Amazon Simple Email Service (SES)

Configuring Email Authentication for Third-Party Controlled Domain Identities

Contents

Introduction 2

Important Information Highlights 2

Process Overview 3

Step 1 – Selecting a Domain 3

Step 2 – Creating a Domain Identity 5

Domain Identity Creation Process 5

Step 3 – Verifying Control Over a Domain via DKIM 8

DKIM configuration verification & DNS record setup process 8

Step 4 – Configuring SPF authentication 11

SPF configuration verification & DNS record setup process 11

STEP 5 – DNS record publishing to configure DMARC 13

DNS record formats 13

DNS record publishing process 14

Appendix 16

DMARC setup verification 16

References 17

Introduction

To send emails via Amazon Simple Email Service (SES) a *verified identity* must be configured and used to specify the "from" / "sender" / "source" address of outbound emails.

Historic regulations

It was previously possible to simply register and verify individual sender email addresses in the SES control panel, but as large email server operators implement more modern security policies this is no longer sufficient.

Current regulations

When these identities are registered on domains (the part of the email address after the @ symbol) outside the direct control of the SES administrator these shall be referred to in this document as *third-party controlled domain identities* for third-party sender domains.

These domain operators/controllers must explicitly grant permissions for Amazon to act on the behalf of the domain when sending emails to ensure secure, reliable delivery occurs. This is part of an industry-wide process underway to prevent email spoofing and reduce spam. [2]

To successfully deliver emails from third-party sender domains into inboxes on modern and well-configured mail servers it is necessary to implement and conform to Domain-based Message Authentication, Reporting & Conformance (DMARC) standards. [1]

This means configuring Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) on the domain specified as the sender and aligning these with settings in the SES control panel.

This is a task which, by design, must be performed (in part) by the operator/controller of the third-party sender domain. They must explicitly grant permission for Amazon SES to send emails as though the emails originated directly from the third-party sender domain.

Important Information Highlights

- **SPF, DKIM and DMARC are all now required for reliable mail delivery**
- **A domain identity must be used in SES to configure these; individual verified email addresses cannot have DKIM or DMARC configured on them**
- **DNS records must be updated to configure SPF, DKIM and DMARC; the domain operator/controller must take part in this process**
- **The domain operator/controller must consent to SES sending emails on behalf of their domain – some domain operators (e.g. Google) cannot do this**
- **The domain operator/controller must fully and correctly update their domain records to grant SES permission to send emails on the behalf of their domain**

Process Overview

There are five steps that must be performed to complete this process. Some steps must be performed by an SES administrator, some by the third-party sender domain operator/controller.

In the case a step has already been performed (such as creation of a domain identity – but without configuration of DKIM being completed) simply proceed to the next step.

	SES administrator	Domain operator/controller
1. Select a domain to use as a third-party sender domain, on which the operator/controller is willing and able to complete the required DNS system configuration changes.		Y
2. Create a domain identity in the SES control panel for this domain.	Y	
3. Verify control over this domain:		
i. Use *Amazon Easy DKIM* to generate a 2048-bit RSA signing key.	Y	
ii. Configure DKIM on the domain by adding the SES provided CNAME records to the DNS entry for this domain – this can be performed separately but is described in Step 5.		Y
4. Specify a "Custom MAIL FROM domain" in SES:		
i. Configure SPF on a subdomain (recommended: *sesmail.<domain.tld>*) in SES.	Y	
ii. Add the SES provided MX and TXT records to the DNS entry for this domain – this can be performed separately but is described in Step 5.		Y
5. Configure DMARC on the domain by adding the SES provided DNS records (for SPF, DKIM and DMARC – as required) to the DNS entry for this domain.		Y

Step 1 – Selecting a Domain

It is only possible to complete the DMARC configuration process for identities registered to third-party sender domains over which the SES administrator can have permission be granted for Amazon SES to send emails on behalf of users/mailboxes.

NB: It will not be possible to set up fully verified identities and send emails from domains which are operated by significant service providers, e.g.: Google, The NHS, Yahoo, because they (correctly) will not grant this permission to systems outside their control.

SES system users who have currently configured sender identities with an address on one of these externally controlled domains will find very few emails can be delivered and the system user will need to migrate their chosen identities and begin sending from a domain they can configure permissions for via DNS record changes.

Step 2 – Creating a Domain Identity

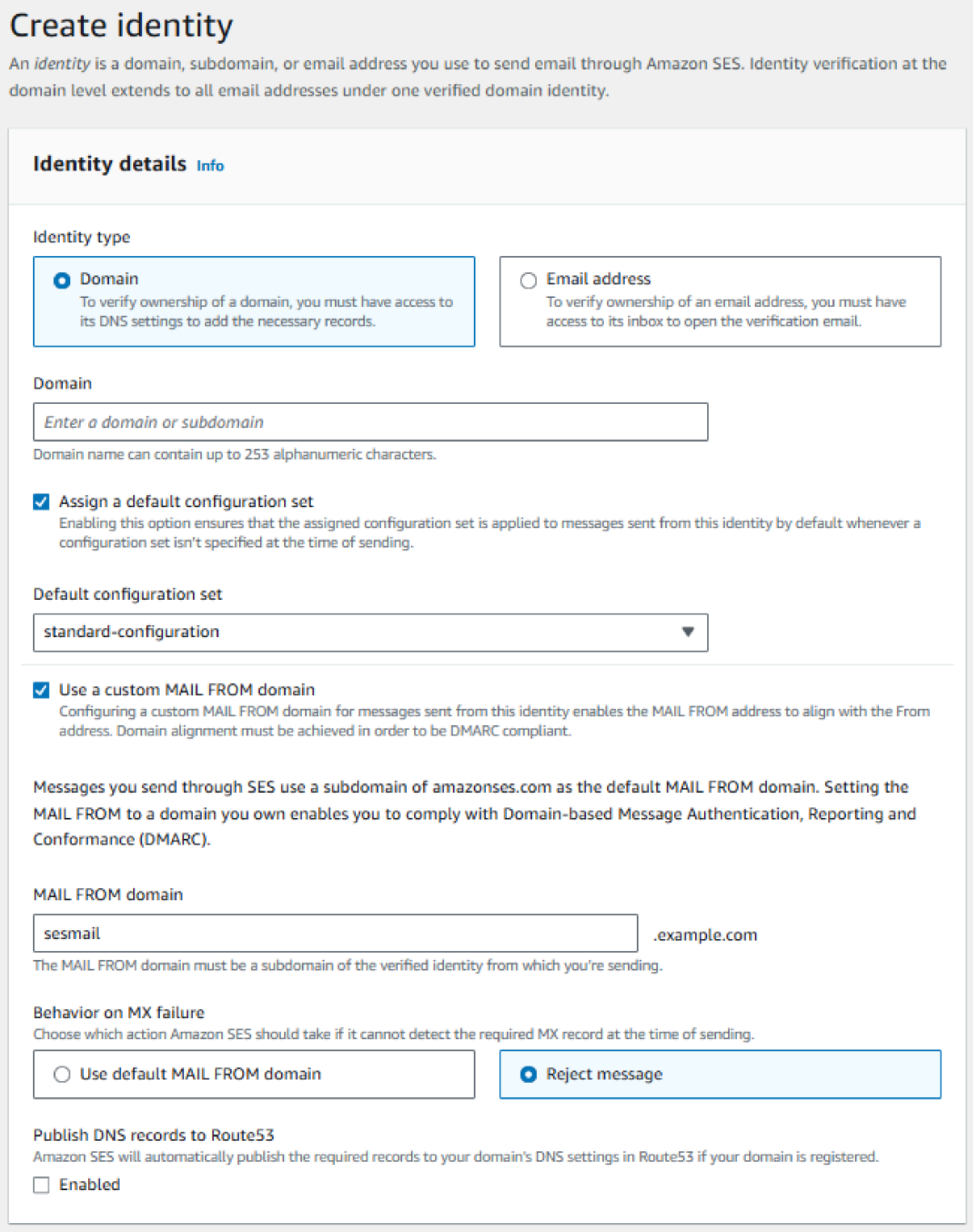
When creating a Domain Identity, it is possible (and straightforward) to set up both DKIM and SPF at identity creation time. The appropriate DNS records can be added to the configured domain immediately afterwards and SES will verify the domain when these record changes propagate through the global DNS system (this may take 48 hours but is usually much quicker – often within an hour)

