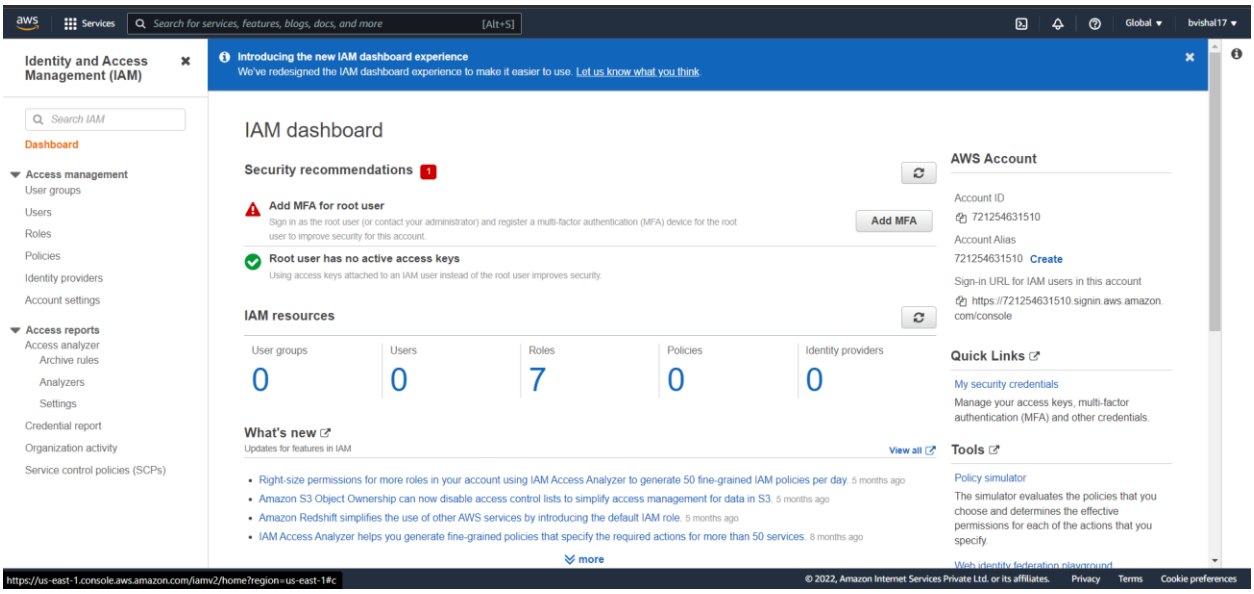
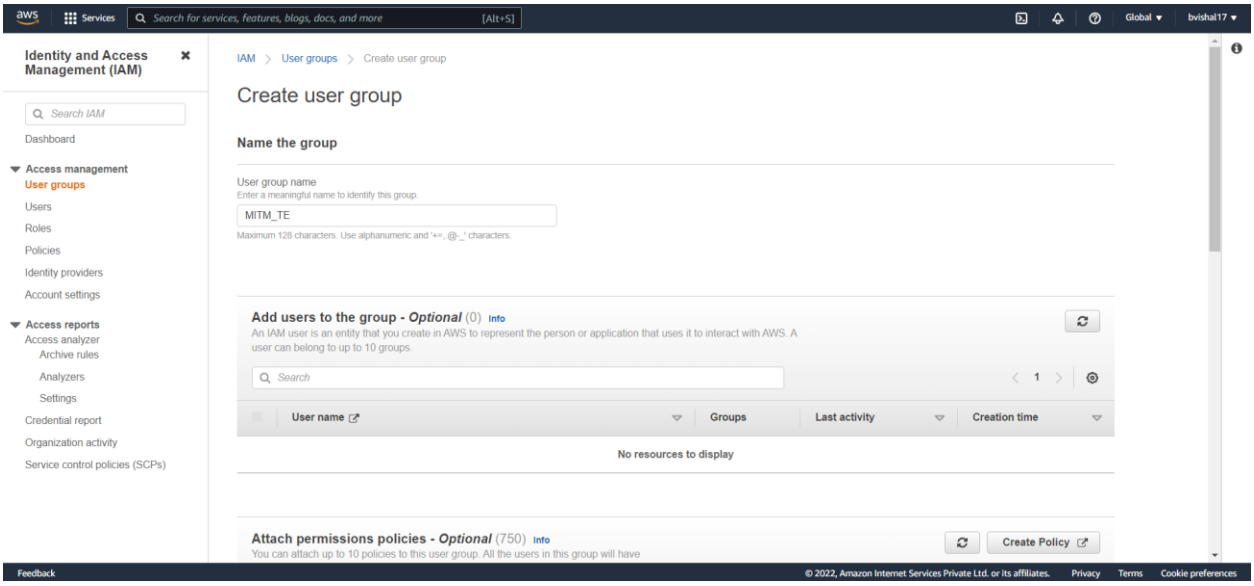
EXPERIMENT NO 8

