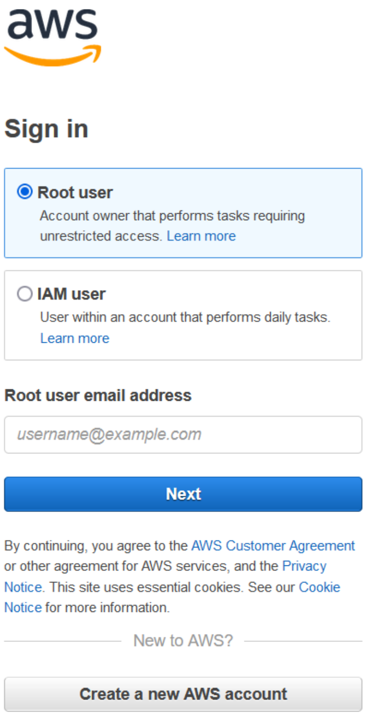
CREATE USERS FOR ROOT ACCOUNT:

Go to https://aws.amazon.com/console/ and login using the root account.



Sign in

● Root user
Account owner that performs tasks requiring unrestricted access. Learn more

○ IAM user
User within an account that performs daily tasks. Learn more

Root user email address

username@example.com

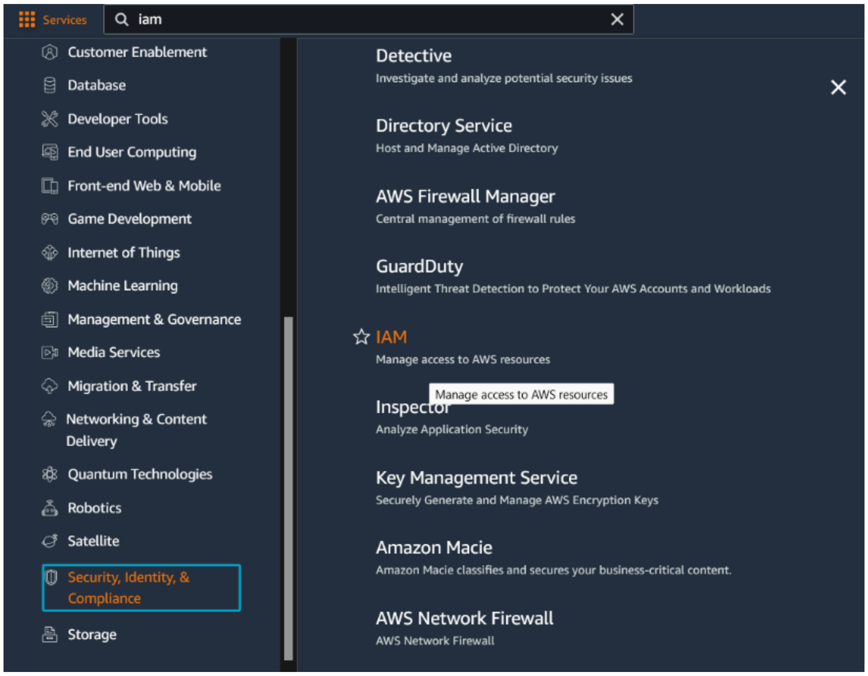
Next

By continuing, you agree to the AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.

New to AWS?