Domain Identity Creation Process

1. Navigate to Amazon SES, selecting the appropriate region for the account.
2. In the left-hand menu, under "Configuration" select "Identities".
3. Click the "Create identity" button, top right.
4. In the "Identity details" section:
    I. Choose the "Domain" option, top left.
    II. Enter the name of the selected third-party sender domain.
    III. A default configuration set should be provided by the Amazon SES account administrator – this is to simplify capture of failure notifications e.g. mail bounce reports. Tick the "Assign a default configuration set" box and use the drop-down menu to select the supplied configuration set name. Creation and management of configuration sets is outside the scope of this document.
    IV. Tick the "Use a custom MAIL FROM domain box and enter the chosen mail subdomain (recommended: *sesmail*).
5. In the "Verifying your domain" section:
    I. Open the "Advanced DKIM settings" subpanel.
    II. Choose the "Easy DKIM" option, on the left.
    III. For the DKIM signing key length, choose: `RSA_2048_BIT`.
    IV. Ensure the DKIM signatures checkbox is enabled.
6. At the bottom of the page, click "Create identity" to complete identity creation.

Example images of this process underway are provided below:

Fig 1: Identity creation – Identity details



Create identity

An *identity* is a domain, subdomain, or email address you use to send email through Amazon SES. Identity verification at the domain level extends to all email addresses under one verified domain identity.

Identity details Info

Identity type

● Domain
To verify ownership of a domain, you must have access to its DNS settings to add the necessary records.

○ Email address
To verify ownership of an email address, you must have access to its inbox to open the verification email.

Domain

Enter a domain or subdomain

Domain name can contain up to 253 alphanumeric characters.

☑ Assign a default configuration set
Enabling this option ensures that the assigned configuration set is applied to messages sent from this identity by default whenever a configuration set isn't specified at the time of sending.

Default configuration set

standard-configuration ▼

☑ Use a custom MAIL FROM domain
Configuring a custom MAIL FROM domain for messages sent from this identity enables the MAIL FROM address to align with the From address. Domain alignment must be achieved in order to be DMARC compliant.

Messages you send through SES use a subdomain of amazonses.com as the default MAIL FROM domain. Setting the MAIL FROM to a domain you own enables you to comply with Domain-based Message Authentication, Reporting and Conformance (DMARC).

MAIL FROM domain

sesmail .example.com

The MAIL FROM domain must be a subdomain of the verified identity from which you're sending.

Behavior on MX failure
Choose which action Amazon SES should take if it cannot detect the required MX record at the time of sending.

