Creating an AWS IAM Admin User

Background: Why Create an IAM Admin User?

IAM (Identity and Access Management) should be the first AWS service used after creating an AWS account. After creating an AWS account, the first thing we can do is to create IAM user.

We use IAM user instead of AWS root user account for daily activity. Why using AWS root user for daily use is not advised ?

We **should not** use the **AWS root user** for daily tasks due to **security and risk management** reasons. Here's why:

Risks of Using the Root User Daily

1. **Unrestricted Access** – The root user has full permissions over everything, including billing, security settings, and account closure. If compromised, it can lead to a **total account takeover**.
2. **No Fine-Grained Access Control** – The root user cannot have policies or roles assigned to limit actions, making it impossible to enforce the **Principle of Least Privilege (PoLP)**.
3. **Prime Target for Attackers** – Hackers often target root credentials, and if leaked, the entire AWS account is at risk.
4. **No Action Tracking** – AWS **CloudTrail** cannot differentiate between different users if everything is done under the root user. Using IAM users ensures better accountability.
5. **Difficult to Rotate Credentials** – Since the root user is tied to the AWS account itself, changing credentials is a high-risk action.

IAM User:

- An IAM user represents an individual or entity that interacts with cloud resources.
- It's a way to give specific permissions to a person or application, allowing them to perform certain actions within the cloud environment.

IAM user with Admin policy :

Instead of using root user for daily activity, we create IAM user and attach the `AdministratorAccess` policy. This policy is one level below root user. The user with admin permission can do nearly everything except modify or close the AWS account. It cannot acces billing unless explicitly granted `AWSBillingAccountAccess` policy, an IAM user can view and modify billing settings.and account-related settings.

Root User vs IAM Admin User

Feature	Root User	IAM Admin User
Access	Full, unrestricted access	Full access, but slightly limited
Usage	Used only for account setup & security tasks	Used for daily AWS management
Account-wide settings	Can modify billing, close account	Cannot modify billing, close account
Security Risk	High (should not be used regularly)	More secure with controlled access
MFA Protection	Strongly recommended	Should always be enabled
Best Practice	Use sparingly & secure credentials	Use this instead of root user for admin tasks

User management best practice:

we don’t attach the policy directly to user but we create an admin-group with the policy. This way, if the user leave the organization, new user can be the new admin with same permission. If we assign permission to every user manually, it has risk to be inconsistent. This practice also applied to other task or responsibility.

Prerequisites

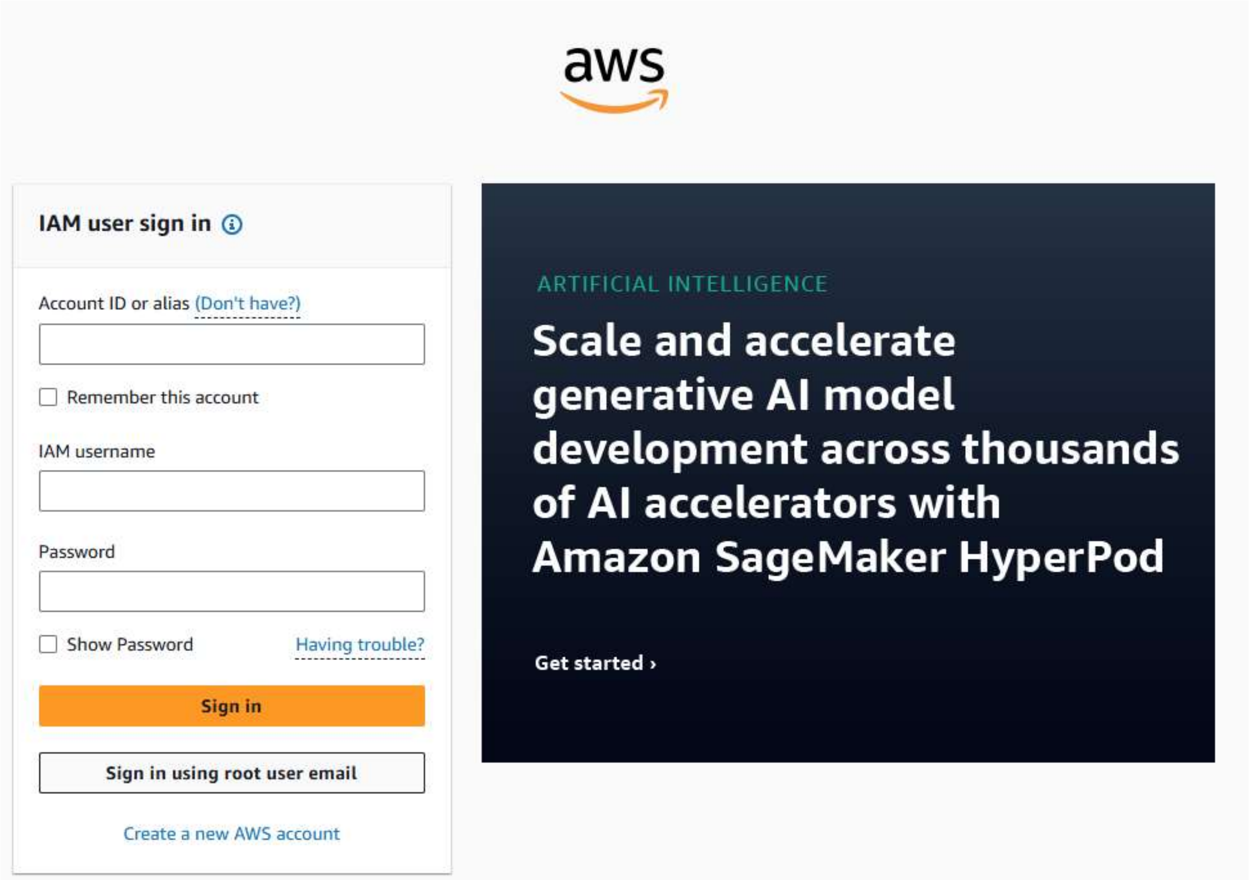
Before creating an IAM Admin User, ensure:

