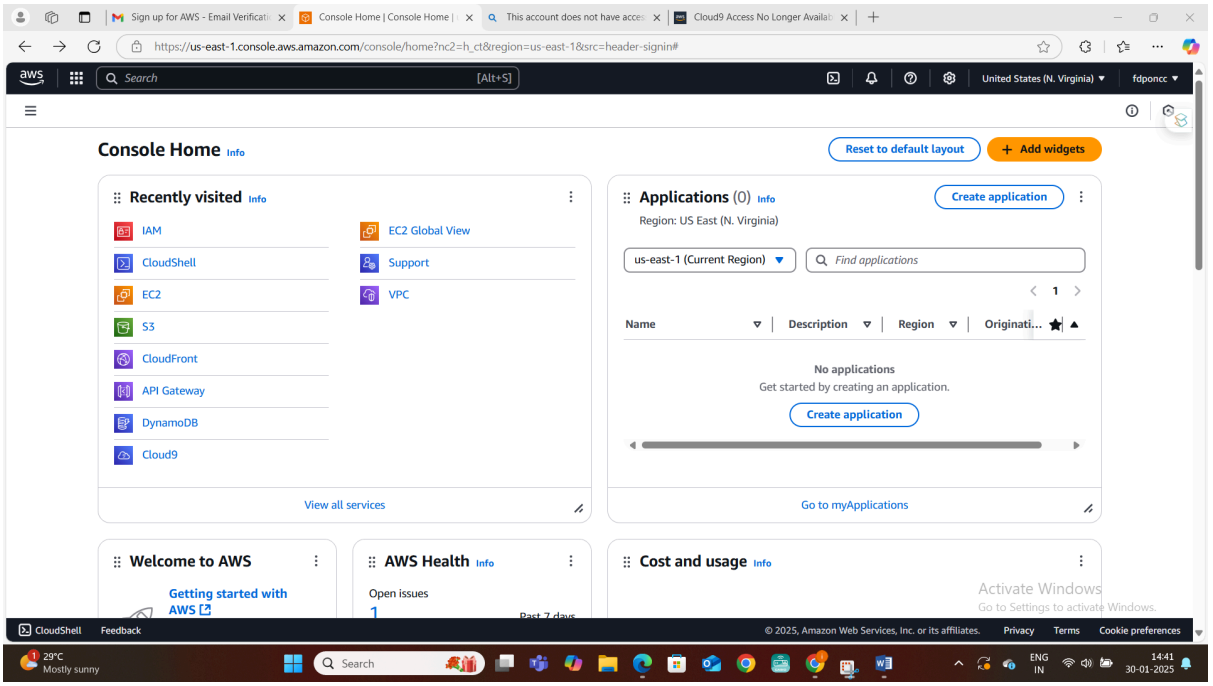
