Loop AWS Config

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

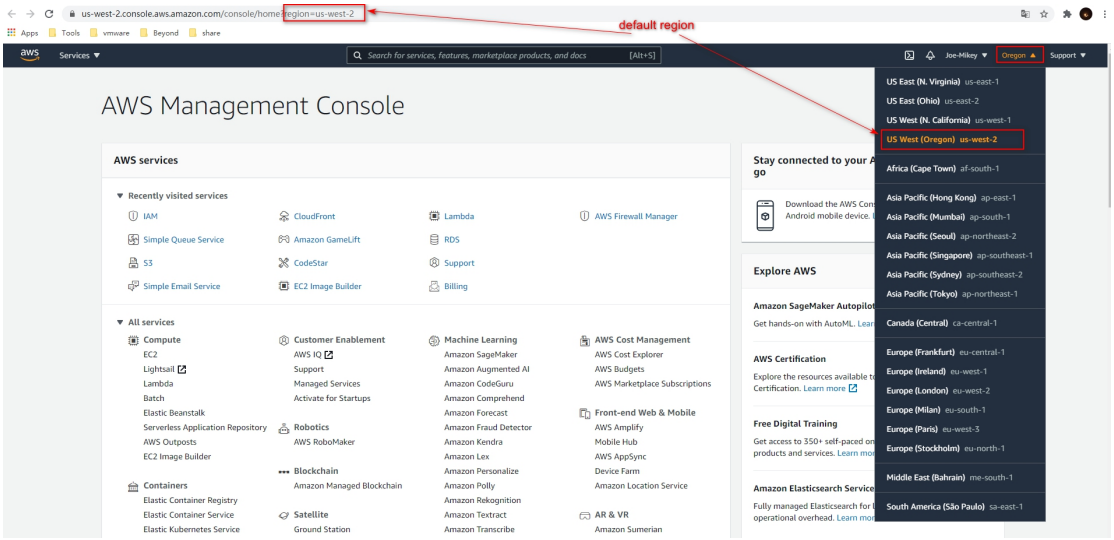
All customer config in this file: **annotation-service/config/app-os.js**

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



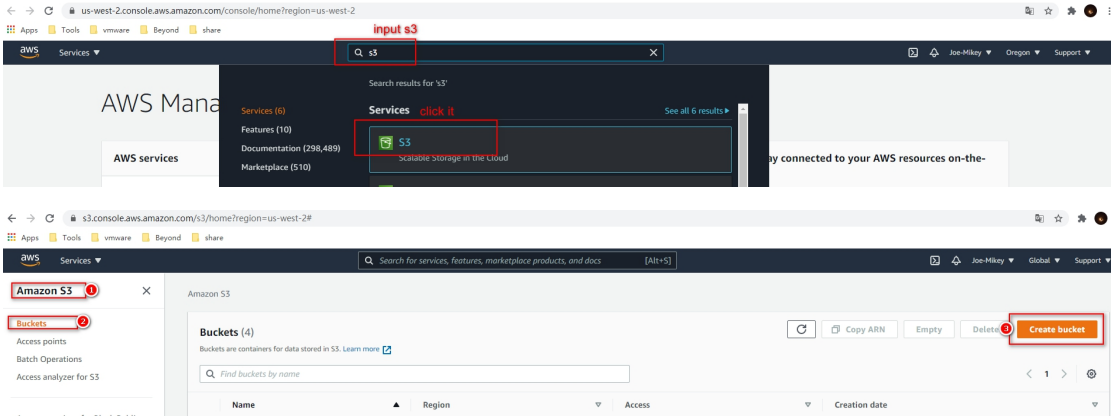
- Replace region

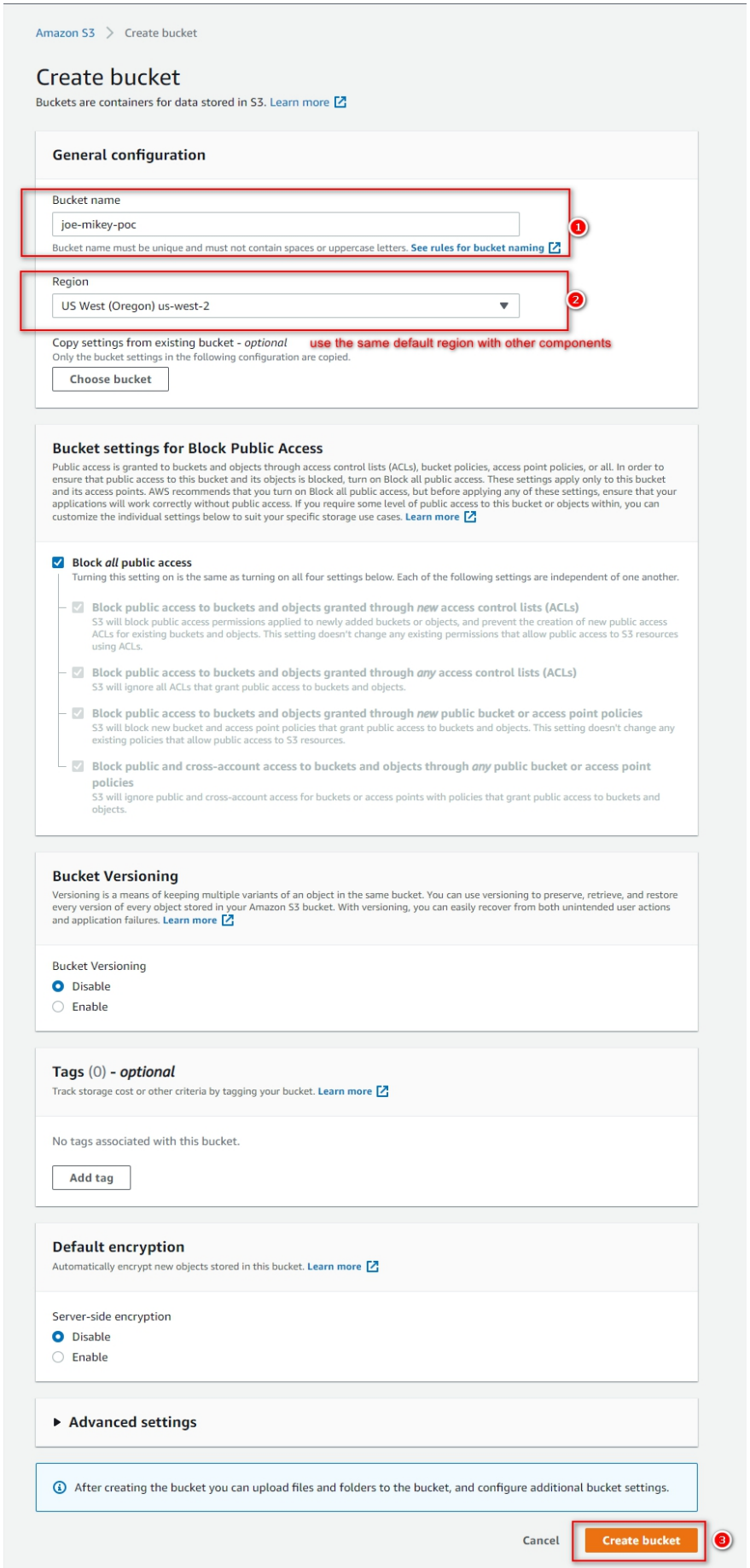
```
region: process.env.REGION || "us-west-2"
```

