**Practical No.7**

**Aim: Study and implement MFA in the environment of popular Cloud Service Provider in AWS.**

**THEORY :**

[AWS multi-factor authentication](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#enable-mfa-for-privileged-users) (MFA) is an [AWS Identity and Access Management (IAM)](https://aws.amazon.com/iam/) best practice that requires a second authentication factor in addition to user name and password sign-in credentials. You can enable MFA at the AWS account level and for root and IAM users you have created in your account.

AWS is expanding eligibility for its free MFA security key program. Verify your eligibility and order your [free MFA key](https://aws.amazon.com/security/amazon-security-initiatives/free-mfa-security-key/).

With MFA enabled, when a user signs in to the [AWS Management Console](https://console.aws.amazon.com/console/home), they are prompted for their user name and password— something they know—and an authentication code from their MFA device— something they have (or if they use a biometrics-enabled authenticator, something they are). Taken together, these factors improve security for your AWS accounts and resources.

We recommend that you require your human users to use temporary credentials when accessing AWS. Your users can use an identity provider to federate into AWS, where they can authenticate with their corporate credentials and MFA configurations. To manage access to AWS and business applications, we recommend that you use [AWS IAM Identity Center](https://aws.amazon.com/iam/identity-center/). For more information, see the [IAM Identity Center User Guide](https://docs.aws.amazon.com/singlesignon/latest/userguide/what-is.html).

See the following available MFA options that you can use with your IAM MFA implementation. You can download virtual authenticator apps through the links provided, or you can acquire a hardware MFA device from the respective manufacturer. After you've acquired a supported virtual or hardware MFA device, AWS does not charge additional fees for using MFA.

Available MFA methods for IAM

You can manage your MFA devices in the [IAM console](https://console.aws.amazon.com/iam/). The following options are the MFA methods that IAM supports.

FIDO security keys

FIDO-certified hardware security keys are provided by third-party providers such as Yubico. The FIDO Alliance maintains a list of all [FIDO-certified products](https://fidoalliance.org/certification/fido-certified-products/)  that are compatible with FIDO specifications. FIDO authentication standards are based on public key cryptography, which enables strong, phishing-resistant authentication that is more secure than passwords. FIDO security keys support multiple root accounts and IAM users using a single security key. For more information about enabling FIDO security keys, see [Enabling a FIDO security key](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_fido.html).

AWS offers a [free MFA security key](https://aws.amazon.com/security/amazon-security-initiatives/free-mfa-security-key/) to eligible AWS account owners in the United States. To determine eligibility and order a key, see the [Security Hub console](https://console.aws.amazon.com/securityhub/home/#/free-mfa-security-key).

