SINCH Mailgun

HANDBOOK

Email authentication in 2024

How to set up DNS records and stay on the right side of the inbox

Table of contents

INTRODUCTION

Getting serious about authentication

It's not easy for senders to keep up with all the changes in email, but we've also got to hand it to mailbox providers like Gmail and Yahoo Mail. They have one tough job on their hands. There are billions of emails flying around the planet every day, and these services have to decide what should happen to these messages in order to protect users.

Is it spam? Is it malicious? Is someone trying to spoof a well-known brand? Or is this a legitimate email that can be trusted? **Determining whether senders are who they say they are gets complicated.**

When Simple Mail Transfer Protocol (SMTP) became the standard protocol for sending and receiving emails, it lacked a good way to authenticate the identity of the sender. This left the door open for bad actors to impersonate a legitimate domain and deceive email recipients. Over the years, the email industry introduced various email authentication protocols and related specifications to help make the email inbox a safer place.

For quite some time, these authentication protocols were considered important, but not always mandatory. While failing to use or configure them correctly could have a negative impact on email deliverability, mailbox providers didn't want to reject or quarantine important messages. So, many times, emails with authentication failures were still allowed to reach the inbox.

New standards from Gmail and Yahoo Mail are changing the story this year.

Why bulk senders must prioritize authentication in 2024

The news hit in October 2023. **Gmail and Yahoo plan to make email authentication a requirement for bulk senders in early 2024.** To put it simply, if you're not helping mailbox providers authenticate your messages by then, you'll soon be struggling to reach their users' inboxes.

Other updates and requirements came along with these announcements. That included one-click unsubscribe functionality and thresholds for spam complaint rates. However, mandatory email authentication is perhaps the biggest and most technically challenging.

The new requirements involve the following protocols:

- Sender Policy Framework (SPF)
- DomainKeys Identified Mail (DKIM)
- Domain-based Message Authentication, Reporting and Conformance (DMARC)

All three protocols are TXT records, which senders and Email Service Providers (ESPs) set up on the Domain Name System (DNS) servers used for sending email. **Bulk senders need to adopt all three in 2024.** That's partly because the protocols are most effective at stopping email spoofing when used together.

Why is this happening?

Email is an extremely popular attack vector for bad actors. It's like a playground for spammers and scammers. Phishing continues to be a huge problem for both businesses and consumers. Proofpoint found that 84% of the organizations it surveyed suffered at least one successful attack in 2022. Generative artificial intelligence (AI) tools are also making it easier than ever to target inboxes with phishing attempts. There's been a 1,265% increase since late 2022.

Despite this, the inbox is also a key form of communication between individuals and businesses, as well as an essential component of the overall customer experience. Gmail and Yahoo want to protect their users and their own reputations as providers of safe and reliable services.

Google says Gmail blocks nearly 15 billion unwanted emails every day. But that's still not enough. Enforcement of email authentication will encourage more senders to get serious about the issue.

When Sinch Mailgun surveyed senders in 2023, we found that many respondents reported they either weren't using some of these authentication protocols, or they simply did not know.

- **SPF:** Not using (12.8%), Unsure (31.8%)
- **DKIM:** Not using (11.1%), Unsure (30.4%)
- **DMARC:** Not using (18.7%), Unsure (38.8%)

While our survey did not ask participants if they were using all three protocols, it's clear that a significant portion of senders need to investigate their approach to email authentication in 2024. Failing to do so could mean your communications are much less likely to reach the inbox.

What can you do?

At Sinch Mailgun, setting our customers up for success is a top priority, especially when it comes to email deliverability. While we already **require the use of SPF and DKIM for customers** of Mailgun Send, we want to make sure our users have the resources they need to correctly configure these DNS TXT records for their organizations.

This exclusive guide for Sinch Mailgun users will cover the following topics:

1. How SPF, DKIM, and DMARC work.
2. How to properly configure DNS TXT records.
3. Additional tips and resources for effective email authentication.

For Deliverability Services customers, our Technical Account Managers (TAMs) at Sinch Mailgun are also available to answer questions and provide guidance as you review, update, and improve your organization's approach to email authentication.

