

SOFTWARE DEVELOPMENT AND IT OPERATIONS LAB

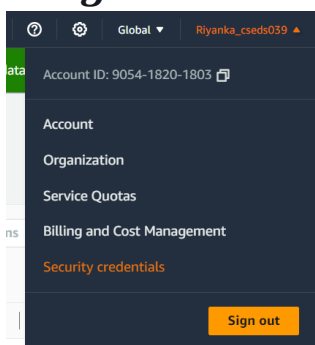
ASSIGNMENT 2: Create MFA for Authentication.

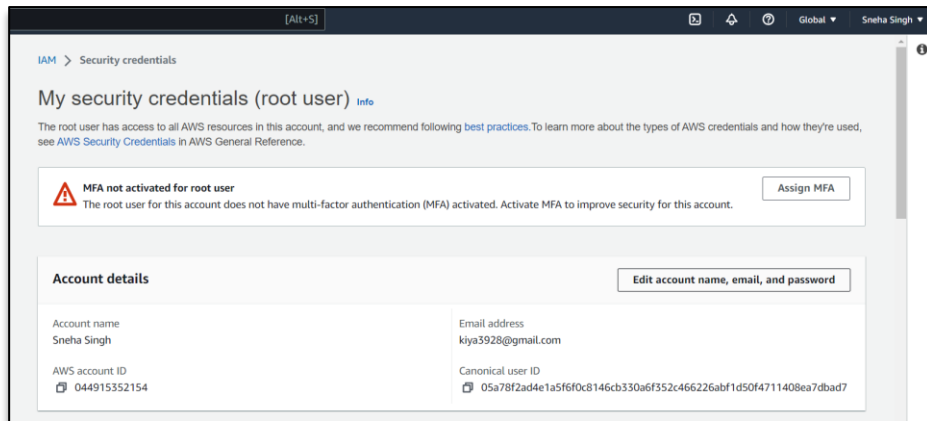
Multi - Factor authentication (MFA):-

MFA adds extra security because it requires users to provide unique authentication from an AWS supported MFA mechanism in addition to their regular sign-in credentials when they access AWS websites or services. For increased security, we recommend that you configure multi-factor authentication (MFA) to help protect your AWS resources. You can enable MFA for the AWS account root user and IAM users. When you enable MFA for the root user, it affects only the root user credentials.

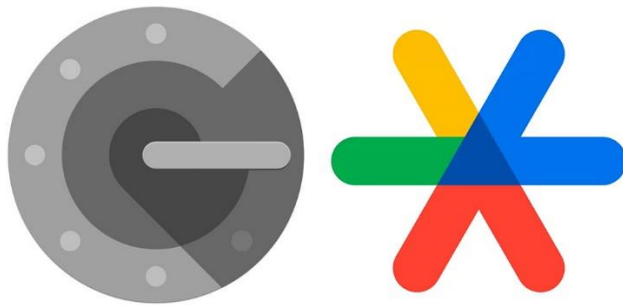
Using Multi-factor authentication (MFA) in AWS:-

1. Sign in to the AWS Management Console.
2. On the right side of the navigation bar, choose your account name, and choose ***Security credentials***. If necessary, choose ***Continue to Security credentials***.
3. In the ***Multi-Factor Authentication (MFA)*** section, choose ***Assign MFA device***.





4. In the wizard, type a ***Device name*** let it be ***d1***, choose ***Authenticator app***(download it from playstore in your smartphone), and then choose ***Next***.



5. It displays configuration information for the virtual MFA device, including a QR code graphic. The graphic is a representation of the secret configuration key that is available for manual entry on devices that do not support QR codes.

IAM > Security credentials > Assign MFA device

Step 1
Select MFA 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.

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.

Step 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, 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](#)

Fill in two consecutive codes from your MFA device.

3

MFA code 1

MFA code 2

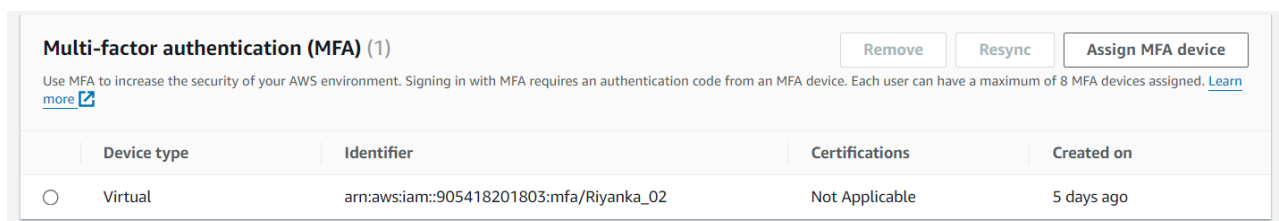
6. Open the virtual MFA app on the device.
7. To use the QR code to configure the virtual MFA device, from the wizard, choose **Show QR code**. Then follow the app instructions for scanning the code. For example, you might need to choose the camera icon or choose a command like **Scan account barcode**, and then use the device's camera to scan the QR code. We have used the **Google Authenticator** app for authentication.
8. The device starts generating six-digit numbers
9. In the wizard, in the **MFA code 1** box, type the one-time password that currently appears in the virtual MFA device. Wait up to 30 seconds for the device to generate a new one-time password. Then type the second one-time password into the **MFA code 2** box. Choose **Add MFA**.



The device is ready for use with AWS. For information about using MFA with the AWS Management Console.

Now , when we sign out of the console , everytime we log in again we need to enter the MFA code generated by the Authenticator app to successfully sign in to our AWS account.

After successful creation of MFA, the MFA details will look like this:



Now once the MFA is created, when you sign in again next time into your account after giving the **Email and Password** it will then ask you to enter the **MFA code** and the code will be provided by the **Authenticator app**.



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: nagriyanka931@gmail.com

MFA code

Submit

[Troubleshoot MFA](#)

[Cancel](#)