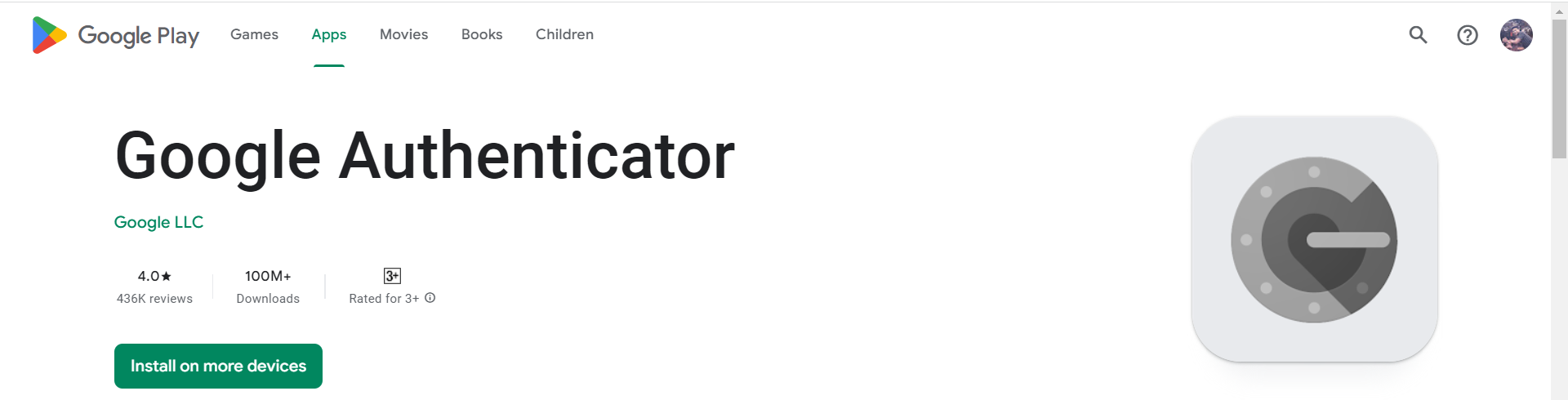
Virtual authenticator apps

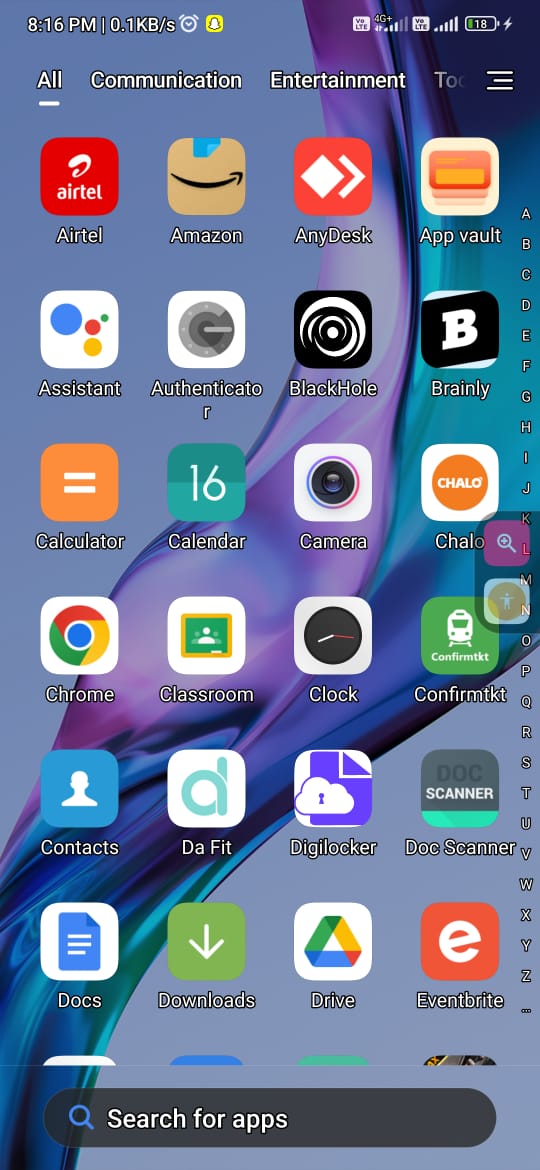
Virtual authenticator apps implement the [time-based one-time password](https://datatracker.ietf.org/doc/html/rfc6238) (TOTP) algorithm and support multiple tokens on a single device. Virtual authenticators are supported for IAM users in the [AWS GovCloud (US) Regions](https://aws.amazon.com/govcloud-us/) and in other AWS Regions. For more information about enabling virtual authenticators, see [Enabling a virtual multi-factor authentication (MFA) device](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_virtual.html).You can install apps for your smartphone from the app store that is specific to your type of smartphone. Some app providers also have web and desktop applications available. See the following table for examples.

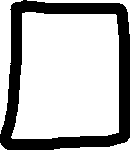
|  |  |
| --- | --- |
| Android | [Twilio Authy Authenticator](https://play.google.com/store/apps/details?id=com.authy.authy), [Duo Mobile](https://play.google.com/store/apps/details?id=com.duosecurity.duomobile), [LastPass Authenticator](https://play.google.com/store/apps/details?id=com.lastpass.authenticator), [Microsoft Authenticator](https://play.google.com/store/apps/details?id=com.azure.authenticator), [Google Authenticator](https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2), [Symantec VIP](https://m.vip.symantec.com/home.v#searchwebsite) |
| iOS | [Twilio Authy Authenticator](https://apps.apple.com/us/app/authy/id494168017), [Duo Mobile](https://apps.apple.com/us/app/duo-mobile/id422663827), [LastPass Authenticator](https://apps.apple.com/us/app/lastpass-authenticator/id1079110004), [Microsoft Authenticator](https://apps.apple.com/us/app/microsoft-authenticator/id983156458), [Google Authenticator](https://apps.apple.com/us/app/google-authenticator/id388497605), [Symantec VIP](https://m.vip.symantec.com/home.v#searchwebsite) |

