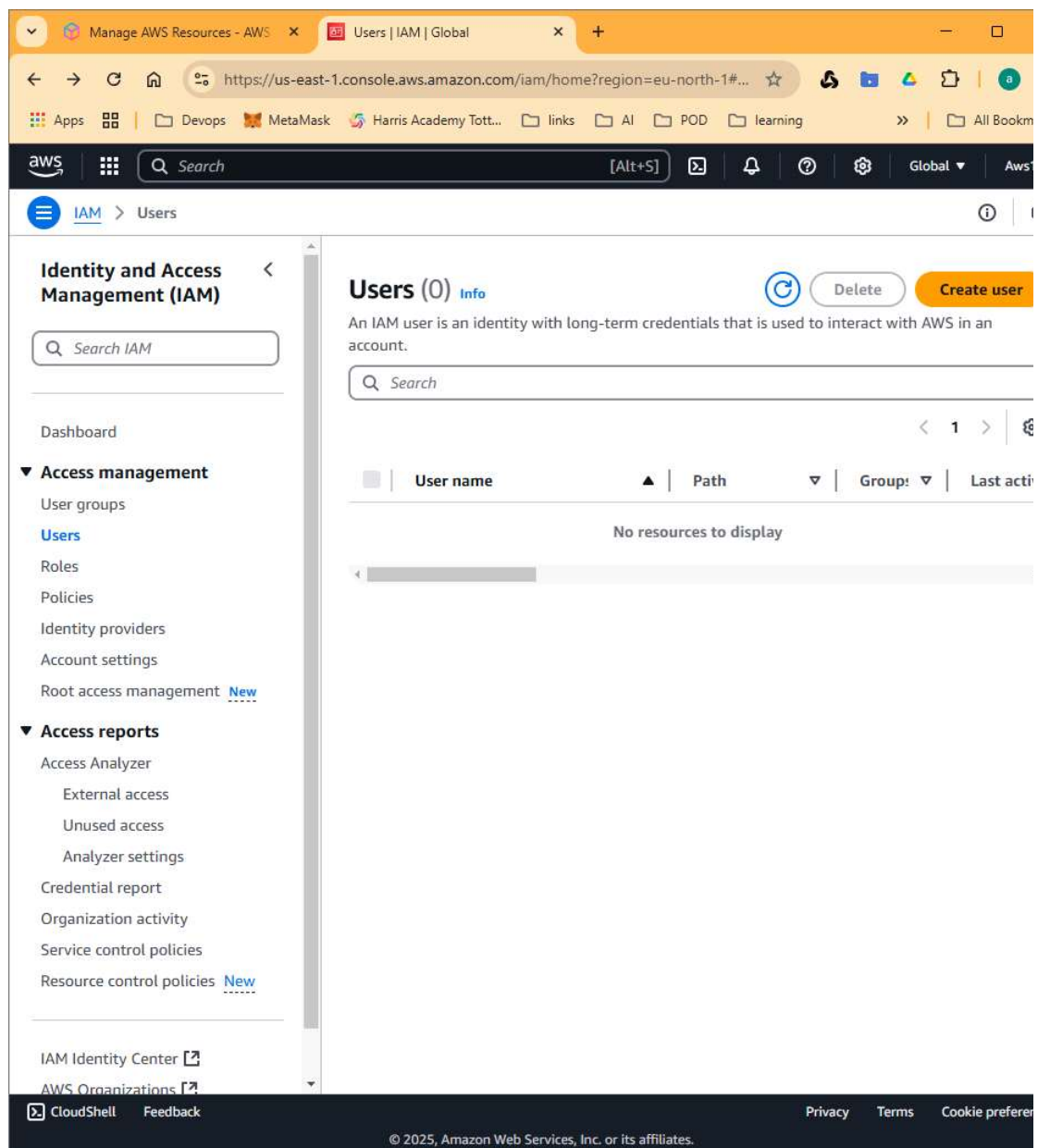


AWS IAM User Creation Lab

Step 3: Create a New IAM User

From the IAM Dashboard, click Users on the left panel.

Click Create user.



Step 4: User Details

Enter a User name (e.g., devops-user).