- You have **AWS root user access** (one-time setup).
- You are signed into the **AWS Management Console**.

Steps to Create an IAM Admin User

Step 1: Go to the AWS IAM Console

1. Sign in to the **AWS Management Console with root user email**
2. Navigate to **IAM service** from service bar or recently visited on home console
3. In the left panel, click **Users**.
4. Click **Add Users**.



IAM user sign in

Account ID or alias (Don't have?)

□ Remember this account

IAM username

Password

□ Show Password Having trouble?

Sign in

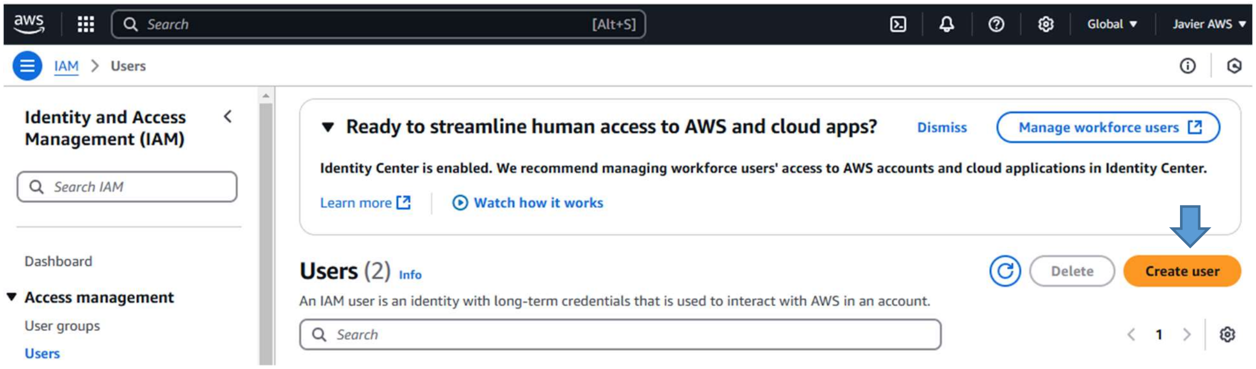
Sign in using root user email

Create a new AWS account

ARTIFICIAL INTELLIGENCE

Scale and accelerate generative AI model development across thousands of AI accelerators with Amazon SageMaker HyperPod

Get started ›



Search [Alt+S] Global ▼ Javier AWS ▼

IAM > Users

Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups

Users

▼ Ready to streamline human access to AWS and cloud apps? Dismiss Manage workforce users

Identity Center is enabled. We recommend managing workforce users' access to AWS accounts and cloud applications in Identity Center.

