What is IAM?

- AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources.
- With IAM, you can manage permissions that control which AWS resources users can access.
- You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources such as ec2 instances, s3 bucket, and DBs.
- IAM provides the infrastructure necessary to control authentication and authorization for your AWS accounts.
- IAM enables you to create and manage users, groups, and roles, each with their own permission and access policies.

Identities:

- When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account.
- This identity is called the AWS account root user and is accessed by signing in with the email address and password that you used to create the account.
- Use IAM to set up other identities in addition to your root user, such as administrators, analysts, and developers, and grant them access to the resources they need to succeed in their tasks.
- Authentication is the process of verifying your identity. You need to provide your login credentials to get authenticated to AWS console.

Access management:

- After a user is set up in IAM, they use their sign-in credentials to authenticate with AWS.
- Once you are authenticated, authorization determines what actions you're allowed to perform or what resources you're allowed to access after your identity has been verified.

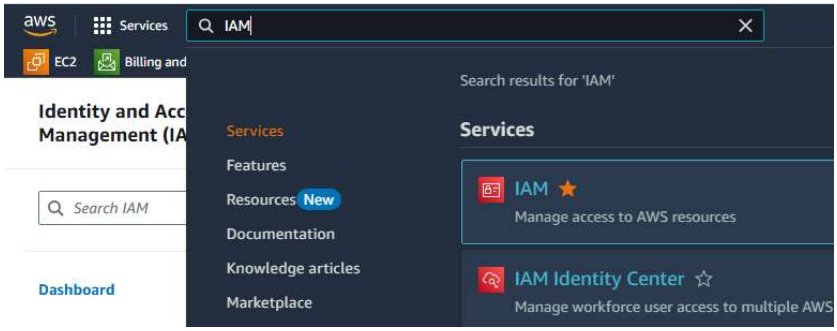
Why use IAM?

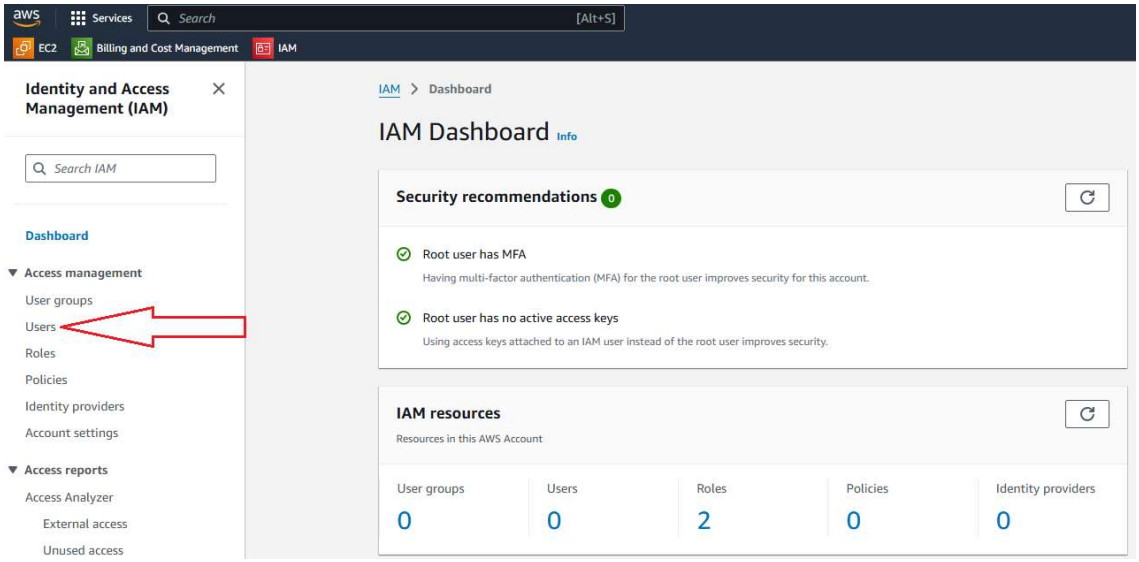
- Use AWS Identity and Access Management (IAM) to manage and scale workload and workforce access securely supporting your agility and innovation in AWS.
- It is not a good practice to perform all the activities by using root user. So, we should create IAM user.

