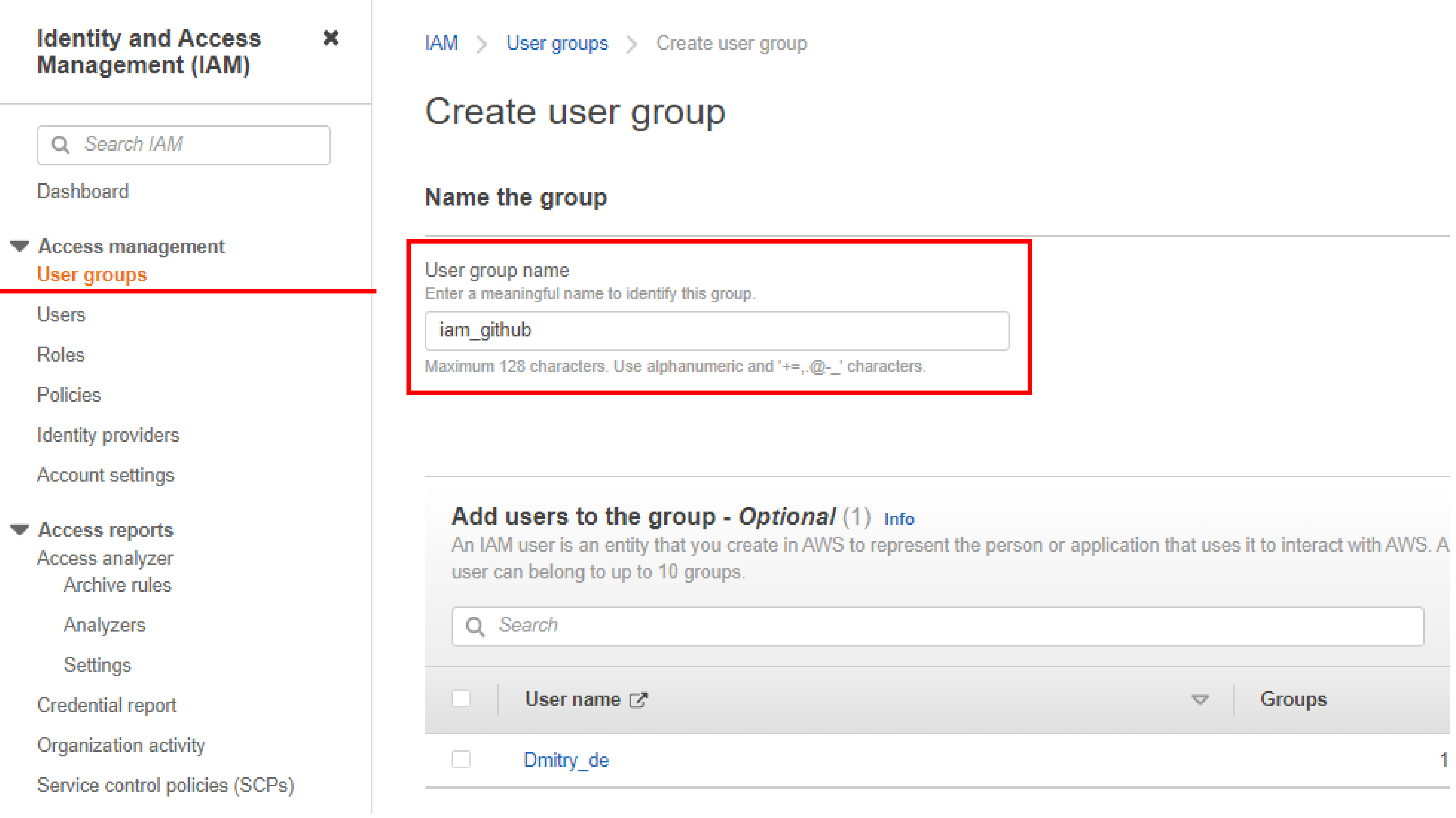
1. Create Group Name:



Identity and Access Management (IAM) ✖

Search IAM

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)

