MARIGOLD™

2024 Sender Requirements & Enforcements

A Guide for Campaign Monitor by Marigold Customers

December 2023

MARIGOLD™

Keep Inboxes More Secure

We're here to be your partners, ensuring you are empowered to create marketing gold.

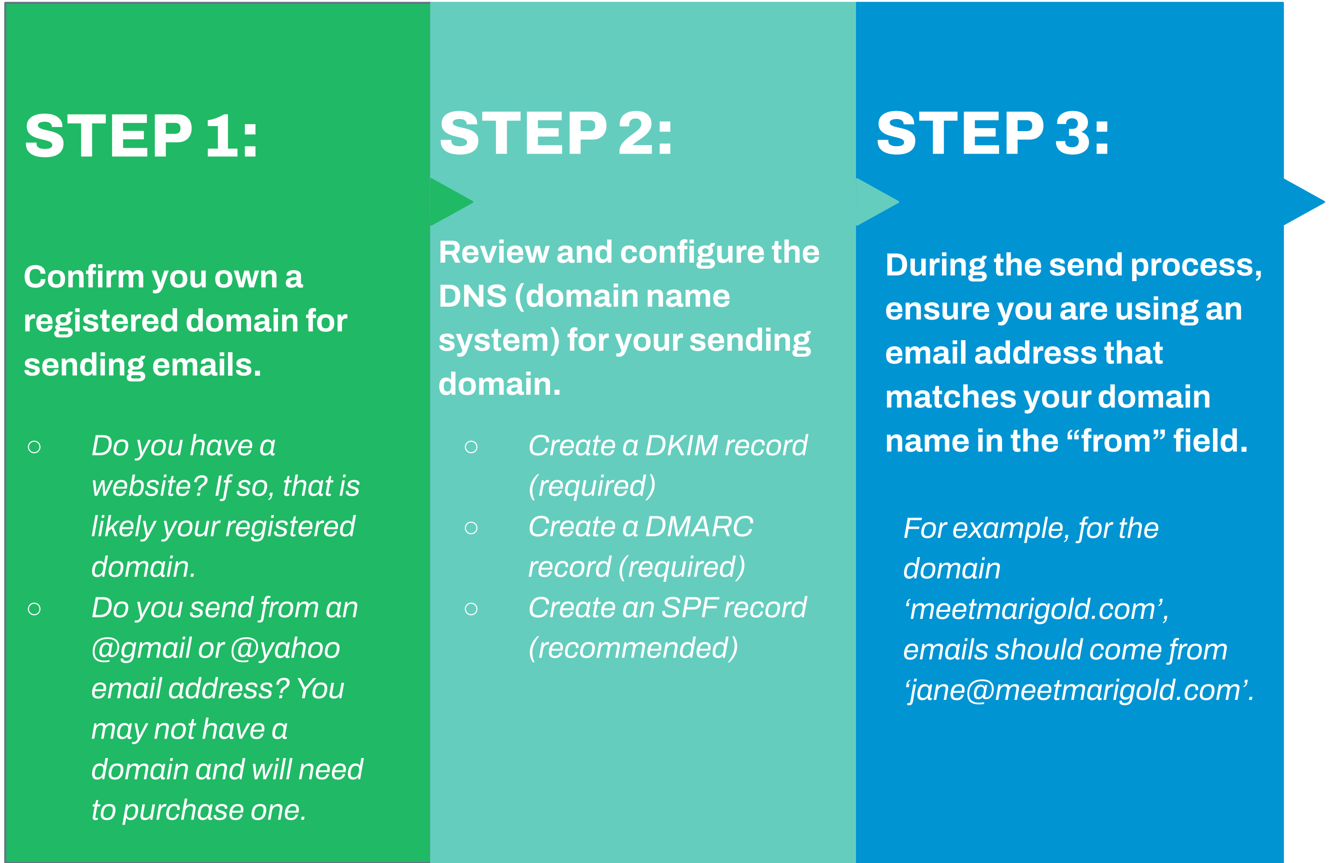
In October 2023, mailbox providers Google and Yahoo announced sender requirement changes in an effort to keep email a reliable source of communication, as well as continue to protect inboxes for their consumers. These changes will go into effect as of February 1, 2024.

To best support you, we have created a step-by-step guide for the actions we recommend you take to avoid any disruption to your email strategy.

2024 Sender Requirements: 3 Themes

	Authenticate your emails	Make unsubscribing easier	Stay below the spam threshold
WHAT YOU'LL NEED TO DO	Confirm DNS records with DKIM, DMARC, and SPF protocols	Make it easier to unsubscribe with the option in the email header	Stay below a 0.3% spam complaint rate
WHO WILL BE RESPONSIBLE	You'll be responsible for confirming these records	Marigold will make this standard within our platforms	We'll work on this together
WHEN TO TAKE ACTION	You'll need to take action prior to January 31, 2024	Marigold will make these changes in mid-January 2024	This work should be ongoing

Action Plan: Stay Compliant for February 2024



STEP 1:

Confirm you own a registered domain for sending emails.

