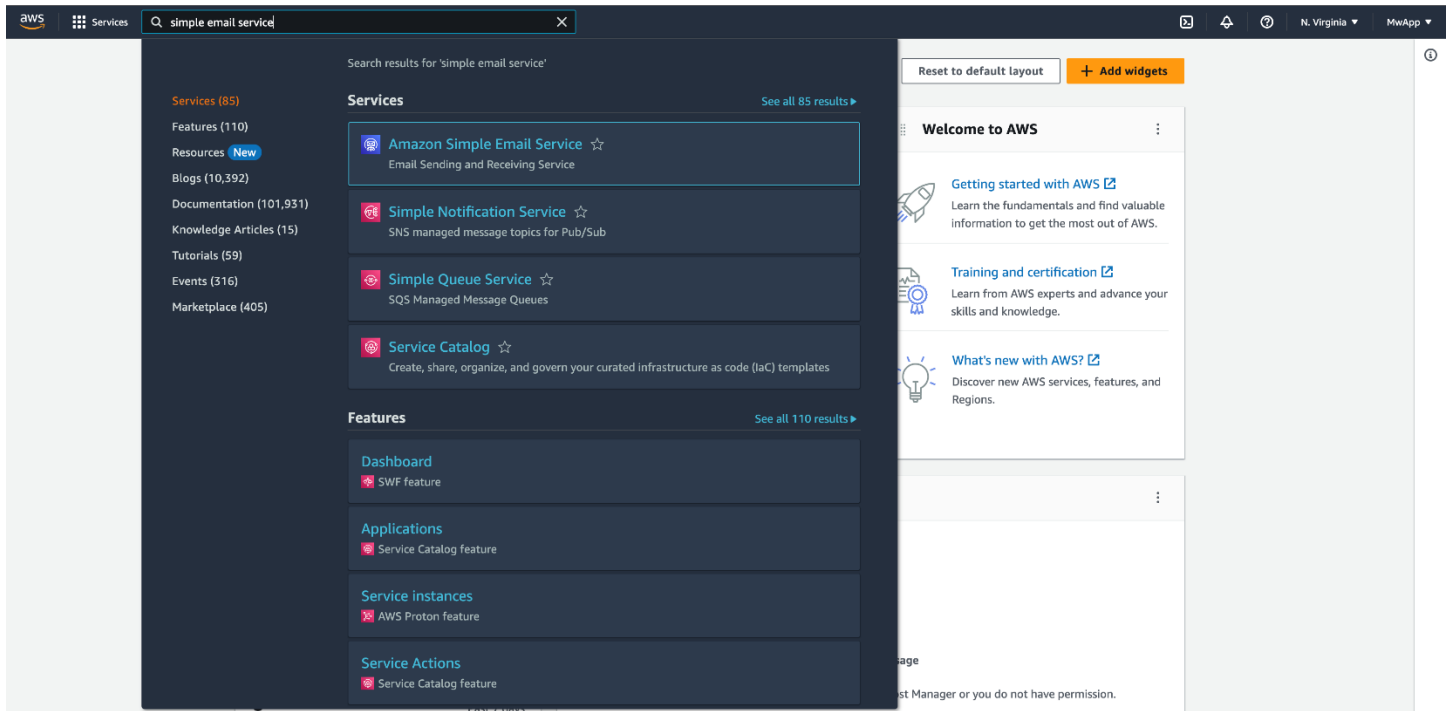


AWS (Web API) Configuration for BestBetMail

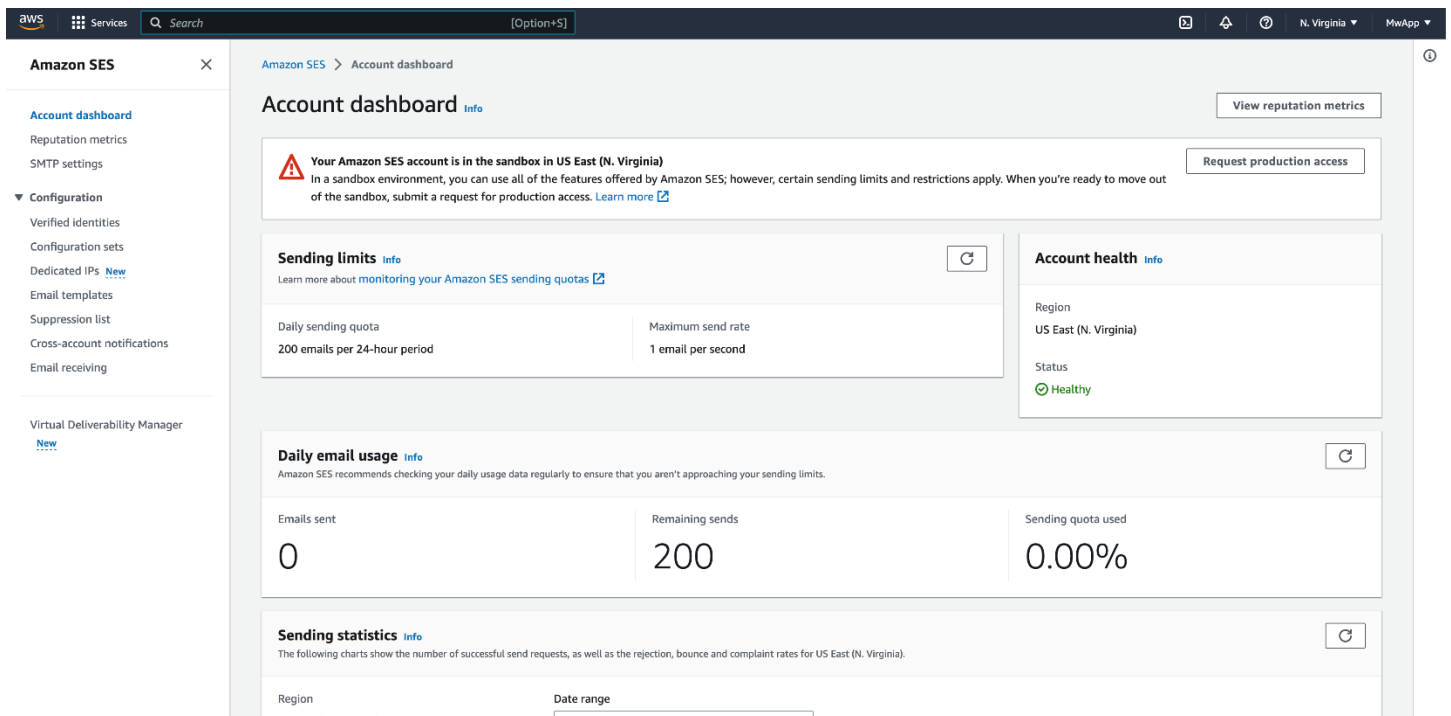
Step 1 – Login to AWS

Login or create an account [here](#).

Once you are logged in, search for SES (Amazon Simple Email Service) and open it.



Your screen should look like the below



Step 2 – Add Your Mail Domain

Preparation:

- You should already have a domain you wish to use as your mail sending domain. This can be an existing domain or a new domain. If you need a new domain you can get one from us [here](#).
- Within your sending domain you should have an email address you would like your marketing emails to come from. This can be an existing mailbox like john.doe@mydomain.com or a generic sending address like mail@mydomain.com. If you're using a new domain, be sure and setup a mailbox for this.

In this step we will setup your mail domain. We will be setting up a custom "Mail From" domain so an existing domain will work just fine. Now, within SES click on "Identities" under Configuration in the left panel, then click the orange "Create Identity" button and you see a screen like below.

1. Select "Domain"
2. Check the box that says "Use a custom MAIL FROM domain"
3. Enter the name of your MAIL FROM domain. This can be anything really, but we recommend something logical like "mail".

Amazon SES > Configuration: Identities > Create identity

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

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

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.

☐ Assign to a tenant
Assigning an identity to a tenant enables the tenant to use the identity for sending emails. The same identity can be assigned to multiple tenants or isolated to a single tenant.

☒ 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

The MAIL FROM domain refers to the domain that appears in the 'From' field of an email message and is recommended for better deliverability, reputation management, and branding purposes. The MAIL FROM domain must be a subdomain of the verified identity from which you're sending.

Behavior on MX failure

Next, scroll down and choose “Easy DKIM”.

Amazon SES > Configuration: Identities > Create identity

MAIL FROM domain

mail.sampledomain.com

The MAIL FROM domain refers to the domain that appears in the 'From' field of an email message and is recommended for better deliverability, reputation management, and branding purposes. 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 your MAIL FROM domain's MX (Mail Exchange) record is not set up correctly.

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

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.

Deterministic Easy DKIM

Utilize the Easy DKIM setup from a parent region and sign the new identity without additional DNS setup.

Provide DKIM authentication token (BYODKIM)

Configure DKIM for this domain by providing your own private key.

Now we want to download all of your DNS records which will need to be added later in this process. We'll expand each of the following sections and download the required records. Be sure and save these files somewhere you can retrieve them from in a later step in this process.