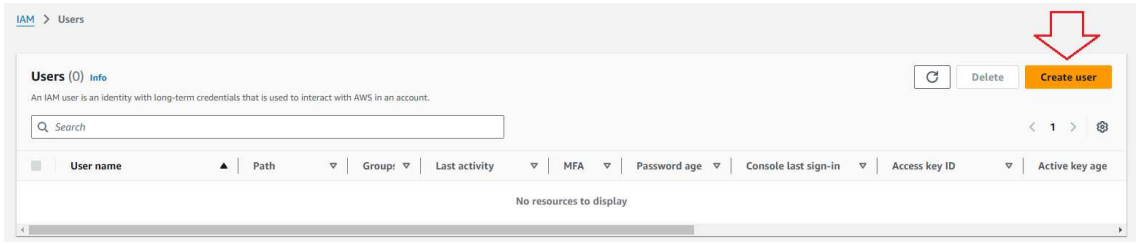
IAM Groups:

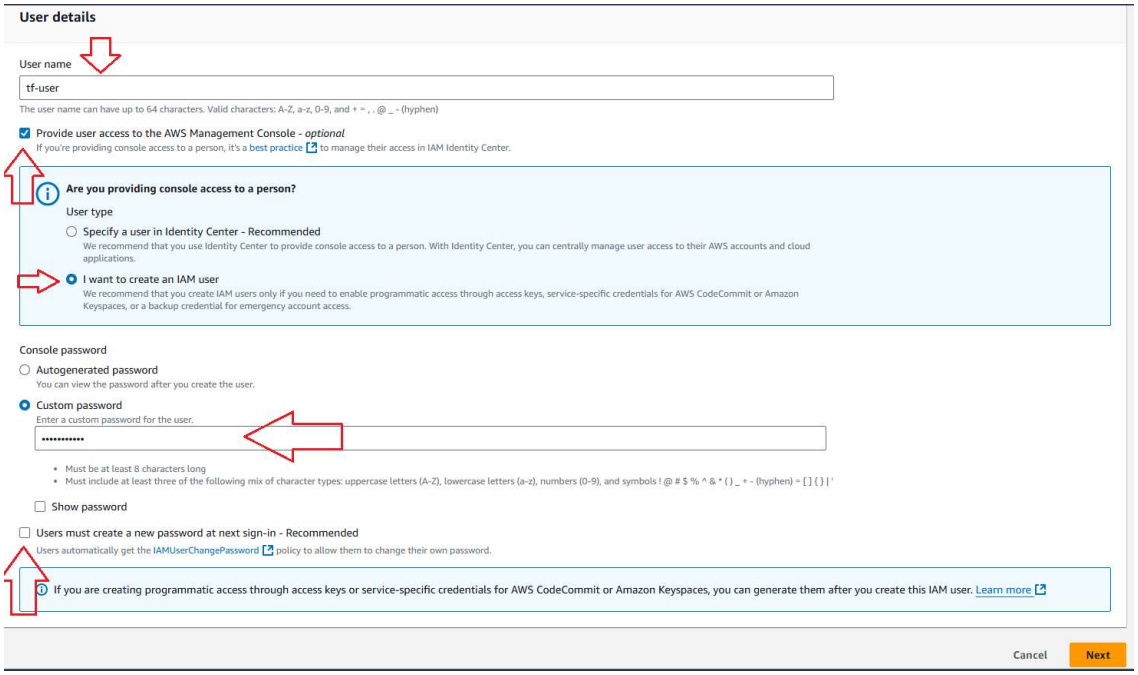
In AWS IAM, "groups" are collections of IAM users. Groups allow you to manage permissions for multiple users collectively, rather than individually assigning permissions for each individual user.