S3

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

Create Bucket

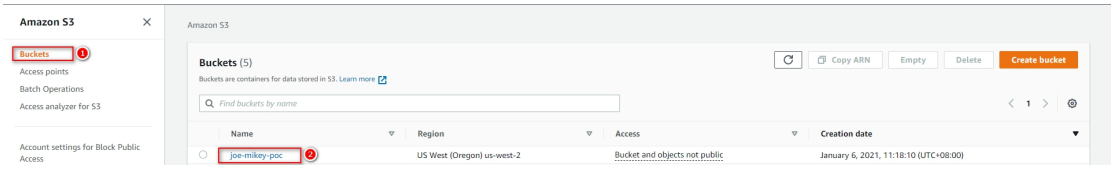


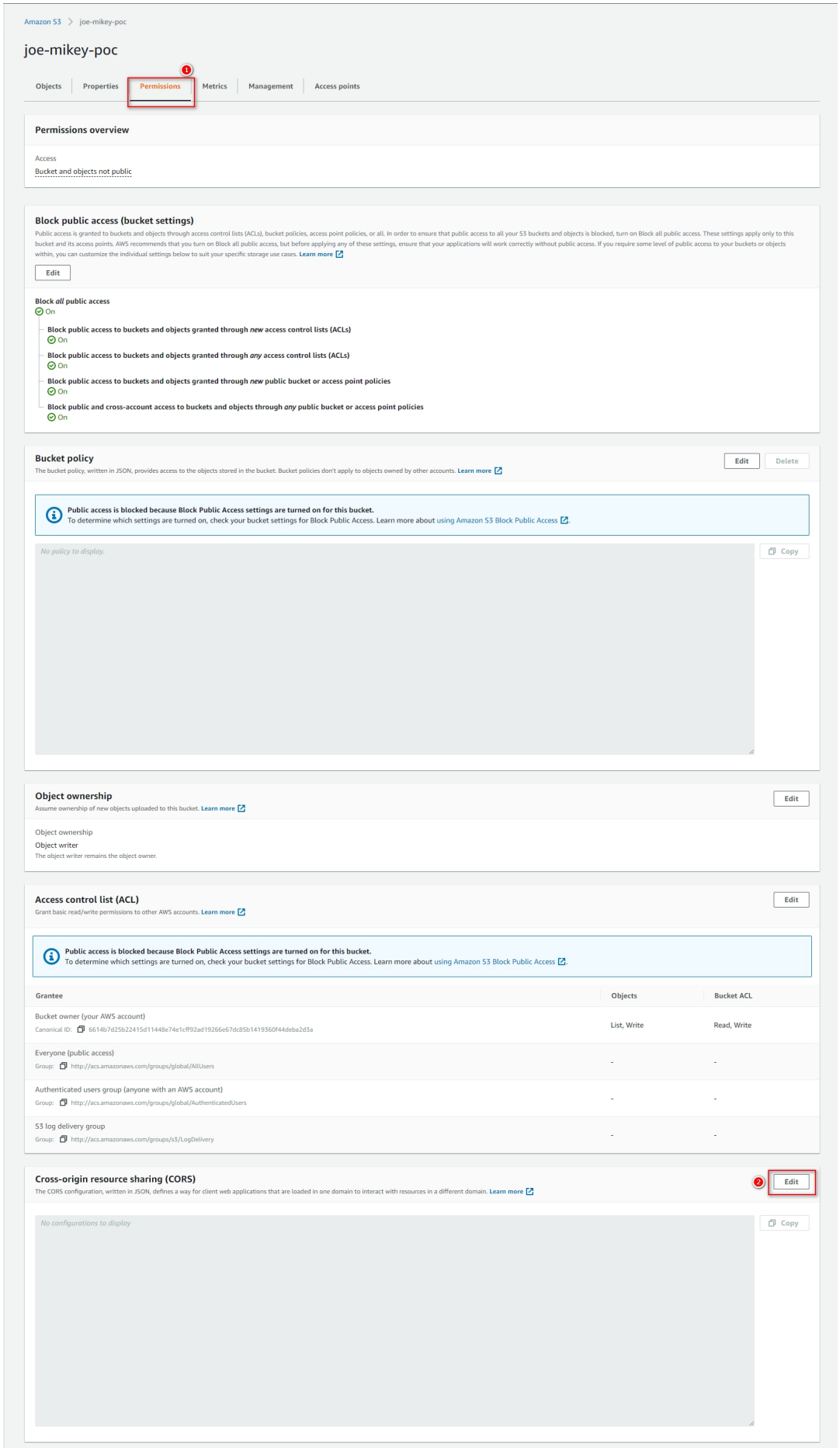

Amazon S3 > Create bucket
Create bucket
Buckets are containers for data stored in S3. Learn more
General configuration
Bucket name
joe-mikey-poc
Bucket name must be unique and must not contain spaces or uppercase letters. See rules for bucket naming
1
Region
US West (Oregon) us-west-2
2
Copy settings from existing bucket - optional
use the same default region with other components
Only the bucket settings in the following configuration are copied.
Choose bucket
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.
Add tag
Default encryption
Automatically encrypt new objects stored in this bucket. Learn more
Server-side encryption
Disable
Enable
Advanced settings
After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.
Cancel
Create bucket
3

- Replace bucketName

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

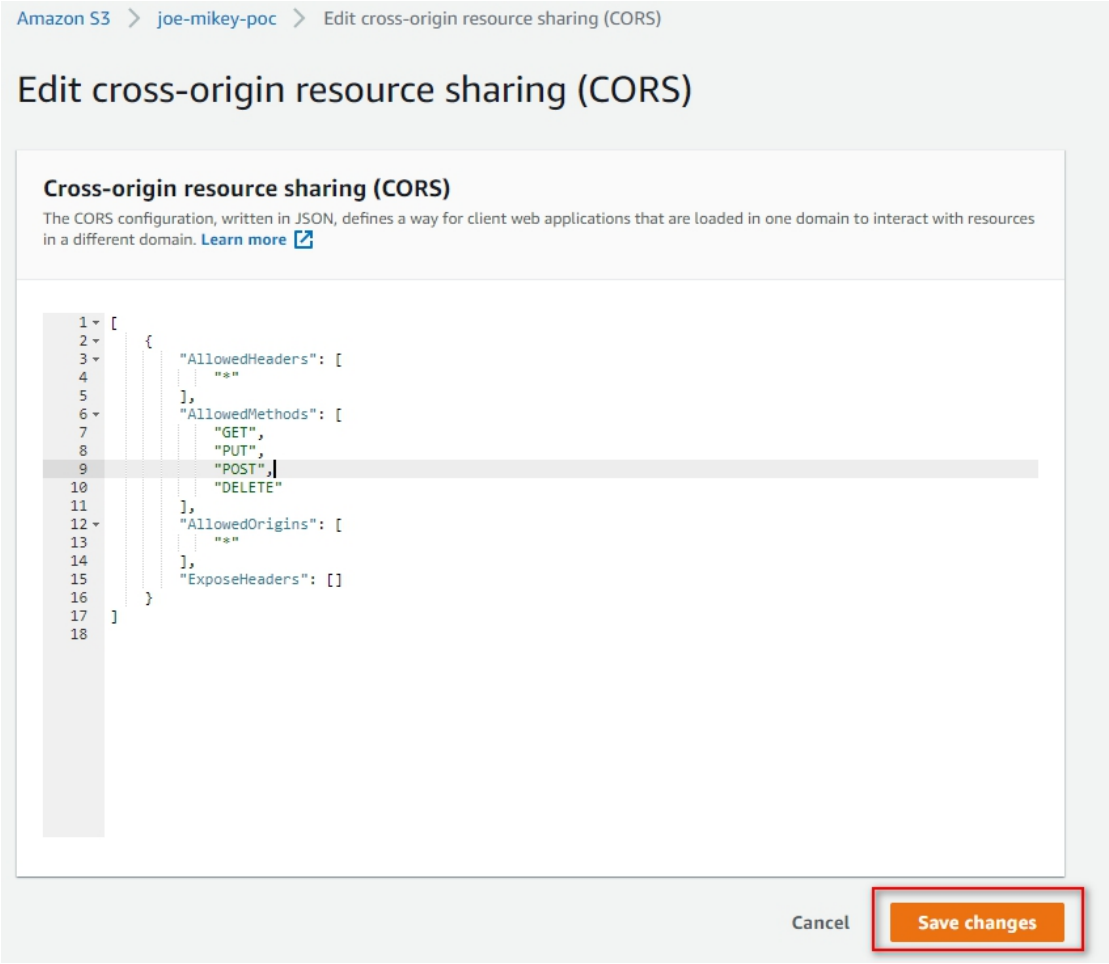
Edit Bucket permissions




Amazon S3 > joe-mikey-poc
joe-mikey-poc
Objects
Properties
Permissions
1
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: 6614b7d25b22415d11448e74e1cff92ad19266e67dc85b1419360f44deba2d3a
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
2
Edit
No configurations to display
Copy

Copy this json the edit input text-area

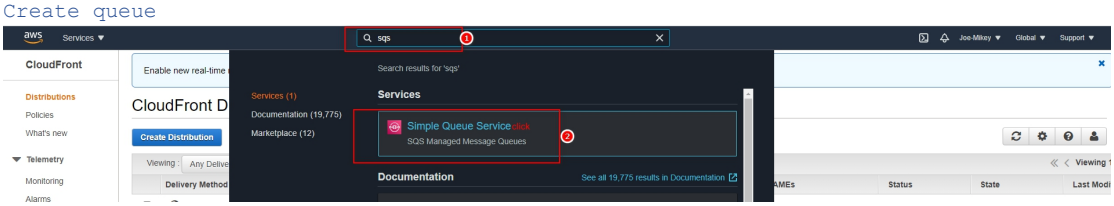
```
[
    {
        "AllowedHeaders": [
            "*"
        ],
        "AllowedMethods": [
            "GET",
            "PUT",
            "POST",
            "DELETE"
        ],
        "AllowedOrigins": [
            "*"
        ],
        "ExposeHeaders": []
    }
]
```

