SocketLabs
the science of hitting the inbox

SocketLabs Best Practices Guidelines for Authentication

Table of Contents

I. Introduction

Due to a steady global increase in malicious email tactics like phishing, spoofing, and forgery, mailbox providers must be very careful about which messages they allow to be delivered. That's why it is incredibly important for every legitimate email sender to follow the best practices to make their messages clearly identifiable as trustworthy in the eyes of mailbox providers.

One of the critical foundational steps when using an email service like SocketLabs is establishing aligned and white-labeled message authentication mechanisms. These measures help demonstrate that your messages are authentic and help facilitate strong inbox placement. Over time, your organization will see improved email performance as you build a trusted sender reputation that further increases the consistency with which your messages are accepted and delivered to the recipient's inbox.
The purpose of this document is to help educate SocketLabs customers about the topic of email authentication and to help explain the important configuration options that you should choose to maximize success. The goal is to help you choose the best path to garner trust, build domain reputation, and help optimize message delivery results.

This document is based off of established industry best practices from M3AAWG – the Messaging, Mobile, Malware Anti-Abuse Working Group. As a member of M3AAWG, SocketLabs is proud to contribute to these documents. For those looking for best practices regarding more wholistic email domain and authentication practices, please see the following documents:

- M3AAWG Sending Domains Best Common Practices
- M3AAWG Email Authentication Recommended Best Practices

II. Authentication at SocketLabs: An Overview

SocketLabs provides a strong, multi-faceted approach to promote the authentication of your email streams. As a standard feature of our platform we provide an initial layer of message authentication that protects every message we send. These “out-of-the-box” settings help validate your messages and allow most customers to enjoy strong deliverability results. However, this success is largely based on the strength of SocketLabs’ reputation. That is because from the viewpoint of mailbox providers that receive your messages, it appears (correctly) that SocketLabs’ domain is sending the messages on your behalf. The more desirable alternative is for you to customize your account settings so that the messages appear to be originating directly from your own domain(s). With these customizations you can start building your own sending reputation and lay the groundwork for greater control of your email programs.

SocketLabs’ customization process has several components which are described below. By implementing all of them, you can maximize your control over your sending environment and ensure every message you send is appropriately identified as yours. Specifically, the outgoing mail will appear to originate from your domain, and you can start growing and maintaining your reputation independent of SocketLabs.

A key concept in the customization process is white-labeling. White-labeling your email is a process that masks the fact that you are using the SocketLabs platform and related domains to deliver your email. Instead, through the process of white-labeling, outbound messages that originate from SocketLabs will reference your domain.

The process of white-labeling allows you to achieve “aligned” authentication in the eyes of the mailbox providers. Specifically, this means that the domain providing authentication is clearly associated with the From address. As explained below, DMARC policies (which are becoming an industry standard authentication practice) require senders to have SPF or DKIM authentication that is aligned.

There are five different settings within a SocketLabs account that customers can customize. These settings are:

- Sending Domain(s)
- Custom Bounce Domains (SPF)
- DKIM Signatures
- DMARC Policies
- Engagement Tracking

III. Understanding Settings and Customization

In this section, we explain each of the key authentication features and explain why they are important for your organization to customize and manage. We also explain the native protections offered with your SocketLabs account and how the process of customization provides your organization with better long-term control. In section IV, we provide instructions on how to customize and modify each of these settings.

A. Sending Domain(s)

The first key step towards advancing your authentication stance is choosing your sending domain(s). This process consists of defining one or more specific email addresses or domains that are permitted in the From address field of your messages. In order for messages to be accepted and processed by SocketLabs, the domains or addresses must be listed is the sending domains list.

All new SocketLabs accounts have the domain of the email address provided at account creation automatically added as the first entry in their Sending Domain list. Messages using any other domain in the From address field will not be accepted for processing, if not added to the Sending Domain list in advance.

SocketLabs customers on enterprise tier service plans may request the Sending Domain list be disabled for their account. This will allow for messages to process through the account using any address or domain in the From address field.

B. Custom Bounce Domain

The bounce address, also known as the return path address, is an email address specified during the SMTP protocol communication process that determines where the receiving mail server sends back its bounced messages.