- *Do you have a website? If so, that is likely your registered domain.*
- *Do you send from an @gmail or @yahoo email address? You may not have a domain and will need to purchase one.*

STEP 2:

Review and configure the DNS (domain name system) for your sending domain.

- *Create a DKIM record (required)*
- *Create a DMARC record (required)*
- *Create an SPF record (recommended)*

STEP 3:

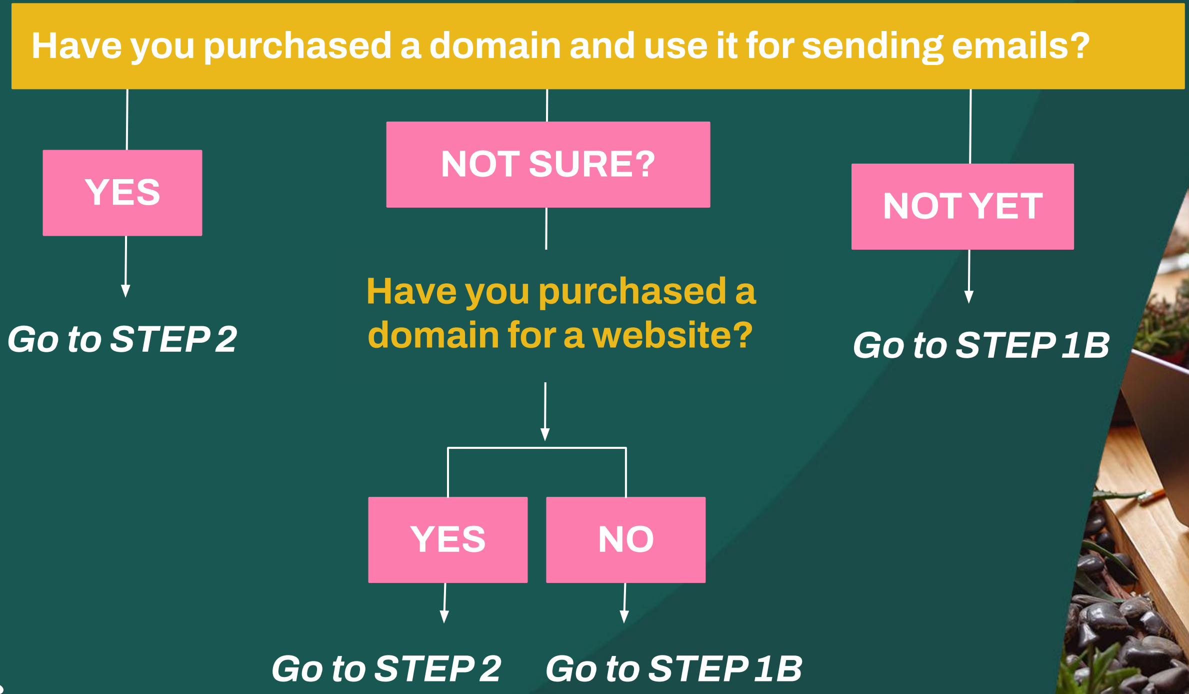
During the send process, ensure you are using an email address that matches your domain name in the “from” field.

For example, for the domain ‘meetmarigold.com’, emails should come from ‘jane@meetmarigold.com’.

STEP 1

START HERE:

Do you have a registered domain?



Have you purchased a domain and use it for sending emails?

YES

Go to STEP 2

NOT SURE?

Have you purchased a domain for a website?

