Create AWS Free Tier Account

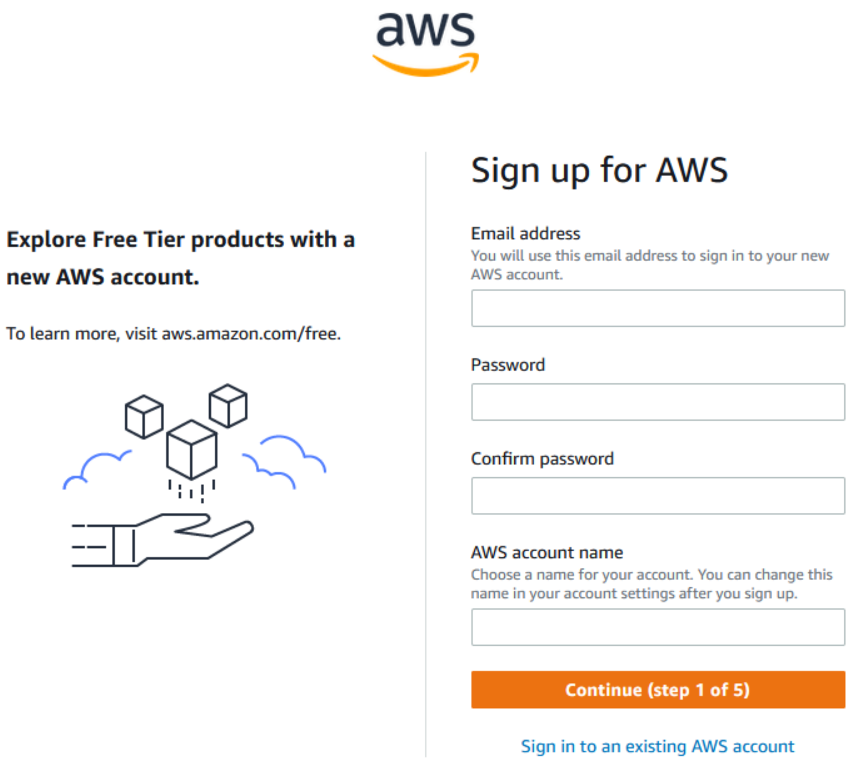
Contents

Important Notes

1. You must follow the instructions strictly to remain within the free tier.
2. You must not use a personal email subscribed early for the free tier because you will not be eligible. A workaround to use another email not used before or create a new one.
3. Suppose there is Active Directory Synchronization, Federation, Single-Sign-On (SSO) integration in place between your organization and public cloud providers (AWS). Most likely, you will not be able to use your organization's email for provisioning resources. Unless you are one of the administrators, please be careful and not use your organization's email.

a) Create an AWS Account

1. Open URL: https://aws.amazon.com/getting-started/
2. Click on **Create an AWS Account**
3. AWS Accounts include 12 months of free tier access for full offer terms, and free tier details visit https://aws.amazon.com/free/
4. Enter the following details: your email address, create a password and choose your preferred AWS account name. Click Continue



Explore Free Tier products with a new AWS account.

To learn more, visit aws.amazon.com/free.

Sign up for AWS

Email address

You will use this email address to sign in to your new AWS account.

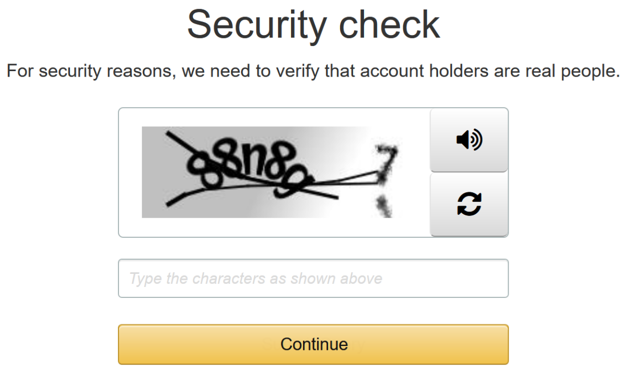
Password

Confirm password

AWS account name

Choose a name for your account. You can change this name in your account settings after you sign up.

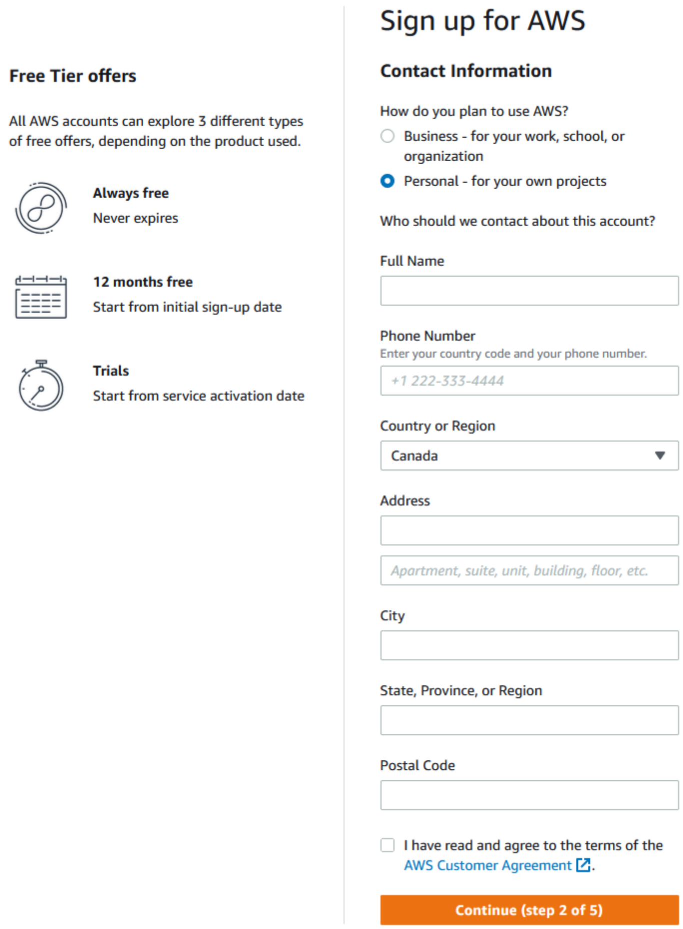
5. Complete the Security check. click Continue



Security check

For security reasons, we need to verify that account holders are real people.

6. Complete the **Contact Information**
   - Select Account Type (Professional OR Personal) **Personal**
   - Enter your full name, phone number, country/region, address, city, state/province or region, postal code, read and accept AWS Customer Agreement



Sign up for AWS

Free Tier offers

All AWS accounts can explore 3 different types of free offers, depending on the product used.

Always free
Never expires

12 months free
Start from initial sign-up date

Trials
Start from service activation date

Contact Information

How do you plan to use AWS?

○ Business - for your work, school, or organization

● Personal - for your own projects

Who should we contact about this account?

Full Name

Phone Number
Enter your country code and your phone number.
+1 222-333-4444

Country or Region
Canada

Address

Apartment, suite, unit, building, floor, etc.

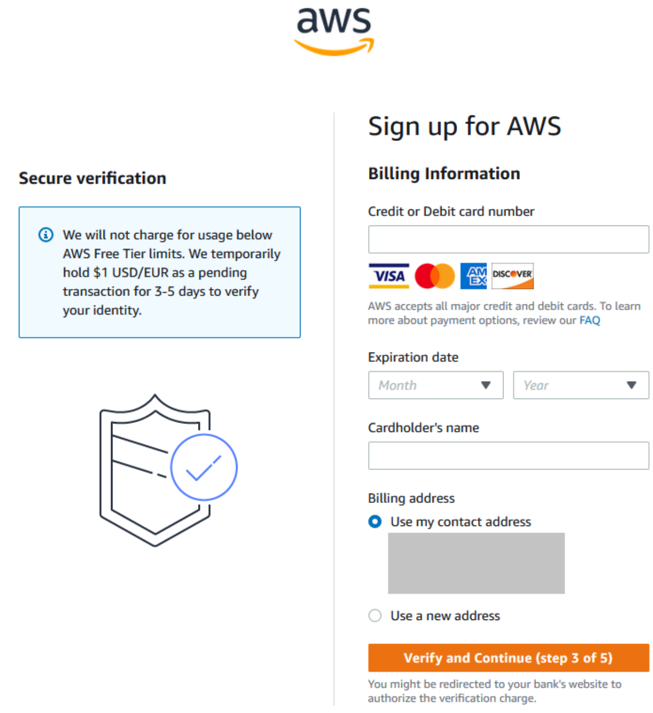
City

State, Province, or Region

Postal Code

□ I have read and agree to the terms of the AWS Customer Agreement.