There is a wide range of terminology used in place of the term "return path" and some of the alternate terms include: reverse path, envelope from, envelope sender, MAIL FROM, 5321-FROM, return address, From_, Errors-to, and sometimes VERP. This value should never be seen by the end recipient, but the aliases cause common confusion between the return path and the traditional From address field.

To allow SocketLabs to capture and analyze bounces on your behalf we use a custom return path address for each and every outbound message you send through our network. This means that we encode unique data about each outbound message into an address and use it in the MAIL FROM SMTP protocol command. In these cases, when a message is received back to our custom return path address we are able to decode the specific message details from the address. This process is known as using a Variable Envelope Return Path

(VERP). Provided below is an example of what a VERP address may look like for a message sent by SocketLabs:

MAIL FROM: <123ab.19.local=example.COM@email-od.com>

The use of a VERP address is an industry standard practice and is acknowledged as a best practice by M3AAWG, as well as by mailbox providers like Gmail, Outlook/Hotmail, and Yahoo/AOL. SocketLabs' use of its own controlled address in the return path also allows us to control Sender Policy Framework (SPF) authentication.

SPF is a mechanism that allows domain owners to publish and maintain, via a standard DNS TXT record, a list of systems authorized to send email on their behalf. The domain used in this check is the domain of the bounce address.

Prior to any customization, the VERP addresses generated for messages will use the domain @email-od.com. This means that by default the SPF record of email-od.com will be used in the authentication process. The SPF record of email-od.com properly authenticates all SocketLabs managed IP addresses. Therefore, all messages will pass SPF authentication when sent by SocketLabs. However, as described later, this is not "aligned" SPF.

Creating a custom bounce domain is the process of replacing email-od.com in the VERP address with your own (sub)domain. SocketLabs recommends setting up a Custom Bounce Domain for every configured Sending Domain, or any domain that will be used in the From address field of messages sent by the account.

The SocketLabs system will automatically apply the proper bounce domain to match the domain in the From address field. If no matching bounce domain is configured, SocketLabs will apply the domain chosen as the default domain. This process allows the SPF authentication checks to achieve proper alignment. Receiving mailboxes look for this alignment as a strong signal that the message is legitimate, and the sender is in control of the system sending the message.

Since SocketLabs helps customers achieve aligned SPF authentication via the use of a bounce domain, we are frequently asked if there is any need to edit the organizational domain's SPF record. Theoretically, the organizational domain's SPF record will never be checked. However, there are some extremely rare circumstances in which this record might impact deliverability. So we label the addition of this record as optional.

Section IV below offers instructions on how to customize your Custom Bounce Domain.

C. DKIM Signatures

The next step in the customization process is establishing a digital signature. Signatures address a critical email threat by ensuring that messages have not been modified during transit. Digital signatures also verifiably associate a message with a domain. This association between message and domain is critical for building domain reputation.

DomainKeys Identified Mail (DKIM) is the name of the industry-standard signature process that is used for signing email. The DKIM process uses a public key/private key system to create a signature for each message. The signature is generated and applied to outbound email during the sending process. Mailbox providers then try to verify the signature on each message upon receipt. If the signature is verified, the receiver has proof that the message was not altered as it traveled the delivery path and can associate the message with the domain that is used to sign the message.

SocketLabs signs all outbound messages with our own DKIM signature, using our own domain of email-od.com. Mailbox providers can evaluate this native DKIM signature to confirm the message integrity. The strong trust that SocketLabs has built using this domain allows customers to achieve great deliverability and performance. This automatic DKIM signature cannot be removed from messages.

While the default SocketLabs signature cannot be removed, we do support dual DKIM signing messages. This means that you can add a second signature to your messages. When two DKIM signatures are present on a message the reputational impact of unaligned signatures are diminished, as mailbox providers will more strongly associate domain reputation when a DKIM signature matches the From address domain. This matching signature would be the aligned DKIM signature. Referring back to the concept of alignment, the native DKIM signature provided by SocketLabs is not aligned (and can never be aligned) because the From address domain and the domain used for the SocketLabs DKIM signature are different.

