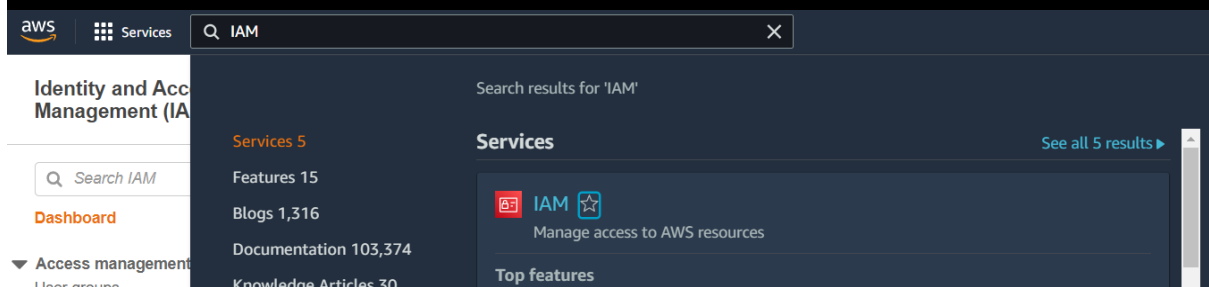


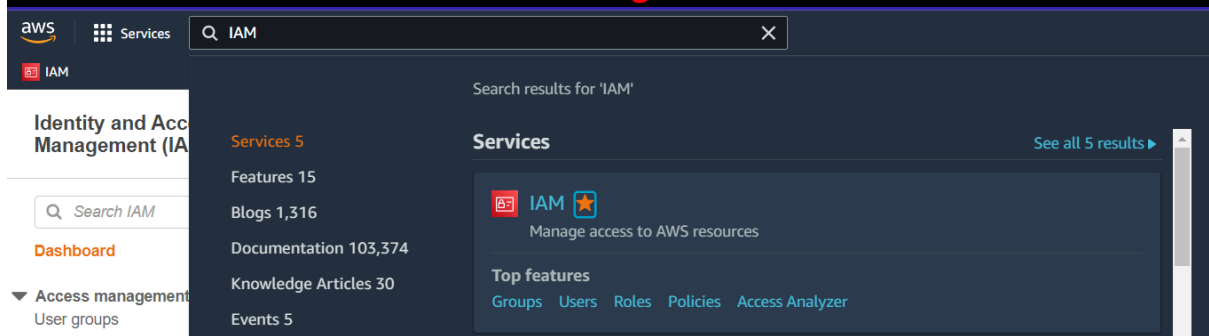
# IAM (Identity Access Management)

## Add to TAG

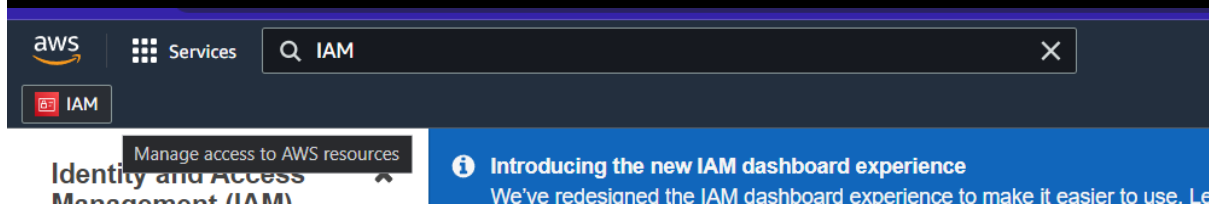
## Search IAM



## Click to start to tag Favourite list

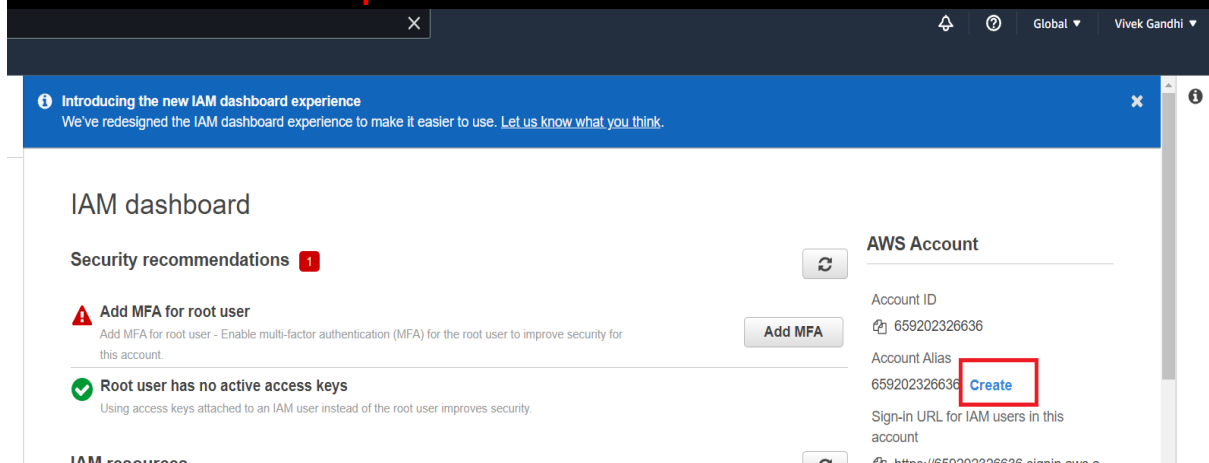


## TAG IAM



## Modified link

## Open IAM services and Alias create



# IAM (Identity Access Management)

## Insert alias name

Create alias for AWS account 659202326636

Preferred alias

Must be not more than 63 characters. Valid characters are a-z, 0-9, and - (hyphen).

Cancel Save changes

## Change Alias successfully

✓ Alias vivekgandhi created for this account

### IAM dashboard

Security recommendations 1

- ⚠ Add MFA for root user  
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.
- ✓ Root user has no active access keys  
Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

User groups Users Roles Policies Identity providers

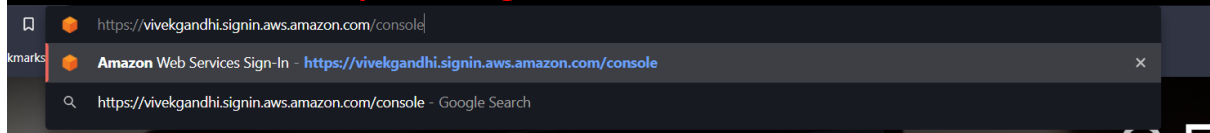
#### AWS Account

Account ID  
659202326636

Account Alias  
vivekgandhi [Edit](#) [Delete](#)

Sign-in URL for IAM users in this account  
<https://vivekgandhi.signin.aws.amazon.com/console>

## Open change alias link how to work



## Automatic add id to replace Alias name to open user account



### Sign in as IAM user

Account ID (12 digits) or account alias

vivekgandhi

IAM user name

|

Password

☐ Remember this account

Sign in

[Sign in using root user email](#)

[Forgot password?](#)

**Expanded Databases Free Tier**

Start today for free including DocumentDB, additional RDS instances, and more!