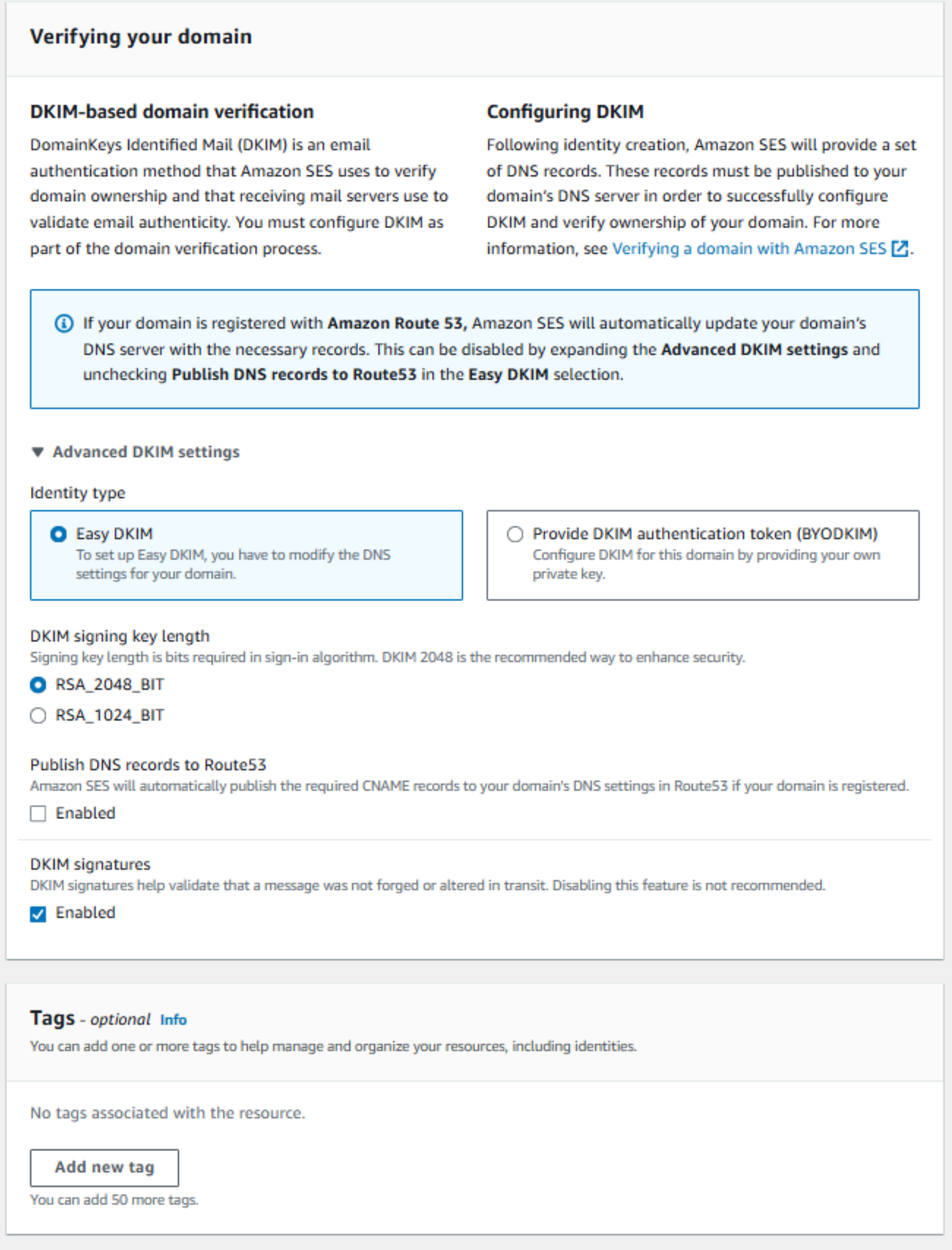
○ Use default MAIL FROM domain

● Reject message

Publish DNS records to Route53
Amazon SES will automatically publish the required records to your domain's DNS settings in Route53 if your domain is registered.

□ Enabled

Fig 2: Identity creation – Verifying your domain



Verifying your domain

DKIM-based domain verification

DomainKeys Identified Mail (DKIM) is an email authentication method that Amazon SES uses to verify domain ownership and that receiving mail servers use to validate email authenticity. You must configure DKIM as part of the domain verification process.

Configuring DKIM

Following identity creation, Amazon SES will provide a set of DNS records. These records must be published to your domain's DNS server in order to successfully configure DKIM and verify ownership of your domain. For more information, see Verifying a domain with Amazon SES.

ⓘ If your domain is registered with **Amazon Route 53,** Amazon SES will automatically update your domain's DNS server with the necessary records. This can be disabled by expanding the **Advanced DKIM settings** and unchecking **Publish DNS records to Route53** in the **Easy DKIM** selection.

▼ Advanced DKIM settings

Identity type

● Easy DKIM
To set up Easy DKIM, you have to modify the DNS settings for your domain.

○ Provide DKIM authentication token (BYODKIM)
Configure DKIM for this domain by providing your own private key.

DKIM signing key length
Signing key length is bits required in sign-in algorithm. DKIM 2048 is the recommended way to enhance security.

● RSA_2048_BIT
○ RSA_1024_BIT

Publish DNS records to Route53
Amazon SES will automatically publish the required CNAME records to your domain's DNS settings in Route53 if your domain is registered.

□ Enabled

DKIM signatures
DKIM signatures help validate that a message was not forged or altered in transit. Disabling this feature is not recommended.

☑ Enabled

Tags - *optional* Info
You can add one or more tags to help manage and organize your resources, including identities.

No tags associated with the resource.

You can add 50 more tags.

This process guide assumes the sender domain is under third party control and operation, and so the “Publish DNS records to Route53” boxes can have no effect.

Step 3 – Verifying Control Over a Domain via DKIM

For verification of domain control, DKIM must be configured with matching values in both SES and some DNS records on the third-party sender domain.

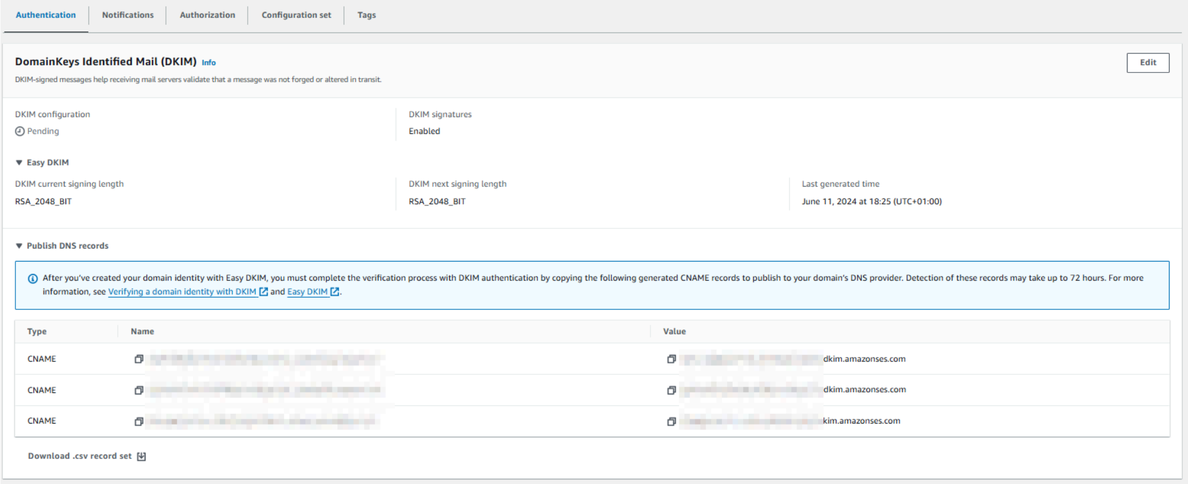
If the domain was created in line with Step 2 in this document then DKIM is already configured correctly in SES and only DNS record setup needs to be performed.

DKIM configuration verification & DNS record setup process

1. Navigate to Amazon SES, selecting the appropriate region for the account.
2. In the left-hand menu, under “Configuration” select “Identities”.
3. Select the domain identity to verify (click the underlined domain name entry).
4. Verify settings in the “Authentication” tab, in the “DomainKeys Identified Mail” panel:
   (If any of these are incorrectly configured, click the “Edit” button top right. Make and save the required configuration changes on the “Edit DKIM settings” page)
   I. Verify DKIM signatures are set to Enabled.
   II. Verify Easy DKIM is being used and there is an “Easy DKIM” toggle to view DKIM signing settings.
   III. Open the “Easy DKIM” subpanel and verify DKIM signing length is `RSA_2048_BIT`.
5. Collect DNS record entries from the “Authentication” tab, in the “DomainKeys Identified Mail” panel:
   I. Open the “Publish DNS records” subpanel.
   II. Copy the provided CNAME record names and values for later use. There should be three (3) records listed and all of them should be published to the domain.
6. Go to the DNS management console / system for the domain to be verified.
   (Examples of DNS management systems provided in Step 5)
7. Create new CNAME DNS records for the domain, using the provided names and values generated by Amazon SES Easy DKIM.
8. Save these record changes. It may take 48 hours for this to propagate through the global DNS system but the process is usually much quicker.
9. Periodically check the Amazon SES Identities page until the Identity status for this domain shows as “Verified”.

