

Creating a New Console User and Programmatic User on AWS

Part 1: Creating a New Console User

Step 1: Navigate to the IAM Dashboard

1. Log in to your AWS Management Console.
2. In the search bar, type **IAM** and select **IAM** from the results to open the IAM Dashboard.

The screenshot displays the AWS Management Console interface. At the top, the navigation bar includes the AWS logo, a search bar, and the user's name 'Pavithra_Athmanathan'. The main content area is divided into two sections. The left section, titled 'Console Home', shows a 'Recently visited' list with links to IAM, IAM Identity Center, EC2, Billing and Cost Management, and Route 53. The right section, titled 'Applications (0)', shows a 'Create application' button and a message stating 'No applications. Get started by creating an application.' Below these sections, there are three widgets: 'Welcome to AWS', 'AWS Health', and 'Cost and usage'. The bottom section of the screenshot shows the 'IAM Dashboard' with a left-hand navigation pane. The navigation pane includes 'Identity and Access Management (IAM)' and 'Access management' (with sub-items: User groups, Users, Roles, Policies, Identity providers, Account settings, Root access management). The main content area of the IAM Dashboard includes 'Security recommendations' (with two recommendations: 'Root user has MFA' and 'Root user has no active access keys'), 'IAM resources' (with a table showing 2 user groups, 2 users, 4 roles, 2 policies, and 0 identity providers), and 'What's new' (with updates for features in IAM). The right-hand side of the dashboard shows 'AWS Account' information (Account ID: 908027404221, Account Alias: aws-pavithra-v11) and 'Quick Links' (My security credentials, Manage your access keys, multi-factor authentication (MFA) and other credentials).

Step 2: Create a New User

1. In the left-hand navigation pane, click **Users**.
2. Click the **Add Users** button.
3. Enter a **User name** (e.g., ConsoleUser).

4. Under **Select AWS access type**, check **AWS Management Console access**.

- Choose **Custom password** and set a password for the user.
- Optionally, require the user to create a new password at next sign-in.

5. Click **Next: Permissions**.

Step 1: Specify user details

Step 2: Set permissions

Step 3: Review and create

Step 4: Retrieve password

Specify user details

User details

User name

Testuser

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.

☐ 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.

☐ 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](#)