[LEARN MORE](#)

# IAM (Identity Access Management)

## Configuration MFA (Multi Factor Authentication)

### Click to Add MFA

IAM dashboard

Security recommendations **1**

**Add MFA for root user**  
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

**Root user has no active access keys**  
Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

User groups	Users	Roles	Policies	Identity providers
0	0	2	0	0

**AWS Account**

Account ID  
659202326636

Account Alias  
vivekgandhi [Edit](#) | [Delete](#)

Sign-in URL for IAM users in this account  
<https://vivekgandhi.signin.aws.amazon.com/console>

**Quick Links**

[My security credentials](#)  
Manage your access keys, multi-factor authentication (MFA), and other

### Click to Activate MFA

Identity and Access Management (IAM)

**Your Security Credentials**

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the [IAM Console](#).

To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

**Multi-factor authentication (MFA)**

Use MFA to increase the security of your AWS environments. Signing in to MFA-protected accounts requires a user name, password, and an authentication code from an MFA device.

**Activate MFA**

**Access keys (access key ID and secret access key)**

**CloudFront key pairs**

### Manage MFA Device

**Manage MFA device**

Choose the type of MFA device to assign:

☒ **Virtual MFA device**  
Authenticator app installed on your mobile device or computer

☐ **Security key**  
Authenticate by touching a hardware security key, such as Yubikey, Feitian, etc.

☐ **Other hardware MFA device**  
Gemalto token

For more information about supported MFA devices, see [AWS Multi-Factor Authentication](#)


[Cancel](#) [Continue](#)

## IAM (Identity Access Management)

**Open QR Scan option to scan and generated MFA code 2 times**

Set up virtual MFA device

2. Use your virtual MFA app and your device's camera to scan the QR code



Alternatively, you can type the secret key. [Show secret key](#)

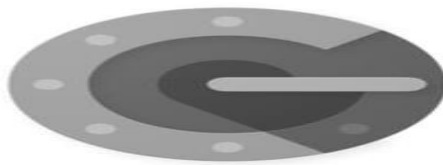
3. Type two consecutive MFA codes below

MFA code 1

MFA code 2

Cancel Previous [Assign MFA](#)

**Install in mobile Google Authenticator application**



## Stronger security with Google Authenticator

Get verification codes for all your accounts using 2-Step Verification

**Click to scan a QR code**



## Setup your first account

Use the QR code or setup key in your 2FA settings (by Google or third-party service). If you're having trouble, go to [g.co/2sv](https://g.co/2sv)



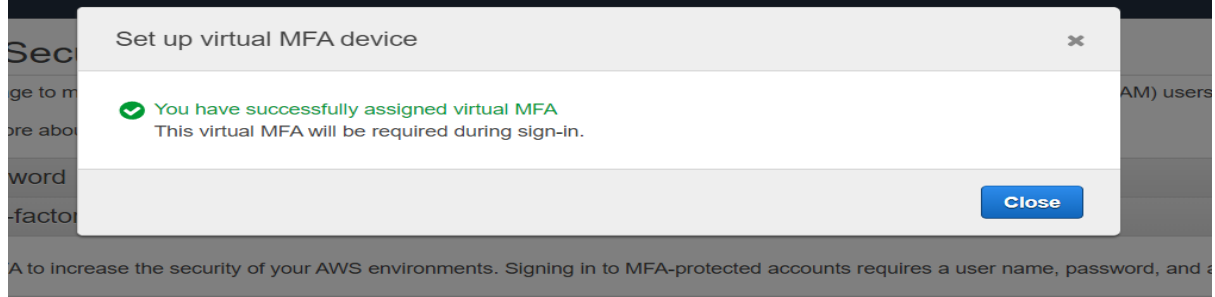
Scan a QR code



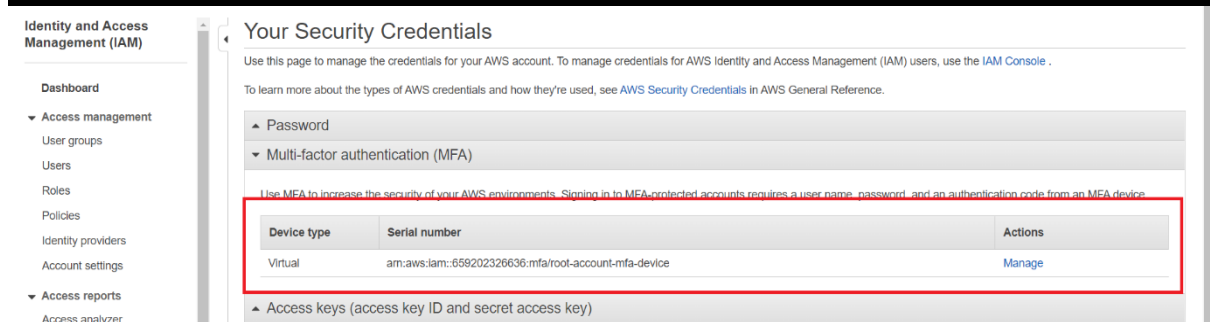
Enter a setup key

# IAM (Identity Access Management)

## Successfully configure MFA



## Overview



## Check login



### Sign in

☒ **Root user**  
Account owner that performs tasks requiring unrestricted access. [Learn more](#)

☐ **IAM user**  
User within an account that performs daily tasks. [Learn more](#)

Root user email address  
gandhivivek2+aws@gmail.com

[Next](#)

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

☐ New to AWS?

[Create a new AWS account](#)

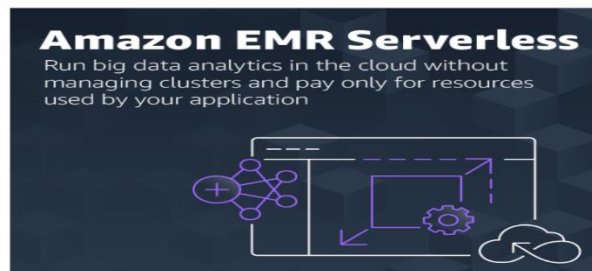


### Security check

Type the characters seen in the image below

3W C 8WC  
FM OMC

[Submit](#)



# IAM (Identity Access Management)



## Root user sign in

Email: gandhivivek2+aws@gmail.com

Password [Forgot password?](#)

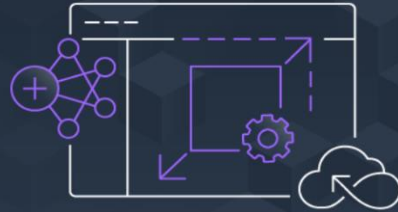
**Sign in**

[Sign in to a different account](#)

[Create a new AWS account](#)

## Amazon EMR Serverless

Run big data analytics in the cloud without managing clusters and pay only for resources used by your application



**MFA option is available to check mobile app auto generate code to insert**



## Multi-factor authentication

Your account is secured using multi-factor authentication (MFA). To finish signing in, turn on or view your MFA device and type the authentication code below.

