 - Recipient's mailbox full temporarily
471 - Temporary error in the local server (additional information provided)
500 - Syntax error (command not recognized)
501 - Syntax error in parameters or command arguments
502 - The command is not implemented
503 - Bad sequence of commands
504 - Command parameter not implemented
510/511 - Bad email address; check the address
512 - DNS error; domain could not be found
515 - Destination mailbox address invalid
517 - Problem with the sender's mail attribute
521 - Domain is not accepting mail
523 - Server limit exceeded; message too large
530 - Access denied; authentication required
531 - Mail system full
541 - No response from host (might be due to anti-spam filter)
550 - Mailbox unavailable/Not found
551 - User not local; please try forwarding
552 - Exceeded storage allocation
553 - Mailbox name is invalid
554 - Transaction failed; recipient server suspects spam or your IP is blacklisted
```

When you use Smartlead to send emails, you also get the advantage of our Community Bounce Feature that can help you reduce bounce rates.

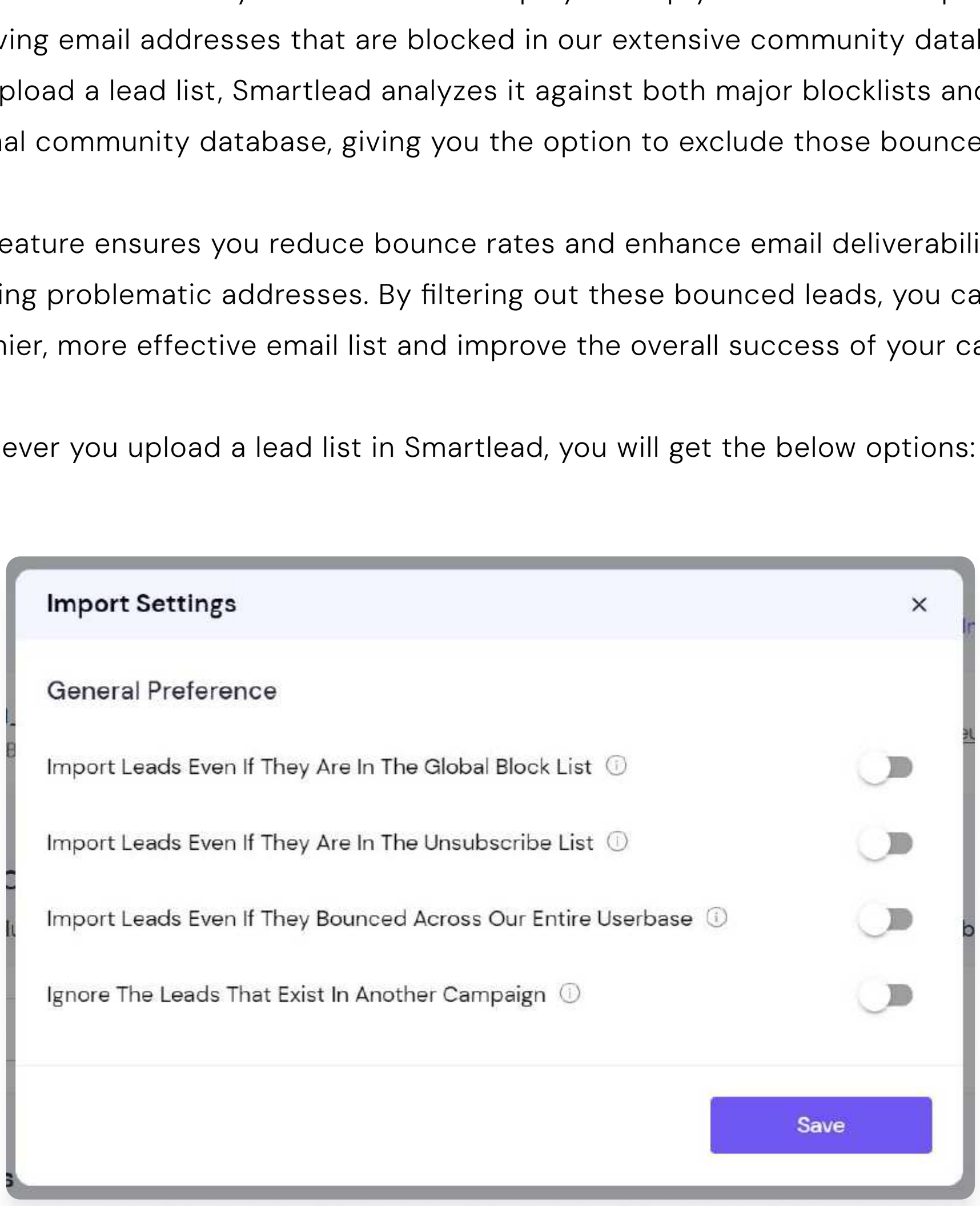
Here's what it is:

Community Bounce Feature

Smartlead's Community Bounce feature helps you keep your lead list in top shape by removing email addresses that are blocked in our extensive community database. When you upload a lead list, Smartlead analyzes it against both major blocklists and our internal community database, giving you the option to exclude those bounced leads.

This feature ensures you reduce bounce rates and enhance email deliverability by avoiding problematic addresses. By filtering out these bounced leads, you can maintain a healthier, more effective email list and improve the overall success of your campaigns.

Whenever you upload a lead list in Smartlead, you will get the below options:



If you enable the **"Import Leads Even If They Bounced Across Our Entire Database"** option, any lead that has bounced across our entire user base will still be imported. We **DO NOT RECOMMEND** to turn this feature on as it may lead to higher bounce rates.

- **Offer an Unsubscribe Option:** Always provide a clear and easy way for people to unsubscribe from your list. This ensures you're only sending emails to those who want to receive them, boosting engagement.

- **Use List Verification Tools:** Several tools can help you verify email addresses and identify invalid ones. These tools can streamline the cleaning process and save you time.

Verify Emails In Smartlead

Smartlead offers two ways to verify email addresses: a free version for individual checks and a paid version for bulk verification. Here's how to effectively use these options and verify emails in your lead list.

Free Version

Manual Check: To check the validity of a single email address, enter it into the free version of Smartlead's email verification tool.

This is ideal for verifying individual addresses but unsuitable for large lists.

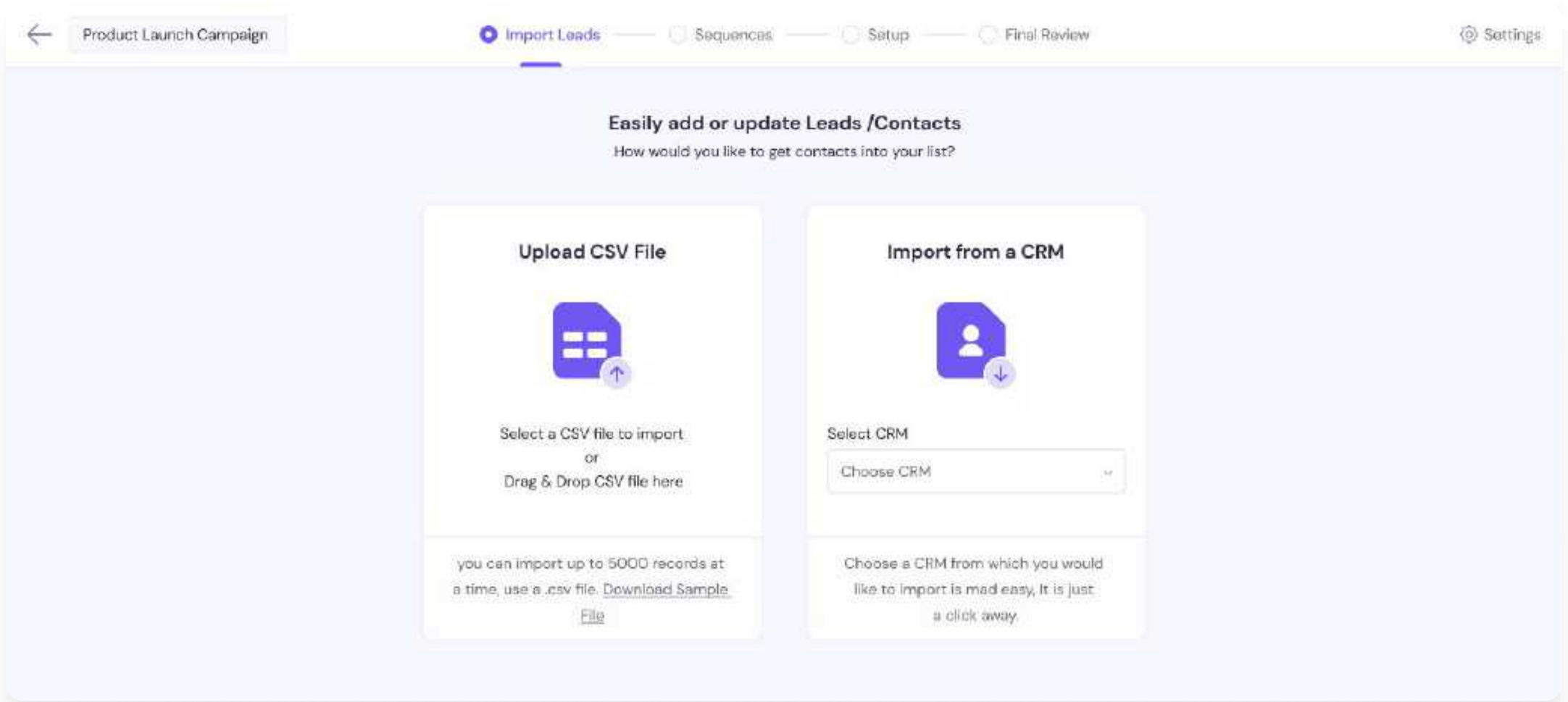
Paid Version

The paid version of Smartlead's email verification tool costs $15 USD for 6,000 credits. You can buy additional credits based on your needs.

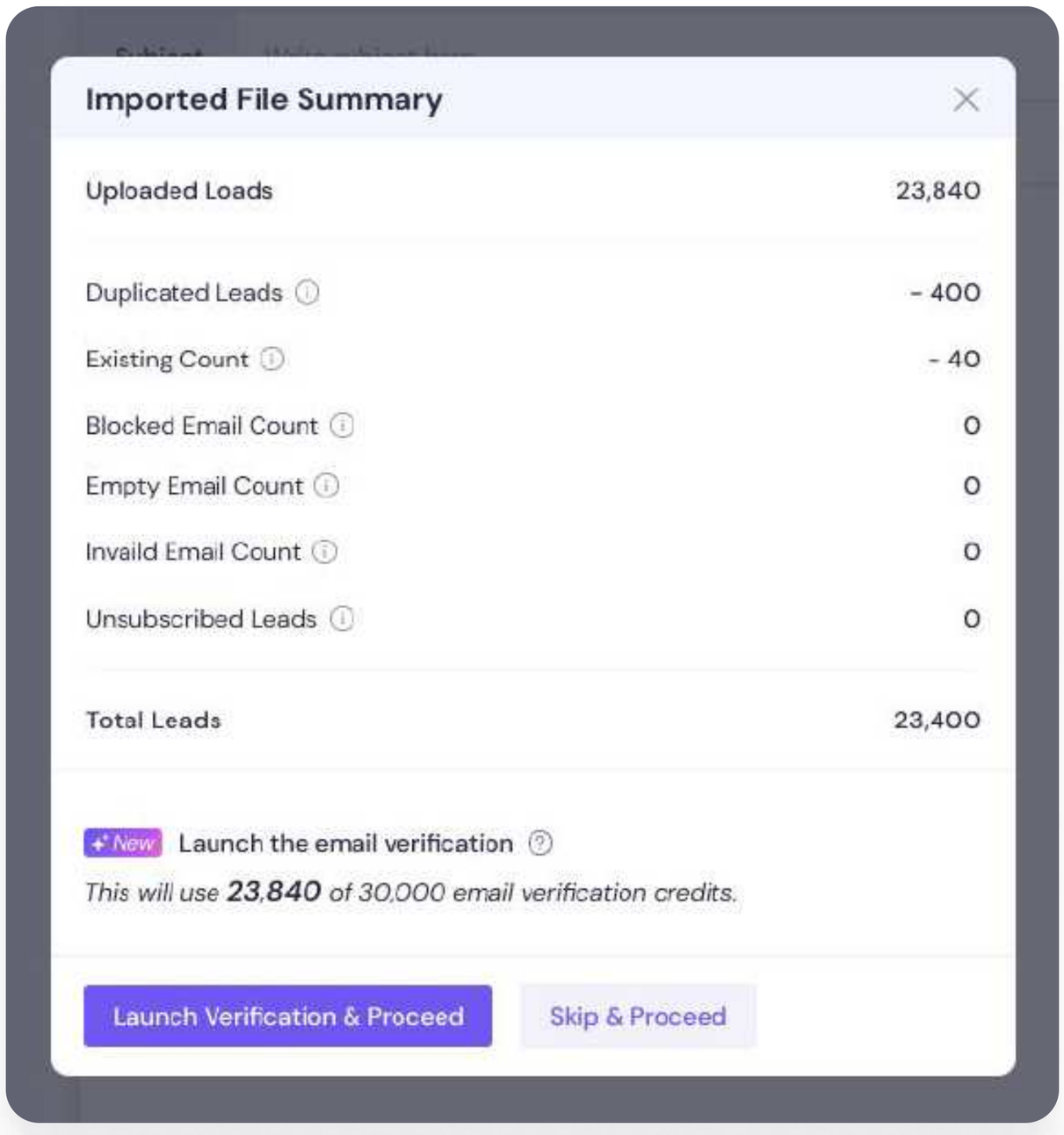
Follow these steps to verify emails in your lead list within Smartlead:

- **Add a New Campaign:** Log in to your Smartlead account and navigate to the campaign section. Click on "Add a New Campaign."

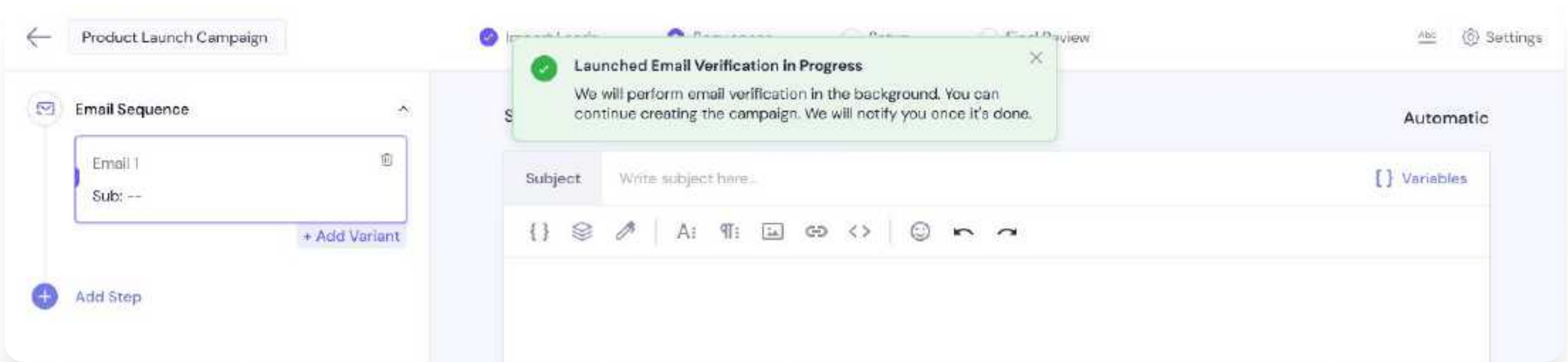
- **Import Your CSV File:** Select and upload your CSV file containing your lead list. Map the necessary fields to ensure proper data handling and click on "Save & Next."



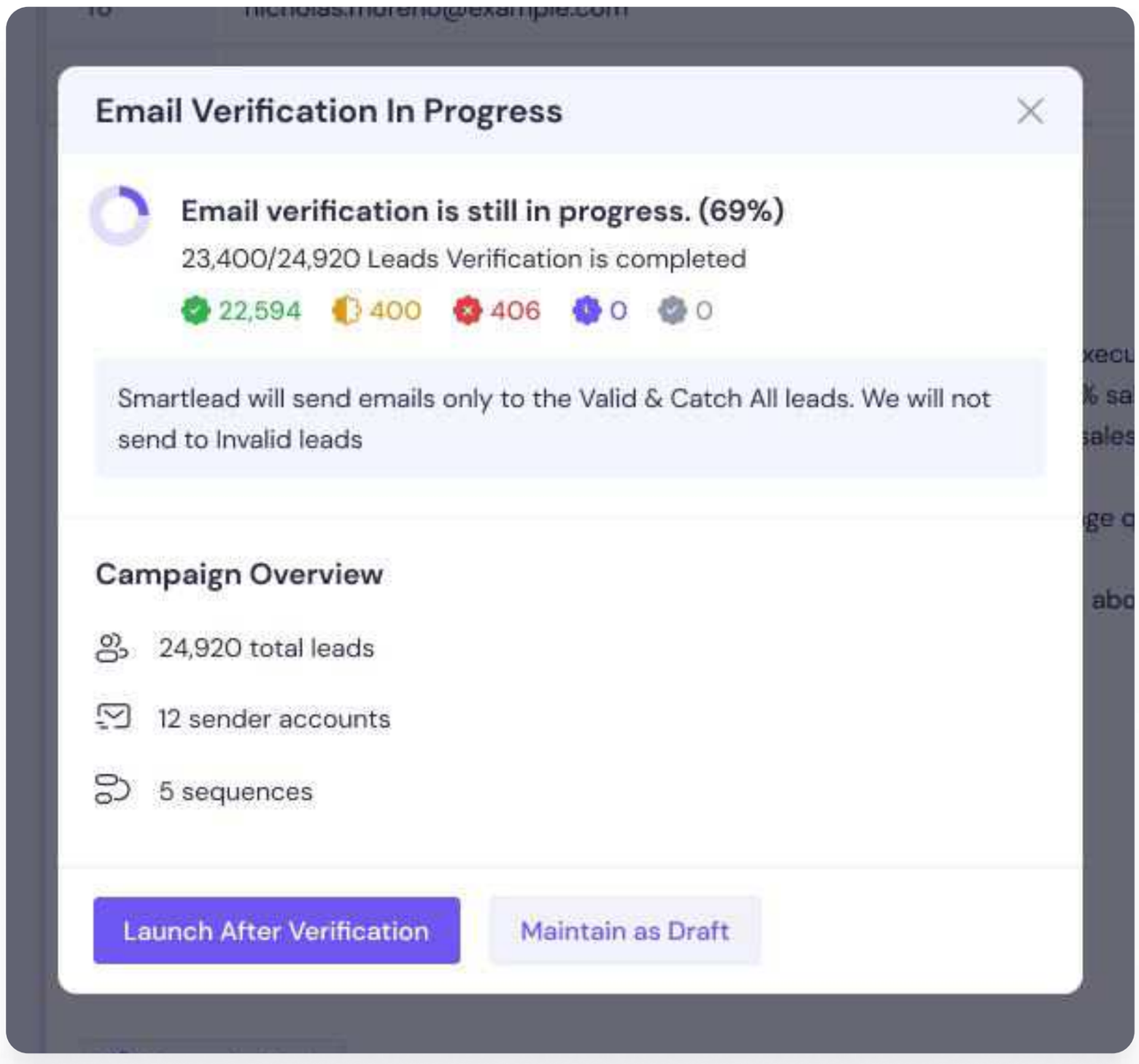
- **Launch Verification:** Click "Launch Verification & Proceed" in the popup window to start the email verification process.



