

rajendra0968jangid

IAM & AWS CLI (Identity and Access Management)

SAA-C03

IAM

In AWS, IAM (Identity and Access Management) is the service used to securely manage access to AWS resources. Two core components of IAM are Users and Groups.



IAM User

- An IAM User is an entity that represents a single person or application that interacts with AWS services.

Feature	Description
Credentials	Can have username + password (for AWS Management Console access) and/or access keys (for API/CLI access).
Permissions	Permissions are assigned directly or via groups .
Use Case	Ideal for individual users such as admins, developers, or applications.
Limits	Default limit is 5,000 IAM users per AWS account.

IAM Group

- An IAM Group is a collection of IAM users. Groups allow you to manage permissions collectively rather than individually.

Feature	Description
No credentials	Groups don't have credentials themselves.
Permission control	Policies attached to the group apply to all users in that group.
Use Case	Useful for managing users with similar roles (e.g., Admins, Developers).
Nesting	Groups cannot contain other groups.

Best Practices

- Use groups to assign permissions wherever possible. Avoid root user for everyday tasks—create IAM users instead.
- Enable MFA (Multi-Factor Authentication) for additional security.
- Use least privilege principle—only give the access needed.
-

Example Scenario

- Let's say you have a team of developers.
- You create an IAM Group called Developers.
- Attach policies like AmazonEC2ReadOnlyAccess to the group.
- Create IAM Users like alice, bob, and charlie.

Add them to the Developers group.

- All three now inherit the same EC2 read-only permissions.

IAM Users & Groups Hands On

- Go to <https://aws.amazon.com/console/>
- Sign in your account

The screenshot shows the AWS IAM console home page. At the top, there is a navigation bar with the AWS logo, a search bar containing 'Search' with a keyboard shortcut '[Alt+S]', and various icons for notifications and account details. The region is set to 'Asia Pacific (Mumbai)' and the user is 'Twinkle%20Sharma'. Below the navigation bar, the page title is 'Console Home' with an 'Info' link. A large search bar labeled 'Search IAM' is centered above two main sections. The left section, titled 'Recently visited' with an 'Info' link, shows a single item: 'EC2'. The right section, titled 'Applications (0) Info' with a 'Create application' button, shows a message: 'No applications' and 'Get started by creating an application.' with a 'Create application' button. At the bottom, there are links for 'CloudShell', 'Feedback', and copyright information: '© 2025, Amazon Web Services, Inc. or its affiliates.', 'Privacy', 'Terms', and 'Cookie preferences'.

aws

Q IAM

Console

Services Features Resources New Documentation Knowledge articles Marketplace Blog posts Events Tutorials

Click here

IAM Manage access to AWS resources Top features Groups Users Roles Policies Access Analyzer

IAM Identity Center Manage workforce user access to multiple AWS accounts and cloud applications

Resource Access Manager Share AWS resources with other accounts or AWS Organizations

Were these results helpful? Yes No

Features Groups IAM feature

Show more

+ Add widgets

Create application

https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws

Search [Alt+S]

rajendra0968jangid

Identity and Access Management (IAM) Dashboard IAM Dashboard

Search IAM

Dashboard

▼ Access management

User groups

Users  Click on Users

Roles

Policies

Identity providers

Account settings

Root access management New

▼ Access reports

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. Add MFA

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

AWS Account

Account ID 235562991793

Account Alias Create

Sign-in URL for IAM users in this account https://235562991793.sigin.aws.amazon.com/console

IAM resources

Resources in this AWS Account

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

Quick Links

My security credentials

Manage your access keys, multi-factor

https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws Search [Alt+S] Global Twinkle%20Sharma

IAM > Users

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings
- Root access management New

Access reports

Users (0) Info

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

Search

User name	Path	Group	Last activity	MFA	Actions
No resources to display					

On clicking here you can see no region is selected At the time of user creation we don't need region selection

United States

- N. Virginia us-east-1
- Ohio us-east-2
- N. California us-west-1
- Oregon us-west-2

Asia Pacific

- Hyderabad ap-south-2
- India ap-south-1
- Osaka ap-northeast-3
- Tokyo ap-northeast-2
- Singapore ap-southeast-1
- Sydney ap-southeast-2
- Auckland ap-southeast-3

Canada

- Central ca-central-1

Manage Regions Manage Local Zones

aws Search [Alt+S] Global Twinkle%20Sharma

IAM > Users

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings
- Root access management New

Access reports

Users (0) Info

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

Search

User name	Path	Group:	Last activity	MFA	Actions
No resources to display					

Click on create user

Create user

rajendra0968jangid

- Step 1
Specify user details
- Step 2
Set permissions
- Step 3
Review and create

Specify user details

User details

User name

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

Provide user access to the AWS Management Console - *optional*

If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

ⓘ If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

[Cancel](#)[Next](#)**rajendra0968jangid**

Enter your
username

Click here

aws Search [Alt+S] Global Twinkle%20Sharma

IAM > Users > Create user

- Review and create
- Step 4
- Retrieve password

twinkle

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

Provide user access to the AWS Management Console - *optional*

If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

ⓘ Are you providing console access to a person?

User type

Specify a user in Identity Center - Recommended

We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

I want to create an IAM user

We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

Autogenerated password

You can view the password after you create the user.

Custom password

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Select this



aws | Search [Alt+S] Global Twinkle%20Sharma

IAM > Users > Create user

Select custom password

Deselect this

Enter password

Autogenerated password
You can view the password after you create the user.

Custom password
Enter a custom password for the user.

Show password

Users must create a new password at next sign-in - Recommended
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Cancel Next

Click on Next

aws | Search [Alt+S] Global Twinkle%20Sharma

IAM > Users > Create user

Step 3 Review and create

Step 4 Retrieve password

Permissions options

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

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

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

Get started with groups
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

Create group

Set permissions boundary - optional

rajendra0968jangid

Cancel Previous Next

Click on create group

aws

Search

IAM > Users > Create

Step 3
Review and create

Step 4
Retrieve password

Enter user group name

Select Policy

CloudShell Feedback

Create user group

Create a user group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

User group name
Enter a meaningful name to identify this group.
admin
Maximum 128 characters. Use alphanumeric and '+,-,_' characters.

Permissions policies (1/1060)
Filter by Type
Search All t... ▾
Policy name ▾ Type Use... Description
  AdministratorAccess AWS managed ... None Provides full access to AWS services
  AdministratorAccess... AWS managed None Grants account administrative per...
  AdministratorAccess... AWS managed None Grants account administrative per...

Cancel Create user group

Global Twinkle%20Sharma

Create group

Previous Next

Click on create user

aws Search [Alt+S]

IAM > Users > Create user

admin user group created.

User groups (1)

Group name ▾ Users Attached policies ▾ Created

admin 0 AdministratorAccess 2025-07-11 (Now)

Set permissions boundary - optional

rajendra0968jangid

Select Group →

Click on Next →

Cancel Previous Next

aws Search [Alt+S] Global Twinkle%20Sharma

IAM > Users > Create user

✓ admin user group created.

Step 1 Specify user details
Step 2 Set permissions
Step 3 Review and create
Step 4 Retrieve password

Review and create

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

User details		
User name twinkle	Console password type Custom password	Require password reset No

Permissions summary

Name	Type	Used as
No resources		

Scroll Down < 1 >

aws Search [Alt+S] Global Twinkle%20Sharma

IAM > Users > Create user

✓ admin user group created.

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

Add new tag 

You can add up to 50 more.

Click on Add tag

rajendra0968jangid

Cancel Previous Create user

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws | Search [Alt+S] Global Twinkle%20Sharma

IAM > Users > Create user

admin user group created.

No resources

Tags - optional
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

Key: department Value - optional: Engineering Remove

Add new tag

You can add up to 49 more tags.

Enter Key & value

Than, click on create user

rajendra0968jangid

Cancel Previous Create user

aws | Search [Alt+S] Global Twinkle%20Sharma

IAM > Users > Create user

User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.

View user

Step 2 Set permissions
Step 3 Review and create
Step 4 Retrieve password

time you can view and download this password.

Console sign-in details

Console sign-in URL: [Email sign-in instructions](#)

User name: twinkle

Console password: ***** Show

Click on return to user list

Download .csv file Return to users list

User is created now

IAM > Users

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings
- Root access management New

Access reports

Users (1) Info

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

User name	Path	Group	Last activity	MFA	Password age
twinkle	/	1	-	-	4 minutes

Search

Delete Create user

Click on dashboard

rajendra0968jangid

IAM > Dashboard

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings
- Root access management New

Access reports

IAM Dashboard Info

New access analyzers available
Access Analyzer now analyzes internal access patterns to your critical resources within a single account or across your entire organization.

Create new analyzer

Security recommendations 1

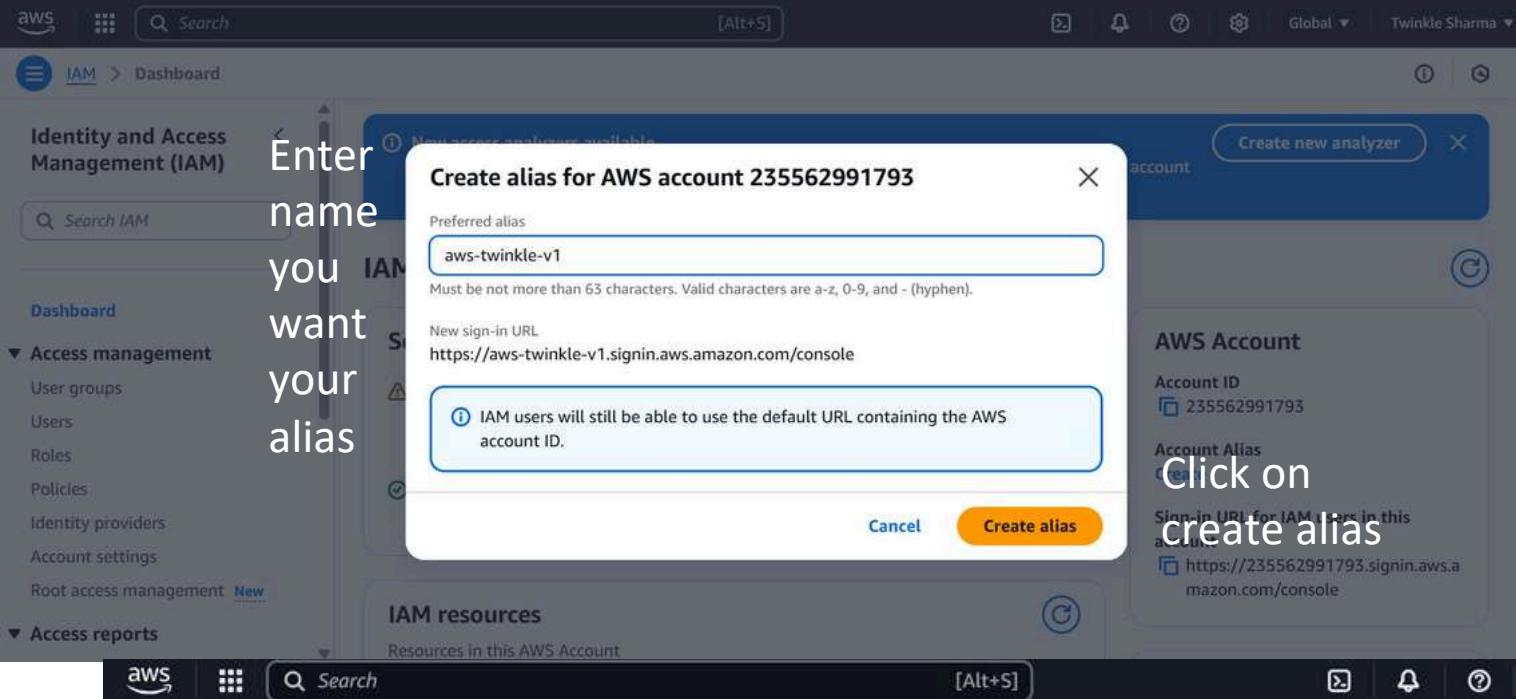
⚠ Add MFA for root user
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

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

AWS Account

Account ID 235562991793
Account Alias Create
Sign-in URL for IAM users in this account https://235562991793.signin.aws.amazon.com/console

Click on create alias



Enter name you want your alias

Click on create alias

rajendra0968jangid

Alias aws-twinkles-v1 created for this account.

Our account alias is created

Copy this URL & paste it in incognite browser for login user

AWS Account

Account ID: 235562991793

Account Alias: aws-twinkles-v1

Sign-in URL for IAM users in this account: https://aws-twinkles-v1.siginin.aws.amazon.com/console

The screenshot shows the AWS IAM Dashboard. A green success message at the top says 'Alias aws-twinkles-v1 created for this account.' On the left, the 'Access management' section is expanded, showing 'User groups', 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings', and 'Root access management'. On the right, there's a 'Security recommendations' section with two items: 'Add MFA for root user' (warning icon) and 'Root user has no active access keys' (checkmark icon). Below that is an 'AWS Account' summary with the account ID, alias, and sign-in URL. A large orange arrow points from the text 'Our account alias is created' to the 'Account Alias' field. Another orange arrow points from the text 'Copy this URL & paste it in incognite browser for login user' to the 'Sign-in URL' field.

Amazon Web Services Sign-In

eu-north-1.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=TxQ3mUqNz7ZS-1m01... Incognito

New sign in ▾ Multi-session disabled ▾ English ▾

You are currently using the improved sign in UI experience. The improved sign in experience will launch soon. During this time, you can still change back to legacy sign in using the dropdown in the upper right corner.

rajendra0968jangid

aws

IAM user sign in ⓘ

Account ID or alias (Don't have?)
aws-twinkles-v1

Remember this account

IAM username

Enter your username

Amazon Lightsail

Lightsail is the easiest way to get started on AWS

Learn more »

Enter Password

After that click on sign-in

Sign in

Having trouble?

Sign in using root user email

Create a new AWS account

By continuing, you agree to 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.

© 2025 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scroll down

This is root user

Console sign-in

Console sign-in link
<https://aws-twinkles-v1.signin.aws.amazon.com/console>

Last console sign-in
Never

Groups (1) Tags (1) Security credentials

Account ID
2355-6299-1793

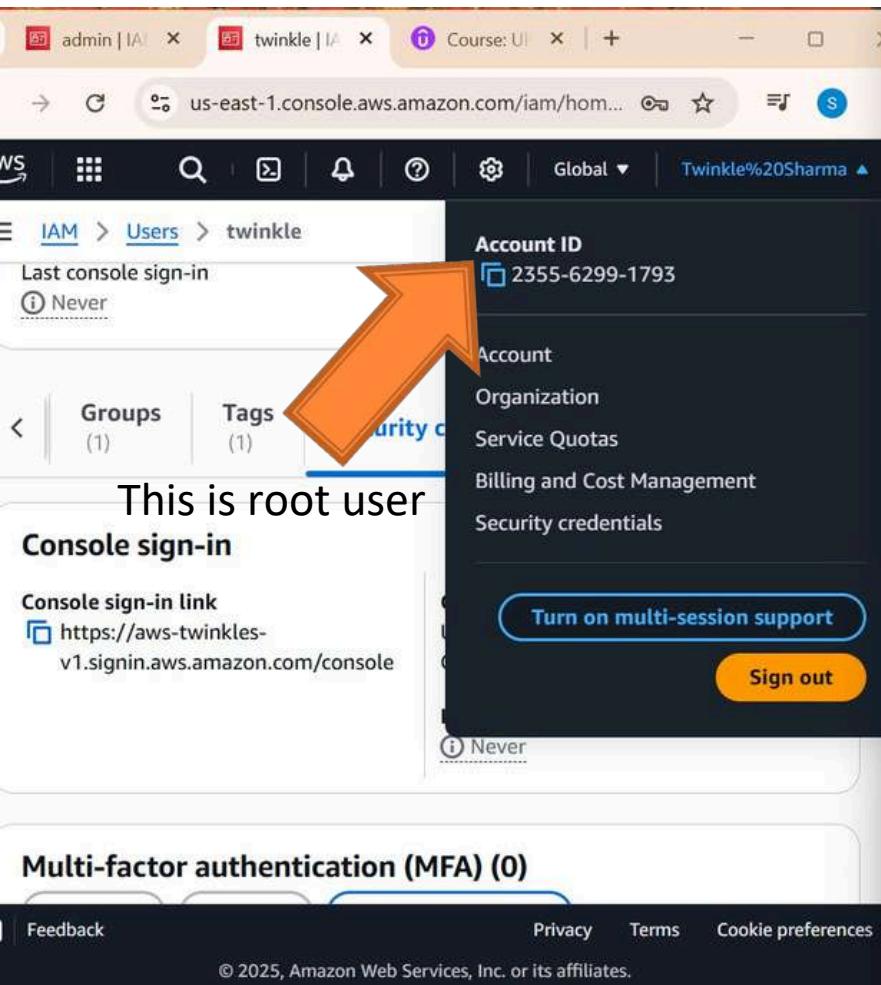
Account Organization Service Quotas Billing and Cost Management Security credentials

Turn on multi-session support Sign out

Never

Feedback Privacy Terms Cookie preferences

© 2025, Amazon Web Services, Inc. or its affiliates.



