

IAM - IDENTITY ACCESS MANAGEMENT

Step-1: Search IAM in the root user account and select.

The screenshot shows two side-by-side pages from the AWS console. On the left, a search results page for 'IAM' is displayed under the 'Services' section. The top result is 'IAM' with the sub-description 'Manage access to AWS resources'. Below it are 'IAM Identity Center', 'Resource Access Manager', and 'AWS App Mesh'. On the right, the 'IAM Identity Center' application page is shown. It has a header with 'Reset to default layout' and '+ Add widgets'. Below the header, there's a table with one row labeled '(0) Info'. A large central area says 'No applications' with the sub-instruction 'Get started by creating an application.' and a 'Create application' button. At the bottom, there's a 'Data unavailable' message with the note 'Have Cost Explorer enabled to view your cost and usage data.'

Step-2: Once we select it shows the page like this and there is no user by default.

The screenshot shows the 'Users' page within the AWS IAM service. The left sidebar includes options like 'Dashboard', 'Access management' (with 'User groups', 'Users', 'Roles', 'Policies', 'Identity providers', and 'Account settings'), 'Access reports' (with 'Access Analyzer', 'External access', 'Unused access', 'Analyzer settings', 'Credential report', 'Organization activity', and 'Service control policies'), and 'Related consoles' (with links to 'IAM Identity Center' and 'AWS Organizations'). The main content area is titled 'Users (0) info' and contains the sub-instruction 'An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.' Below this is a search bar and a table header with columns: 'User name', 'Path', 'Group', 'Last activity', 'MFA', 'Password age', 'Console last sign-in', 'Access key ID', and 'Active key age'. A message at the bottom of the table area states 'No resources to display'.

Step 3: Create a User by giving the user details.

The screenshot shows the 'Specify user details' step of the IAM User creation wizard. The left sidebar lists steps 1 through 4. Step 1 is 'Specify user details' (selected), Step 2 is 'Set permissions', Step 3 is 'Review and create', and Step 4 is 'Retrieve password'. The main area is titled 'User details' and contains a 'User name' field with 'Sakthi-123'. Below it is a note about character restrictions. A checkbox 'Provide user access to the AWS Management Console - optional' is checked, with a note about managing access in IAM Identity Center. A section titled 'Are you providing console access to a person?' has two options: 'Specify a user in Identity Center - Recommended' (radio button) and 'I want to create an IAM user' (radio button, selected). A note says '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 Kinesis, or a backup credential for emergency account access.' Below this is a 'Console password' section with 'Autogenerated password' (radio button) and 'Custom password' (radio button, selected, with 'Welcome123' entered). A note says 'Must be at least 8 characters long' and '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 (! @ # % ^ & * () _ - { } [] = [])`.' Checkboxes for 'Show password' and 'Users must create a new password at next sign-in - Recommended' are also present.

Step-4: Give permissions for the user.

The screenshot shows the 'Set permissions' step of the IAM User creation wizard. The left sidebar lists steps 1 through 4. Step 1 is 'Specify user details' (selected), Step 2 is 'Set permissions' (selected), Step 3 is 'Review and create', and Step 4 is 'Retrieve password'. The main area is titled 'Permissions options' and contains three choices: 'Add user to group' (selected), 'Copy permissions', and 'Attach policies directly'. A note says 'Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.' A 'Create group' button is available. Below this is a 'Get started with groups' note: 'Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions.' A 'Create group' button is also here. At the bottom is a note 'Set permissions boundary - optional' and buttons for 'Cancel', 'Previous', and 'Next' (highlighted).

Step-5: Once we give the permission, then create the user. Here the user only has permission to reset the password.

