1

Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
0	0	2	0	0

What's new

View all

Updates for features in IAM

- AWS IAM announces support for encrypted SAML assertions. *3 months ago*
- AWS CodeBuild announces support for project ARN and build ARN IAM condition keys. *3 months ago*
- IAM Roles Anywhere credential helper now supports TPM 2.0. *5 months ago*
- Announcing AWS STS support for ECDSA-based signatures of OIDC tokens. *6 months ago*

more

Show more results

Sign-in URL for IAM users in this account

https://[redacted].signin.aws.amazon.com/console

Quick Links

My security credentials

Manage your access keys, multi-factor authentication (MFA) and other credentials.

Tools

Policy simulator

The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.

Additional information

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management
- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings
- Root access management New

Access reports
- Access Analyzer
  - External access
  - Unused access
  - Analyzer settings

Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
0	0	2	0	0

What's new

View all

Updates for features in IAM

- AWS IAM announces support for encrypted SAML assertions. *3 months ago*
- AWS CodeBuild announces support for project ARN and build ARN IAM condition keys. *3 months ago*
- IAM Roles Anywhere credential helper now supports TPM 2.0. *5 months ago*
- Announcing AWS STS support for ECDSA-based signatures of OIDC tokens. *6 months ago*

more

Tools

Policy simulator

The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.

Additional information

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management
- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings
- Root access management New

Access reports
- Access Analyzer
  - External access
  - Unused access
  - Analyzer settings

Account ID [redacted]

Account
Organization
Service Quotas
Billing and Cost Management
2 Security credentials

Turn on multi-session support
Sign out

Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings

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

Actions

Account name
ModestusMadu

AWS account ID
[redacted]

Email address
[redacted]

Canonical user ID
a0[redacted]ffa6af[redacted]

Multi-factor authentication (MFA) (1)

Remove Resync Assign MFA device

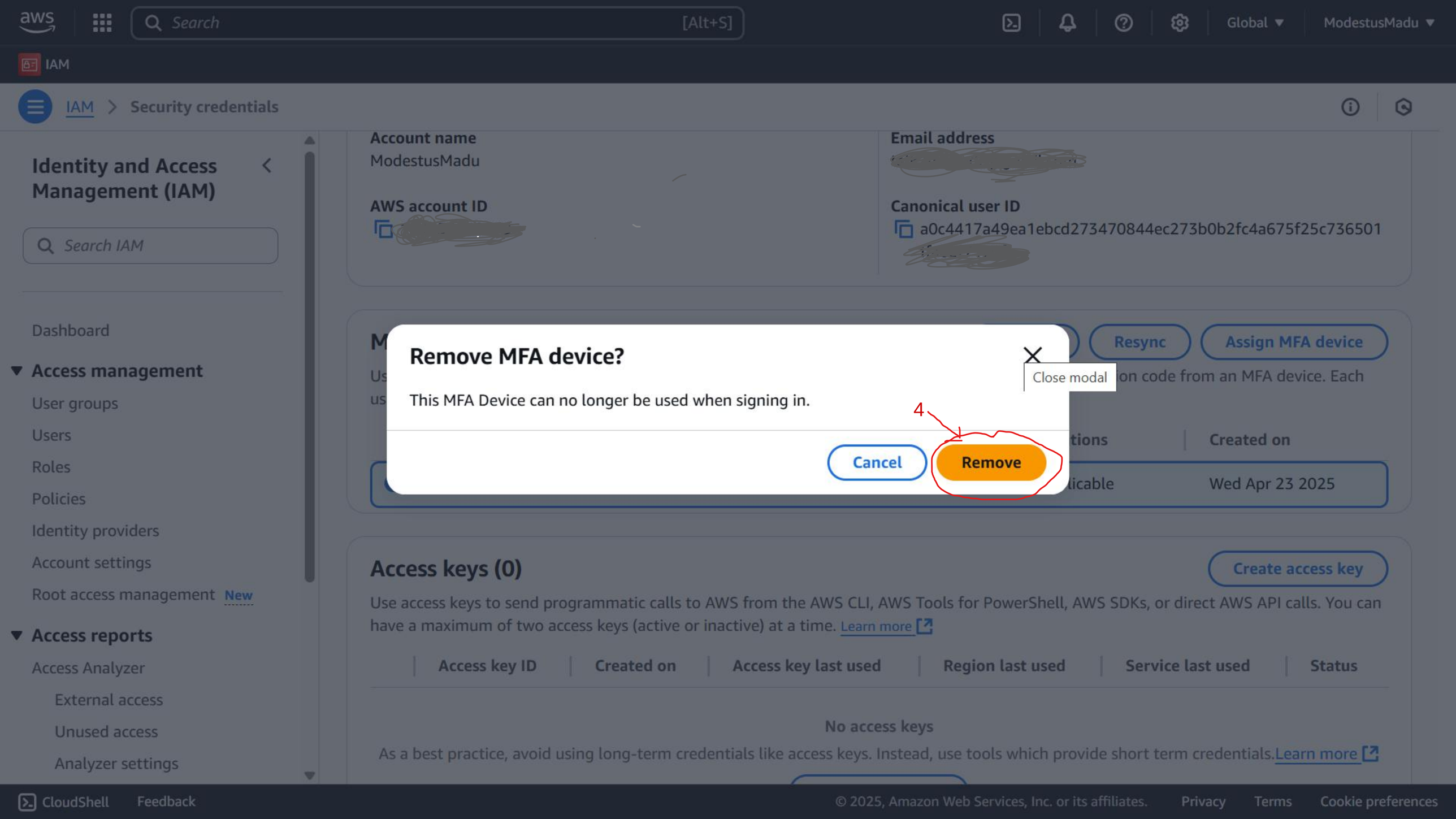
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more

Type	Identifier	Certifications	Created on
Virtual	arn:aws:iam::114354040272:mfa/Authapp	Not Applicable	Wed Apr 23 2025

3

Access keys (0)

Create access key


Search [Alt+S]
Global
ModestusMadu
IAM
IAM > Security credentials
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Account name
ModestusMadu
AWS account ID
Email address
Canonical user ID
a0c4417a49ea1ebcd273470844ec273b0b2fc4a675f25c736501
Resync
Assign MFA device
Remove MFA device?
Close modal
This MFA Device can no longer be used when signing in.
4
Cancel
Remove
Created on
Wed Apr 23 2025
Access keys (0)
Create access key
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
Access key ID
Created on
Access key last used
Region last used
Service last used
Status
No access keys
As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. Learn more
CloudShell
Feedback
© 2025, 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
Root access management New

Access reports
Access Analyzer
External access
Unused access
Analyzer settings

MFA device deleted.

Multi-factor authentication (MFA) (0)

Remove | Resync | Assign MFA device

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

No MFA devices. Assign an MFA device to improve the security of your AWS environment

Assign MFA device

Access keys (0)

Create access key

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

Access key ID	Created on	Access key last used	Region last used	Service last used	Status

No access keys

As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. Learn more

Create access key