Check Provide user access to AWS Management Console

Choose I want to create an IAM user

Set Console password:

Choose Autogenerated password or Custom password.

(Optional) Check Users must create a new password at next sign-in - Recommended for first login.

Click Next.

Manage AWS Resources - AWS x Create user | IAM | Global

https://us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#...

Apps Devops MetaMask Harris Academy Tott... links AI POD learning All Bookm

aws Search [Alt+S] Global Aws1

IAM > Users > Create user

Set permissions
Step 3
Review and create
Step 4
Retrieve password

User details

User name

devops-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.

CloudShell Feedback Privacy Terms Cookie preferences

© 2025, Amazon Web Services, Inc. or its affiliates.

Step 5: Set Permissions

You have three options:

Add user to group: Choose an existing group with the right permissions or create a new group.

Attach policies directly: Attach policies like AdministratorAccess or AmazonEC2FullAccess.

Copy permissions: Copy all group memberships, attached managed policies, and inline

policies from an existing user.

For this lab, choose Attach policies directly and select:

AmazonEC2FullAccess (for EC2 access)

AmazonS3ReadOnlyAccess (for S3 access)

Click Next.

The screenshot shows the AWS IAM console 'Create user' page, specifically Step 2: Set permissions. The left sidebar shows the progress: Step 1 (Specify user details), Step 2 (Set permissions), Step 3 (Review and create), and Step 4 (Retrieve password). The main content area is titled 'Set permissions' and includes a sub-header 'Permissions options'. There are three radio button options: 'Add user to group', 'Copy permissions', and 'Attach policies directly'. The 'Attach policies directly' option is selected. Below this, there is a section 'Permissions policies (2/1328)' with a search bar containing 'AmazonEC2FullAccess' and a 'Filter by Type' dropdown set to 'All types'. A table lists the search results, showing one match: 'AmazonEC2FullAcc...' with a type of 'AWS managed' and 0 attached entities. At the bottom, there is a section 'Set permissions boundary - optional' with a checkbox for 'Use a permissions boundary to control the maximum permissions'.

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

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.

Permissions policies (2/1328)

Choose one or more policies to attach to your new user. [Create policy](#)

Filter by Type
All types 1 match

<input checked="" type="checkbox"/>	Policy name	Type	Attached entities
<input checked="" type="checkbox"/>	AmazonEC2FullAcc...	AWS managed	0

Set permissions boundary - optional

Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. [Learn more](#)

☐ Use a permissions boundary to control the maximum permissions
You can select one of the existing permissions policies to define the boundary.

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Step 6: Add Tags (Optional)

Add key-value pairs (e.g., Department: DevOps).

Click Next.

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.

