Module 1

Select email, account name, and password

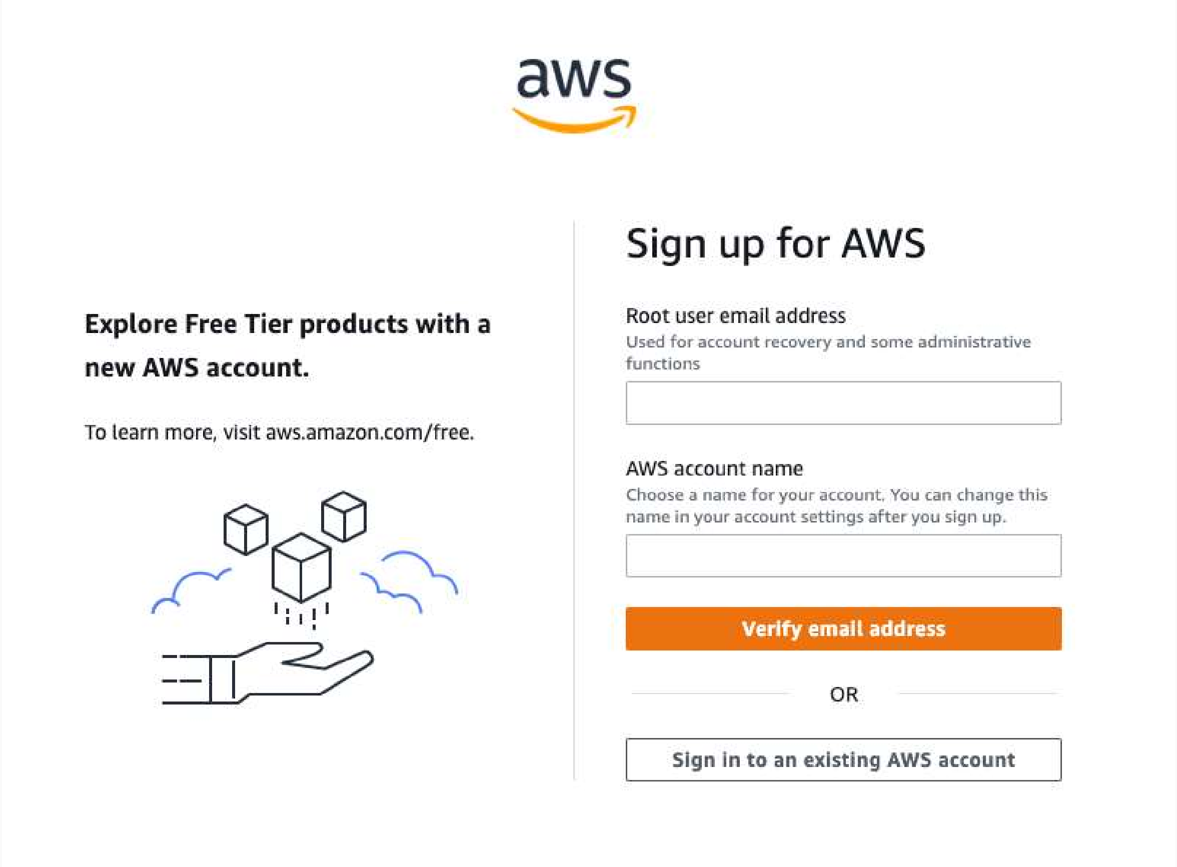
To create a new AWS account, go to aws.amazon.com and choose Create an AWS Account.

First, choose an email address and an account name.

Carefully consider which email address you want to use. If you are setting up for a personal account, we don't recommend using a work email address because you may change jobs at some point. Conversely, for business accounts, we recommend using an email alias that can be managed because the person setting up the account may, at some point, change roles or companies.

Once you fill out the email and account name fields, choose Verify email address. You will get a verification code in your email. Enter the verification code and choose Verify.

You will be redirected to a new screen where you will create your root user password.



Sign up for AWS

Explore Free Tier products with a new AWS account.

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

Root user email address

Used for account recovery and some administrative functions

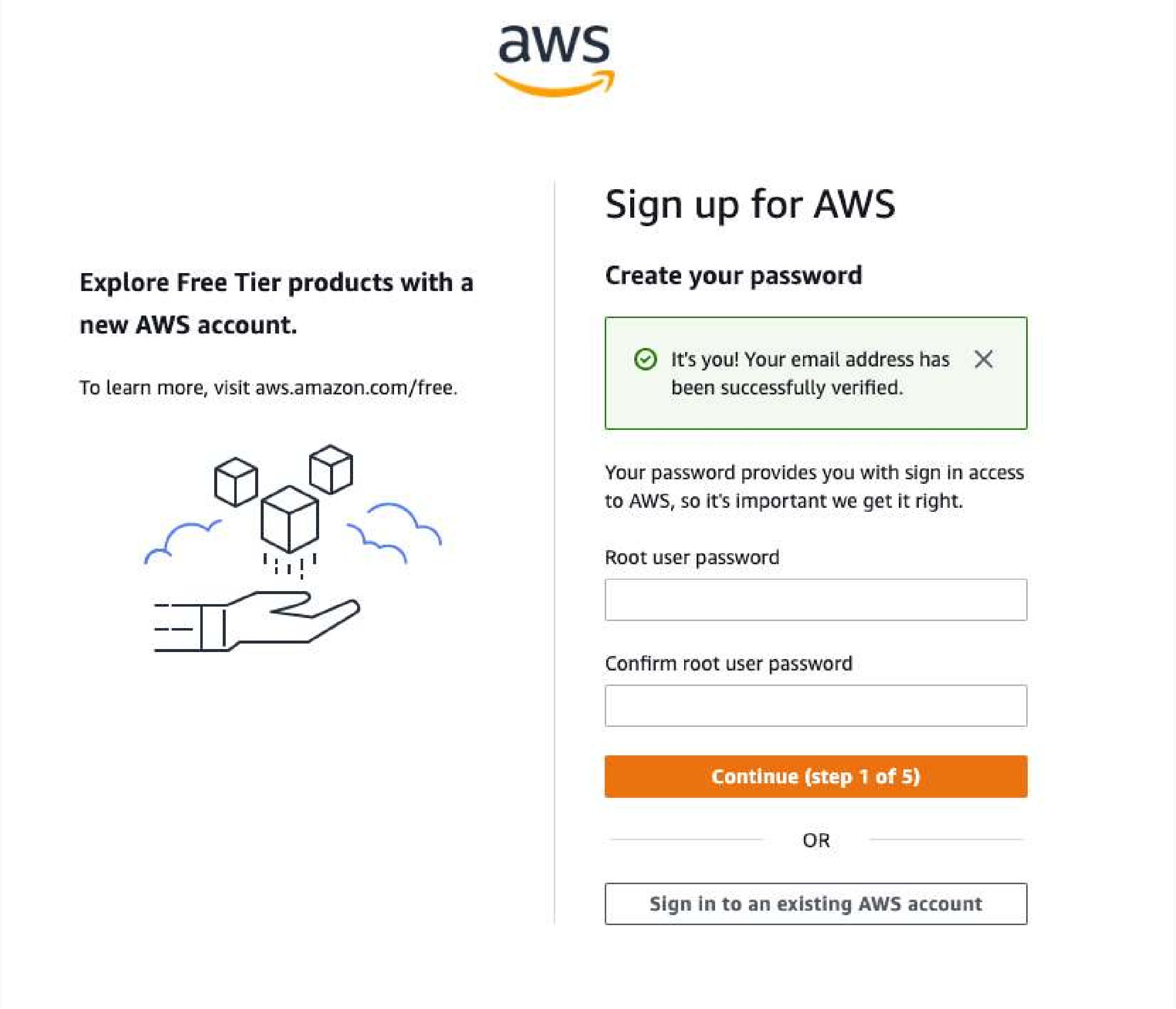
AWS account name

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

Create your root user password. The password you choose is extremely sensitive, and should be shared only with people who have access to the credit card that will be used on this account.

Your password must include: uppercase letters, lowercase letters, numbers, and non-alphabetic characters.

Once you have entered and confirmed your password, choose Continue (step 1 of 5).



Sign up for AWS

Create your password

It's you! Your email address has been successfully verified.

Your password provides you with sign in access to AWS, so it's important we get it right.

Root user password

Confirm root user password

aws
Explore Free Tier products with a new AWS account.
To learn more, visit aws.amazon.com/free.
Continue (step 1 of 5)
OR
Sign in to an existing AWS account

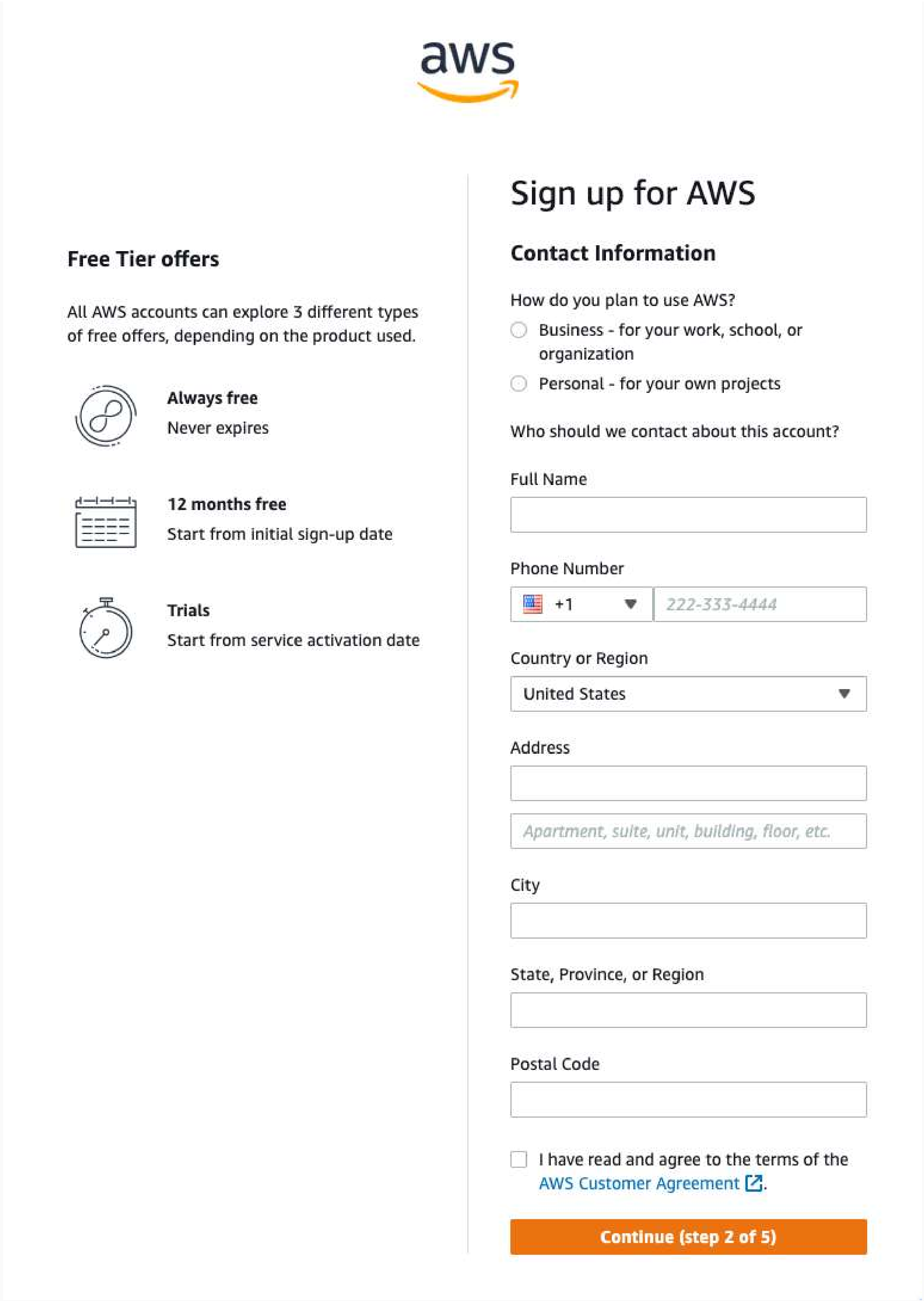
Add contact information

Now you need to add your contact information and select how you plan to use AWS.

In the next screen, choose between a business or personal account. There is no difference in account type or functionality, but there is a difference in the type of information required to open the account for billing purposes. For a business account, choose a phone number that is tied to the business and can be reached if the person setting up the account is not available.

Once you have selected the account type, fill out the the contact information about the account. Save these details in a safe place. If you ever lose access to the email or your two-factor authentication device, AWS Support can use these details to confirm your identity.

At the end of this form, please read through the terms of the AWS Customer Agreement and select the checkbox to accept them. Choose Continue (step 2 of 5) to proceed to the next screen.



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

Sign up for AWS

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

+1 ▼ *222-333-4444*

Country or Region

United States ▼

Address

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

City

State, Province, or Region

Postal Code

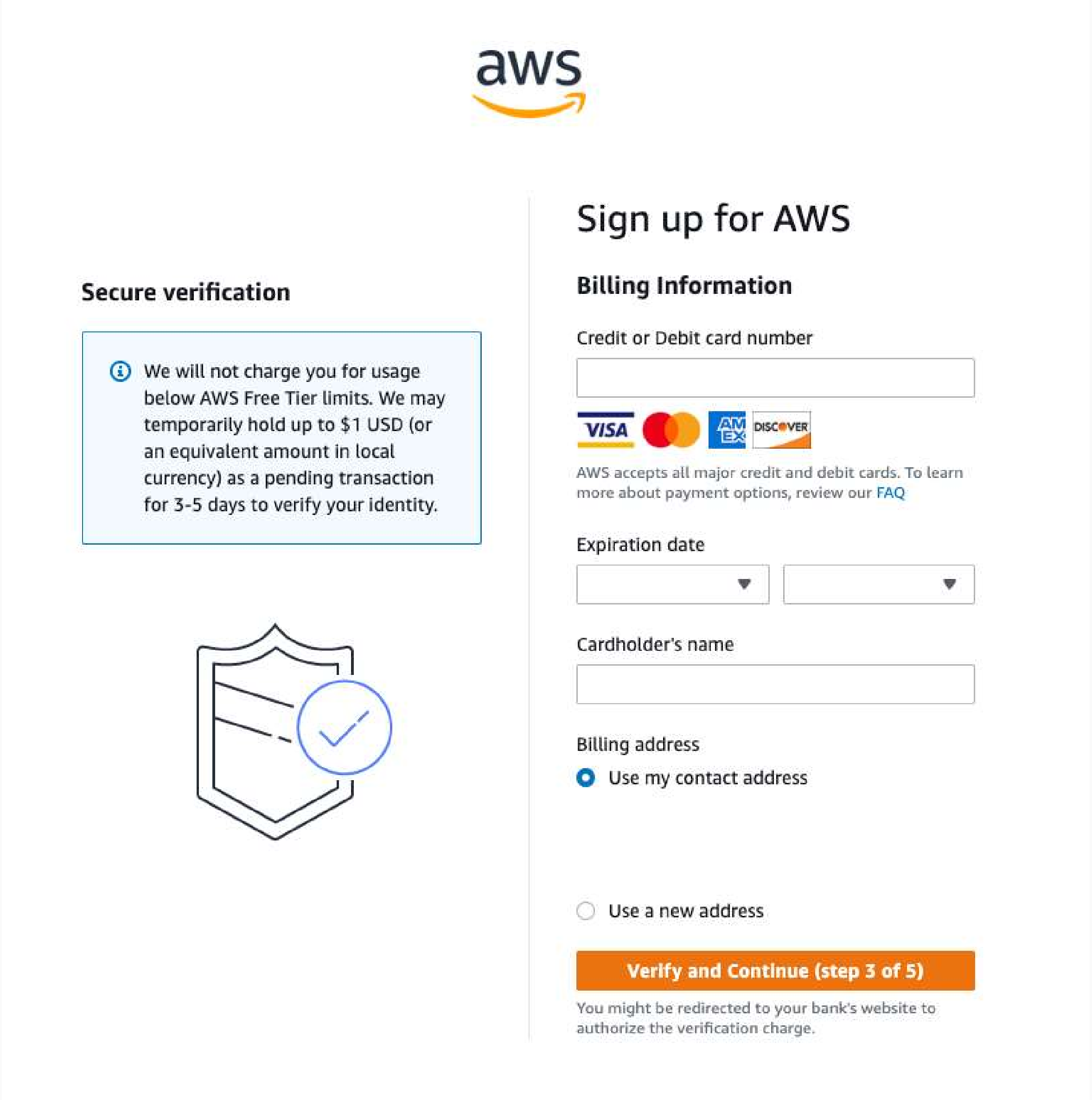
□ I have read and agree to the terms of the AWS Customer Agreement.

Add a payment method

In the following screen, add your preferred credit or debit card to use for payment.

A small hold will be placed on the card, so the address must match what your financial institution has on file for you or your business.

Once you're ready, choose Verify and Continue (step 3 of 5) to proceed.



Sign up for AWS

Secure verification

We will not charge you for usage below AWS Free Tier limits. We may temporarily hold up to $1 USD (or an equivalent amount in local currency) 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

Cardholder's name

Billing address

● Use my contact address

○ Use a new address

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

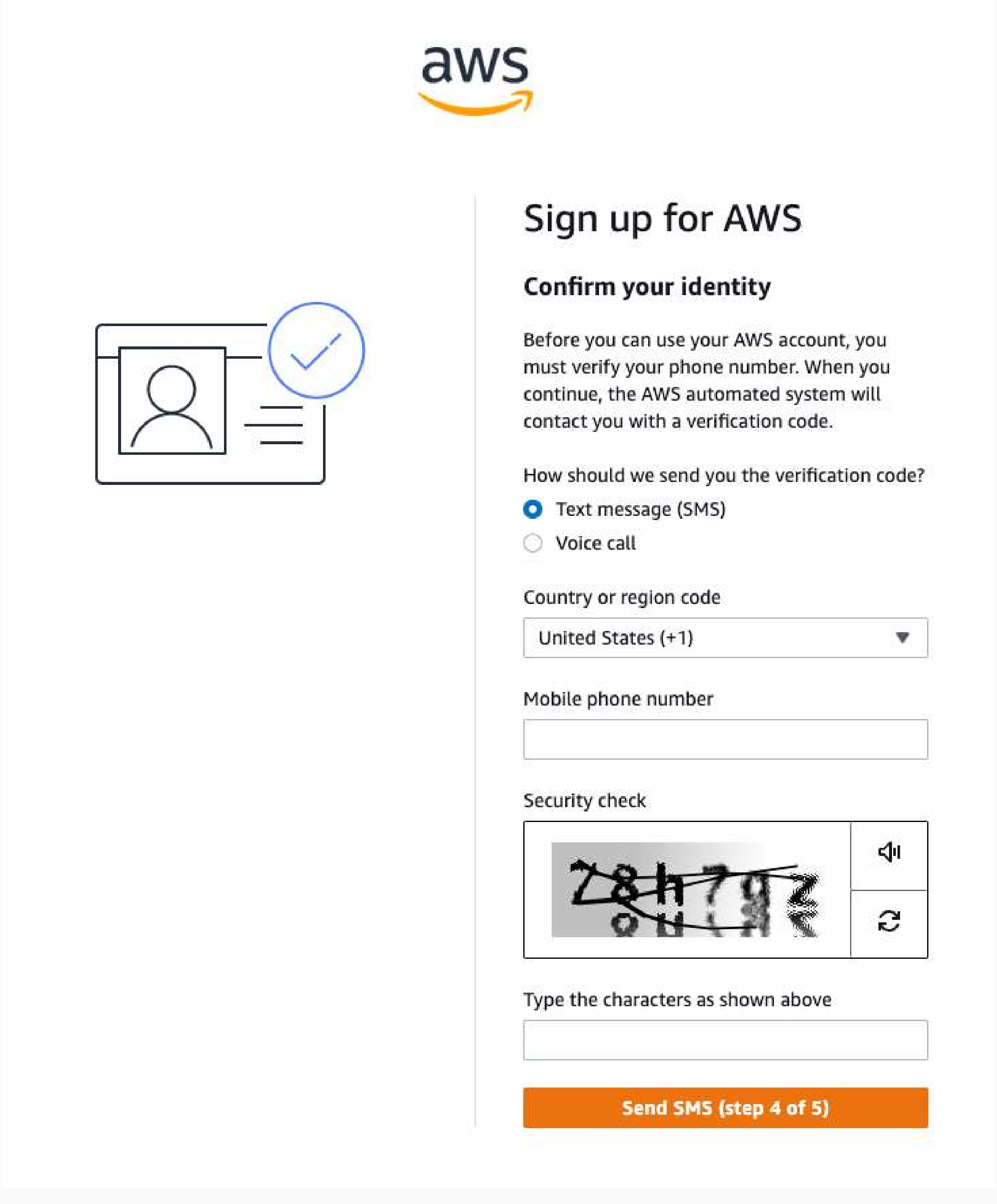
Confirm your identity

Now you need to verify your account.

You can verify your account either through a text message (SMS) or a phone call on the number you are associating with this account.

For the text message (SMS) option, you will be sent a numeric code to enter on the next screen after you choose Send SMS. For the Voice call option, you will be shown a code on the screen to enter after being prompted by the automated voice verification system.

Enter the code as appropriate for your verification choice, then choose Continue to proceed to the final step.



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

United States (+1) ▼

Mobile phone number

Security check

Type the characters as shown above

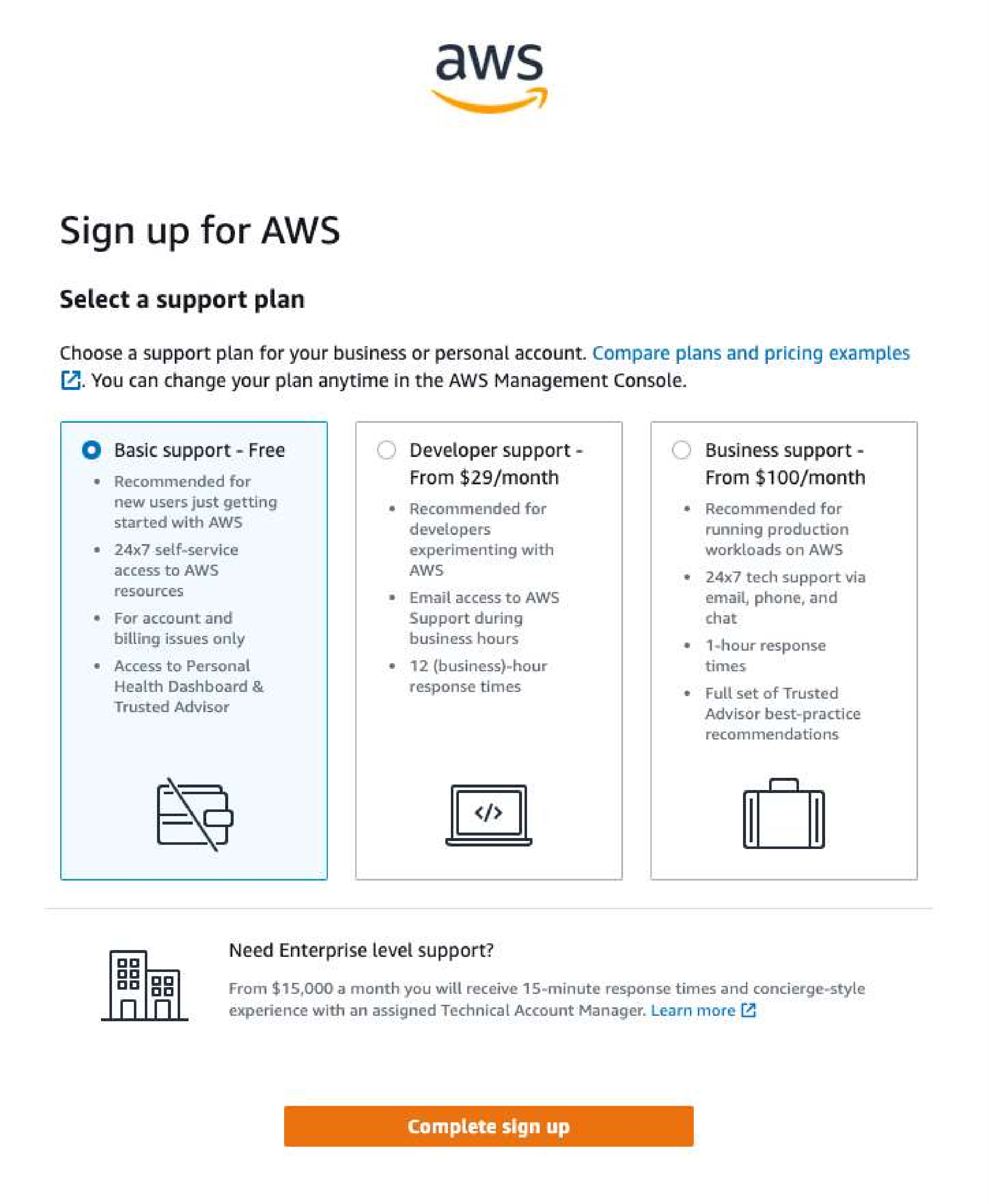
Select a support plan

For the last step, choose a support plan for your AWS account.

You have three options for support plans. The default option is called Basic Support and is free of charge. If you are not sure, select Basic Support. You can always change support tiers at a later date.

To see the full list of differences between the tiers, see Compare AWS Support Plans.

To finish creating your account, choose Complete sign up.



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

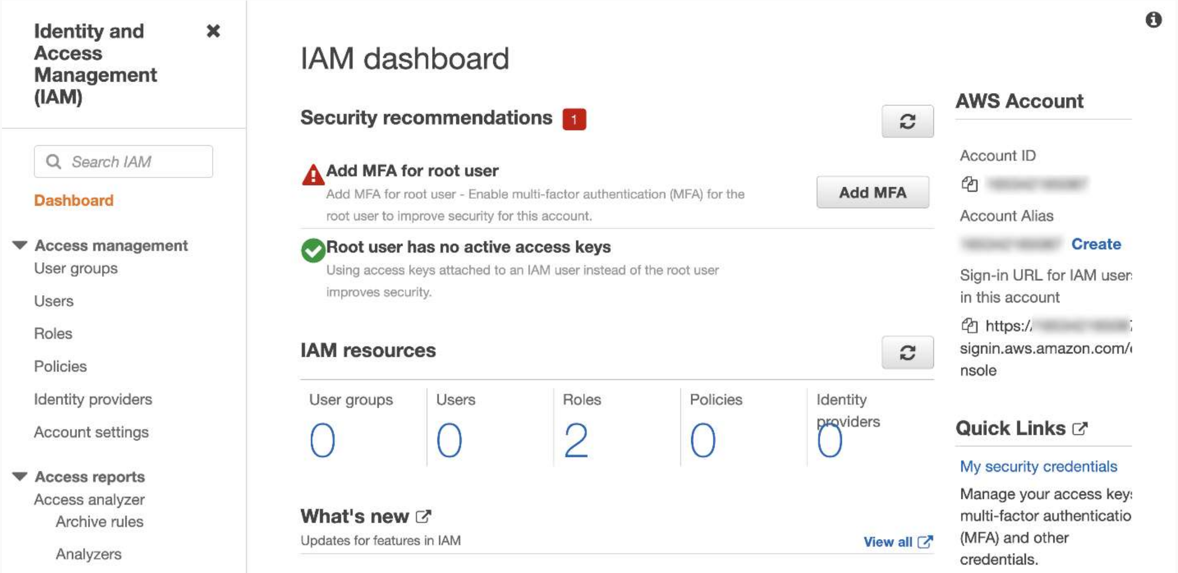
Module 2

Secure the root user

Let's start by securing the root user. To do that, we'll use the AWS IAM service. See What is IAM? for more context.

When you're ready to start, log in to your newly created AWS account using the credentials created in the previous module. Once your login is successful, you will be redirected to the AWS Management Console.

In the search bar, enter IAM, and then select IAM. You will be redirected to the IAM dashboard. Under Security recommendations, there will be a prompt to secure the root user with Multi-factor authentication (MFA). Choose Add MFA, then Activate MFA on the next screen.



Identity and Access Management (IAM) ✖

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access analyzer

Archive rules

Analyzers

IAM dashboard

Security recommendations 1

Add MFA for root user

Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

Add MFA

✓ Root user has no active access keys

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

IAM resources

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

What's new

Updates for features in IAM

View all

AWS Account

Account ID

[redacted]

Account Alias

[redacted] Create

Sign-in URL for IAM users in this account

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

Quick Links

My security credentials

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

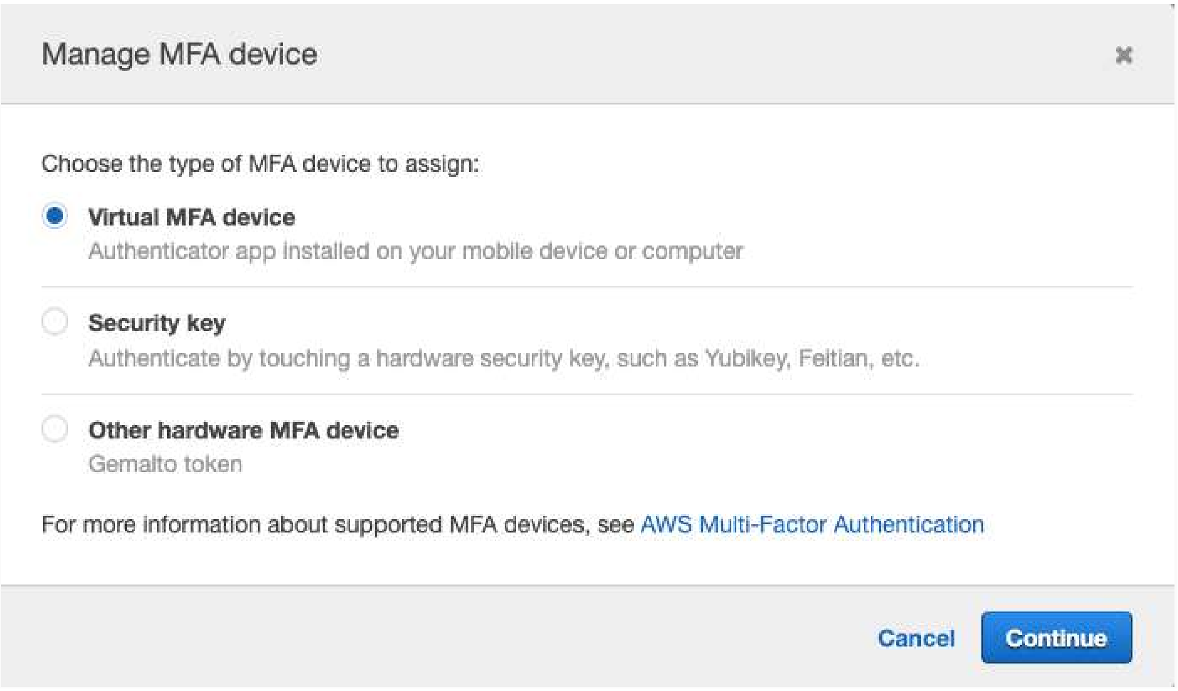
Now, you need to choose between the available MFA options:

- Virtual MFA device
- Security key
- Other hardware MFA device

To see an overview of the options, see Multi-Factor Authentication.

If you're not sure which option you should pick, choose Virtual MFA device and install one of the apps available for your mobile phone. Take note of how the authenticator app you chose handles backups, because you might need to set up the app on a different phone at a later date.

Once you have selected the type of MFA device, choose Continue. The following screen provides the steps required to connect the device to your account. When everything is ready, choose Assign MFA. Your root user is now secure.



Manage MFA device

Choose the type of MFA device to assign:

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

○ **Security key**
Authenticate by touching a hardware security key, such as Yubikey, Feitian, etc.

○ **Other hardware MFA device**
Gemalto token

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

Set up additional users

It is considered a security best practice to not use your root account for day-to-day use. We recommend that you create separate users for specific roles and functions.

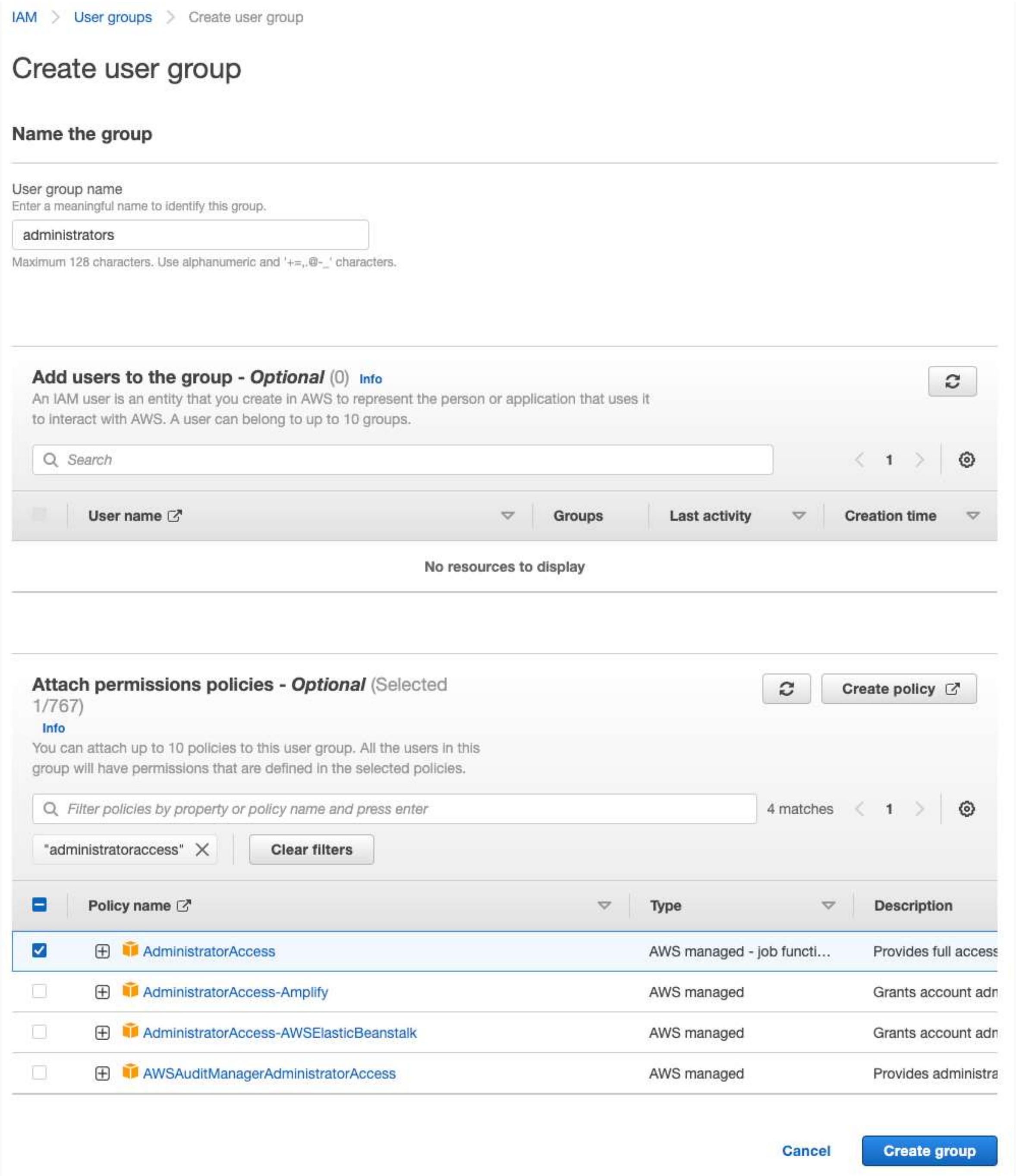
Again, we'll use the IAM service to create users and assign them permissions. IAM users are not separate accounts; they are users within your account. Each user can have their own password for access to the [AWS Management Console.](https://) You can also create an individual access key for each user so that they can make programmatic requests to work with resources in your account.

Before setting up a new user, we'll create a user group.

User groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users. For example, you could have a user group called Admins and give that user group typical administrator permissions. Any user in that user group automatically has Admins group permissions. If a new user joins your organization and needs administrator privileges, you can assign the appropriate permissions by adding the user to the Admins user group. If a person changes jobs in your organization, instead of editing that user's permissions, you can remove them from the old user groups and add them to the appropriate new user groups.

For this example, we are creating a group of users with administrator access.

In the IAM console, choose User groups in the left-side navigation and then choose Create group. Enter the User group name (in this case, *administrators*), then scroll down to the Attach permissions policies section. Search for "AdministratorAccess", then select the box next to the policy with the name "AdministratorAccess", scroll down, and choose Create group.



IAM > User groups > Create user group

Create user group

Name the group

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

administrators

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

Add users to the group - *Optional* (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. A user can belong to up to 10 groups.

Search

☐	User name	Groups	Last activity	Creation time

No resources to display

Attach permissions policies - *Optional* (Selected 1/767)
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.

Filter policies by property or policy name and press enter

4 matches

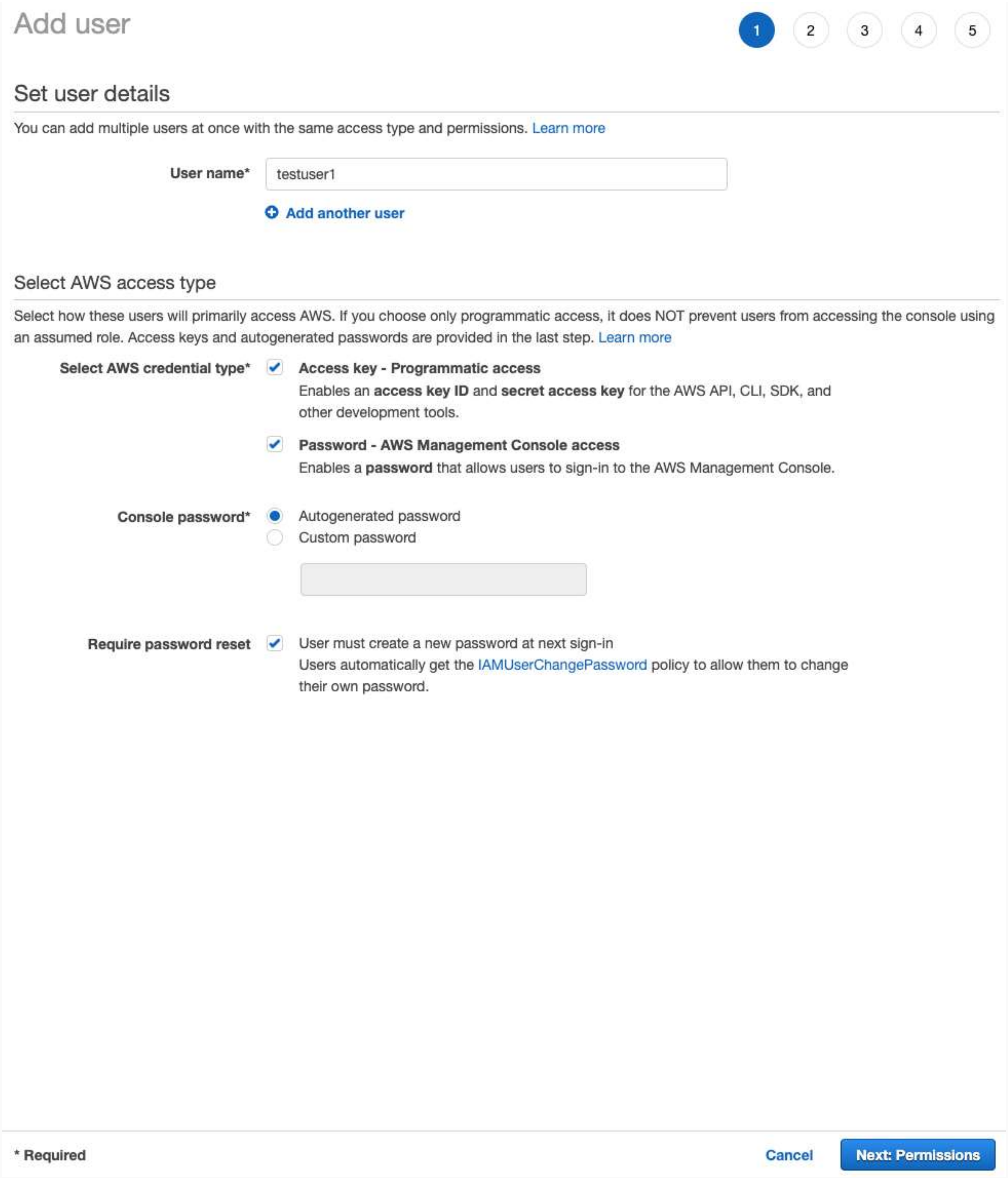
"administratoraccess" ✕ Clear filters

▬	Policy name	Type	Description
☑	⊞ AdministratorAccess	AWS managed - job functi…	Provides full access
☐	⊞ AdministratorAccess-Amplify	AWS managed	Grants account adı
☐	⊞ AdministratorAccess-AWSElasticBeanstalk	AWS managed	Grants account adı
☐	⊞ AWSAuditManagerAdministratorAccess	AWS managed	Provides administra

Now we need to create users to add to our group.

In IAM, select Users in the left-side navigation bar and then choose Add users. Enter a User name and select an AWS access type for that user. Programmatic access creates an access key ID and secret pair for use with the AWS CLI, CDK, and other applications. AWS Management Console access allows the user to log in to the AWS console for this account.

For the purposes of this tutorial, select both options. Then, choose Next: Permissions.



Set user details

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

User name* testuser1

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. Learn more

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

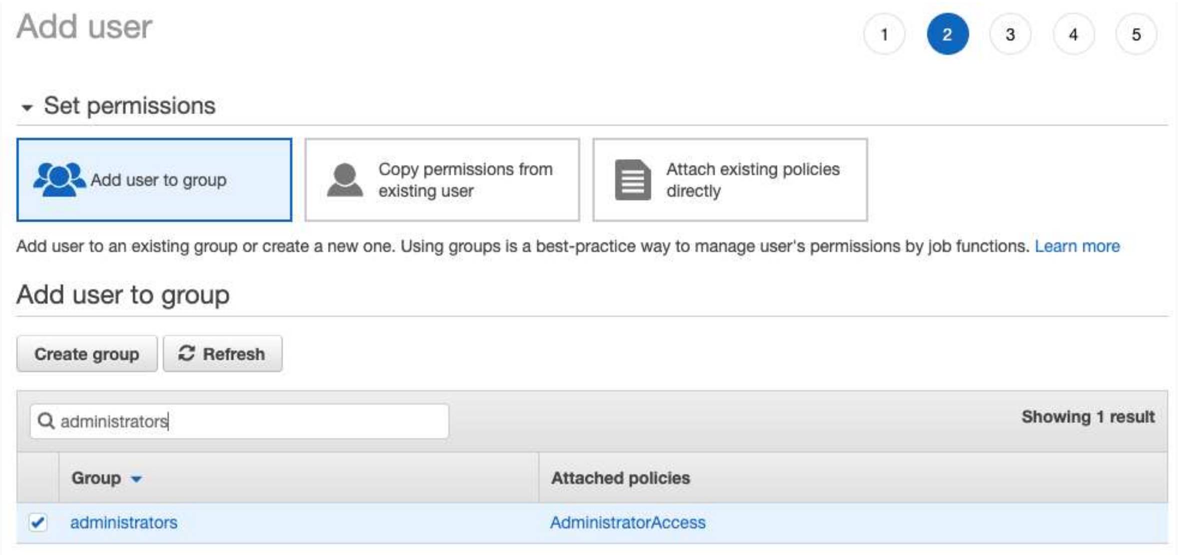
☑ **Password - AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password* ● Autogenerated password
○ Custom 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

In the following screen, add the user to the administrators group we just created and choose Next: Tags.


Add user
1
2
3
4
5
Set permissions
Add user to group
Copy permissions from existing user
Attach existing policies directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Add user to group

administrators

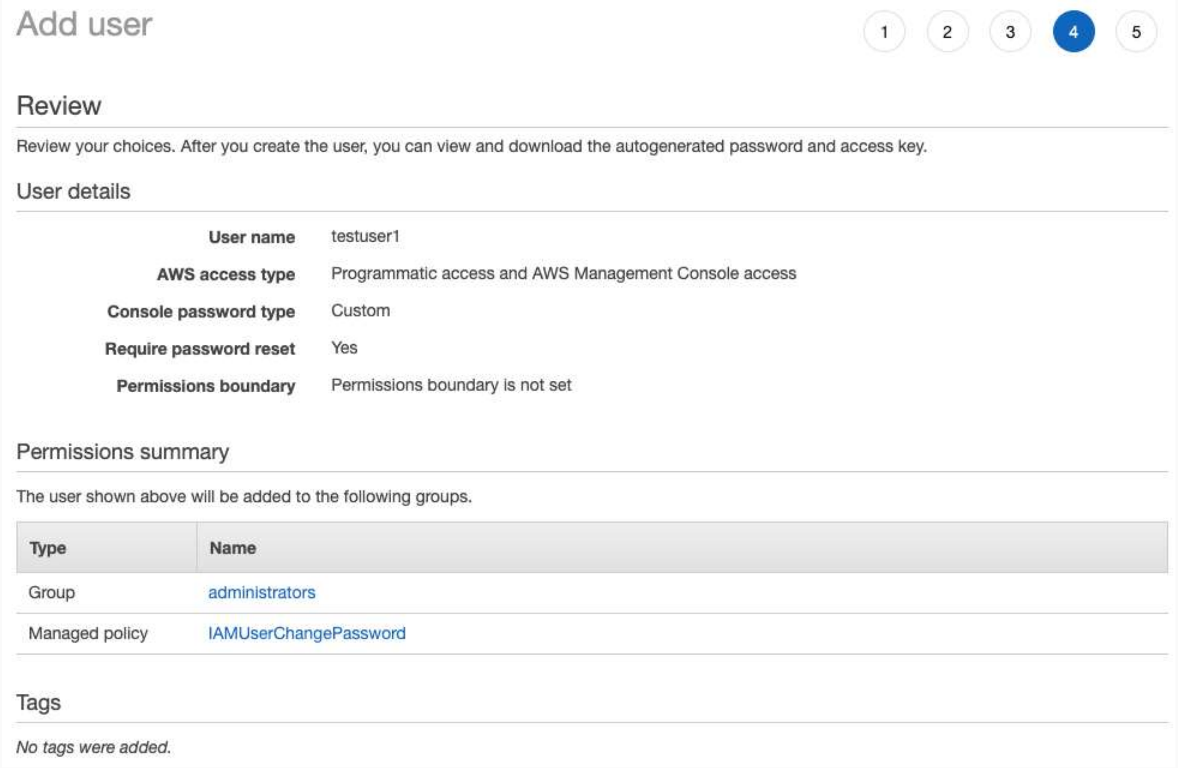
Showing 1 result

	Group	Attached policies
☑	administrators	AdministratorAccess

Tags are useful to search for resources across services, or to add metadata like *department.* For our use case, choose Next: Review without adding a tag.

You can now review the values set for the user you are creating before actually creating it.

You will notice there is an additional managed policy called "IAMUserChangePassword" added beneath the "administrators" one we created. This is added to any user where the option to force them to change their password was selected as not all IAM policies may have the required permissions in them.



Review

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

User details

User name	testuser1
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	administrators
Managed policy	IAMUserChangePassword

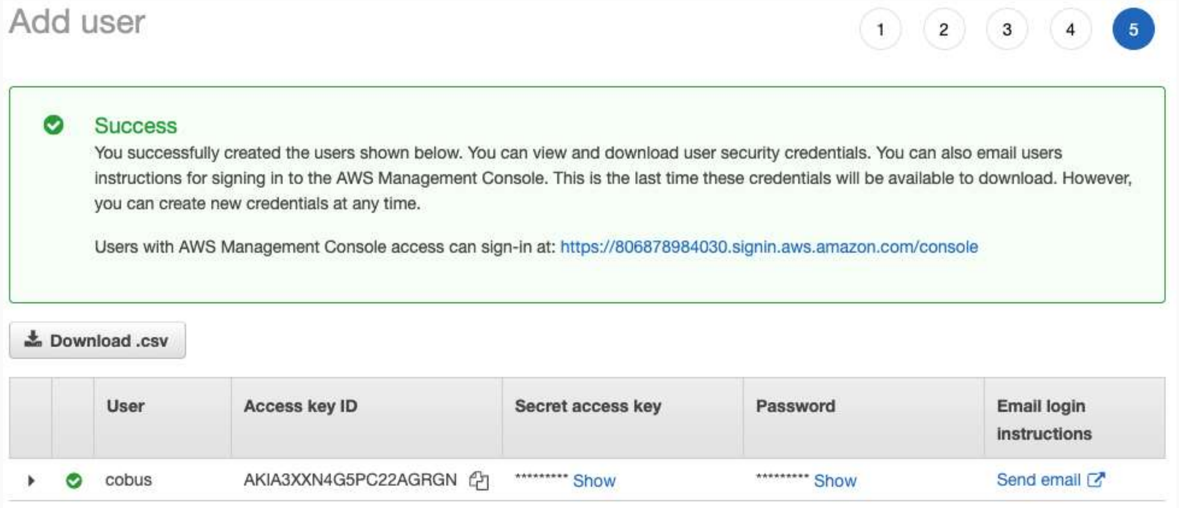
Tags

No tags were added.

Choose Create user to create the user. You will see the confirmation screen for the user, but do not choose the Close button yet.

The auto-generated password and the secret access key for API access can only be accessed from this screen once. Write down the Access key ID, Secret access key, and Password; we will use them in the next module of this tutorial. You can also choose Download .csv to get a copy of the information. Afterwards, choose Close.

For additional information, see IAM users.



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://806878984030.signin.aws.amazon.com/console

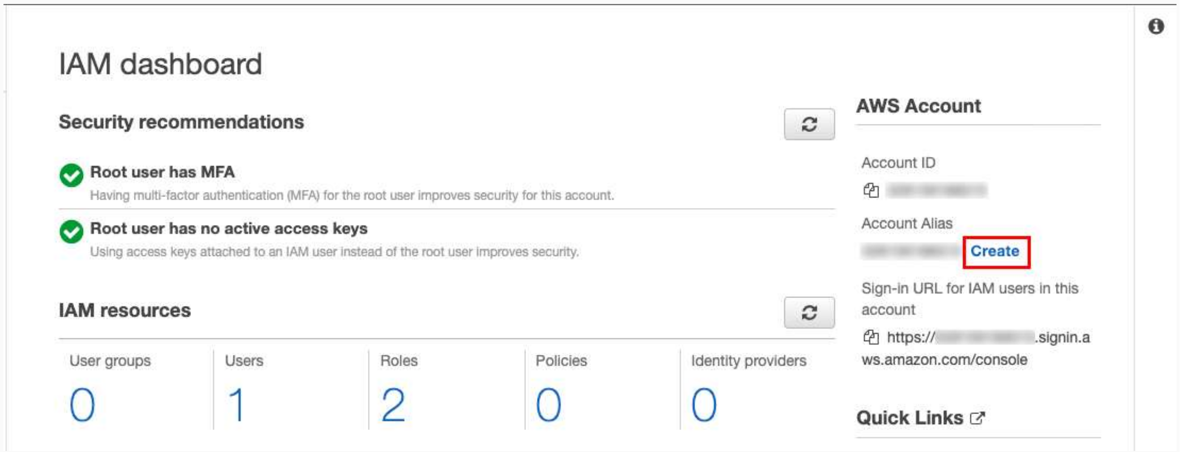
		User	Access key ID	Secret access key	Password	Email login instructions
▸	✓	cobus	AKIA3XXN4G5PC22AGRGN	********* Show	********* Show	Send email

Set account alias and enable regions

While still in IAM, we'll complete a few more steps to make your account easier to manage.

First, let's set an alias for your account, which should be easier to remember than the 12-digit account ID.

To set it, select Dashboard in the left navigation bar, then choose Create under the AWS Account section in the right panel. You can now set an alias for your account. This alias needs to be globally unique across all AWS accounts, so your first choice may not be available.



Security recommendations

✓ Root user has MFA
Having multi-factor authentication (MFA) for the root user improves security for this account.

✓ Root user has no active access keys
Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

User groups	Users	Roles	Policies	Identity providers
0	1	2	0	0

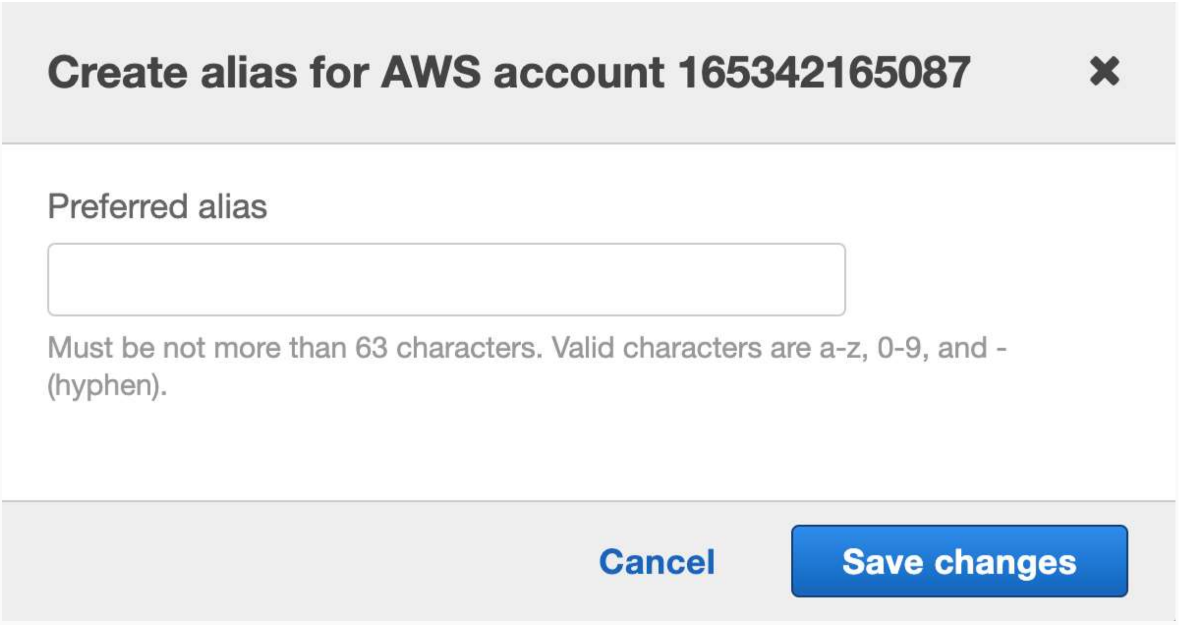
AWS Account

Account ID
[redacted]

Account Alias
[redacted] Create

Sign-in URL for IAM users in this account
https://[redacted].signin.aws.amazon.com/console

Once you set the alias, choose Save changes. Then, copy the URL generated for later use in this tutorial. It will have the format of https://<*your-text*>.signin.aws.amazon.com/console.



Create alias for AWS account 165342165087

Preferred alias

Must be not more than 63 characters. Valid characters are a-z, 0-9, and - (hyphen).

The last step that needs to be completed is to enable any Regions that you may need to use. This only applies to Regions launched after March 20, 2019. Currently, this includes:

- Africa (Cape Town)
- Asia Pacific (Hong Kong)
- Asia Pacific (Jakarta)
- Europe (Milan)
- Middle East (Bahrain)

Follow the instructions here if you need to enable any of these Regions.