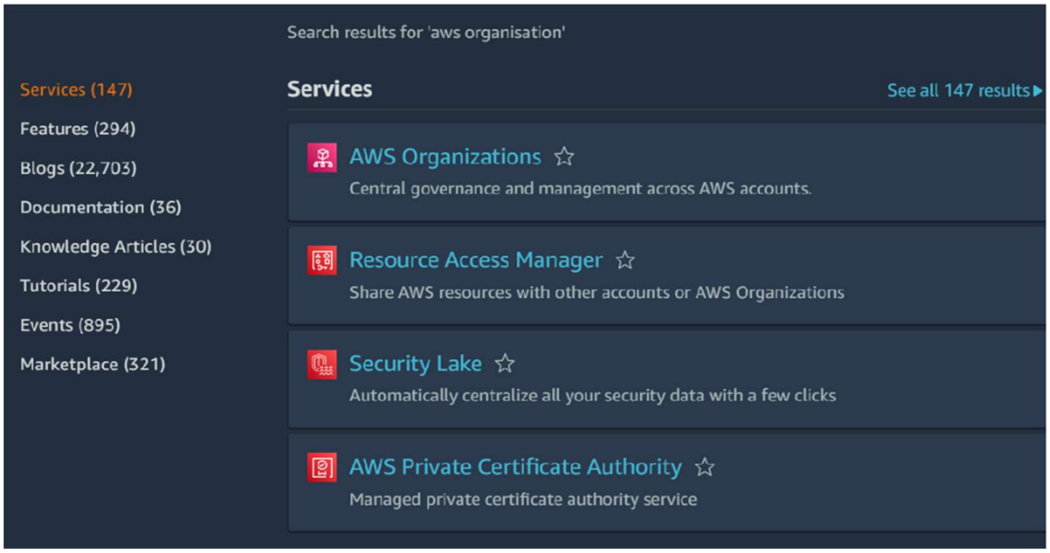
# PRACTICAL 8

## Aim: Study and implementation of Single-Sign-On.

## STEPS:

1. Create an AWS root user account and sign in as root user.



Search results for 'aws organisation'

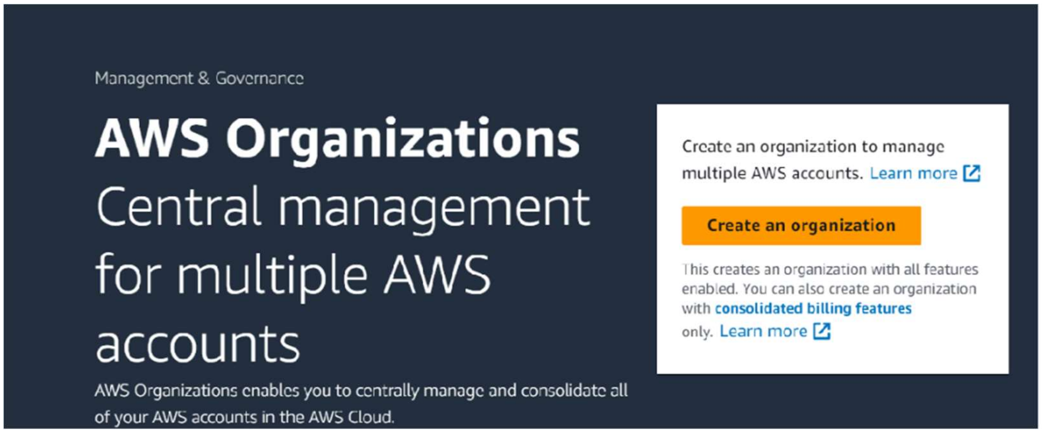
AWS Organizations ☆
Central governance and management across AWS accounts.