User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

Retrieve password

Console sign-in details

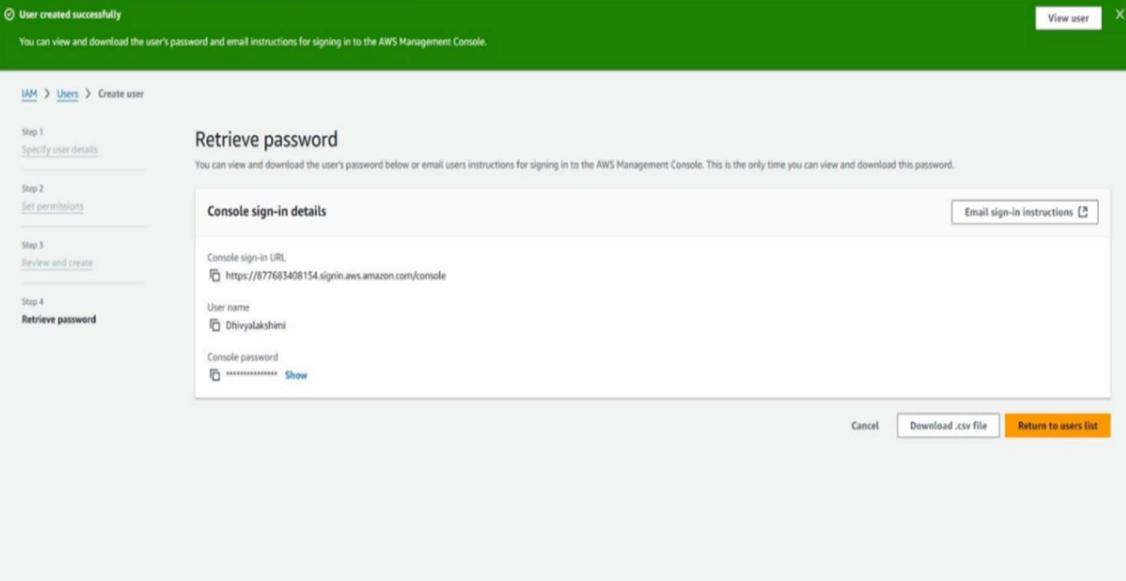
Console sign-in URL:
<https://877683408154.sigin.aws.amazon.com/console>

User name:
 Dhivyalakshmi

Console password:
 ***** [Show](#)

Email sign-in instructions [View user](#) [X](#)

Cancel [Download .csv file](#) [Return to users list](#)



Step 6: Once the user is created, log in to AWS with the created user credentials.

Try the new sign in UI
See our new improved Amazon Web Services sign in experience before we officially launch.
[Enable new sign in](#) [X](#)

aws

Sign in as IAM user

Account ID (12 digits) or account alias

IAM user name

Password

Remember this account

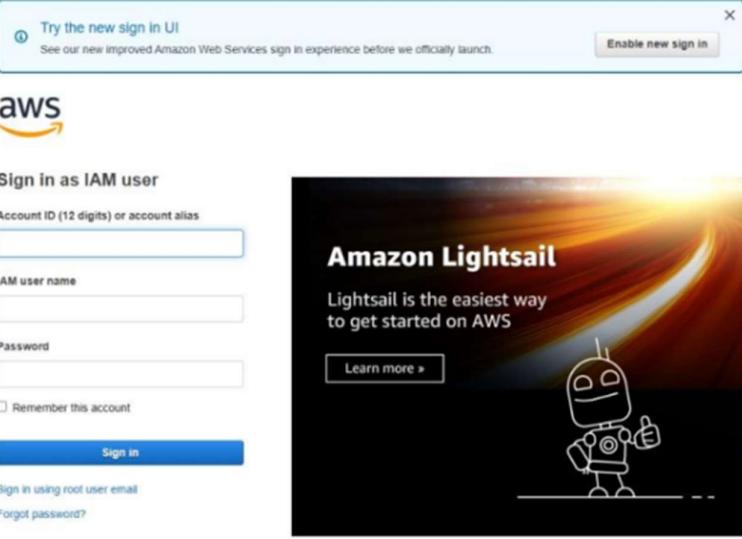
[Sign in](#)

[Sign in using root user email](#)
[Forgot password?](#)

