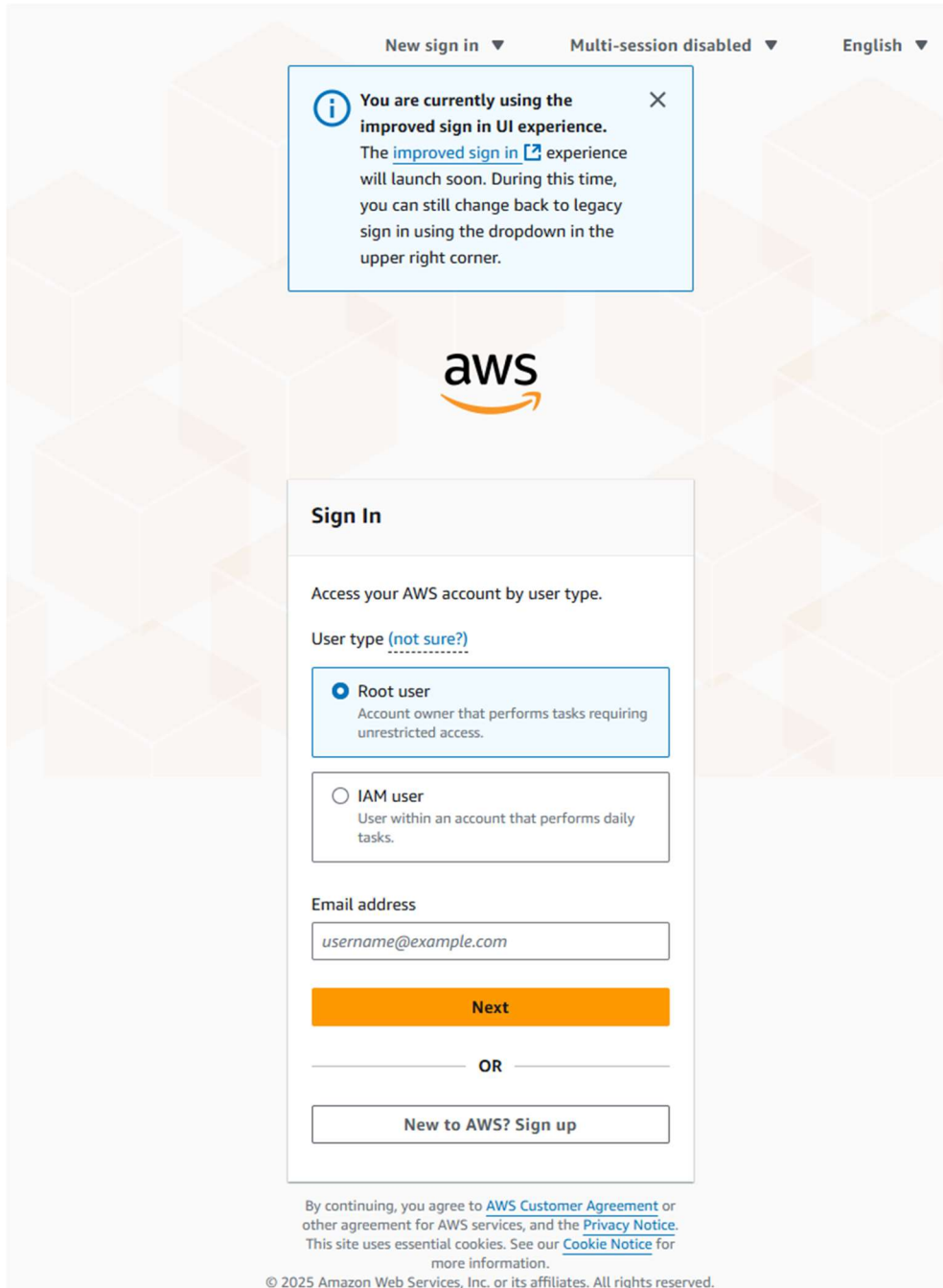


Sign in to the AWS Management Console

1. Open your browser and go to <https://aws.amazon.com>.
2. Click **Sign in to the Console** (top right).
3. Select **Root user**, enter the *root email* and password.