Amazon SES > Configuration: Identities > sampledomain.com

Amazon SES

Get set up

Account dashboard

Reputation metrics

SMTP settings

What's new

Configuration

Identities

Configuration sets

Tenants

Dedicated IPs

Global endpoints

Email templates

Suppression list

Email receiving

WorkMail

Overview

Get set up

Virtual Deliverability Manager

Overview

Mail Manager

Overview

Get set up

DomainKeys Identified Mail (DKIM)

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

October 9, 2025 at 09:01 (UTC-05:00)

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	kagm5napwgviyloliiimaywx46cjresf5_domainkey.sampledomain.com	kagm5napwgviyloliiimaywx46cjresf5.dkim.amaz
CNAME	q5x4pj5pp26nxqagges77dnmujgdooomm_domainkey.sampledomain.com	q5x4pj5pp26nxqagges77dnmujgdooomm.dkim.amaz
CNAME	f44wge26mtzyaet2famgfdnz3qqudifj_domainkey.sampledomain.com	f44wge26mtzyaet2famgfdnz3qqudifj.dkim.amaz

Download .csv record set

Amazon SES > Configuration: Identities > sampledomain.com

▼ Configuration

Identities

Configuration sets

Tenants [New](#)

Dedicated IPs

Global endpoints

Email templates

Suppression list

Email receiving

▼ WorkMail

Overview

Get set up [?](#)

▼ Virtual Deliverability Manager

Overview

▼ Mail Manager

Overview

Get set up

Dashboard

Address lists

Traffic policies

Rule sets

Ingress endpoints

Email add-ons

SMTP relays

Email archiving

Custom MAIL FROM domain [Info](#) [Edit](#)

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

Pending

mail.sampledomain.com

Use default MAIL FROM domain

▼ 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	mail.sampledomain.com	10 feedback-smtp.us-east-1.amazonaws.com
TXT	mail.sampledomain.com	"v=spf1 include:amazonses.com ~all"

[Download .csv record set](#)

Domain-based Message Authentication, Reporting, and Conformance (DMARC)

DMARC specifies how email servers should handle messages that fail the authentication checks.

► Publish DNS records

Overview

Get set up [?](#)

▼ Virtual Deliverability Manager

Overview

▼ Mail Manager

Overview

Get set up

Dashboard

Address lists

Traffic policies

Rule sets

Ingress endpoints

Email add-ons

SMTP relays

Email archiving

Domain-based Message Authentication, Reporting, and Conformance (DMARC)

DMARC specifies how email servers should handle messages that fail the authentication checks.

▼ Publish DNS records

You can edit the *Value* provided below to modify the DMARC policy you want to apply to your domain. [Learn more](#)

Type	Name	Value
TXT	_dmarc.sampledomain.com	"v=DMARC1; p=none;"

[Download .csv record set](#)

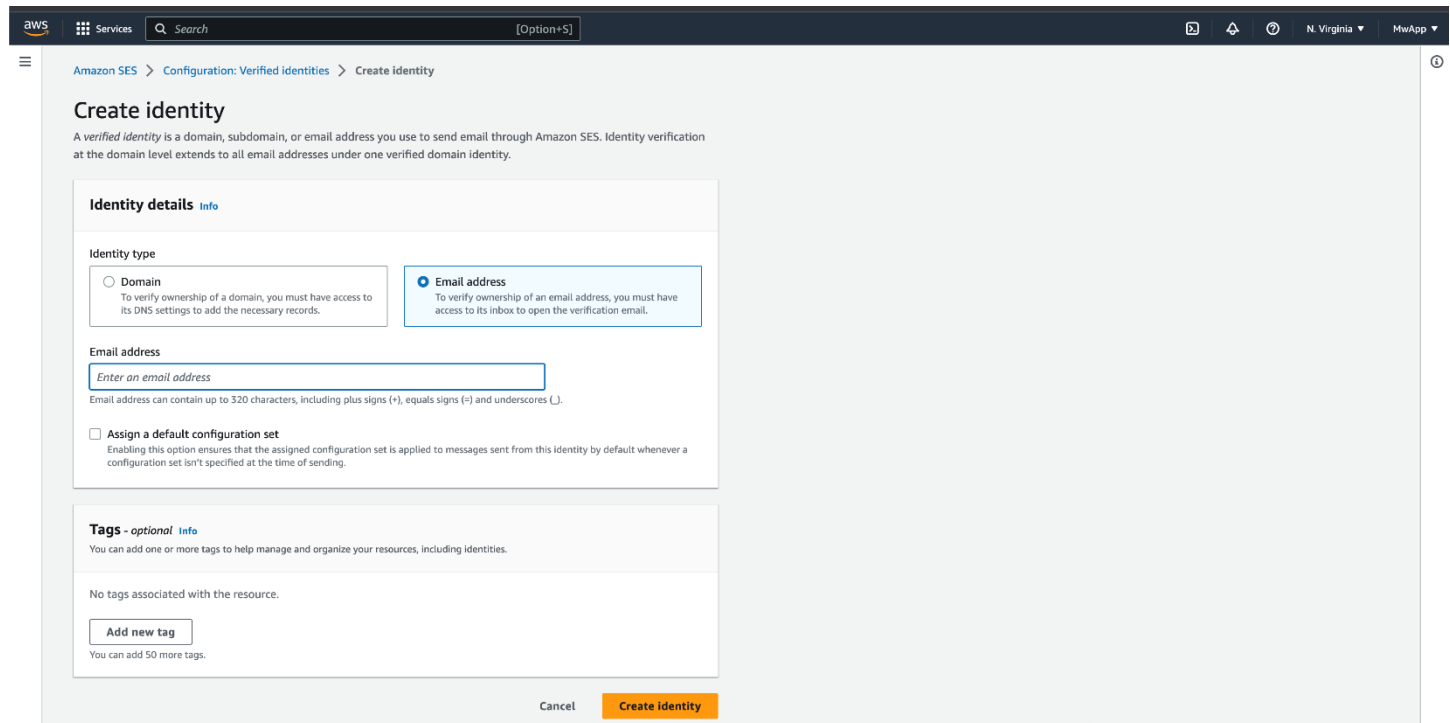
When finished, you should have downloaded and saved the following csv record sets.