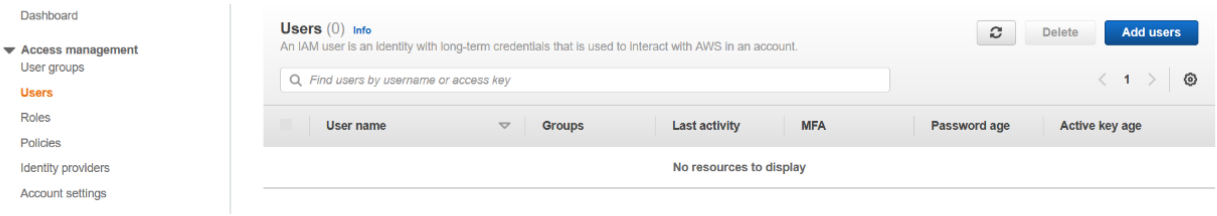
Create a new AWS account

In services, select **Security, Identity & Compliace,** and select **IAM.**



Services
iam
Customer Enablement
Database
Developer Tools
End User Computing
Front-end Web & Mobile
Game Development
Internet of Things
Machine Learning
Management & Governance
Media Services
Migration & Transfer
Networking & Content Delivery
Quantum Technologies
Robotics
Satellite
Security, Identity, & Compliance
Storage
Detective
Investigate and analyze potential security issues
Directory Service
Host and Manage Active Directory
AWS Firewall Manager
Central management of firewall rules
GuardDuty
Intelligent Threat Detection to Protect Your AWS Accounts and Workloads
IAM
Manage access to AWS resources
Manage access to AWS resources
Inspector
Analyze Application Security
Key Management Service
Securely Generate and Manage AWS Encryption Keys
Amazon Macie
Amazon Macie classifies and secures your business-critical content.
AWS Network Firewall
AWS Network Firewall

Under Dashboard, under **Access Management,** select **Users**. Click on **Create Users.**



Users (0) Info

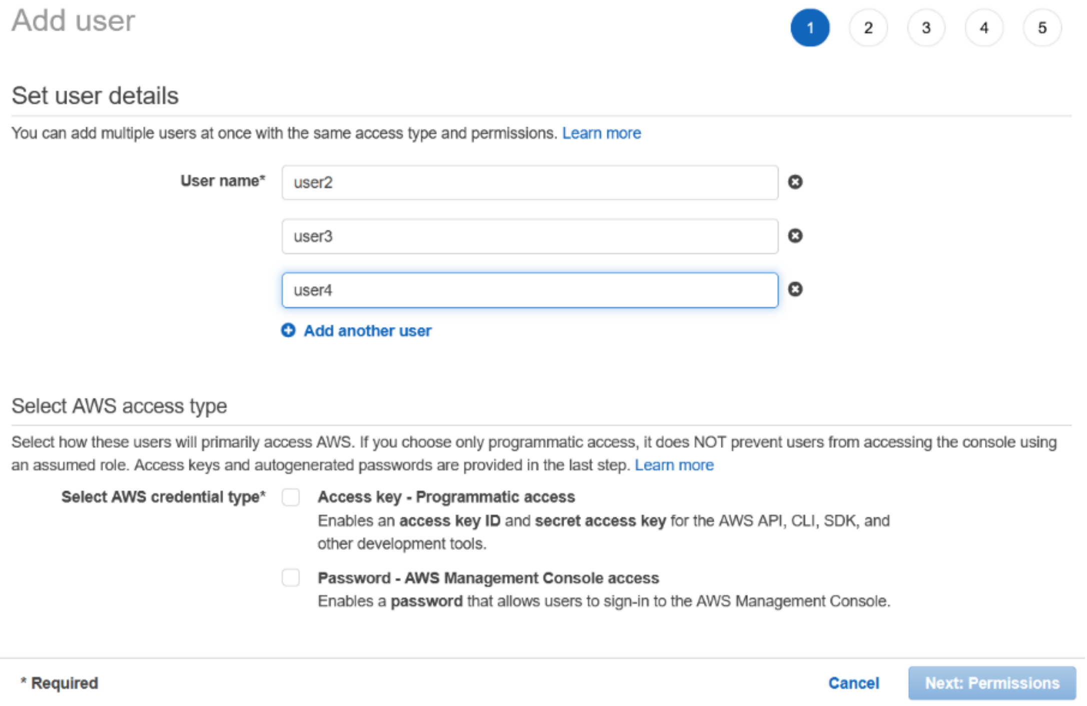
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Find users by username or access key

User name	Groups	Last activity	MFA	Password age	Active key age

No resources to display

Add all the User Names.



