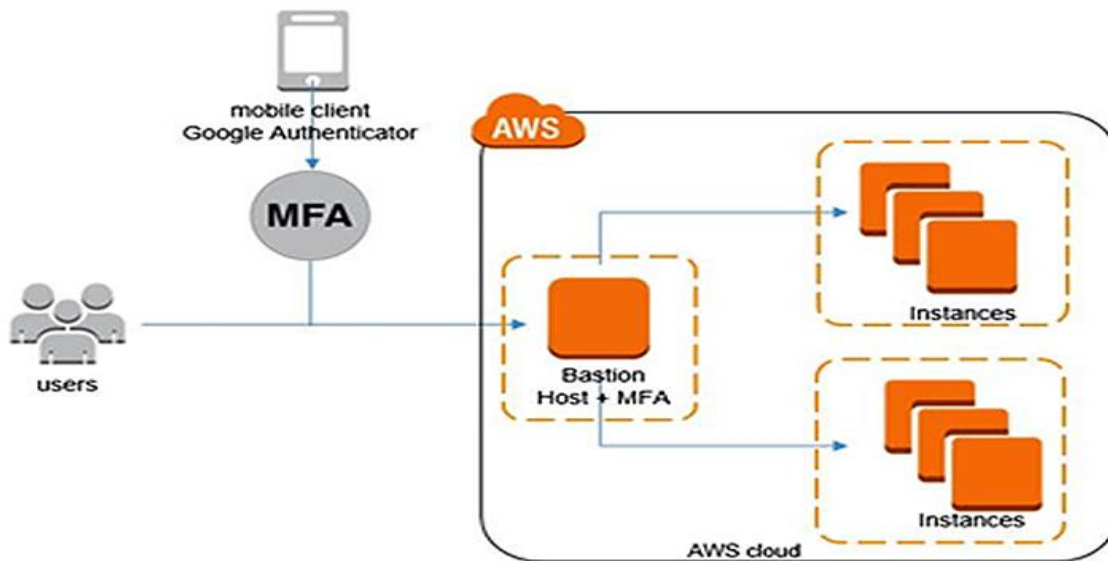


Overview of AWS MFA:

AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of your username and password. With MFA enabled, when a user signs in to an [AWS Management Console](#), they will be prompted for their user's name and password (the first factor is what they know), as well as for an authentication code from their AWS MFA device (the second factor is what they have). Taken together, these multiple factors provide increased security for your AWS account settings and resources.

Why AWS MFA is Required:

- Users have access to your account and can possibly change configurations and delete resources in your AWS account, so to overcome this it is required
- If you want to protect your root accounts and IAM user.
- Even if the password is stolen or hacked, the account is not compromised.
- When you enable this authentication for the root user, it affects only the root user credentials. IAM users in the account are distinct identities with their own credentials, and each identity has its own MFA configuration.



MFA Device Options In AWS

The following are the MFA device options in AWS:

- **Virtual MFA Device:** Support for multiple tokens on a single device e.g **Google Authenticator** (Phone Only) **Authy** (Multi-Device)
- **Universal 2nd Factor (U2F) Security Key:** Supports multiple root and IAM users using a single security key. e.g **Yubikey** by Yubico (Third Party)
- **Hardware Key Fob MFA Device:** Provided by Gemalto (Third Party)
- **Hardware Key Fob MFA Device AWS GovCloud (US):** Provided by SurePassID (Third Party)

Enabling MFA on Root Account


- 1) Log in to your AWS account.
- 2) On the right side of the navigation bar, choose your account name, and choose **My Security Credentials**.

The screenshot shows the AWS IAM dashboard interface. On the right side, the navigation menu is open, displaying several options. The 'My Security Credentials' option is highlighted with a red box, and a red arrow points to it from the account name '889610009184' at the top of the menu. The main content area of the dashboard includes sections for IAM resources (Users: 0, Roles: 8, Groups: 0, Identity providers: 0), Security alerts (warning that MFA is not enabled on the root user), and Best practices (Grant least privilege access, Enable identity federation).

3) Click on Assign MFA device.

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.

 **MFA not activated for root user**
The root user for this account does not have multi-factor authentication (MFA) activated. Activate MFA to improve security for this account.

[Assign MFA](#)

4) Choose **Virtual MFA Device** and click on **Continue**.

Select MFA device

Specify MFA device name




Device name
Enter a meaningful name to identify this device.

ABC

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.

Cancel [Next](#)

5) Now Install Google Authenticator on your phone.

Android: [Click here](#)


IOS: [Click here](#)

6) Now Click on Show QR Code and open the Google Authenticator app on your phone.