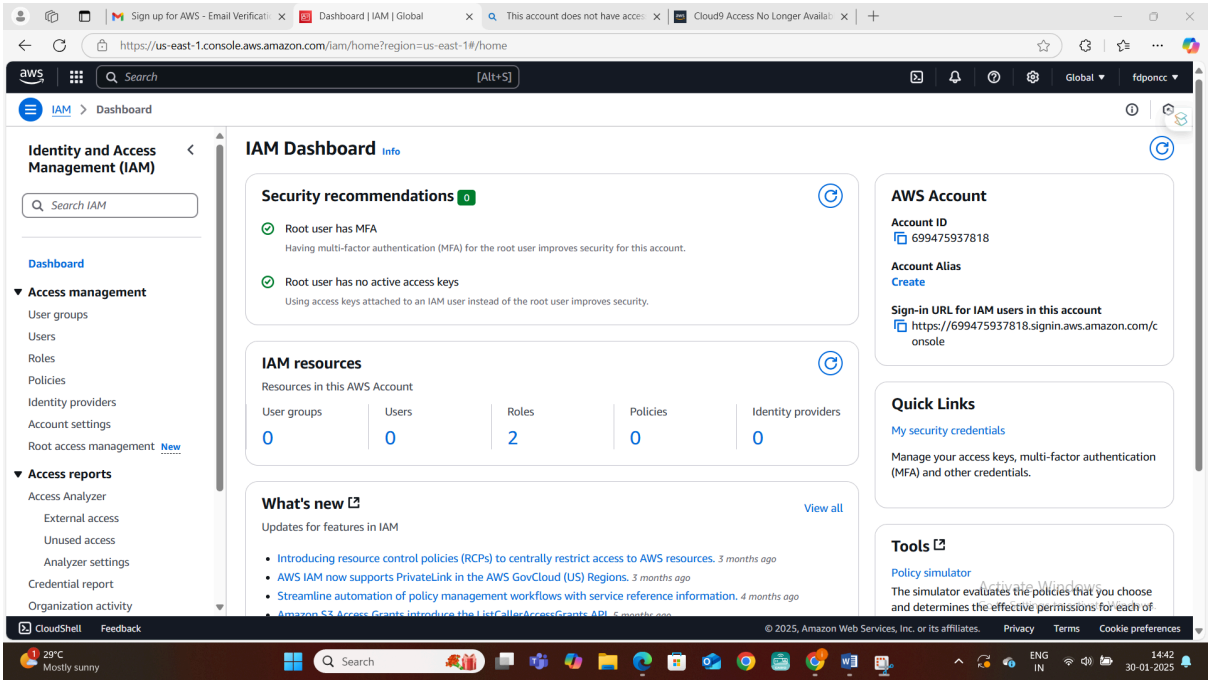
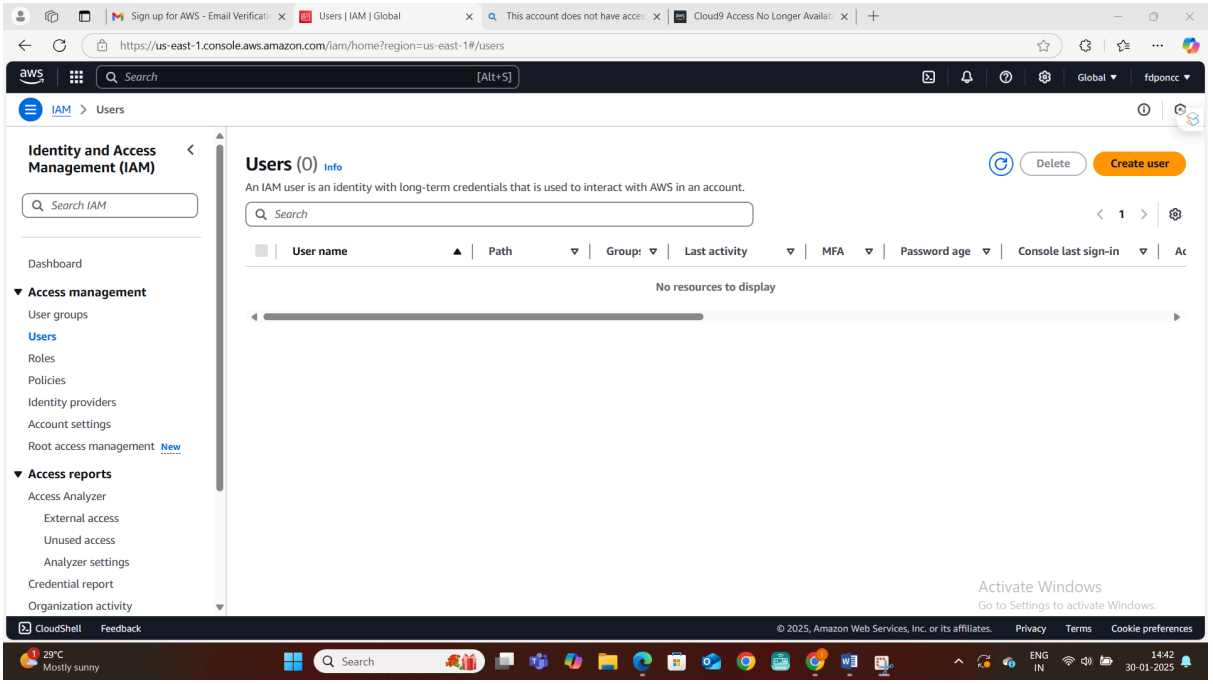