Add user

Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* user2

user3

user4

Add another user

Select AWS access type

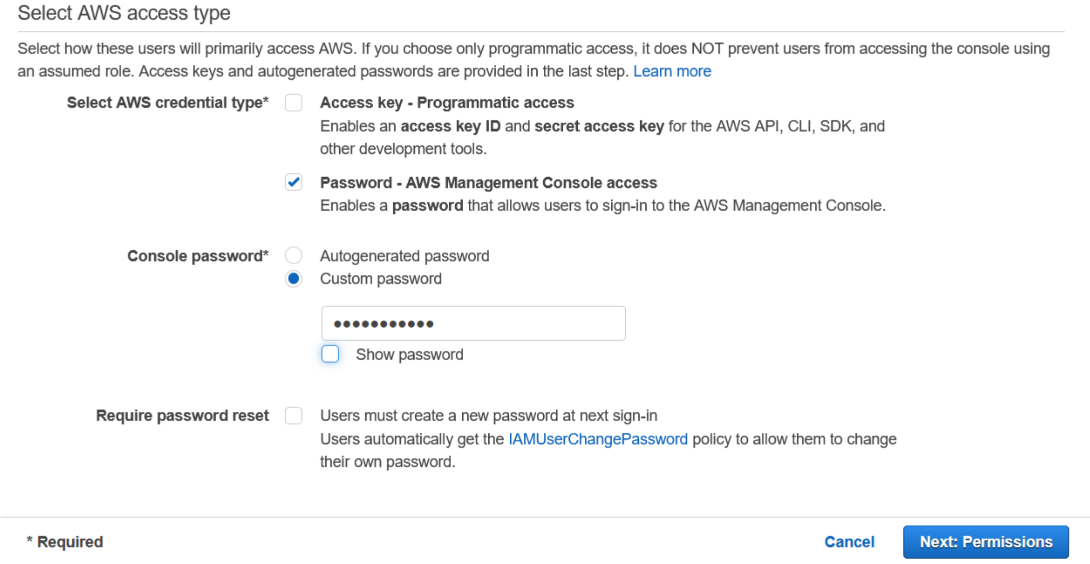
Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. Learn more

Select AWS credential type* □ **Access key - Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

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

* Required

In **Select AWS access type**, chose either access key or password.



Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. Learn more

Select AWS credential type* □ **Access key - Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

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

Console password* ○ Autogenerated password
● Custom password

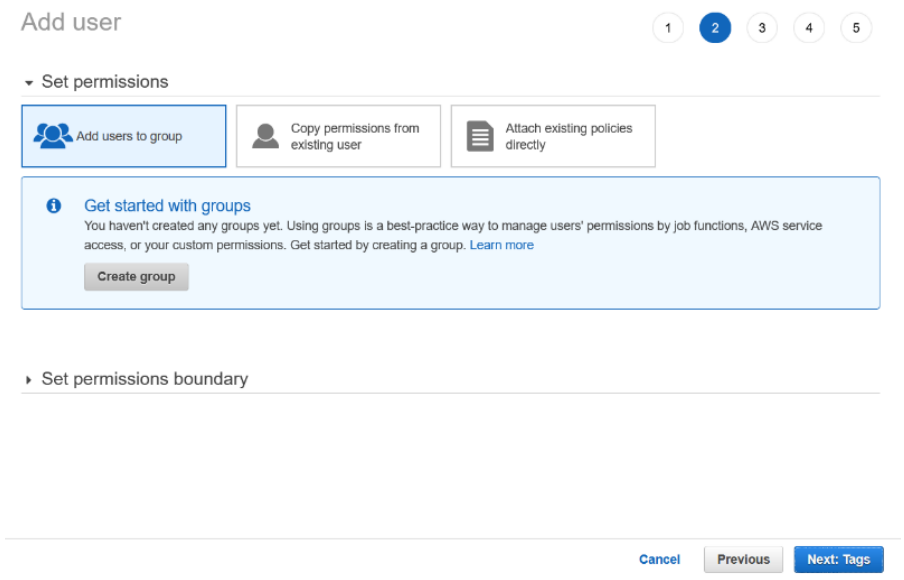
●●●●●●●●●●●

□ Show password

Require password reset □ Users must create a new password at next sign-in
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

* Required

To add all the users in a group, create a group, and give permissions. Here, we’re giving S3 full access permissions to our group.



Add user

Set permissions

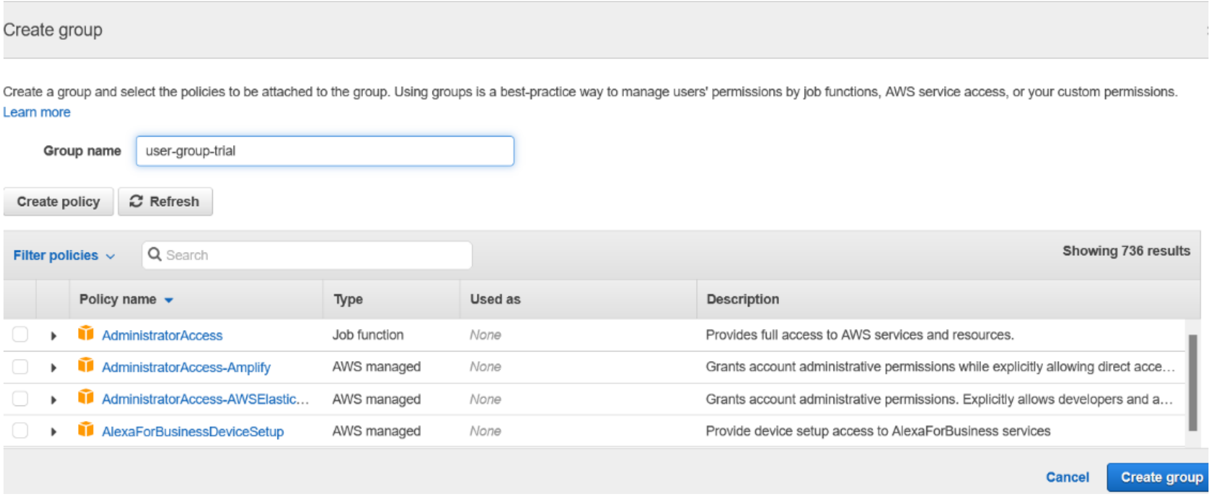
Add users to group
Copy permissions from existing user
Attach existing policies directly

Get started with groups

You haven't created any groups yet. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Get started by creating a group. Learn more

Set permissions boundary

Cancel
Previous
Next: Tags



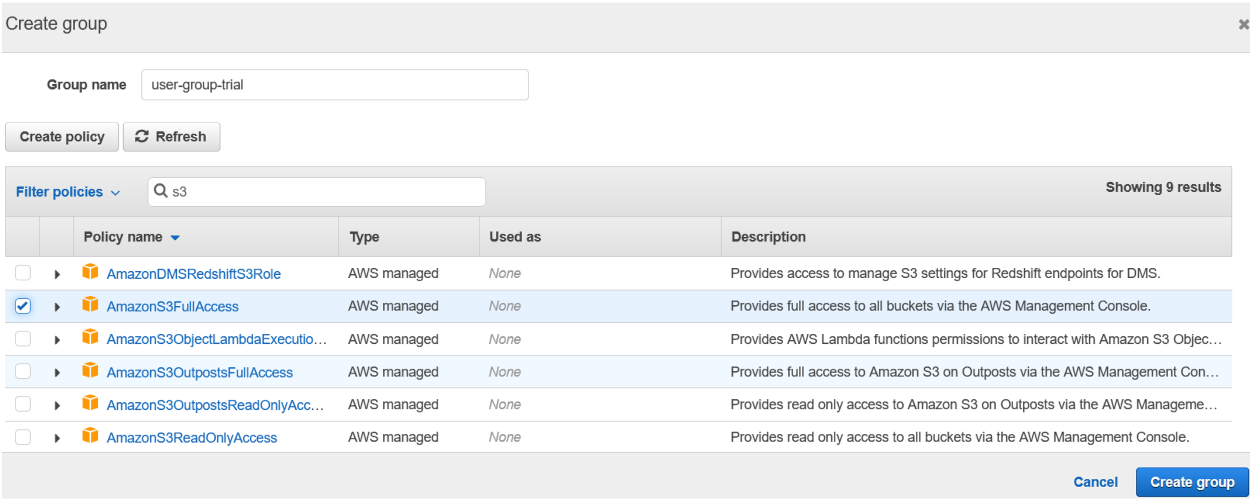
Create group

Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Learn more

Group name: user-group-trial

Showing 736 results

		Policy name	Type	Used as	Description
□	▸	AdministratorAccess	Job function	None	Provides full access to AWS services and resources.
□	▸	AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permissions while explicitly allowing direct acce…
□	▸	AdministratorAccess-AWSElastic…	AWS managed	None	Grants account administrative permissions. Explicitly allows developers and a…
□	▸	AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaForBusiness services



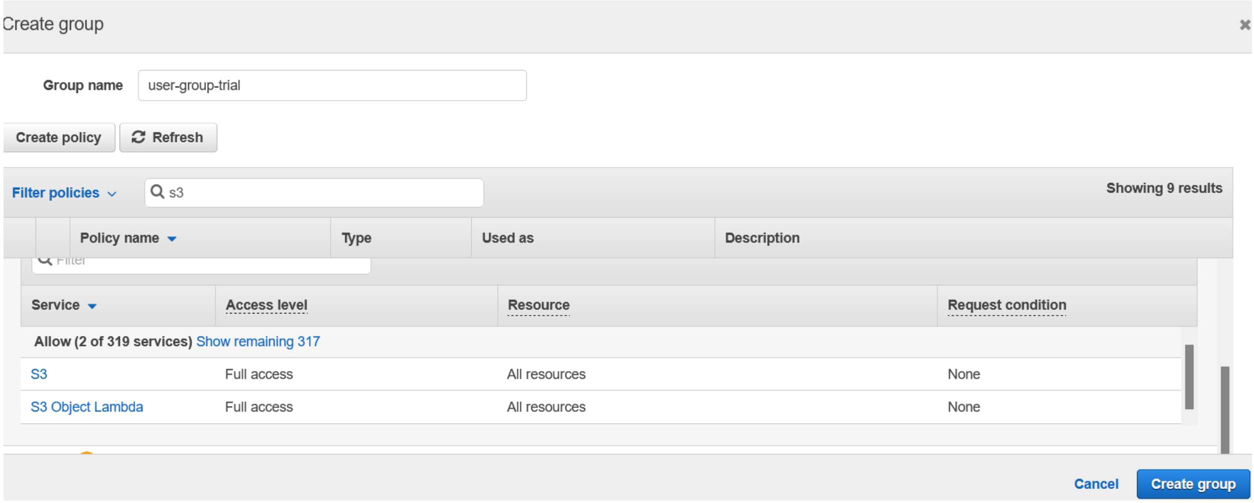
Create group

Group name: user-group-trial

Search: s3

Showing 9 results

		Policy name	Type	Used as	Description
□	▸	AmazonDMSRedshiftS3Role	AWS managed	None	Provides access to manage S3 settings for Redshift endpoints for DMS.
☑	▸	AmazonS3FullAccess	AWS managed	None	Provides full access to all buckets via the AWS Management Console.
□	▸	AmazonS3ObjectLambdaExecutio…	AWS managed	None	Provides AWS Lambda functions permissions to interact with Amazon S3 Objec…
□	▸	AmazonS3OutpostsFullAccess	AWS managed	None	Provides full access to Amazon S3 on Outposts via the AWS Management Con…
□	▸	AmazonS3OutpostsReadOnlyAcc…	AWS managed	None	Provides read only access to Amazon S3 on Outposts via the AWS Manageme…
□	▸	AmazonS3ReadOnlyAccess	AWS managed	None	Provides read only access to all buckets via the AWS Management Console.