- **Wait for Verification to Complete:** The time required for verification depends on the size of your CSV file. During this time, you can continue creating and setting up your campaign. You will receive a notification once the verification is completed.



- **Review the Report:** After the verification process is complete, check the full report provided by Smartlead. This report will detail the status of each email address.



- **Launch or Save Your Campaign:** You can now launch your campaign or save it as a draft. When you launch the campaign after verification, Smartlead will ensure that emails are only sent to valid addresses and catch-all leads.
- **Download Verified Leads:** The verified lead list can be downloaded as a separate CSV file from the "Import Lead" tab.

Please note that once a campaign is live, you cannot verify leads within that campaign. If you need to verify leads, it's best to set up a new campaign and use the email verification tool before launching it.

Personalize And Segment Your Email List

Segmentation involves dividing your email list into smaller groups based on specific criteria. This lets you send targeted emails with relevant and engaging content to each segment.

Subscribers are more likely to open and click on emails that are relevant to their interests. Higher engagement metrics signal to email service providers that you send valuable content, positively impacting deliverability.

Here are some ways to segment your email list:

- **Demographics:** Segment by age, gender, location, etc., to tailor content based on audience demographics.
- **Behavior:** Segment based on past purchases, website visits, or email engagement to send targeted offers or content.
- **Interests:** Segment based on subscriber preferences or expressed interests to deliver highly relevant content.

Once you have a clean, verified, and segmented lead list, you can proceed with warming up your domains.

2.2.2 Warm Up Your Domains

Domain warming refers to gradually increasing the emails sent from a new domain. This helps establish a positive reputation with ESPs and improves your chances of landing in inboxes.

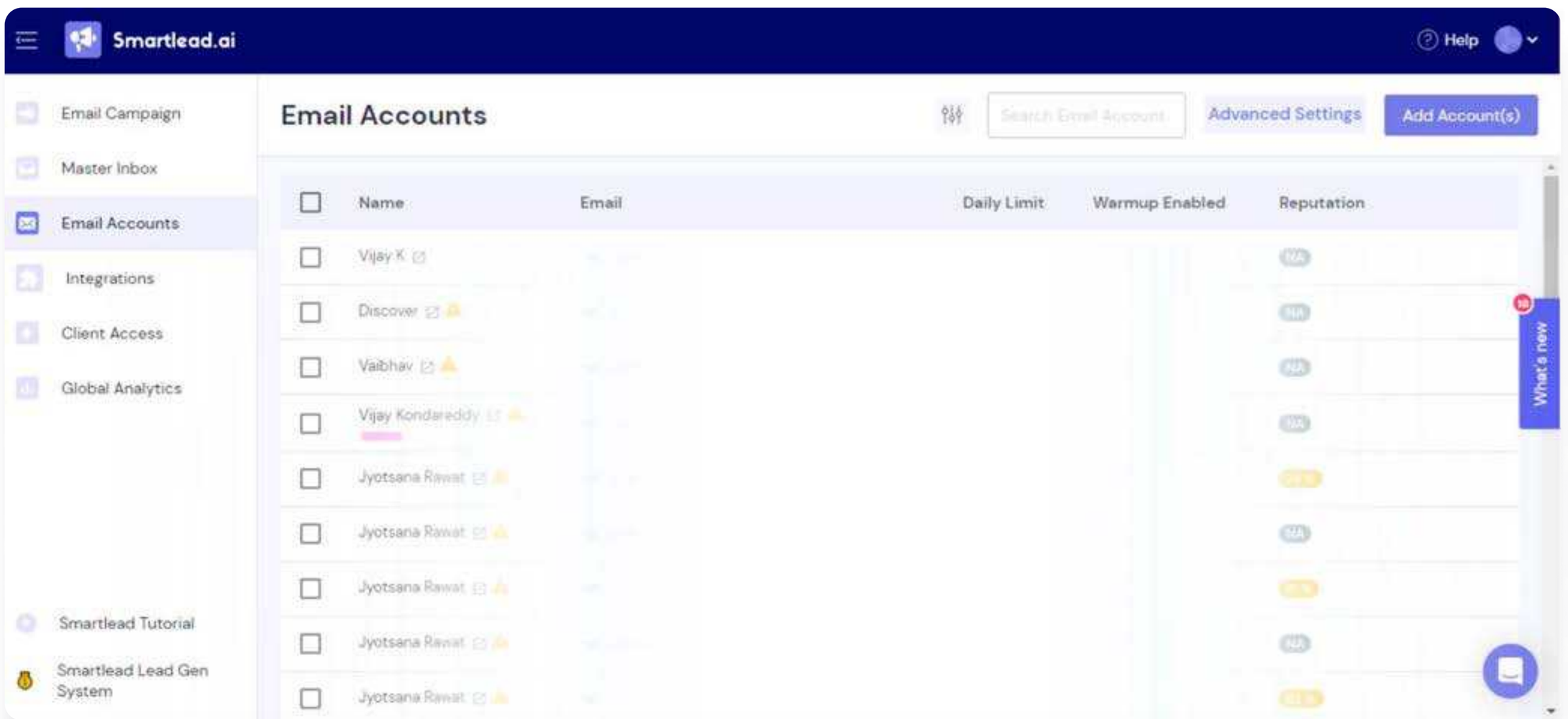
If you're using Smartlead to send cold emails, here's how you set up warmup settings.

Email Warmup Using Smartlead

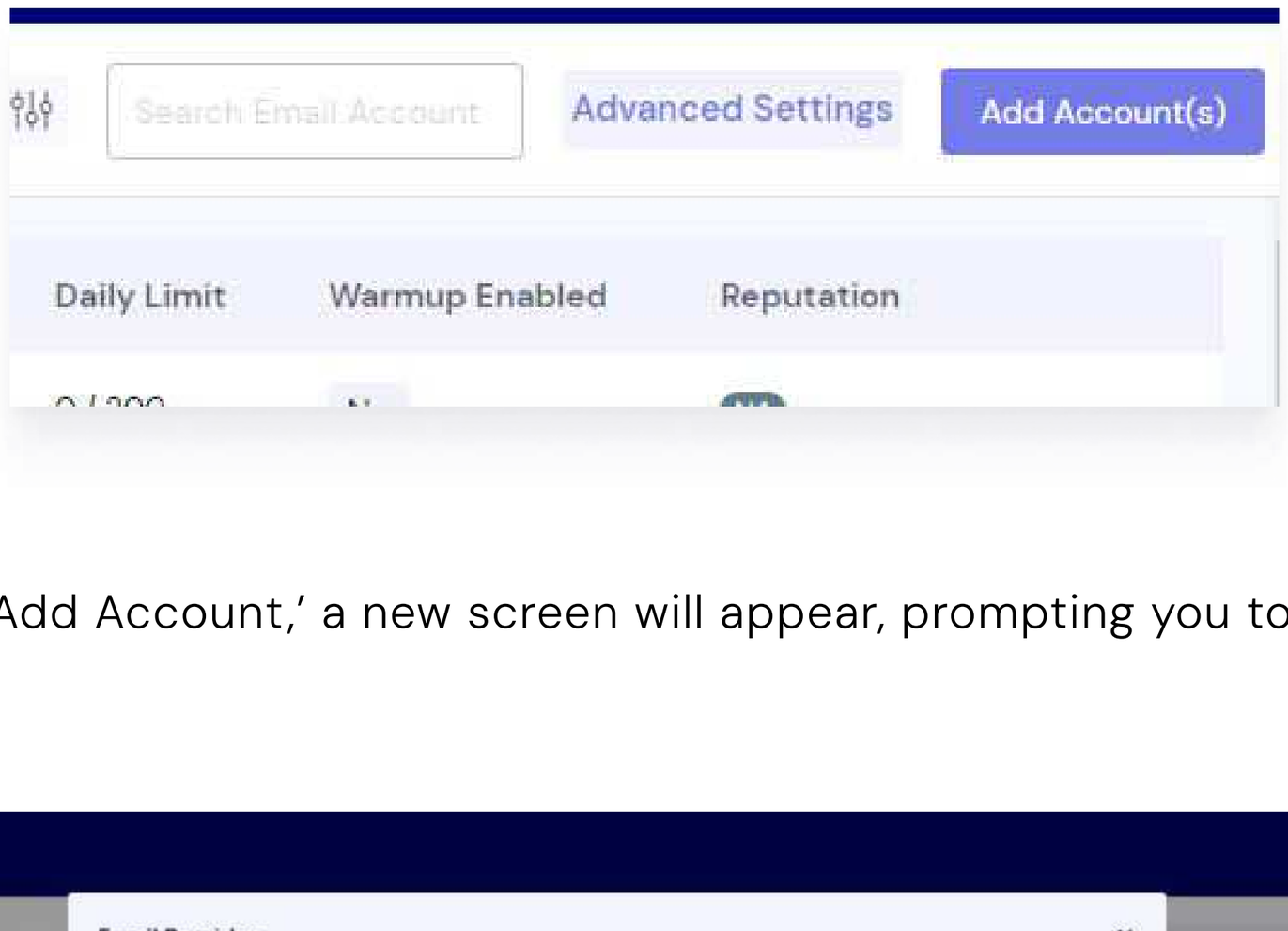
Smartlead offers an AI-powered solution to streamline the warmup process.

Let's Walk Through the Smartlead warm-up Process:

- **Set Up Your Account:** Sign in and navigate to the "Email Accounts" tab.



- Click "Add Account" and choose your email provider (Gmail, Outlook, etc.).



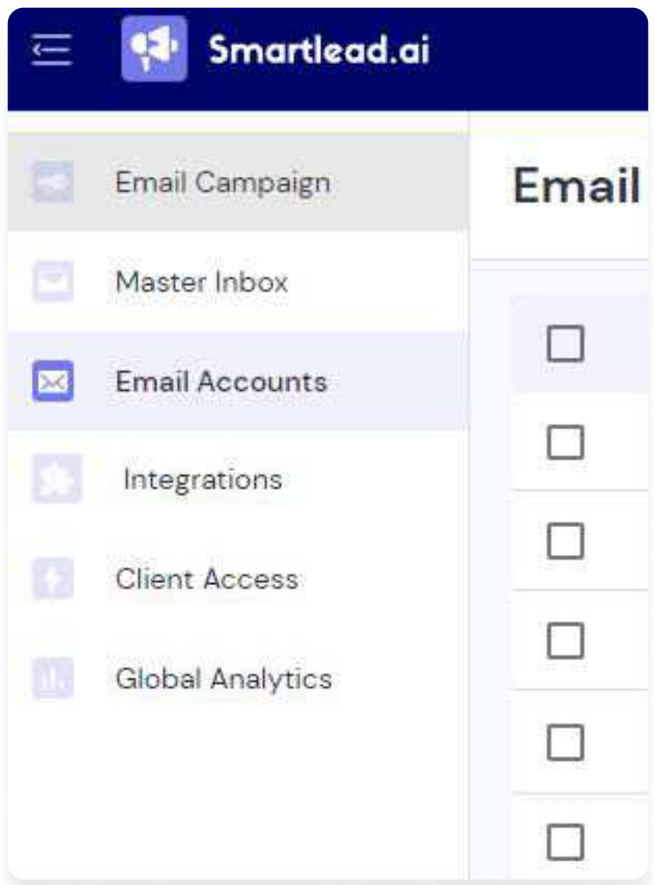
Once you click 'Add Account,' a new screen will appear, prompting you to select your email service.

Complete authentication (SPF, DKIM, DMARC, & MX) based on your selected service. If you are using Smartlead, check out this article to learn more.

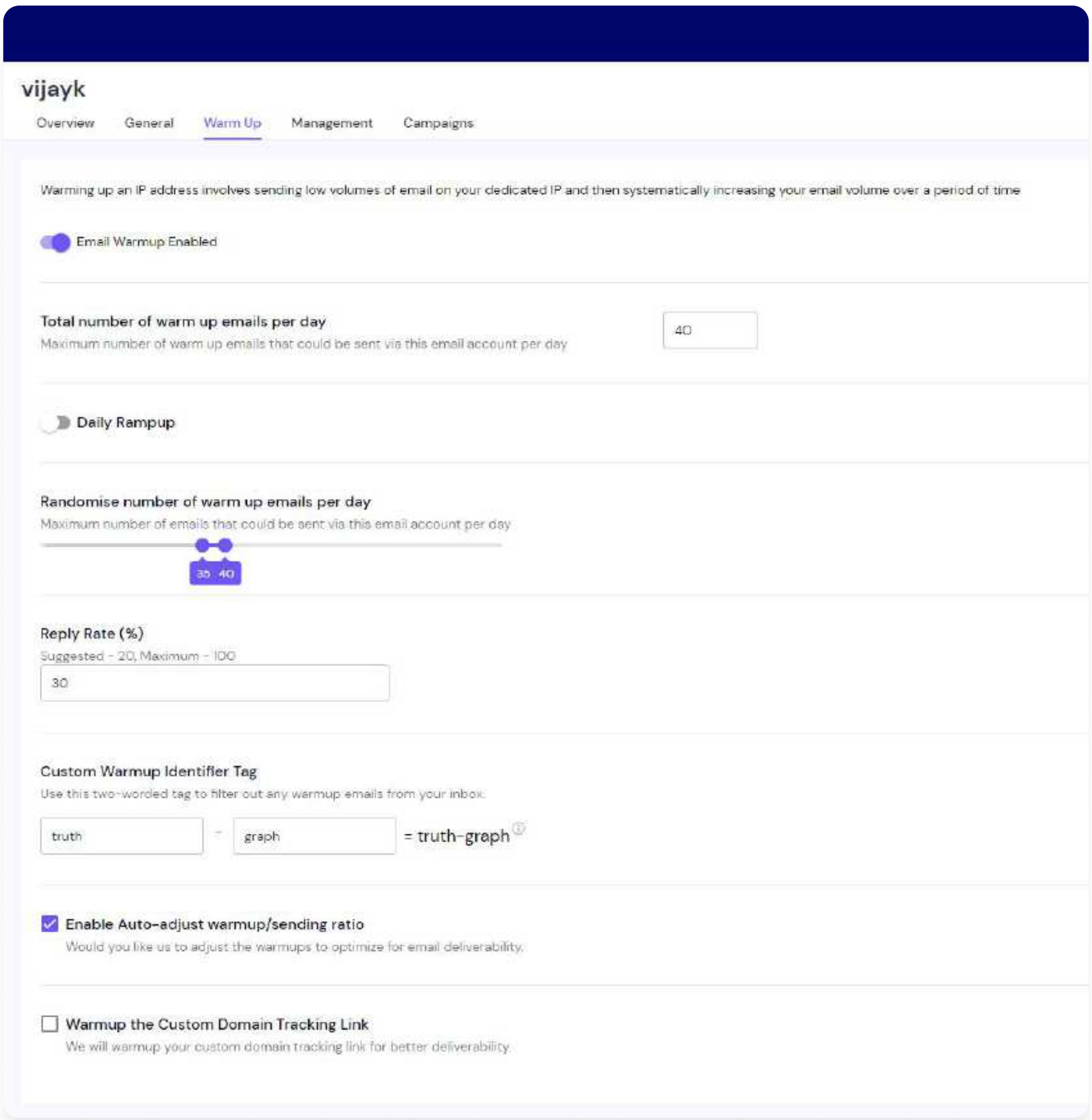
These settings are crucial for email deliverability. Smartlead provides resources to guide you through this step.

Once the authentication is done, you can continue with the warm-up process.

- In the "Email Accounts" tab, choose the email address you want to warm up.



Configure Warm-Up Settings:



- **Daily Emails:** Keep it under 40 initially.
- **Daily Ramp Up:** Gradually increase sending volume over time (recommended for new domains).
- **Randomize Daily Volume:** Mimic natural sending patterns.
- **Reply Rate:** Set between 30-40% to simulate engagement.
- **Custom Warm-Up Identifier Tag:** Filter warm-up emails from your inbox.

Click "Save/Update" to initiate the warm-up. Smartlead's dashboard allows you to track the progress.

2.2.3 Avoid Being Listed On Any Blacklists

A blacklist in the context of email marketing is a list of IP addresses or domains that are known or suspected to send spam. When an IP address or domain is blacklisted, emails sent from it are more likely to be blocked or sent to the spam folder by ESPs.

A high spam rate can indicate that your domain can be blacklisted on any of the blacklists. These blacklists go around by multiple names like real-time blackhole lists (RBLs), DNS blacklists, or simply email blacklists. If your domain is on one of them, your emails will land in spam folders.

Let's look at some of the most common RBLs as well as their return codes.

List of Popular RBLs

a) Spamhaus Block List (SBL)

Impact: High

One of the most well-known and respected blacklists, maintained by Spamhaus, a non-profit organization dedicated to fighting spam. The SBL identifies email addresses and IP addresses associated with spammers.

It maintains several other lists, including:

- Exploits Blocklist (XBL)
- Combined Spam Sources blocklist (CSS) (dataset included in the SBL DNSBL zone)
- Policy Blocklist (PBL)

Listing Criteria

- Snowshoe Spam: Poor or frequently changing identification in IP ranges and domains.
- Spam Hosting: IPs hosting spam-advertised websites or resources.
- Spam Operations: Known spam/malware operations listed in ROKSO.