7. Complete the Payment Information (You need **Valid** Credit Card)



Sign up for AWS

Secure verification

We will not charge for usage below AWS Free Tier limits. We temporarily hold $1 USD/EUR as a pending transaction for 3-5 days to verify your identity.

Billing Information

Credit or Debit card number

AWS accepts all major credit and debit cards. To learn more about payment options, review our FAQ

Expiration date
Month Year

Cardholder's name

Billing address

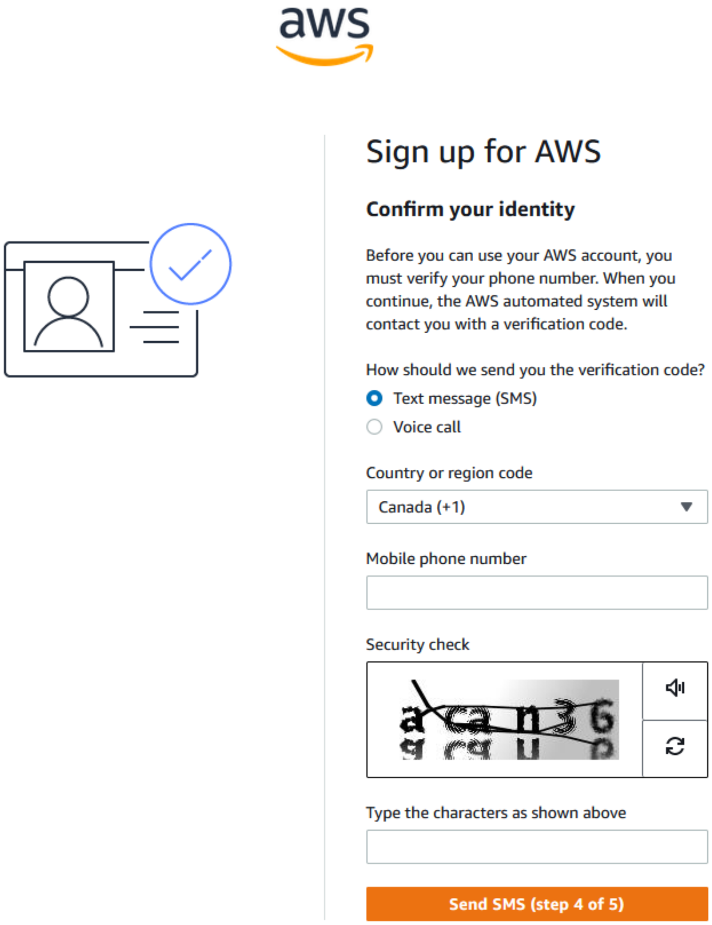
● Use my contact address

[redacted]

○ Use a new address

You might be redirected to your bank's website to authorize the verification charge.

8. Confirm your identity. (Your identity has been verified successfully)



Sign up for AWS

Confirm your identity

Before you can use your AWS account, you must verify your phone number. When you continue, the AWS automated system will contact you with a verification code.

How should we send you the verification code?

● Text message (SMS)

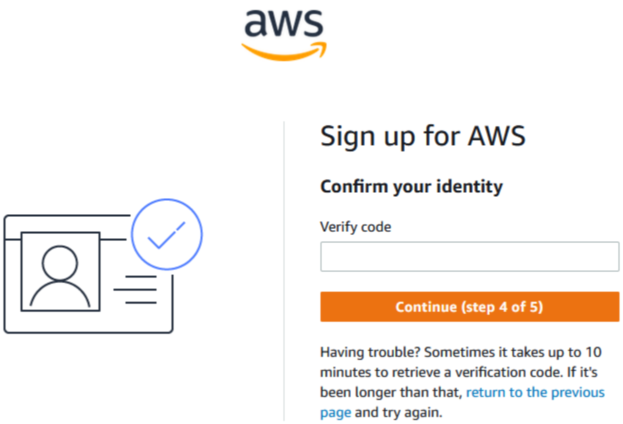
○ Voice call

Country or region code: Canada (+1)

Mobile phone number

Security check

Type the characters as shown above



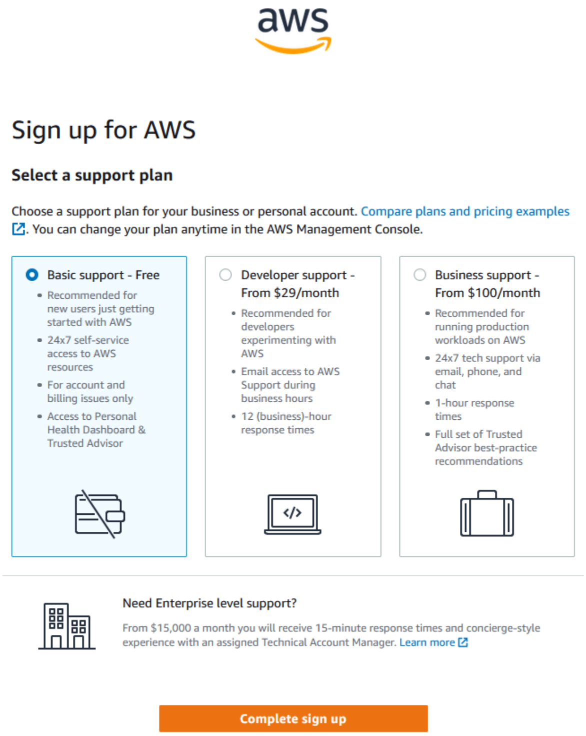
Sign up for AWS

Confirm your identity

Verify code

Having trouble? Sometimes it takes up to 10 minutes to retrieve a verification code. If it's been longer than that, return to the previous page and try again.

9. Select a support plan (select **Basic** for Free Tier)



Sign up for AWS

Select a support plan

Choose a support plan for your business or personal account. Compare plans and pricing examples. You can change your plan anytime in the AWS Management Console.

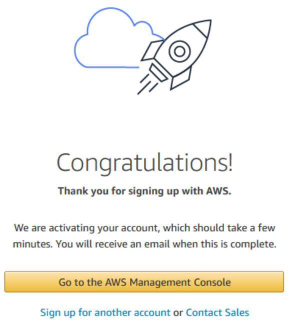
● Basic support - Free
- Recommended for new users just getting started with AWS
- 24x7 self-service access to AWS resources
- For account and billing issues only
- Access to Personal Health Dashboard & Trusted Advisor

○ Developer support - From $29/month
- Recommended for developers experimenting with AWS
- Email access to AWS Support during business hours
- 12 (business)-hour response times

○ Business support - From $100/month
- Recommended for running production workloads on AWS
- 24x7 tech support via email, phone, and chat
- 1-hour response times
- Full set of Trusted Advisor best-practice recommendations

Need Enterprise level support?

From $15,000 a month you will receive 15-minute response times and concierge-style experience with an assigned Technical Account Manager. Learn more



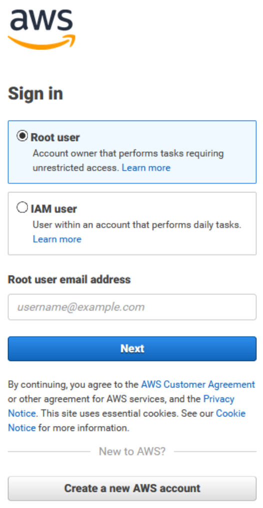
Congratulations!

Thank you for signing up with AWS.

We are activating your account, which should take a few minutes. You will receive an email when this is complete.

Sign up for another account or Contact Sales

10. Sign in to the AWS console



aws

Sign in

● Root user
Account owner that performs tasks requiring unrestricted access. Learn more

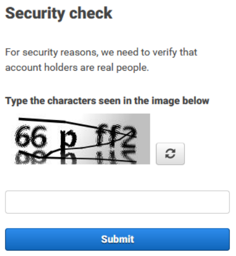
○ IAM user
User within an account that performs daily tasks. Learn more

Root user email address

username@example.com

By continuing, you agree to the AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.

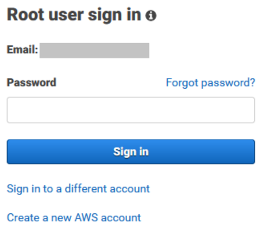
New to AWS?



Security check

For security reasons, we need to verify that account holders are real people.

