**Enabling MFA for IAM User**

**Objective:** To enable Multi-Factor Authentication (MFA) for an IAM user, enhancing the security of AWS accounts

**Tools required:** AWS Console and Google Authenticator

**Prerequisites:** None

Steps to be followed:

1. Create an IAM user
2. Install Google Authenticator
3. Assign an MFA device to the IAM User
4. Sign in with MFA

**Step 1: Create an IAM user**

1. Open the **AWS Management Console** in your practice environment

A screenshot of a computer

Description automatically generated

1. Search for **IAM** in the search bar and click on the **IAM** service  
     
   A screenshot of a computer

   Description automatically generated
2. Choose **Users** in the left navigation pane and click on **Create user**  
   A screenshot of a computer

   Description automatically generated
3. Enter a desired name in the **User name** field  
     
   A screenshot of a computer

   Description automatically generated
4. Select the check box of AWS Management Console access, choose **Custom password**, and set a password  
     
   A screenshot of a computer

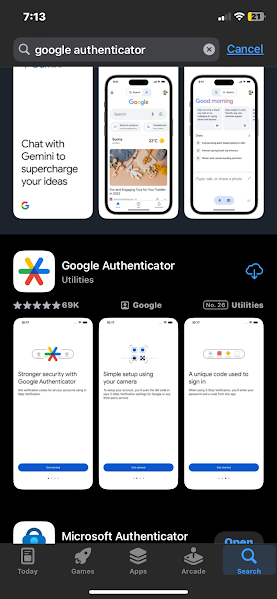
   Description automatically generated
5. Deselect **User must create a new password at next sign-in - Recommended** and click on **Next**  
     
   A screenshot of a computer

   Description automatically generated
6. Keep the default settings and click **Next**  
     
   A screenshot of a computer

   Description automatically generated
7. Click on **Create user**  
     
   A screenshot of a computer

   Description automatically generated

**Step 2:** **Install Google Authenticator**

1. Install Google authenticator on your mobile device  
     
     
     
   Open the app and get ready for the next steps.

**Step 3: Assign an MFA device to the IAM User**

1. Navigate back to the AWS Management Console and click on the created IAM user  
     
   A screenshot of a computer

   Description automatically generated
2. Click on **Security credentials**  
     
   A screenshot of a computer

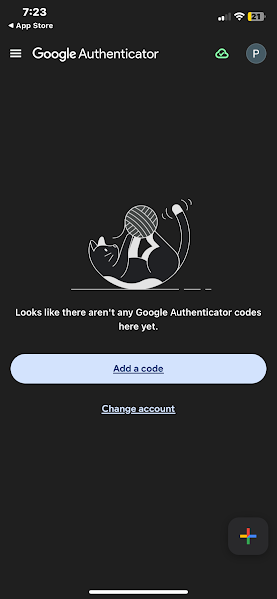
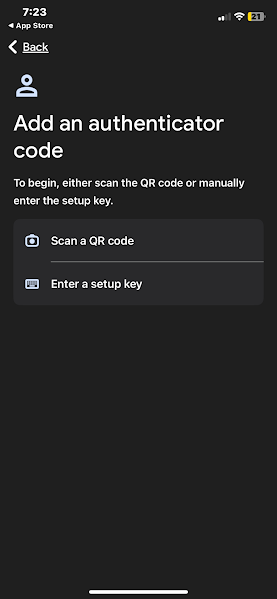
   Description automatically generated
3. Click on **Assign MFA device**  
     
   A screenshot of a computer

   Description automatically generated
4. Provide a name for the MFA device in the **Device name** field  
     
   A screenshot of a computer

   Description automatically generated
5. Select **Authenticator app**  
     
   A screenshot of a computer

   Description automatically generated
6. Click on **Next**  
     
   A screenshot of a computer

   Description automatically generated
7. Click on **Show QR code**  
     
   A screenshot of a computer

   Description automatically generated
8. Open **Google Authenticator** on your mobile device and tap on **Add a code**  
     
   
9. Select **Scan a QR code**  
     
   
10. Scan the QR code displayed on the AWS Management Console with your mobile device  
      
    A screenshot of a computer

    Description automatically generated
11. Enter the generated MFA codes from your device and click on **Add MFA**  
      
    A screenshot of a computer

    Description automatically generated
12. Confirm that the MFA device has been successfully assigned  
      
    A screenshot of a computer

    Description automatically generated

**Step 4: Sign in with MFA**

1. Log in using the IAM user credentials created and click on **Sign in**  
     
   A screenshot of a computer

   Description automatically generated
2. Enter the MFA code generated by your mobile device and click on **Sign in**  
     
   A screenshot of a computer

   Description automatically generated
3. Confirm that you have successfully signed in to the IAM user account with MFA enabled  
     
   A screenshot of a computer

   Description automatically generated

By following these steps, you have successfully enabled Multi-Factor Authentication (MFA) for an IAM user to enhance the security of AWS accounts.