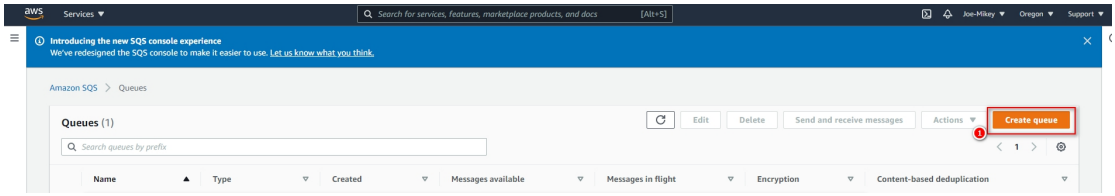


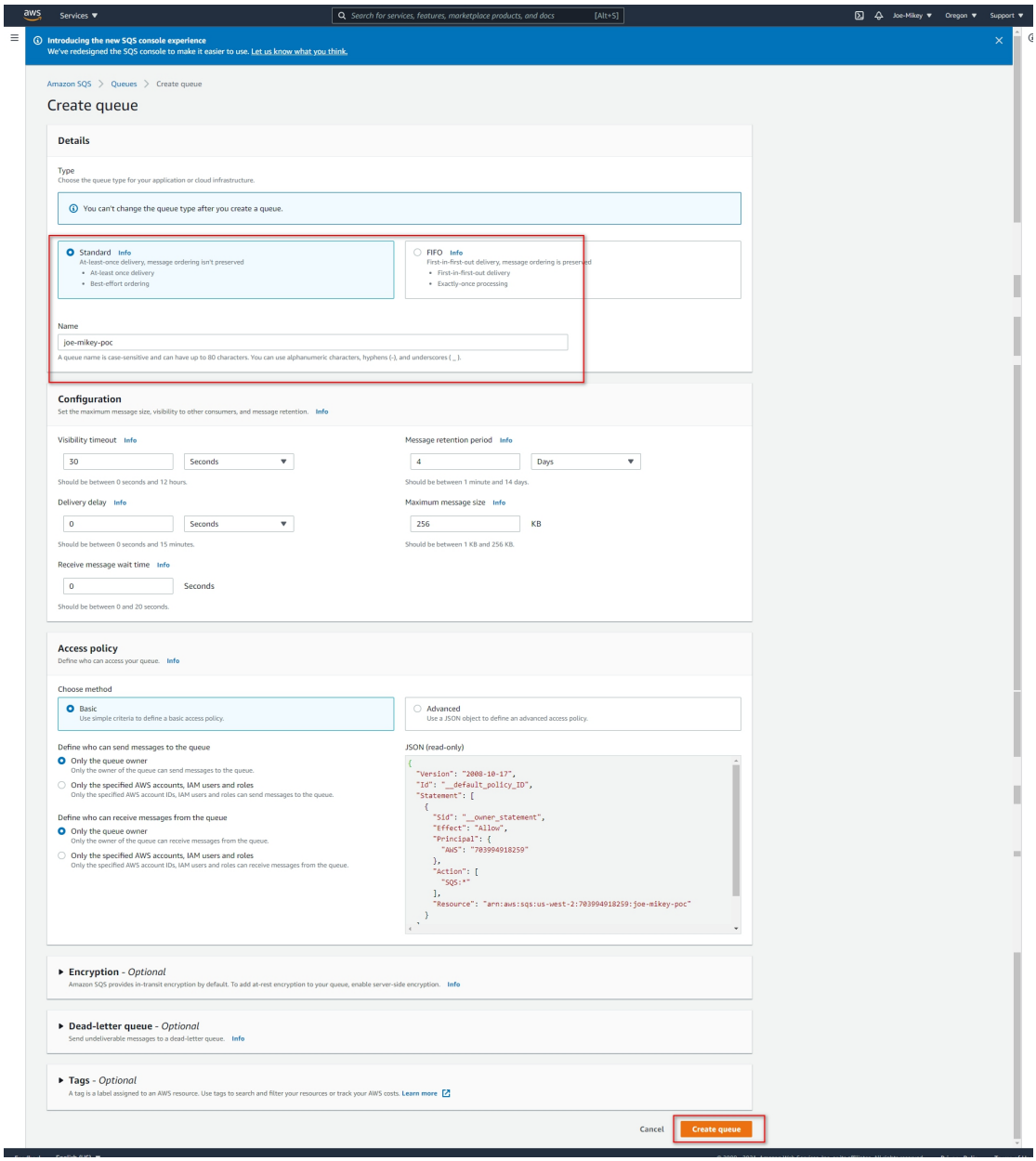
SQS

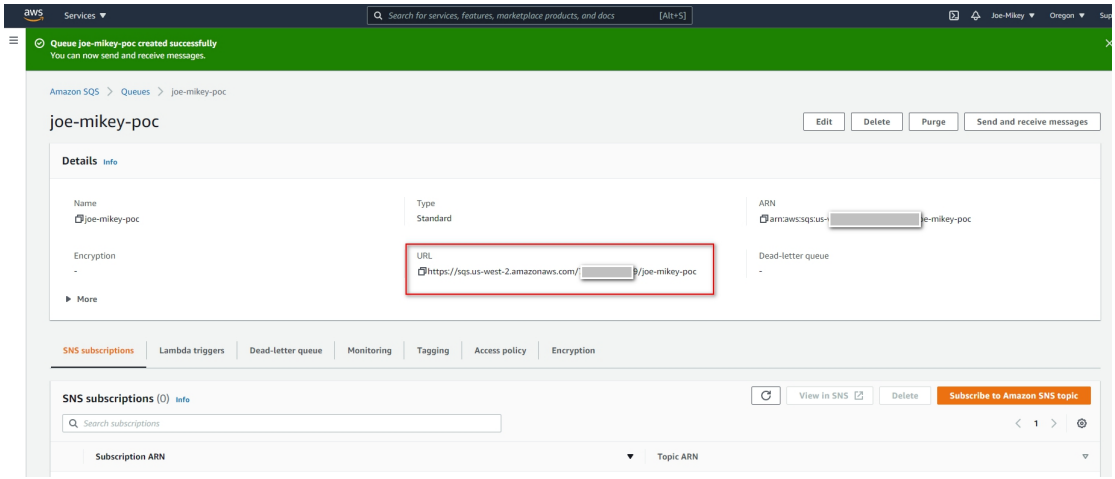
You can reference the official guideline from here https://docs.aws.amazon.com/sqs/index.html

`Create queue`




Services
Search for services, features, marketplace products, and docs [Alt+S]
Joe-Mikey
Oregon
Support
Introducing the new SQS console experience
We've redesigned the SQS console to make it easier to use. Let us know what you think.
Amazon SQS > Queues
Queues (1)
Edit
Delete
Send and receive messages
Actions
Create queue
Search queues by prefix
Name
Type
Created
Messages available
Messages in flight
Encryption
Content-based deduplication


Services
Search for services, features, marketplace products, and docs [Alt+S]
Joe-Mikey
Oregon
Support
Introducing the new SQS console experience
We've redesigned the SQS console to make it easier to use. Let us know what you think.
Amazon SQS > Queues > Create queue
Create queue
Details
Type
Choose the queue type for your application or cloud infrastructure.
You can't change the queue type after you create a queue.
Standard Info
At-least-once delivery, message ordering isn't preserved
At-least once delivery
Best-effort ordering
FIFO Info
First-in-first-out delivery, message ordering is preserved
First-in-first-out delivery
Exactly-once processing
Name
joe-mikey-poc
A queue name is case-sensitive and can have up to 80 characters. You can use alphanumeric characters, hyphens (-), and underscores (_).
Configuration
Set the maximum message size, visibility to other consumers, and message retention. Info
Visibility timeout Info
30
Seconds
Should be between 0 seconds and 12 hours.
Message retention period Info
4
Days
Should be between 1 minute and 14 days.
Delivery delay Info
0
Seconds
Should be between 0 seconds and 15 minutes.
Maximum message size Info
256
KB
Should be between 1 KB and 256 KB.
Receive message wait time Info
0
Seconds
Should be between 0 and 20 seconds.
Access policy
Define who can access your queue. Info
Choose method
Basic
Use simple criteria to define a basic access policy.
Advanced
Use a JSON object to define an advanced access policy.
Define who can send messages to the queue
Only the queue owner
Only the owner of the queue can send messages to the queue.
Only the specified AWS accounts, IAM users and roles
Only the specified AWS account IDs, IAM users and roles can send messages to the queue.
Define who can receive messages from the queue
Only the queue owner
Only the owner of the queue can receive messages from the queue.
Only the specified AWS accounts, IAM users and roles
Only the specified AWS account IDs, IAM users and roles can receive messages from the queue.
JSON (read-only)
{
"Version": "2008-10-17",
"Id": "__default_policy_ID",
"Statement": [
{
"Sid": "__owner_statement",
"Effect": "Allow",
"Principal": {
"AWS": "703994918259"
},
"Action": [
"SQS:*"
],
"Resource": "arn:aws:sqs:us-west-2:703994918259:joe-mikey-poc"
}
Encryption - Optional
Amazon SQS provides in-transit encryption by default. To add at-rest encryption to your queue, enable server-side encryption. Info
Dead-letter queue - Optional
Send undeliverable messages to a dead-letter queue. Info
Tags - Optional
A tag is a label assigned to an AWS resource. Use tags to search and filter your resources or track your AWS costs. Learn more
Cancel
Create queue

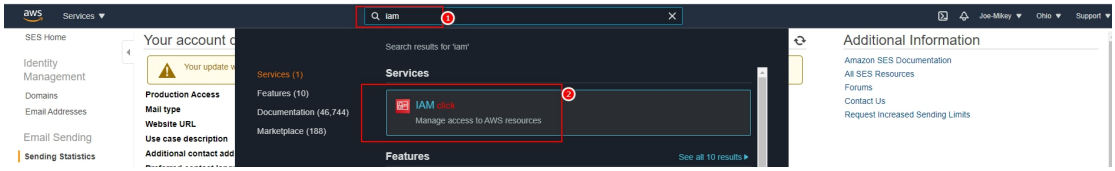


- Replace sqsUrl

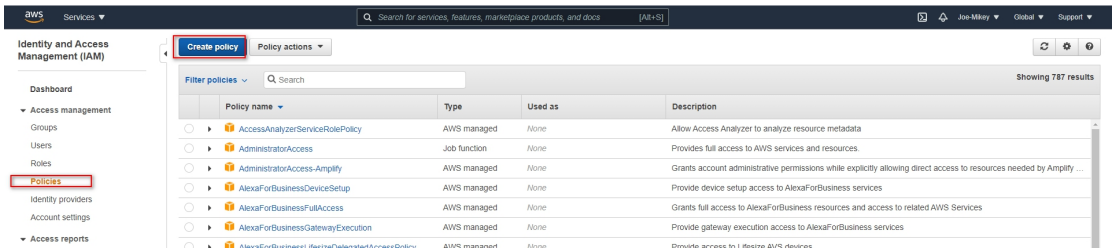
```
sqsUrl: process.env.SQS_URL || https://sqs.us-west-2.amazonaws.com/xxx/joe-mikey-poc
```