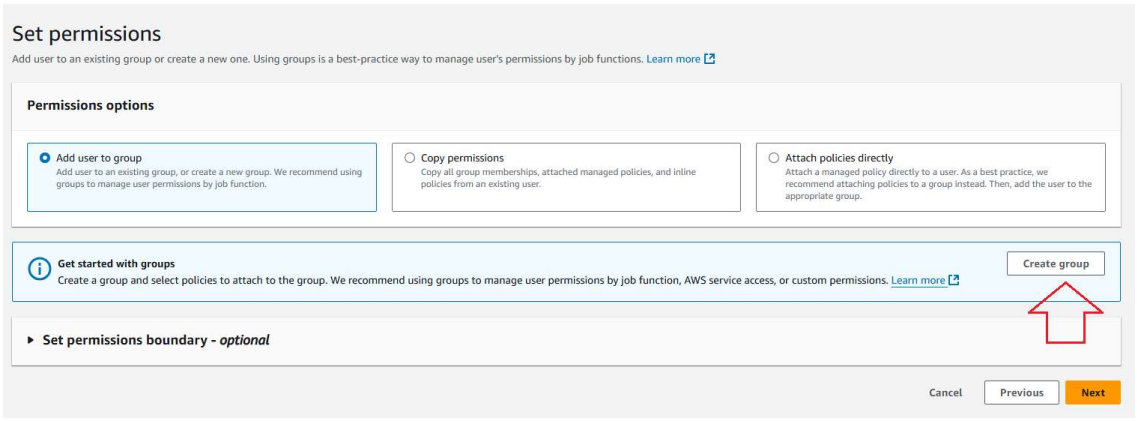
Login to AWS console as root user. Click on Services, and search for IAM. Click on IAM.