Spamhaus Return Codes

Return codes for public IP zones are as below (Format: Return Code/Zone/Description)

- 127.0.0.2 (SBL): Spamhaus SBL Data
- 127.0.0.3 (SBL): Spamhaus CSS Data
- 127.0.0.4 (XBL): CBL Data
- 127.0.0.9 (SBL): Spamhaus DROP/EDROP Data (in addition to 127.0.0.2, since 01-Jun-2016)
- 127.0.0.10 (PBL): ISP Maintained
- 127.0.0.11 (PBL): Spamhaus Maintained

How to delist?

- Notification**:** Spamhaus researchers notify the responsible network or hosting company when an IP is listed.
- Action: If you are an end-user, contact your ISP or hosting provider to address the issue and request removal.
- Removal Request: The network owner must notify Spamhaus of any changes and request removal using the details provided in the listing notification.
- Check Listing: Use Spamhaus Check with the IP, IP range, or SBL ticket number to view and manage listings.

b) Barracuda Reputation Block List (BRBL)

Impact: High

Maintained by Barracuda Networks, a leading security provider, this RBL identifies IPs associated with spammers and phishing attacks.

Barracuda Return Codes:

- 127.0.0.2: Listed
- 127.0.0.3: Not listed
-

How to delist?

- Form Submission: Enter your email server's IP address, email address, phone number, and optional reason for removal on the Barracuda Reputation System's removal request form.
- Validation: Provide valid information, as incomplete or multiple requests will be ignored.
- Processing: Delist requests are typically processed within 12 hours if the information provided is valid.

c) SpamCop Blocking List (SCBL)

Impact: High

This RBL aggregates spam reports from users to identify spammers. It has a high impact on email deliverability.

SpamCop Return Code

- 127.0.0.2: Listed
- 127.0.0.3: Listed (less frequently used)

How to delist?

SpamCop will automatically remove your server from the blacklist after 24 hours, provided there are no additional spam reports.

d) Composite Blocking List (CBL)

Impact: High

Also maintained by Spamhaus, this RBL focuses on IPs with a high volume of spam complaints.

How to delist?

Removing your IP address from The CBL is straightforward. Visit The CBL IP address lookup page and request removal. If your IP is listed, the results will include detailed instructions on why you were listed and how to proceed with the removal.

e) SORBS (Spam and Open Relay Blocking System)

Impact: Moderate to High Impact

Maintains multiple RBLs for spam sources, open relays (unsecured servers that can be misused for spam), and dynamic IPs (frequently changing IPs). The overall impact can range from moderate to high, depending on the specific SORBS list.

SORBS Return Codes

127.0.0.2: General spam sources

127.0.0.3: Open proxies

127.0.0.4: Open relays

127.0.0.5: Open SOCKS proxies

127.0.0.6: HTTP proxy servers

127.0.0.7: Spam server

How to delist?

- **Listing Size:** If the listing includes more than a single IP, ensure the spammer is no longer using the address space to reduce the listing size.
- **Time-Based Penalty:** Be aware that a time-based penalty approach may apply.
- **Action:** Submit a delisting request through the SORBS website once the spam issue is resolved.

f) UCEPROTECT

Impact: Moderate

Offers various levels of RBLs targeting specific spam activities. The impact can be moderate depending on the specific list used.

UCEPROTECT Return Codes

- 127.0.0.2: Level 1 (Direct spam source)
- 127.0.0.3: Level 2 (Downstream spam sources)
- 127.0.0.4: Level 3 (Upstream spam sources)

How to delist?

To remove your server's IP address from UCEPROTECT, start by visiting their website at www.uceprotect.net. Navigate to the "Delisting Request" page, enter your server's IP address in the provided form, and follow the instructions to verify your IP address.

g) INVALUEMENT

Impact: Moderate

Invaluement offers several RBLs aimed at enhancing email security and minimizing spam:

- **IVRBL (IP-based):** This list focuses on identifying and blocking IP addresses known for sending spam. It is designed to provide high-accuracy listings to ensure minimal false positives, making it a reliable resource for email service providers and enterprises.
- **ivmSIP (Spammy IPs):** This RBL is dedicated to identifying spammy IP addresses that may not be listed by other well-known services like Spamhaus. It includes:
  - IPs from botnets.
  - IPs used by elusive snowshoe spammers.
  - IPs from black-hat mailbox providers.
- **ivmSIP/24 (Spammy IP Ranges):** This variant of ivmSIP focuses on identifying and listing sub-networks (/24 ranges) of IP addresses that exhibit spam-sending behavior, helping to block entire ranges of spam sources.

- **ivmURI (Spammy Domains and IPs):** This list targets Uniform Resource Identifiers (URIs), including both domains and selected IP addresses associated with spammers. It aims to detect and block spam content at the domain level, ensuring comprehensive coverage against spam originating from various sources.

Invaluement Return Codes

- 127.0.0.2: ivmSIP (Spam IP List)
- 127.0.0.3: ivmSIP/24 (Spam IP range)
- 127.0.0.4: ivmURI (Spam URI)

How to delist?

- Ensure No Spam: Cease all spam from your server and ensure email authentication.
- Visit Invaluement: Access the Invaluement Blacklist Removal Page and query your IP.
- Submit Request: If your IP is blacklisted, follow the delisting instructions provided.
- Send Email: Contact Invaluement with reasons for blacklisting (if known) and explanation for delisting.

Send emails from legitimate providers and avoid using free email services like Yahoo, Gmail, Hotmail, etc..

Note: Invaluement may disregard removal requests lacking genuine contact details or those sent from free email services.

h) SURBL

Impact: High

SURBL (Spam URI Real-time Blocklists) is another domain-based RBL. It lists domains that appear in spam emails, helping to block emails that promote spammy websites. SURBL data is used in conjunction with other spam filters to enhance detection accuracy.

SURBL Return Codes

- 127.0.0.2 - Indicates a site listed for spam or abuse.
- 127.0.0.4 - Lists domains used for disposable email services.
- 127.0.0.8 - Identifies phishing sites.
- 127.0.0.16 - Marks sites known to host or distribute malware.
- 127.0.0.32 - Specifies domains used for click tracking.
- 127.0.0.64 - Covers domains involved in various types of abuse, including spam.
- 127.0.0.128 - Indicates sites that offer cracked or illegally distributed software.

The IP address 127.0.0.X encodes which lists a domain is on:

Single List: The value of the last octet directly corresponds to a list.

- Example: 127.0.0.8 means the domain is on the phishing list (PH).
- Example: 127.0.0.64 means the domain is on the ABUSE list.

Multiple Lists: The last octet's value is the sum of the bit values of the lists.

- Example: 127.0.0.80 means the domain is on both MW and ABUSE (16 + 64 = 80).

How to delist?

- Security Measures: Remove all phishing sites, malware, and other security vulnerabilities from your website and systems.
- Audit: Consider a full security audit by a professional to ensure your site and systems are secure.
- Request Removal: Submit a removal request for the CR (Cracked), PH (Phishing), or MW (Malware) lists after securing your site.

Note: Check DNS infrastructure for malicious subdomains and secure it before contacting SURBL.

i) URIBL (Uniform Resource Identifier Blacklist)

Impact: High

URIBL is a domain-based RBL that lists domains found in the body of spam emails. It helps identify and block emails that contain links to known spammy domains, complementing IP-based RBLs.

URIBL Return Codes

The multi.uribl.com list consolidates data from multiple lists and is recommended for queries to get comprehensive results. When a domain is found on the multi-list, it returns an IP address of 127.0.0.X, where X indicates which list the domain is on. The return codes are as follows:

X Binary On List
---
1 00000001 Query blocked, possibly due to high volume
2 00000010 black
4 00000100 grey
8 00001000 red
14 00001110 black, grey, red (for test points)

How to delist?

- Account Registration: Register for an account with URIBL.
- Lookup: Use the URI lookup feature to confirm if your domain is listed.
- Delist Request: Use the same form to submit delisting requests

j) Mailspike

Impact: Moderate to High

Mailspike BL (Blacklist) is part of the Mailspike suite of DNS-based blacklists (DNSBLs) that are used to identify and block IP addresses associated with spam and other malicious activities. Mailspike provides several lists, including the blacklist (BL), to help email servers and administrators filter out unwanted emails and improve email security.

How to delist?

Category/ Level	Description	Category/ Level
L5 (-5)	Worst possible reputation	127.0.0.10
L4 (-4)	Very bad reputation	127.0.0.11
L3 (-3)	Bad reputation	127.0.0.12
L2 (-2)	Suspicious behavior reputation	127.0.0.13
L1 (-1)	Neutral - Probably spam	127.0.0.14
LHO	Neutral	127.0.0.15
H1 (+1)	Neutral - Probably legit	127.0.0.16
H2 (+2)	Possible legit sender	127.0.0.17
H3 (+3)	Good Reputation	127.0.0.18
H4 (+4)	Very Good Reputation	127.0.0.19
H5 (+5)	Excellent Reputation	127.0.0.20

How to delist?

- Form Submission: If your IP is blacklisted, fill out the "Request Delist" form available on the results page.
- Automatic Processing: Delist requests are automatic and typically fulfilled within one hour after submission.

Important Note: The return codes for the above-listed RBLs are usually returned by DNS queries to the RBL DNS server when an IP is checked against a blacklisted database. The specific meanings can vary between different RBLs, so it's important to check the documentation of the specific RBL you are querying to understand what each code signifies in their context.

General Interpretation of RBL Return Codes

RBL return codes are used to indicate why an IP address or domain has been listed on a blacklist. These codes help email administrators understand the specific reason for the listing and take appropriate actions to resolve the issue. Here's a more detailed interpretation of common return codes:

127.0.0.2

Meaning: General spam listing.

Use Case: This code is often used to indicate that an IP address or domain is listed for sending unsolicited bulk email (spam). It is a broad category and may encompass various types of spam activities.

127.0.0.3

Meaning: Additional reasons such as phishing, open proxy, or compromised server.

Use Case: This code can specify that an IP address or domain is involved in activities beyond general spam, such as phishing attempts, operating an open proxy that relays spam, or being part of a compromised server network used to send spam.

127.0.0.4

Meaning: Specific types of malicious activities.

Use Case: Often used to indicate more detailed reasons for listing, such as being part of a botnet, distributing malware, or engaging in snowshoe spamming (using multiple IP addresses to spread out the volume of spam to avoid detection).

127.0.0.5 and higher (e.g., 127.0.0.6, 127.0.0.10, etc.)

Meaning: Granular classification of spam-related issues.

Use Case: These codes are used for highly specific listings that detail the nature of the spam activity or other malicious behaviors. For example, a specific return code might indicate that the IP is part of a known botnet, another might indicate that it is associated with high volumes of spam over a short period (snowshoe spam), and another might indicate involvement in sending spam from a dynamically assigned IP address.

2.2.4 How To Check If Your Domain/IP Is Blacklisted?

At Smartlead, we offer a free blacklist checker tool that can help you identify if your domain or IP is blacklisted under any of the email blacklists we covered previously. The tool checks against a wide range of blacklists, including well-known ones such as Spamhaus, SURBL, URIBL, and more.

Steps to Use the Smartlead Blacklist Checker Tool:

- Visit the Smartlead Blacklist Checker Tool Page.
- In the designated field, input the IP address or domain name you wish to check.
- Press the "Lookup" button to initiate the blacklist check.

A sample report has been shared below for an IP that was listed on one of the blacklists and hence failed the check.

Summary

Total Tests: 38 Total Blacklist: 1 Total Tested OK: 37 IP: [redacted]

STATUS	TEST	REASON	RESPONSE TIME
✗ Failed	rbl	127.0.40.2 was listed	285 ms
✓ OK	blackhole	-	12 ms
✓ OK	nordspam	-	8 ms
✓ OK	scientificspam	-	5 ms
✓ OK	tiopan	-	2 ms
✓ OK	rhsbl	-	23 ms
✓ OK	rhsbl	-	23 ms
✓ OK	fmb	-	140 ms

Check Your Spam Score

One of the key aspects to monitor and optimize for better deliverability is your spam score. SpamAssassin, a widely-used spam filtering technology, plays a vital role in assessing the likelihood of your emails being classified as spam.

Understanding SpamAssassin Score

Many renowned email deliverability tools, including GlockApps, Email Acid, and Litmus, rely on SpamAssassin to evaluate email content. This robust filtering system employs over 700 tests, ranging from Bayesian filtering to DNS checks, to determine the probability of an email being spam.

SpamAssassin scores emails as follows:

- Negative values: Indicate that an email is unlikely to be spam, contributing to a lower overall score.
- Neutral: A score of "0" has little impact on the classification.
- Positive values: Suggest a higher likelihood of the email being spam.

To ensure optimal email deliverability, it's essential to regularly monitor and optimize your spam score. Here are some strategies to improve your SpamAssassin score:

- Build a Good Sending History: Maintain a positive reputation by consistently delivering relevant and engaging content to your subscribers. Avoid sudden spikes in email volume, as this may trigger spam filters.
- Use a Reputable IP: Send your emails from a reputable IP address with a clean sending history. Avoid shared IPs or those associated with spammy activity to safeguard your deliverability.
- Authenticate Your Emails: Implement authentication mechanisms like SPF, DKIM, and DMARC to verify the legitimacy of your emails and prevent spoofing.
- Avoid Spammy Words: Refrain from using spam-triggering words or phrases in your email content. Focus on delivering valuable and relevant content that resonates with your audience.

Check Inbox Placement Rate

Check your Inbox Placement Rate (IPR) to gauge the effectiveness of your email campaigns. IPR measures the percentage of emails that successfully reach the main or primary inbox folder. It's a crucial metric that indicates the deliverability and engagement of your emails. The formula for calculating IPR is:

$$\text{IPR} = \frac{\text{Emails Delivered to Inbox}}{\text{Total Emails Delivered}} \times 100$$

Monitoring your IPR helps you understand how well your emails are performing and whether they are landing in recipients' inboxes or getting filtered into spam or other folders.

With Smartlead, you can run a comprehensive email deliverability and inbox placement test, using our email deliverability testing tool. It simulates the delivery of your emails to various email providers and provides detailed reports on inbox placement rates across different platforms. This allows you to identify deliverability issues and optimize your campaigns for better inbox placement.

We will cover more on this in later sections of the ebook.

Secure Email Gateway

A Secure Email Gateway (SEG) is essential for defending against email-based threats. It protects organizations by identifying and blocking malicious emails before they reach users' inboxes. SEGs play a crucial role in preventing common cyberattacks like phishing, which are among the most frequent security threats businesses encounter.

How SEGs Operate

SEGs use a combination of signature-based detection and machine learning to scrutinize email content for potential threats. Here's how they work:

1. Signature Analysis: This method involves looking for known patterns of malware. SEGs compare email content against a database of identified threats, blocking any messages that match these signatures.
2. Machine Learning**:** To tackle more sophisticated attacks, SEGs employ machine learning algorithms that analyze email behavior and patterns. This helps in identifying novel or evolving threats that may not fit traditional signature patterns.

Methods of Integration

SEGs typically integrate with email systems using one of two methods:

1. DNS MX Record: An MX record is a DNS entry that directs email traffic to the correct server. SEGs can insert themselves into this pathway by updating the organization's MX record to point to the SEG.

- This setup routes all incoming email through the SEG for inspection before delivering it to the recipient's inbox. Think of it as a security checkpoint on a highway where every vehicle is checked before entering the city.

2. API Integration: Many email platforms like Google Workspace and Microsoft 365 offer APIs that allow third-party applications to interact with email systems. SEGs can use these APIs to monitor email content after it has arrived in the inbox, without rerouting traffic. This method is akin to having security personnel review vehicles on the road rather than at a checkpoint.

Additional Safeguards Provided by SEGs

1. Phishing Protection: SEGs identify and block phishing attempts that aim to deceive users into revealing sensitive information. They analyze email content, sender reputation, and URL links to detect malicious intent.
2. Spam Filtering: They filter out spam emails, reducing the volume of unwanted messages and preventing potential threats from cluttering the inbox.
3. Malware Detection: SEGs scan attachments and embedded links for malware, ensuring that harmful software does not reach users.
4. Data Loss Prevention (DLP): SEGs can monitor outgoing emails to prevent sensitive data from being leaked outside the organization. They detect and block messages containing confidential information.
5. Advanced Threat Intelligence: By leveraging threat intelligence feeds, SEGs stay updated with the latest threats and adapt their defenses accordingly.
6. Content Filtering: SEGs evaluate email content for inappropriate or harmful material, blocking messages that do not meet the organization's security policies.

2.2.5 IP Signatures Impact On Deliverability

IP signatures, often referred to as email headers, are bits of metadata added to an email's SMTP trail. These include the sender's IP address, the recipient's IP address, and the route the email took to reach its destination. These headers are vital for email

deliverability because they help email servers verify the sender's legitimacy and determine whether an email is spam.

For example, consider an email header that shows:

- Sender's IP address: 192.168.1.1
- Recipient's IP address: 203.0.113.1
- Path: 192.168.1.1 -> 203.0.113.1

This information helps email servers authenticate the sender and ensure the email hasn't been spoofed or tampered with, thus improving the likelihood that legitimate emails land in the recipient's inbox.

How Smartlead Helps

Smartlead, as an email-sending platform, connects to your email outbox, like Outlook or Gmail, to send emails on your behalf. While Smartlead isn't the originator of your emails, it serves as the engine that automates the sending process.

Since Smartlead sends emails to you, there's a digital footprint, especially when using the SMTP protocol. This footprint can influence how your emails are perceived by recipient servers.

Smartlead's email warm-up policy gradually increases the volume of emails sent from your account. This helps establish a positive sending reputation over time, which is crucial for improving email deliverability.

OAuth Process

To use Smartlead, you add your Gmail account as an internal application, enabling an OAuth process. This process is more secure than using Gmail's normal 2FA or secondary application password. OAuth helps prevent disconnects and is related to the SMTP protocol, ensuring secure email sending.

IP Address Rotation

Smartlead rotates IP addresses for each email sent. This rotation helps avoid the negative consequences of an IP address gaining a bad reputation for sending spam. If one IP address gets flagged, rotating to another can prevent emails from being marked as spam or blocked.