By creating and applying an aligned DKIM signature for each of your sending domains, you can significantly improve the trust of your messages in the eyes of the mailbox providers. SocketLabs recommends setting up Advanced DKIM signing for every configured Sending Domain, or any domain that will be used in the From address field of messages sent by the account.

The SocketLabs system will automatically apply the proper DKIM signature to match the domain in the From address field. If no DKIM keys are configured for the domain in the From address field, SocketLabs will only apply the default signature. For those looking to build email infrastructure to operate ESP-like services, please contact the SocketLabs Enterprise Sales and Services team to learn more about opportunities to customize the default DKIM signing process.

Section IV below offers instructions on how to configure a DKIM signature.

D. DMARC

Domain-based Message Authentication, Reporting & Conformance, or DMARC, is a DNS policy that allows a domain owner to declare that their email messages will use aligned authentication. Also, it allows for the domain owner to instruct receiving systems how to deal with messages that do not meet the aligned authentication requirements. Finally, it allows domain owners to publish an email address for which they will receive reports regarding the authentication status of messages received by mailbox providers. If you are not familiar with DMARC and how to create and publish a DMARC policy in your DNS records, then we recommend checking out our whitepaper Understanding DMARC: Your Guide to Powerful Email Authentication.

DMARC can be an extremely useful resource to prevent direct domain spoofing, and receive aggregated reports about the authentication status of messages. Implementation is an organizational decision though, as any published DMARC policy will impact all mail sent on behalf of a domain, including mail a domain may send outside of the SocketLabs service. Before publishing a DMARC policy, domain owners should consider their particular risk profile regarding spoofing and phishing of their domain. For domains with low spoofing risks, or extremely complex organizational structures, DMARC may not make sense to implement from a value and cost perspective. With that being said, SocketLabs recommends setting up a DMARC policy for every configured Sending Domain, or any domain that will be used in the From address field of messages sent by the account. The policy should be as restrictive as can be reasonably achieved by the domain owner.

All SocketLabs customers are able to send mail with properly aligned DKIM and SPF authentication, making it possible to use our service with a domain that has a Reject or Quarantine DMARC policy. By establishing your sending domain and customizing the bounce domain and DKIM signature, your mail will be in the best for successfully reaching the inbox.

E. Engagement Tracking

The Engagement Tracking feature allows you to detect how your email recipients are interacting with messages sent to them; specifically, if they are opening the message, clicking on links within the message, or if the recipient has requested to be unsubscribed from the messages they are receiving.

Although engagement is not a mechanism of email authentication, it is something that needs to be white-labeled and can impact email deliverability. Since tracking click events requires rewriting the destination link within a message, it is ideal to have this domain align with the From address field and be consistent across all of the links in the message.

Using your own domain in the links within your messages is important because the domain is scrutinized from a reputation perspective. Just as with white-labeling authentication features, the reputation of links can be insulated from the reputation of others by using your own aligned domain.

Tracking engagement is valuable as it is one of the primary performance metrics and correlates closely to inbox placement performance. Since inbox placement rates cannot be accurately tracked, open rate is one of the next best metrics to use in monitoring performance.

SocketLabs recommends setting up an Engagement Tracking hostname for every configured Sending Domain, or any domain that will be used in the From address field of messages sent by the account.

The SocketLabs system will automatically use the proper Engagement Tracking domain to match the domain in the From address field. When the domain in the From address field does not have an aligning Engagement Tracking domain, then the default domain will be used. If no default Engagement Tracking domain is established, engagement will not be tracked.

IV. Customizing Your Settings

A. Create Your Custom Sending Domain(s)

Your default sending domain within the SocketLabs platform is the domain you signed up with. This is the domain that will appear in the “From” field on your outbound messages. The recommended approach is to use this default domain name, or one of its subdomains, as your primary sending domain, especially if it identifies your brand.

You may set up as many additional sending domains or subdomains as you need to support your business and use cases. If you wish to add additional sending domains or subdomains to your account, there are multiple options:

- Add each one manually in the Configuration Options
- Add them through the Management API
- Contact SocketLabs to have all domain restrictions removed (Enterprise only)

The option to have all domain restrictions removed reduces account security and is restricted to customers on Enterprise service tiers.