AIM: To study and Implement Security as a Service on AWS/Azure

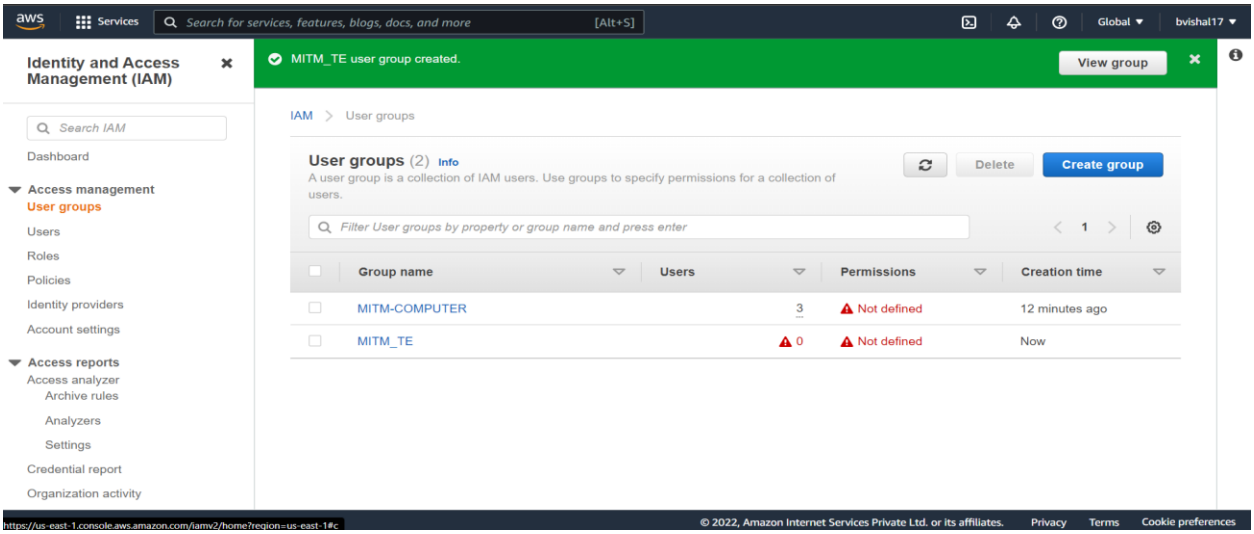
STEP 1: Open the AWS home page, Search the IAM, Open the IAM dashboard,



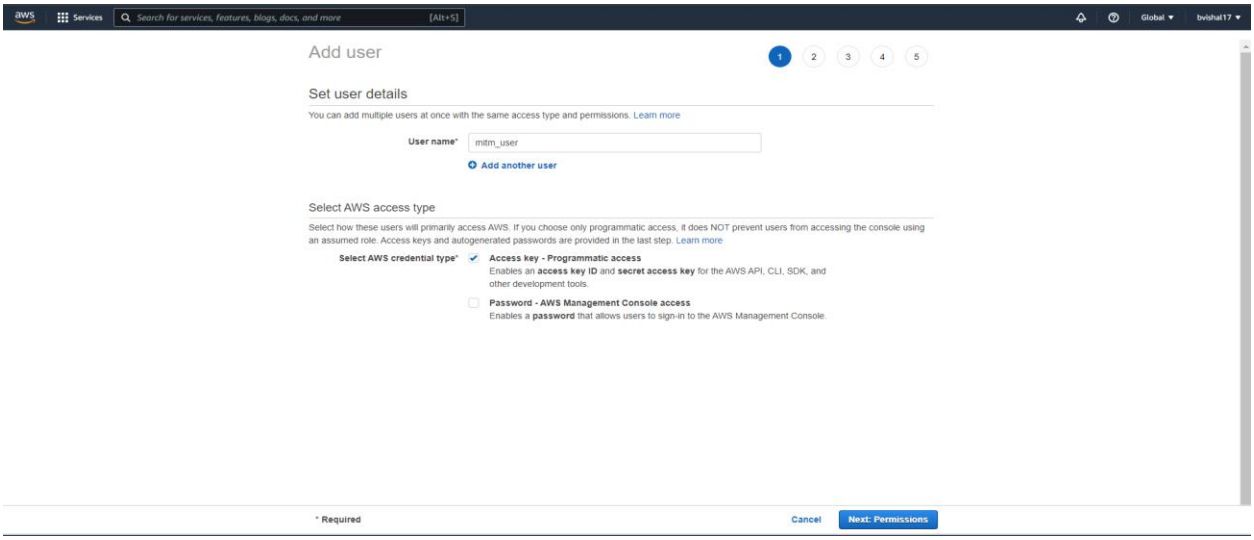
STEP 2: Create one user group: **MITM_TE**

