aws Services More

Search

Search IAM

Filter

Clear All | Select All

- ☑ Users
- ☑ Groups
- ☑ Roles
- ☑ Policies
- ☑ Providers
- ☑ Help
- ☑ Info

To start searching your IAM entities (users, groups, roles, providers) just start typing in the text field above.

Identity and Access Management (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
- Service control policies (SCPs)

Search IAM

AWS account ID:
793666650440

Your Security Credentials

Feedback Change language Privacy Terms Cookie preferences

To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference.

Password

You use an email address and password to sign in to secure pages on AWS, such as the AWS Management Console, AWS Forums, and AWS Support. For your protection, create a password that contains many characters, including numbers and punctuation. Store your password securely, do not share it, and change it periodically.
Click here to change the password, name, or email address for your root AWS account.

Multi-factor authentication (MFA)

Use MFA to increase the security of your AWS environments. Signing in to MFA-protected accounts requires a user name, password, and an authentication code from an MFA device.
Device type
Serial number
Actions
Virtual
arn:aws:iam::793666650440:mfa/root-account-mfa-device
Manage

Access keys (access key ID and secret access key)

Use access keys to make programmatic calls to AWS from the AWS CLI, 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.

For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation.
If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.
Learn more

Created	Access Key ID	Last Used	Last Used Region	Last Used Service	Status	Actions
Sep 3rd 2022	AKIA3RSRYAFEG7KY5QVZ	2022-09-08 20:50 UTC+0600	us-east-2	ses	Active	Make Inactive | Delete
Sep 23rd 2022	AKIA3RSRYAFEEGGLUA4R	N/A	N/A	N/A	Active	Make Inactive | Delete

Create New Access Key

Root user access keys provide unrestricted access to your entire AWS account. If you need long-term access keys, we recommend creating a new IAM user with limited permissions and generating access keys for that user instead. Learn more

CloudFront key pairs

You use key pairs in Amazon CloudFront to create signed URLs. Note: You use different key pairs to launch and access Amazon EC2 instances. Those key pairs are managed in the EC2 console . For your protection, store your key pairs securely and do not share them. In addition, AWS recommends that you change your key pairs periodically.

Note: You can have a maximum of two CloudFront key pairs (active or inactive) at a time.

Created	Access Key ID	Status	Actions

Create New Key Pair Upload Your Own Key Pair

X.509 certificate

do not share them. In addition, AWS recommends that you rotate your certificates periodically.

Note: You can have a maximum of two X.509 certificates (active or inactive) at a time.

Created	Thumbprint	Status	Actions

Create New Certificate Upload Your Own Certificate

Account identifiers

You use your 12-digit account ID to reference your account programmatically and in other contexts. You use your canonical user ID to configure Amazon S3 access control lists (ACLs).

AWS Account ID: **793666650440**

Canonical User ID: **b9d741df7698dd32eaa2a201c6280faf1ec26d394b7523b9db0fce8966d77a90**