

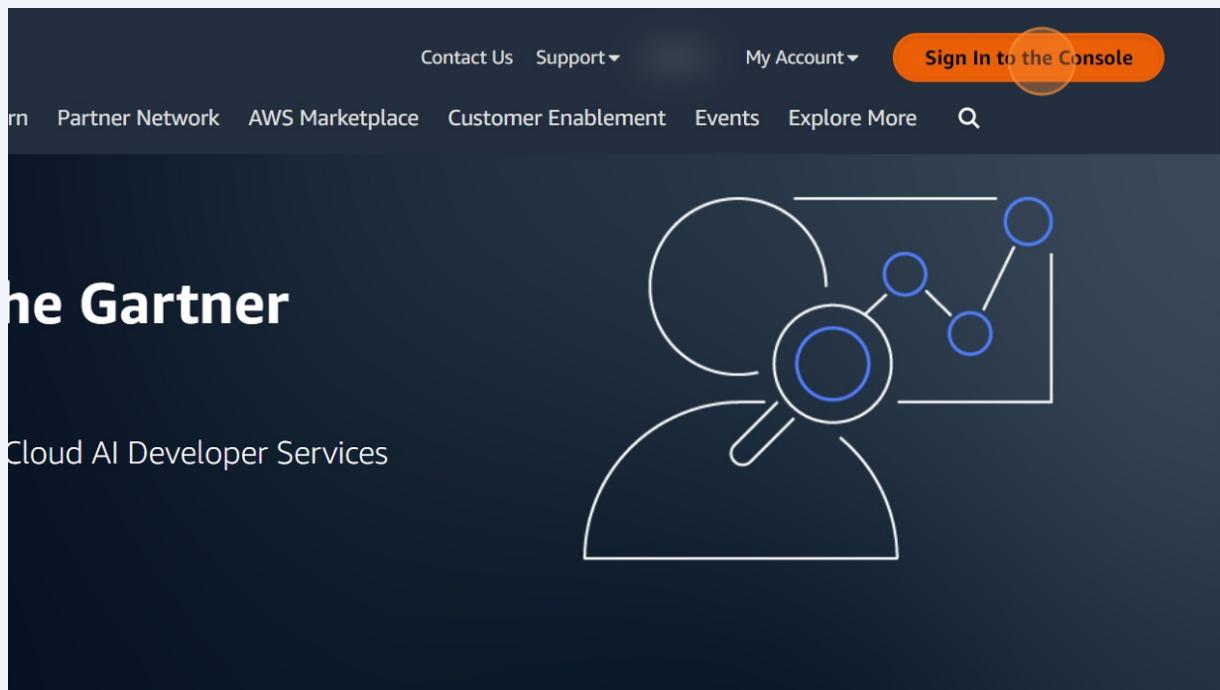
How to Create an IAM User

This guide provides step-by-step instructions on how to create an IAM user in AWS. It explains the process in a clear and concise manner, allowing users to easily follow along and create a user with the necessary permissions. By following this guide, users can effectively manage access to their AWS resources and ensure the security of their account.

This guide was created by Nijat Hajiyev

- 1 Navigate to <https://aws.amazon.com/>

- 2 Click "Sign In to the Console"



3 Click the "Search" field.

The screenshot shows the AWS Console Home page. At the top, there's a navigation bar with the AWS logo, a 'Services' dropdown, a search bar containing the word 'Search' with a magnifying glass icon, and a keyboard shortcut '[Alt+S]' to its right. Below the search bar is a row of service icons: EC2, S3, VPC, IAM, AWS Budgets, AWS Cost Explorer, RDS, Route 53, DynamoDB, and others partially visible. The main content area has a header 'Console Home' with an 'Info' link. On the left, there's a 'Recently visited' section with a list of services: EC2, Amazon Textract, AWS Budgets, Amazon Forecast, Amazon Comprehend, and Amazon Polly. To the right, there's a 'Welcome to AWS' section with two items: 'Getting started with AWS' (with a rocket icon) and 'Training and certification' (with a gear and ribbon icon). Both sections have descriptive text below their respective icons.

4 Type "IAM"

5 Click "IAM"

The screenshot shows the AWS Management Console search results for 'IAM'. The search bar at the top contains 'IAM'. Below the search bar, there is a sidebar with 'Recently viewed' services: EC2, Amazon Te, AWS Budget, Amazon Fo, Amazon Co, Amazon Po, and others. The main content area shows 'Search results for 'IAM'' and 'Try searching with longer queries for more relevant results'. A section titled 'Services' lists 'Services (10)', 'Features (20)', and 'Resources New'. Under 'Services', the 'IAM' service is highlighted with a yellow circle. Other services listed include Documentation (48,528), Knowledge Articles (20), Marketplace (695), Blogs (1,668), Events (12), and Tutorials (2). To the right of the services list, there are sections for 'Top features' (Groups, Users, Roles, Policies, Access Analyzer), 'IAM Identity Center' (Manage workforce user access to multiple AWS accounts and cloud apps), and 'Resource Access Manager' (Share AWS resources with other accounts or AWS Organizations).