IAM

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

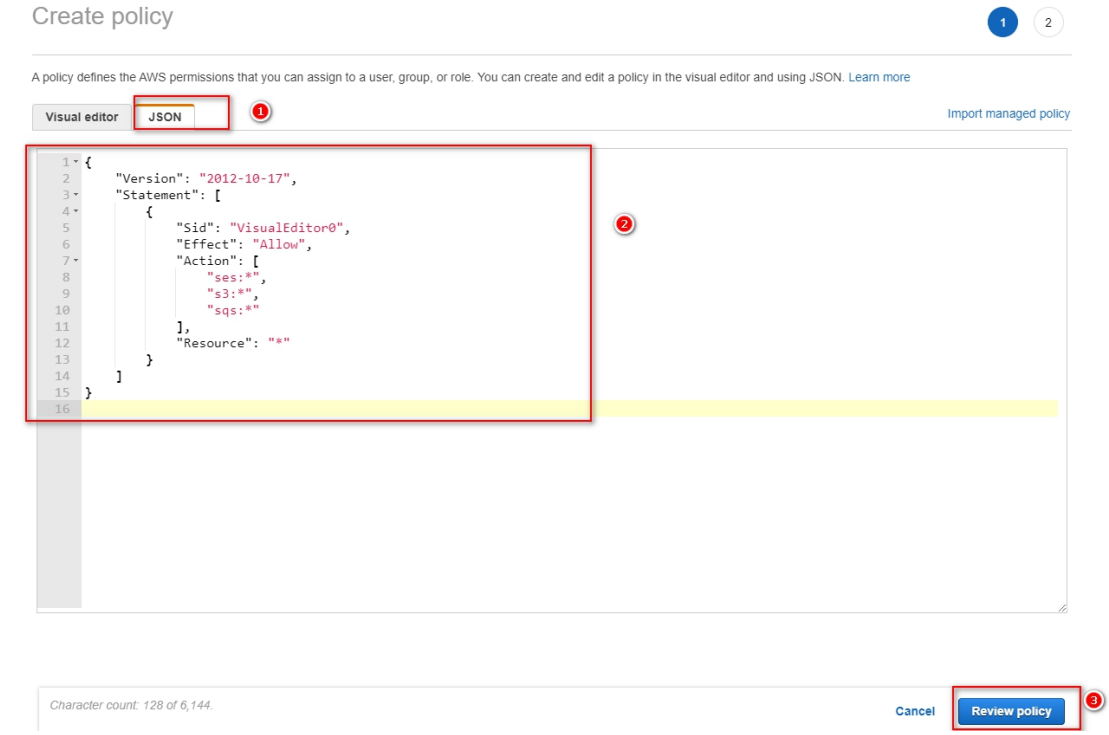


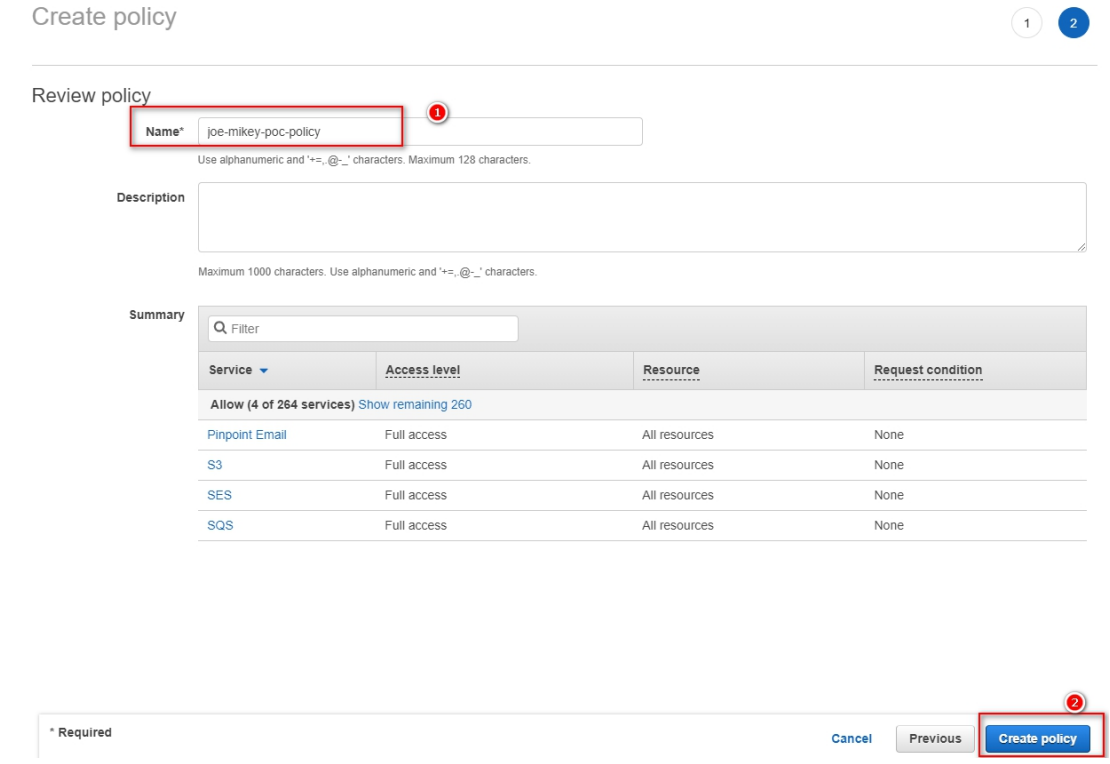
Create policy



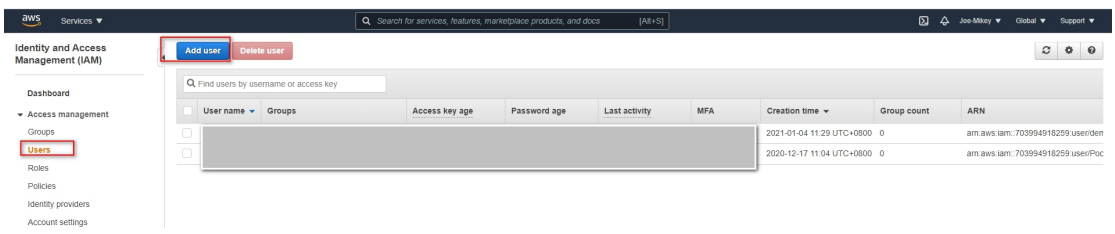
Copy the json to the text-area

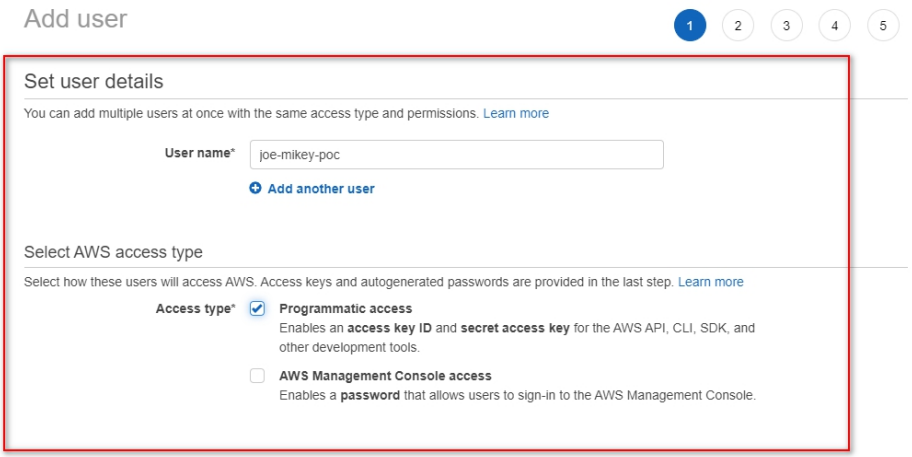
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ses:*",
                "s3:*",
                "sqs:*"
            ],
            "Resource": "*"
        }
    ]
}
```


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
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "VisualEditor0",
"Effect": "Allow",
"Action": [
"ses:*",
"s3:*",
"sqs:*"
],
"Resource": "*"
}
]
}
2
Character count: 128 of 6,144.
Cancel
Review policy
3

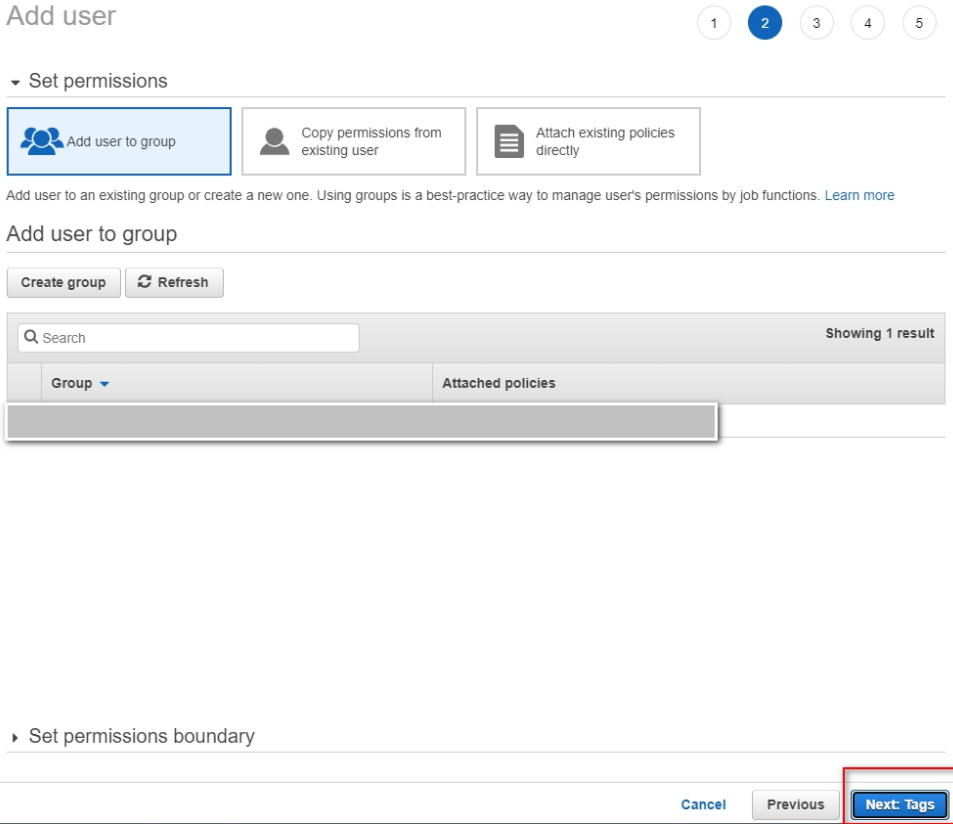

Create policy
1
2
Review policy
Name*
joe-mikey-poc-policy
1
Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.
Description
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.
Summary
Filter
Service
Access level
Resource
Request condition
Allow (4 of 264 services) Show 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
2
* Required
Cancel
Previous
Create policy

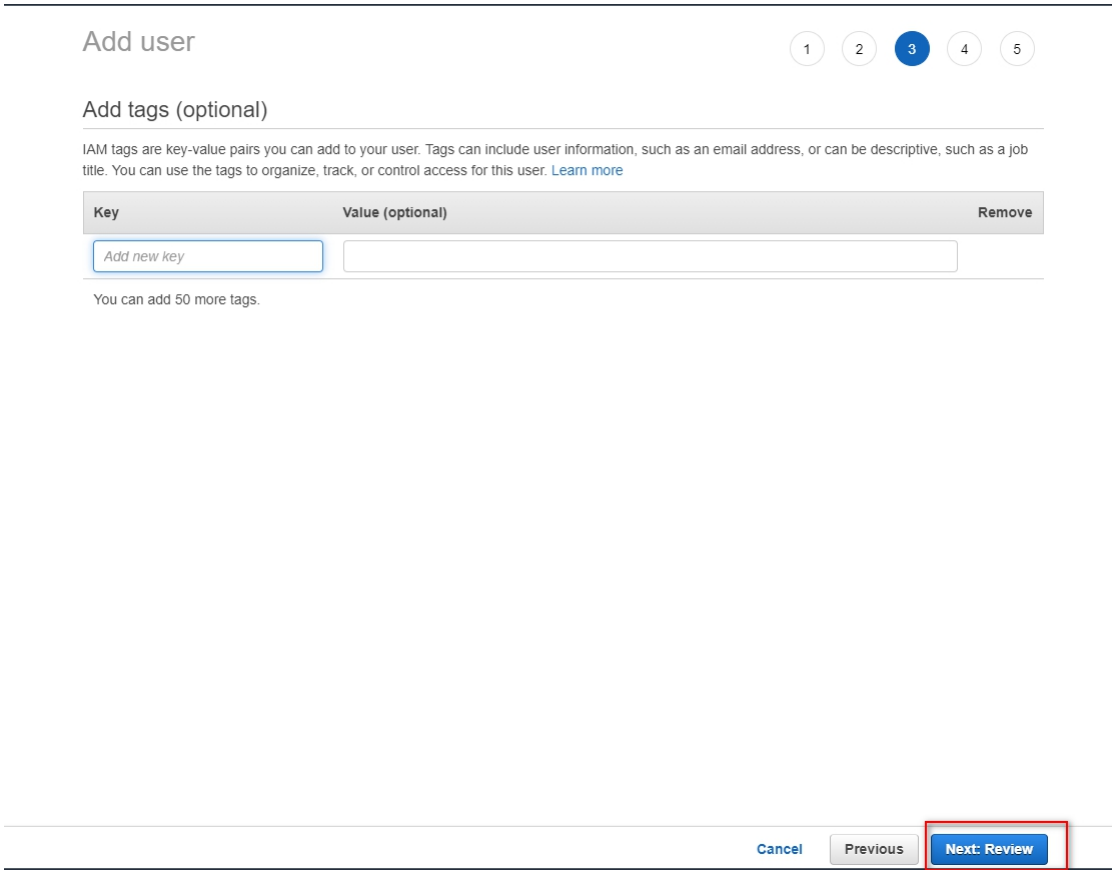
Create user

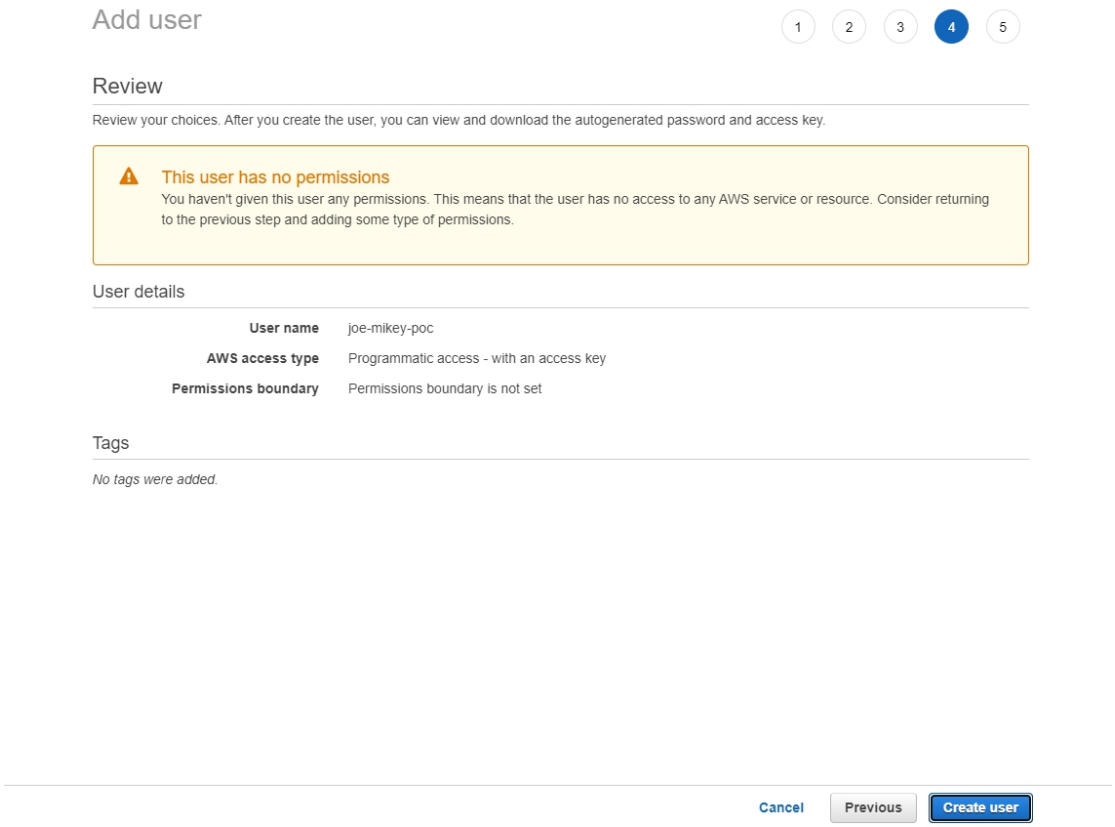

