

Assignment-2

Instructions to Enable Multi-Factor Authentication (MFA) in AWS

Objective: Configure Multi-Factor Authentication (MFA) for enhanced security of your AWS account.

Steps

1. **Sign in to the AWS Management Console:**
 - Open your preferred browser and navigate to the [AWS Management Console](#).
 - Log in using your root user or IAM user credentials.
2. **Access Security Credentials:**
 - In the top-right corner of the navigation bar, click your account name.
 - Select **Security credentials** from the dropdown.
 - If prompted, click **Continue to Security credentials**.
3. **Initiate MFA Setup:**
 - Scroll down to the **Multi-Factor Authentication (MFA)** section.
 - Click **Assign MFA device** to start the configuration wizard.
4. **Choose MFA Device Type:**
 - In the wizard, enter a **Device name** (e.g., "d1") to identify the MFA device.
 - Select **Authenticator app** as the device type.
 - Click **Next**.
5. **Obtain the QR Code:**
 - The wizard will display a QR code and its corresponding secret key (for devices that don't support QR codes).
 - This QR code is used to configure your virtual MFA device.
6. **Set Up the Authenticator App:**
 - Download and install a virtual MFA app (e.g., **Google Authenticator** or **Authy**) on your mobile device if not already installed.
 - Open the app and choose the option to add a new account.
 - Use your device's camera to scan the QR code displayed in the AWS wizard.
 - **Remark:** If your app doesn't support QR code scanning, manually enter the secret configuration key provided in the wizard.
7. **Generate MFA Codes:**
 - After successfully scanning the QR code, the app will start generating six-digit one-time passwords (OTP).
8. **Verify MFA Device:**
 - In the AWS wizard, enter the first OTP in the **MFA code 1** field.
 - Wait for the app to generate a new OTP (approximately 30 seconds) and enter it in the **MFA code 2** field.
 - Click **Add MFA** to finalize the setup.
9. **Completion:**
 - Your MFA device is now enabled and linked to your AWS account.
 - Log out and log back into your AWS account to test the configuration. Each login attempt will now require the six-digit MFA code from your authenticator app.

Remarks

- **Why Enable MFA?**
 - MFA adds an additional layer of security by requiring both your password and a dynamically generated code for authentication. This mitigates the risk of unauthorized access.
 - **Recommended Apps:**
 - Use popular and reliable authenticator apps such as **Google Authenticator**, **Authy**, or **Microsoft Authenticator**.
 - **Troubleshooting:**
 - If you face issues scanning the QR code or entering the OTP, ensure:
 - Your device's time is synchronized with an accurate time source.
 - The authenticator app is installed and updated.
 - For further assistance, refer to the [AWS MFA documentation](#).
-