- DKIM CNAME records.
- Custom MAIL FROM domain records.
- DMARC TXT record.

Step 3 – Confirm your sender identity

Return to the Amazon SES main screen (type SES in the search box if necessary). Next we'll setup your sender identity, so you will need to validate an email address **not** a domain. This should be the email address you want to send mail from and must be valid as you will receive an email validation link you must click. If necessary, create a new mailbox for this purpose.

Enter our email address and click the orange "Create Identity" button.



The screenshot shows the Amazon SES console's 'Create Identity' page. The breadcrumb trail is 'Amazon SES > Configuration: Verified Identities > Create Identity'. The page title is 'Create identity'. A description states: 'A verified 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.'

The 'Identity details' section includes an 'Identity type' choice with two options: 'Domain' (unselected) and 'Email address' (selected). The 'Email address' option has a note: 'To verify ownership of an email address, you must have access to its inbox to open the verification email.' Below this is an 'Email address' input field with the placeholder 'Enter an email address' and a note: 'Email address can contain up to 320 characters, including plus signs (+), equals signs (=) and underscores (_).' There is also an unchecked checkbox for 'Assign a default configuration set' with a note: '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.'

The 'Tags - optional' section states: 'You can add one or more tags to help manage and organize your resources, including identities.' It shows 'No tags associated with the resource.' and an 'Add new tag' button with a note: 'You can add 50 more tags.'

At the bottom right, there are 'Cancel' and 'Create identity' buttons.

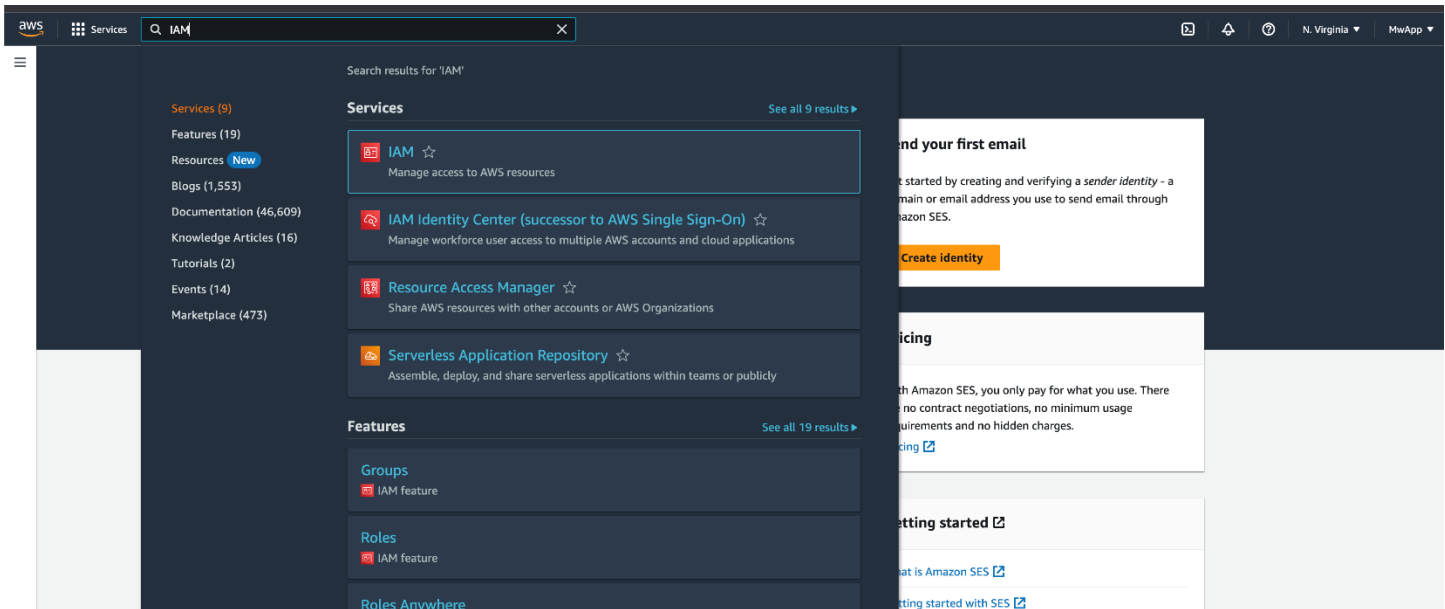
Step 4 – Update your DNS records.