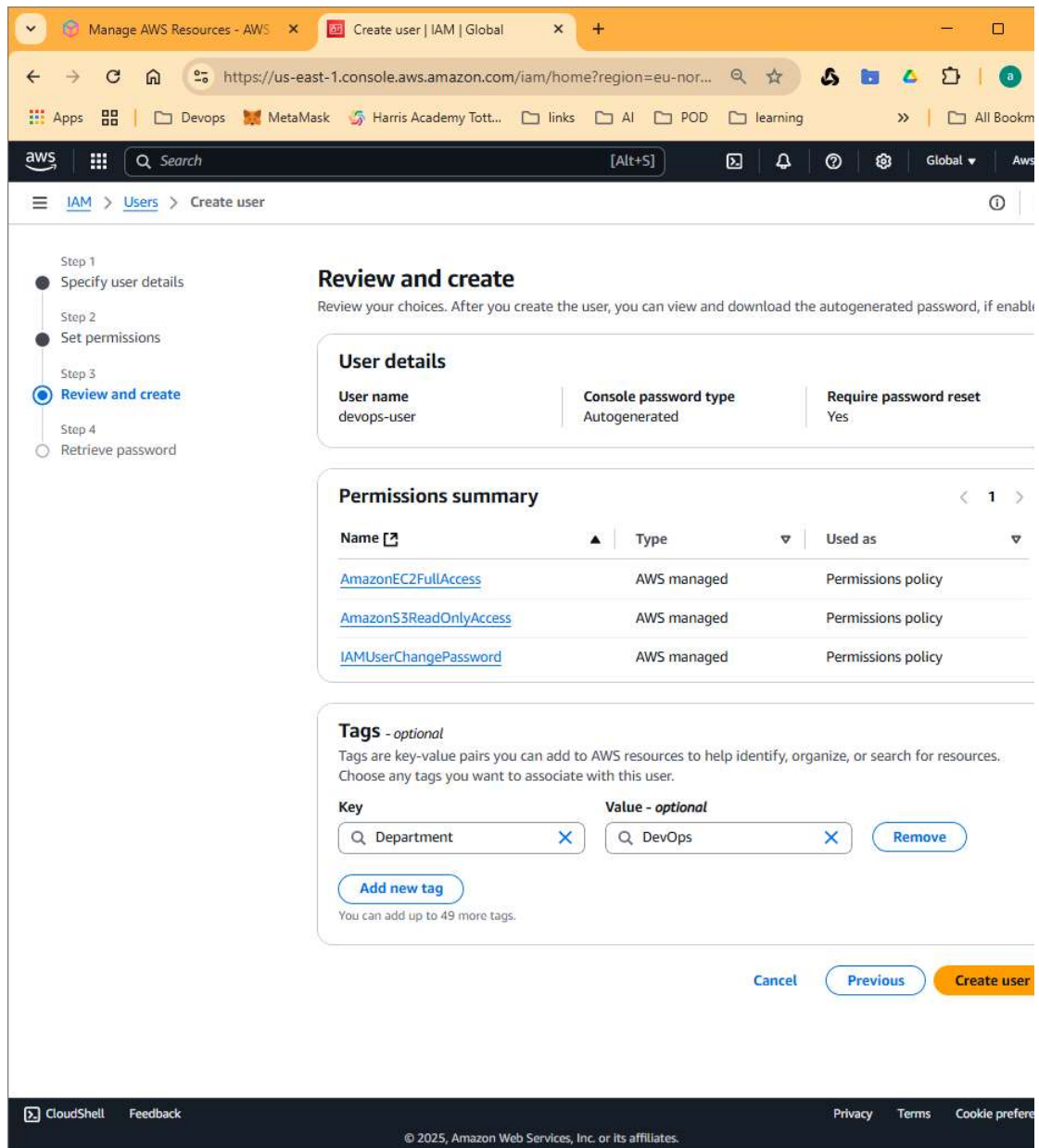
Key	Value - <i>optional</i>	
<input type="text" value="Department"/>	<input type="text" value="DevOps"/>	<button>Remove</button>
<button>Add new tag</button>		

You can add up to 49 more tags.

Step 7: Review and Create

Review all the configurations.

