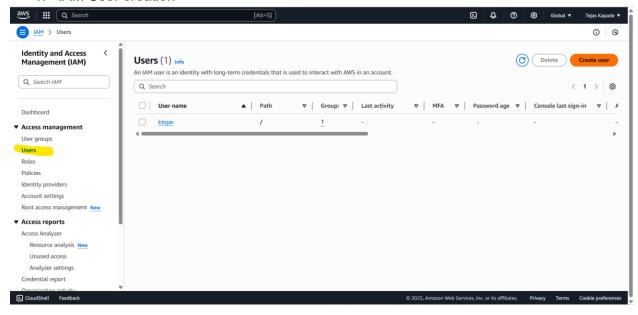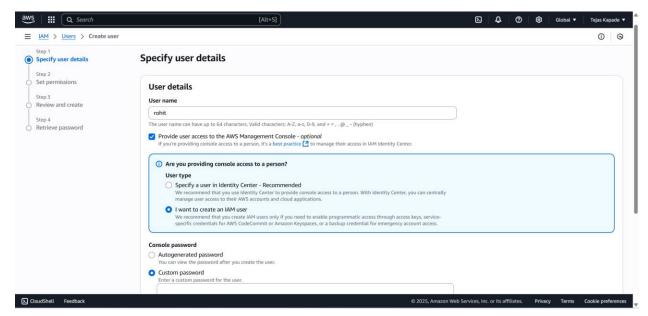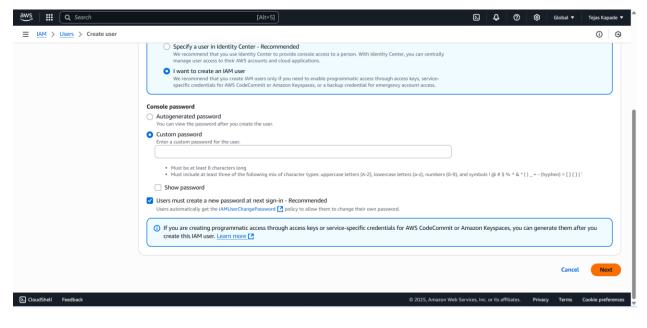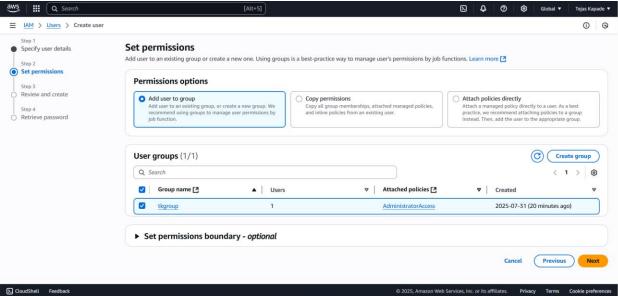AWS Documentation. User and Group Creation
31-07-2025
Tejas Kapade

1. IAM User creation

○ Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

● I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

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 ⎘

Cancel   Next

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	○ Copy permissions	○ Attach policies directly
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.	Copy all group memberships, attached managed policies, and inline policies from an existing user.	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.

User groups (1/1)   ⟳ Create group

[Q Search   ]   ‹ 1 › ⚙

☑	Group name ⎘ ▲	Users ▽	Attached policies ⎘ ▽	Created ▽
☑	tkgroup	1	AdministratorAccess	2025-07-31 (20 minutes ago)

▶ Set permissions boundary - *optional*

Cancel   Previous   Next
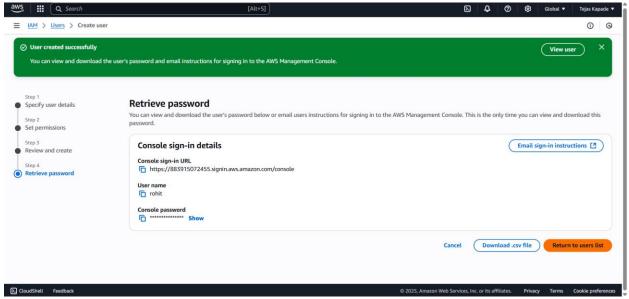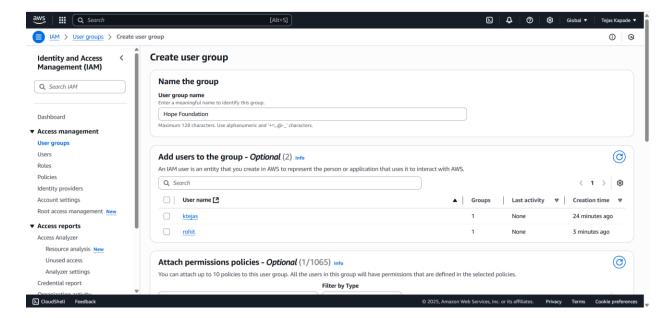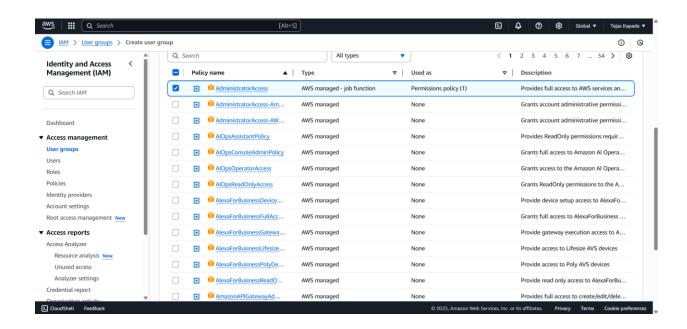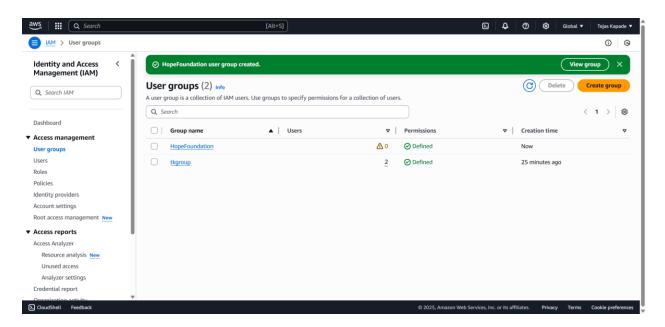
IMP: make sure to copy the console sign-in URL as shown above, which will be used to login in AWS UI.

2. Create group

IAM > User groups > Create user group

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
- Resource analysis New
- Unused access
- Analyzer settings
- Credential report
- Organization activity

Search | All types ▼ | < 1 2 3 4 5 6 7 ... 54 >

		Policy name	Type	Used as	Description
☑	⊞	AdministratorAccess	AWS managed - job function	Permissions policy (1)	Provides full access to AWS services an…
☐	⊞	AdministratorAccess-Am…	AWS managed	None	Grants account administrative permissi…
☐	⊞	AdministratorAccess-AW…	AWS managed	None	Grants account administrative permissi…
☐	⊞	AIOpsAssistantPolicy	AWS managed	None	Provides ReadOnly permissions requir…
☐	⊞	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…
☐	⊞	AlexaForBusinessDevice…	AWS managed	None	Provide device setup access to AlexaFo…
☐	⊞	AlexaForBusinessFullAcc…	AWS managed	None	Grants full access to AlexaForBusiness …
☐	⊞	AlexaForBusinessGatewa…	AWS managed	None	Provide gateway execution access to A…
☐	⊞	AlexaForBusinessLifesize…	AWS managed	None	Provide access to Lifesize AVS devices
☐	⊞	AlexaForBusinessPolyDe…	AWS managed	None	Provide access to Poly AVS devices
☐	⊞	AlexaForBusinessReadO…	AWS managed	None	Provide read only access to AlexaForBu…
☐	⊞	AmazonAPIGatewayAd…	AWS managed	None	Provides full access to create/edit/dele…

IAM > User groups

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
- Resource analysis New
- Unused access
- Analyzer settings
- Credential report
- Organization activity

✓ HopeFoundation user group created. | View group | ✕

User groups (2) Info

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

Delete | Create group

Search | < 1 >

	Group name ▲	Users ▼	Permissions ▼	Creation time ▼
☐	HopeFoundation	⚠ 0	✓ Defined	Now
☐	tkgroup	2	✓ Defined	25 minutes ago

3. Select users to add in group

IAM > Users

Identity and Access Management (IAM)

Search IAM

Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management **New**

Access reports
Access Analyzer
Resource analysis **New**
Unused access
Analyzer settings
Credential report

⊘ MergedGroup user group created.   [View group] ✕

Users (4) Info

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

[Delete] [Create user]

☐	User name ▲	Path ▽	Groups ▽	Last activity ▽	MFA ▽	Password age ▽	Console last sign-in ▽	A
☐	hope1	/	2	-	-	◠	-	-
☐	hope2	/	1	-	-	◠	-	-
☐	ktejas	/	2	-	-	◠	-	-
☐	rohit	/	1	-	-	◠	-	-