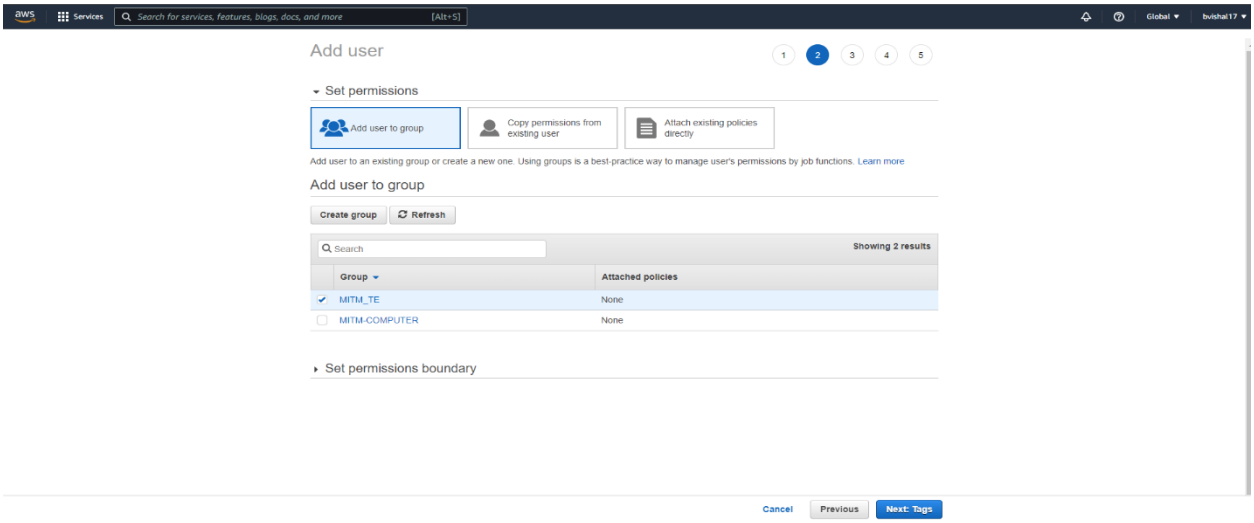


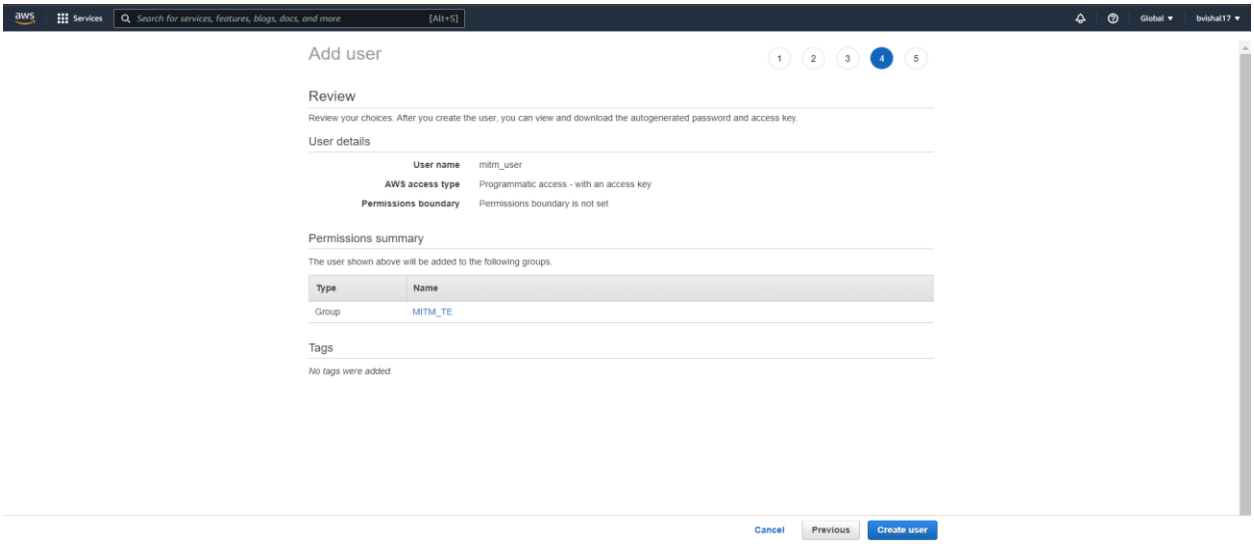
STEP 3: MITM TE group created. NO user is present in this group.