The screenshot shows the AWS Sign In page. At the top, there are links for "New sign in", "Multi-session disabled", and "English". A blue information box states: "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." The AWS logo is centered. Below it, the "Sign In" section prompts the user to "Access your AWS account by user type." and offers two options: "Root user" (selected) and "IAM user". The "Root user" option is described as "Account owner that performs tasks requiring unrestricted access." The "IAM user" option is described as "User within an account that performs daily tasks." Below these options is a text input field for "Email address" with the placeholder "username@example.com". An orange "Next" button is below the email field. Below the "Next" button is an "OR" separator. At the bottom of the sign-in section is a button that says "New to AWS? Sign up". At the very bottom, there is a disclaimer: "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 more information." and a copyright notice: "© 2025 Amazon Web Services, Inc. or its affiliates. All rights reserved."

New sign in ▼ Multi-session disabled ▼ English ▼

Sign In

Access your AWS account by user type.

User type [\(not sure?\)](#)

☒ **Root user**
Account owner that performs tasks requiring unrestricted access.

☐ **IAM user**
User within an account that performs daily tasks.

Email address

Next

OR

New to AWS? Sign up

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 more information.

© 2025 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Create an IAM user with Console access

1. In the AWS Console search bar, type **IAM** and open **IAM (Identity & Access Management)**.
2. In the left navigation, click **Users**.
3. Click **Add users** (or **Create user**).
4. **User name**: type the desired user name (User_1).
5. **Check Provide user access to the AWS Management Console** (this enables console login). Then select **I want to create an IAM user**. A password area will appear.
6. Choose **Custom password**.
7. Enter the password you want to assign.
8. **Uncheck User must create a new password at next sign-in** (this prevents the forced password change).

The screenshot shows the AWS IAM 'Create user' console. The top navigation bar includes the AWS logo, a search bar, and account information (Account ID: 6780-2503-6602, Shaikh Ateeb Ahmed). The left sidebar shows the navigation menu with 'IAM' selected, and 'Users' > 'Create user' is the current path. The main content area is titled 'Specify user details' and contains the following sections:

- Step 1: Specify user details** (selected in the left sidebar). Other steps include 'Set permissions', 'Review and create', and 'Retrieve password'.
- User details**
 - User name**: A text input field containing 'User_1'. Below it, a note states: '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**. A note below says: '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**. A note: '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**. A note: '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**. A note: 'You can view the password after you create the user.'
 - ☒ **Custom password**. A note: 'Enter a custom password for the user.' Below this is a password input field with masked characters '*****'.

At the bottom of the form, there are additional options and a note:

- ☐ **Show password**
- ☐ **Users must create a new password at next sign-in - Recommended**. A note: 'Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.'
- A blue information box: '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](#)'

The bottom of the console features a 'Cancel' button and a 'Next' button.

9. Set permissions (choose how this user gets 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](#)

☐ 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 (1/1387)

Choose one or more policies to attach to your new user.

Filter by Type
All types

< 1 2 3 4 5 6 7 ... 70 >

CloudShell




















Feedback

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

Privacy

Terms

Cookie preferences

<input checked="" type="checkbox"/>	 AdministratorAccess	AWS managed - job function
<input type="checkbox"/>	 AdministratorAccess-Amplify	AWS managed
<input type="checkbox"/>	 AdministratorAccess-AWSElasticBeanst...	AWS managed
<input type="checkbox"/>	 AIOpsAssistantPolicy	AWS managed
<input type="checkbox"/>	 AIOpsConsoleAdminPolicy	AWS managed
<input type="checkbox"/>	 AIOpsOperatorAccess	AWS managed
<input type="checkbox"/>	 AIOpsReadOnlyAccess	AWS managed
<input type="checkbox"/>	 AlexaForBusinessDeviceSetup	AWS managed
<input type="checkbox"/>	 AlexaForBusinessFullAccess	AWS managed
<input type="checkbox"/>	 AlexaForBusinessGatewayExecution	AWS managed
<input type="checkbox"/>	 AlexaForBusinessLifesizeDelegatedAcc...	AWS managed
<input type="checkbox"/>	 AlexaForBusinessNetworkProfileServic...	AWS managed
<input type="checkbox"/>	 AlexaForBusinessPolyDelegatedAccess...	AWS managed
<input type="checkbox"/>	 AlexaForBusinessReadOnlyAccess	AWS managed
<input type="checkbox"/>	 AmazonAPIGatewayAdministrator	AWS managed
<input type="checkbox"/>	 AmazonAPIGatewayInvokeFullAccess	AWS managed
<input type="checkbox"/>	 AmazonAPIGatewayPushToCloudWatc...	AWS managed
<input type="checkbox"/>	 AmazonAppFlowFullAccess	AWS managed
<input type="checkbox"/>	 AmazonAppFlowReadOnlyAccess	AWS managed

► Set permissions boundary - optional

Cancel

Previous

Next

10. **Review and create.** Carefully review: **Console access = Enabled**, **Password = Custom**, **Force password reset = Unchecked**, and **Permissions = selected group/policies**.

The screenshot shows the AWS IAM console's 'Create user' wizard, specifically the 'Review and create' step. On the left, a progress bar indicates four steps: 'Specify user details', 'Set permissions', 'Review and create' (which is the active step), and 'Retrieve password'. The main content area is titled 'Review and create' and includes a sub-header 'Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.' Below this, there are three sections: 'User details' showing 'User name' as 'User_1', 'Console password type' as 'Custom password', and 'Require password reset' as 'No'; 'Permissions summary' showing a table with one entry 'AdministratorAccess' of type 'AWS managed - job function' used as a 'Permissions policy'; and 'Tags - optional' with a note that no tags are currently associated. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Create user'.

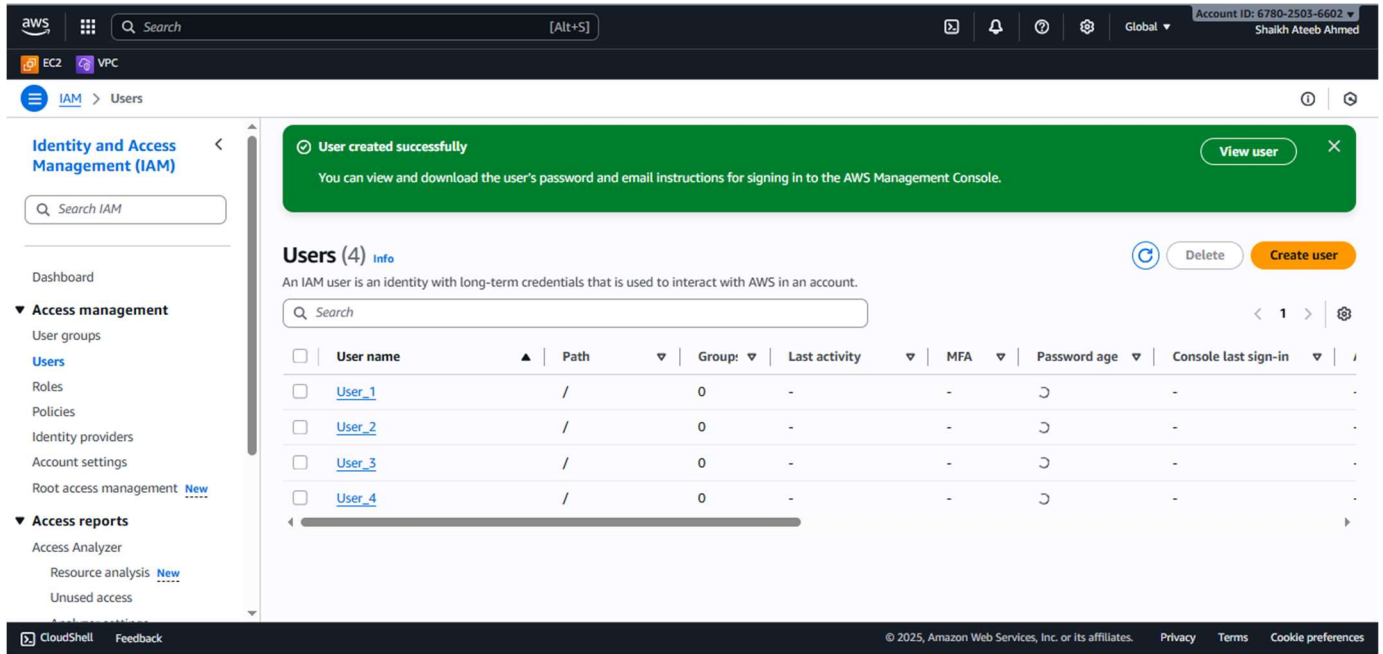
11. Click **Create user**.

12. **Save the results.** On the success page, **download the .csv** (if available) or **copy the sign-in URL and username**.

