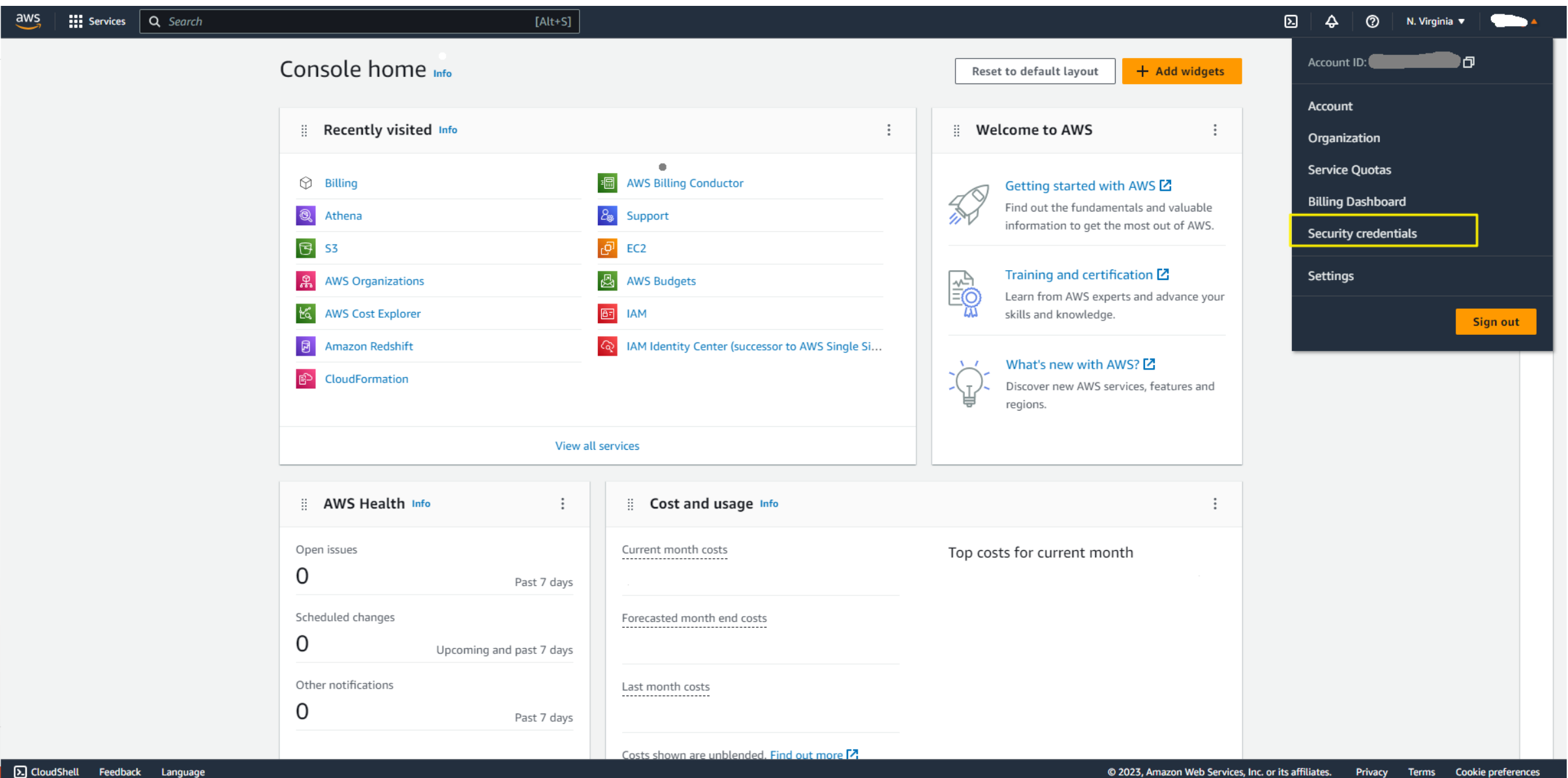


Multi-Factor Authentication(MFA)

1. AWS Management Console 접속 > 우상단 계정 이름(Alias) 클릭 > Security Credential 접속



2. My Security Credentials > Multi-factor authentication (MFA)의 [Assign MFA device] 클릭

aws

Services

Search

[Alt+S]

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
 - Archive rules
 - Analyzers
 - Settings
- Credential report
- Organization activity

IAM > Security credentials

My security credentials

Root user

Info

The root user has access to all AWS resources in this account, and we recommend following [best practices](#). To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference

Account details

Edit account name, email, and password

Account name

Email address

AWS account ID

Canonical user ID

Multi-factor authentication (MFA) (1)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

Remove

Resync

Assign MFA device

| Device type | Identifier | Certifications | Created on |
|-------------|------------|----------------|------------|
| | | | |

3. OTP 어플리케이션 다운로드 > Device Name 입력 > Authenticator app 클릭 > Next 클릭

IAM > Security credentials > Assign MFA device

Step 1
Select MFA device

Step 2
Set up device

Select MFA device [Info](#)

MFA device name

Device name

Enter a meaningful name to identify this device.


Device name

Maximum 128 characters. Use alphanumeric and '+ = , . @ - _ ' characters.

MFA device

Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.


☒



Authenticator app

Authenticate using a code generated by an app installed on your mobile device or computer.


☐



Security Key

Authenticate using a code generated by touching a YubiKey or other supported FIDO security key.

☐



Hardware TOTP token

Authenticate using a code displayed on a hardware Time-based one-time password (TOTP) token.

Cancel

Next

4. Show QR code 클릭 > QR 이미지 출력시 인증 앱으로 QR 스캔
> 연속으로 출력되는 6자리 code를 순차적으로 입력 > Add MFA 클릭

IAM > Security credentials > Assign MFA device

Step 1
[Select MFA device](#)

Step 2
Set up device

Set up device [Info](#)

Authenticator app

A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

1

Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.
[See a list of compatible applications](#)

2

Show QR code

Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code.
Alternatively, you can type a secret key. [Show secret key](#)

3

Fill in two consecutive codes from your MFA device.

MFA code 1

MFA code 2

Cancel

Previous

Add MFA

감사합니다.