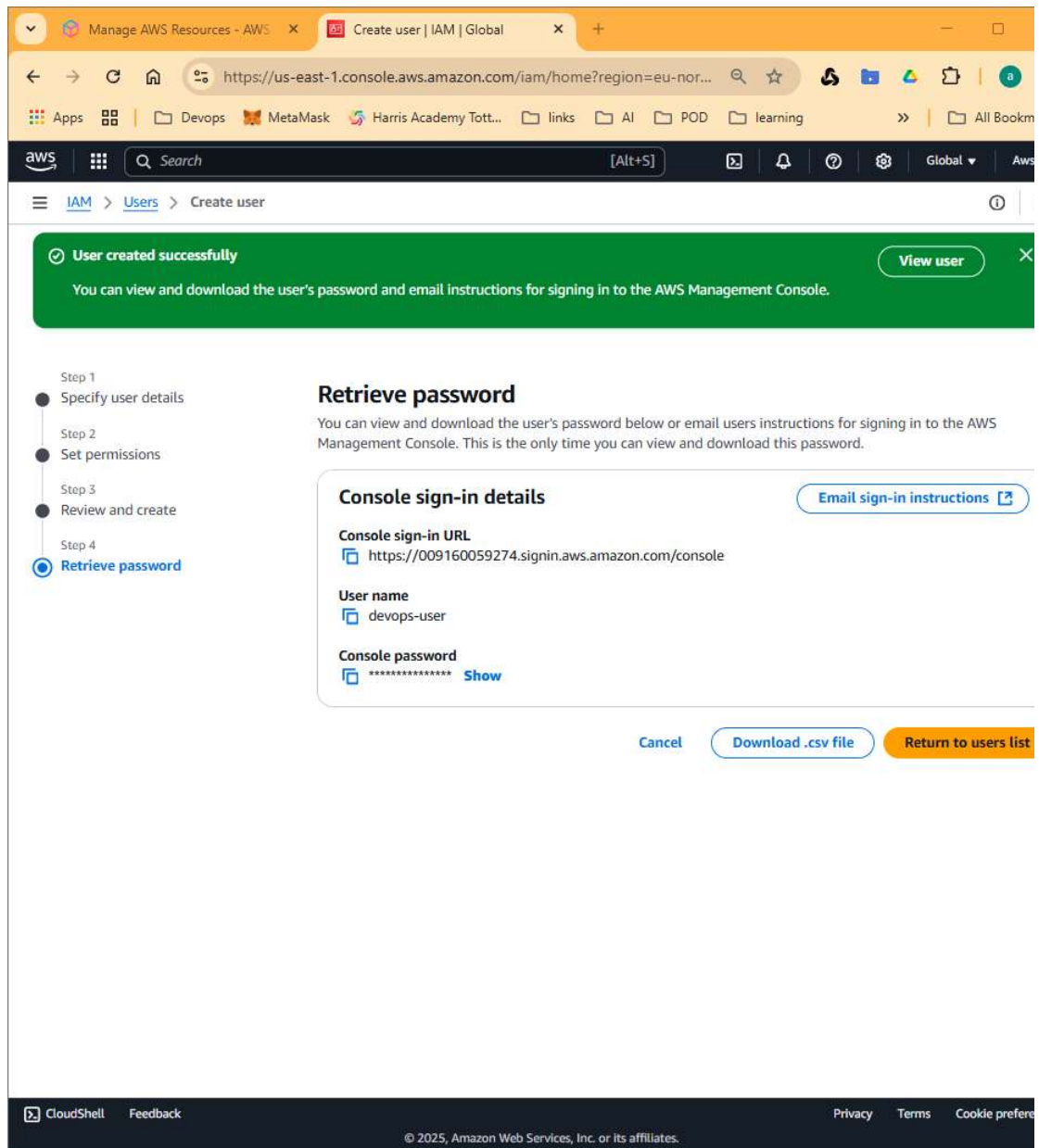
Click Create user.



Step 8: Retrieve Credentials

Download the .csv file with the Access Key ID and Secret Access Key.

Copy the Console URL for user login.



Verification

Log out of the AWS Console.

Open the Console URL from the IAM user credentials.

Log in with the new IAM user credentials.

Manage AWS Resources - AWS

Amazon Web Services Sign-In

Amazon Web Services Sign-In

https://eu-north-1.signin.aws.amazon.com/oauth?client_id=arn%3Aa...

AppsDevopsMetaMaskHarris Academy Tott...linksAIPODlearningAll Bookm

New sign inMulti-session disabledEnglish

You are currently using the improved sign in UI experience.

The improved sign in experience will launch soon. During this time, you can still change back to legacy sign in using the dropdown in the upper right corner.

aws

IAM user sign in

Account ID (12 digits) or account alias

009160059274

IAM username

devops-use

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 »

By continuing, you agree to [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for

8

Manage AWS Resources - AWS x Console Home | Console Home x Amazon Web Services Sign-In x


https://eu-north-1.console.aws.amazon.com/console/home?region=... Apps Devops MetaMask Harris Academy Tott... links AI POD learning All Bookm

aws Search [Alt+S] Europe (Stockhol devops-user @ 0091-6005-927

Console Home Info

[Reset to default layout](#) [+ Add widgets](#)

Recently visited Info

 IAM

[View all services](#)


Applications (0) Info

[Create application](#)

Region: Europe (Stockholm)

eu-north-1 (Current Region) < 1 >

Name	Description	Region	Originati...	★
------	-------------	--------	--------------	---

 Access denied to servicecatalog:ListApplications [Diagnose with Amazon Q](#)

CloudShell Feedback Privacy Terms Cookie preference

© 2025, Amazon Web Services, Inc. or its affiliates.