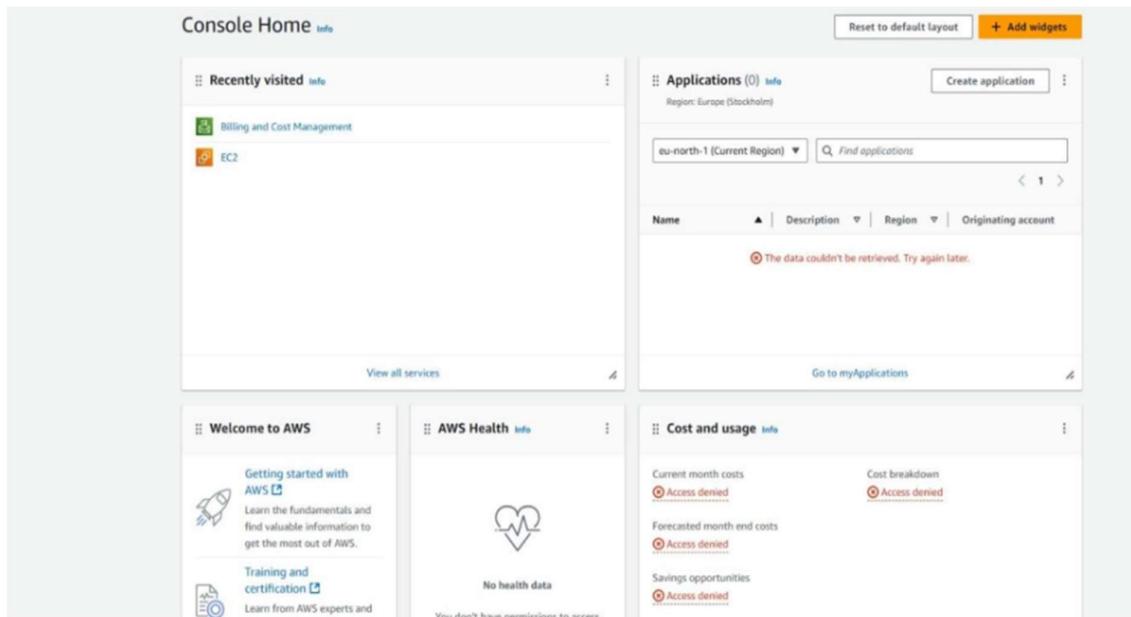
Amazon Lightsail
Lightsail is the easiest way to get started on AWS
[Learn more >](#)

English [▼](#)

Terms of Use Privacy Policy © 1999-2024, Amazon Web Services, Inc. or its affiliates.



Step-7: Once you log in, it shows the console page of the created user like this.



Step-8: Here we don't have permission to access the ec2 and the rest of the things.

This screenshot shows the IAM User details page for 'Sakthi-123'. The left sidebar lists various IAM management options like Access management, Access reports, and Related consoles. The main panel shows the user's ARN (arn:aws:iam::540168446522:user/Sakthi-123), creation date (October 15, 2024), and console access status (Enabled without MFA, Last console sign-in today). The 'Permissions' tab is selected, showing a table with one row: 'Policy name' (not set), 'Type' (All types), and 'Attached via' (Loading policies). Other tabs include Groups, Tags, Security credentials, and Last Accessed.

Step-9: Go back to root user account > IAM Console > User > Select the created user > Permit by selecting add permission >select AmazonS3FullAccess.

Screenshot of the AWS IAM 'Add permissions' step 1: Add permissions. The 'Attach policies directly' option is selected. A search bar finds 's3fullaccess' in the 'Permissions policies' list, which contains one item: 'AmazonS3FullAccess'.

Step-10: After selecting the permission give add permission.

Screenshot of the AWS IAM 'Review' step 2: Review. It shows the user details (User name: Sakthi-123) and the permissions summary (AmazonS3FullAccess). The 'Add permissions' button is highlighted in orange.