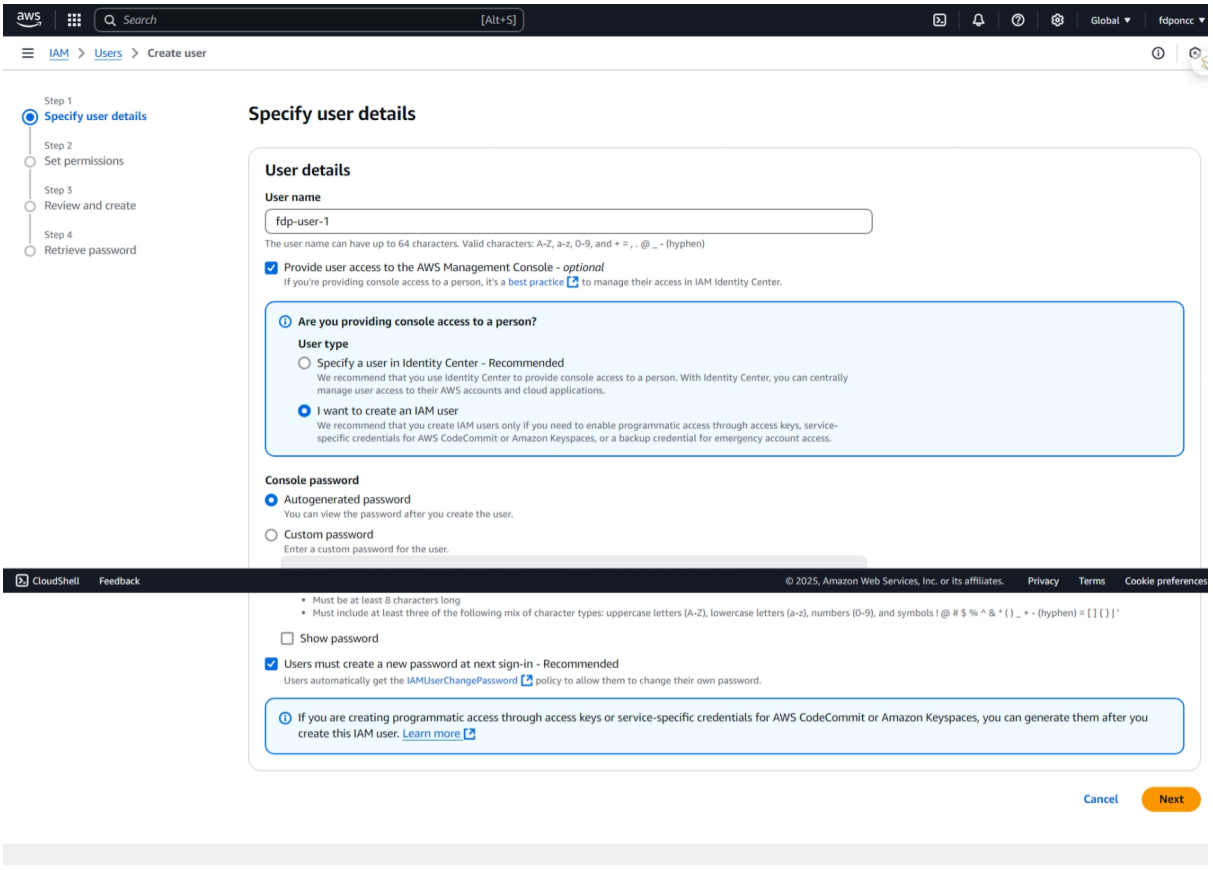
IAM