Resource Access Manager ☆
Share AWS resources with other accounts or AWS Organizations

Security Lake ☆
Automatically centralize all your security data with a few clicks

AWS Private Certificate Authority ☆
Managed private certificate authority service

2. Click on AWS organization.



Management & Governance

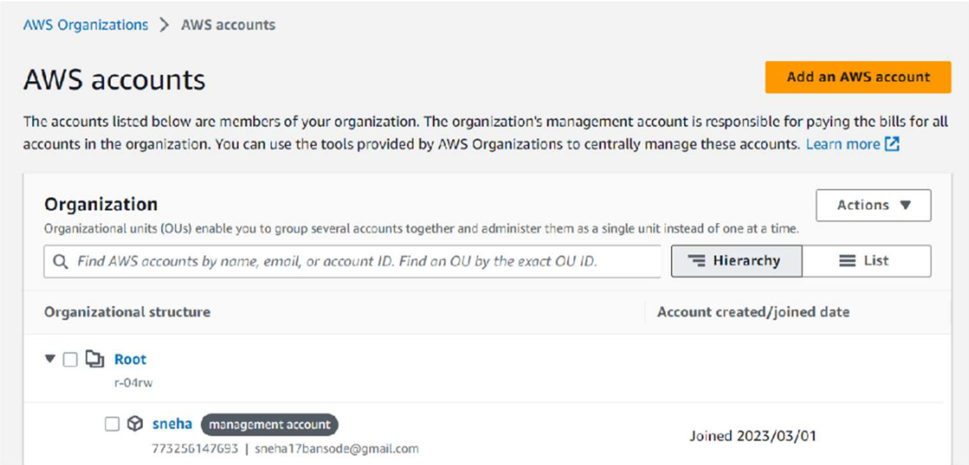
AWS Organizations
Central management for multiple AWS accounts

AWS Organizations enables you to centrally manage and consolidate all of your AWS accounts in the AWS Cloud.

Create an organization to manage multiple AWS accounts. Learn more

This creates an organization with all features enabled. You can also create an organization with consolidated billing features only. Learn more

3. Click on create an organization.



AWS accounts

The accounts listed below are members of your organization. The organization's management account is responsible for paying the bills for all accounts in the organization. You can use the tools provided by AWS Organizations to centrally manage these accounts. Learn more

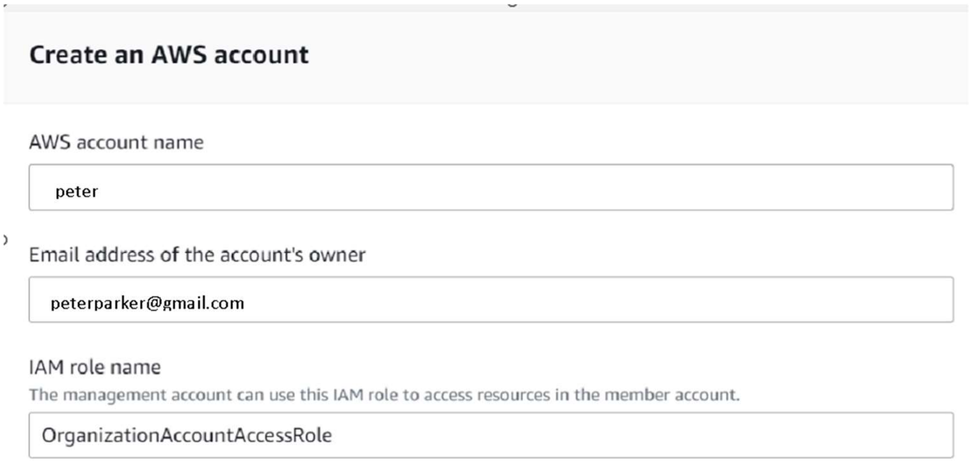
Organization

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

Actions ▼
Find AWS accounts by name, email, or account ID. Find an OU by the exact OU ID.
Hierarchy
List

| Organizational structure | Account created/joined date |
|---|---|
| ▼ □ Root<br>r-04rw | |
| □ sneha management account<br>773256147693 \| sneha17bansode@gmail.com | Joined 2023/03/01 |