Email providers often monitor the volume of emails from a single IP address and flag sudden increases as suspicious. By distributing the sending volume across different IP addresses, Smartlead reduces the risk of being flagged and increases the diversity of IP addresses used, signaling to ESPs that the sender is legitimate.

2.2.6 Avoid Spam Traps

Spam traps are email addresses specifically created by email providers and anti-spam organizations to catch spammers. These addresses are not actively used by real people and are only included in mailing lists through deceptive practices. When an email is sent to a spam trap, it's a clear sign that the sender might be a spammer.

If your email lands in a spam trap, it can negatively impact your email deliverability in several ways:

- **Reduced Inbox Placement:** Email providers might start sending your emails to the spam folder of recipients, even legitimate ones.
- **Reputation Damage:** Sending to spam traps can damage your sender reputation, making it harder for future emails to reach inboxes.
- **Blacklisting:** In severe cases, your email address or domain name might be blacklisted, completely blocking your emails from reaching recipients.

Types of Spam Traps

- **Pristine Spam Traps:** These are pristine email addresses that have never been actively used by real individuals. They are often generic addresses like admin@domain.com or contact@domain.com.

- **Recycled Spam Traps:** These email addresses were once active accounts but have been abandoned and repurposed as spam traps by email providers like Hotmail or Yahoo.

- **Typo Spam Traps:** These traps are designed to catch senders who purchase email lists without verifying them for typos. They contain common typos of legitimate email addresses, such as johndoe@gmial.com or janedoe@yaho.com.

To protect your emails from spam traps, practice regular list cleaning and email verification.

2.2.7 Maintain Sending Frequency

Finding the right balance in email sending frequency is crucial for maintaining engagement and email deliverability. Consistent sending habits demonstrate that you're a reliable sender, not a spammer blasting out random emails, which translates to improved deliverability.

Regular communication keeps your brand top-of-mind with your subscribers. If you disappear for months between emails, they might lose interest and forget who you are. Consistent sending helps maintain a connection with your audience.

There's a sweet spot in sending frequency that maximizes open and click-through rates. Sending too often can lead to fatigue, and sending too infrequently might make your emails get buried.

How to Determine the Right Sending Frequency?

- Start by analyzing historical data on your email campaigns' open and click-through rates. Look for patterns related to sending frequency.
- Research average sending frequencies within your industry. This provides a baseline reference point.

- Different segments of your audience might prefer different email frequencies. Segment your list and consider sending it at varying intervals based on preferences.
- Run A/B tests to compare different sending frequencies and see which resonates best with your audience.

Once you establish a sending frequency that works for your audience, stick to it as much as possible.

2.3 Craft The Winning Email Content

Personalize Your Emails Using Spintax

Spintax is a powerful tool that enables you to effortlessly generate multiple versions of a sentence or phrase by incorporating various options within curly brackets. This feature can significantly streamline your email content creation process, saving you valuable time compared to crafting each variation manually.

By leveraging Spintax, you can create multiple iterations of your email content, enabling you to conduct A/B tests and gauge which variations resonate most effectively with your audience. This invaluable data empowers you to refine and optimize your future email campaigns for enhanced engagement and conversion rates.

In Smartlead, harnessing the power of Spintax is remarkably straightforward. Simply structure your copy using Spintax syntax like this:

{Hi|Hello|Hey|What's up}

This single line generates four distinct emails, each with subtly different copy variations. Not only does this approach boost your email deliverability, but it also provides invaluable insights into which phrasing yields the most favorable results. With Spintax in your toolkit, you can elevate your email marketing strategy to new heights of effectiveness and efficiency.

Ensure a good email copy and CTAs

The success of your email campaigns hinges on your email copy, especially your subject line, main body, and CTAs.

Your subject line is crucial as it's the first impression your email makes. A compelling subject line grabs attention and improves email deliverability by avoiding spam triggers and deceptive language. It entices users to open your email, increasing engagement and response rates.

Craft subject lines that spark curiosity or highlight your email's value proposition. Keep your email content concise and focused on the value you offer, guiding recipients with clear CTAs like "Download Now," "Shop Now," or "Learn More."

Ensure your content is free from spam trigger words to maintain deliverability and engagement.

Here's a non-exhaustive list of some common spam trigger words to avoid (remember, it's always best to consult your email marketing platform for the latest guidance):

- **All Caps:** Writing your email in ALL CAPS is a red flag for spam filters.
- **Exclamation Points!!!:** Excessive use of exclamation points can make your email sound desperate.
- **Urgency and Scarcity:** Phrases like "Limited Time Offer!" or "Act Now!" can trigger spam filters.
- **Free!:** Overusing "Free" can make your email seem like a cheap sales pitch.
- **Guaranteed/Risk-Free:** Guaranteeing results or claiming no risk can raise suspicion.
- **Increase/Boost/Maximize:** These words are often used in spammy, get-rich-quick schemes.
- **Work from Home/Make Money Fast:** Avoid language promoting unrealistic financial gains.
- **Urgency/Scarcity:** Act Now!, Don't Miss Out!, Limited Time Offer!, While Supplies Last!, Once-in-a-Lifetime Opportunity!, Urgent!

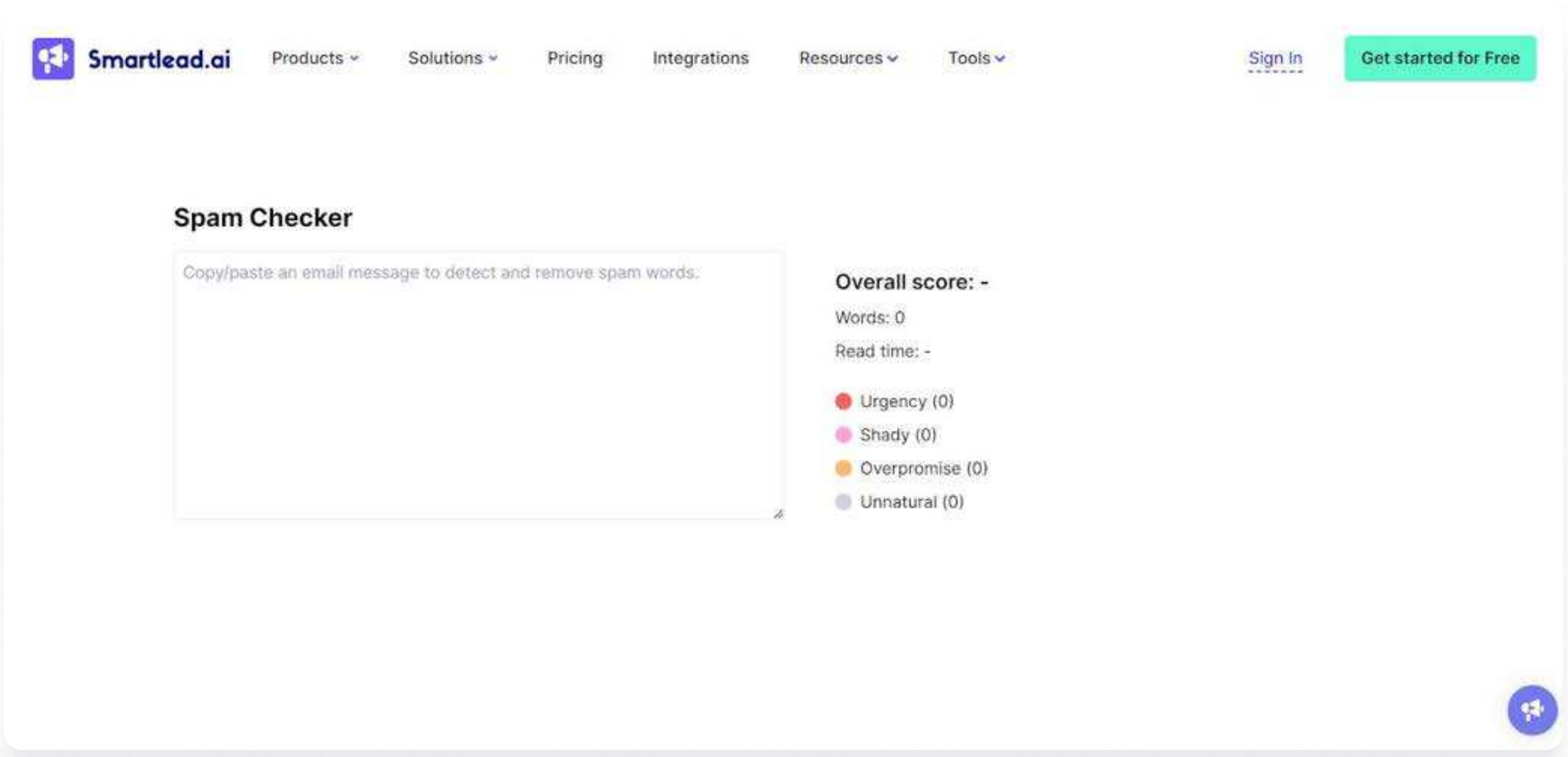
- **Financial Gain:** Earn Extra Cash!, Get Rich Quick!, Double Your Income!, etc.
- **Phishing and Deception:** Urgent! Update Your Account Now!, You Have Been Selected!, Congratulations! You've Won!

Also, avoid misspelled words or phrases. Always run a spell check and double-check the content.

With Smartlead, you can do a spam check for free.

Smartlead's Free Spam Checker is a powerful tool designed to help you avoid common pitfalls that lead to emails being marked as spam. It scans your email content for words and phrases that are known to trigger spam filters, ensuring that your messages don't end up in your recipients' spam folders. By identifying these red flags, the Spam Checker helps you refine your email content to improve deliverability.

With this tool, you can optimize your emails for better performance and higher engagement. By addressing potential issues before sending, you increase the chances of your emails reaching the inbox and capturing the attention of your audience.



Cold Email's Signature - Simple Or Fancy?

While often overlooked, cold email signatures can trigger spam filters if not designed with deliverability in mind.

While some deliverability experts prefer to keep it simple, others think signatures can help build trust and connect better with people. At Smartlead, we prefer to keep it simple.

However, you might want to include various details in your signature, thinking that it makes you seem more credible. It does to a certain extent, but if you are not careful, it can easily trigger spam alerts.

If you want to include a signature in your cold emails, try to keep it simple and straightforward. Avoid fancy-looking signatures with too much extra stuff like a bio or irrelevant social media networks. You should avoid adding your email address to the signature because your recipients have already received it. So, what can you add to your signatures without comprising deliverability? You can add your name and job, company website, embedded images (if absolutely necessary), or any social media links (again, only the truly necessary ones) in plain text.

A better way to go about this is to just A/B test versions of your emails - one with a signature and one without one. Or one with a fancy image or too many colors, and one simple plain text.

2.4 A/B Test Your Email Versions

Imagine sending two slightly different versions of your email to separate groups of subscribers and analyzing which one performs better. This is the essence of A/B testing. It helps you identify what resonates most with your audience, leading to:

Improved Open Rates: By testing different subject lines, preheader text, or "From" names, you can discover what elements entice subscribers to open your emails.

Higher Click-Through Rates: A/B testing variations of your email content, CTAs, or button designs can help you determine what drives click and conversions.

Enhanced Deliverability: Metrics like open and click-through rates signal engagement to ESPs. A/B testing helps you optimize your emails for better engagement, which improves deliverability by demonstrating that your audience's content is relevant and desired.

What to A/B Test in Your Emails:

Here are some common elements you can A/B test in your email marketing campaigns:

Subject Lines: Test different subject line variations to see which ones capture attention and generate the most open.

Preheader Text: The preheader text appears next to the subject line in many inboxes. Test variations to pique curiosity and encourage opens.

"From" Name/Email Address: Experiment with different sender names and email addresses to see what resonates best with your audience.

Email Content: Test variations of your email body content, including CTAs, image placement, or overall design elements.

Send Time: A/B tests different sending times to see when your audience is most receptive to your emails.

3 Measuring Email Deliverability – Tools and Resources

3.1 How To Monitor Email Deliverability

Key Metrics:

- **Delivery Rate:** This shows the percentage of emails successfully delivered to the recipient's server, regardless of inbox placement.
- **Bounce Rate:** Tracks emails that couldn't be delivered due to invalid addresses, full mailboxes, or server issues. Bounce rates are categorized as soft bounces (temporary issues) and hard bounces (permanent issues).
- **Open Rate:** Indicates the percentage of recipients who opened your email. A low open rate suggests deliverability problems or lack of engagement.
- **Click-Through Rate (CTR):** Measures the percentage of recipients who clicked on a link within your email. Similar to open rates, a low CTR can signal deliverability concerns.
- **Spam Complaint Rate:** Tracks the number of recipients who mark your email as spam. High spam complaint rates can significantly hurt your sender reputation.

3.2 Email Deliverability Testing With Smartlead

We know how important email deliverability is for your email campaigns' success - hence our SmartDelivery tool is designed to improve your deliverability rate and thus help you get higher ROI.

SmartDelivery is designed with a singular purpose: to enhance the performance of your email campaigns by ensuring your messages land right where they should – in the

primary inbox of your recipients.

It features key tools aimed at improving your email campaign performance through comprehensive spam testing and monitoring.

Here's how the tool can help you:

- Improved Copywriting: Our tool will help you refine your email content, removing spam trigger words that might otherwise send your emails straight to the spam folder.
- Revenue Generation: By ensuring your emails reach the primary inbox, you'll see increased engagement and, ultimately, more revenue from your campaigns.
- Unified Email Infrastructure: No need for multiple tools – our suite will aggregate your entire email infrastructure in one convenient place.
- Detailed Campaign Overview: Get an in-depth view of your campaign performance and actionable insights on how to improve.
- Immediate Feedback: With IP monitors and blacklist alerts, you'll get real-time feedback on your email health.

Let's dive into the key components of the tool:

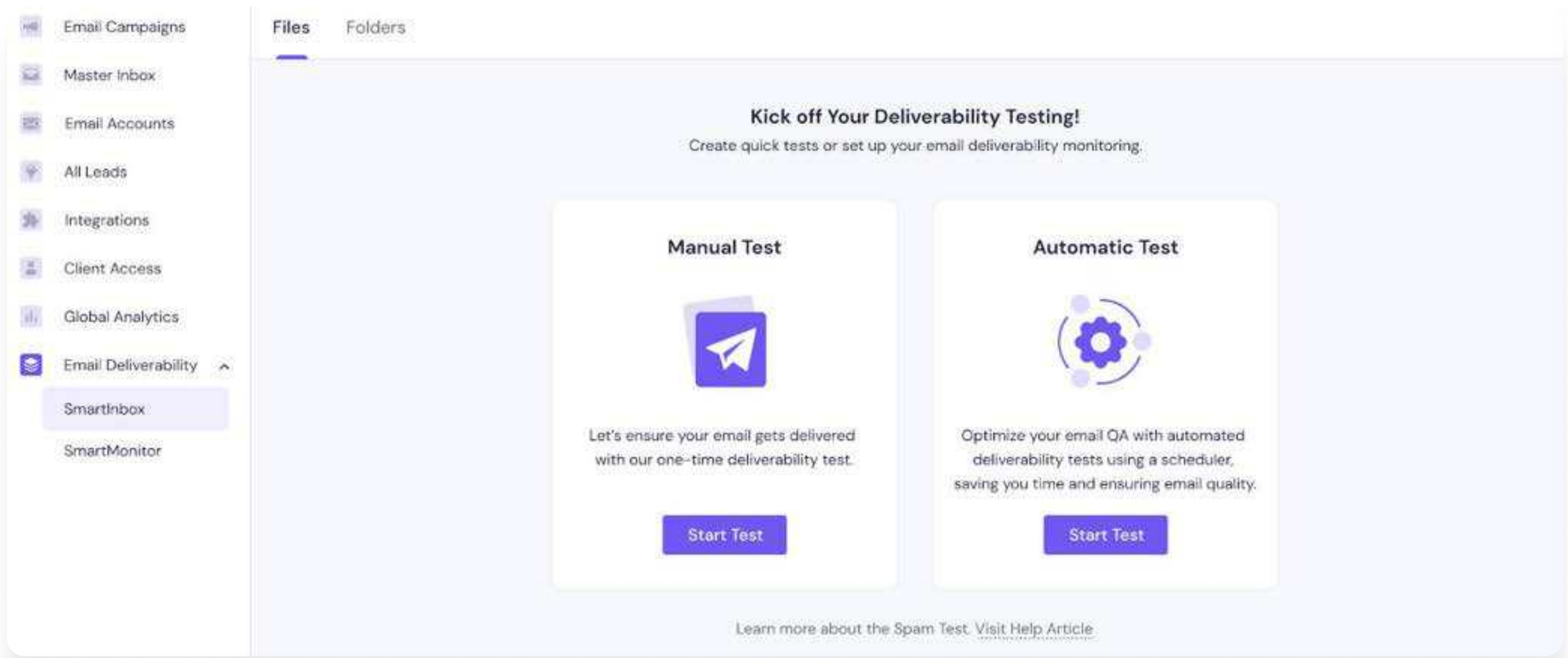
A) SmartInbox

The SmartInbox is a cornerstone of our Email Deliverability Suite. Its goal is to enable you to test and optimize email deliverability across different mailbox providers.

How To Use SmartInbox for Email Deliverability Testing

Initiate the Manual Test

Begin by clicking on the "Manual Test" option from the SmartInbox dashboard. This will lead you to the settings page specifically designed for manual spam testing.