PART 1

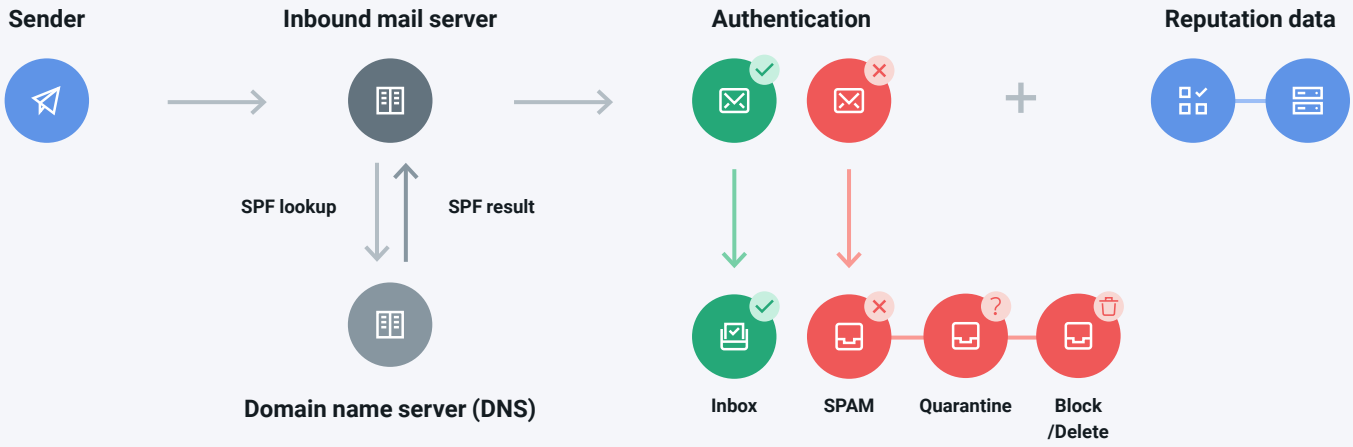
SPF: What you need to know

Sender Policy Framework (SPF) is an email authentication method that lists the IP addresses of mail servers and domain names you've authorized to send mail on your behalf. Think of it like the VIP list for a nightclub. If you're not on the list, the bouncer won't let you in. SPF is the VIP list, receiving mail servers are the bouncer, and the inbox is the nightclub where you want to go.

How SPF works

When mailbox providers use SPF authentication, the incoming mail server checks the email header for the return path (aka reverse path, envelope sender, MAIL FROM, etc.). It then verifies that the email originated from one of the IP addresses listed in the DNS TXT record.

How SPF authentication works



If the incoming mail server verifies the IP, authentication of the sender's identity is confirmed. Unless there are sender reputation issues, the email will likely be delivered to the inbox. If the IP is not found, the email could be blocked from delivery or sent to spam. This decision is up to the mailbox provider, but the way you write an SPF record also suggests how to filter authentication failures.

The SPF record

Let's look at an example of an SPF record. Then, we'll break down each part of the DNS TXT record.

```
1   v=spf1 ip4:61.949.100.188 ip6:98.422.200.766 a:smtp.example.com -all
```

The version of SPF utilized:

This should always be "`v=spf1`" (the first version) because all others have been discontinued.

The list of authorized senders:

Any domain that is sending mail on your behalf should be listed using mechanisms such as IP addresses, hostnames, or "a" records. You can choose to use all of the same type of mechanism or mix and match.

There are several different mechanisms to choose from:

1. The `ip4` or `ip6` mechanism lists the actual IP addresses authorized to send on your behalf.
2. The "`a`" **mechanism** allows the incoming server to reference the "a" records of a domain, instead of a specific IP. As long as the IP where the email originates is found among the "a" records, the email will pass SPF authentication.
3. The `MX` mechanism indicates the IP addresses that your domain uses to receive mail. If an email is sent from one of those IPs, the incoming mail server should accept it.
4. The "`include`" mechanism is also used to include the SPF record of the given domain. This is what Sinch Mailgun uses as a means for customers to add our sending IPs to their SPF.