4. Click on Add an AWS account.



Create an AWS account

AWS account name

peter

Email address of the account's owner

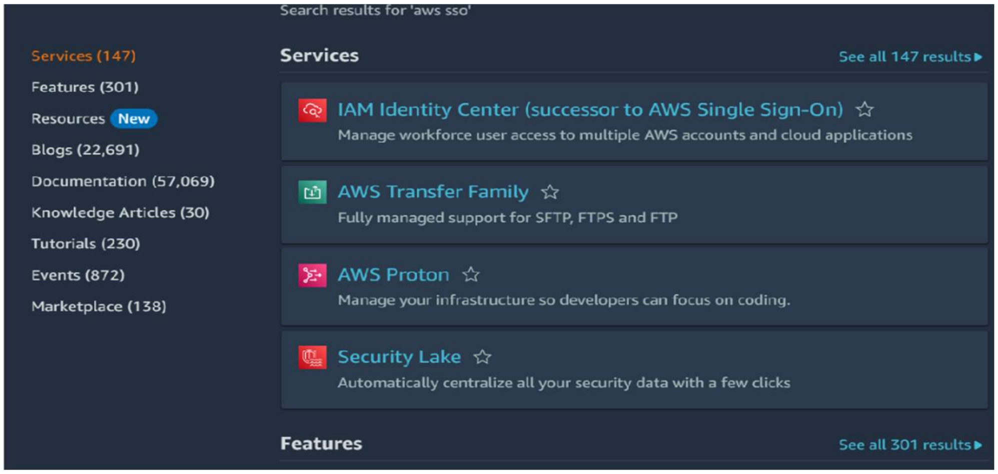
peterparker@gmail.com

IAM role name

The management account can use this IAM role to access resources in the member account.

OrganizationAccountAccessRole

5. Click on create AWS account and create one more AWS account. Enter AWS SSO in the search box.



Search results for 'aws sso'

Services

IAM Identity Center (successor to AWS Single Sign-On) ☆

Manage workforce user access to multiple AWS accounts and cloud applications

AWS Transfer Family ☆

Fully managed support for SFTP, FTPS and FTP

AWS Proton ☆

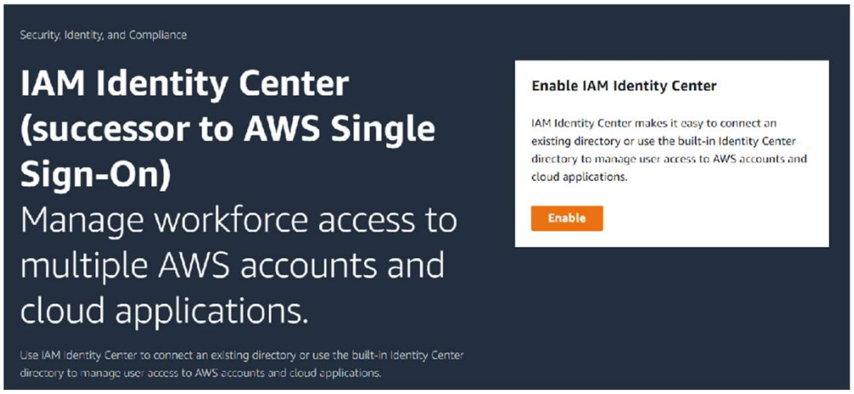
Manage your infrastructure so developers can focus on coding.

Security Lake ☆

Automatically centralize all your security data with a few clicks

Features

6. Click on IAM identity center.



Security, Identity, and Compliance

IAM Identity Center (successor to AWS Single Sign-On)

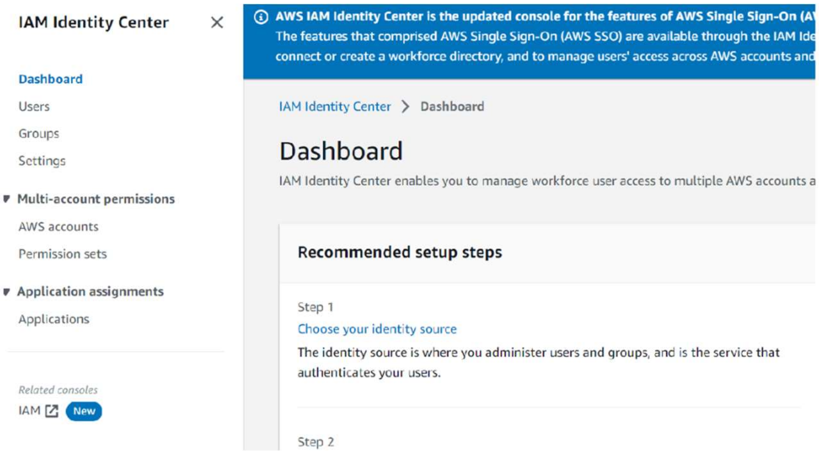
Manage workforce access to multiple AWS accounts and cloud applications.

Use IAM Identity Center to connect an existing directory or use the built-in Identity Center directory to manage user access to AWS accounts and cloud applications.

Enable IAM Identity Center

IAM Identity Center makes it easy to connect an existing directory or use the built-in Identity Center directory to manage user access to AWS accounts and cloud applications.

7. Click on enable



AWS IAM Identity Center is the updated console for the features of AWS Single Sign-On (A
The features that comprised AWS Single Sign-On (AWS SSO) are available through the IAM Ide
connect or create a workforce directory, and to manage users' access across AWS accounts and

IAM Identity Center > Dashboard

Dashboard

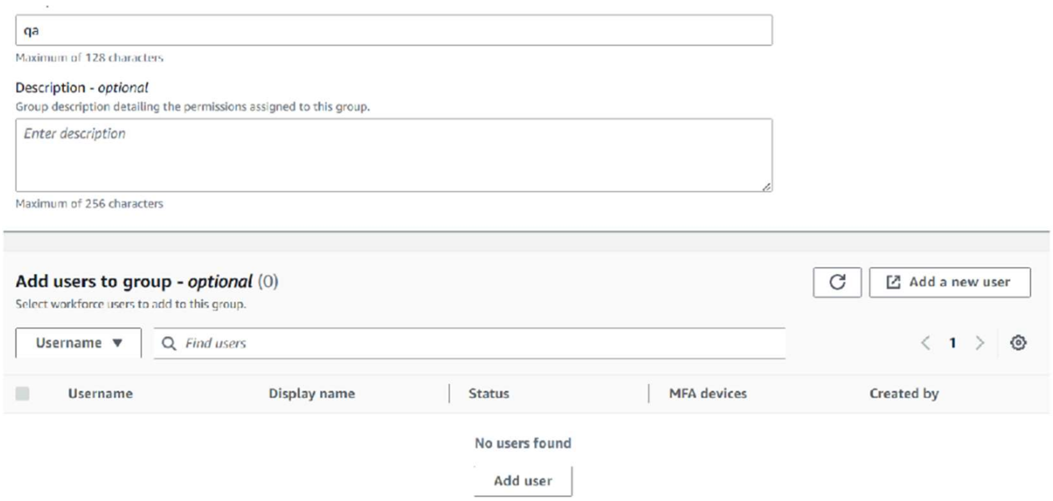
IAM Identity Center enables you to manage workforce user access to multiple AWS accounts a

Recommended setup steps

Step 1
Choose your identity source
The identity source is where you administer users and groups, and is the service that authenticates your users.

Step 2

8. Click on groups and create users. And click on ADD USERS. And enter the username.



qa
Maximum of 128 characters

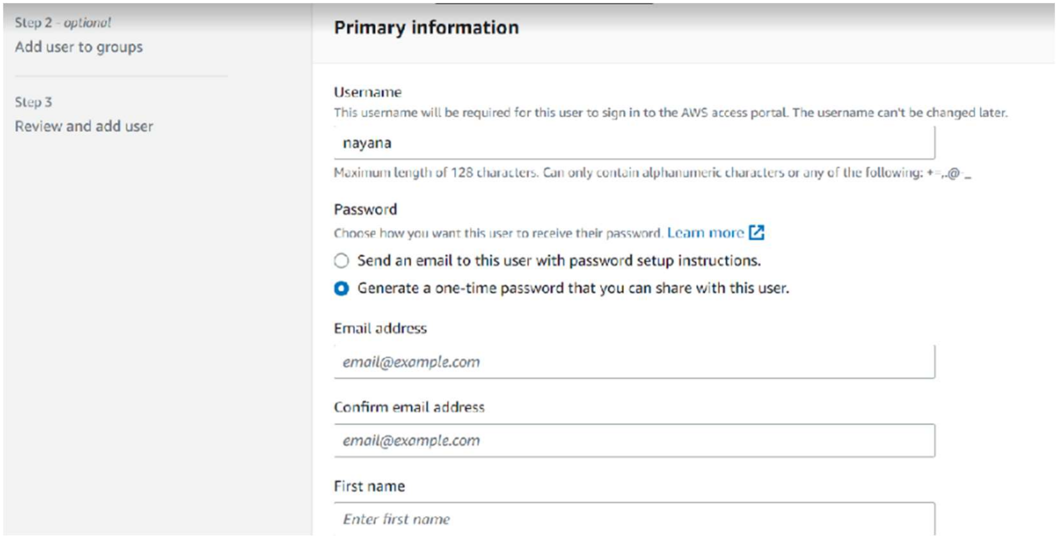
Description - *optional*
Group description detailing the permissions assigned to this group.
*Enter description*
Maximum of 256 characters

Add users to group - *optional* (0)
Select workforce users to add to this group.

| Username | Display name | Status | MFA devices | Created by |
|---|---|---|---|---|

No users found

9. Click on generate a one time password.



Step 2 - optional
Add user to groups

Step 3
Review and add user

**Primary information**

Username
This username will be required for this user to sign in to the AWS access portal. The username can't be changed later.
nayana
Maximum length of 128 characters. Can only contain alphanumeric characters or any of the following: +=,.@-_

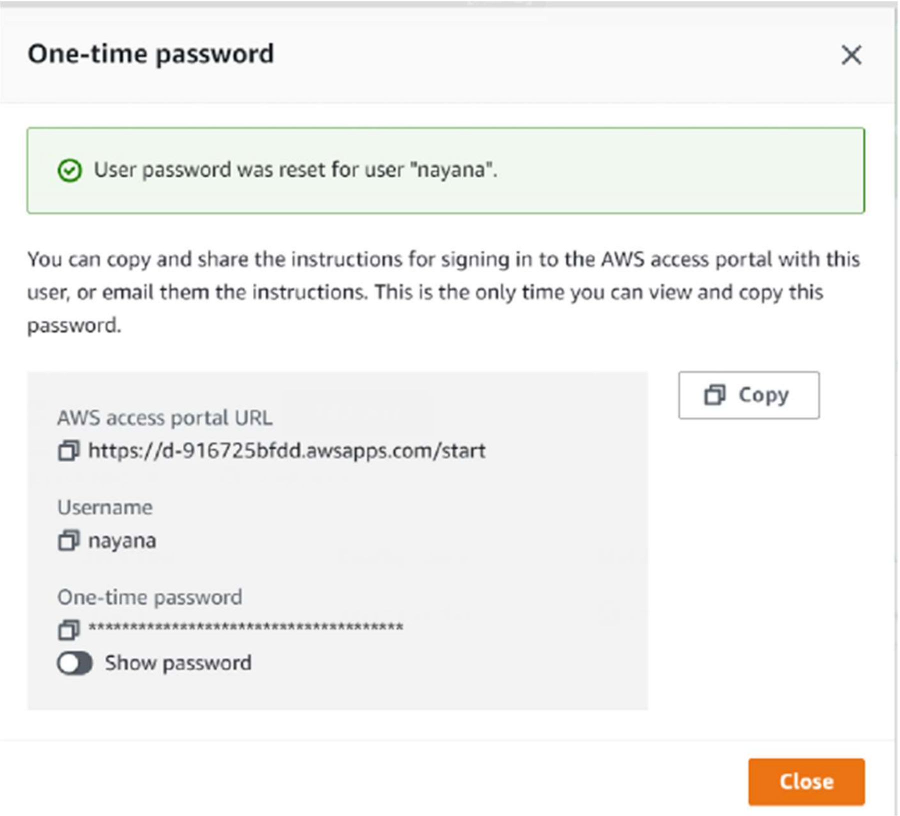
Password
Choose how you want this user to receive their password. Learn more
○ Send an email to this user with password setup instructions.
● Generate a one-time password that you can share with this user.

Email address
email@example.com

Confirm email address
email@example.com

First name
Enter first name

10. Once the user is created you get the following screen.



**One-time password**

User password was reset for user "nayana".

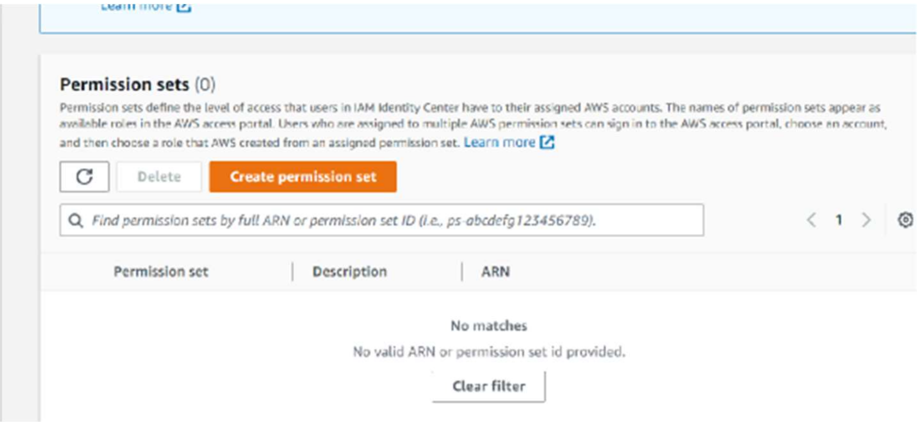
You can copy and share the instructions for signing in to the AWS access portal with this user, or email them the instructions. This is the only time you can view and copy this password.

