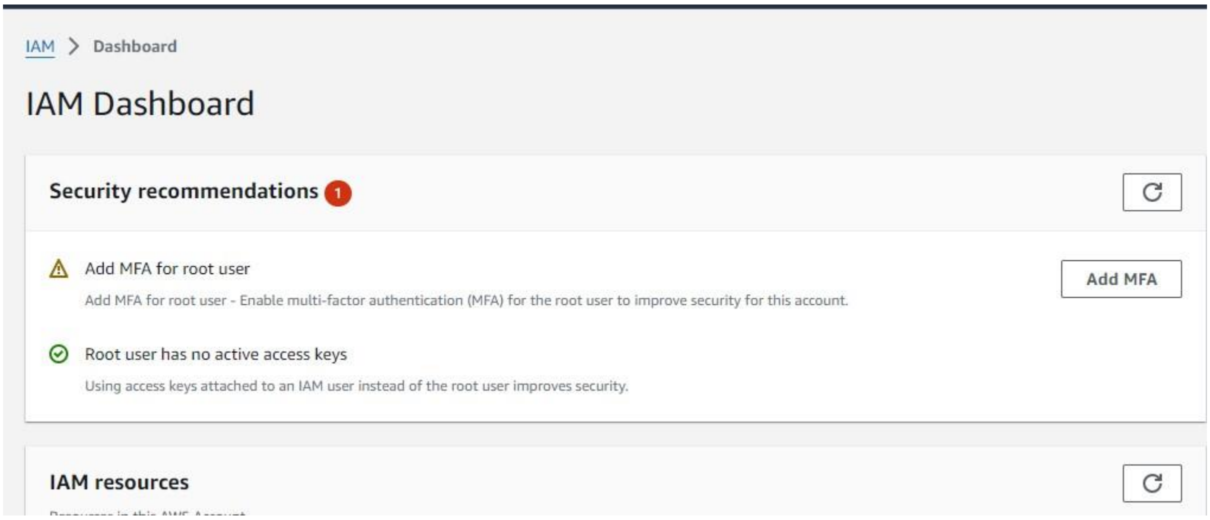
Practical – 6 - MFA



IAM Dashboard

Security recommendations

⚠ Add MFA for root user

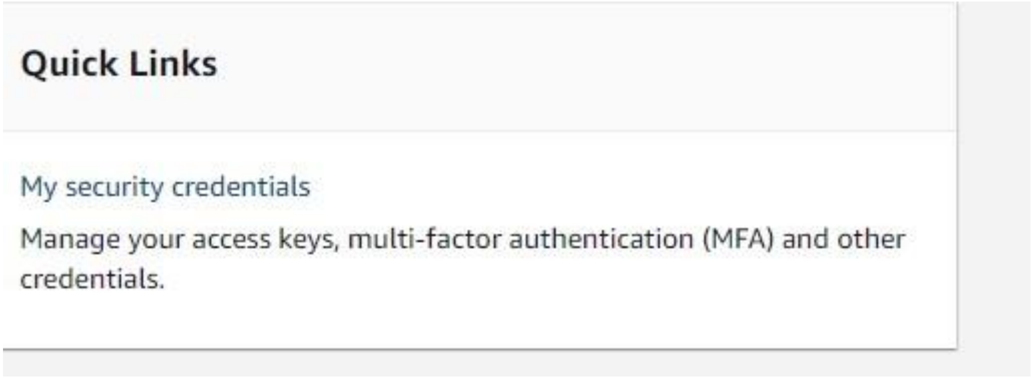
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