Email address: gandhivivek2+aws@gmail.com

MFA code

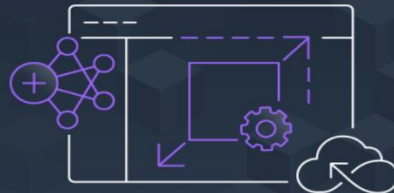
**Submit**

[Troubleshoot MFA](#)

[Cancel](#)

## Amazon EMR Serverless

Run big data analytics in the cloud without managing clusters and pay only for resources used by your application



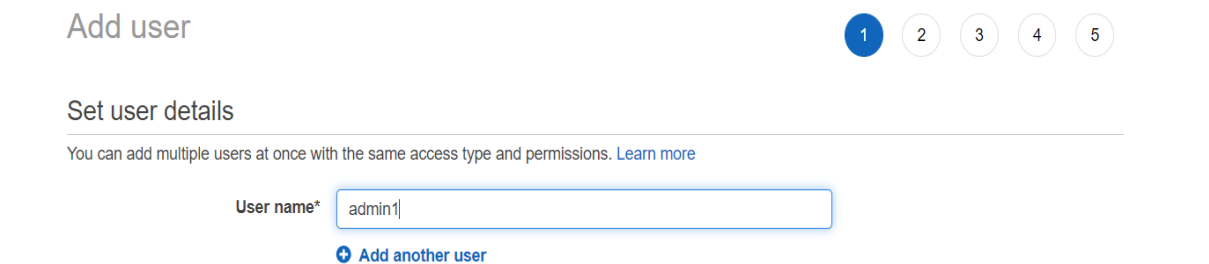
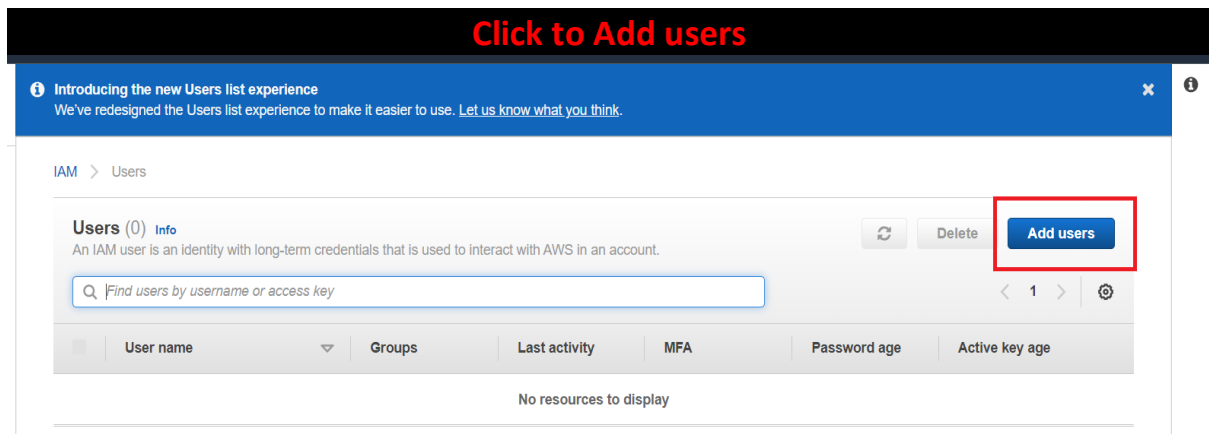
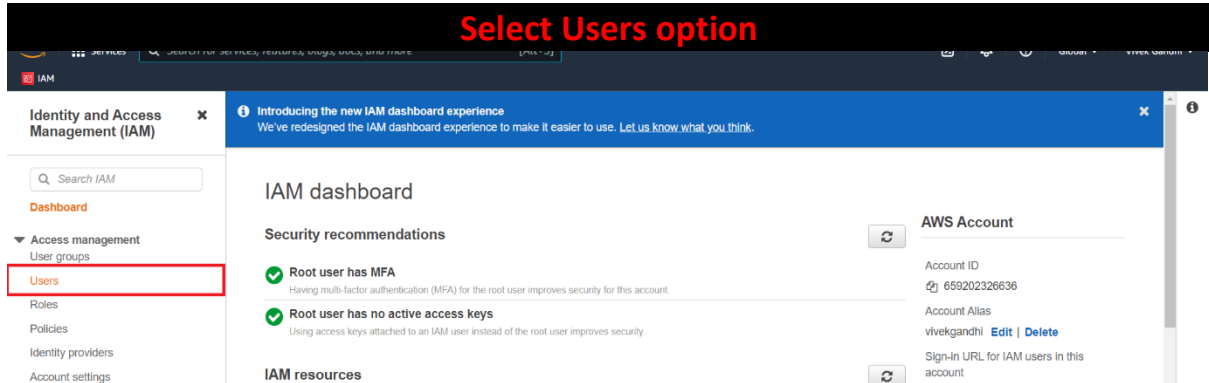
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

English

## Open main page

# IAM (Identity Access Management)

User Create to GUI Base with custom password and not create password next sign-in Users automatically



## 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.

# IAM (Identity Access Management)

## Create custom password

Console password\* ☐ Autogenerated password  
☒ Custom password

admin@123

☒ Show password

## Click to untick to not create a new password to user

Require password reset ☐ User must create a new password at next sign-in  
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

ui red

Cancel

Next: Permissions

## If you create group direct user to group

Add user

1


2


3


4

5

### Set permissions

 Add user to group

 Copy permissions from existing user

 Attach existing policies directly

#### Get started with groups

You haven't created any groups yet. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Get started by creating a group. [Learn more](#)

Create group

### Set permissions boundary

Set a permissions boundary to control the maximum permissions this user can have. This is an advanced feature used to delegate permission management to others. [Learn more](#)

- ☒ Create user without a permissions boundary  
☐ Use a permissions boundary to control the maximum user permissions

Cancel

Previous

Next: Tags

## Insert group name

Create group

Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. [Learn more](#)

Group name admin1

Create policy

Refresh

Filter policies

Search

Showing 754 results

	Policy name	Type	Used as	Description
<input checked="" type="checkbox"/>	AdministratorAccess	Job function	None	Provides full access to AWS services and resources.
<input type="checkbox"/>	AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permissions while explicitly allowing direct acc...




# IAM (Identity Access Management)


## Create group to user and assign policies


### 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

Q Search		Showing 1 result
Group	Attached policies	
<input checked="" type="checkbox"/> admin1	AdministratorAccess	

#### Set permissions boundary

Set a permissions boundary to control the maximum permissions this user can have. This is an advanced feature used to delegate permission management to others. [Learn more](#)

Cancel

Previous

Next: Tags


## Create 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
Managment	devops	

## Review

### Review

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

#### User details

User name	admin1
AWS access type	AWS Management Console access - with a password
Console password type	Custom
Require password reset	No
Permissions boundary	Permissions boundary is not set

#### Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	admin1

#### Tags

The new user will receive the following tag

Key	Value
Managment	devops

# IAM (Identity Access Management)

## Add user successfully

### 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://vivekgandhi.signin.aws.amazon.com/console>

Download .csv

User	Email login instructions
<div>admin1</div>	<div>Send email</div>

Created user admin1

Added user admin1 to group admin1

Created login profile for user admin1

## Download .csv file

Download .csv

User	Email login instructions
<div>admin1</div>	<div>Send email</div>

## Download .csv file

Feedback Looking for language selection? Find it in the new [Unified Settings](#)



