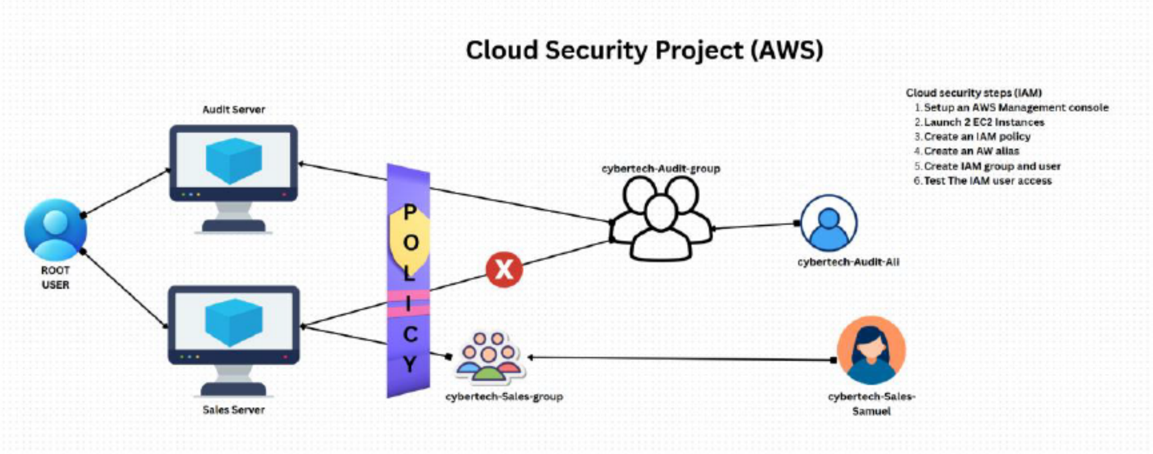
AWS IAM Cloud Security Project

1. Project Overview

I completed this project on cloud security controls in Amazon Web Services (AWS), focusing on Identity and Access Management (IAM). The goal was to create a least- privilege policy, attach it to a user or group, and verify that the policy correctly restricts actions on Amazon EC2 instance.



Cloud Security Project (AWS)

Cloud security steps (IAM)

1. Setup an AWS Management console
2. Launch 2 EC2 Instances
3. Create an IAM policy
4. Create an AW alias
5. Create IAM group and user
6. Test The IAM user access

In this project, we will be creating Users, User groups, buckets, cloudtrails, polices and implementing those policies and verifying them.

Standard practice prescribes that we don’t do anything on root user, i.e we do not create EC2, S3 buckets from the root user, however we can use it to create a user with admin privileges. one we are done with this, we log out and go to the login page where we will be given the option to log in as IAM user.. please proceed with this and you can now start creatin all we need from this new login channel

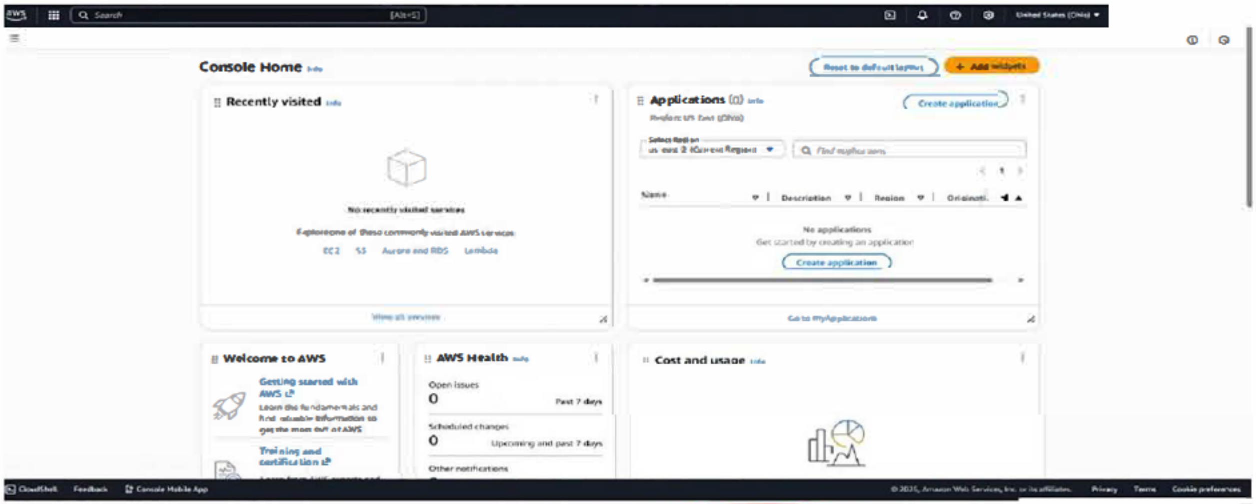
In AWS, we use services to create everything

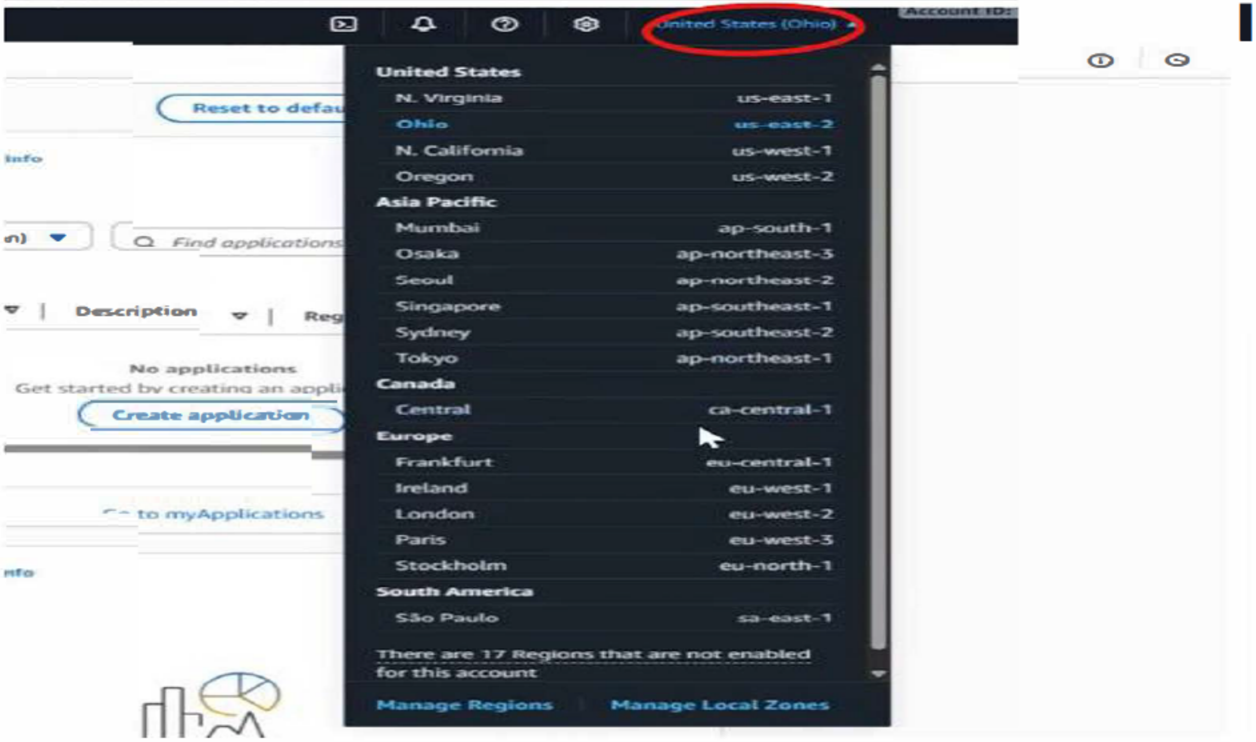
Firstly we can create an AWS trail account for 6 month on the website at Cloud Computing Services - Amazon Web Services (AWS), a credit card will be required however you will get a credit to use to run your simulation.

CREATING THE IAM USER AND GROUPS

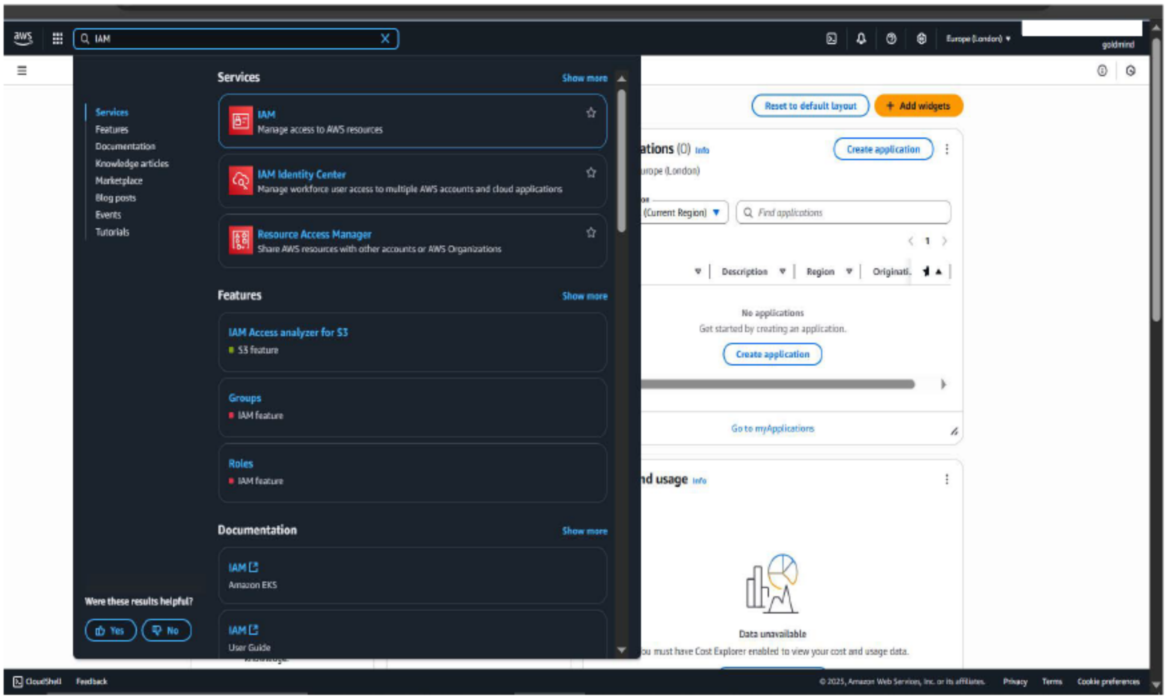
Upon creating an account and logging in, it will be a root user, so we will set up MFA (to make it secure) and create a user with admin privileges.

Firstly, we need to change our geographical location to our closest location



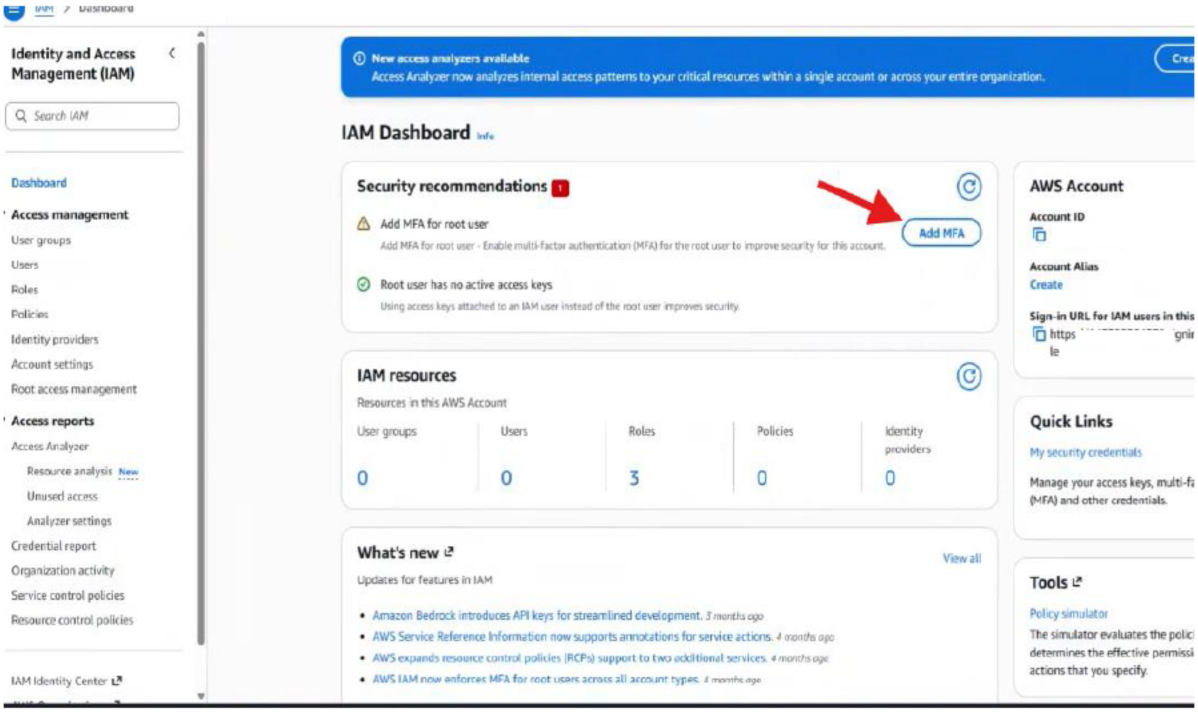


In the search bar, find the IAM service , as best practice, set up MFA



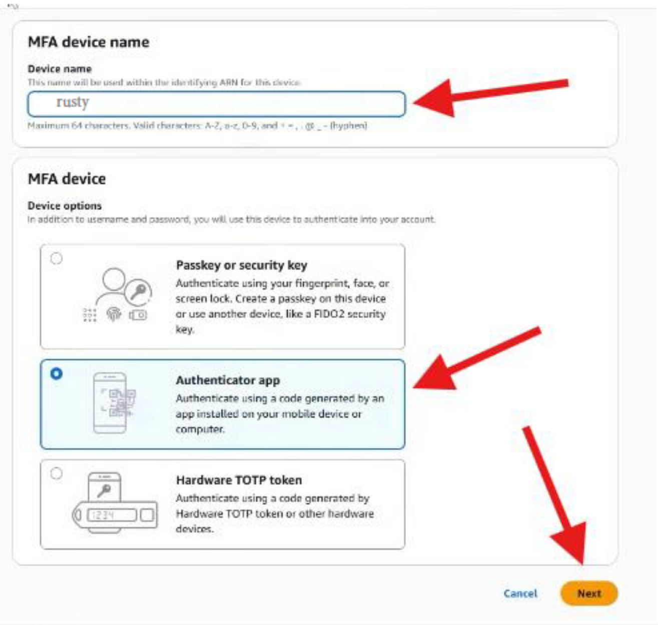
Search for IAM from the search column

click on IAM


IAM > Dashboard
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies
IAM Identity Center
New access analyzers available
Access Analyzer now analyzes internal access patterns to your critical resources within a single account or across your entire organization.
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.
Add MFA
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
0
Users
0
Roles
3
Policies
0
Identity providers
0
What's new
Updates for features in IAM
View all
Amazon Bedrock introduces API keys for streamlined development. 3 months ago
AWS Service Reference Information now supports annotations for service actions. 4 months ago
AWS expands resource control policies (RCPs) support to two additional services. 4 months ago
AWS IAM now enforces MFA for root users across all account types. 4 months ago
AWS Account
Account ID
Account Alias
Create
Sign-in URL for IAM users in this
Quick Links
My security credentials
Manage your access keys, multi-fa (MFA) and other credentials.
Tools
Policy simulator
The simulator evaluates the polic determines the effective permissi actions that you specify.

Add MFA

Give the device a name and select a MFA device of your choice, in this instance we will use an Authentication app



MFA device name

Device name

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

rusty

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

MFA device

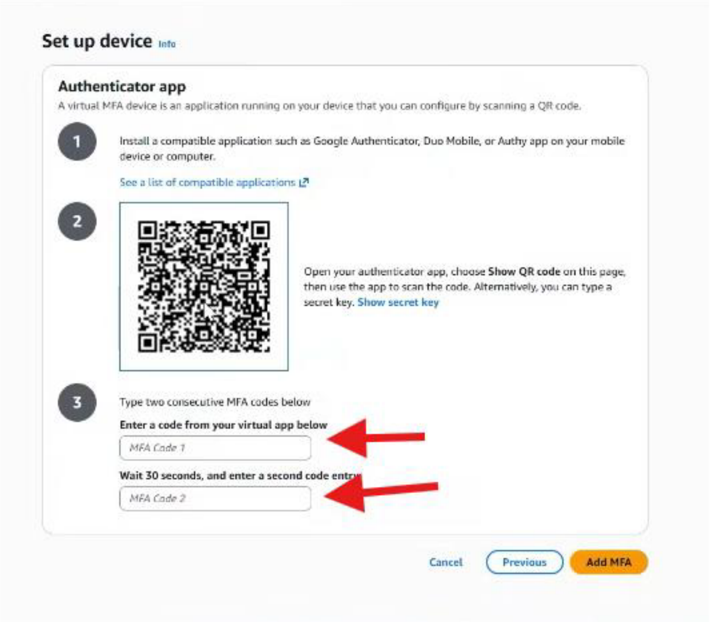
Device options

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.



Set up device

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. 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

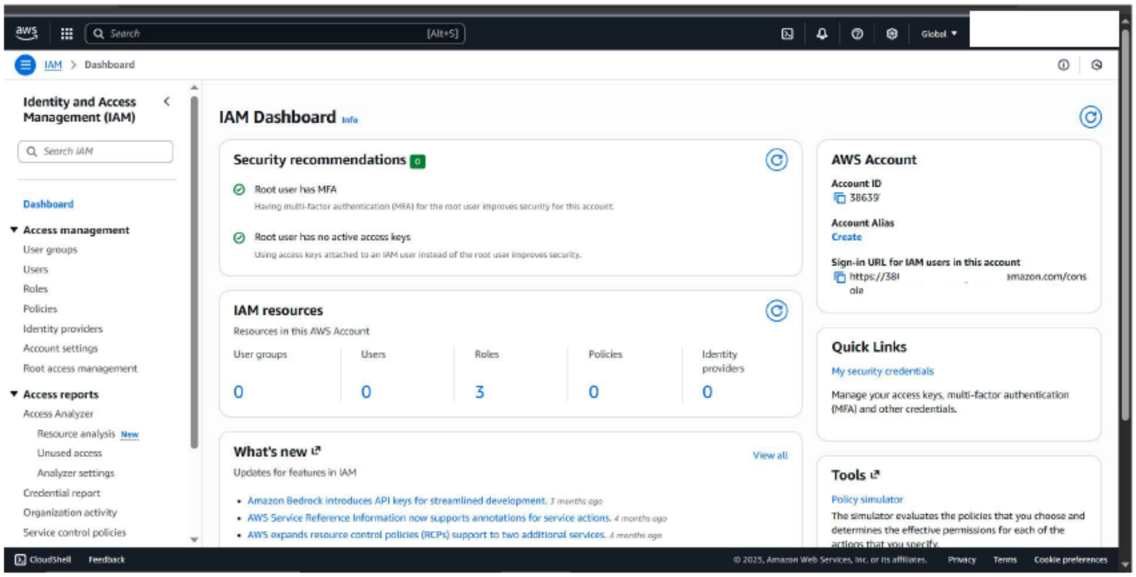
3. Type two consecutive MFA codes below

   Enter a code from your virtual app below

   MFA Code 1

   Wait 30 seconds, and enter a second code entry

   MFA Code 2



[redacted]

IAM Dashboard Info

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	3	0	0

What's new

Updates for features in IAM

View all

- Amazon Bedrock introduces API keys for streamlined development. 3 months ago
- AWS Service Reference Information now supports annotations for service actions. 4 months ago
- AWS expands resource control policies (RCPs) support to two additional services. 4 months ago

AWS Account

Account ID
38639

Account Alias
Create

Sign-in URL for IAM users in this account
https://38[redacted]amazon.com/console

Quick Links

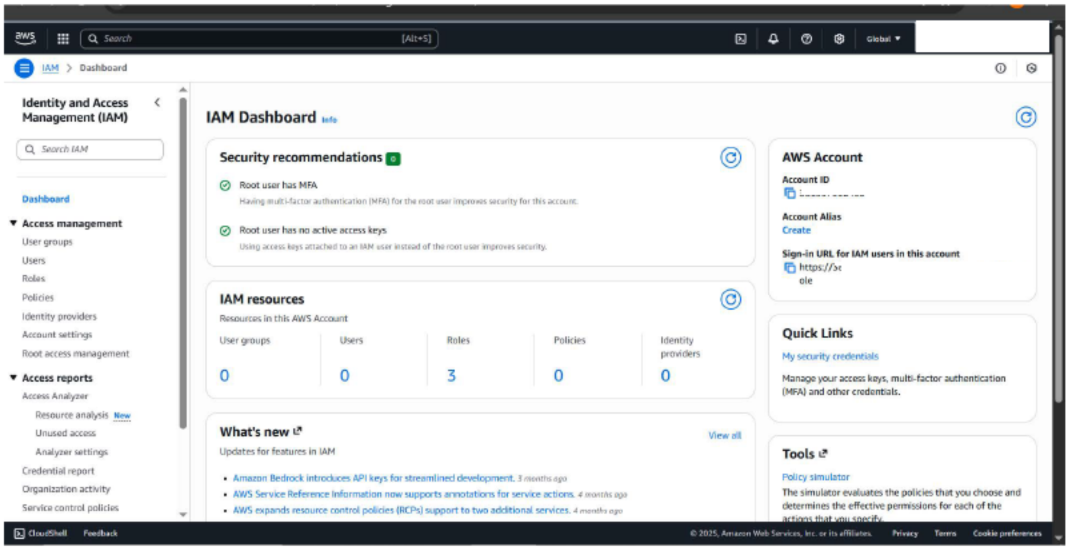
My security credentials

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 the actions that you specify.



IAM Dashboard Info

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	3	0	0

What's new

Updates for features in IAM

View all

- Amazon Bedrock introduces API keys for streamlined development. 3 months ago
- AWS Service Reference Information now supports annotations for service actions. 4 months ago
- AWS expands resource control policies (RCPs) support to two additional services. 4 months ago

AWS Account

Account ID

Account Alias
Create

Sign-in URL for IAM users in this account
https://3[redacted]
ole

Quick Links

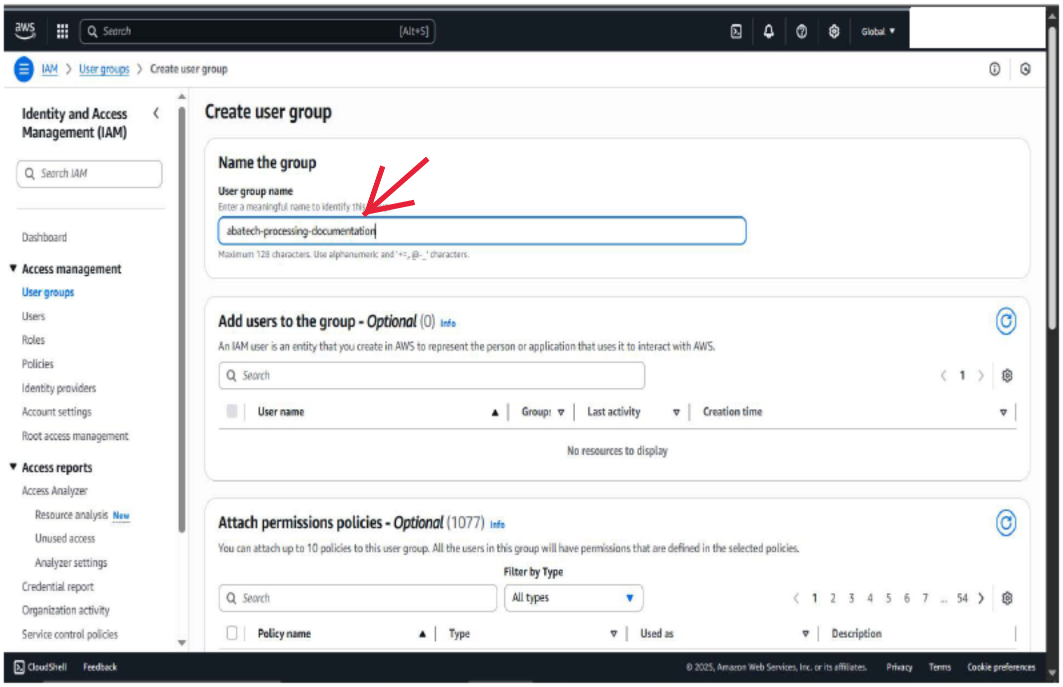
My security credentials

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.



Create user group

Name the group

User group name

Enter a meaningful name to identify this

abatech-processing-documentation

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

Add users to the group - *Optional* (0) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

User name	Groups	Last activity	Creation time

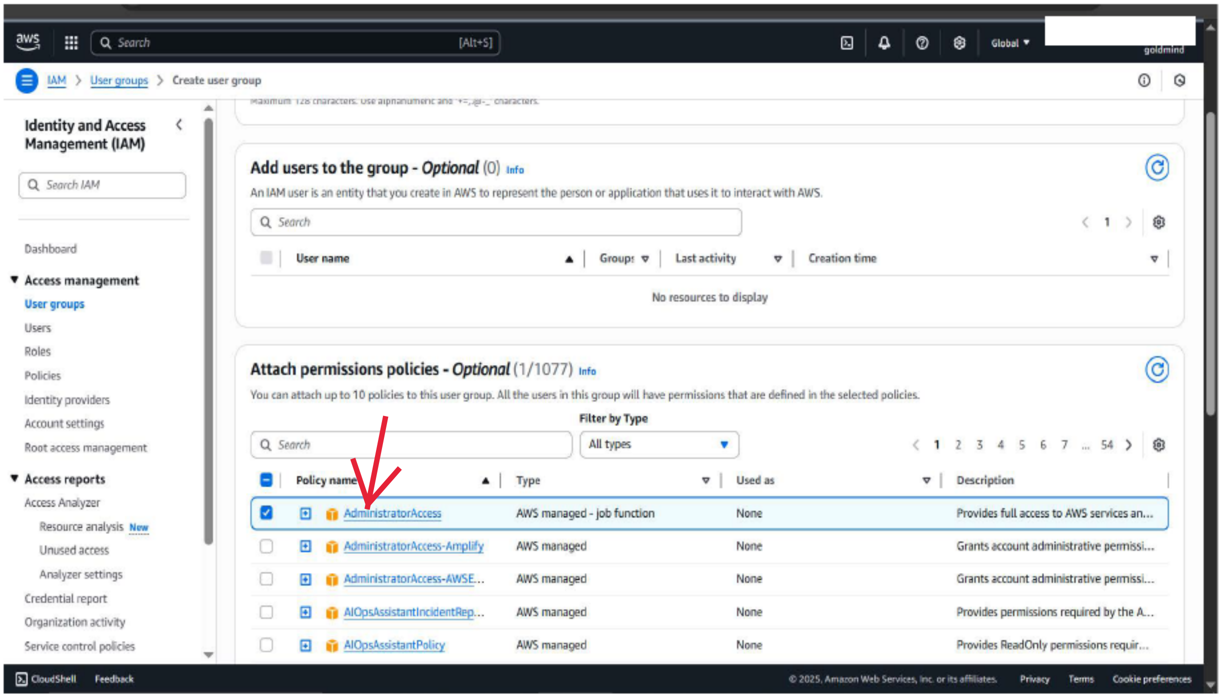
No resources to display

Attach permissions policies - *Optional* (1077) Info

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter by Type: All types

Policy name	Type	Used as	Description



Identity and Access Management (IAM)

Search IAM

Dashboard

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

▼ Access reports
- Access Analyzer
  - Resource analysis New
  - Unused access
  - Analyzer settings
- Credential report
- Organization activity
- Service control policies

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

Add users to the group - *Optional* (0) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Search ‹ 1 ›

□	User name ▲	Groups ▽	Last activity ▽	Creation time ▽

No resources to display

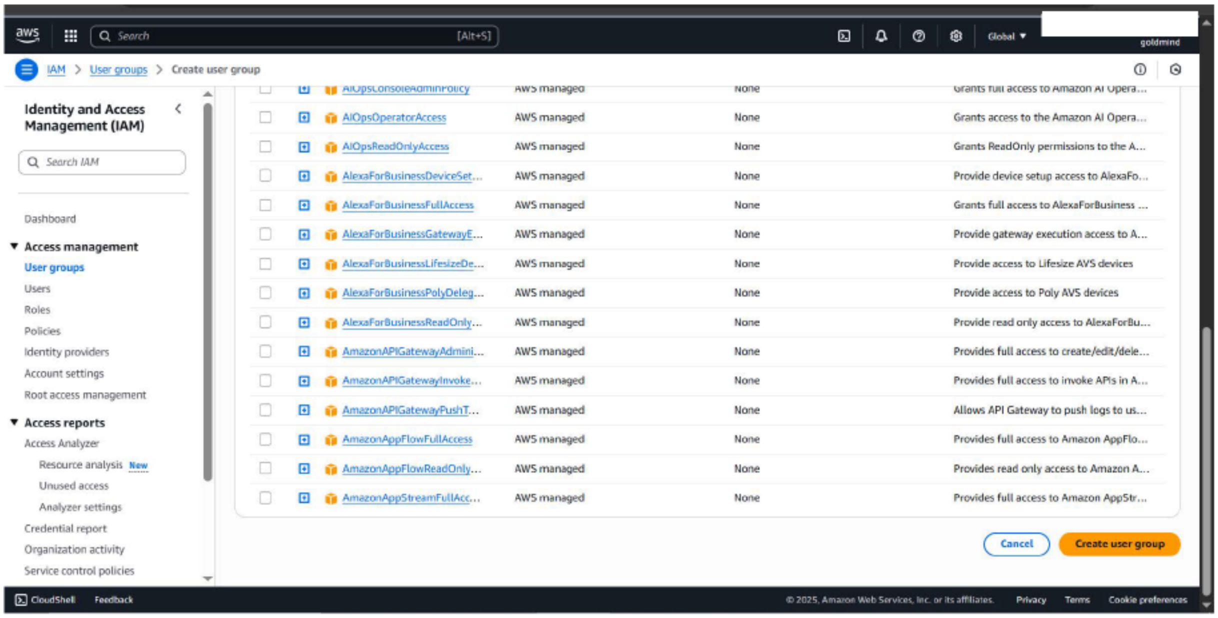
Attach permissions policies - *Optional* (1/1077) Info

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter by Type

Search | All types ▾ | ‹ 1 2 3 4 5 6 7 ... 54 ›

☐	Policy name ▲	Type ▽	Used as ▽	Description
☑	AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services an...
□	AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permissi...
□	AdministratorAccess-AWSE...	AWS managed	None	Grants account administrative permissi...
□	AIOpsAssistantIncidentRep...	AWS managed	None	Provides permissions required by the A...
□	AIOpsAssistantPolicy	AWS managed	None	Provides ReadOnly permissions requir...



Identity and Access Management (IAM)

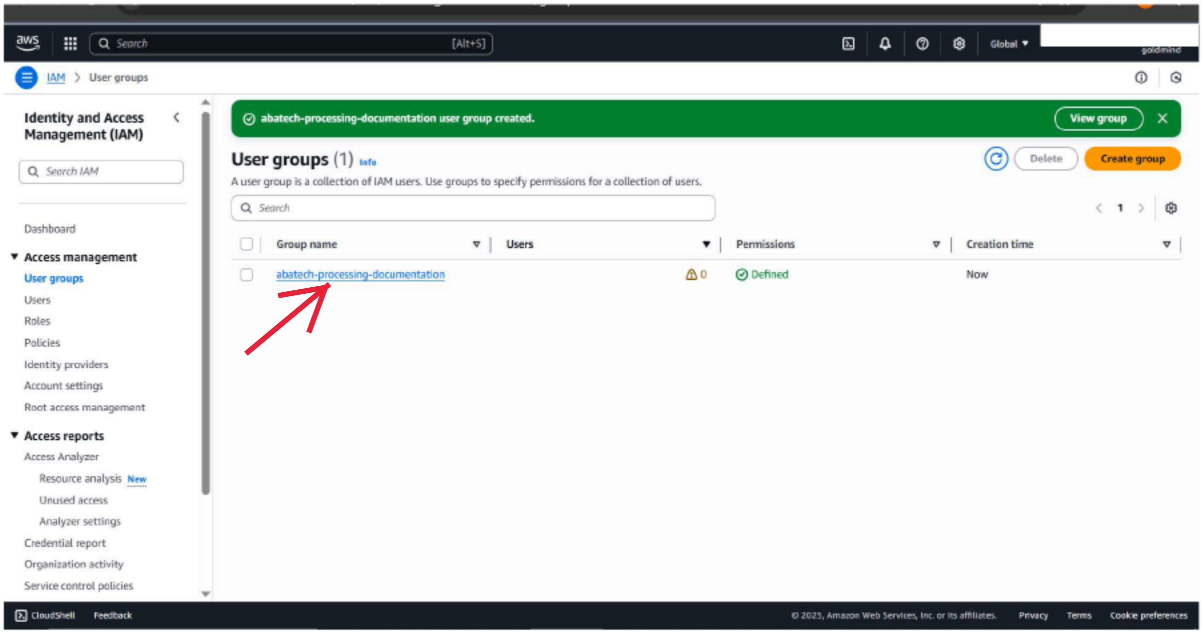
Search IAM

Dashboard

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

▼ Access reports
- Access Analyzer
  - Resource analysis New
  - Unused access
  - Analyzer settings
- Credential report
- Organization activity
- Service control policies

□	Policy name	Type	Used as	Description
□	AIOpsConsoleAdminPolicy	AWS managed	None	Grants full access to Amazon AI Opera...
□	AIOpsOperatorAccess	AWS managed	None	Grants access to the Amazon AI Opera...
□	AIOpsReadOnlyAccess	AWS managed	None	Grants ReadOnly permissions to the A...
□	AlexaForBusinessDeviceSet...	AWS managed	None	Provide device setup access to AlexaFo...
□	AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness ...
□	AlexaForBusinessGatewayE...	AWS managed	None	Provide gateway execution access to A...
□	AlexaForBusinessLifesizeDe...	AWS managed	None	Provide access to Lifesize AVS devices
□	AlexaForBusinessPolyDeleg...	AWS managed	None	Provide access to Poly AVS devices
□	AlexaForBusinessReadOnly...	AWS managed	None	Provide read only access to AlexaForBu...
□	AmazonAPIGatewayAdmini...	AWS managed	None	Provides full access to create/edit/dele...
□	AmazonAPIGatewayInvoke...	AWS managed	None	Provides full access to invoke APIs in A...
□	AmazonAPIGatewayPushT...	AWS managed	None	Allows API Gateway to push logs to us...
□	AmazonAppFlowFullAccess	AWS managed	None	Provides full access to Amazon AppFlo...
□	AmazonAppFlowReadOnly...	AWS managed	None	Provides read only access to Amazon A...
□	AmazonAppStreamFullAcc...	AWS managed	None	Provides full access to Amazon AppStr...



Identity and Access Management (IAM)

Search IAM

Dashboard

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

▼ Access reports
- Access Analyzer
  - Resource analysis New
  - Unused access
  - Analyzer settings
- Credential report
- Organization activity
- Service control policies

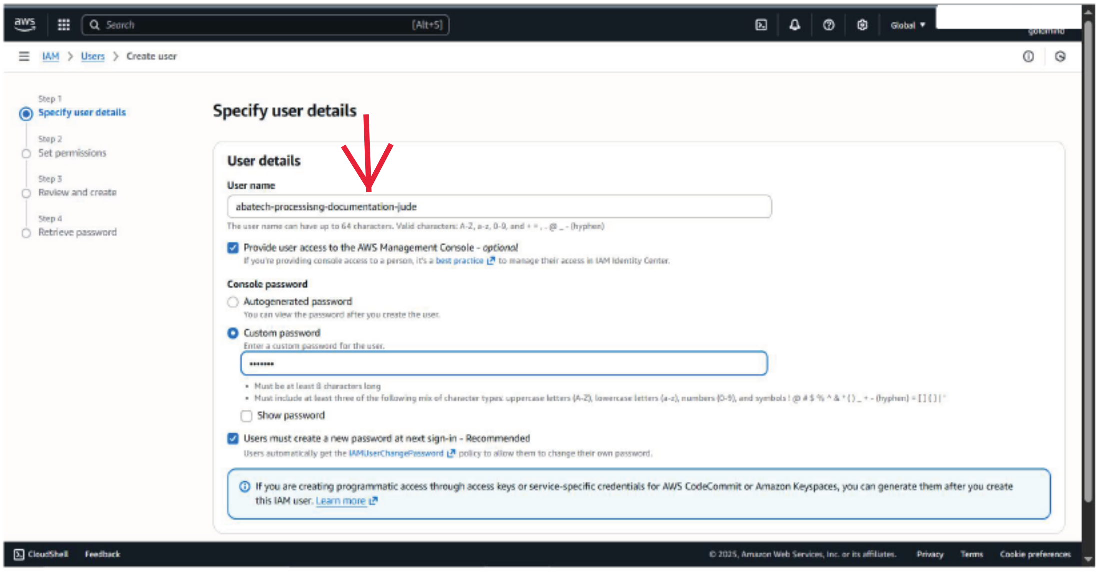
abatech-processing-documentation user group created.

User groups (1) Info

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

Search ‹ 1 ›

□	Group name ▽	Users ▽	Permissions ▽	Creation time ▽
□	abatech-processing-documentation	⚠ 0	✓ Defined	Now



Search [Alt+S] Global ▾ goldmind

IAM > Users > Create user

Step 1
● Specify user details

Step 2
○ Set permissions

Step 3
○ Review and create

Step 4
○ Retrieve password

Specify user details

User details

User name

abatech-processisng-documentation-jude

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.

Console password

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

● Custom password
Enter a custom password for the user.

•••••••

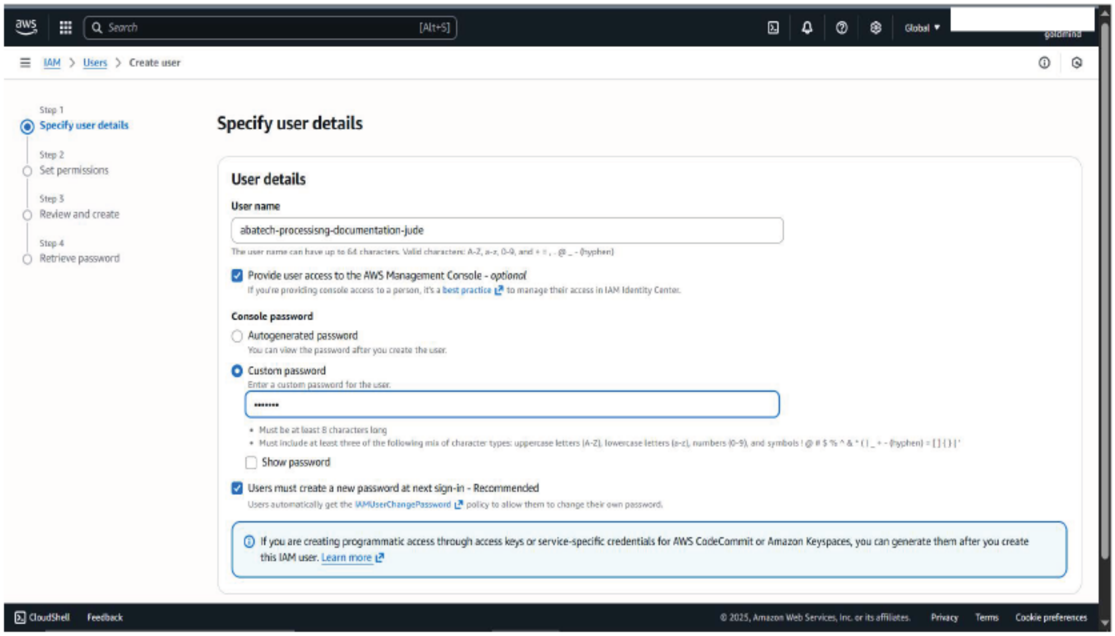
- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

□ 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

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



Search [Alt+S] Global ▾ goldmind

IAM > Users > Create user

Step 1
● Specify user details

Step 2
○ Set permissions

Step 3
○ Review and create

Step 4
○ Retrieve password

Specify user details

User details

User name

abatech-processisng-documentation-jude

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.

Console password

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

● Custom password
Enter a custom password for the user.

•••••••

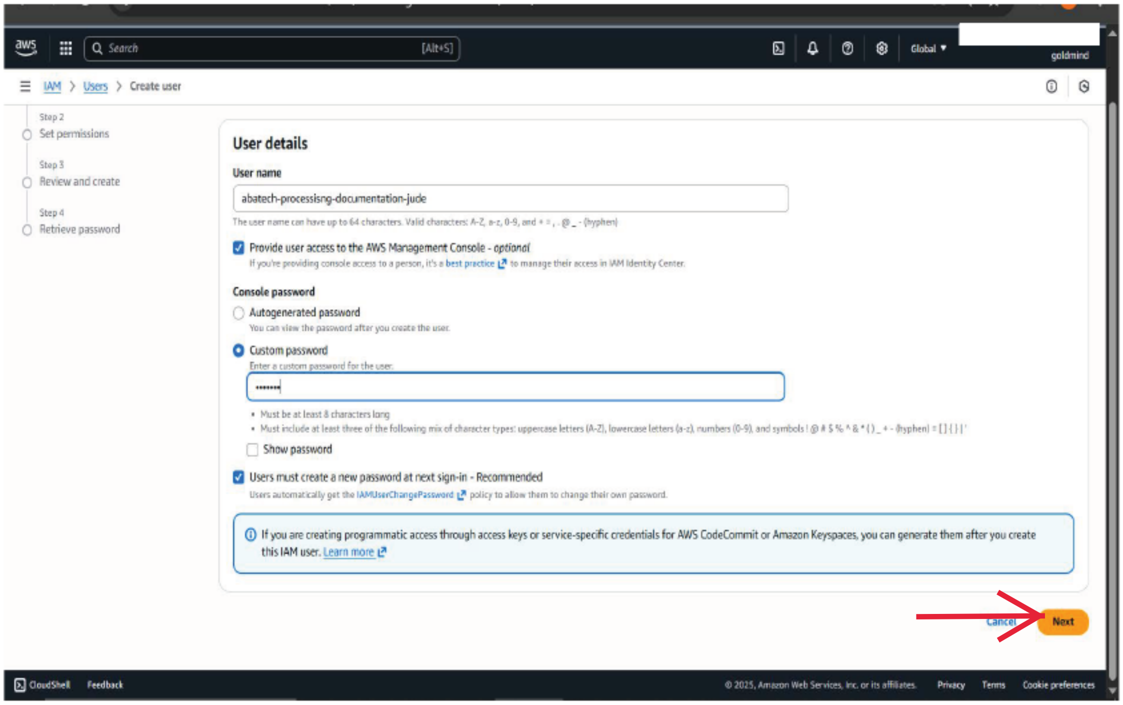
- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

□ 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

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



Search [Alt+S] Global ▾ goldmind

IAM > Users > Create user

Step 2
○ Set permissions

Step 3
○ Review and create

Step 4
○ Retrieve password

User details

User name

abatech-processisng-documentation-jude

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.

Console password

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

● Custom password
Enter a custom password for the user.

•••••••

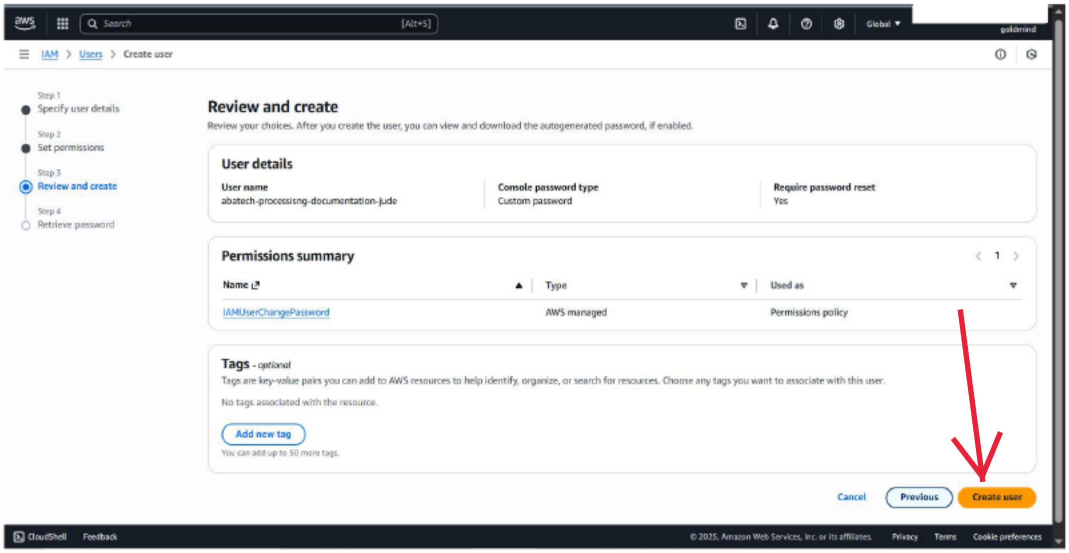
- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

□ 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

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



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	Console password type	Require password reset
abatech-processisng-documentation-jude	Custom password	Yes

Permissions summary

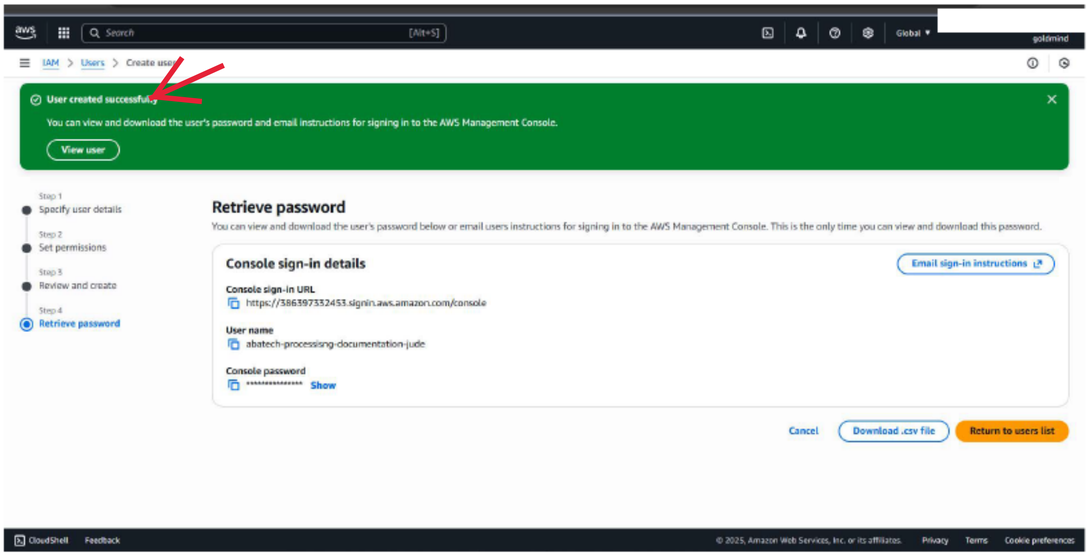
Name	Type	Used as
IAMUserChangePassword	AWS managed	Permissions policy

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.

You can add up to 50 more tags.



User created successfully

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

Retrieve password

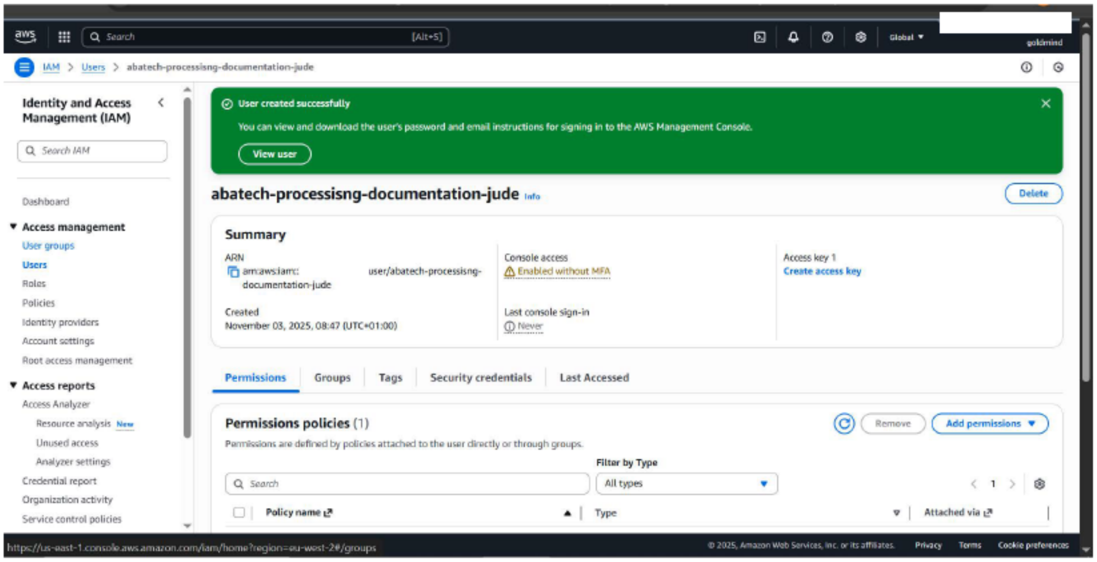
You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Console sign-in URL
https://386397332453.signin.aws.amazon.com/console

User name
abatech-processisng-documentation-jude

Console password
*************** Show



User created successfully

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

abatech-processisng-documentation-jude

Summary

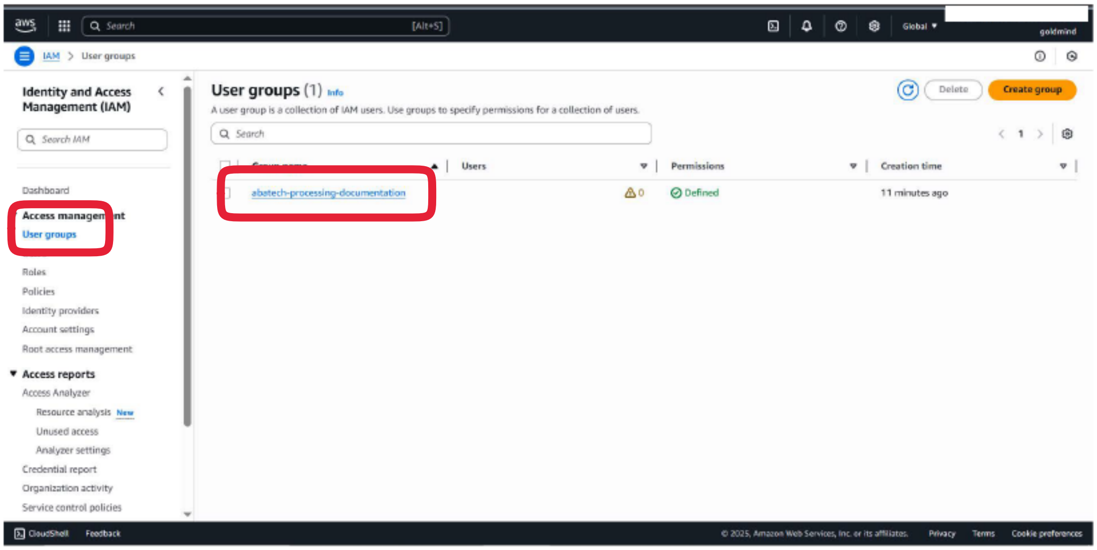
ARN	Console access	Access key 1
arn:aws:iam:: user/abatech-processisng-documentation-jude	⚠ Enabled without MFA	Create access key
Created	Last console sign-in	
November 03, 2025, 08:47 (UTC+01:00)	Never	

Permissions policies (1)

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

Remove
Add permissions ▾
Filter by Type
Search
All types
Policy name
Type
Attached via
https://us-east-1.console.aws.amazon.com/iam/home?region=eu-west-2#/groups
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

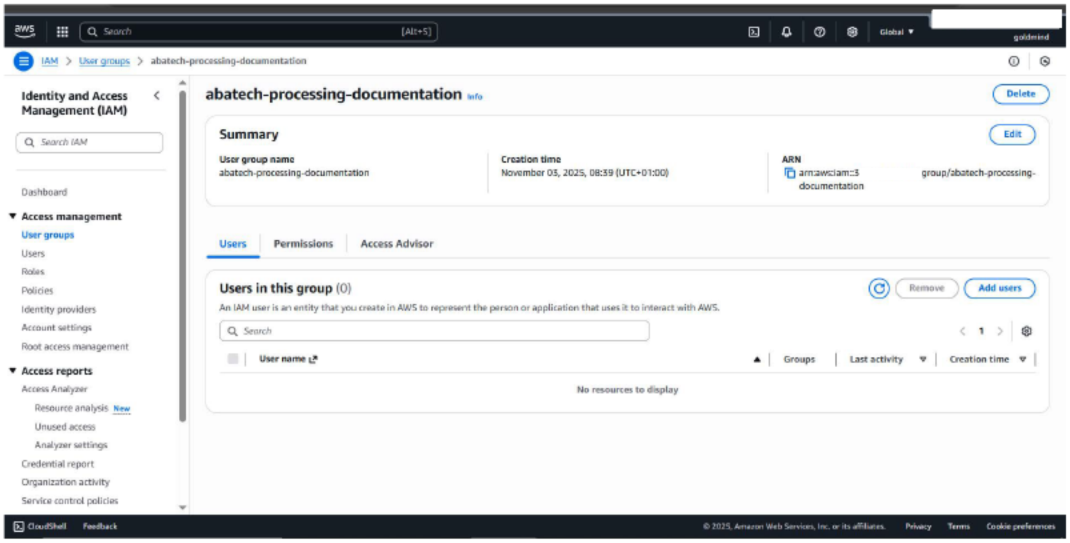
ADDING THE USER TO A GROUP



User groups (1) Info

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

Group name	Users	Permissions	Creation time
abatech-processing-documentation	⚠ 0	✓ Defined	11 minutes ago



abatech-processing-documentation Info

Summary

User group name
abatech-processing-documentation

Creation time
November 03, 2025, 08:39 (UTC+01:00)