✓ Root user has no active access keys

Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

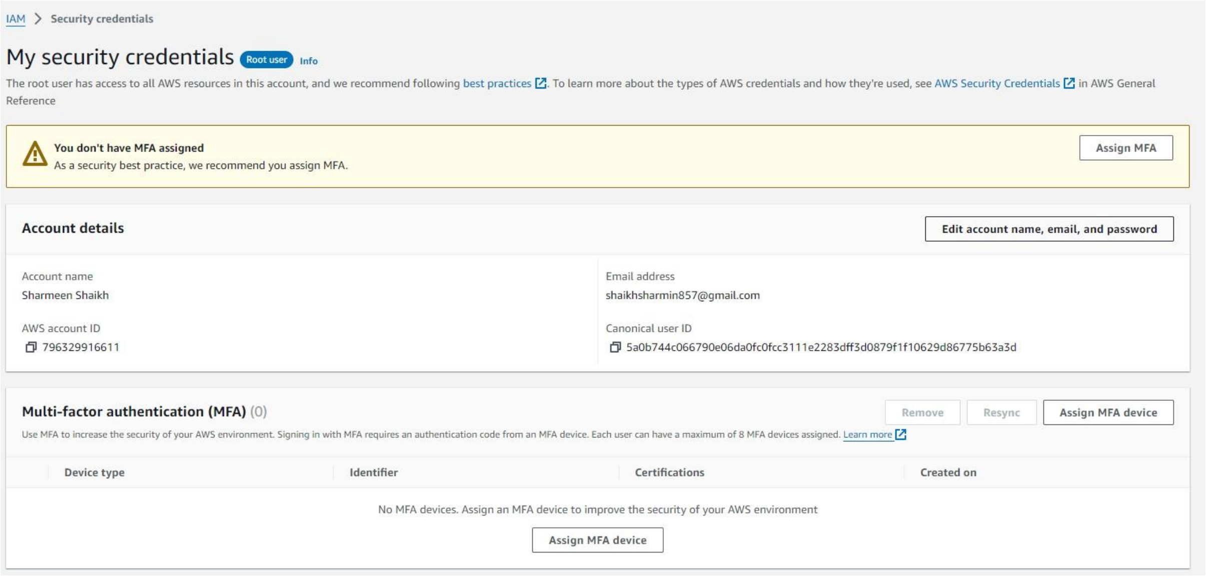
Resources in this AWS Account



Quick Links

My security credentials

Manage your access keys, multi-factor authentication (MFA) and other credentials.



IAM > Security credentials

My security credentials Root user Info

The root user has access to all AWS resources in this account, and we recommend following best practices. To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference

You don't have MFA assigned
As a security best practice, we recommend you assign MFA.

Account details

Account name
Sharmeen Shaikh

Email address
shaikhsharmin857@gmail.com

AWS account ID
796329916611

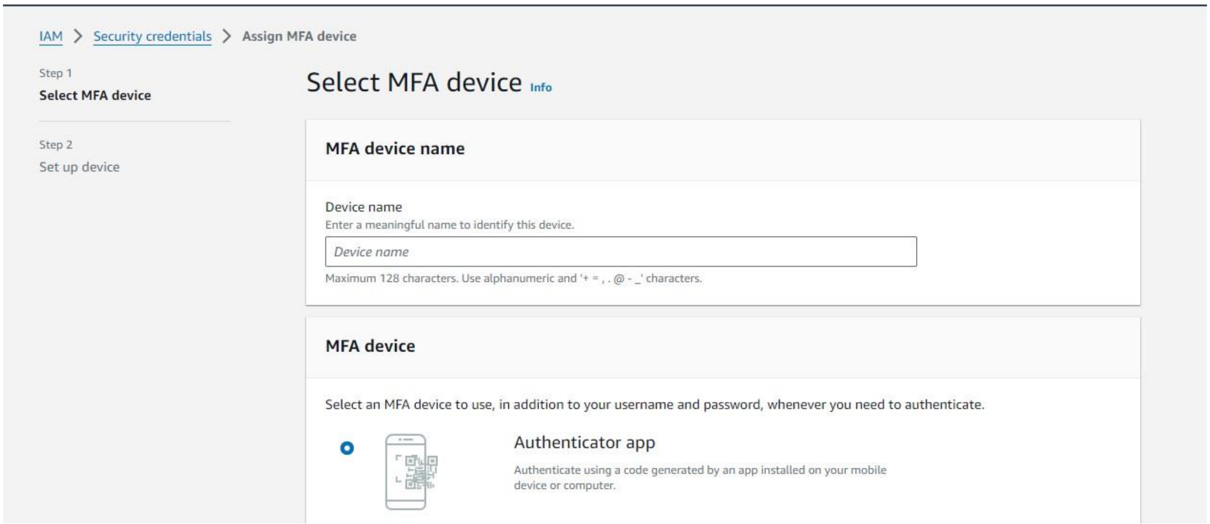
Canonical user ID
5a0b744c066790e06da0fc0fcc3111e2283dff3d0879f1f10629d86775b63a3d

Multi-factor authentication (MFA) (0)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more

Device type	Identifier	Certifications	Created on

No MFA devices. Assign an MFA device to improve the security of your AWS environment



IAM > Security credentials > Assign MFA device

Step 1
Select MFA device

Step 2
Set up device

Select MFA device Info

MFA device name

Device name
Enter a meaningful name to identify this device.