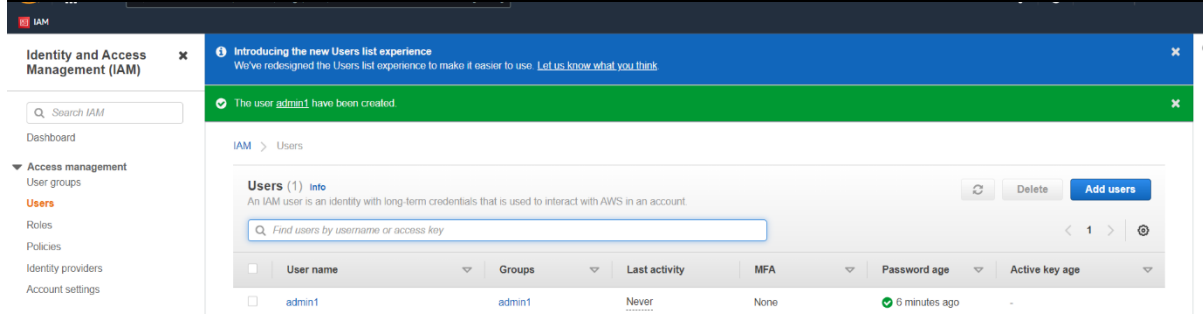
new\_user\_credenti....csv

## Download file details

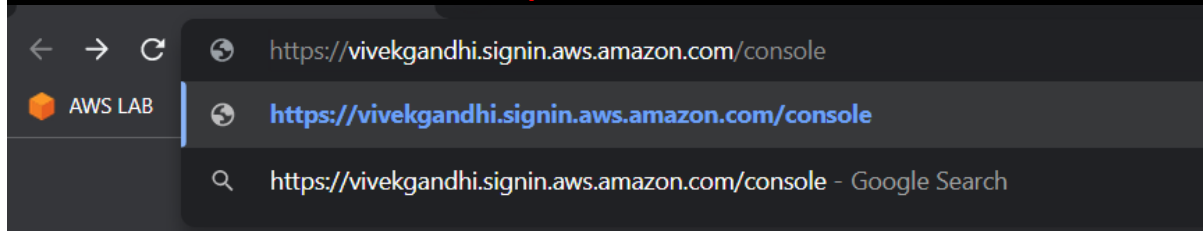
	A	B	C	D	E	F	G	H	I	J
1	User name	Password	Access key ID	Secret access key	Console login link					
2	admin1				<a href="https://vivekgandhi.signin.aws.amazon.com/console">https://vivekgandhi.signin.aws.amazon.com/console</a>					
3										
4										

# IAM (Identity Access Management)

All configuration done



Open this link



Open user account



Sign in as IAM user

Account ID (12 digits) or account alias

vivekgandhi

IAM user name

admin1

Password

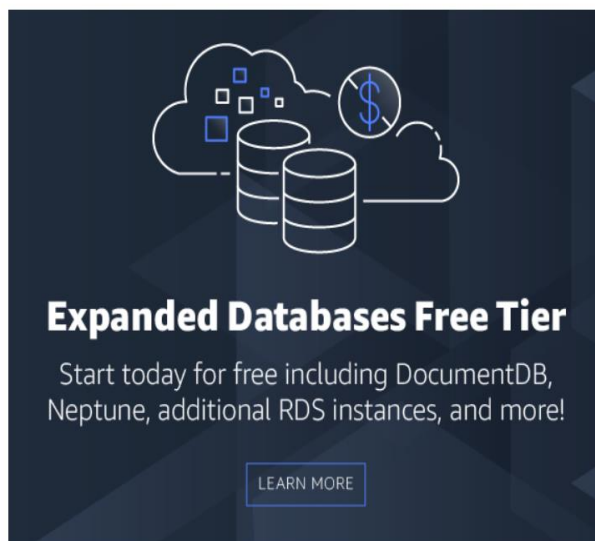
\*\*\*\*\*

☐ Remember this account

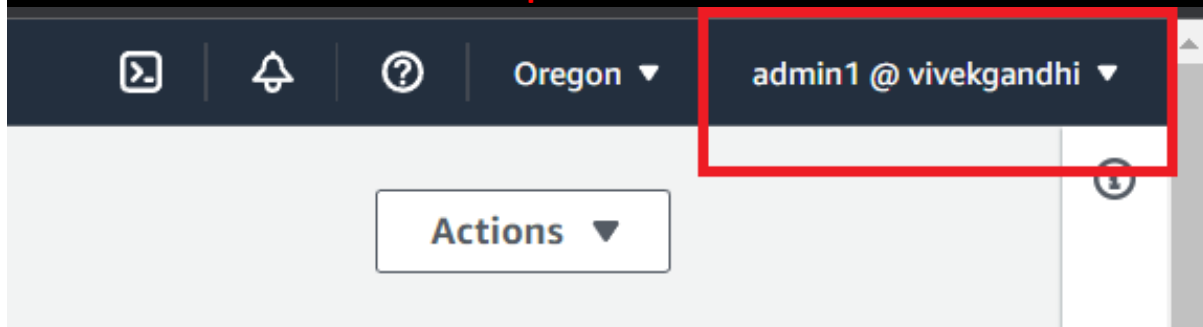
Sign in

[Sign in using root user email](#)

[Forgot password?](#)



