Assuming AWS Role using AWS CLI (MFA Required)

Step 1 (IAM User Profile)

First our AWS Profile should be set to that of the IAM User.

We can use the following command to verify.

```
aws sts get-caller-identity
```

We will get the following Response.

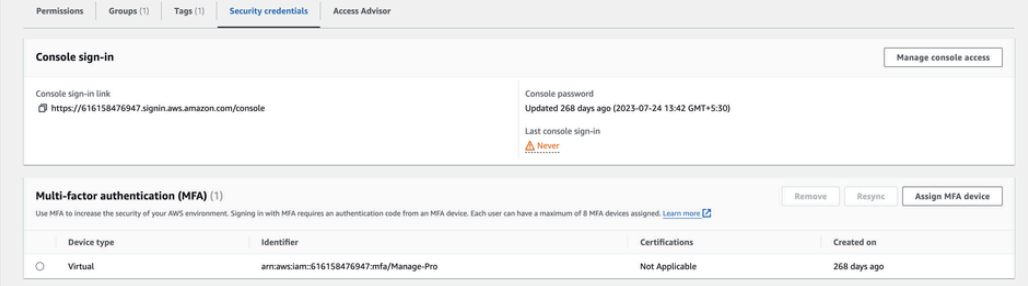
```
{
    "UserId": "XXXVPMMRNDSWXXXXXXX",
    "Account": "3766]4125XXXX",
    "Arn": "arn:aws:iam::3766412XXXXX:user/axxxx@alamy.com"
}
```

Step 2 (Retrieving MFA Serial)

We will have to retrieve the **MFA Serial** from the AWS Console.

AWS Console -> IAM -> Users -> Security Credentials

Now, we will see the following Screen.



Now, the value under Multi-Factor Authentication Table under Identifier is our MFA Serial Code.

Step 3 (Making Profile Ready In Config)

Now, we can open the **"config"** File of AWS and add the Profile like following.

```
[dev]
region = ap-south-1

[profile encodedev]
role_arn = arn:aws:iam::253921XXXXXX:role/encode
source_profile = alamy
mfa_serial = arn:aws:iam::376641XXXXXX:mfa/amxxx@alamy.com
region = eu-west-1

[alamy]
region = eu-west-1
```

Step 4 (Assuming Role In IAM User)

Now, we can assume the Role using the following command.

```
aws sts assume-role --role-arn "arn:aws:iam::2509213XXXXX:role/encode" --role-session-name AWSCLI-Session --token
```

Replace the **MFA Token** with the **6 Digit MFA Code** in your **Authenticator App**.

Session Name can be anything which suits us.

We should get a response like following.

```
{
    "Credentials": {
        "AccessKeyId": "ASIATU3ATYMYV6XXXXXX",
        "SecretAccessKey": "pIqW4KaXXXXXXJUeygVyuisDKNBZxqOlafXXXXXX",
        "SessionToken": "FwoGZXIvYXdzEKz//////////wEaDCLLzkCdd0xGYTcWNiKyAc/lt8kxPSNjLTX+6hNs2EF+jhhvI9PPnTwkFeL
        "Expiration": "2024-04-17T11:15:58+00:00"
    },
    "AssumedRoleUser": {
        "AssumedRoleId": "AROATU3ATYMY5V3XXXXXX:AWSCLI-Session",
        "Arn": "arn:aws:sts::250921XXXXXX:assumed-role/encode/AWSCLI-Session"
    }
}
```

Step 5 (Manually Creating Assumed Profile)

If we now run the following command.

```
awa sts get-caller-identity
```

It should ideally return us the Assumed Role but for some reason if it does not we can open the "config" File manually and then make the Assumed Profile like following.

```
[dev]
region = ap-south-1

[profile encodedev]
role_arn = arn:aws:iam::250921XXXXXX:role/encode
source_profile = alamy
mfa_serial = arn:aws:iam::376641XXXXXX:mfa/amaxx@alamy.com
region = eu-west-1

[profile encodedevassumed]
region = eu-west-1
aws_access_key_id = ASIATU3ATYMYX3XXXXXX
aws_secret_access_key = KS62Cz85XXXXXXcmu8xo7WAPmpWLT9DnelXXXXXX
aws_session_token = FwoGZXIvYXdzEKz//////////wEaDF0wRQTT2BSgSQWudiKyAcuo+4QYuWYMhLDUvbtu3fskK5ID9g5qvKGxKsXmQC01

[alamy]
region = eu-west-1
```

Access Key Id, **Secret Key** & **Token** we can manually add the one we generated in **Step 4**.

Then we can switch the "**AWS_PROFILE**" Environment Variable to the Profile which we just created.