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, 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**

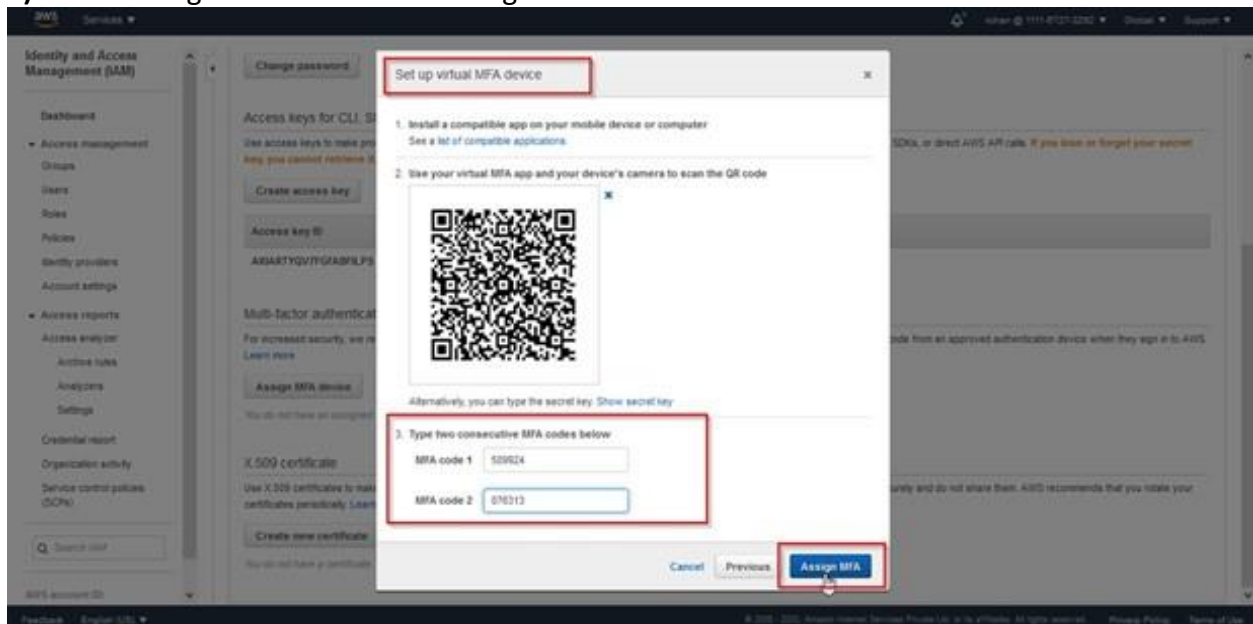
Note: Take a screenshot of the code so that in the future if you lose your phone, you can use it to re-enable MFA.

7) Now open the Google Authenticator App Click on Get started and scan the QR code.

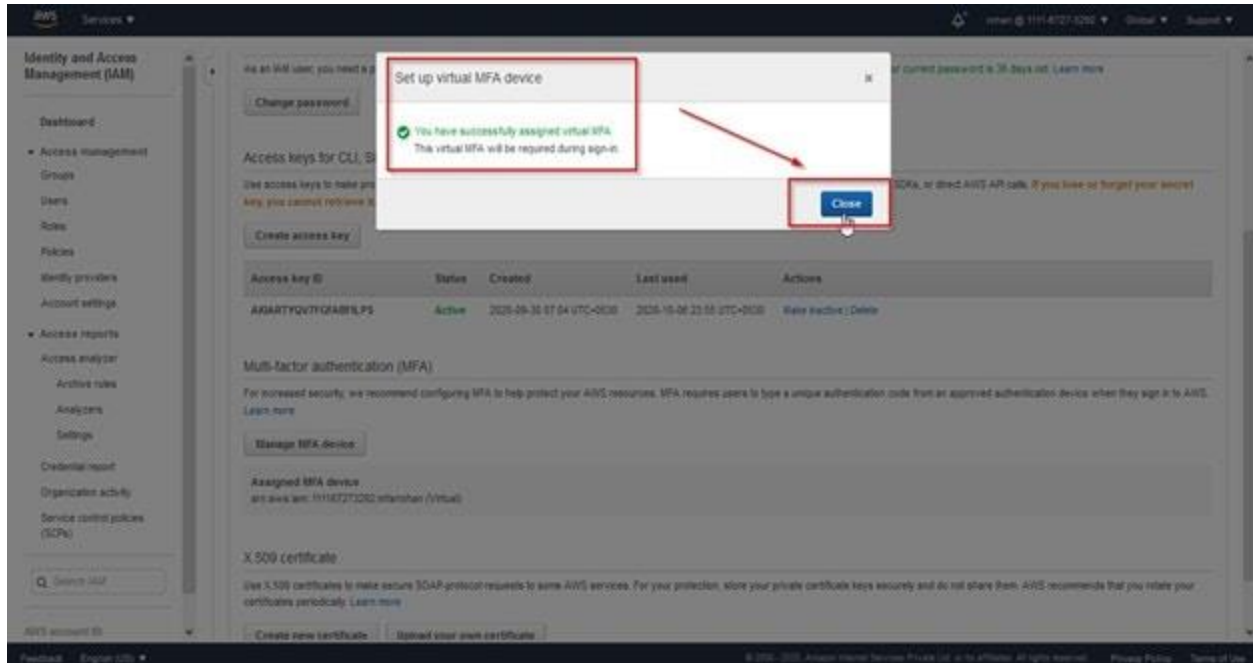


8) Now enter the code from your Phone into MFA code 1 and MFA code 2.

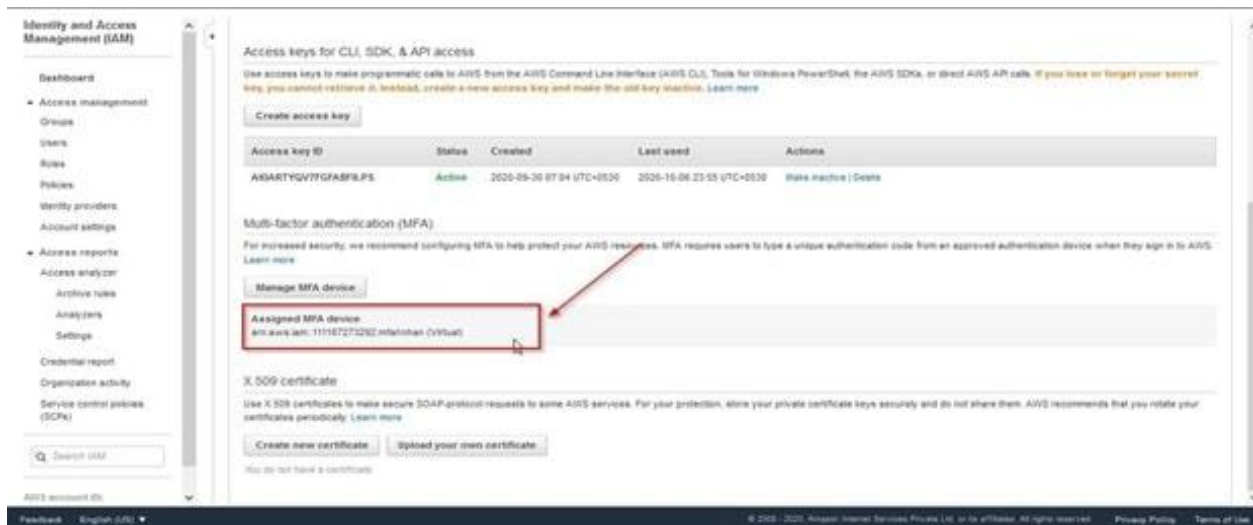
9) After adding MFA code click on Assign MFA.



10) You will get a success message then click on Close.



11) Now you will see that the device has been added for MFA.



12) Now you have successfully **Activated MFA on your root account setting.**

Accessing AWS Console Using MFA:

- 1) Open your AWS console login page and click on Root User then enter your email.



Sign in

Root user

Account owner that performs tasks requiring unrestricted access. [Learn more](#)

IAM user

User within an account that performs daily tasks. [Learn more](#)

Root user email address

XXXXXXXXXXXXXXXXXXXX@EXAMPLE.COM

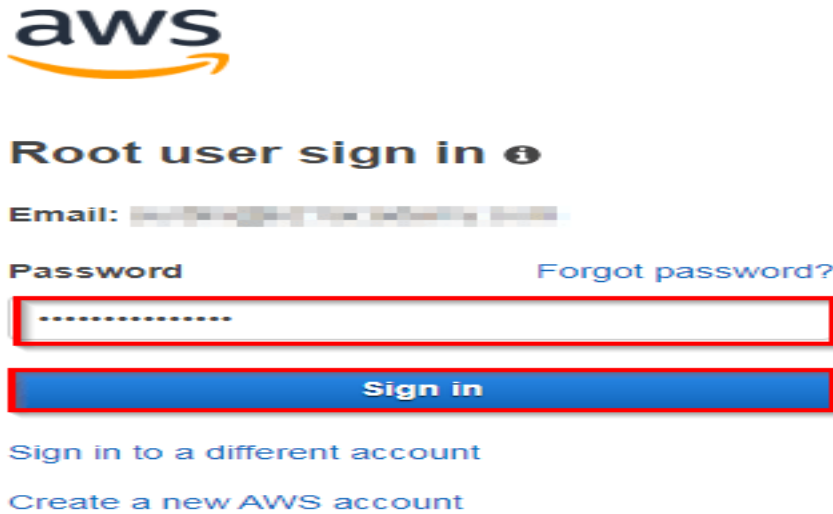
Next

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

————— New to AWS? —————

Create a new AWS account

- 2) Enter your password corresponding to the Email address.



aws

Root user sign in ⓘ

Email: [redacted]

Password [Forgot password?](#)

.....

Sign in

[Sign in to a different account](#)

[Create a new AWS account](#)

- 3) Use your **Google Authenticator** Application on mobile and enter MFA code in AWS Console.



aws

Multi-factor authentication

Your account is secured using multi-factor authentication (MFA). To finish signing in, turn on or view your MFA device and type the authentication code below.

Email address:
[redacted]

MFA code

695768

Submit

[Troubleshoot MFA](#)

[Cancel](#)

CONGRATULATION. You've set up AWS MFA and enable it.