Console Home | Console Home

eu-north-1.console.aws.amazon.com/console/home?region=eu-north-1

aws Europe (Stockholm) twinkle @ aws-twinkles-v1

Console Home Info

Recently visited Info This is IAM User

No recently visited services

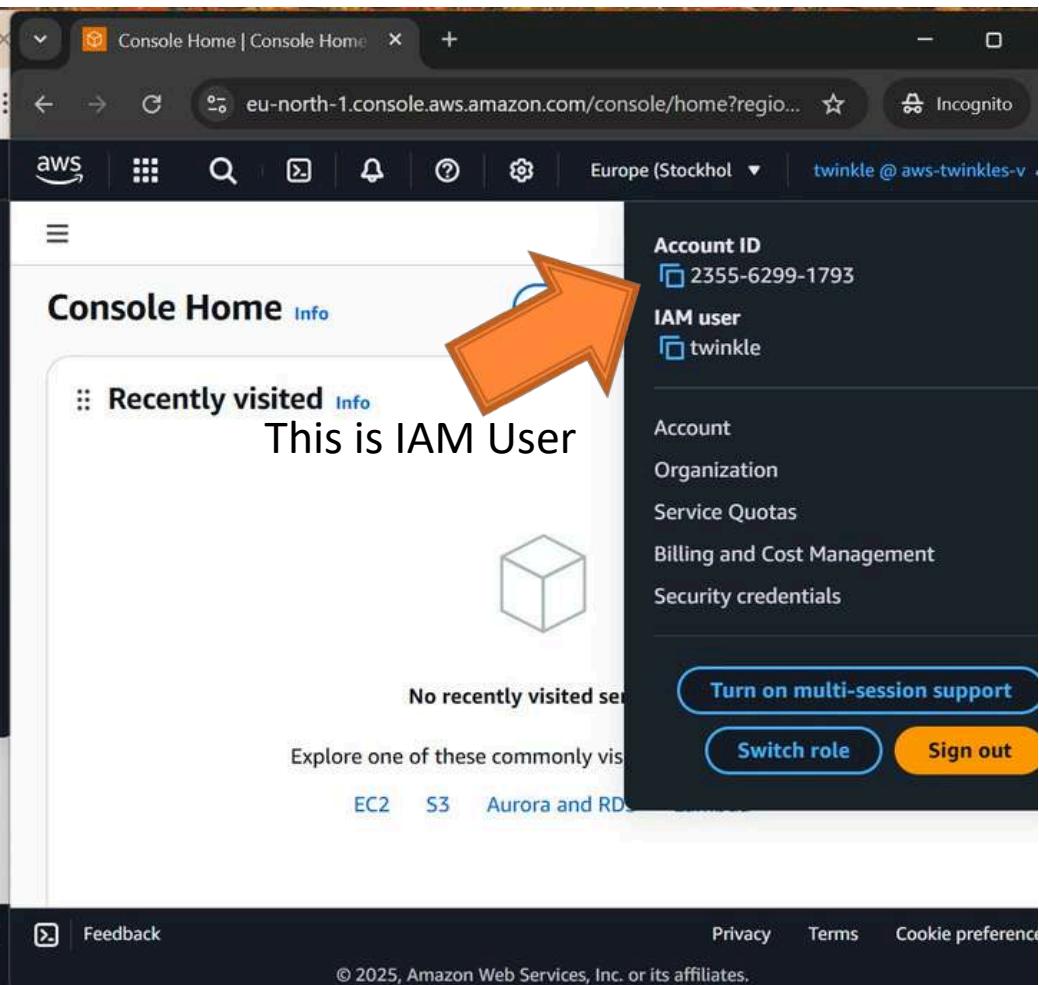
Explore one of these commonly visited services

EC2 S3 Aurora and RDS

Turn on multi-session support Switch role Sign out

Feedback Privacy Terms Cookie preferences

© 2025, Amazon Web Services, Inc. or its affiliates.



rajendra0968jangid

IAM Policy

An IAM policy is a set of rules written in JSON format that determines whether a request is allowed or denied. It controls access to AWS services and resources.

Types of IAM Policies

Type	Description	Example
Identity-based policies	Attached to users, groups, or roles to grant permissions.	"Allow EC2 start for developers"
Resource-based policies	Attached directly to resources (like S3 buckets or SNS topics).	"Allow another account to access my bucket"
Permissions boundaries	Set limits on the maximum permissions an identity-based policy can grant.	"User can't delete EC2 even if a policy says yes"
Organizations SCPs	Service Control Policies applied at AWS Organization level.	"Deny root account from disabling CloudTrail"
Session policies	Passed when assuming a role (temporary permissions).	"Allow temporary upload to S3 during session"

Structure of an IAM Policy

A basic IAM policy contains the following key elements:

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "s3:PutObject",  
      "Resource": "arn:aws:s3:::my-bucket/*"  
    }  
  ]  
}
```

Breakdown of the Policy Structure:

json

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "s3:PutObject",  
      "Resource": "arn:aws:s3:::my-bucket/*"  
    }  
  ]  
}
```

Element	Description
"Version"	Specifies the policy language version. Always use "2012-10-17" (latest version).
"Statement"	One or more individual permission blocks.
"Effect"	Either "Allow" or "Deny" — determines if the action is permitted or blocked.
"Action"	Specifies the AWS service actions (like s3:GetObject , ec2:StartInstances).
"Resource"	Specifies the ARN of the resource the action applies to.
"Condition" (Optional)	Adds conditions to when the policy is in effect (e.g., based on IP address, time, MFA).

Identity and Access Management (IAM)

Search IAM
Here we have policies
Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management [New](#)

▼ Access reports

[IAM](#) > [Policies](#) > IAMAccessAdvisorReadOnly

Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management [New](#)

▼ Access reports

On clicking IAM


Policies (1372) [Info](#)

A policy is an object in AWS that defines permissions.

On Searching IAM here



Actions ▾

Delete

Create policy

Filter by Type

Search

All types

1 2 3 4 5 6 7 ... 69



Policy name	Type	Used as	Description
AccessAnalyzerSer...	AWS managed	None	-
AdministratorAccess	AWS managed - job fu...	Permissions policy (1)	Provides full access to AWS services an...
AdministratorAcce...	AWS managed	None	Grants account administrative perm iss...
AdministratorAcce...	AWS managed	None	Grants account administrative perm iss...
AIOpsAssistantPolicy	AWS managed	None	Provides ReadOnly permissions requir...
AIOpsConsoleAdmi...	AWS managed	None	Grants full access to Amazon AI Opera...
AIOpsOperatorAcc...	AWS managed	None	Grants access to the Amazon AI Opera...

Type
AWS managedCreation time
June 22, 2019, 01:03
(UTC+05:30)Edited time
June 22, 2019, 01:03
(UTC+05:30)ARN
[arn:aws:iam::aws:policy/IAMAccessAdvisorReadOnly](#)

Permissions

Entities attached

Policy versions
(1)

Last Accessed

Permissions defined in this policy [Info](#)

Summary

JSON

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Search

Allow (2 of 445 services)

Show remaining 443 services

Service

Access level

Resource

Request condition

IAM

Limited: List, Read

All resources

None

aws | Search [Alt+S] Global Twinkle%20Sharma

IAM > Policies > IAMAccessAdvisorReadOnly

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies**
- Identity providers
- Account settings
- Root access management [New](#)

Access reports

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies**
- Identity providers
- Account settings
- Root access management [New](#)

Access reports

Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

Search

< Services Actions in IAM (13 of 176)

Read (8 of 34)

Action	Resource	Request conditions
GenerateCredentialReport	All resources	None
GenerateOrganizationsAccessReport	All resources	None
GenerateServiceLastAccessedDetails	All resources	None
GetOrganizationsAccessReport	All resources	None
GetPolicy	All resources	None

Show remaining 163 actions

It is showing summary

On clicking JSON u will see the JSON code permissions defined

Copy Summary **JSON**

```
1: {
2:     "Version": "2012-10-17",
3:     "Statement": [
4:         {
5:             "Effect": "Allow",
6:             "Action": [
7:                 "iam>ListRoles",
8:                 "iam>ListUsers",
9:                 "iam>ListGroups",
10:                "iam>ListPolicies",
11:                "iam>ListPoliciesGrantingServiceAccess",
12:                "iam>GenerateServiceLastAccessedDetails",
13:                "iam>GenerateOrganizationsAccessReport",
14:                "iam>GenerateCredentialReport",
15:                "iam>GetRole",
16:                "iam>GetPolicy",
17:                "iam>GetServiceLastAccessedDetails",
18:                "iam>GetServiceLastAccessedDetailsWithEntities",
19:                "iam>GetOrganizationsAccessReport",
20:                "organizations>DescribeAccount",
21:                "organizations>DescribeOrganization",
22:                "organizations>DescribeOrganizationalUnit",
23:                "organizations>DescribePolicy",
24:                "organizations>ListChildren",
25:                "organizations>ListParents",
26:                "organizations>ListPoliciesForTarget",
27:                "organizations>ListRoots",
28:                "organizations>ListPolicies",
29:                "organizations>ListTargetsForPolicy"
30:            ],
31:            "Resource": "*"
32:        }
33:    ]
34: }
```

rajendra0968jangid

IAM Policies Hand On

- Go to portal login root user
- Go to IAM

The screenshot shows the AWS IAM Dashboard. At the top left, there's a navigation bar with the AWS logo, a search bar, and a global dropdown for 'Twinkle%20Sharma'. Below the navigation bar, the main content area has a header 'Root user has no active access keys' with a note about improving security by using IAM users instead of the root user. A large orange arrow points to the 'IAM' link in the breadcrumb trail ('IAM > Dashboard').

IAM resources

User groups	Users	Roles	Policies	Identity providers
1	1	2	0	0

What's new

Updates for features in IAM

- AWS IAM announces support for encrypted SAML assertions. *5 months ago*
- AWS CodeBuild announces support for project ARN and build ARN IAM condition keys. *6 months ago*
- IAM Roles Anywhere credential helper now supports TPM 2.0. *7 months ago*
- Announcing AWS STS support for ECDSA-based signatures of OIDC tokens. *8 months ago*

Quick Links

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

Tools

Policy simulator
The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.

aws Search [Alt+S] Global Twinkle%20Sharma

IAM > Dashboard

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings
- Root access management New

Access reports

- Access Analyzer
- Resource analysis New
- Unused access
- Analyzer settings

Click on Policies

IAM Dashboard Info

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.

AWS Account

Account ID 235562991793

Account Alias aws-twinkles-v1 [Edit](#) | [Delete](#)

Sign-in URL for IAM users in this account
 <https://aws-twinkles-v1.signin.aws.amazon.com/console>

aws Search [Alt+S] Global Twinkle%20Sharma

IAM > Policies

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies**
- Identity providers
- Account settings
- Root access management New

Access reports

Click on create policy

Policies (1372) Info

A policy is an object in AWS that defines permissions.

Filter by Type

Search All types

Policy name	Type	Used as	Description
AccessAnalyzerSer...	AWS managed	None	-
AdministratorAccess	AWS managed - job fu...	Permissions policy (1)	Provides full access to AWS services an...
AdministratorAcce...	AWS managed	None	Grants account administrative permis...
AdministratorAcce...	AWS managed	None	Grants account administrative permis...
AIOpsAssistantPolicy	AWS managed	None	Provides ReadOnly permissions requir...
AIOpsConsoleAdmi...	AWS managed	None	Grants full access to Amazon AI Opera...
AIOpsOperatorAcc...	AWS managed	None	Grants access to the Amazon AI Opera...

- Step 1
Specify permissions
- Step 2
Review and create

Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

[Visual](#)[JSON](#)[Actions ▾](#)

▼ Select a service

Specify what actions can be performed on specific resources in a service.

Service

[Choose a service](#)[+ Add more permissions](#)

Click here to select service

[Cancel](#)[Next](#)

aws Search [Alt+S] Global Twinkle%20Sharma

☰ IAM > Policies > Create policy

Step 1
Specify permissions

Step 2
Review and create

Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

Visual | JSON | Actions ▾ | Copy

▼ Select a service

Specify what actions can be performed on specific resources in a service.

Service

Choose a service

+ Add more permissions

Click here to select service

Cancel Next

Filter services

Commonly used services

- Auto Scaling
- CloudFront
- EC2
- IAM
- Lambda
- RDS
- S3
- SNS

Choose a service

Select IAM

rajendra0968jangid

Cancel Next

Screenshot of the AWS IAM Policy editor interface showing the 'Visual' tab selected. The main section is titled 'IAM' with the sub-section 'Actions allowed'. A search bar labeled 'Filter Actions' contains the text 'listuser'. To the right of the search bar are buttons for 'Effect' (Allow selected), 'Add actions' (disabled), and 'Actions' (dropdown). Below the search bar, there's a list of actions under 'Access level': 'List (39)' (selected) and 'Read (32)'. A large orange arrow points from the text 'Search permission you want to assign for now I am searching listuser' to the search bar.

Visual JSON Actions

IAM

Set permissions for IAM

Specify what actions can be performed on specific resources in IAM.

Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Effect

Allow Deny

Manual actions | Add actions

All IAM actions (iam:*)

Access level

List (39)

Read (32)

Write (6)

Expand all | Collapse all

Search permission you want to assign for now I am searching listuser

Screenshot of the AWS IAM Policy editor interface showing the 'Visual' tab selected. The main section is titled 'IAM' with the sub-section 'Actions allowed'. A search bar labeled 'listuser' has a checked checkbox next to it. To the right of the search bar are buttons for 'Effect' (Allow selected), 'Add actions' (disabled), and 'Actions' (dropdown). Below the search bar, there's a list of actions under 'List': 'ListUserPolicies' (unchecked) and 'ListUsers' (checked). A large orange arrow points from the text 'Select it' to the 'ListUsers' checkbox. A smaller orange arrow points from the text 'Select it' to the 'ListUsers' checkbox.

Visual JSON Actions

IAM

Allow 1 Action

Specify what actions can be performed on specific resources in IAM.

Actions allowed

Specify actions from the service to be allowed.

listuser

Effect

Allow Deny

List

ListUserPolicies Info

ListUsers Info

ListUserTags Info

Select it

Resources

Specified resource ARNs for these actions.

All resources

Screenshot of the AWS IAM Policy editor interface showing the 'Actions allowed' section.

The 'Actions allowed' section includes a search bar labeled 'Filter Actions' with an orange arrow pointing to it, and a list of actions categorized by access level:

- Manual actions | Add actions
- All IAM actions (iam:*)
- Access level
 - ▶ List (39)
 - ▶ Read (32)
 - ▶ Write (6)

Effect: Allow (radio button selected) Deny

Specify what actions can be performed on specific resources in IAM.

Search permission you want to assign for now I am searching Getuser

Screenshot of the AWS IAM Policy editor interface showing the 'Actions allowed' section after searching for 'getuser'.

The 'Actions allowed' section shows the results of the search:

- Read
 - GetUser | Info (arrow pointing to this item)
 - GetUserPolicy | Info

Effect: Allow (radio button selected) Deny

Specify what actions can be performed on specific resources in IAM.

Select it

Specify actions from the service to be allowed.

Filter Actions

Effect

Allow Deny

Manual actions | Add actions

All IAM actions (iam:*)

Access level

- ▶ List (Selected 1/39)
- ▶ Read (Selected 1/32)
- ▶ Write (66)
- ▶ Permissions management (23)
- ▶ Tagging (16)

Expand all | Collapse all

List & Read is assigned

▼ Resources

Specify resource ARNs for these actions.

All



Search



Search

▼ Resources

Specify resource ARNs for these actions.

All

Specific

⚠ The all wildcard "*" may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.

▶ Request conditions - optional

Actions on resources are allowed or denied only when these conditions are met.

+ Add more permissions

!

Security: 0

Errors: 0

⚠ Warnings: 0

💡 Suggestions: 0

Click on Next

Cancel Next

- Step 1
Specify permissions
- Step 2
Review and create

Review and create Info

Review the permissions, specify details, and tags.

Policy details

Policy name

Enter a meaningful name to identify this policy.

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

Description - optional

Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+=.,@-_` characters.

Enter policy name you want to give to your policy

Than scroll down

Permissions defined in this policy Info

Edit

Search

Allow (1 of 445 services)

Show remaining 444 services

Service	Access level	Resource	Request condition
IAM	Limited: List, Read	All resources	None

Add tags - optional Info

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 new tag

You can add up to 50 more tags.