1. Enter General Details

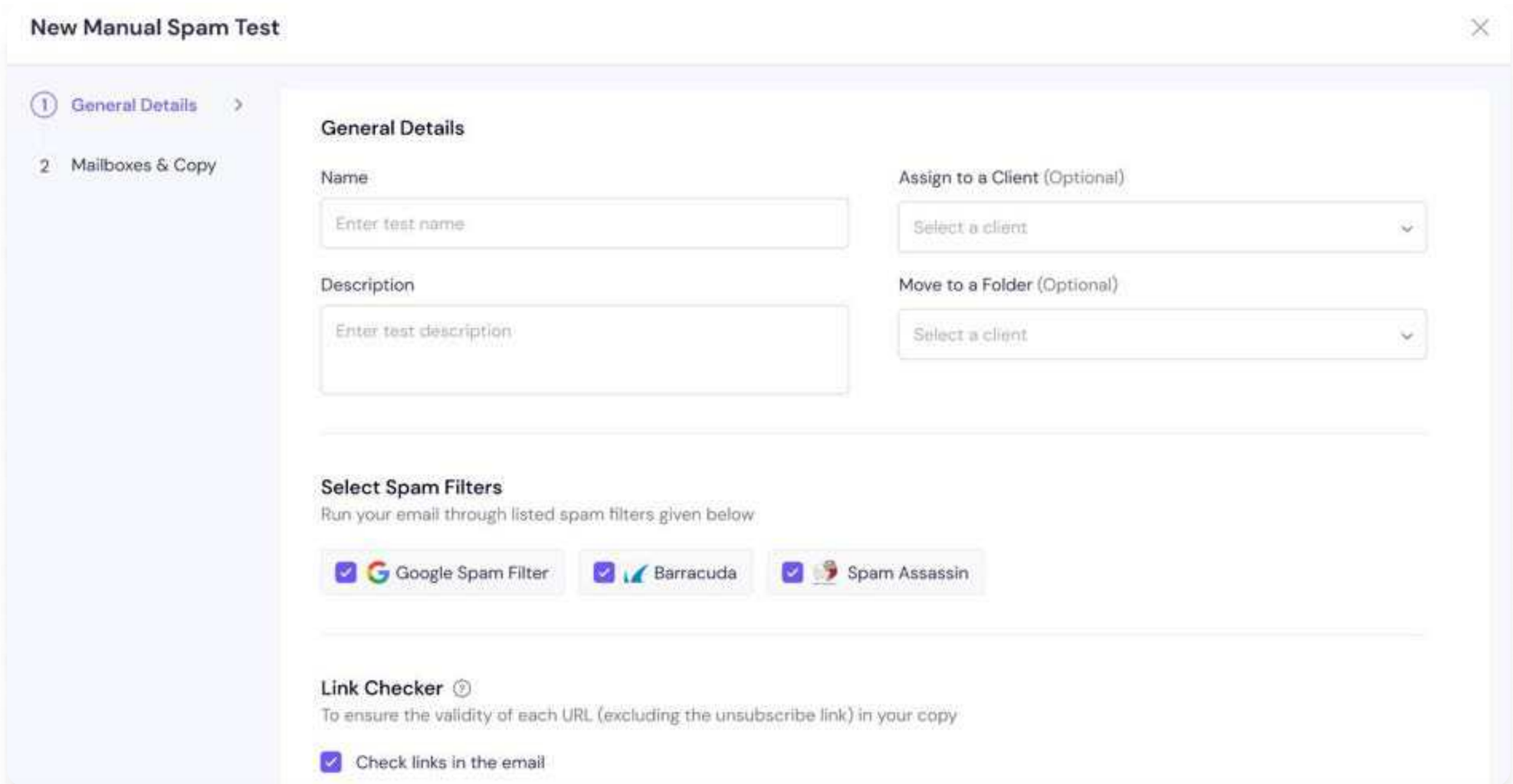
Fill in the essential information for your test:

- Name: Assign a unique name to your test.
- Description: Provide a brief description of the test.
- Folders: Choose the folders where you want the test results to be stored. You can create these folders in advance, ensuring a smooth setup process.

2. Select Spam Filters

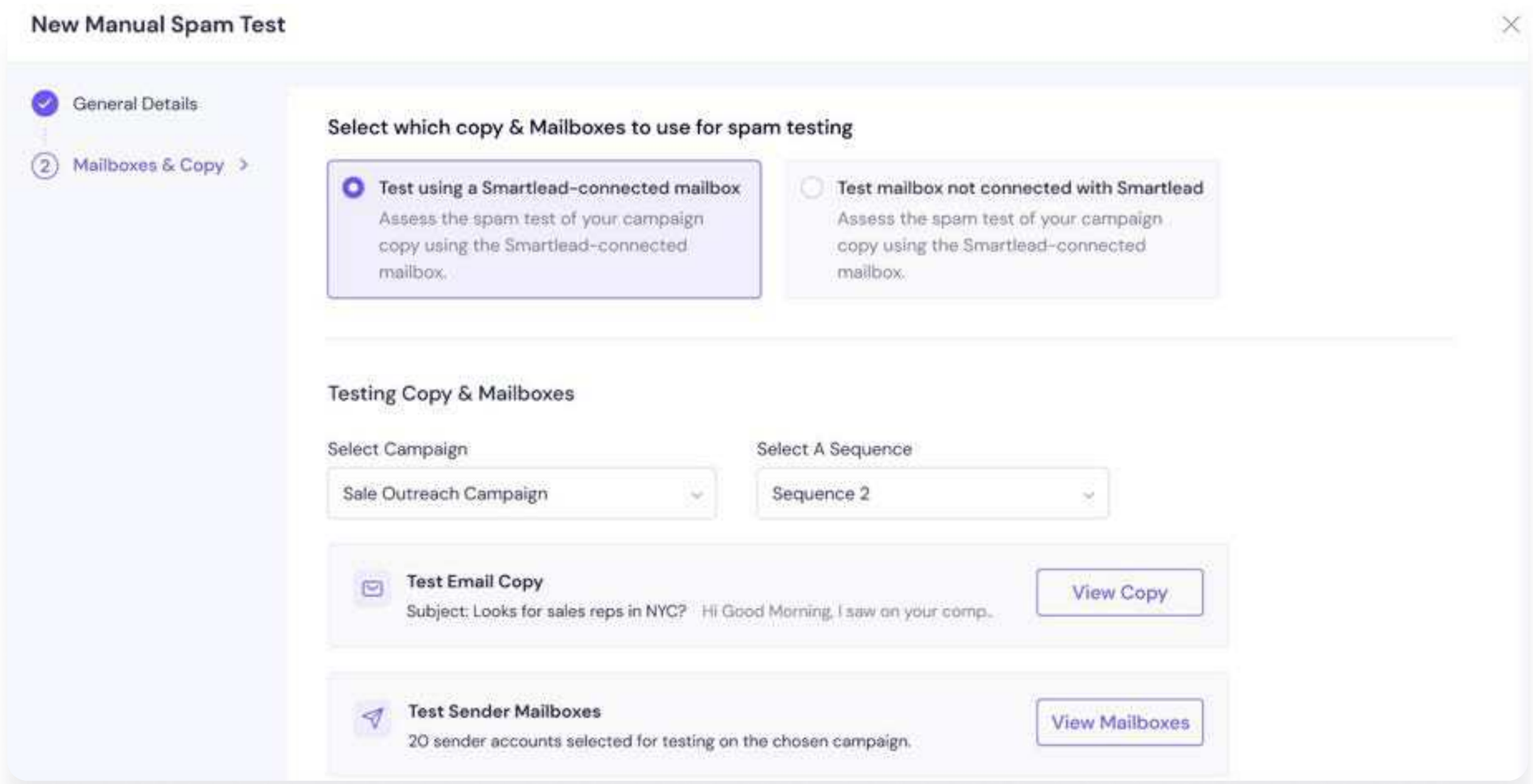
- Next, move to the spam filter settings. Here, you can choose from the following filters:
  - **Google Spam Filter**
  - **Barracuda**
  - **SpamAssassin**

- Additionally, you have the option to enable the **Link Checker,** which will verify the functionality of all links within your email copy.



3. **Configure Mailboxes and Content**

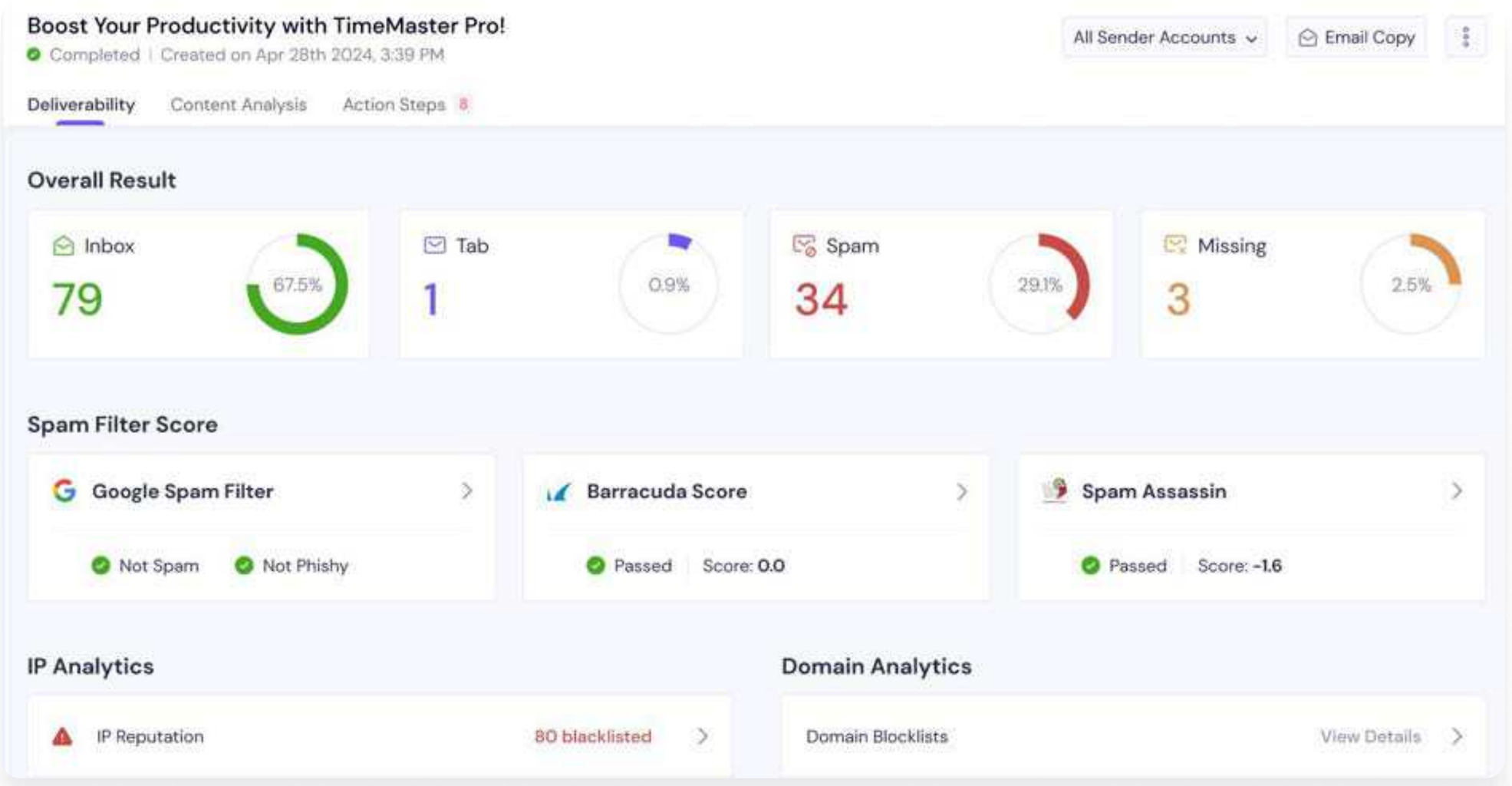
- Now, select the mailboxes and email content for the test:
  - Mailboxes: Choose the specific mailboxes for testing, including those connected with Smartlead.
  - Campaigns and Sequences: Select the campaigns and sequences from which the email content will be tested.
  - Sender Mailboxes and Providers: Pick the sender mailboxes and the mailbox providers (e.g., Gmail, Outlook) against which you want to run the test.
  - Seed List Option: If you need to test mailboxes not connected to Smartlead, you can send your test to a seed list for broader analysis.



4. Run the Test and Analyze Results

After configuring all settings, run the test. Once completed, SmartInbox will provide you with:

- Detailed Deliverability Insights: Understand where your emails land and how different filters treat your messages.

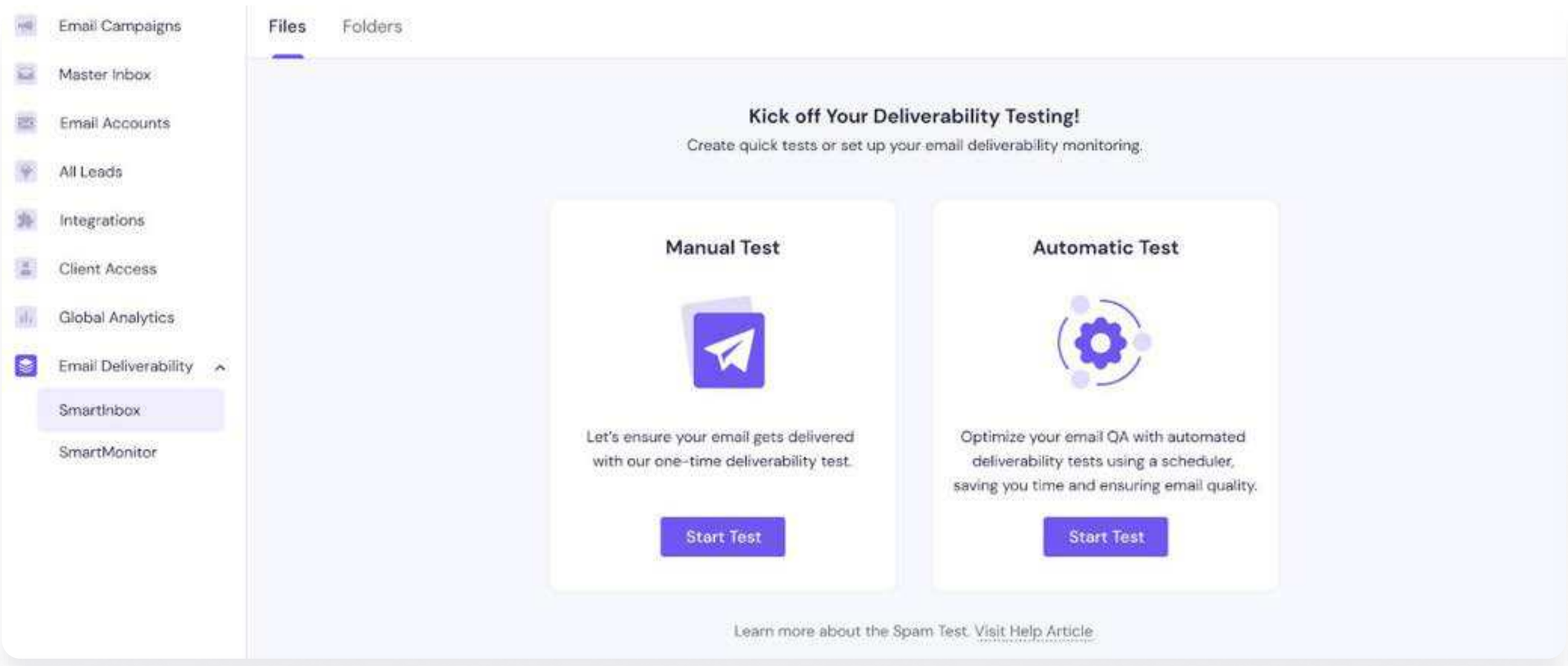


- Content Analysis: Review the email's content, including spam triggers and link functionality.

- Action Steps: Get actionable recommendations to improve your email deliverability based on the test results.

Automatic Spam Testing

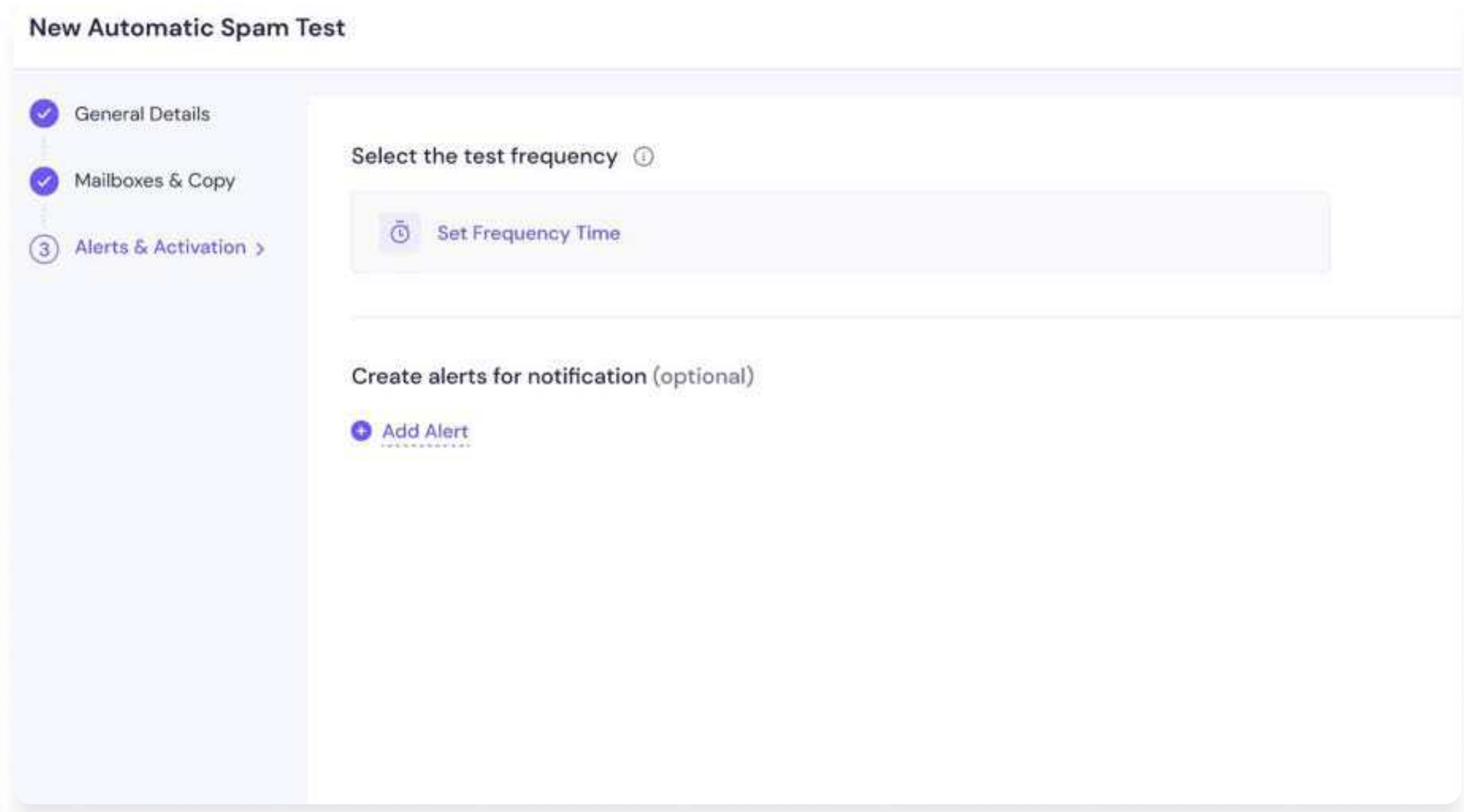
Select the "Automatic Test" option in SmartInbox, which will lead you to the settings page for ongoing, automated spam testing.



