

Practical-6 Implementing MFA.

Writeup:-

• MFA

Multi-factor authentication (MFA) is a multi-step account login process that requires users to enter more information than just a password. For example, along with the password, users might be asked to enter a code sent to their email, answer a secret question, or scan a fingerprint. A second form of authentication can help prevent unauthorized account access if a system password has been compromised.

BENEFITS:

Reduces security risk

Multi-factor authentication minimizes risks due to human error, misplaced passwords, and lost devices.

Enables digital initiatives

Organizations can undertake digital initiatives with confidence. Businesses use multi-factor authentication to help protect organizational and user data so that they can carry out online interactions and transactions securely.

Improves security response

Companies can configure a multi-factor authentication system to actively send an alert whenever it detects suspicious login attempts. This helps both companies and individuals to respond faster to cyberattacks, which minimizes any potential damage.

• Types of MFA

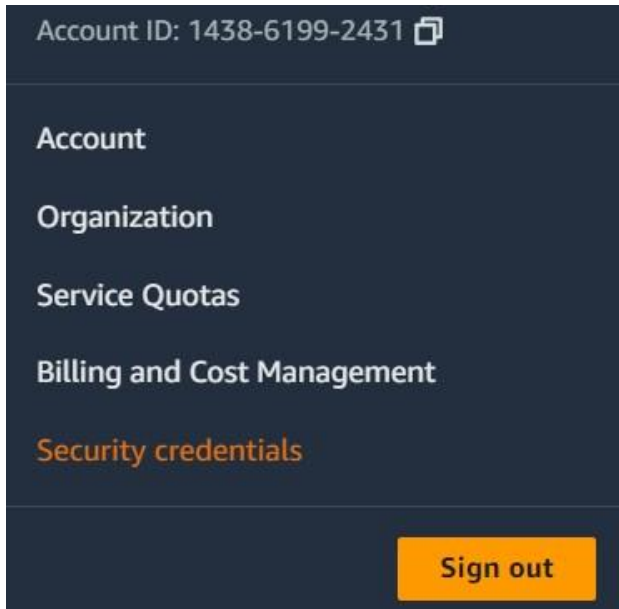
SMS-Based MFA: In this method, after entering the username and password, the user receives a one-time code via SMS (Short Message Service) on their registered mobile phone. They then enter this code to complete the authentication process.

Time-Based One-Time Password (TOTP): TOTP is a type of MFA where a temporary numeric code is generated based on the current time and a shared secret key. This code is typically generated by a smartphone app such as Google Authenticator or Authy. The user must enter this code along with their username and password to authenticate.

Hardware Tokens: Hardware tokens are physical devices that generate one-time passwords. These tokens can be USB tokens, smart cards, or key fobs. When a user needs to authenticate, they simply press a button on the token, and it generates a unique code that they enter along with their other credentials.

PRACTICAL IMPLEMENTATION USING GOOGLE AUTHENTICATOR.

Study and implement MFA in the environment of popular Cloud Service Provider



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.



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](#)

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

123456

MFA code 2

879564

Cancel

Previous

Add MFA

CREATE USER AND ASSIGN MFA

Users (1)

Refresh

Delete users

Add user

Users listed here can sign in to the AWS access portal to access AWS accounts and assigned cloud applications. [Learn more](#)

Username

Find users

< 1 >

Settings

<input type="checkbox"/>	Username	Display name	Status	MFA devices	Created by
<input type="checkbox"/>	sunny	Sunny Singh	<div>Enabled</div>	1 device	Manual

sunny

General information

Profile

Groups (1)

AWS accounts

Applications

MFA devices (1)

Active sessions (0)

[Register MFA device](#)

Register MFA device

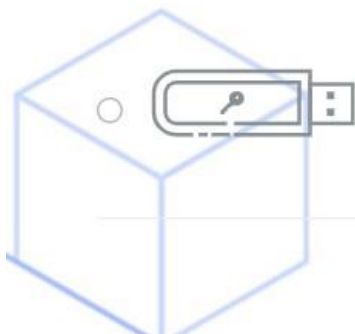
Username:

Choose one of the following MFA device types for sunny. [Learn more](#)



Authenticator app

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



Security key

Authenticate by touching a hardware security key such as YubiKey, Feitian, etc.

Cancel


Next

Set up the authenticator app

Username:

1



Install either the Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer. [See a list of compatible apps](#) 

2



Use your virtual MFA app or your device's camera to scan the QR code ([show secret key](#))

3

Please enter the six digit code from your authenticator app

Authenticator code

Cancel

Assign MFA