Learn more | Watch how it works

Users (2) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

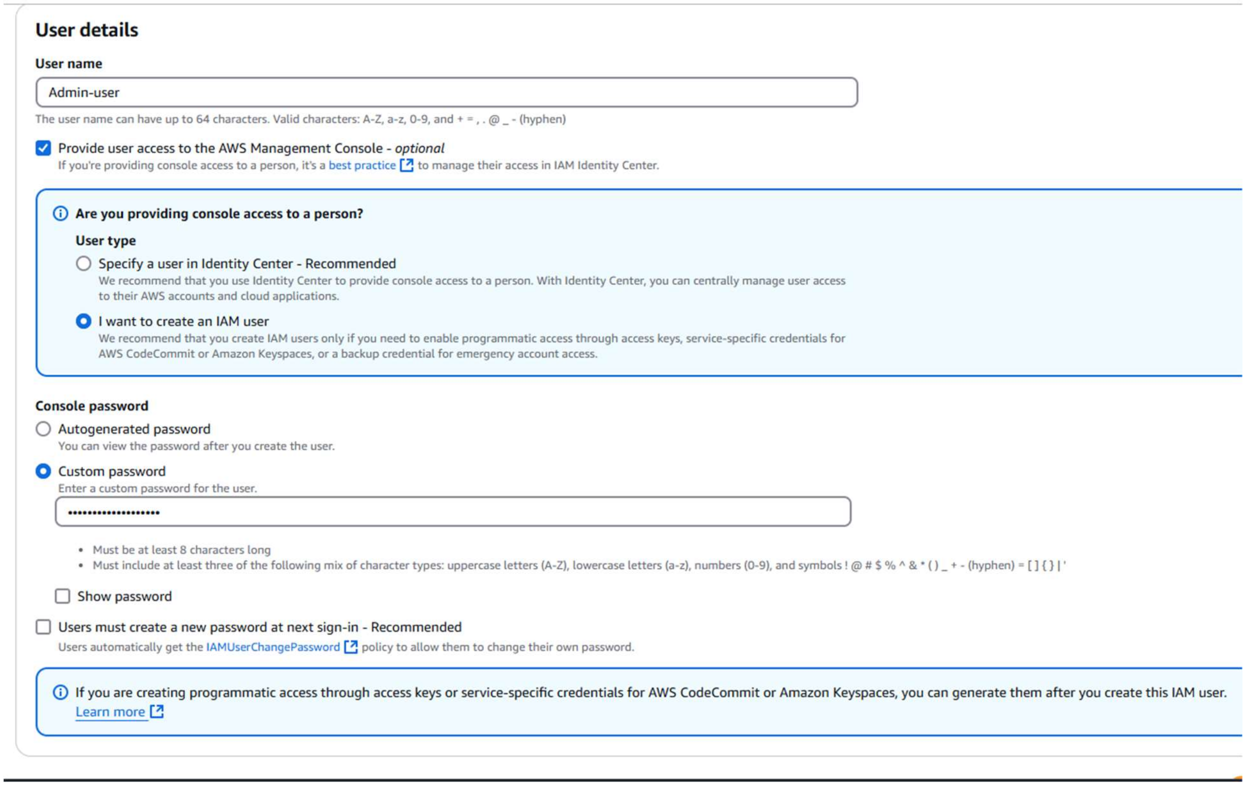
Delete Create user

Search

< 1 >

Step 2: Create the IAM User

1. **Enter a username** (e.g., AdminUser1).
2. **Select AWS Access Type**:
   - **"AWS Management Console access"** (for GUI access). This option is recommended for beginners as it provides graphical interface that makes navigating AWS service easier to understand.
   - Select “I want to create an IAM user” to make it simple setup.
3. Set a **custom password**.
4. Uncheck **Require password reset**.
5. Click **Next: Permissions**.



User details

User name

Admin-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.

••••••••••••••••••••

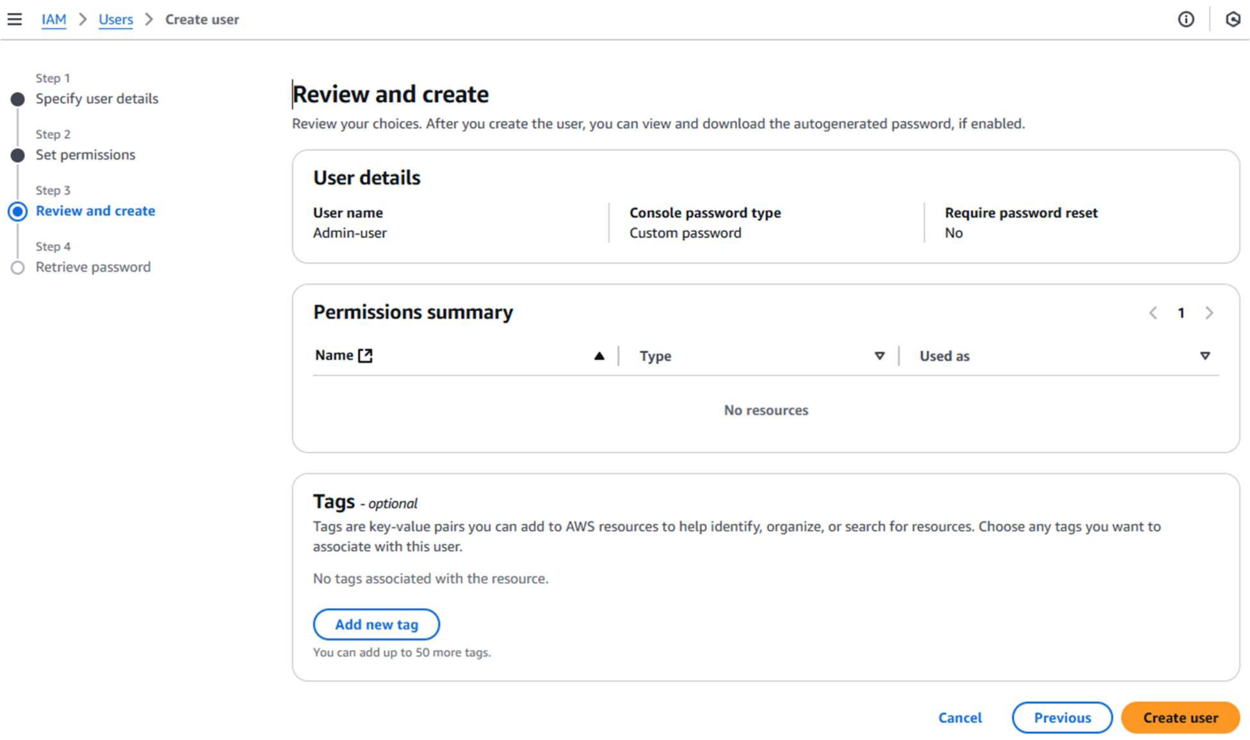
- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

