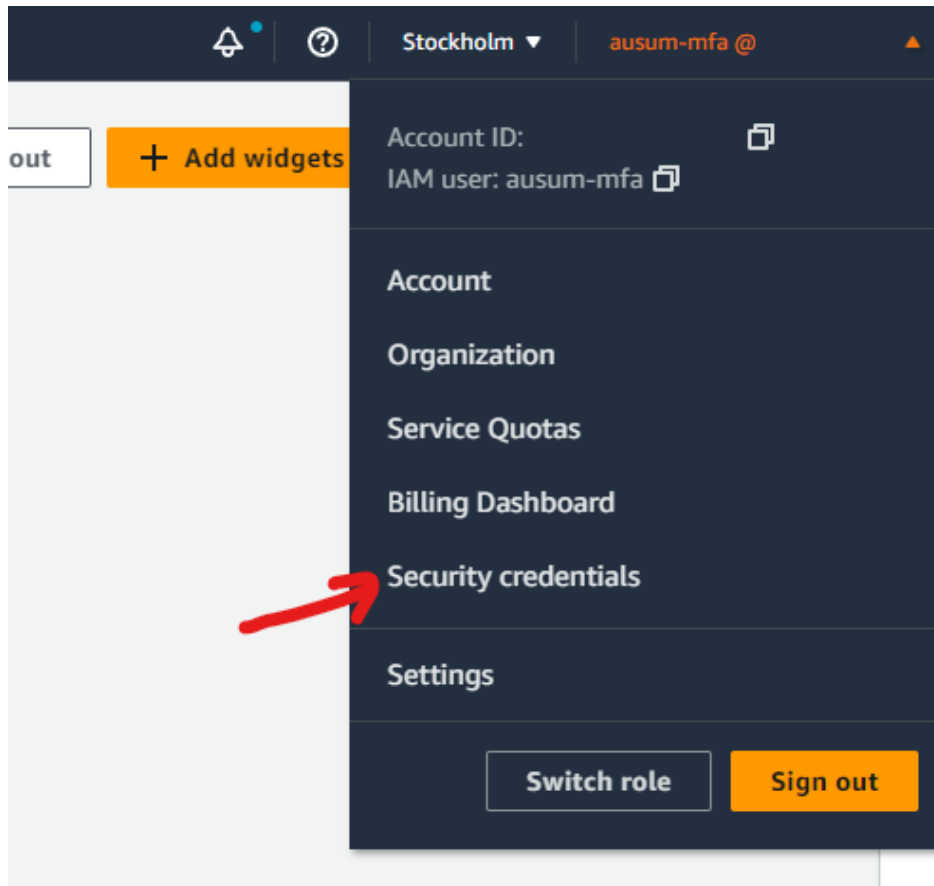


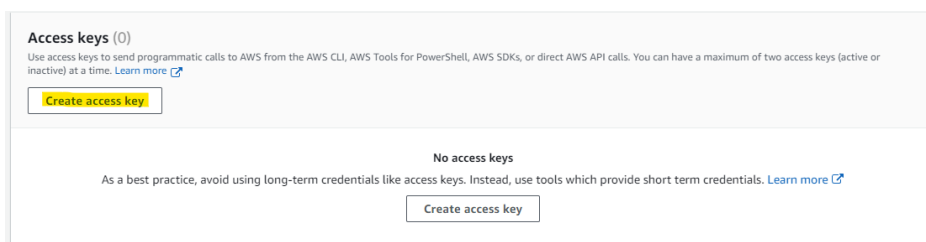
AWS CLI AND ACCESS KEYS USAGE

Create an Access Key

Go to your profile under security credentials:



Press Create Access key button under Access keys section:



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

☒ **Command Line Interface (CLI)**
 You plan to use this access key to enable the AWS CLI to access your AWS account.


☐ **Local code**
 You plan to use this access key to enable application code in a local development environment to access your AWS account.

☐ **Application running on an AWS compute service**
 You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

☐ **Third-party service**
 You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

☐ **Application running outside AWS**
 You plan to use this access key to enable an application running on an on-premises host, or to use a local AWS client or third-party AWS plugin.

☐ **Other**
 Your use case is not listed here.

 **Alternatives recommended**

- Use [AWS CloudShell](#), a browser-based CLI, to run commands. [Learn more](#)
- Use the [AWS CLI V2](#) and enable authentication through a user in IAM Identity Center. [Learn more](#)

☒ I understand the above recommendation and want to proceed to create an access key.

Cancel **Next**

Create access key

Set description tag - *optional*

The description for this access key will be attached to this user as a tag and shown alongside the access key.

Description tag value

Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidently later.

Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: _ . : / = + - @



Cancel **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.

Retrieve access keys

Access key

If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key	Secret access key
 AKIARISYTLDTPAO6HZE4	 ***** Show

Access key best practices

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the [Best practices for managing AWS access keys](#).