The "all" mechanism or fail qualifier:

An "all" mechanism is found at the end of every SPF record. It informs incoming mail servers on what to do if a message fails authentication.

- `-all`: If an exact match is not found, the email has failed. The message will be blocked and won't make it to the inbox in any capacity. This is the best way to use SPF to stop spoofing.
- `~all`: If an exact match is not found, the email fails but will still be delivered. However, it is marked as suspicious and will likely go to the spam folder.
- `+all`: This allows any server to send from your domain. It should rarely be used because everything will pass SPF authentication. That means anyone could spoof you as a sender.
- `?all`: This is a neutral setting. The messages don't pass or fail SPF authentication if the IP isn't listed. It leaves the decision up to the mailbox provider.

In our SPF record example, the `-all` mechanism is used as the fail qualifier where the record tells receiving mail servers SPF failures should be blocked from delivery.

PART 2

DKIM: What you need to know

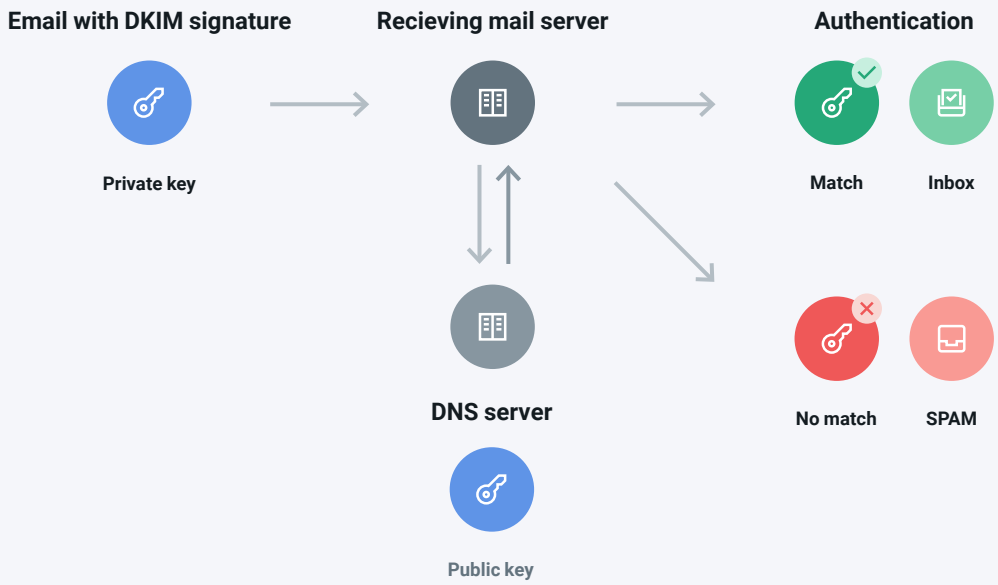
DomainKeys Identified Mail (DKIM) is a protocol that combines two methods for authenticating email senders: Yahoo's "DomainKeys" and Cisco's "Identified Internet Mail." DKIM also helps determine whether an email message was altered during transit.

Put simply, this protocol gives senders a way to digitally sign their mail. DKIM signs messages to signal they originated from the server that created the message – not from an imposter that intercepted the message and altered it for malicious purposes.

How DKIM works

The DKIM protocol involves the use of two keys. These keys are unique to the sender and should be protected as well as rotated on a regular basis. DKIM includes a private key and a public key. The private or encrypted key is part of what's known as a DKIM signature, which is found inside the email header. The public key resides on the DNS server while the encrypted key travels with the email.

How DKIM authentication works



The DKIM signature tells mailbox providers and mail transfer agents (MTAs) where to retrieve the public key. If the public key pairs with the encrypted signature, the email is more likely to be delivered to the inbox. If there is no match, or if there's no DKIM signature at all, the email is more likely to be rejected or filtered into spam.