B. Determine Custom Bounce Domain(s)

The second customization step is to set up your custom bounce domain. This process requires a CNAME record to be established with your DNS service provider. A CNAME record will need to be established in DNS for each of the domains for which you would like to have this feature enabled.

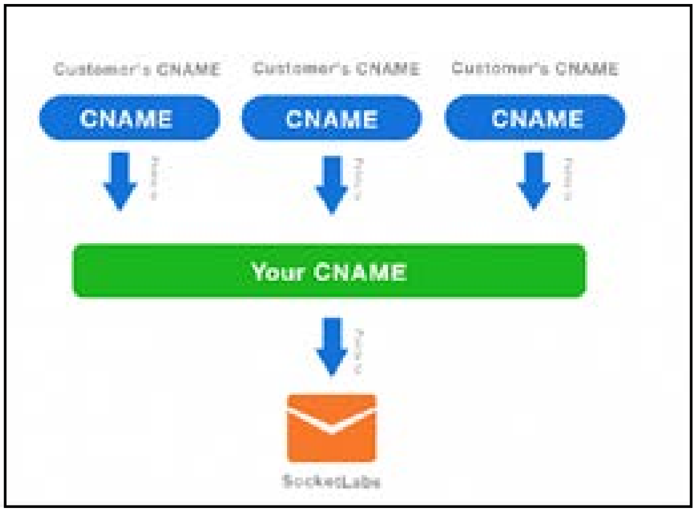
Each CNAME record should point to [tracking.socketlabs.com]. An example of this DNS entry is provided below:

Example Company: Customer Example Co.
Primary Domain: customerexample.com
Subdomain Created to Receive Email Bounces: bounces.customerexample.com

Customer Example Co.'s DNS Entry for Custom Bounce Domain			
Sending Domain	**Hostname**	**Record Type**	**Value**
customerexample.com	bounces.customerexample.com	CNAME	tracking.socketlabs.com

If You Send Email on Behalf of Others

If your organization provides services to sub-clients, we support the white-labeling the DNS records you ask your sub-clients to create. This requires each sub-client to create a CNAME record which references another CNAME record you first create, pointing to SocketLabs, as illustrated to the right, and shown in the example provided below:



Example Company: Customer Example Co.
Primary Domain: customerexample.com
Client of Smart Email Company: Hitting The Inbox Co.

Customer Example Co.s' DNS Entry for Custom Bounce Domain			
Sending Domain	**Hostname**	**Record Type**	**Value**
customerexample.com	bounces.customerexample.com	CNAME	tracking.socketlabs.com

Hitting the Inboxs Co.'s DNS Entry for Custom Bounce Domain

Sending Domain	Hostname	Record Type	Value
hittingtheinbox.com	bounces.hittingtheinbox.com	CNAME	bounces.customerexample.com

Once each DNS record has been created, you need to add each custom bounce domain to your SocketLabs account. There are multiple options for how you can add them:

- Add each one manually in the Configuration Options of the SocketLabs Control Panel

- Add them through calls to the SocketLabs Management API

- For more scalable and dynamic validation mechanisms contact SocketLabs Support.

If you have already implemented an SPF record on your organizational domain then you can merge the provided SocketLabs "include" statement into your existing record. Proper SPF syntax permits only a single TXT DNS SPF record per domain. For example, if your domain already has an SPF record that looks something like the example below (authenticating Google Apps):

Example Organizational Domain SPF Record

Sending Domain	Hostname	Record Type	Value
hittingtheinbox.com	hittingtheinbox.com	TXT	v=spf1 include:_spf.google.com ~all

Adding in our record would change the above example to:

Example Organizational Domain SPF Record

Sending Domain	Hostname	Record Type	Value
hittingtheinbox.com	hittingtheinbox.com	TXT	v=spf1 include:_spf.google.com include:email-od.com ~all

This would allow both SocketLabs and Google Apps to transmit messages on-behalf of your domain. It is important to note that further steps may be required to authenticate other forms in which messages may be processing on behalf of your domain outside of the SocketLabs service. The organizational SPF record is a domain level configuration that can impact mail sent by your domain outside of the SocketLabs service.

