

AWS services

Find a service by name or feature (for example, EC2, S3 or VM, storage).

Recently visited services

IAM Cost Explorer Billing

DynamoDB

All services

fem-dryrun N. Virginia Support

AWS services

Find a service by name or feature (for example, EC2, S3 or VM, storage).

Recently visited services



IAM



Cost Explorer



Billing



DynamoDB

All services

Build a solution

Get started with simple wizards and automated workflows.



Launch a virtual machine

With EC2

~2-3 minutes



Build a web app

With Elastic Beanstalk

~6 minutes



Build using virtual servers

With Lightsail

~1-2 minutes



Connect an IoT device

With AWS IoT

~5 minutes



Start a development project

With CodeStar

~5 minutes



Register a domain

With Route 53

~3 minutes

See more

Helpful tips



Manage your costs

Monitor your AWS costs, usage, and reservations using AWS Budgets. [Start now](#)



Create an organization

Use AWS Organizations for policy-based management of multiple AWS accounts.

[Start now](#)

Explore AWS

Machine Learning with Amazon SageMaker

The fastest way to build, train, and deploy machine learning models. [Learn more](#).

Amazon Relational Database Service (RDS)

RDS manages and scales your database for you. RDS supports Aurora, MySQL, PostgreSQL, MariaDB, Oracle, and SQL Server. [Learn more](#).

AWS Fargate Runs Containers for You

console.aws.amazon.com/iam/home?region=us-east-1#/home

aws Services Resource Groups

fem-dryrun Global Support

Search IAM

Dashboard

- Groups
- Users
- Roles
- Policies
- Identity providers
- Account settings
- Credential report

Encryption keys

Welcome to Identity and Access Management

IAM users sign-in link:
<https://613943640677.signin.aws.amazon.com/console>

IAM Resources

Users: 0	Roles: 2
Groups: 0	Identity Providers: 0
Customer Managed Policies: 0	

Security Status 1 out of 5 complete.

- Delete your root access keys
- ⚠ Activate MFA on your root account
- ⚠ Create individual IAM users
- ⚠ Use groups to assign permissions
- ⚠ Apply an IAM password policy

Feature Spotlight

Introduction to AWS IAM



1 / 1

Additional Information

- IAM best practices
- IAM documentation
- Web Identity Federation
- Playground
- Policy Simulator
- Videos, IAM release history and additional resources

console.aws.amazon.com/iam/home?region=us-east-1#/home

Welcome to Identity and Access Management

IAM users sign-in link:
<https://613943640677.signin.aws.amazon.com/console>

IAM Resources

Users: 0	Roles: 2
Groups: 0	Identity Providers: 0
Customer Managed Policies: 0	

Security Status

1 out of 5 complete.

- Delete your root access keys
- ⚠ Activate MFA on your root account
 - Activate multi-factor authentication (MFA) on your AWS root account to add another layer of protection to help keep your account secure. [Learn More](#)
 - [Manage MFA](#)
- ⚠ Create individual IAM users
- ⚠ Use groups to assign permissions
- ⚠ Apply an IAM password policy

Feature Spotlight

Introduction to AWS IAM



0:00 / 2:16

Additional Information

- [IAM best practices](#)
- [IAM documentation](#)
- [Web Identity Federation](#)
- [Playground](#)
- [Policy Simulator](#)
- [Videos, IAM release history and additional resources](#)

console.aws.amazon.com/iam/home?region=us-east-1#/home

Welcome to Identity and Access Management

IAM users sign-in link:

<https://613943640677.signin.aws.amazon.com/console>

Manage MFA device

Select the type of MFA device to activate:

A virtual MFA device

A hardware MFA device

For more information about supported MFA devices, see [AWS Multi-Factor Authentication](#).

[Cancel](#) [Next Step](#)

Additional Information

- best practices
- documentation
- Identity Federation
- CloudSimulator
- videos, IAM release history and additional resources

Feedback **English (US)**

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy Terms of Use

console.aws.amazon.com/iam/home?region=us-east-1#/home

Manage MFA device

If your virtual MFA application supports scanning QR codes, scan the following QR code with your smartphone's camera.



▶ [Show secret key for manual configuration](#)

After the application is configured, enter two consecutive authentication codes in the boxes below and choose **Activate virtual MFA**.

Authentication code 1

Authentication code 2

[Cancel](#) [Previous](#) [Activate virtual MFA](#)