TASK 4: Enable Multi-Factor Authentication (MFA) for "S3-User":

To enable Multi-Factor Authentication (MFA) for "S3-User":

1. Select "S3-User" from IAM and here we can see its permissions , groups , Tags , Security Credentials and Access Advisor options .

2. Then Navigate to Security Credentials and Scroll down to "Multi-factor authentication (MFA)" and click on "Assign MFA Device"

3. Now Give the Device name and Select Authenticator app from MFA device list and Then click on next.

MFA device name

Device name
Enter a meaningful name to identify this device.

Venis-PC

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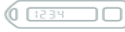
Authenticator app
Authenticate using a code generated by an app installed on your mobile device or computer.

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.

4. Install the Microsoft Authenticator on your device(Phone) and scan the QR code . Then we'll get codes in the interval of 30 seconds . Enter any two consecutives codes as MFA code1 and MFA code2 and then select "Add MFA".

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

Fill in two consecutive codes from your MFA device.

MFA code 1

520219

MFA code 2

3. 250940

Cancel   Previous   **Add MFA**

5. Now we'll be navigated to IAM>Users>S3-Users and we can see that MFA device has been assigned to the user .