1. **Enter General Details**
   - Similar to manual testing, input your test's name, description, and folders for organizing results.

2. **Configure Spam Filters, Mailboxes, and Content**
   - Select spam filters (Google, Barracuda, SpamAssassin), mailboxes, campaigns, and sender mailboxes as done in manual testing. You can also send tests to a seed list if needed.

3. **Set Alerts and Activation**
   - Test Frequency: Choose how often the test should run—daily, weekly, or monthly.
   - Alerts: Set up alerts to notify you when specific conditions are met, such as a drop in deliverability or the detection of spam triggers.
   - Activation: Save and activate the automated testing process, allowing SmartInbox to run the tests continuously based on your defined schedule.

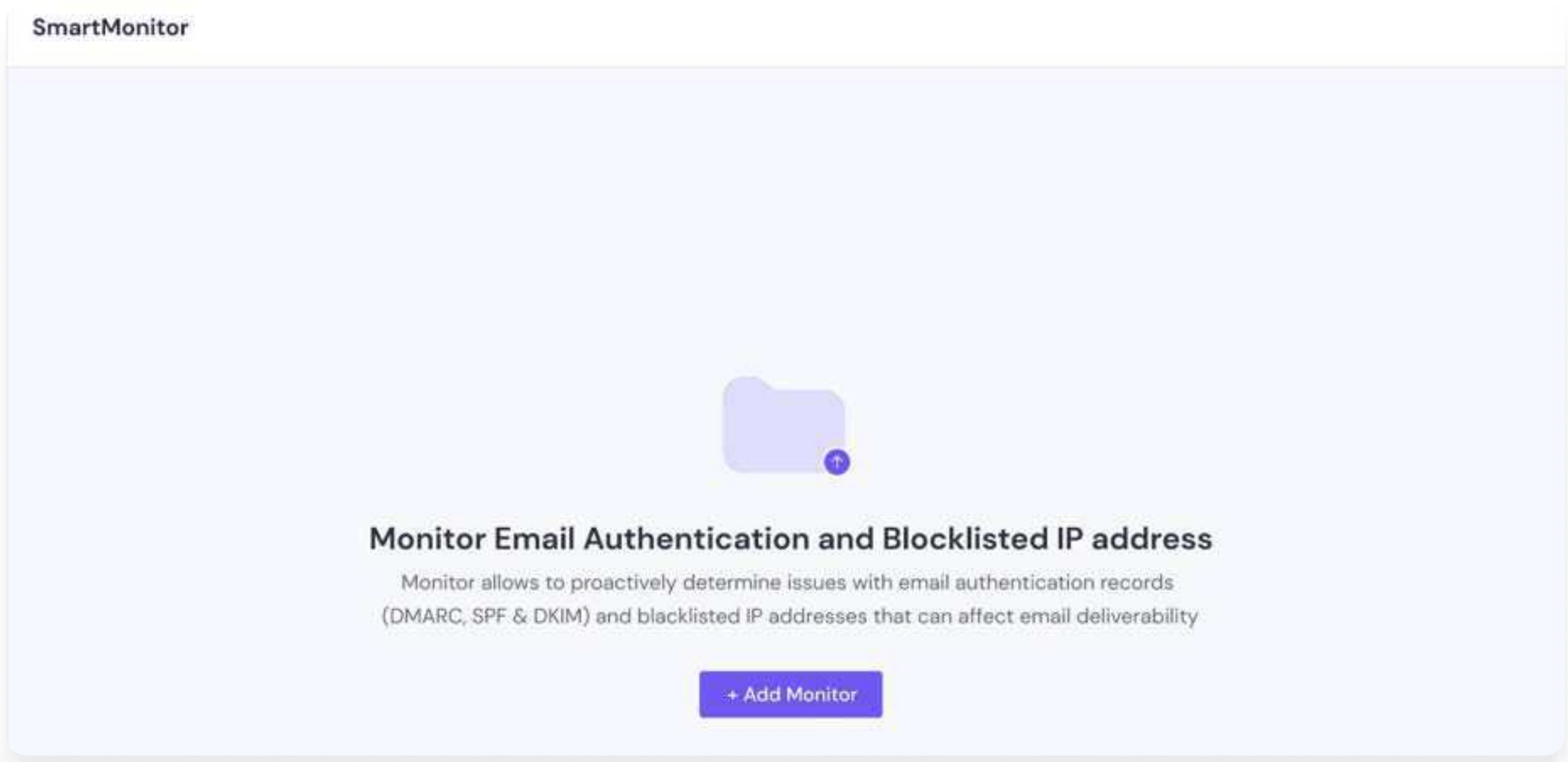


4. Review Results and Take Action

- As with manual testing, SmartInbox provides detailed insights, content analysis, and actionable steps after each automated test.

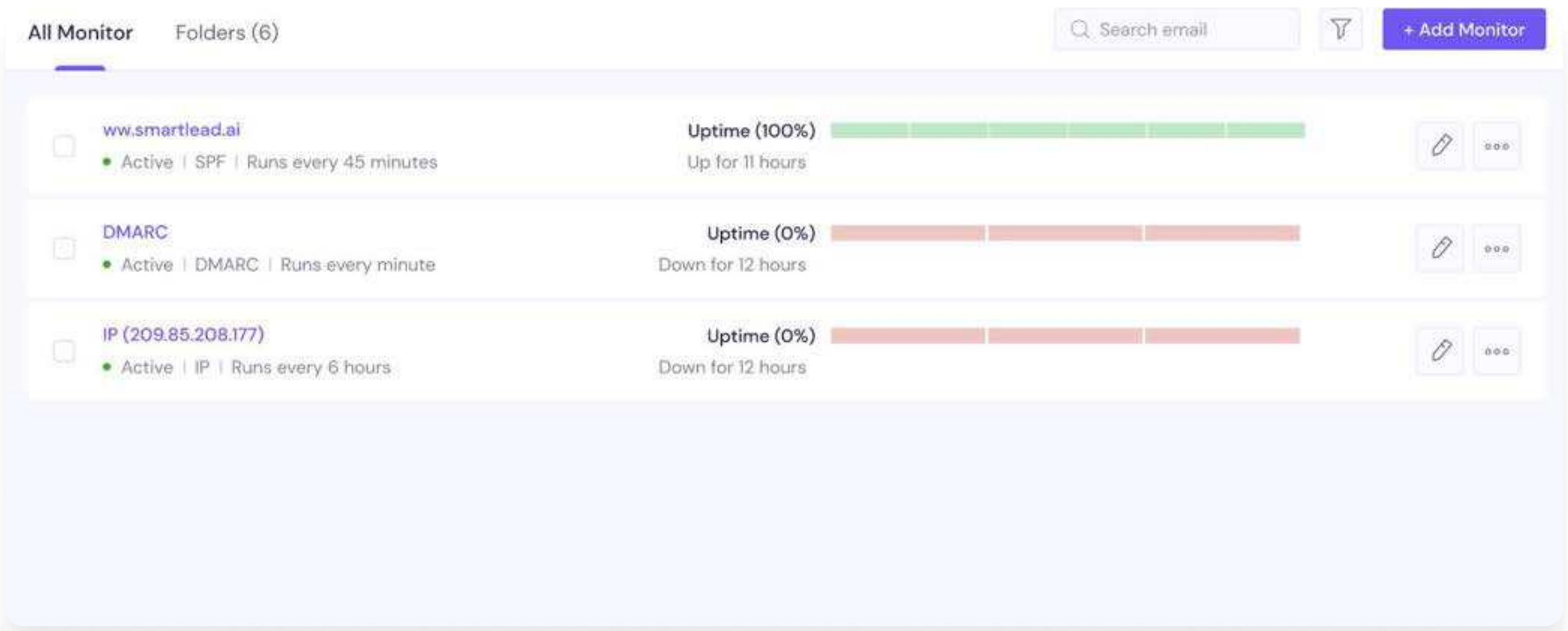
B) SmartMonitor

The SmartMonitor is designed to provide ongoing monitoring of your email health attributes, helping you identify and rectify issues affecting email deliverability preemptively.



Here's what you can expect:

- **Monitor Setup:** Configure new monitors through an intuitive interface, selecting the domains and authentication records you wish to monitor. Advanced options allow for customizing check frequencies and alert thresholds.
- **Monitoring and Alerts:** Our system will perform automated checks at scheduled intervals. If anomalies or issues are detected, you'll receive immediate alerts with suggestions for quick resolution.



- **Review and Reporting:** Users receive detailed reports based on their monitoring settings, with historical data analysis available for trend identification and long-term planning.

With SmartMonitor, you can keep a vigilant eye on your email health, ensuring any potential issues are addressed promptly to maintain high deliverability rates.

***Some features related to Email Deliverability Testing (SmartDelivery) might not be live at the time of publishing this ebook. They're set to roll out in the coming weeks. If you have any specific questions regarding any feature, feel free to reach out to our chat support.*

4 Sending Automated Email Campaigns Using Smartlead For High Deliverability

When it comes to sending bulk emails, you cannot (and should not) depend on Gmail, Outlook, or similar platforms, as they have restrictions on the number of cold emails that can be sent per day. Smartlead is designed to help you send bulk emails without triggering spam filters.

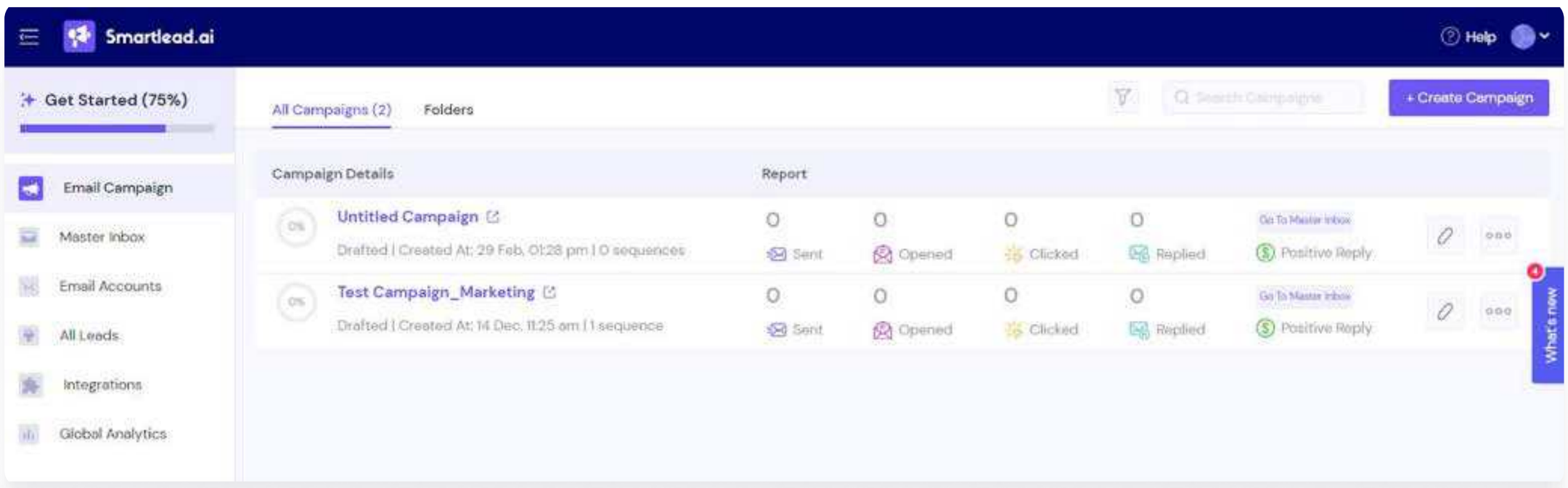
Prerequisites for setting up an email campaign using Smartlead:

- Purchase Secondary Domains
- Add Bulk Email Accounts
- Complete Email Authentication (SPF, DKIM, DMARC, MX)
- Set Up Email Warmup

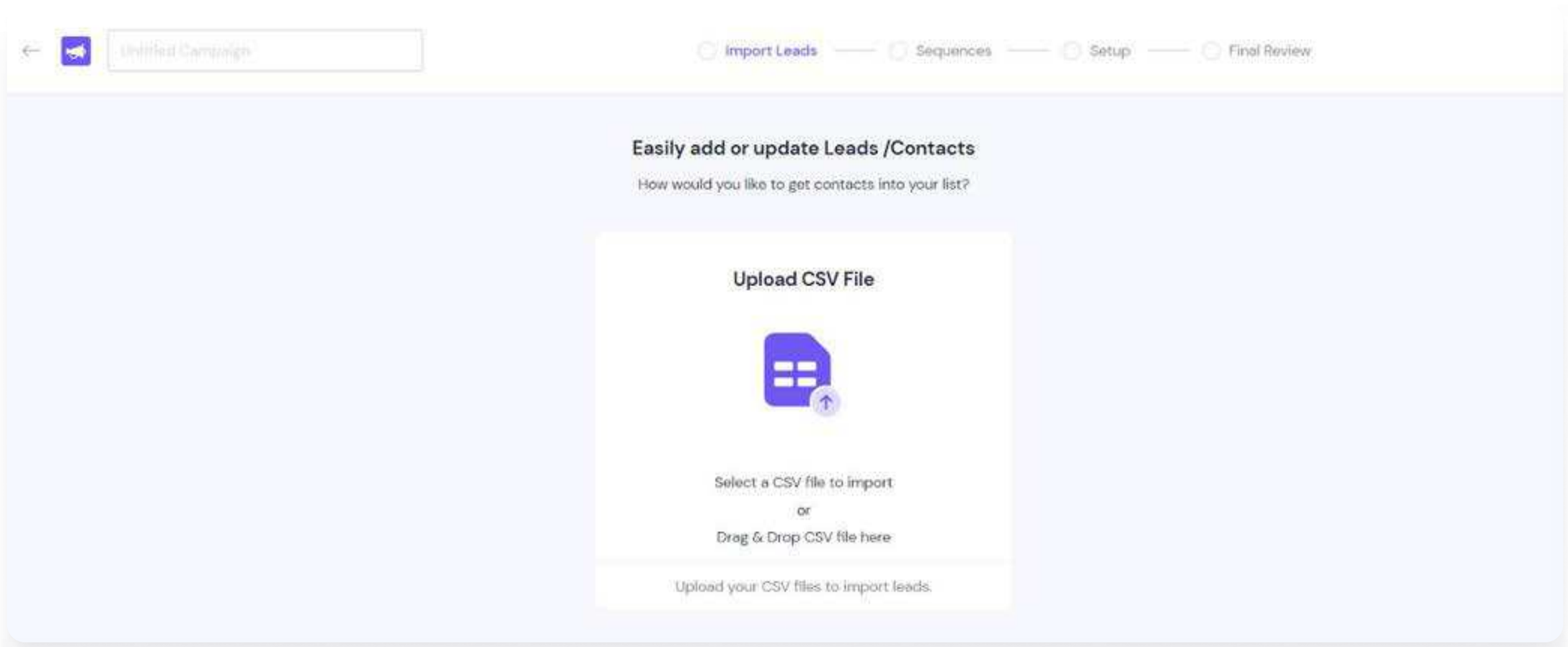
Once you have ensured the above prerequisites, you can proceed with the following steps:

Upload the list on Smartlead

You can now upload the created list to Smartlead. Log in to your Smartlead account, and from the Email Campaign section, go to the ‘Create Campaign’ tab.



You can either upload the lead list as a CSV file or import it directly from your CRM.

