

Credential Report

Management

ps

providers

settings

ess management [New](#)

reports

Analyzer

mal access

sed access

lyzer settings

ntial report

ization activity

ontrol policies

orce control policies [New](#)

idShell

Feedback

3°C

partly cloudy

Credentials report of IAM users in this account Info

The credentials report lists all your IAM users in this account and the sta

Credentials report

[Download credentials report](#)

Report last created: Now.

Restricted Mode is intended for safe code browsing. Trust this window to enable all features. [Manage](#)

status_reports_Fri Mar 29 2025 00_29_35 GMT+0530 (India Standard Time)

C:\Users> javanya > Downloads > status_reports_Fri Mar 29 2025 00_29_35 GMT+0530 (India Standard Time)

```
1 user,arn,user_creation_time,password_enabled,password_last_
2 <root_account>,arn:aws:iam::522814729380:root,2024-10-27T00:00:00.000Z,
3 jc,arn:aws:iam::522814729380:user/jc,2025-03-27T18:56:28Z,tru
```

I

Drivers want to install the recommended Windows OS



Search



United States

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

Asia Pacific

🔒 Hong Kong	ap-east-1
🔒 Hyderabad	ap-south-2
🔒 Mumbai	ap-south-1
🔒 Osaka	ap-northeast-3
🔒 Seoul	ap-northeast-2
🔒 Singapore	ap-southeast-1
🔒 Sydney	ap-southeast-2
🔒 Tokyo	ap-northeast-1

Canada

🔒 Central	ca-central-1
-----------	--------------

Europe

🔒 Frankfurt	eu-central-1
🔒 Ireland	eu-west-1



Edit

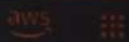
email address

[Manage Regions](#) | [Manage Local Zones](#)

regional STS endpoints, no
If you intend to enable a new

s that can contro

s from regional ST
zonaws.com) are v



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

Access Analyzer

External access

Unused access

Analyzer settings

Roles (1/4) 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

Search



Role name



Trusted entities



[AWSServiceRoleForElasticLoadBalancing](#)

AWS Service: elasticloadbalancing (S



[AWSServiceRoleForSupport](#)

AWS Service: support (Service-Linker



[AWSServiceRoleForTrustedAdvisor](#)

AWS Service: trustedadvisor (Service



[demoroleofec2](#)

AWS Service: ec2

Roles Anywhere Info

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



Access AWS from your non AWS workloads

Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.



X.509 Standard

Use your own existing PKI infrastructure or use AWS [Certificate Manager Private Certificate Authority](#) to authenticate identities.



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

Access Analyzer

External access

Unused access

Analyzer settings

Summary

Creation date

March 27, 2025, 19:43 (UTC+05:30)

Last activity

-

ARN

arn:aws:iam::522814729380:role/demoroleofec2

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.

Search

Filter by Type

All types

☐

Policy name

☐

Type

☐

[IAMReadOnlyAccess](#)

AWS managed

Permissions boundary (not set)

IAM > Security credentials

Multi-factor authentication (MFA) (1)

- Remove
- Resync
- Assign MFA device

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	Certificate
<input type="radio"/> Virtual	arn:aws:iam::522814729380:mfa/Myandroid	Not App

Access keys (1)

- Actions
- Create access key

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](#)

Created on	Access key last used	Region last used	Service last used
147 days ago	Yesterday	eu-north-1	ec2

CloudFront key pairs (0)

- Actions
- Upload
- Create CloudFront key pair

IAM > Users > Create user

group. we recommend using groups to manage user permissions by job function.

managed policies, and inline 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.

Permissions policies (1/1337)



Create

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

Filter by Type

All types

< 1 2 3 4 5 6 7 ...

<input type="checkbox"/>	Policy name	Type	Attach
<input checked="" type="checkbox"/>	AccessAnalyzerSer...	AWS managed	0
<input type="checkbox"/>	AdministratorAccess	AWS managed - job f...	1
<input type="checkbox"/>	AdministratorAcce...	AWS managed	0
<input type="checkbox"/>	AdministratorAcce	AWS managed	0

[Feedback](#)[Privacy](#)[Terms](#)

Search

✓ User "Lavanya" deleted.

User details

User name

jc


Console password type

Custom password

Require password reset

Yes

Permissions summary

Name 



Type



Used as

[AccessAnalyzerServiceRolePolicy](#)

AWS managed

Permissions policy

[IAMUserChangePassword](#)

AWS managed

Permissions policy

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.



Identity and Access Management (IAM)

Search IAM

Groups

Providers
Settings
Access management [New](#)

Reports

Analyzer
Access
Access

Users (1) [Info](#)

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

<input type="checkbox"/>	User name	Path	Group	Last activity
<input type="checkbox"/>	jc	/	1	-

Identity and Access Management (IAM)

Search IAM

Groups

Providers
Settings
Access management [New](#)

Reports

Analyzer
Access
Access

Users (1) [Info](#)

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

<input type="checkbox"/>	User name	Path	Group	Last activity
<input type="checkbox"/>	jc	/	1	-

✔ 1 user added to this group.

User groups (1) [Info](#)

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

🔍 Search

<input type="checkbox"/>	Group name	▲ Users	▼
<input type="checkbox"/>	admin		1