The screenshot shows the AWS IAM console's 'Retrieve password' step. A green success banner at the top states 'User created successfully' and provides a 'View user' link. The progress bar on the left now shows 'Retrieve password' as the active step. The main content area is titled 'Retrieve password' and includes a sub-header '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.' Below this, the 'Console sign-in details' section shows the 'Console sign-in URL' as 'https://678025036602.signin.aws.amazon.com/console', the 'User name' as 'User_1', and the 'Console password' as 'Ateeb@6867' with a 'Hide' link. At the bottom right, there are three buttons: 'Cancel', 'Download .csv file', and 'Return to users list'.

Create Multiple IAM Users in AWS

1. **Repeat Steps for three more users: User 2** → username: user_2, assign custom password, uncheck forced reset. **User 3** → username: user_3, assign custom password, uncheck forced reset. **User 4** → username: user_4, assign custom password, uncheck forced reset.
2. **Each user will now have:** IAM login credentials. Console access with your chosen password.



Create IAM user groups and add users

Create Group 1

1. Open **IAM**. In the left navigation panel click **User groups**.
2. Click **Create group**.
3. **Group name**: enter Developers.
4. Under **Attach permissions policies** → in the search box type AdministratorAccess. Check the box next to **AdministratorAccess** (this is the AWS managed policy that grants full admin). Click **Next**.

Name the group

Enter a meaningful name to identify this group.

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

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

< 1 >

User name

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.

 Policy name

5. **Add users:** check user1 and user4. Review, then click **Create group**.
6. After creation, click the group name to open its details and confirm **Permissions** and **Users** tabs show the attached policy and the two users.

Create Group 2

1. In **IAM** → **User groups** click **Create group** again.
2. **Group name:** enter ReadOnly (or preferred name).
3. Under **Attach permissions policies** search for AmazonEC2ReadOnlyAccess.
4. Check **AmazonEC2ReadOnlyAccess**.
5. Click **Next**, then on the **Add users** page select user2 and user3.

Developers user group created. [View group](#)

Create user group

Name the group

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

ReadOnly
Maximum 128 characters. Use alphanumeric and ".,@_-:" characters.

Add users to the group - Optional (2/4) [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.

Search

<input type="checkbox"/>	User name	Groups	Last activity	Creation time
<input type="checkbox"/>	User_1	1	None	33 minutes ago
<input checked="" type="checkbox"/>	User_2	0	None	25 minutes ago
<input checked="" type="checkbox"/>	User_3	0	None	24 minutes ago
<input type="checkbox"/>	User_4	1	None	24 minutes ago

Attach permissions policies - Optional (1/1072) [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.

Search: AmazonEC2ReadOnlyAccess

Filter by Type: All types (1 match)

<input checked="" type="checkbox"/>	Policy name	Type	Used as	Description
<input checked="" type="checkbox"/>	AmazonEC2ReadOnlyAccess	AWS managed	None	Provides read only access to Amazon EC2 via the AWS Manage...

[Cancel](#) [Create user group](#)

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Merge group policies

1. **Create group.** **Group name:** enter the group name FullAccess.
2. Under **Attach permissions policies**, in the search box type **AmazonS3FullAccess**. Check the box next to **AmazonS3FullAccess**
3. Click **Next**.
4. **Add users** select the existing users user2 and user4.
5. **Next: Review.** Review the group name, attached policy and users, then click **Create group**.

Create user group

Name the group

User group name

Enter a meaningful name to identify this group.

Fullaccess

Maximum 128 characters. Use alphanumeric and "+, @, -, ." characters.

Add users to the group - Optional (2/4) [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.

Search

<input type="checkbox"/>	User name	Groups	Last activity	Creation time
<input type="checkbox"/>	User_1	1	None	41 minutes ago
<input checked="" type="checkbox"/>	User_2	1	None	32 minutes ago
<input type="checkbox"/>	User_3	1	None	32 minutes ago
<input checked="" type="checkbox"/>	User_4	1	None	31 minutes ago

Attach permissions policies - Optional (1/1072) [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

Search: AmazonS3FullAccess

All types 1 match

<input checked="" type="checkbox"/>	Policy name	Type	Used as	Description
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS managed	None	Provides full access to all buckets via the AWS Management Console.

[Cancel](#) [Create user group](#)

To add AmazonS3FullAccess to an existing group and add users

- IAM → User groups → click the group name → **Permissions** → **Attach policies** → search AmazonS3FullAccess → attach.
- Then **Users** → **Add users** → check user2 and user4 → **Add users**.