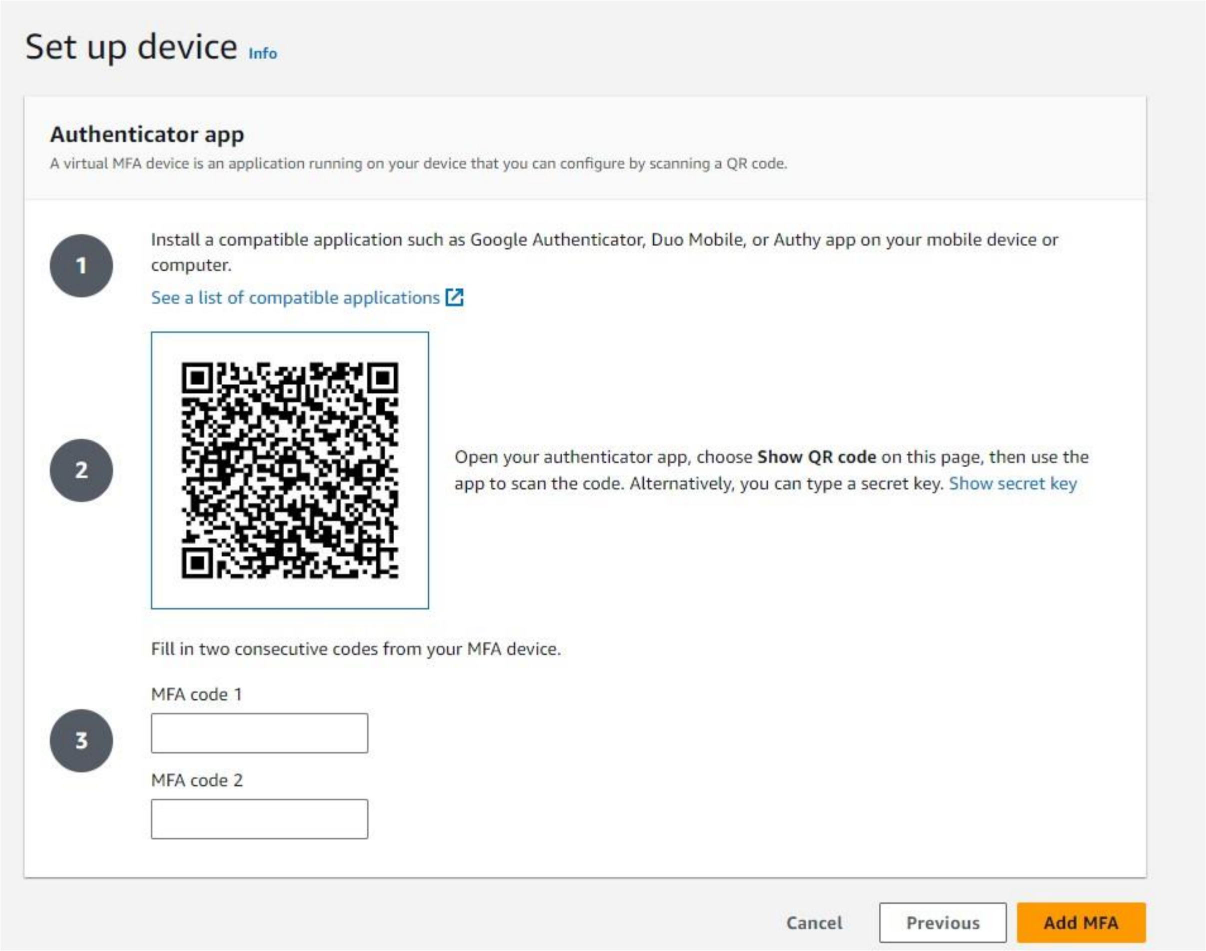
Maximum 128 characters. Use alphanumeric and '+ = , . @ - _' characters.

MFA device

Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.

● Authenticator app
Authenticate using a code generated by an app installed on your mobile device or computer.

Click next



Set up device Info

Authenticator app

A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

1 Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.