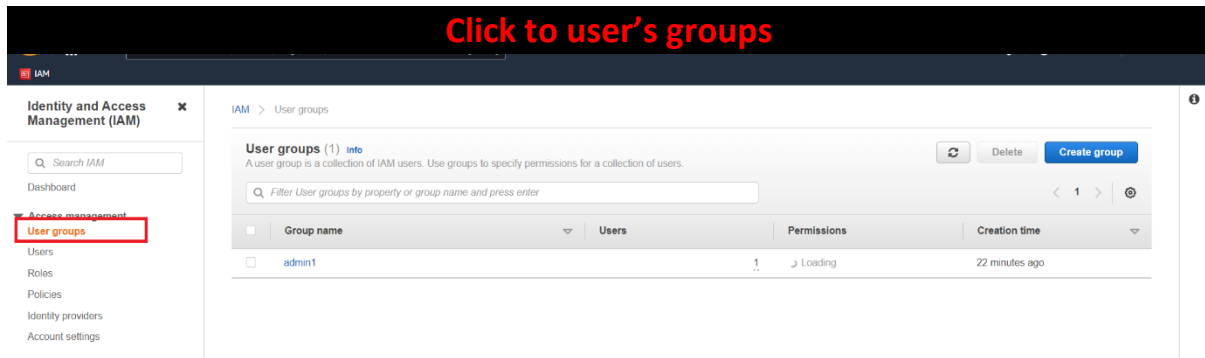
Open account



# IAM (Identity Access Management)

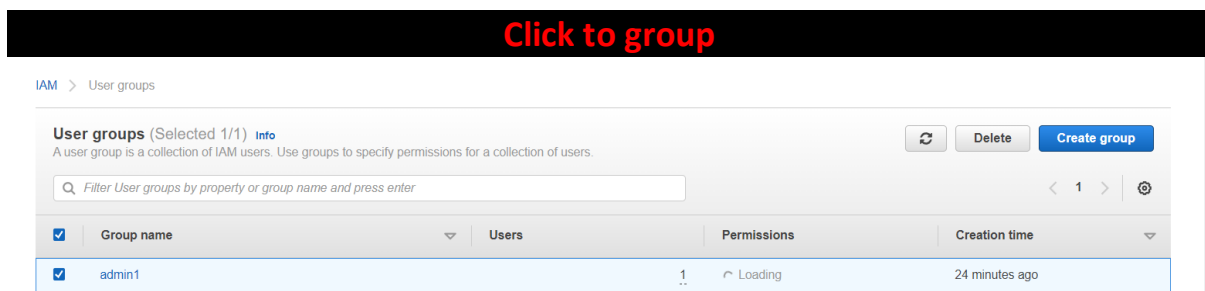
## Edit group name

### Click to user's groups



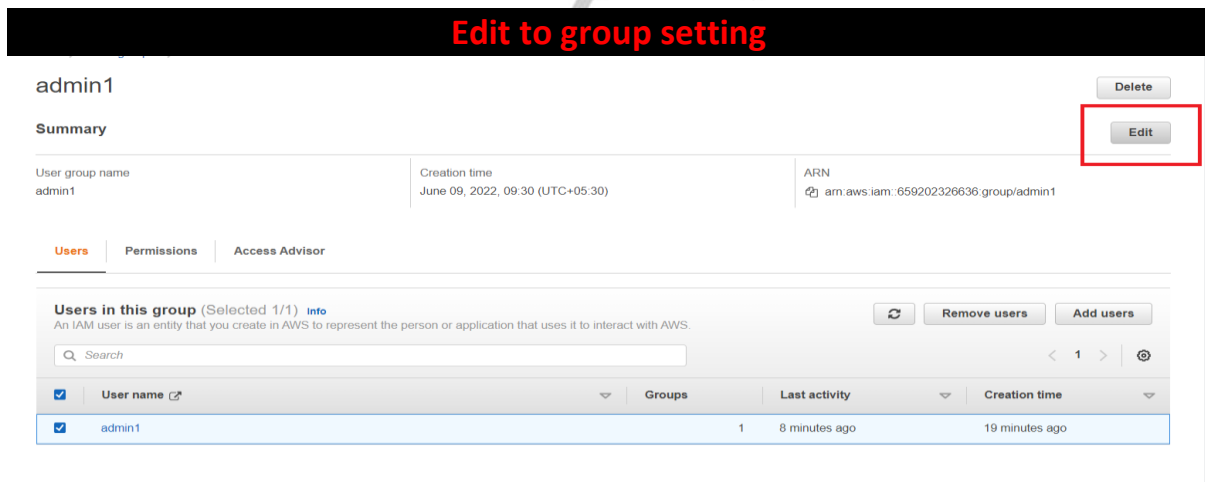
The screenshot shows the AWS IAM console interface. On the left, the 'User groups' link under the 'Access management' section is highlighted with a red box. The main content area shows the 'User groups' page with a table listing existing groups. The 'admin1' group is visible in the table.

### Click to group



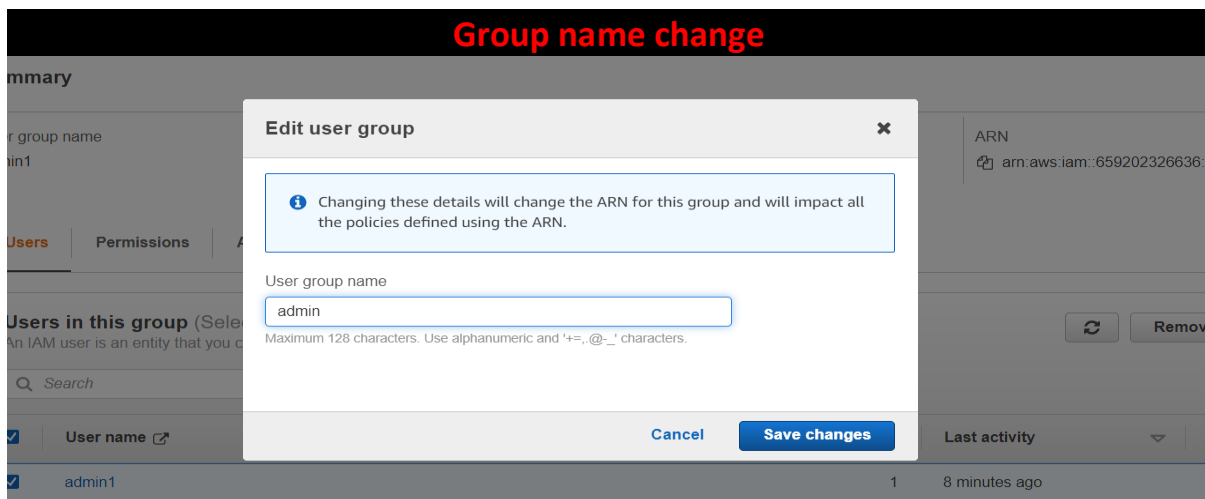
The screenshot shows the 'User groups' page with the 'admin1' group selected. The row for 'admin1' is highlighted in blue. The 'Edit' button in the top right corner is highlighted with a red box.

### Edit to group setting



The screenshot shows the 'admin1' group settings page. The 'Edit' button in the top right corner is highlighted with a red box. The page displays summary information for the group, including its creation time and ARN.

### Group name change



The screenshot shows the 'admin1' group settings page with the 'Edit user group' modal open. The modal displays a warning message: 'Changing these details will change the ARN for this group and will impact all the policies defined using the ARN.' Below the warning, the 'User group name' field is visible with the text 'admin' entered. The 'Save changes' button is highlighted in blue.

# IAM (Identity Access Management)

Edit successfully

## User groups (1) [Info](#)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.



Delete

Create group

Q Filter User groups by property or group name and press enter

< 1 > ⚙

<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	admin	⌂ Loading	⌂ Loading	32 minutes ago

Also, automatic update user

## Users (1) [Info](#)

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



Delete

Add users

Q Find users by username or access key

< 1 > ⚙

<input type="checkbox"/>	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	admin1	admin	✓ 16 minutes ago	None	✓ 27 minutes ago	-



# IAM (Identity Access Management)

## User Create to GUI Base with Auto password and next sign-in Users Manually

### Add to users

IAM > Users

**Users (2)** [info](#)

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

[Refresh](#) [Delete](#) [Add users](#)

<input type="checkbox"/>	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	admin1	admin	1 hour ago	None	1 hour ago	-
<input type="checkbox"/>	admin2	admin	8 minutes ago	None	11 minutes ago	1 hour ago

### 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 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.

Console password\*

☒ Autogenerated password  
☐ Custom password

Require password reset ☒ User must create a new password at next sign-in  
Users automatically get the `IAMUserChangePassword` policy to allow them to change their own password.


\* Required


[Cancel](#)


[Next: Permissions](#)

### Not create group

#### 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](#)

Showing 1 result

Group	Attached policies
<input type="checkbox"/> admin	AdministratorAccess

#### Set permissions boundary

# IAM (Identity Access Management)

## Add tags

### 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
production	auto password	✕
Add new key		

You can add 49 more tags.

## Review

### Review

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

#### User details

User name	Production
AWS access type	AWS Management Console access - with a password
Console password type	Autogenerated
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

#### Permissions summary

The user shown above will be added to the following groups.