The DKIM record and signature

First, let's look at how the DNS TXT record for DKIM might look. This is where the public key is found. Then, we'll break down the parts of the DKIM signature, which travels with the email in the header.

The DNS record

```
dk2048-2023._domainkey.example.com TXT "v=DKIM1; t=y; k=rsa;
p=MIGfMA0GCSqGSiuTHjQWercnvEr54A2CA;"
```

Here's an explanation of what's inside this TXT record:

- `v=` The version of the protocol used.
- `t=` This optional tag indicates if the sending domain is testing DKIM.
- `k=` The key type, which is usually RSA
- `p=` The public key, which pairs with the encrypted DKIM signature.

Sinch Mailgun (or your current ESP) will provide you with the public key for the DNS record. We then digitally sign your mail with the encrypted key in the header.

The DKIM signature header

```
DKIM-Signature v=1; a=rsa-sha256; q=dns; d=example.com; s= dk1024-
2012; t=1117574938; x=1118006938; h=Content-Type: Mime Version:
Subject: From: To: Sender; Date: List-Unsubscribe
bh=PV3AoaeTApQYJwe3qgbuUFFTVhjwhv1q2gGNBL+KHU=;
b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

Here's an explanation of the tags found in the sample DKIM signature above:

- v= The version of DKIM.
- a= The signing algorithm.
- q= The default query method.
- d= The signing domain associated with a selector record to locate a public key.
- s= The selector, which is used to lookup the public key and allows multiple keys on a domain.
- t= The signature timestamp.
- x= The expire time
- h= The list of headers that will be used in the signing algorithm
- bh= The body hash after being canonicalized by Base64, which turns binary code into text
- b= The actual DKIM signature of headers and body, which is encoded with Base64. It is generated from the bh and h tags.

So, b= contains the digital signature (encrypted key), which is used to pair with the public key on the DNS server after it is unscrambled. Base64 is used to safely carry data that has been encrypted, or stored, in a binary format over channels that usually only support text, like HTML and CSS.

DKIM keys can be 1024-bit or 2048-bit in length. Because hackers have been able to break 1024-bit DKIM keys, using 2048-bit is now highly recommended.

There are also some optional DKIM tags that can be added to the header information. Other DKIM header tags are required: v, a, d, s, h, bh, and b. Still others, like t and x, are optional but recommended.

PART 3

DMARC: What you need to know

Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email specification that combines the benefits of SPF and DKIM. This forms a more powerful way to identify senders and stop email spoofing.