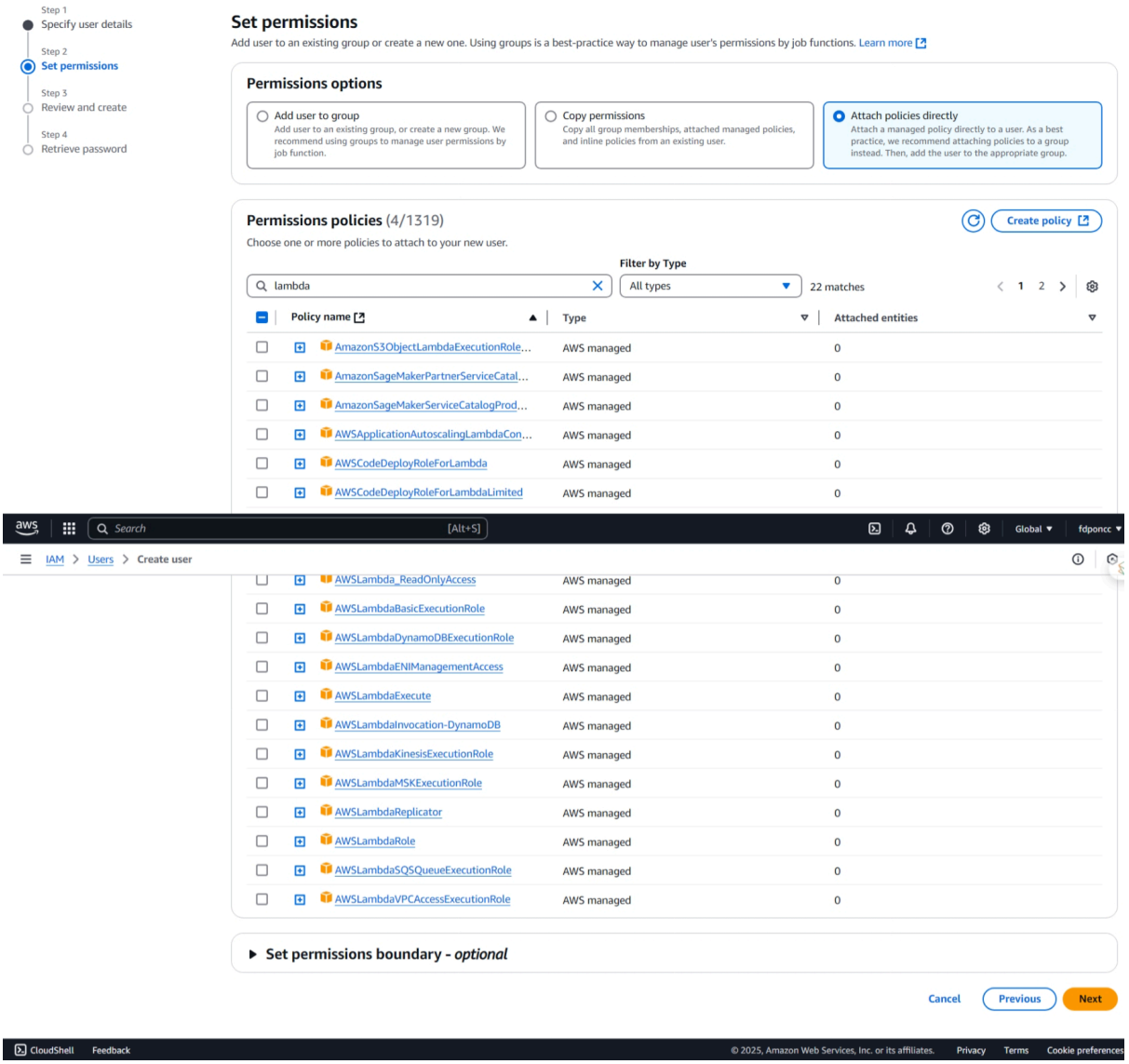

Console Home Info
Reset to default layout
Add widgets
Recently visited Info
IAM
CloudShell
EC2
S3
CloudFront
API Gateway
DynamoDB
Cloud9
EC2 Global View
Support
VPC
View all services
Applications (0) Info
Region: US East (N. Virginia)
Create application
us-east-1 (Current Region)
Find applications
Name
Description
Region
Originati...
No applications
Get started by creating an application.
Create application
Go to myApplications
Welcome to AWS
Getting started with AWS
AWS Health Info
Open issues
1
Cost and usage Info
Activate Windows
Go to Settings to activate Windows.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