Type the characters seen in the image below



Root user sign in

Email: [redacted]

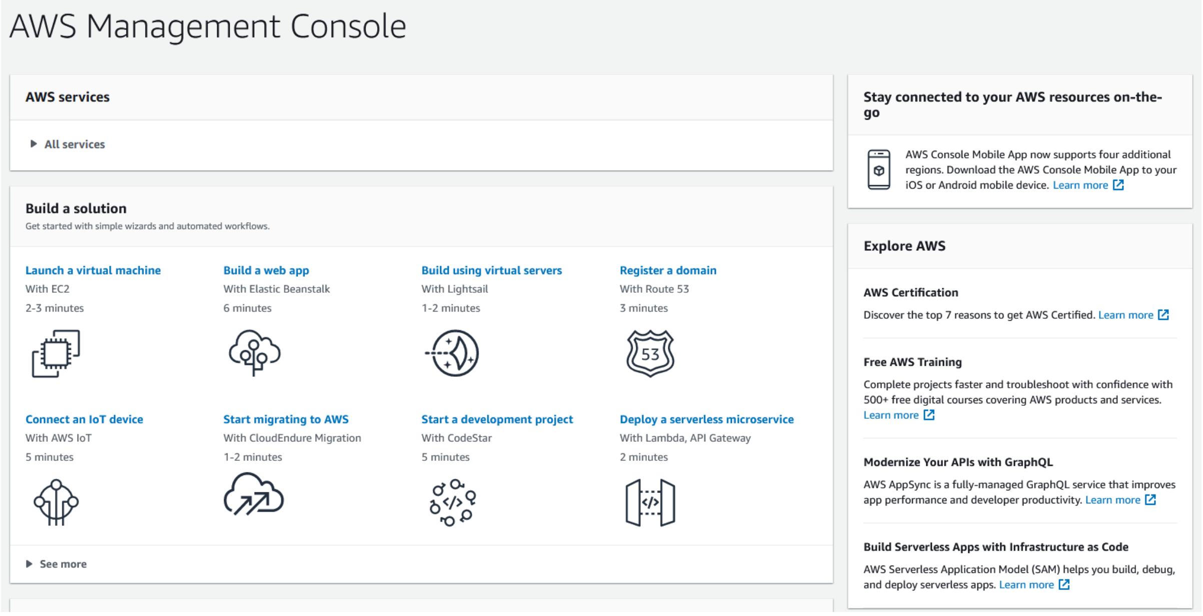
Password

Forgot password?

Sign in to a different account

Create a new AWS account

b) Navigate AWS Console (Optional)



AWS Management Console

AWS services

▶ 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

Register a domain
With Route 53
3 minutes

Connect an IoT device
With AWS IoT
5 minutes

Start migrating to AWS
With CloudEndure Migration
1-2 minutes

Start a development project
With CodeStar
5 minutes

Deploy a serverless microservice
With Lambda, API Gateway
2 minutes

▶ See more

Stay connected to your AWS resources on-the-go

AWS Console Mobile App now supports four additional regions. Download the AWS Console Mobile App to your iOS or Android mobile device. Learn more

Explore AWS

AWS Certification

Discover the top 7 reasons to get AWS Certified. Learn more

Free AWS Training

Complete projects faster and troubleshoot with confidence with 500+ free digital courses covering AWS products and services. Learn more

Modernize Your APIs with GraphQL

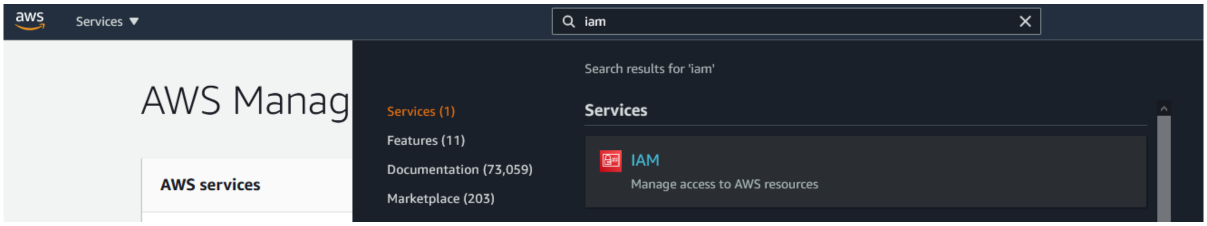
AWS AppSync is a fully-managed GraphQL service that improves app performance and developer productivity. Learn more

Build Serverless Apps with Infrastructure as Code

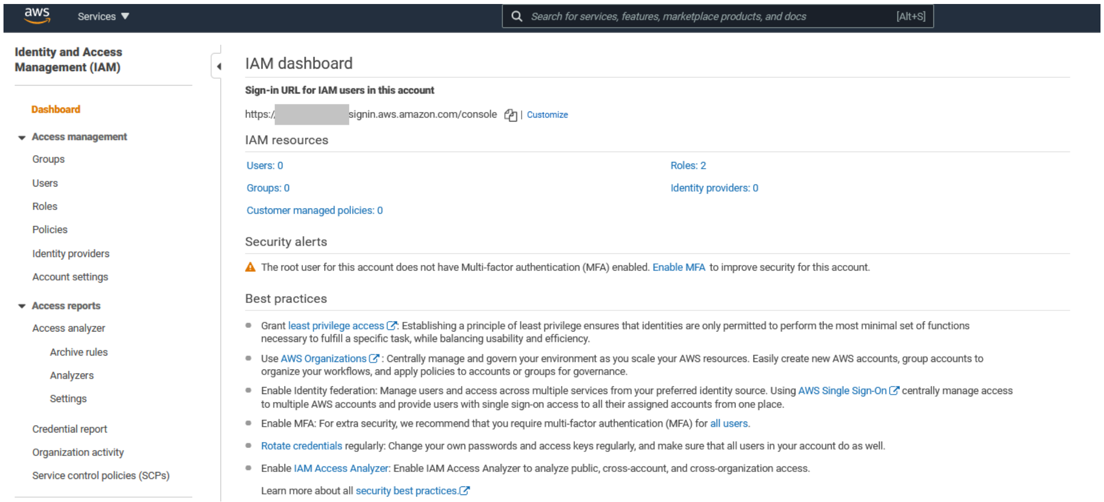
AWS Serverless Application Model (SAM) helps you build, debug, and deploy serverless apps. Learn more

C) AWS Identity and Access Management (Bouns)

1. Navigate to IAM



2. Secure your AWS account based on best practices



IAM dashboard

Sign-in URL for IAM users in this account

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

IAM resources

Users: 0	Roles: 2
Groups: 0	Identity providers: 0
Customer managed policies: 0	

Security alerts

⚠ The root user for this account does not have Multi-factor authentication (MFA) enabled. Enable MFA to improve security for this account.

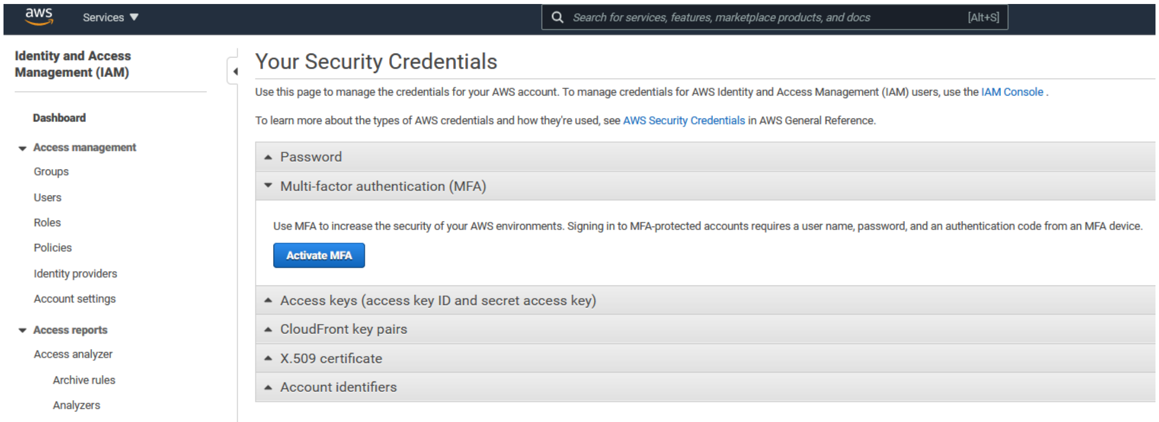
Best practices

- Grant least privilege access: Establishing a principle of least privilege ensures that identities are only permitted to perform the most minimal set of functions necessary to fulfill a specific task, while balancing usability and efficiency.
- Use AWS Organizations: Centrally manage and govern your environment as you scale your AWS resources. Easily create new AWS accounts, group accounts to organize your workflows, and apply policies to accounts or groups for governance.
- Enable Identity federation: Manage users and access across multiple services from your preferred identity source. Using AWS Single Sign-On centrally manage access to multiple AWS accounts and provide users with single sign-on access to all their assigned accounts from one place.
- Enable MFA: For extra security, we recommend that you require multi-factor authentication (MFA) for all users.
- Rotate credentials regularly: Change your own passwords and access keys regularly, and make sure that all users in your account do as well.
- Enable IAM Access Analyzer: Enable IAM Access Analyzer to analyze public, cross-account, and cross-organization access.