6 Click "Users"

The screenshot shows the IAM Dashboard. On the left, there is a navigation sidebar with 'Management console' at the top, followed by a search bar 'Search IAM'. Below this, there are sections for 'Dashboard', 'Access management' (with 'User groups', 'Users' highlighted with a yellow circle, and 'Roles', 'Policies', 'Identity providers', and 'Account settings'), and 'Access reports' (with 'Analyzer' and 'Live rules'). On the right, the main content area is titled 'IAM Dashboard' and contains a 'Security recommendations' section with one item: 'Add MFA for root user' (warning icon) - 'Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.' Below this is an 'IAM resources' section with a table showing 'User groups', 'Users', 'Roles', and 'Policies'.

7

Click "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.

The screenshot shows the AWS IAM 'Users (0) Info' page. At the top, it says 'An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.' Below is a search bar labeled 'Search'. A table header includes columns for 'User name', 'Path', 'Group', 'Last activity', and 'M'. A message 'No resources to display' is centered below the table. The bottom right corner of the page footer contains the text '© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.'

8

Click "Global" to see that IAM is Global, not Region based

The screenshot shows the AWS IAM 'Users' page. The top navigation bar includes links for RDS, Route 53, DynamoDB, Amazon SageMaker, and Lambda, along with a 'Global' dropdown menu which is highlighted with an orange circle. Other items in the top bar include '[Alt+S]', a search icon, a bell icon, a help icon, a settings icon, and a user profile for 'Nijat Hajiyev'. Below the top bar is a message about IAM users interacting with AWS. The main table has columns for 'Path', 'Group', 'Last activity', 'MFA', 'Password age', and 'Actions'. A 'Create user' button is at the top right of the table area. The message 'No resources to display' is centered below the table. The bottom right corner of the page footer contains an information icon.

9

The screenshot shows the AWS IAM console with the 'Global' dropdown menu highlighted. The main area displays a list of AWS Regions with their respective names and IDs:

Region Name	Region ID
US East (N. Virginia)	us-east-1
US East (Ohio)	us-east-2
US West (N. California)	us-west-1
US West (Oregon)	us-west-2
Asia Pacific (Mumbai)	ap-south-1
Asia Pacific (Osaka)	ap-northeast-3
Asia Pacific (Seoul)	ap-northeast-2
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1

10 Click "Create user"

The screenshot shows the AWS IAM console with the 'Create user' button highlighted. The main area displays a list of users with their status and creation date:

User	Status	Created
Administrator Access	Active	2023-09-15T12:00:00Z
Test User	Active	2023-09-15T12:00:00Z

11 Click the "User name" field.

The screenshot shows the AWS IAM 'Create user' wizard. The current step is 'Step 1: Specify user details'. On the left, there are three navigation steps: 'Step 1 Specify user details' (selected), 'Step 2 Set permissions' (disabled), and 'Step 3 Review and create' (disabled). The main area is titled 'Specify user details' and contains a 'User details' section. Within this section, there is a 'User name' input field, which is highlighted with an orange circle. Below the input field is a checkbox labeled 'Provide user access to the AWS Management Console - optional'. A note below the checkbox says, 'If you're providing console access to a person, it's a [best practice](#) to manage their access in the AWS Management Console.' At the bottom of the 'User details' section, there is a callout box with an info icon that says, 'If you are creating programmatic access through access keys or service-specific endpoints, you can generate them after you create this IAM user. [Learn more](#)'.

12 Type "DemoUser"

13 Click "Next"

The screenshot shows the 'Set permissions' step of the IAM user creation wizard. It includes fields for the user name ('DemoUser') and a checkbox for 'Provide user access to the AWS Management Console - optional'. A note explains that this grants programmatic access through access keys or service-specific credentials. The 'Next Step' button is highlighted with an orange circle.

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

Programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keypairs, you can generate them after you create this IAM user. [Learn more](#)

Cancel Next

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

14 Click this checkbox.

The screenshot shows the 'Set permissions' step of the IAM user creation wizard. It includes fields for the user name ('DemoUser') and a checkbox for 'Provide user access to the AWS Management Console - optional'. A note explains that this grants programmatic access through access keys or service-specific credentials. The 'Next Step' button is highlighted with an orange circle.

