

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

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

Access reports

- Access Analyzer
- External access
- Unused access
- Analyzer settings
- Credential report
- Organization activity
- Service control policies

IAM Identity Center

AWS Organizations

MFA device assigned

You can register up to 8 MFA devices of any combination of the currently supported MFA types with your AWS account root and IAM user. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the AWS CLI with that user.

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

MKohronas

Email address

mkohronas@student.fullsail.edu

AWS account ID

851725234981

Canonical user ID

043b547f5d4c0580a3f08457c2811a7372d8b40fc2ac18e55b50b8379bf26149

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](#)

Type

Identifier

Certifications

Created on

☐

Virtual

arn:aws:iam::851725234981:mfa/Authy

Not Applicable

Mon Jul 15 2024

Access keys (0)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

Create access key

Access key ID

Created on

Access key last used

Region last used

Service last used

Status

No access keys

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

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

Access reports

- Access Analyzer
- External access
- Unused access
- Analyzer settings
- Credential report
- Organization activity
- Service control policies

Related consoles

IAM Identity Center

AWS Organizations

STS for Canada (Central) region is deactivated.

Region name	Endpoint	STS status
Global Endpoint	https://sts.amazonaws.com	Always active
US East (N. Virginia)	https://sts.us-east-1.amazonaws.com	Always active
Asia Pacific (Tokyo)	https://sts.ap-northeast-1.amazonaws.com	Inactive
Asia Pacific (Seoul)	https://sts.ap-northeast-2.amazonaws.com	Inactive
Asia Pacific (Osaka)	https://sts.ap-northeast-3.amazonaws.com	Inactive
Asia Pacific (Mumbai)	https://sts.ap-south-1.amazonaws.com	Inactive
Asia Pacific (Singapore)	https://sts.ap-southeast-1.amazonaws.com	Inactive
Asia Pacific (Sydney)	https://sts.ap-southeast-2.amazonaws.com	Inactive
Canada (Central)	https://sts.ca-central-1.amazonaws.com	Inactive
Europe (Frankfurt)	https://sts.eu-central-1.amazonaws.com	Inactive
Europe (Stockholm)	https://sts.eu-north-1.amazonaws.com	Inactive
Europe (Ireland)	https://sts.eu-west-1.amazonaws.com	Inactive
Europe (London)	https://sts.eu-west-2.amazonaws.com	Inactive
Europe (Paris)	https://sts.eu-west-3.amazonaws.com	Inactive
South America (São Paulo)	https://sts.sa-east-1.amazonaws.com	Inactive
US East (Ohio)	https://sts.us-east-2.amazonaws.com	Active
US West (N. California)	https://sts.us-west-1.amazonaws.com	Active
US West (Oregon)	https://sts.us-west-2.amazonaws.com	Active

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

