Aon Assessment Email Solution Setup

DNS Administrators' Guide

12.05.2020

Empower Results®

1. Summary

When using Aon Assessment's web applications to send emails under your company email address, a few configuration steps in your company DNS are required. These configurations ensure that your emails reliably reach their recipients and are not marked as spam. It also helps with protecting Aon's mail servers from being blacklisted by major email providers.

It is important to authorize Aon's mail servers for sending emails under your company domain by including them in your SPF record (see 2.). Optionally, you may also enable DKIM signing by creating CNAME records that point to your Aon-managed DKIM key set (see 3.).

2. SPF Configuration

A SPF record is a specially formatted TXT record. It lists the servers that are authorized to send emails for its domain. You can include Aon's email system in three different ways. Only one of these options below has to be configured, depending on your preference:

2.1 Include a DNS record

Aon provides a SPF record for the application email systems under the hostname

spf.mail.aas.services.

By using the include statement, you can add it to your SPF record:

Type	Record Location	Value
TXT	<*sender domain*>	"v=spf1 <*your authorized mail servers*> include:spf.mail.aas.services -all"

2.2 Include the IP addresses

To verify the record that is shown above, requires a DNS lookup, creating network traffic and a small latency on the receiving system. The SPF standard also allows for only ten DNS lookups during a verification cycle. Hence, you might prefer to include the IP addresses directly:

Type	Record Location	Value
TXT	<*sender domain*>	"v=spf1 <*your authorized mail servers*> ip4:20.40.137.116 ip4:20.40.137.117 ip4:20.40.137.118 ip4:20.40.137.119 ip4:20.40.137.120 ip4:20.40.137.121 ip4:20.40.137.122 ip4:20.40.137.123 ip4:20.40.137.124 ip4:20.40.137.125 ip4:20.40.137.126 ip4:20.40.137.127 -all"

2.2 Include the subnets

If you want to include IP addresses instead of a DNS record, but prefer a shorter notation, you may include the subnets as CIDR blocks:

Type	Record Location	Value
TXT	<*sender domain*>	"v=spf1 <*your authorized mail servers*> ip4:20.40.137.116/30 ip4:20.40.137.120/29 -all"

Please take extra care in checking the subnet mask, in order to not authorize illegitimate IP addresses. Instead of specifying the two subnets, you can also refer to just the network 20.40.137.112/28. It contains four additional addresses that will not be used for sending emails but are also under the control of Aon and can be included safely.

3. DKIM Configuration

The DKIM configuration allows Aon to add a digital signature to the emails. The signature can be verified by the recipient via a public key which is stored in the DNS, to confirm the authenticity of the message.

3.1 Create CNAME records

Since DKIM requires an active key management that affects the mail server configuration as well as the DNS, the public keys are not published in the client DNS directly. Instead, we kindly ask you to set up CNAME records that point to your key sets:

Type	Record Location	Value
CNAME	aas.1._domainkey.<*sender domain*>	dkim.<*sender domain*>.1.aas.services.
CNAME	aas.2._domainkey.<*sender domain*>	dkim.<*sender domain*>.2.aas.services.
CNAME	aas.3._domainkey.<*sender domain*>	dkim.<*sender domain*>.3.aas.services.

All installed keys are domain-specific; please do not point CNAME records for different sender domains to the same keys, since this will not be reflected by Aon's server configuration. The example below shows a correct configuration for two sender domains:

Type	Record Location	Value
CNAME	aas.1._domainkey.contoso.com	dkim.contoso.com.1.aas.services.
CNAME	aas.2._domainkey.contoso.com	dkim.contoso.com.2.aas.services.
CNAME	aas.3._domainkey.contoso.com	dkim.contoso.com.3.aas.services.
CNAME	aas.1._domainkey.contoso.co.uk	dkim.contoso.co.uk.1.aas.services.
CNAME	aas.2._domainkey.contoso.co.uk	dkim.contoso.co.uk.2.aas.services.
CNAME	aas.3._domainkey.contoso.co.uk	dkim.contoso.co.uk.3.aas.services.

Please note that the DKIM selector, being part of an automated solution, cannot be customized.

3.2 Request DKIM setup

When you have created the CNAME records, please notify your local Aon Assessment Solution contact. Aon will then create the DKIM configuration on its servers and DNS and verify proper operation. No further action on your end is required.

4. How Aon Assessment manages DKIM keys

For security reasons, and to avoid dependencies between clients and client entities, individual DKIM keys are managed for each sender domain. The keys are 2048-bit RSA keys, created by *opendkim-genkey*.

Three key pairs are used in order to accommodate for delays in DNS replication and signature verification: One active, one future and one past key pair. Keys are rotated every three months. Therefore, a single key pair persists in the DNS and on the mail server for a total of nine months, which is considered acceptable for the given key length.

The renewal follows this process:

When a sender domain is first enrolled to the email system, three key pairs with the selectors *aas.1*, *aas.2* and *aas.3* are generated and registered in the DNS (creating the complete set right at the beginning allows to check for DNS configuration errors). The key with the selector *aas.1* is put in active use on the mail server.

During the first renewal cycle after a maximum of three months, the mail server configuration is changed to use key *aas.2*, while the future key *aas.3* is recreated on the system and in the DNS. The decommissioned key *aas.1* is left in the DNS.

With the next renewal cycle, the system moves to key *aas.3* for message signing and refreshes *aas.1*. After additional three months, the system switches to *aas.1* and renews *aas.2*, and so on.