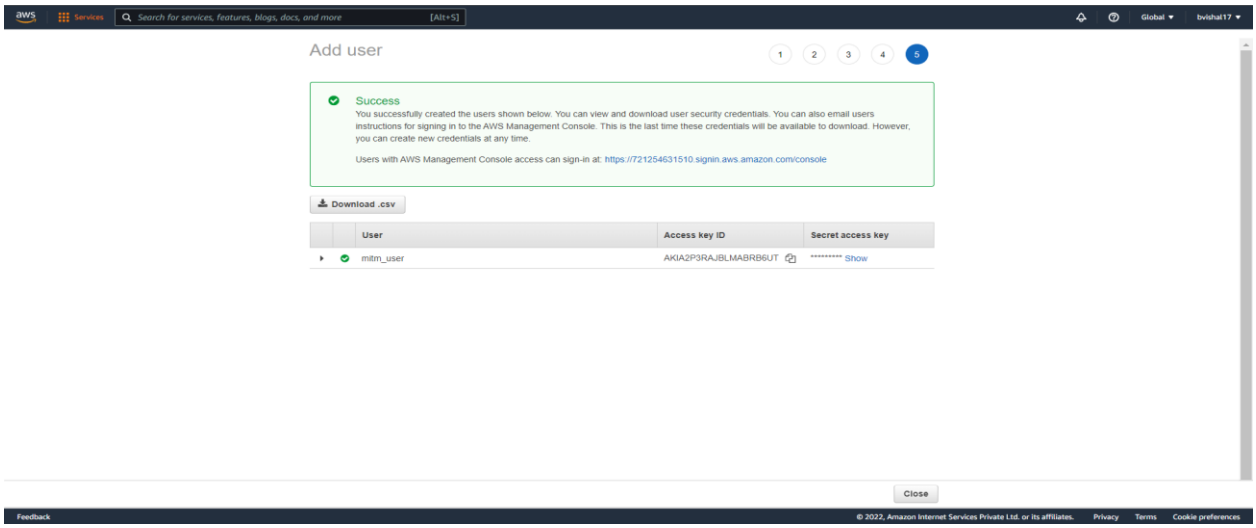


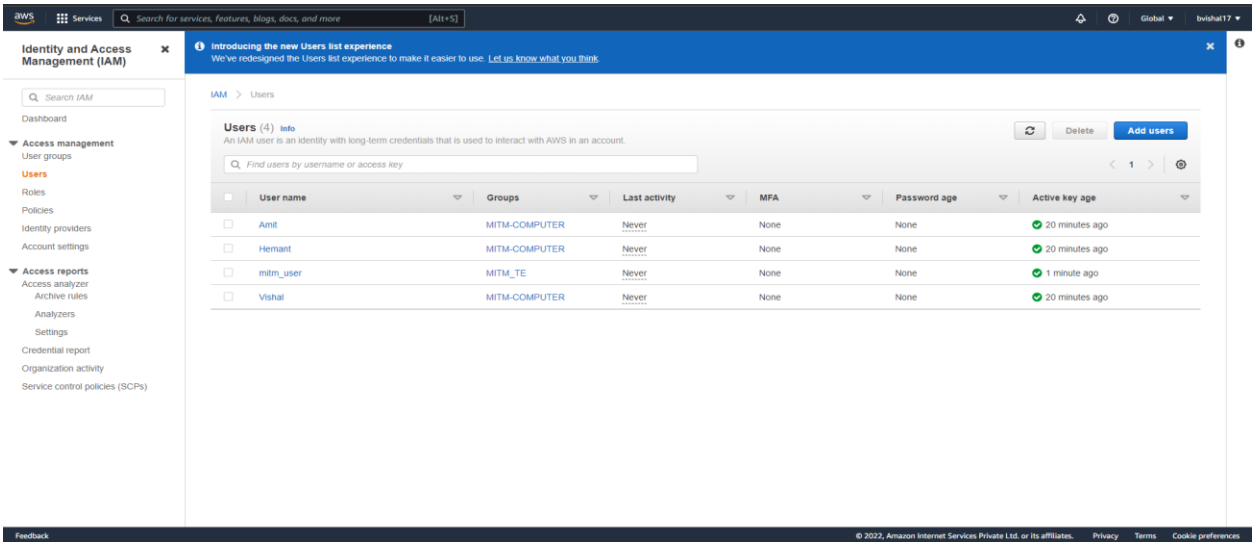
Step 4:Add USER in MITM_TE group



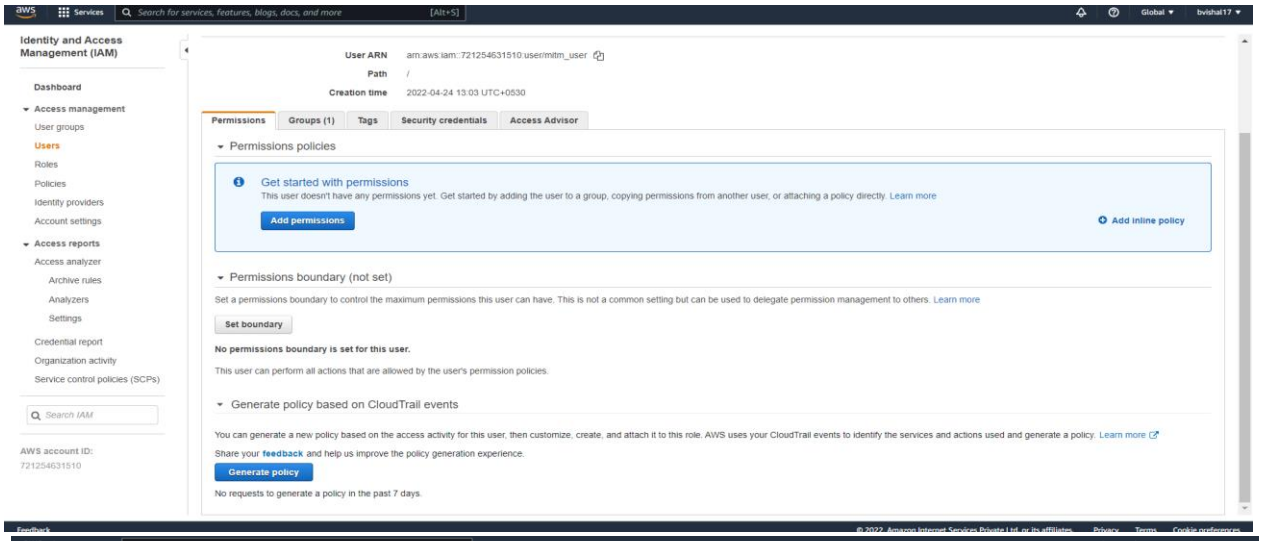


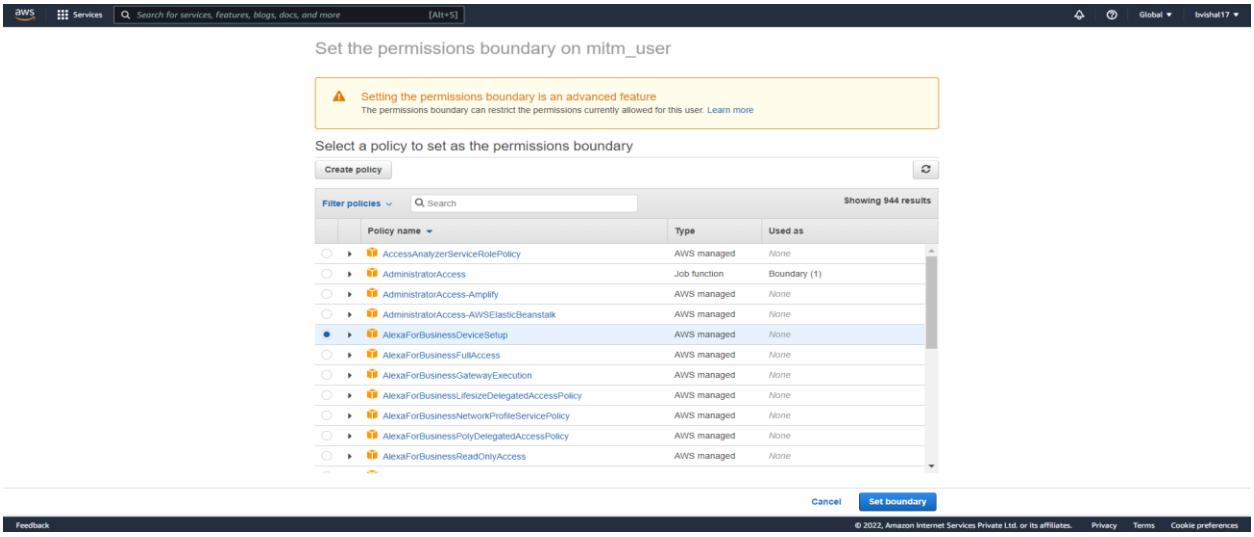

Add user
1 2 3 4 5
Review
Review your choices. After you create the user, you can view and download the autogenerated password and access key.
User details
User name mitm_user
AWS access type Programmatic access - with an access key
Permissions boundary Permissions boundary is not set
Permissions summary
The user shown above will be added to the following groups.
Type Name
Group MITM_TE
Tags
No tags were added.
Cancel
Previous
Create user