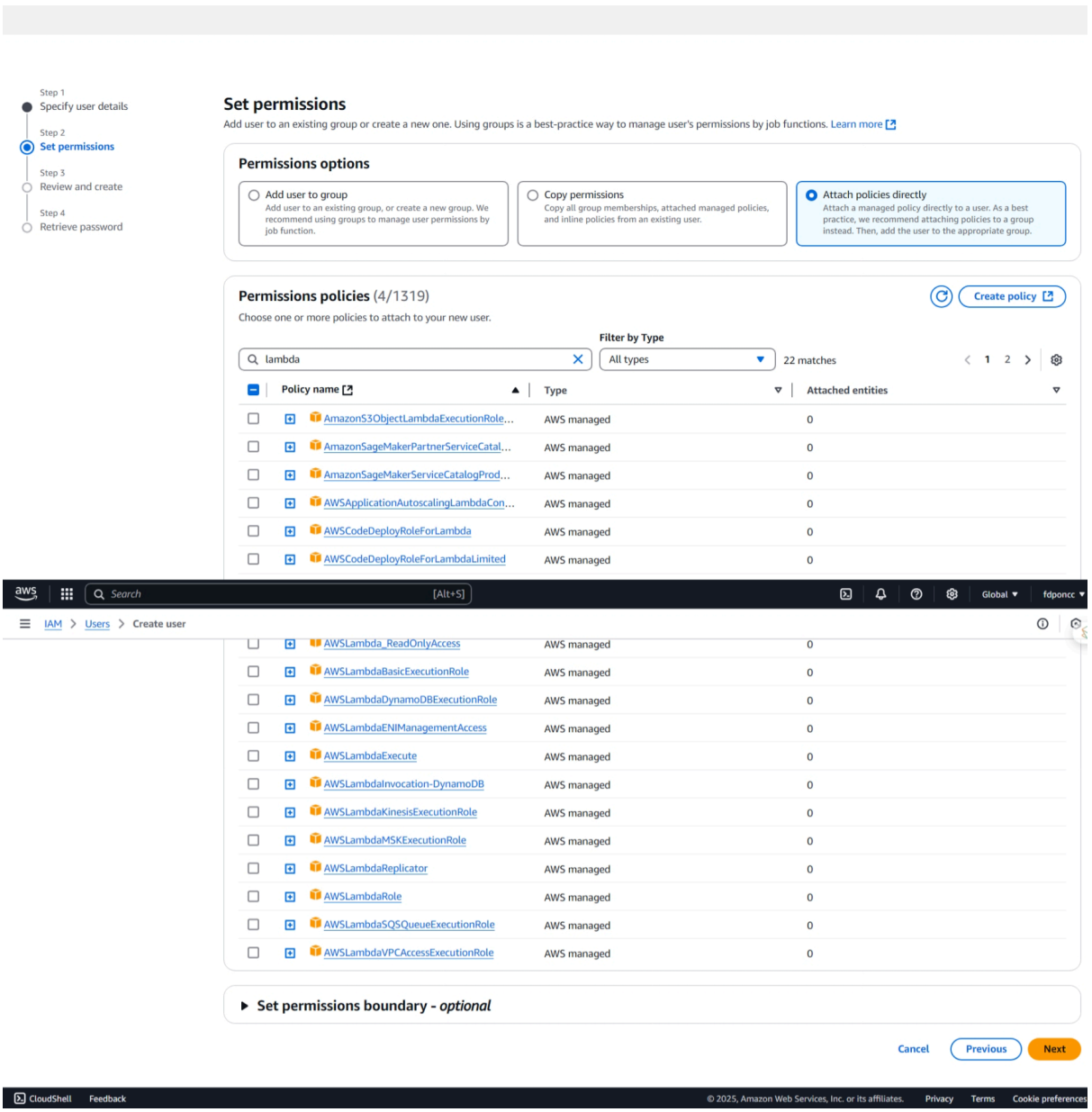

IAM Dashboard Info
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Security recommendations 0
Root user has MFA
Having multi-factor authentication (MFA) for the root user improves security for this account.
Root user has no active access keys
Using access keys attached to an IAM user instead of the root user improves security.
IAM resources
Resources in this AWS Account
User groups
Users
Roles
Policies
Identity providers
0
0
2
0
0
What's new
View all
Updates for features in IAM
Introducing resource control policies (RCPs) to centrally restrict access to AWS resources. 3 months ago
AWS IAM now supports PrivateLink in the AWS GovCloud (US) Regions. 3 months ago
Streamline automation of policy management workflows with service reference information. 4 months ago
AWS Account
Account ID
699475937818
Account Alias
Create
Sign-in URL for IAM users in this account
https://699475937818.signin.aws.amazon.com/console
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
Activate Windows
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