AWS access portal URL
https://d-916725bfdd.awsapps.com/start

Username
nayana

One-time password
****************************************

11. Click on create permission set and create a permission set with administrator access.



Permission sets (0)

Permission sets define the level of access that users in IAM Identity Center have to their assigned AWS accounts. The names of permission sets appear as available roles in the AWS access portal. Users who are assigned to multiple AWS permission sets can sign in to the AWS access portal, choose an account, and then choose a role that AWS created from an assigned permission set. Learn more

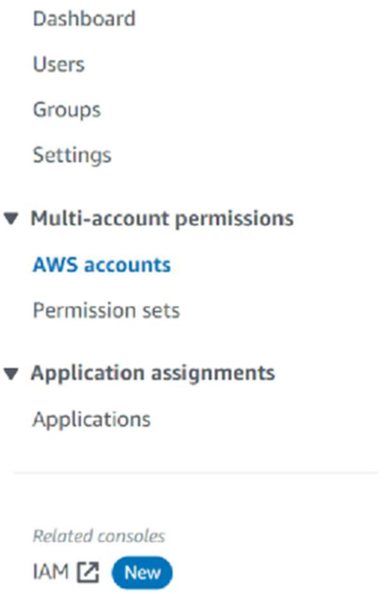
Find permission sets by full ARN or permission set ID (i.e., ps-abcdefg123456789).

| Permission set | Description | ARN |
|---|---|---|

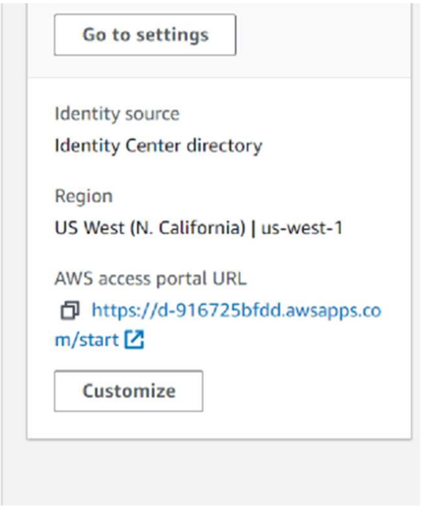
No matches

No valid ARN or permission set id provided.

12. Click on assign users or groups and assign the accounts to the user in the group.



13. Click on applications, add application and assign user to the application. Click on dashboard.

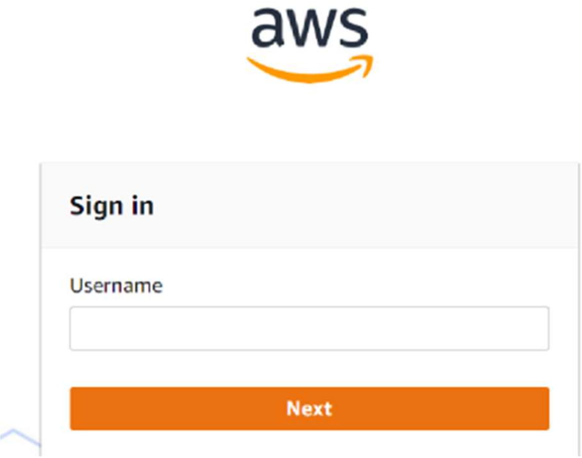


Identity source
Identity Center directory

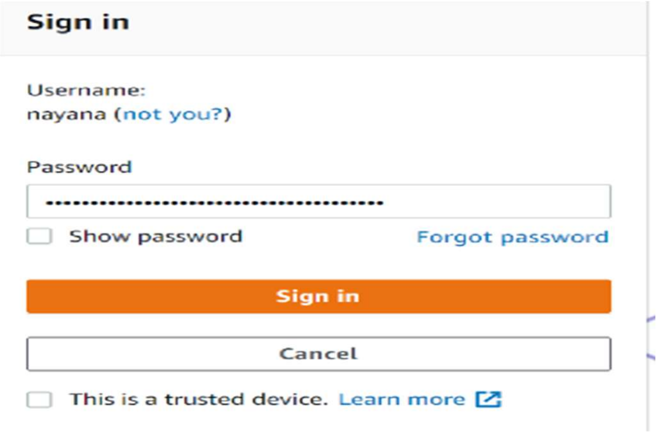
Region
US West (N. California) | us-west-1