aws
Services
Search for services, features, marketplace products, and docs
[Alt+S]
Joe-Mikey
Global
Support
Identity and Access Management (IAM)
Add user
Delete user
Dashboard
Access management
Groups
Users
Roles
Policies
Identity providers
Account settings
Find users by username or access key
User name
Groups
Access key age
Password age
Last activity
MFA
Creation time
Group count
ARN
2021-01-04 11:29 UTC+0800
0
2020-12-17 11:04 UTC+0800
0

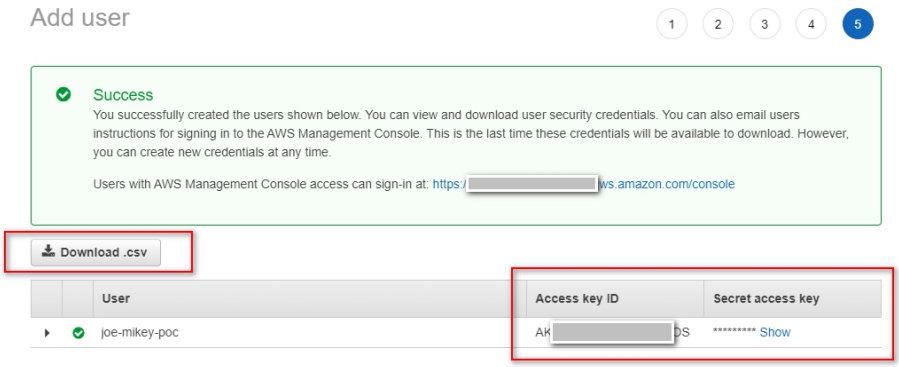

Add user
1 2 3 4 5
Set user details
You can add multiple users at once with the same access type and permissions. Learn more
User name*
joe-mikey-poc
Add another user
Select AWS access type
Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. 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 group
Copy permissions from existing user
Attach existing policies directly
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
Add new key
You can add 50 more tags.
Cancel
Previous
Next: Review

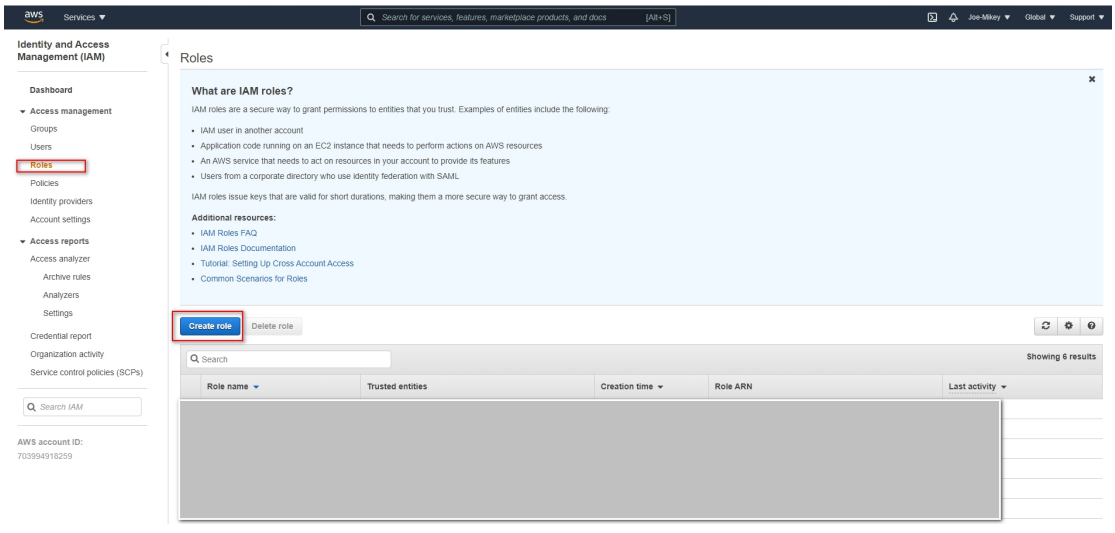

Add user
1 2 3 4 5
Review
Review your choices. After you create the user, you can view and download the autogenerated password and access key.
This user has no permissions