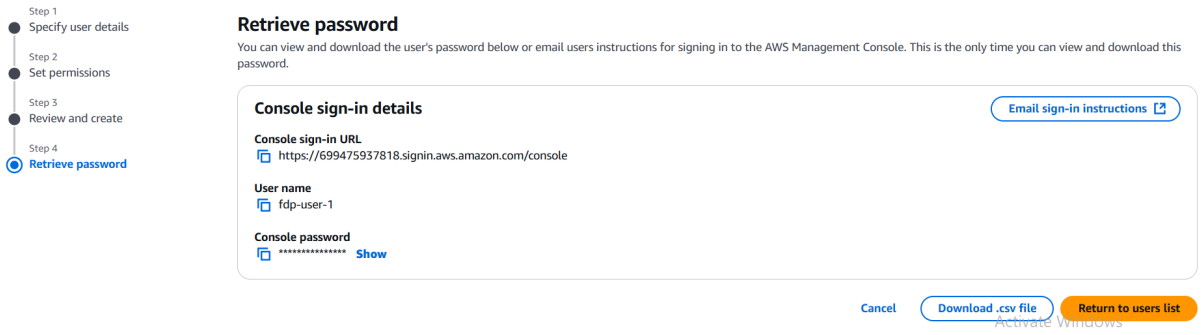


ATTACH POLICIES WITH FULL ACCESS FOR S3, LAMDA, DYNAMODB, CLOUD9

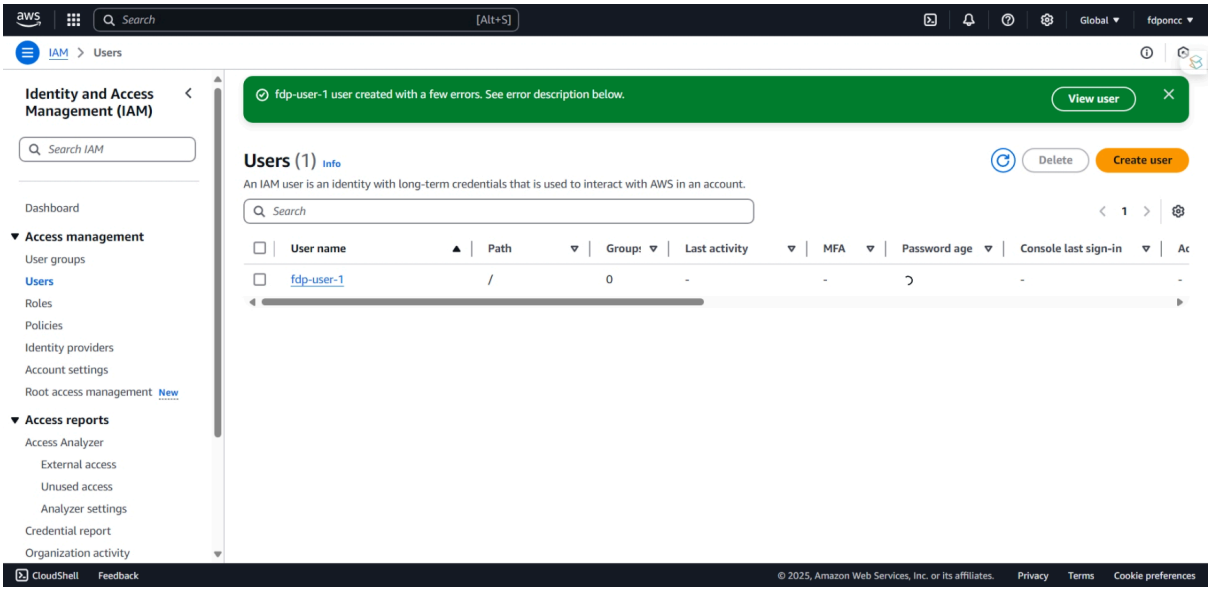

Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Set permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more
Permissions options
Add user to group
Add 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.
Permissions policies (4/1319)
Choose one or more policies to attach to your new user.
Create policy
Filter by Type
lambda
All types
22 matches
1
2
Policy name
Type
Attached entities
AmazonS3ObjectLambdaExecutionRole...
AmazonSageMakerPartnerServiceCatal...
AmazonSageMakerServiceCatalogProd...
AWSApplicationAutoscalingLambdaCon...
AWSCodeDeployRoleForLambda
AWSCodeDeployRoleForLambdaLimited
AWS managed
0
aws
Search
[Alt+S]
Global
fdponcc
IAM
Users
Create user
AWSLambda_ReadOnlyAccess
AWSLambdaBasicExecutionRole
AWSLambdaDynamoDBExecutionRole
AWSLambdaENIManagementAccess
AWSLambdaExecute
AWSLambdaInvocation-DynamoDB
AWSLambdaKinesisExecutionRole
AWSLambdaMSKExecutionRole
AWSLambdaReplicator
AWSLambdaRole
AWSLambdaSQSQueueExecutionRole
AWSLambdaVPCAccessExecutionRole
Set permissions boundary - optional
Cancel
Previous
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



DOWNLOAD .CSV FILE for future use



USER HAS BEEN CREATED



SIGN IN TO AWS CONSOLE USING NEW LOGIN CREADENTIALS