□ 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

6. Set permission
   - Select add user to group. We don’t attach policies directly. This is for following management user best practice.



IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

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	Console password type	Require password reset
Admin-user	Custom password	No

Permissions summary

Name	Type	Used as
No resources		

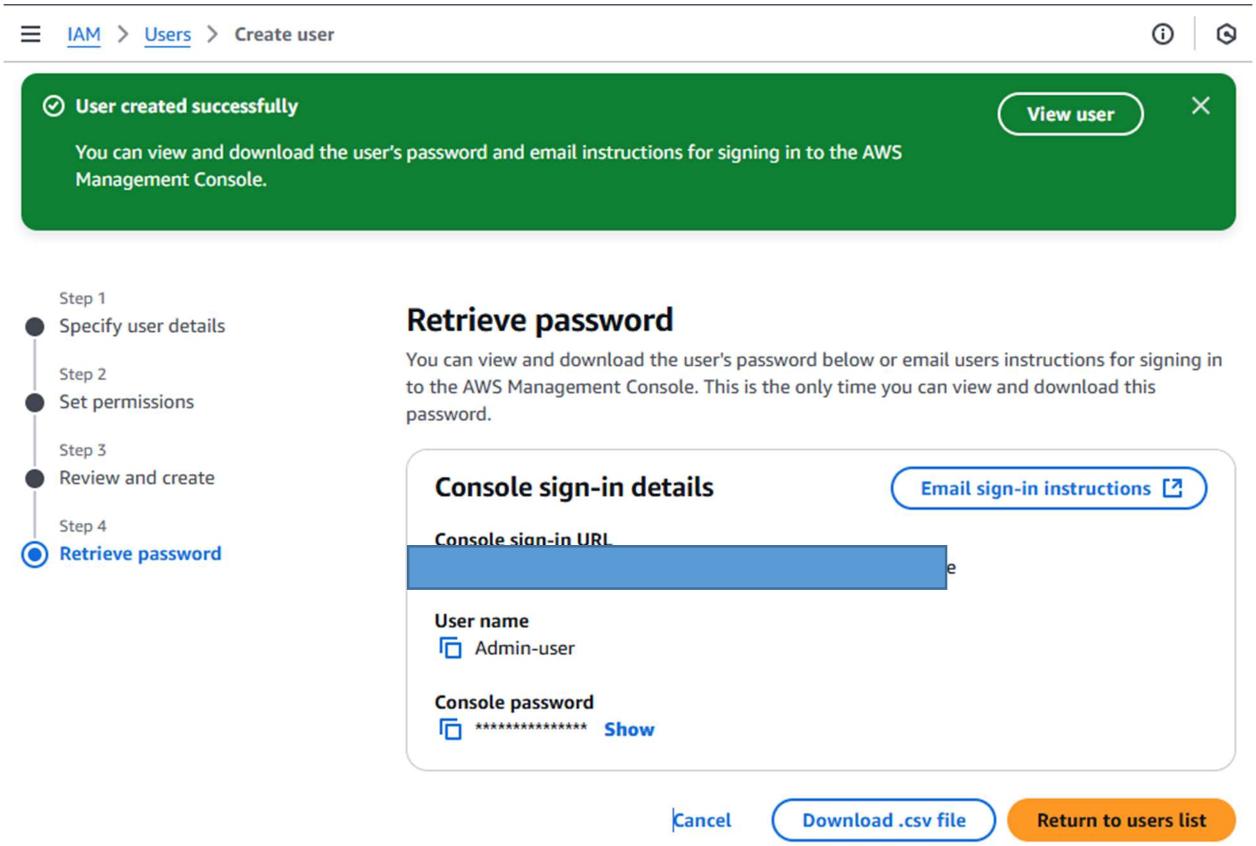
Tags *- optional*

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.

You can add up to 50 more tags.

7. Create user



IAM > Users > 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.

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

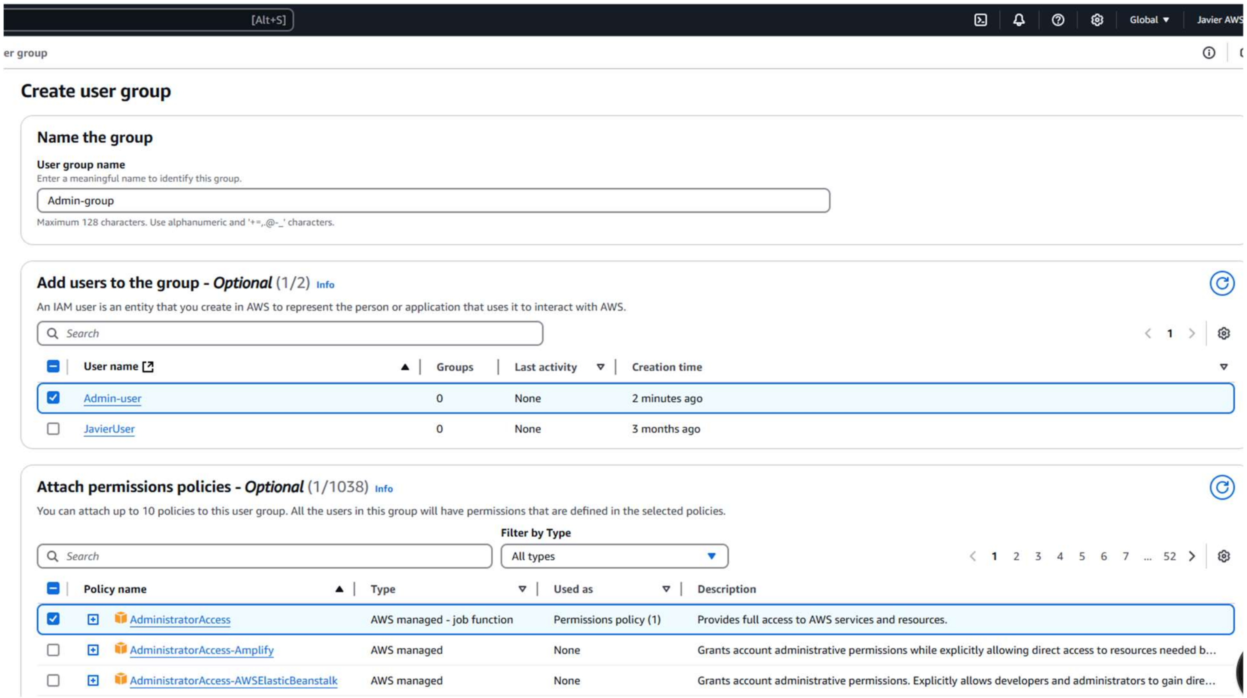
Console sign-in URL
[redacted]

User name
Admin-user

Console password
*************** Show

Step 3 : Create a New User Group

1. Click User groups in the left panel > create group > enter group name (e.g. Admin-group)
2. Add users to the group, check the Admin-user.
3. Attach the "AdministratorAccess" Policy. In the **Permissions** section, search for **AdministratorAccess**. Check the box next to **AdministratorAccess**.
4. Click Create group.



Create user group

Name the group

User group name
Enter a meaningful name to identify this group.
Admin-group
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Add users to the group - *Optional* (1/2) 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.

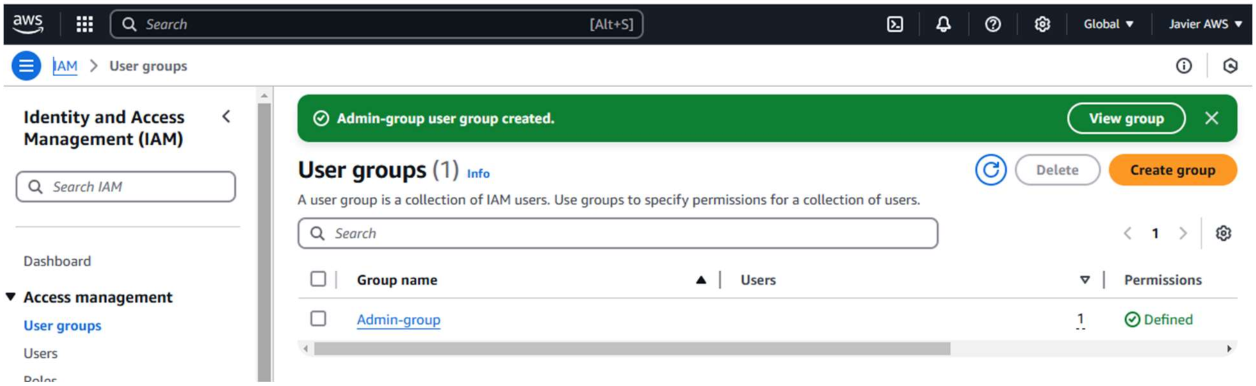
	User name	Groups	Last activity	Creation time
☑	Admin-user	0	None	2 minutes ago
□	JavierUser	0	None	3 months ago

Attach permissions policies - *Optional* (1/1038) 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 by Type: All types

	Policy name	Type	Used as	Description
☑	AdministratorAccess	AWS managed - job function	Permissions policy (1)	Provides full access to AWS services and resources.
□	AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permissions while explicitly allowing direct access to resources needed b...
□	AdministratorAccess-AWSElasticBeanstalk	AWS managed	None	Grants account administrative permissions. Explicitly allows developers and administrators to gain dire...



✓ Admin-group user group created.

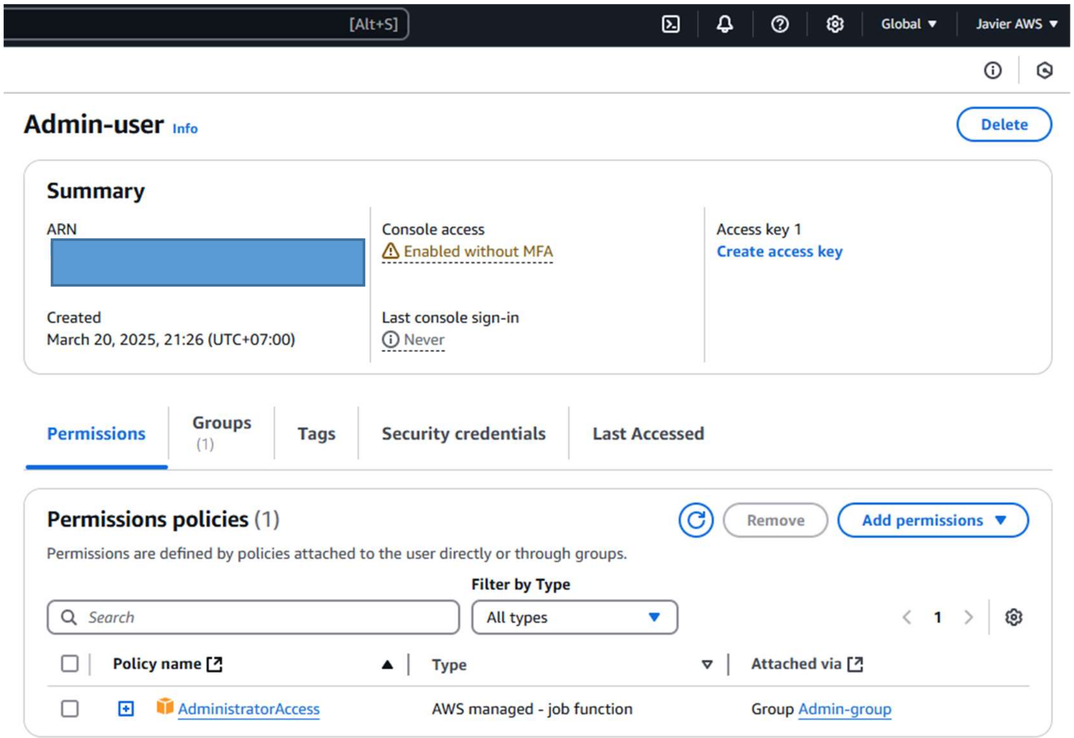
User groups (1) Info

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

	Group name	Users	Permissions
□	Admin-group	1	✓ Defined

Step 4 : Check the Admin-user permission

1. Click users in the left panel and click on Admin-user to see the detail.
2. On The permission policies box we can see AdminitratorAccess is attached.
3. Click security credential tab to get Console sign in link. We can copy the link to sign in with the admin-user credential. Or we can sign in from AWS management console but we have to put the AWS account ID. This Account ID we can see it from the account name (top-right corner)



Admin-user Info

Summary

ARN
[redacted]

Created
March 20, 2025, 21:26 (UTC+07:00)

