SkillAssure

AWS Fundamental

Principle of Least Privilege

Minimal Privilege

- The principles of least privilege is practise of limiting access to minimal level that will allow normal functioning.

- A user should only have access to data, hardware that they need, to be able to perform their assigned duties.

Use Case

Alice in an intern who has joined your organization as an intern System Administrator. Since your infrastructure is hosted in AWS, you need to give access to Alice to view the AWS console. What kind of Access will you give ?

- Share with her the ROOT Credentials of the AWS.
- Create a new user Alice with full Permission for everything.
- Create a new user Alice with ReadOnlyAccess.

It goes Deeper than Expected

A software developer wants to access an application server to see the logs. You being a system administrator, you need to provide him access. How will you give access?

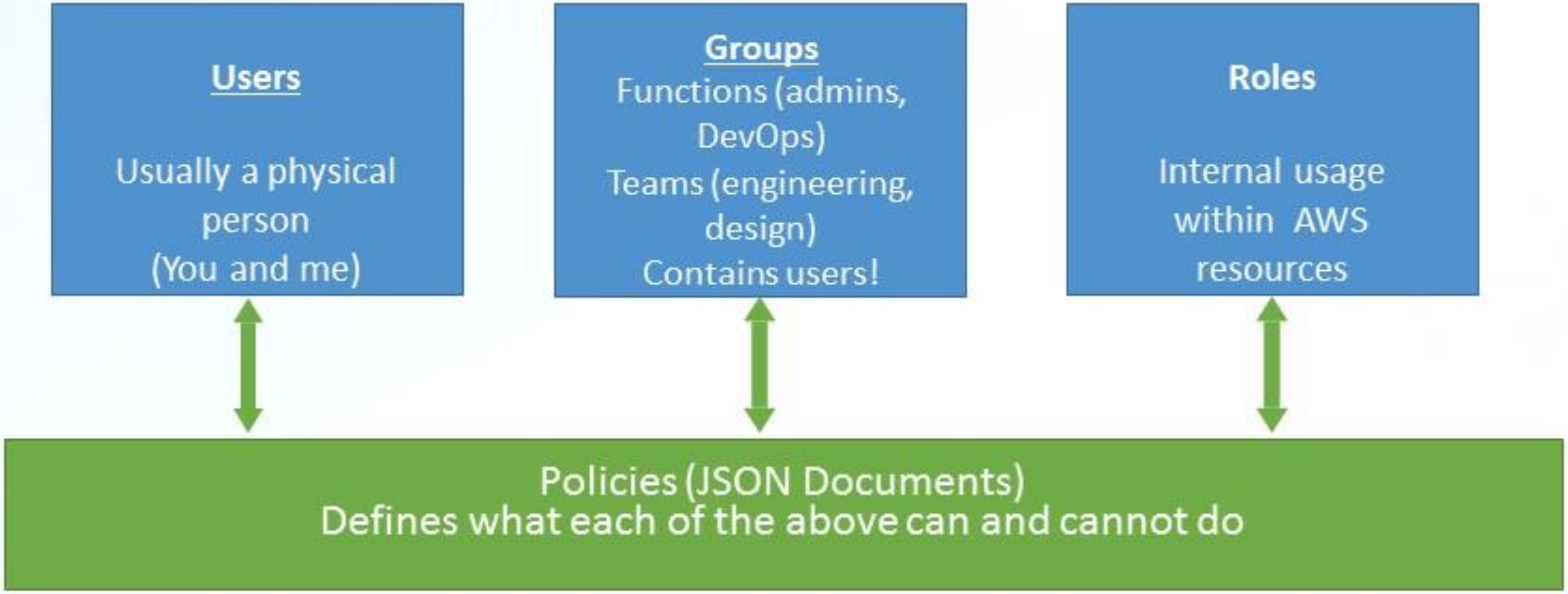
- Create the user with the user add command &Share credentials.
- Create the user with user add command and add him to sudoers list.
- Ask the developer on what log file he wants to access, verify if his access is justified and only allow him to have access to that specific log file and nothing else.

IAM Introduction

IAM Introduction

- IAM (Identity and Access Management)
- Your whole AWS security is there:
  - Users
  - Groups
  - Roles
- Root account should never be used (and shared)
- Users must be created with proper permissions
- IAM is at the center of AWS
- Policies are written in JSON (JavaScript Object Notation)

IAM Introduction



Users

Usually a physical person
(You and me)

Groups
Functions (admins, DevOps)
Teams (engineering, design)
Contains users!

Roles

Internal usage within AWS resources

Policies (JSON Documents)
Defines what each of the above can and cannot do

IAM Introduction

- IAM has a **global** view
- Permissions are governed by Policies (JSON)
- MFA (Multi Factor Authentication) can be setup
- IAM has predefined “managed policies”
- We’ll see IAM policies in details in the future
- It’s best to give users the minimal amount of permissions they need to perform their job (least privilege principles)

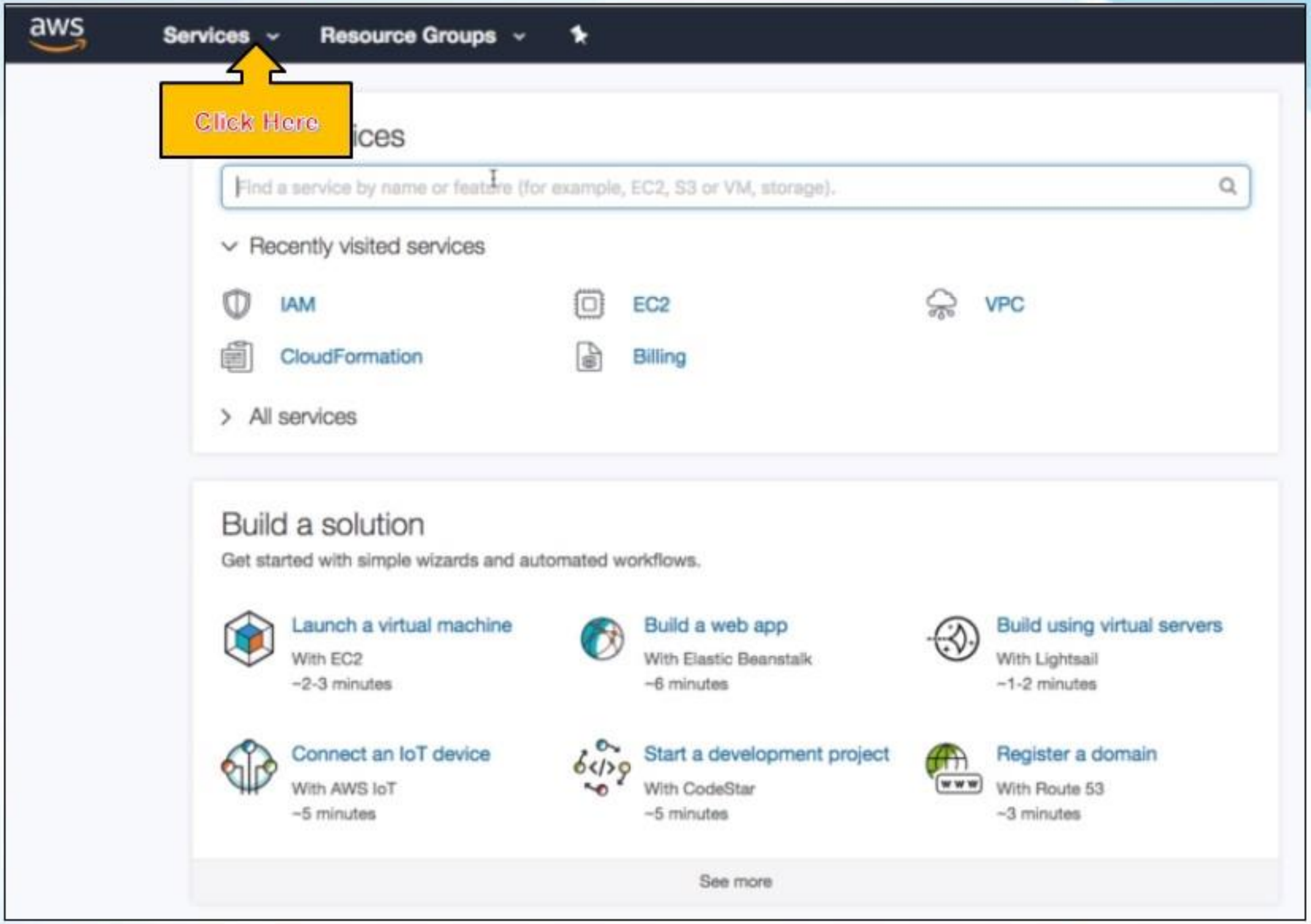
IAM Federation

- Big enterprises usually integrate their own repository of users with IAM
- This way, one can login into AWS using their company credentials
- Identity Federation uses the SAML standard (Active Directory)

IAM |0| Brain Dump

- One IAM **User** per PHYSICAL PERSON
- One IAM **Role** per Application
- IAM credentials should NEVER BE SHARED
- Never, ever, ever, ever, write IAM credentials in code. EVER.
- And even less, NEVER EVER EVER COMMIT YOUR IAM credentials
- **Never use the ROOT account except for initial setup.**
- **Never use ROOT IAM Credentials**

IAM Hands On

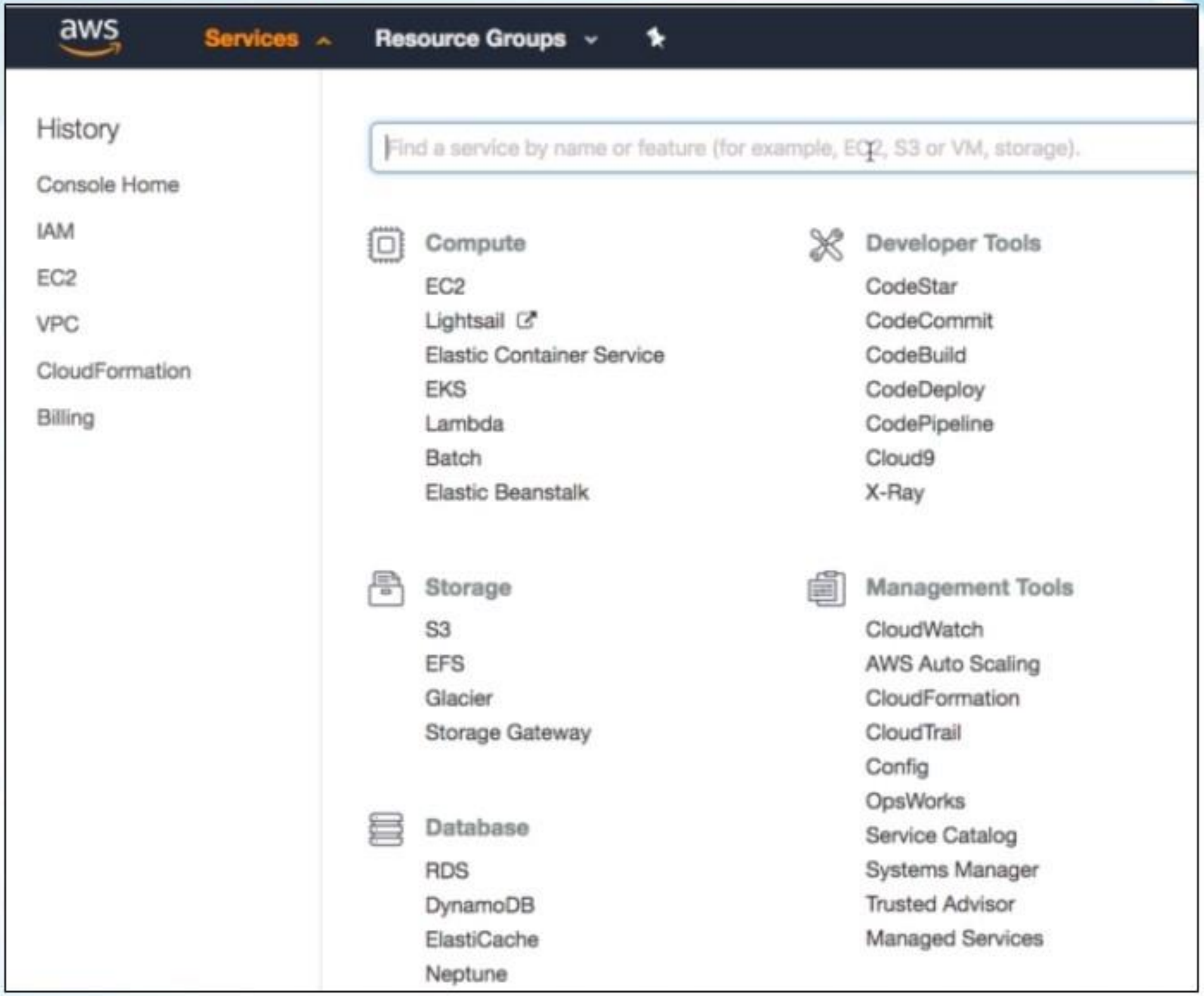


ices

Find a service by name or feature (for example, EC2, S3 or VM, storage).

Build a solution

Get started with simple wizards and automated workflows.



History

- Console Home
- IAM
- EC2
- VPC
- CloudFormation
- Billing

Find a service by name or feature (for example, EC2, S3 or VM, storage).

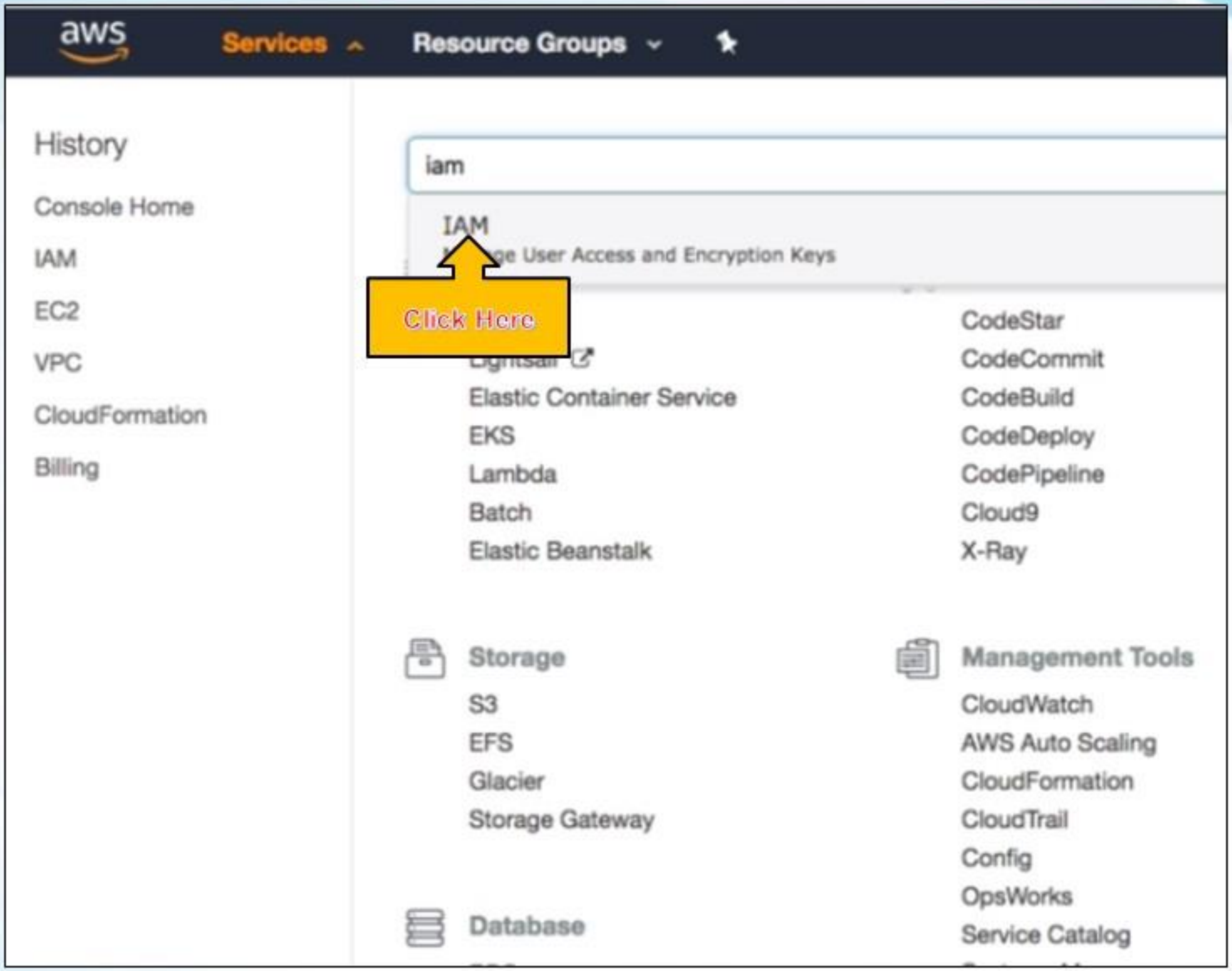
Compute
- EC2
- Lightsail
- Elastic Container Service
- EKS
- Lambda
- Batch
- Elastic Beanstalk

Storage
- S3
- EFS
- Glacier
- Storage Gateway

Database
- RDS
- DynamoDB
- ElastiCache
- Neptune

Developer Tools
- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- Cloud9
- X-Ray

Management Tools
- CloudWatch
- AWS Auto Scaling
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Systems Manager
- Trusted Advisor
- Managed Services

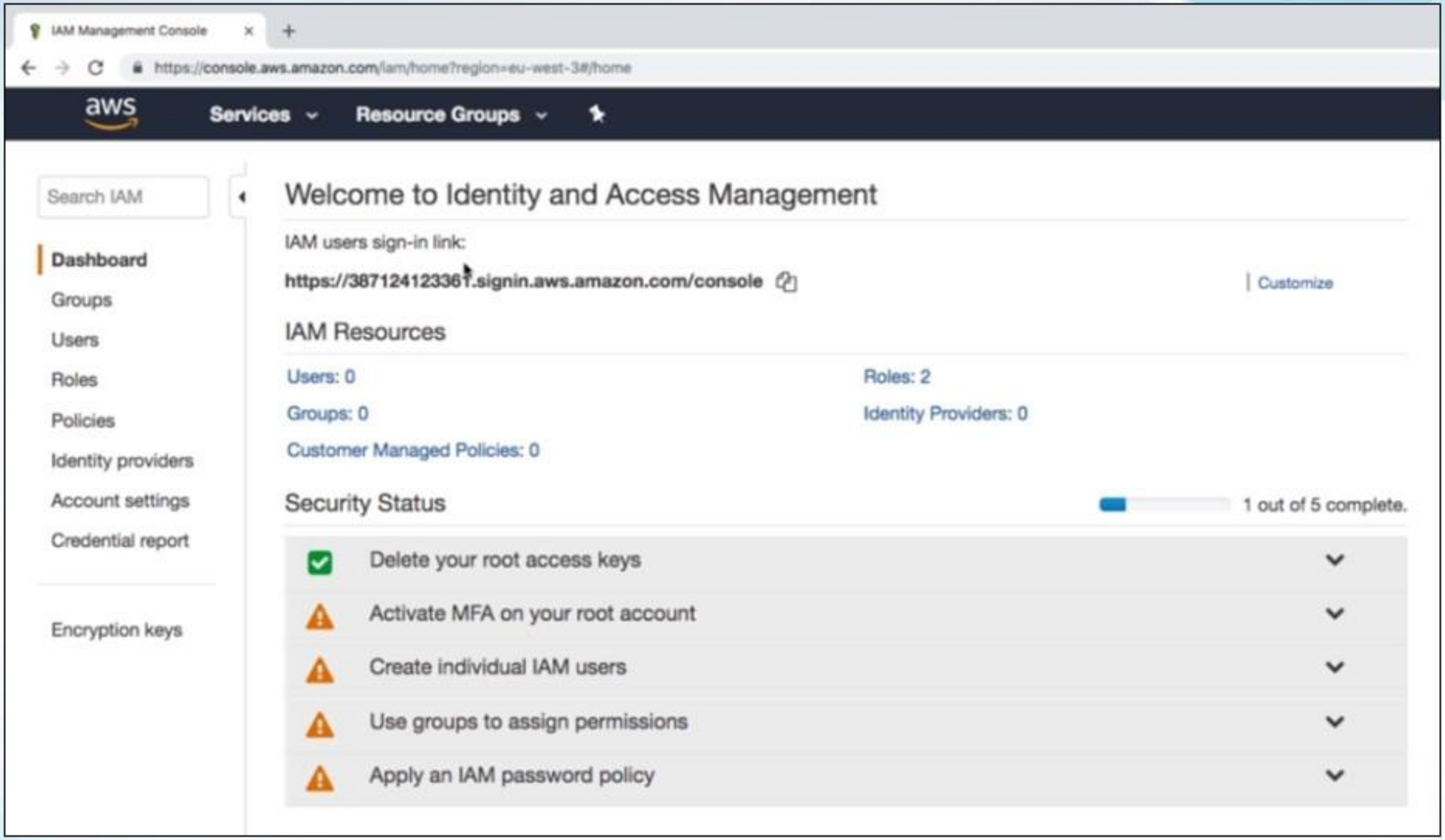


iam

IAM

Manage User Access and Encryption Keys

Click Here



Welcome to Identity and Access Management

IAM users sign-in link:

https://387124123361.signin.aws.amazon.com/console

IAM Resources

Users: 0

Groups: 0

Customer Managed Policies: 0

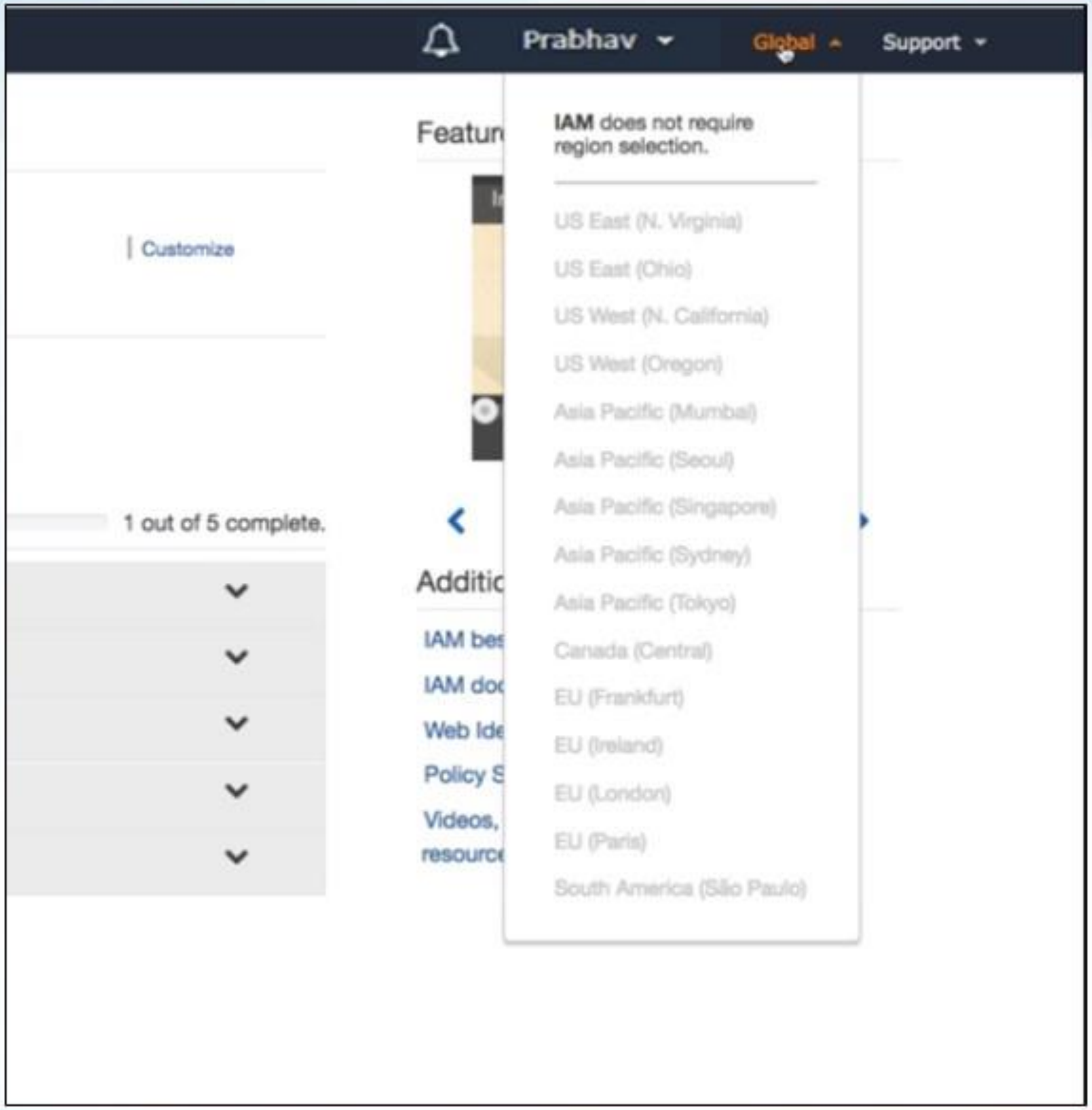
Roles: 2

Identity Providers: 0

Security Status

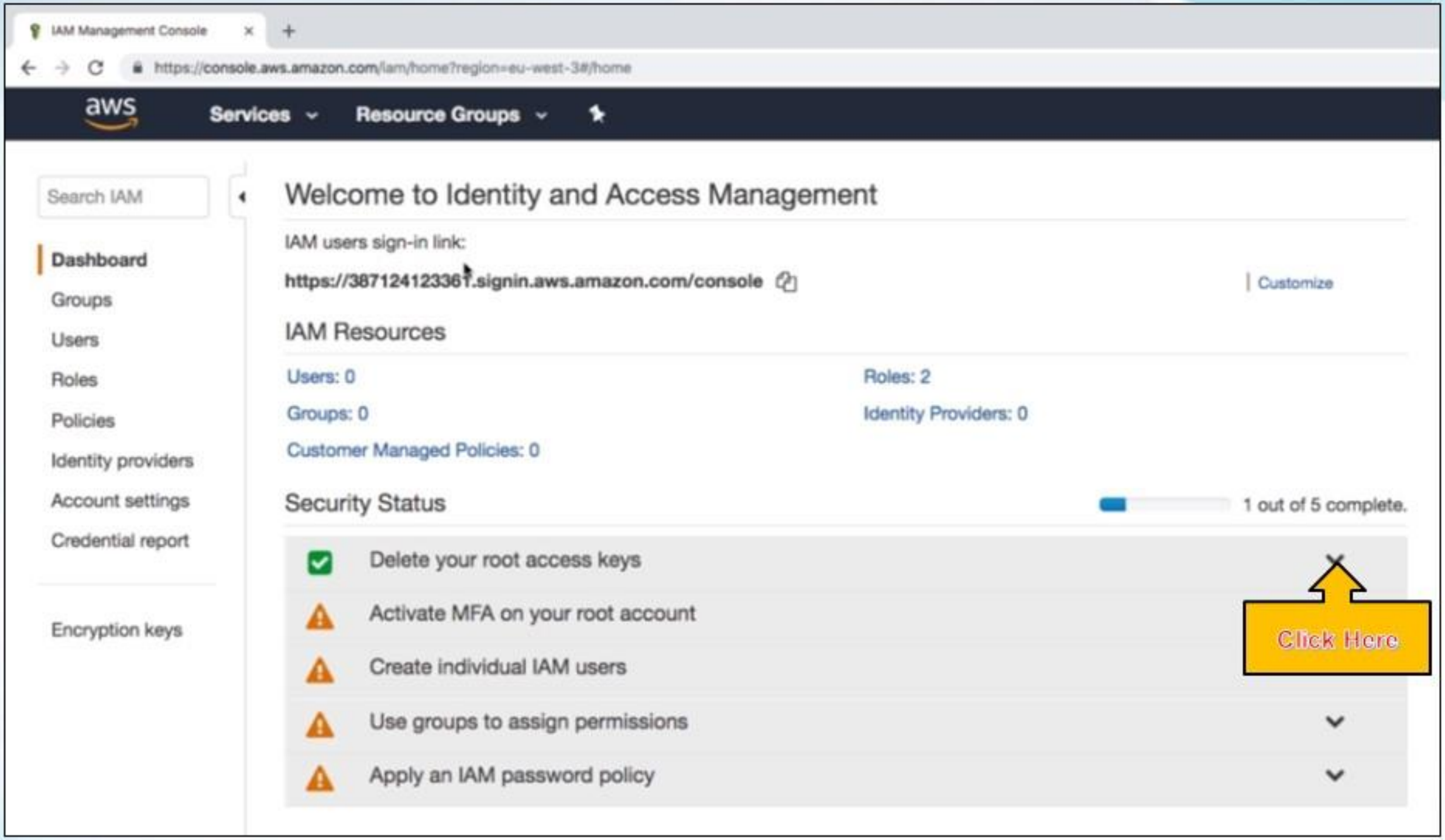
1 out of 5 complete.

- ☑ Delete your root access keys
- ⚠ Activate MFA on your root account
- ⚠ Create individual IAM users
- ⚠ Use groups to assign permissions
- ⚠ Apply an IAM password policy



IAM does not require region selection.

1 out of 5 complete.



Welcome to Identity and Access Management

IAM users sign-in link:

https://387124123361.signin.aws.amazon.com/console

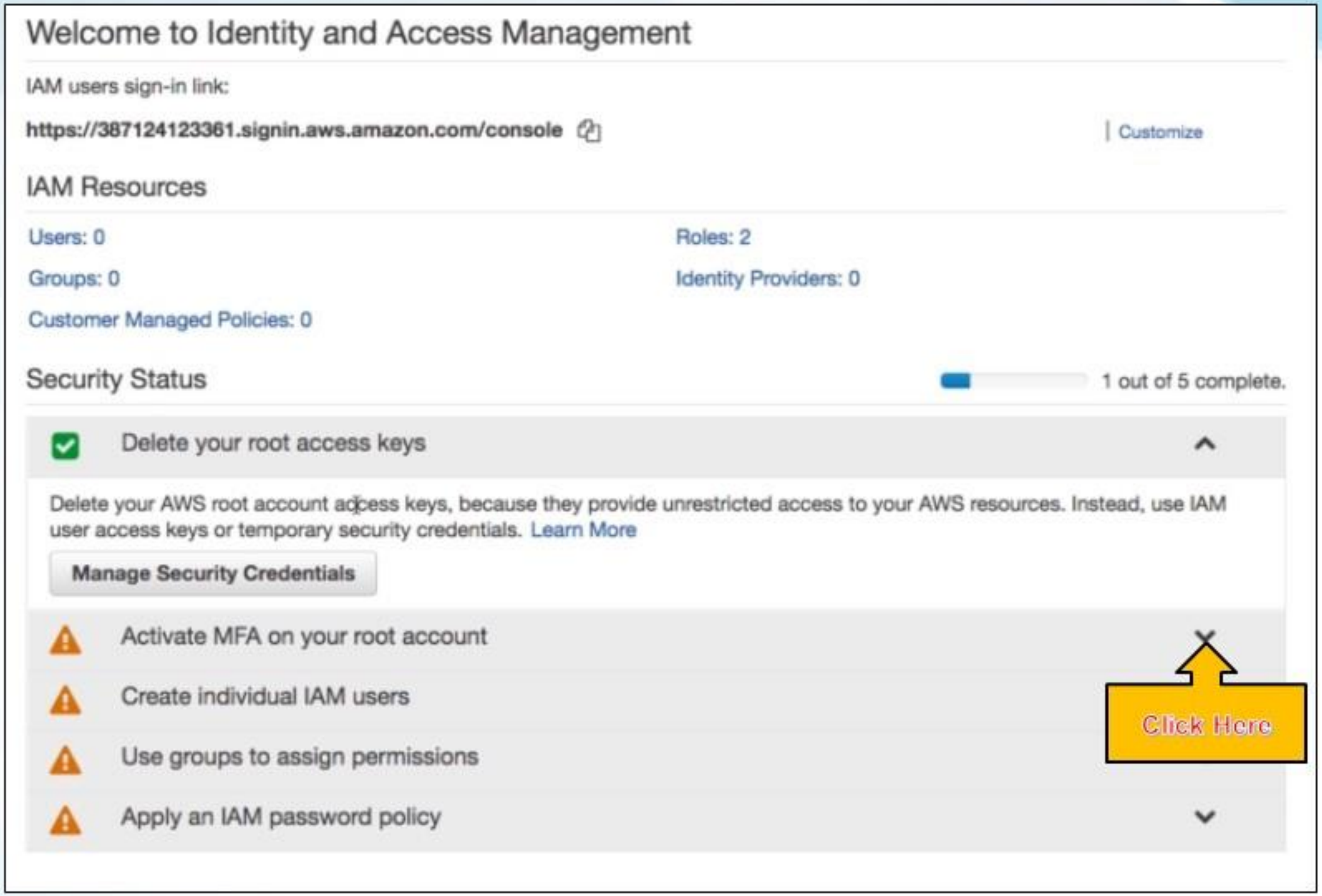
IAM Resources

Users: 0	Roles: 2
Groups: 0	Identity Providers: 0
Customer Managed Policies: 0	

Security Status

1 out of 5 complete.

- ✓ Delete your root access keys
- ⚠ Activate MFA on your root account
- ⚠ Create individual IAM users
- ⚠ Use groups to assign permissions
- ⚠ Apply an IAM password policy



Welcome to Identity and Access Management

IAM users sign-in link:

https://387124123361.signin.aws.amazon.com/console

IAM Resources

Users: 0

Roles: 2

Groups: 0

Identity Providers: 0

Customer Managed Policies: 0

Security Status

1 out of 5 complete.

☑ Delete your root access keys

Delete your AWS root account access keys, because they provide unrestricted access to your AWS resources. Instead, use IAM user access keys or temporary security credentials. Learn More

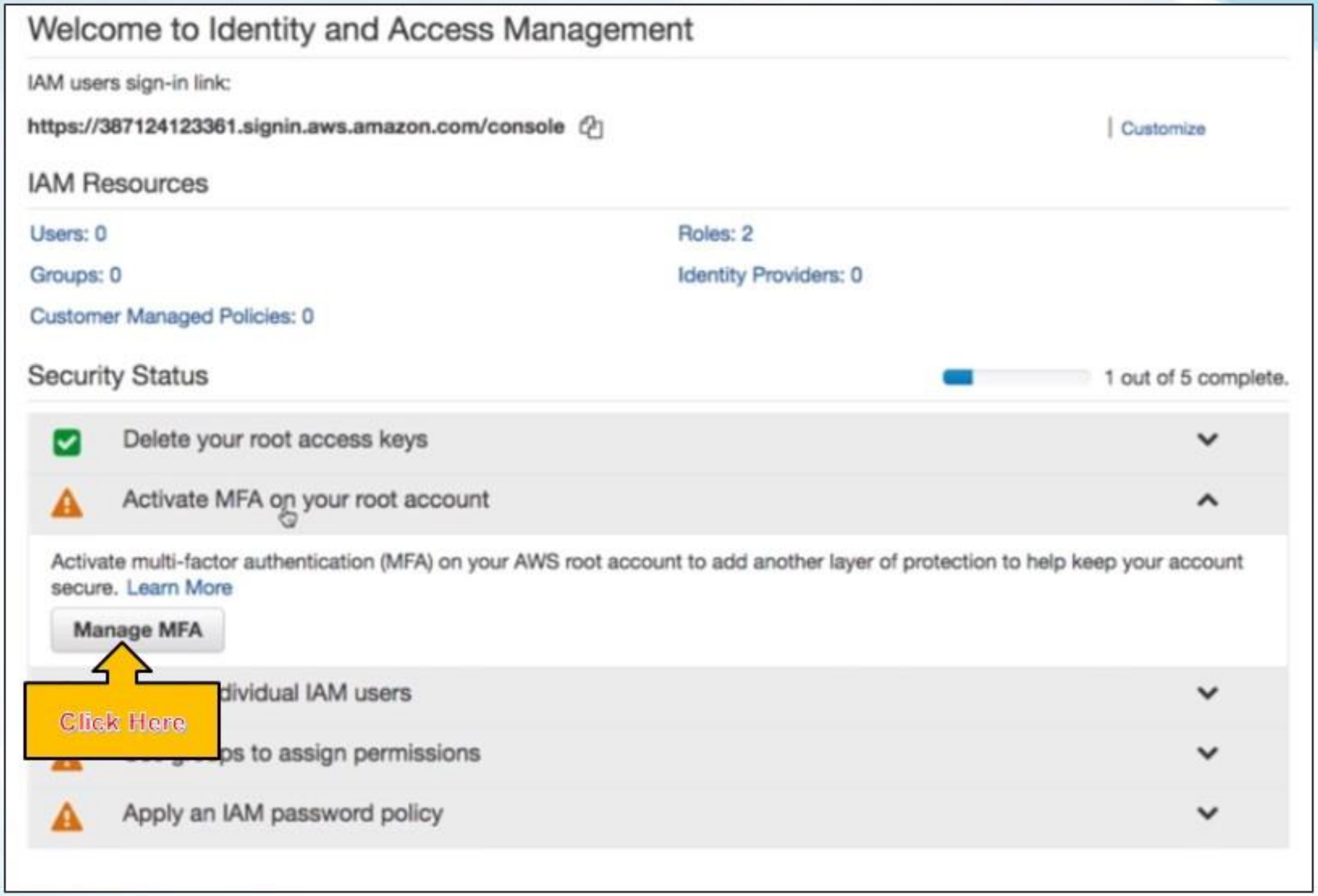
⚠ Activate MFA on your root account

⚠ Create individual IAM users

⚠ Use groups to assign permissions

⚠ Apply an IAM password policy

Click Here



Welcome to Identity and Access Management

IAM users sign-in link:

https://387124123361.signin.aws.amazon.com/console | Customize

IAM Resources

Users: 0	Roles: 2
Groups: 0	Identity Providers: 0
Customer Managed Policies: 0	

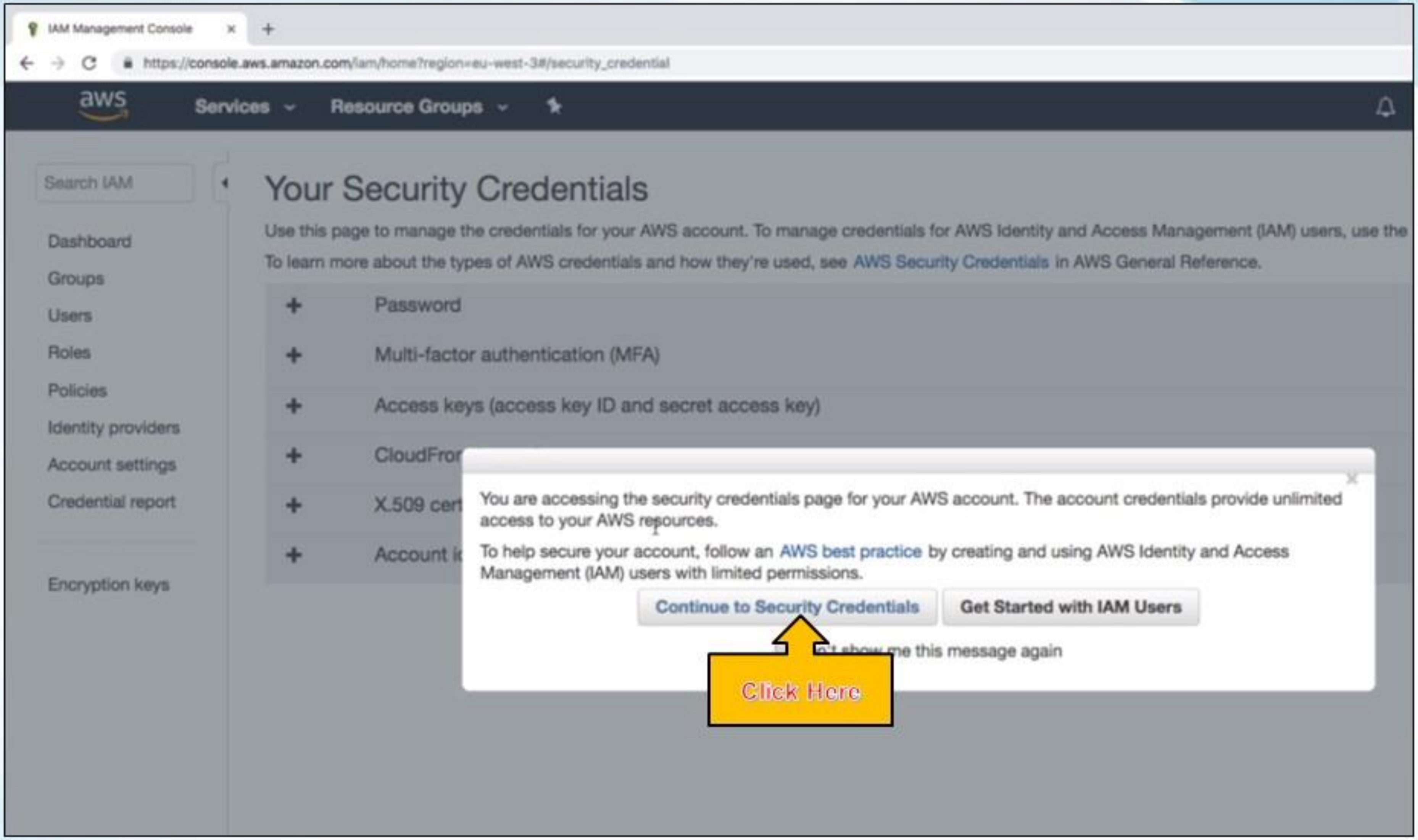
Security Status

1 out of 5 complete.

- ☑ Delete your root access keys
- ⚠ Activate MFA on your root account

  Activate multi-factor authentication (MFA) on your AWS root account to add another layer of protection to help keep your account secure. Learn More

- dividual IAM users
- ⚠ ps to assign permissions
- ⚠ Apply an IAM password policy



Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the

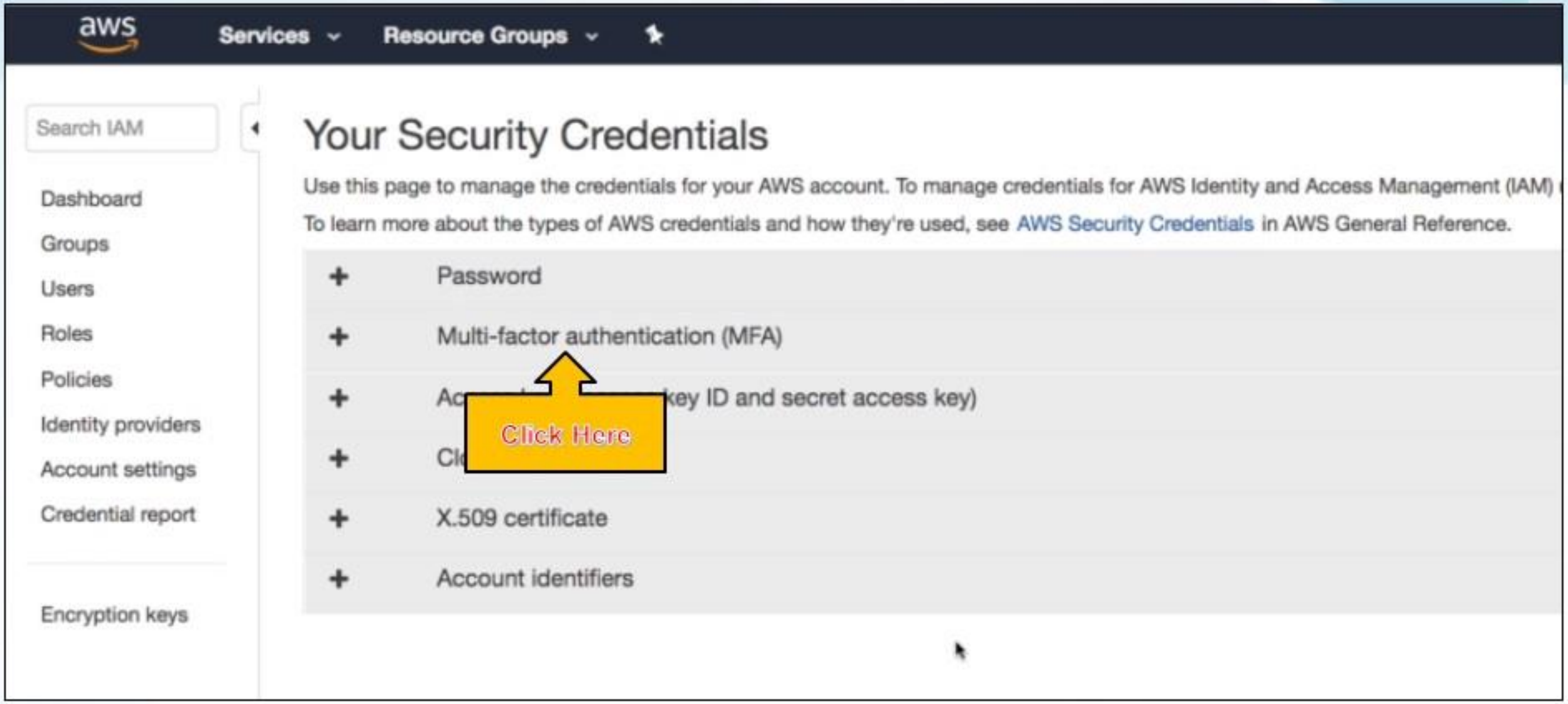
To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference.

- Password
- Multi-factor authentication (MFA)
- Access keys (access key ID and secret access key)
- CloudFron
- X.509 cert
- Account i

You are accessing the security credentials page for your AWS account. The account credentials provide unlimited access to your AWS resources.

To help secure your account, follow an AWS best practice by creating and using AWS Identity and Access Management (IAM) users with limited permissions.

Continue to Security Credentials
Get Started with IAM Users
n't show me this message again
Click Here



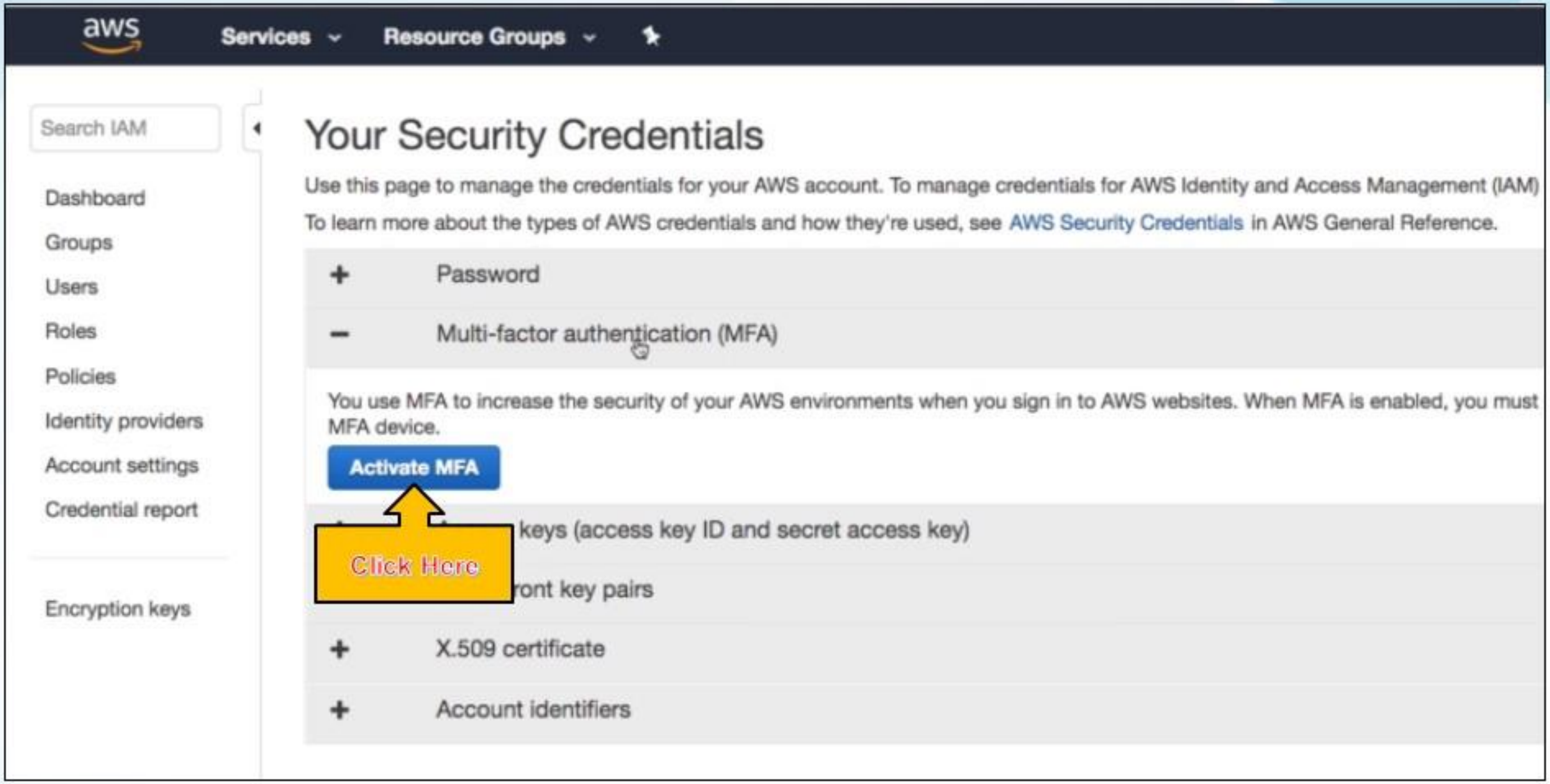
Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM)

To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference.

+ Password
+ Multi-factor authentication (MFA)
+ Ac key ID and secret access key)
+ Cl
+ X.509 certificate
+ Account identifiers

Click Here



Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM)

To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference.

+ Password

– Multi-factor authentication (MFA)

You use MFA to increase the security of your AWS environments when you sign in to AWS websites. When MFA is enabled, you must MFA device.

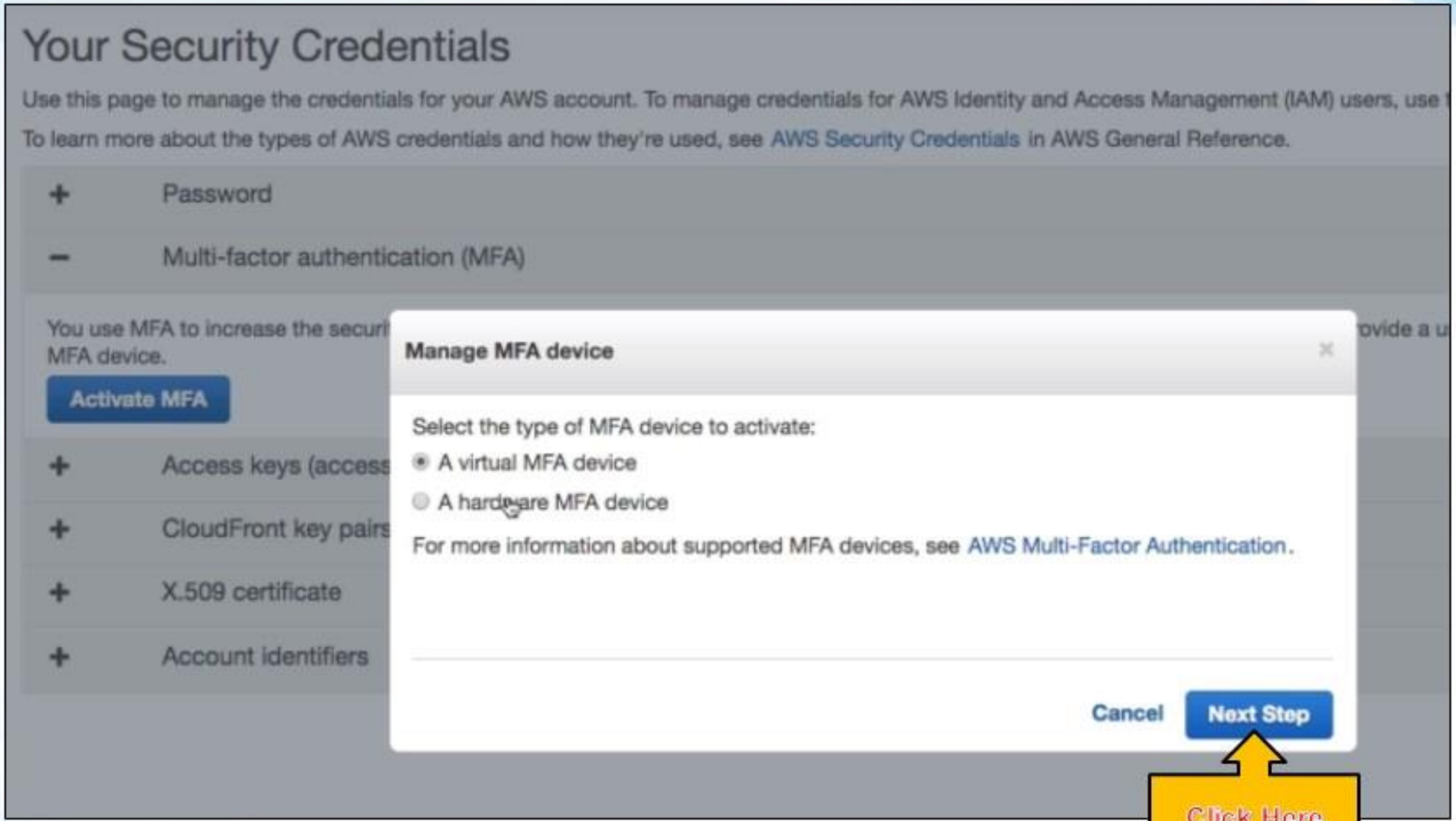
keys (access key ID and secret access key)

ront key pairs

+ X.509 certificate

+ Account identifiers

Click Here



Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use t

To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference.

You use MFA to increase the securi ovide a u MFA device.

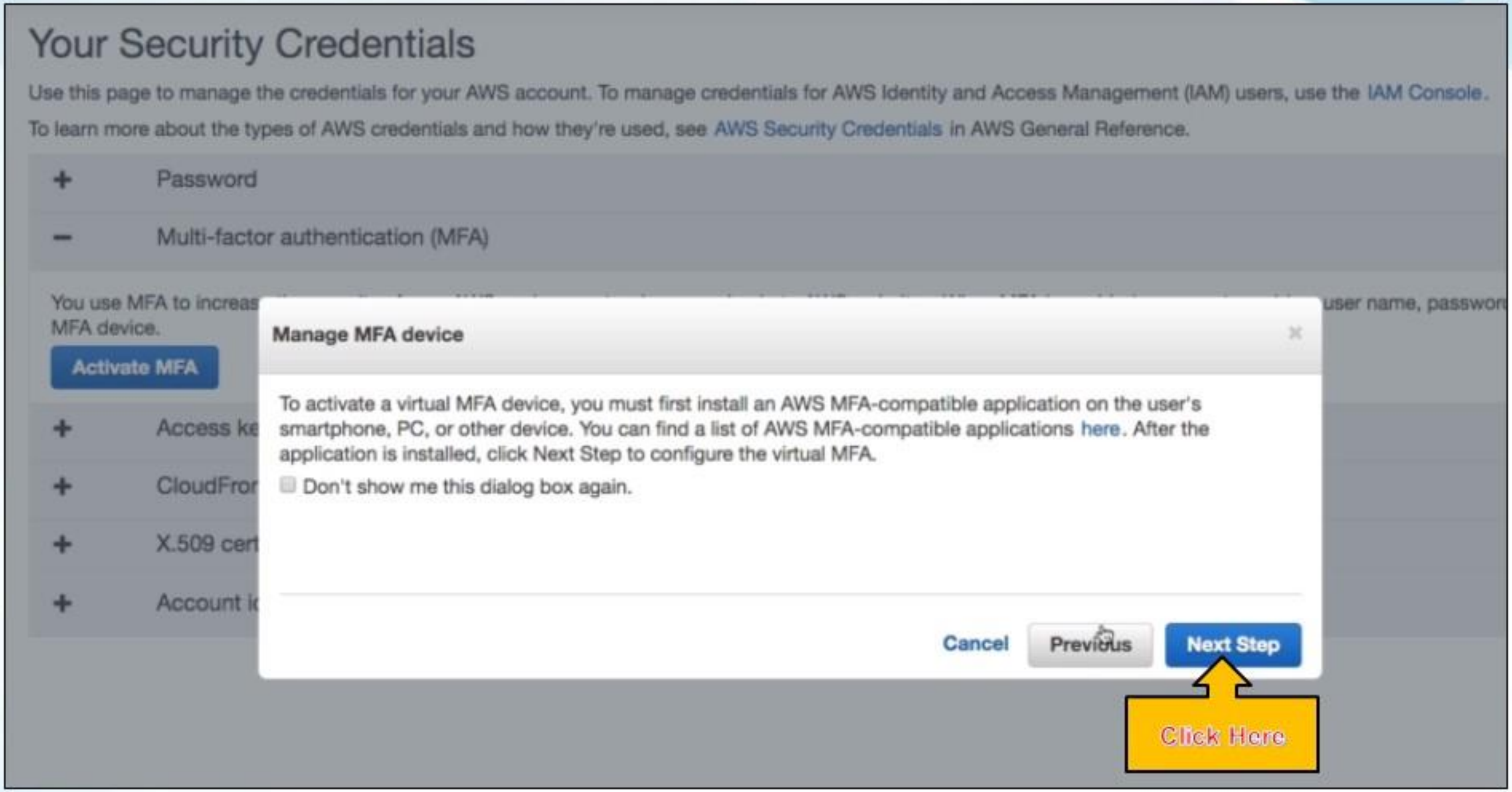
Manage MFA device

Select the type of MFA device to activate:

- ● A virtual MFA device
- ○ A hardware MFA device

For more information about supported MFA devices, see AWS Multi-Factor Authentication.

Click Here



Your Security Credentials

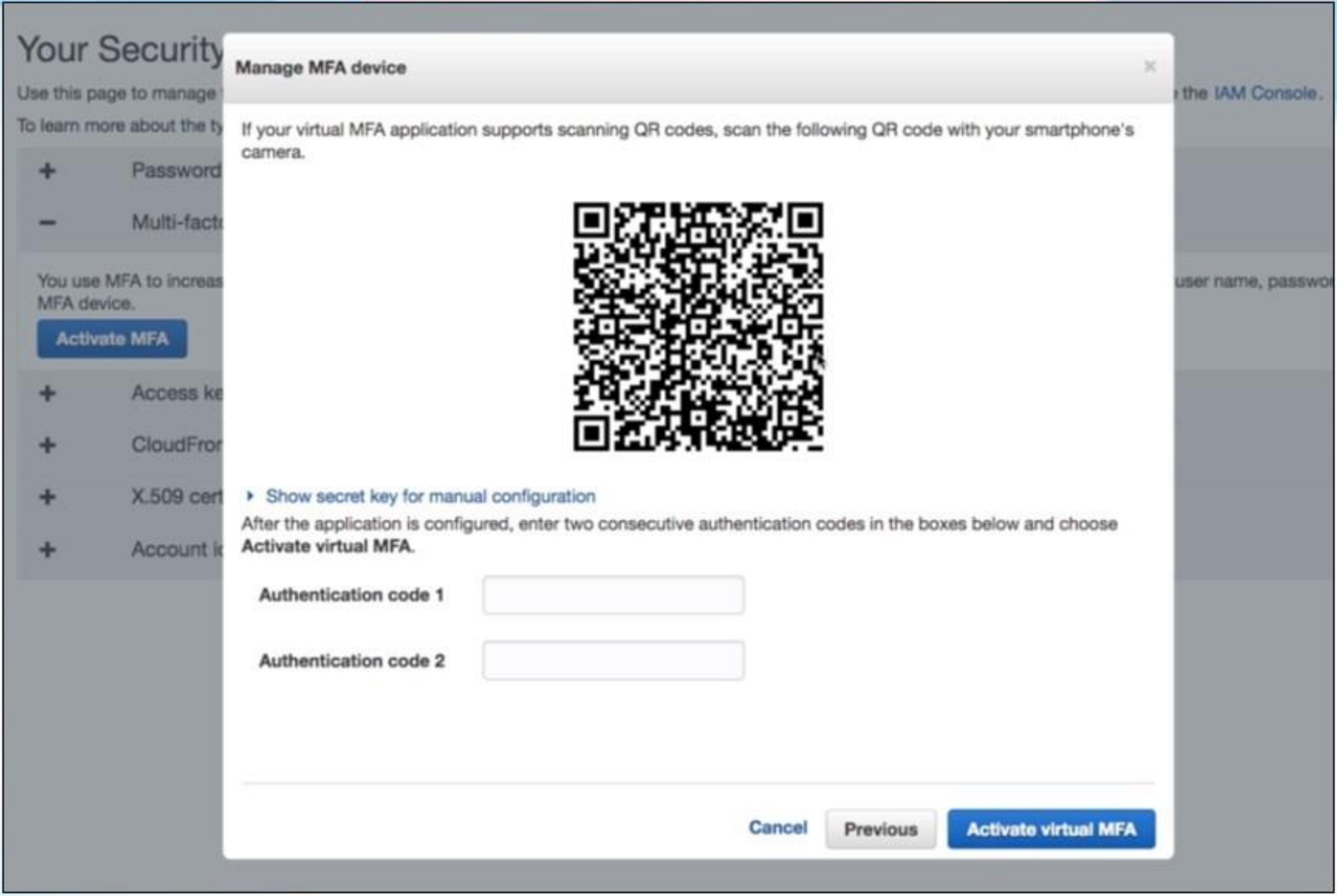
Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the IAM Console.

To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference.

Manage MFA device

To activate a virtual MFA device, you must first install an AWS MFA-compatible application on the user's smartphone, PC, or other device. You can find a list of AWS MFA-compatible applications here. After the application is installed, click Next Step to configure the virtual MFA.

□ Don't show me this dialog box again.



Your Security

Use this page to manage

the IAM Console.

To learn more about the ty

You use MFA to increas

user name, passwo

MFA device.

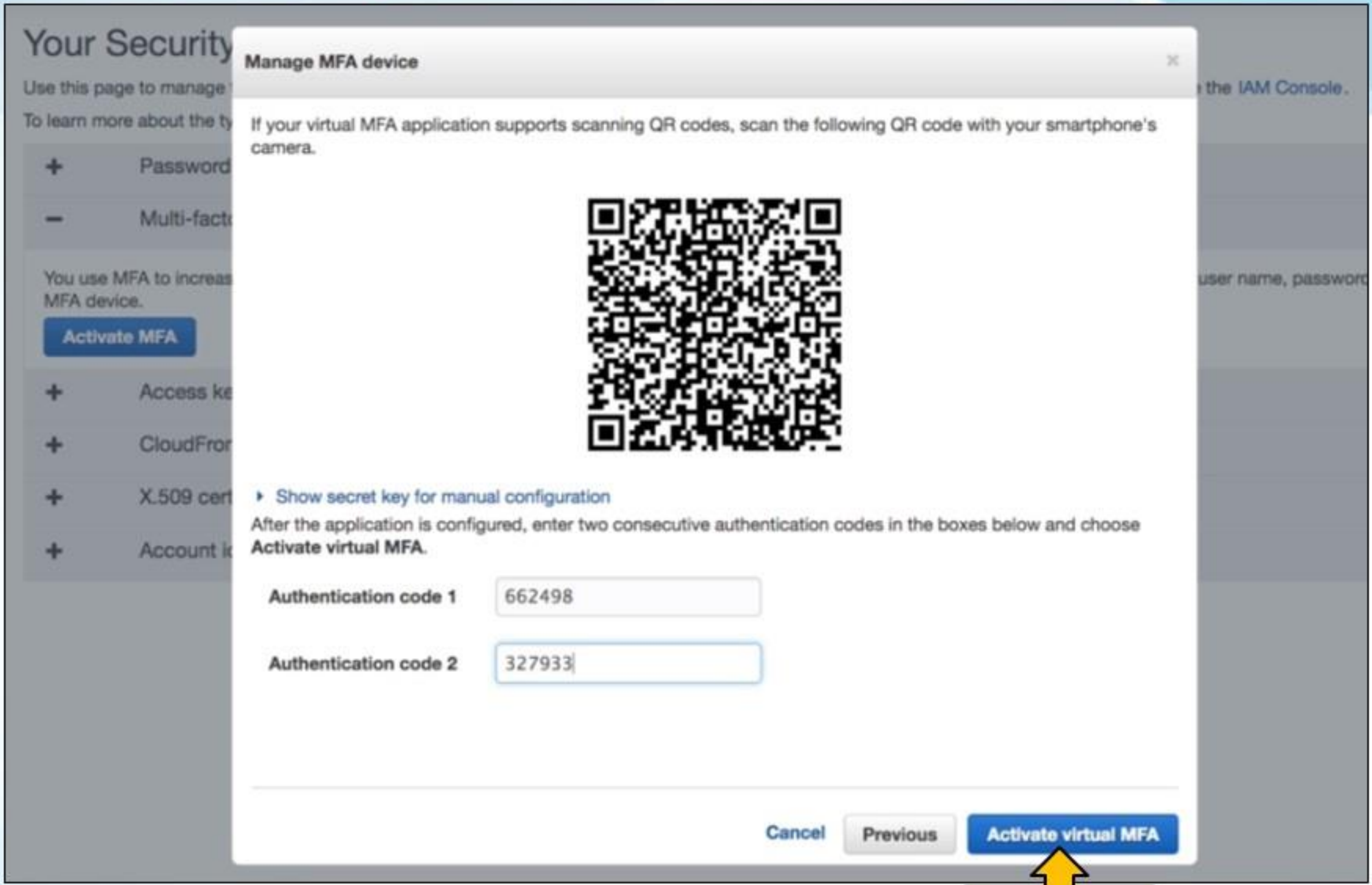
Manage MFA device

If your virtual MFA application supports scanning QR codes, scan the following QR code with your smartphone's camera.

▸ Show secret key for manual configuration

After the application is configured, enter two consecutive authentication codes in the boxes below and choose **Activate virtual MFA.**

Authentication code 1	
Authentication code 2	



Your Security

Use this page to manage … the IAM Console.

To learn more about the t…

You use MFA to increas… user name, password … MFA device.

Manage MFA device

If your virtual MFA application supports scanning QR codes, scan the following QR code with your smartphone's camera.

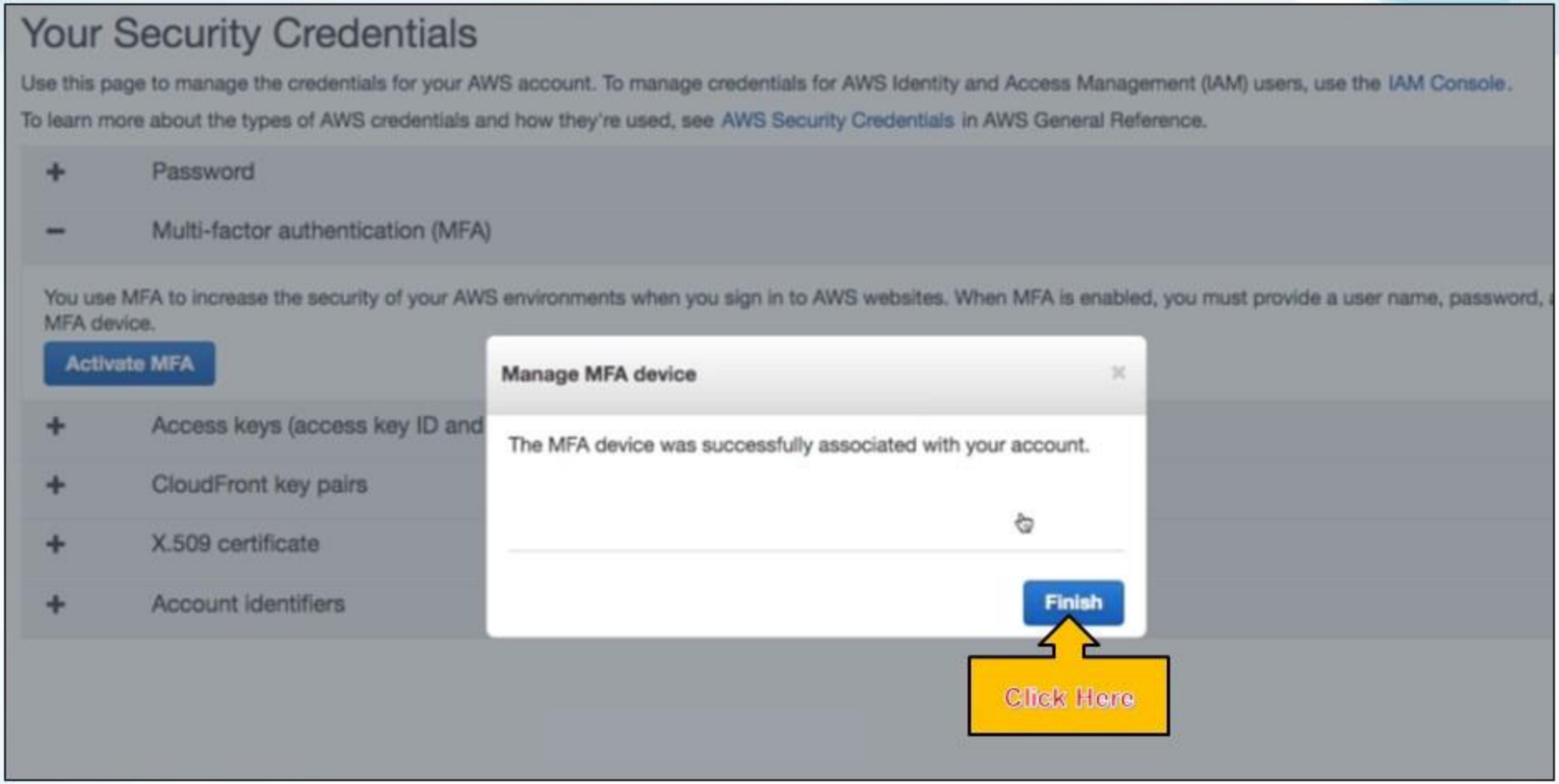
▸ Show secret key for manual configuration

After the application is configured, enter two consecutive authentication codes in the boxes below and choose **Activate virtual MFA**.

Authentication code 1 662498

Authentication code 2 327933

Click Here



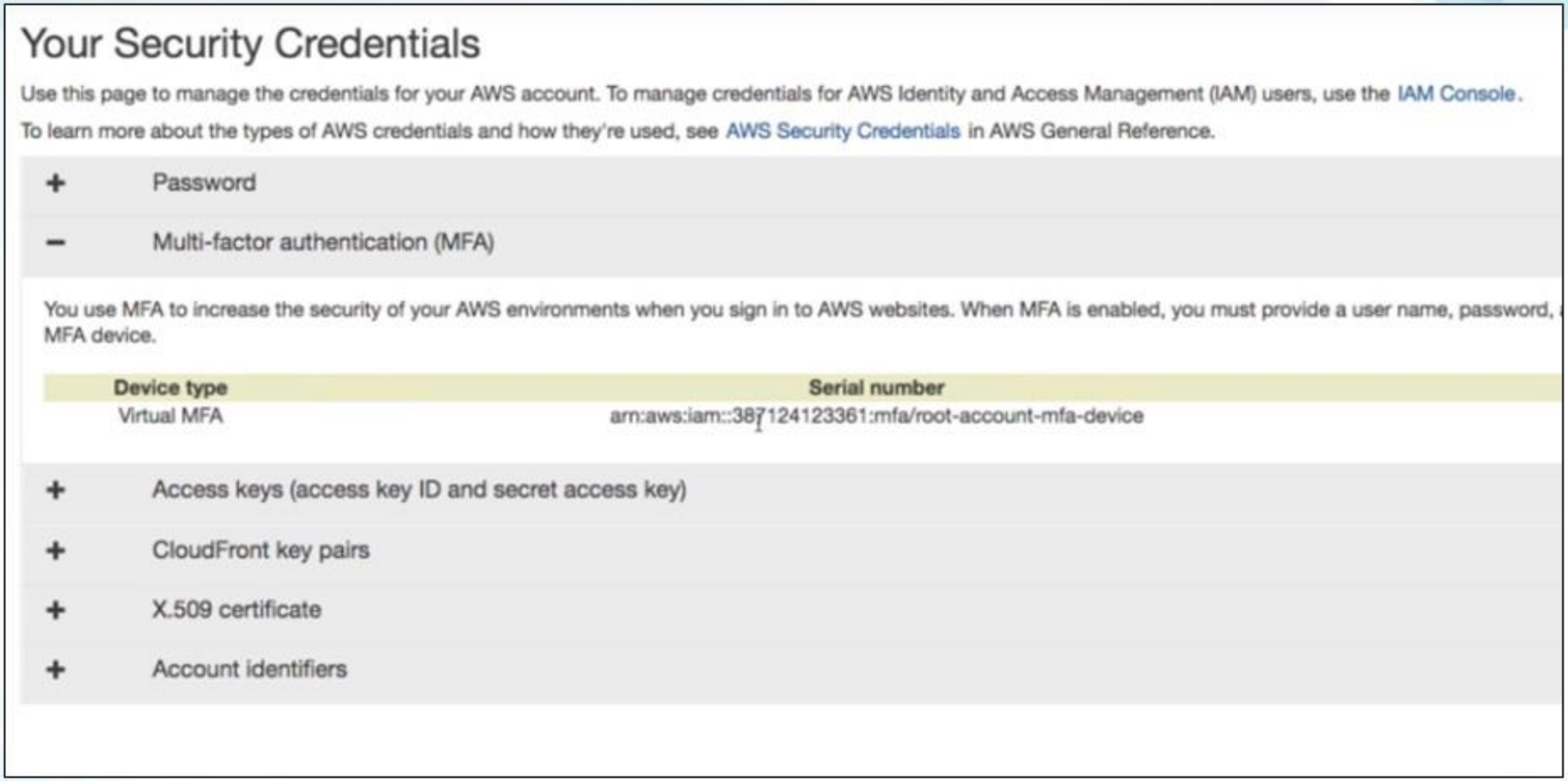
Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the IAM Console.

To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference.

You use MFA to increase the security of your AWS environments when you sign in to AWS websites. When MFA is enabled, you must provide a user name, password,
MFA device.

The MFA device was successfully associated with your account.



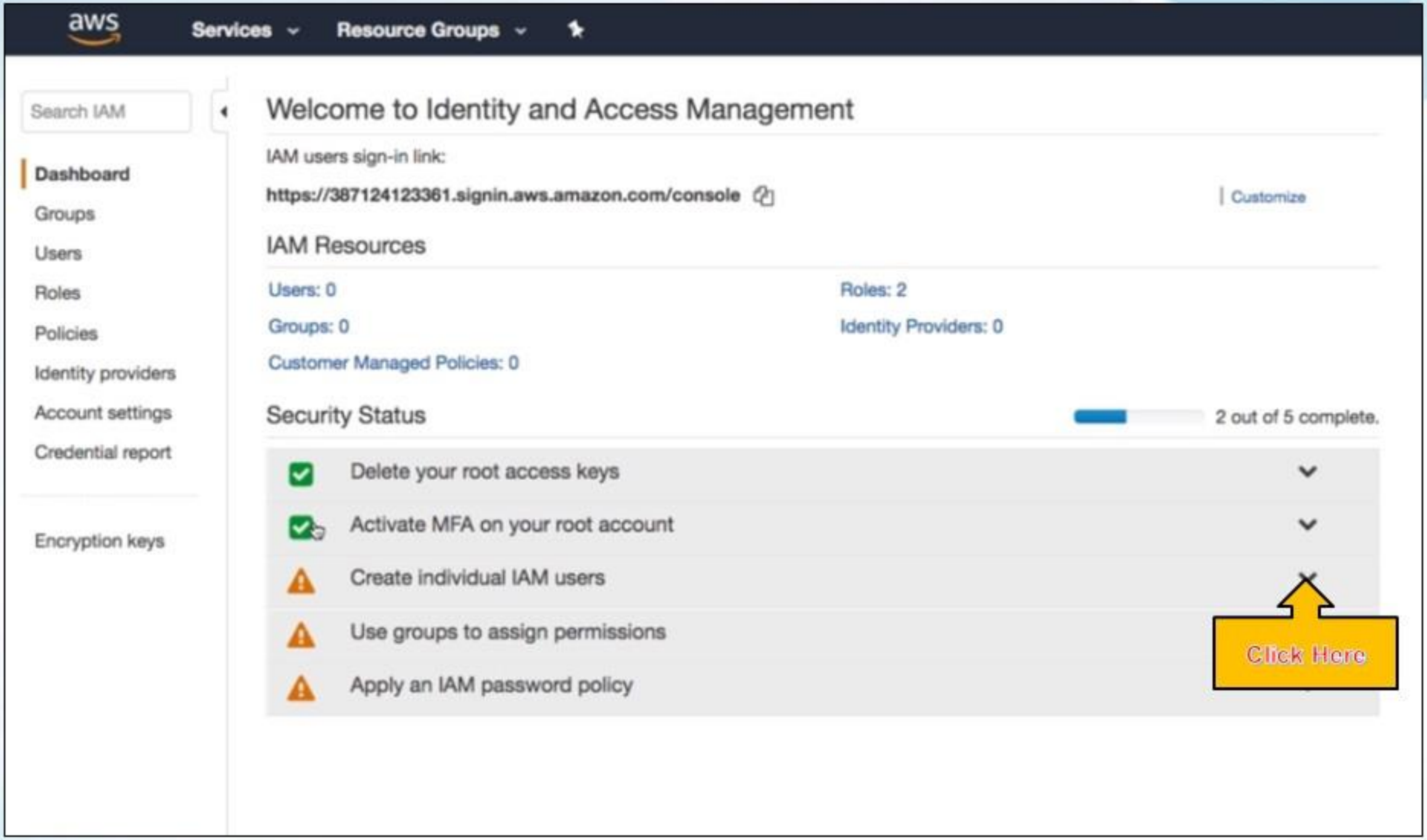
Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the IAM Console.

To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference.

You use MFA to increase the security of your AWS environments when you sign in to AWS websites. When MFA is enabled, you must provide a user name, password,
MFA device.

Device type	Serial number
Virtual MFA	arn:aws:iam::387124123361:mfa/root-account-mfa-device



Welcome to Identity and Access Management

IAM users sign-in link:

https://387124123361.signin.aws.amazon.com/console

IAM Resources

Users: 0

Roles: 2

Groups: 0

Identity Providers: 0

Customer Managed Policies: 0

Security Status

2 out of 5 complete.

✓ Delete your root access keys

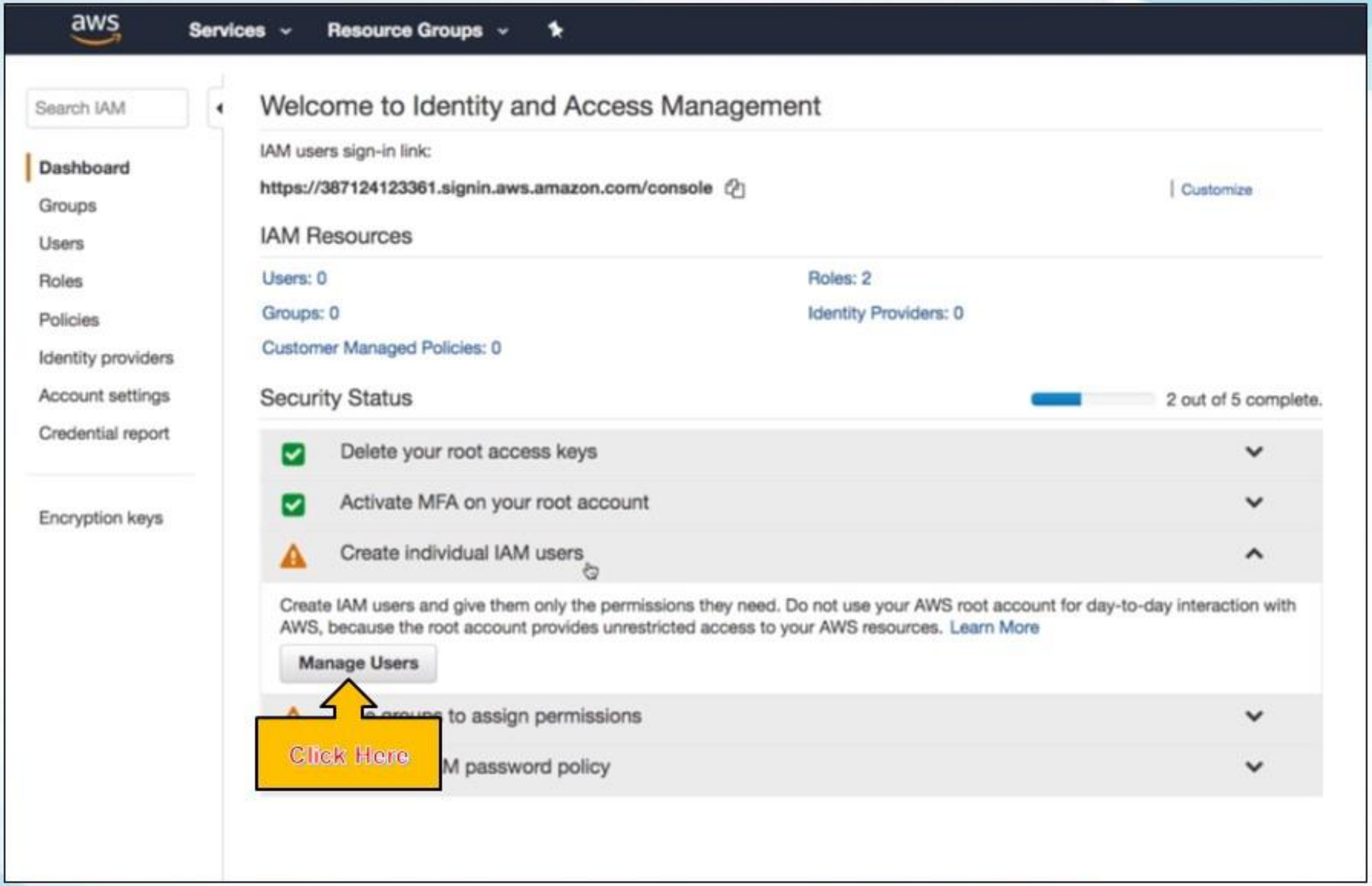
✓ Activate MFA on your root account

⚠ Create individual IAM users

⚠ Use groups to assign permissions

⚠ Apply an IAM password policy

Click Here



Welcome to Identity and Access Management

IAM users sign-in link:

https://387124123361.signin.aws.amazon.com/console

IAM Resources

Users: 0

Groups: 0

Customer Managed Policies: 0

Roles: 2

Identity Providers: 0

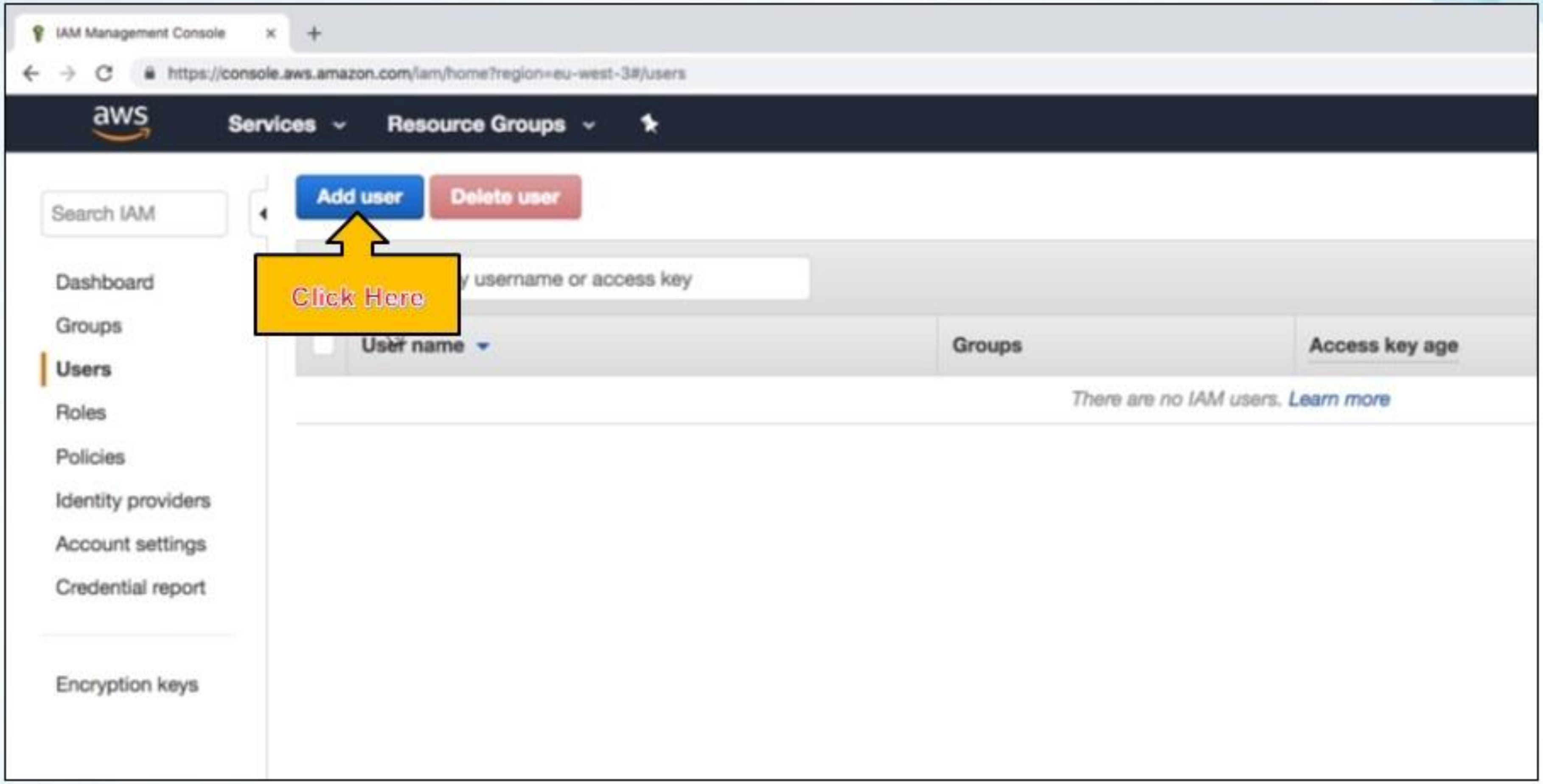
Security Status

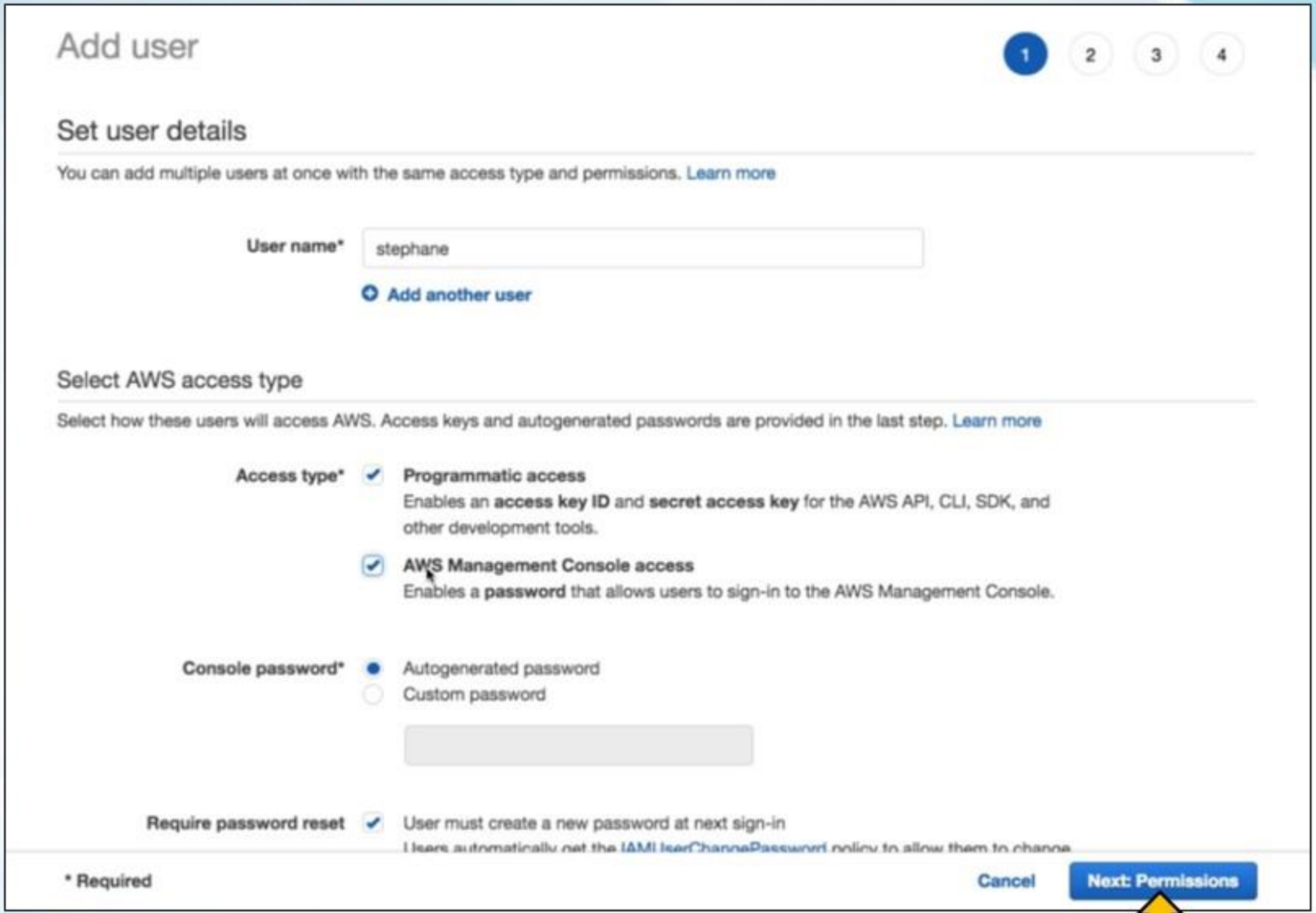
2 out of 5 complete.

- ✓ Delete your root access keys
- ✓ Activate MFA on your root account
- ⚠ Create individual IAM users

Create IAM users and give them only the permissions they need. Do not use your AWS root account for day-to-day interaction with AWS, because the root account provides unrestricted access to your AWS resources. Learn More

- ⚠ groups to assign permissions
- M password policy

IAM Management Console
https://console.aws.amazon.com/iam/home?region=eu-west-3#/users
aws
Services
Resource Groups
Search IAM
Dashboard
Groups
Users
Roles
Policies
Identity providers
Account settings
Credential report
Encryption keys
Add user
Delete user
Click Here
y username or access key
User name
Groups
Access key age
There are no IAM users. Learn more



Add user

1 2 3 4

Set user details

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

User name* stephane

⊕ Add another user

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

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

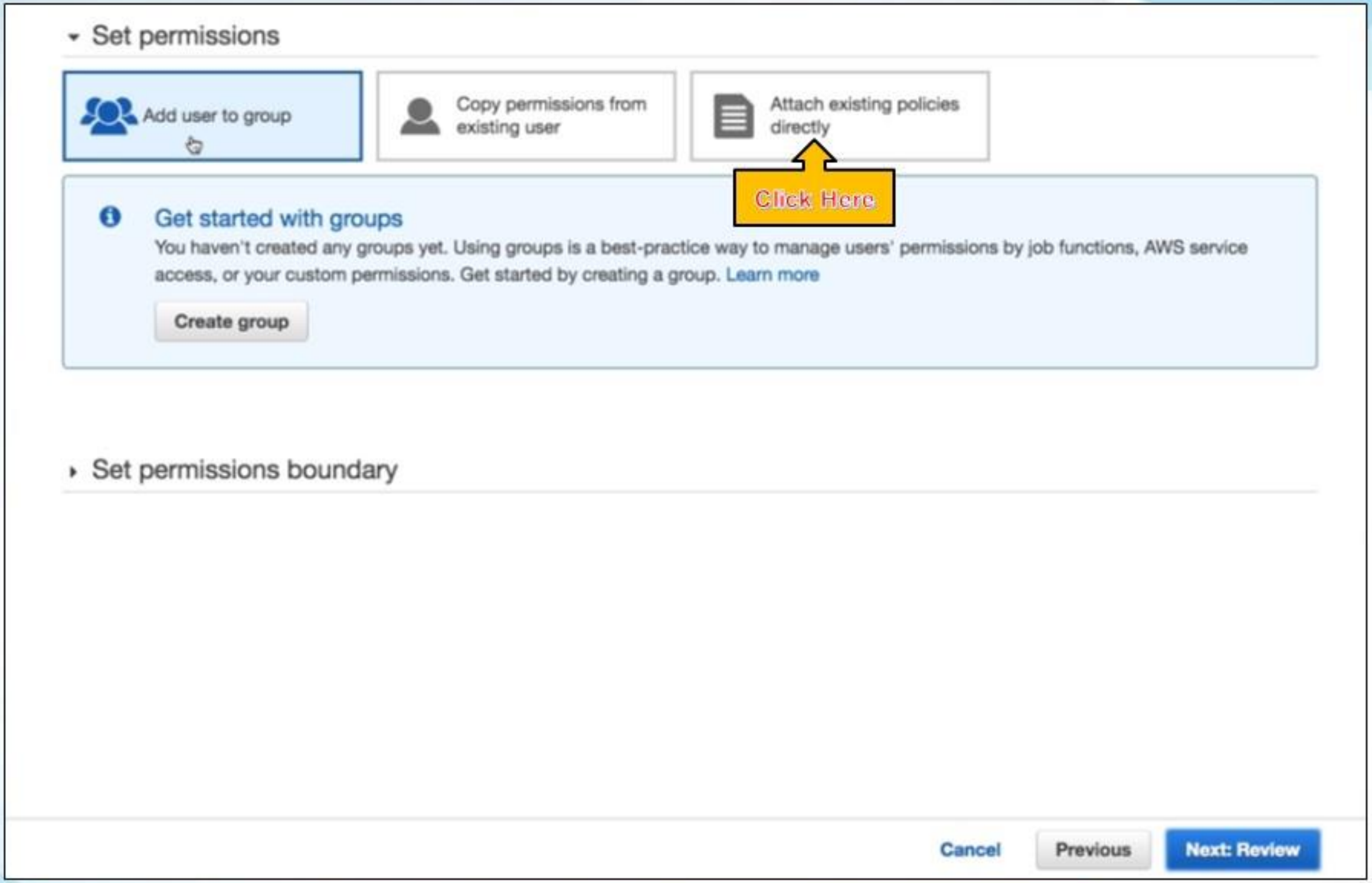
☑ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password* ● Autogenerated password
○ Custom 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

* Required

Click Here



▾ Set permissions

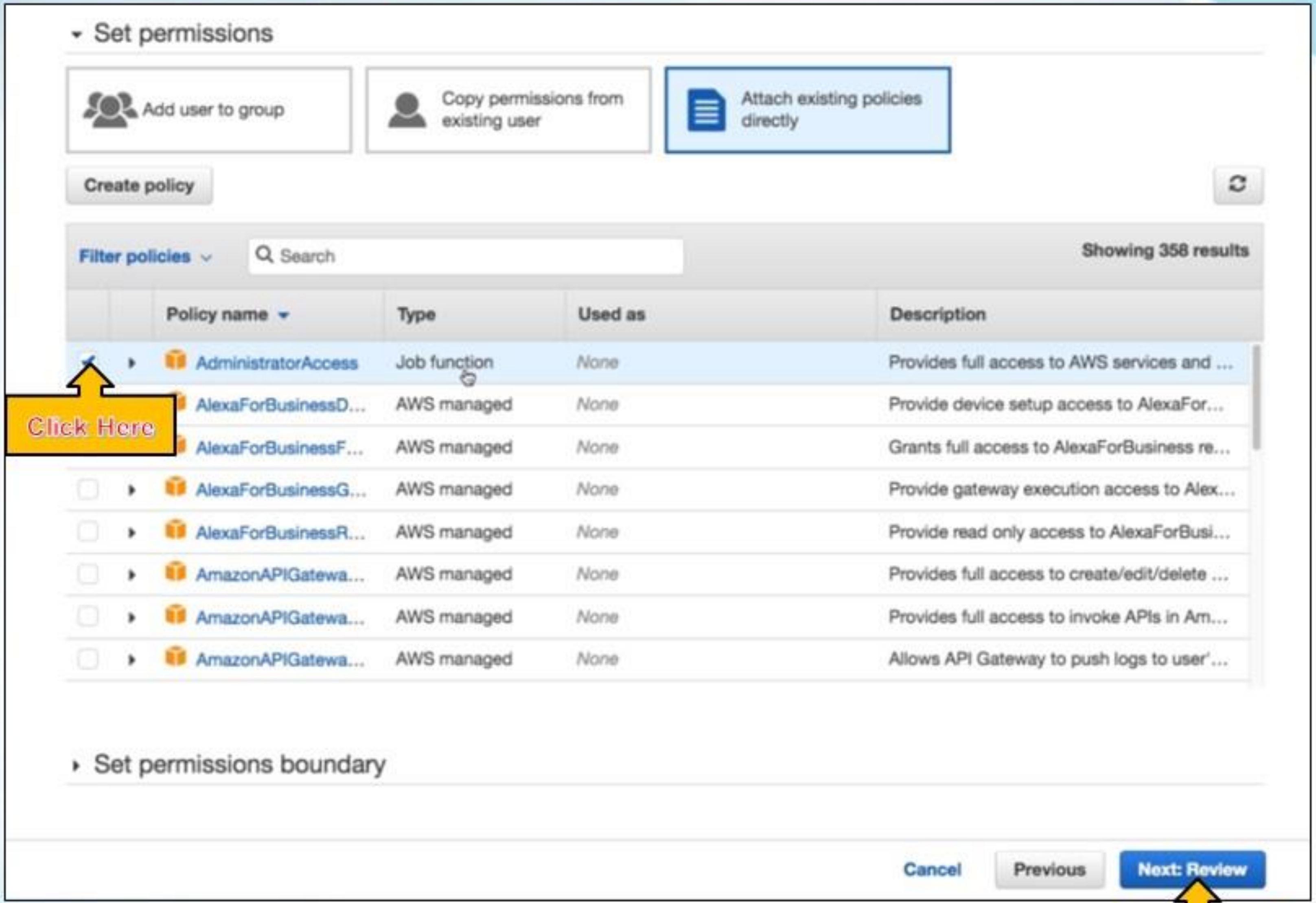
Add user to group
Copy permissions from existing user
Attach existing policies directly

Click Here

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

Create group
▸ Set permissions boundary
Cancel
Previous
Next: Review



▾ Set permissions

Add user to group

Copy permissions from existing user

Attach existing policies directly

Create policy

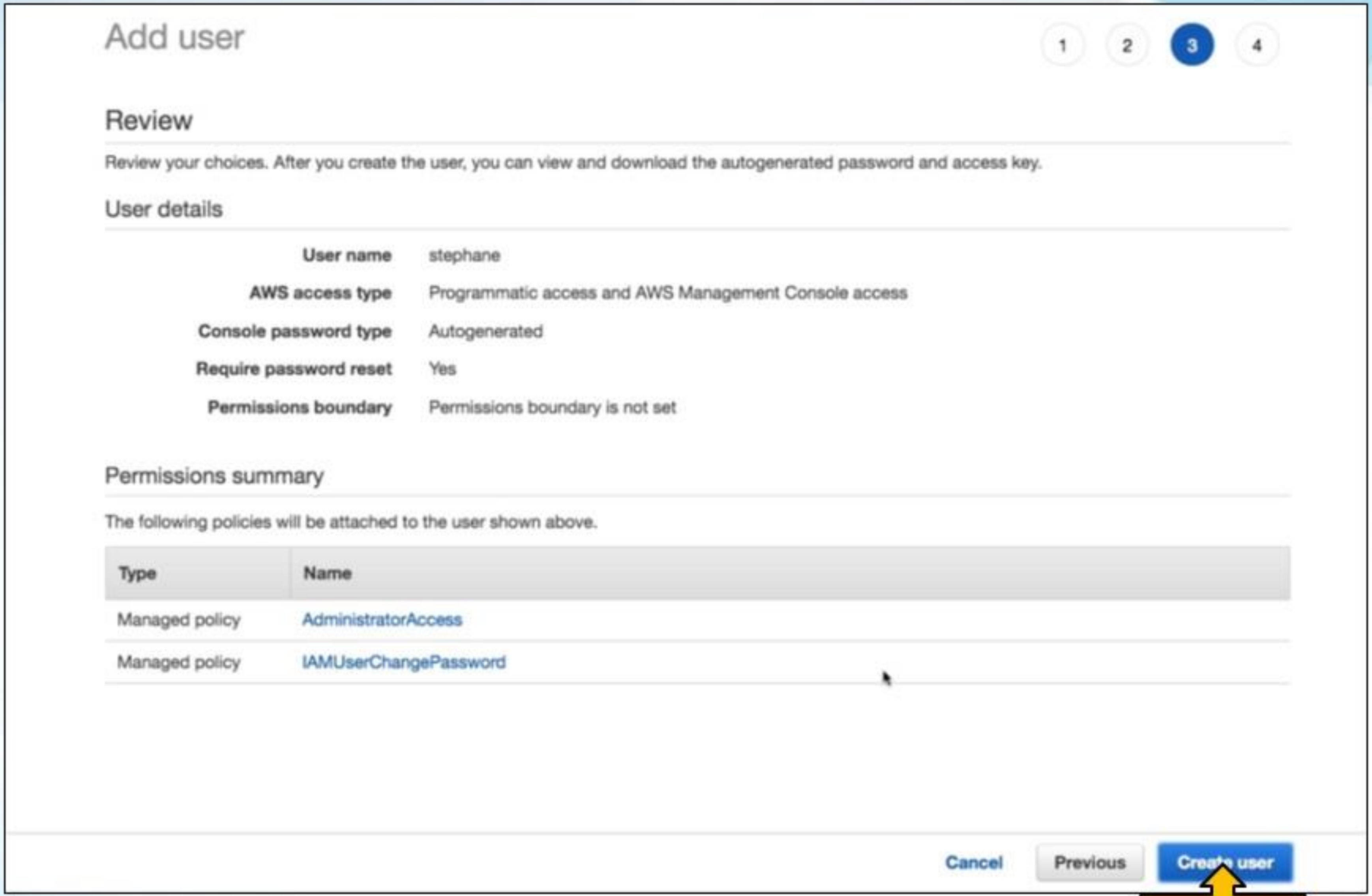
Filter policies ⌄ Search Showing 358 results

		Policy name ▾	Type	Used as	Description
☑	▸	AdministratorAccess	Job function	None	Provides full access to AWS services and ...
		AlexaForBusinessD...	AWS managed	None	Provide device setup access to AlexaFor...
		AlexaForBusinessF...	AWS managed	None	Grants full access to AlexaForBusiness re...
☐	▸	AlexaForBusinessG...	AWS managed	None	Provide gateway execution access to Alex...
☐	▸	AlexaForBusinessR...	AWS managed	None	Provide read only access to AlexaForBusi...
☐	▸	AmazonAPIGatewa...	AWS managed	None	Provides full access to create/edit/delete ...
☐	▸	AmazonAPIGatewa...	AWS managed	None	Provides full access to invoke APIs in Am...
☐	▸	AmazonAPIGatewa...	AWS managed	None	Allows API Gateway to push logs to user'...

▸ Set permissions boundary

Click Here

Click Here



Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

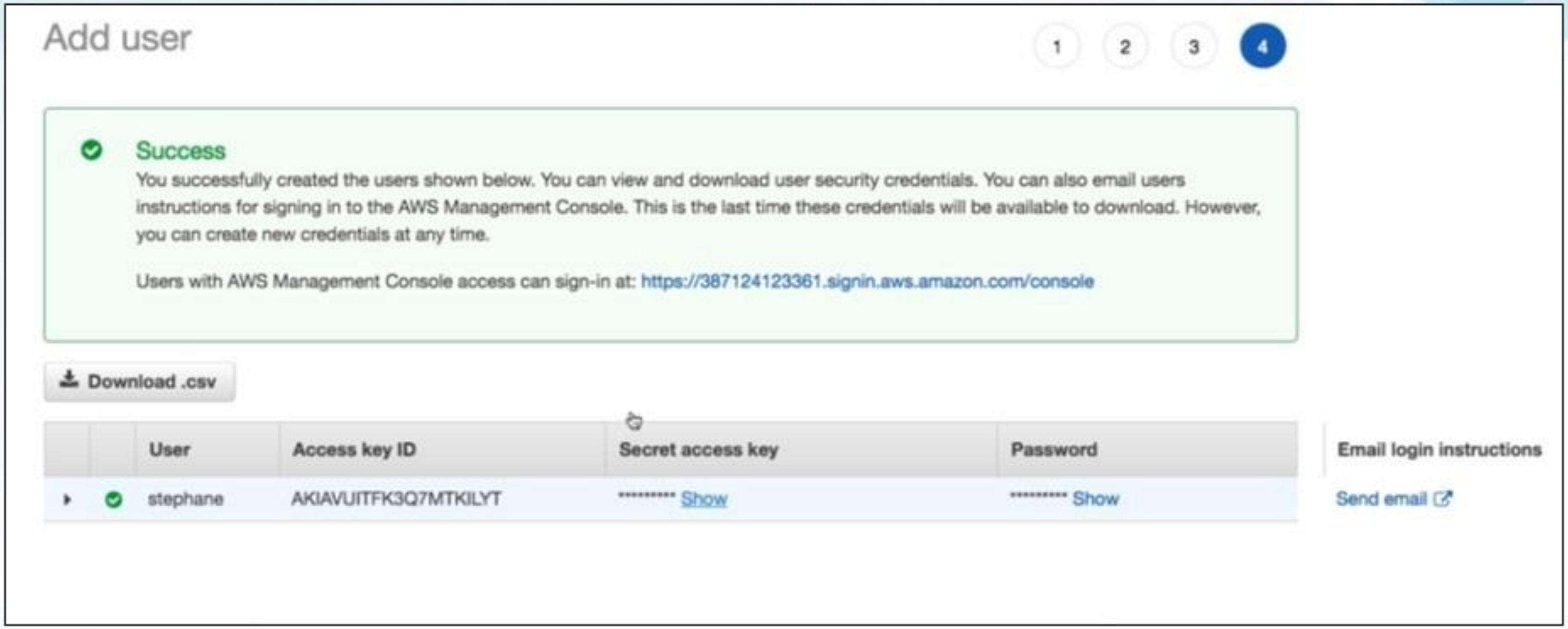
User name	stephane
AWS access type	Programmatic access and AWS Management Console access
Console password type	Autogenerated
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	AdministratorAccess
Managed policy	IAMUserChangePassword

Click Here



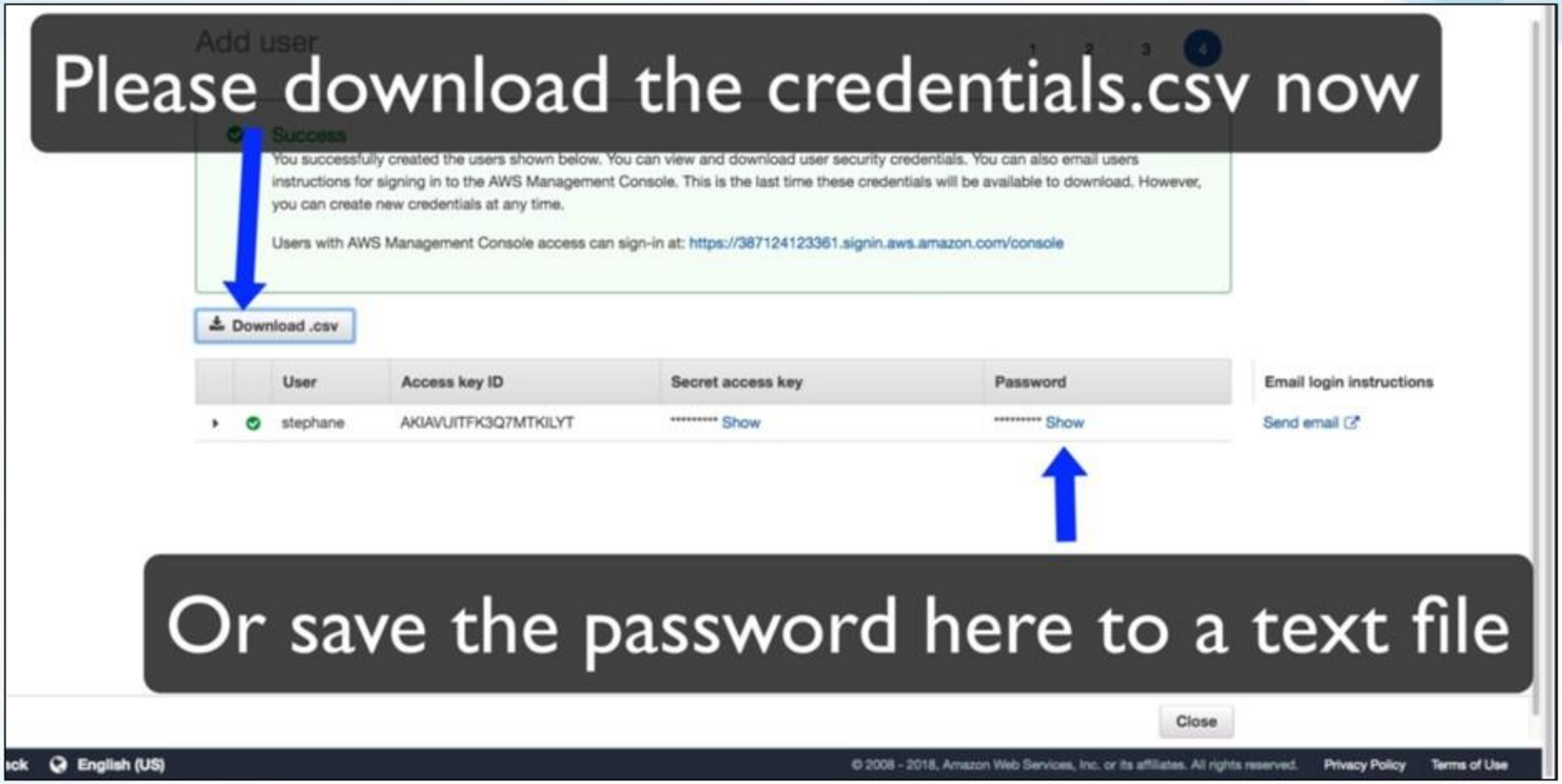
Add user

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://387124123361.signin.aws.amazon.com/console

		User	Access key ID	Secret access key	Password	Email login instructions
▸	✓	stephane	AKIAVUITFK3Q7MTKILYT	********** Show	********** Show	Send email



Please download the credentials.csv now

Add user

Success

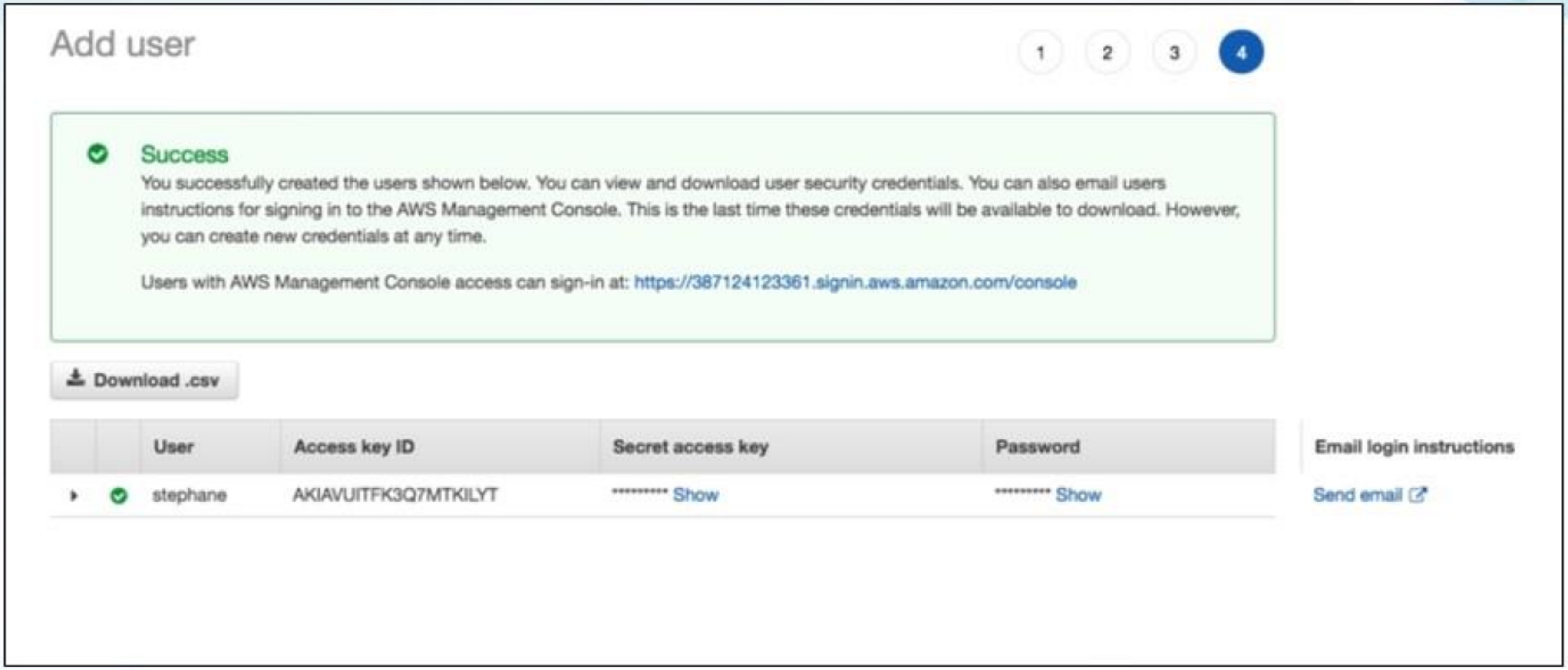
You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: https://387124123361.signin.aws.amazon.com/console

User	Access key ID	Secret access key	Password	Email login instructions
stephane	AKIAVUITFK3Q7MTKILYT	********** Show	********** Show	Send email

Or save the password here to a text file

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.



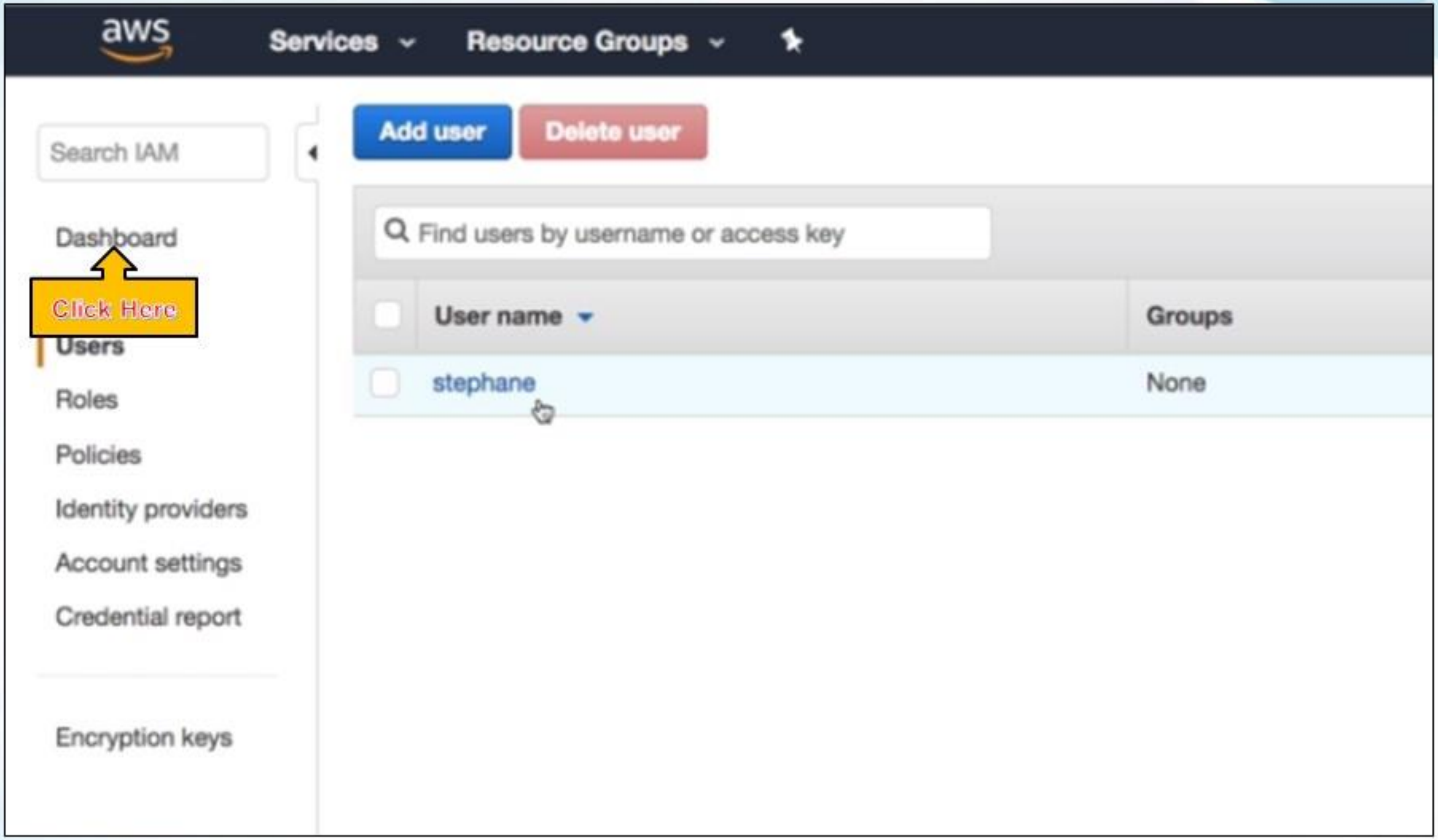
Add user

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.

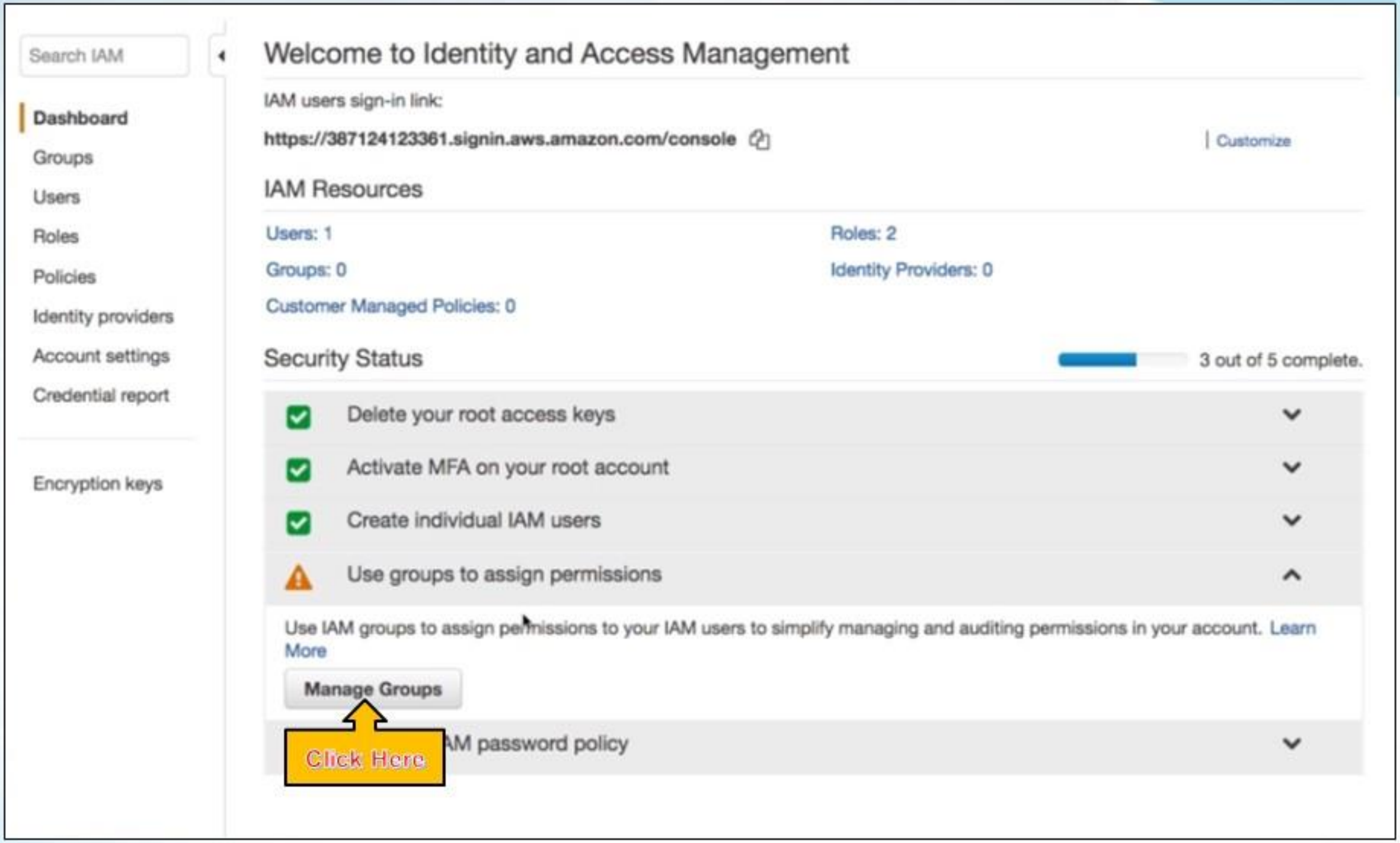
Users with AWS Management Console access can sign-in at: https://387124123361.signin.aws.amazon.com/console

		User	Access key ID	Secret access key	Password	Email login instructions
▸	✓	stephane	AKIAVUITFK3Q7MTKILYT	********** Show	********** Show	Send email



Click Here

User name	Groups
stephane	None



Welcome to Identity and Access Management

IAM users sign-in link:

https://387124123361.signin.aws.amazon.com/console

IAM Resources

Users: 1	Roles: 2
Groups: 0	Identity Providers: 0
Customer Managed Policies: 0	

Security Status

3 out of 5 complete.

☑ Delete your root access keys

☑ Activate MFA on your root account

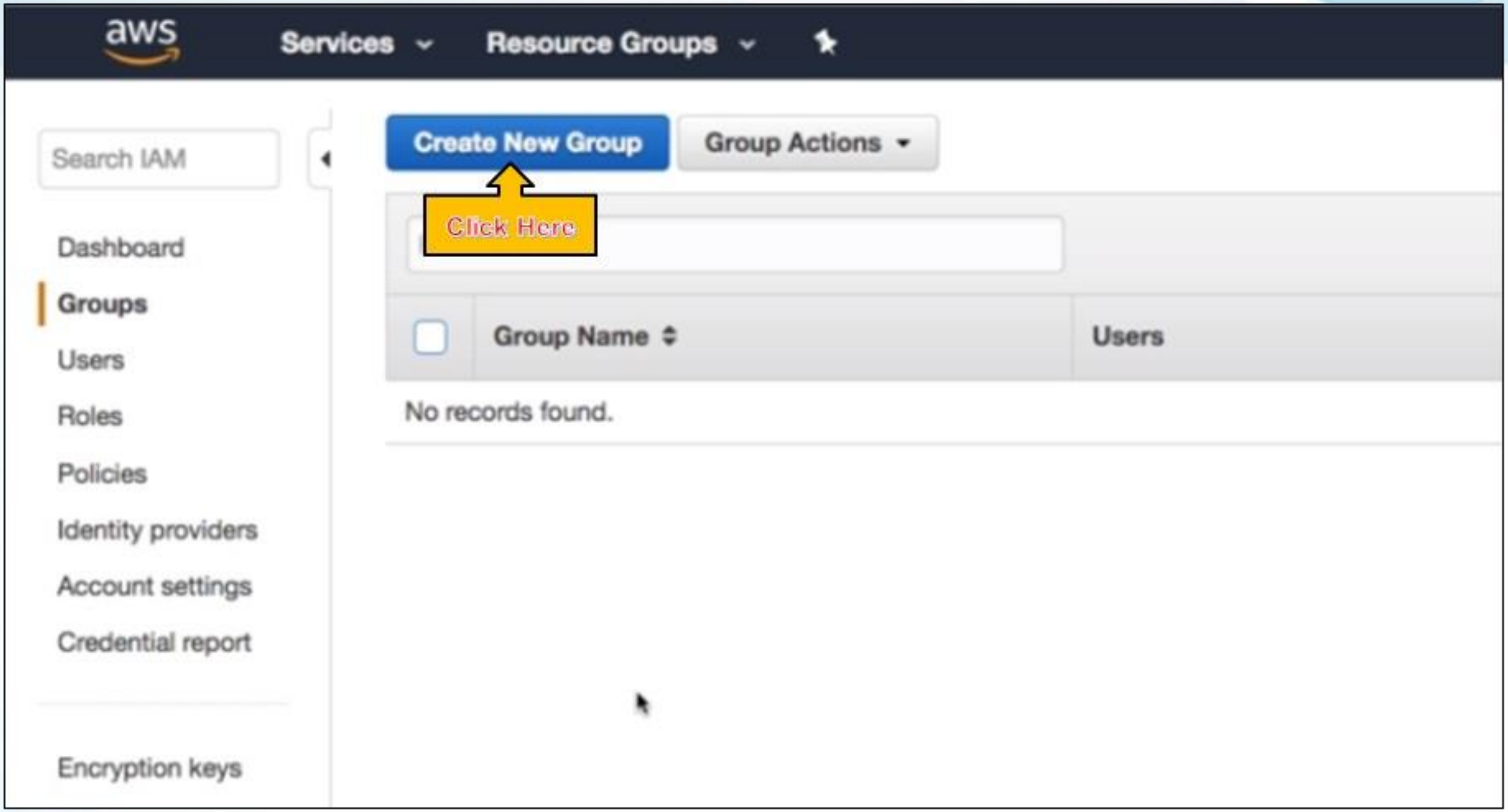
☑ Create individual IAM users

⚠ Use groups to assign permissions

Use IAM groups to assign permissions to your IAM users to simplify managing and auditing permissions in your account. Learn More

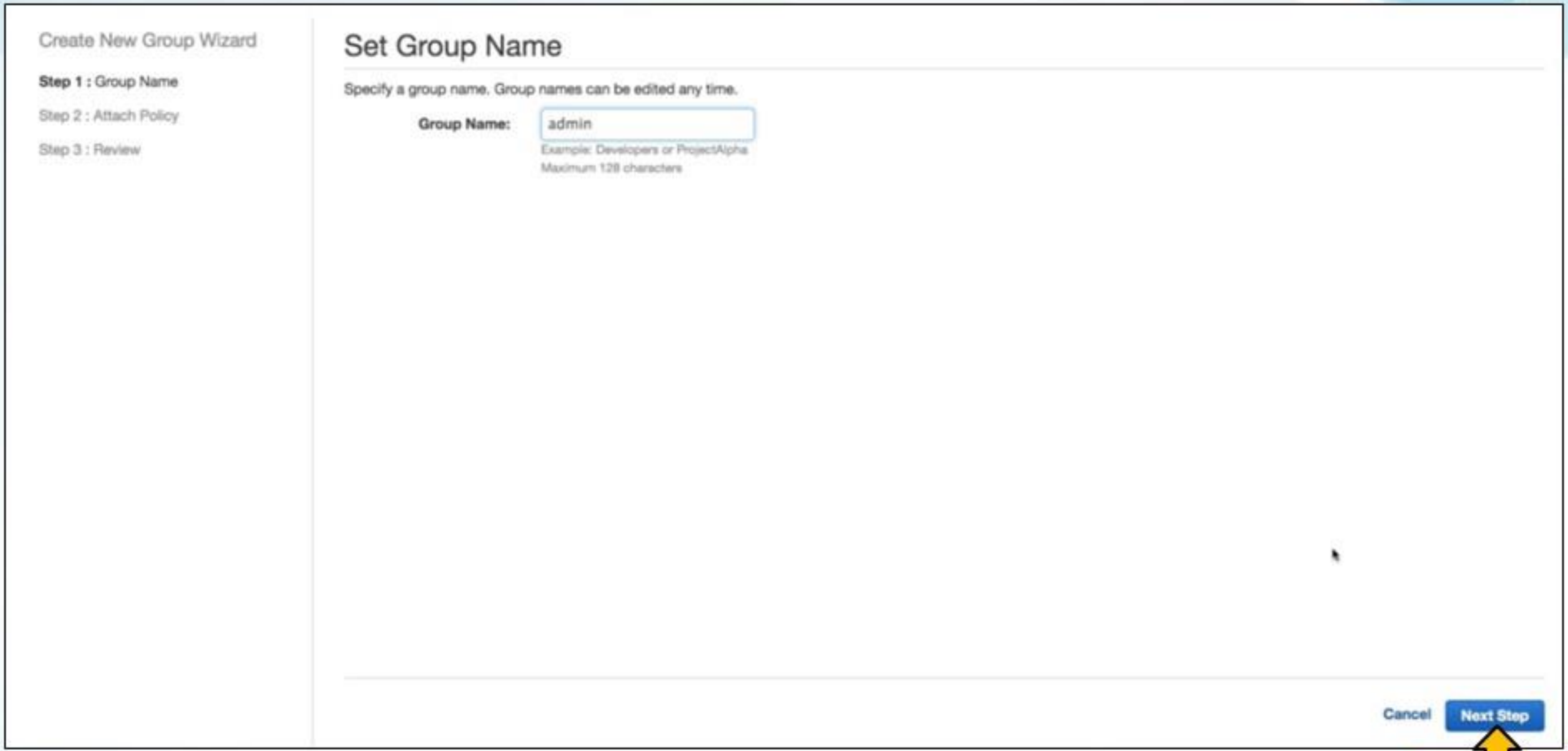
AM password policy

Click Here



Click Here

No records found.



Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

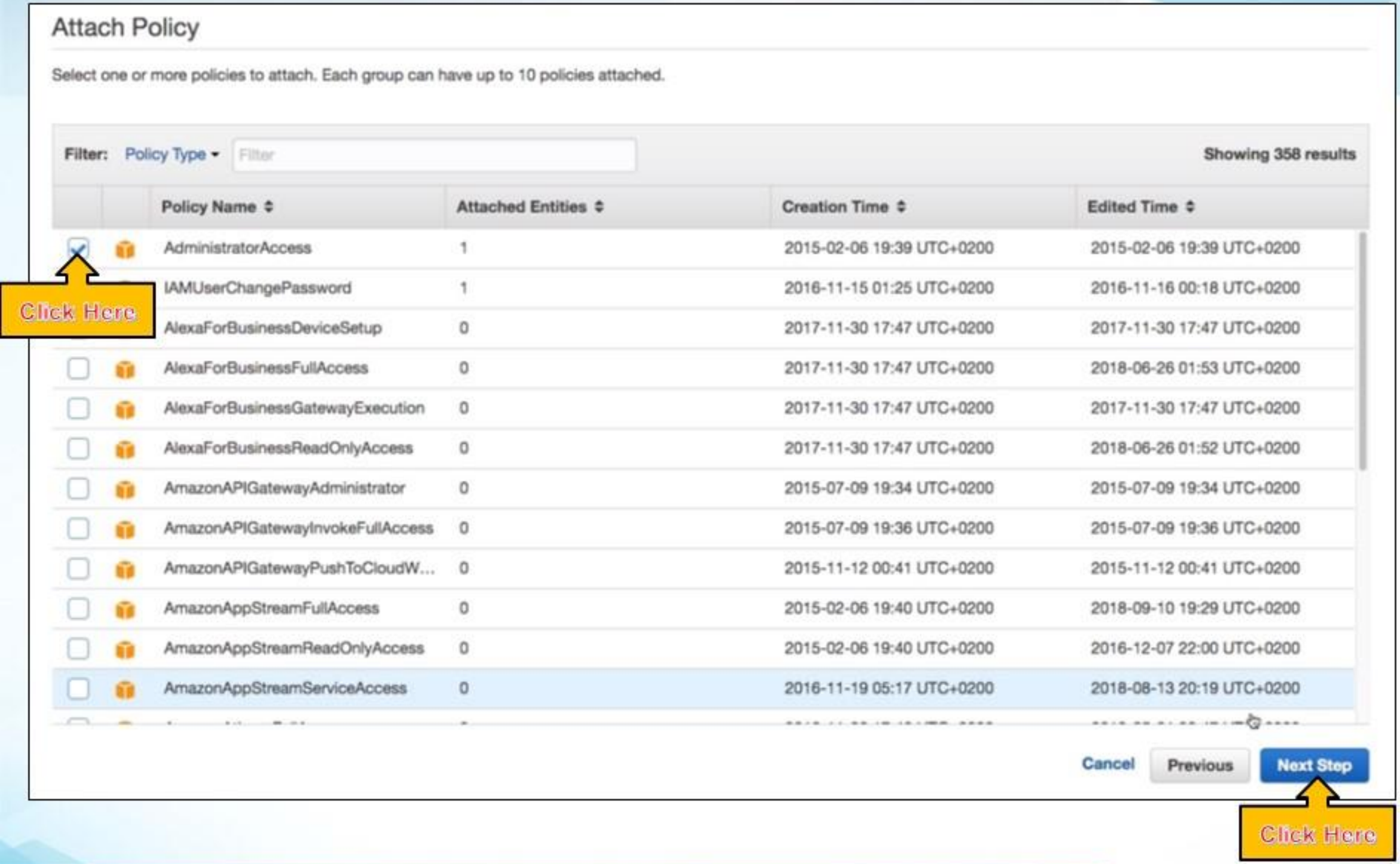
Set Group Name

Specify a group name. Group names can be edited any time.

Group Name: admin

Example: Developers or ProjectAlpha
Maximum 128 characters

Click Here



Attach Policy

Select one or more policies to attach. Each group can have up to 10 policies attached.

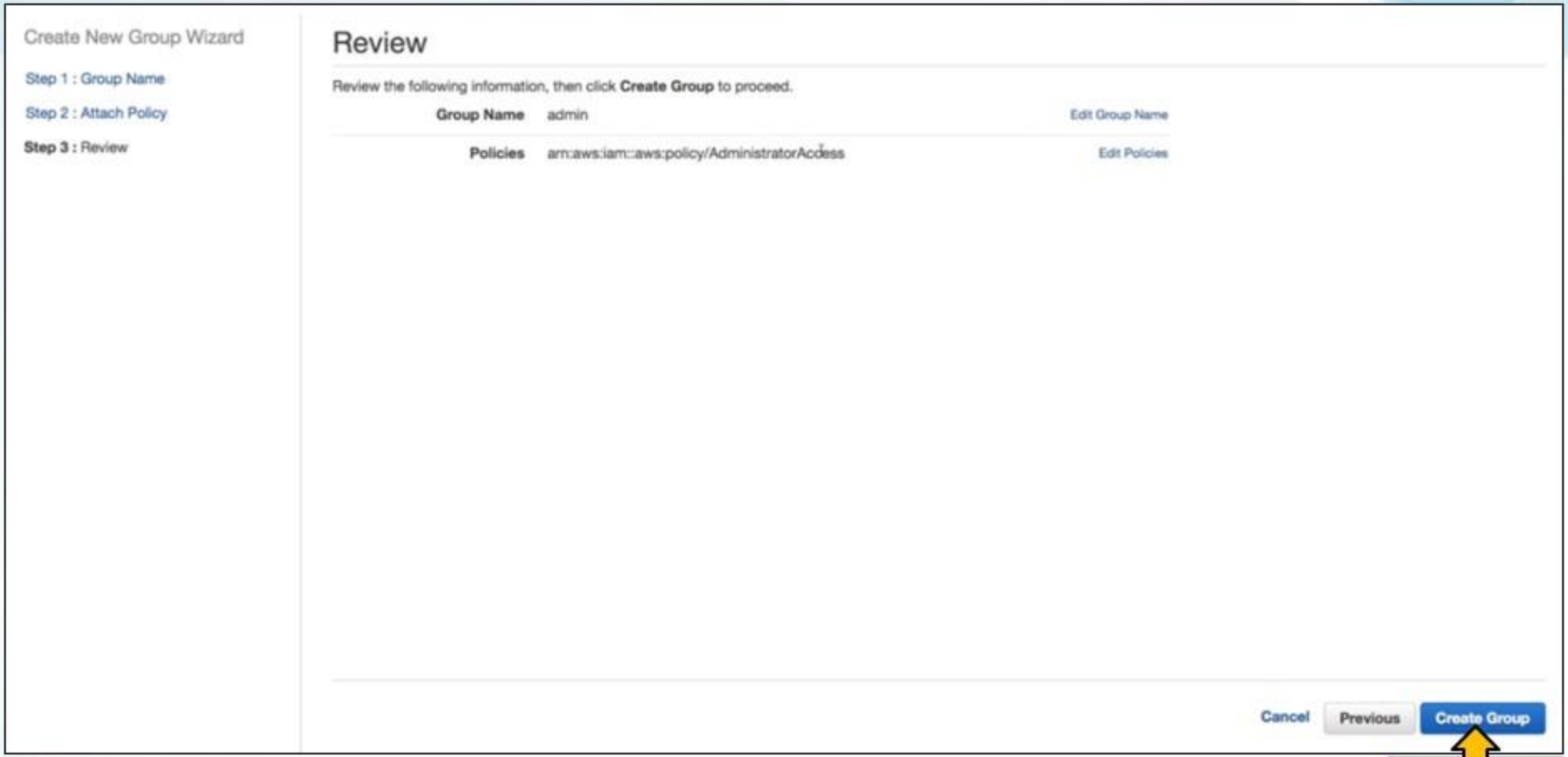
Filter: Policy Type ▾ Filter

Showing 358 results

	Policy Name ⇕	Attached Entities ⇕	Creation Time ⇕	Edited Time ⇕
☑	AdministratorAccess	1	2015-02-06 19:39 UTC+0200	2015-02-06 19:39 UTC+0200
	IAMUserChangePassword	1	2016-11-15 01:25 UTC+0200	2016-11-16 00:18 UTC+0200
	AlexaForBusinessDeviceSetup	0	2017-11-30 17:47 UTC+0200	2017-11-30 17:47 UTC+0200
☐	AlexaForBusinessFullAccess	0	2017-11-30 17:47 UTC+0200	2018-06-26 01:53 UTC+0200
☐	AlexaForBusinessGatewayExecution	0	2017-11-30 17:47 UTC+0200	2017-11-30 17:47 UTC+0200
☐	AlexaForBusinessReadOnlyAccess	0	2017-11-30 17:47 UTC+0200	2018-06-26 01:52 UTC+0200
☐	AmazonAPIGatewayAdministrator	0	2015-07-09 19:34 UTC+0200	2015-07-09 19:34 UTC+0200
☐	AmazonAPIGatewayInvokeFullAccess	0	2015-07-09 19:36 UTC+0200	2015-07-09 19:36 UTC+0200
☐	AmazonAPIGatewayPushToCloudW...	0	2015-11-12 00:41 UTC+0200	2015-11-12 00:41 UTC+0200
☐	AmazonAppStreamFullAccess	0	2015-02-06 19:40 UTC+0200	2018-09-10 19:29 UTC+0200
☐	AmazonAppStreamReadOnlyAccess	0	2015-02-06 19:40 UTC+0200	2016-12-07 22:00 UTC+0200
☐	AmazonAppStreamServiceAccess	0	2016-11-19 05:17 UTC+0200	2018-08-13 20:19 UTC+0200

Click Here

Click Here



Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

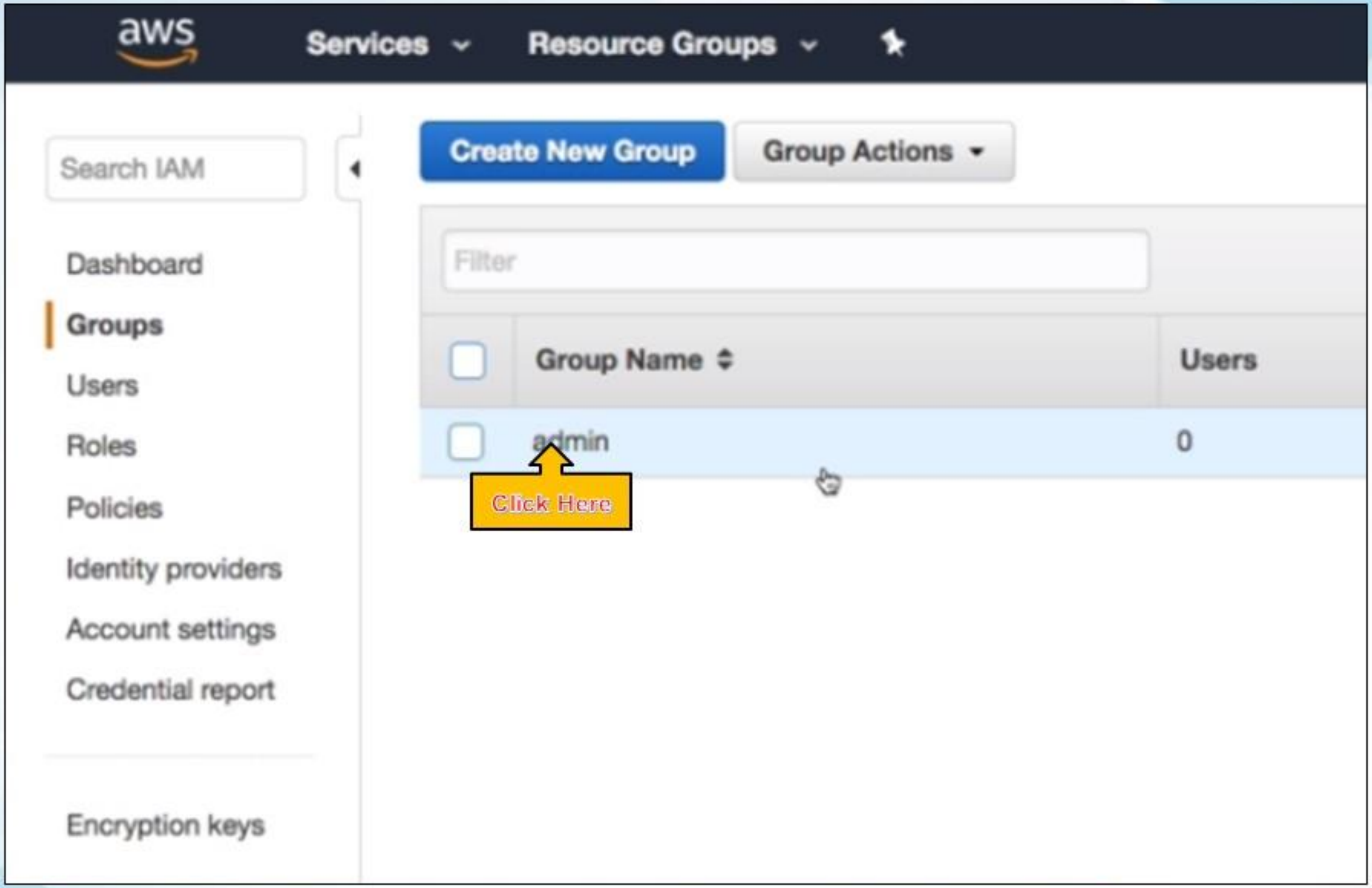
Step 3 : Review

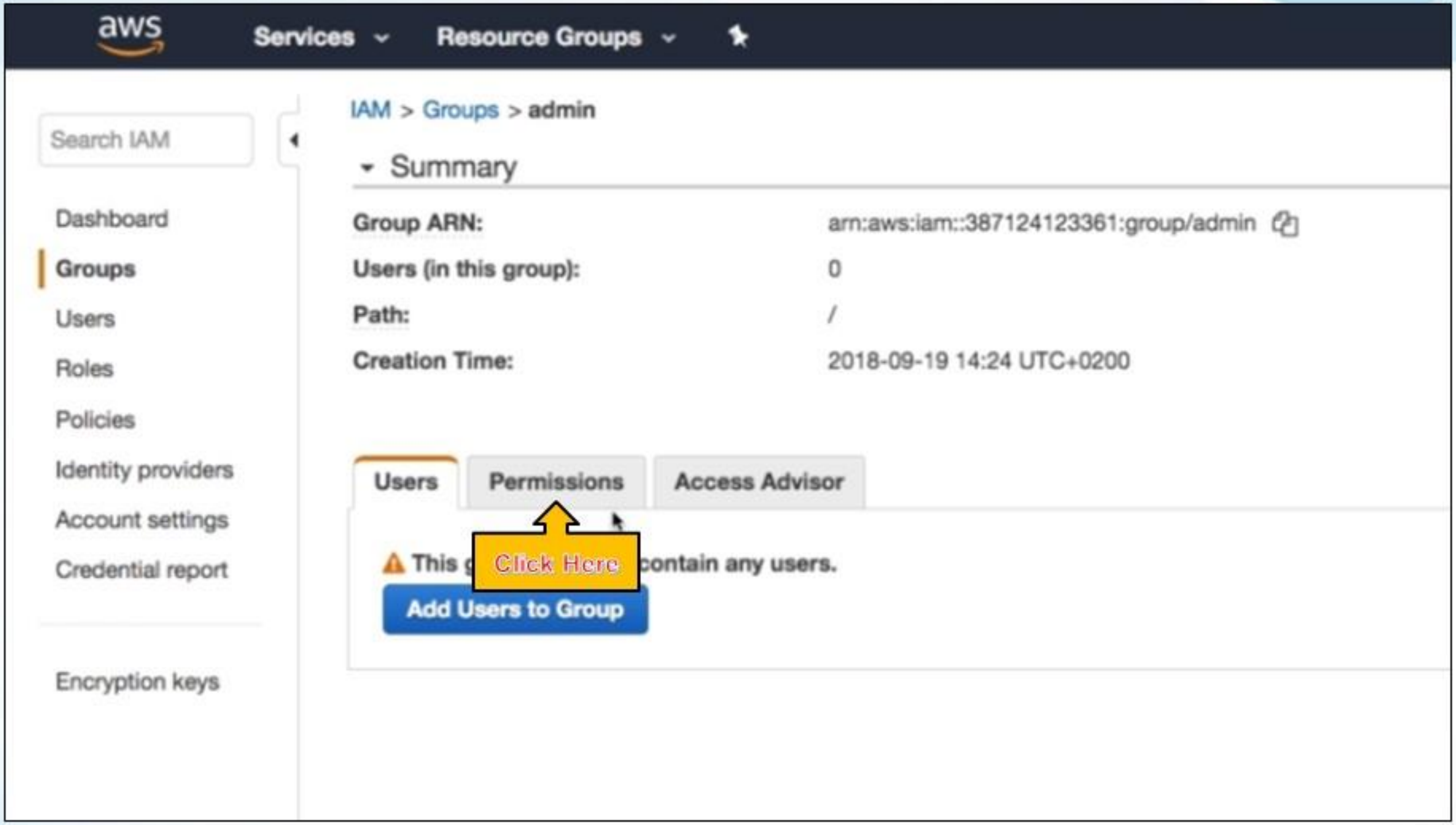
Review

Review the following information, then click **Create Group** to proceed.

Group Name	admin	Edit Group Name
Policies	arn:aws:iam::aws:policy/AdministratorAccess	Edit Policies

Click Here


aws
Services
Resource Groups
Search IAM
Dashboard
Groups
Users
Roles
Policies
Identity providers
Account settings
Credential report
Encryption keys
Create New Group
Group Actions
Filter
Group Name
Users
admin
0
Click Here

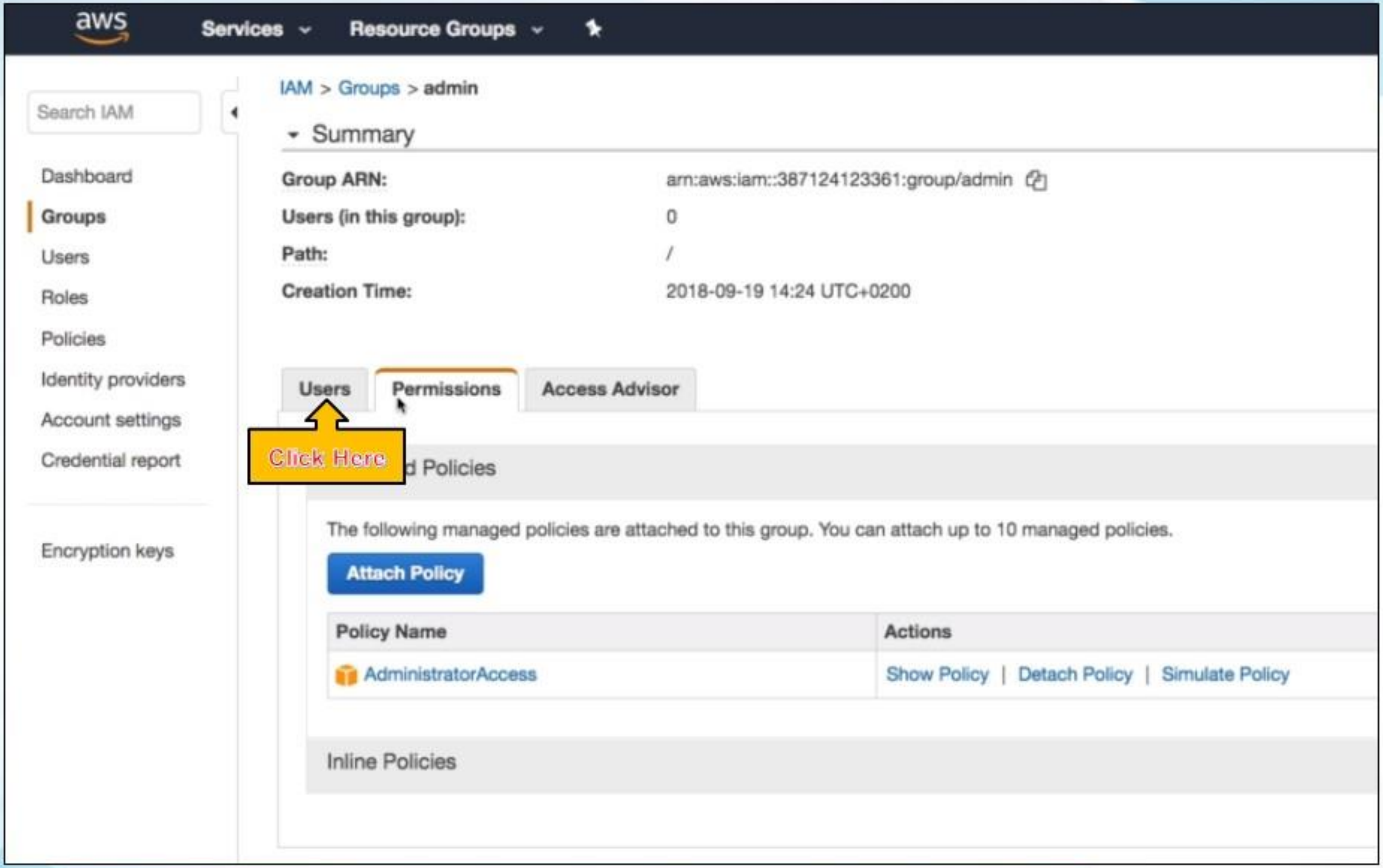


Group ARN: arn:aws:iam::387124123361:group/admin

Users (in this group): 0

Path: /

Creation Time: 2018-09-19 14:24 UTC+0200



IAM > Groups > admin

Summary

Group ARN: arn:aws:iam::387124123361:group/admin

Users (in this group): 0

Path: /

Creation Time: 2018-09-19 14:24 UTC+0200

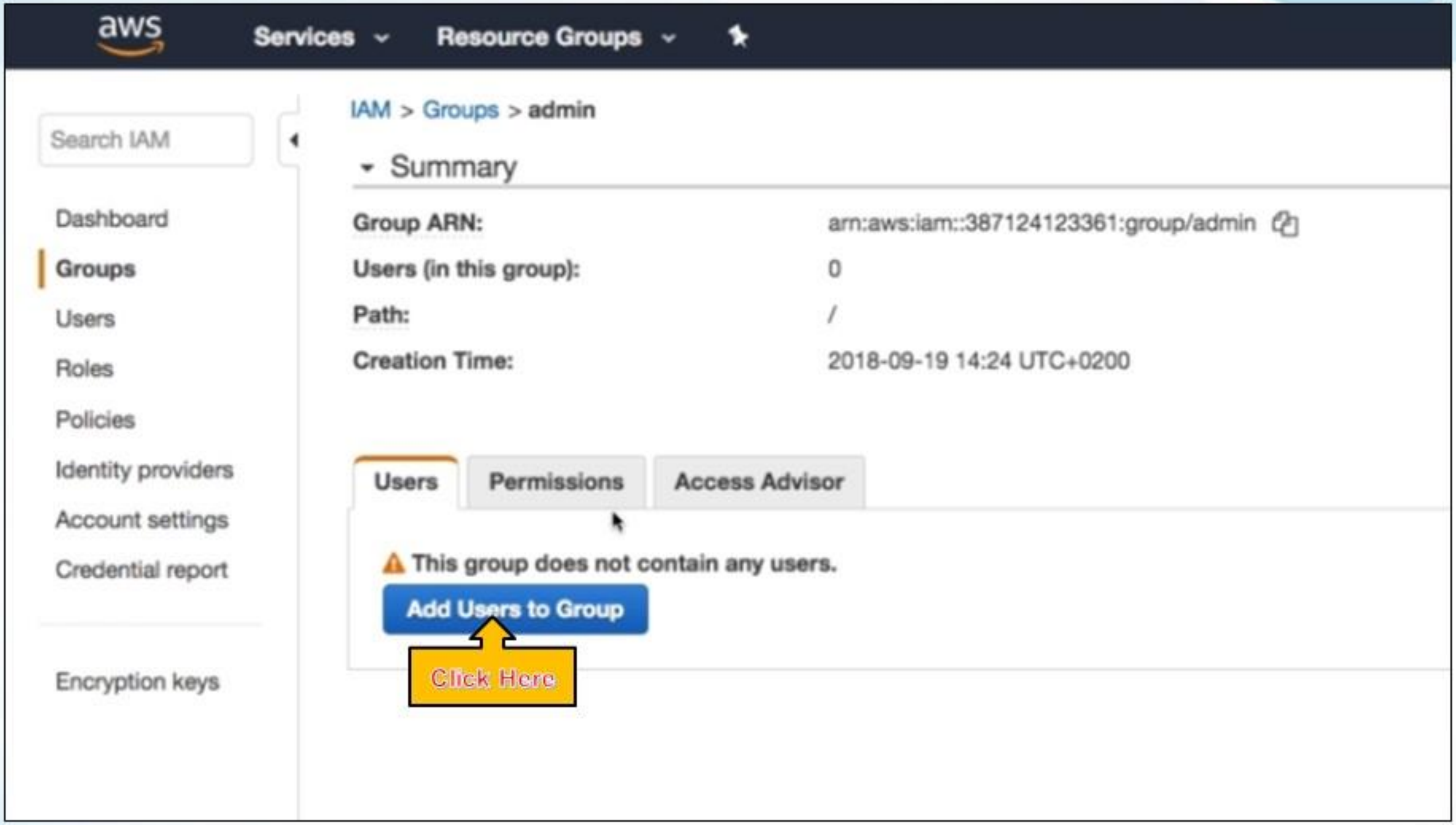
Click Here

d Policies

The following managed policies are attached to this group. You can attach up to 10 managed policies.

Policy Name	Actions
AdministratorAccess	Show Policy | Detach Policy | Simulate Policy

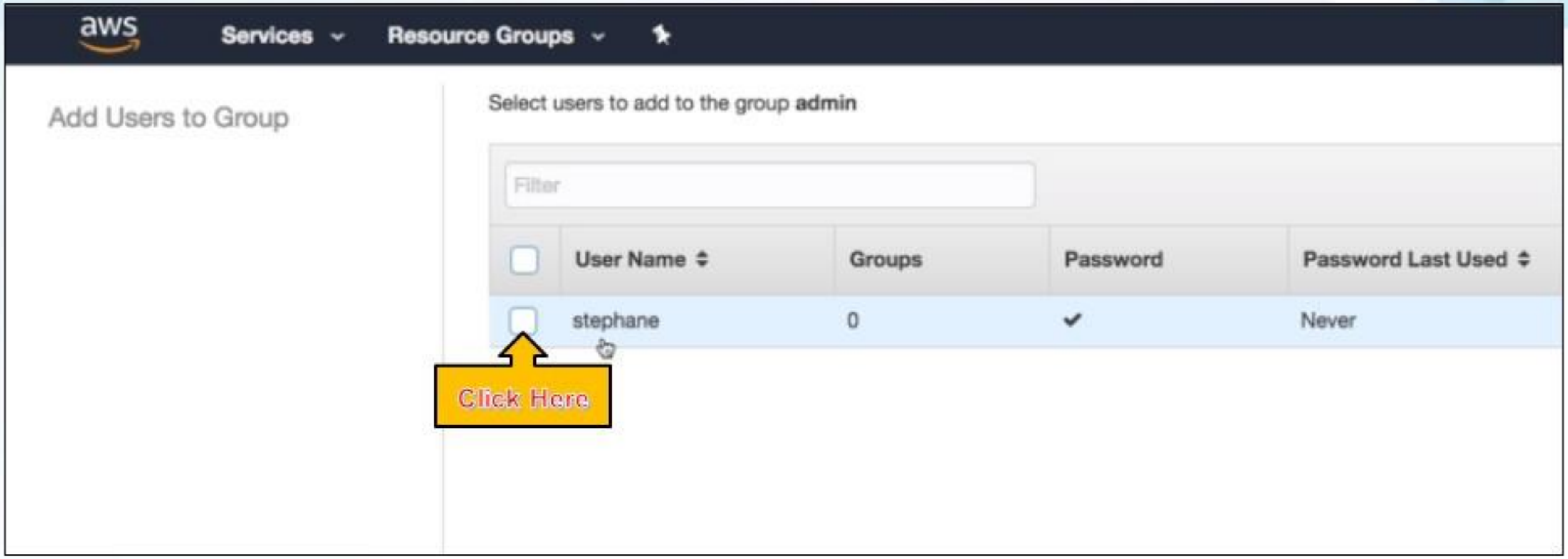
Inline Policies



Group ARN:	arn:aws:iam::387124123361:group/admin
Users (in this group):	0
Path:	/
Creation Time:	2018-09-19 14:24 UTC+0200

This group does not contain any users.

Click Here

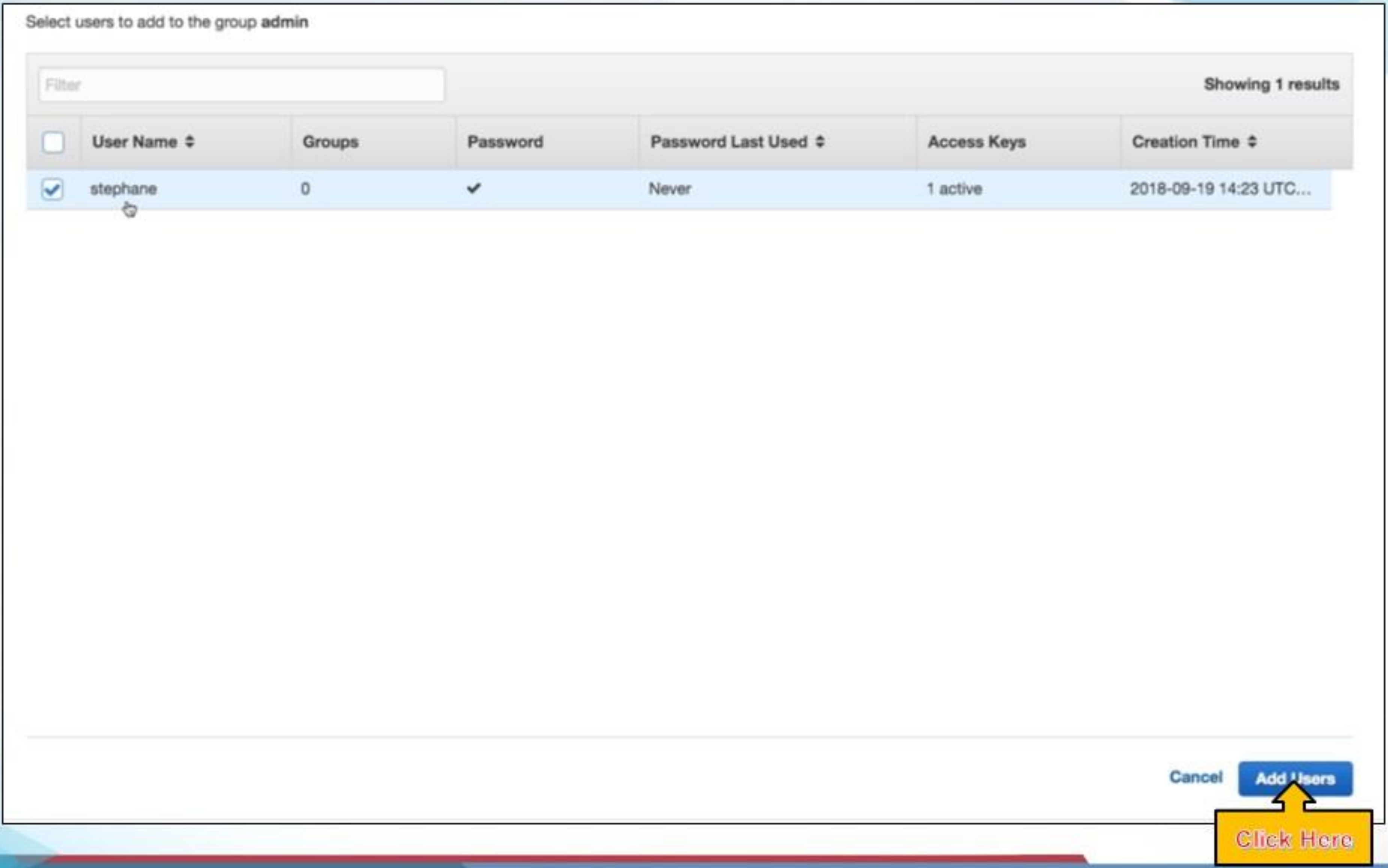


Add Users to Group

Select users to add to the group **admin**

□	User Name	Groups	Password	Password Last Used
□	stephane	0	✓	Never

Click Here

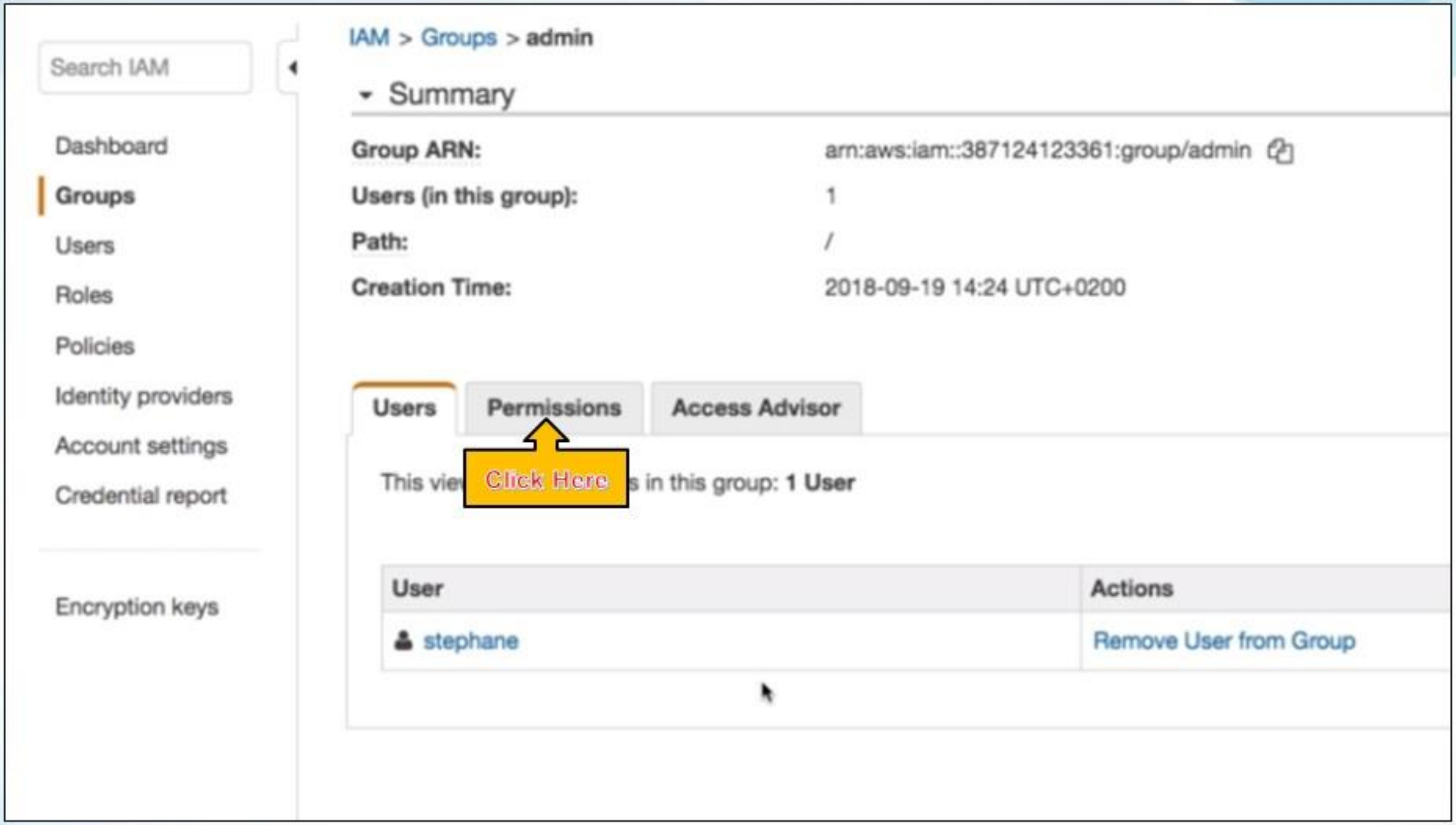


Select users to add to the group **admin**

Showing 1 results

□	User Name ⇕	Groups	Password	Password Last Used ⇕	Access Keys	Creation Time ⇕
☑	stephane	0	✓	Never	1 active	2018-09-19 14:23 UTC...

Click Here

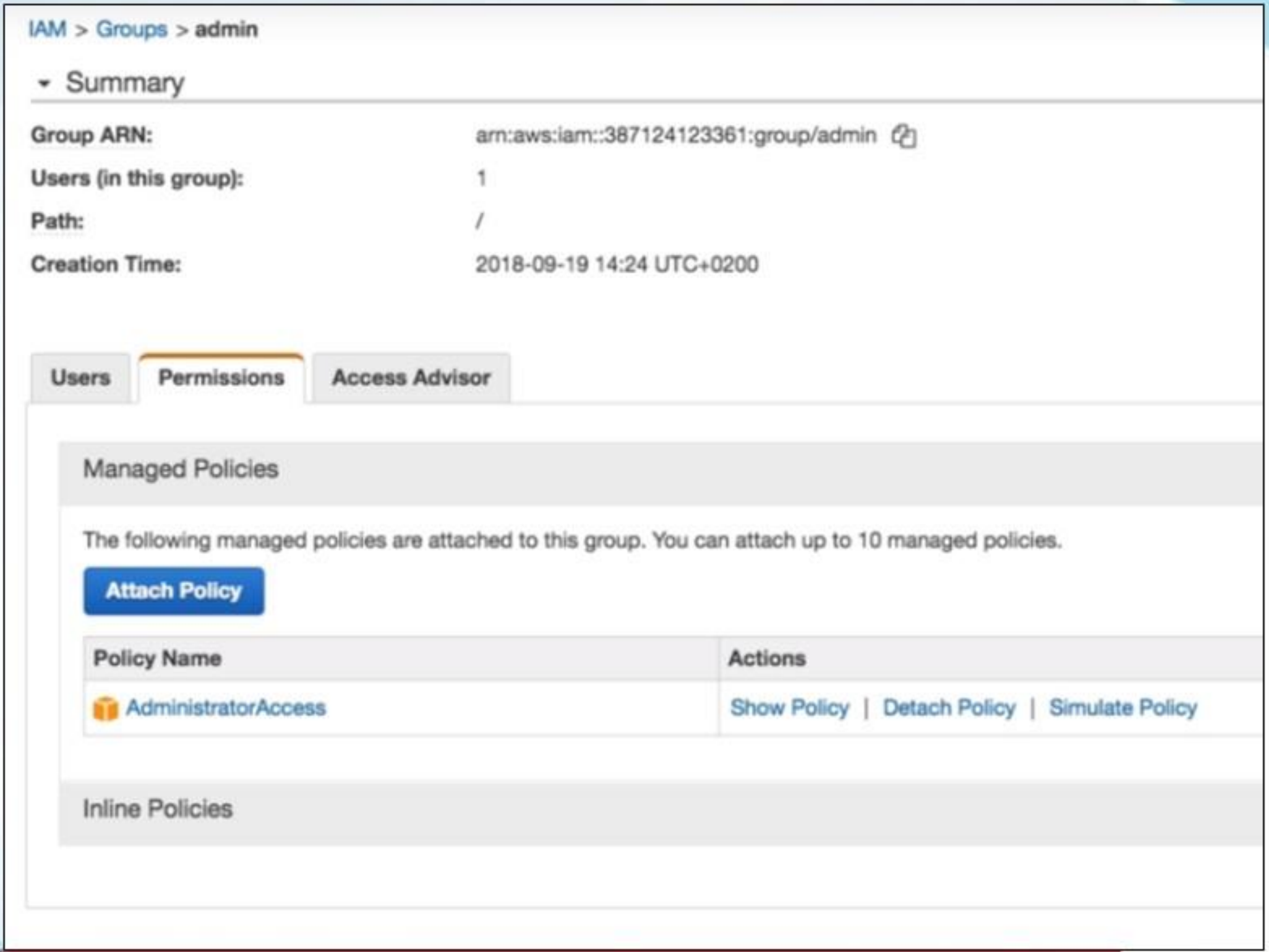


Group ARN:	arn:aws:iam::387124123361:group/admin
Users (in this group):	1
Path:	/
Creation Time:	2018-09-19 14:24 UTC+0200

This vie s in this group: **1 User**

User	Actions
stephane	Remove User from Group

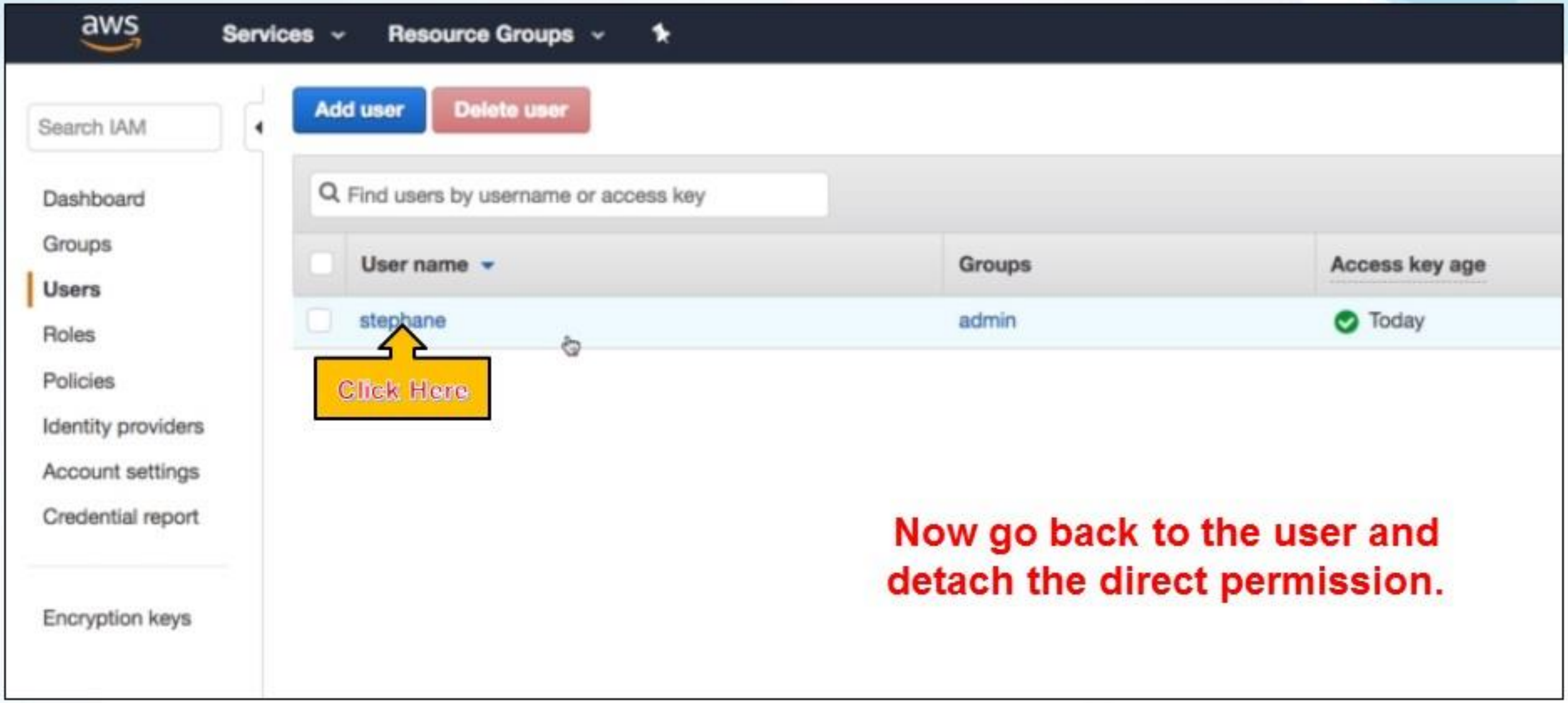
Click Here



Group ARN:	arn:aws:iam::387124123361:group/admin
Users (in this group):	1
Path:	/
Creation Time:	2018-09-19 14:24 UTC+0200

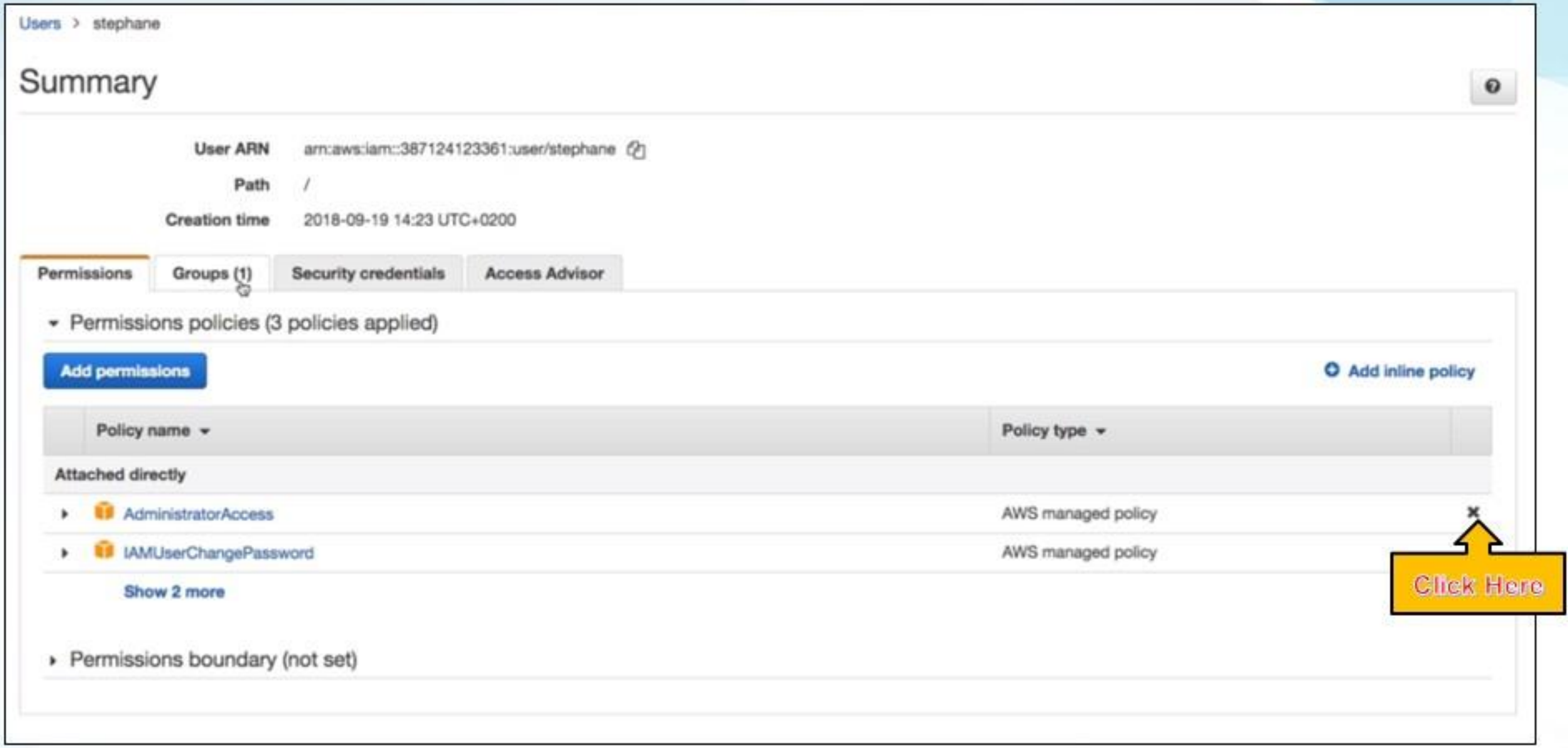
The following managed policies are attached to this group. You can attach up to 10 managed policies.

Policy Name	Actions
AdministratorAccess	Show Policy | Detach Policy | Simulate Policy



□	User name	Groups	Access key age
□	stephane	admin	✓ Today

Now go back to the user and detach the direct permission.



Users > stephane

Summary

User ARN arn:aws:iam::387124123361:user/stephane

Path /

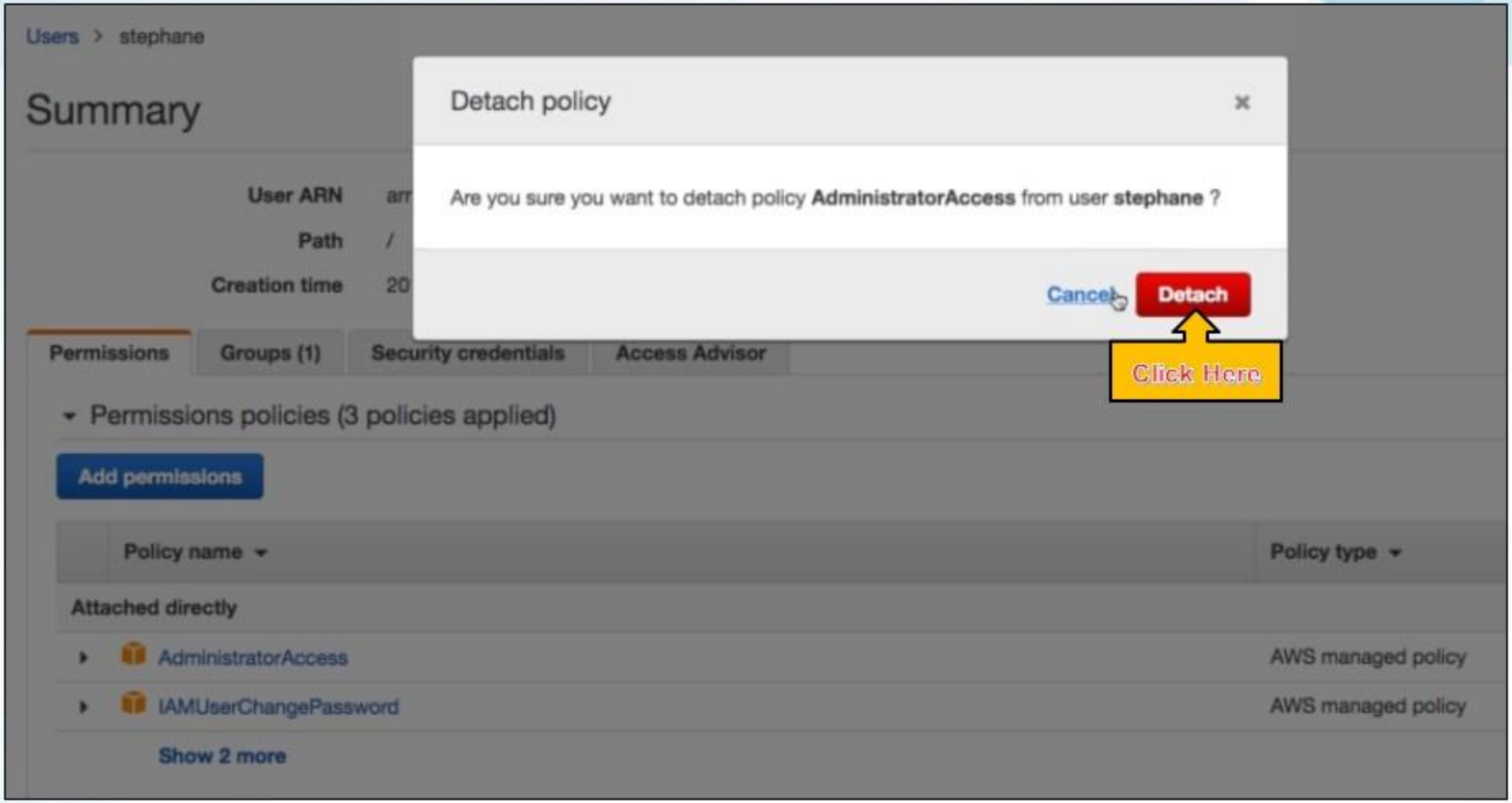
Creation time 2018-09-19 14:23 UTC+0200

▾ Permissions policies (3 policies applied)

Policy name ▾	Policy type ▾
Attached directly	
AdministratorAccess	AWS managed policy
IAMUserChangePassword	AWS managed policy

▸ Permissions boundary (not set)

Click Here



Users > stephane

Summary

User ARN ar

Path /

Creation time 20

Detach policy ×

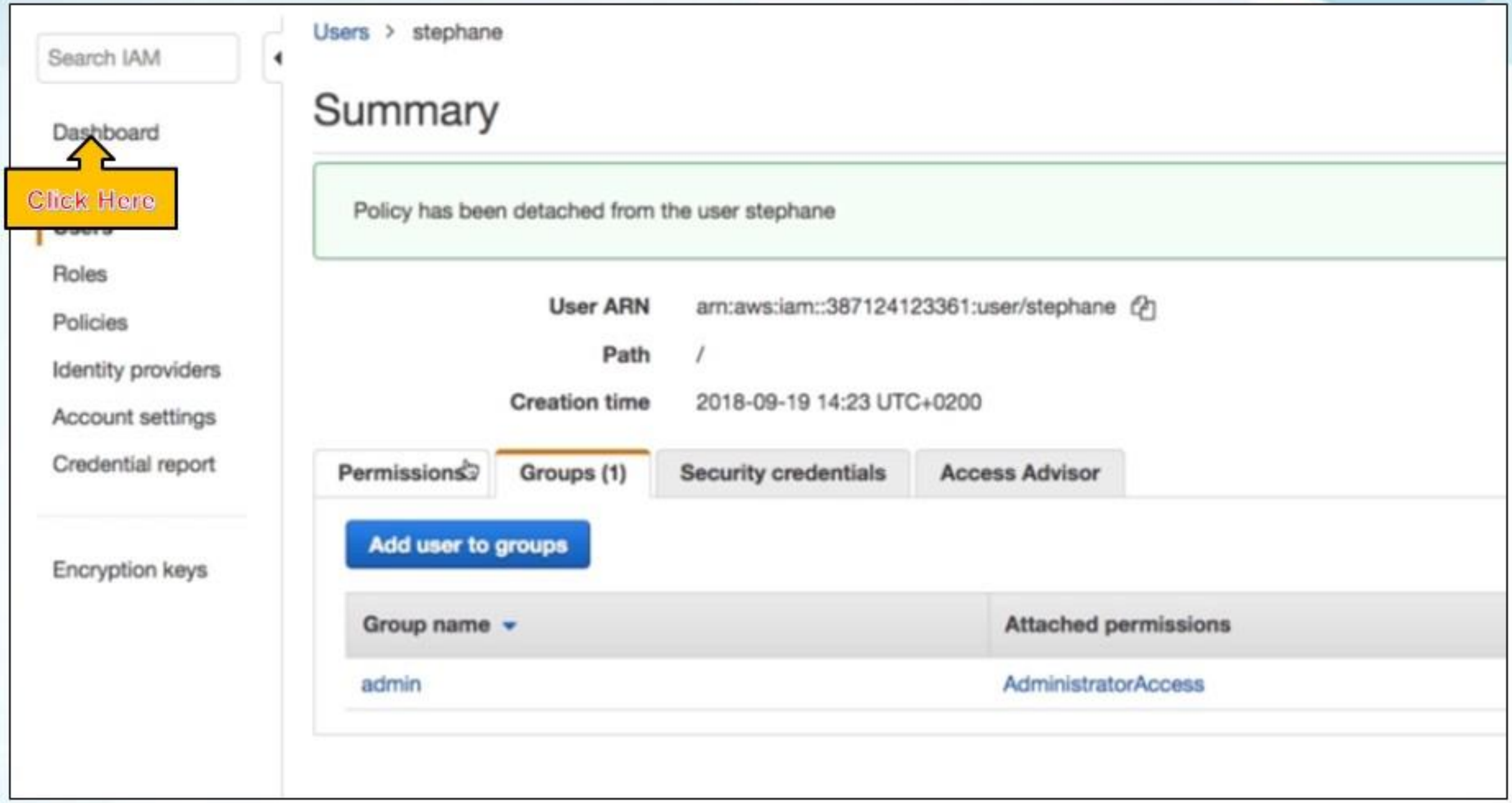
Are you sure you want to detach policy **AdministratorAccess** from user **stephane** ?

Cancel Detach

Click Here

Permissions policies (3 policies applied)

Policy name	Policy type
Attached directly	
AdministratorAccess	AWS managed policy
IAMUserChangePassword	AWS managed policy
Show 2 more	



Summary

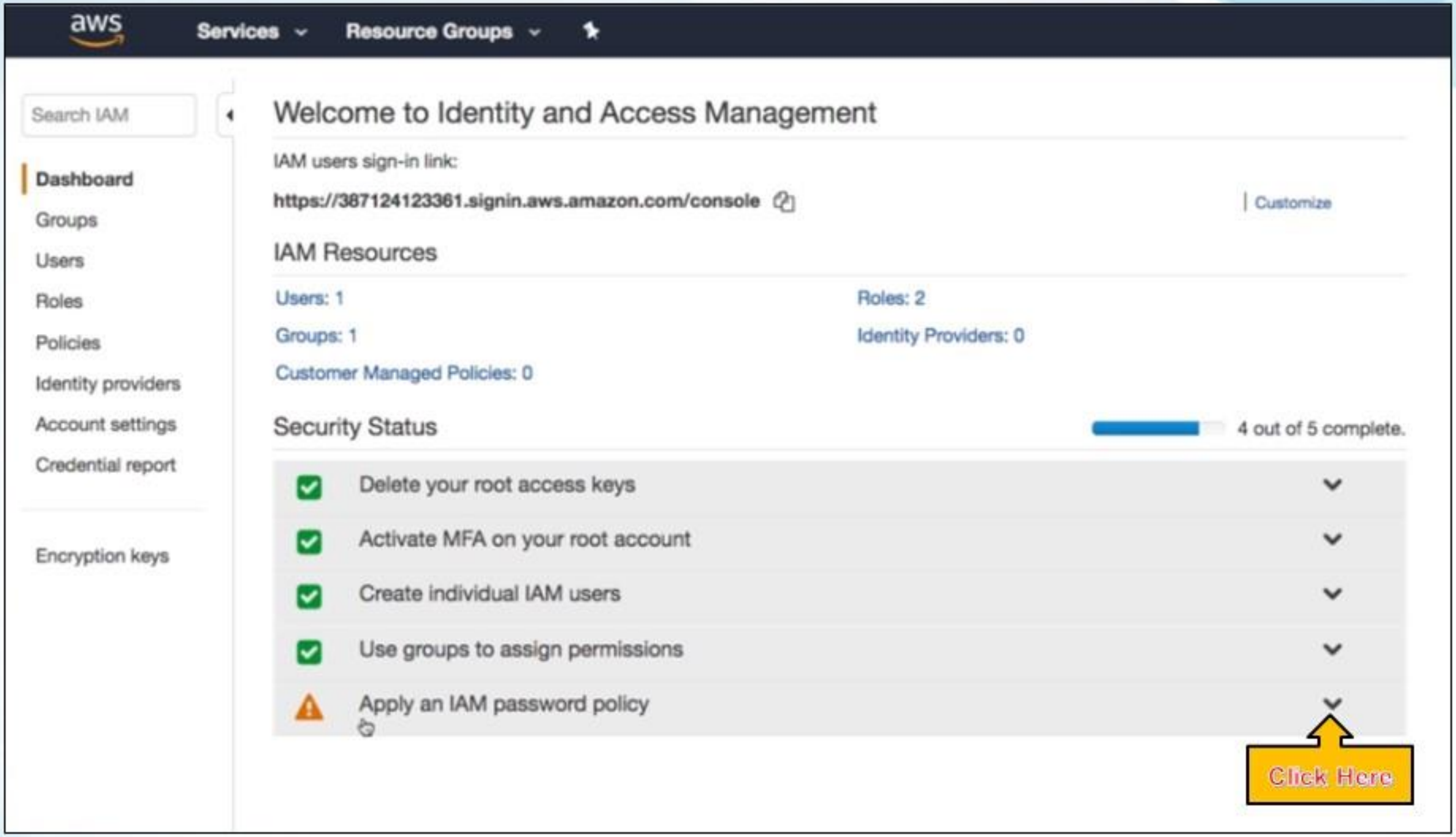
Policy has been detached from the user stephane

User ARN arn:aws:iam::387124123361:user/stephane

Path /

Creation time 2018-09-19 14:23 UTC+0200

Group name	Attached permissions
admin	AdministratorAccess



Welcome to Identity and Access Management

IAM users sign-in link:

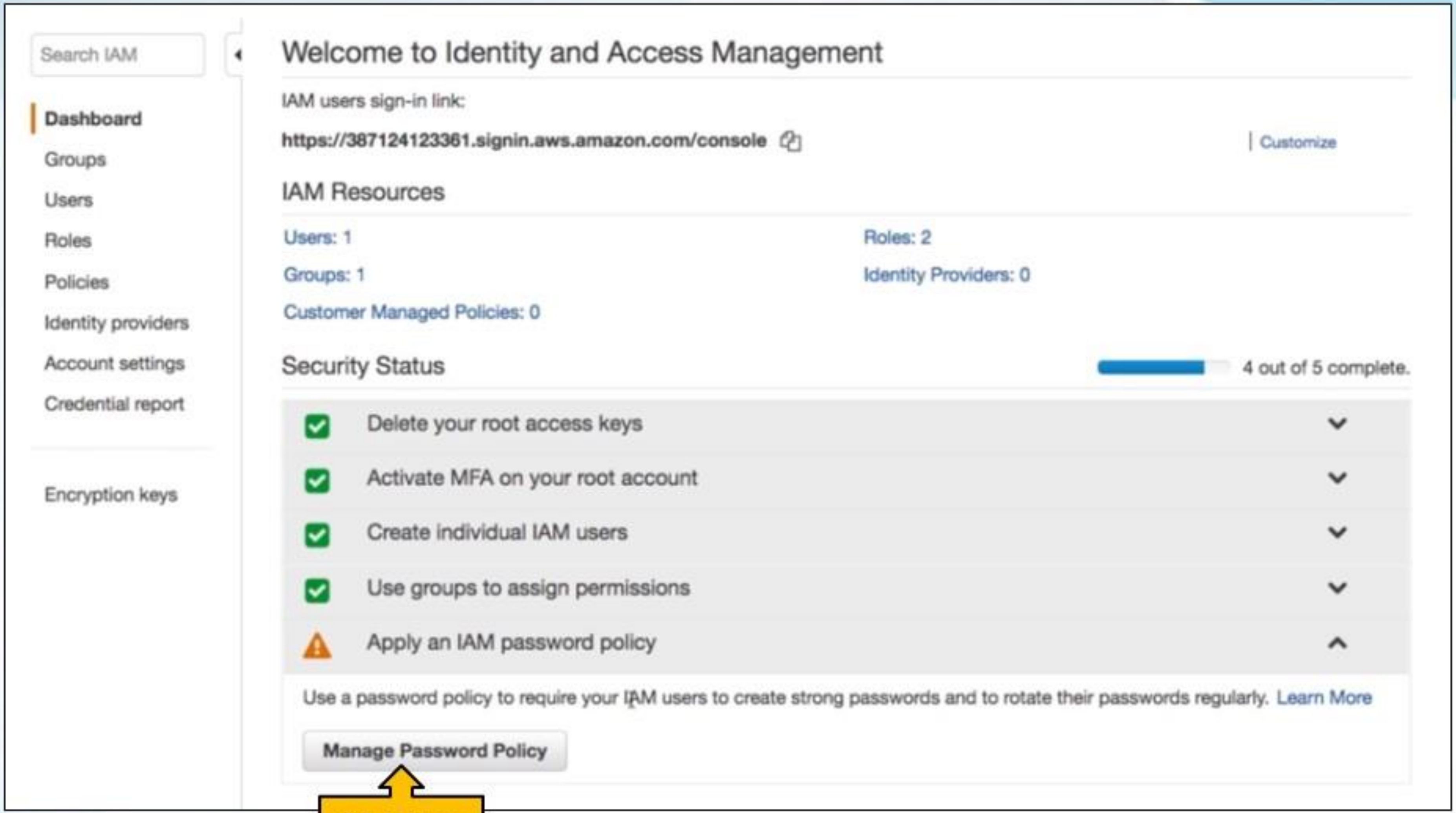
https://387124123361.signin.aws.amazon.com/console

IAM Resources

Users: 1	Roles: 2
Groups: 1	Identity Providers: 0
Customer Managed Policies: 0	

Security Status — 4 out of 5 complete.

- ✓ Delete your root access keys
- ✓ Activate MFA on your root account
- ✓ Create individual IAM users
- ✓ Use groups to assign permissions
- ⚠ Apply an IAM password policy



Welcome to Identity and Access Management

IAM users sign-in link:

https://387124123361.signin.aws.amazon.com/console

IAM Resources

Users: 1	Roles: 2
Groups: 1	Identity Providers: 0
Customer Managed Policies: 0	

Security Status

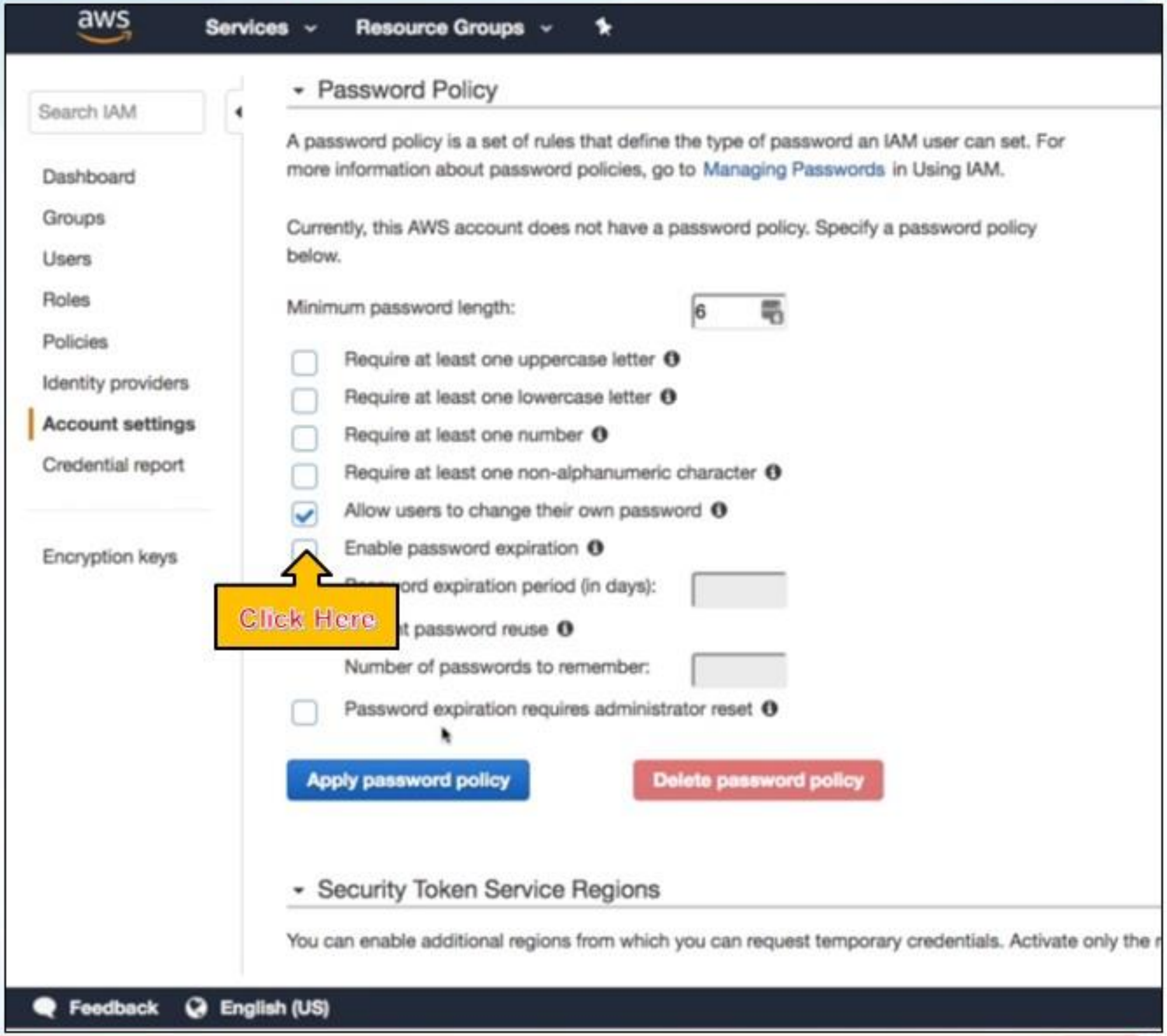
4 out of 5 complete.

- ☑ Delete your root access keys
- ☑ Activate MFA on your root account
- ☑ Create individual IAM users
- ☑ Use groups to assign permissions
- ⚠ Apply an IAM password policy

Use a password policy to require your IAM users to create strong passwords and to rotate their passwords regularly. Learn More

Manage Password Policy

Click Here



Password Policy

A password policy is a set of rules that define the type of password an IAM user can set. For more information about password policies, go to Managing Passwords in Using IAM.

Currently, this AWS account does not have a password policy. Specify a password policy below.

Minimum password length: 6

□ Require at least one uppercase letter

□ Require at least one lowercase letter

□ Require at least one number

□ Require at least one non-alphanumeric character

☑ Allow users to change their own password

□ Enable password expiration

ord expiration period (in days):

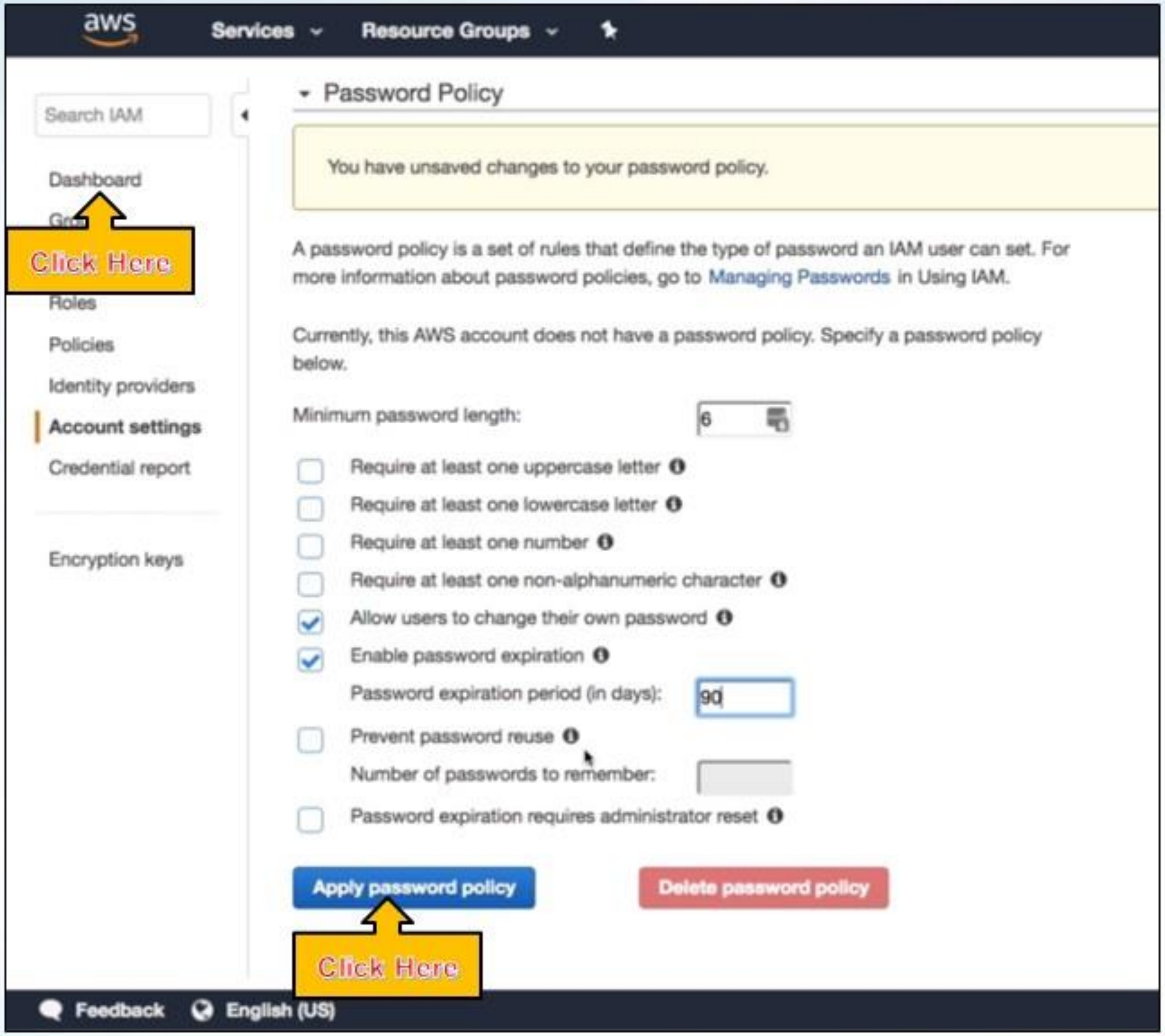
t password reuse

Number of passwords to remember:

□ Password expiration requires administrator reset

Security Token Service Regions

You can enable additional regions from which you can request temporary credentials. Activate only the



Click Here

Password Policy

You have unsaved changes to your password policy.

A password policy is a set of rules that define the type of password an IAM user can set. For more information about password policies, go to Managing Passwords in Using IAM.

Currently, this AWS account does not have a password policy. Specify a password policy below.

Minimum password length: 6

□ Require at least one uppercase letter

□ Require at least one lowercase letter

□ Require at least one number

□ Require at least one non-alphanumeric character

☑ Allow users to change their own password

☑ Enable password expiration

Password expiration period (in days): 90

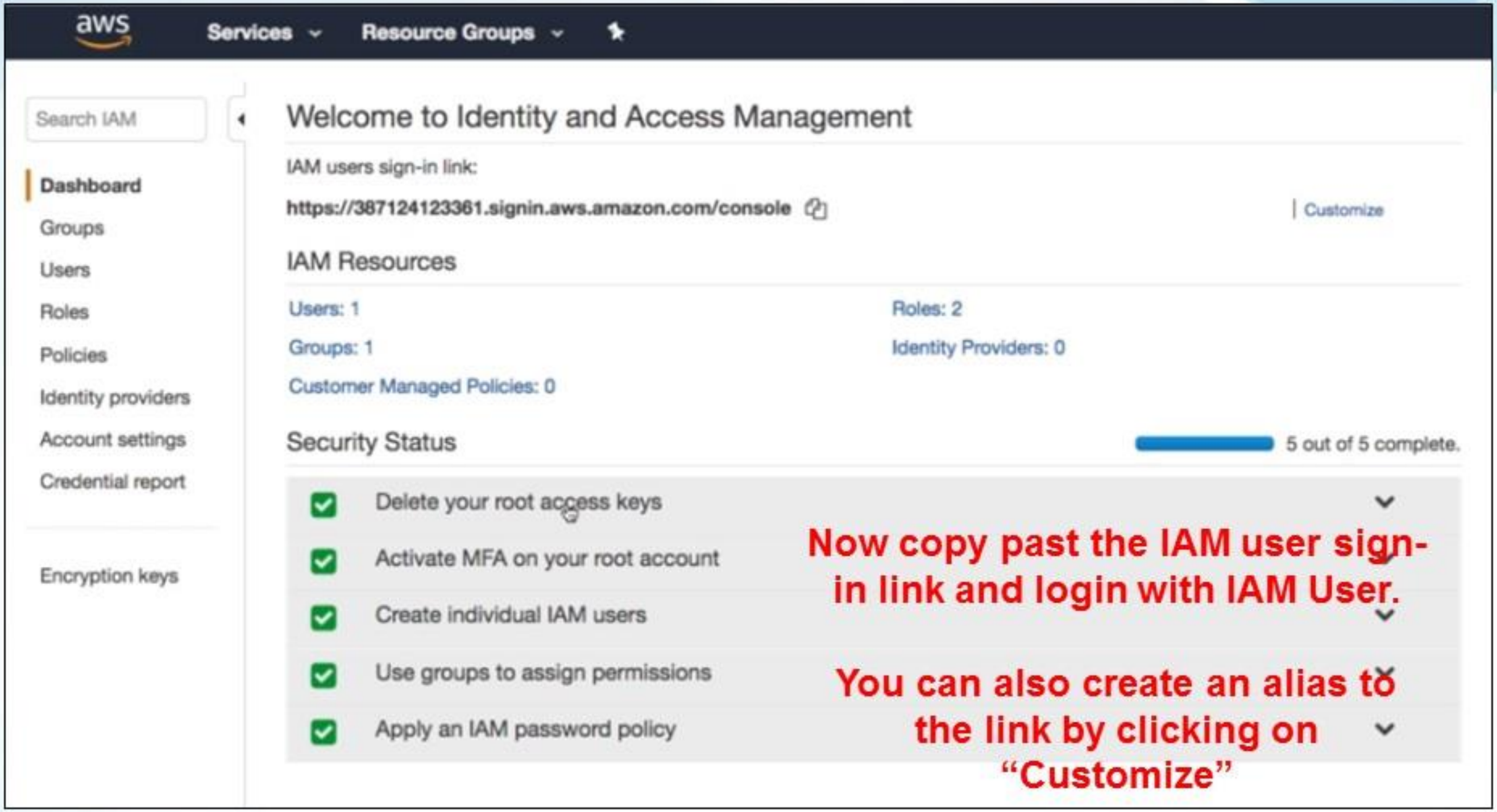
□ Prevent password reuse

Number of passwords to remember:

□ Password expiration requires administrator reset

Click Here

SkillAssure



Welcome to Identity and Access Management

IAM users sign-in link:

https://387124123361.signin.aws.amazon.com/console

Customize

IAM Resources

Users: 1

Groups: 1

Customer Managed Policies: 0

Roles: 2

Identity Providers: 0

Security Status

5 out of 5 complete.

☑ Delete your root access keys

☑ Activate MFA on your root account

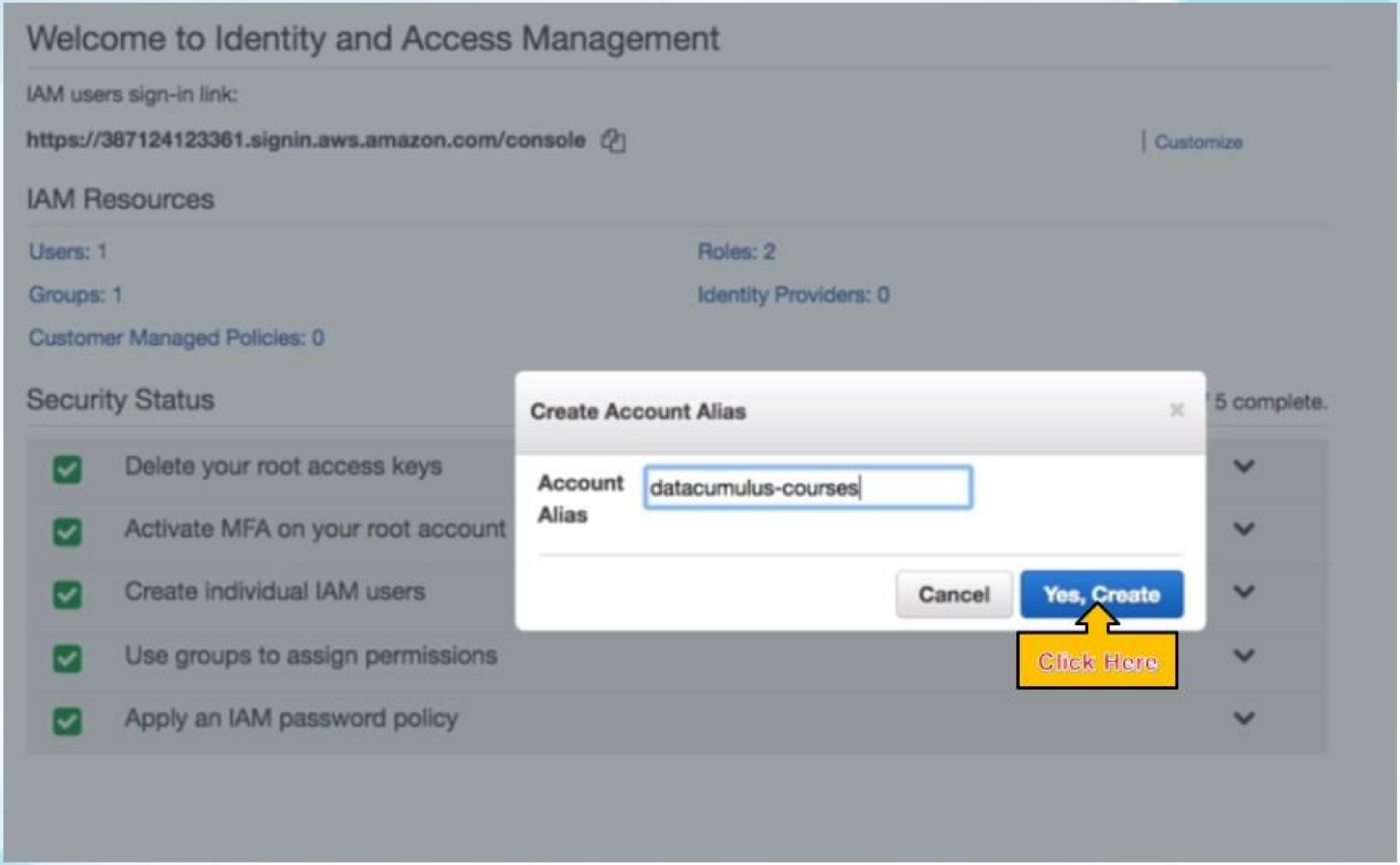
☑ Create individual IAM users

☑ Use groups to assign permissions

☑ Apply an IAM password policy

Now copy past the IAM user sign-in link and login with IAM User.

You can also create an alias to the link by clicking on "Customize"



Welcome to Identity and Access Management

IAM users sign-in link:

https://387124123361.signin.aws.amazon.com/console

IAM Resources

Users: 1

Roles: 2

Groups: 1

Identity Providers: 0

Customer Managed Policies: 0

Security Status

5 complete.