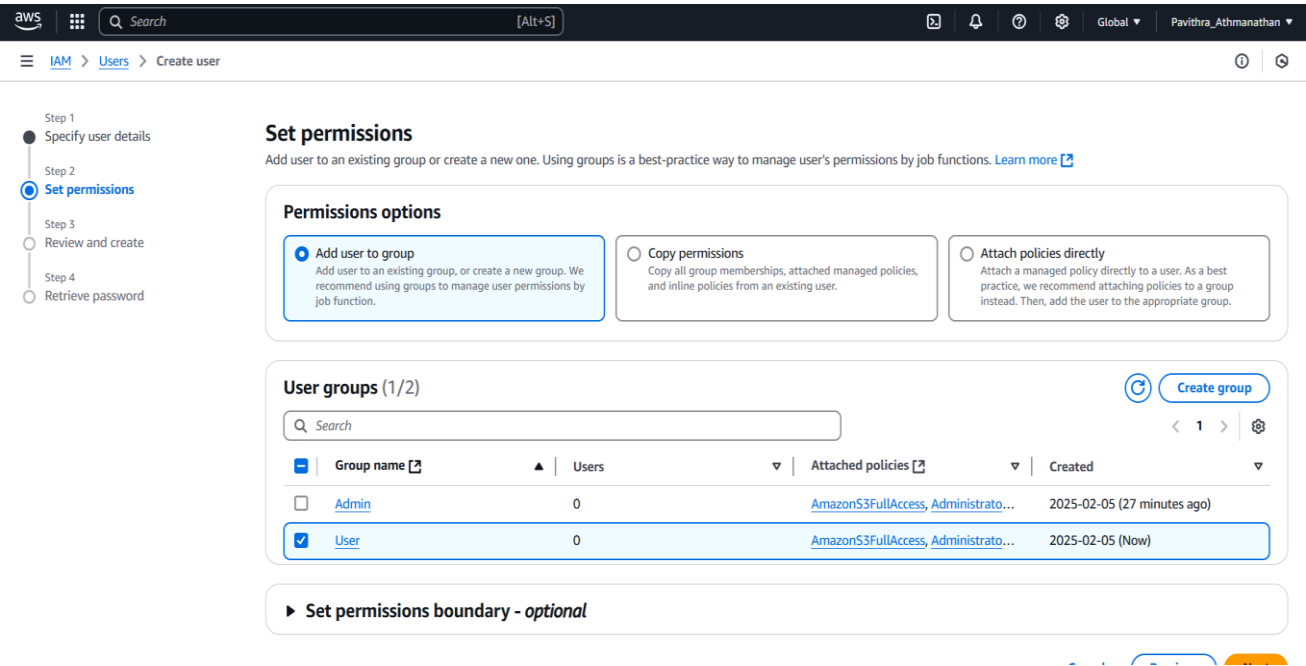
Cancel Next

Step 3: Assign Permissions

1. Choose how to assign permissions:

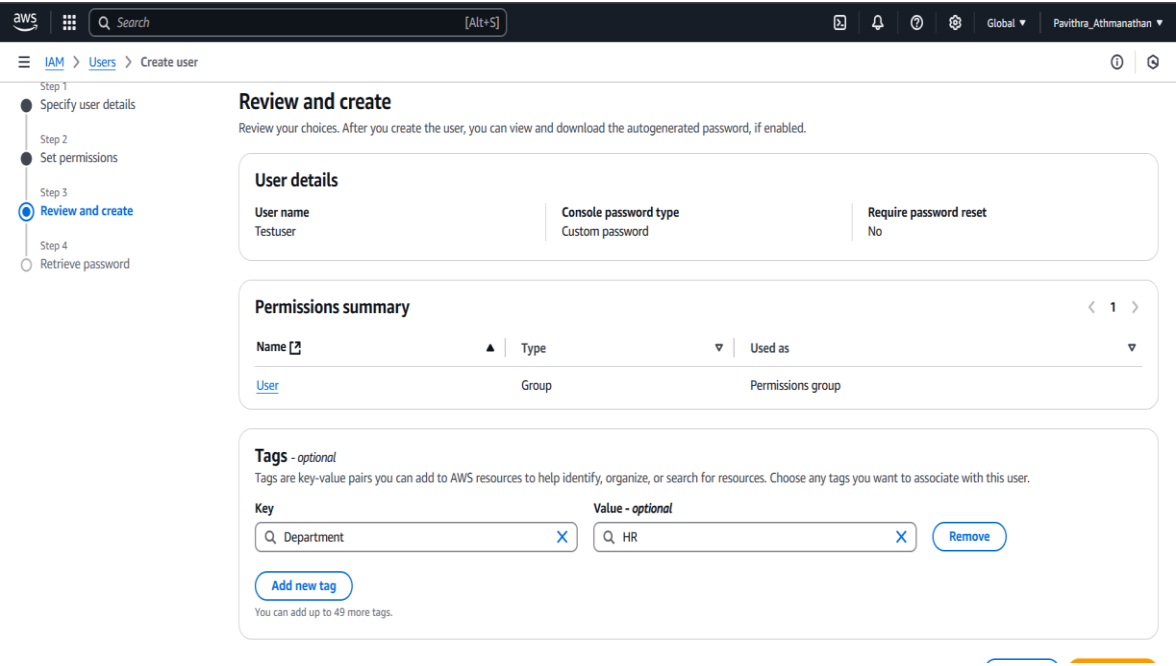
- **Add user to group:** Select an existing group with the required permissions.
- **Attach policies directly:** Select a policy, such as **AdministratorAccess**, **PowerUserAccess**, or a specific policy like **AmazonS3FullAccess**.
- **Copy permissions from existing user:** Copy permissions from another user if applicable.