If domain a verification shows as “Failed” in the SES Identities page, this generally means that DKIM record detection has timed out – perhaps because signatures were created previously but CNAME records were not published to the domain as required. Ensure CNAME records have been correctly published to the domain.

Fig 3: Domain verification – DKIM verification pending



DomainKeys Identified Mail (DKIM) Info

DKIM-signed messages help receiving mail servers validate that a message was not forged or altered in transit.

DKIM configuration: Pending

DKIM signatures: Enabled

▼ Easy DKIM

DKIM current signing length: RSA_2048_BIT

DKIM next signing length: RSA_2048_BIT

Last generated time: June 11, 2024 at 18:25 (UTC+01:00)

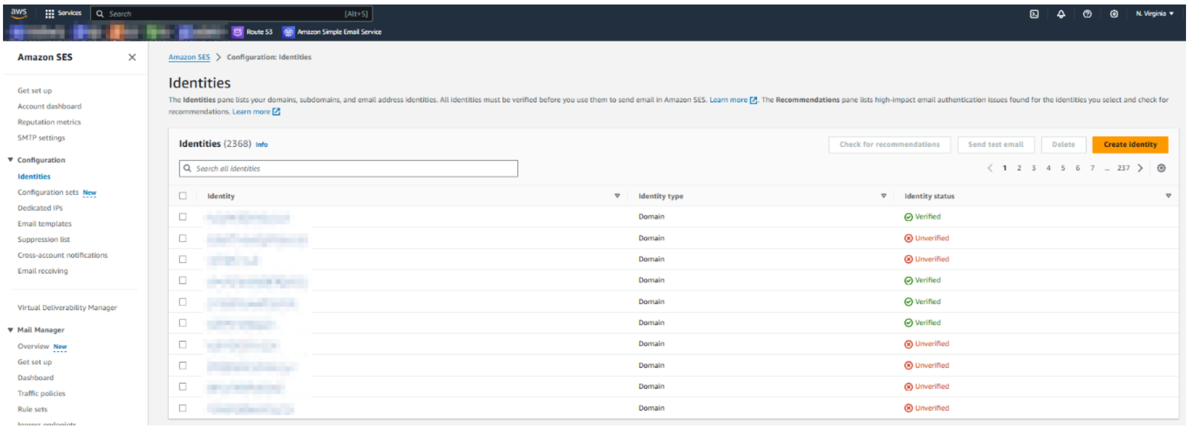
▼ Publish DNS records

After you've created your domain identity with Easy DKIM, 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. For more information, see Verifying a domain identity with DKIM and Easy DKIM.

Type	Name	Value
CNAME	[redacted]	[redacted]dkim.amazonses.com
CNAME	[redacted]	[redacted]dkim.amazonses.com
CNAME	[redacted]	[redacted]kim.amazonses.com

Download .csv record set

Fig 4: Domain verification – Domain identities verification status



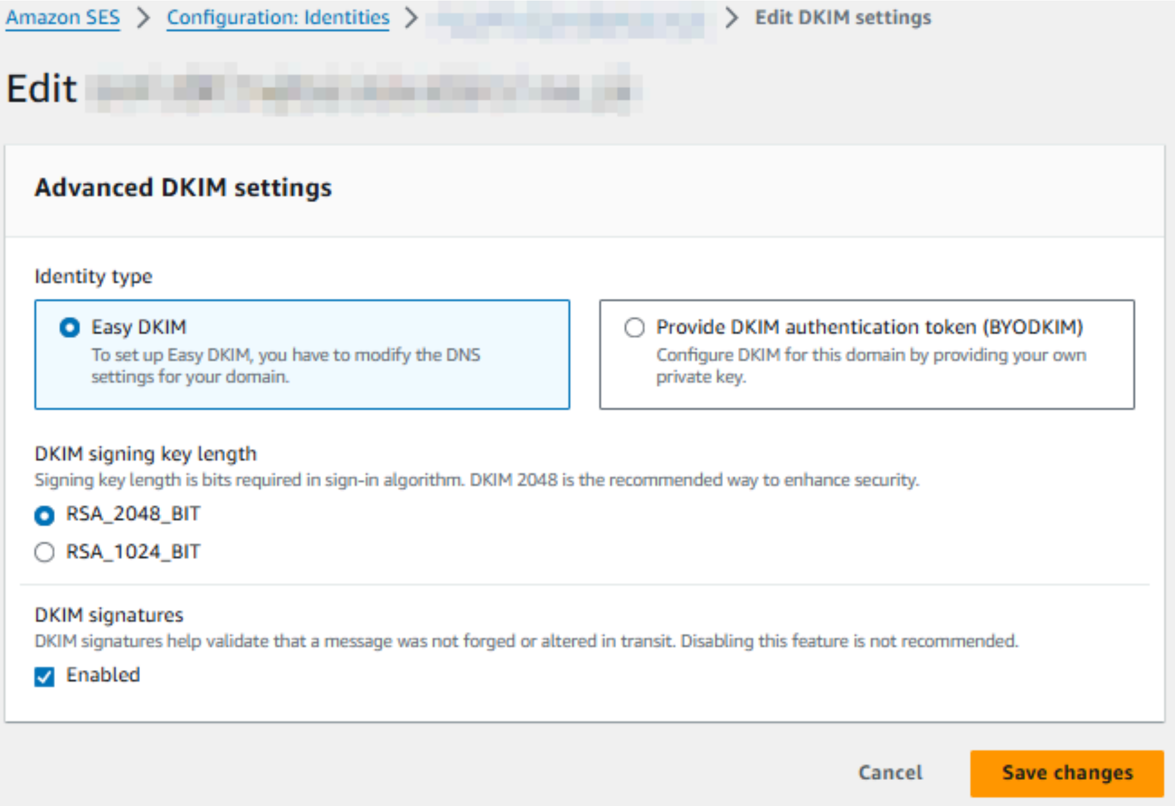
Identities

The **Identities** pane lists your domains, subdomains, and email address identities. All identities must be verified before you use them to send email in Amazon SES. Learn more. The **Recommendations** pane lists high-impact email authentication issues found for the identities you select and check for recommendations. Learn more

Identities (2368) Info

□	Identity	Identity type	Identity status
□	[redacted]	Domain	Verified
□	[redacted]	Domain	Unverified
□	[redacted]	Domain	Unverified
□	[redacted]	Domain	Verified
□	[redacted]	Domain	Verified
□	[redacted]	Domain	Verified
□	[redacted]	Domain	Unverified
□	[redacted]	Domain	Unverified
□	[redacted]	Domain	Unverified
□	[redacted]	Domain	Unverified

Fig 5: DKIM configuration – Edit DKIM settings page



Amazon SES > Configuration: Identities > [redacted] > Edit DKIM settings

Edit [redacted]

Advanced DKIM settings

Identity type

● Easy DKIM
To set up Easy DKIM, you have to modify the DNS settings for your domain.

○ Provide DKIM authentication token (BYODKIM)
Configure DKIM for this domain by providing your own private key.

DKIM signing key length
Signing key length is bits required in sign-in algorithm. DKIM 2048 is the recommended way to enhance security.

● RSA_2048_BIT
○ RSA_1024_BIT

DKIM signatures
DKIM signatures help validate that a message was not forged or altered in transit. Disabling this feature is not recommended.

☑ Enabled

Step 4 – Configuring SPF authentication

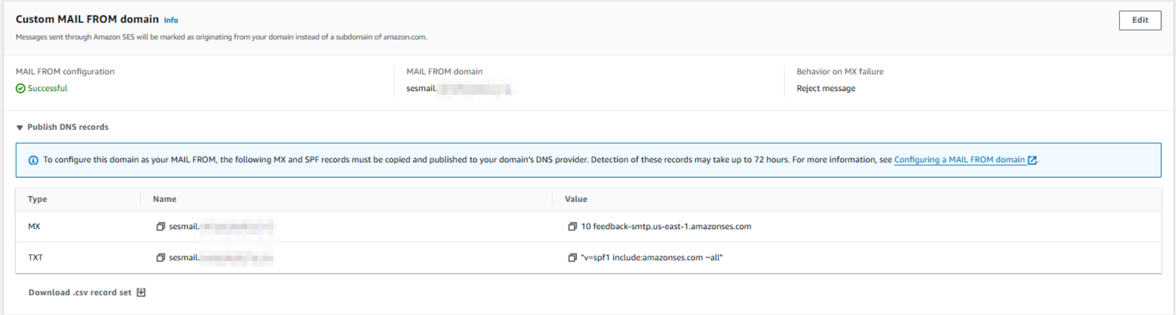
For authentication of email sending permission for a third-party sender domain, SPF must be configured on a subdomain of the third-party sender domain. This must be configured to permission for Amazon SES to send emails on the behalf of this domain.

If the domain was created in line with Step 2 in this document then a custom MAIL FROM subdomain is already configured correctly in SES and only DNS record setup needs to be performed.

SPF configuration verification & DNS record setup process

1. Navigate to Amazon SES, selecting the appropriate region for the account.
2. In the left-hand menu, under “Configuration” select “Identities”.
3. Select the domain identity to configure (click the underlined domain name entry).
4. Verify settings in the “Authentication” tab, in the “Custom MAIL FROM domain” panel:
   (If any of these are incorrectly configured, click the “Edit” button top right. Make and save the required configuration changes on the “Edit custom MAIL FROM domain” page.)
   I. Verify a custom MAIL FROM domain has been configured.
5. Collect DNS record entries from the “Authentication” tab, in the “Custom MAIL FROM domain” panel:
   I. Open the “Publish DNS records” subpanel.
   II. Copy the provided MX and TXT record names and values for later use. There will be one (1) of each record type listed.
6. Go to the DNS management console / system for the domain to be verified.
7. Create a new MX DNS record for the subdomain, using the provided value, to configure a return path for email to Amazon SES in the correct region.
8. Create a new TXT DNS record for the subdomain, using the provided value, to configure SPF on this subdomain granting SES authorisation to send emails from the subdomain.
9. Save these record changes. It may take 48 hours for this to propagate through the global DNS system but the process is usually much quicker.
10. Periodically check the Configuration Identity page until the MAIL FROM configuration status for this domain shows as “Successful”.

Fig 6: SPF verification – SPF configuration successful



Custom MAIL FROM domain Info

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

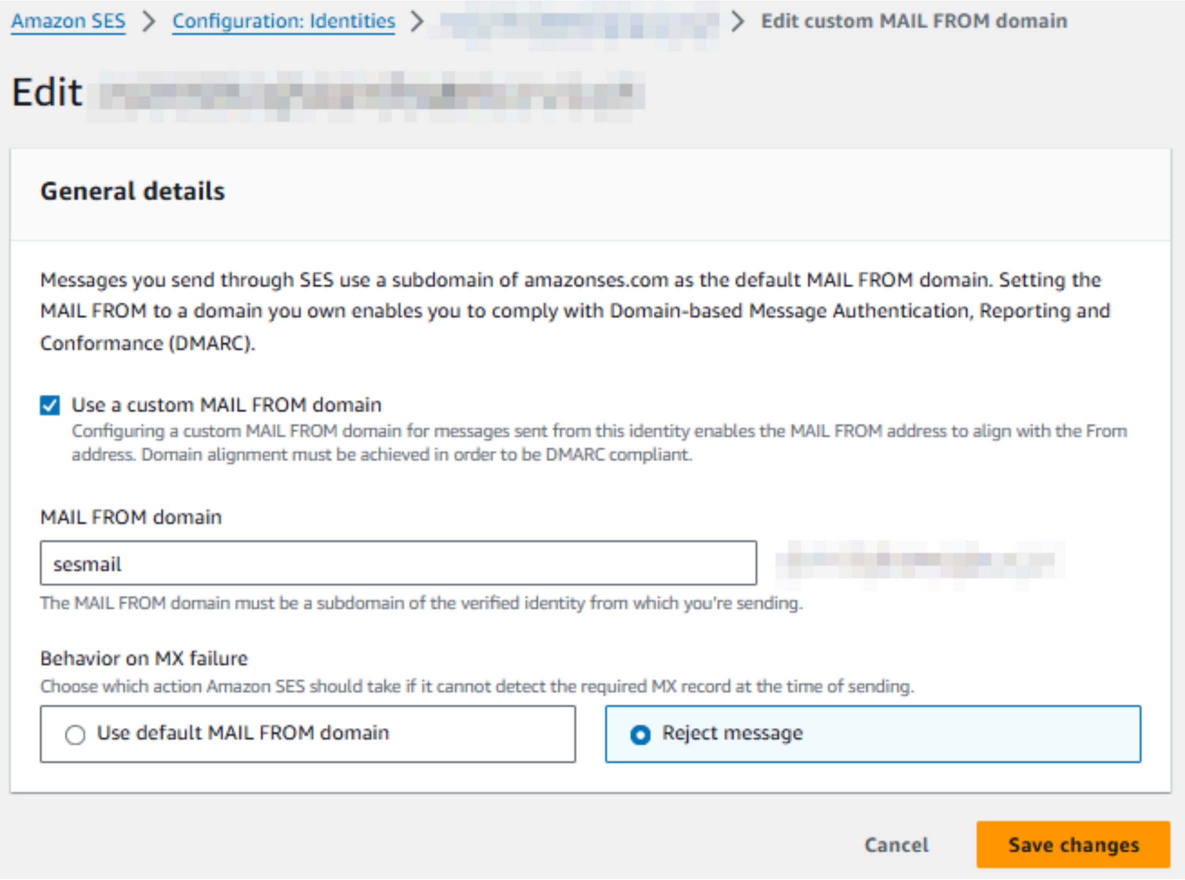
MAIL FROM configuration	MAIL FROM domain	Behavior on MX failure
✓ Successful	sesmail.[redacted]	Reject message

▼ Publish DNS records

ⓘ 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. For more information, see Configuring a MAIL FROM domain.

Type	Name	Value
MX	sesmail.[redacted]	10 feedback-smtp.us-east-1.amazonses.com
TXT	sesmail.[redacted]	"v=spf1 include:amazonses.com ~all"

Fig 7: SPF configuration – Edit custom MAIL FROM domain page



Amazon SES > Configuration: Identities > > Edit custom MAIL FROM domain

Edit

General details

Messages you send through SES use a subdomain of amazonses.com as the default MAIL FROM domain. Setting the MAIL FROM to a domain you own enables you to comply with Domain-based Message Authentication, Reporting and Conformance (DMARC).

☑ Use a custom MAIL FROM domain
Configuring a custom MAIL FROM domain for messages sent from this identity enables the MAIL FROM address to align with the From address. Domain alignment must be achieved in order to be DMARC compliant.

MAIL FROM domain

sesmail

The MAIL FROM domain must be a subdomain of the verified identity from which you're sending.

Behavior on MX failure
Choose which action Amazon SES should take if it cannot detect the required MX record at the time of sending.

○ Use default MAIL FROM domain

● Reject message

STEP 5 – DNS record publishing to configure DMARC

DNS records for SPF, DKIM and DMARC all need to be added (or updated) for the third-party sender domain being configured.

These can be updated individually, but for simplicity this guide details all these changes together (because they are all configured in the same external system).

The exact method to configure these will depend upon the DNS provider / nameserver hosting the domain. These changes should be performed by a competent, authorised individual and it is expected that they should be able to account for differences between the examples and the actual system in use.

DNS record formats

Feature	DNS record type	Name	Value
DKIM	CNAME	[KEY]._domainkey.<domain.tld>	[KEY].dkim.amazonses.com
SPF	MX	sesmail.<domain.tld>	feedback-smtp.[REGION].amazonses.com
SPF	TXT	sesmail.<domain.tld>	"v=spf1 include:amazonses.com ~all"
DMARC	TXT	_dmarc.<domain.tld>	"v=DMARC1; p=[OPTION];"
DMARC	TXT	_dmarc.sesmail.<domain.tld>	"v=DMARC1; p=[OPTION];"

Text in angled brackets < > should be replaced with the domain being configured. These may be pre-populated by the DNS management console / system.

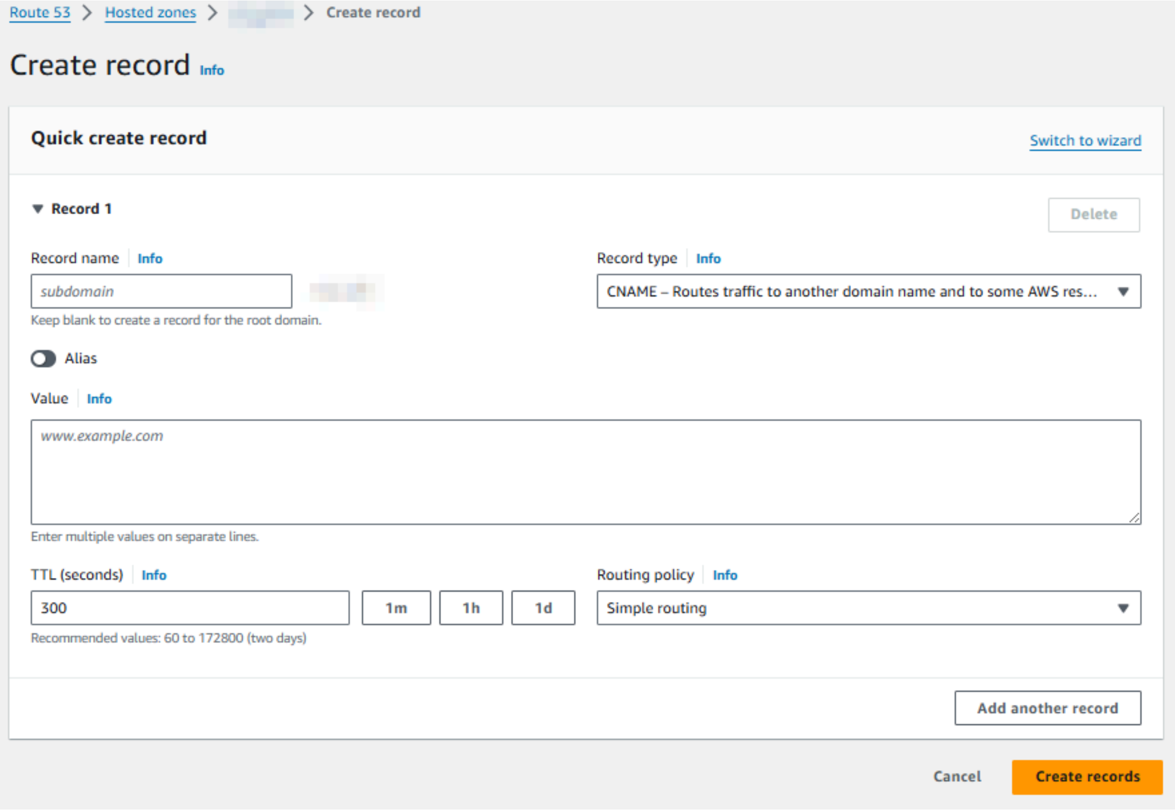
Text in square brackets [ ] should be replaced as detailed below:

Text	Details
[KEY]	Three values supplied by Amazon SES. These should be matched in the name and value of each DNS record.
[REGION]	The Amazon SES region the mail server is operating in.
[OPTION]	DMARC supports the following: *none*, *quarantine*, *reject*. We recommend the setting *quarantine* for DMARC to be effective. The setting *none* is provided by Amazon as an example, but this causes DMARC to have minimal positive effect.

DNS record publishing process

1. Go to the DNS management console / system for the domain to be verified.
2. To configure DKIM:
   I. Create three (3) new CNAME DNS records for the domain, using the provided names and values generated by Amazon SES Easy DKIM.
3. To configure SPF:
   I. Create a new MX DNS record for the subdomain, using the provided value, to configure a return path for email to Amazon SES in the correct region.
   II. Create a new TXT DNS record for the subdomain, using the provided value, to configure SPF on this subdomain granting SES authorisation to send emails from the subdomain.
4. To configure DMARC:
   I. Create two new TXT DNS records, one for the domain, and one for the SPF subdomain, to configure DMARC and ensure best possible alignment.
   It is recommended to configure DMARC at the "quarantine" level.
5. Save these record changes. It may take 48 hours for these to propagate through the global DNS system but the process is usually much quicker.

Fig 8: DNS record configuration – Amazon Route 53



Route 53 > Hosted zones > [redacted] > Create record

Create record Info

Quick create record

Switch to wizard

▼ Record 1

Delete

Record name | Info

subdomain [redacted]

Keep blank to create a record for the root domain.

Record type | Info

CNAME – Routes traffic to another domain name and to some AWS res... ▼

Alias

Value | Info

www.example.com

Enter multiple values on separate lines.

TTL (seconds) | Info

300

1m 1h 1d

Recommended values: 60 to 172800 (two days)

Routing policy | Info

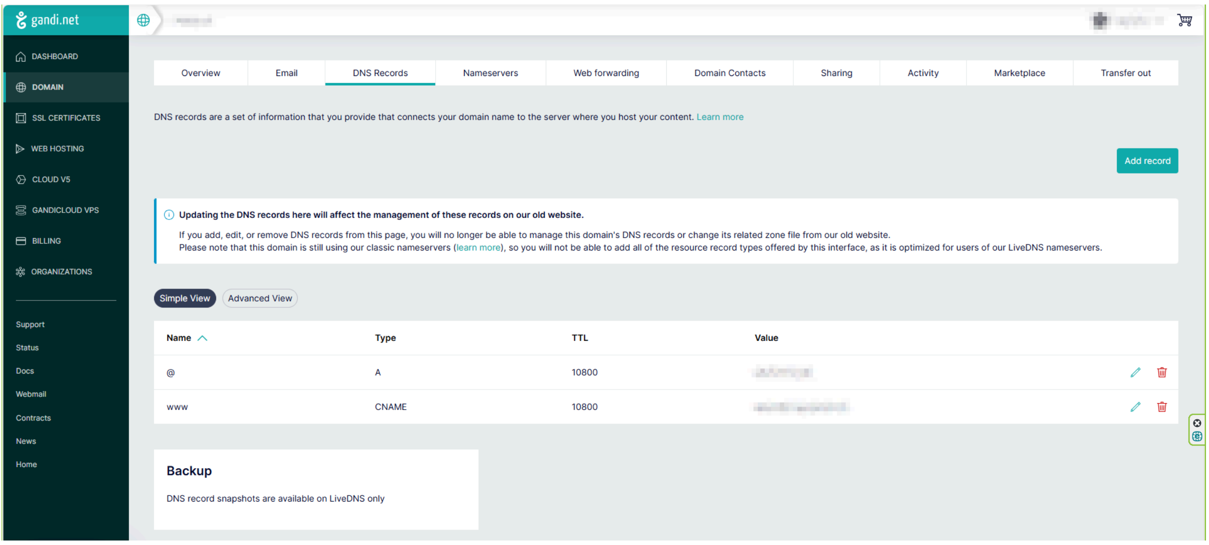
Simple routing ▼

Add another record

Cancel

Create records

Fig 9: DNS record configuration – Gandi (classic)



DNS records are a set of information that you provide that connects your domain name to the server where you host your content. Learn more

Updating the DNS records here will affect the management of these records on our old website.

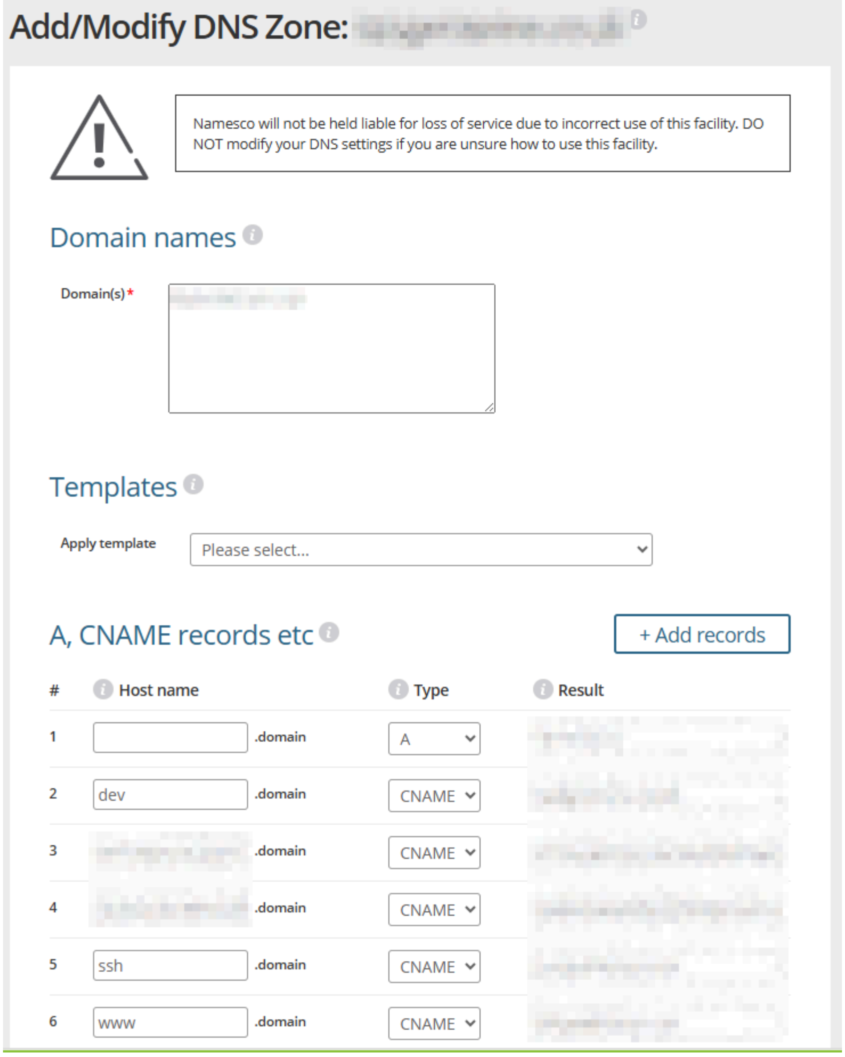
If you add, edit, or remove DNS records from this page, you will no longer be able to manage this domain's DNS records or change its related zone file from our old website.
Please note that this domain is still using our classic nameservers (learn more), so you will not be able to add all of the resource record types offered by this interface, as it is optimized for users of our LiveDNS nameservers.

Name	Type	TTL	Value
@	A	10800	[redacted]
www	CNAME	10800	[redacted]

Backup

DNS record snapshots are available on LiveDNS only

Fig 10: DNS record configuration – Namesco



Add/Modify DNS Zone: [redacted]

Namesco will not be held liable for loss of service due to incorrect use of this facility. DO NOT modify your DNS settings if you are unsure how to use this facility.

Domain names

Domain(s)* [redacted]

Templates

Apply template: Please select...

A, CNAME records etc

#	Host name		Type	Result
1		.domain	A	[redacted]
2	dev	.domain	CNAME	[redacted]
3	[redacted]	.domain	CNAME	[redacted]
4	[redacted]	.domain	CNAME	[redacted]
5	ssh	.domain	CNAME	[redacted]
6	www	.domain	CNAME	[redacted]

Appendix

SPF, DKIM & DMARC setup verification

There are a variety of free services that will perform DNS lookup checks on a domain to verify SPF, DKIM and DMARC are configured. These should be independently verified: having DMARC configured and verified in isolation is not sufficient to demonstrate SPF and DKIM are configured correctly and without these permission for SES to deliver mails on behalf of a domain is not granted.

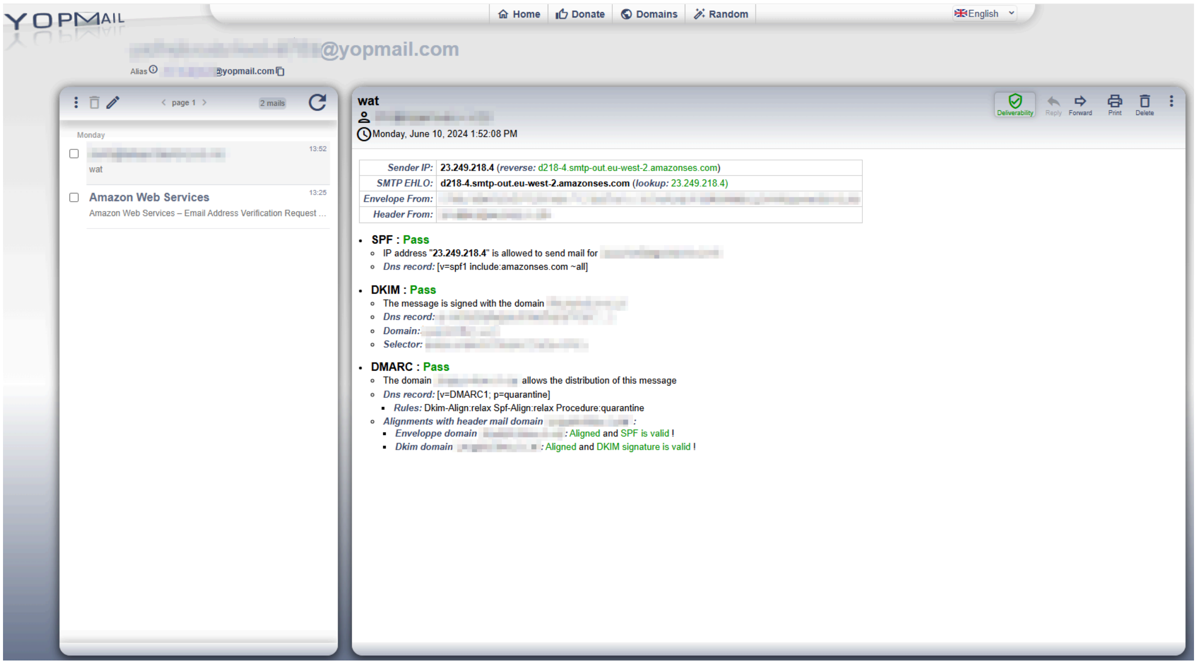
It is beyond the scope of this guide to detail all of these services.

End to End testing

Test emails sent from a third-party sender domain can be examined (especially the headers) for compliance with SPF, DKIM and DMARC.

Because email sent from incorrectly configured domains may be rejected by the receing server it may be necessary to conduct testing with an email service which will not apply this verification – but can report on it. There are free services which can make this easier, for example yopmail.com has an excellent delivery report information tool.

Fig 11: Delivery report – yopmail



[redacted]@yopmail.com

Alias [redacted]@yopmail.com

Monday

□ [redacted] 13:52
wat

□ Amazon Web Services 13:25
Amazon Web Services – Email Address Verification Request ...

wat

[redacted]

Monday, June 10, 2024 1:52:08 PM

Sender IP:	**23.249.218.4** (*reverse:* d218-4.smtp-out.eu-west-2.amazonses.com)
SMTP EHLO:	**d218-4.smtp-out.eu-west-2.amazonses.com** (*lookup:* 23.249.218.4)
Envelope From:	[redacted]
Header From:	[redacted]

- **SPF : Pass**
  - IP address "**23.249.218.4**" is allowed to send mail for [redacted]
  - *Dns record:* [v=spf1 include:amazonses.com ~all]
- **DKIM : Pass**
  - The message is signed with the domain [redacted]
  - *Dns record:* [redacted]
  - *Domain:* [redacted]
  - *Selector:* [redacted]
- **DMARC : Pass**
  - The domain [redacted] allows the distribution of this message
  - *Dns record:* [v=DMARC1; p=quarantine]
    - *Rules:* Dkim-Align:relax Spf-Align:relax Procedure:quarantine
  - *Alignments with header mail domain* [redacted] *:*
    - *Enveloppe domain* [redacted] *:* Aligned and SPF is valid !
    - *Dkim domain* [redacted] *:* Aligned and DKIM signature is valid !

References

1. https://dmarc.org
2. https://dmarcian.com/yahoo-and-google-dmarc-required
3. Google Email Sending Guidance
4. Yahoo Email Sending Guidance
5. Amazon SES & DMARC setup guides