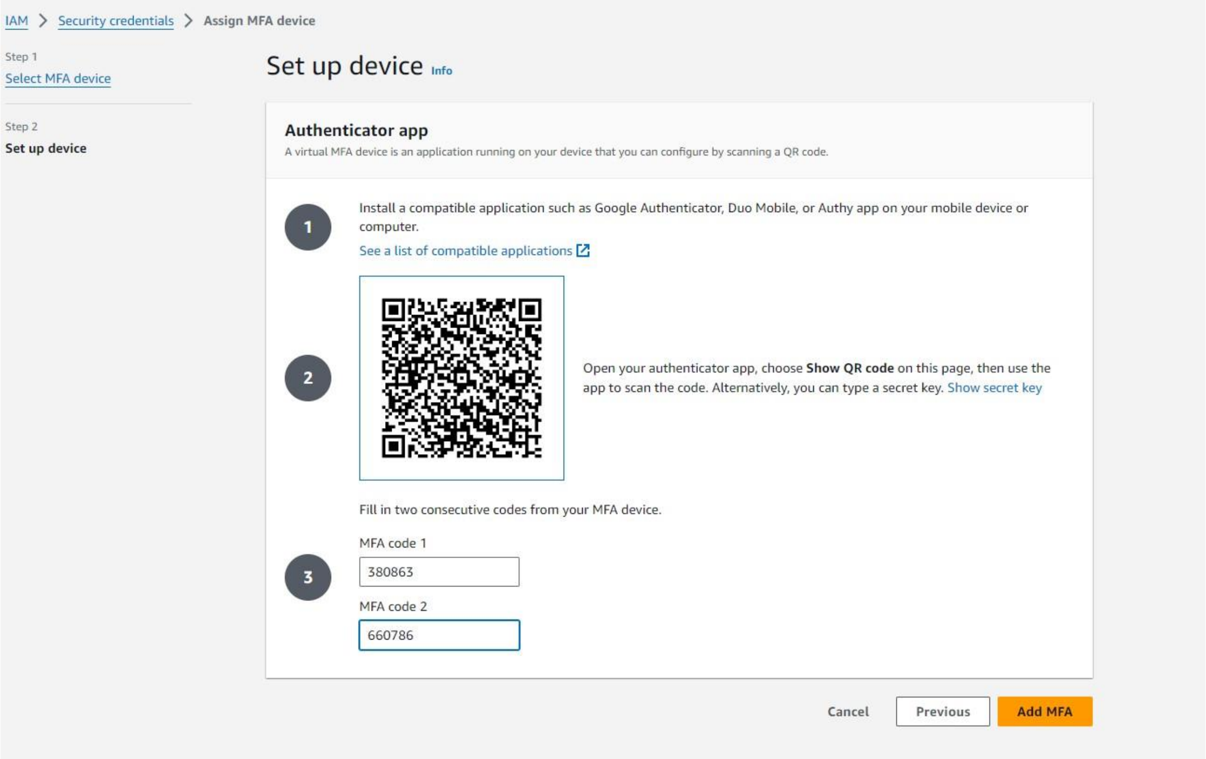
See a list of compatible applications

2 Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key. Show secret key

3 Fill in two consecutive codes from your MFA device.

MFA code 1

MFA code 2



IAM > Security credentials > Assign MFA device

Step 1
Select MFA device

Step 2
Set up device

Set up device Info

Authenticator app

A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

1 Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.

See a list of compatible applications

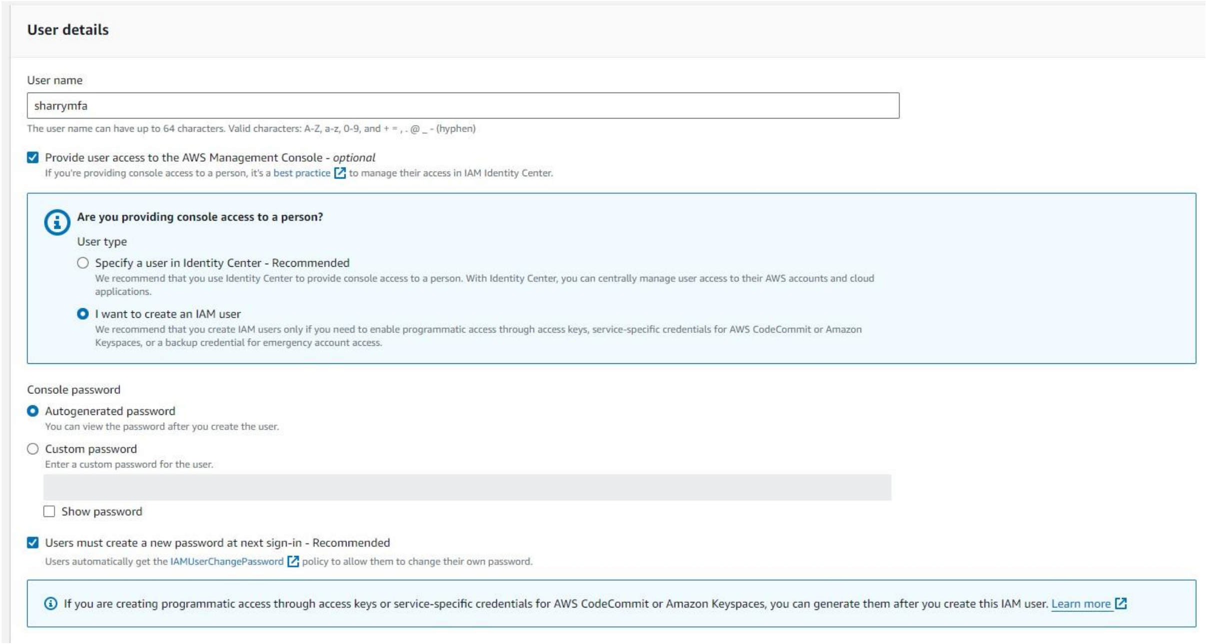
2 Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key. Show secret key

