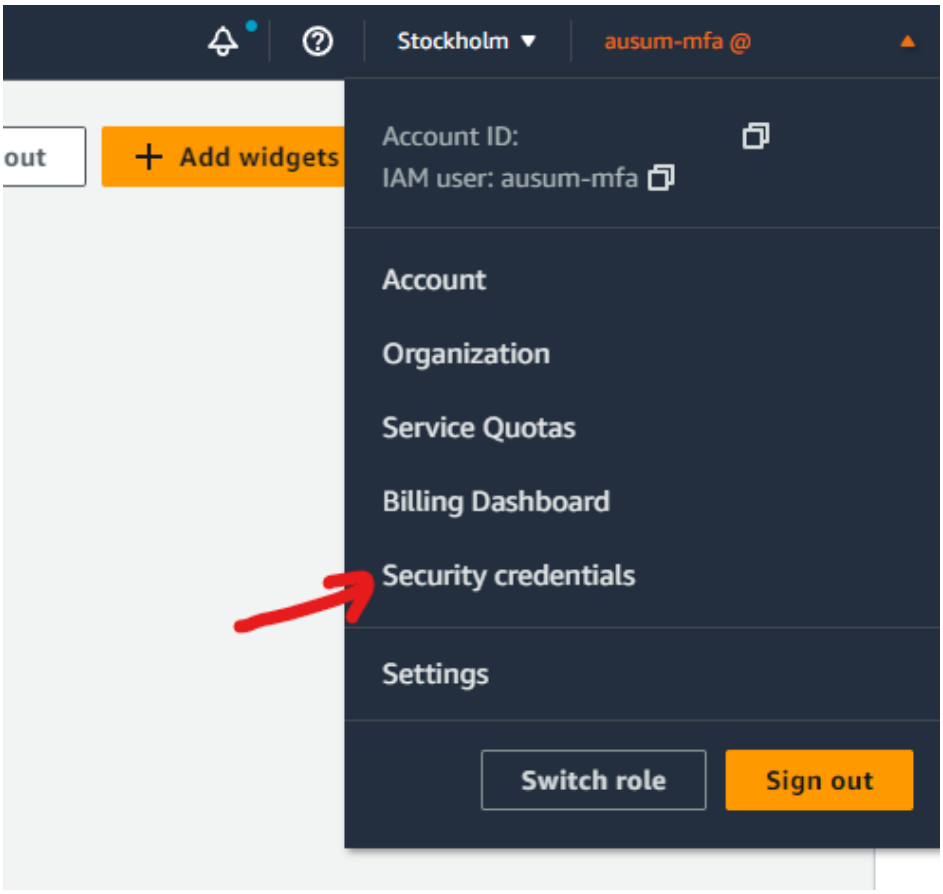
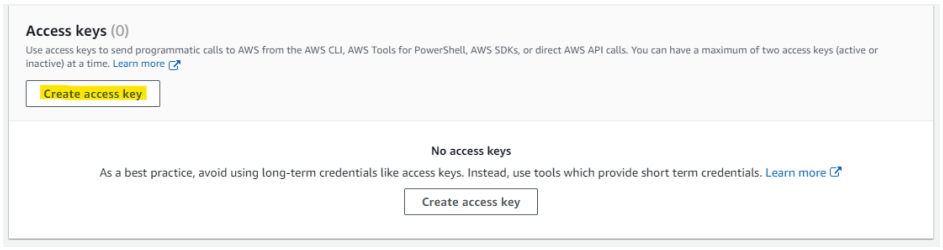
AWS CLI AND ACCESS KEYS USAGE

Create an Access Key

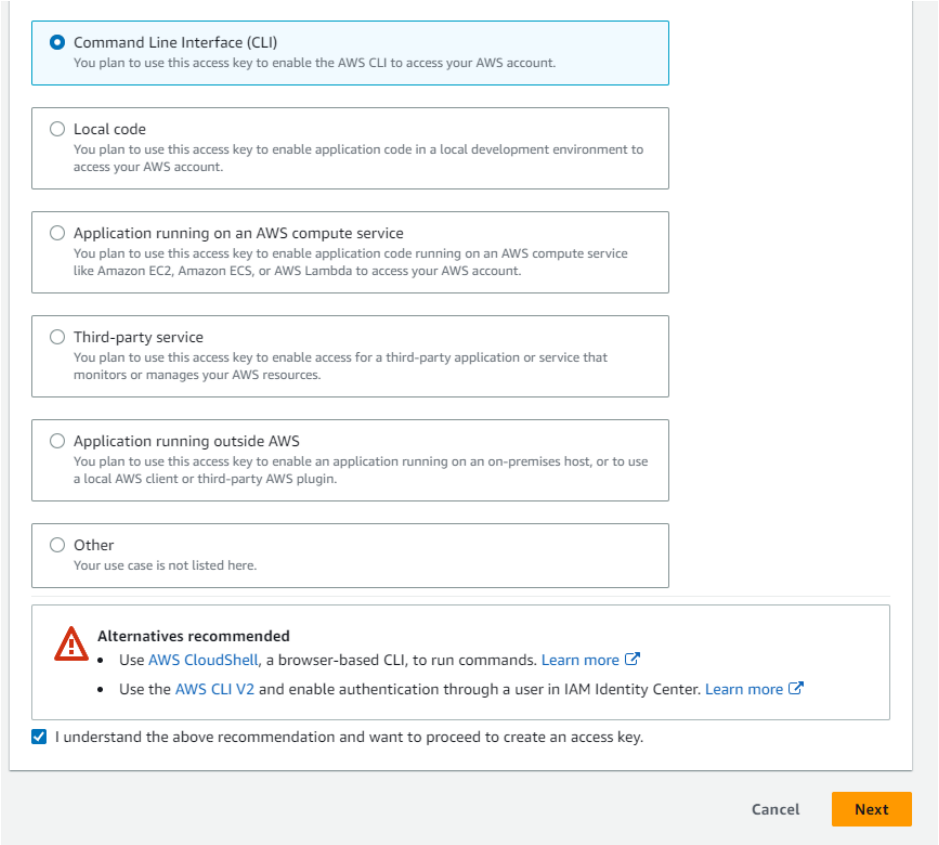
Go to your profile under security credentials:



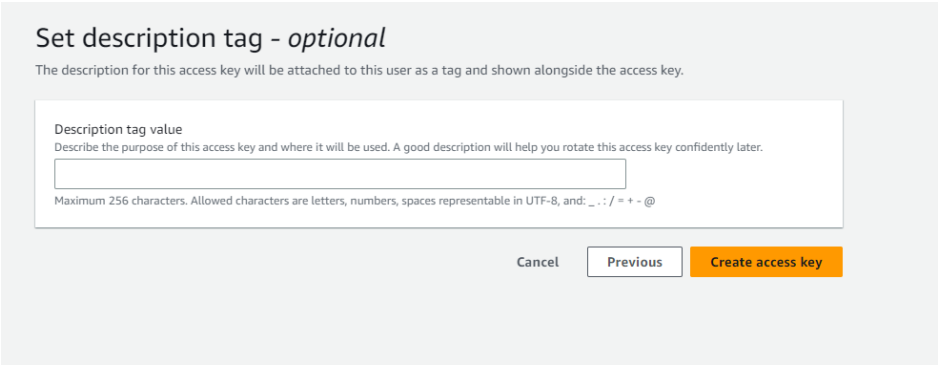
Presh Create Access key button under Access keys section:



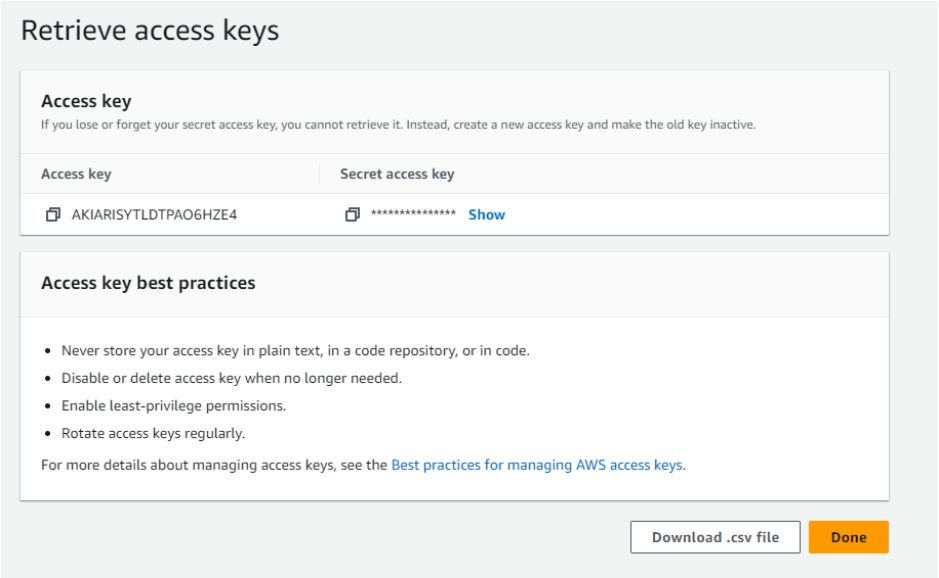
Select Command Line Interface (CLI), accept recommendations and continue.



Create access key



At next window we will get our key id and password. Copy and save this as we are going to use it before.



Instal AWS Cli

Just follow steps for your system:

https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html

Configue AWS Cli with your credentials

Add your access key to credentials file (located at C:\users\username\.aws\credentials or ~/.aws/credentials).

[default]

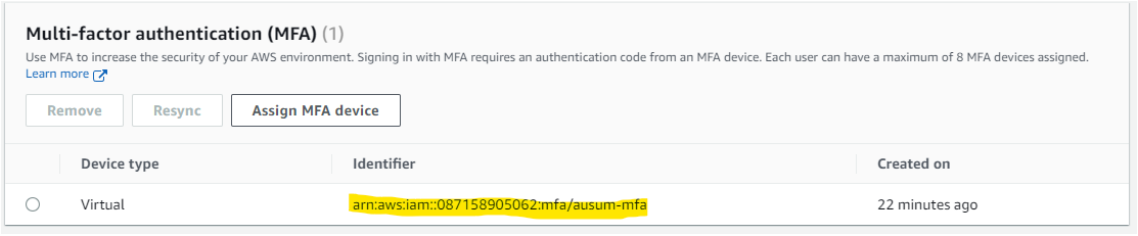
aws_access_key_id=AKIAIOSFODNN7EXAMPLE

aws_secret_access_key=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

Once added content to file execute following command to get temp MFA credentials and token:

aws sts get-session-token --serial-number arn-of-the-mfa-device --token-code code-from-token --duration-seconds 129600

arn-of-the-mfa-device can be retrieved at your profile Security Credentials:



code-from-token it's your MFA app active token/number.

Once executed you will receive respone like:

```
PS C:\Users\hecto> aws sts get-session-token --serial-number arn:aws:iam::087158905062:mfa/ausum-mfa --token-code 257885
 --duration-seconds 129600
{
    "Credentials": {
        "AccessKeyId": "ASIARISYTLDTPSONWN5U",
        "SecretAccessKey": "YczXX0tz7Q8CQPvVUG/axTDGnNdhrNFXYn4kZrBK",
        "SessionToken": "IQoJb3JpZ2luX2VjEFkaCmV1LXNvdXRoLTEiRzBFAiAoUKNWVdnyV6A+TGRWswRA01yE6av5u3ZLA7LaL2EsXwIhAKCpO8e
EI4Yj7Q+mkY5M8ET8rz6eYCo3WJtefbRYTDQ2Ku8BCDIQABoMMDg3MTU4OTA1MDYyIgxzZ8zDoi68+G4eDmwqzAFf215w6uZjqZ/g8wV8QfOWSMa+Tq6bUOE
lfEZE08Dco4CEteNsWU+OZmY54seSBYUMJv6u3miMZ1BOP9dKwp3Na9cTLmLRZeUvtL7wfbnM/s4NPM1jX9LA1lztl1XLJG0hIo+UMnE9YHT0fBN4/+9rh+S
MyZYEVdW7A4X27KFII87PU557iCc7eo+DkmogVfQxAdsybXfIPe8uTfkmOWWP2JRM63ijtr5Q8WiRZI/D6TdqQWMHJwbqemrrO75sxbcCS7oX3MUS3yqEChA
w75KHoQY6mAFcoGuQ1s/NGfa/jWg9n71zAhSbuBH5WAPCeZQXBGBvZP+7rK7V/Wyz46tn116JH1+mVnou74tdPCLv/qq471QZE/gkcFYb4BVgWYUwPmYlnvn
N5A+qTvZa1nq9bpJ4UK1Z0xbY9foXVeQMHsXZvagCwwdVYDOLgolND8Uyiu3chlOFV8iIJlQr3G/Gry38HIQWWlCAqMdSQg==",
        "Expiration": "2023-03-29T04:50:55+00:00"
    }
}

PS C:\Users\hecto>
```

Create new profile at your credentials file with obtained data (C:\users\username\.aws\credentials or ~/.aws/credentials)

[default]

aws_access_key_id=XXXXXXXXXXXXXXXXXXX

aws_secret_access_key=XXXXXXXXXXXXXXXXXXXXXX

[mfa]

aws_access_key_id = ASIARISYTLDTPSONWN5U

aws_secret_access_key = YczXX0tz7Q8CQPvVUG/axTDGnNdhrNFXYn4kZrBK

aws_session_token =
IQoJb3JpZ2luX2VjEFkaCmV1LXNvdXRoLTEiRzBFAiAoUKNWVdnyV6A+TGRWswRA01yE6av5u3ZL
A7LaL2EsXwIhAKCpO8eEI4Yj7Q+mkY5M8ET8rz6eYCo3WJtefbRYTDQ2Ku8BCDIQABoMMDg3M
TU4OTA1MDYyIgxzZ8zDoi68+G4eDmwqzAFf215w6uZjqZ/g8wV8QfOWSMa+Tq6bUOElfEZE08D
co4CEteNsWU+OZmY54seSBYUMJv6u3miMZ1BOP9dKwp3Na9cTLmLRZeUvtL7wfbnM/s4NPM1
jX9LA1lztl1XLJG0hIo+UMnE9YHT0fBN4/+9rh+SMyZYEVdW7A4X27KFII87PU557iCc7eo+DkmogV
fQxAdsybXfIPe8uTfkmOWWP2JRM63ijtr5Q8WiRZI/D6TdqQWMHJwbqemrrO75sxbcCS7oX3MU
S3yqEChAw75KHoQY6mAFcoGuQ1s/NGfa/jWg9n71zAhSbuBH5WAPCeZQXBGBvZP+7rK7V/Wyz
46tn116JH1+mVnou74tdPCLv/qq471QZE/gkcFYb4BVgWYUwPmYlnvnN5A+qTvZa1nq9bpJ4UK1
Z0xbY9foXVeQMHsXZvagCwwdVYDOLgolND8Uyiu3chlOFV8iIJlQr3G/Gry38HIQWWlCAqMdSQg
==

Once don we could execute commands with –profile mfa parameter and get Access to resources:

```
PS C:\Users\hecto> aws sts get-caller-identity --profile mfa
{
    "UserId": "AIDARISYTLDTKGMKAGOB2",
    "Account": "
    "Arn": "arn:aws:iam:           ;2:user/ausum-mfa"
}
```

MFA credentials will be active for 36 hours (--duration-seconds 129600).

Assume Playlogiq DEV/STA role to access dev and staging account

You will have to add config profile with role config to Access dev and staging account and resources. Edit config file (C:\users\username\.aws\credentials or ~/.aws/credentials) and add as follows:

[default]

region = eu-south-1

[profile mfa]

region = eu-south-1

[profile playlogiqdev]

region = eu-south-1

role_arn = arn:aws:iam::129323733169:role/playlogiq

source_profile = mfa

To execute commands using this profile and Access to dev/staging resources you Will need to add –profile playlogiqdev:

```
PS C:\Users\hecto> aws sts get-caller-identity --profile assumed-role
{
    "UserId": "AROAR4HCLSCYTAPSPOL5O:botocore-session-1679936566",
    "Account": "129
    "Arn": "arn:aws:sts::129       ;9:assumed-role/playlogiq/botocore-session-1679936566"
}
```

Retrieve logs using aws-cli (example)

If you need to get all logs for last day you will have to run command following commands:

Betmaker – PRO

aws logs tail betmaker --since 1d > betmaker_pro.log

Betmaker – Staging

aws logs tail betmaker-sta --since 1d --profile playlogiqdev > betmaker_sta.log

Betmaker – Dev

aws logs tail betmaker-dev --since 1d --profile playlogiqdev > betmaker_dev.log

Backoffice – PRO

aws logs tail backoffice --since 1d > backoffice_pro.log

Backoffice – Staging

aws logs tail backoffice-sta --since 1d --profile playlogiqdev > backoffice_sta.log

Backoffice – Dev

aws logs tail backoffice-dev --since 1d --profile playlogiqdev > backoffice_dev.log

This are example command you can use filters or other commands to get logs just check AWS doc if you need more data:

https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/SearchDataFilterPattern.html