

Loop AWS Config

Loop need S3, CloudFront, SQS, SES, IAM as core dependency, below will show how to create these components.

All customer config in this file: **annotation-service/config/app-os.js**

Index	Version	Brief Description	Name	Time
1	V0	Aws config draft include S3, CloudFront, SQS, SES, IAM	Joe Qiao	2021/01/06
2	V0.1	Remove CloudFront	Joe Qiao	2021/02/09

Login

Login to AWS console: <https://console.aws.amazon.com/console/home>

Please Note create all AWS component in the same region

The screenshot shows the AWS Management Console homepage with a red arrow pointing from the URL bar (which says 'us-west-2') to the 'Region' dropdown menu in the top right corner. The dropdown menu lists various AWS regions, with 'US West (Oregon) us-west-2' highlighted in red.

- Replace region

```
region: process.env.REGION || "us-west-2"
```

S3

You can reference the official guideline from here <https://docs.aws.amazon.com/s3/index.html>

Create Bucket

The screenshot shows two screenshots of the AWS Management Console. The top screenshot shows the search results for 'S3' in the search bar, with the 'S3' service card highlighted in red. The bottom screenshot shows the 'Amazon S3' service page, where a red box highlights the 'Create bucket' button.

Create bucket

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name

①

Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

Region

②

Copy settings from existing bucket - optional [use the same default region with other components](#)
Only the bucket settings in the following configuration are copied.

Bucket settings for Block Public Access

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

- Disable
- Enable

Tags (0) - optional

Track storage cost or other criteria by tagging your bucket. [Learn more](#)

No tags associated with this bucket.

Default encryption

Automatically encrypt new objects stored in this bucket. [Learn more](#)

Server-side encryption

- Disable
- Enable

► Advanced settings

④ After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.

⑤

- Replace bucketName

```
bucketName: process.env.BUCKET_NAME || "joe-mikey-poc"
```

Edit Bucket permissions



The screenshot shows the Amazon S3 console. On the left, a sidebar menu includes 'Buckets' (which is selected and highlighted in red), 'Access points', 'Batch Operations', and 'Access analyzer for S3'. Below this is a section for 'Account settings for Block Public Access'. The main content area is titled 'Amazon S3' and shows the 'Buckets' section with the heading 'Buckets (5)'. A sub-instruction 'Buckets are containers for data stored in S3. Learn more' is present. There is a search bar labeled 'Find buckets by name'. A table lists five buckets: 'joe-mikey-poc' (selected and highlighted in red), 'us-west-2', 'Bucket and objects not public', and 'January 6, 2021, 11:18:10 (UTC+08:00)'. To the right of the table are buttons for 'Copy ARN', 'Empty', 'Delete', and 'Create bucket'.

Amazon S3 > joe-mikey-poc

joe-mikey-poc

Objects Properties **Permissions** Metrics Management Access points

Permissions overview

Access Bucket and objects not public

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

[Edit](#)

Block all public access

On

- Block public access to buckets and objects granted through **new** access control lists (ACLs)
 - On
 - Block public access to buckets and objects granted through **any** access control lists (ACLs)
 - On
 - Block public access to buckets and objects granted through **new** public bucket or access point policies
 - On
 - Block public and cross-account access to buckets and objects through **any** public bucket or access point policies
 - On

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

[Edit](#) [Delete](#)

Public access is blocked because Block Public Access settings are turned on for this bucket.
To determine which settings are turned on, check your bucket settings for Block Public Access. Learn more about using Amazon S3 Block Public Access.

No policy to display. [Copy](#)

Object ownership

Assume ownership of new objects uploaded to this bucket. [Learn more](#)

[Edit](#)

Object ownership
Object writer
The object writer remains the object owner.

Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. [Learn more](#)

[Edit](#)

Public access is blocked because Block Public Access settings are turned on for this bucket.
To determine which settings are turned on, check your bucket settings for Block Public Access. Learn more about using Amazon S3 Block Public Access.