Click on create policy



rajendra0968jangid

Cancel

Previous

Create policy

aws [Alt+S] Global Twinkle%20Sharma

IAM > Policies > newiam

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies**
- Identity providers
- Account settings
- Root access management New

Access reports

newiam Policy created

Edit Delete

Policy details

Type	Creation time	Edited time	ARN
Customer managed	July 14, 2025, 15:27 (UTC+05:30)	July 14, 2025, 15:27 (UTC+05:30)	arn:aws:iam::235562991793:policy/newiam

Permissions Entities attached Tags Policy versions (1) Last Accessed

Permissions defined in this policy Edit Summary JSON

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Search

Allow (1 of 445 services) Show remaining 444 services

aws [Alt+S] Global Twinkle%20Sharma

IAM > Policies > newiam

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User group
- Users
- Roles
- Policies**
- Identity providers
- Account settings
- Root access management New

Access reports

On this policy this 2 policies

Permissions defined in this policy Edit Summary JSON

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Search

< Services Actions in IAM (2 of 176) Show remaining 174 actions

Read (1 of 34)

Action	Resource	Request conditions
GetUser	All resources	None

List (1 of 37)

Action	Resource	Request conditions
ListUsers	All resources	None

Assign Direct policy to user

- Go to IAM
- Go to user

The screenshot shows the AWS IAM Users page. On the left, there's a navigation sidebar with 'Identity and Access Management (IAM)' at the top, followed by 'Dashboard', 'Access management' (which is expanded to show 'User groups', 'Users' - which is currently selected and highlighted in blue, 'Roles', 'Policies', 'Identity providers', 'Account settings', and 'Root access management'), and 'Access reports'. The main content area is titled 'Users (1) Info' and contains a table with one row. The table has columns for 'User name' (with 'twinkle' listed), 'Path' (with a slash '/'), 'Group' (with '1'), and 'Last activity' (with '2 hours ago'). A large orange arrow points from the text 'Click on user' to the 'User name' column of the 'twinkle' row. At the top of the page, there's a search bar, a global dropdown for 'Global', and a user dropdown for 'Twinkle%20Sharma'. On the right side of the main content area, there are 'Delete' and 'Create user' buttons.

User name	Path	Group	Last activity
twinkle	/	1	2 hours ago

rajendra0968jangid

aws [Alt+S] Global Twinkle%20Sharma

IAM > Users > twinkle

Identity and Access Management (IAM)

Search IAM

Created July 11, 2025, 14:34 (UTC+05:30) Last console sign-in Today

Permissions Groups (1) Tags (1) Security credentials Last Accessed

Click on Add permissions

Permissions policies (1)

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

Filter by Type Search All types

Policy name ▾ Type Attached via ▾

AdministratorAccess AWS managed - job function Group admin

▶ Permissions boundary (not set)

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings
- Root access management New

Access reports

aws [Alt+S] Global Twinkle%20Sharma

IAM > Users > twinkle > Add permissions

Step 1 Add permissions Step 2 Review

Add 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](#)

Click on policy directly

Permissions options

- Add user to group Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- Copy permissions Copy all group memberships, attached managed policies, inline policies, and any existing permissions boundaries from an existing user.
- Attach policies directly Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

User groups (0)

Create group

Search

Group name Users Attached policies Created

Q iam



All types

14 matches



1



Policy name

Type

Attached entities

 [AWSIAMIdentityCenterAllo...](#)

AWS managed

0

 [AWSQuickSightListIAM](#)

AWS managed

0

 [IAMAccessAdvisorReadOnly](#)

AWS managed

0

 [IAMAccessAnalyzerFullAccess](#)

AWS managed

0

 [IAMAccessAnalyzerReadO...](#)

AWS managed

0

 [IAmAuditRootUserCredent...](#)

AWS managed

0

 [IAMCreateRootUserPassword](#)

AWS managed

0

 [IAMDeleteRootUserCreden...](#)

AWS managed

0

 [IAMFullAccess](#)

AWS managed

0

 [IAMReadOnlyAccess](#)

AWS managed

0

Select the policy

aws | Search [Alt+S] Global Twinkle%20Sharma

☰ IAM > Users > twinkle > Add permissions

Q Search

	Policy name	Type	Attached entities
<input type="checkbox"/>	IAMAccessAnalyzerReadU...	AWS managed	0
<input type="checkbox"/>	IAmAuditRootUserCredent...	AWS managed	0
<input type="checkbox"/>	IAMCreateRootUserPassword	AWS managed	0
<input type="checkbox"/>	IAMDeleteRootUserCreden...	AWS managed	0
<input type="checkbox"/>	IAMFullAccess	AWS managed	0
<input type="checkbox"/>	IAMReadOnlyAccess	AWS managed	0
<input type="checkbox"/>	IAMSelfManageServiceSpe...	AWS managed	0
<input type="checkbox"/>	IAMUserChangePassword	AWS managed	0
<input type="checkbox"/>	IAMUserSSHKeys	AWS managed	0
<input type="checkbox"/>	newiam	Customer managed	0

Click on Next

[Next](#)

[Cancel](#)

aws | Search [Alt+S] Global Twinkle%20Sharma

IAM > Users > twinkle > Add permissions

Step 1 Add permissions

Step 2 Review

Review

The following policies will be attached to this user. Learn more ↗

User details

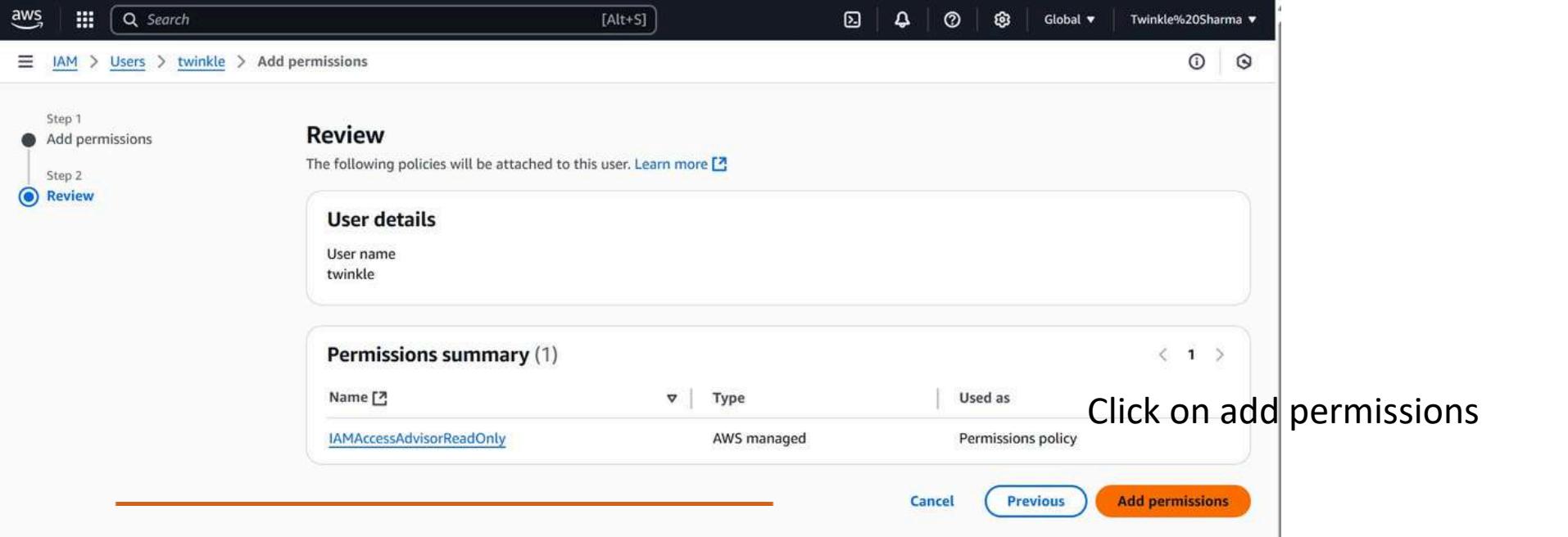
User name
twinkle

Permissions summary (1)

Name	Type	Used as
IAMAccessAdvisorReadOnly	AWS managed	Permissions policy

Cancel Previous Add permissions

Click on add permissions



aws | Search [Alt+S] Global Twinkle%20Sharma

IAM > Users > twinkle

Identity and Access Management (IAM)

Permissions Groups Tags Security credentials Last Accessed

Permissions policies (2)

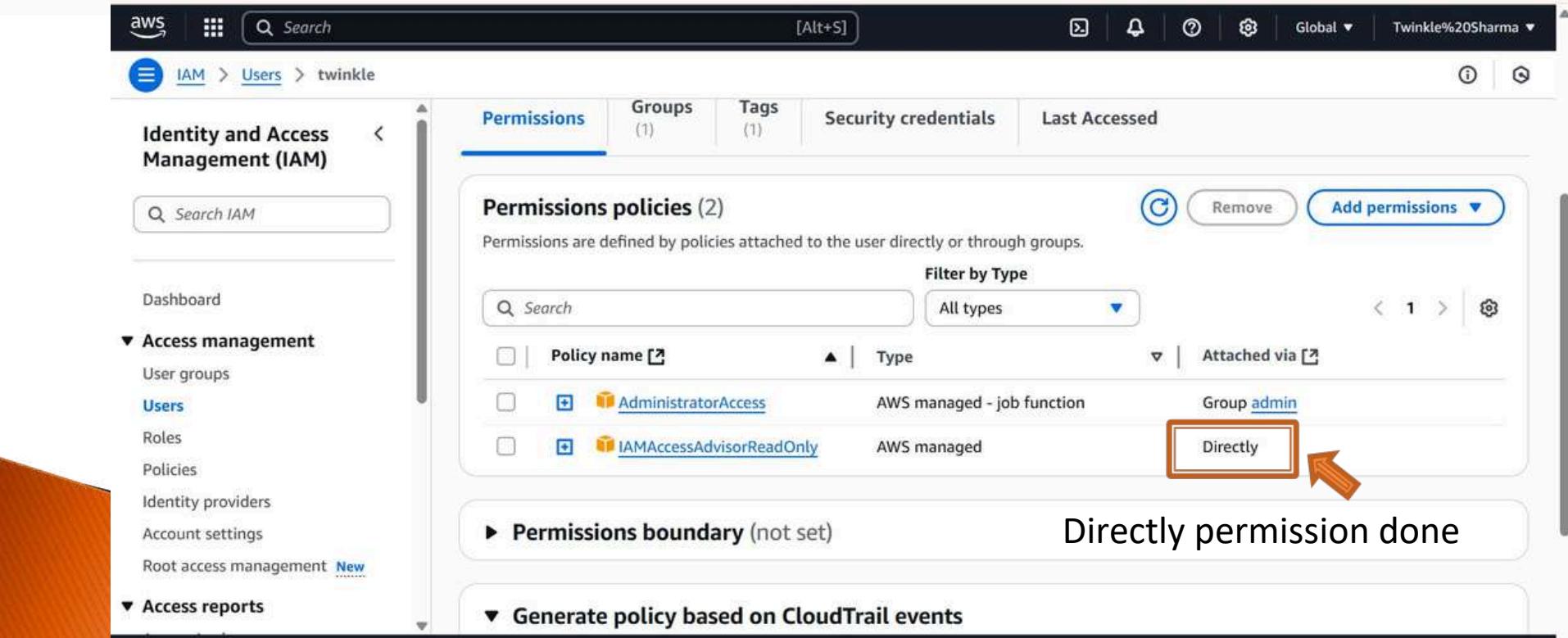
Permissions are defined by policies attached to the user directly or through groups.

Filter by Type

Policy name	Type	Attached via
AdministratorAccess	AWS managed - job function	Group admin
IAMAccessAdvisorReadOnly	AWS managed	Directly

Add permissions

Directly permission done



IAM – Password Policy

An IAM Password Policy in AWS defines the rules for creating and managing console passwords for IAM users. It helps ensure users create strong, secure passwords.

IAM Password Policy Options

Policy Setting	Description
<input checked="" type="checkbox"/> Minimum password length	Set a length from 6 to 128 characters
<input checked="" type="checkbox"/> Require uppercase letters	Must include at least one A–Z
<input checked="" type="checkbox"/> Require lowercase letters	Must include at least one a–z
<input checked="" type="checkbox"/> Require numbers	Must include at least one 0–9
<input checked="" type="checkbox"/> Require non-alphanumeric characters	Must include symbols like !@#\$%
<input checked="" type="checkbox"/> Allow users to change their own password	Users can update their passwords
<input checked="" type="checkbox"/> Enable password expiration	Force password change after X days (up to 1,095 days)
<input checked="" type="checkbox"/> Prevent password reuse	Remember and block reuse of last N passwords (1–24)
<input checked="" type="checkbox"/> Require password reset on next sign-in	When manually creating or updating a password

IAM – MFA (Multi-Factor Authentication)

- MFA requires users to enter:
Username + Password (first factor)
One-time code from a virtual/hardware device (second factor)
- Best practice: Enable MFA for all users who log in to the AWS Management Console—especially the root account.

Why Use MFA in IAM?

- Adds an extra security layer
Prevents unauthorized access

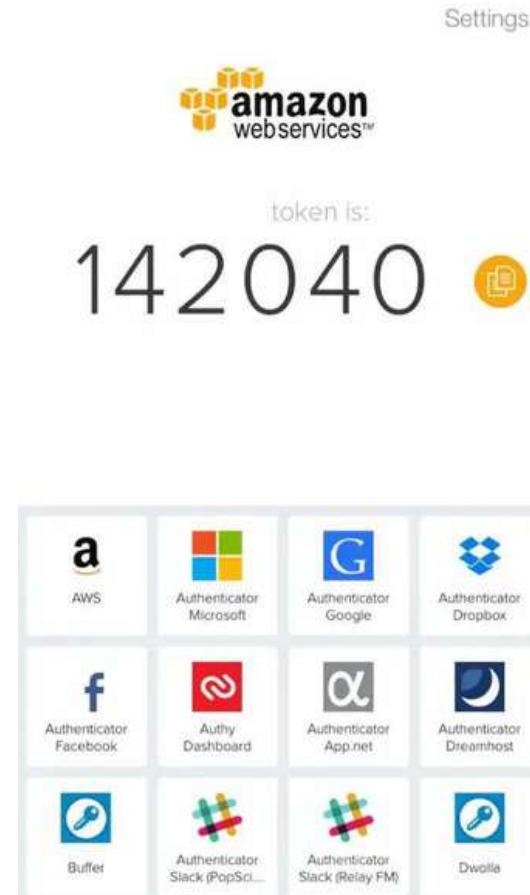
Protects sensitive AWS resources and management actions

MFA Devices Options in AWS

VIRTUAL MFA Device



Google Authenticator
(phoneonly)



Authy
(phone only)

MFA Devices Options in AWS

Universal 2nd Factor (U2F) Security Key



Yubikey by Yubico (3rd Party)

MFA Devices Options in AWS

Hardware Key FOB MFA
Device



Provided by Gemalto (3rd Party)

Hardware Key FOB MFA Device for
AWS Gov Cloud (US)



Provided by SurePassID (3rd Party)

MFA – Hands ON

□ Login to AWS Console Portal

The screenshot shows the AWS IAM Dashboard. On the left, there's a sidebar with navigation links like 'Identity and Access Management (IAM)', 'Dashboard', 'Access management' (with 'User groups', 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings', and 'Root access management'), and 'Access reports'. The main area has a search bar and a 'Global' dropdown. The 'IAM resources' section shows 1 User group, 1 User, 2 Roles, 2 Policies, and 0 Identity providers. Below it is a 'What's new' section with three items. To the right, there's an 'AWS Account' summary with the Account ID (235562991793), Account Alias (aws-twinkle-v4), and a Sign-in URL (https://aws-twinkle-v4.signin.aws.amazon.com/console). A 'Quick Links' section includes 'My security credentials' and 'Manage your access keys, multi-factor'. An orange arrow points to the user name 'Sharma' in the top right corner.

aws | Search [Alt+S] | Global ▾ | Sharma

IAM > Dashboard

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings
- Root access management New

Access reports

IAM Dashboard Info

IAM resources

Resources in this AWS Account
User groups
Users
Roles
Policies
Identity providers

1 1 2 2 0

What's new View all

- AWS IAM announces support for encrypted SAML assertions. 5 months ago
- AWS CodeBuild announces support for project ARN and build ARN IAM condition keys. 6 months ago
- IAM Roles Anywhere credential helper now supports TPM 2.0. 7 months ago

AWS Account

Account ID
235562991793

Account Alias
aws-twinkle-v4 [Edit](#) | [Delete](#)

Sign-in URL for IAM users in this account
<https://aws-twinkle-v4.signin.aws.amazon.com/console>

Quick Links

[My security credentials](#)

[Manage your access keys, multi-factor](#)

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws Search [Alt+S] Global Twinkle%20Sharma

IAM > Dashboard

Identity and Access Management (IAM)

Search IAM

Dashboards

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings
- Root access management New

Access reports

IAM Dashboard Info

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
1	1	2	2	0

Click on security credentials

What's new View all

Updates for features in IAM

- AWS IAM announces support for encrypted SAML assertions. 5 months ago
- AWS CodeBuild announces support for project ARN and build ARN IAM condition keys. 6 months ago
- IAM Roles Anywhere credential helper now supports TPM 2.0. 7 months ago

Account ID: 2355-6299-1793

Account Organization Service Quotas Billing and Cost Management Security credentials

Turn on multi-session support Sign out v4.signin.aws.amazon.com/console

aws Search [Alt+S] Global Twinkle%20Sharma

IAM > Security credentials

Identity and Access Management (IAM)

Search IAM

Access management

- Dashboard
- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings
- Root access management New

Access reports

My security credentials Root user Info

The root user has access to all AWS resources in this account, and we recommend following [best practices](#). To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference

You don't have MFA assigned
As a security best practice, we recommend you assign MFA.