Specify user details

Step 2
[Set permissions](#)

Step 3
Review and create

User details

User name
DemoUser

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

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keypairs, you can generate them after you create this IAM user. [Learn more](#)

CloudShell Feedback

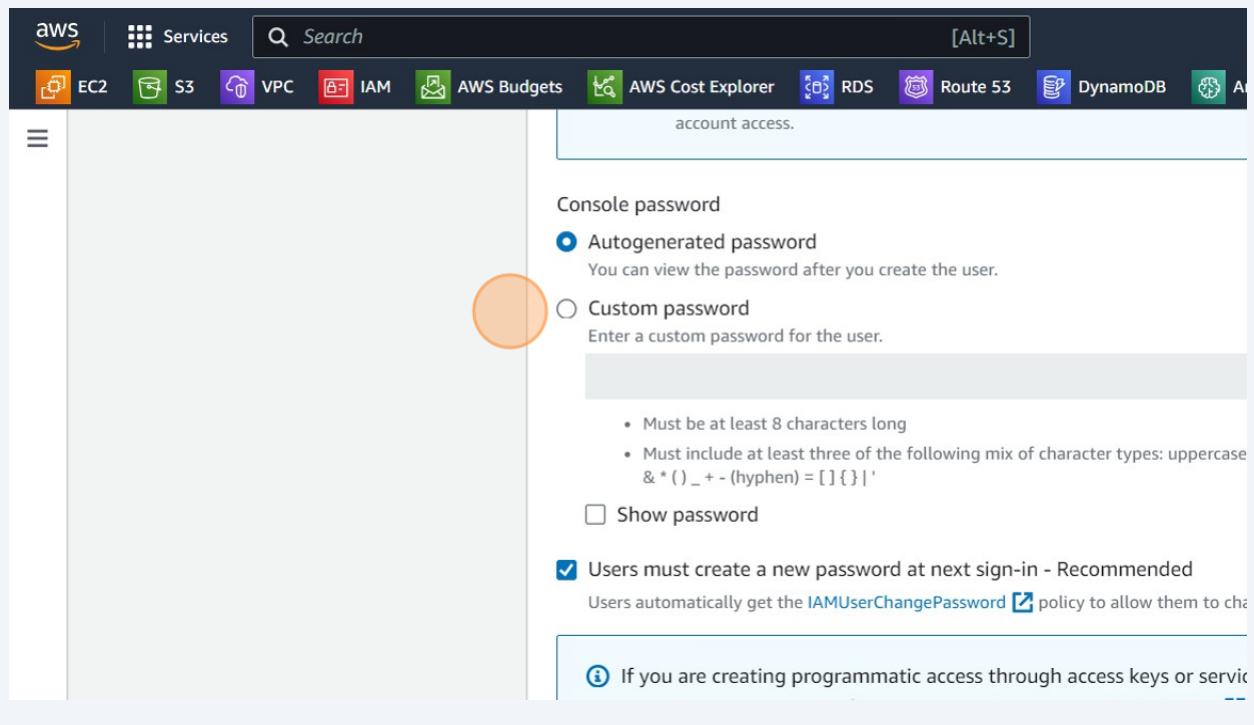
15 Click this radio button.

The screenshot shows the 'User type' section of the AWS IAM User Creation Wizard. It asks if you're providing console access to a person. Two options are shown: 'Specify a user in Identity Center - Recommended' (radio button is checked) and 'I want to create an IAM user' (radio button is unselected and highlighted with an orange circle). A note below says: 'We recommend that you create IAM users only if you need to enable programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or account access.' Below this, another note says: 'If you are creating programmatic access through access keys or service-specific credentials, you can generate them after you create this IAM user. [Learn more](#)'.

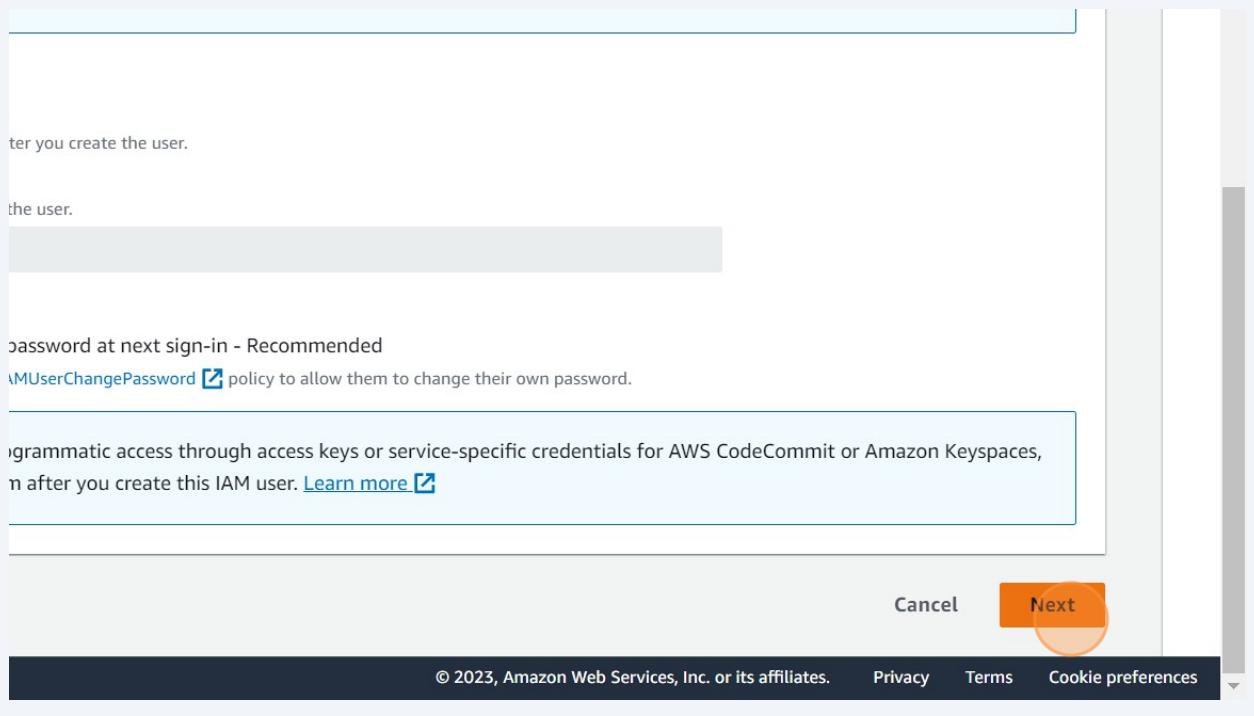
16 Click this radio button.