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: 661407d25b22415d11440e74e1cff92ad19266e67dc85b1419360f44deba2d5a	List, Write	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	-	-
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	-	-
S3 log delivery group Group: http://acs.amazonaws.com/groups/s3/LogDelivery	-	-

Cross-origin resource sharing (CORS)

The CORS configuration, written in JSON, defines a way for client web applications that are loaded in one domain to interact with resources in a different domain. [Learn more](#)

[Edit](#)

No configurations to display. [Copy](#)

Copy this json the edit input text-area

```
[  
  {  
    "AllowedHeaders": [  
      "*"  
    ],  
    "AllowedMethods": [  
      "GET",  
      "PUT",  
      "POST",  
      "DELETE"  
    ],  
    "AllowedOrigins": [  
      "*"  
    ],  
    "ExposeHeaders": []  
  }  
]
```

Amazon S3 > joe-mikey-poc > Edit cross-origin resource sharing (CORS)

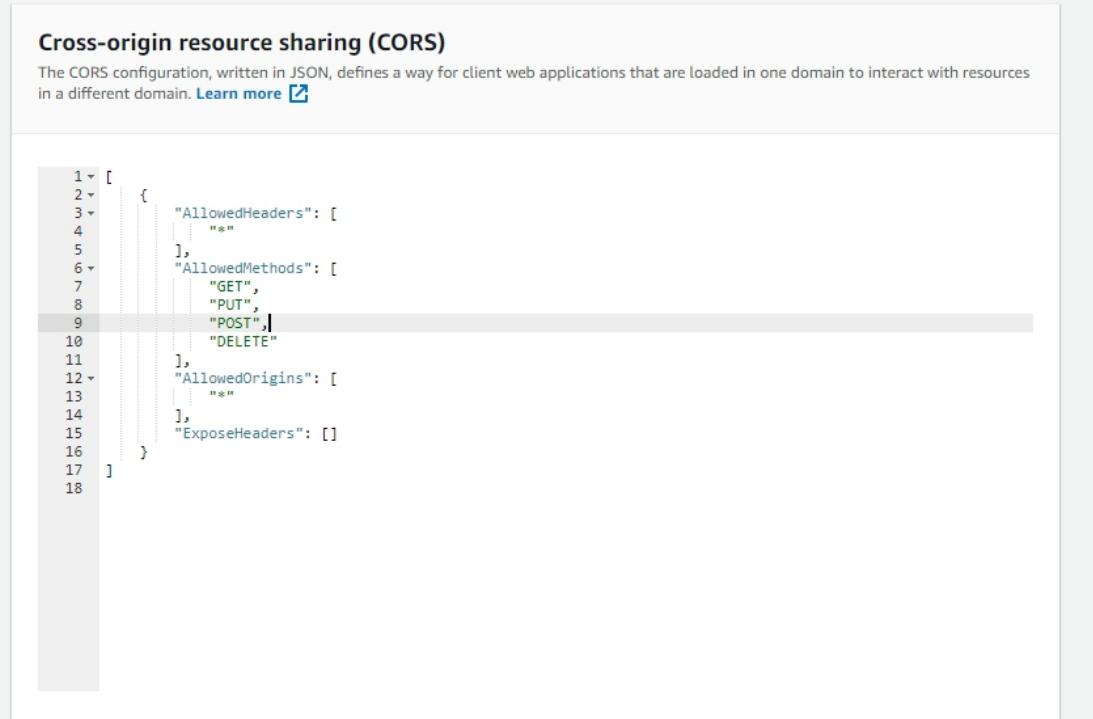
Edit cross-origin resource sharing (CORS)

Cross-origin resource sharing (CORS)

The CORS configuration, written in JSON, defines a way for client web applications that are loaded in one domain to interact with resources in a different domain. [Learn more](#)

```
1 [  
2 {  
3   "AllowedHeaders": [  
4     "*"  
5   ],  
6   "AllowedMethods": [  
7     "GET",  
8     "PUT",  
9     "POST",  
10    "DELETE"  
11  ],  
12  "AllowedOrigins": [  
13    "*"  
14  ],  
15  "ExposeHeaders": []  
16}  
17]  
18
```

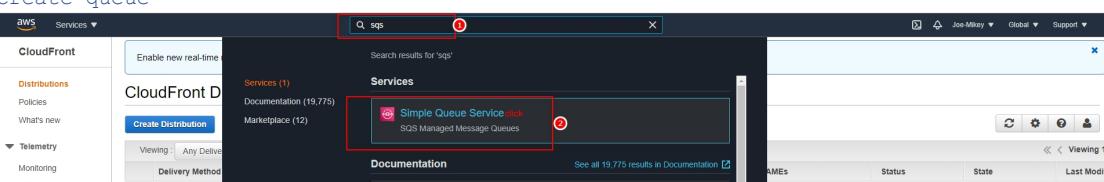
Cancel Save changes



SQS

You can reference the official guideline from here <https://docs.aws.amazon.com/sqs/index.html>