DMARC checks for SPF and DKIM alignment and defines a policy that informs the receiving server how authentication failures should be handled. When DMARC is implemented, mailbox providers check for both SPF and DKIM and then refer to the policy, which the sender defines in the DMARC DNS record.

DMARC policy options are:

- **Reject:** Messages that fail authentication should not be delivered (`p=reject`).
- **Quarantine:** Messages that fail authentication should be filtered into the spam folder (`p=quarantine`).
- **None:** Provides no guidance. Mailbox providers must decide how to filter authentication failures (`p=none`).

The `p=none` policy is the least strict. It means no specific policy is being enforced. While Gmail is making DMARC implementation a requirement in 2024, it has said it will accept a policy of `p=none`. But that doesn't mean the requirement will remain that way.

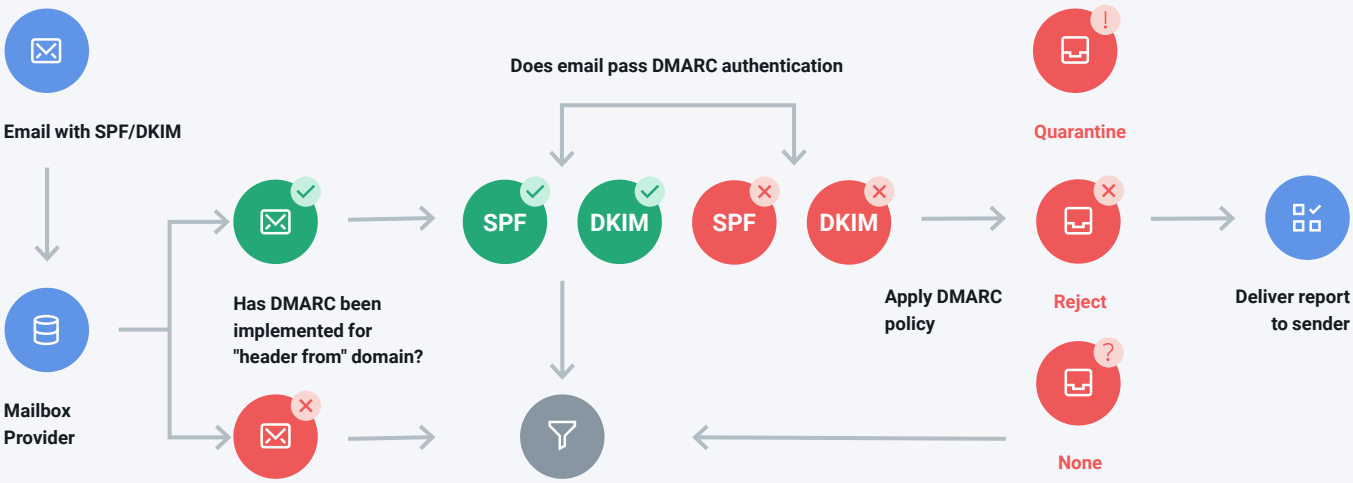
"Mailbox providers are accepting a DMARC policy of none for now, but it's unlikely to remain that way. Expect a requirement to implement a policy of quarantine or reject in the future. The p=none policy does not do anything to protect from spoofing, and that's the ultimate goal."

Nick Schafer, Sr. Manager of Deliverability & Compliance, Sinch Mailgun

How DMARC works

When a sender has implemented DMARC, the mailbox provider checks to see if it passes SPF and DKIM. Then it enforces the policy listed in the DNS record and filters the email accordingly. Finally, a report is delivered to the sender with information about the email traffic sent on behalf of the domain and how it was handled.

How a DMARC Policy Works



It's important to realize that your DMARC policy is a suggestion, not a directive to mailbox providers like Gmail and Yahoo Mail. Setting a policy to `p=none` is not a guarantee your emails will make it to the inbox if they fail authentication.

Some senders use the `p=none` policy while testing and troubleshooting DMARC implementation, or they use it to receive DMARC reports without enforcing a stricter policy. The best way to use DMARC to fight email spoofing is to enforce a policy of `p=quarantine` or `p=reject`.

"Our recommendation is usually to start with a p=none policy. This lets you see the potential impact if it were set to anything else. Some senders might discover mail streams they'd forgotten about, which would fail authentication. A p=none policy is a good way to catch those and adjust before enforcing a policy of quarantine or reject."

Renate Burns, Deliverability Operations Team Lead, Sinch Mailgun

The DMARC record

DMARC records can be fairly simple or complex with lots of tags. Let's first look at a basic DMARC record. Then, we'll explain all the possible tags you could use with DMARC.

```
v=DMARC1; p=quarantine; sp=none; rua=mailto:dmarc-reports@example.com; pct=100; aspf=s; adkim=s
```

While not all of them are in our example, the following tags can be used to create a DMARC record:

- `v=` The version of DMARC used.
- `p=` The DMARC enforcement policy: none, quarantine, or reject.
- `rua=` A list of email addresses where DMARC aggregate reports are sent.
- `pct=` The percentage of messages that are subject to the enforcement policy. Default is pct=100.
- `aspf=` Defines the alignment mode for SPF, which could be strict or relaxed with pass/fail scenarios.
- `adkim=` Defines the alignment mode for DKIM, which could be strict or relaxed with pass/fail scenarios.
- `sp=` Represents different enforcement policies for subdomains.
- `ruf=` Lists email addresses for sending DMARC failure/forensic reports, which are more detailed than aggregate reports.
- `fo=` Indicates the options for creating a DMARC failure/forensic report.
- `rf=` Declares the forensic reporting format for message-specific failure reports.
- `ri=` Sets the interval for sending DMARC reports, which is defined in seconds but is usually 24 hours or more.

In our DNS TXT record example, the sender has a DMARC policy set to `p=quarantine` with no difference for any subdomains. There's an email address for receiving aggregate reports. 100% of messages are subject to the DMARC policy, and both SPF and DKIM alignment modes are set to "strict." **When set to "strict", if either SPF or DKIM fails authentication, then the entire DMARC check fails.**

The `pct=` tag in your DMARC record allows you to **specify a percentage of messages to which your policy should be applied**. That means you can evaluate the impact that a `p=quarantine` or `p=reject` policy might have on inbox placement. Then, you can troubleshoot any problems using DMARC reports and gradually increase the percentage to which the policy is applied.

More about DMARC

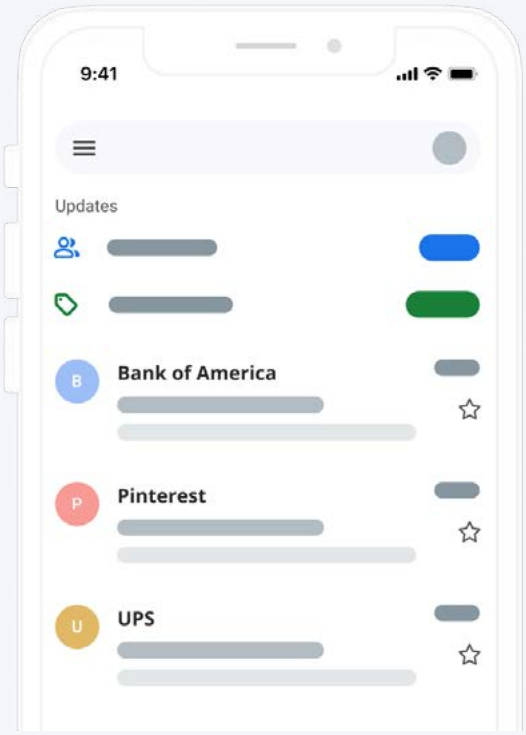
As mentioned, another benefit of implementing DMARC is the reports sent to senders on a regular basis. These provide visibility into who may be trying to send mail on your domain's behalf.

There are two types of DMARC reports:

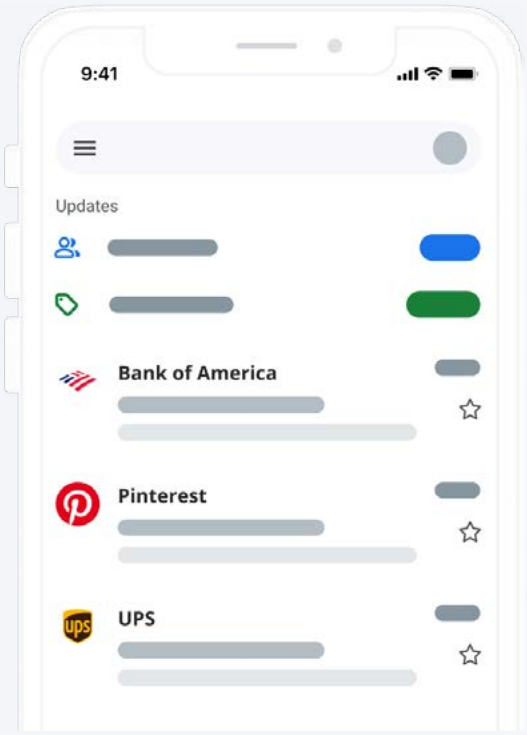
1. **Aggregate DMARC reports** are sent daily unless otherwise specified. They provide information about failures, overall email traffic, and details about the IPs and sources using your domain in the "From" field.
2. **Forensic DMARC reports** are sent every time an email fails DMARC authentication because SPF and/or DKIM are not aligned. Also known as **failure reports**, they are very helpful for investigating spoofing if you need additional details.

Brand Indicators for Message Identification (BIMI) is another email specification that is connected to authentication and DMARC. When senders have correctly implemented DMARC with a policy of reject or quarantine, senders are eligible to have a verified, trademarked logo appear at the message level in the inbox. **BIMI is not included in the new bulk sender requirements.** Instead, it can be considered a potential reward for senders who enforce strong email authentication.