The screenshot shows the 'Console password' section of the AWS IAM User Creation Wizard. It asks if you're providing console access to a person. Two options are shown: 'Specify a user in Identity Center - Recommended' (radio button is unselected) and 'I want to create an IAM user' (radio button is selected and highlighted with an orange circle). A note below says: 'We recommend that you create IAM users only if you need to enable programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or account access.' Below this, another note says: 'You can view the password after you create the user.' A third option 'Custom password' is also listed with the note: 'Enter a custom password for the user.'

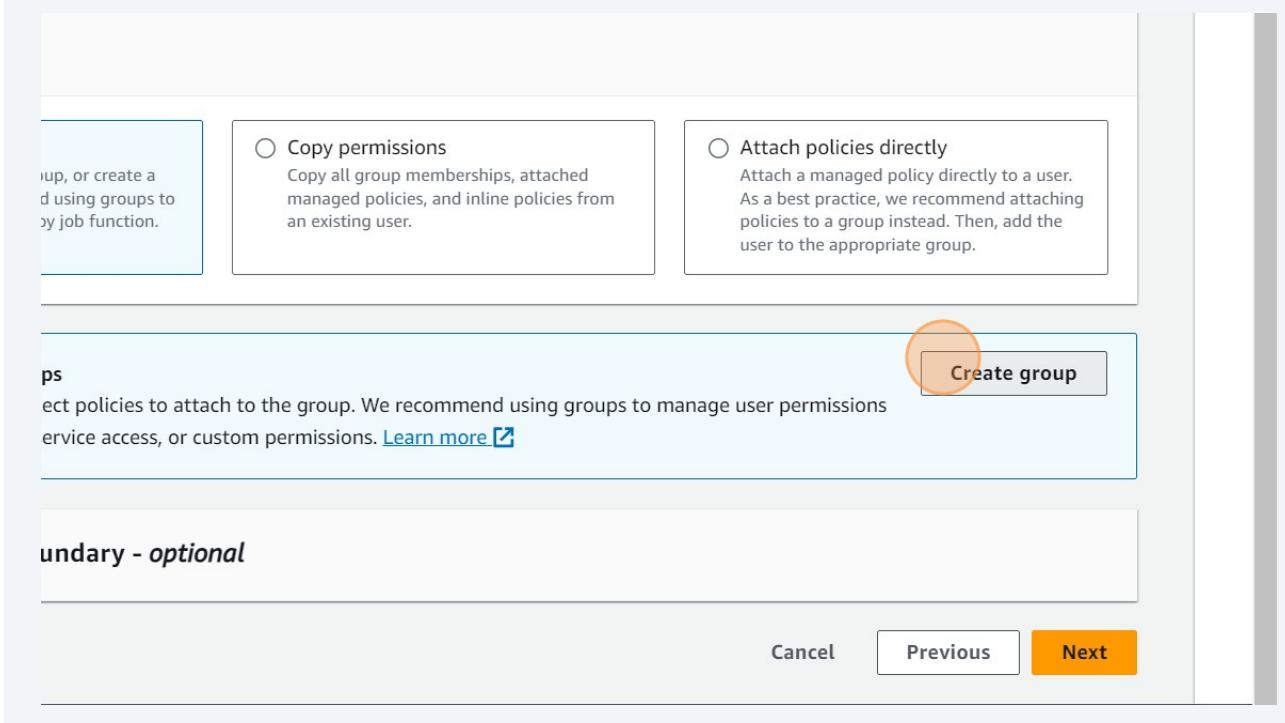
17 Choose Autogenerate password or Custom password based on choice



