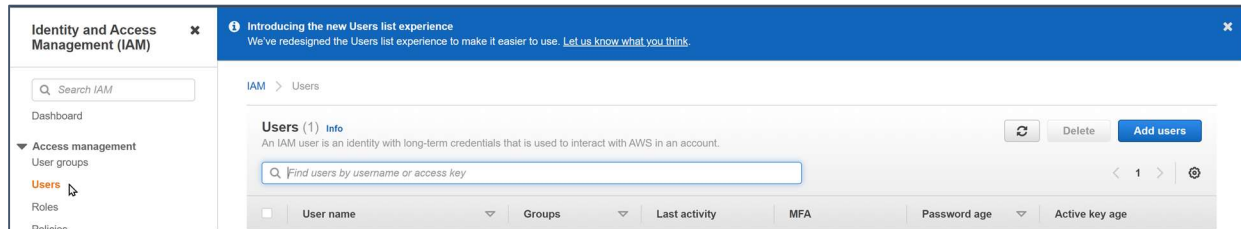


AWS IAM

User creation:

Navigate to IAM Dashboard and click on users



Enter username “user1” and select AWS credential type as “Access key”

Add user

12345

Set user details

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

User name*

user1

+ Add another user

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Select AWS credential type*

☒ Access key - Programmatic access

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

☐ Password - AWS Management Console access

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

* Required

Cancel

Next: Permissions

Attach the Administrator Access for this demo purpose so that we do not have any restrictions

Add user

12345

Set permissions

Add user to group

Copy permissions from existing user

Attach existing policies directly

Create policy

Filter policies

Showing 730 results

	Policy name	Type	Used as
<input checked="" type="checkbox"/>	AdministratorAccess	Job function	None
<input type="checkbox"/>	AdministratorAccess-Amplify	AWS managed	None
<input type="checkbox"/>	AdministratorAccess-AWSElasticBeanstalk	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessFullAccess	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessLifeSizeDelegatedAccessPolicy	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessReadOnlyAccess	AWS managed	None
<input type="checkbox"/>	allow_all	Customer managed	Permissions policy (1)
<input type="checkbox"/>	AmazonAPIGatewayAdministrator	AWS managed	None
<input type="checkbox"/>	AmazonAPIGatewayInvokeFullAccess	AWS managed	None
<input type="checkbox"/>	AmazonAPIGatewayPushToCloudWatchLogs	AWS managed	None
<input type="checkbox"/>	AmazonAppFlowFullAccess	AWS managed	None

CancelPreviousNext: Tags

Add tags (optional)

Add user

12345

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"/>	

You can add 50 more tags.

CancelPreviousNext: Review

Review and Create user.

Add user

12345

Review

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

User details

User name	user1
AWS access type	Programmatic access - with an access key
Permissions boundary	Permissions boundary is not set

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	AdministratorAccess

Tags

No tags were added.

CancelPreviousCreate user

User creation complete.

Add user

12345

✓ 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://566716581275.signin.aws.amazon.com/console>

Download .csv

	User	Access key ID	Secret access key
▶ ✓	user1	AKIAYH4XQYWN7ZIY73N6	***** Show

Save the Access Key ID and Secret access key that will be used in configuring on the EC2 instance under `~/.aws/credentials` file

Add user

12345

✓ **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://566716581275.signin.aws.amazon.com/console>

Download .csv

	User	Access key ID	Secret access key
▼	✓ user1	AKIAYH4XQYWN7ZIY73N6	BN0exPKyjgm/C6IRQpGSd bQJhQ0pg8UZdzKjNv7V Hide

✓ Created user user1

✓ Attached policy AdministratorAccess to user user1

✓ Created access key for user user1

Close

After creation, User listed under IAM dashboard.

