

Introducing the new Users list experience

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

✓ User vinay.0212 deleted.

[IAM](#) > Users

Users (0) [Info](#)

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



Delete

Add users

🔍 Find users by username or access key

< 1 >



User name ▼

Groups ▼

Last activity ▼

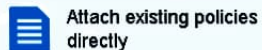
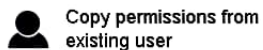
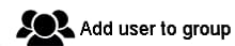
MFA ▼

Password ... ▼

Active key age ▼

No resources to display

▼ Set permissions

[Create policy](#)[Filter policies](#) ▼

Q s3fu

Showing 1 result

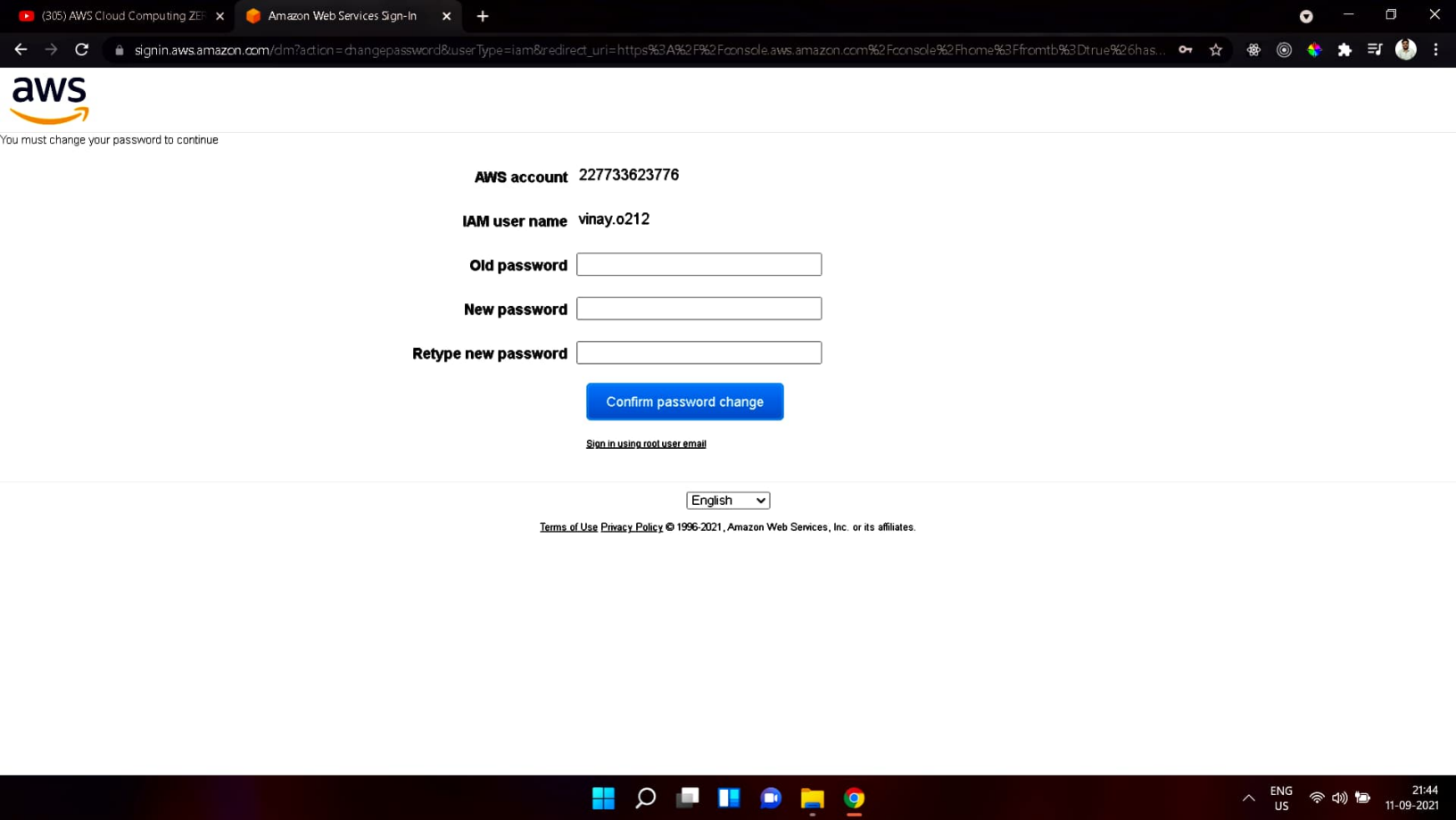
| | Policy name ▼ | Type | Used as |
|-------------------------------------|--------------------|-------------|---------|
| <input checked="" type="checkbox"/> | AmazonS3FullAccess | AWS managed | None |

▼ Set permissions boundary

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

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

[Cancel](#)[Previous](#)[Next: Tags](#)



You must change your password to continue

AWS account 227733623776

IAM user name vinay.o212

Old password

New password

Retype new password

Confirm password change

[Sign in using root user email](#)

English

[Terms of Use](#) [Privacy Policy](#) © 1996-2021, Amazon Web Services, Inc. or its affiliates.



Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://227733623776.signin.aws.amazon.com/console>

Download .csv

| | User | Access key ID | Secret access key | Email login instructions |
|---|--------------|----------------------|----------------------------|----------------------------|
| ▶ | ✓ vinay.o212 | AKIATKBP3KPQGBGQFW65 | ***** Show | Send email |

Close

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

Service control policies
(SCPs)

Search IAM

Path

/

Creation time

2021-09-11 21:39 UTC+0530

Permissions

Groups

Tags

Security credentials

Access Advisor

▼ Permissions policies (2 policies applied)

Add permissions

+ Add inline policy

Policy name ▼


Policy type ▼

Attached directly

| | | |
|---|--------------------|---|
| ▶  AmazonS3FullAccess | AWS managed policy | ✕ |
| ▶  IAMUserChangePassword | AWS managed policy | ✕ |

▶ Permissions boundary (not set)

▼ Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. [Learn more](#) 

Share your [feedback](#) and help us improve the policy generation experience.

Generate policy

No requests to generate a policy in the past 7 days.

Set user details

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

User name*

[+](#) Add another user

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type* ☒

Programmatic access

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



AWS Management Console access

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

Console password*



Autogenerated password



Custom password



Show password

Require password reset ☒

User must create a new password at next sign-in

Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

* Required

[Cancel](#)

[Next: Permissions](#)

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

Service control policies
(SCPs)

Search IAM

Path /

Creation time 2021-09-11 21:39 UTC+0530

Permissions

Groups

Tags

Security credentials

Access Advisor

▼ Permissions policies (2 policies applied)

Add permissions


| Policy name ▼ | Policy type | |
|---------------|-------------|--|
|---------------|-------------|--|

Attached directly

| | | |
|---|--------------------|---|
| ▶  AmazonS3FullAccess | AWS managed policy | ✕ |
| ▶  IAMUserChangePassword | AWS managed policy | ✕ |

▶ Permissions boundary (not set)

▼ Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. [Learn more](#) 

Share your [feedback](#) and help us improve the policy generation experience.

Generate policy

No requests to generate a policy in the past 7 days.

My Account 227733623776

My Organization

My Service Quotas

My Billing Dashboard

My Security Credentials

Sign Out

Add inline policy

Add user

1

2

3

4

5

Set user details

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

User name*

[+](#) Add another user

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type* ☐

Programmatic access

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

☐

AWS Management Console access

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

* Required

Cancel

Next: Permissions

Create bucket [Info](#)

Buckets are containers for data stored in S3. [Learn more](#) 

General configuration

Bucket name

Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#) 

AWS Region

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Choose bucket

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

Service control policies (SCPs)

IAM dashboard

Security recommendations



✖ You do not have the permission required to perform this operation. Ask your administrator to add permissions.
User: arn:aws:iam::227733623776:user/vinay.o212 is not authorized to perform: iam:GetAccountSummary on resource: *

✖ You do not have the permission required to perform this operation. Ask your administrator to add permissions.
User: arn:aws:iam::227733623776:user/vinay.o212 is not authorized to perform: iam:ListMFADevices on resource: user vinay.o212

✖ You do not have the permission required to perform this operation. Ask your administrator to add permissions.
User: arn:aws:iam::227733623776:user/vinay.o212 is not authorized to perform: iam:ListAccessKeys on resource: user nullvinay.o212

IAM resources



✖ You do not have the permission required to perform this operation. Ask your administrator to add permissions.

AWS Account

✖ You do not have the permission required to perform this operation. Ask your administrator to add permissions.

User:
arn:aws:iam::227733623776:user /vinay.o212 is not authorized to perform:
iam:ListAccountAliases on resource: *

Quick Links

[My security credentials](#)

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

Tools

Resources



You are using the following Amazon EC2 resources in the US East (Ohio) Region:

| | | | |
|-------------------------------------|-------------|---------------------------------|-------------|
| Instances (running) | ⊗ API Error | Dedicated Hosts | ⊗ API Error |
| Elastic IPs | ⊗ API Error | Instances | ⊗ API Error |
| Key pairs | ⊗ API Error | Load balancers | ⊗ API Error |
| Placement groups | ⊗ API Error | Security groups | ⊗ API Error |
| Snapshots | ⊗ API Error | Volumes | ⊗ API Error |

Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. [Learn more](#)

Account attributes



[Supported platforms](#)

[Default VPC](#)

Settings

[EBS encryption](#)

[Zones](#)

[EC2 Serial Console](#)

[Default credit specification](#)

[Console experiments](#)

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

[Launch instance](#) ▼

Note: Your instances will launch in the US East (Ohio)

Service health



Region

US East (Ohio)

Status

✓ This service is operating normally

Explore AWS



Save up to 90% on EC2 with Spot Instances

Optimize price-performance by combining EC2 purchase options in a single EC2 ASG. [Learn more](#)

Get Up to 40% Better Price Performance

T4g instances deliver the best price performance for burstable

Review

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

User details

| | |
|-------------------------------|---|
| User name | vinay.o212 |
| AWS access type | Programmatic access and AWS Management Console access |
| Console password type | Custom |
| Require password reset | Yes |
| Permissions boundary | Permissions boundary is not set |

Permissions summary

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

| Type | Name |
|----------------|---------------------------------------|
| Managed policy | AmazonS3FullAccess |
| Managed policy | IAMUserChangePassword |

Tags

No tags were added.

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