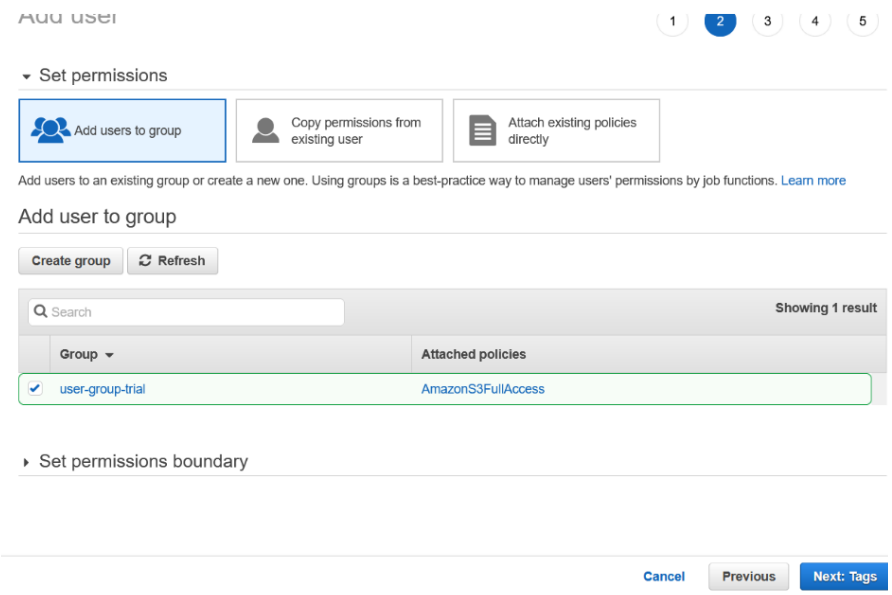
Create group

Group name: user-group-trial

s3

	Policy name	Type	Used as	Description

Service	Access level	Resource	Request condition
Allow (2 of 319 services) Show remaining 317			
S3	Full access	All resources	None
S3 Object Lambda	Full access	All resources	None



Add user

Set permissions

Add users to group
Copy permissions from existing user
Attach existing policies directly

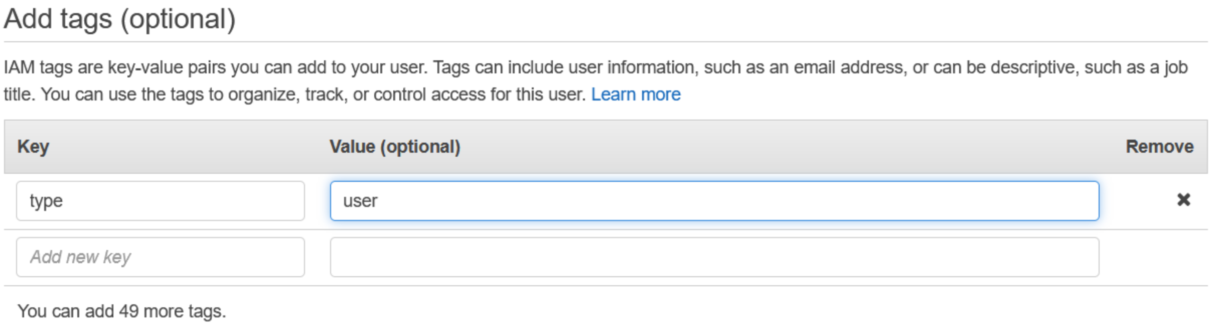
Add users to an existing group or create a new one. Using groups is a best-practice way to manage users' permissions by job functions. Learn more

Add user to group

	Group	Attached policies
☑	user-group-trial	AmazonS3FullAccess

Set permissions boundary

Add tags, which are optional.



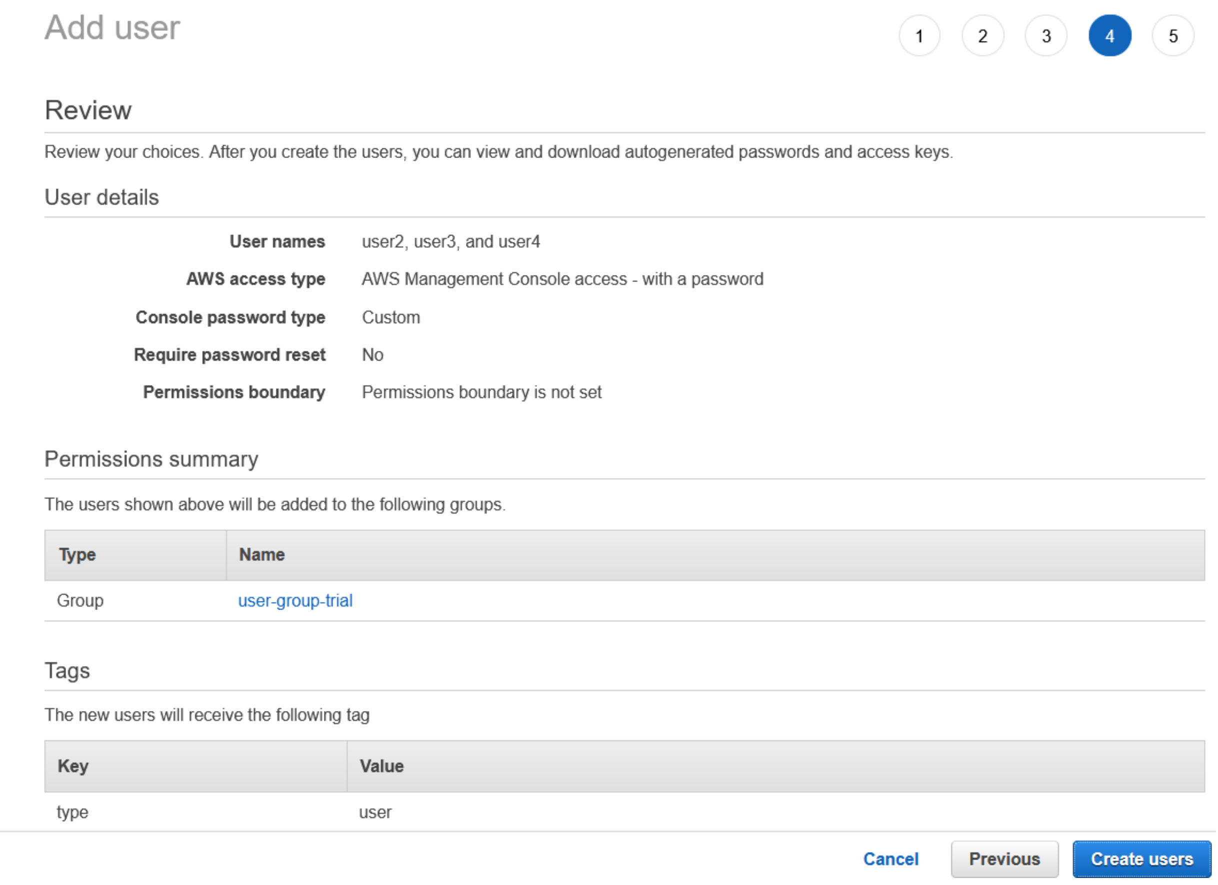
Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. Learn more

Key	Value (optional)	Remove
type	user	✖
Add new key		

You can add 49 more tags.

Review and click on **Create Users.**



Add user

Review

Review your choices. After you create the users, you can view and download autogenerated passwords and access keys.

User details

User names	user2, user3, and user4
AWS access type	AWS Management Console access - with a password
Console password type	Custom
Require password reset	No
Permissions boundary	Permissions boundary is not set

Permissions summary

The users shown above will be added to the following groups.

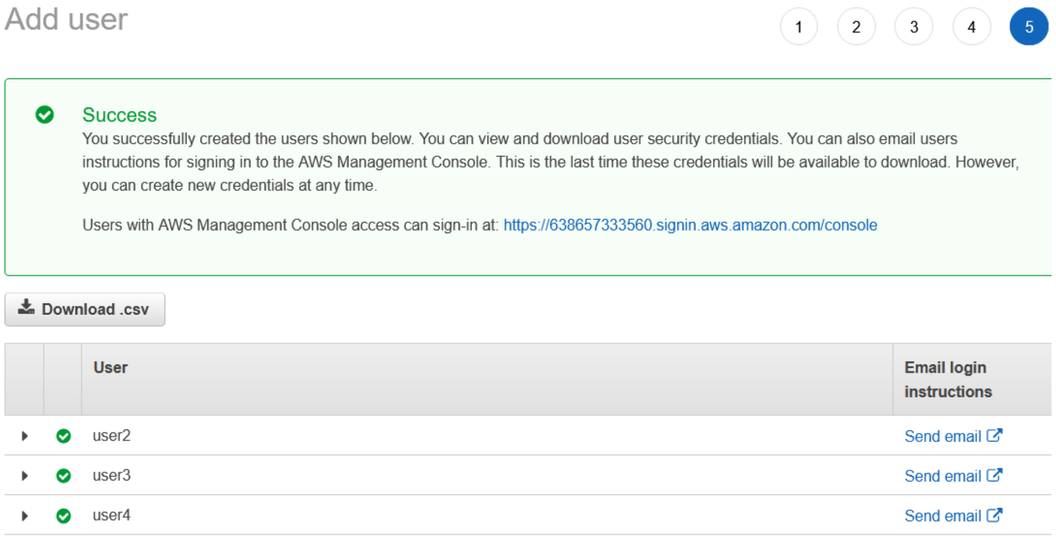
Type	Name
Group	user-group-trial

Tags

The new users will receive the following tag

Key	Value
type	user

Our users in a group with policies are now created!



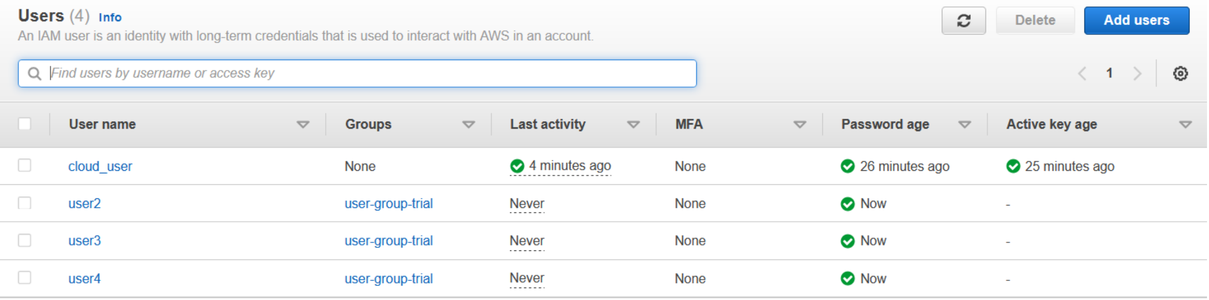
Add user

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://638657333560.signin.aws.amazon.com/console

		User	Email login instructions
▸	✓	user2	Send email
▸	✓	user3	Send email
▸	✓	user4	Send email



Users (4) Info

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

□	User name	Groups	Last activity	MFA	Password age	Active key age
□	cloud_user	None	✓ 4 minutes ago	None	✓ 26 minutes ago	✓ 25 minutes ago
□	user2	user-group-trial	Never	None	✓ Now	-
□	user3	user-group-trial	Never	None	✓ Now	-
□	user4	user-group-trial	Never	None	✓ Now	-