Identity and Access Management (IAM)

Unable to load search
Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Introducing the new Users list experience

IAM > Users

Users (3) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Find users by username or access key

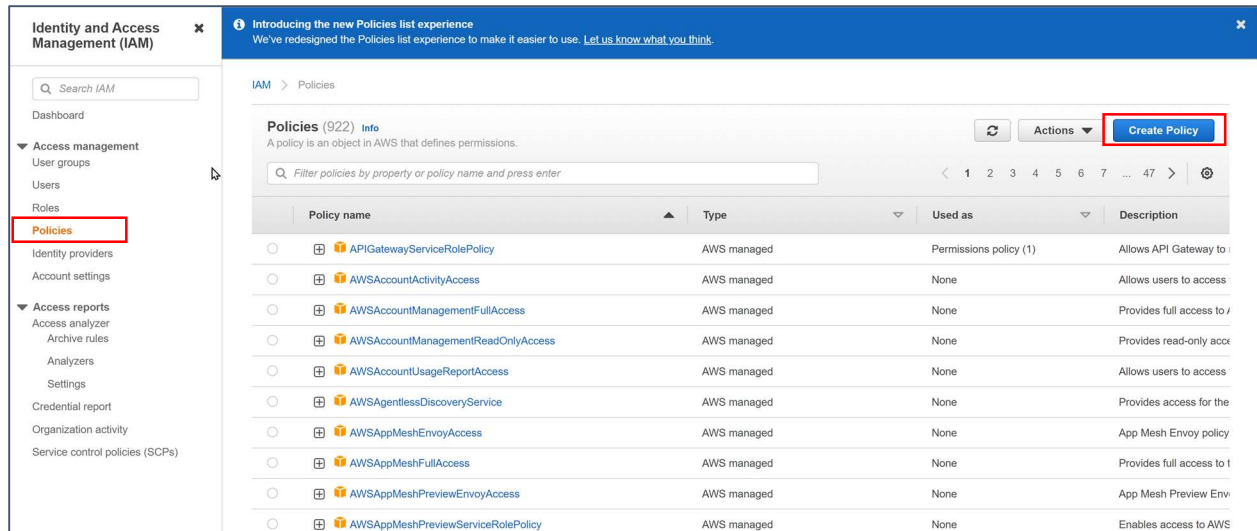
Refresh Delete Add users

< 1 > ⚙

	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	corestack-d9918	None	Never	None	⚠ 600 days ago	-
<input type="checkbox"/>	user1	None	✓ 2 hours ago	None	None	✓ 3 hours ago

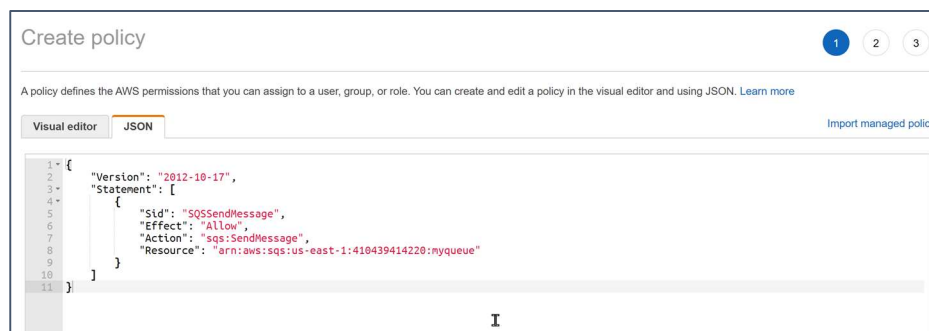
Policy Creation:

On the IAM dashboard, navigate to Policies and **Create Policy**

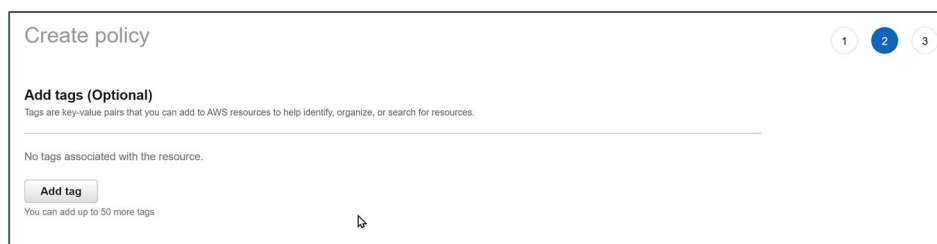


Create a policy to Send Message Action. Use the JSON panel to add the following code snippet