Create queue



A screenshot of the AWS CloudFront search results page. The search bar at the top contains the text 'sq'. Below the search bar, there is a 'Search results for 'sq'' section. Under the 'Services' heading, the 'Simple Queue Service' is listed with a blue link. Other items like 'Documentation (19,775)' and 'Marketplace (12)' are also visible.

The screenshot shows two side-by-side AWS SQS console pages. The left page displays the 'Queues' list with one item ('joe-mikey-poc') and a prominent orange 'Create queue' button. The right page is the 'Create queue' wizard, step 1: 'Details'. It includes sections for 'Type' (Standard or FIFO), 'Name' (joe-mikey-poc), and 'Configuration' (Visibility timeout, Message retention period, Delivery delay, Maximum message size, Receive message wait time). The 'Access policy' section is expanded, showing 'Basic' selected and a JSON editor containing a default policy. The 'Encryption - Optional' and 'Dead-letter queue - Optional' sections are also visible.

Queue joe-mikey-poc created successfully
You can now send and receive messages.

joe-mikey-poc

Details Info

Name: joe-mikey-poc Type: Standard

Encryption: -

URL: <https://sqs.us-west-2.amazonaws.com/xxxx/joe-mikey-poc>

ARN: arn:aws:sqs:us-west-2:xxxx:joe-mikey-poc

Dead-letter queue: -

SNS subscriptions | Lambda triggers | Dead-letter queue | Monitoring | Tagging | Access policy | Encryption

SNS subscriptions (0) Info

Subscription ARN Topic ARN

- Replace sqsUrl

```
sqsUrl: process.env.SQS_URL || https://sqs.us-west-2.amazonaws.com/xxxx/joe-mikey-poc
```

IAM

You can reference the official guideline from here <https://docs.aws.amazon.com/iam/index.html>

Your account contains 1 service and 1 feature.

Search results for 'iam'

Services (1)

IAM click Manage access to AWS resources

Features (10)

Documentation (46,744)

Marketplace (188)

See all 10 results ▾

Additional Information

Amazon SES Documentation
All SES Resources
Forums
Contact Us
Request Increased Sending Limits

Create policy

Identity and Access Management (IAM)

Dashboard

Access management

Groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Create policy Policy actions ▾

Filter policies Search

Policy name	Type	Used as	Description
AccessAnalyzerServiceRolePolicy	AWS managed	None	Allow Access Analyzer to analyze resource metadata
AdministratorAccess	Job function	None	Provides full access to AWS services and resources
AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permissions while explicitly allowing direct access to resources needed by Amplify ...
AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaForBusiness services
AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness resources and access to related AWS Services
AlexaForBusinessGatewayExecution	AWS managed	None	Provide gateway execution access to AlexaForBusiness services
AlexaForBusinessGatewayFullAccess	AWS managed	None	Provide access to iterative API services

Showing 787 results

Copy the json to the text-area

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ses:*",
        "s3:*",
        "sns:*"
      ],
      "Resource": "*"
    }
  ]
}
```

Create policy

1 2

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor **JSON** ①

Import managed policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "VisualEditor0",  
6       "Effect": "Allow",  
7       "Action": [  
8         "ses:*",  
9         "s3:*",  
10        "sns:*"  
11      ],  
12      "Resource": "*"  
13    }  
14  ]  
15}  
16
```

Character count: 128 of 6,144.

Cancel **Review policy** ③

Create policy

1 2

Review policy

Name* ①

Use alphanumeric and '+-, @-' characters. Maximum 128 characters.

Description

Maximum 1000 characters. Use alphanumeric and '+-, @-' characters.