This step requires you to set the DNS records that you downloaded earlier. Go to your domain registrar and add the 3 sets of DNS records. If you purchased the domain from us, go to your [hosting control panel](#), login and go to your client area, then click "Hosting". Click Manage on your domain and you'll find "Manage DNS" under "Domain Names". If you purchased your domain elsewhere, go to that registrar and add your DNS records there. If you are unsure how to add the records, a simply Google search on "How to add DNS records for [your registrar]". This should return a number of articles on how to do this.

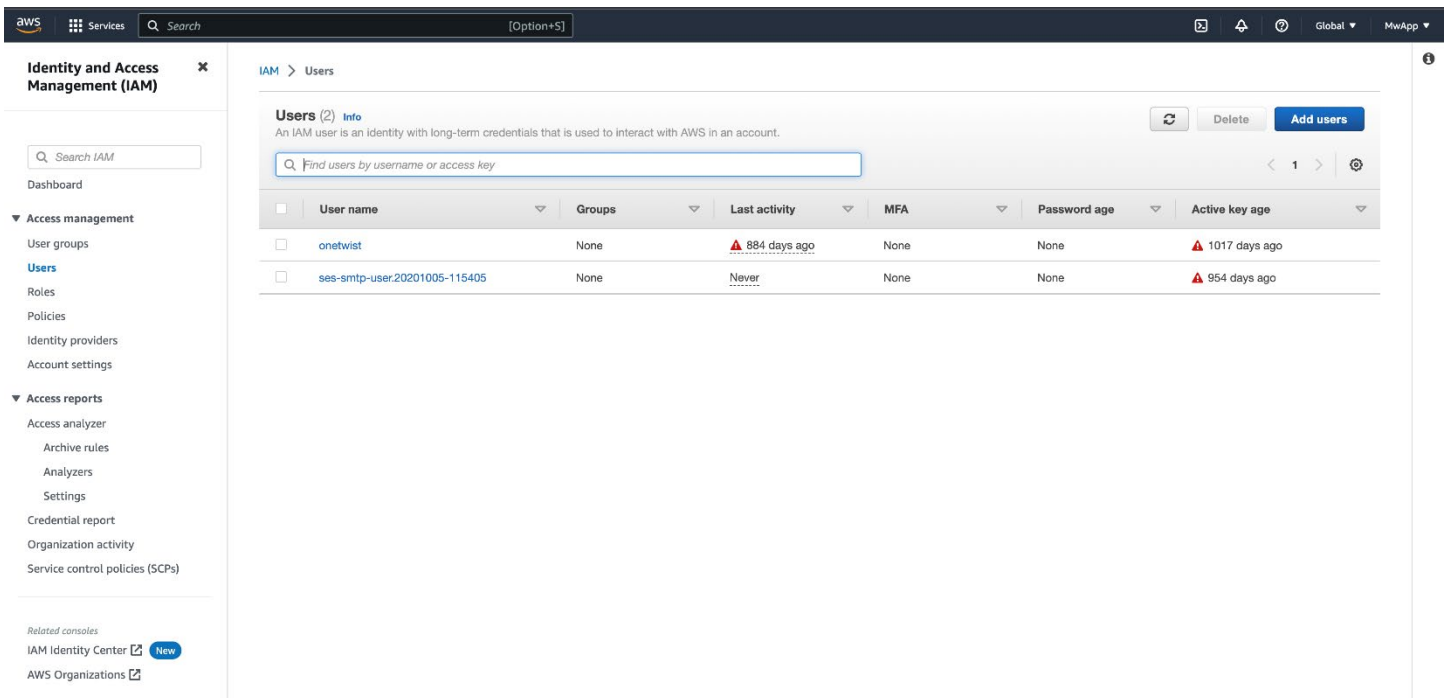
Note: It can take up to 24 hours for DNS to propagate, but usually less than an hour. After an hour or so, return to SES Identities and make sure your domain says "Verified". Also click your domain and be sure the DKIM Configuration says Successful.