Type	Name
Managed policy	<a href="#">IAMUserChangePassword</a>

#### Tags

The new user will receive the following tag

Key	Value
production	auto password

[Cancel](#)

[Previous](#)

[Create user](#)

## DOWNLOAD FILE

### ✓ 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://vivekgandhi.signin.aws.amazon.com/console>

[Download .csv](#)

User	Password	Email login instructions
▶ ✓ Production	***** Show	<a href="#">Send email</a>

## Excel file open to get automatic password check

A	B	C	D	E	F	G	H	I
User name	Password	Access key	Secret acc	Console login link				
Production	oS6TQ!&nrZnD _			<a href="https://vivekgandhi.signin.aws.amazon.com/console">https://vivekgandhi.signin.aws.amazon.com/console</a>				

# IAM (Identity Access Management)

## Create user successfully

**Users (3)** [Info](#)

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

< 1 >

<input type="checkbox"/>	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	admin1	admin	✓ 1 hour ago	None	✓ 1 hour ago	-
<input type="checkbox"/>	admin2	admin	✓ 18 minutes ago	None	✓ 21 minutes ago	✓ 1 hour ago
<input type="checkbox"/>	Production	None	Never	None	✓ Now	-

## Open in portal

### Sign in as IAM user

Account ID (12 digits) or account alias

vivekgandhi

IAM user name

production

Password

.....

☐ Remember this account

Sign in

[Sign in using root user email](#)

[Forgot password?](#)

## Introducing new AWS Amplify Studio

Build scalable, full-stack web and mobile apps in hours with new visual interface

GET STARTED



## Change password

AWS account 659202326636

IAM user name Production

Old password

New password

Retype new password

Confirm password change

[Sign in using root user email](#)

## Open account

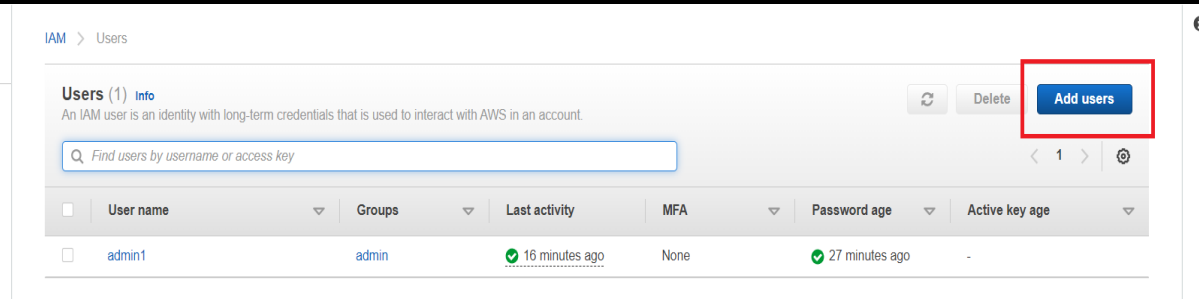
Oregon ▼ Production @ vivekgandhi ▼



# IAM (Identity Access Management)

## User Create to CLI Base

### Click Add users



IAM > Users

**Users (1)** 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

	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	admin1	admin	✓ 16 minutes ago	None	✓ 27 minutes ago	-

### Add user configure

#### Add user



#### Set user details

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

User name\* admin2

[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.

### Add group in user

#### 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](#)

Showing 1 result

Group	Attached policies
<input checked="" type="checkbox"/> admin	AdministratorAccess

#### Set permissions boundary

# IAM (Identity Access Management)

## Add tags

### 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
Managment	Manuall password	✕
Add new key		

You can add 49 more tags.

## Review

### Review

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

#### User details

User name	admin2
AWS access type	Programmatic access - with an access key
Permissions boundary	Permissions boundary is not set

#### Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	<a href="#">admin</a>

#### Tags

The new user will receive the following tag

Key	Value
Managment	Manuall password

## Download .csv file if I forget download file than

### ✓ 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://vivekgandhi.signin.aws.amazon.com/console>

Download .csv

	User	Access key ID	Secret access key
▶ ✓	admin2	AKIAZS64FIBWLYLVPCRD 	***** <a href="#">Show</a>

# IAM (Identity Access Management)

## Create user but still not download .csv file than click user

IAM > Users

**Users (2)** [Info](#)  
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

<input type="checkbox"/>	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	admin1	admin	32 minutes ago	None	42 minutes ago	-
<input type="checkbox"/>	admin2	admin	Never	None	None	4 minutes ago

## Click to security credentials

Users > admin2

**Summary** [Delete user](#) [?](#)

**User ARN** arn:aws:iam::659202326636:user/admin2 [🔗](#)  
**Path** /  
**Creation time** 2022-06-09 10:15 UTC+0530

[Permissions](#) [Groups \(1\)](#) [Tags \(1\)](#) **[Security credentials](#)** [Access Advisor](#)

**Sign-in credentials**

**Summary** • User does not have console management access

**Console password** Disabled | [Manage](#)  
**Assigned MFA device** Not assigned | [Manage](#)  
**Signing certificates** None [🔗](#)

## Create access key

**Access keys**

Use access keys to make programmatic calls to AWS from the AWS CLI, Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time.

For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation.  
If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make the old key inactive. [Learn more](#)

[Create access key](#)

Access key ID	Created	Last used	Status
AKIAZS64FIBWLYLVPCRD	2022-06-09 10:15 UTC+0530	N/A	Active   <a href="#">Make inactive</a> <a href="#">✕</a>

SSH keys for AWS CodeCommit

## Create access key popup and download .csv file

**Create access key** [✕](#)

**Warning**  
Never post your secret access key on public platforms, such as GitHub. This can compromise your account security.

**Success**  
This is the **only** time that the secret access keys can be viewed or downloaded. You cannot recover them later. However, you can create new access keys at any time.

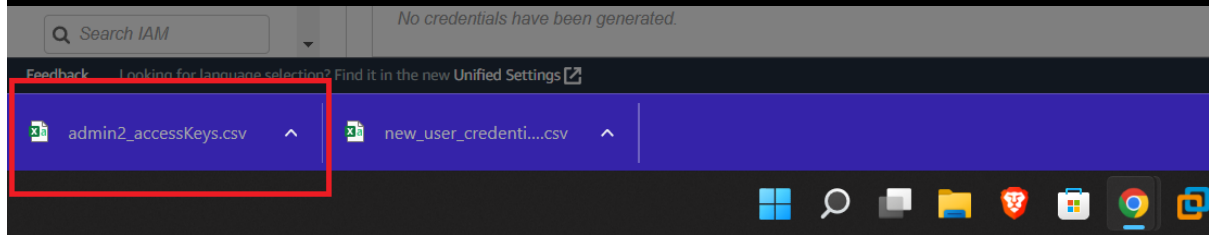
[Download .csv file](#)

Access key ID	Secret access key
AKIAZS64FIBWNOZSUKRS	***** <a href="#">Show</a>

[Close](#)

# IAM (Identity Access Management)

## Download file



```
C:\windows\system32>aws --version
aws-cli/2.7.7 Python/3.9.11 Windows/10 exe/AMD64 prompt/off

C:\windows\system32>.
```

## Excel file check

1	Access key ID	Secret access key		
2	AKIAZS64FIBWNOZSUKRS	TgcZRvg4REDVFu2xy7BQU1cp3GoiMUTgjlveZJef		
3				

## Access to CLI

```
C:\windows\system32>aws configure
AWS Access Key ID [None]: AKIAZS64FIBWNOZSUKRS
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-1
Default output format [None]:
```

