

Influence Outbound Email Domain Configuration

As of February 1, 2024, many major email providers will have made DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF) authentications mandatory. The primary goal of these authentications is to protect senders and recipients from unwanted emails and reduce spam.

To continue sending emails from your Brandwatch Influence account after the change, you will need to configure your sender domain in Influence and set up a few new records in your domain's domain name system (DNS) provider.

In this article, learn more about the change and how to configure your email domain in Influence.

What is DomainKeys Identified Mail?

DomainKeys Identified Mail is an email authentication method that helps the email recipient verify that an email was indeed sent and authorized by the sender domain, and that it wasn't tampered with in transit.

What is Sender Policy Framework?

Sender Policy Framework is used to authenticate the sender of an email. It protects your domain from spoofing and helps your emails avoid getting delivered to the recipient's spam folder.

What is a custom MAIL FROM domain?

When an email is sent, the MAIL FROM address indicates where the message originated. By setting up a custom MAIL FROM domain, you can use a subdomain of a domain that you own to have emails originating from your domain instead of Amazon Simple Email Service (SES). Custom MAIL FROM domains can be configured with Sender Policy Framework to tell email providers which servers are allowed to send emails from your custom MAIL FROM domain.

Configuring your email domain in Influence

1. Log into your Brandwatch Influence account and go to **Settings > Company > Outbound Email**.

2. Click **Configuration Settings** (available above the outbound email you've added to Influence).

You need to configure this domain. Go to "Configuration Settings" tab and activate DKIM and Custom MAIL FROM domain.

example.com
⚠ Not configured

Emails **Configuration Settings**

Domain Keys Identified Mail (DKIM) is **inactive**

DKIM is a standard email authentication method that adds a digital signature to outgoing messages. Receiving mail servers that get messages signed with DKIM can verify messages actually came from the sender, and not someone impersonating the sender.

[Start DKIM configuration](#)

Custom MAIL FROM domain is **inactive**

Messages sent through Amazon SES will be market as originating from your domain instead of a subdomain of amaozn.com

[Start MAIL FROM configuration](#)

DMARC policy is **missing**

It is recommended to have DMARC policy set to none (p=none) if no policy is specified.

3. Click **Start DKIM configuration**. The DKIM configuration status for this domain will now show as "Pending."

You need to configure this domain. Go to "Configuration Settings" tab and activate DKIM and Custom MAIL FROM domain.

example.com
⚠ Not configured

Emails **Configuration Settings**

Domain Keys Identified Mail (DKIM) is **pending**

DKIM is a standard email authentication method that adds a digital signature to outgoing messages. Receiving mail servers that get messages signed with DKIM can verify messages actually came from the sender, and not someone impersonating the sender.

You must complete the verification process with DKIM authentication by copying the following generated CNAME records to publish to your domain's DNS provider. Detection of these records may take up to 72 hours.

TYPE	NAME	VALUE
CNAME	wngyrqilyzi5qpgi5n3rw7dslqstc2_domainkey.example.com	wngyrqilyzi5qpgi5n3rw7dslqstc2.dkim.amazonses.com
CNAME	uht4jj5oju5ckniaoeidjftcfjoomi2k_domainkey.example.com	uht4jj5oju5ckniaoeidjftcfjoomi2k.dkim.amazonses.com
CNAME	wpoam4igdbreuslyqdpftvkrrzfxahyx_domainkey.example.com	wpoam4igdbreuslyqdpftvkrrzfxahyx.dkim.amazonses.com

Custom MAIL FROM domain is **inactive**

Messages sent through Amazon SES will be market as originating from your domain instead of a subdomain of amaozn.com

[Start MAIL FROM configuration](#)

DMARC policy is **missing**

It is recommended to have DMARC policy set to none (p=none) if no policy is specified.