Step 5 – Create an IAM user

Search for “IAM” and click on it, be it just says “IAM” and NOT “IAM Identity Center”



Next, add a new user. Name it something like “bestbetmail” or another identifying name. DO NOT check the box to grant console access.



Next step will be to set the user permissions. Select “Attach Policies Directly”. Now search for “amazonses” under Permissions Policies, and check the box next to “AmazonSESFULLAccess”.

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

☐ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

☒ Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (Selected 3/1089)
Choose one or more policies to attach to your new user.

Policy name	Type	Attached entities
-------------	------	-------------------

Click Next, then click “Create User”. You should now see your new user.

Step 6 – Create your access key.

While still on the IAM Users screen, Click on your newly created user. Then click on “Create Access Key”.

S3

IAM > Users > test

test

Info Delete

Summary

ARN
[arn:aws:iam::286198982291:user/test](#)

Console access
Disabled

Access key 1
[Create access key](#)

Created
October 08, 2025, 19:01 (UTC-05:00)

Last console sign-in
-

Permissions Groups Tags Security credentials Last Accessed

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

Policy name	Type
☐ AmazonSESFULLAccess	AWS managed

Permissions boundary (not set)

Generate policy based on CloudTrail events
You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your

You'll need select "Third Party Service" and click Next

The screenshot shows the AWS IAM console interface. The top navigation bar includes the AWS logo, 'Services' menu, a search bar, and a '[Option+S]' button. The left sidebar shows the navigation menu with 'Step 1: Access key best practices & alternatives' selected. The main content area is titled 'Access key best practices & alternatives' and includes a warning about long-term credentials. It lists six use cases for access keys, with 'Third-party service' selected. Below the list is an 'Alternative recommended' section with a warning icon and text advising the use of temporary security credentials (IAM roles) instead of long-term credentials like access keys. A checkbox at the bottom indicates understanding of the recommendation. At the bottom right, there are 'Cancel' and 'Next' buttons.

Step 1
Access key best practices & alternatives

Step 2 - optional
Set description tag

Step 3
Retrieve access keys

Access key best practices & alternatives

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

- ☐ **Command Line Interface (CLI)**
You plan to use this access key to enable the AWS CLI to access your AWS account.
- ☐ **Local code**
You plan to use this access key to enable application code in a local development environment to access your AWS account.
- ☐ **Application running on an AWS compute service**
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.
- ☒ **Third-party service**
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.
- ☐ **Application running outside AWS**
You plan to use this access key to enable an application running on an on-premises host, or to use a local AWS client or third-party AWS plugin.
- ☐ **Other**
Your use case is not listed here.

Alternative recommended
As a best practice, use temporary security credentials (IAM roles) instead of creating long-term credentials like access keys, and don't create AWS account root user access keys. [Learn more](#)

☒ I understand the above recommendation and want to proceed to create an access key.

Cancel Next

You'll need to copy and paste both the Access Key and Secret Key. Save them somewhere safe as we'll need them later, then click "Done".

The screenshot shows the AWS IAM console interface. The top navigation bar includes the AWS logo, 'Services' menu, a search bar, and a '[Option+S]' button. The left sidebar shows the navigation menu with 'Step 2: Retrieve access keys' selected. The main content area is titled 'Retrieve access keys' and displays the generated access key and secret access key. The access key is AKIAW7KZYFCRDBEFJMY. The secret access key is masked with asterisks and has a 'Show' link. Below the keys is a section titled 'Access key best practices' with a list of recommendations. At the bottom right, there are 'Download .csv file' and 'Done' buttons.

Access key created
This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.

IAM > Users > mailwizz > Create access key

Step 1
Access key best practices & alternatives

Step 2 - optional
Set description tag

Step 3
Retrieve access keys

Retrieve access keys

Access key
If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key	Secret access key
AKIAW7KZYFCRDBEFJMY	***** Show