Assign MFA

Click on Assign MFA

Account details

Account name: Twinkle Sharma
AWS account ID: 235562991793

Email address: studyravish@gmail.com
Canonical user ID: 6acd0fafa077a484308a7e05f1d9d18e430f282d1238398ad4a09b1adaae9cf8

Multi-factor authentication (MFA) (0)

Actions ▾ Remove Resync Assign MFA device

- Step 1:
 Select MFA device
Step 2:
 Set up device

Select MFA device Info

MFA device name

Device name

This name will be used within the identifying ARN for this device.

 Twinklephone

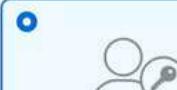
Maximum 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

Enter Device Name

MFA device

Device options

In addition to username and password, you will use this device to authenticate into your account.



Passkey or security key

Authenticate using your fingerprint, face, or screen lock. Create a passkey on this device or use another device, like a FIDO2 security key.

Choose authentication option
For Now I am selecting authenticator App



aws | Search [Alt+S] Global Twinkle%20Sharma

☰ IAM > Security credentials > Assign MFA device

Device options
In addition to username and password, you will use this device to authenticate into your account.

Passkey or security key
Authenticate using your fingerprint, face, or screen lock. Create a passkey on this device or use another device, like a FIDO2 security key.

Authenticator app
Authenticate using a code generated by an app installed on your mobile device or computer.

Hardware TOTP token
Authenticate using a code generated by Hardware TOTP token or other hardware devices.

Passkey display name - Optional
This name will be shown when signing in using passkey. The default suggested name can be customized if needed.
 Use default Passkey display name
235562991793-root-Twinklephone

Maximum 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

aws Search [Alt+S] Global Twinkle%20Sharma

IAM > Security credentials > Assign MFA device

MFA device

Device options

In addition to username and password, you will use this device to authenticate into your account.

- Passkey or security key**
Authenticate using your fingerprint, face, or screen lock. Create a passkey on this device or use another device, like a FIDO2 security key.
- Authenticator app**
Authenticate using a code generated by an app installed on your mobile device or computer.
- Hardware TOTP token**
Authenticate using a code generated by Hardware TOTP token or other hardware devices.

Click on Next

Cancel Next

Install any App in
your mobile Phone
As I Have Android I
am installing google
authenticator



You can install apps for your smartphone from the app store that is specific to your type of smartphone. Some app providers also have web and desktop applications available. See the following table for examples.

You can choose according to your device

Android: [Twilio Authy Authenticator](#), [Duo Mobile](#), [Microsoft Authenticator](#), [Google Authenticator](#), [Symantec VIP](#)

IOS: [Twilio Authy Authenticator](#), [Duo Mobile](#), [Microsoft Authenticator](#), [Google Authenticator](#), [Symantec VIP](#)

aws | Search [Alt+S] Global Twinkle%20Sharma

IAM > Security credentials > Assign MFA device

Step 1
Select MFA device
Step 2
Set up device

Set up device Info

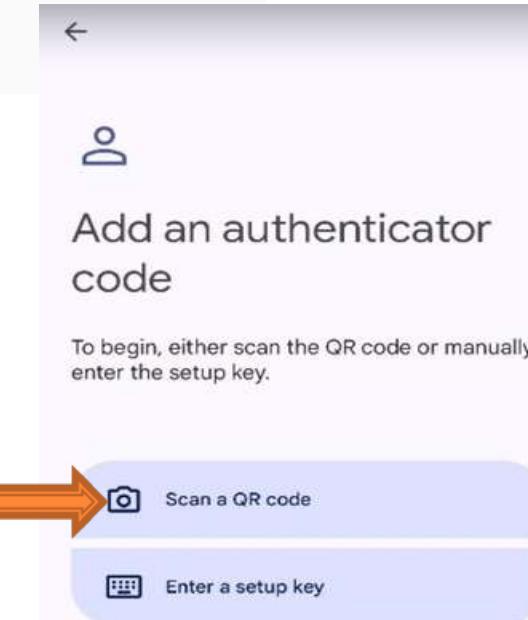
Authenticator app

A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

- 1 Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.
[See a list of compatible applications](#)
- 2  Show QR code
Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key.
[Show secret key](#)
- 3 Type two consecutive MFA codes below
Enter a code from your virtual app below

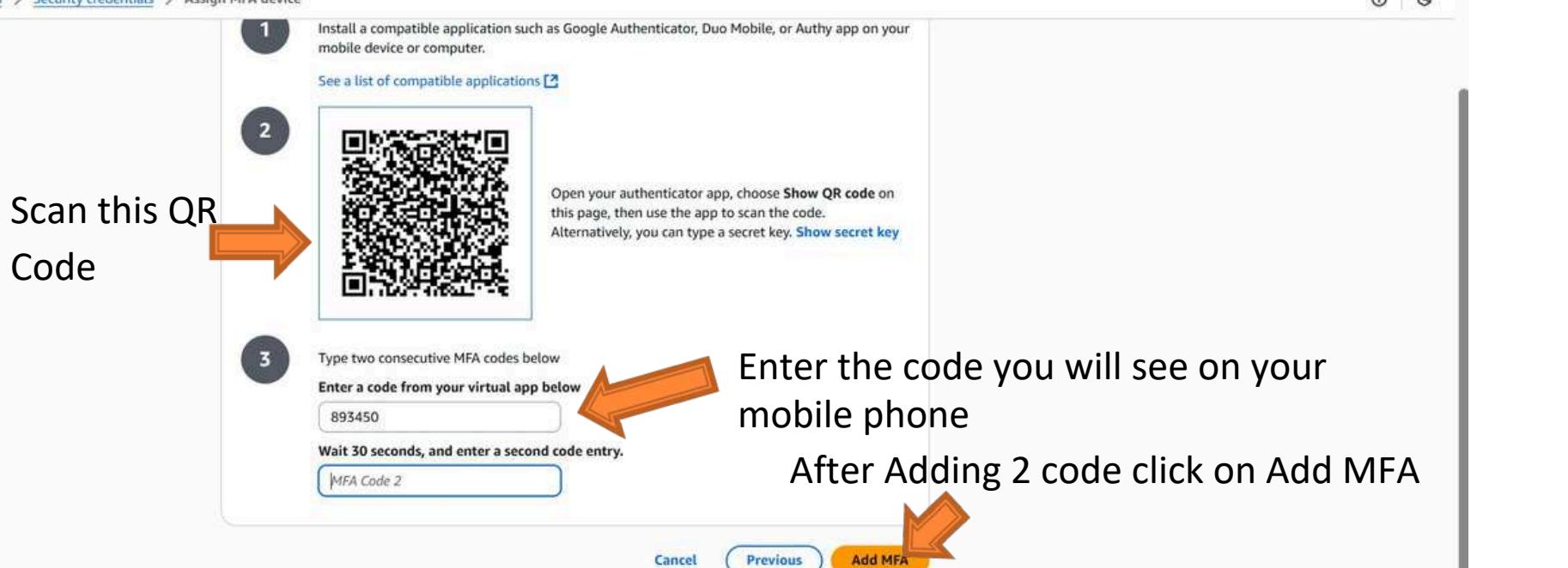
After Installing app click on show QR Code

Open google Authenticator App
inmobilephone



Touch on scan a QR Code

rajendra0968jangid



MFA device assigned
You can register up to 8 MFA devices of any combination of the currently supported MFA types with your AWS account root and IAM user. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the AWS CLI with that user.

MFA completed

Multi-factor authentication (MFA) (1)
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more \[?\]](#)

Type	Identifier	Certifications	Created on
Virtual	arn:aws:iam::235562991793:mfa/Twinklephone	Not Applicable	Fri Jul 18 2025

Access keys (0)
Use access keys to send programmatic calls to AWS from the AWS CLI, AWS 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. [Learn more \[?\]](#)

Access key ID	Created on	Access key last used	Region last used	Service last used	Status
No access keys					

As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. [Learn more \[?\]](#)

Create access key

Here is your device Showing [Create access key](#)

What is access key in AWS?

- An AWS Access Key is a pair of security credentials that allow programmatic access to your AWS account using tools like the AWS CLI, SDKs, or API calls.

What Is an AWS Access Key?

It consists of two parts:

Component	Example Format
Access Key ID	AKIAIOSFODNN7EXAMPLE
Secret Access Key	wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

Together, these are used to **authenticate** your application/script to AWS.

AWS CLI (Command Line Interface)

- The AWS CLI is a unified tool that provides a consistent interface for interacting with AWS services using commands in your shell (PowerShell, Bash, etc.).

What is the AWS SDK (Software Development Kit)?

The AWS SDK allows you to:

Call AWS services programmatically (like EC2, S3, DynamoDB)

Sign requests, handle retries, parse responses

Integrate AWS into mobile, web, and backend applications

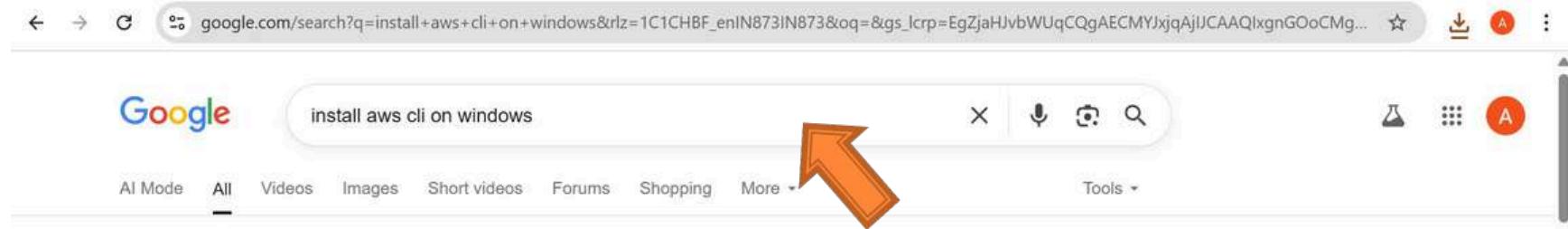
Use temporary credentials, MFA, and roles

It simplifies using AWS APIs in your language of choice.

Popular AWS SDKs by Language

Language	SDK Name	Package Manager
Python	boto3	<code>pip install boto3</code>
JavaScript/Node.js	aws-sdk / @aws-sdk/client-s3	<code>npm install</code>
Java	AWS SDK for Java	Maven/Gradle
C#/.NET	AWS SDK for .NET	NuGet
Go	AWS SDK for Go	<code>go get</code>
PHP	AWS SDK for PHP	Composer
Ruby	AWS SDK for Ruby	<code>gem install</code>

AWS CLI Setup on windows



Search this on browser

Installing or updating to the latest version of the AWS CLI

Install or update the AWS CLI · Unzip the installer. If your Linux distribution doesn't have a built-in unzip command, use an equivalent to unzip it. · Run the ...

Windows

By default, the AWS CLI version 1 installs to C:\Program Files ...

Setting up the AWS CLI

Configuring using AWS CLI commands. For general use, the ...

More results from amazon.com »

Getting started with the AWS CLI

After that, click here

rajendra0968jangid



AWS Command Line Interface

User Guide for Version 2

- ▶ About the AWS CLI
- ▼ Get started
 - Prerequisites
 - Install/Update
 - Past releases
 - Build and install from source
 - Amazon ECR Public/Docker
 - Setup
- ▶ Configure the AWS CLI
- ▶ Authentication and access credentials
- ▶ Using the AWS CLI
- ▶ Code examples

<https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html>

This chapter provides steps to get started with version 2 of the AWS Command Line Interface (AWS CLI) and provides links to the relevant instructions.

1. **Complete all prerequisites** - To access AWS services with the AWS CLI, you need at minimum an AWS account and IAM credentials. To increase the security of your AWS account, we recommend that you do not use your root account credentials. You should create a user with least privilege to provide access credentials to the tasks you'll be running in AWS.
2. Install or gain access to the AWS CLI using one of the following methods:
 - **(Recommended)** [Installing or updating to the latest version of the AWS CLI](#).
 - [Installing past releases of the AWS CLI version 2](#). Installing a specific version is primarily used if your team aligns their tools to a specific version.
 - [Building and installing the AWS CLI from source](#). Building the AWS CLI

▼ Recommended tasks

How to

- [Set up AWS CLI to use with services](#)
- [Enable and configure IAM Identity Center](#)
- [Sign in to AWS CLI with IAM Identity Center](#)

Click here

Did this page help you?

- [Yes](#)
- [No](#)



AWS Command Line Interface

User Guide for Version 2

- ▶ About the AWS CLI
- ▼ Get started
 - Prerequisites
 - [Install/Update](#)
 - Past releases
 - Build and install from source
 - Amazon ECR Public/Docker
 - Setup
- ▶ Configure the AWS CLI
- ▶ Authentication and access credentials
- ▶ Using the AWS CLI
- ▶ Code examples

For installation instructions, expand the section for your operating system.

▶ Linux

▶ macOS

▶ Windows

Scroll Down

On this page

- [AWS CLI install and update instructions](#)
- [Troubleshooting AWS CLI install and uninstall errors](#)
- [Next steps](#)

▼ Recommended tasks

How to

- [Verify Session Manager plugin installation](#)

Learn about

- [Supported AWS Regions for CloudShell](#)

Click on windows

Troubleshooting AWS CLI install and uninstall errors

If you come across issues after installing or uninstalling the AWS CLI, see [Troubleshooting errors for the AWS CLI](#) for troubleshooting steps. For the most relevant troubleshooting steps, see [Command not found errors](#), [The "aws --version" command returns a different version than you installed](#), and [The "aws --version" command returns a version after uninstalling the AWS CLI](#).



AWS Command Line Interface

User Guide for Version 2

- ▶ About the AWS CLI
- ▼ Get started
 - Prerequisites
 - Install/Update**
 - Past releases
 - Build and install from source
 - Amazon ECR Public/Docker
 - Setup
- ▶ Configure the AWS CLI
- ▶ Authentication and access credentials
- ▶ Using the AWS CLI

Code examples
<https://awscli.amazonaws.com/AWSCLIV2.ms>

- We support the AWS CLI on Microsoft-supported versions of 64-bit Windows.
- Admin rights to install software

Install or update the AWS CLI

To update your current installation of AWS CLI on Windows, download a new installer each time you update to overwrite previous versions. AWS CLI is updated regularly. To see when the latest version was released, see the [AWS CLI version 2 Changelog](#) on GitHub.

1. Download and run the AWS CLI MSI installer for Windows (64-bit):

<https://awscli.amazonaws.com/AWSCLIV2.msi>

Alternatively, you can run the `msiexec` command to run the MSI installer.

Click here



On this page

[AWS CLI Install and update instructions](#)

Troubleshooting AWS CLI install and uninstall errors

Next steps

▼ Recommended tasks

How to

[Verify Session Manager plugin installation](#)

Learn about

[Supported AWS Regions for CloudShell](#)

Recent download history

AWSCLIV2.msi
39.2 MB • Done



Click on
downloaded File



AWS Command Line Interface

User Guide for Version 2

- ▶ About the AWS CLI
- ▼ Get started
 - Prerequisites
 - Install/Update**
 - Past releases
 - Build and install from source
 - Amazon ECR Public/Docker
 - Setup
- ▶ Configure the AWS CLI
- ▶ Authentication and access credentials
- ▶ Using the AWS CLI
- ▶ Code examples

- We support the AWS CLI on Microsoft-supported versions of 64-bit Windows.
- Admin rights to install software

Install or update the AWS CLI

To update your current installation of AWS CLI on Windows, download a new installer each time you update to overwrite previous versions. AWS CLI is updated regularly. To see when the latest version was released, see the [AWS CLI version 2 Changelog](#) on GitHub.

1. Download and run the AWS CLI MSI installer for Windows (64-bit):

<https://awscli.amazonaws.com/AWSCLIV2.msi>

Alternatively, you can run the `msiexec` command to run the MSI installer.

