TẠO TÀI KHOẢN AWS ĐẦU TIÊN

Tổng quan

Trong bài lab đầu tiên này, bạn sẽ tạo mới **tài khoản AWS** đầu tiên của mình, tạo **MFA** (Multi-factor Authentication) để gia tăng bảo mật tài khoản của bạn. Bước tiếp theo bạn sẽ tạo **Admin Group**, **Admin User** để quản lý quyền truy cập vào các tài nguyên trong tài khoản của mình thay vì sử dụng user root.
Cuối cùng, nếu quá trình xác thực tài khoản của bạn có vấn đề, bạn sẽ được hướng dẫn hỗ trợ xác thực tài khoản với **AWS Support**.

Tài khoản AWS (AWS Account)

Tài khoản AWS là phương tiện để bạn có thể truy cập và sử dụng những tài nguyên và dịch vụ của AWS. Theo mặc định, mỗi tài khoản AWS sẽ có một *root user*. *Root user* có toàn quyền với tài khoản AWS của bạn, và quyền hạn của root user không thể bị giới hạn. Nếu bạn mới sử dụng tài khoản AWS lần đầu tiên, bạn sẽ truy cập vào tài khoản dưới danh nghĩa của *root user*.

Chính vì quyền hạn của **root user** không thể bị giới hạn, AWS khuyên bạn không nên sử dụng trực tiếp *root user* cho bất kỳ công tác nào. Thay vào đó, bạn nên tạo ra một *IAM User* và trao quyền quản trị cho *IAM User* đó để dễ dàng quản lý và giảm thiểu rủi ro.

MFA (Multi-factor Authentication)

MFA là một tính năng được sử dụng để gia tăng bảo mật của tài khoản AWS. Nếu MFA được kích hoạt, bạn sẽ phải nhập mã OTP (One-time Password) mỗi lần bạn đăng nhập vào tài khoản AWS.

IAM Group

IAM Group là một công cụ quản lý người dùng (*IAM User*) của AWS. Một IAM Group có thể chứa nhiều IAM User. Các IAM User ở trong một IAM Group đều hưởng chung quyền hạn mà IAM Group đó được gán cho.

IAM User

IAM User là một đơn vị người dùng của AWS. Khi bạn đăng nhập vào AWS, bạn sẽ phải đăng nhập dưới danh nghĩa của một IAM User. Nếu bạn mới đăng nhập vào AWS lần đầu tiên, bạn sẽ đăng nhập dưới danh nghĩa của *root user* (tạm dịch là người dùng

gốc). Ngoài *root user* ra, bạn có thể tạo ra nhiều IAM User khác để cho phép người khác truy cập **dài hạn** vào tài nguyên AWS trong tài khoản AWS của bạn.

AWS Support

AWS Support là một đơn vị cung cấp các dịch vụ hỗ trợ khách hàng của AWS.

Nội dung chính

TẠO MỚI TÀI KHOẢN AWS

Nội dung:

Tạo tài khoản AWS

1. Đi đến trang Amazon Web Service homepage.
2. Chọn **Create an AWS Account** ở góc trên bên phải.
    - ***Ghi Chú:*** *Nếu bạn không thấy* ***Create an AWS Account****, chọn* ***Sign In to the Console*** *sau đó chọn* ***Create a new AWS Account****.*
3. Nhập thông tin tài khoảng và chọn **Continue**.
    - ***Quan Trọng****: Hãy chắc chắn bạn nhập đúng thông tin, đặc biệt là email.*
4. Chọn loại account.
    - ***Ghi chú****: Personal và Professional đều có chung tính năng.*
5. Nhập thông tin công ty hoặc thông tin cá nhân của bạn.
6. Đọc và đồng ý AWS Customer Agreement.
7. Chọn **Create Account** và **Continue**.

Thêm phương thức thanh toán

- Nhập thông tin thẻ tín dụng của bạn và chọn **Verify and Add**.
    - ***Ghi chú****: Bạn có thể chọn 1 địa chỉ khác cho tài khoản của bạn bằng cách chọn* ***Use a new address*** *trước khi* ***Verify and Add****.*

Xác thực số điện thoại của bạn

1. Nhập số điện thoại.
2. Nhập mã security check sau đó chọn **Send SMS**.
3. Nhập mã code được gửi đến số điện thoại của bạn.

Chọn Support Plan

- Trong trang **Select a support plan**, chọn 1 plan có hiệu lực, để so sánh giữa cách plan, bạn hãy xem Compare AWS Support Plans.

Đợi account của bạn được kích hoạt

- Sau khi chọn **Support plan**, account thường được kích sau sau vài phút, nhưng quá trình có thể cần tốn đến 24 tiếng. Bạn vẫn có thể đăng nhập vào account AWS lúc này, Trang chủ AWS có thể sẽ hiển thị một nút “Complete Sign Up” trong thời gian này, cho dù bạn đã hoàn thành tất cả các bước ở phần đăng kí.
- Sau khi nhận được email xác nhận account của bạn đã được kích hoạt, bạn có thể truy cập vào tất cả dịch vụ của AWS.

MFA CHO TÀI KHOẢN AWS

Trong bước ngày, bạn có sử dụng ba thiết bị MFA khác nhau.
Một là các thiết bị (ứng dụng) MFA ảo trên smartphone như là Microsoft Authenticator, Google Authenticator, và Okta Verify.
Hai là khóa bảo mật U2F cứng.
Ba là các thiết bị MFA phần cứng khác như khóa bảo mật Gemalto.

Nội Dung

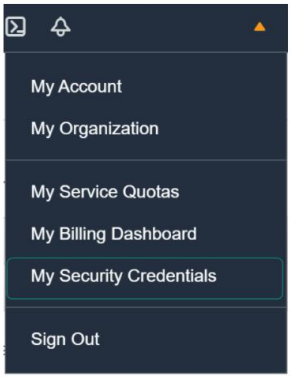
THIẾT BỊ MFA ẢO

Để kích hoạt MFA, bạn cần đăng nhập vào AWS sử dụng root user.

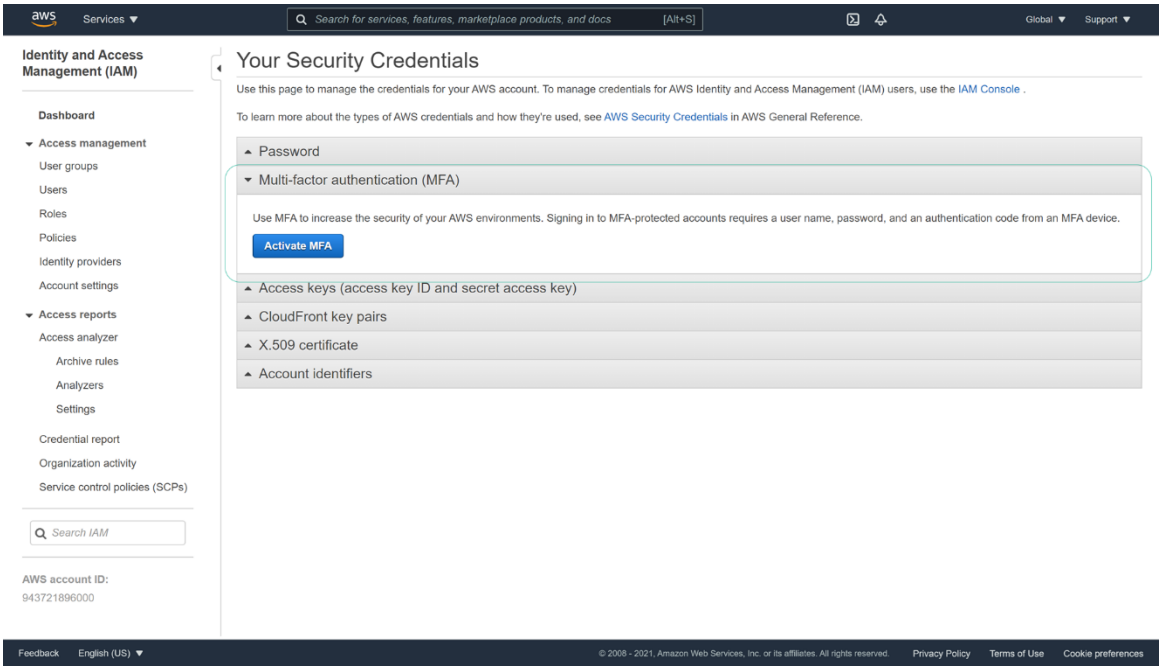
Kích hoạt thiết bị MFA ảo thông qua Console