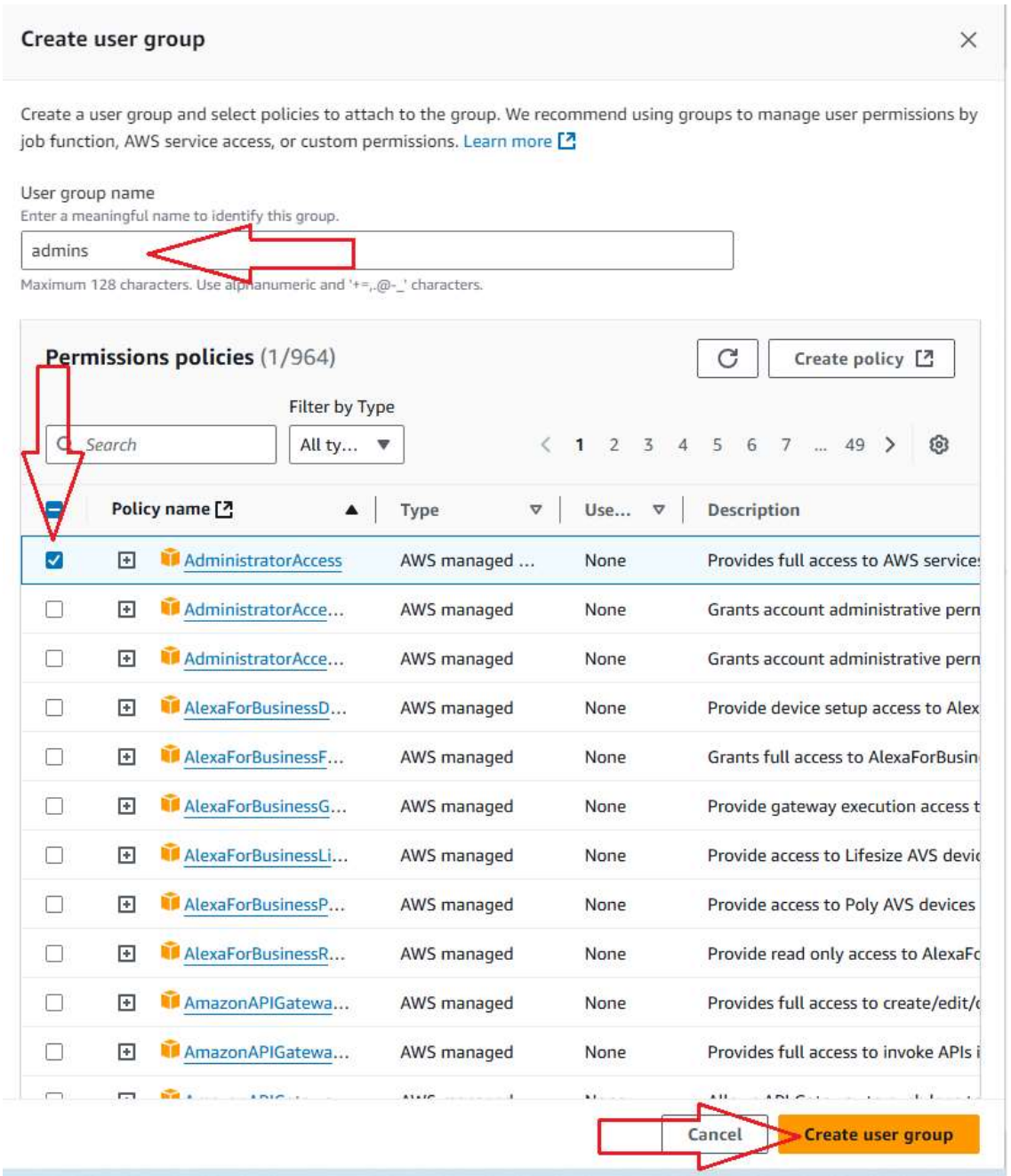


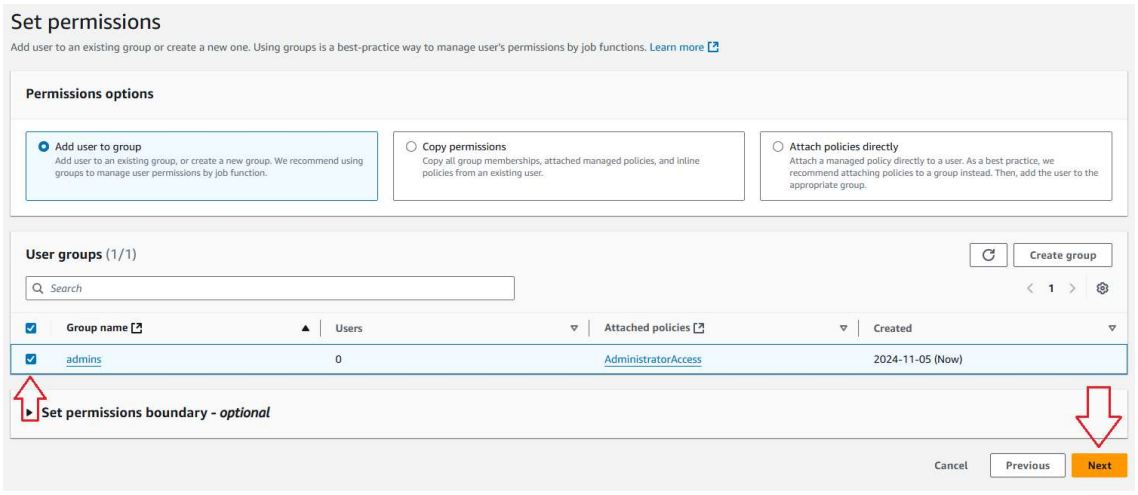

aws
Services
Search
[Alt+S]
EC2
Billing and Cost Management
IAM
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
IAM > Dashboard
IAM Dashboard Info
Security recommendations 0
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
Resources in this AWS Account
User groups 0
Users 0
Roles 2
Policies 0
Identity providers 0