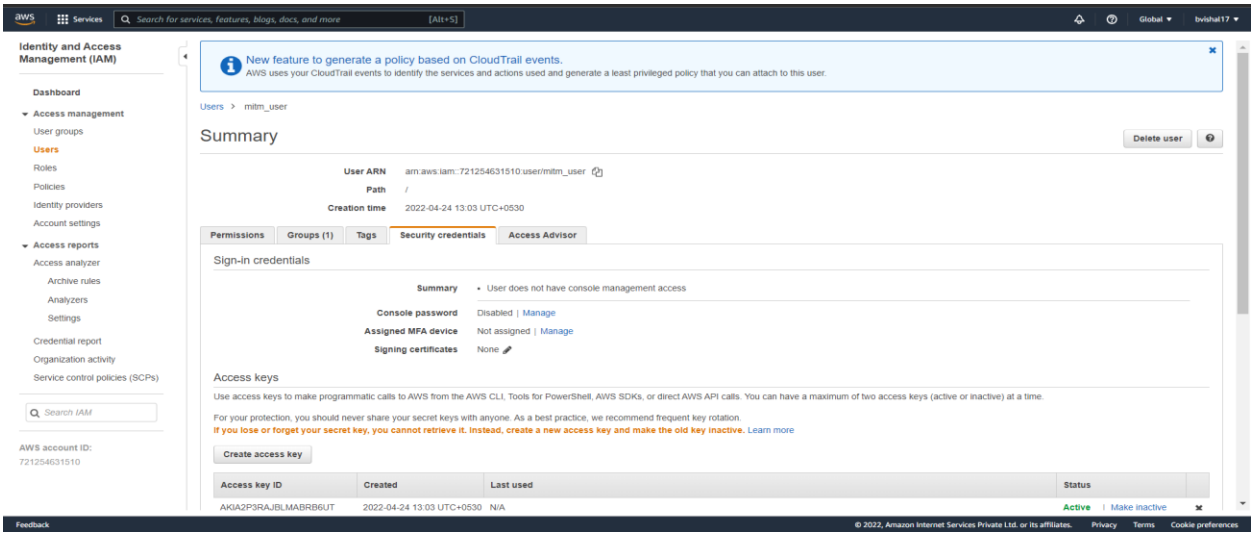

Add user
1 2 3 4 5
Success
You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.
Users with AWS Management Console access can sign-in at: https://721254631510.signin.aws.amazon.com/console
Download .csv
User
Access key ID
Secret access key
mitm_user
AKIA2P3RAJBLMABRB6UT
Show
Close
Feedback
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences


Identity and Access Management (IAM)
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.
IAM > Users
Users (4) 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
User name
Groups
Last activity
MFA
Password age
Active key age
Amit MITM-COMPUTER Never None None 20 minutes ago
Hemant MITM-COMPUTER Never None None 20 minutes ago
mitm_user MITM_TE Never None None 1 minute ago
Vishal MITM-COMPUTER Never None None 20 minutes ago
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)
Feedback
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

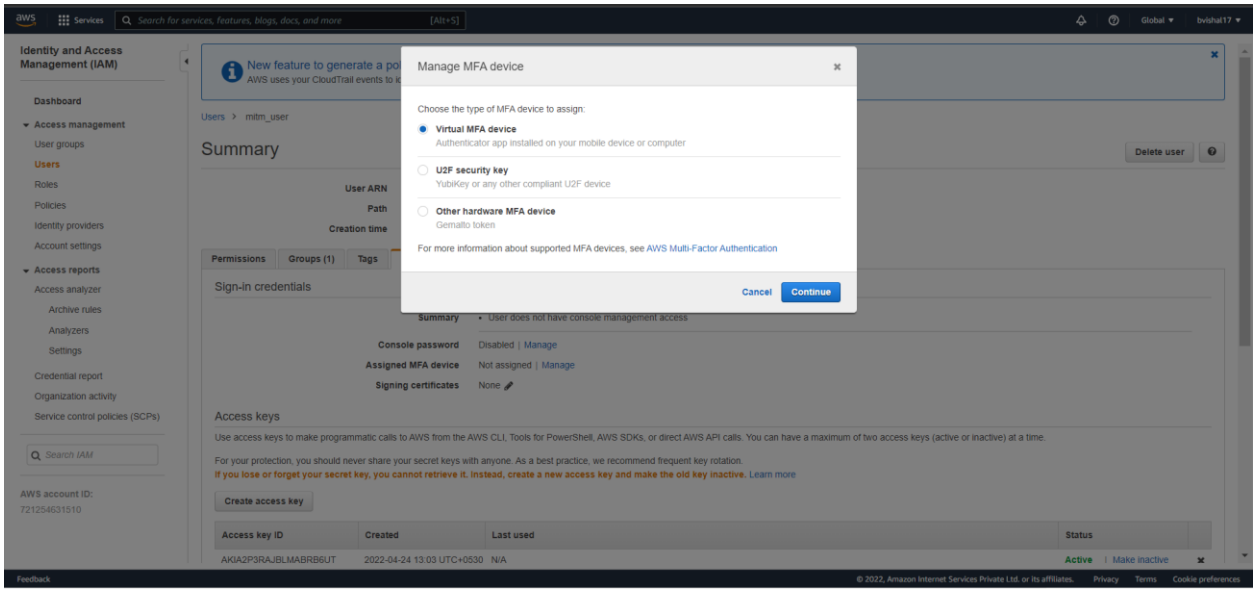
STEP 5: Set the permission boundry to the USER , select any policy for USER