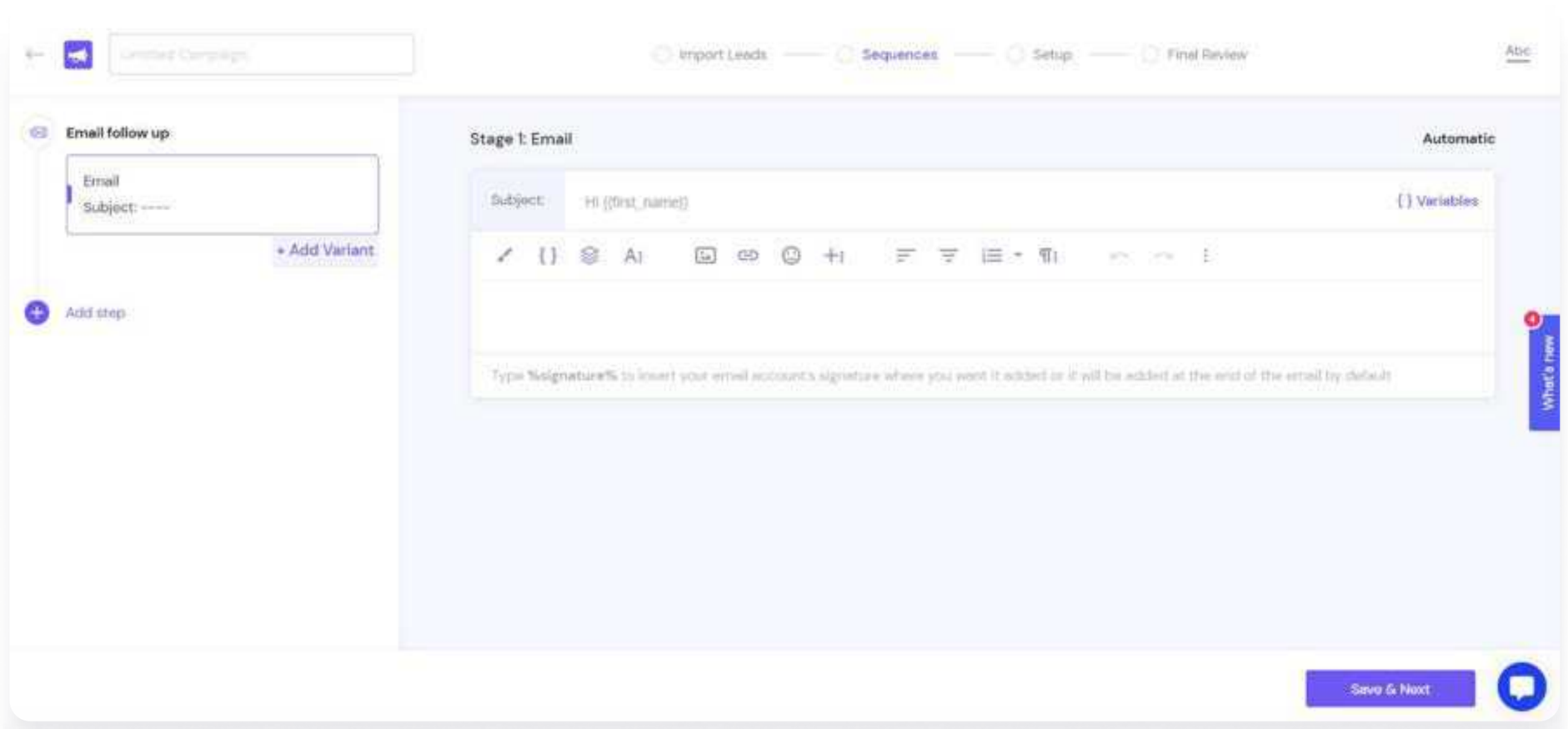


Write the email sequence

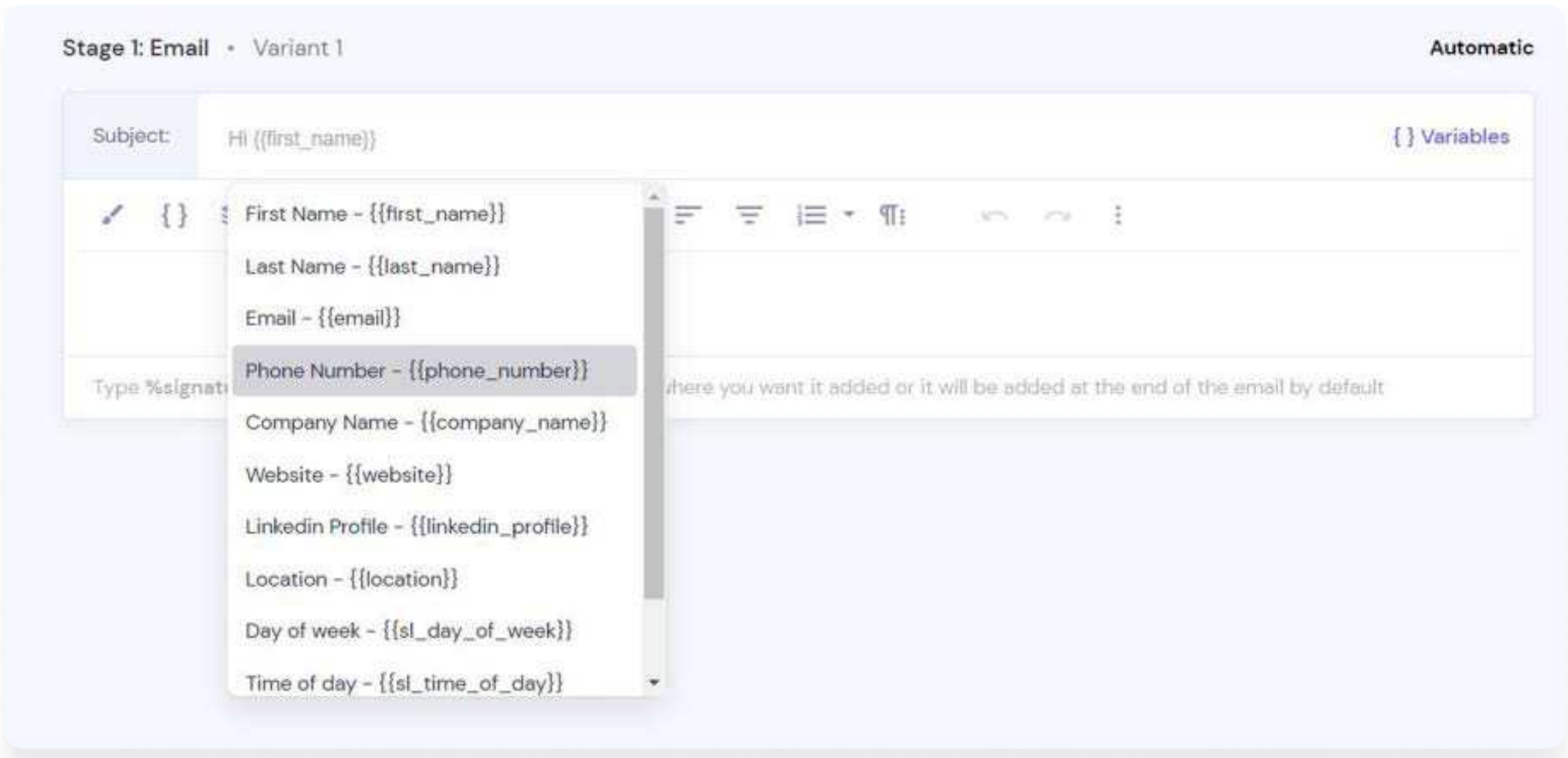
Craft compelling email content and subject lines that resonate with your target audience. If you're a Smartlead's Pro Plan user, you can also utilize the AI copywriter to write compelling email copy for your campaigns right within the platform.

Smartlead also has an in-built spam content checker feature to optimize your email copy and minimize the risk of triggering spam filters.

Leverage Smartlead's integration with Clay to hyper-personalize your emails.



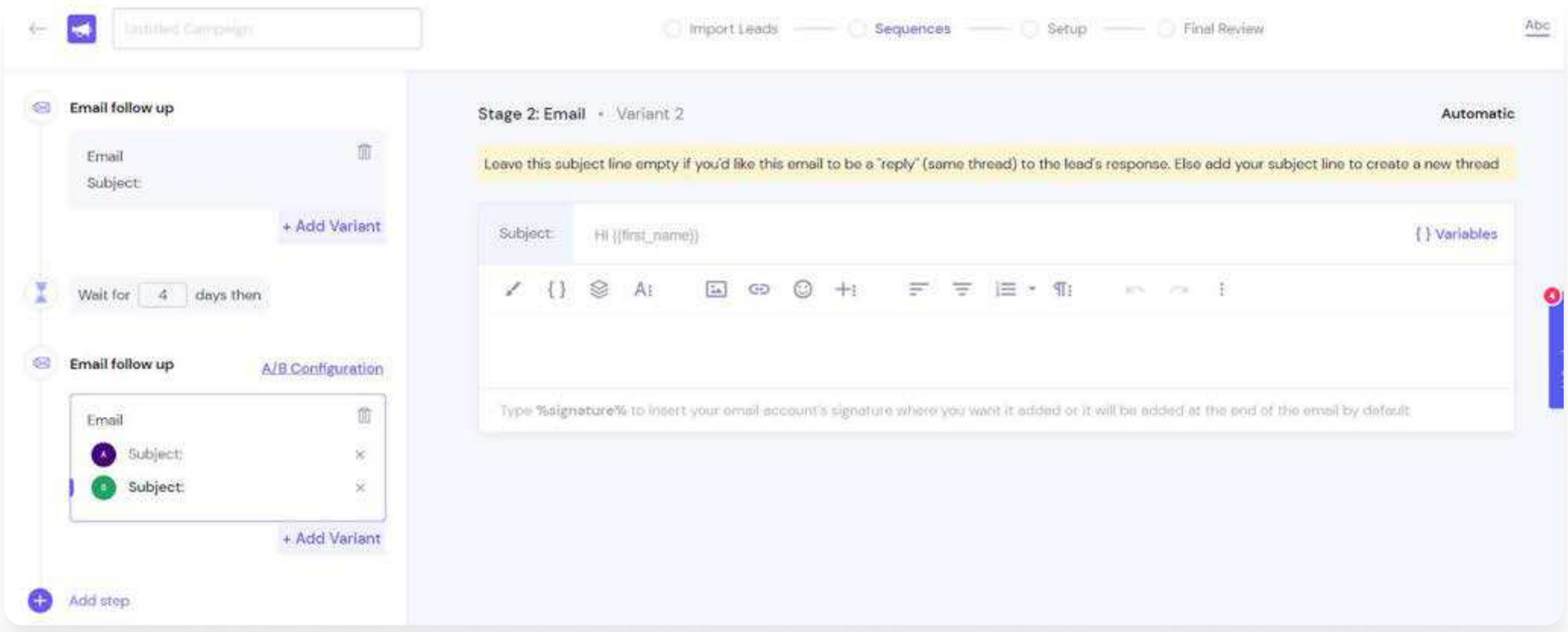
You can personalize your emails and add variables for large-scale personalization.



Set Automated Follow-ups

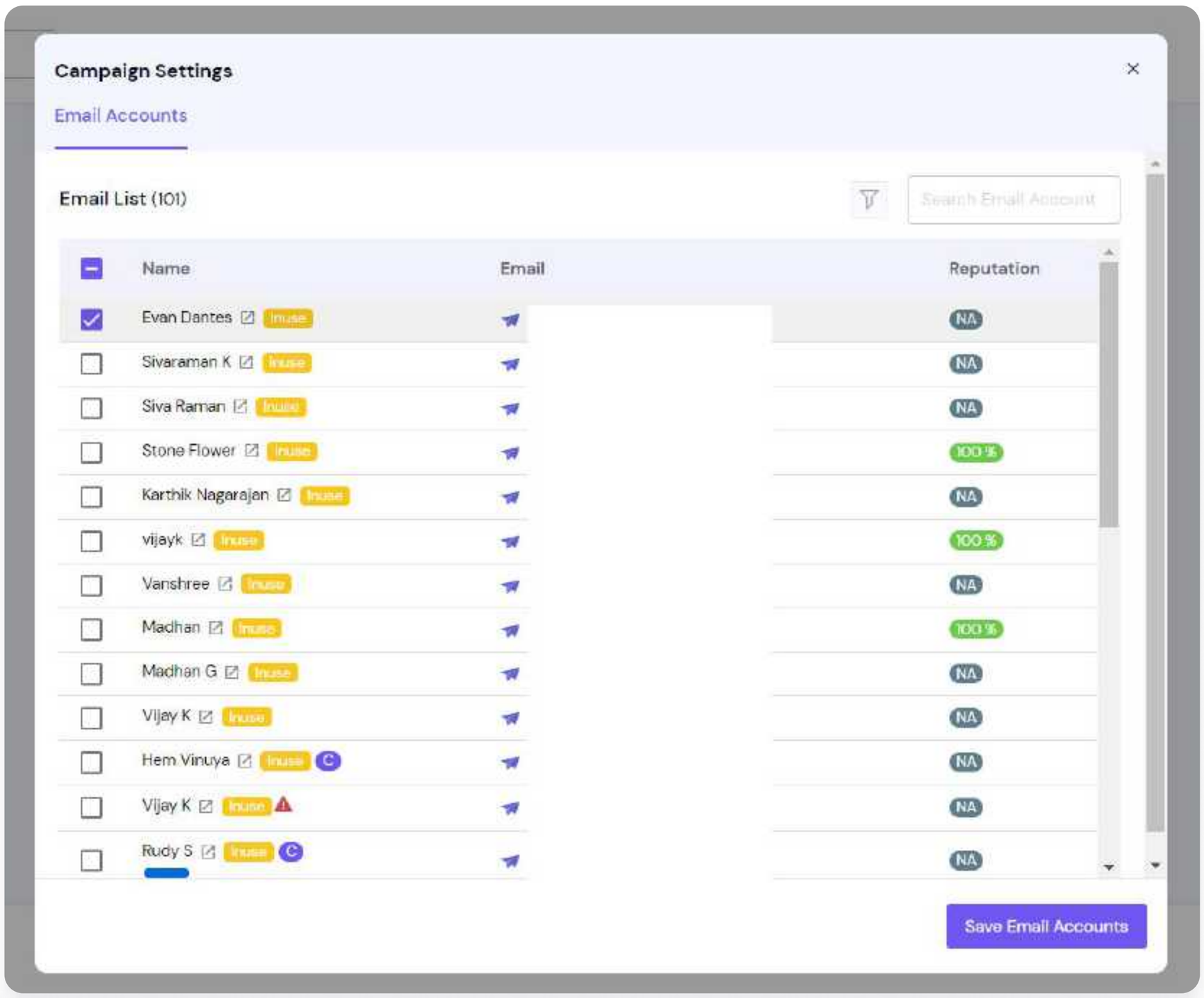
Configure follow-up emails strategically to maximize response rates and engagement. Set appropriate intervals between follow-up emails to avoid overwhelming recipients and maintain a positive rapport.

You can also create multiple variants of your follow-ups (subject line) to see which one performs better in A/B testing.



Choose Sender Accounts

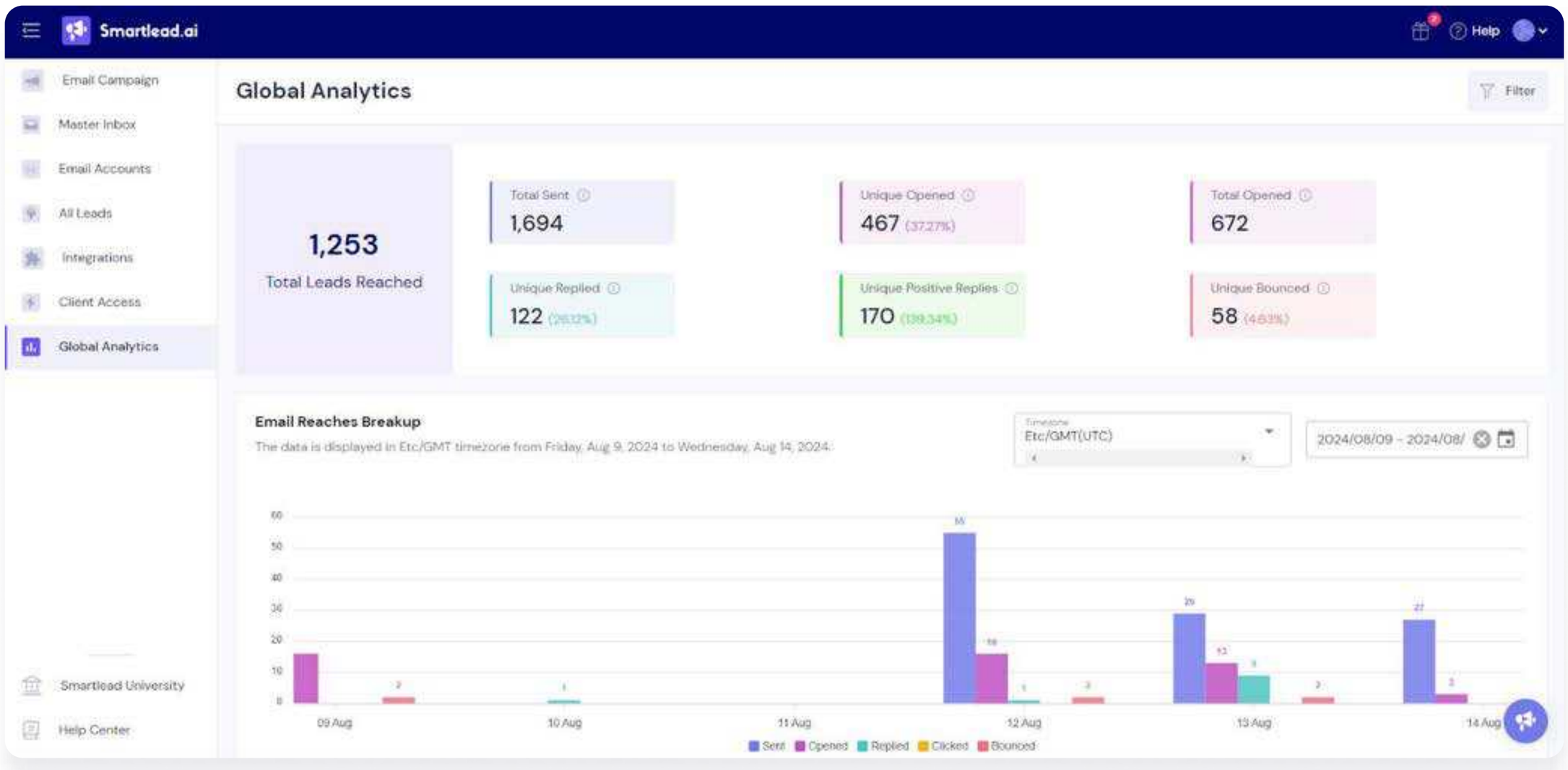
Once everything is set up, you can go ahead and select the email accounts from which you want to send these emails.



Monitor Your Progress - Leverage Master Inbox 3.0

Smartlead lets you monitor your email campaigns in real-time and manage leads using Global Analytics and Master Inbox.

The global analytics in Smartlead lets you have a detailed insight into your key campaign metrics - open rate, replies, positive replies, etc.



Campaign Hygiene Checker

Smartlead's Campaign Hygiene Feature is all about making sure your campaigns run smoothly and effectively. You'll find this feature in the [Performance tab] of each campaign, and it gives you a clear picture of how things are going.