Summary

Service	Access level	Resource	Request condition
Allow (4 of 264 services) Show remaining 260			
Pinpoint Email	Full access	All resources	None
S3	Full access	All resources	None
SES	Full access	All resources	None
SQS	Full access	All resources	None

* Required Cancel Previous **Create policy** ②

Create user

aws Services ▾

Identity and Access Management (IAM)

Dashboard

Access management

Groups

Users

Roles

Policies

Identity providers

Account settings

Add user Delete user

Find users by username or access key

User name	Groups	Access key age	Password age	Last activity	MFA	Creation time	Group count	ARN
am.aws.iam.703994918259.user/ten		2021-01-04 11:29 UTC+0800	0			2021-01-04 11:29 UTC+0800	0	arn:aws:iam:703994918259:user/ten
am.aws.iam.703994918259.user/Poc		2020-12-17 11:04 UTC+0800	0			2020-12-17 11:04 UTC+0800	0	arn:aws:iam:703994918259:user/Poc

Add user

1 2 3 4 5

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name* [Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type* **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

AWS Management Console access
Enables a **password** that allows users to sign-in to the AWS Management Console.

* Required

Cancel [Next: Permissions](#)

Add user

1 2 3 4 5

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](#)

Add user to group

[Create group](#) [Refresh](#)

Search		Showing 1 result
Group	Attached policies	

▶ Set permissions boundary

Cancel Previous [Next: Tags](#)

Add user

1 2 3 4 5

Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. [Learn more](#)

Key	Value (optional)	Remove
<input type="text" value="Add new key"/>	<input type="text"/>	Remove

You can add 50 more tags.

[Cancel](#) [Previous](#) [Next: Review](#)

Add user

1 2 3 4 5

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

⚠ This user has no permissions

You haven't given this user any permissions. This means that the user has no access to any AWS service or resource. Consider returning to the previous step and adding some type of permissions.

User details

User name joe-mikey-poc
AWS access type Programmatic access - with an access key
Permissions boundary Permissions boundary is not set

Tags

No tags were added.

[Cancel](#) [Previous](#) [Create user](#)

Add user

1 2 3 4 5

Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://aws.amazon.com/console>

Download .csv

	User	Access key ID	Secret access key
▶	joe-mikey-poc	AK [REDACTED]	***** Show

Close

- Replace `accessKeyId`, `secretAccessKey`

```
accessKeyId: process.env.ACCESSKEY_ID || "xxxxxxxxxx"
secretAccessKey: process.env.SECRET_ACCESS_KEY || "xxxxxxxxxx"
```

Create role

aws Services ▾ **Identity and Access Management (IAM)** **Joe-Mikey Global Support ▾**

Roles

Create role **Delete role**

Role name	Trusted entities	Creation time	Role ARN	Last activity
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Create role

Select type of trusted entity

AWS service EC2, Lambda and others	Another AWS account Belonging to you or 3rd party	Web identity Cognito or any OpenID provider	SAML 2.0 federation Your corporate directory
---------------------------------------	--	--	---

Allows entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

Account ID* 70 [redacted] [Edit](#) [Remove](#)

Options Require external ID (Best practice when a third party will assume this role) Require MFA [?](#)

* Required [Cancel](#) [Next: Permissions](#) [Previous](#)

Create role

Attach permissions policies

Choose one or more policies to attach to your new role.

[Create policy](#) [Filter policies](#) [Search](#) Showing 788 results

Policy name	Used as
AccessAnalyzerServiceRolePolicy	None
AdministratorAccess	None
AdministratorAccess-Amplify	None
AlexaForBusinessDeviceSetup	None
AlexaForBusinessFullAccess	None
AlexaForBusinessGatewayExecution	None
AlexaForBusinessLifecycleDelegatedAccessPolicy	None
AlexaForBusinessNetworkProfileServicePolicy	None

Set permissions boundary

* Required [Cancel](#) [Previous](#) [Next: Tags](#) [Next: Review](#)

Create role

Add tags (optional)

IAM tags are key-value pairs you can add to your role. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this role. [Learn more](#)

Key	Value (optional)	Remove
Add new key		

You can add 50 more tags.

* Required [Cancel](#) [Previous](#) [Next: Tags](#) [Next: Review](#)

Create role

Review

Provide the required information below and review this role before you create it.

Role name*	joe-mikey-poc-roles
Use alphanumeric and *-@_- characters. Maximum 64 characters.	
Role description	
Maximum 1000 characters. Use alphanumeric and *-@_- characters.	
Trusted entities	The ac...
Policies	Policies not attached
Permissions boundary	Permissions boundary is not set
No tags were added.	