You haven't given this user any permissions. This means that the user has no access to any AWS service or resource. Consider returning 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

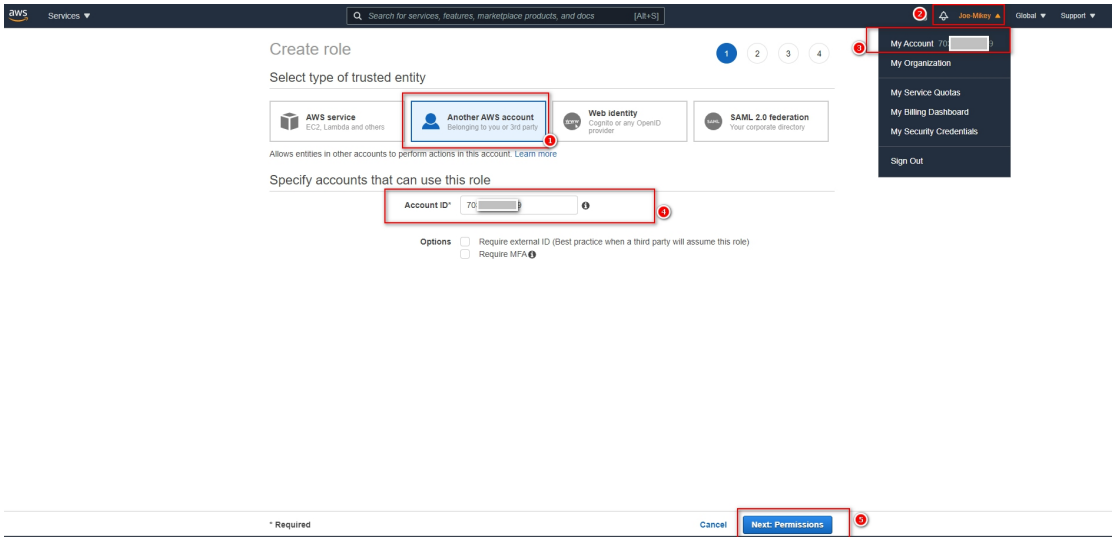


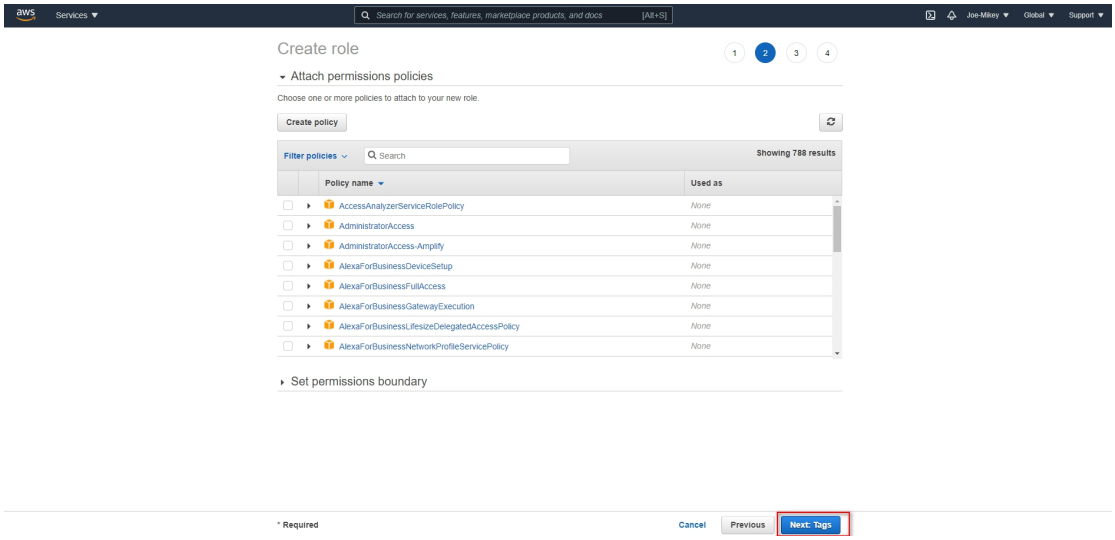
- Replace accessKeyId, secretAccessKey

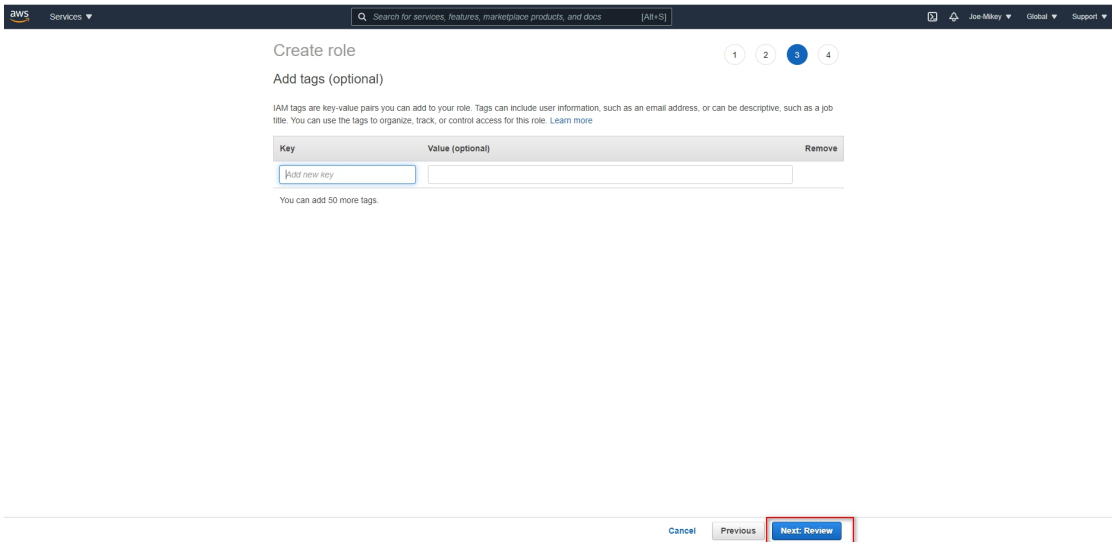
```
accessKeyId: process.env.ACCESSKEY_ID || "xxxxxxxxx"
secretAccessKey: process.env.SECRET_ACCESS_KEY || "xxxxxxxxx"
```

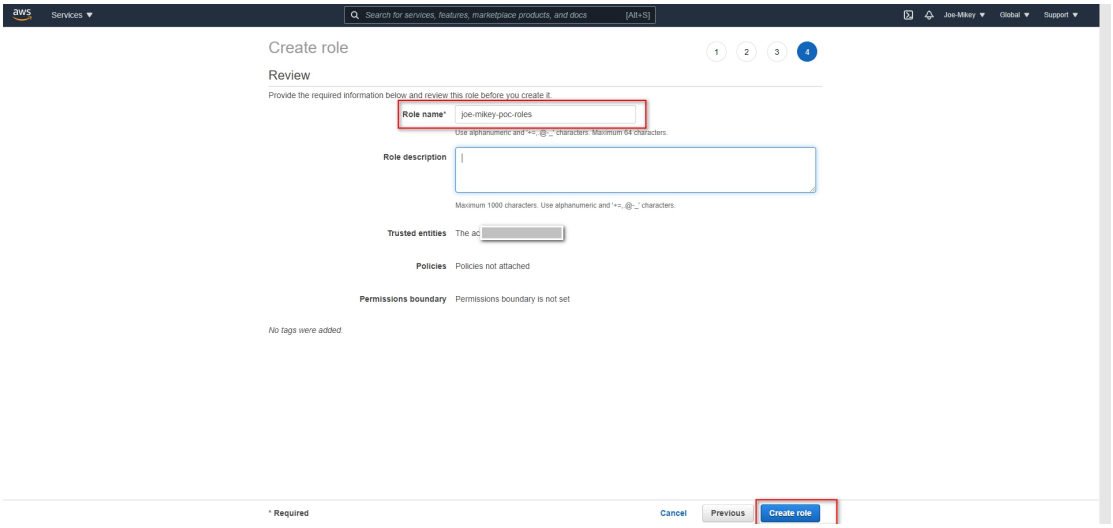
Create role



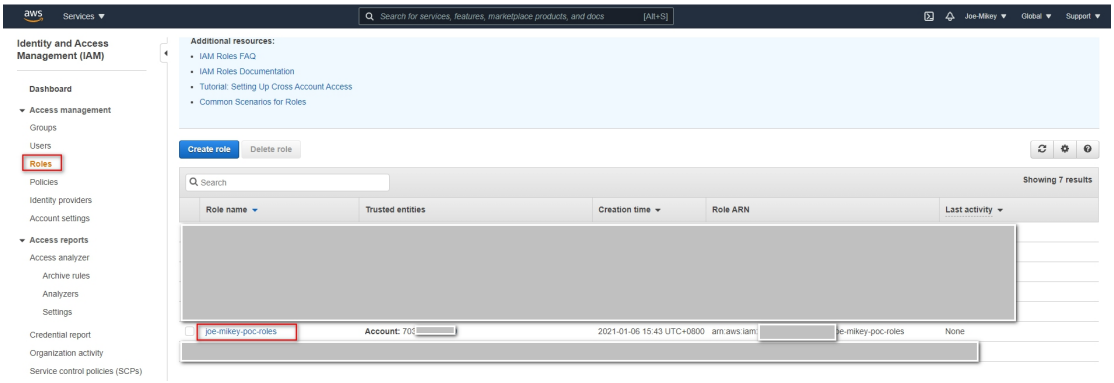

Services
Search for services, features, marketplace products, and docs [Alt+S]
Joe-Mikey
Global
Support
My Account
My Organization
My Service Quotas
My Billing Dashboard
My Security Credentials
Sign Out
Create role
Select type of trusted entity
AWS service
EC2, Lambda and others
Another AWS account
Belonging 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*
Options
Require external ID (Best practice when a third party will assume this role)
Require MFA
* Required
Cancel
Next: Permissions

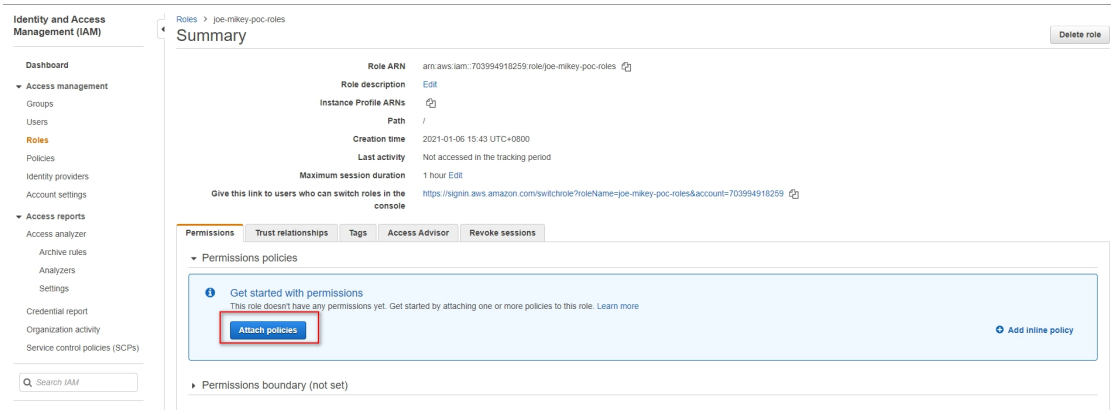

Services
Search for services, features, marketplace products, and docs [Alt+S]
Joe-Mikey
Global
Support
Create role
Attach permissions policies
Choose one or more policies to attach to your new role.
Create policy
Filter policies
Search
Showing 788 results
Policy name
Used as
AccessAnalyzerServiceRolePolicy
AdministratorAccess
AdministratorAccess-Amplify
AlexaForBusinessDeviceSetup
AlexaForBusinessFullAccess
AlexaForBusinessGatewayExecution
AlexaForBusinessLifesizeDelegatedAccessPolicy
AlexaForBusinessNetworkProfileServicePolicy
None
Set permissions boundary
* Required
Cancel
Previous
Next: Tags

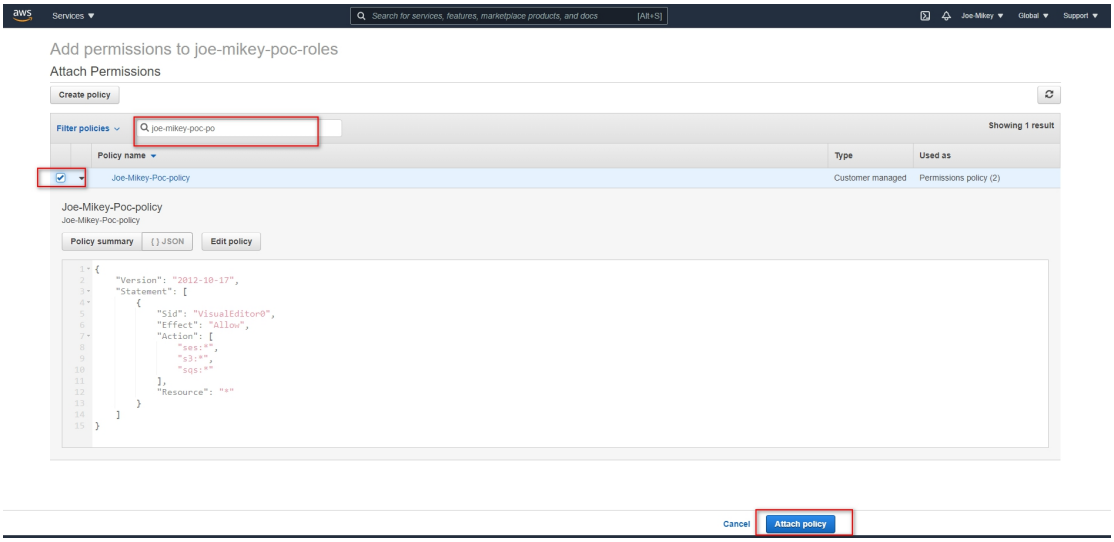

Services
Search for services, features, marketplace products, and docs [Alt+S]
Joe-Mikey
Global
Support
Create role
Add tags (optional)
IAM tags are key-value pairs you can add to your role. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can 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.
Cancel
Previous
Next: Review



Edit roles permissions

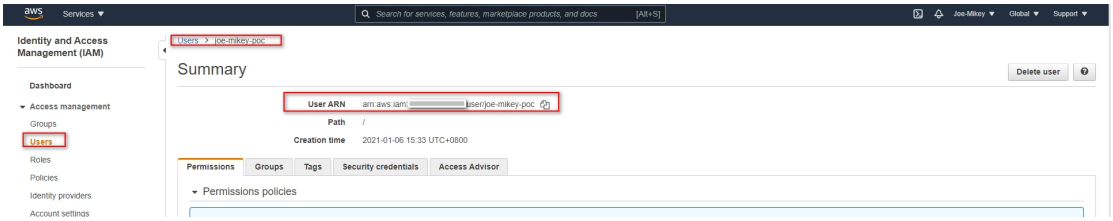




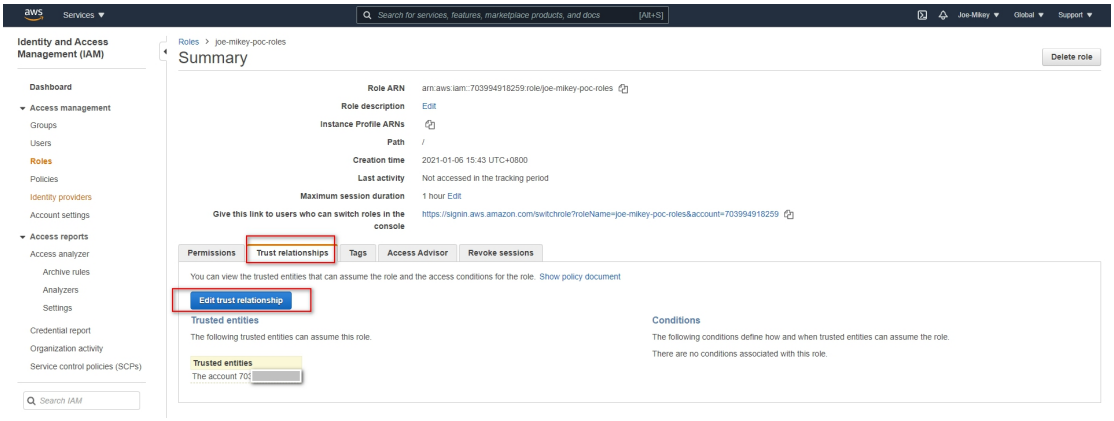


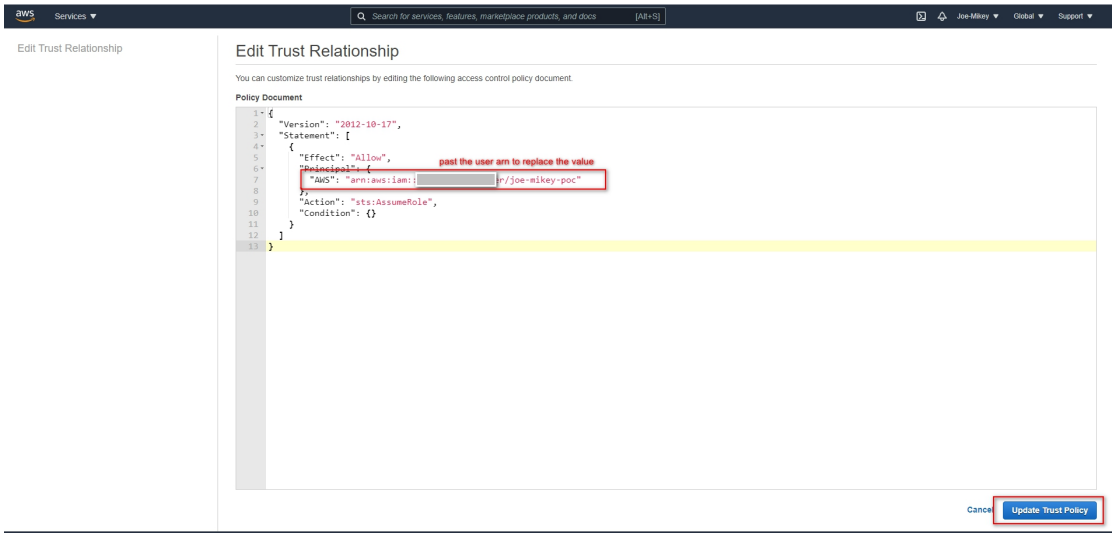
Edit roles trust relationships

Copy user arn

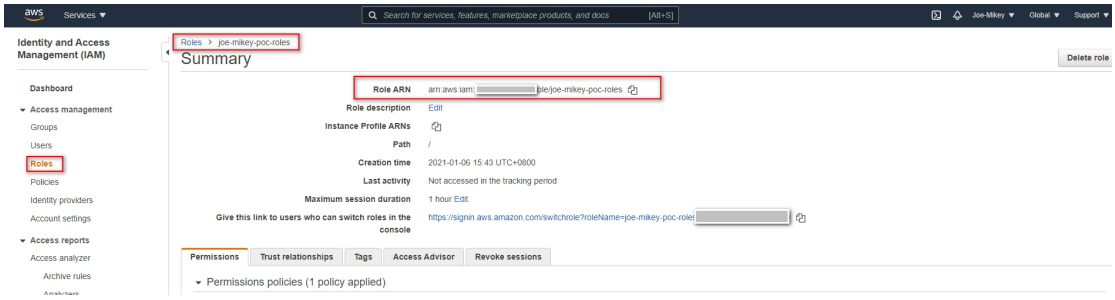


Edit trust relationship





- Replace s3RoleArn, sqsRoleArn

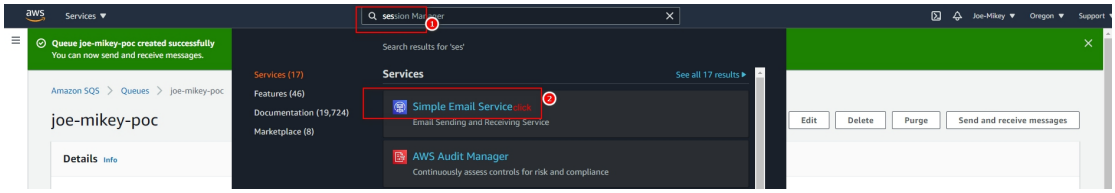



```
s3RoleArn: process.env.S3_ROLEARN || "arn:aws:iam::xxx:role/xxx"
sqsRoleArn: process.env.SQS_ARN || "arn:aws:iam:: xxx:role/xxx"
```

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.

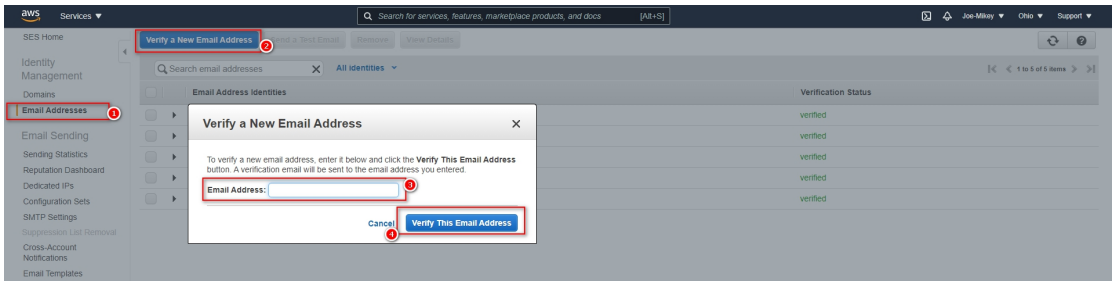
You can reference the official guideline from here https://docs.aws.amazon.com/ses/index.html



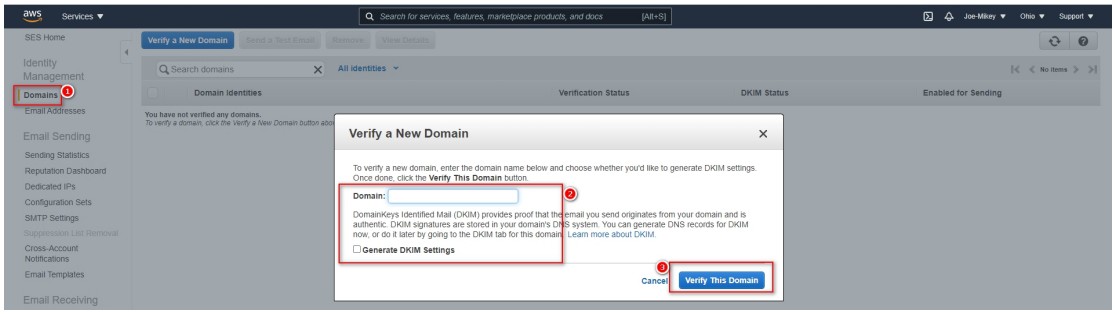
Sandbox

Sandbox environment need validation sender and to email address.

Email address verification

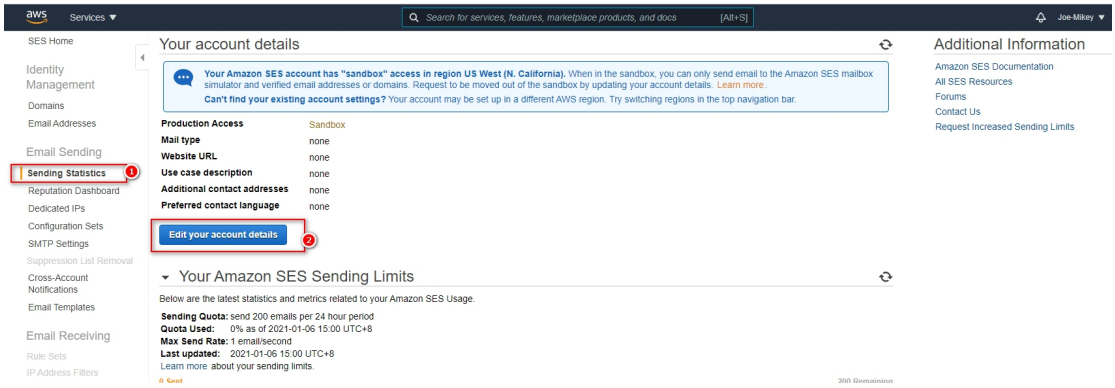


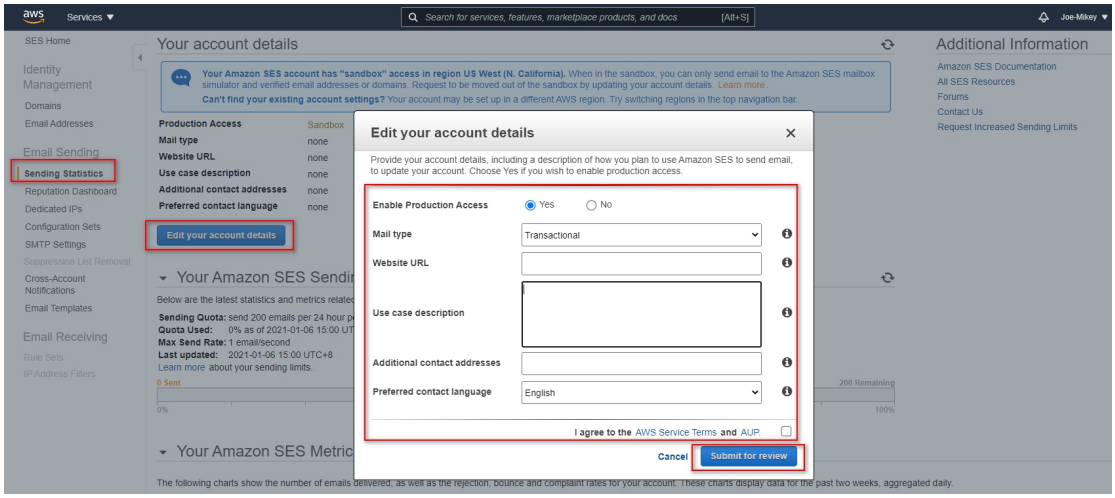
Domain verification



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"
```