Campaign Progress Overview

First up, we have the Campaign Progress Overview. This is super handy because it lets you see the status of your leads at a glance:

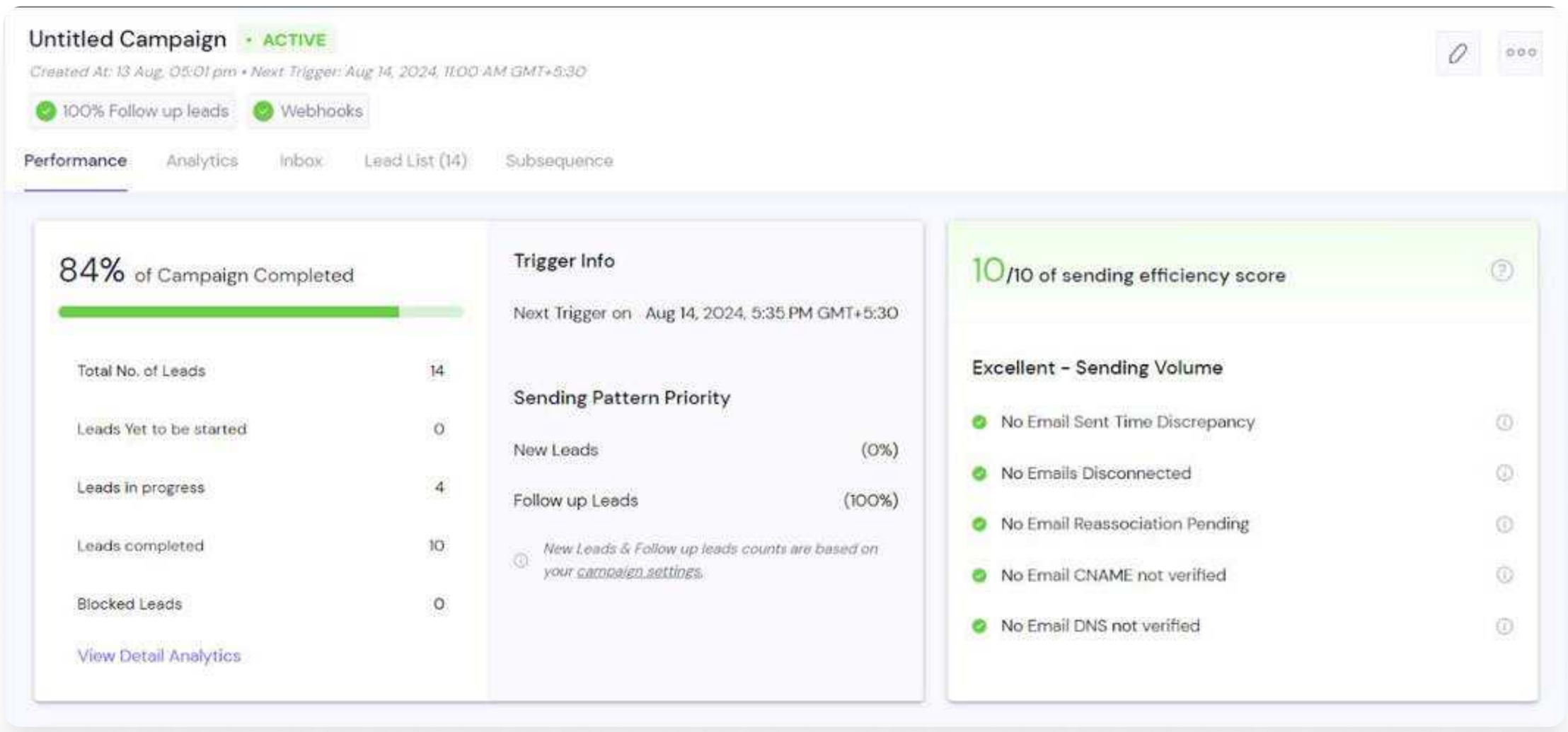
- **Not Started:** Easily spot which leads haven't been engaged yet.
- **Completed:** Keep track of leads that have successfully gone through the campaign.
- **Blocked:** Quickly identify any leads that are facing issues or have been blocked.

Campaign Sending Score

Next, let's talk about the Campaign Sending Score. We know you want to aim for a perfect 10, so we've broken it down into five key areas to help you get there:

- **Sent Time Discrepancy:** Make sure your emails are being sent at the best possible times for engagement.
- **CNAME Not Working:** Check that your CNAME records are set up correctly to keep your domain reputation intact.
- **DNS Validation:** Validate your DNS settings to avoid any delivery hiccups.
- **Disconnected:** Identify and fix any disconnections that might be affecting your campaign.
- **Re-associated Accounts:** Manage any accounts that have been re-associated to ensure everything is running smoothly.

We've designed this feature to make sure your campaigns are delivered seamlessly. If any issues pop up, we'll highlight the affected accounts right away so you can fix the settings without any hassle.

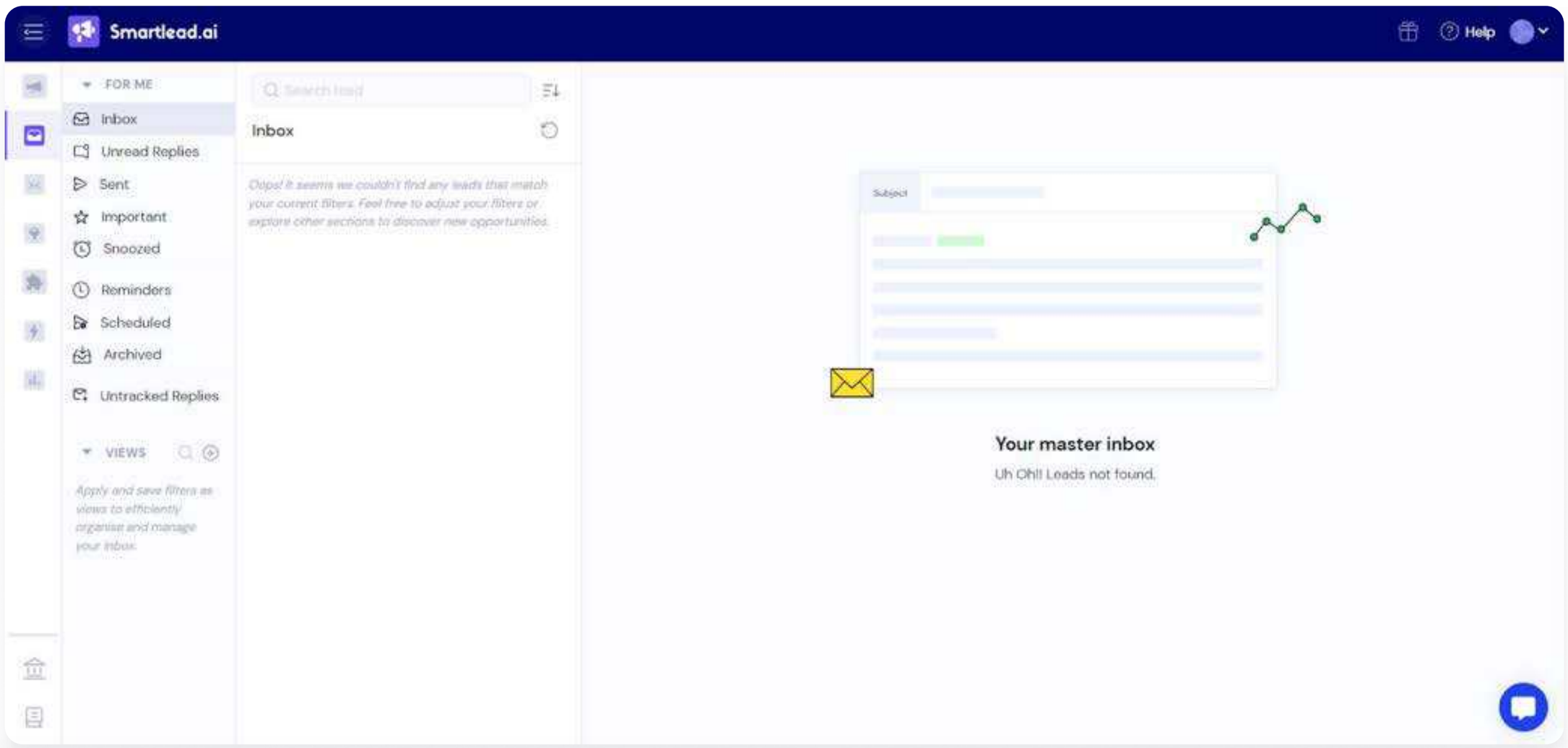


With the Campaign Hygiene Feature, you can keep your campaigns in tip-top shape, making sure they reach your audience effectively and without any problems. It's a game-changer for optimizing your campaign performance and getting the best results. Give it a try and see the difference for yourself!

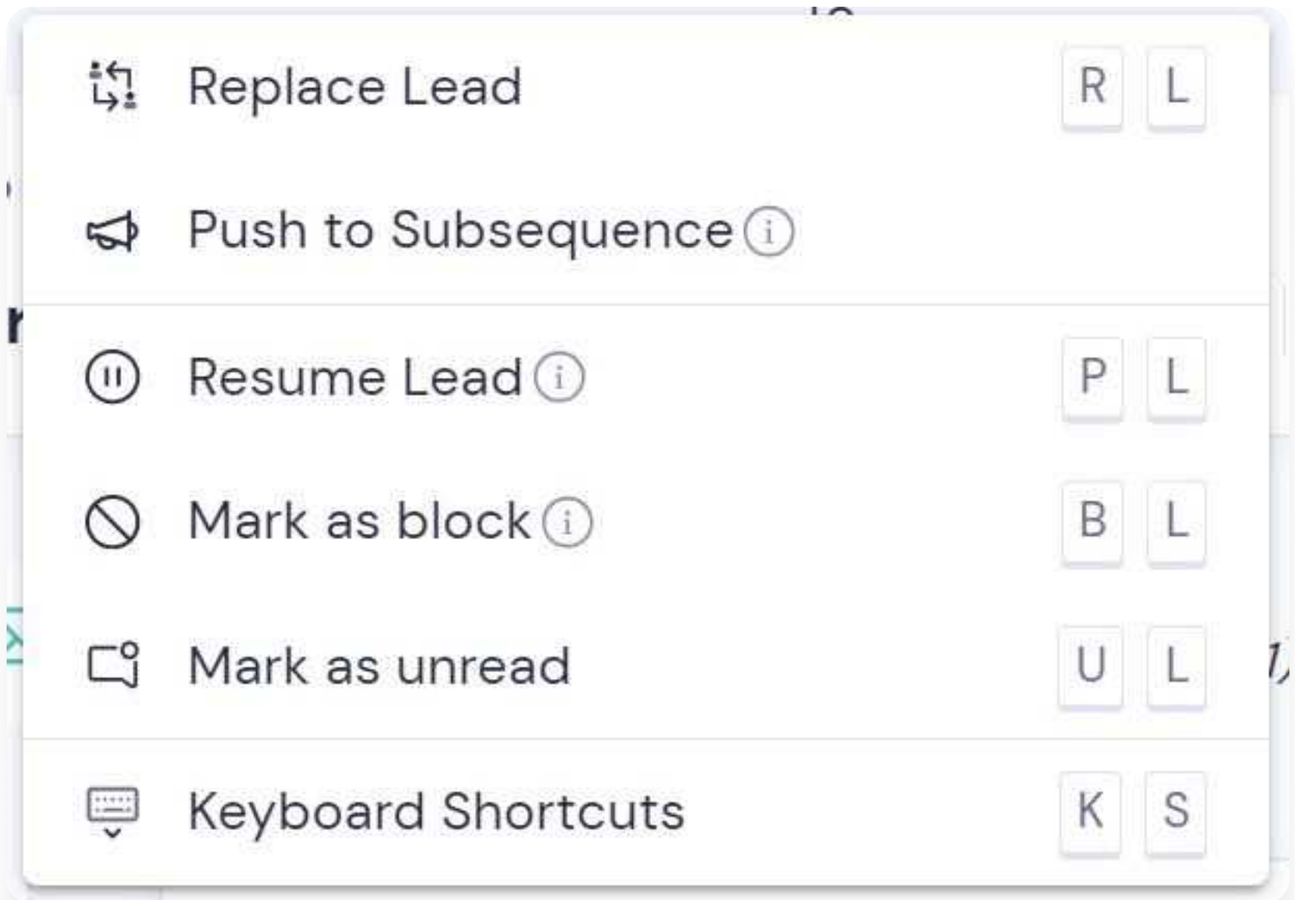
Master Inbox

Similarly, you can also manage and view your campaign leads from within Smartlead with the help of Master Inbox.

This is what your Master Inbox looks like:



Within your Master Inbox, you will find lots of capabilities related to lead management, like below:



You can create and assign lead categories. Smartlead supports AI-based lead categorization, so you don't miss out on any leads. Know more about it here.

Learn more about the master inbox here.

5 Key Takeaways and Next Step

Congratulations on taking the time to explore the intricacies of email deliverability!

You've learned how critical it is for your email marketing success.

To summarize things for you, there should be three primary things you should focus on when it comes to email deliverability:

- Set up your email authentication (SPF, DKIM, DMARC)
- Monitor your sender reputation, blacklist status, and spam score
- Optimize your email content by personalizing and sharing relevant content

Smartlead, as a leader in email deliverability, can help you navigate all these challenges and convert more leads into customers - eventually helping you increase your revenues. With features like AI-powered warmups, automated email account rotation, email spam and deliverability testing, uptime monitoring, and real-time campaign learning, Smartlead streamlines the process and optimizes your outreach efforts.

As the next step, you can simply have a first-hand experience of things we covered in this ebook, by creating a free trial account on Smartlead. See the Smartlead difference yourself!

Remember, exceptional deliverability is an ongoing journey, not a one-time fix.

Appendix

Free Tools

If you're looking for tools that can help you monitor key aspects related to your email campaigns and overall sending infrastructure, here're some free tools from Smartlead to explore:

Blacklist Checker**:** Verify if your domain or IP address is blacklisted across various spam databases.

Spam Complaint Rate Calculator: Calculate the rate of spam complaints received based on email campaigns sent.

DKIM Generator: Generate DKIM (DomainKeys Identified Mail) keys to authenticate your emails and prevent spoofing.

SSL Checker: Check the SSL certificate status and configuration of your domain for secure communication.

DMARC Record Checker: Validate and verify DMARC (Domain-based Message Authentication, Reporting & Conformance) records for email authentication.

SPF Checker: Validate SPF (Sender Policy Framework) records to prevent email spoofing and improve deliverability.

DKIM Checker/Lookup: Verify and check the status of DKIM signatures for email authentication.

CNAME Lookup Tool: Look up CNAME (Canonical Name) records associated with your domain.

Email Verifier: Verify the validity and existence of email addresses to reduce bounce rates and improve deliverability.

Email Verification Calculator: Calculate the potential impact of email verification on campaign effectiveness and ROI.

SPF Generator: Generate SPF records to specify which mail servers are allowed to send emails on behalf of your domain.

Email Bounce Rate Calculator: Calculate the bounce rate of your email campaigns to optimize deliverability.

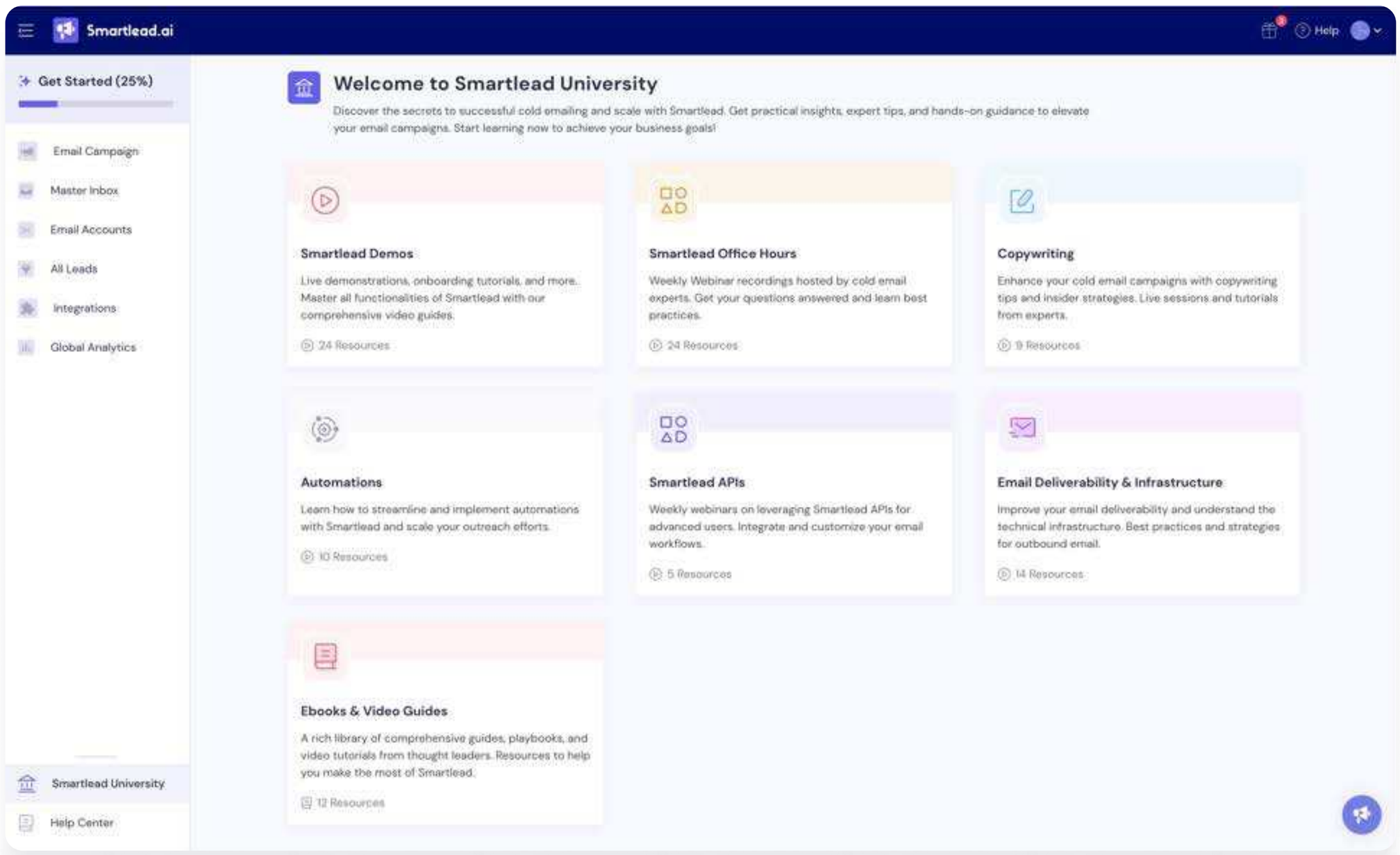
Email Open Rate Calculator: Calculate the percentage of recipients who open your emails to measure campaign engagement.

Click-to-Open Rate Calculator: Calculate the ratio of email recipients who clicked on links to those who opened the email, indicating content relevance and engagement.

Domain Checker: Check the availability and registration details of domains.

Smartlead University - Become a Cold Emailing Expert

Unlock the power of cold emailing with Smartlead. Gain practical insights, expert tips, and step-by-step guidance to elevate your email campaigns. Start learning today and drive your business to success!



To access, simply create an account on Smartlead.

Smartlead.ai

Convert Cold Emails To Consistent Revenue.

Scale your outreach confidently with unlimited mailboxes, unlimited warmups, a limitless multi-channel infrastructure, and a unibox to handle your entire revenue cycle in one place.

www.smartlead.ai