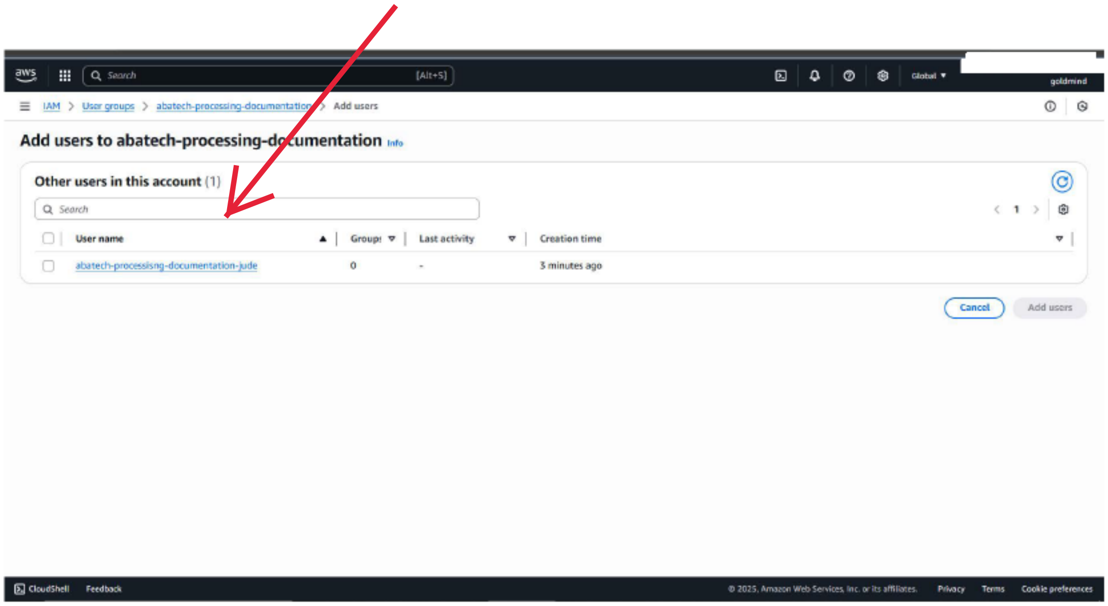
ARN
arn:aws:iam::3[redacted]group/abatech-processing-documentation

Users in this group (0)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

User name	Groups	Last activity	Creation time

No resources to display

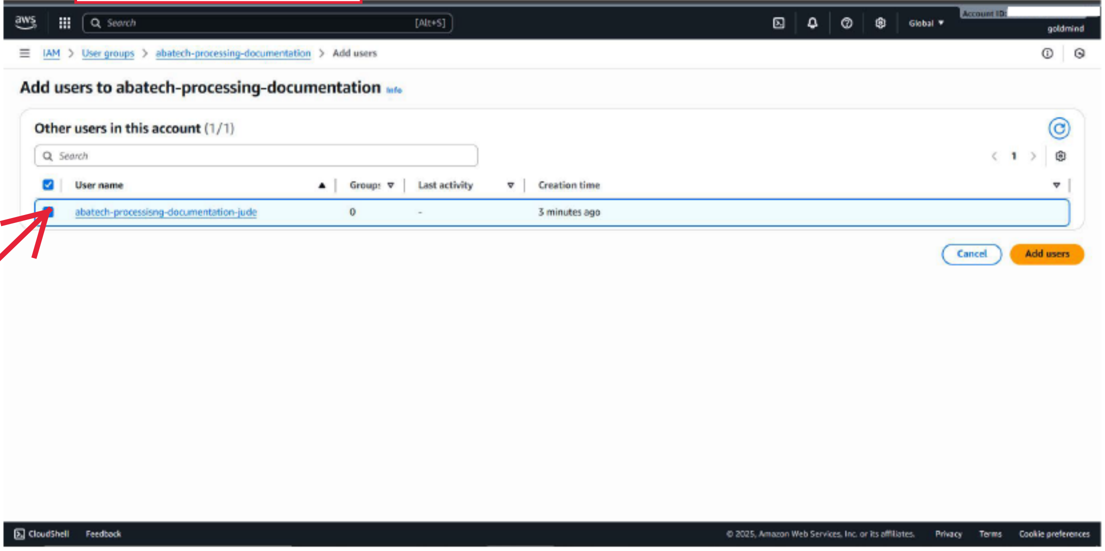

aws
Search [Alt+S]
Global ▾
goldmind
IAM > User groups > abatech-processing-documentation > Add users
Cancel
Add users
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Add users to abatech-processing-documentation Info

Other users in this account (1)

□	User name	Groups	Last activity	Creation time
□	abatech-processisng-documentation-jude	0	-	3 minutes ago

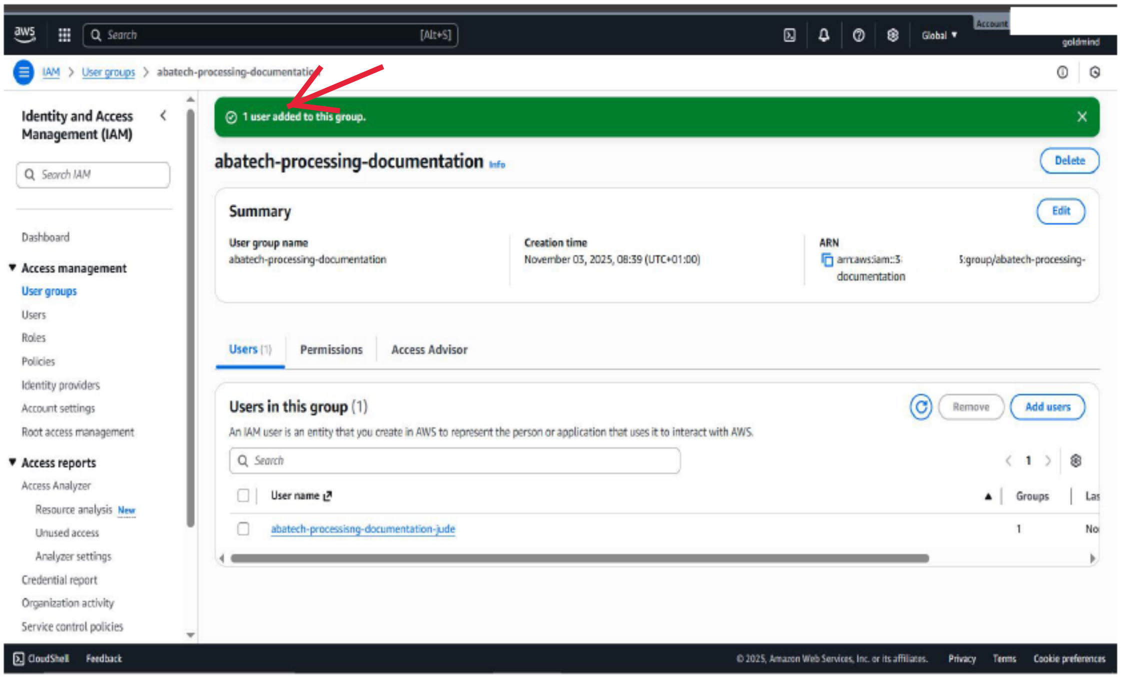
ADD abatech processing-documentation - jude to the group


aws
Search [Alt+S]
Global ▾
Account ID: [redacted]
goldmind
IAM > User groups > abatech-processing-documentation > Add users

Add users to abatech-processing-documentation Info

Other users in this account (1/1)

☑	User name ▲	Groups ▽	Last activity ▽	Creation time ▽
☑	abatech-processisng-documentation-jude	0	-	3 minutes ago



1 user added to this group.

abatech-processing-documentation Info

Summary

User group name
abatech-processing-documentation

Creation time
November 03, 2025, 08:39 (UTC+01:00)

ARN
arn:aws:iam::3[redacted]5:group/abatech-processing-documentation

Users in this group (1)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

□	User name ▲	Groups	Las
□	abatech-processisng-documentation-jude	1	No