Để thiết lập và kích hoạt thiết bị MFA ảo:

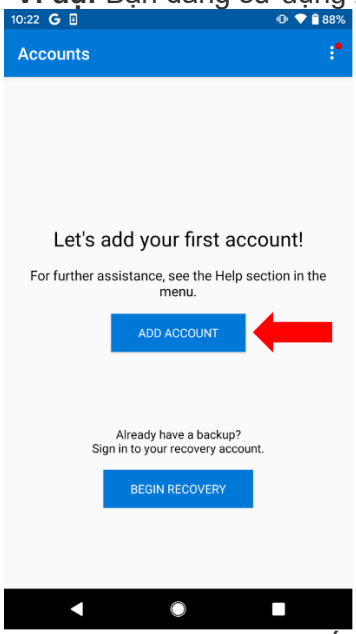
1. Đăng nhập vào AWS Console.
2. Góc trên bên phải, bạn sẽ thấy tên account của bạn, chọn vào và chọn **My Security Credentials**.

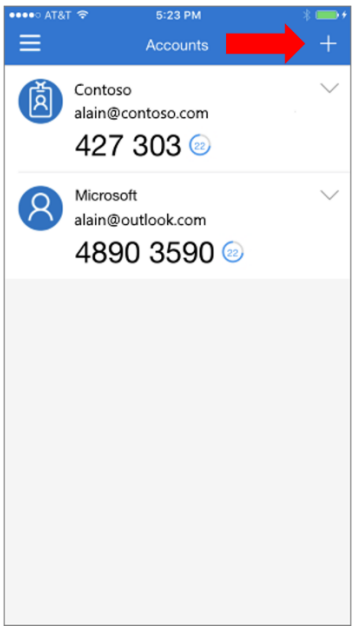


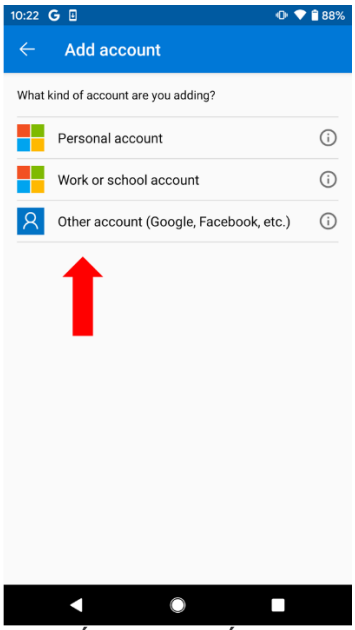
3. Mở rộng **Multi-factor authentication (MFA)** và chọn **Active MFA**.



4. Trong Manage MFA Device, chọn **Virtual MFA device** sau đó chọn **Continue**.
5. Cài đặt ứng dụng tương thích trên điện thoại của bạn. Danh sách ứng dụng MFA.
6. Sau khi cài đặt ứng dụng, chọn **Show QR Code** và dùng điện thoại đang mở ứng dụng MFA của bạn để scan mã QR.
    - ***Ví dụ:** Bạn đang sử dụng *Microsoft Authenticator*.







7. Ở ô **MFA code 1**, nhập 6 kí tự số trong app, đợi 30 giây sau đó nhập tiếp 6 kí tự số vào ô **MFA Code 2** và chọn **Assign MFA**.
8. Bây giờ bạn đã hoàn thành kích hoạt **thiết bị MFA ảo**.

KHÓA BẢO MẬT U2F

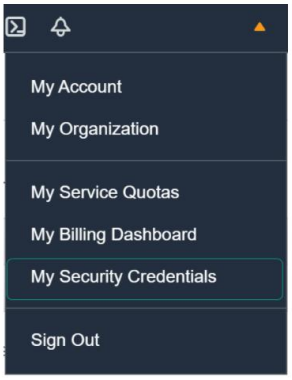
Nội dung

Nếu bạn không có thiết bị phần cứng , có thể bỏ qua các thao tác dưới đây nhé.

Kích hoạt khóa bảo mật U2F thông qua Console

U2F Security Key là một giao thức chứng thực mở cho phép người dùng có thể truy cập các dịch vụ trực tuyếp với một khóa bảo mật duy nhất mà không cần sử dụng đến bất kì phần mềm nào.

1. Đăng nhập vào AWS Console.
2. Góc trên bên phải, bạn sẽ thấy tên account của bạn, chọn vào và chọn **My Security Credentials** sau đó mở rộng Multi-factor authentication (MFA).