Before BIMI



After BIMI



PART 4

Recapping the changes for senders

The new requirements for bulk senders in 2024 may be cause for concern for some, but if you've already been following best practices for email authentication, you're likely in good shape. Gmail and Yahoo have other updates to their policies for bulk senders, which also reflect current best practices.

The changes apply to anyone who is sending thousands of emails per day to Gmail users. Representatives from Yahoo and Gmail worked together to define these requirements making them quite similar:

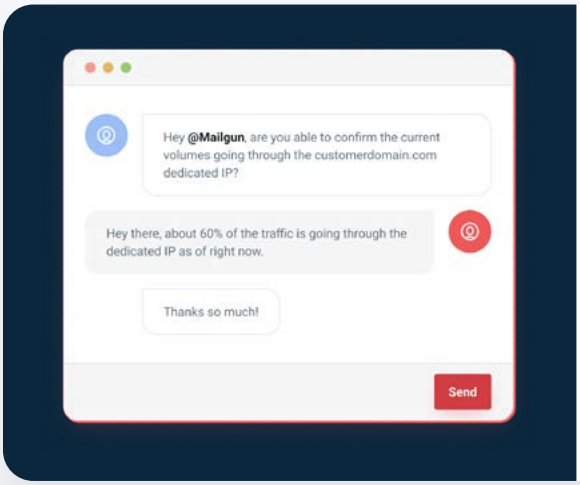
The change	The details
Required email authentication protocols	Bulk senders must use both SPF and DKIM along with DMARC. The DMARC policy can be set to p=none. The domain in the sender's "From:" header should align with either the SPF domain or the DKIM domain. This is required to pass DMARC.
One-click unsubscribe functionality	It must be easy to unsubscribe from all marketing emails. This requires specific headers and a visible link in the message body. Senders must follow through within two days. The requirement does not apply to purely transactional messages.
ARC headers for forwarding	Bulk senders who regularly forward emails must implement ARC headers. This identifies the sender as the one forwarding the message. It also checks the previous authentication status before forwarding.
Spam complaint threshold	Senders should consistently keep spam rates below 0.1% (1 for every 1,000 emails). Temporary spikes in the spam complaint rate should not reach or exceed 0.3%.

Whether it was Apple Mail Privacy Protection in 2021 or GDPR in 2018, bulk senders have had moments like this before and there will be others in the future. While such changes can cause headaches, they ultimately make the inbox a better place.

Not only do these requirements protect recipients, which includes customers, they also support your brand's reputation as an organization that can be trusted.

"I think the importance of protecting a sender's brand is becoming a bigger topic in the email space because of the way the industry is changing. Brand is everything. If people lose confidence in your company because they're unsure if emails that appear to be from you are safe, it can permanently damage your reputation."

Jonathan Torres, TAM Team Manager, Sinch Mailgun



Get authentic advice from the experts

Are you a Sinch Mailgun customer with questions about email authentication, new bulk sender requirements, and your sending practices? We're here for you:

Contact Sinch Mailgun Support

Resources

Looking for additional information and helpful resources for addressing new bulk sender requirements in 2024? Check out our list of suggestions, including Sinch Mailgun content and support documentation.