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SQSSendMessage",
      "Effect": "Allow",
      "Action": "sqs:SendMessage",
      "Resource": "arn:aws:sqs:us-east-1:410439414220:myqueue"
    }
  ]
}
```



Next, adding tags is not mandatory but can be useful for filtering. We will not add any tags at this point.



Review and Create Policy SQSSendMessagePolicy

Create policy

1 2 3

Review policy

Name* SQSSendMessagePolicy

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

Description

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

Summary

Filter

Service	Access level	Resource	Request condition
Allow (1 of 315 services) Show remaining 314			
SQS	Limited: Write	QueueName string like MyQueue	None

Tags

Key	Value
No tags associated with the resource.	

Create another policy to Receive and Delete Message Action. Use the JSON panel to add the following code snippet

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SQSReceiveDeleteMessage",
      "Effect": "Allow",
      "Action": [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage"
      ],
      "Resource": "arn:aws:sqs:us-east-1:410439414220:myqueue"
    }
  ]
}
```

Create policy

1 2 3

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

Import managed policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "SQSReceiveDeleteMessage",
6       "Effect": "Allow",
7       "Action": [
8         "sqs:ReceiveMessage",
9         "sqs:DeleteMessage"
10      ],
11       "Resource": "arn:aws:sqs:us-east-1:410439414220:myqueue"
12     }
13   ]
14 }
```

Review and Create Policy SQSReceiveDeleteMessagePolicy

Create policy

1 2 3

Review policy

Name*

Use alphanumeric and "+=, @, _" characters. Maximum 128 characters.

Description

Maximum 1000 characters. Use alphanumeric and "+=, @, _" characters.

Summary

Filter

Service	Access level	Resource	Request condition
Allow (1 of 315 services) Show remaining 314			
SQS	Limited: Read, Write	QueueName string like myqueue	None

Tags

Key	Value
No tags associated with the resource.	

* Required

Cancel Previous **Create policy**

View the created Policies on the IAM Dashboard.

Identity and Access Management (IAM)

Unable to load search

Dashboard

Access management

- User groups
- Users
- Roles
- Policies**
- Identity providers
- Account settings

Access reports

The policy **SQSReceiveDeleteMessagePolicy** has been created.

IAM > Policies

Policies (924) Info

A policy is an object in AWS that defines permissions.

Filter policies by property or policy name and press enter

Policy name	Type	Used as	Description
<input type="radio"/> class_policy_active	Customer managed	Permissions policy (2)	
<input type="radio"/> SQSReceiveDeleteMessagePolicy	Customer managed	None	
<input type="radio"/> SQSSendMessagePolicy	Customer managed	None	

Creating Roles

On the IAM dashboard, navigate to Roles and **Create role**

Identity and Access Management (IAM)

Introducing the new IAM roles experience

We've redesigned the IAM roles experience to make it easier to use. [Let us know what you think.](#)

IAM > Roles

Roles (39) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Search

Role name	Trusted entities	Last activity
arn:aws:iam::123456789012:role/ExampleRole	arn:aws:iam::123456789012:role/ExampleRole	

Create role

Select AWS service and EC2 use case

The screenshot shows the 'Create role' page in the AWS IAM console. The left sidebar indicates the current step is 'Step 1: Select trusted entity'. The main content area is titled 'Select trusted entity'. Under 'Trusted entity type', the 'AWS service' option is selected and highlighted with a red box. Below this, under 'Use case', the 'EC2' option is selected and highlighted with a red box. At the bottom right, the 'Next' button is highlighted with a red box.

Introducing the new IAM roles experience
We've redesigned the IAM roles experience to make it easier to use. [Let us know what you think](#)

IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity

Trusted entity type

- ☒ AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- ☐ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- ☐ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- ☐ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- ☐ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Common use cases