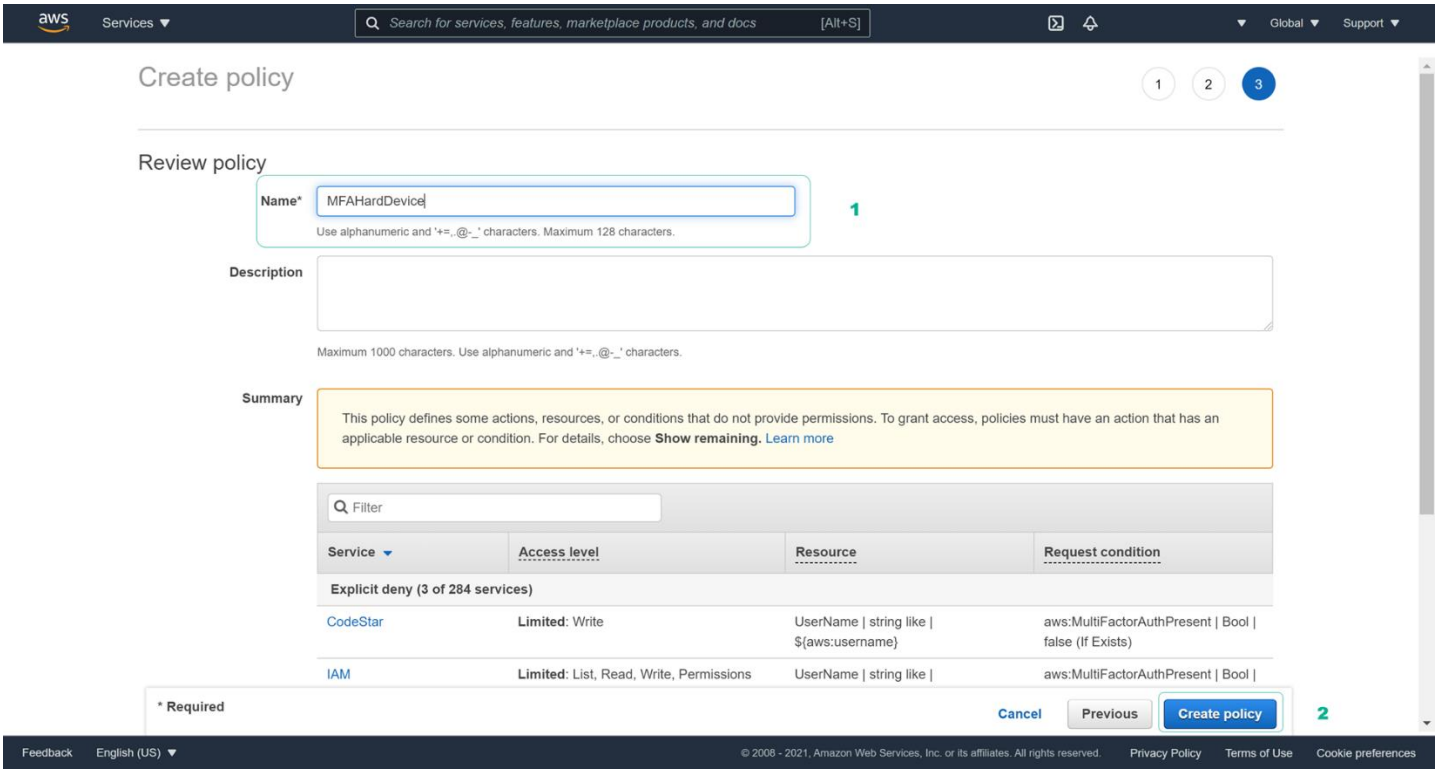


3. Để quản lí khóa bảo mật U2F, bạn phải có quyền từ bộ quyền sau. ở thanh bên trái, chọn **Policies** sau đó chọn **Create policy**, chọn **JSON** tab và dán phần bên dưới vào:

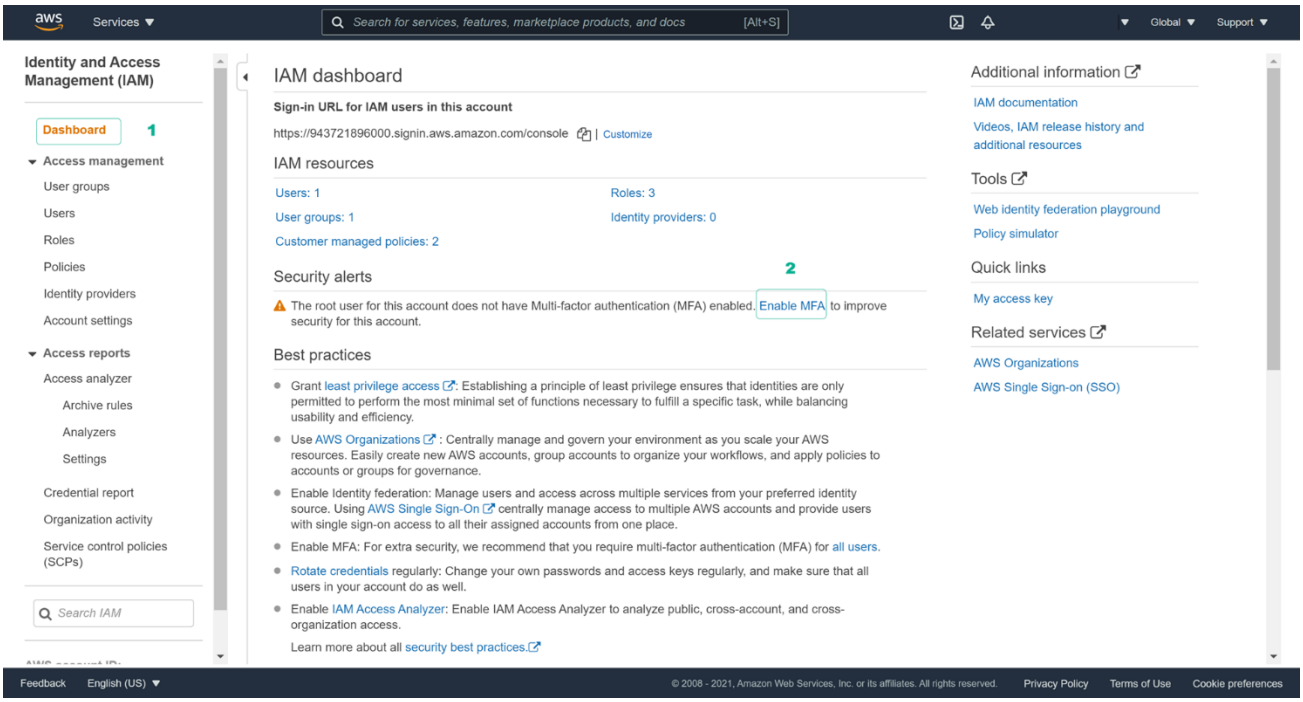
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowManageOwnUserMFA",
            "Effect": "Allow",
            "Action": [
                "iam:DeactivateMFADevice",
                "iam:EnableMFADevice",
```

```
                "iam:GetUser",
                "iam:ListMFADevices",
                "iam:ResyncMFADevice"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}"
        },
        {
            "Sid": "DenyAllExceptListedIfNoMFA",
            "Effect": "Deny",
            "NotAction": [
                "iam:EnableMFADevice",
                "iam:GetUser",
                "iam:ListMFADevices",
                "iam:ResyncMFADevice"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": "false"
                }
            }
        }
    ]
}
```

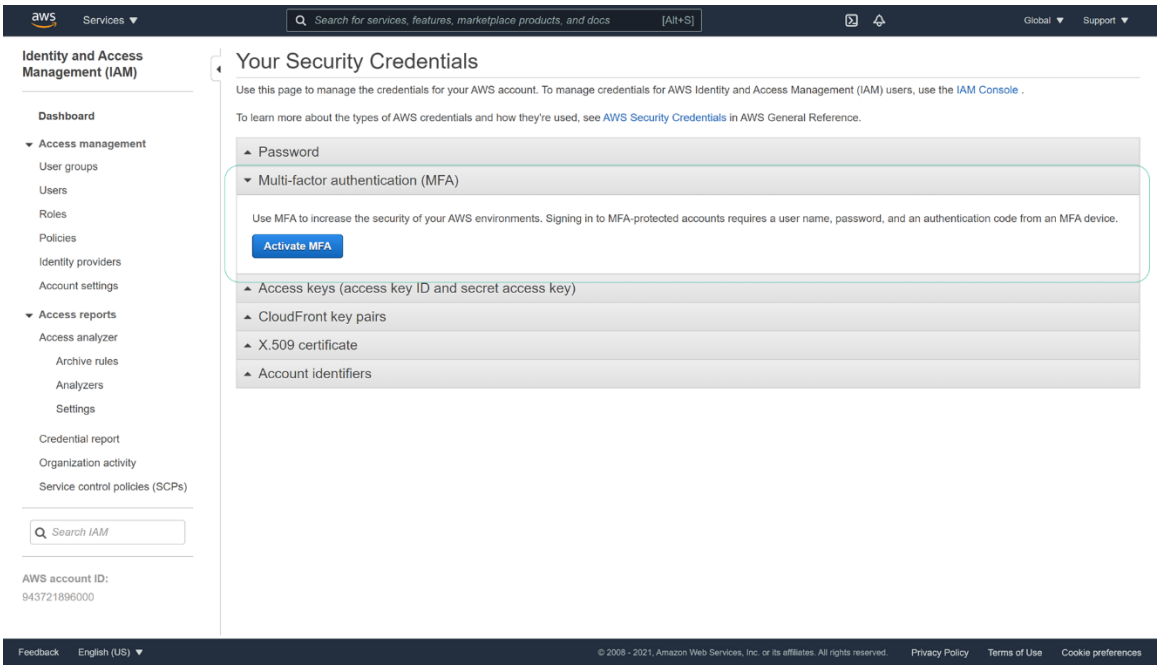
4. Chọn **Next: Tags**. Đây là màn hình về **Tags** một công cụ dùng để phân biệt các tài nguyên của AWS.
5. Chọn **Next: Review**. Đây là màn hình cho phép bạn review về bộ quyền mà bạn đang tạo ra.
6. Nhập tên bộ quyền (ví dụ: MFAHardDevice) và chọn **Create policy**.



7. Ở thanh bên trái , chọn **Dashboard** và sau đó chọn **Enable MFA**.



8. Mở rộng Multi-factor authentication (MFA) sau đó chọn **Active MFA**.



8. Trong **Manage MFA Device**, chọn **U2F security key** sau đó nhấn **Continue**.
9. Cắm khóa bảo mật U2F vào cổng USB của máy tính.

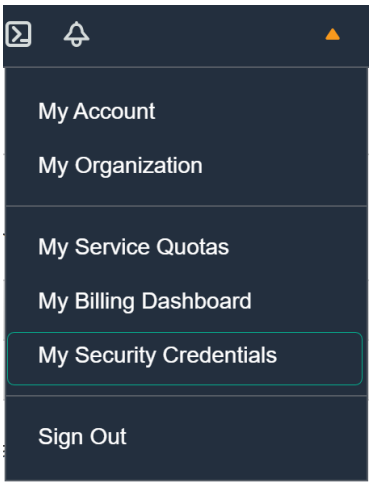
10. Nhấn vào khóa bảo mật U2F, và sau đó chọn **Close** khi U2F thiết lập thành công.

THIẾT BỊ MFA CỨNG

Nội dung

Kích hoạt thiết bị MFA phần cứng khác thông qua Console

1. Đăng nhập vào AWS Console.
2. Góc trên bên phải, bạn sẽ thấy tên account của bạn, chọn vào và chọn **My Security Credentials** sau đó mở rộng Multi-factor authentication (MFA).

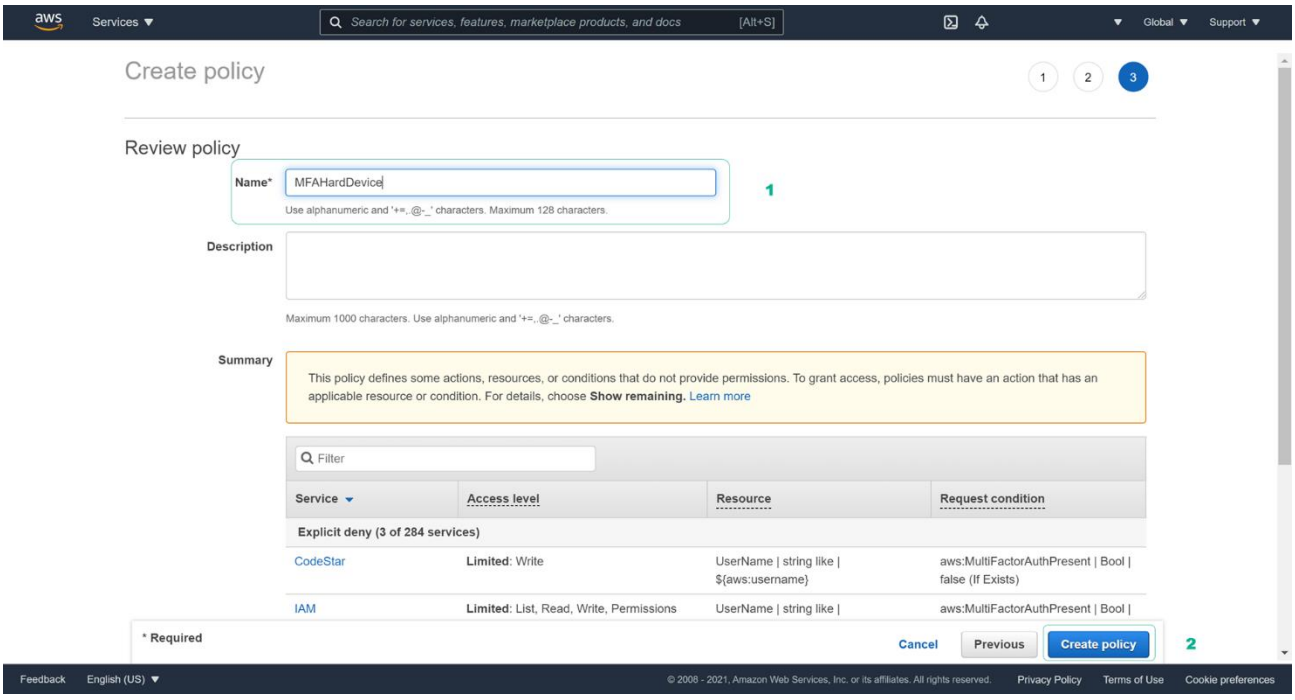


3. Để quản lí khóa bảo mật U2F, bạn phải có quyền từ bộ quyền sau. ở thanh bên trái, chọn **Policies** sau đó chọn **Create policy**, chọn **JSON** tab và dán phần bên dưới vào:

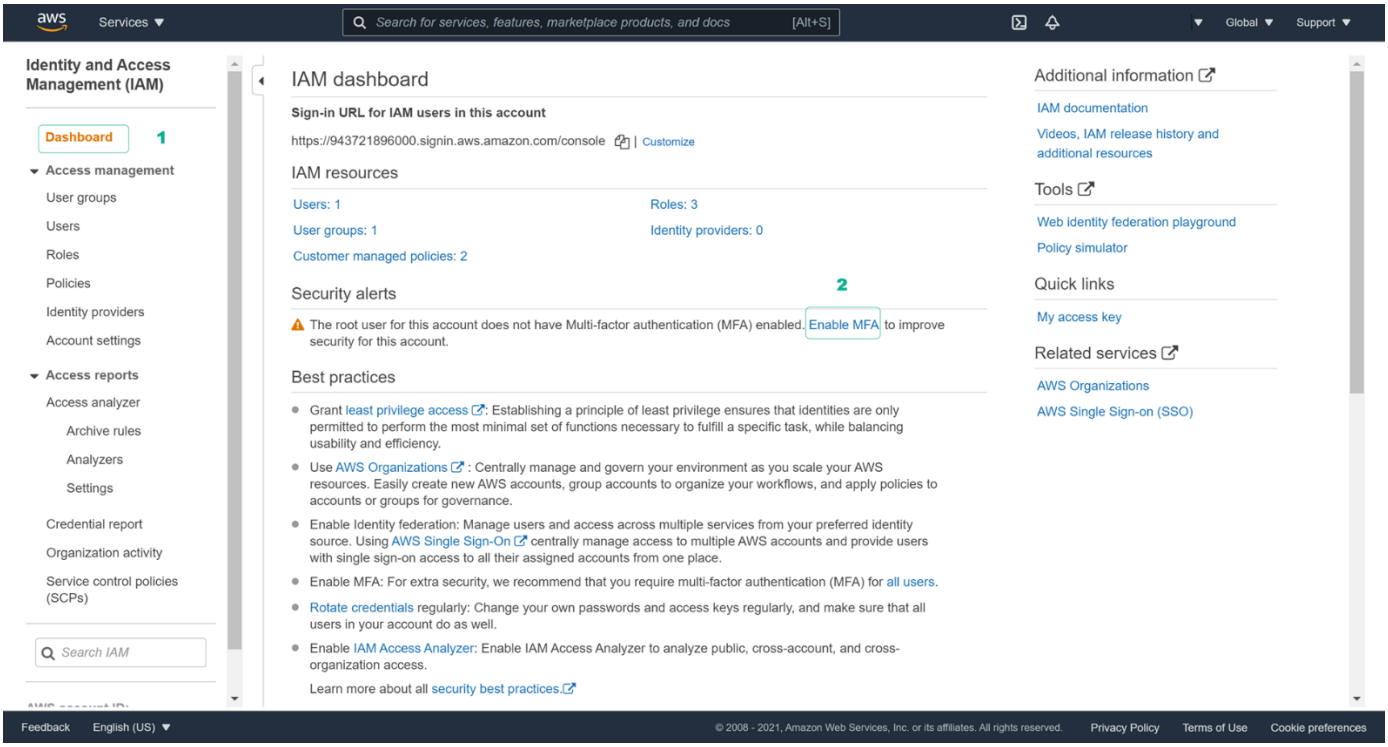
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowManageOwnUserMFA",
            "Effect": "Allow",
            "Action": [
                "iam:DeactivateMFADevice",
                "iam:EnableMFADevice",
                "iam:GetUser",
                "iam:ListMFADevices",
                "iam:ResyncMFADevice"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}"
        },
```

```
        {
            "Sid": "DenyAllExceptListedIfNoMFA",
            "Effect": "Deny",
            "NotAction": [
                "iam:EnableMFADevice",
                "iam:GetUser",
                "iam:ListMFADevices",
                "iam:ResyncMFADevice"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": "false"
                }
            }
        }
    ]
}
```

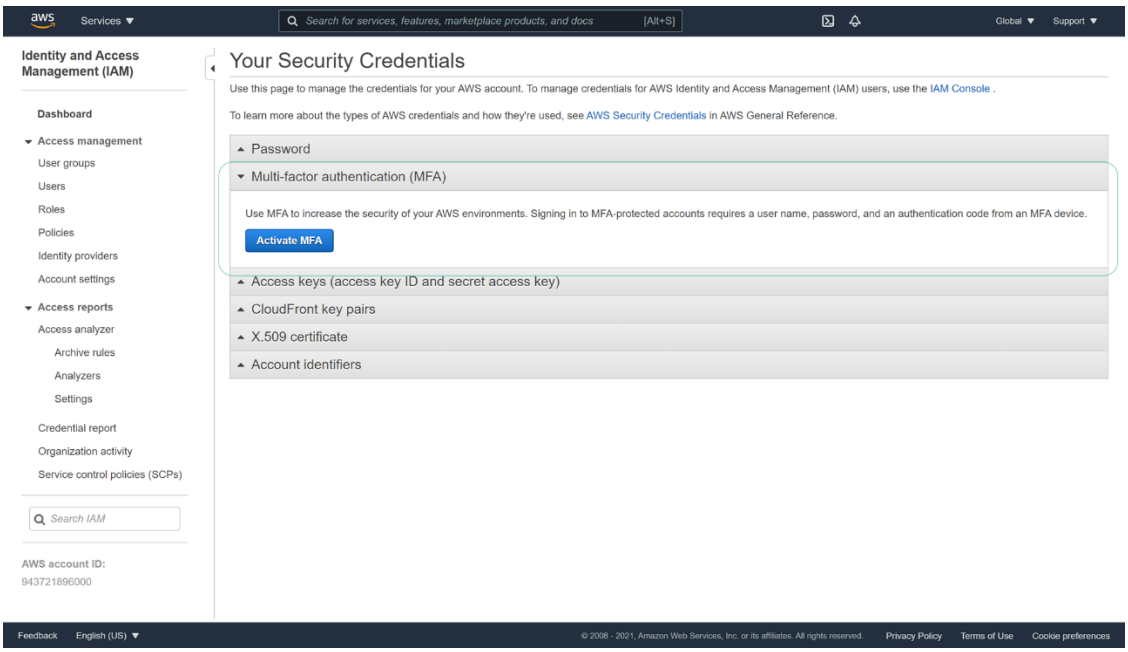
4. Chọn **Next: Tags**. Đây là màn hình về **Tags** một công cụ dùng để phân biệt các tài nguyên của AWS.
5. Chọn **Next: Review**. Đây là màn hình cho phép bạn review về bộ quyền mà bạn đang tạo ra.
6. Nhập tên bộ quyền (ví dụ: MFAHardDevice) và chọn **Create policy**.



7. Ở thanh bên trái , chọn **Dashboard** và sau đó chọn **Enable MFA**.



8. Mở rộng Multi-factor authentication (MFA) sau đó chọn **Active MFA**.



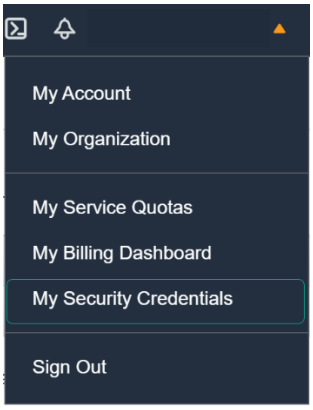
8. Trong **Manage MFA Device**, chọn **Other Hardware MFA Device** sau đó nhấn **Continue**.
9. Nhập **Serial Number** ở đằng sau thiết bị.

10. Nhập MFA code 1 sau đó đợi 30 giây và nhập MFA code 2.
11. Chọn **Assign MFA**.

TẠO ADMIN GROUP VÀ ADMIN USER

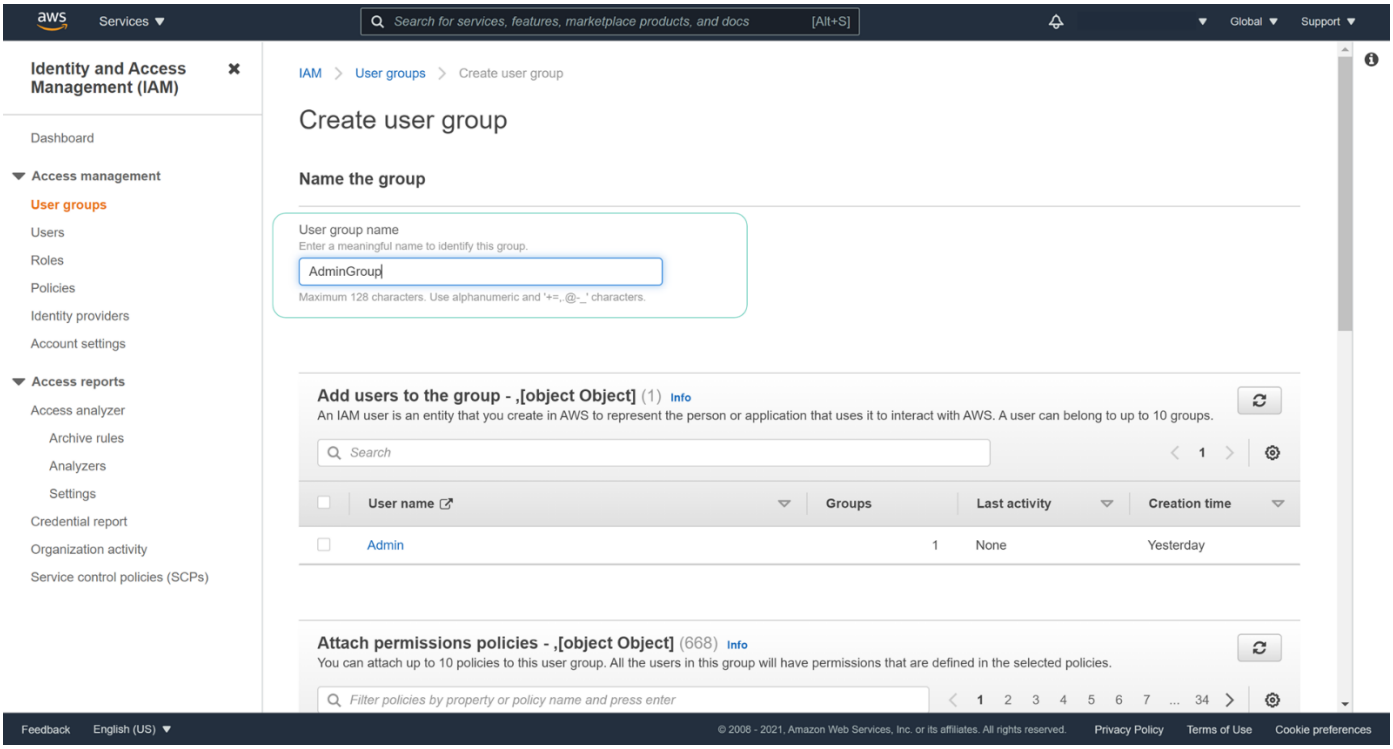
Tạo Admin Group

1. **Đăng nhập vào Bảng điều khiển** ở trang [AWS Web Service page]
2. Nhấn vào tên tài khoản ở góc trên bên phải và chọn **My Security Credentials**

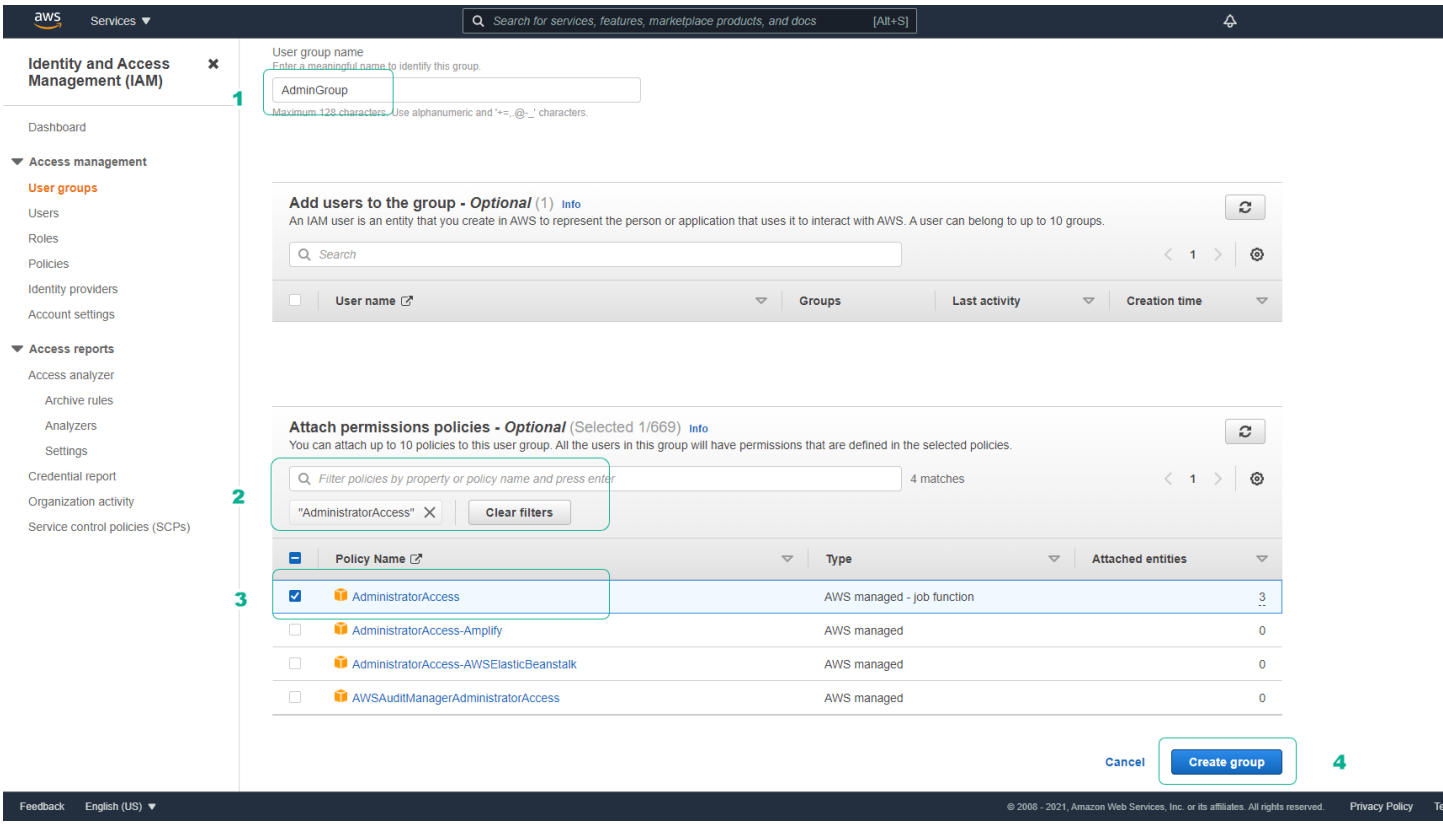


3. Ở thanh bên trái, chọn **User Groups** sau đó chọn **Create Group**

4. Dưới mục **Name the group**, nhập tên Group (Ví dụ: *AdminGroup*) và cuộn chuột xuống dưới



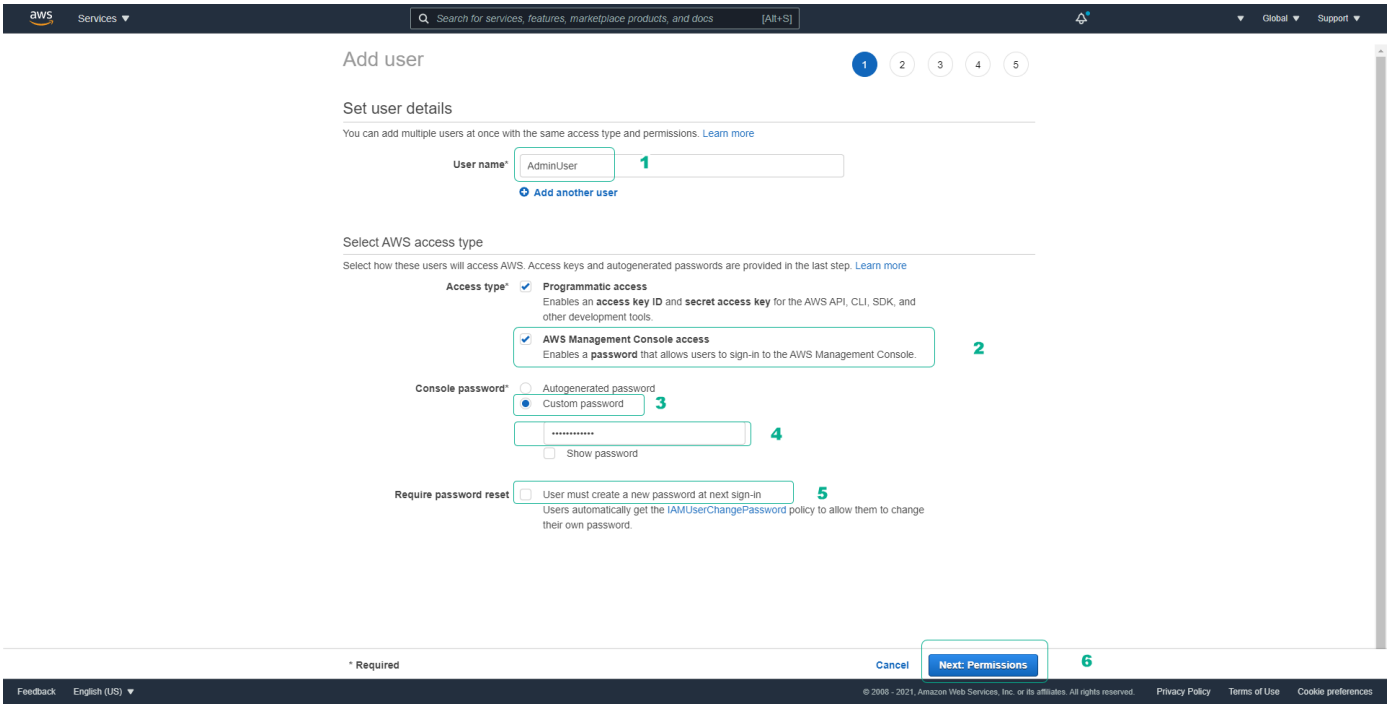
5. Ở phần **Attach permissions policies**, gõ **AdministratorAccess** vào thanh tìm kiếm và nhấn chọn nó. Cuối cùng, chọn **Create Group**.



Tạo Admin User

1. Ở thanh bên trái, chọn **Users** sau đó chọn **Add User**
2. Nhập tên User (Ví dụ: *AdminUser*).

- Click **AWS Management Console access**.
- Click **Programmatic Access**.
- Click **Custom password** rồi gõ một password tùy ý của bạn (lưu ý: bạn phải ghi nhớ mật khẩu này cho những lần đăng nhập trong tương lai).
- Bỏ chọn mục **User must create a new password…**.
- Click **Next:Permissions**.



Bằng cách chọn **AWS Management Console access**, bạn vừa cho phép IAM User được truy cập vào AWS thông qua bảng điều khiển AWS trên web.
Việc bỏ mục **User must create a new password…** cho phép người dùng khi lần đầu đăng nhập vào IAM User đó không cần phải tạo mật khẩu mới.

3. Click tab **Add user to group** và click **AdminGroup** mà chúng ta tạo trước đó.
4. Click **Next:Tags**
    - Tags (thẻ) là một tùy chọn không bắt buộc để tổ chức, theo dõi, hoặc điều khiển truy cập của user, thế nên bạn có thể thêm tags hoặc không.
5. Click **Next:Review**.
6. Kiểm tra thông tin chi tiết user sau đó chọn **Create User**.

Sau khi tạo user, bạn sẽ thấy hiện lên hộp thoại download thông tin access key và secret key. Đây là thông tin dùng để thực hiện **Programmatic access** tới các tài nguyên của AWS thông qua **AWS CLI** và **AWS SDK**. Tạm thời chúng ta sẽ chưa sử dụng tới.

HỖ TRỢ XÁC THỰC TÀI KHOẢN

Nội dung:

Trong quá trình khởi tạo tài khoản AWS, ở bước xác thực thông tin số điện thoại liên lạc, đôi khi sẽ xảy ra tình trạng không nhận được tin nhắn SMS hoặc cuộc gọi từ phía AWS. Trong trường hợp đó, hãy làm theo các bước sau để hoàn thành việc xác nhận thông tin tài khoản:

Kiểm tra các thông tin

Đầu tiên, hãy kiểm tra lại các thông tin tài khoản của bạn và đảm bảo chúng đã được nhập chính xác:

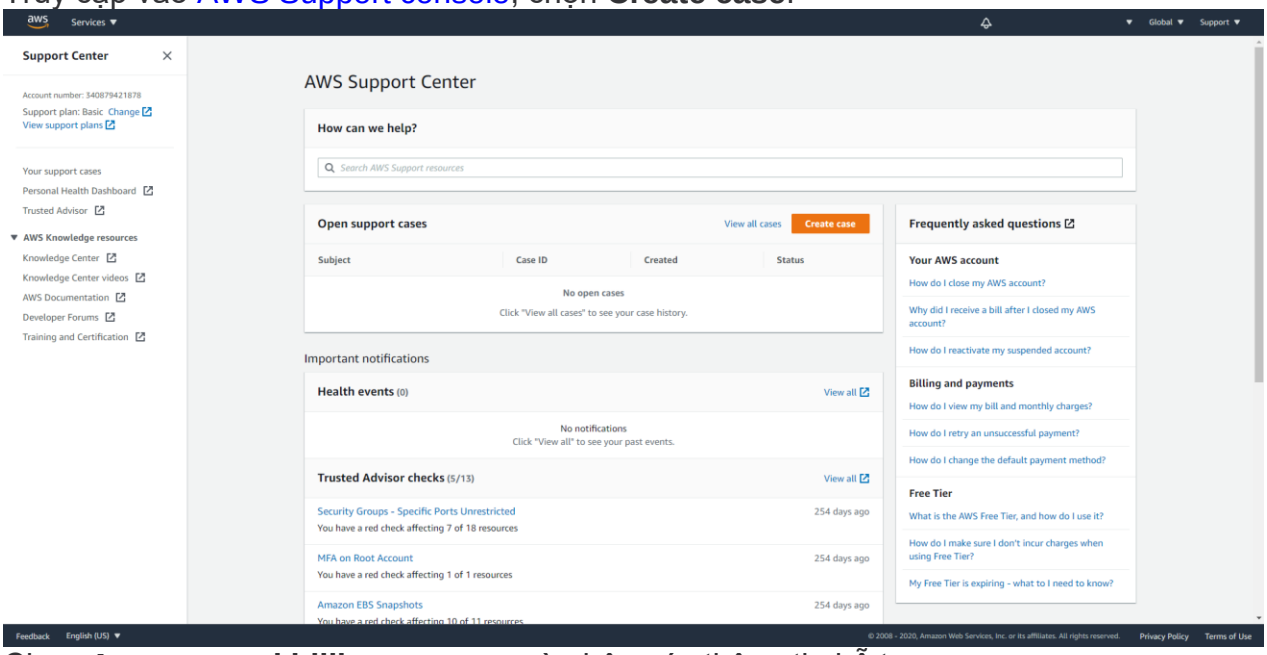
- Bạn đã nhập thông tin số điện thoại và chọn mã vùng quốc tế chính xác để nhận SMS hay cuộc gọi.
- Nếu bạn sử dụng điện thoại di động, kiểm tra điện thoại của bạn để chắc chắn bạn vẫn đang trong vòng phủ sóng để nhận SMS hay cuộc gọi.
- Thông tin về phương thức thanh toán đã được nhập chính xác.

> Hãy chắc chắn rằng số điện thoại mà bạn cung cấp trong tài khoản AWS của bạn có thể liên lạc được.

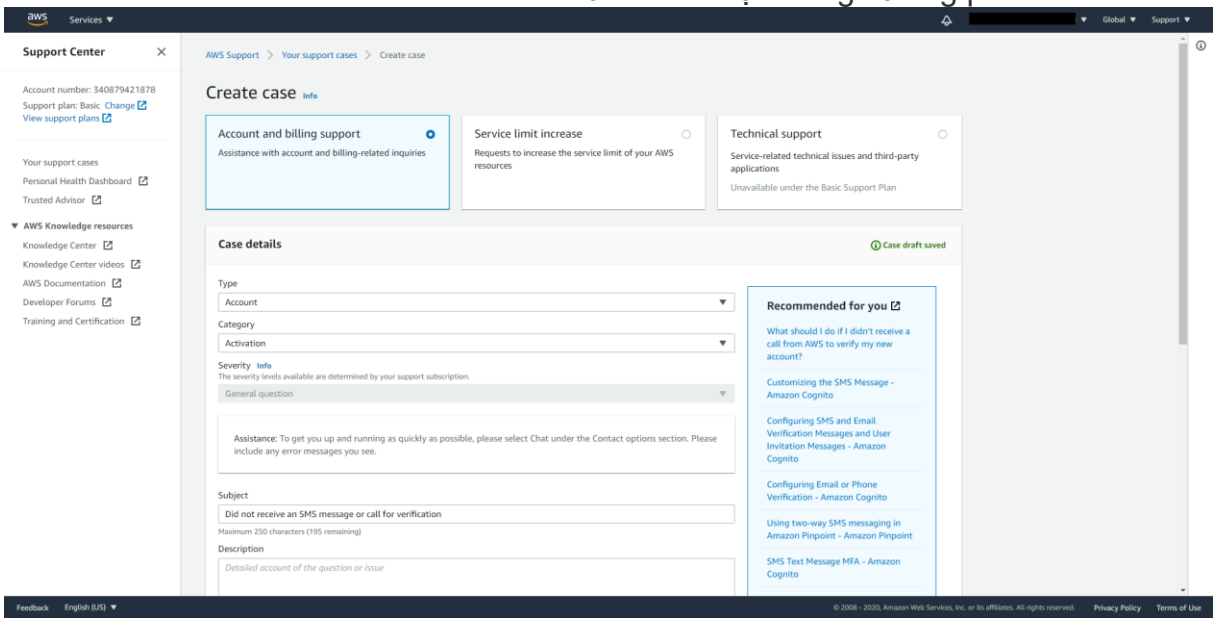
Tạo case hỗ trợ với AWS Support

Sau khi kiểm tra thông tin chính xác nhưng vẫn chưa nhận được tin nhắn SMS hoặc cuộc gọi xác thực, AWS Support sẽ hỗ trợ bạn kích hoạt tài khoản một cách thủ công.

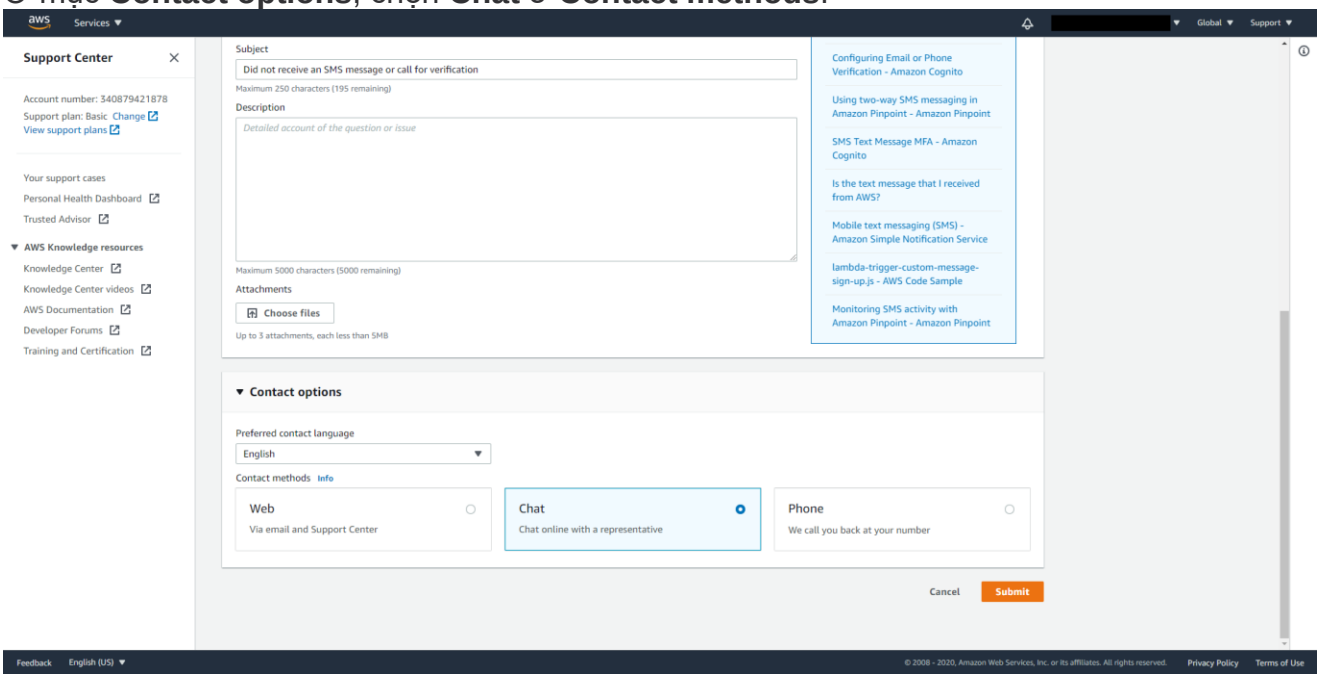
1. Truy cập vào AWS Support console, chọn **Create case**.



2. Chọn **Account and billing support** và nhập các thông tin hỗ trợ:
   - Type: chọn **Account**.
   - Category: chọn **Activation**.
   - Subject: viết ngắn gọn tình trạng gặp phải của bạn (VD: **Did not receive an SMS message or call for verification**)
   - Description: Cung cấp chi tiết tình trạng gặp phải và thông tin về thời gian bạn cần hỗ trợ kích hoạt tài khoản.
   - Attachments: Đính kèm hình ảnh mô tả bước xác thực đang vướng phải.



3. Ở mục **Contact options**, chọn **Chat** ở **Contact methods**.



4. Chọn **Submit**.
5. Đội ngũ AWS Support sẽ liên lạc và hỗ trợ kích hoạt tài khoản của bạn.

Bạn có thể tạo yêu cầu hỗ trợ với AWS Support ngay cả khi tài khoản của bạn chưa được kích hoạt.