<C:\> msiexec.exe /i https://awscli.amazonaws.com/AWSCLIV2.msi>

For various parameters that can be used with `msiexec`, see [msiexec](#)

Full download history

Supported AWS Regions for CloudShell



Get started

Service

AWS Command Line Interface v2 Setup

Create an AWS Account

AWS Command Line Interface

User Guide for Version 2

▶ About the AWS CLI

▼ Get started

Prerequisites

Install/Update

Past releases

Build and install from source

Amazon ECR Public/Docker

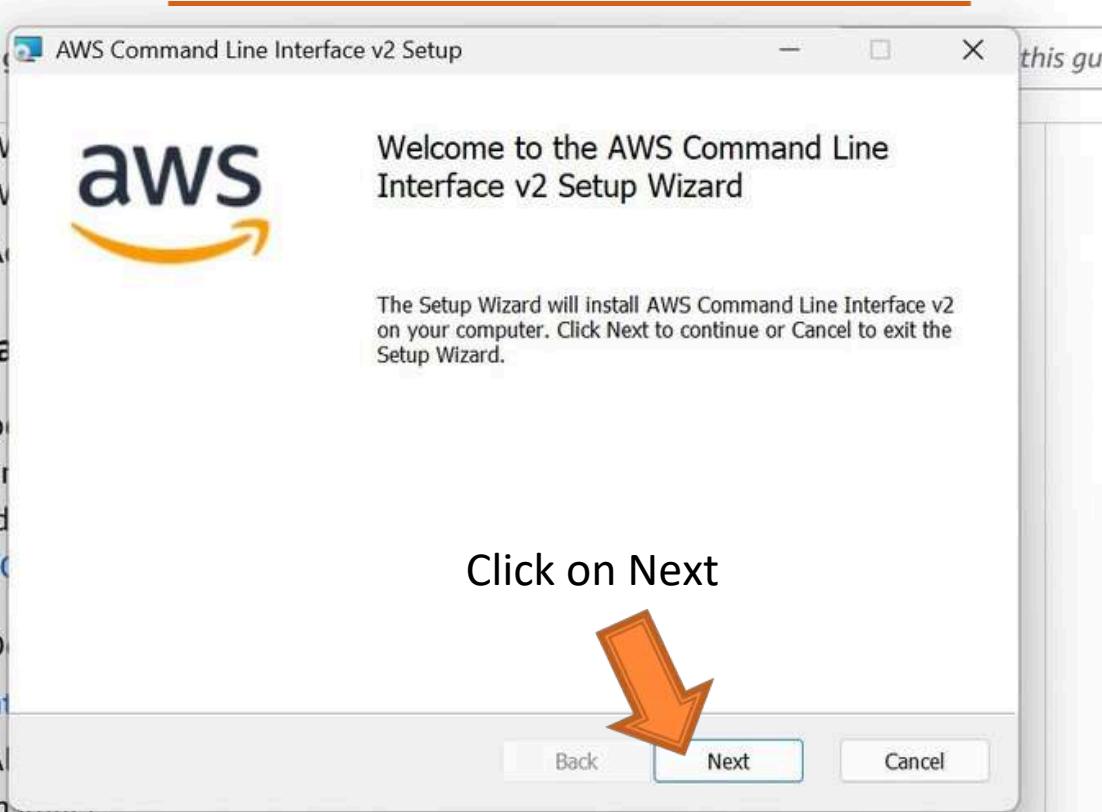
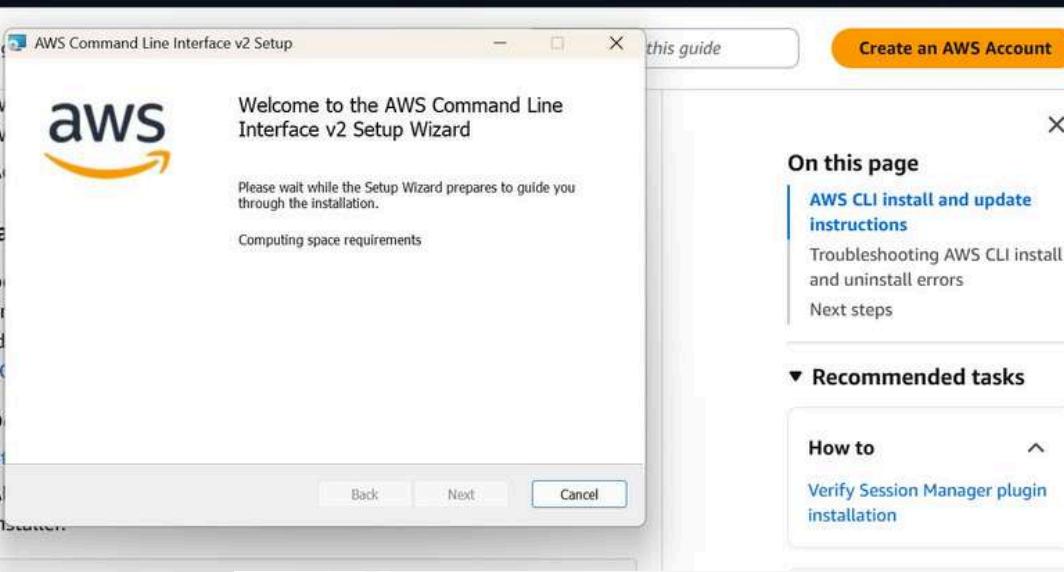
Setup

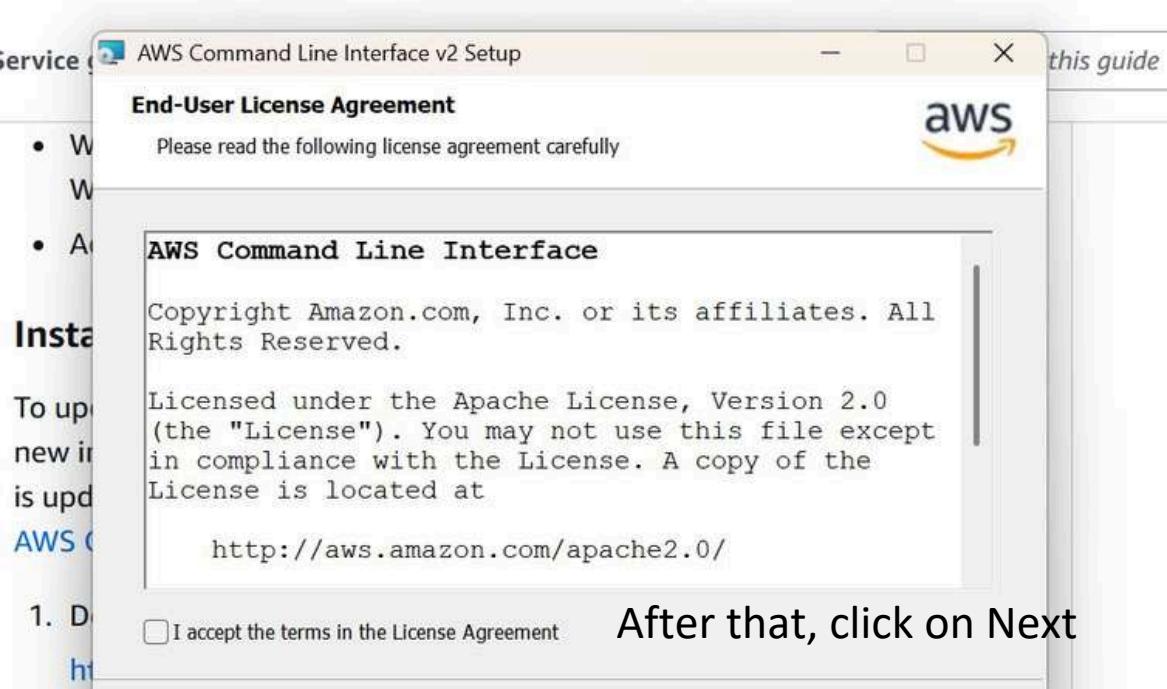
▶ Configure the AWS CLI

▶ Authentication and access credentials

▶ Using the AWS CLI

▶ Code examples

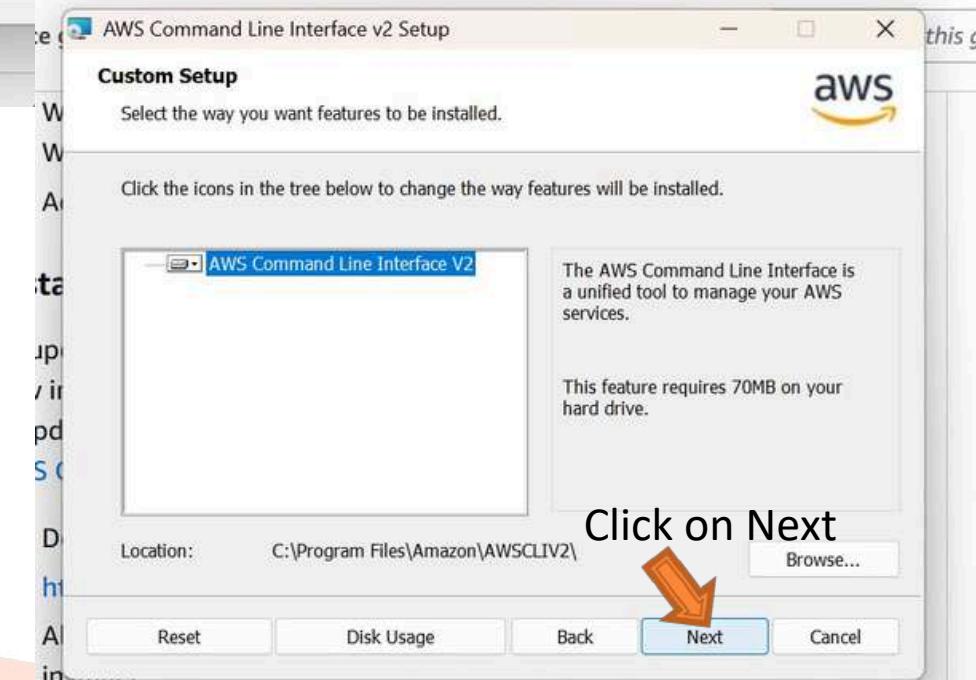




After that, click on Next

Check this

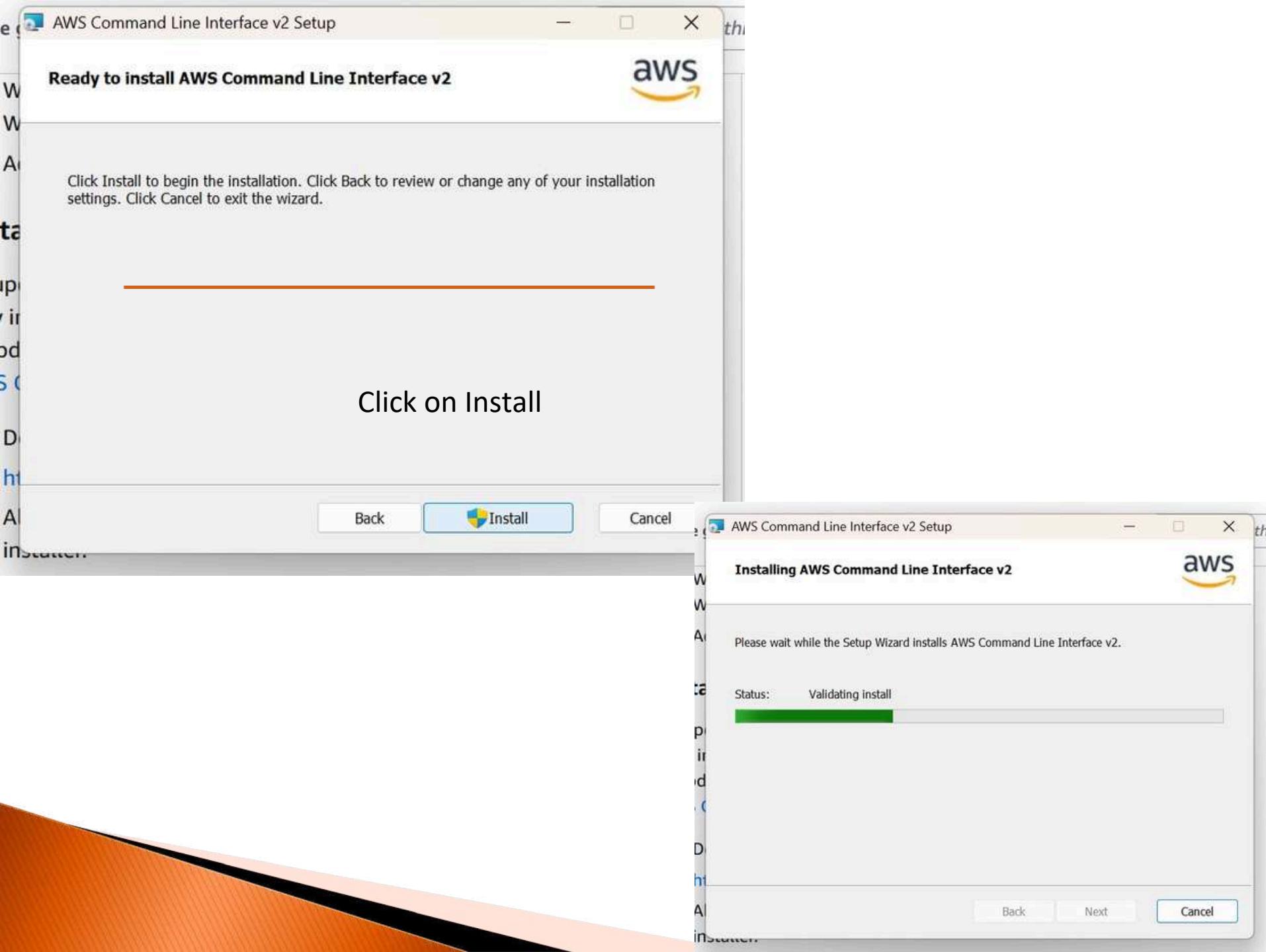
Print Back Next Cancel



Click on Next



Next





Completed the AWS Command Line Interface v2 Setup Wizard

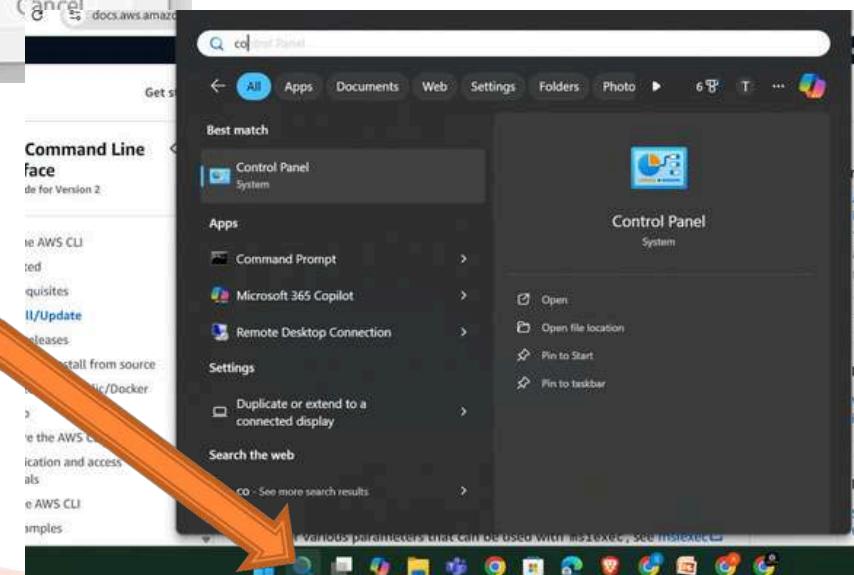
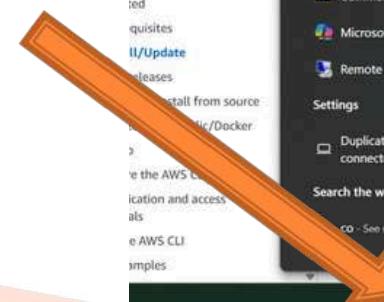
Click the Finish button to exit the Setup Wizard.

Click on Finish



Finish

Click on search, command Prompt



```
C:\Users\██████s>aws --version  
aws-cli/2.27.54 Python/3.13.1 Windows/11 exe/AMD64
```

Type this & press enter

You will see this

AWS CLI Setup on Mac OS X

Google search results for "aws cli install for mac os".

The first result is a link to the AWS Documentation for installing the AWS CLI on macOS.

Search this

Click here

Amazon AWS Documentation
<https://docs.aws.amazon.com/cli/getting-started-install>

Installing or updating to the latest version of the AWS CLI

This topic describes how to install or update the latest release of the AWS Command Line Interface (AWS CLI) on supported operating systems.

macOS Past releases Setting up the AWS CLI Uninstall

Amazon AWS Documentation
<https://docs.aws.amazon.com/userguide/install-macos>

Installing, updating, and uninstalling the AWS CLI version 1 ...