More about bulk sender requirements

Guide to the 2024 Gmail and Yahoo changes: Get Sinch Mailgun's comprehensive guide to enhancing compliance and optimizing your email program for new requirements.

What it means to your email program: Follow along on the Sinch Mailgun blog as we update the situation around Gmail and Yahoo's new standards.

Gmail sender guidelines: Visit Google's help center to see how it explains the changes for senders.

Yahoo bulk sender best practices: Visit Yahoo's sender hub to review the mailbox provider's updated requirements.

Interview with Yahoo's Marcel Becker: Listen to an episode of the Sinch Mailgun podcast Email's not Dead and get detailed answers to common questions about the new sender guidelines.

More about email authentication

Domain verification walkthrough: Get step-by-step guidance on how to verify a domain through the Mailgun Send platform. This includes links to documentation from major DNS hosting providers.

The basics of SPF records: Dig deeper into how the SPF authentication protocol works and how to create your record within Mailgun Send.

How DKIM authentication works: Learn more about DKIM signatures, get the details on how the protocol verifies email senders, and see how to set up the protocol with Maigun Send.

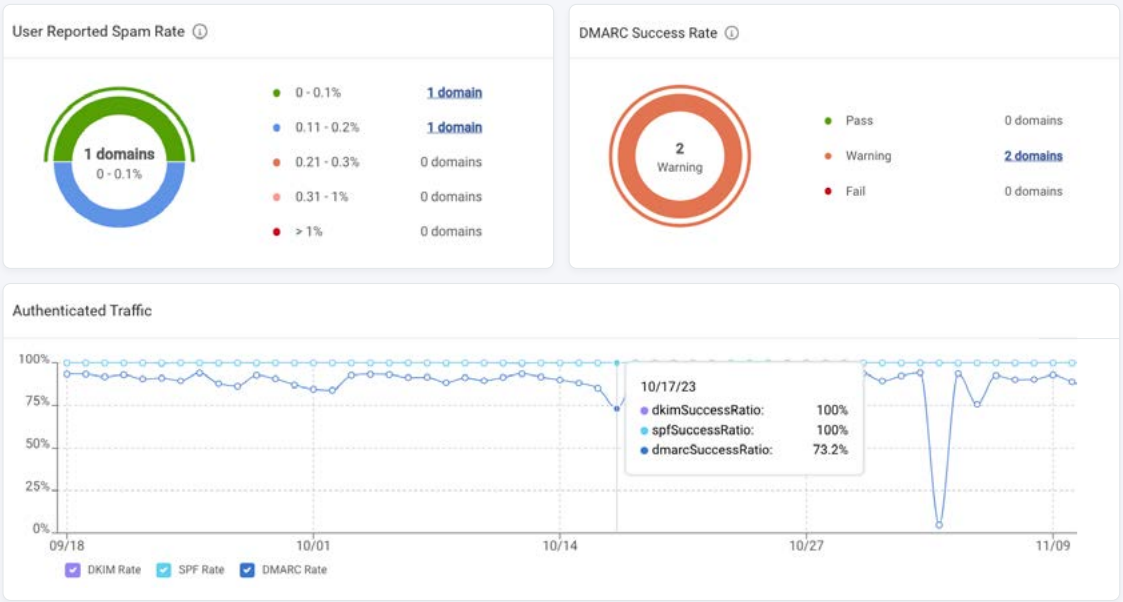
How to implement DMARC: Find out how this powerful email specification checks for SPF and DKIM alignment to stop spoofing. Get advice for rolling out DMARC on your domain.

The basics of subdomains: Find out how to properly use subdomains as an email sender, including details on authentication.

How to check email authentication status

Mailgun Optimize customers can take advantage of the product's integration with Google Postmaster Tools to troubleshoot and test whether authentication protocols are set up properly and working.

Monitor your spam complaint rate in Gmail to avoid thresholds. Plus, find your pass/fail rates for SPF, DKIM, and DMARC with Reputation Monitoring.



Over 100,000 companies worldwide use Sinch Mailgun to create elegant email experiences for their customers through world-class infrastructure. Brands like Microsoft, Lyft, and Etsy trust Mailgun's innovative technology and reliable infrastructure to send billions of emails every year. Built with development teams in mind, Mailgun makes sending, receiving, and tracking emails effortless for email senders of all sizes.

Mailgun was founded in 2010 as a response to the lack of developer-friendly, API-based email services. Since then, Mailgun has joined **Sinch**, a leading Communication Platform as a Service (CPaaS) provider, to become the developer-first email solution for their global customer base. GDPR, HIPAA, and SOC I & II compliant, Mailgun aims to provide the best email service possible with the utmost security and privacy.

For more information, please visit **mailgun.com**.