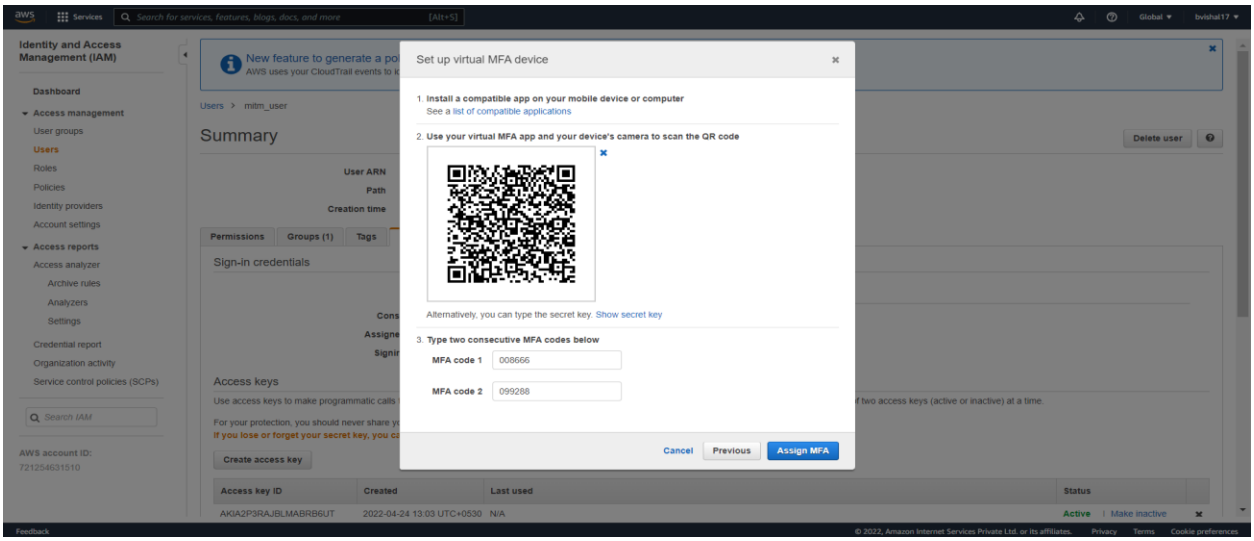


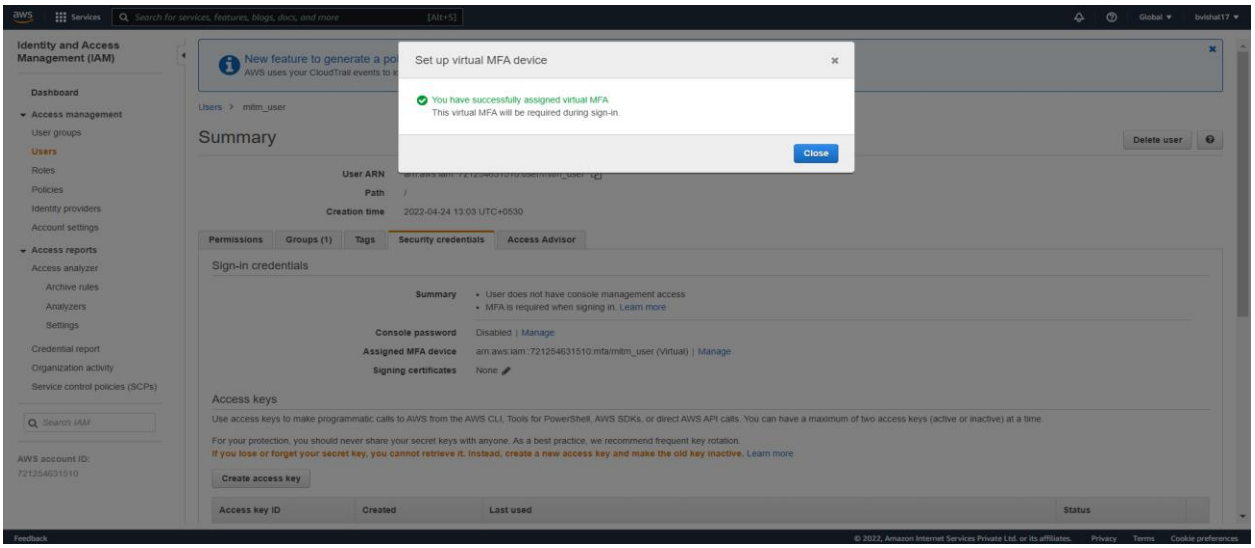


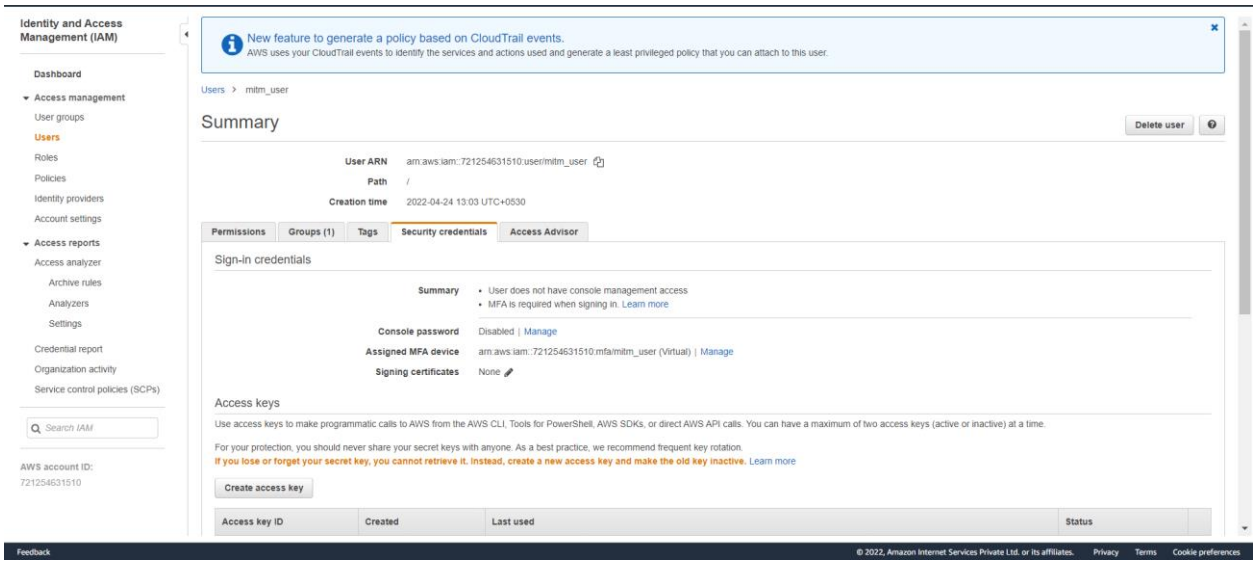
STEP 6: Assigned MFA Device, click on Manage and select the Virtual MFA Device



STEP 7: Download the Google Authenticator application on your mobile device , scan the Qr code & submit the Mfa code1 & MFA code 2.




Identity and Access Management (IAM)
Set up virtual MFA device
You have successfully assigned virtual MFA
This virtual MFA will be required during sign-in.
Close
Summary
Delete user
User ARN
Path
Creation time
2022-04-24 13:03 UTC+0530
Permissions
Groups (1)
Tags
Security credentials
Access Advisor
Sign-in credentials
Summary
User does not have console management access
MFA is required when signing in. Learn more
Console password
Disabled | Manage
Assigned MFA device
arn:aws:iam::721254631510:mfa/mitm_user (Virtual) | Manage
Signing certificates
None
Access keys
Use access keys to make programmatic calls to AWS from the AWS CLI, Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time.
For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation.
If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make the old key inactive. Learn more
Create access key
Access key ID
Created
Last used
Status


Identity and Access Management (IAM)
New feature to generate a policy based on CloudTrail events.
AWS uses your CloudTrail events to identify the services and actions used and generate a least privileged policy that you can attach to this user.
Summary
Delete user
User ARN
arn:aws:iam::721254631510:user/mitm_user
Path
Creation time
2022-04-24 13:03 UTC+0530
Permissions
Groups (1)
Tags
Security credentials
Access Advisor
Sign-in credentials
Summary
User does not have console management access
MFA is required when signing in. Learn more
Console password
Disabled | Manage
Assigned MFA device
arn:aws:iam::721254631510:mfa/mitm_user (Virtual) | Manage
Signing certificates
None
Access keys
Use access keys to make programmatic calls to AWS from the AWS CLI, Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time.
For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation.
If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make the old key inactive. Learn more
Create access key
Access key ID
Created
Last used
Status
Feedback
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences