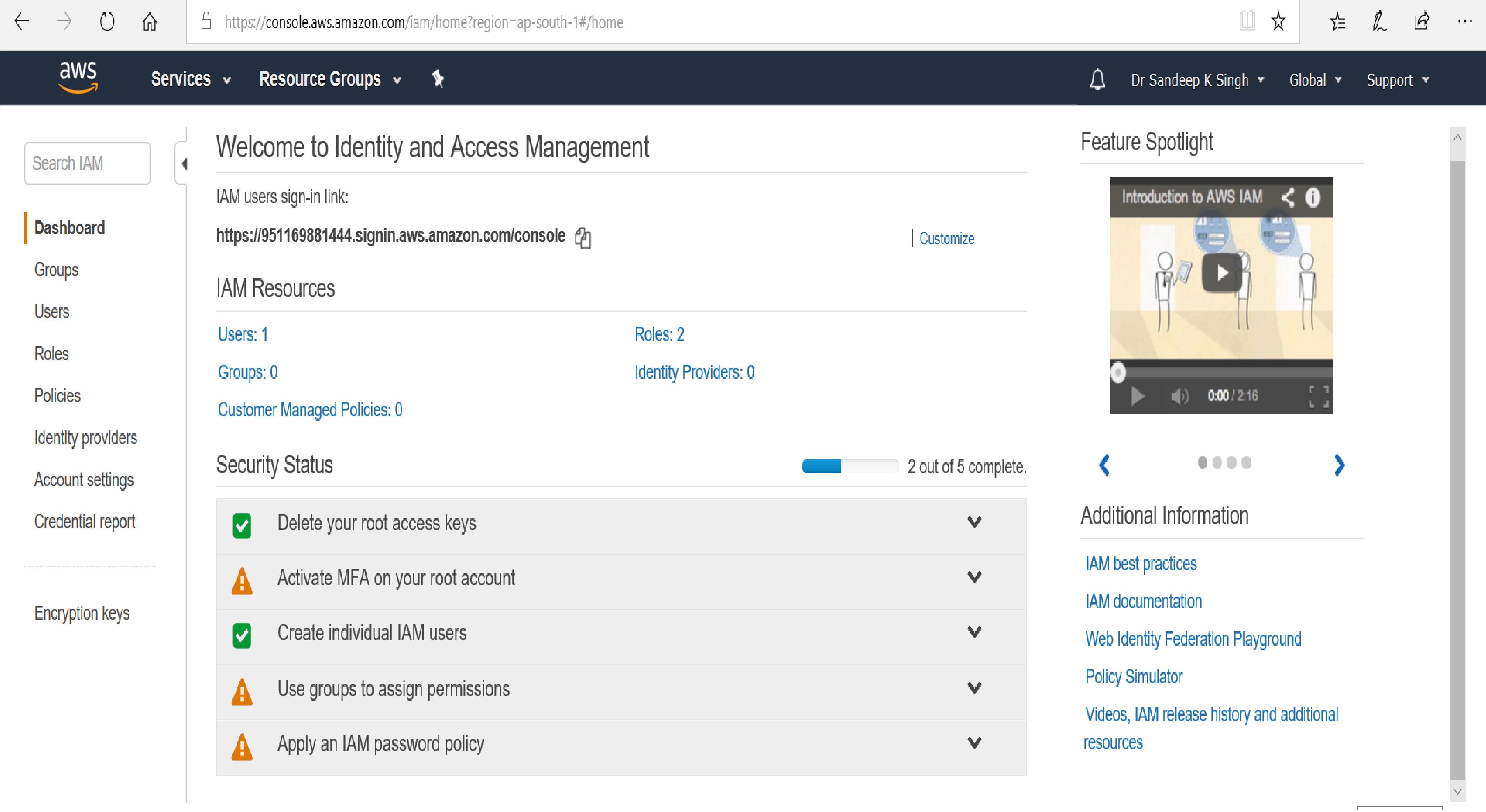
Identity and Access Management in AWS (IAM)

IAM

- Close control- who(U), which(A) and what(R)
- AWS Group-block network traffic based on IP or traffic type(protocol or port number)
- Give Users Unique account identities- IAM Service
- Manage users, authentication credentials, password rotation policies, Multi-factor authentication (MFA)
- Access via Console, CLI, SDK or as HTTPS API.

Root Account vs IAM User

- Sign up to use AWS
- Using email and password
- Unrestricted access to all resources inc billing , account settings and pwd policy
- Additional layer by MFA- both pwd and authentication code 6 digit numeric code
- MFA device- hardware(Germalto) or Virtual(Google authenticator)



Welcome to Identity and Access Management

IAM users sign-in link:

https://951169881444.signin.aws.amazon.com/console

Customize

IAM Resources

Users: 1	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

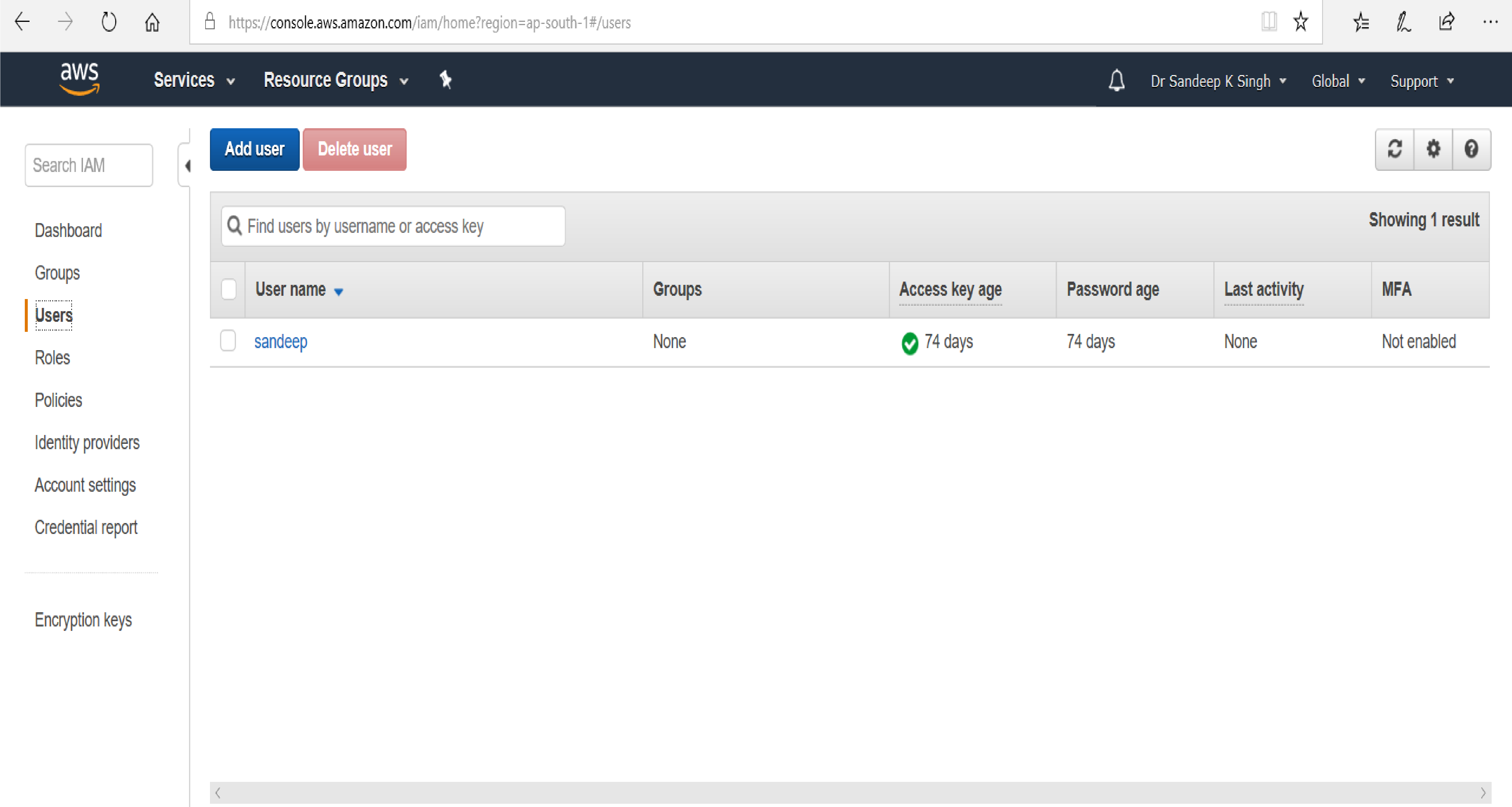
Feature Spotlight

Additional Information

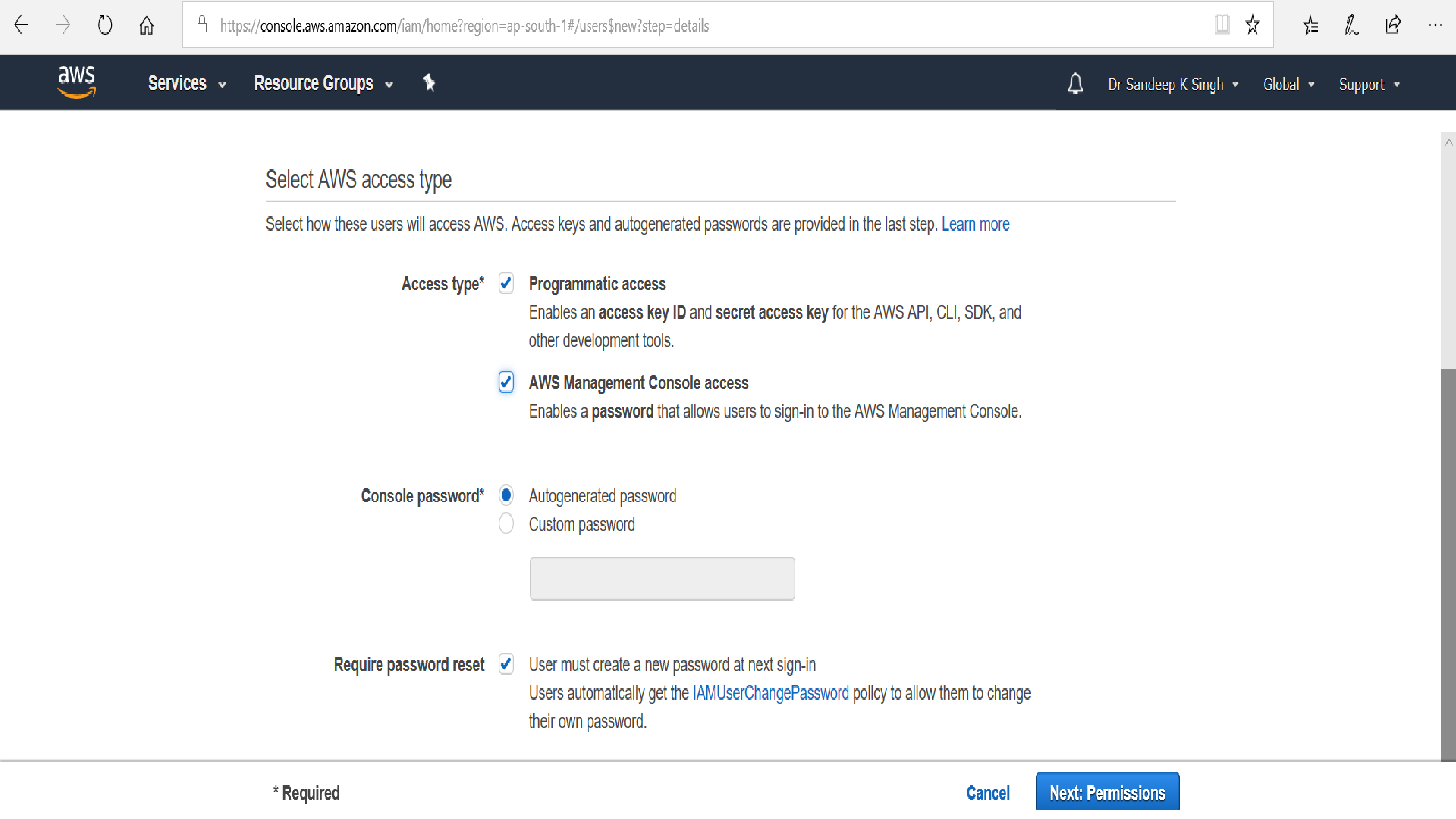
- IAM best practices
- IAM documentation
- Web Identity Federation Playground
- Policy Simulator
- Videos, IAM release history and additional resources

Users

- IAM user – a user or an application -no power
- Dedicated sign-in link, pwd and access keys.
- IAM Account within an root account
- As top root owner you can create accounts, assign policies, generate passwords and security credentials.
- 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.



□	User name	Groups	Access key age	Password age	Last activity	MFA
□	sandeep	None	✓ 74 days	74 days	None	Not enabled



https://console.aws.amazon.com/iam/home?region=ap-south-1#/users$new?step=details
aws
Services
Resource Groups
Dr Sandeep K Singh
Global
Support

Select AWS access type

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

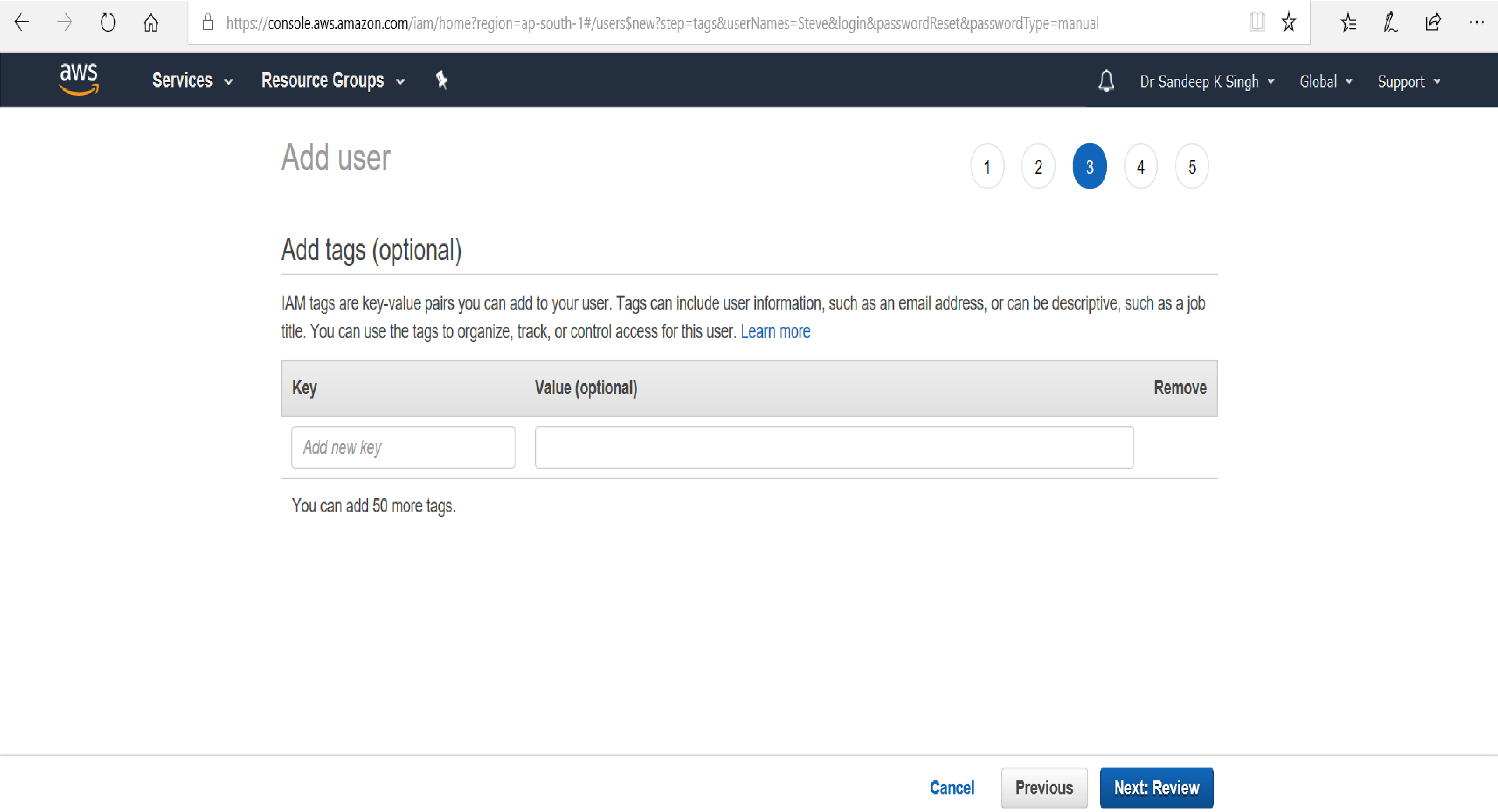
Access type* ☑ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☑ **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 their own password.

* Required



https://console.aws.amazon.com/iam/home?region=ap-south-1#/users$new?step=tags&userNames=Steve&login&passwordReset&passwordType=manual
aws
Services
Resource Groups
Dr Sandeep K Singh
Global
Support
1
2
3
4
5

Add user

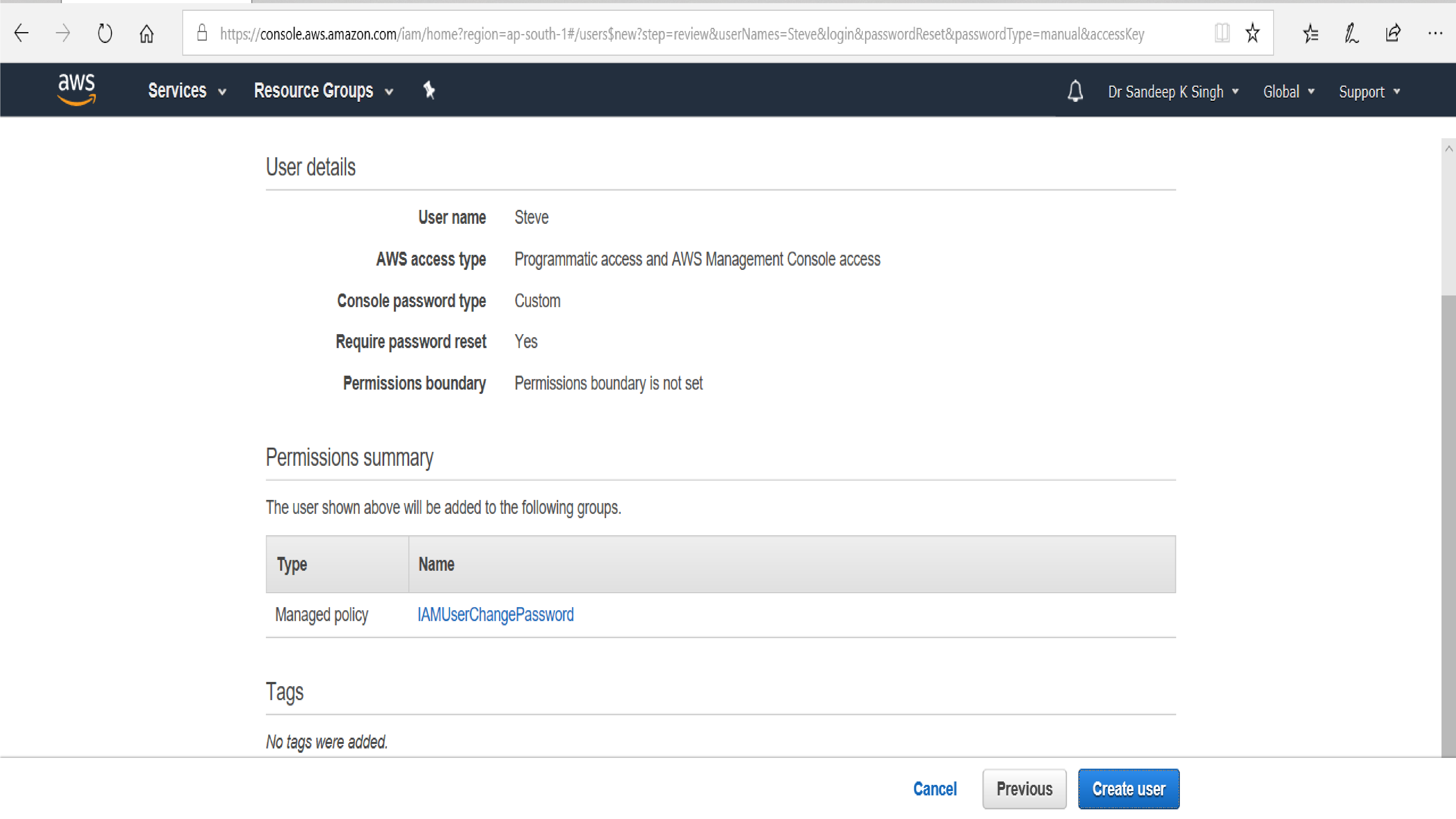
Add tags (optional)

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
Add new key		

You can add 50 more tags.

Cancel
Previous
Next: Review



https://console.aws.amazon.com/iam/home?region=ap-south-1#/users$new?step=review&userNames=Steve&login&passwordReset&passwordType=manual&accessKey
aws
Services
Resource Groups
Dr Sandeep K Singh
Global
Support

User details

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

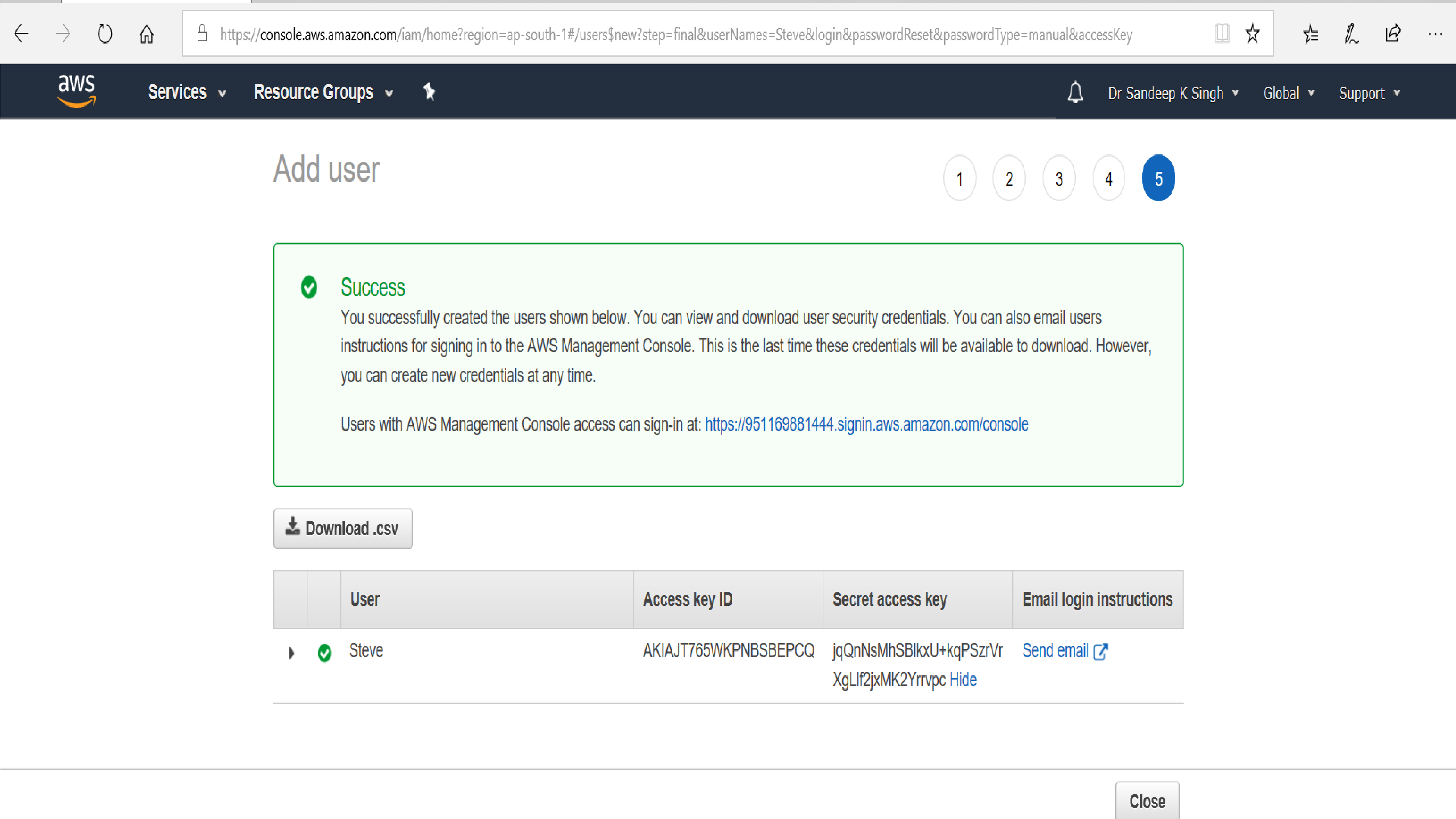
Permissions summary

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

Type	Name
Managed policy	IAMUserChangePassword

Tags

No tags were added.



https://console.aws.amazon.com/iam/home?region=ap-south-1#/users$new?step=final&userNames=Steve&login&passwordReset&passwordType=manual&accessKey
aws
Services
Resource Groups
Dr Sandeep K Singh
Global
Support

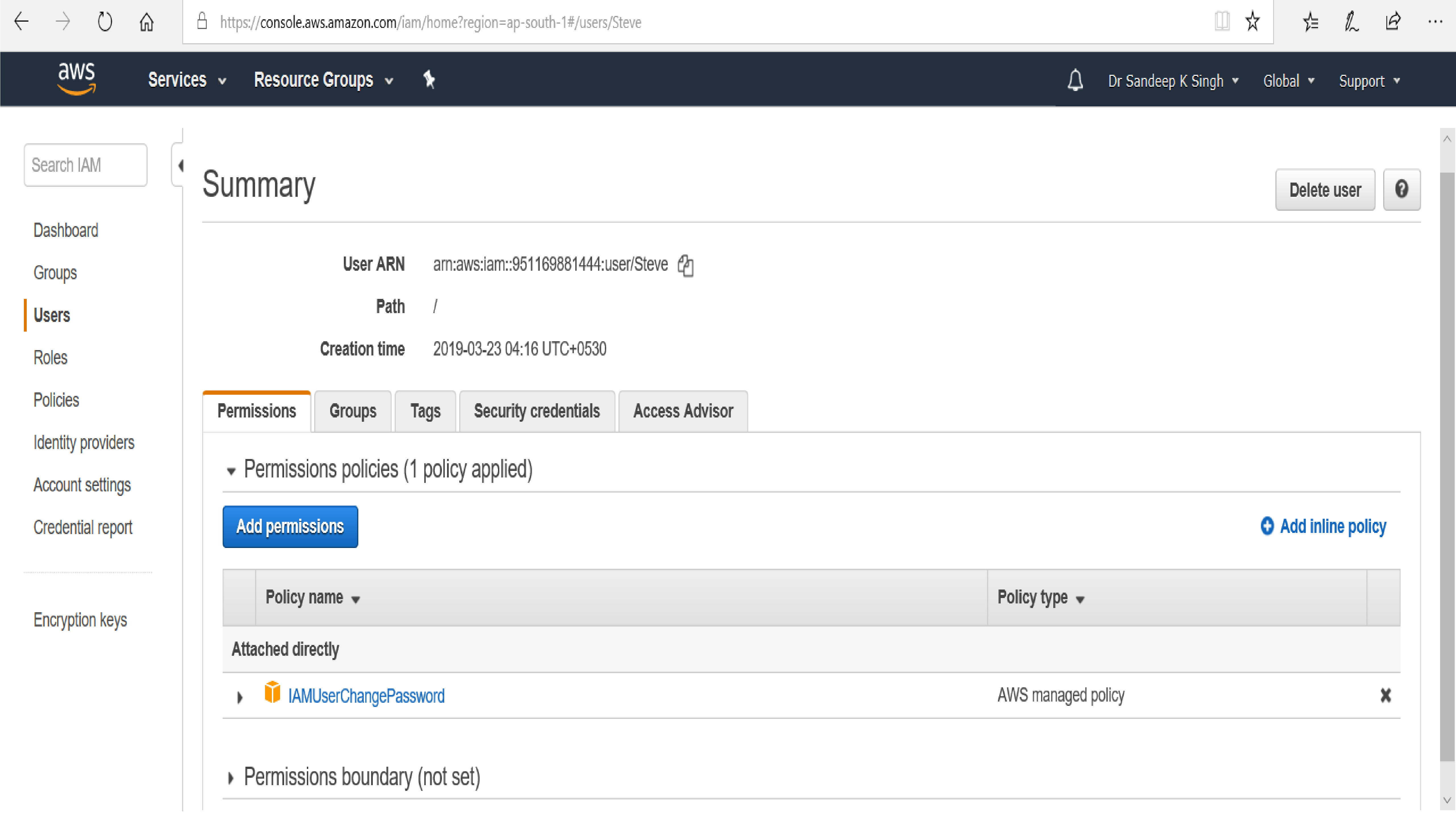
Add user

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://951169881444.signin.aws.amazon.com/console

		User	Access key ID	Secret access key	Email login instructions
▸	✓	Steve	AKIAJT765WKPNBSBEPCQ	jqQnNsMhSBlkxU+kqPSzrVrXgLlf2jxMK2Yrrvpc Hide	Send email



Summary

User ARN arn:aws:iam::951169881444:user/Steve

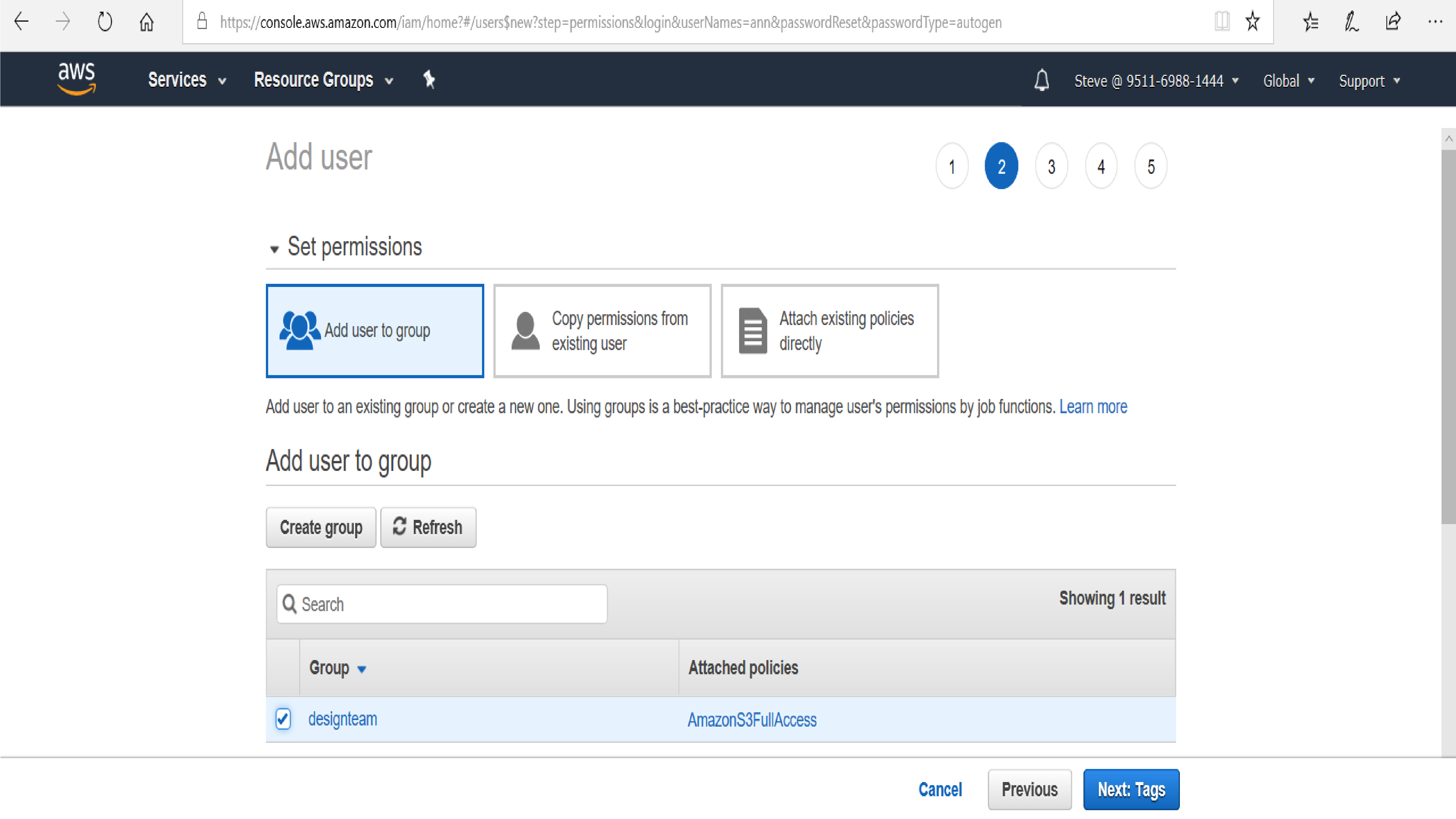
Path /

Creation time 2019-03-23 04:16 UTC+0530

Permissions policies (1 policy applied)

Policy name	Policy type
Attached directly	
IAMUserChangePassword	AWS managed policy

Permissions boundary (not set)



https://console.aws.amazon.com/iam/home?#/users$new?step=permissions&login&userNames=ann&passwordReset&passwordType=autogen
aws
Services
Resource Groups
Steve @ 9511-6988-1444
Global
Support
1
2
3
4
5
Create group
Refresh
Search
Cancel
Previous
Next: Tags

Add user

Set permissions

☑ Add user to group

Copy permissions from existing user

Attach existing policies directly

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

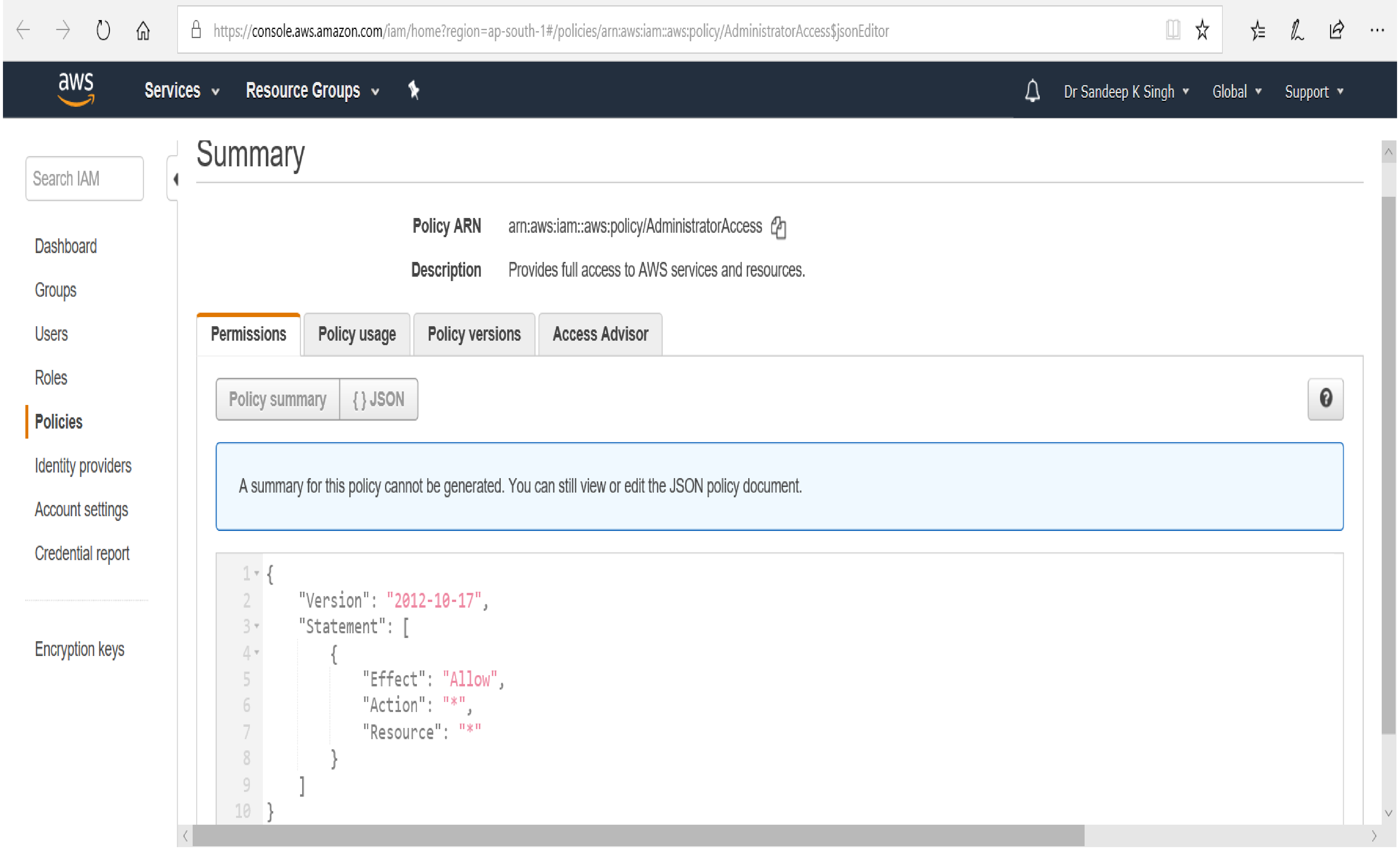
Add user to group

Showing 1 result

	Group	Attached policies
☑	designteam	AmazonS3FullAccess

Policies: who, which and what

- JSON Document- grant permission to user, group and role
- User based or resource based
- Principal defined by Amazon Resource Names (ARN)
- Policy Action
- Target Resource identified by its ARN



Summary

Policy ARN arn:aws:iam::aws:policy/AdministratorAccess

Description Provides full access to AWS services and resources.

A summary for this policy cannot be generated. You can still view or edit the JSON policy document.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

Group

- Logical entity to organize users.
- Members inherit from group
- Individual credentials to gain group access.
- Permit ease in binding the policies.