## Get command to user

```
C:\windows\system32>aws iam get-user
{
  "User": {
    "Path": "/",
    "UserName": "admin2",
    "UserId": "AIDAZS64FIBWGBDCJIL7Z",
    "Arn": "arn:aws:iam::659202326636:user/admin2",
    "CreateDate": "2022-06-09T04:45:28+00:00",
    "Tags": [
      {
        "Key": "Managment",
        "Value": "Manuall password"
      }
    ]
  }
}
```

# IAM (Identity Access Management)

## User add in CLI

### Open CMD in window

aws iam create-user --user-name cli1

```
C:\windows\system32>aws iam create-user --user-name cli1
{
  "User": {
    "Path": "/",
    "UserName": "cli1",
    "UserId": "AIDAZS64FIBWFROKE5FUI",
    "Arn": "arn:aws:iam::659202326636:user/cli1",
    "CreateDate": "2022-06-09T08:11:56+00:00"
  }
}
```

### Check AWS account creates or not

**Users (4)** 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

<input type="checkbox"/>	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	admin1	admin	3 hours ago	None	4 hours ago	-
<input type="checkbox"/>	admin2	admin	2 hours ago	None	2 hours ago	3 hours ago
<input type="checkbox"/>	cli1	None	Never	None	None	-
<input type="checkbox"/>	Production	None	2 hours ago	None	2 hours ago	-

## Create group

aws iam create-group --group-name Developers

```
C:\windows\system32>aws iam create-group --group-name Developers
{
  "Group": {
    "Path": "/",
    "GroupName": "Developers",
    "GroupId": "AGPAZS64FIBWP5NZ4TBZ6",
    "Arn": "arn:aws:iam::659202326636:group/Developers",
    "CreateDate": "2022-06-09T08:20:16+00:00"
  }
}
```

### Check AWS account creates or not

**User groups (2)** Info  
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Filter User groups by property or group name and press enter

<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	admin	2	Defined	4 hours ago
<input type="checkbox"/>	Developers	0	Not defined	2 minutes ago

# IAM (Identity Access Management)

## User add to group

aws iam add-user-to-group --user-name cli1 --group-name developers

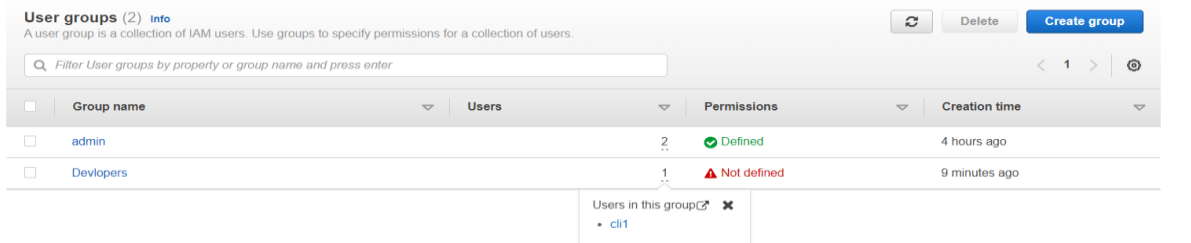
```
C:\windows\system32>aws iam add-user-to-group --user-name cli1 --group-name developers
C:\windows\system32>
```

## Check to command line

aws iam get-group --group-name Developers

```
C:\windows\system32>aws iam get-group --group-name Developers
{
  "Users": [
    {
      "Path": "/",
      "UserName": "cli1",
      "UserId": "AIDAZS64FIBWFROKE5FUI",
      "Arn": "arn:aws:iam::659202326636:user/cli1",
      "CreateDate": "2022-06-09T08:11:56+00:00"
    }
  ],
  "Group": {
    "Path": "/",
    "GroupName": "Developers",
    "GroupId": "AGPAZS64FIBWP5NZ4TBZ6",
    "Arn": "arn:aws:iam::659202326636:group/Developers",
    "CreateDate": "2022-06-09T08:20:16+00:00"
  }
}
```

## Check AWS account



Group name	Users	Permissions	Creation time
admin	2	Defined	4 hours ago
Developers	1	Not defined	9 minutes ago

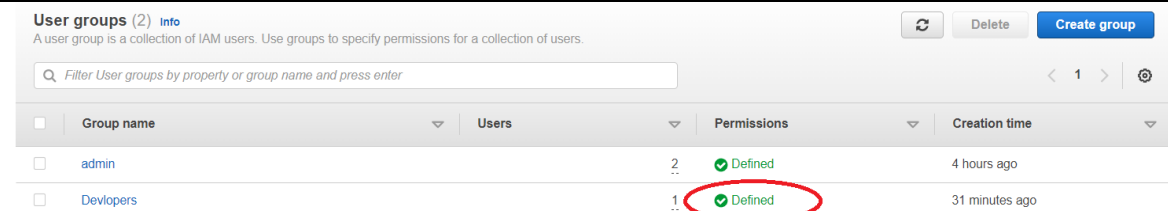
Users in this group  
• cli1

## Policy applies to group

aws iam attach-group-policy --policy-arn arn:aws:iam::aws:policy/ReadOnlyAccess --group-name Developers

```
C:\windows\system32>aws iam attach-group-policy --policy-arn arn:aws:iam::aws:policy/ReadOnlyAccess --group-name Developers
C:\windows\system32>
```

## Policy applies successfully check to GUI AWS



Group name	Users	Permissions	Creation time
admin	2	Defined	4 hours ago
Developers	1	Defined	31 minutes ago

# IAM (Identity Access Management)

## CHECK which permission apply in group

### Permissions policies (1) [Info](#)

You can attach up to 10 managed policies.

[Simulate](#)[Remove](#)[Add permissions](#) ▼[<](#) 1 [>](#)

<input type="checkbox"/>	Policy name ↗	Type	Description
<input type="checkbox"/>	ReadOnlyAccess	AWS managed	Provides read-only access to AWS services and resources.

## Assign Access key and secret key

```
C:\windows\system32>aws iam create-access-key --user-name cli1
{
  "AccessKey": {
    "UserName": "cli1",
    "AccessKeyId": "AKIAZS64FIBWIGK2WPAT",
    "Status": "Active",
    "SecretAccessKey": "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",
    "CreateDate": "2022-06-09T09:22:36+00:00"
  }
}
```

AKIAZS64FIBWIGK2WPAT

WwrbP3qS8zN0vXhojeFIJKng2MqeE/lKvDoiKDUu

## Check AWS GUI

If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make the old key inactive. [Learn more](#)

[Create access key](#)

Access key ID	Created	Last used	Status
AKIAZS64FIBWIGK2WPAT	2022-06-09 14:52 UTC+0530	N/A	Active   <a href="#">Make inactive</a>

SSH keys for AWS CodeCommit

Use SSH public keys to authenticate access to AWS CodeCommit repositories. [Learn more](#)

## Try to access in cli

An error occurred (LimitExceeded) when calling the CreateAccessKey operation: Cannot exceed quota for AccessKeysPerUser

```
C:\windows\system32>aws configure
AWS Access Key ID [*****UKRS]: AKIAZS64FIBWIGK2WPAT
AWS Secret Access Key [*****ZJeF]: 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
Default region name [us-east-1]:
Default output format [None]:
```