YES

Go to STEP 2

NO

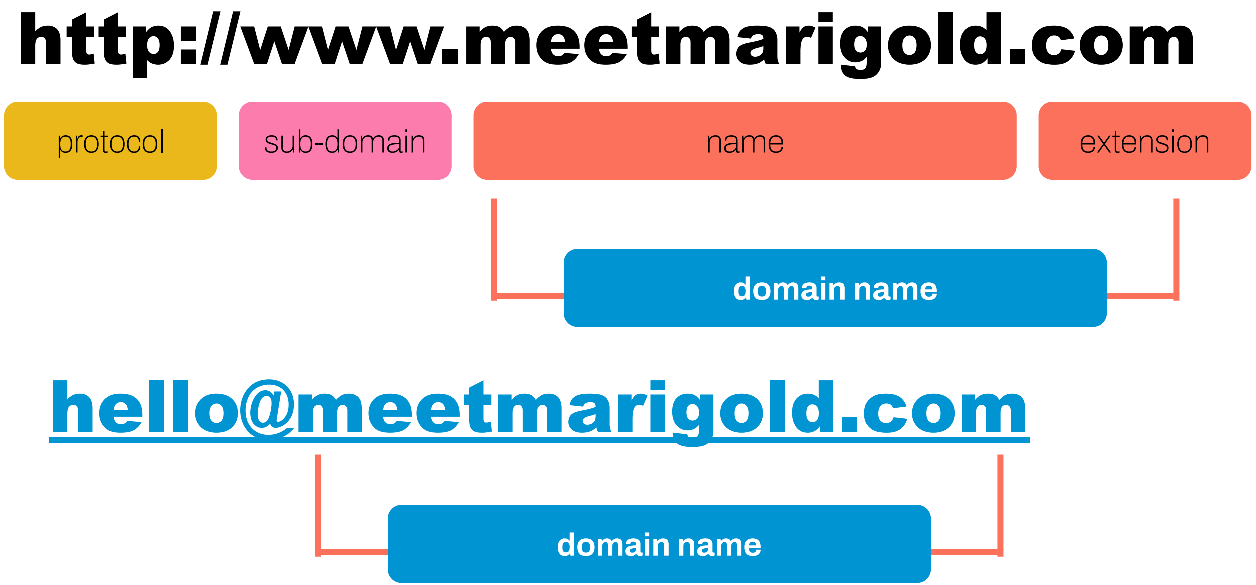
Go to STEP 1B

NOT YET

Go to STEP 1B

STEP 1B

Purchase a registered domain for sending emails



http://www.meetmarigold.com

protocol

sub-domain

name

extension

domain name

hello@meetmarigold.com

domain name

- If you have never purchased a domain, such as a website or owned domain for sending emails, you will need to purchase a domain as part of the new sender requirements from Google and Yahoo.

- Domains MUST BE REGISTERED for 30 days before use, so be sure to take action on this as soon as possible, at least before the end of the calendar year.

STEP 1B

Frequently Asked Questions

QUESTION: What is a domain?

Every website has an IP address, essentially the coordinates for finding the website. However, as those IP addresses are just a series of numbers, they can be hard to remember. A structure called Domain Name System (DNS) translates the IP address into a memorable domain name (i.e. meetmarigold.com).

QUESTION: How do you buy a domain?

There are several domain registrars, or services that sell domains. You'll be able to select a domain name and check to make sure you're the only one using that particular domain name. Then, you'll be able to sign-up, either for a year or multiple years, for that domain. Look for names ending in .com, .net, or .org as well as a domain name that will be recognized by your recipients.

QUESTION: How much does a domain cost?

The price of owning a domain varies by domain registrar, but many are available for a small fee each year. Be sure to plan on renewing your domain, or having one every year, moving forward.

QUESTION: Do I need a domain and an email service provider (ESP)?

Yes, you'll need both. Think of a domain like a nametag, that helps your customers find you online and associate your name and brand with your emails. Your ESP, Campaign Monitor by Marigold, allows you to design, send, and track emails being delivered. However, you'll need to use a domain for sending emails (i.e. annexample@meetmarigold.com) regardless of your ESP as of February 2024.

QUESTION: Does Marigold recommend a particular Domain Registrar?

We do not, and there are so many options available. We recommend looking at details like pricing, length of contract, and additional services (if needed) like website design. A few of the more popular options for domain registrars include Bluehost, HostGator, GoDaddy, and Domain.com.

STEP 2

Configure your DNS

DNS (Domain Name System) will need to configured for your sending domain.

You’ll do this by setting up three DNS records within your domain registrar. **Our recommendation:** open two tabs now, one with your **r**egistrar and one with Campaign Monitor.

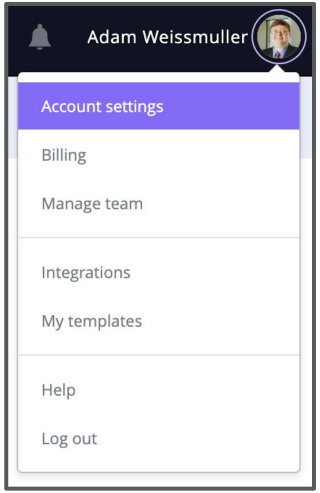
Follow the directions that follow to set-up protocols for SPF, DKIM, and DMARC. If you want a refresher on these, see the appendix.

Need additional help with STEP 2?
Contact our Support team for assistance.

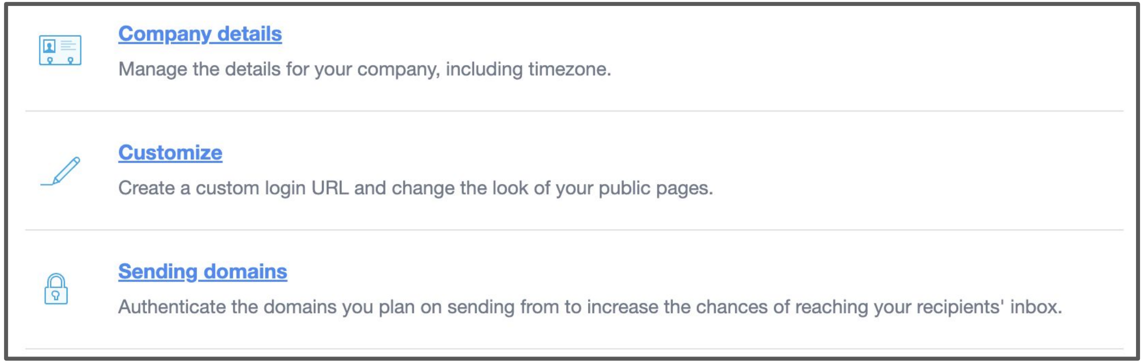
Authenticate your emails

STEP 2 Configure your DNS

1 Open your domain registrar of choice and locate the instructions for updating your DNS or managing your DNS records



2 Locate your ‘Account Settings’ in the menu under your profile in Campaign Monitor.



Company details

Manage the details for your company, including timezone.