2. Click **Next: Tags.**



Step 4: Add Tags (Optional)

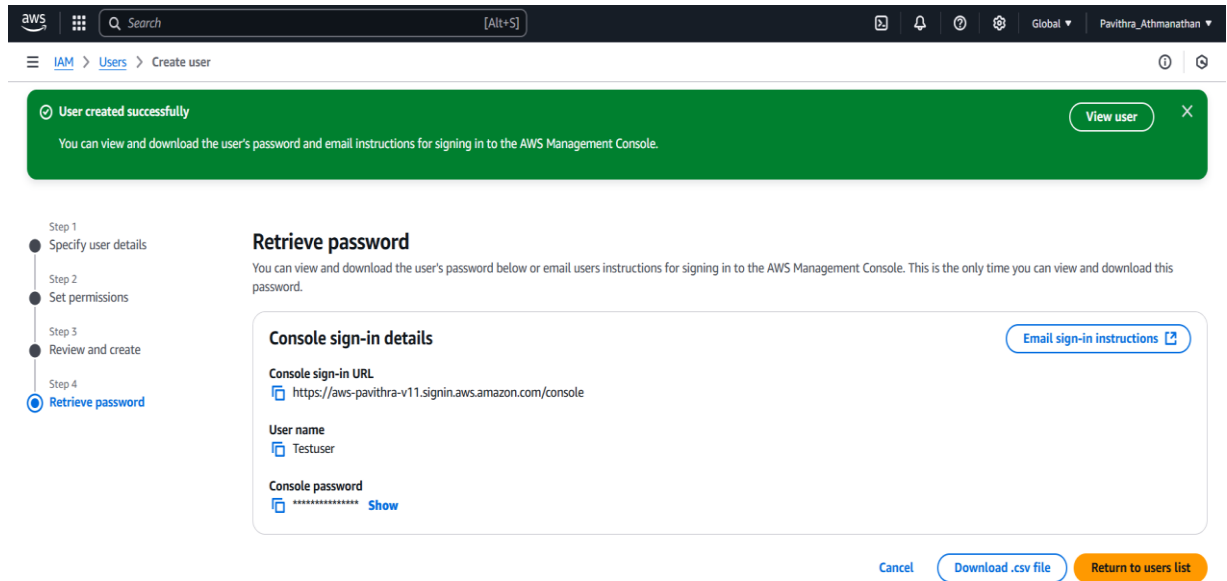
- 1. Add tags to help identify and manage the user (e.g., Key: Department, Value: IT).
- 2. Click **Next: Review.**



Step 5: Review and Create

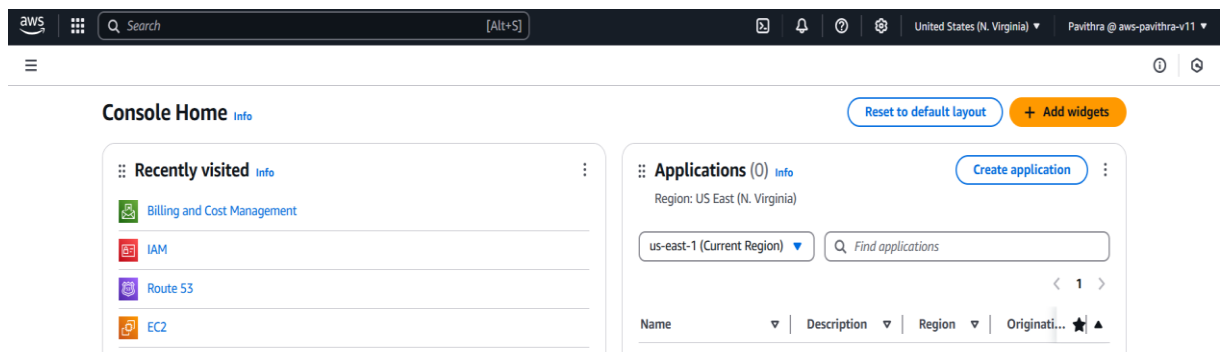
- 1. Review the user details.

2. Click **Create user**.
3. Note the login URL and provide it to the user.



Step 6: Test the Console User

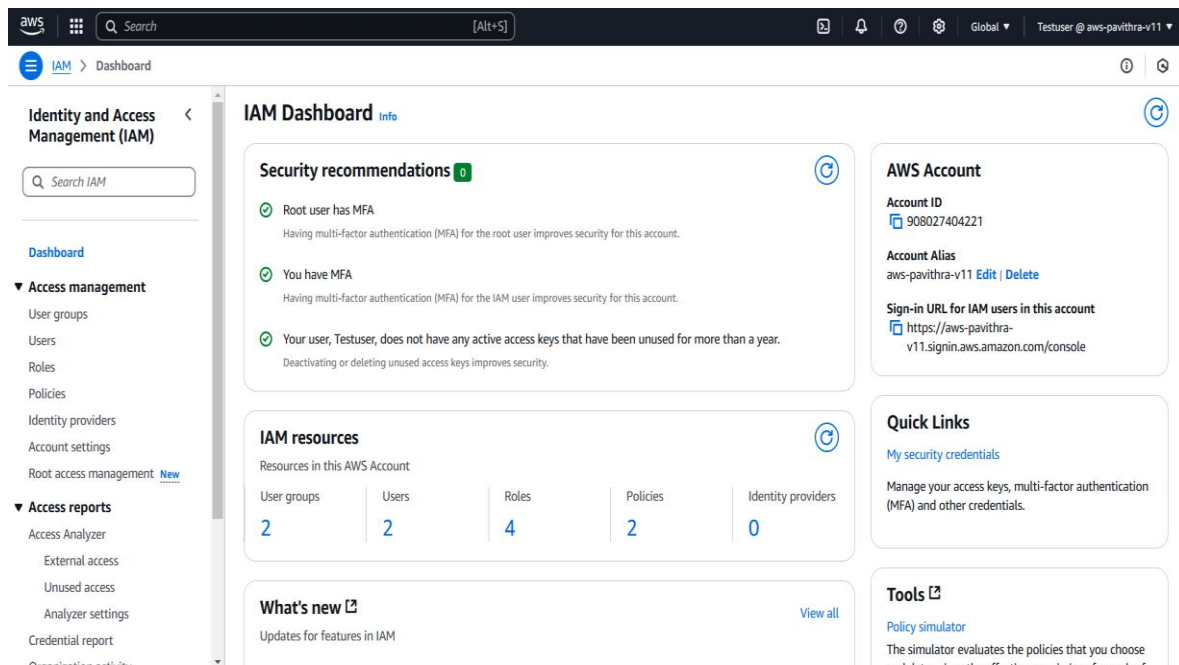
1. Log out of your AWS account.
2. Use the user login URL provided to sign in as the new user.
3. Verify that the user has access to the services specified by the permissions.



Part 2: Creating a Programmatic User

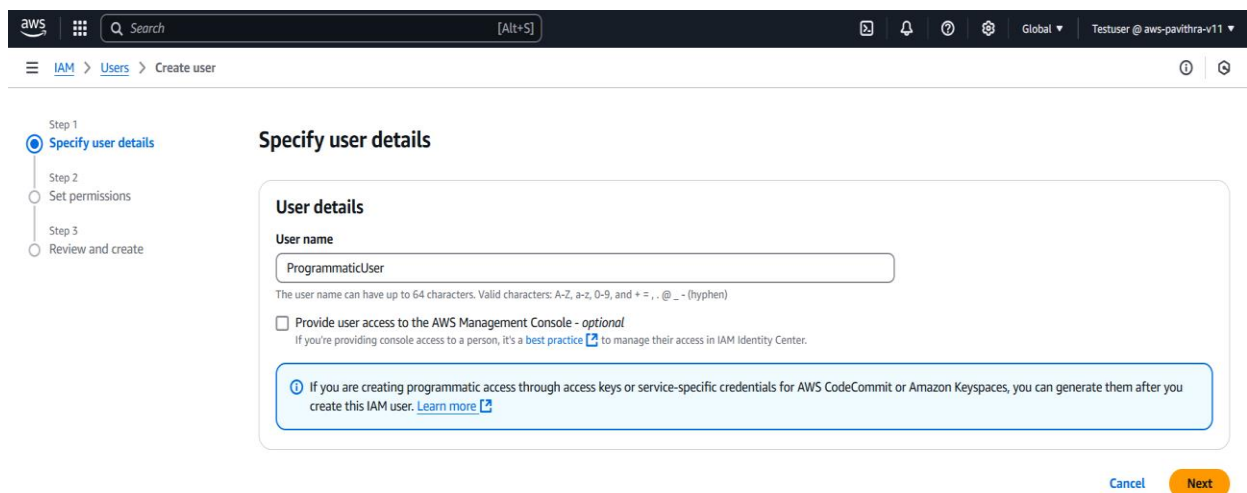
Step 1: Navigate to the IAM Dashboard

1. Log in to your AWS Management Console.
2. In the search bar, type **IAM** and select **IAM** from the results to open the IAM Dashboard.



Step 2: Create a New User

1. In the left-hand navigation pane, click **Users**.
2. Click the **Add Users** button.
3. Enter a **User name** (e.g., ProgrammaticUser).
4. Under **Select AWS access type**, check **Access key - Programmatic access**.
5. Click **Next: Permissions**.



Step 3: Assign Permissions

1. Choose how to assign permissions:
 - **Add user to group:** Select an existing group with the required permissions.

- **Attach policies directly:** Select a policy, such as **AdministratorAccess**, **PowerUserAccess**, or a specific policy like **AmazonS3FullAccess**.
- **Copy permissions from existing user:** Copy permissions from another user if applicable.

2. Click **Next: Tags**.

The screenshot shows the 'Set permissions' step of the AWS IAM 'Create user' wizard. On the left, a progress bar indicates four steps: 'Specify user details', 'Set permissions' (current), 'Review and create', and 'Set permissions boundary - optional'. The main content area is titled 'Set permissions' and includes a sub-header 'Permissions options' with three radio buttons: 'Add user to group' (selected), 'Copy permissions', and 'Attach policies directly'. Below this is a 'User groups (1/2)' section with a search bar and a table listing groups. The table has columns for 'Group name', 'Users', 'Attached managed policies', and 'Created'. Two groups are listed: 'Admin' and 'User'. The 'User' group is selected with a checkbox. At the bottom, there is a link to 'Set permissions boundary - optional'.

Group name	Users	Attached managed policies	Created
Admin	0	Amazon...	2025-02-05 (38 minutes ago)
User	2	Amazon...	2025-02-05 (11 minutes ago)

Step 4: Add Tags (Optional)

