Addressing Alignment Issues

https://campus.barracuda.com/doc/90442894/

DMARC Alignment Overview

DMARC performs an alignment check to validate the From domain for an email with the email's SPF or DKIM domain. This check ensures that the email is being sent from a valid source. DMARC alignment has the following possible outcomes:

- **Pass** – if either the SPF or DKIM domains align.
- **Fail** – if the source for the email does not sign the SPF or DKIM signature with your domain.

Alignment via SPF

The following sample email would pass/align for SPF.

Notice the domains in green are the same for both the **Mail From** and **From** fields.

Mail From: <sending_address@ **example.com**>
From: sending_address@ **example.com**
Date: Fri, Feb 15 2022
To: receiving_address@example.org
Subject: This email will pass DMARC via SPF

The following chart shows how SPF failure and alignment failure affect DMARC failure. The email in this section falls under Row 1.

	SPF Domain	SPF Alignment	DKIM Domain	DKIM Alignment	DMARC Result
1	PASS	PASS			PASS
2	PASS	FAIL			FAIL
3	FAIL	FAIL			FAIL

Alignment via DKIM

The following sample email would pass/align for DKIM.

Notice the domains shown in green are identical for the **DKIM d-Parameter**, **Return-Path**, and **From** fields.

DKIM d-Parameter: **example.com**
Return-Path: LQGtWLKekefgheNTPMCq@bounces.marketing.**example.com**
Mail From: sending_address@marketingcompany.com
From: sending_address@ **example.com**
Date: Fri, Feb 15 2022
To: receiving_address@example.org
Subject: This email will pass DMARC via DKIM

The following chart shows The following chart shows how DKIM failure and alignment failure affect DMARC failure. The email in this section falls under Row 1.

	SPF Domain	SPF Alignment	DKIM Domain	DKIM Alignment	DMARC Result
1			PASS	PASS	PASS
2			PASS	FAIL	FAIL
3			FAIL	FAIL	FAIL

Alignment via Both SPF and DKIM

The following sample email would pass/align for both SPF and DKIM.

Notice the domains shown in green are identical for the **DKIM d-Parameter**, **Return-Path**, **Mail From**, and **From** fields.

DKIM d-Parameter: **example.com**
Return-Path: LQGtWLKekefgheNTPMCq@bounces.marketing.**example.com**
Mail From: sending_address@ **example.com**
From: sending_address@ **example.com**
Date: Fri, Feb 15 2022
To: receiving_address@example.org
Subject: This email will pass DMARC via SPF && DKIM

The following chart shows The following chart shows how SPF failure, DKIM failure, and alignment failure affect DMARC failure. The email in this section falls under Row 1.

	SPF Domain	SPF Alignment	DKIM Domain	DKIM Alignment	DMARC Result
1	PASS	PASS	PASS	PASS	PASS
2	PASS	PASS	PASS	FAIL	PASS
3	PASS	PASS	FAIL	FAIL	PASS
4	PASS	FAIL	PASS	PASS	PASS
5	FAIL	FAIL	PASS	PASS	PASS
6	FAIL		FAIL		FAIL
7	PASS	FAIL	PASS	FAIL	FAIL
8	FAIL	FAIL	PASS	FAIL	FAIL
9	PASS	FAIL	FAIL	FAIL	FAIL

Addressing Alignment Issues

This section includes ideas to help you address issues with DMARC alignment.

Only SPF or DKIM Configured

If you have *only* SPF *or* DKIM configured, configure the other as well.

You can see in the charts above that if you are able to configure *both* SPF *and* DKIM for your approved sources, your success rate for DMARC increases. There are more opportunities where DMARC will pass because there are more checks and combinations of potential results.

Your source provider might make DMARC alignment difficult for you in the following ways:

1. The provider does not allow for both SPF and DKIM protocols
2. Neither SPF or DKIM allow you to sign with your domain

Most large and reputable sources are aware of the workings of DMARC and will have at least one protocol available to you. It is possible, though, that they might have only one protocol that actually will sign with your domain. When initially choosing and later choosing to renew with a source, strongly consider its policies on DMARC alignment requirements and its commitment to helping you protect your domain reputation.

Both SPF and DKIM Configured

Examine how the source is implementing SPF and DKIM. Reach out to your source to learn more.

1. They might not be signing any of your emails with your domain. This would cause an alignment failure. As described above, strongly consider the source's policies on DMARC alignment requirements and its commitment to helping you protect your domain reputation when initially choosing and later choosing to renew with a source.
2. There might be multiple SPF or DKIM records that could be signing the email with another domain.