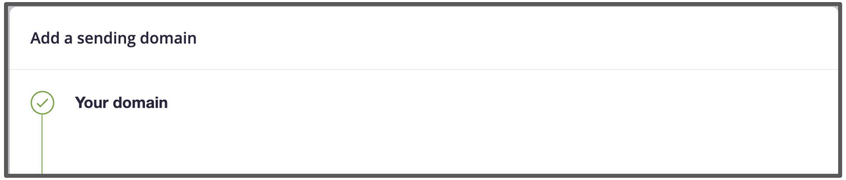
Customize

Create a custom login URL and change the look of your public pages.

Sending domains

Authenticate the domains you plan on sending from to increase the chances of reaching your recipients' inbox.

3 Select ‘Sending domains’ from the menu.

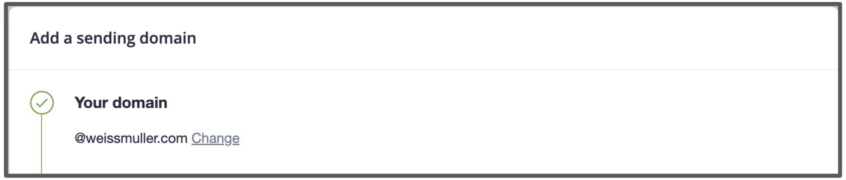


4 Then select ‘Add a sending domain’.

STEP 2

Configure your DNS

Authenticate your emails

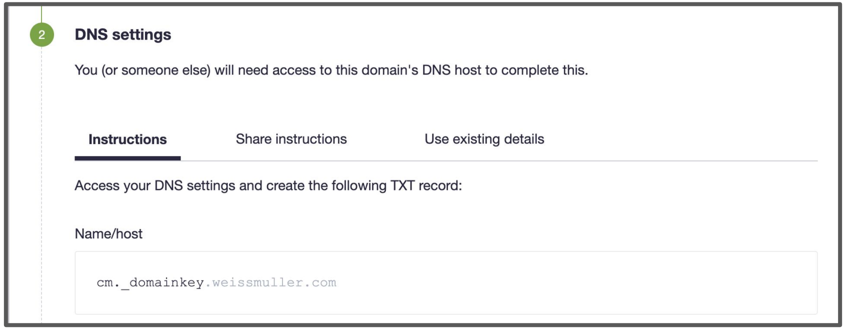


Add a sending domain

Your domain

@weissmuller.com Change

5 Add your domain name, such as ‘meetmarigold.com’ or ‘emailrocks.net’.



2 DNS settings

You (or someone else) will need access to this domain's DNS host to complete this.

Instructions | Share instructions | Use existing details

Access your DNS settings and create the following TXT record:

Name/host

```
cm._domainkey.weissmuller.com
```

6 Before switching back to your domain registrar, copy the code listed under ‘Name/host’. It will be different than the example above and should include your custom domain.

7 Now you’ll click over to the tab for your domain registrar. As there are hundreds of options and each is a little different, note that labels may differ slightly. You’ll now enter the DNS values to create a record for SPF and DMARC.

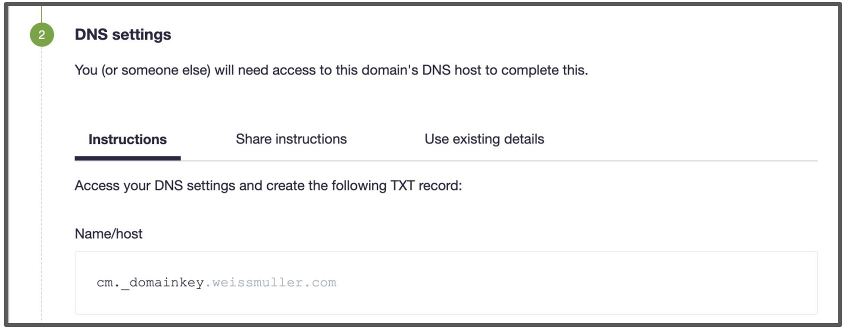
8 First, find the section of your domain registrar labeled DNS record, or manage your DNS. You’ll want to add a new record.

9 For users of the Campaign Monitor platform, each record (3 total) will be a TXT record. Select the type of record to add as TXT.

STEP 2

Configure your DNS

Authenticate your emails



2 **DNS settings**

You (or someone else) will need access to this domain's DNS host to complete this.

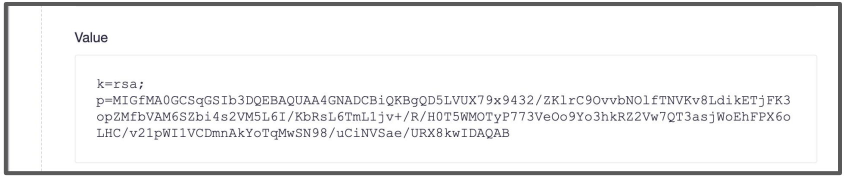
Access your DNS settings and create the following TXT record:

Name/host

```
cm._domainkey.weissmuller.com
```

10 Once you select to add a TXT record, paste the value you previously copied from Campaign Monitor (Name/host) as the name of the new record.

11 Switch back over to Campaign Monitor and now copy the code beneath labeled “Value”. Paste that value into the record you’re creating in the domain registrar.



Value

```
k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQD5LVUX79x9432/ZKlrC9OvvbNOlfTNVKv8LdikETjFK3
opZMfbVAM6SZbi4s2VM5L6I/KbRsL6TmL1jv+/R/H0T5WMOTyP773VeOo9Yo3hkRZ2Vw7QT3asjWoEhFPX6o
LHC/v21pWI1VCDmnAkYoTqMwSN98/uCiNVSae/URX8kwIDAQAB
```

12 Finally, in the domain registrar, select an option for TTL. We recommend using 300 seconds, or a half hour, depending on what options are listed in your domain registrar.

13 Save that record in the domain registrar - Congratulations! You have successfully added a DKIM record.

14 In the domain registrar, add another new record. Now you’ll be adding an SPF record:

⚠️ - If you already have a record that contains ‘v=spf1’, only add ‘include:_spf.createsend.com’ immediately after that text in your existing record.

- Select TXT as the type
- Enter ‘@’ for the name
- Copy and paste this code exactly as is:
    - v=spf1 include:_spf.createsend.com ~all
- Select the TTL value (300 seconds - 30 minutes)
- Save this SPF record

Configure your DNS

15

Still in the domain registrar, you're now adding the third and final record for DMARC:

⚠️ - If you already have a record that starts with _dmarc, skip this step!

- Select TXT as the type
- Enter '_dmarc' for the name
- Copy and paste this code exactly as is:
  - v=DMARC1; p=none;
- Select the TTL value (300 seconds - 30 minutes)
- Save this DMARC record

16

From your domain registrar DNS records, you should see all three records successfully added .

HELPFUL TIP!

Having trouble with the copy / paste of these codes? You may have accidentally added a space to the front or back while copying. Ensure no extra spaces or additional characters are included while pasting, and then try again.

STEP 2

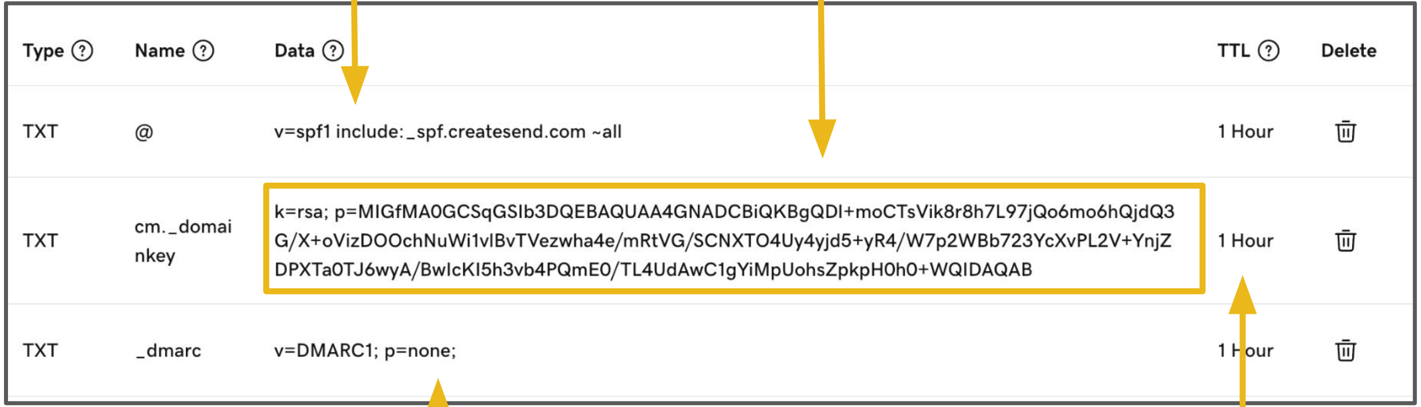
Configure your DNS

This is an example of what your domain registrar might look like; all domain registrars may be slightly different.

Authenticate your emails

This is your SPF record. You'll copy this text (step #14) exactly as is and paste.

This is your DKIM record. This is a unique code that you'll copy from Campaign Monitor and paste into your domain registrar.



Type ?	Name ?	Data ?	TTL ?	Delete
TXT	@	v=spf1 include:_spf.createsend.com ~all	1 Hour	🗑
TXT	cm._domainkey	k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDI+moCTsVik8r8h7L97jQo6mo6hQjdQ3G/X+oVizDOOchNuWi1vlBvTVezwha4e/mRtVG/SCNXTO4Uy4yjd5+yR4/W7p2WBb723YcXvPL2V+YnjZDPXTa0TJ6wyA/BwIcKI5h3vb4PQmE0/TL4UdAwC1gYiMpUohsZpkpH0h0+WQIDAQAB	1 Hour	🗑
TXT	_dmarc	v=DMARC1; p=none;	1 Hour	🗑

Use 'TXT' for each type and these name values for your records.

This is your DMARC record. You'll copy this text (step #15) exactly as is and paste.

Select the TTL value (300 seconds - 30 minutes). This may vary by domain registrar.

STEP 3

Verify your domain

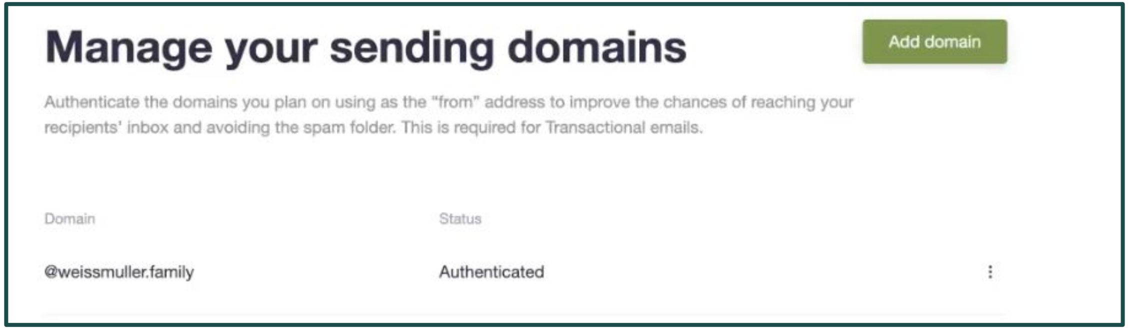
Connect your domain with your email service provider to be in compliance with the new sender requirements.

Verify that the account(s) you have with Campaign Monitor include your registered domain.

STEP 3

Verify your domain

Authenticate your emails



Manage your sending domains

Authenticate the domains you plan on using as the "from" address to improve the chances of reaching your recipients' inbox and avoiding the spam folder. This is required for Transactional emails.

Domain	Status
@weissmuller.family	Authenticated

Go back to Campaign Monitor and select ‘Authenticate Now’ from the DNS screen to finalize the DNS records in Campaign Monitor. Once completed, you should see your domain name and a successful status of ‘Authenticated’.

Need more help?

STEP 4

Authenticate your emails

Match sender name to domain

Remove any questions for your audience and send emails from your domain.

By linking your domain with Campaign Monitor, you can send emails from your own domain. For example, when you receive an email from megan@meetmarigold.com, you can be sure it is coming from Marigold and from your known contact, Megan.

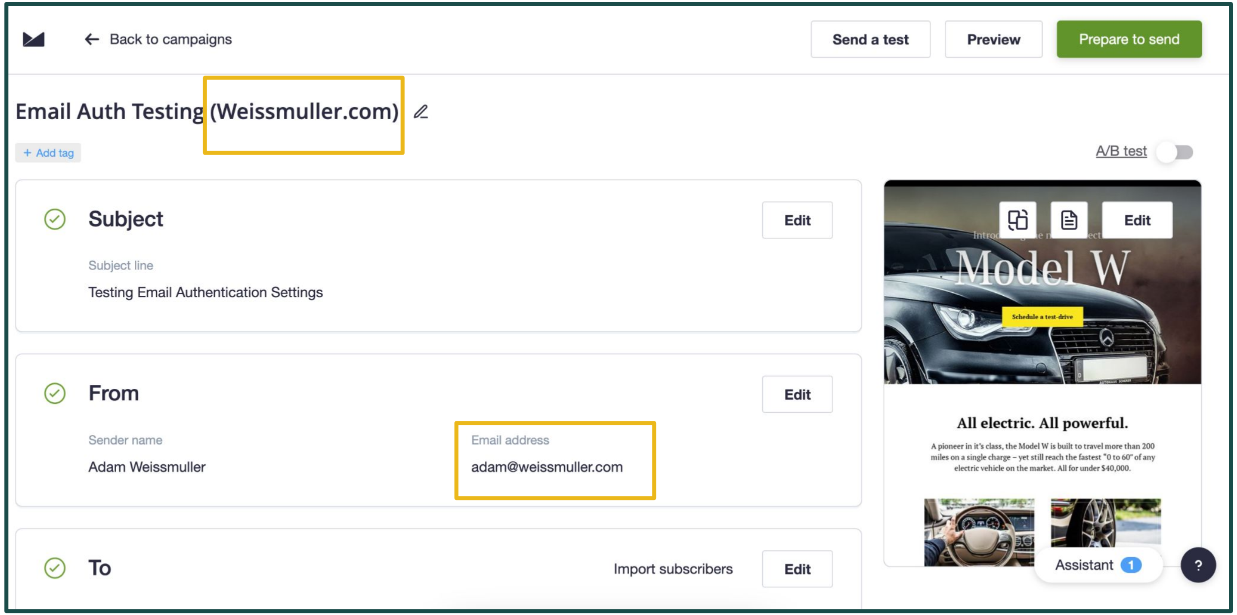
STEP 4

Match sender name to domain

Authenticate your emails

When sending an email or using an email template, ensure that the name and email sending in the 'From' line matches your domain.

For example, if your domain is 'meetmarigold.com', then emails should be sent from [name]@meetmarigold.com such as 'adam@meetmarigold.com'.



Email Auth Testing (Weissmuller.com)

Subject

Subject line: Testing Email Authentication Settings

From

Sender name: Adam Weissmuller

Email address: adam@weissmuller.com

To

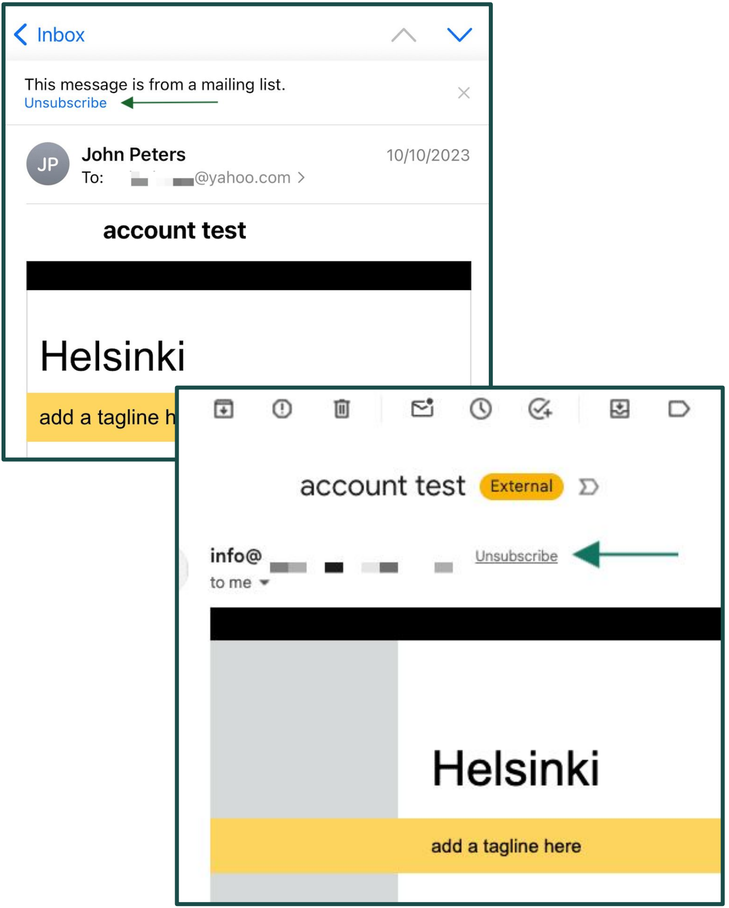
Back to campaigns
Send a test
Preview
Prepare to send
+ Add tag
A/B test
Edit
Edit
Edit
Import subscribers
Edit
Edit
Model W
Schedule a test-drive
All electric. All powerful.
A pioneer in it's class, the Model W is built to travel more than 200 miles on a single charge – yet still reach the fastest "0 to 60" of any electric vehicle on the market. All for under $40,000.
Assistant 1
?

Sender Requirements: 3 Themes

	Authenticate your emails	Make unsubscribing easier	Stay below the spam threshold
WHAT YOU'LL NEED TO DO	Confirm DNS records with DKIM, DMARC, and SPF protocols	Make it easier to unsubscribe with the option in the email header	Stay below a 0.3% spam complaint rate
WHO WILL BE RESPONSIBLE	You'll be responsible for confirming these records	Marigold will make this standard within our platforms	We'll work on this together
WHEN TO TAKE ACTION	You'll need to take action prior to January 31, 2024	Marigold will make these changes in mid-January 2024	This work should be ongoing

New Unsubscribe Feature Coming

Make unsubscribing easier



This message is from a mailing list.
Unsubscribe

John Peters 10/10/2023
To: [redacted]@yahoo.com

account test

Helsinki

add a tagline h

account test External

info@[redacted] Unsubscribe
to me

Helsinki

add a tagline here

As part of the new sender requirements, recipients must be able to unsubscribe with ease, and senders must process and honor unsubscribe requests within two days. While unsubscribe links have been a legal requirement for over two decades, one-click unsubscribe functionality is a new requirement. While CAN-SPAM allows senders a ten-day grace period to process opt-outs, Google and Yahoo are requiring a faster unsubscribe period as part of these requirements.

Campaign Monitor by Marigold will be further enhancing our existing unsubscribe headers to comply with the one-click requirement. This addition will be automatically updated in mid-January and will apply to all current campaigns, drafted emails, and templates. Additionally, your existing unsubscribe link in the footer of the message is also required and should continue to work as it currently does. This may go to a Preference Center or other type of confirmation page.

Want to learn more about how Marigold is making unsubscribing easier? Join our January 2024 Roadmap Webinar for this new release, plus other new releases, coming to Campaign Monitor.

Sender Requirements: 3 Themes

	Authenticate your emails	Make unsubscribing easier	Stay below the spam threshold
WHAT YOU'LL NEED TO DO	Confirm DNS records with DKIM, DMARC, and SPF protocols	Make it easier to unsubscribe with the option in the email header	Stay below a 0.3% spam complaint rate
WHO WILL BE RESPONSIBLE	You'll be responsible for confirming these records	Marigold will make this standard within our platforms	We'll work on this together
WHEN TO TAKE ACTION	You'll need to take action prior to January 31, 2024	Marigold will make these changes in mid-January 2024	This work should be ongoing

Stay below the spam threshold

0.3%

(or below) Spam Rate

Avoid spam by staying below the ‘clear spam rate’ **threshold**

GOOD NEWS! This isn’t new.