C. Create an Advanced DKIM Signature

The process of creating DKIM signature starts by creating a private and public DKIM key using SocketLabs' DKIM Key Generator. The SocketLabs Management API also has a built-in DKIM Key Generator that you can call from your own application.

Follow the steps in the DKIM Key Generator to complete the key creation process. The generator will ask you to choose a 'selector value' which is a unique alphanumeric value/ name that you choose each time you are creating a new key pair. It is basically serving as a name that you will use to refer to the DKIM keys you are creating. SocketLabs recommends using your vendor name in your selector. For example, "socketlabs" helps identify the key as being used for SocketLabs. For organizations that send on behalf of sub-clients, an ideal selector may be their name/ product, such as "Customer Example Co." from prior examples.

Once you have your private/public key pair, the next step is to create a DNS entry on your domain to publish the public key. An example is provided below:

Example Company: Customer Example Co.
Primary Domain: customerexample.com
Selector Value: (named during DKIM Key Generator process) Socketlabs
DKIM Public Key: (produced by DKIM Key Generator) k=rsa; p=MIGfMA0GCSqGSIb
3DQEBAQUAA4GNADCBiQ KBgQCzEOwlTkZskm6nyMFSR9xPUgqe6X1oE1Se

Example of DKIM Record

Sending Domain	DKIM Selector	NameSpace	Record Type	Value

customerexample.com	customerdkim	customerx1._domainkey.customerexample.com	TXT	k=ra
				p=MIGfMAOFOLle

After creating the necessary DNS entries, add the following information into the appropriate fields to add the DKIM details to your SocketLabs account.

- DKIM Domain/Sending Domain
- DKIM Selector
- DKIM Private Key – the private key generated by the generator.

Please ensure the header and footer generated in the generator are fully intact when submitting your private key.
There are multiple options for how you can add these details to your account:

- Add each one manually in the Configuration Options of the SocketLabs Control Panel

- Add them through calls to the SocketLabs Management API

- For more scalable and dynamic validation mechanisms contact SocketLabs Support.

Note: We recommend following the best practice which is to set up a DKIM signature for each sending domain. However, if a DKIM signature is not created, your mail will still be signed by the SocketLabs default and unaligned DKIM signature.

D. Set Up Engagement Tracking

In order to set-up engagement tracking you need to create a single DNS CNAME record. An example of the CNAME record you need to create is provided below:

Customer Example Co's DNS Entry for Engagement Tracking

Sending Domain	Hostname	Record Type	Value
customerexample.com	clicks.customerexample.com	CNAME	tracking.socketlabs.com

Once the CNAME record has been created, the hostname must be added to your SocketLabs account. There are multiple options for how you can turn on engagement tracking:

·Add each one manually in the Configuration Options of the SocketLabs Control Panel

· Add them through calls to the SocketLabs Management API

· For more scalable and dynamic validation mechanisms contact SocketLabs Support.

After the credentials have been added you can "turn on" the engagement tracking features within the Configuration Options. SocketLabs recommends enabling tracking for Opens, Clicks, and the Automatic Tracking option to have the pixels and links tracked automatically. Unsubscribe tracking requires placeholder tag insertion into your content. Placeholder tags can also optionally be used instead of automatic tracking. They allow more refined control over which messages, or even which links, are individually tracked within a message.

V. Summary of Recommended DNS Records

Example DNS Record List			
Sending Domain	**Hostname**	**Record Type**	**Value**
customerexample.com	bounces.customerexample.com	CNAME	tracking.socketlabs.com
	clicks.customerexample.com	CNAME	tracking.socketlabs.com
	socketlabs._domainkey.smartemailco.com	TXT	k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCzEOwlTkZskm6nyMFSR9xPUgqe6X1oE1Se
	_dmarc.customerexample.com	TXT	v=DMARC1; p=none; rua=mailto:dmarc.ag@smartemailco.com; ruf=mailto:dmarc.fr@smartemailco.com;
	customerexample.com.com	TXT	v=spf1 include:_spf.google.com include:email-od.com ~all

VI. Key Authentication Terms

Phishing/Spoofing – These terms refer to a malicious emailing practice where an unsuspecting person will receive an email with a forged address; it appears to originate from one source, when in reality it was sent from another source. Email spoofing is a classic spammer tactic used to coerce unsuspecting users into disclosing secure or confidential information without their knowledge or authorization. A common example is emails that are purportedly from a bank or financial institution, alerting the user that their account has been compromised, and in order to resolve the situation, they must click the link in the email to log into their account.