Download .csv file

Done

Instal AWS Cli

Just follow steps for your system:

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

Configure AWS Cli with your credentials

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

[default]

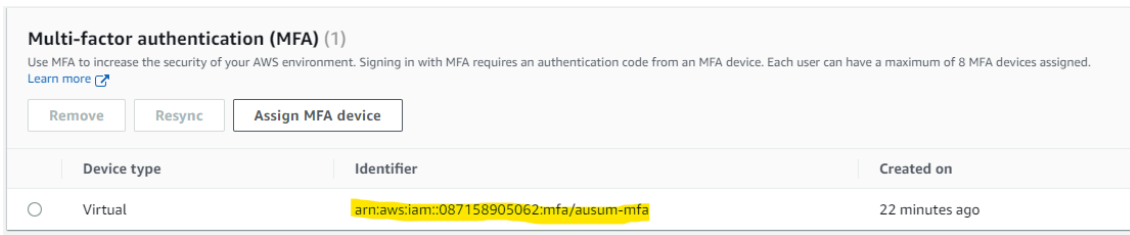
aws_access_key_id=AKIAIOSFODNN7EXAMPLE

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 response 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": "ASIARISYTLTPSONWN5U",
    "SecretAccessKey": "YczXX0tz7Q8CQPvVUG/axTDGnNdhrNFXyn4kZrBK",
    "SessionToken": "IQoJb3JpZ2luX2VjEFkaCmV1LXNvdXRoLTEiRzBFaIAoUKNWVdnyV6A+TGRWswRA01yE6av5u3ZLA7LaL2EsXwIhAKCpO8eEI4Yj7Q+mkY5M8ET8rz6eYCo3WJtefbRYTDQ2Ku8BCDIQABoMMDg3MTU4OTA1MDYyIgxzZ8zDoi68+G4eDmwqzAFf215w6uZjqZ/g8wV8QfOWSMa+Tq6bUOEIfEZE08Dco4CEteNsWU+OZmY54seSBYUMJv6u3miMZ1BOP9dKwp3Na9cTlMLRZeUvtL7wfbnM/s4NPM1jX9LA1lzt1XLJG0hlo+UMnE9YHTOfBN4/+9rh+SMYzYEVdW7A4X27KFII87PU557iCc7eo+DkmogVfQxAdsYbXfIPe8uTfkmOWWP2JRM63ijtr5Q8WiRZl/D6TdQqQWMHJwbqemrrO75sxbCS7oX3MUS3yqEChAw75KHoQY6mAFcoGuQ1s/NGfa/jWg9n71zAhSbuBH5WAPCeZQXBGbvZP+7rK7V/Wyz46tn116JH1+mVnou74tdPCLv/q471QZE/gkCFYb4BVgWYUwPmYlnvnN5A+qTvZa1nq9bpj4UK1Z0xbY9foXVeQMHSXZvagCwwdVYDOLgolND8Uyiu3chIOFV8iJlQr3G/Gry38HIQWWICAqMdSQg==",
    "Expiration": "2023-03-29T04:50:55+00:00"
  }
}
```

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

[default]

aws_access_key_id=XXXXXXXXXXXXXXXXXXXX

aws_secret_access_key=XXXXXXXXXXXXXXXXXXXX

[mfa]

aws_access_key_id = ASIARISYTLTPSONWN5U

aws_secret_access_key = YczXX0tz7Q8CQPvVUG/axTDGnNdhrNFXyn4kZrBK

aws_session_token =

IQoJb3JpZ2luX2VjEFkaCmV1LXNvdXRoLTEiRzBFaIAoUKNWVdnyV6A+TGRWswRA01yE6av5u3ZLA7LaL2EsXwIhAKCpO8eEI4Yj7Q+mkY5M8ET8rz6eYCo3WJtefbRYTDQ2Ku8BCDIQABoMMDg3MTU4OTA1MDYyIgxzZ8zDoi68+G4eDmwqzAFf215w6uZjqZ/g8wV8QfOWSMa+Tq6bUOEIfEZE08Dco4CEteNsWU+OZmY54seSBYUMJv6u3miMZ1BOP9dKwp3Na9cTlMLRZeUvtL7wfbnM/s4NPM1jX9LA1lzt1XLJG0hlo+UMnE9YHTOfBN4/+9rh+SMYzYEVdW7A4X27KFII87PU557iCc7eo+DkmogVfQxAdsYbXfIPe8uTfkmOWWP2JRM63ijtr5Q8WiRZl/D6TdQqQWMHJwbqemrrO75sxbCS7oX3MUS3yqEChAw75KHoQY6mAFcoGuQ1s/NGfa/jWg9n71zAhSbuBH5WAPCeZQXBGbvZP+7rK7V/Wyz46tn116JH1+mVnou74tdPCLv/q471QZE/gkCFYb4BVgWYUwPmYlnvnN5A+qTvZa1nq9bpj4UK1Z0xbY9foXVeQMHSXZvagCwwdVYDOLgolND8Uyiu3chIOFV8iJlQr3G/Gry38HIQWWICAqMdSQg==

Once done 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": "AIDARISYTLDTKGMBKAGOB2",
  "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": "AROAR4HCLSCYTAPOL50: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>