IAM > User groups > Create user group

Create user group

Name the group

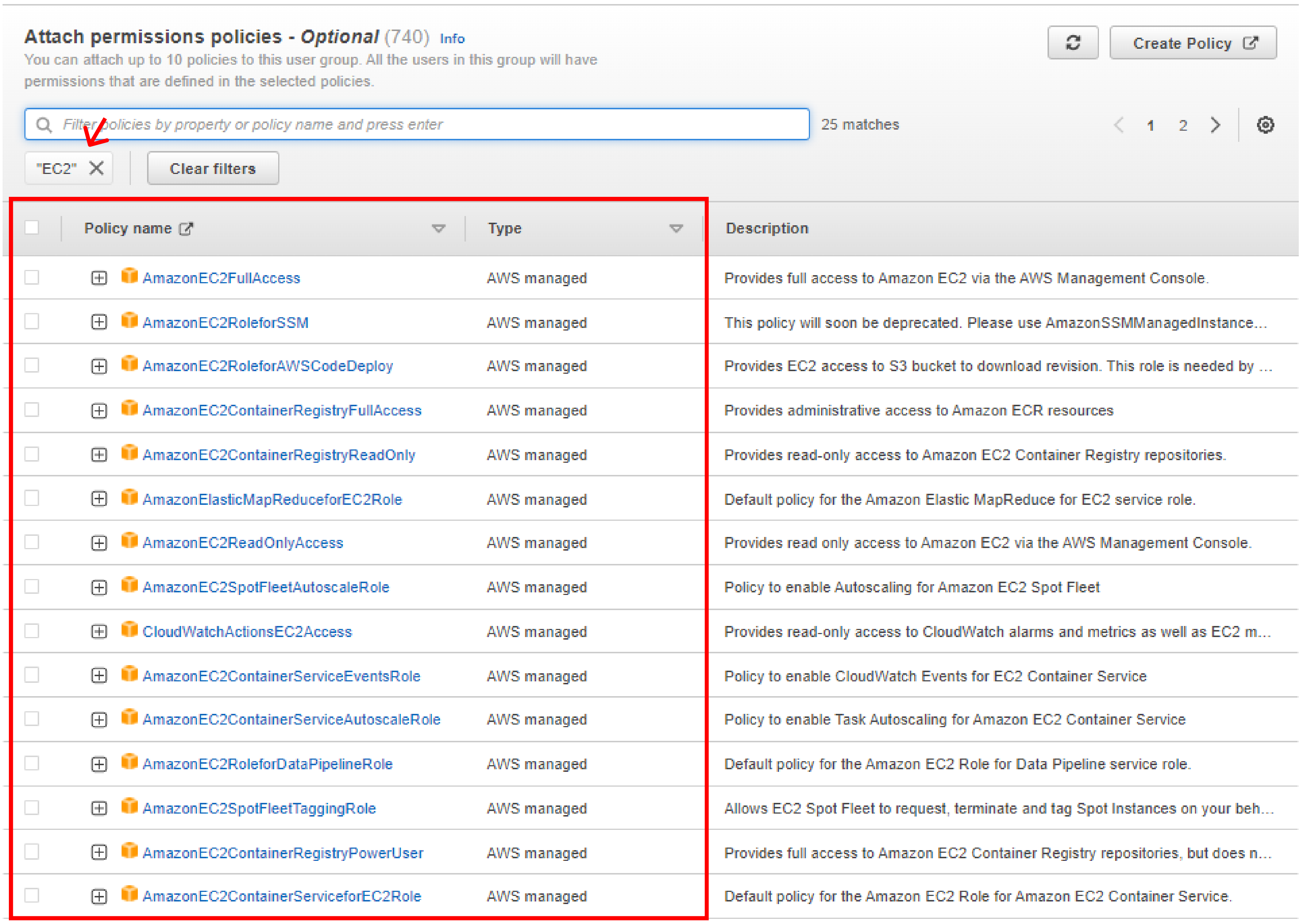
User group name
Enter a meaningful name to identify this group.
iam_github
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Add users to the group - *Optional* (1) 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. A user can belong to up to 10 groups.

Search

□	User name	Groups
□	Dmitry_de	1

2. Choose Policies:



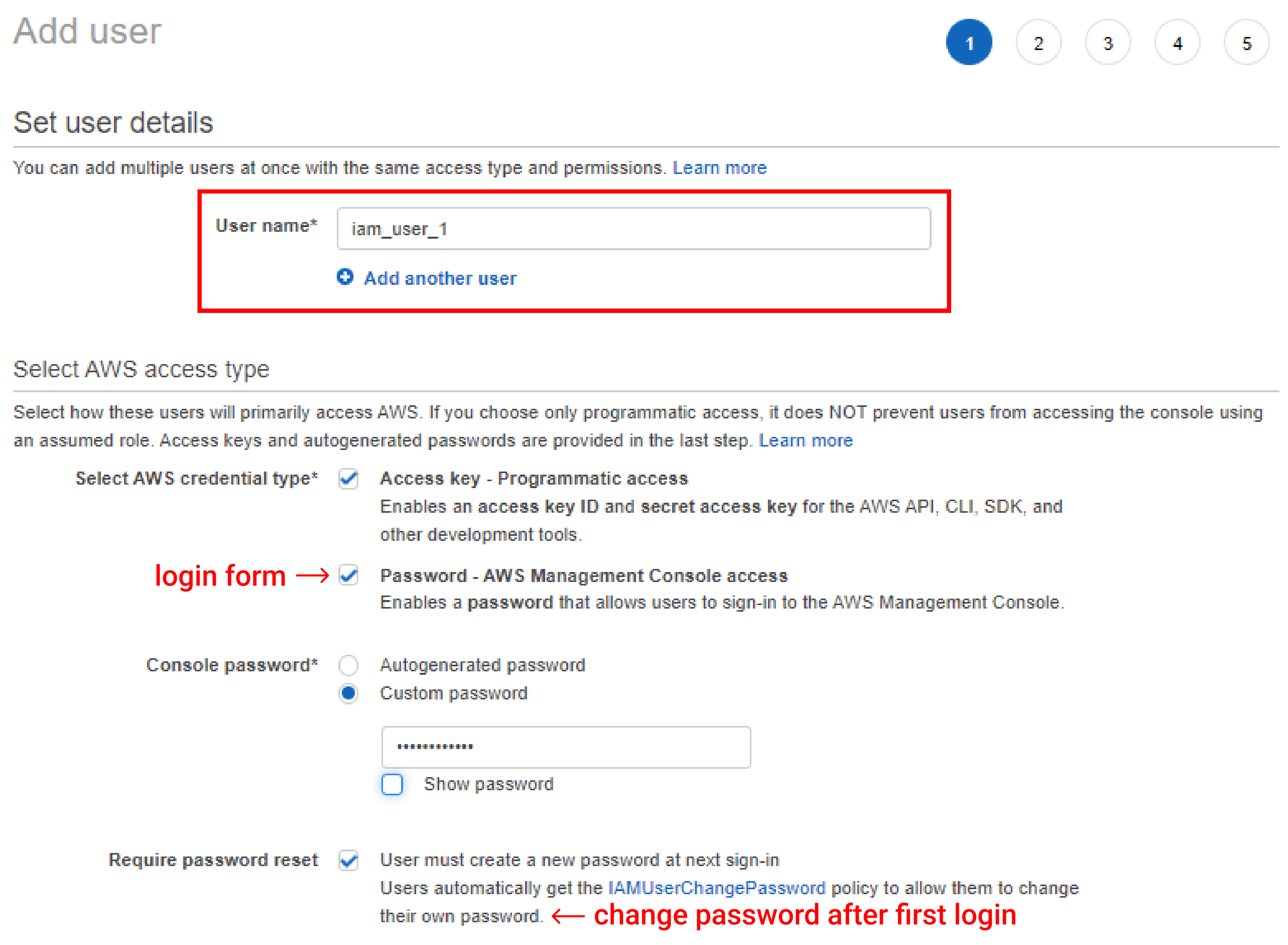
Attach permissions policies - *Optional* (740) Info
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter policies by property or policy name and press enter — 25 matches — < 1 2 >

"EC2" ✕ Clear filters

□	Policy name	Type	Description
□	AmazonEC2FullAccess	AWS managed	Provides full access to Amazon EC2 via the AWS Management Console.
□	AmazonEC2RoleforSSM	AWS managed	This policy will soon be deprecated. Please use AmazonSSMManagedInstance…
□	AmazonEC2RoleforAWSCodeDeploy	AWS managed	Provides EC2 access to S3 bucket to download revision. This role is needed by …
□	AmazonEC2ContainerRegistryFullAccess	AWS managed	Provides administrative access to Amazon ECR resources
□	AmazonEC2ContainerRegistryReadOnly	AWS managed	Provides read-only access to Amazon EC2 Container Registry repositories.
□	AmazonElasticMapReduceforEC2Role	AWS managed	Default policy for the Amazon Elastic MapReduce for EC2 service role.
□	AmazonEC2ReadOnlyAccess	AWS managed	Provides read only access to Amazon EC2 via the AWS Management Console.
□	AmazonEC2SpotFleetAutoscaleRole	AWS managed	Policy to enable Autoscaling for Amazon EC2 Spot Fleet
□	CloudWatchActionsEC2Access	AWS managed	Provides read-only access to CloudWatch alarms and metrics as well as EC2 m…
□	AmazonEC2ContainerServiceEventsRole	AWS managed	Policy to enable CloudWatch Events for EC2 Container Service
□	AmazonEC2ContainerServiceAutoscaleRole	AWS managed	Policy to enable Task Autoscaling for Amazon EC2 Container Service
□	AmazonEC2RoleforDataPipelineRole	AWS managed	Default policy for the Amazon EC2 Role for Data Pipeline service role.
□	AmazonEC2SpotFleetTaggingRole	AWS managed	Allows EC2 Spot Fleet to request, terminate and tag Spot Instances on your beh…
□	AmazonEC2ContainerRegistryPowerUser	AWS managed	Provides full access to Amazon EC2 Container Registry repositories, but does n…
□	AmazonEC2ContainerServiceforEC2Role	AWS managed	Default policy for the Amazon EC2 Role for Amazon EC2 Container Service.

3. Add users:



Add user

Set user details

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

User name* iam_user_1

➕ 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

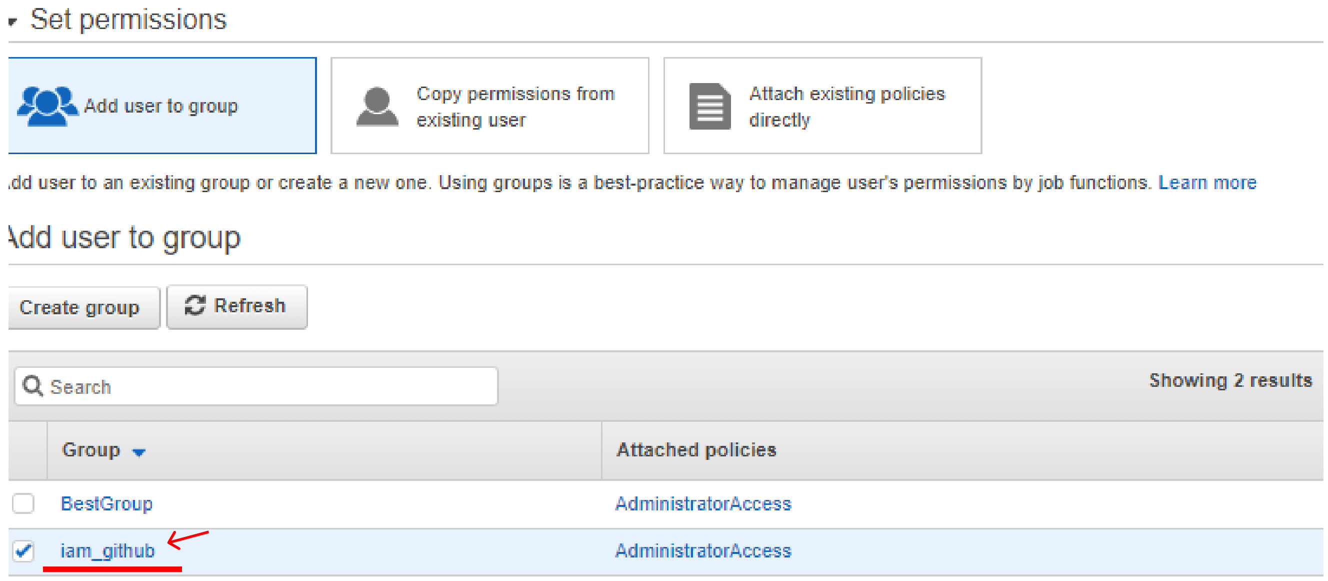
Select AWS credential type* ☑ **Access key - Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

login form → ☑ **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 ☑ User must create a new password at next sign-in
Users automatically get the IAMUserChangePassword policy to allow them to change their own password. ⟵ change password after first login

4. Users into group:



▾ Set permissions

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

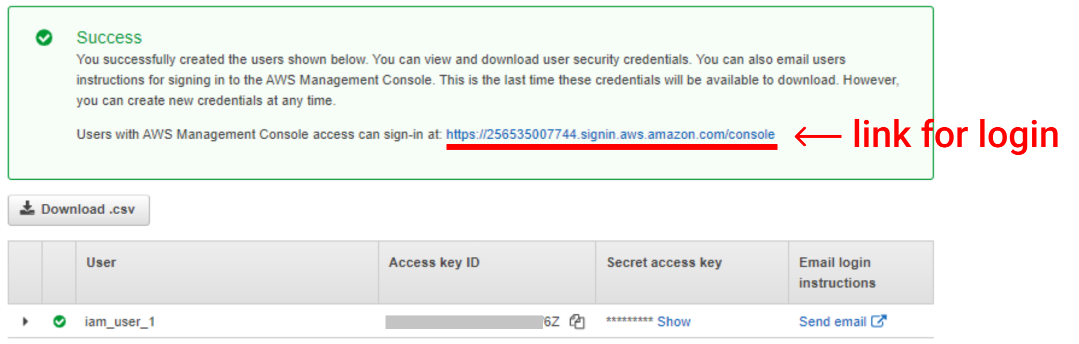
.dd user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

\dd user to group

Search — Showing 2 results

	Group	Attached policies
□	BestGroup	AdministratorAccess
☑	iam_github ←	AdministratorAccess

5. Success:



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://256535007744.signin.aws.amazon.com/console ⟵ link for login

		User	Access key ID	Secret access key	Email login instructions
▸	✓	iam_user_1	[redacted]6Z	********* Show	Send email