Domain Authentication in Office 365

Last Modified on 23/01/2020 2:31 pm GMT

In order to ensure emails are coming from the sender it says it is from, Office 365 utilises a number of Domain Authentication checks against inbound emails to the Exchange Online service. This is to help combat the common practice of Spoofing, where a sender impersonates another domain by email.

SPF – This is a record added to the sending domain that specifies which servers the emails for that domain should originate from.

DKIM – This is a digital signature that can be used to confirm an email originated from the correct domain and to confirm if an email was modified after leaving the sender's servers.

DMARC – This expands on the SPF & DKIM policies to check if an email has originated from a legitimate source.

Whilst these checks are considered as part of a spam filtering process, passing these checks is only a means to confirm the email is from a certain domain. They should not be used to decide if an email is not spam.

It is important to note when understanding Domain Authentication that emails utilise two FROM addresses. In most cases, these will be the same, but there are legitimate use cases for these to differ.

Envelope From: This is the email address used by email systems when handling the message. This is often referred to as the 'True' sender.

Header From: This is the From address you will see in an application like Outlook. This is who the email should be from.

SPF

When a sender is using SPF for their emails, they will have published a record on their domain containing details of the servers where emails should originate from.

When SPF checks are applied, the receiving server will check the source of the email against the SPF record for the sending domain. One of the following results will be given:

SPF None – The sender does not publish an SPF record

SPF PermError – The sender has an invalid SPF record published

SPF SoftFail – The IP address of the sender was not published in the SPF record of the sender & the sender's SPF record requests a SoftFail (SPF record ends with ~all)

SPF HardFail - The IP address of the sender was not published in the SPF record of the sender & the sender's SPF record requests a HardFail (SPF record ends with -all)

SPF Pass – The IP address of the sender is in the published SPF record of the sender

SPF operates against the **Envelope From** address of an email. As such, these checks are not always applied against the email address the email looks to be from.

Inbound Emails

The Exchange Online Protection service used by Exchange Online & Office 365 handles SPF checks as part of it's spam filtering. When an email fails SPF checks, it will commonly be marked as spam and handled according to your organisation's spam filter settings.

Outbound Emails

You don't need to enable anything in Office 365 for outbound SPF, as this is published on your domain.

If you use Office 365 for emails and have an SPF record published on your domain, you should ensure Office 365 is included in your record. The default SPF record for Office 365 is:

Type: TXT
Hostname: @ (or blank if not supported)
Value: v=spf1 include:spf.protection.outlook.com -all
TTL: 3600

If you have other email systems outside of Office 365, such as an email marketing

system or web form, the above record should be modified to include this. You should check with the provider for those systems what details will need to be included. You should only have 1 SPF record on your domain of less than 10 lookups against other domains.

DKIM

The functions of DKIM can generally be broken into two parts:

Firstly, the sending server will take the information about the email and put it through an algorithm to generate a string of text, known as a hash. Given the same email data and algorithm, this will always turn out the same, until the email data is changed.

Secondly, a set of encryption keys are used against that hash. This set of keys includes a Private Key, known only to the sender, and a Public Key, that the sender publishes on their domain. The Public Key can be used to reverse encryption that uses the Private Key.

When an email is DKIM signed, the hash is generated and encrypted with the Private Key. The end result is sent alongside the email with the details on where the Public Key can be found and how the hash was generated.

When the same email arrives at the receiving server, the hash is generated again and the DKIM signature is decrypted using the Public Key. These are them compared and a result of the check will be given:

DKIM Fail: The newly generated hash did not match the decrypted signature

DKIM Pass: The newly generated hash matched the decrypted signature

When an email passes DKIM checks, it can be used as a form of confirmation that the email came from the domain the Public Key is hosted against. It should not be used as a form of spam scanning, but rather for additional verification of the sending address. It can also be used to check if the email was modified after it was sent by the sender.

Inbound Emails

DKIM is supported by Exchange Online, but a Mail Flow Rule must be configured to determine how to handle these emails.

Outbound Emails

By default, Exchange Online will generate a DKIM signature using your tenant domain (your .onmicrosoft.com domain). You can switch which domain is used in the Exchange Admin Center. Before you can enable DKIM signing on a domain, you must add the required records for the Public Key.

You should not have Exchange Online DKIM sign your emails if you use an email gateway such as Mimecast or Messagelabs. DKIM signatures should always be applied by the last hop in your email infrastructure.

DMARC

DMARC extends the functions of SPF and DKIM by requiring them to align to the sending address, known as SPF Alignment & DKIM Alignment.

SPF Alignment occurs when the Envelope From and Header From addresses match.

DKIM Alignment occurs when the signing domain matches the Header Form address.

When this alignment fails, DMARC checks will result in a failure.

When a sender is using DMARC, they will publish a record onto their domain instructing how to handle emails that fail the checks. One of the following instructions will be given:

P=none – Ignore the results of the failure

P=quarantine – Handle the email as spam

P=reject – Block and delete the email

Inbound Emails

DMARC is honoured by Exchange Online automatically. However, it handles both Quarantine and Reject requests the same, handling them both as spam.

Outbound Emails

Nothing is needed in Exchange Online to enable this for your domain, you will need to publish a DMARC record on your domain.

If you use other email systems other than Office 365, you should first check they are compatible. If you use a bulk emailing system, it is generally recommended to switch this to a subdomain when implementing DMARC, which should have it's own DMARC record for no action.

FAQ

"I Have Set Up SPF/DKIM/DMARC but a Recipient Still Accepted a Spoofed Email From My Domain"

It is up to the recipient server how they handle these checks, having these in place only gives the recipient a means to perform them.