# IAM (Identity Access Management)

## Check all users list

```
C:\windows\system32>aws iam list-users
{
  "Users": [
    {
      "Path": "/",
      "UserName": "admin1",
      "UserId": "AIDAZS64FIBWF6MPIO3QD",
      "Arn": "arn:aws:iam::659202326636:user/admin1",
      "CreateDate": "2022-06-09T04:06:39+00:00",
      "PasswordLastUsed": "2022-06-09T04:17:29+00:00"
    },
    {
      "Path": "/",
      "UserName": "admin2",
      "UserId": "AIDAZS64FIBWGBDCJIL7Z",
      "Arn": "arn:aws:iam::659202326636:user/admin2",
      "CreateDate": "2022-06-09T04:45:28+00:00"
    },
    {
      "Path": "/",
      "UserName": "cli1",
      "UserId": "AIDAZS64FIBWFROKESFUI",
      "Arn": "arn:aws:iam::659202326636:user/cli1",
      "CreateDate": "2022-06-09T08:11:56+00:00",
      "PasswordLastUsed": "2022-06-09T09:07:40+00:00"
    },
    {
      "Path": "/",
      "UserName": "Production",
      "UserId": "AIDAZS64FIBWDSLIZGUEK",
      "Arn": "arn:aws:iam::659202326636:user/Production",
      "CreateDate": "2022-06-09T06:00:53+00:00",
      "PasswordLastUsed": "2022-06-09T06:06:42+00:00"
    }
  ]
}
```

## Check all group list

```
C:\windows\system32>aws iam list-groups
{
  "Groups": [
    {
      "Path": "/",
      "GroupName": "admin",
      "GroupId": "AGPAZS64FIBWNZT4HCJ4L",
      "Arn": "arn:aws:iam::659202326636:group/admin",
      "CreateDate": "2022-06-09T04:00:32+00:00"
    },
    {
      "Path": "/",
      "GroupName": "Developers",
      "GroupId": "AGPAZS64FIBWP5NZ4TBZ6",
      "Arn": "arn:aws:iam::659202326636:group/Developers",
      "CreateDate": "2022-06-09T08:20:16+00:00"
    }
  ]
}
```



# IAM (Identity Access Management)

## How to create group and assign user

### Open User group and click to create group

**User groups (2)** [Info](#)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

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

<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	admin	<a href="#">Loading</a>	<a href="#">Loading</a>	8 hours ago
<input type="checkbox"/>	Developers	<a href="#">Loading</a>	<a href="#">Loading</a>	4 hours ago

### Insert group name

[IAM](#) > [User groups](#) > [Create user group](#)

## Create user group

### Name the group

User group name

Enter a meaningful name to identify this group.

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

### Add user to the group

**Add users to the group - Optional (Selected 1/4)** [Info](#)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user can belong to up to 10 groups.

<input type="checkbox"/>	User name <a href="#">↗</a>	Groups	Last activity	Creation time
<input type="checkbox"/>	admin1	1	8 hours ago	8 hours ago
<input type="checkbox"/>	admin2	1	None	8 hours ago
<input type="checkbox"/>	cli1	1	3 hours ago	4 hours ago
<input checked="" type="checkbox"/>	Production	0	6 hours ago	6 hours ago

### If you create new customized policy than click create policy

**Attach permissions policies - Optional (754)** [Info](#)

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

[Refresh](#) [Create Policy \[↗\]\(#\)](#)

<input type="checkbox"/>	Policy name <a href="#">↗</a>	Type	Description
<input type="checkbox"/>	<a href="#">AWSDirectConnectReadOnlyAccess</a>	AWS managed	Provides read only access to AWS Direct Connect via the AWS Management Co...
<input type="checkbox"/>	<a href="#">AmazonGlacierReadOnlyAccess</a>	AWS managed	Provides read only access to Amazon Glacier via the AWS Management Console.

# IAM (Identity Access Management)

## 2 types create a custom policy

### 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

Expand all | Collapse all

Select a service

Service

Choose a service

Actions

Choose a service before defining actions

Resources

Choose actions before applying resources

Request conditions

Choose actions before specifying conditions

Add additional permissions

## 1. Create visual editor and expand service option

### 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

Expand all | Collapse all

EC2

Service

Select a service below

IAM

RDS IAM Authentication

Actions

Select actions

Resources

Choose actions before applying resources

Request conditions

Choose actions before specifying conditions

Add additional permissions

## Apply access level

EC2 (525 actions) 44 warnings

Service

EC2

Actions

Specify the actions allowed in EC2

Manual actions (add actions)

☐ All EC2 actions (ec2:\*)

Access level

☒ List (139 selected)

☒ Read (38 selected)

☐ Tagging

☒ Write (348 selected)

☐ Permissions management

Action warnings

\* ec2:CreateNetworkInsightsPath action requires 1 more action to provide full permissions

# IAM (Identity Access Management)

## Configure resources

▼ Resources ☒ Specific [close](#) ☐ All resources

<b>access-report</b> ?	Specify <b>access-report</b> resource ARN for the <b>GenerateOrganizationsAccessReport</b> action. <a href="#">Add ARN</a> to restrict access	<input type="checkbox"/> Any in this account
<b>group</b> ?	Specify <b>group</b> resource ARN for the <b>AddUserToGroup</b> and 14 more actions. <a href="#">Add ARN</a> to restrict access	<input type="checkbox"/> Any in this account
<b>instance-profile</b> ?	Specify <b>instance-profile</b> resource ARN for the <b>TagInstanceProfile</b> and 8 more actions. <a href="#">Add ARN</a> to restrict access	<input type="checkbox"/> Any in this account

## Add request conditions

▼ Request conditions ☐ **MFA required** [close](#)  
Requires console users and those with temporary credentials to authenticate with an MFA device for these actions. [Learn more](#)

☐ **Source IP**  
Allow access to the specified actions only when the request comes from the specified IP address range.

[Add condition](#)

## If add multiple condition can be apply to click add additional permission

[+ Add additional permissions](#)

[Cancel](#)

[Next: Tags](#)

## Review configuration

### 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](#)

[Expand all](#) | [Collapse all](#)

▶ IAM (All actions)	<a href="#">Clone</a> <a href="#">Remove</a>
▶ EC2 (All actions)	<a href="#">Clone</a> <a href="#">Remove</a>

[+ Add additional permissions](#)

## All modification than click next tags

[Cancel](#)

[Next: Tags](#)

© 2022 Amazon Internet Services Private Ltd. or its affiliates

# IAM (Identity Access Management)

If you add tag than click add tag

## 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

Add name policy and description and create policy

## Review policy

Name\* IAMEC2

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

Description IAM AND EC2 BOTH SERVICE INCLUDE IN THIS POLICY GROUP

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

## Summary

Filter			
Service	Access level	Resource	Request condition
Allow (2 of 327 services) Show remaining 325			
EC2	Full access	All resources	None
IAM	Full access	All resources	None

## Tags

Key	Value
-----	-------

No tags associated with the resource.

\* Required

Cancel

Previous

Create policy

Create successfully and apply to policy in this group

The policy IAMEC2 has been created.

IAM > Policies

**Policies** (1/952) 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
IAMEC2	Customer managed	None	IAM AND EC2 BOTH SEF

Create group and attach user to group successfully

Management user group created.

IAM > User groups

**User groups** (3) Info  
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Filter User groups by property or group name and press enter

Group name	Users	Permissions	Creation time
admin	^ Loading	^ Loading	9 hours ago
Developers	^ Loading	^ Loading	4 hours ago
Managment	1	Defined	4 minutes ago

Users in this group

- Production