Console access
⚠ Enabled without MFA

Last console sign-in
ⓘ Never

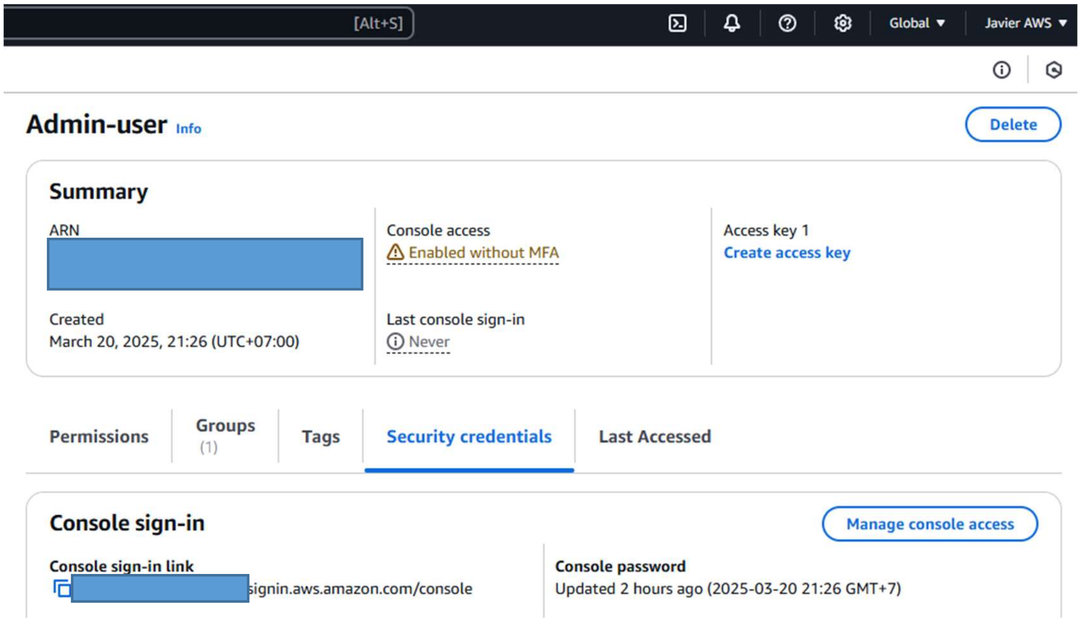
Access key 1
Create access key

Permissions | Groups (1) | Tags | Security credentials | Last Accessed

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

□	Policy name ▲	Type	Attached via
□	⊞ AdministratorAccess	AWS managed - job function	Group Admin-group



Admin-user Info

Summary

ARN
[redacted]

Created
March 20, 2025, 21:26 (UTC+07:00)