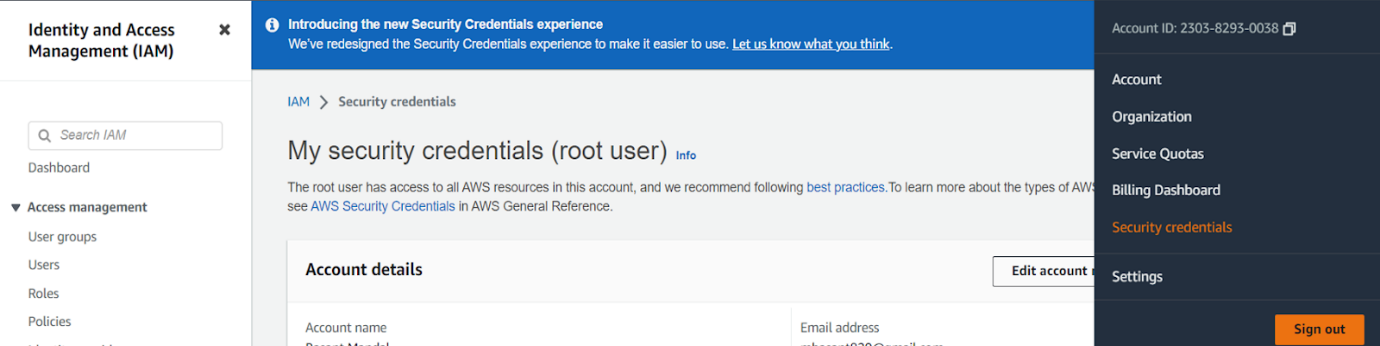
**GOOGLE APP FOR AUTHENTICATION :**

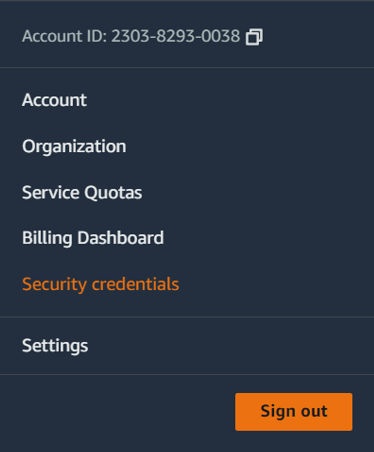
<https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2>

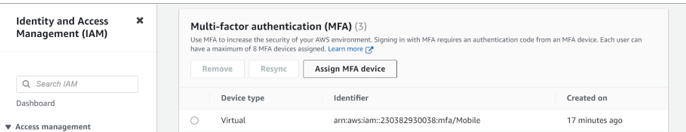


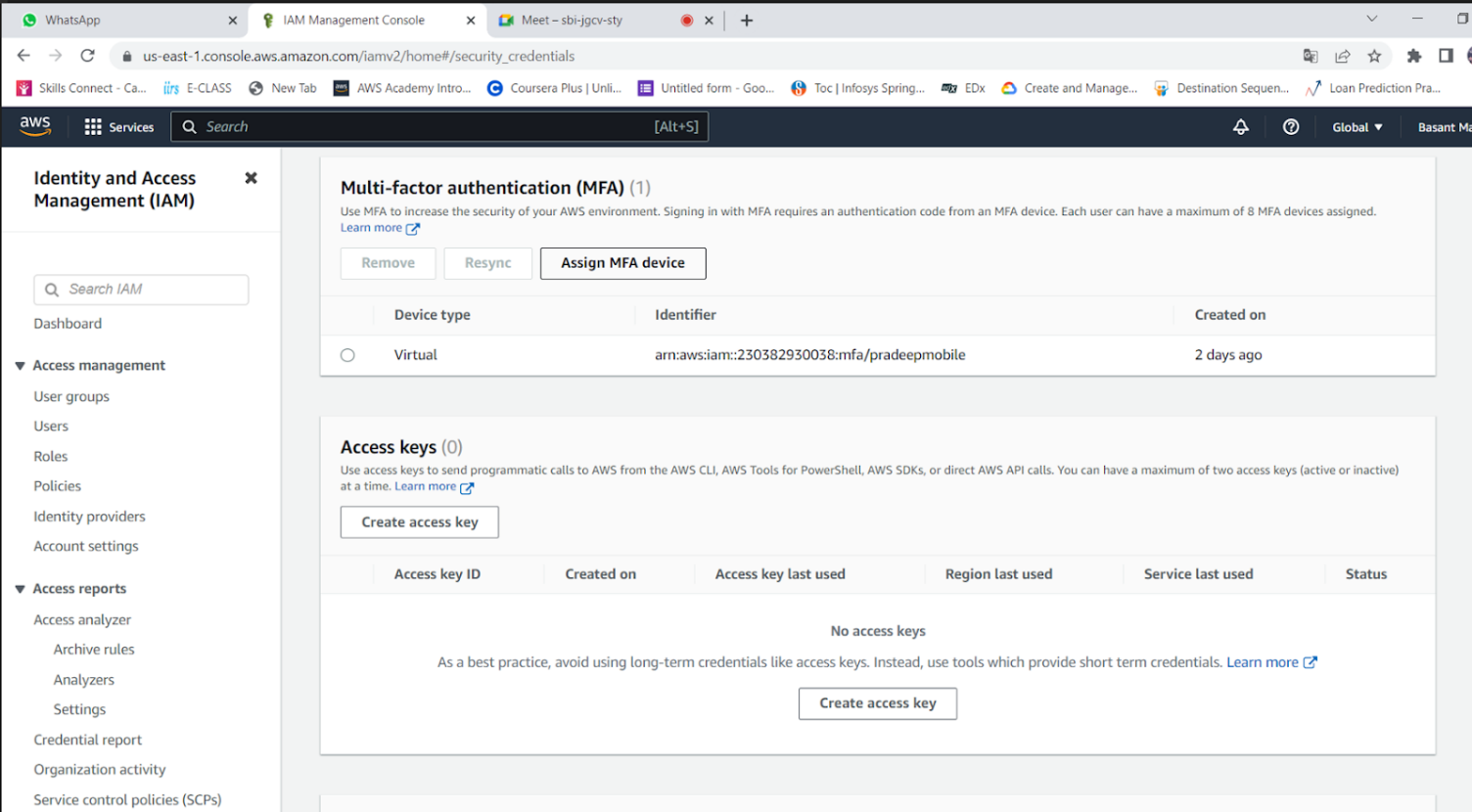
 **IMPLEMENTATION:**

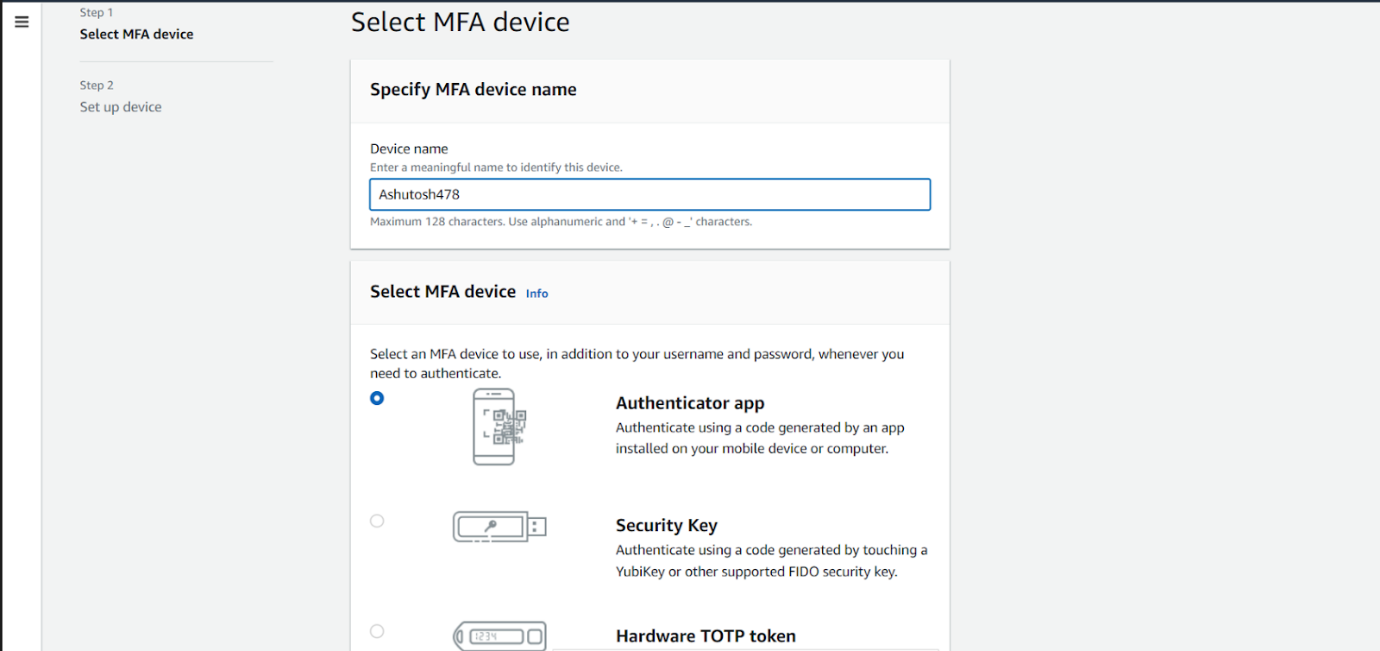


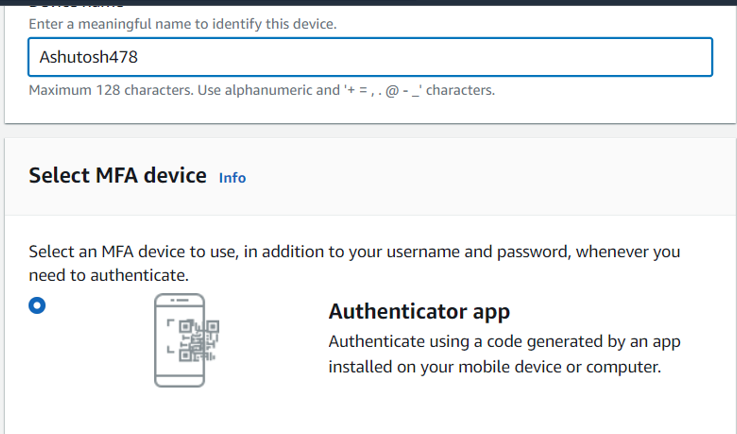




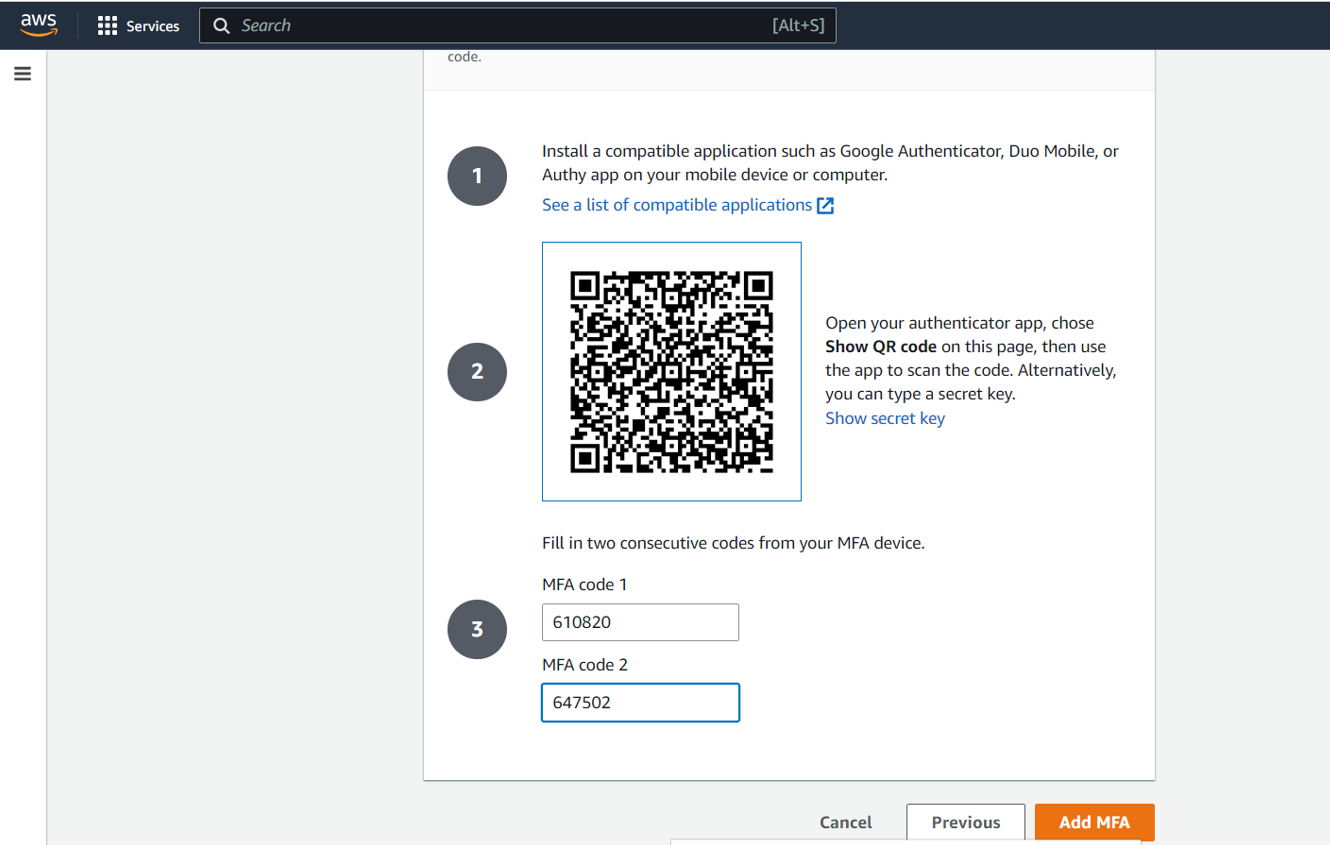


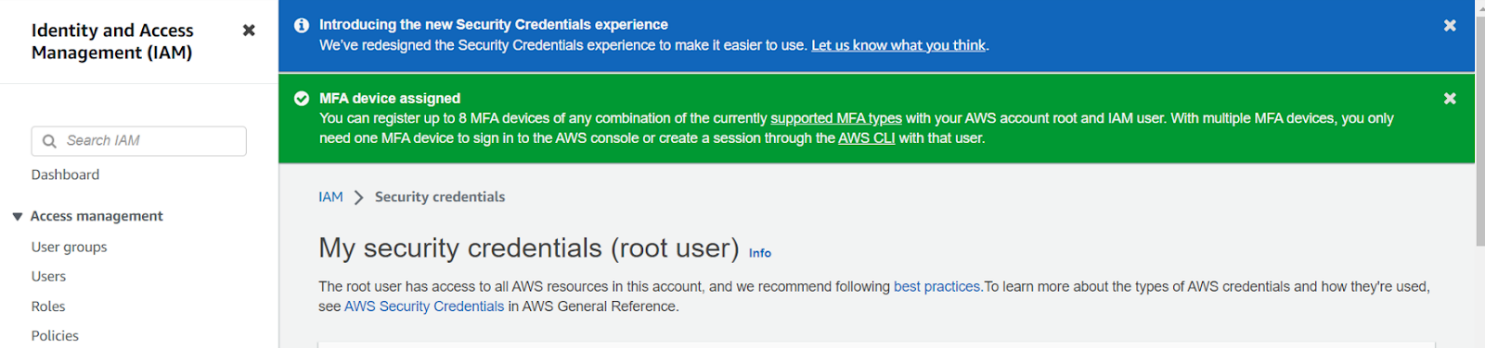






**USE GOOGLE AUTHENTICATOR APP FOR OTP:**





**CONCLUSION** : Successfully Implemented [AWS multi-factor authentication](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#enable-mfa-for-privileged-users) (MFA).