Sending Domain – The From address domain or the address the recipient sees as the sender in the 'From' address.

Sender Policy Framework (SPF) – SPF is a form of email authentication that specifically protects and authenticates the return path address used in the message delivery process, preventing 'From address' forgery common to phishing or spoofing attacks. SPF allows senders to publish a list of IP addresses, or server names that are authorized to send on their behalf. SPF authenticates the domain used in the "envelope" or return-path email address. SocketLabs' use of a variable envelope return path (VERP) allows us to automatically authenticate all outbound messages with our own SPF record.

Domain Name System (DNS) – DNS refers to the broad system of information that contains the IP addresses, domain names, hosting, and other registration information for every website on the Internet. DNS records act as instructions for DNS servers, so the server knows which domain names each IP address is associated with. DNS records contain a lot of different syntax and commands for how the server should respond to the request. As part of the process of email customization and white-labeling, companies must modify certain syntax in the DNS records where their domains are hosted.

Customer Host Name (CNAME) – CNAME is a DNS syntax entry which specifies that one domain is an alias of second domain (referred to as the "canonical" name). Editing the CNAME record is an essential component of white-labeling email because it allows outbound email to reflect your organization's own domain name, while the actual infrastructure responsible for the email is SocketLabs' platform.

TXT Record – A DNS entry that provides text information about a domain that is human- or machine-readable. TXT records often store information for authentication at a domain.

Custom Bounce Domain– A custom bounce domain is another term for the return path address. This is an email address that is configured by SocketLabs customers to receive responses when a receiving mail server sends back bounce or error messages. This configuration is achieved by editing the CNAME record.

DKIM (DomainKeys Identified Mail) – DKIM is a form of email authentication that allows the receiving mail server to know if a message has been altered during transit. The receiving server checks and verifies an encrypted signature placed on the message by the sending server. If verified, it ensures the message arrived in the same form that it was sent, and was not intercepted, hacked, or manipulated by malicious actors.

The signature is created and encrypted using sender's private key, and then decrypted at the point of receipt by the mailbox provider by referencing the sender's "public key" which is published in the sender's DNS records. If the mailbox provider can confirm that the signatures match, the message is considered to have "passed" DKIM authentication.

Private Key – A sequence of numbers and/or letters that is used to encode outgoing email messages prior to sending. A calculation combines the message content and the private key to produce a value that the receiving mailbox will attempt to verify when the message is received.

Public Key – A sequence of numbers and/or letters that is published on your domain for recipient mail systems use for purposes of verifying the integrity of incoming messages. If the value calculated by combining the public key and the incoming message content matches the value of the private key and the message content, the recipient knows the message was not modified.

Domain-based Message Authentication, Reporting, and Conformance (DMARC) – DMARC is an authentication framework that unifies SPF and DKIM authentication. To pass DMARC, an incoming email must meet one of these two standards and there must be domain alignment. In addition, by establishing a DMARC within their DNS, domain owners can establish a policy that instructs receiving mail servers how to react when the domain owner's messages do not pass. For example, they can request that the message be delivered, quarantined, or rejected.

Engagement Tracking – This feature measures how recipients are interacting with your email. Common engagement metrics include message opens, link clicks, and unsubscribe requests. SocketLabs provides many advanced engagement tracking features including encrypted links and one-click configuration of secure engagement tracking.

Simple Mail Transfer Protocol (SMTP) – SMTP is the industry standard protocol for email sending. With SMTP you are sending, relaying, or forwarding messages from a mail client (like Microsoft Outlook) to a receiving email server. A sender will use an SMTP server to carry out the process of transmitting an email message. Third-party email delivery services like Socketlabs provide SMTP servers that helps companies effectively send marketing and transactional emails.