4. Access your domain's DNS provider and create a new CNAME record.
5. Copy the "Hostname" and "Value" from the first row listed on the DKIM configuration settings tab in your Influence account, and then paste them into the related CNAME fields in your DNS provider.
6. Save and repeat steps 4-5 for the remaining CNAME values. You will need to create three new CNAME records in total for the DKIM configuration.
7. Next, click **Start MAIL FROM configuration** on the Configuration Settings tab in Influence. The Custom MAIL FROM configuration status for this domain will now show as "Pending."

You need to configure this domain. Go to "Configuration Settings" tab and activate DKIM and Custom MAIL FROM domain.

example.com

⚠ Not configured

Emails **Configuration Settings**

Domain Keys Identified Mail (DKIM) is **pending**

DKIM is a standard email authentication method that adds a digital signature to outgoing messages. Receiving mail servers that get messages signed with DKIM can verify messages actually came from the sender, and not someone impersonating the sender.

You must complete the verification process with DKIM authentication by copying the following generated CNAME records to publish to your domain's DNS provider. Detection of these records may take up to 72 hours.

TYPE	NAME	VALUE
CNAME	wngyrqiyzi5qpgi5n3rw7dslqstc2._domainkey.example.com	wngyrqiyzi5qpgi5n3rw7dslqstc2.dkim.amazonses.com
CNAME	uht4jj5oju5ckniaoeidjftcfjoomi2k._domainkey.example.com	uht4jj5oju5ckniaoeidjftcfjoomi2k.dkim.amazonses.com
CNAME	wpoam4igdbreuslyqdpftvkrzfxahyx._domainkey.example.com	wpoam4igdbreuslyqdpftvkrzfxahyx.dkim.amazonses.com

Custom MAIL FROM domain is **pending**

Messages sent through Amazon SES will be marked as originating from your domain instead of a subdomain of amazon.com

To configure this domain as your MAIL FROM, the following MX and SPF records must be copied and published to your domain's DNS provider. Detection of these records may take up to 72 hours.

TYPE	NAME	VALUE
MX	email.example.com	10 feedback-smtp.us-east-1.amazonses.com
TXT	email.example.com	v=spf1 include:amazonses.com -all

DMARC policy is **missing**

It is recommended to have DMARC policy set to none (p=none) if no policy is specified.

8. Access your domain's DNS provider and create a mail exchange (MX) record using the "Hostname" and "Value" found on the Configuration Settings tab in Influence.

Note:

The number "10" listed in the beginning of the MX value is the preference order for the mail server and may need to be entered into a separate value (priority) field when creating the MX record, depending on your DNS provider. If this is the case for you, input "10" in the priority field and then omit the preceding "10" from the value you copied from Influence and paste the remaining string into the MX value field in your DNS provider.

9. Create a new TXT record in Influence using the "Hostname" and "Value" found on the Configuration Settings tab.
10. Once Influence detects that you've created these DNS records correctly, your domain will display as "Configured" on the Outbound Settings page in Influence.

The screenshot displays the 'Company' settings page in Influence, with the 'Outbound Email' tab selected. The page shows two domains: paladinsoftware.com and brandwatch.com, both marked as 'Configured'.

paladinsoftware.com

✓ Configured

Buttons: Emails, Configuration Settings

VERIFIED SENDER E-MAIL	NAME	SENDER E-MAIL FOR	UPDATED	STATUS
support@paladinsoftware.com	Paladin Software	CAMPAIGNS PAYMENTS INFLUENCERS	Jun 19, 2018	✓ Verified

brandwatch.com

✓ Configured

Buttons: Emails, Configuration Settings

VERIFIED SENDER E-MAIL	NAME	SENDER E-MAIL FOR	UPDATED	STATUS
influence-support@brandwatch.com	Brandwatch Influence		Jan 25, 2024	Initial

In the Configuration Settings tab, you will also see a section for "DMARC Policy" (Domain-based Message Authentication, Reporting, and Conformance). No action is required here, unless your domain sends over 5,000 emails per day, but it's recommended to set up a DMARC record in your DNS provider and have the policy set to "None."