* Required

Cancel Previous Create role

Edit roles permissions

Identity and Access Management (IAM)

- Dashboard
- Access management
 - Groups
 - Users
 - Roles**
 - Policies
 - Identity providers
 - Account settings
- Access reports
 - Access analyzer
 - Archive rules
 - Analyzers
 - Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Create role Delete role

Search

Role name	Trusted entities	Creation time	Role ARN	Last activity
joe-mikey-poc-roles	Account: 703994918259	2021-01-06 15:43 UTC+0800	arn:aws:iam::703994918259:role/joe-mikey-poc-roles	None

Identity and Access Management (IAM)

- Dashboard
- Access management
 - Groups
 - Users
 - Roles**
 - Policies
 - Identity providers
 - Account settings
- Access reports
 - Access analyzer
 - Archive rules
 - Analyzers
 - Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Summary

Role ARN: arn:aws:iam::703994918259:role/joe-mikey-poc-roles

Role description: Edit

Instance Profile ARNs: /

Creation time: 2021-01-06 15:43 UTC+0800

Last activity: Not accessed in the tracking period

Maximum session duration: 1 hour

Give this link to users who can switch roles in the console: <https://signin.aws.amazon.com/switchrole?roleName=joe-mikey-poc-roles&account=703994918259>

Permissions Trust relationships Tags Access Advisor Revoke sessions

Permissions policies

Get started with permissions: This role doesn't have any permissions yet. Get started by attaching one or more policies to this role. Learn more

Attach policies Add inline policy

Permissions boundary (not set)

Add permissions to joe-mikey-poc-roles

Attach Permissions

Joe-Mikey-Poc-policy

Joe-Mikey-Poc-policy

```

1 * {
2     "Version": "2012-10-17",
3     "Statement": [
4         {
5             "Sid": "VisualEditor0",
6             "Effect": "Allow",
7             "Action": [
8                 "execute-api:Invoke"
9             ],
10            "Resource": "*"
11        }
12    ]
13 }
14 }
15 }
```

Attach policy

Edit roles trust relationships

Copy user arn

Users > joe-mikey-poc

User ARN: arn:aws:iam::█████████████████████:user/joe-mikey-poc

Path: /

Creation time: 2021-01-06 15:33 UTC+0800

Permissions Groups Tags Security credentials Access Advisor

Permissions policies

Edit trust relationship

Roles > joe-mikey-poc-roles

Role ARN: arn:aws:iam:703994918259:role/joe-mikey-poc-roles

Role description: Edit

Instance Profile ARNs: Edit

Path: /

Creation time: 2021-01-06 15:43 UTC+0800

Last activity: Not accessed in the tracking period

Maximum session duration: 1 hour Edit

Give this link to users who can switch roles in the console: <https://signin.aws.amazon.com/switchrole?roleName=joe-mikey-poc-roles&account=703994918259>

Permissions Trust relationships Tags Access Advisor Revoke sessions

Edit trust relationship

Trusted entities: The account 703

Conditions: There are no conditions associated with this role.

- Replace s3RoleArn, sqsRoleArn

```
s3RoleArn: process.env.S3_ROLEARN || "arn:aws:iam::xxx:role/xxx"
sqsRoleArn: process.env.SQS_ARN || "arn:aws:iam:: xxx:role/xxx"
```

SES [optional]

If you want to use AWS SES as the email service, you can config this settings below, otherwise you can skip this part.

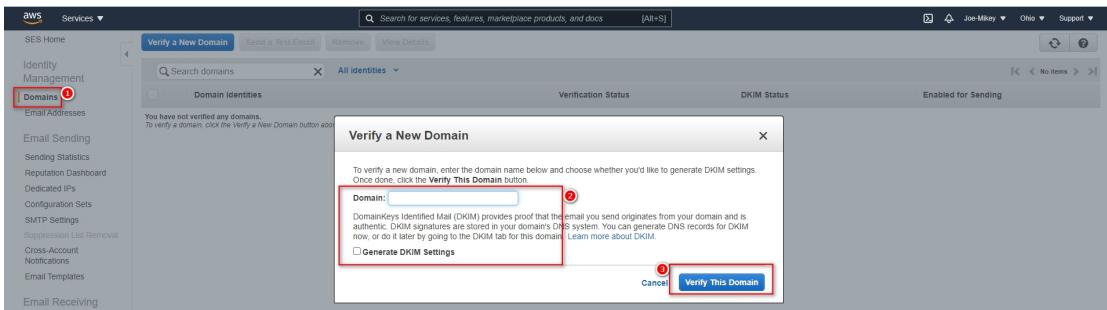
You can reference the official guideline from here <https://docs.aws.amazon.com/ses/index.html>

Sandbox

Sandbox environment need validation sender and to email address.