AWS access portal URL
https://d-916725bfdd.awsapps.com/start

14. Click on AWS access portal URL and enter the URL.

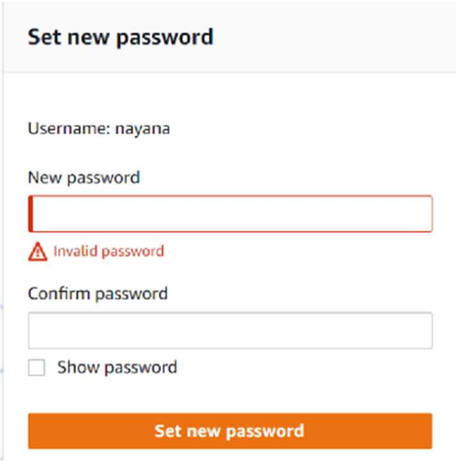


15. Enter the password and sign in.



Username:
nayana (not you?)

16. Now change the password.



**Set new password**

Username: nayana

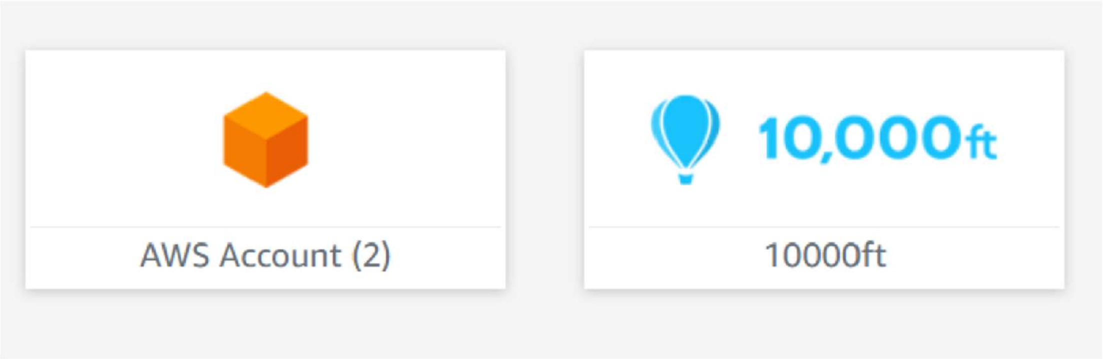
New password

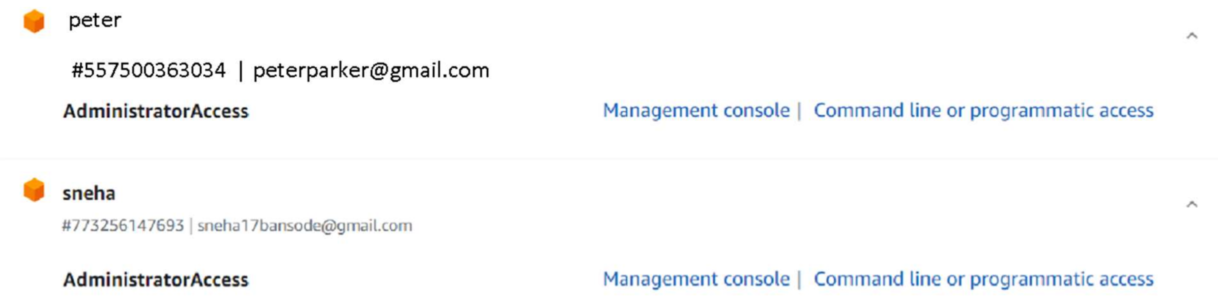
⚠ Invalid password

Confirm password

□ Show password

17. Now the user can sign in to the AWS accounts and application.





peter

#557500363034 | peterparker@gmail.com

AdministratorAccess — Management console | Command line or programmatic access

sneha

#773256147693 | sneha17bansode@gmail.com

AdministratorAccess — Management console | Command line or programmatic access