Console access
⚠ Enabled without MFA

Last console sign-in
ⓘ Never

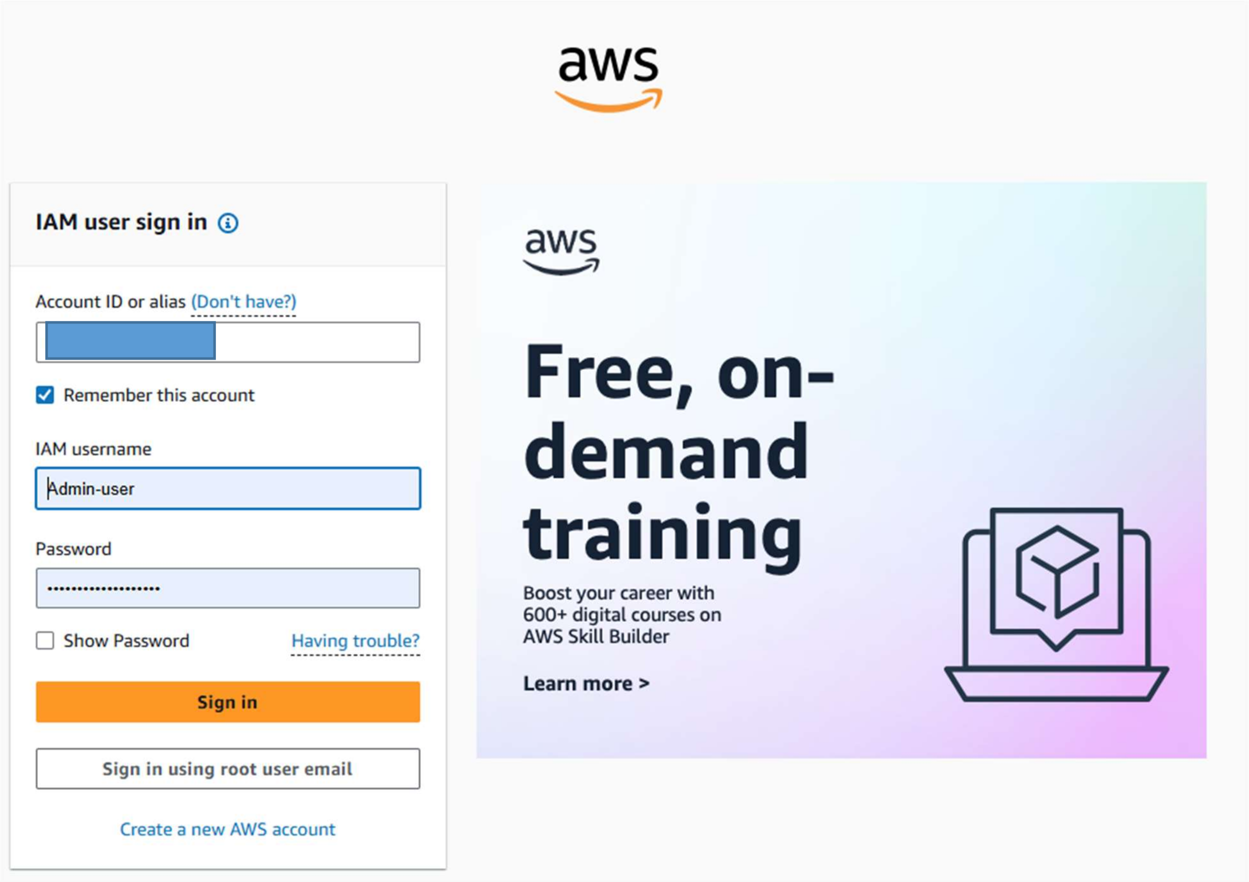
Access key 1
Create access key

Permissions | Groups (1) | Tags | Security credentials | Last Accessed

Console sign-in

Console sign-in link
[redacted]signin.aws.amazon.com/console

Console password
Updated 2 hours ago (2025-03-20 21:26 GMT+7)



IAM user sign in

Account ID or alias (Don't have?)

[redacted]

☑ Remember this account

IAM username

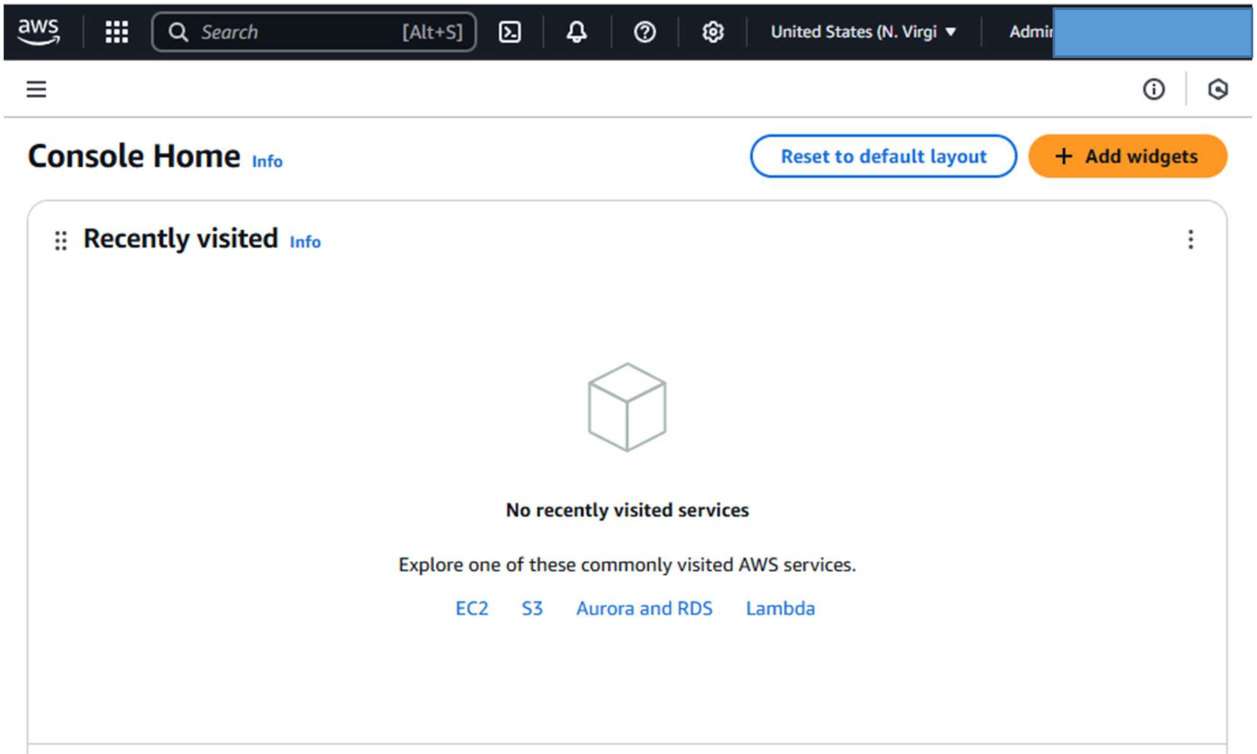
Admin-user

Password

•••••••••••••••••••

□ Show Password

Having trouble?
Sign in
Sign in using root user email
Create a new AWS account
Free, on-demand training
Boost your career with 600+ digital courses on AWS Skill Builder
Learn more >



[redacted]

Console Home Info

Recently visited Info

No recently visited services

Explore one of these commonly visited AWS services.

Security Best Practices

DO NOT use the root user for daily tasks.

- Use **IAM roles** instead of users for automation.
- Rotate IAM user passwords periodically.
- Review & remove unused IAM users.
- Apply **least privilege** policies where necessary.

Now we have a secure IAM Admin User to manage AWS instead of using the root account!