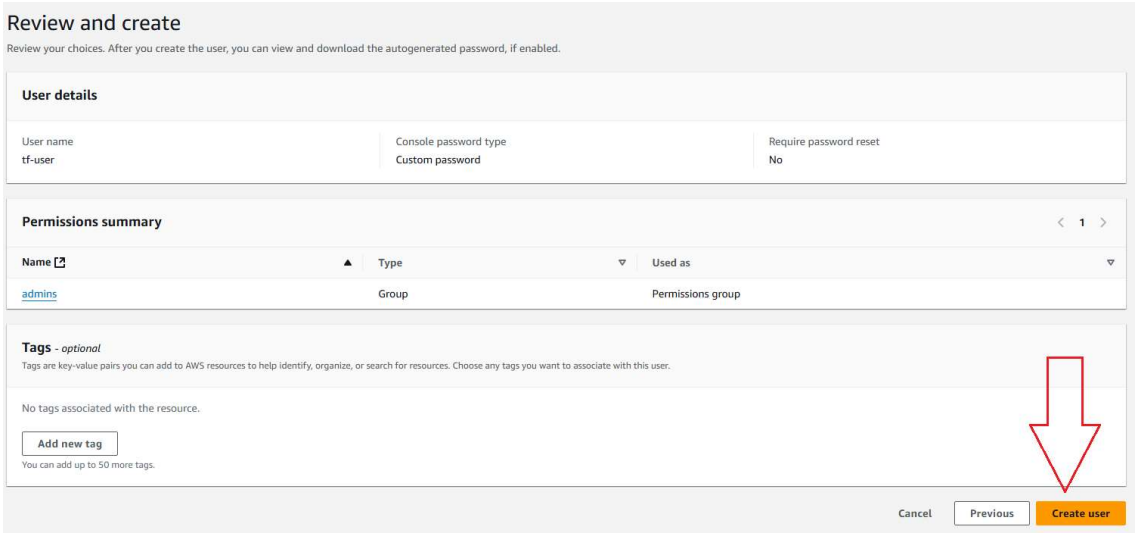

IAM > Users
Users (0) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Create user
Search
User name
Path
Groups
Last activity
MFA
Password age
Console last sign-in
Access key ID
Active key age
No resources to display

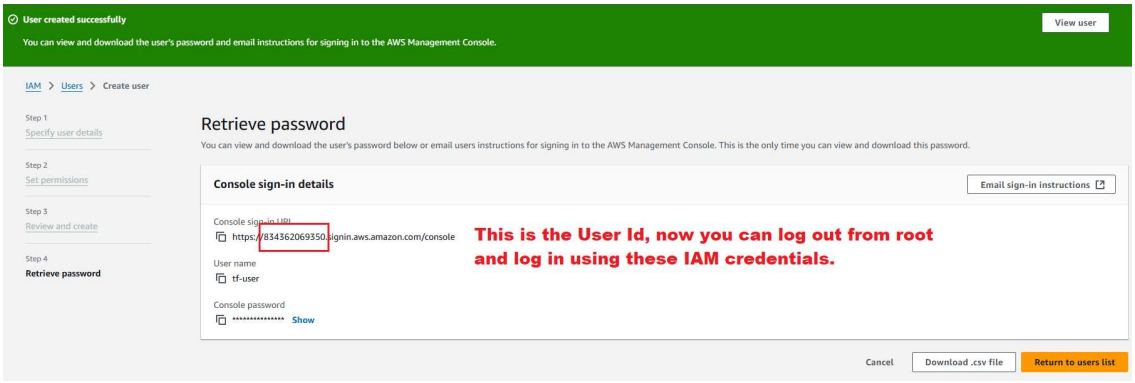

User details
User name
tf-user
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)
Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.
Are you providing console access to a person?
User type
Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.
I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.
Console password
Autogenerated password
You can view the password after you create the user.
Custom password
Enter a custom password for the user.
Must be at least 8 characters long
Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '
Show password
Users must create a new password at next sign-in - Recommended
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.
If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more
Cancel
Next

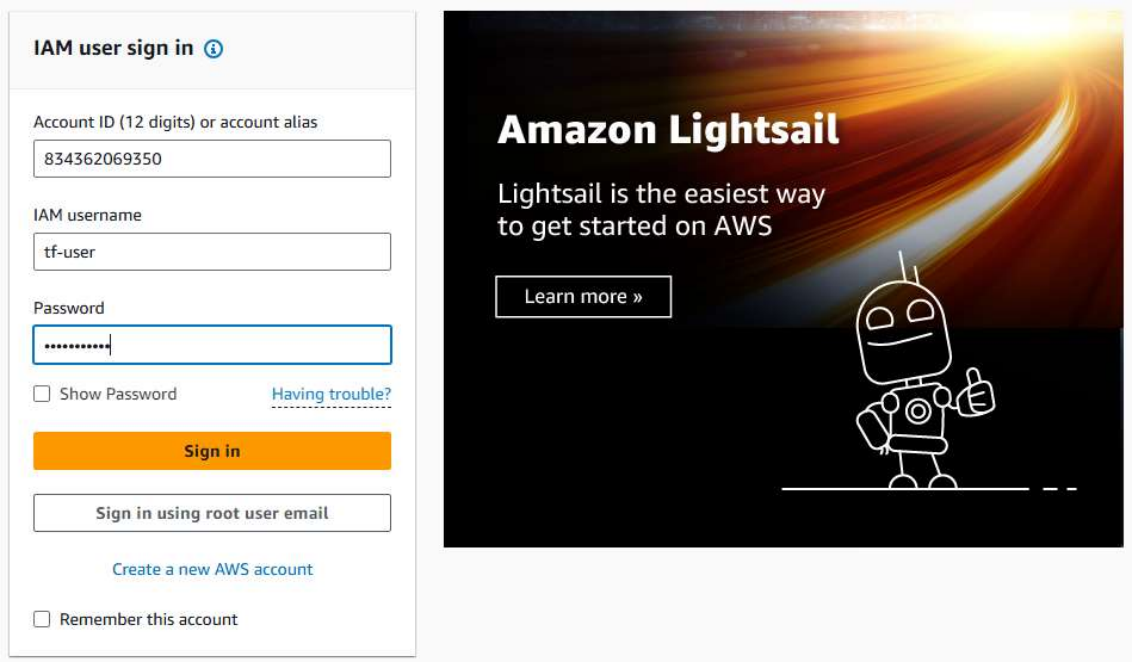

Set permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more
Permissions options
Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.
Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.
Get started with groups
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. Learn more
Create group
Set permissions boundary - optional
Cancel
Previous
Next

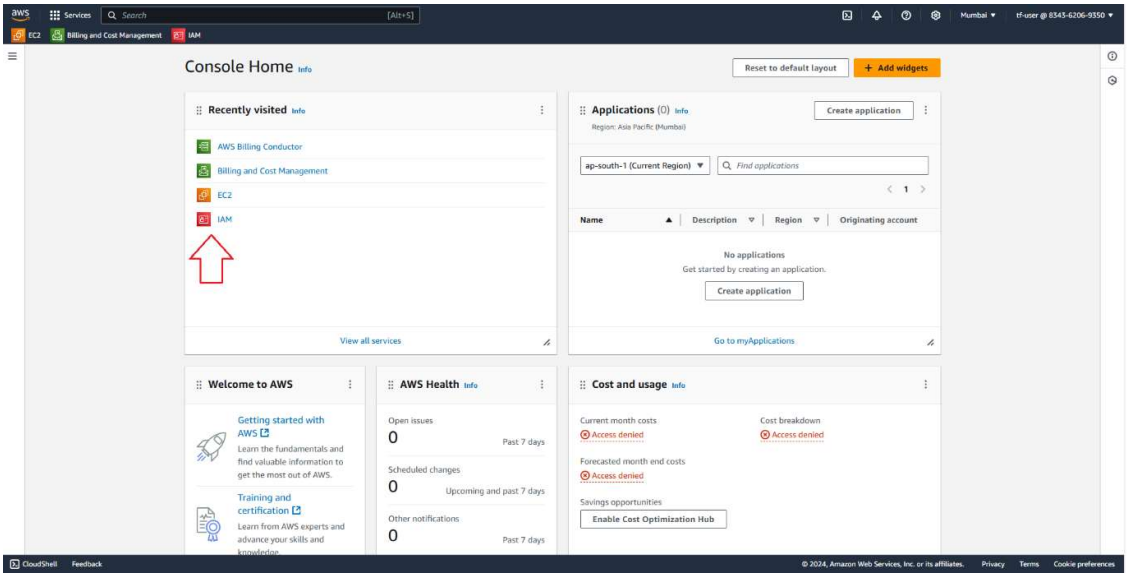

Create user group
Create a user group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. Learn more
User group name
Enter a meaningful name to identify this group.
admins
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Permissions policies (1/964)
Create policy
Filter by Type
Search
All ty...
1 2 3 4 5 6 7 ... 49
Policy name
Type
Use...
Description
AdministratorAccess
AWS managed ...
None
Provides full access to AWS service
AdministratorAcce...
AWS managed
None
Grants account administrative perm
AdministratorAcce...
AWS managed
None
Grants account administrative perm
AlexaForBusinessD...
AWS managed
None
Provide device setup access to Alex
AlexaForBusinessF...
AWS managed
None
Grants full access to AlexaForBusin
AlexaForBusinessG...
AWS managed
None
Provide gateway execution access t
AlexaForBusinessLi...
AWS managed
None
Provide access to Lifesize AVS devic
AlexaForBusinessP...
AWS managed
None
Provide access to Poly AVS devices
AlexaForBusinessR...
AWS managed
None
Provide read only access to AlexaFc
AmazonAPIGatewa...
AWS managed
None
Provides full access to create/edit/
AmazonAPIGatewa...
AWS managed
None
Provides full access to invoke APIs i
Cancel
Create user group

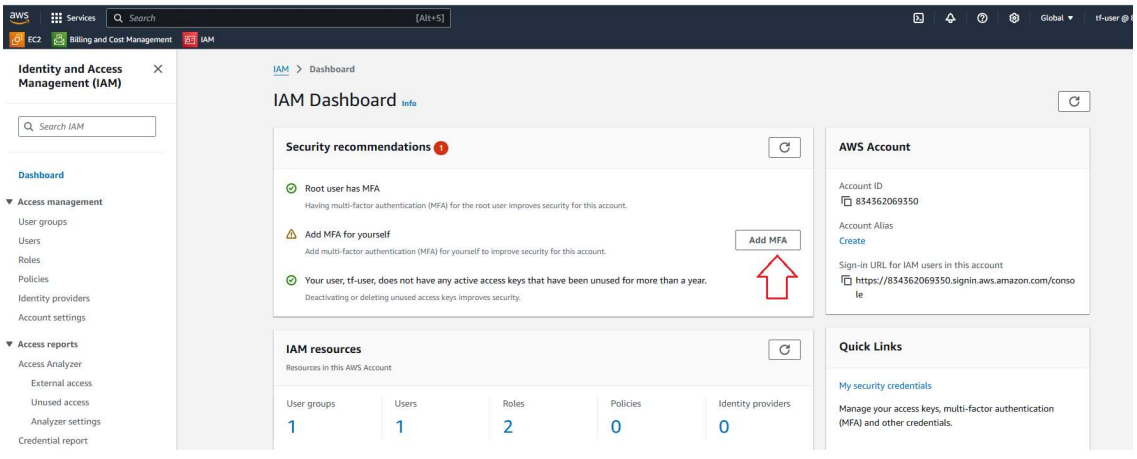

Set permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more
Permissions options
Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.
Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.
User groups (1/1)
Create group
Search
Group name
Users
Attached policies
Created
admins
0
AdministratorAccess
2024-11-05 (Now)
Set permissions boundary - optional
Cancel
Previous
Next


Review and create
Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.
User details
User name
tf-user
Console password type
Custom password
Require password reset
No
Permissions summary
Name
Type
Used as
admins
Group
Permissions group
Tags - optional
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.
No tags associated with the resource.
Add new tag
You can add up to 50 more tags.
Cancel
Previous
Create user


User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
View user
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Retrieve password
You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.
Console sign-in details
Email sign-in instructions
Console sign-in URL
https://834362069350.signin.aws.amazon.com/console
User name
tf-user
Console password
Show
This is the User Id, now you can log out from root and log in using these IAM credentials.
Cancel
Download .csv file
Return to users list


IAM user sign in
Account ID (12 digits) or account alias
834362069350
IAM username
tf-user
Password
Show Password
Having trouble?
Sign in
Sign in using root user email
Create a new AWS account
Remember this account
Amazon Lightsail
Lightsail is the easiest way to get started on AWS
Learn more »


Console Home
Reset to default layout
+ Add widgets
Recently visited
AWS Billing Conductor
Billing and Cost Management
EC2
IAM
Applications (0)
Create application
No applications
Get started by creating an application.
Create application
View all services
Go to myApplications
Welcome to AWS
Getting started with AWS
Training and certification
AWS Health
Open issues
0
Past 7 days
Scheduled changes
0
Upcoming and past 7 days
Other notifications
0
Past 7 days
Cost and usage
Current month costs
Access denied
Cost breakdown
Access denied
Forecasted month end costs
Access denied
Savings opportunities
Enable Cost Optimization Hub


Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
IAM > Dashboard
IAM Dashboard
Security recommendations 1
Root user has MFA
Having multi-factor authentication (MFA) for the root user improves security for this account.
Add MFA for yourself
Add multi-factor authentication (MFA) for yourself to improve security for this account.
Add MFA
Your user, tf-user, does not have any active access keys that have been unused for more than a year.
Deactivating or deleting unused access keys improves security.
AWS Account
Account ID
834362069350
Account Alias
Create
Sign-in URL for IAM users in this account
https://834362069350.signin.aws.amazon.com/console
IAM resources
Resources in this AWS Account
User groups
1
Users
1
Roles
2
Policies
0
Identity providers
0
Quick Links
My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.

Select MFA device Info

MFA device name

Device name
This name will be used within the identifying ARN for this device.

Samsung

Maximum 64 characters. Use alphanumeric and '+ = , . @ - _' characters.

MFA device

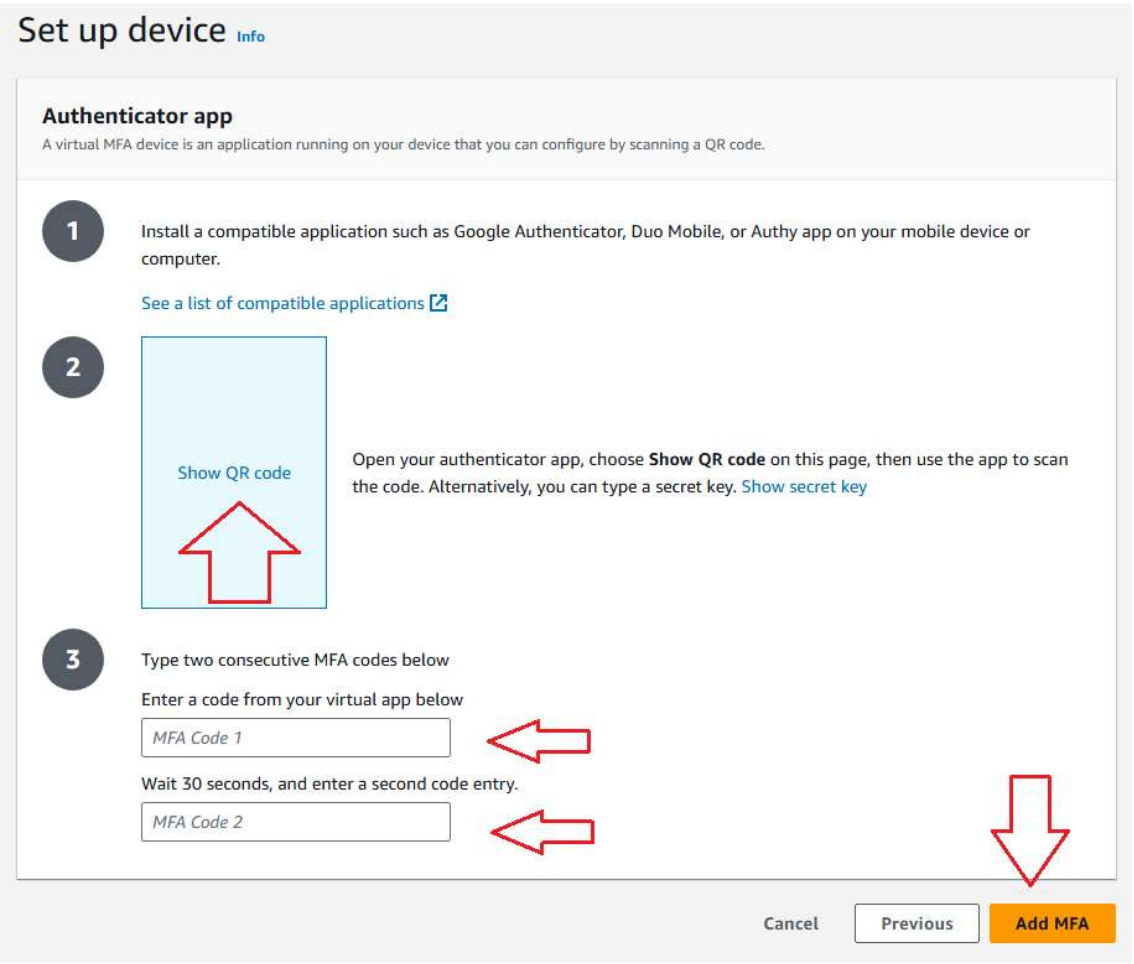
Device options
In addition to username and password, you will use this device to authenticate into your account.

Passkey or security key
Authenticate using your fingerprint, face, or screen lock. Create a passkey on this device or use another device, like a FIDO2 security key.

Authenticator app
Authenticate using a code generated by an app installed on your mobile device or computer.

Hardware TOTP token
Authenticate using a code generated by Hardware TOTP token or other hardware devices.

Cancel Next



Now come to IAM Dashboard, it should look like: