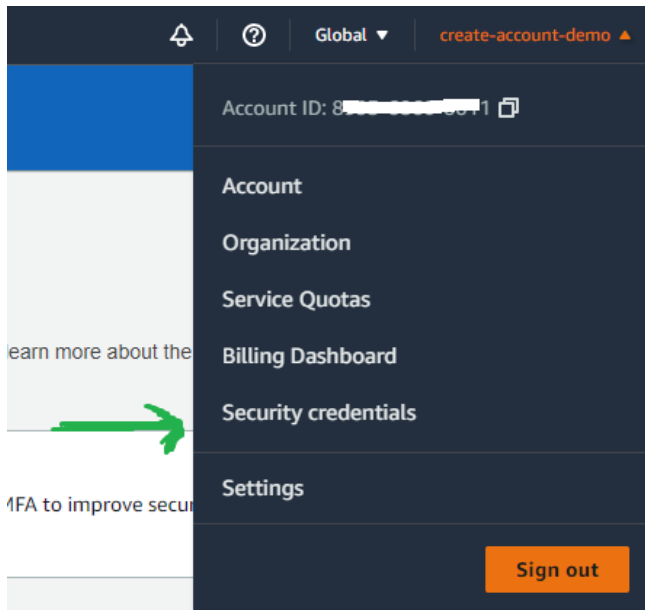


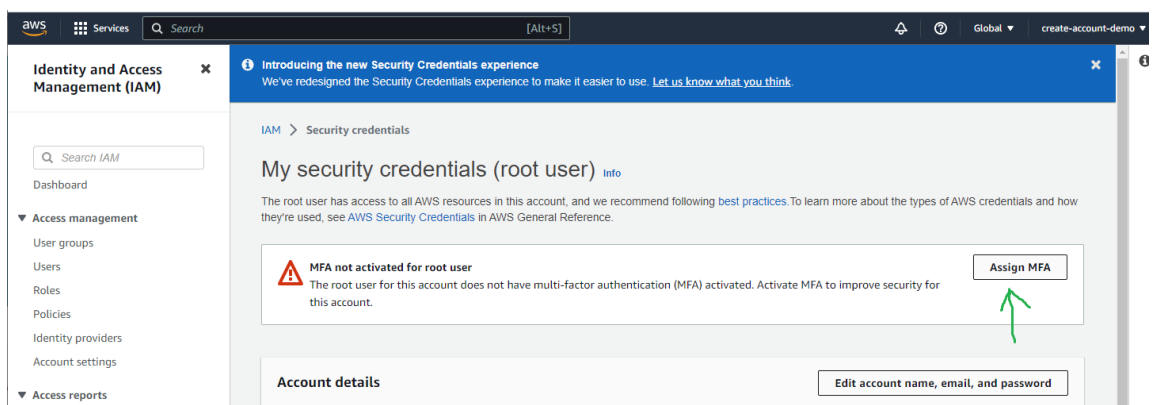
## Enable MFA for root account

**You should apply the same steps for the IAM user.**

### 1- Sign in root user and click security credentials



### 2- Click Assign MFA



### 3- Select MFA device

The screenshot shows the AWS IAM console interface for the 'Assign MFA device' process. The breadcrumb trail is 'IAM > Security credentials > Assign MFA device'. The left sidebar shows 'Step 1: Select MFA device' as the active step, with 'Step 2: Set up device' below it. The main content area is titled 'Select MFA device'. It contains a 'Specify MFA device name' section with a text input field containing 'Phone'. Below this is the 'Select MFA device' section, which has three radio button options: 'Authenticator app' (selected), 'Security Key', and 'Hardware TOTP token'. Each option has a corresponding icon and a brief description. At the bottom right, there are 'Cancel' and 'Next' buttons, with an arrow pointing to the 'Next' button.

Step 1  
Select MFA device

Step 2  
Set up device

### Select MFA device

**Specify MFA device name**

Device name  
Enter a meaningful name to identify this device.  
Maximum 128 characters. Use alphanumeric and "> - . @ \_ : " characters.

Phone

**Select MFA device** Info

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.

☐ **Security Key**  
Authenticate using a code generated by touching a YubiKey or other supported FIDO security key.

☐ **Hardware TOTP token**  
Authenticate using a code displayed on a hardware Time-based one-time password (TOTP) token.

Cancel **Next**

### 4- Add MFA and click Show QR code

The screenshot shows the AWS IAM console interface for the 'Set up device' step. The breadcrumb trail is 'IAM > Security credentials > Assign MFA device'. The left sidebar shows 'Step 2: Set up device' as the active step. The main content area is titled 'Set up device'. It contains a 'Set up your authenticator app' section with a description: 'A virtual MFA device is an application running on your device that you can configure by scanning a QR code.' Below this are three numbered steps: 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. 'Show QR code' with a blue box containing a QR code. 3. 'Fill in two consecutive codes from your MFA device.' with two input fields labeled 'MFA code 1' and 'MFA code 2'. At the bottom right, there are 'Cancel', 'Previous', and 'Add MFA' buttons.

Step 1  
Select MFA device

Step 2  
Set up device

### Set up device

**Set up your 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 **Show QR code**  
Open your authenticator app, chose **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

Cancel Previous **Add MFA**

## 5- Install a compatible app on your mobile device or computer

Mac: Authy

Android: Google Authenticator or Authy

## 6- Scan the QR Code and enter two consecutive MFA codes as MFA code 1 and MFA code 2

The screenshot shows the AWS IAM console 'Set up device' page. The page is titled 'Set up device' and has a sub-header 'Set up your authenticator app'. It includes a QR code for scanning and two input fields for MFA codes. The first code is 170133 and the second is 824126. Arrows point from the QR code to the first code field and from the second code field to the 'Add MFA' button.

## IAM dashboard

### Security recommendations 1



#### Root user has MFA

Having multi-factor authentication (MFA) for the root user improves 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.



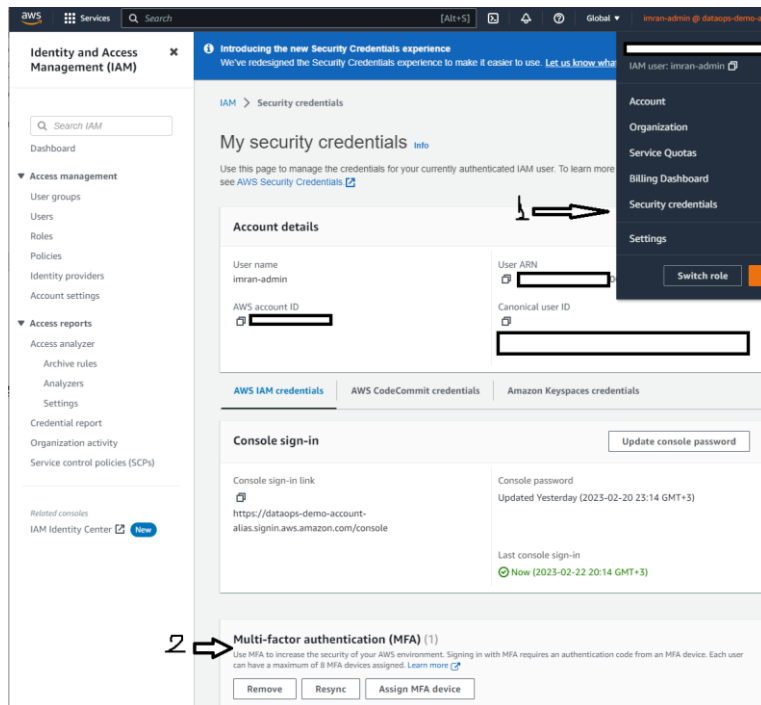
#### Update your access permissions for AWS Billing, Cost Management, and Account consoles

We are replacing the following IAM actions for Billing, Cost Management, and Account consoles with granular IAM actions: `aws-portal:ViewBilling`, `aws-portal:ModifyBilling`, `aws-portal:ViewAccount`, `aws-portal:ModifyAccount`, `aws-portal:ViewPaymentMethods`, `aws-portal:ModifyPaymentMethods`, `aws-portal:ViewUsage`, `purchase-orders:ViewPurchaseOrders`, and `purchase-orders:ModifyPurchaseOrders`. To ensure you don't lose access to AWS Billing, Cost Management, and Account console based features, update your existing IAM policies to include the new IAM actions before July 2023. Examples of features impacted include AWS Cost Explorer, AWS Budgets, Billing console, and more. For more information, please visit [blog](#)

View affected policies

## Enable MFA for IAM user account

- 1- Sign in IAM user and click security credentials
- 2- Click Assign MFA device



### 3- Select MFA device

aws Services Search [Alt+S]

IAM > Security credentials > Assign MFA device

Step 1  
Select MFA device

Step 2  
Set up device

## Select MFA device

### Specify MFA device name


Device name  
Enter a meaningful name to identify this device.

Phone-IAM-user


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

### Select MFA device [Info](#)


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.

☐

**Security Key**  
Authenticate using a code generated by touching a YubiKey or other supported FIDO security key.

☐

**Hardware TOTP token**  
Authenticate using a code displayed on a hardware Time-based one-time password (TOTP) token.

Next

#### 4- Set up device

Scan the QR Code and enter two consecutive MFA codes as MFA code 1 and MFA code 2

**Set up device**

**Set up your 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, then use the app to scan the QR code. Alternatively, you can type a secret key.  
[Show QR code on this page](#)  
[Show secret key](#)

3 Fill in two consecutive codes from your MFA device.

MFA code 1  
145305

MFA code 2  
952486

Cancel Previous Add MFA

Now, you can see below MFA devices and identifier

**Account details**

User name: imran-admin  
User ARN: arn:aws:iam::[redacted]:user/imran-admin  
AWS account ID: [redacted]  
Canonical user ID: 477bb1a02fad03e4a918b351335682e80c839bd2cad8601190d4f7cb9f966a5f

**Console sign-in**

Console sign-in link: <https://dataops-demo-account-alias.signin.aws.amazon.com/console>  
Console password: Updated Yesterday (2023-02-20 23:14 GMT+3)  
Last console sign-in: 11 minutes ago (2023-02-22 20:14 GMT+3)

**Multi-factor authentication (MFA) (2)**  
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](#)

Remove Resync Assign MFA device

Device type	Identifier	Created on
Virtual	arn:aws:iam::[redacted]:mfa/Phone-IAM	4 hours ago
Virtual	arn:aws:iam::[redacted]:mfa/Phone-IAM-user	Now