3 Fill in two consecutive codes from your MFA device.

MFA code 1: 380863

MFA code 2: 660786

Go to users



User details

User name

sharrymfa

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☑ Provide user access to the AWS Management Console - *optional*

If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

Are you providing console access to a person?

User type

○ Specify a user in Identity Center - Recommended

We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

● I want to create an IAM user

We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

● Autogenerated password

You can view the password after you create the user.

○ Custom password

Enter a custom password for the user.

□ Show password

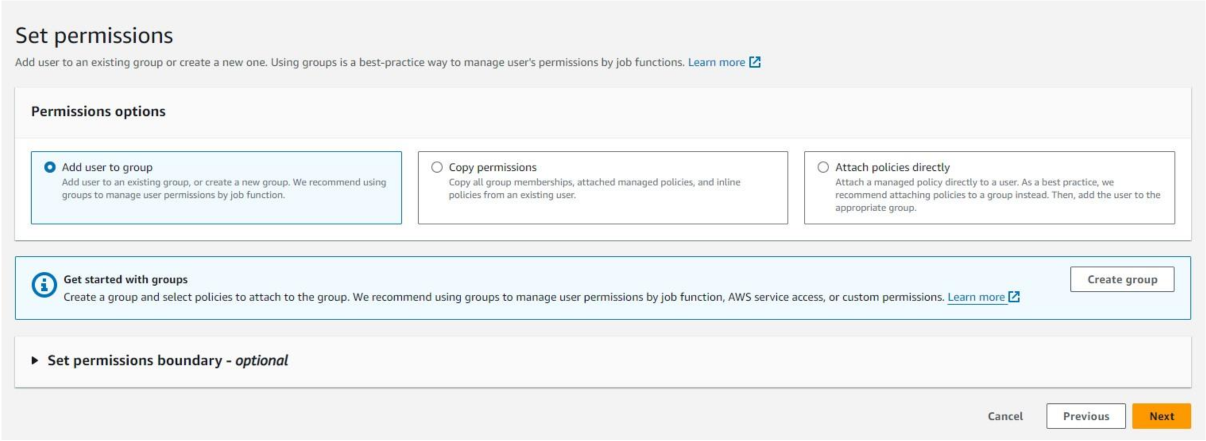
☑ Users must create a new password at next sign-in - Recommended

Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more

Click next

Just click next



Set permissions

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

Permissions options

● Add user to group

Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

○ Copy permissions

Copy all group memberships, attached managed policies, and inline policies from an existing user.

○ Attach policies directly

Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

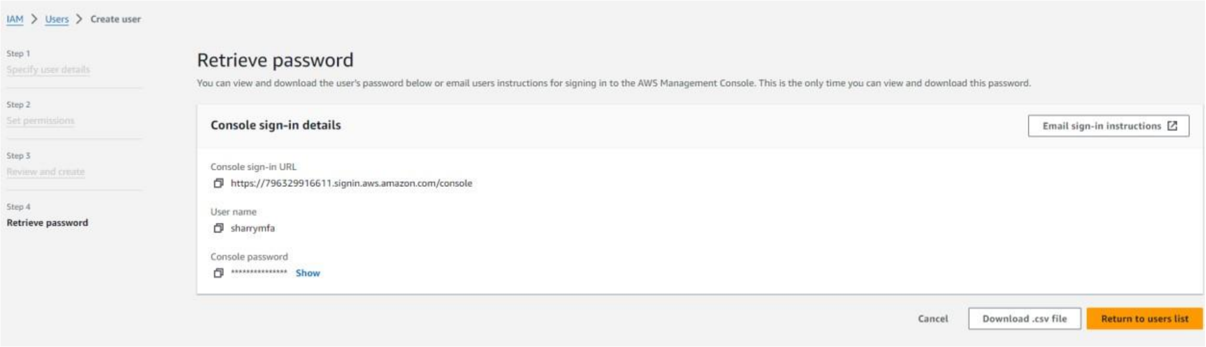
Get started with groups

Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. Learn more

Set permissions boundary - *optional*

Next

Download csv file



Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

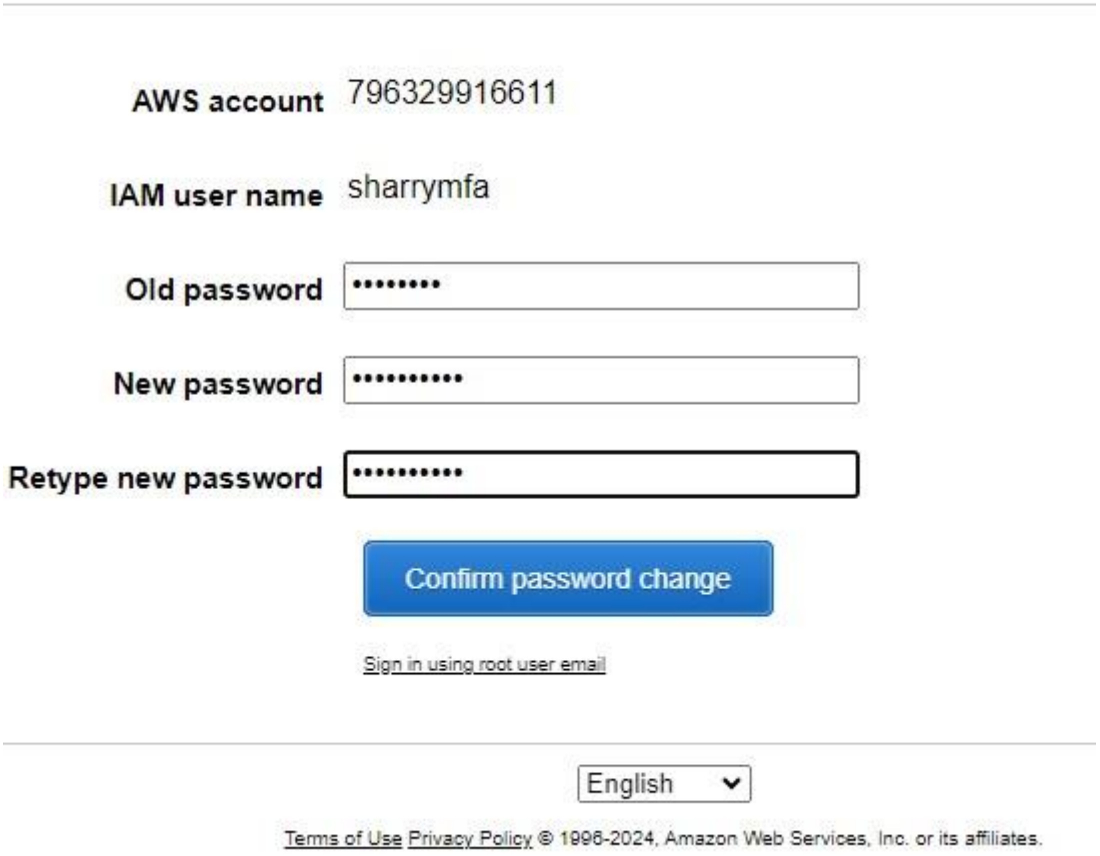
Console sign-in URL
https://796329916611.signin.aws.amazon.com/console

User name
sharrymfa

Console password
*************** Show

Copy and open link in incognito

Copy username password from excel or prev window



AWS account 796329916611

IAM user name sharrymfa

Old password •••••••••

New password •••••••••••

Retype new password •••••••••••

Terms of Use Privacy Policy © 1996-2024, Amazon Web Services, Inc. or its affiliates.