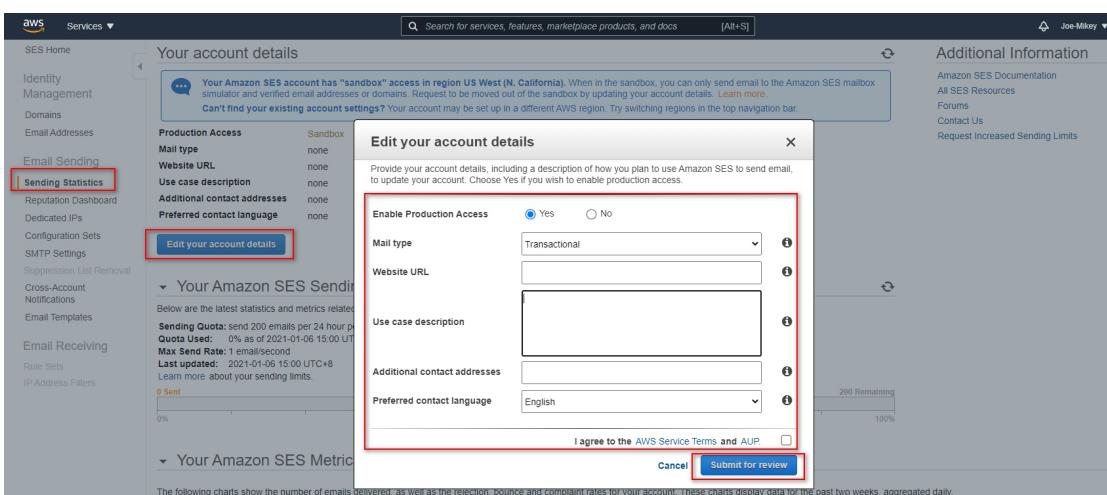
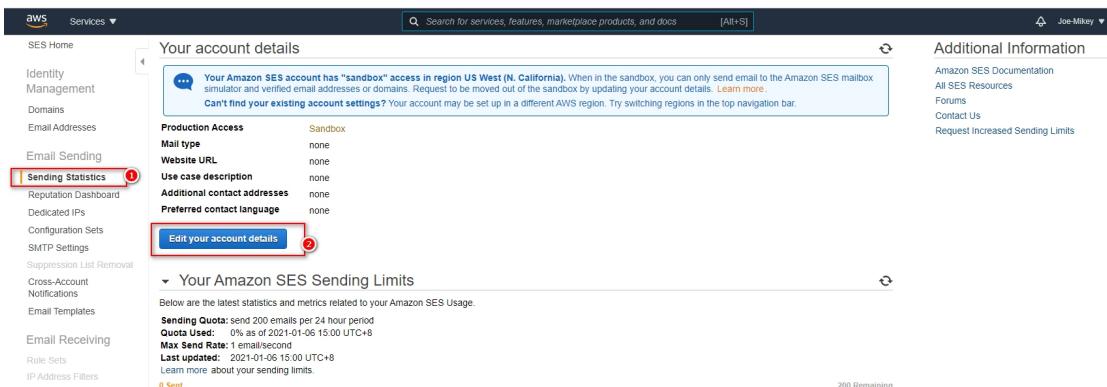
Email address verification

Domain verification



Production

Production environment can send email to any email address, but need raise application from aws team.



- Replace enableEmail, useAWSSES, sender

if you want to enable send email function and want to use AWS SES as the email service replace the sender, and change enableEmail to true and change useAWSSES to true

```
enableEmail: process.env.ENABLE_EMAIL || true
useAWSSES: process.env.USE_AWS_SES || true
sender: process.env.EMAIL_FROM || "xxx@xxx.com"
```