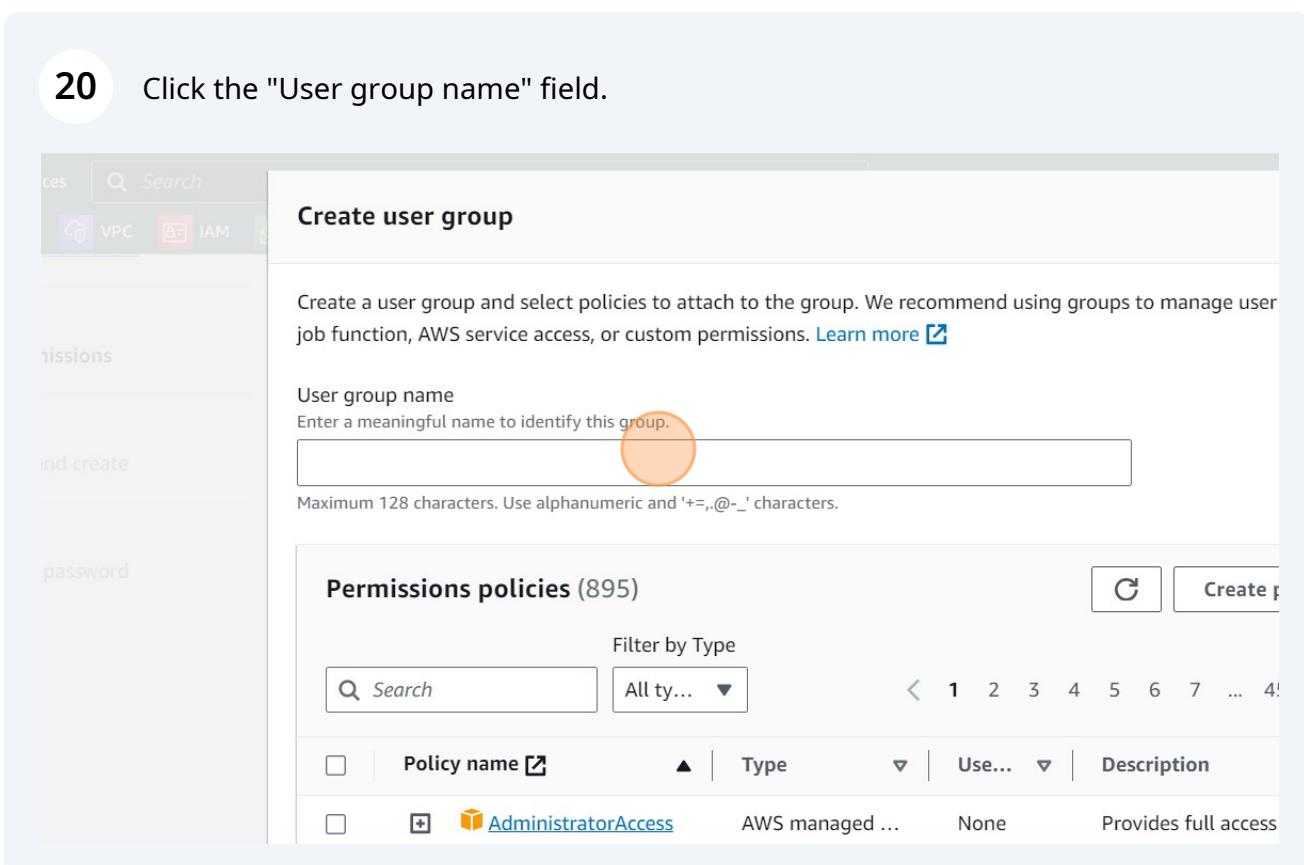
18 Click "Next"