☑ Delete your root access keys

☑ Activate MFA on your root account

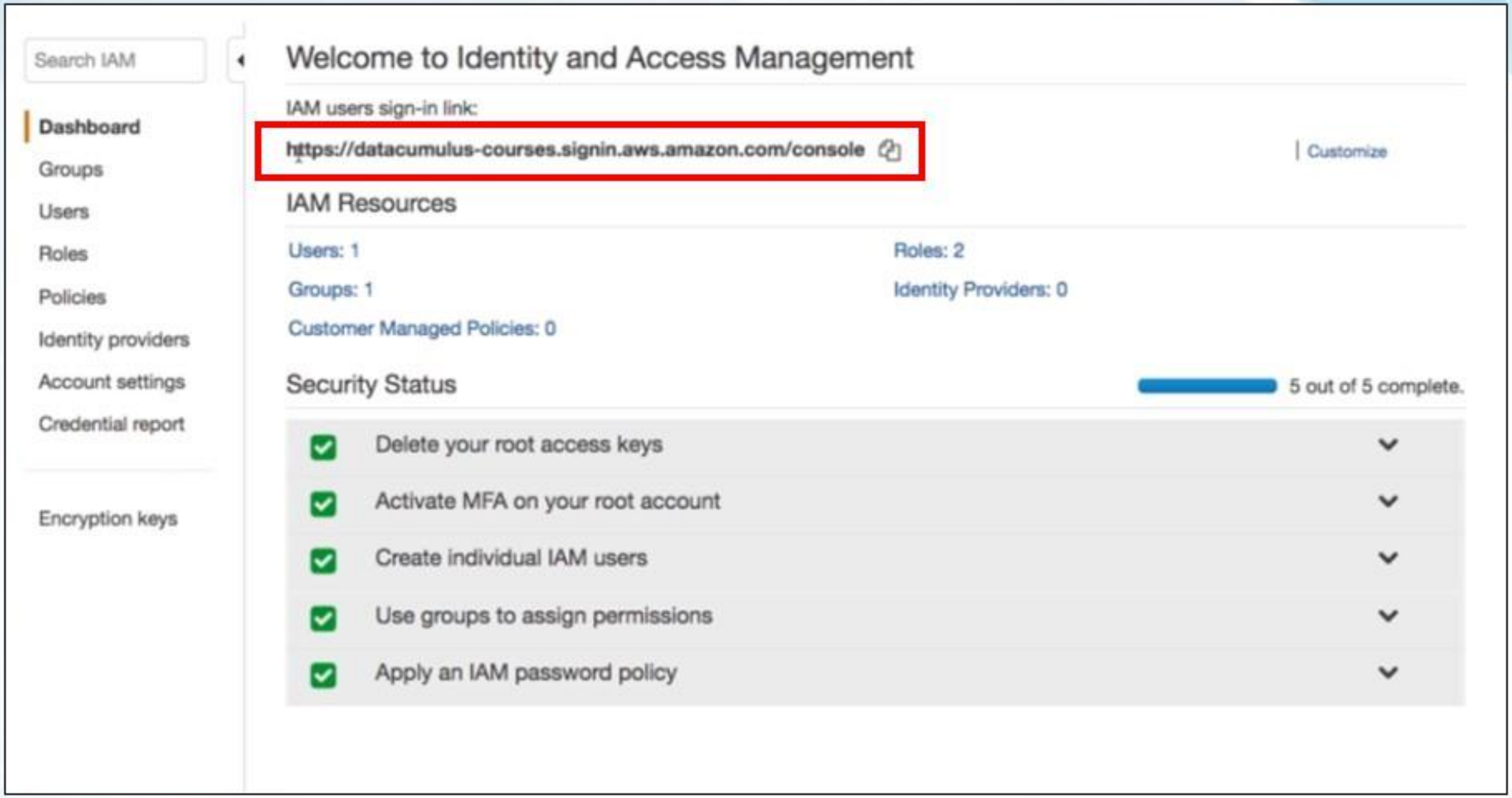
☑ Create individual IAM users

☑ Use groups to assign permissions

☑ Apply an IAM password policy

Create Account Alias

Account Alias: datacumulus-courses



Search IAM

- Dashboard
- Groups
- Users
- Roles
- Policies
- Identity providers
- Account settings
- Credential report
- Encryption keys

Welcome to Identity and Access Management

IAM users sign-in link:

https://datacumulus-courses.signin.aws.amazon.com/console

Customize

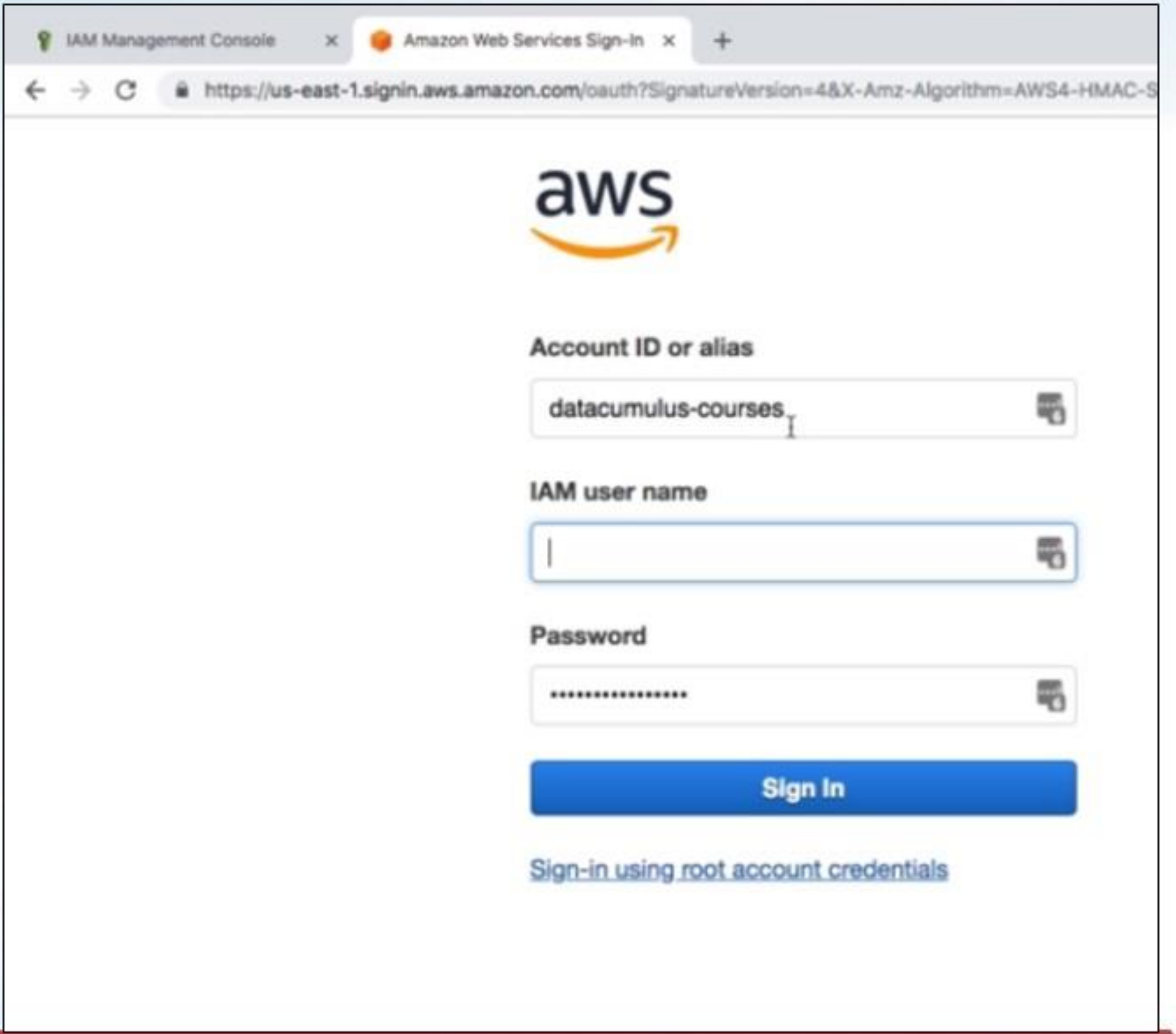
IAM Resources

Users: 1	Roles: 2
Groups: 1	Identity Providers: 0
Customer Managed Policies: 0	

Security Status

5 out of 5 complete.

- ☑ Delete your root access keys
- ☑ Activate MFA on your root account
- ☑ Create individual IAM users
- ☑ Use groups to assign permissions
- ☑ Apply an IAM password policy



IAM Management Console
Amazon Web Services Sign-In
https://us-east-1.signin.aws.amazon.com/oauth?SignatureVersion=4&X-Amz-Algorithm=AWS4-HMAC-S
aws

Account ID or alias

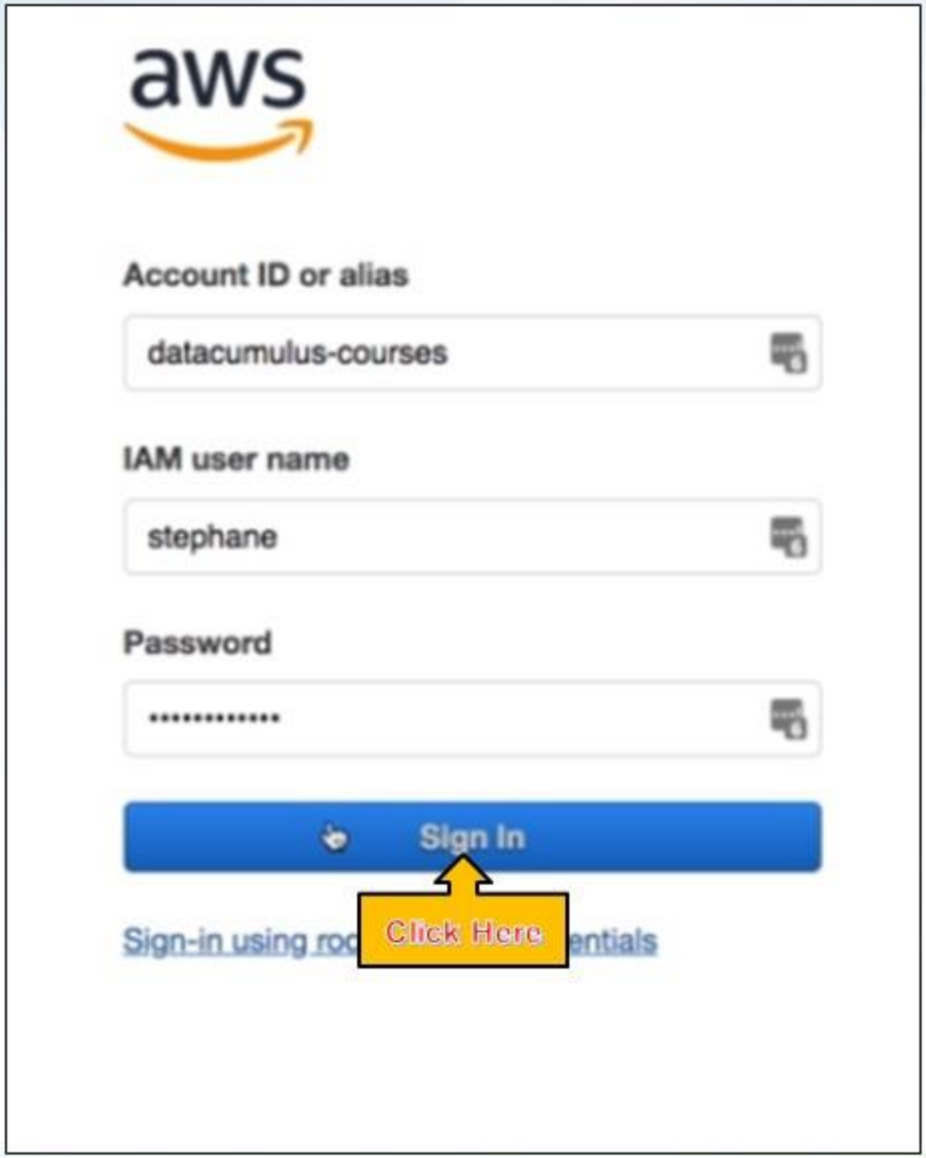
datacumulus-courses

IAM user name

Password

•••••••••••••••••

Sign In
Sign-in using root account credentials



Account ID or alias

datacumulus-courses

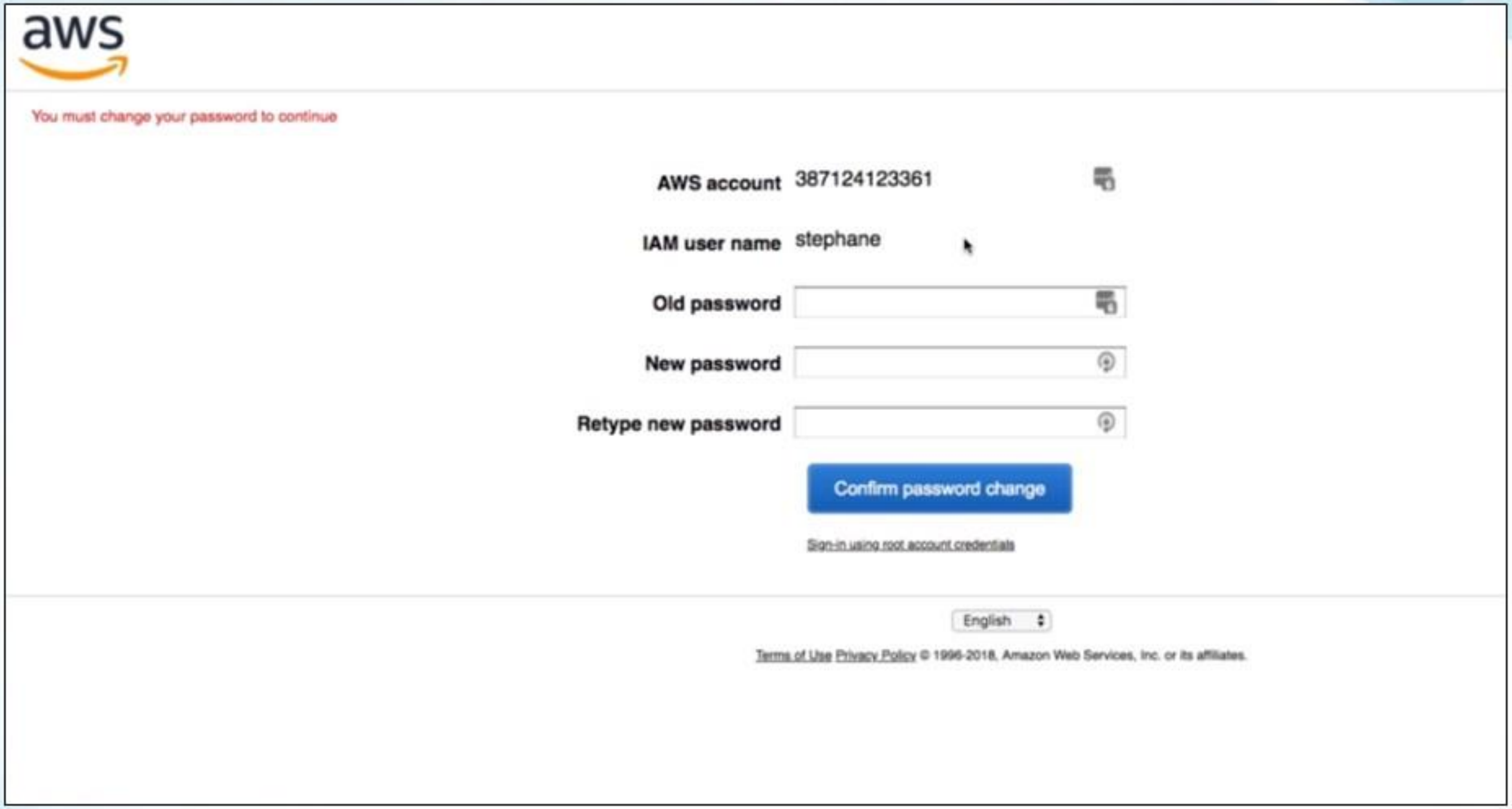
IAM user name

stephane

Password

•••••••••••••

Click Here



You must change your password to continue

AWS account 387124123361

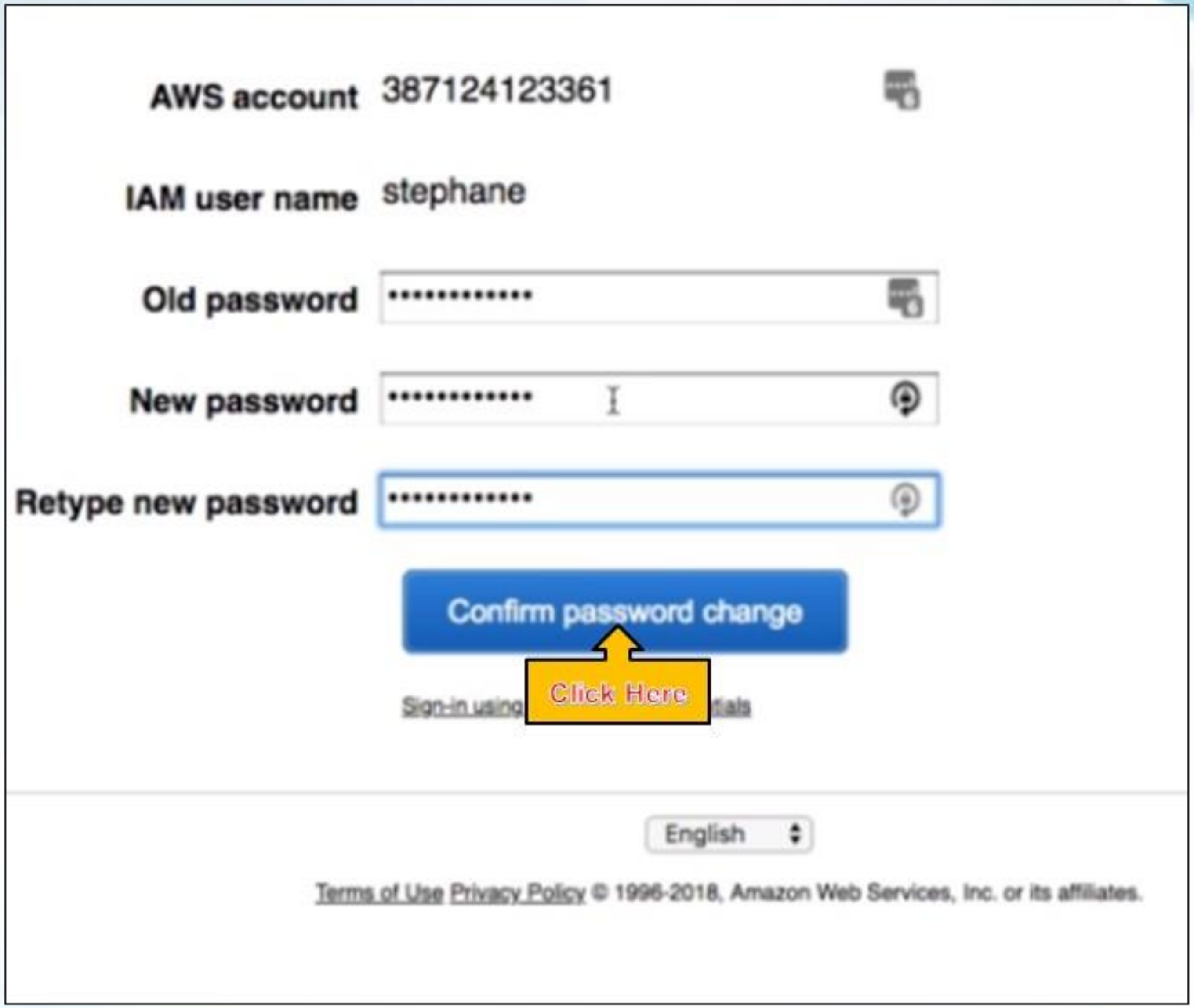
IAM user name stephane

Old password

New password

Retype new password

Terms of Use Privacy Policy © 1996-2018, Amazon Web Services, Inc. or its affiliates.



AWS account 387124123361

IAM user name stephane

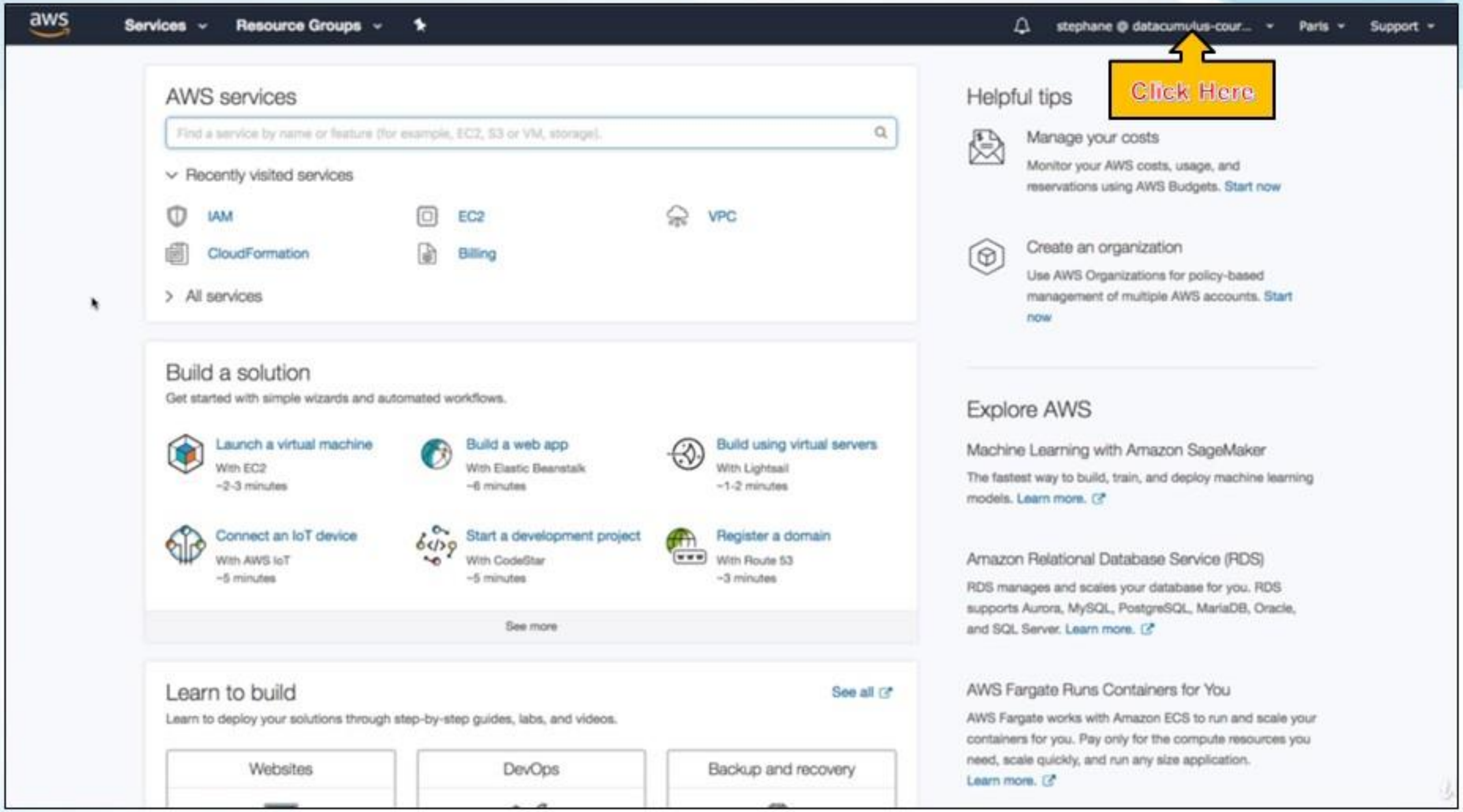
Old password •••••••••••••

New password •••••••••••••

Retype new password •••••••••••••

Click Here

Terms of Use Privacy Policy © 1996-2018, Amazon Web Services, Inc. or its affiliates.



Click Here

AWS services

Find a service by name or feature (for example, EC2, S3 or VM, storage).

Recently visited services

- IAM
- EC2
- VPC
- CloudFormation
- Billing

All services

Build a solution

Get started with simple wizards and automated workflows.

- Launch a virtual machine
  With EC2
  ~2-3 minutes
- Build a web app
  With Elastic Beanstalk
  ~6 minutes
- Build using virtual servers
  With Lightsail
  ~1-2 minutes
- Connect an IoT device
  With AWS IoT
  ~5 minutes
- Start a development project
  With CodeStar
  ~5 minutes
- Register a domain
  With Route 53
  ~3 minutes

See more

Learn to build

See all

Learn to deploy your solutions through step-by-step guides, labs, and videos.

Websites | DevOps | Backup and recovery

Helpful tips

Manage your costs

Monitor your AWS costs, usage, and reservations using AWS Budgets. Start now

Create an organization

Use AWS Organizations for policy-based management of multiple AWS accounts. Start now

Explore AWS

Machine Learning with Amazon SageMaker

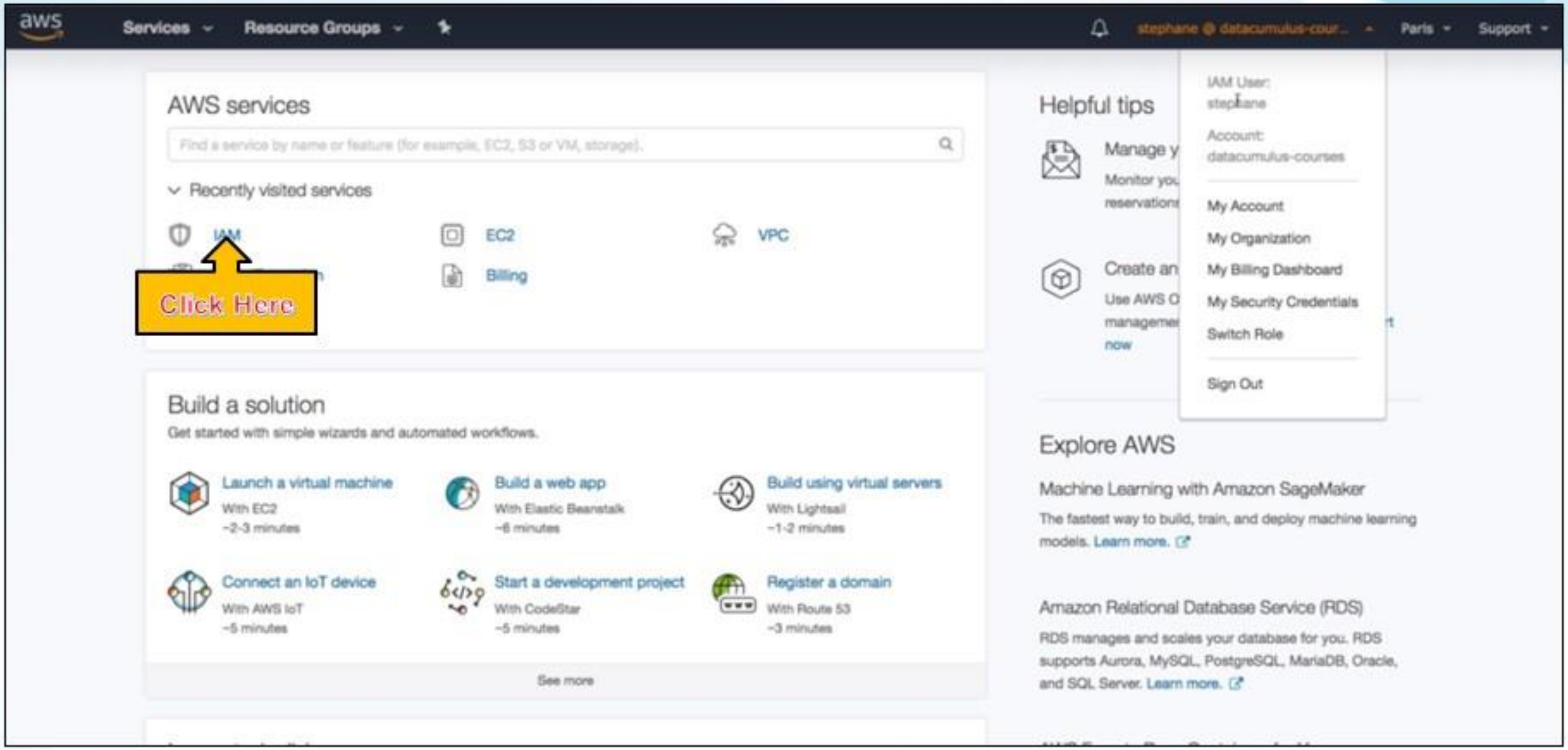
The fastest way to build, train, and deploy machine learning models. Learn more.

Amazon Relational Database Service (RDS)

RDS manages and scales your database for you. RDS supports Aurora, MySQL, PostgreSQL, MariaDB, Oracle, and SQL Server. Learn more.

AWS Fargate Runs Containers for You

AWS Fargate works with Amazon ECS to run and scale your containers for you. Pay only for the compute resources you need, scale quickly, and run any size application. Learn more.



AWS services

Find a service by name or feature (for example, EC2, S3 or VM, storage).

Helpful tips

Build a solution

Get started with simple wizards and automated workflows.

Launch a virtual machine
With EC2
~2-3 minutes

Build a web app
With Elastic Beanstalk
~6 minutes

Build using virtual servers
With Lightsail
~1-2 minutes

Connect an IoT device
With AWS IoT
~5 minutes

Start a development project
With CodeStar
~5 minutes

Register a domain
With Route 53
~3 minutes

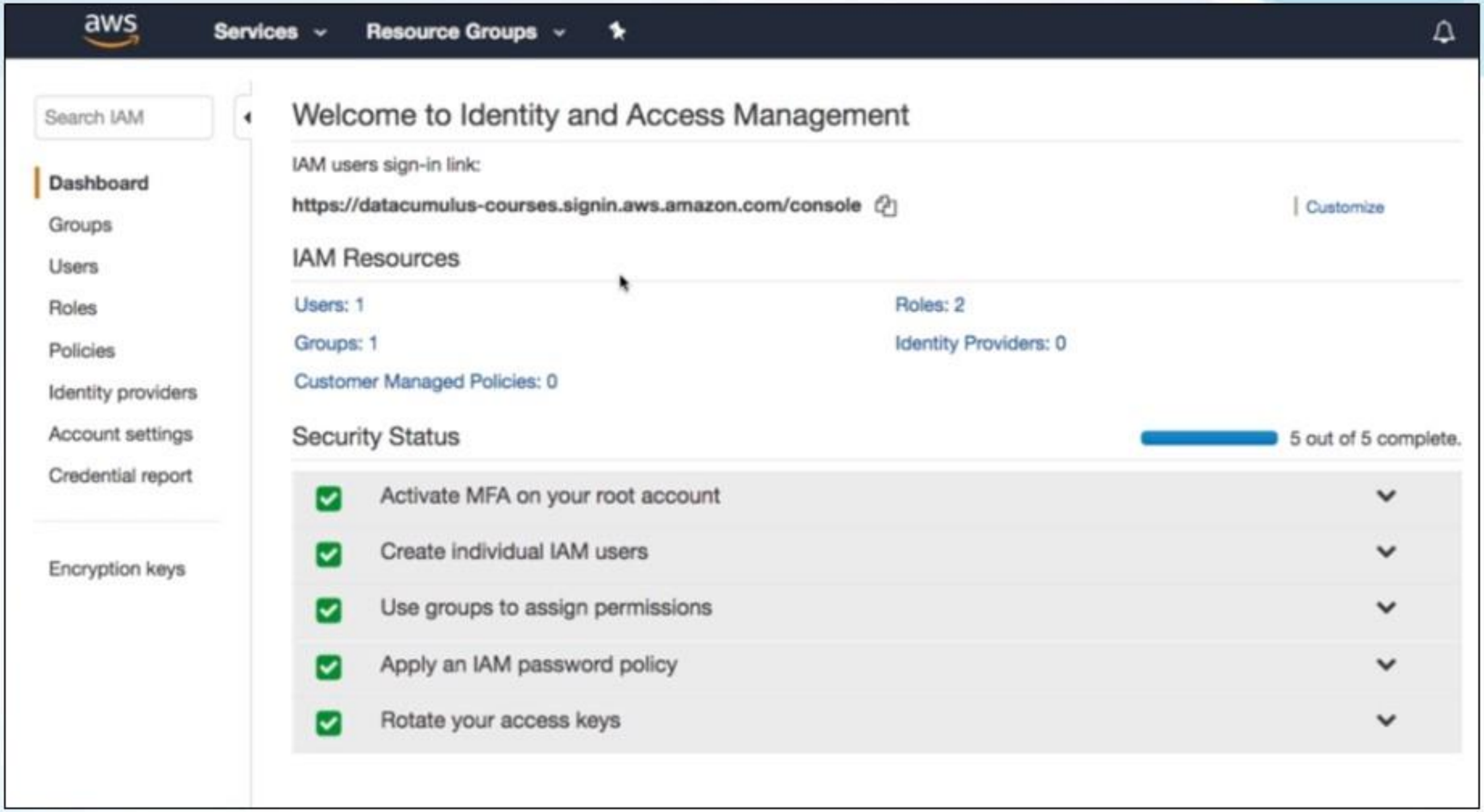
Explore AWS

Machine Learning with Amazon SageMaker

The fastest way to build, train, and deploy machine learning models. Learn more.

Amazon Relational Database Service (RDS)

RDS manages and scales your database for you. RDS supports Aurora, MySQL, PostgreSQL, MariaDB, Oracle, and SQL Server. Learn more.



Welcome to Identity and Access Management

IAM users sign-in link:

https://datacumulus-courses.signin.aws.amazon.com/console

IAM Resources

Users: 1

Roles: 2

Groups: 1

Identity Providers: 0

Customer Managed Policies: 0

Security Status

5 out of 5 complete.

- ☑ Activate MFA on your root account
- ☑ Create individual IAM users
- ☑ Use groups to assign permissions
- ☑ Apply an IAM password policy
- ☑ Rotate your access keys

Exercise

Alice in an intern who has joined your organization as an intern System Administrator. Since your infrastructure is hosted in AWS, you need to give access to Alice to view the AWS console.

Thank You