Learn more about all security best practices

3. Enable MFA on your root account (Google Authenticator)

1. Click on Enable MFA Under Security alerts



Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the IAM Console .

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

▲ Password

▼ 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.

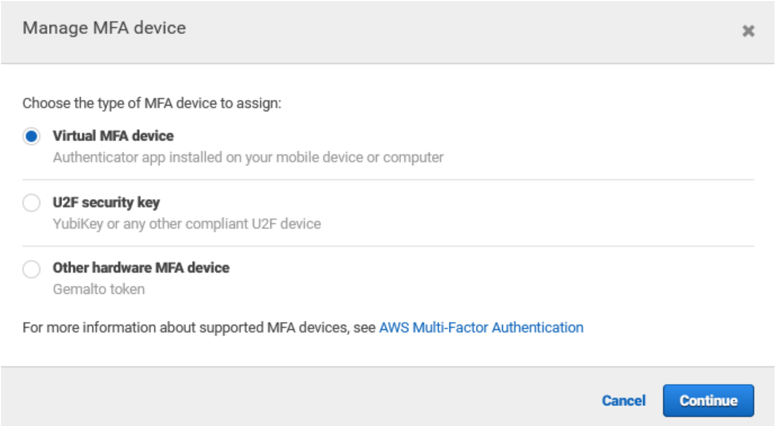
Activate MFA

▲ Access keys (access key ID and secret access key)

▲ CloudFront key pairs

▲ X.509 certificate

▲ Account identifiers



Manage MFA device

Choose the type of MFA device to assign:

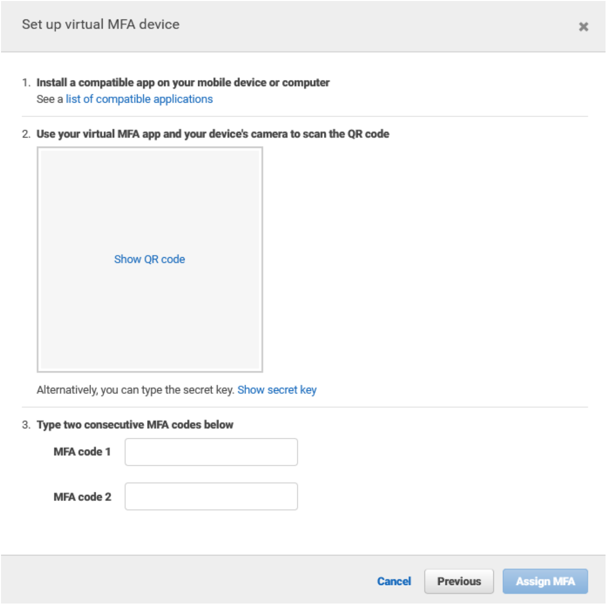
● **Virtual MFA device**
Authenticator app installed on your mobile device or computer

○ **U2F security key**
YubiKey or any other compliant U2F device

○ **Other hardware MFA device**
Gemalto token

For more information about supported MFA devices, see AWS Multi-Factor Authentication

2. Set up virtual MFA device

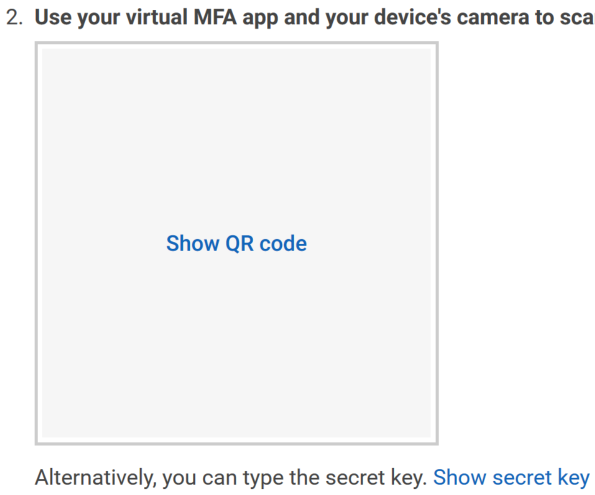


Set up virtual MFA device

1. **Install a compatible app on your mobile device or computer**
   See a list of compatible applications
2. **Use your virtual MFA app and your device's camera to scan the QR code**
   Alternatively, you can type the secret key. Show secret key
3. **Type two consecutive MFA codes below**
   MFA code 1
   MFA code 2

Install a compatible app on your mobile device or computer
See a list of compatible applications

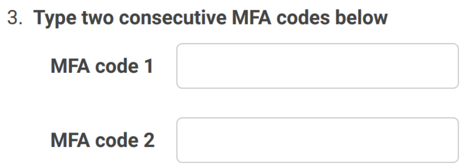
3. Use your virtual MFA app and your device's camera to scan the QR code



2. **Use your virtual MFA app and your device's camera to scan the QR code**

Alternatively, you can type the secret key. Show secret key

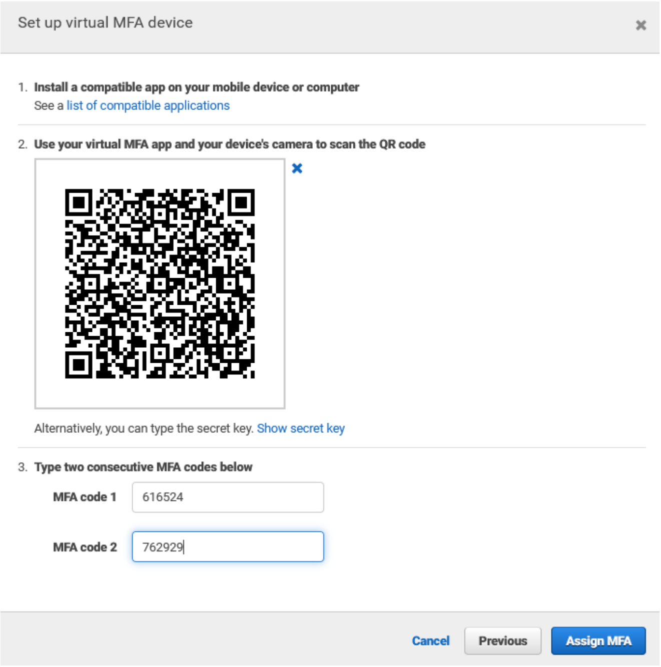
4. Type two consecutive MFA codes below



3. **Type two consecutive MFA codes below**

MFA code 1

MFA code 2



Set up virtual MFA device

1. **Install a compatible app on your mobile device or computer**
   See a list of compatible applications

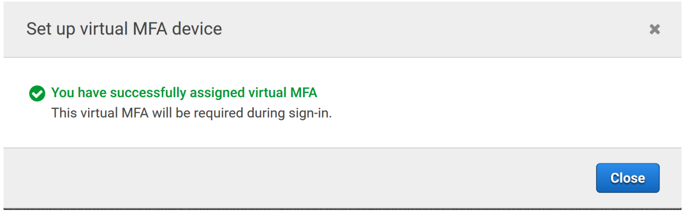
2. **Use your virtual MFA app and your device's camera to scan the QR code**

   Alternatively, you can type the secret key. Show secret key

3. **Type two consecutive MFA codes below**

   MFA code 1 616524

   MFA code 2 762929



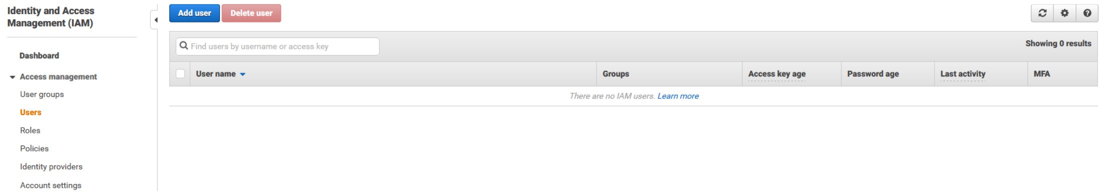
Set up virtual MFA device ✖

✅ You have successfully assigned virtual MFA

This virtual MFA will be required during sign-in.

4. Create individual IAM users

1. Select Users under Access Management

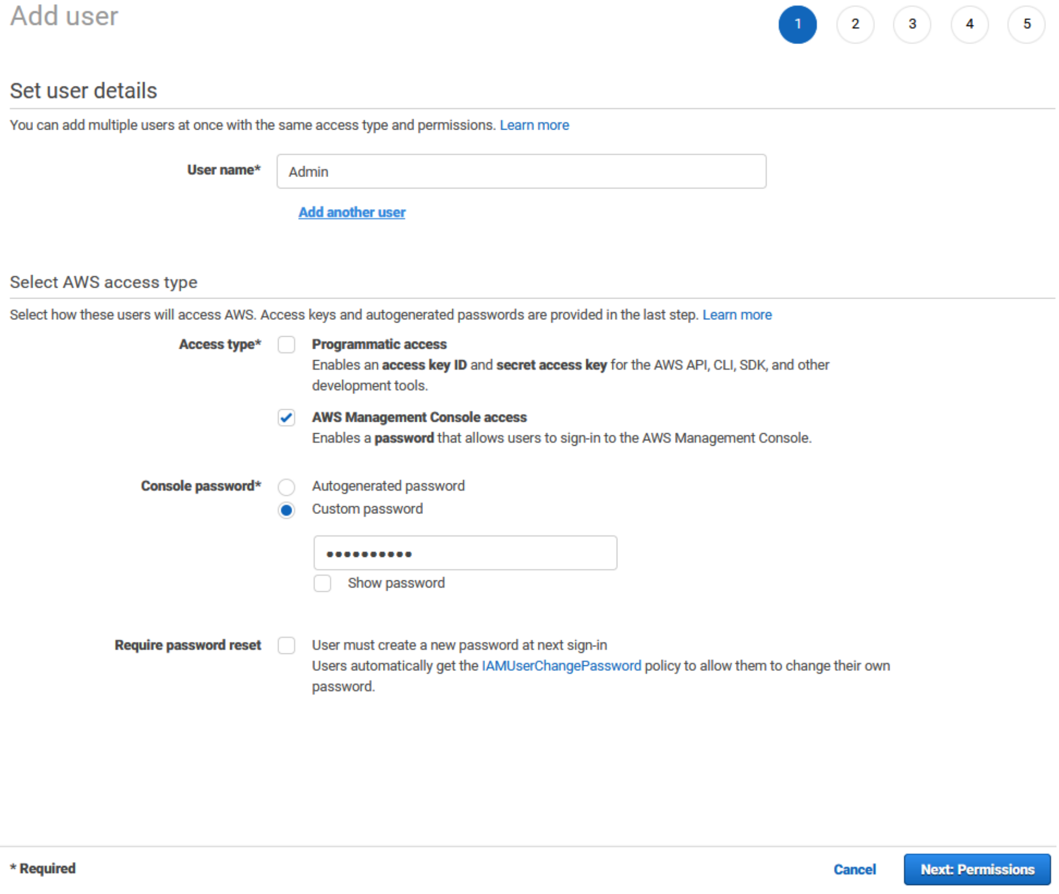


☐	User name	Groups	Access key age	Password age	Last activity	MFA

There are no IAM users. Learn more

4.2. Add User

- ○ Set user details
  - ■ User name: Admin
- ○ Select AWS access type:
  - ■ Access type: Select AWS Management Console access
  - ■ Console password: Select Custom password and insert a password
  - ■ Require password reset: Unselect (User must create a new password at next sign-in)



Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* Admin

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

Access type* ☐ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☑ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password* ○ Autogenerated password
● Custom password

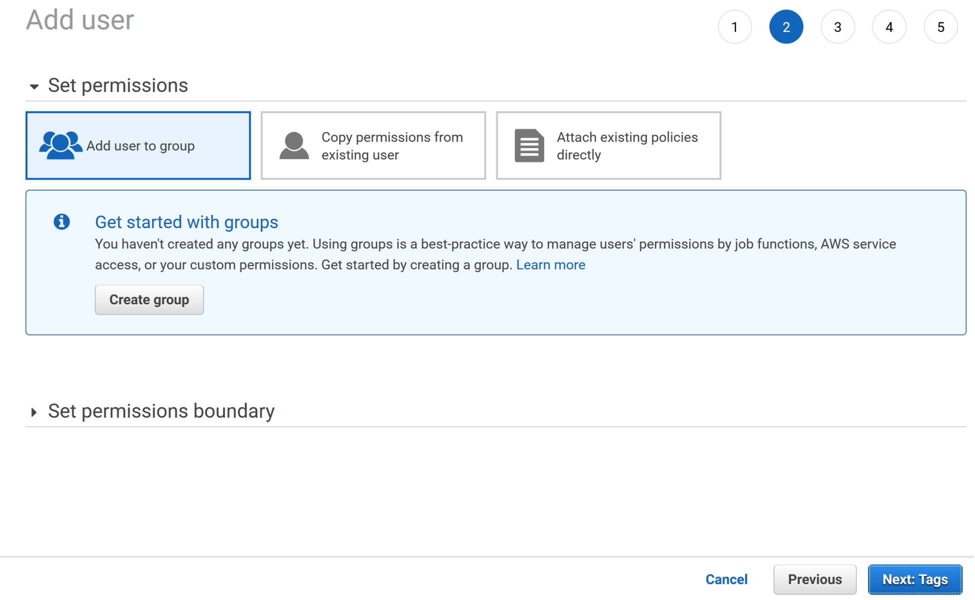
••••••••••

☐ Show password

Require password reset ☐ User must create a new password at next sign-in
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

* Required

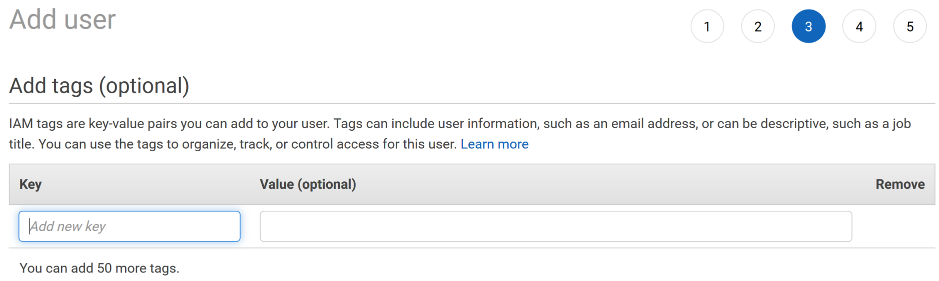
- Set Permissions



Get started with groups

You haven't created any groups yet. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Get started by creating a group. Learn more

- Add tags (optional)

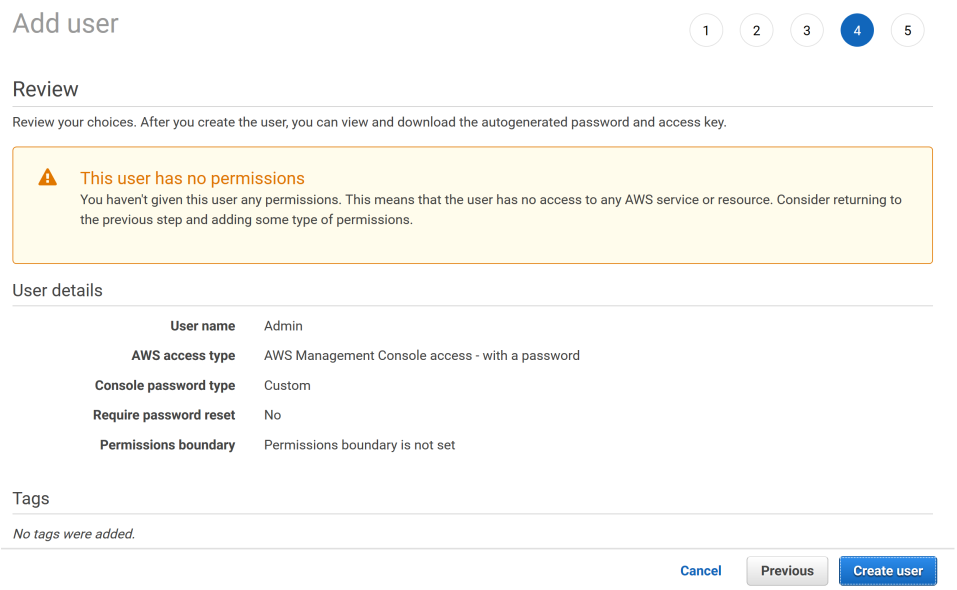


IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. Learn more

Key	Value (optional)	Remove
Add new key		

You can add 50 more tags.

- Review



Add user

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

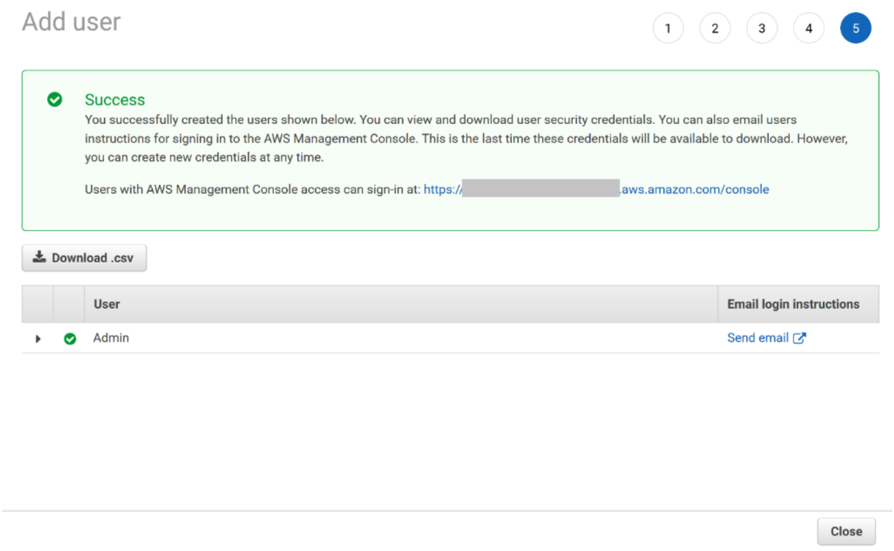
This user has no permissions
You haven't given this user any permissions. This means that the user has no access to any AWS service or resource. Consider returning to the previous step and adding some type of permissions.

User details

User name	Admin
AWS access type	AWS Management Console access - with a password
Console password type	Custom
Require password reset	No
Permissions boundary	Permissions boundary is not set

Tags

No tags were added.

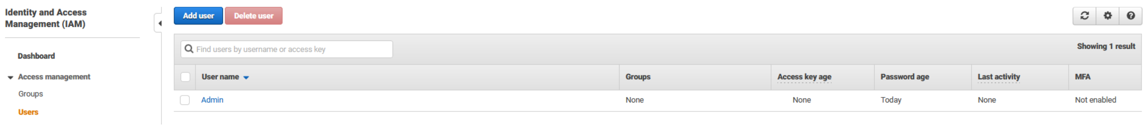


Add user

Success
You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: https://[redacted].aws.amazon.com/console

User	Email login instructions
Admin	Send email

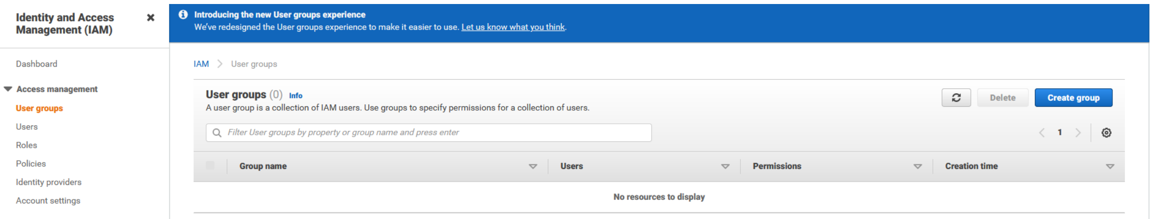

Identity and Access Management (IAM)
Dashboard
Access management
Groups
Users
Add user
Delete user
Find users by username or access key

Showing 1 result

User name	Groups	Access key age	Password age	Last activity	MFA
Admin	None	None	Today	None	Not enabled

5. Use groups to assign permissions

1. Select Users under Access Management



Introducing the new User groups experience
We've redesigned the User groups experience to make it easier to use. Let us know what you think.

IAM > User groups

User groups (0) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

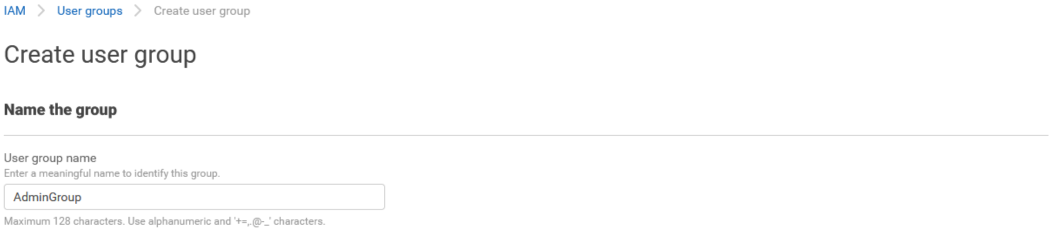
Delete
Create group
Filter User groups by property or group name and press enter
1

Group name	Users	Permissions	Creation time

No resources to display

5.2. Create Group

- ○ Group Name: AdminGroup



IAM > User groups > Create user group

Create user group

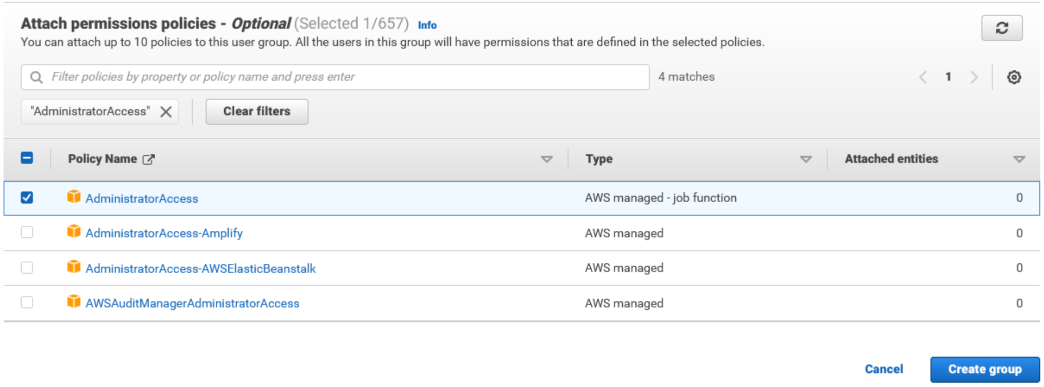
Name the group

User group name
Enter a meaningful name to identify this group.

AdminGroup

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

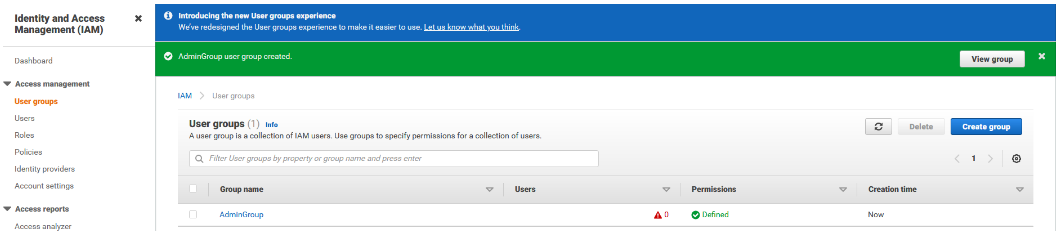
- ○ Attach Policy AdministratorAccess



Attach permissions policies - *Optional* (Selected 1/657) Info

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

	Policy Name	Type	Attached entities
☑	AdministratorAccess	AWS managed - job function	0
□	AdministratorAccess-Amplify	AWS managed	0
□	AdministratorAccess-AWSElasticBeanstalk	AWS managed	0
□	AWSAuditManagerAdministratorAccess	AWS managed	0



Introducing the new User groups experience
We've redesigned the User groups experience to make it easier to use. Let us know what you think.

AdminGroup user group created.

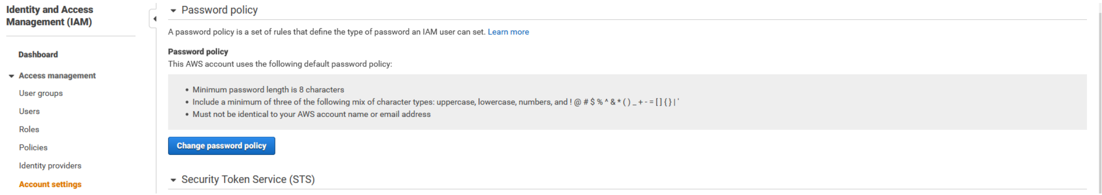
User groups (1)
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Filter User groups by property or group name and press enter

□	Group name	Users	Permissions	Creation time
□	AdminGroup	⚠ 0	✓ Defined	Now

6. Apply an IAM password policy

1. Select Account Settings under Access Management



Password policy

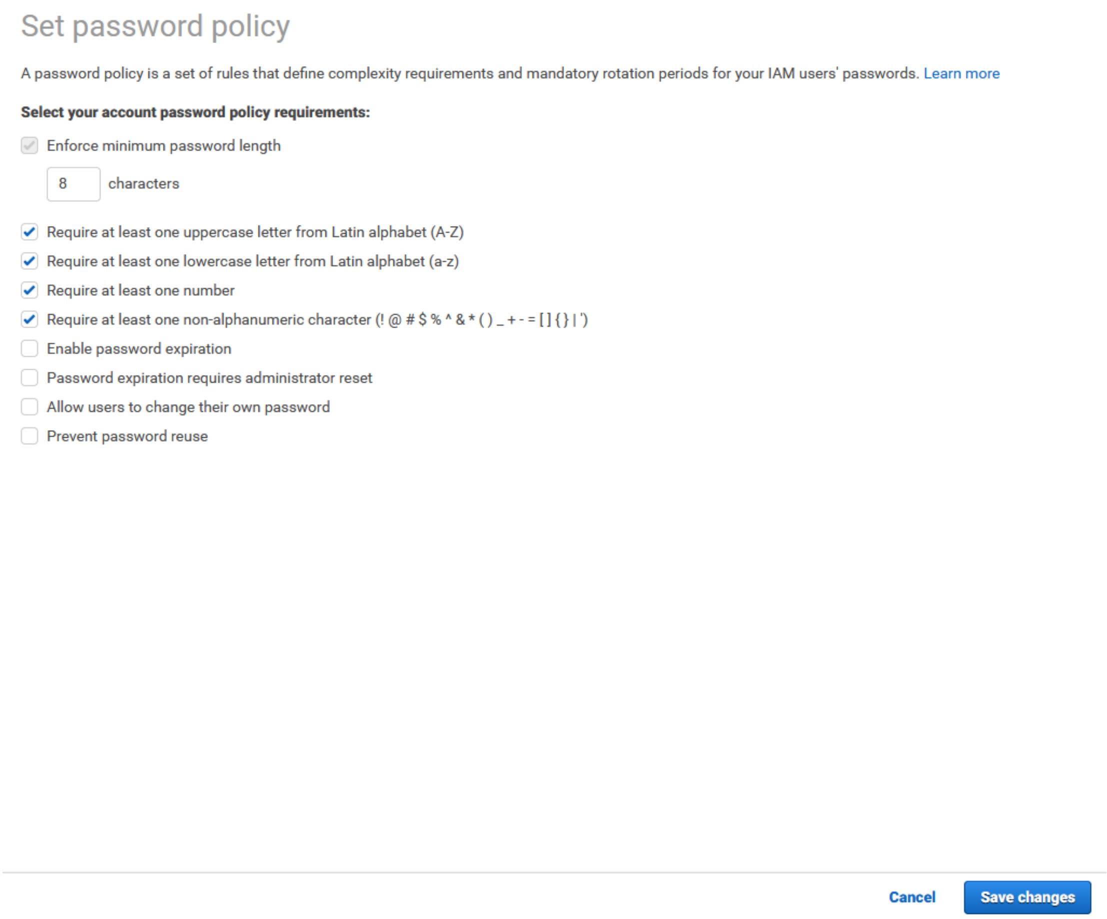
A password policy is a set of rules that define the type of password an IAM user can set. Learn more

Password policy
This AWS account uses the following default password policy:

- Minimum password length is 8 characters
- Include a minimum of three of the following mix of character types: uppercase, lowercase, numbers, and ! @ # $ % ^ & * ( ) _ + - = [ ] { } | '
- Must not be identical to your AWS account name or email address

Security Token Service (STS)

2. Select Change password policy



Set password policy

A password policy is a set of rules that define complexity requirements and mandatory rotation periods for your IAM users' passwords. Learn more

Select your account password policy requirements:

☑ Enforce minimum password length

8 characters

☑ Require at least one uppercase letter from Latin alphabet (A-Z)

☑ Require at least one lowercase letter from Latin alphabet (a-z)

☑ Require at least one number

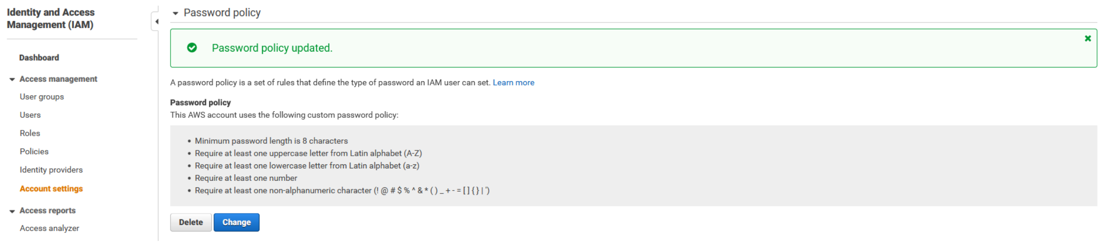
☑ Require at least one non-alphanumeric character (! @ # $ % ^ & * ( ) _ + - = [ ] { } | ')

□ Enable password expiration

□ Password expiration requires administrator reset

□ Allow users to change their own password

□ Prevent password reuse



Password policy updated.

A password policy is a set of rules that define the type of password an IAM user can set. Learn more

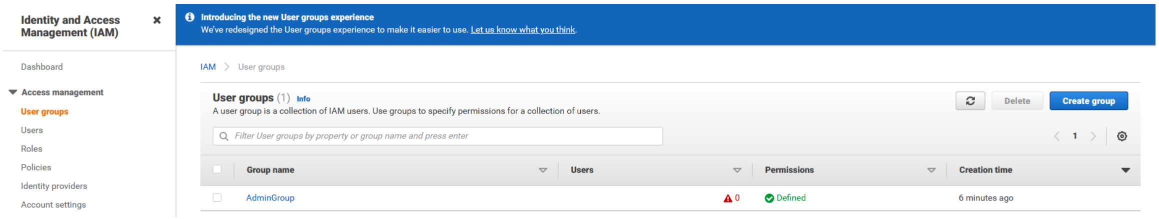
Password policy

This AWS account uses the following custom password policy:

- Minimum password length is 8 characters
- Require at least one uppercase letter from Latin alphabet (A-Z)
- Require at least one lowercase letter from Latin alphabet (a-z)
- Require at least one number
- Require at least one non-alphanumeric character (! @ # $ % ^ & * ( ) _ + - = [ ] { } | ')

7. Add the Admin user to the AdminGroup

1. Click on the AdminGroup



Introducing the new User groups experience

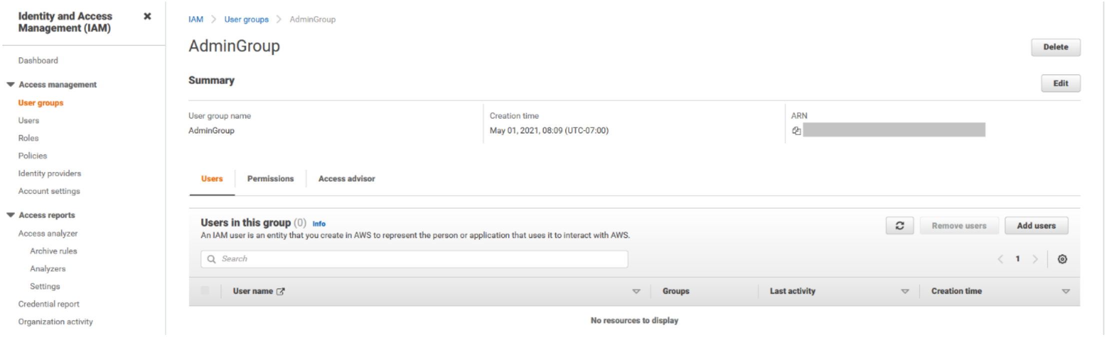
We've redesigned the User groups experience to make it easier to use. Let us know what you think.

User groups (1) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

	Group name	Users	Permissions	Creation time
□	AdminGroup	⚠ 0	✓ Defined	6 minutes ago

2. Click on the Add users and then select the User name **Admin**



AdminGroup

Summary

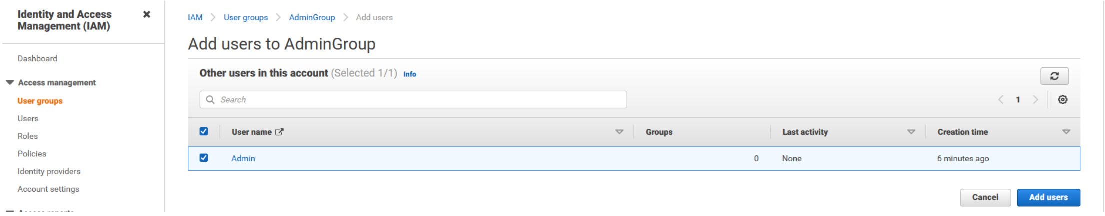
User group name	Creation time	ARN
AdminGroup	May 01, 2021, 08:09 (UTC-07:00)	[redacted]

Users in this group (0) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

User name	Groups	Last activity	Creation time

No resources to display

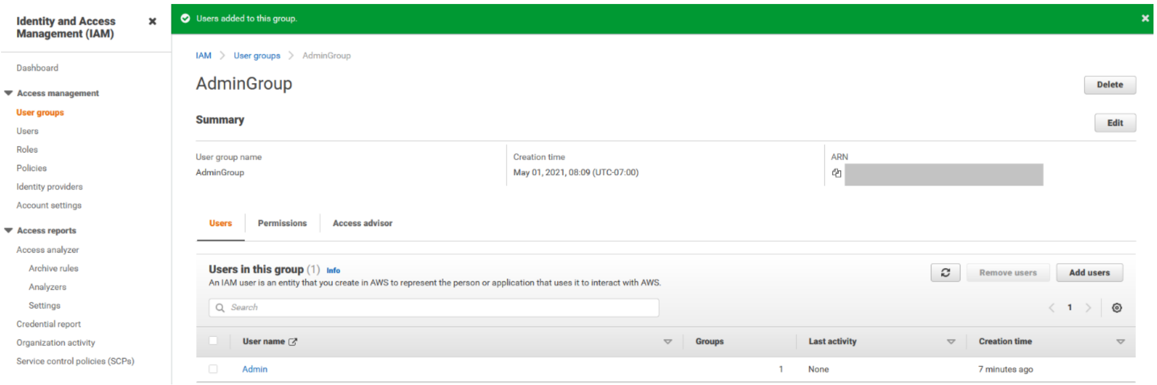


Add users to AdminGroup

Other users in this account (Selected 1/1) Info

☑	User name	Groups	Last activity	Creation time
☑	Admin	0	None	6 minutes ago

3. Click on Add Users



Users added to this group.

AdminGroup

Summary

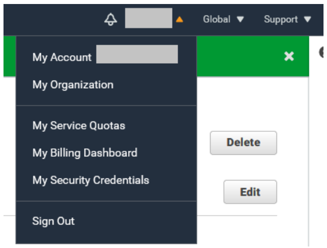
User group name	Creation time	ARN
AdminGroup	May 01, 2021, 08:09 (UTC-07:00)	[redacted]

Users in this group (1) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

□	User name	Groups	Last activity	Creation time
□	Admin	1	None	7 minutes ago

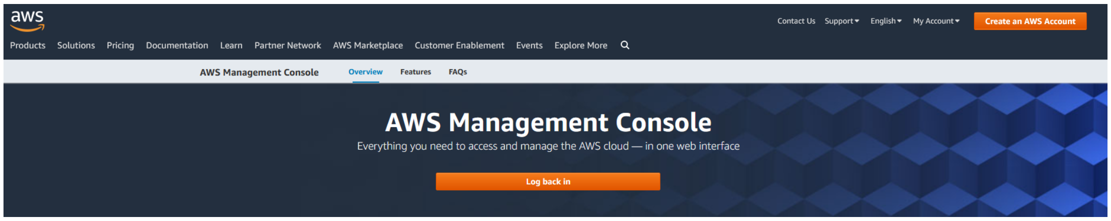
4. Take a not of you Account Number (My Account)



[redacted]

My Account [redacted]

5. Now Sign out from the root user



Contact Us Support English My Account **Create an AWS Account**

Products Solutions Pricing Documentation Learn Partner Network AWS Marketplace Customer Enablement Events Explore More

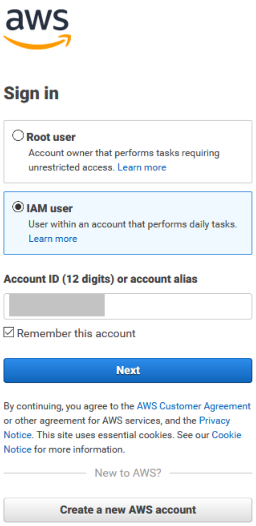
AWS Management Console Overview Features FAQs

AWS Management Console

Everything you need to access and manage the AWS cloud — in one web interface

Log back in

6. Click Log back in
7. Sing in with Admin user. You can also setup MFA for the Admin user following the same steps done previously for the root user



Sign in

○ **Root user**
Account owner that performs tasks requiring unrestricted access. Learn more

● **IAM user**
User within an account that performs daily tasks. Learn more

Account ID (12 digits) or account alias

[redacted]

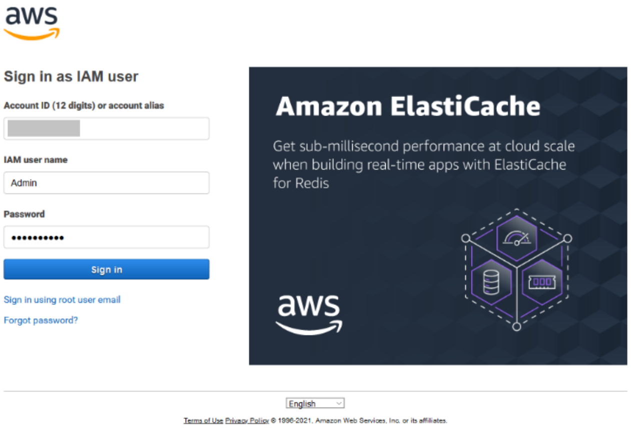
☑ Remember this account

Next

By continuing, you agree to the AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.

New to AWS?

Create a new AWS account



Sign in as IAM user

Account ID (12 digits) or account alias

[redacted]

IAM user name

Admin

Password

••••••••••

Sign in

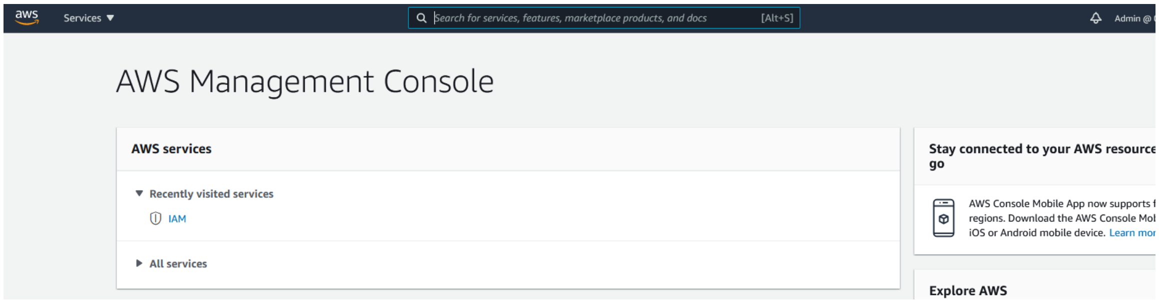
Sign in using root user email

Forgot password?

Amazon ElastiCache
Get sub-millisecond performance at cloud scale when building real-time apps with ElastiCache for Redis
aws

English

Terms of Use Privacy Policy © 1996-2021, Amazon Web Services, Inc. or its affiliates.



aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
Admin @

AWS Management Console

AWS services

▼ Recently visited services

IAM

▶ All services

Stay connected to your AWS resource go

AWS Console Mobile App now supports regions. Download the AWS Console Mol iOS or Android mobile device. Learn mor

Explore AWS