19 Click "Create group"



20 Click the "User group name" field.



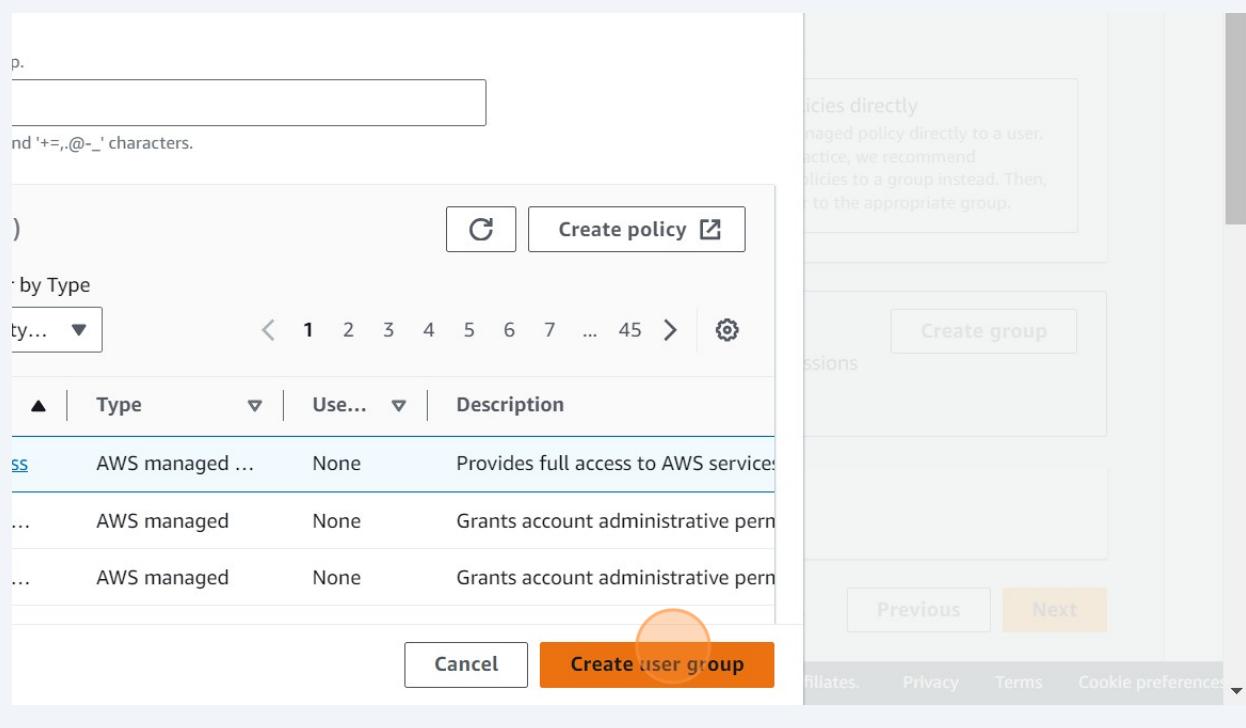
21 Type "GROUP NAME"

22 Give needed permissions

The screenshot shows the AWS IAM console during the creation of a new user group. On the left, a sidebar indicates 'Step 3: Review and create' and 'Step 4: Retrieve password'. At the bottom left is a blue circular icon with a red dot. The main area is titled 'User group name' with the value 'admin'. Below it is a note: 'Maximum 128 characters. Use alphanumeric and '+,-,@-' characters.' A search bar and a filter dropdown are present. The 'Permissions policies' section lists three policies: 'AdministratorAccess', 'AdministratorAccess', and 'AdministratorAccess'. The first row is highlighted with an orange circle around its checkbox. The table has columns for Policy name, Type, and Use... .

Policy name	Type	Use...
AdministratorAccess	AWS managed	None
AdministratorAccess	AWS managed	None
AdministratorAccess	AWS managed	None

23 Click "Create user group"



24 Click Group name checkbox.

The screenshot shows the 'User groups' page in the AWS IAM console. On the left, a sidebar indicates 'Step 4' and 'Retrieve password'. The main area displays a table titled 'User groups (1)'. The table has columns for 'Group name' and 'Users'. One row is shown, with the 'admin' group name highlighted by a large orange circle. Below the table is a section with the heading '► Set permissions boundary - optional'. At the bottom of the page is a dark footer bar with icons for CloudShell and Feedback.

25 Click "Next"

Using groups to manage policies, inline policies from an existing user.

As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

The screenshot shows the AWS IAM Groups page. At the top, there are three buttons: a refresh icon, a 'Create group' button, and a settings gear icon. Below this is a search bar. The main table has columns for 'Users', 'Attached policies', and 'Created'. A single row is visible, showing 0 users, the policy [AdministratorAccess](#), and the creation date 2023-10-29 (Now). At the bottom of the page are navigation buttons for 'Cancel', 'Previous', and 'Next' (which is highlighted with an orange circle), and links for '© 2023, Amazon Web Services, Inc. or its affiliates.', 'Privacy', 'Terms', and 'Cookie preferences'.

If you need to add Tag:

26 Click "Add new tag"

The screenshot shows the AWS IAM Groups page. At the top, there's a table with two rows:

Name	Type
admin	Group

Below the table is a section titled "Tags - optional" with the sub-instruction: "Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for them." It displays a message: "No tags associated with the resource." A prominent "Add new tag" button is centered, with an orange circle highlighting it. Below the button, a note says: "You can add up to 50 more tags." At the bottom of the page, there's a navigation bar with icons for CloudShell and Feedback, and a copyright notice: "© 2023, Amazon Web Services, Inc. or its affiliates."

27 Click the "Key" field.

The screenshot shows the AWS IAM Groups page. The interface is identical to the previous one, featuring a table with the "admin" group and a "Tags - optional" section. In the "Tags" section, there's a "Key" input field with the placeholder "Enter key", which is highlighted with an orange circle. To the right of the key field is a "Value - optional" input field with the placeholder "Enter value". Below these fields is a note: "You can add up to 49 more tags." The bottom navigation bar includes CloudShell, Feedback, and a copyright notice: "© 2023, Amazon Web Services, Inc. or its affiliates."

28 Type "KEY NAME"

29 Click the "Value - optional" field.

The screenshot shows the AWS IAM User creation wizard. In Step 3, the user is setting permissions. The 'Tags' section is visible, showing a table of existing tags and a form for adding new ones. A red circle highlights the 'Value - optional' input field in the 'Add new tag' row.

Name	Type	Used as
Admin	Group	Permissions group
MUserChangePassword	AWS managed	Permissions policy

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.

Add new tag

Value - optional

Enter value

Cancel Previous Create

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms

30 Type "VALUE NAME"

31 Click "Create user"

Add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

Value - optional

X Engineering X Remove

Cancel Previous Create user Terms Cookie preferences

32 Click "Return to users list"

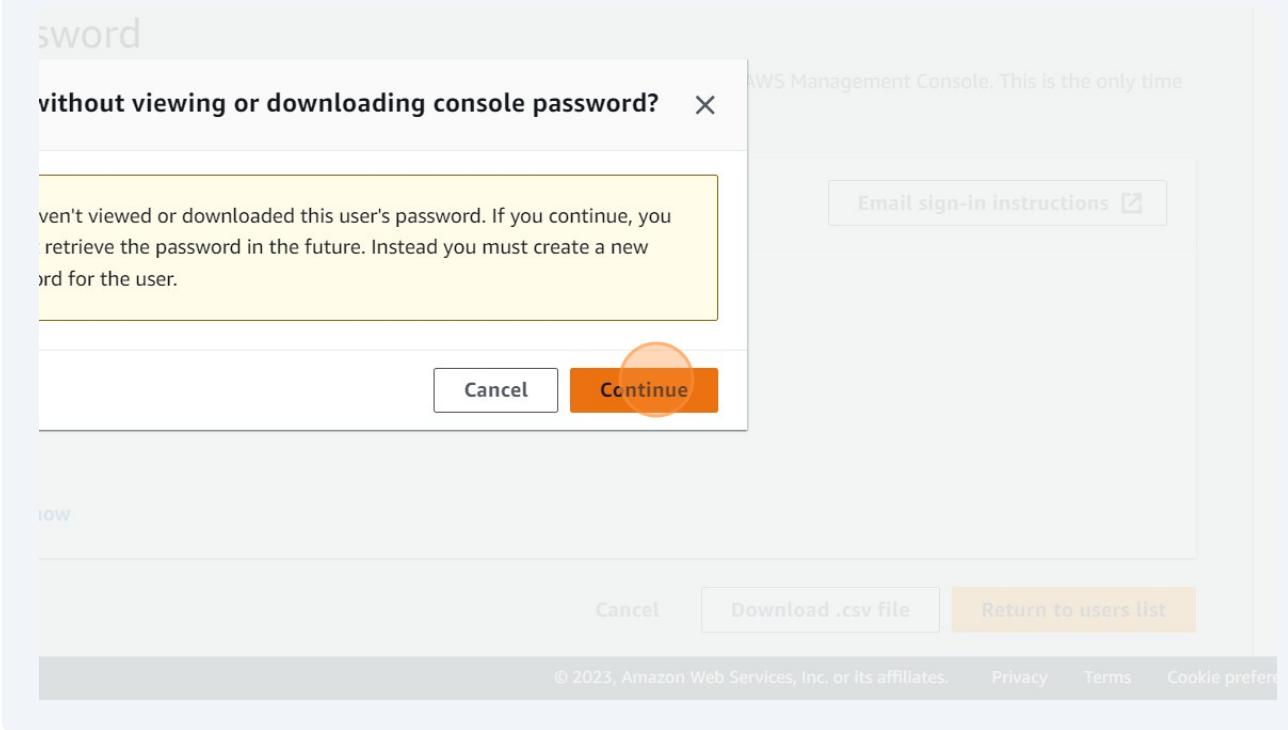
.s

Email sign-in instructions

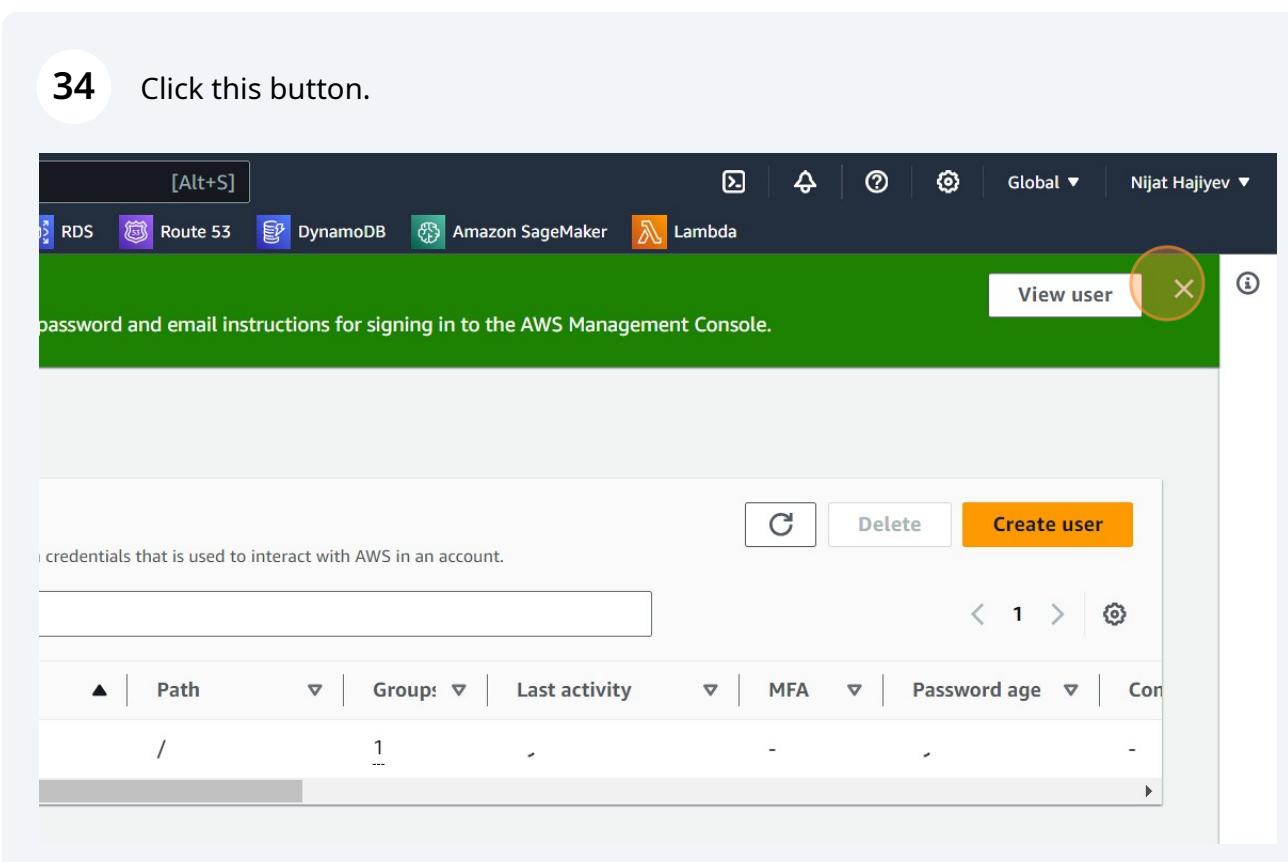
signin.aws.amazon.com/console

Cancel Download .csv file Return to users list Privacy Terms Cookie preferences

33 Click "Continue"



34 Click this button.



35 Click this button.

The screenshot shows the AWS IAM Users page. At the top, there's a navigation bar with tabs for RDS, Route 53, DynamoDB, Amazon SageMaker, and Lambda. On the far right of the bar are icons for Global, Nijat Hajiyev, and a help symbol. Below the bar is a search bar and a message about IAM users. The main area is a table listing users, with one row for 'DemoUser' highlighted by a large orange circle around its edit button.

	Path	Groups	Last activity	MFA	Password age	Con
<input type="checkbox"/>	/	1	0	-	0	-

36 Click "DemoUser" to check information of the user

The screenshot shows the AWS IAM Users page. The left sidebar has links for Dashboard, Access management, User groups, Users (which is selected and highlighted in blue), Roles, Policies, Identity providers, Account settings, Access reports, and analyzer. The main content area shows the 'Users (1)' section with a table. One row in the table is highlighted with a large orange circle around the 'User name' column entry 'DemoUser'.

	User name	Path	Groups
<input type="checkbox"/>	DemoUser	/	1

37 Click "User groups" to see groups

The screenshot shows the AWS Identity and Access Management (IAM) console. On the left, the navigation pane has sections like Dashboard, Access management (with User groups and Users highlighted), Roles, Policies, Identity providers, and Account settings. Under Access reports, there's a CloudTrail analyzer icon. The main content area is titled "Identity and Access Management (IAM)" and shows a table of policies. The first two rows are "AdministratorAccess" (AWS managed - job function) and "IAMUserChangePassword" (AWS managed). Below the table, a section titled "Permissions boundary (not set)" is shown. Further down, a section titled "Generate policy based on CloudTrail events" includes a "Generate policy" button and a note that no requests have been made in the past 7 days.

Policy name	Type
AdministratorAccess	AWS managed - job function
IAMUserChangePassword	AWS managed

38 Click "admin" group to check information of this group

This screenshot shows the "User groups" page within the AWS IAM console. The left sidebar is identical to the previous screenshot. The main content area shows a table titled "User groups (1) Info". It contains one row for a group named "admin". A search bar is at the top of the table, and a "Users" column shows there is 1 user associated with this group. The "admin" group name is highlighted with an orange circle.

Group name	Users
admin	1



You have successfully created User and Group