- ☒ EC2
Allows EC2 instances to call AWS services on your behalf.
- ☐ Lambda
Allows Lambda functions to call AWS services on your behalf.

Use cases for other AWS services:

Choose a service to view use case

Cancel Next

Add the **SQSSendMessagePolicy** to the role

The screenshot shows the 'Add permissions' page in the AWS IAM console. The left sidebar indicates the current step is 'Step 2: Add permissions'. The main content area is titled 'Add permissions'. Under 'Permissions policies (Selected 1/732)', the 'SQSSendMessagePolicy' is selected and highlighted with a red box.

IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Add permissions

Permissions policies (Selected 1/732)
Choose one or more policies to attach to your new role.

Filter policies by property or policy name and press enter

	Policy name	Type	Description
<input type="checkbox"/>	elastic_policy_active	Custom...	
<input type="checkbox"/>	SQSReceiveDeleteMessagePolicy	Custom...	
<input checked="" type="checkbox"/>	SQSSendMessagePolicy	Custom...	

add Role name as **SQSSendMessageRole**.

The screenshot shows the 'Name, review, and create' page in the AWS IAM console. The left sidebar indicates the current step is 'Step 3: Name, review, and create'. The main content area is titled 'Name, review, and create'. Under 'Role details', the 'Role name' field is filled with 'SQSSendMessageRole' and highlighted with a red box.

IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Name, review, and create

Role details

Role name
Name must be unique in this account. Use alphanumeric characters and hyphens.

SQSSendMessageRole

Description
Add a short explanation for this policy.

Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and "+", "@", "_" characters.

Step 1: Select trusted entities

Edit

1 - 0
2 - "Version": "2012-10-17",

Review the config and Create role

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
SQSSendMessagePolicy	Customer managed	Permissions policy

Tags

Add tags (Optional)
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

[Add tag](#)
You can add up to 50 more tags.

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

Similarly, create another role named **SQSReceiveDeleteMessageRole** and attach the SQSReceiveDeleteMessagePolicy.

IAM > Roles > Create role

Step 1: Select trusted entity

Step 2: Add permissions

Step 3: Name, review, and create

Add permissions

Permissions policies (Selected 1/732)
Choose one or more policies to attach to your new role.

Enter policies by property or policy name and press enter

5 matches

Clear filters

Policy name	Type	Description
<input checked="" type="checkbox"/> SQSReceiveDeleteMessagePolicy	Custom...	

IAM > Roles > Create role

Step 1: Select trusted entity

Step 2: Add permissions

Step 3: Name, review, and create

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.

SQSReceiveDeleteMessageRole

Description
Add a short explanation for this policy.

Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and "*/_@." characters.

View the roles created on the IAM Dashboard

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users**
- Roles**
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analysers
- Settings

Introducing the new IAM roles experience
We've redesigned the IAM roles experience to make it easier to use. [Let us know what you think.](#)

Role SQSReceiveDeleteMessageRole created [View role](#)

IAM > Roles

Roles (41) info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

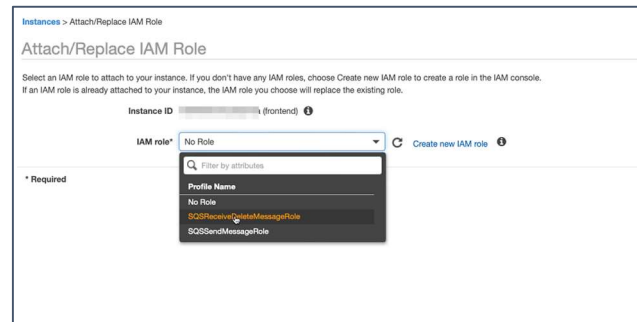
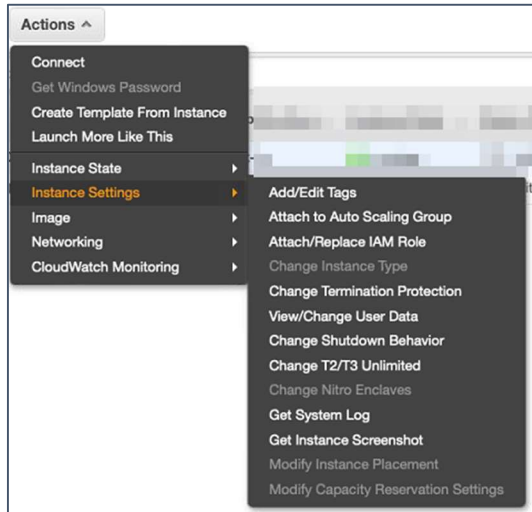
2 matches

Role name	Trusted entities	Last activity
<input type="checkbox"/> SQSReceiveDeleteMessageRole	AWS Service: ec2	-
<input type="checkbox"/> SQSSendMessageRole	AWS Service: ec2	-

Attach the roles to Frontend and Backend EC2 instance.

Navigate to EC2 dashboard and select an instance and click on Actions → Instance Settings → Attach/Replace IAM Role.

On Frontend select the “SQSSendMessageRole” and on Backend “SQSReceiveDeleteMessageRole”



Attach the respective roles and save.