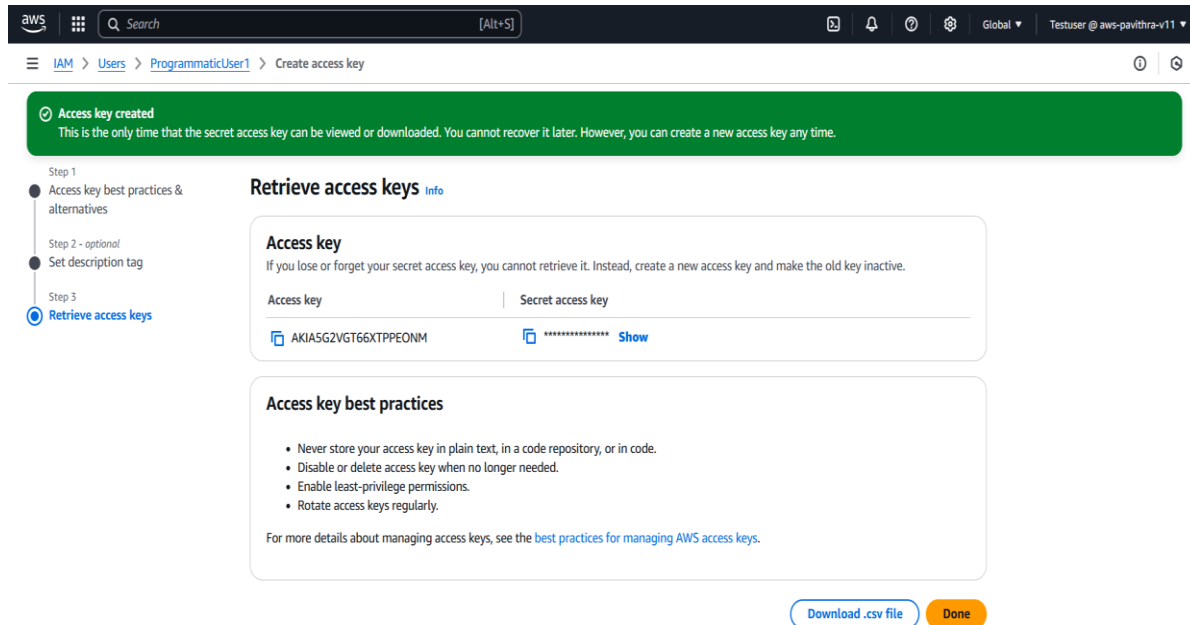
1. Add tags to help identify and manage the user (e.g., Key: Department, Value: DevOps).
2. Click **Next: Review**.

The screenshot shows the 'Review and create' step of the AWS IAM 'Create user' wizard. On the left, the progress bar shows four steps: 'Specify user details', 'Set permissions', 'Review and create' (current), and 'Set permissions boundary - optional'. The main content area is titled 'Review and create' and includes a sub-header 'User details' with three fields: 'User name' (ProgrammaticUser1), 'Console password type' (None), and 'Require password reset' (No). Below this is a 'Permissions summary' section with a table showing the user's permissions. The table has columns for 'Name', 'Type', and 'Used as'. One entry is shown: 'User' (Group) with 'Permissions group'. At the bottom, there is a 'Tags - optional' section with a search bar and a list of tags. Two tags are listed: 'Department' and 'DevOps'. There is a 'Remove' button and an 'Add new tag' button.

Name	Type	Used as
User	Group	Permissions group

Step 5: Review and Create

1. Review the user details.
2. Click **Create user**.
3. Download the **.csv file** containing the **Access Key ID** and **Secret Access Key**.
4. Click **Close**.



Step 6: Test the Programmatic User

1. **Configure AWS CLI:**
 - Open a terminal or command prompt.
 - Run the command: `aws configure`.
 - Enter the **Access Key ID** and **Secret Access Key**.
 - Specify the default region (e.g., `us-east-1`).
 - Specify the output format (e.g., `json`).
2. **Test Access:**
 - Run a simple AWS CLI command, such as:
 - `aws s3 ls`
 - If the permissions allow, this will list the S3 buckets in your account.

```
Invalid choice: 'config', maybe you meant:
```

- * configure
- * appconfig

```
~ $ aws configure
```

```
AWS Access Key ID [*****EONM]: AKIASGZVGT66XTTPEONM
```

```
AWS Secret Access Key [*****4UGR]:
```

```
Default region name [us-east-1]: us-east-1
```

```
Default output format [aws s3 ls]: json
```

```
~ $ aws s3 ls
```

```
~ $ aws s3 ls
```

```
2025-02-06 05:53:40 pavi-bckt
```