You can install the AWS Command Line Interface (AWS CLI) version 1 and its dependencies on macOS by using the bundled installer or pip.

Amazon AWS Documentation
<https://docs.aws.amazon.com/cli/getting-started-version>

Installing past releases of the AWS CLI version 2



AWS Command Line Interface

User Guide for Version 2

- ▶ About the AWS CLI
- ▼ Get started
 - Prerequisites
 - Install/Update**
 - Past releases
 - Build and install from source
 - Amazon ECR Public/Docker
 - Setup
- ▶ Configure the AWS CLI
- ▶ Authentication and access credentials
- ▶ Using the AWS CLI
- ▶ Code examples

For installation instructions, expand the section for your operating system.

▶ Linux

▶ macOS

▶ Windows

Scroll Down

On this page

AWS CLI install and update instructions

Troubleshooting AWS CLI install and uninstall errors

Next steps

▼ Recommended tasks

How to

Verify Session Manager plugin installation

Learn about

Supported AWS Regions for CloudShell

Click on Mac Os

Troubleshooting AWS CLI install and uninstall errors

If you come across issues after installing or uninstalling the AWS CLI, see Troubleshooting errors for the AWS CLI for troubleshooting steps. For the most relevant troubleshooting steps, see Command not found errors, The "aws --version" command returns a different version than you installed, and The "aws --version" command returns a version after uninstalling the AWS CLI.



AWS Command Line Interface

User Guide for Version 2

- ▶ About the AWS CLI
- ▼ Get started
 - Prerequisites
 - Install/Update**
 - Past releases
 - Build and install from source
 - Amazon ECR Public/Docker
 - Setup
- ▶ Configure the AWS CLI
- ▶ Authentication and access credentials
- ▶ Using the AWS CLI
- ▶ Code examples

GUI installer

Command line installer - All users

The following steps show how to install the latest version of the AWS CLI by using the standard macOS user interface and your browser.

1. In your browser, download the macOS pkg file:

<https://awscli.amazonaws.com/AWSCLIV2.pkg>

2. Open your downloaded file and follow the on-screen instructions.

You can choose to install the AWS CLI in the following ways:

- For all users on the computer (requires sudo)

You can install to any folder, or choose the recommended default folder of /usr/local/aws-cli.

- The installer automatically creates a symlink at /usr/local/bin/aws that links to the main program in the installation folder you chose.

- For only the current user (doesn't require sudo)

- You can install to any folder to which you have write

Click here

On this page

AWS CLI install and update instructions

Troubleshooting AWS CLI install and uninstall errors

Next steps

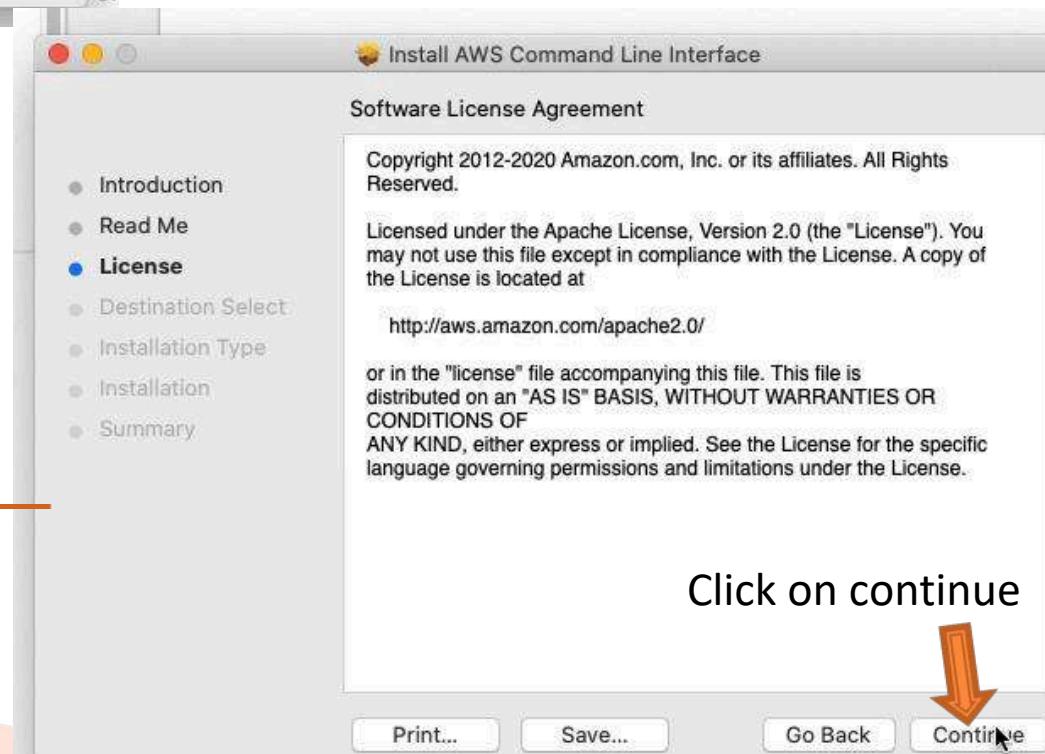
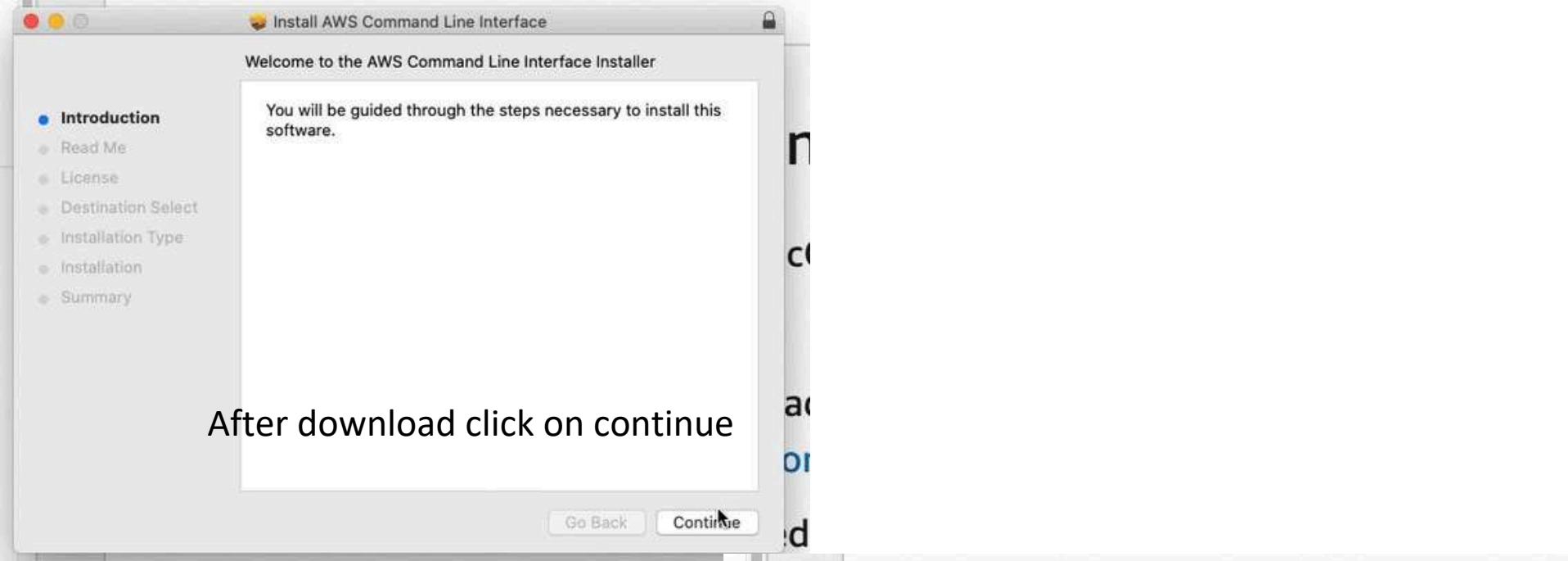
▼ Recommended tasks

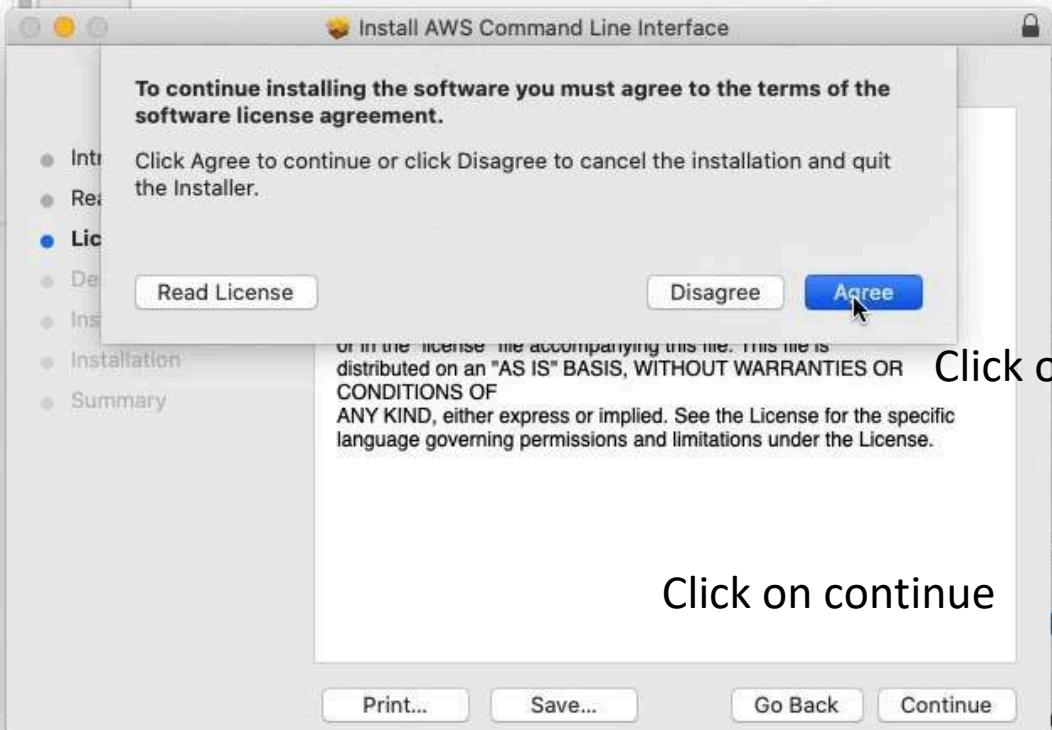
How to

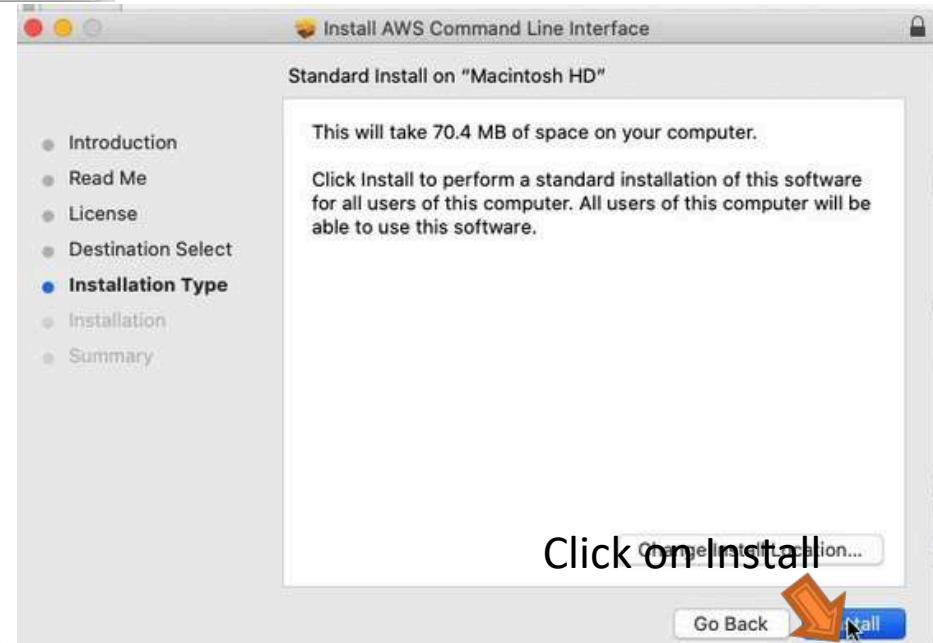
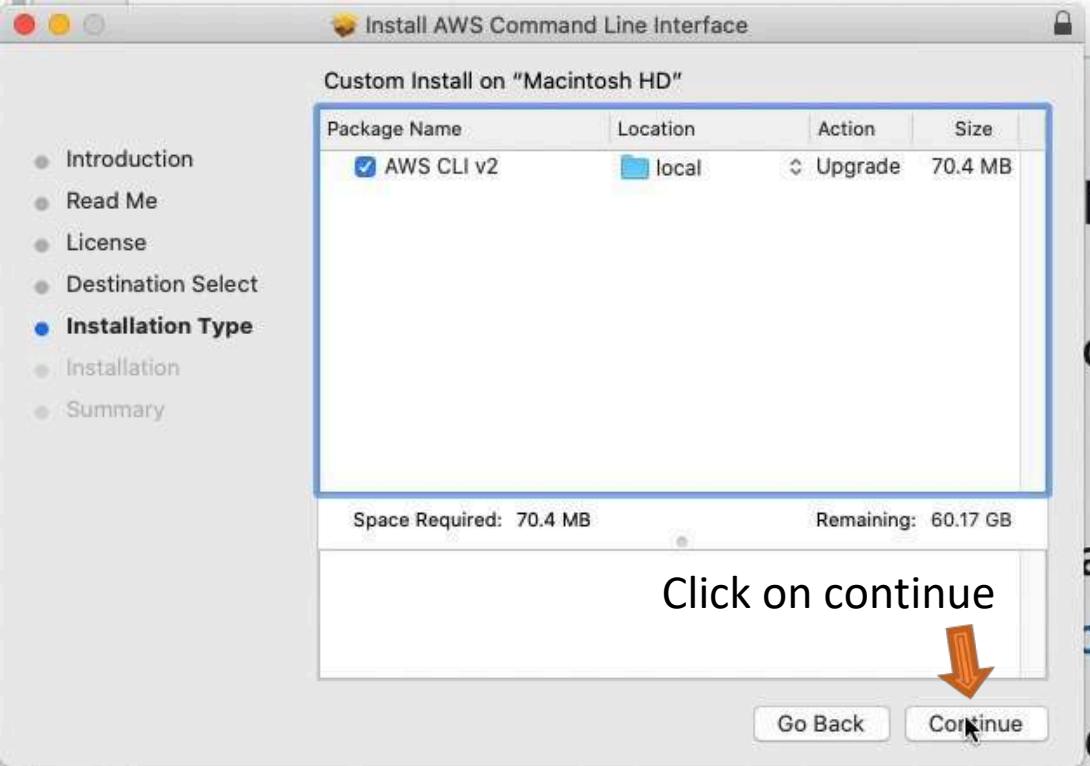
Verify Session Manager plugin installation

Learn about

Supported AWS Regions for CloudShell









Installer is trying to install new software.

Enter your password to allow this.

User Name: Stephane Maarek

Password: [REDACTED]

Cancel

Install Software

Enter password

Click on install software

Install AWS Command Line Interface

The installation was completed successfully.

- Introduction
- Read Me
- License
- Destination Select
- Installation Type
- Installation
- Summary



The installation was successful.

The software was installed.

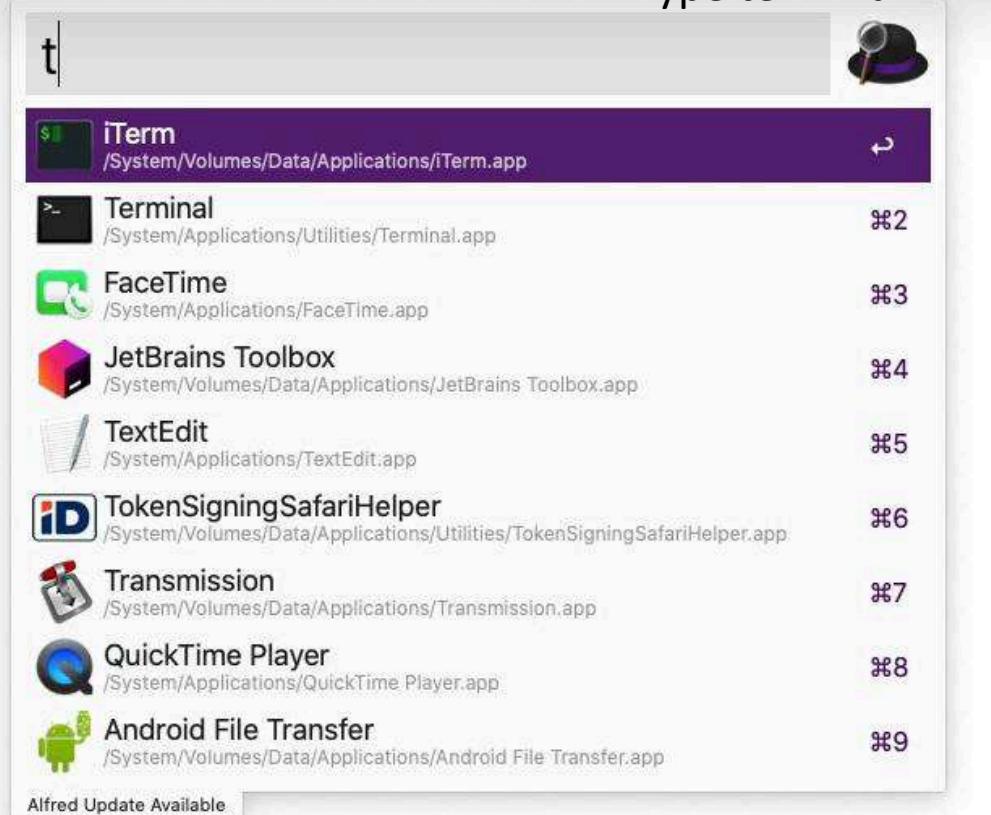
Click on Close



Go Back

Close

Type terminal



```
aws --version
```

Type this & press enter

```
aws --version
aws-cli/2.0.10 Python/3.7.4 Darwin/19.3.0 botocore/2.0.0dev14
```



It will show this when cli is installed

AWS CLI Setup on Linux

← → ⌂ google.com/search?q=install+aws+cli+on+linux&rlz=1C1CHBF_enIN873IN873&oq=install+aws+cli+on+linux&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIICA... ☆ ⬇ A :

Google X |

AI Mode All Videos Short videos Images Forums Shopping More Tools

Search this

[Amazon AWS Documentation](https://docs.aws.amazon.com/cli/getting-started-install)
https://docs.aws.amazon.com › cli › getting-started-install

Installing or updating to the latest version of the AWS CLI

This topic describes how to install or update the latest release of the AWS Command Line Interface (AWS CLI) on supported operating systems.

[Linux](#) [Past releases](#) [Setting up the AWS CLI](#) [Migration guide](#)

[Amazon AWS Documentation](https://docs.aws.amazon.com/userguide/install-linux)
https://docs.aws.amazon.com › userguide › install-linux

Installing, updating, and uninstalling the AWS CLI version 1 ...

You can install the AWS Command Line Interface (AWS CLI) version 1 and its dependencies on most Linux distributions by using the pip package manager or the ...

[eG Innovations](https://www.eginnovations.com/documentation/installation/)
https://www.eginnovations.com › documentation › Inst...

Installing AWS CLI version 2 on Windows and Linux

<https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html> i-screen instructions. By default, the AWS CLI



AWS Command Line Interface

User Guide for Version 2

- ▶ About the AWS CLI
- ▼ Get started
- Prerequisites
- Install/Update**
- Past releases
- Build and install from source
- Amazon ECR Public/Docker
- Setup
- ▶ Configure the AWS CLI
- ▶ Authentication and access credentials
- ▶ Using the AWS CLI
- ▶ Code examples

AWS CLI install and update instructions

For installation instructions, expand the section for your operating system.

▶ Linux

▶ macOS

▶ Windows

Click on Linux

Scroll Down

On this page

[AWS CLI install and update instructions](#)

Troubleshooting AWS CLI install and uninstall errors

Next steps

▼ Recommended tasks

How to

[Verify Session Manager plugin installation](#)

Learn about

[Supported AWS Regions for CloudShell](#)

Troubleshooting AWS CLI install and uninstall errors



AWS Command Line Interface

User Guide for Version 2

- ▶ About the AWS CLI
- ▼ Get started
- Prerequisites
- Install/Update**
- Past releases
- Build and install from source
- Amazon ECR Public/Docker
- Setup
- ▶ Configure the AWS CLI
- ▶ Authentication and access credentials
- ▶ Using the AWS CLI
- ▶ Code examples

\$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" > awscliv2.zip

- **Downloading from the URL** – To download the installer with your browser, use the following URL:

https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip

2. (Optional) Verifying the integrity of your downloaded zip file

If you chose to manually download the AWS CLI installer package .zip in the above steps, you can use the following steps to verify the signatures by using the GnuPG tool.

The AWS CLI installer package .zip files are cryptographically signed using PGP signatures. If there is any damage or alteration of the files, this verification fails and you should not proceed with installation.

- a. Download and install the gpg command using your package manager. For more information about GnuPG, see the [GnuPG website](#).

- b. To create the public key file, create a text file and paste in the

On this page

[AWS CLI install and update instructions](#)

Troubleshooting AWS CLI install and uninstall errors

Next steps

▼ Recommended tasks

How to

[Verify Session Manager plugin installation](#)

Learn about

[Supported AWS Regions for CloudShell](#)

Click here



□Do whole process

The screenshot shows the AWS Command Line Interface User Guide for Version 2. On the left sidebar, under the 'Install/Update' section, there are two links: 'Past releases' and 'Build and install from source'. A large orange arrow points from the text 'Copy & paste this' to the 'Build and install from source' link. Below this, another orange arrow points from the text 'At last type this you will get the version of CLI' to a terminal window at the bottom right.

AWS Command Line Interface
User Guide for Version 2.

Get started Service guides Developer tools AI resources

Search in this guide Create an AWS Account

On this page

- AWS CLI install and update instructions
- Troubleshooting AWS CLI install and uninstall errors
- Next steps

Recommended tasks

How to

- Verify Session Manager plugin installation

Learn about

- Supported AWS Regions for CloudShell

Copy & paste this

a. Download and install the `gpg` command using your package manager. For more information about GnuPG, see the [GnuPG website](#).

b. To create the public key file, create a text file and paste in the following text.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----  
  
mQINBF2Cr7UBEADJZHcgusOj17ENSy whole block of text
```

At last type this you will get the version of CLI

```
File Edit View Search Terminal Help  
Inflating: aws/dist/botocore/data/discovery/2015-11-01/paginator...  
creating: aws/dist/botocore/data/appstream/2016-12-01/  
Inflating: aws/dist/botocore/data/appstream/2016-12-01/service-2.json  
Inflating: aws/dist/botocore/data/appstream/2016-12-01/examples-1.json  
Inflating: aws/dist/botocore/data/appstream/2016-12-01/paginator...  
Inflating: aws/dist/botocore/data/appstream/2016-12-01/waiters-2.json  
Creating: aws/dist/botocore/data/appconfig/2019-10-09/  
Inflating: aws/dist/botocore/data/appconfig/2019-10-09/service-2.json  
Inflating: aws/dist/botocore/data/appconfig/2019-10-09/paginator...  
Creating: aws/dist/botocore/data/events/2015-10-07/  
Inflating: aws/dist/botocore/data/events/2015-10-07/service-2.json  
Inflating: aws/dist/botocore/data/events/2015-10-07/examples-1.json  
Inflating: aws/dist/botocore/data/events/2015-10-07/paginator...  
Creating: aws/dist/botocore/data/comprehendmedical/2018-10-30/  
Inflating: aws/dist/botocore/data/comprehendmedical/2018-10-30/service-2.json  
Inflating: aws/dist/botocore/data/comprehendmedical/2018-10-30/paginator...  
on  
parallels@parallels-Parallels-Virtual-Platform:~$ sudo ./aws/install  
[sudo] password for parallels:  
You can now run: /usr/local/bin/aws --version  
parallels@parallels-Parallels-Virtual-Platform:~$ aws --version  
$ awscli/2.0.10 Python/3.7.3 Linux/4.15.0-74-generic botocore/2.0.0dev14  
parallels@parallels-Parallels-Virtual-Platform:~$
```

AWS CLI - Hands On

- Go to aws console
- Go to IAM than to Users

The screenshot shows the AWS Identity and Access Management (IAM) service interface. The left sidebar is titled 'Identity and Access Management (IAM)' and includes sections for 'Dashboard', 'Access management' (with 'User groups', 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings', and 'Root access management'), and 'Access reports' (with 'Access Analyzer', 'Resource analysis', 'Unused access', 'Analyzer settings', 'Credential report', and 'Organization activity'). The main content area is titled 'Users (1)' and contains a table with one row. The table columns are 'User name', 'Path', 'Groups', 'Last activity', 'MFA', 'Password age', 'Console last sign-in', and 'Access key ID'. The single user listed is 'twinkle', with a checkmark in the 'Last activity' column indicating it was 2 days ago. A large orange arrow points to the 'twinkle' entry in the table, and the text 'Click Here' is overlaid on the arrow. The top navigation bar includes the AWS logo, a search bar, and various global navigation links.

User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Access key ID
twinkle	/	1	2 days ago	-	2 days	July 16, 2025, 13:06 (...)	-

Click Here

rajendra0968jangid

aws Q Search [Alt+S] Global Twinkle%20Sharma

IAM > Users > twinkle

twinkle Info

Summary

ARN: arn:aws:iam::235562991793:user/twinkle
Created: July 16, 2025, 13:04 (UTC+05:30)
Console access: Enabled without MFA
Last console sign-in: 2 days ago
Access key 1: Create access key

Permissions Groups (1) Tags (1) Security credentials Last Accessed

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

Filter by Type: All types
Policy name ▲ Type ▾ Attached via ▾
Loading policies

Access keys (0)
No access keys. As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. Learn more

Create access key

API keys for Amazon Bedrock (0)
Use API keys for Amazon Bedrock to integrate into your library of choice and make API requests programmatically. You can have a maximum of two long-term API keys (active, inactive, or expired) at a time. Learn more

Actions Generate API Key

SSH public keys for AWS CodeCommit (0)
Use SSH public keys to authenticate access to AWS CodeCommit repositories. You can have a maximum of five SSH public keys (active or inactive) at a time. Learn more

Actions Upload SSH public key

Click on security credentials

scroll Down

Click on create Access Key

Identity and Access Management (IAM)

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management New

Access reports

Access Analyzer

Resource analysis New

Unused access

Analyzer settings

Credential report

Organization activity

Search IAM

Search [Alt+S]

Global Twinkle%20Sharma

aws | Search [Alt+S] Global ▾ Twinkle%20Sharma ▾

IAM > Users > twinkle > Create access key

Set description tag
Step 3
Retrieve access keys

Use case

Command Line Interface (CLI)
You plan to use this access key to enable the AWS CLI to access your AWS account.

Local code
You plan to use this access key to enable application code in a local development environment to access your AWS account.

Application running on an AWS compute service
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

Third-party service
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

Application running outside AWS
You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.

Other
Your use case is not listed here.

Alternatives recommended

- Use [AWS CloudShell](#), a browser-based CLI, to run commands. [Learn more](#)
- Use the [AWS CLI V2](#) and enable authentication through a user in IAM Identity Center. [Learn more](#)

Select CLI

aws | Search [Alt+S] Global ▾ Twinkle%20Sharma ▾

IAM > Users > twinkle > Create access key

Application running on an AWS compute service
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

Third-party service
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

Application running outside AWS
You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.

Other
Your use case is not listed here.

Alternatives recommended

- Use [AWS CloudShell](#), a browser-based CLI, to run commands. [Learn more](#)
- Use the [AWS CLI V2](#) and enable authentication through a user in IAM Identity Center. [Learn more](#)

Confirmation

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

Check this → **Click on Next** → **Next**

- Step 1 Access key best practices & alternatives
- Step 2 - optional Set description tag
- Step 3 Retrieve access keys

Set description tag - optional Info

The description for this access key will be attached to this user as a tag and shown alongside the access key.

Description tag value

Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidently later.

Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: _ . / = + - @

[Cancel](#)[Previous](#)[Create access key](#)

Click on create access key

After creating access key copy & paste your access key in notepad - go to command prompt

```
C:\Users\twinkle>aws --version
aws-cli/2.27.54 Python/3.13.4 Windows/11 exe/AMD64
C:\Users\twinkle>aws configure  Type AWS Configure
AWS Access Key ID [*****TL50]:
```

```
C:\Users\tinas>aws --version  
aws-cli/2.27.54 Python/3.13.4 Windows/11 exe/AMD64
```

```
C:\Users\tinas>aws configure  
AWS Access Key ID [*****TL50]: AKIATNWFGACY3FLIACH6  
AWS Secret Access Key [*****hDvr]:
```



Paste your access key ID & access secret key

```
C:\Users\tina>aws --version  
aws-cli/2.27.54 Python/3.13.4 Windows/11 exe/AMD64
```

```
C:\Users\tina>aws configure  
AWS Access Key ID [*****TL50]: AKIATNWFGACY3FLIACH6  
AWS Secret Access Key [*****hDvr]:  
Default region name [Default Region Name ]none] : eu-west-1]: ap-south-2  
Default output format [None]:
```



Enter region

```
C:\Users\*****>aws --version  
aws-cli/2.27.54 Python/3.13.4 Windows/11 exe/AMD64  
  
C:\Users\*****>aws configure  
AWS Access Key ID [*****TL5O]: AKIATNWFAGACY3FLIACH6  
AWS Secret Access Key [*****hDvr]: *****  
Default region name [Default Region Name ]none] : eu-west-1: ap-south-2  
Default output format [None]:
```

```
C:\Users\tinas>aws iam list-users
```

```
"Users": [  
    {  
        "Path": "/",  
        "UserName": "twinkle",  
        "UserId": "AIDATNWFAGACYQJ6CAIWDK",  
        "Arn": "arn:aws:iam::235562991793:user/twinkle",  
        "CreateDate": "2025-07-16T07:34:39+00:00",  
        "PasswordLastUsed": "2025-07-16T07:36:39+00:00"  
    }  
]
```

Type this & click on enter

You will see all the details

AWS Cloudshell

- It's a pre-authenticated shell environment provided by AWS, accessible through the console, with built-in tools like the AWS CLI, Python, Node.js, Git, and more.
- Key Features of CloudShell

Feature	Description
<input checked="" type="checkbox"/> Pre-authenticated	No need to configure credentials — uses the IAM role of your console user
<input checked="" type="checkbox"/> Built-in CLI & SDKs	AWS CLI v2, Python, Node.js, and more pre-installed
<input checked="" type="checkbox"/> Persistent storage	1 GB of persistent home directory (<code>~/</code>) storage per region
<input checked="" type="checkbox"/> Runs in browser	No software installation needed
<input checked="" type="checkbox"/> Multi-region support	Each region has its own shell environment
<input checked="" type="checkbox"/> Free to use	No cost for usage (within limits)

AWS Cloudshell – Region

Availability

Find this list here

It is not yet available in all regions, and you can find the region list



<https://docs.aws.amazon.com/cloudshell/latest/userguide/supported-aws-regions.html>

The following are the supported AWS Regions for CloudShell, Docker, and CloudShell VPC environment:

- US East (Ohio)
- US East (N. Virginia)
- US West (N. California)
- US West (Oregon)
- Africa (Cape Town)
- Asia Pacific (Hong Kong)
- Asia Pacific (Jakarta)
- Asia Pacific (Mumbai)
- Asia Pacific (Osaka)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Canada (Central)
- Europe (Frankfurt)
- Europe (Ireland)
- Europe (London)
- Europe (Milan)
- Europe (Paris)
- Europe (Stockholm)
- Middle East (Bahrain)
- Middle East (UAE)
- South America (São Paulo)

Please switch to one of these regions if you want to do the next (optional) hands-on.

AWS Cloudshell

The screenshot shows the AWS Cloudshell interface. At the top, there is a navigation bar with the AWS logo, a search bar, and various icons. A large orange arrow points upwards from the bottom of the screen towards the navigation bar.

Console Home Info

Welcome to AWS

- Getting started with AWS** Info
Learn the fundamentals and find valuable information to get the most out of AWS.
- Training and certification** Info
Learn from AWS experts and advance your skills and knowledge.
- What's new with AWS?** Info
Discover new AWS services, features, and

AWS Health Info

- Open issues**: 0 Past 7 days
- Scheduled changes**: 0 Upcoming and past 7 days
- Other notifications**: 0 Past 7 days

Applications (0) Info

Region: US East (Ohio)

Select Region: us-east-2 (Current Region) ▼

Find applications 🔍

Name | Description | Region | Origin ★ ▲

No applications
Get started by creating an application.

Create application

Click here

Reset to default layout Reset **+ Add widgets** Add

rajendra0968jangid

CloudShell

us-east-2 +

~ \$ aws

```
usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:
```

```
aws help
aws <command> help
aws <command> <subcommand> help
```

Type this on cloud shell

~ \$ aws --version

```
aws-cli/2.27.50 Python/3.13.4 Linux/6.1.141-155.222.amzn2023.x86_64 exec-env/CloudShell exe/x86_64.amzn.2023
```

~ \$

You will see this

CloudShell

us-east-2 +

~ \$ aws --version

```
aws-cli/2.27.50 Python/3.13.4 Linux/6.1.141-155.222.amzn2023.x86_64 exec-env/CloudShell exe/x86_64.amzn.2023
```

~ \$ clear



Enter clear here & press enter

All things will remove

rajendra0968jangid

CloudShell

us-east-2



Actions ▾



```
~ $ aws iam list-users
{
  "Users": [
    {
      "Path": "/",
      "UserName": "twinkle",
      "UserId": "AIDATNNWFGACYQJ6CAIWDK",
      "Arn": "arn:aws:iam::235562991793:user/twinkle",
      "CreateDate": "2025-07-16T07:34:39+00:00",
      "PasswordLastUsed": "2025-07-16T07:36:39+00:00"
    }
  ]
}
```

By typing this you will get the user details as in commandprompt

```
~ $ echo "text" >demo.txt
~ $ cat demo.txt
text
~ $ pwd
/home/cloudshell-user
~ $
```

By this tags it is going to create text file

CloudShell

us-east-2

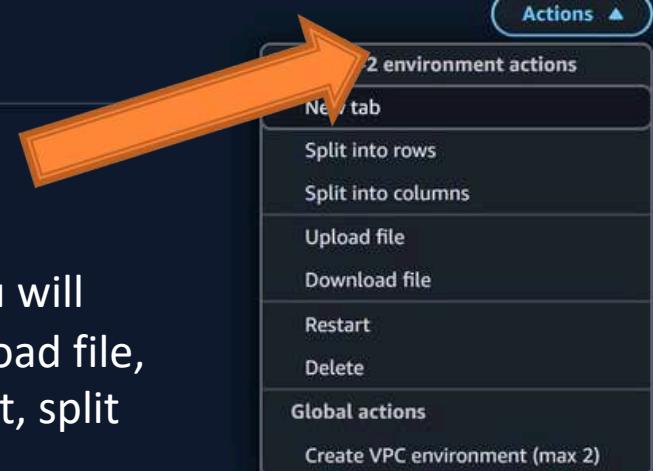


```
~ $ aws iam list-users --regions
usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:
  aws help
  aws <command> help
  aws <command> <subcommand> help

Unknown options: --regions

~ $ echo "text" >demo.txt
~ $ cat demo.txt
text
~ $ pwd
/home/cloudshell-user
~ $
```

By clicking on actions you will get the options to download file, upload file, delete, restart, split column



CloudShell

us-east-2 +

~ \$ aws iam list-users --reg

usage: aws [options] <command>
To see help text, you can run:

aws help
aws <command> help
aws <command> <subcommand>

Unknown options: --regions

~ \$ echo "text" >demo.txt

~ \$ cat demo.txt

text

~ \$ pwd
/home/cloudshell-user

~ \$

Display options

Font size

- Smallest
- Small
- Medium
- Large
- Largest

Example font size

AWS CloudShell theme

- Light
- Dark

Terminal preferences

Enable Safe Paste

Verify multiline text that you've copied before pasting.

Amazon Q inline suggestions

Displays command suggestions as you type, when using Z shell.

Requires specific IAM permissions. [Learn more](#)

To disable, run the following command:

q inline disable



By clicking on setting

You will get the options for make changes in UI of cloud shell

Cancel

Confirm

rajendra0968jangid

IAM Roles For AWS Services

- IAM Roles in AWS are temporary permission sets that allow AWS services, applications, or users to access resources securely without using long-term credentials (like access keys).

They are essential when:

- An EC2 instance needs to access S3 or DynamoDB
- A Lambda function needs to read from a database
- An ECS task or Glue job needs access to other AWS resources

How AWS Services Use IAM Roles

Here's how some common AWS services use IAM roles:

AWS Service	Role Used For	Example Action
EC2	EC2 instance profile (instance role)	Read/write S3, access secrets
Lambda	Execution role	Access DynamoDB or SNS
ECS Tasks	Task execution role	Pull container images, logs
Glue	Job role	Read from S3, write to Redshift
CodeBuild	Build role	Access S3, CodeCommit, ECR
SageMaker	Execution role	Access training data in S3
Step Functions	State machine role	Invoke Lambda, access DynamoDB
CloudFormation	Service role	Create/delete AWS resources

IAM Roles Hands On

The screenshot shows the AWS IAM Dashboard. On the left, there is a navigation sidebar with the following menu items:

- Identity and Access Management (IAM) (selected)
- Dashboard
- Access management
 - User groups
 - Users
 - Roles (highlighted with an orange arrow)
 - Policies
 - Identity providers
 - Account settings
 - Root access management [New](#)
- Access reports

The main content area displays the following information:

IAM Dashboard [Info](#)

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
1	1	2	2	0

What's new

Updates for features in IAM

- AWS IAM announces support for encrypted SAML assertions. *5 months ago*
- AWS CodeBuild announces support for project ARN and build ARN IAM condition keys. *6 months ago*
- IAM Roles Anywhere credential helper now supports TPM 2.0. *7 months ago*

[View all](#)

AWS Account

Account ID
235562991793

Account Alias
aws-twinkle-v4 [Edit](#) | [Delete](#)

Sign-in URL for IAM users in this account
<https://aws-twinkle-v4.signin.aws.amazon.com/console>

Quick Links

[My security credentials](#)

rajendra0968jangid

aws Search [Alt+S] Global Twinkle%20Sharma

IAM > Roles

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings
- Root access management New

Access reports

Roles (2) 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
AWSServiceRoleForSupport	AWS Service: support (Service-Linker)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service)	-

Click on create role

Roles Anywhere Info

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads

X.509 Standard

Temporary credentials

Manage

aws Search [Alt+S] Global Twinkle%20Sharma

IAM > Roles > Create role

Add permissions Step 3 Name, review, and create

For now select AWS service Because we are creating role for aws service

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.

Service or use case

rajendra0968jangid

Use case

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

Service or use case

EC2

Choose a use case for the specified service.

Use case EC2

Allows EC2 instances to call AWS services on your behalf.

 EC2 Role for AWS Systems Manager

Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

 EC2 Spot Fleet Role

Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.

 EC2 - Spot Fleet Auto Scaling

Allows Auto Scaling to access and update EC2 spot fleets on your behalf.

 EC2 - Spot Fleet Tagging

Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.

 EC2 - Spot Instances

Select use case for EC2

aws | Search [Alt+S] Global Twinkle%20Sharma

☰ IAM > Roles > Create role

Use case

EC2
Allows EC2 instances to call AWS services on your behalf.

EC2 Role for AWS Systems Manager
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

EC2 Spot Fleet Role
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.

EC2 - Spot Fleet Auto Scaling
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.

EC2 - Spot Fleet Tagging
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.

EC2 - Spot Instances
Allows EC2 Spot Instances to launch and manage spot instances on your behalf.

EC2 - Spot Fleet
Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.

EC2 - Scheduled Instances
Allows EC2 Scheduled Instances to manage instances on your behalf.

Click on Next

Cancel Next

- Add permissions
- Step 3
- Name, review, and create

For now I am giving IAMReadonly permission

Permissions policies (1/1067) Info

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

Filter by Type

Search: IAM



All types

15 matches



1



Policy name	Type	Description
<input type="checkbox"/> AWSIAMIdentityCenterAll...	AWS managed	Provides the list of actions that are all...
<input type="checkbox"/> AWSQuickSightListIAM	AWS managed	Allow QuickSight to list IAM entities
<input type="checkbox"/> IAMAccessAdvisorReadOnly	AWS managed	This policy grants access to read all acc...
<input type="checkbox"/> IAMAccessAnalyzerFullAc...	AWS managed	Provides full access to IAM Access Anal...
<input type="checkbox"/> IAMAccessAnalyzerRead...	AWS managed	Provides read only access to IAM Acces...
<input type="checkbox"/> IAmAuditRootUserCreden...	AWS managed	Provides access required to check the ...
<input type="checkbox"/> IAMCreateRootUserPass...	AWS managed	Provides access required to create a ro...
<input type="checkbox"/> IAMDeleteRootUserCred...	AWS managed	Provides access required to delete all r...

aws | Search [Alt+S] Global Twinkle%20Sharma

☰ IAM > Roles > Create role

<input type="checkbox"/>	IAMDeleteRootUserCred...	AWS managed	Provides access required to delete all r...
<input type="checkbox"/>	IAMFullAccess	AWS managed	Provides full access to IAM via the AW...
<input checked="" type="checkbox"/>	IAMReadOnlyAccess	AWS managed	Provides read only access to IAM via th...
<input type="checkbox"/>	IAMSelfManageServiceSp...	AWS managed	Allows an IAM user to manage their o...
<input type="checkbox"/>	IAMUserChangePassword	AWS managed	Provides the ability for an IAM user to ...
<input type="checkbox"/>	IAMUserSSHKeys	AWS managed	Provides the ability for an IAM user to ...
<input type="checkbox"/>	myiampolicy	Customer managed	-
<input type="checkbox"/>	newiam	Customer managed	-

Click on Next

▶ Set permissions boundary - optional

Cancel Previous Next

aws Search [Alt+S] Global Twinkle%20Sharma

IAM > Roles > Create role

Add permissions Step 3 Name, review, and create

Type Role Name

Role details

Role name
Enter a meaningful name to identify this role.
DemoroleEC2
Maximum 64 characters. Use alphanumeric and '+,-,_' characters.

Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=,. @-/[\[\]]!#\$%^*();,"`

Step 1: Select trusted entities Edit

Trust policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Action": "sts:AssumeRole",  
6       "Effect": "Allow",  
7       "Principal": "ec2.amazonaws.com"  
8     }  
9   ]  
10 }
```

aws Search [Alt+S] Global Twinkle%20Sharma

IAM > Roles > Create role

Permissions policy summary

Policy name	Type	Attached as
IAMReadOnlyAccess	AWS managed	Permissions policy

Step 3: Add tags

Add tags - optional Info
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 new tag
You can add up to 50 more tags.

Click on create role 

Cancel Previous Create role

IAM > Roles

Identity and Access Management (IAM)

Role DemoroleEC2 created.

View role X

Roles (3) 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

Trusted entities Last activity

Role name	Trusted entities	Last activity
AWSServiceRoleForSupport	AWS Service: support (Service-Linked)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked)	-
DemoroleEC2	AWS Service: ec2	-

Role is created now

Roles Anywhere Info

Manage

Authenticate your non AWS workloads and securely provide access to AWS services.

IAM > Roles > DemoroleEC2

Identity and Access Management (IAM)

Search IAM

Last activity Maximum session duration

1 hour

Permissions Trust relationships Tags Last Accessed Revoke sessions

Permissions policies (1) Info

You can attach up to 10 managed policies.

Simulate Remove Add permissions

Filter by Type

All types Attached entities

Policy name Type Attached entities

Policy name	Type	Attached entities
IAMReadOnlyAccess	AWS managed	1

On clicking role you will see the permissions

Permissions boundary (not set)

IAM Security Tools in AWS

Tool	Purpose
IAM Access Analyzer	Detects unused or publicly shared resources
IAM Policy Simulator	Test and simulate IAM policy behavior before applying
Credential Reports	View the age/status of passwords, access keys, and MFA for users
Access Advisor	Shows services used by users/roles to help reduce over-permissioning
AWS Organizations SCPs	Apply service control policies to limit actions across accounts
AWS Config Rules	Detect non-compliance with IAM rules (e.g., missing MFA)
CloudTrail	Logs all IAM and user activity for auditing
GuardDuty	Threat detection (e.g., unusual credential use)
AWS Security Hub	Centralized security findings from IAM and other tools

IAM Security Tools Hands On

The screenshot shows the AWS IAM Roles page for the role 'DemoroleEC2'. The 'Permissions' tab is selected. In the 'Permissions policies' section, there is one policy named 'IAMReadOnlyAccess' attached. A red arrow points to the 'Credential report' link in the left sidebar.

Click on credential Report

Policies
Identity providers
Account settings
Root access management [New](#)
▼ Access reports
Access Analyzer
Resource analysis [New](#)
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies [New](#)
IAM Identity Center
AWS Organizations

Last activity: -
Maximum session duration: 1 hour

Permissions [Trust relationships](#) [Tags](#) [Last Accessed](#) [Revoke sessions](#)

Permissions policies (1) [Info](#)
You can attach up to 10 managed policies.
Filter by Type
Search: All types: [▼](#)
Policy name: IAMReadOnlyAccess [Type](#) [Attached entities](#): 1

▶ Permissions boundary (not set)

rajendra0968jangid

Identity and Access Management (IAM)[Search IAM](#)[Dashboard](#)**Access management**[User groups](#)[Users](#)[Roles](#)[Policies](#)[Identity providers](#)[Account settings](#)[Root access management](#) New**Access reports****Credentials report of IAM users in this account** Info

The credentials report lists all your IAM users in this account and the status of their various credentials. After a report is created, it is stored for up to four hours.

Credentials report[Download credentials report](#)

No report created in the past 4 hours. A new report will be created.

Click on download credentials report

status_reports_Fri Jul 18 2025 14_31_57 GMT+0530 (India Standard Time).csv - Microsoft Excel

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	user	arn:aws:iam::2025-07-0:root	user_creation_date	password_last_changed	password_expires	mfa_active	access_key_1_active	access_key_1_last_used_time	access_key_1_last_used_region	access_key_1_last_used_service	access_key_2_active	access_key_2_last_used_time	access_key_2_last_used_region	access_key_2_last_used_service	certified_user	last_password_change_time	last_password_change_time	last_password_change_time	
2	<root_account>	arn:aws:iam::2025-07-0:root	TRUE	2025-07-1	2025-07-0	not_supported	TRUE	FALSE	N/A	N/A	N/A	N/A	N/A	FALSE	N/A	N/A	N/A	FALSE	N/A
3	twinkle	arn:aws:iam::2025-07-1:twinkle	TRUE	2025-07-1	2025-07-1	N/A	FALSE	TRUE	2025-07-1	2025-07-1	us-east-1	iam	N/A	FALSE	N/A	N/A	N/A	FALSE	N/A
4																			
5																			
6																			
7																			
8																			
9																			
10																			
11																			
12																			
13																			
14																			
15																			
16																			
17																			
18																			
19																			
20																			
21																			
22																			
23																			
24																			

In this Sheet
you will get all
the details of
users



Identity and Access Management (IAM)

 Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management [New](#)

▼ Access reports

Credentials report of IAM users in this account [Info](#)

The credentials report lists all your IAM users in this account and the status of their various credentials. After a report is created, it is stored for up to four hours.

Credentials report

[Download credentials report](#)

Report last created: Now.

After that go to users

rajendra0968jangid

aws [Alt+S] Global Twinkle%20Sharma

IAM > Users

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management [New](#)

Access reports

Users (1) [Info](#)

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

User name	Path	Group	Last activity	MFA	Password age
twinkle	/	1	1 hour ago	-	2 days

Click on user

aws Search [Alt+S] Global Twinkle%20Sharma

IAM > Users > twinkle

twinkle Info

Summary

ARN arn:aws:iam::235562991793:user/twinkle	Console access Enabled without MFA	Access key 1 AKIATNWFGACY3FLIACH6 - Active Used today. Created today.
Created July 16, 2025, 13:04 (UTC+05:30)	Last console sign-in 2 days ago	Access key 2 Create access key

Permissions Groups Tags Security credentials Last Accessed

Last accessed information shows the services that this user can access and when those services were last accessed. Review this data to remove unused permissions. [Learn More](#)

Allowed services (426)
IAM reports activity for services and management actions. [Learn more](#) about action last accessed information. To see actions, choose the appropriate service name from the list.

Click on last accessed

Here you will see the last accessed service by user & also the permissions granted

IAM > Users > twinkle

Identity and Access Management (IAM)

Dashboard

Access management

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings
- Root access management [New](#)

Access reports

Allowed services (426)
IAM reports activity for services and management actions. [Learn more](#) about action last accessed information. To see actions, choose the appropriate service name from the list.

Filter by services access history			
Service	Policies granting permissions	Last accessed	
User Notifications	AdministratorAccess	2 days ago	
Free Tier	AdministratorAccess	2 days ago	
AWS IAM Identity Center	AdministratorAccess	2 days ago	
Amazon EC2	AdministratorAccess	2 days ago	
AWS Signin	AdministratorAccess	2 days ago	
AWS Service Catalog	AdministratorAccess	2 days ago	

IAM Guidelines & Best Practices

- Don't use the root account except for AWS account setup
- One physical user = One AWS user
- Assign users to groups and assign permissions to groups
Create a strong password policy
- Use and enforce the use of Multi Factor Authentication (MFA)
- Create and use Roles for giving permissions to AWS services
- Use Access Keys for Programmatic Access (CLI/ SDK)
Audit permissions of your account using IAM credentials
- Report & IAM Access Advisor
- Never share IAM users & Access Keys
-