Access key best practices

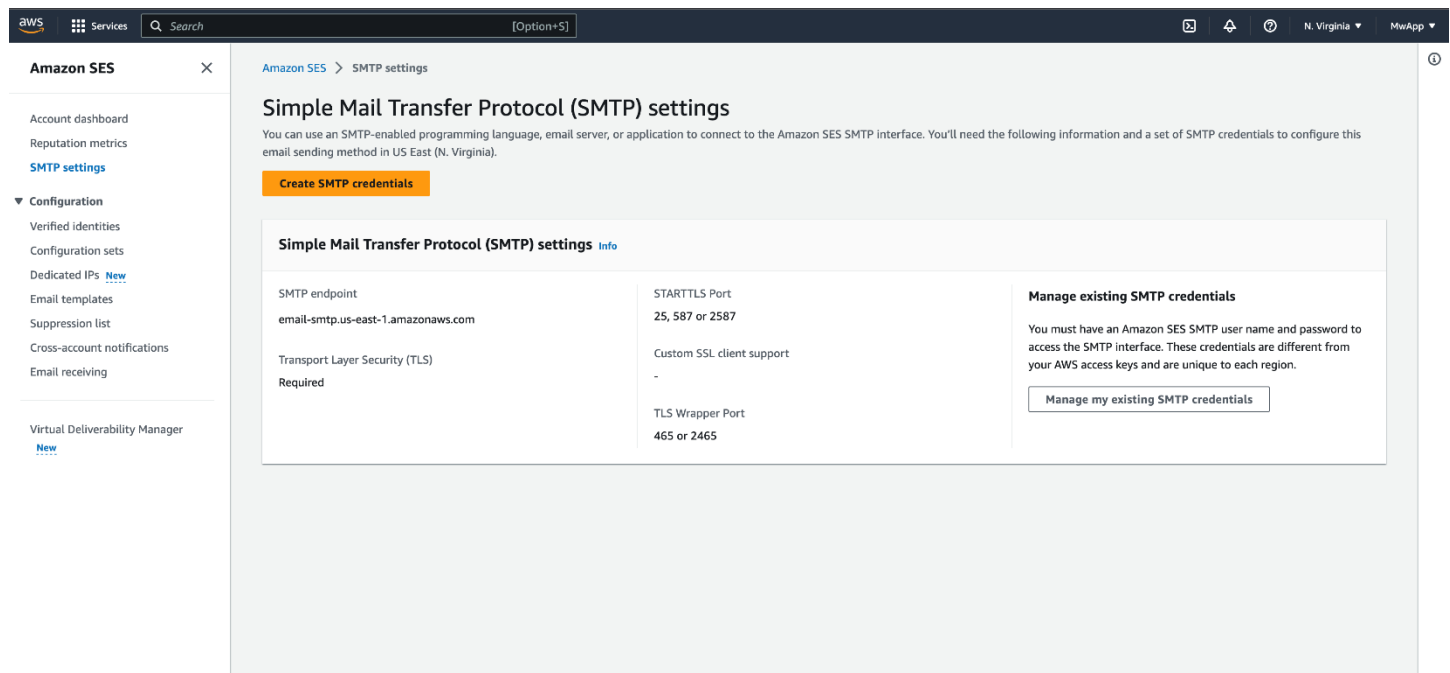
- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the [Best practices for managing AWS access keys](#).

Download .csv file Done

Step 7 – Get your SMTP Server

Return to your SES home page in the dashboard and access *SMTP Settings*. You will need to copy and paste the *SMTP endpoint* in the same document as your Access keys, since you will need it inside the BestBetMail setup also.



You should now have the following information.

- Access Key
- Secret Access Key
- SMTP Endpoint
- Confirmed SES email address

Step 8 – Request production access

Back on the SES screen you'll see that your SES access currently says "Sandbox". We need to request production access. However, before requesting production access we need to verify a few things that are very important to getting production access.

1. Make sure your sending domain has been verified in SES beforehand.
2. Your website should have a valid Terms of Use and Privacy Policy
3. On your website contact form, opt-in form/user registration form, make sure you have a checkbox that states "I agree to receiving marketing and transactional emails."
4. Your forms should have reCAPTCHA protection to prevent bots from spamming your email database.

Getting out of the sandbox

1. Open the Amazon SES console at <https://console.aws.amazon.com/ses/>.
2. In the navigation panel, choose **Account dashboard**.
3. In the warning box at the top of the console that says, "Your Amazon SES account is in the sandbox", on the right-hand side, choose **View Get set up page** followed by **Request production access**.
4. In the account details modal, select either the **Marketing** or **Transactional** radio button that best describes the majority of mail you'll be sending.
 - *Marketing email* - Sent on a one-to-many basis to a targeted list of prospects or customers containing marketing and promotional content such as to make a purchase, download information, etc.
 - *Transactional email* - Sent on a one-to-one basis unique to each recipient usually triggered by a user action such as a website purchase, a password reset request, etc.
5. In **Website URL**, enter the URL of your website to help us better understand the kind of content you plan on sending.
6. **Use-case description**: Enter your use case description being sure to describe your opt-in process, bounce and complaint handling and compliance. See the sample text below

Only registered users that opt'd in (via double opt-in) will receive emails from us. Our website's address is <https://mydomain.com/>. We use Google reCAPTCHA to protect our forms against spam.

We send opt-in newsletters and transactional emails using a custom Mailwizz application to verified subscribers. Our lists are GDPR/Can-Spam compliant and we handle bounces and complaints through Amazon SNS topics. We also include an unsubscribe link in every email we send.

In the event of a permanent bounce, the application unsubscribes the lead immediately. There will be no further emails sent to that address. If the bounce is temporary, the application saves the bounce response (along with the timestamp, type, and subtype) for future reference.

In response to complaints, the application immediately unsubscribes the email address. There will be no further emails sent to that address.

The application will also help us create email campaigns with the required content and format (as advised by AWS) to help us maintain a good email sending reputation.

7. In **Additional contacts**, tell us where you want to receive communications about your account. This can be a comma-separated list of up to 4 email addresses.
8. In **Preferred contact language**, choose whether you want to receive communications in **English** or **Japanese**.
9. In **Acknowledgement**, check the box that you agree to only send email to individuals who've explicitly requested it and confirm that you have a process in place for handling bounce and complaint notifications.
10. Choose the **Submit request** button - a banner will display to confirm your request was submitted and is currently under review.

It may take 1 – 2 business days to receive a response, but you should receive an email saying production access has been granted. You can also check your Amazon SES account to see that your access says “Production”. If your request has been rejected, follow the instructions and respond with the required information. If necessary, open a support ticket at <https://bestbetmedia.com/support/> and we can provide assistance.

Amazon configuration is now complete.

Step 9 – Setup your Delivery Server in BestBetMail

Login to your BestBetMail account here: <https://bestbetmail.com/customer/>

Next navigate to **Servers -> Delivery Servers** and click on “Create New Server”

The screenshot shows the 'View delivery servers' page in the BestBetMail dashboard. The page has a sidebar with navigation icons and a top bar with user information (Michael Green). The main content area displays a table of delivery servers. The table has columns for ID, Name, Hostname, Username, From email, Type, Status, and Options. A single server is listed with ID 6, Name 'BestBetMedia Amazon 1 >', Hostname 'email-smtp.us-east-1.amazonaws.com >', Username 'AKIAQHLE5KUO6YA3UKHI', From email 'newsletter@mail.bestbetmedia.com', Type 'Amazon Ses Web Api', and Status 'Active'. Above the table are buttons for 'Toggle columns', 'Create new server', 'Import', 'Export', and 'Refresh'. Below the table is a pagination control showing '10' items per page.

ID	Name	Hostname	Username	From email	Type	Status	Options
6	BestBetMedia Amazon 1 >	email-smtp.us-east-1.amazonaws.com >	AKIAQHLE5KUO6YA3UKHI	newsletter@mail.bestbetmedia.com	Amazon Ses Web Api	Active	

Click on Server Type “Amazon SES Web API”

The screenshot shows a modal dialog box titled 'Select a delivery server type'. It has a search bar containing the text 'amazon ses'. Below the search bar, the option 'Amazon Ses Web Api' is displayed with a right-pointing arrow icon. A 'Close' button is located at the bottom right of the dialog.

Here you will need to fill in the info that you noted from the Amazon SES setup steps. Be sure and enter a valid **Reply-To email**.

The screenshot shows a form titled "Create new delivery server" with a "Cancel" button in the top right. The form is divided into four columns. Red boxes and arrows highlight specific fields: "Server name from Amazon SES setup" points to the "Hostname *" field (value: "i.e: email-smtp.us-east-1.amazonaws."); "Amazon SES Access Key ID" points to the "Access Key ID *" field (value: "i.e: AKIAIYYYYYYYYYUBBFQ"); "Amazon SES Secret Access Key" points to the "Secret Access Key *" field (value: "i.e: pnSXPeHkmapf6gghCyflDz8YJce!"); and "Verified email with Amazon SES" points to the "From email *" field (value: "you@domain.com"). Other fields include "Name", "From name", "Probability" (100 %), "Hourly quota" (0), "Daily quota" (0), "Monthly quota" (0), "Pause after send" (0), "Tracking domain" (Choose), "Use for" (All), "Force FROM" (Always), "Reply-To email" (you@domain.com), and "Force Reply-To" (Never).

Save the form and then you will need to verify your server. In the verification step you should enter a valid email address where you will receive an email containing the verification link.

That's it.

From here you'll want to:

1. Create a test list with valid test email accounts.
2. Send a test campaign to make sure everything is working.

Periodically check your Amazon SES Reputation and make sure things are working properly. Reputation is very important. If bounces or complaints start climbing in Amazon SES, you'll want to address the issue promptly.

1. Check for spam email addresses making it into our system. If so, correct the issue by securing your opt-in forms.
2. Make sure your reCAPTCHA's are working on all your forms, even contact forms.
3. Check your outgoing campaigns and see if there is a particular campaign that's generating complaints and address those issues.

Happy Marketing,

BestBetMail