Google and Yahoo have always had a spam complaint rate threshold, and the penalty for violation has always been restricted email delivery.

Reduce Complaints

- Manage the registration process to meet future expectations
- Always respect unsubscribe requests
- Make sure your emails are clear and well branded
- Use appropriate mail frequency
- Stay consistent & relevant
- Customize and personalize messaging
- Sunset dormant contacts

Stay below the spam threshold

More resources from Marigold

Supporting you every step of the way

- Contact our Support team, for in-person help and guidance.
- Plan to join our January webinars, where our experts will walk through each step of this process.
- Check out our Help articles, linked below, with more instructions.
  - Authenticate your sending domains
  - Deliverability issues
  - Email authentication
  - DKIM authentication troubleshooting
- Review the appendix slides, included, for even more insight into the new sender requirements.

Appendix

The New Gmail and Yahoo Deliverability Rules

Effective February 2024

Why are Gmail and Yahoo Making this Change?

Gmail and Yahoo seek to deliver messages that consumers want to receive and filter out the messages they don’t.

A pivotal aspect of this involves sender validation using email authentication standards to guarantee the email sender’s identity to prevent malicious actors from exploiting resources.

How is Marigold Responding

- Our team is actively investigating the potential implications from the recent Gmail and Yahoo announcement.
- As a portfolio, we already have several of these requirements fully or partially in place, as we constantly work to offer deliverability best practices.
- We’ll share additional recommendations in the weeks and months ahead.

What Requirements are Changing?

- Authenticate your email using industry standards like SPF, DKIM and DMARC.
- Make it easier for audiences to unsubscribe, using one-click unsubscribe.
- Keep your average spam rates below 0.3%.

Who Needs to Take Action?

Everyone!

If you have contacts with Gmail and Yahoo email addresses in your subscriber and customer lists, this change will impact you.

Also affected are domains that are hard to spot – like those using Google Workspace for custom domains like meetmarigold.com.

Verify your sender identity with standard protocols

1

Set up SPF

Sender Policy Framework **(SPF)** is a mechanism by which a receiving domain can check whether an email has originated from a sending IP that is authorized to send emails on behalf of the admins of a given domain.

Platform specific SPF instructions will be provided.

2

Set up DKIM

DomainKeys Identified Mail **(DKIM)** is a form of email authentication that helps verify that an email's sender address is legitimate and is not being spoofed by a third party.

Platform specific DKIM instructions will be provided.

3

Establish DMARC

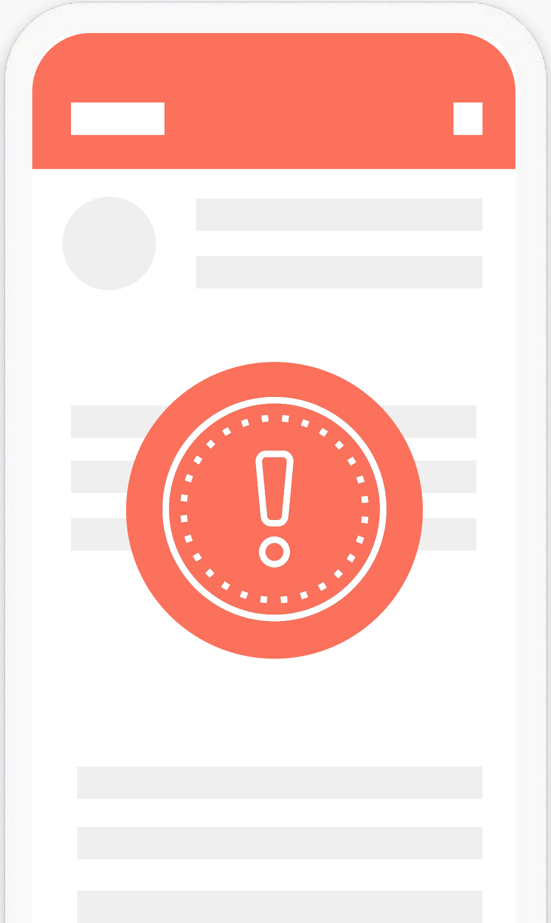
Domain-based Message Authentication Reporting & Conformance **(DMARC)** uses both SPF and DKIM to authenticate email. It lets domain owners choose how receiving servers should manage unauthorized/unauthenticated messages.
Policy = "None"

Don’t send from Gmail.com

Don't impersonate other domains or senders without permission. This practice is called spoofing, and Gmail may mark these messages as spam.

Don’t impersonate Gmail from: headers.

- Gmail will begin using a DMARC quarantine enforcement policy, and impersonating Gmail From: headers might impact your email delivery.
- If you don't own the domain you should not send the email from the domain. Own and authenticate properly.



Thank you!

MARIGOLD™