

Experiment 3 — Create IAM User with S3 Access

Aim:

To create an IAM user and grant S3 full access.

Procedure:

1. IAM → Users → Create User.

The screenshot shows the AWS search interface with the query 'iam'. The top result is the 'IAM' service card, which is highlighted with a blue border. The card contains the text 'Manage access to AWS resources' and 'Top features: Groups, Users, Roles, Policies, Access Analyzer'. Below the service card, there are other cards for 'IAM Identity Center' and 'Resource Access Manager'. On the left sidebar, there are links for 'Services', 'Features', 'Documentation', 'Marketplace', 'Blog posts', 'Events', and 'Tutorials'. At the bottom of the search results, there are 'Yes' and 'No' buttons for a survey question: 'Were these results helpful?'. The URL in the address bar is <https://us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/us...>.

The screenshot shows the 'Users' page under the 'Identity and Access Management (IAM)' section. The left sidebar has navigation links for 'Dashboard', 'Access Management' (with 'Users' selected), 'Policies', 'Identity providers', 'Account settings', 'Root access management', and 'Temporary delegation requests'. The main content area is titled 'Users (0) Info' and states 'An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.' A search bar and a table header for 'User name' are visible. The message 'No resources to display' is centered below the table. The URL in the address bar is <https://us-east-1.console.aws.amazon.com/iam/users?region=eu-north-1>.

2. Enter username.
3. Enable console access.

Screenshot of the AWS IAM 'Create user' wizard Step 1: Specify user details.

User details

- User name:** mjuser
- Provide user access to the AWS Management Console - optional:** In addition to console access, users with SignInLocalDevelopmentAccess permissions can use the same console credentials for programmatic access without the need for access keys.
- Console password:**
 - Autogenerated password: You can view this 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) - [] { }

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](#)

Next Step

4. Attach policy → **AmazonS3FullAccess**.

Screenshot of the AWS IAM 'Create user' wizard Step 2: Set permissions.

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 (1/1445)

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

Policy name	Type	Attached entities
<input checked="" type="checkbox"/> AmazonS3FullAccess	AWS managed	0
<input type="checkbox"/> AmazonDMSRedshiftS3Role	AWS managed	0
<input type="checkbox"/> AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	0
<input type="checkbox"/> AmazonS3OutpostsFullAccess	AWS managed	0
<input type="checkbox"/> AmazonS3OutpostsReadOnlyAccess	AWS managed	0
<input type="checkbox"/> AmazonS3ReadOnlyAccess	AWS managed	0
<input type="checkbox"/> AmazonS3TablesFullAccess	AWS managed	0

Screenshot of the AWS IAM 'Create user' wizard Step 3: Review and create.

Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

- User name:** mjuser
- Console password type:** Custom password
- Require password reset:** Yes

Permissions summary

Name	Type	Used as
AmazonS3FullAccess	AWS managed	Permissions policy
IAMUserChangePassword	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.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Create user

5. Create user.

The screenshot shows the AWS Console Home page. On the left, there's a sidebar with 'Recently visited' links for IAM, Billing and Cost Management, and S3. The main area is titled 'Applications (0)' with a 'Create application' button. It shows a message: 'No applications. Get started by creating an application.' Below this is a 'Create application' button. At the bottom of the page, there are links for CloudShell, Feedback, and Console Mobile App.

The screenshot shows the 'IAM user sign in' page. It has fields for 'Account ID or alias' (232351105360), 'Remember this account' (unchecked), 'IAM username' (mjuser), 'Password' (*****), 'Show Password' (unchecked), 'Having trouble?' (link), and a 'Sign in' button. To the right is a promotional banner for 'Amazon Lightsail' with the text 'Lightsail is the easiest way to get started on AWS' and a 'Learn more' link. The AWS logo is at the top center.

The screenshot shows the 'User created successfully' confirmation message in a green box: 'You can view and download the user's password and email instructions for signing in to the AWS Management Console.' Below it, the 'View user' button is visible. On the left, a vertical navigation bar shows steps: Step 1 (Specify user details), Step 2 (Set permissions), Step 3 (Review and create), and Step 4 (Retrieve password) which is currently selected. The main area is titled 'Retrieve password' with 'Console sign-in details'. It shows the 'Console sign-in URL' (https://232351105360.signin.aws.amazon.com/console), 'User name' (mjuser), and 'Console password' (*****). There's a 'Show' link next to the password field. Buttons for 'Cancel', 'Download .csv file', and 'Return to users list' are at the bottom.

Result:

IAM user created with S3 permissions.

IAM users allow controlled access instead of root login.

6. Go to IAM → User groups.

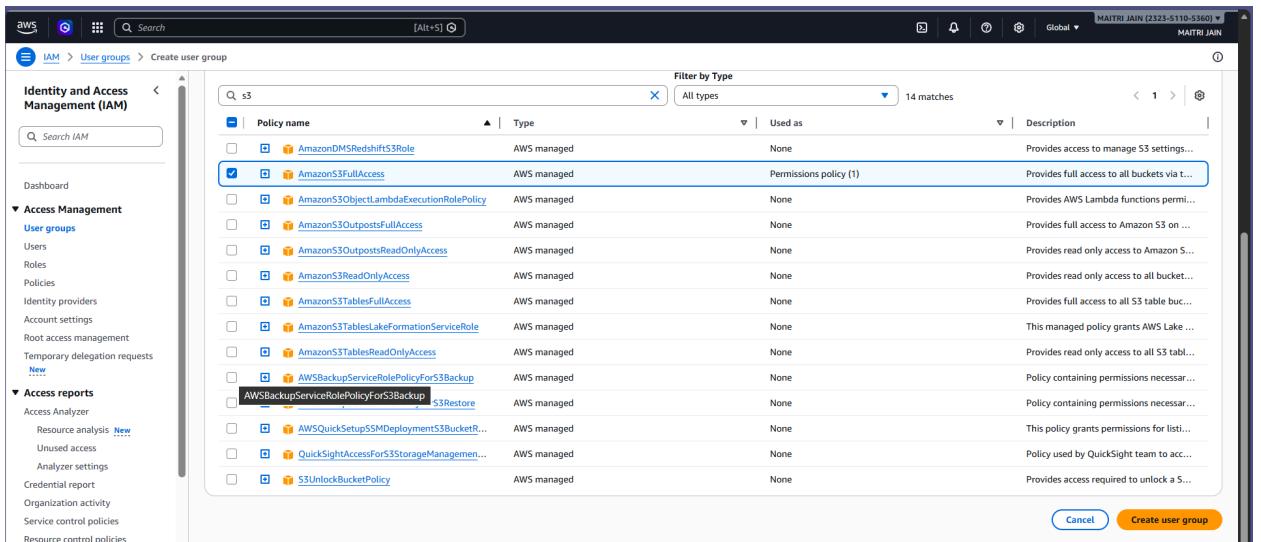
The screenshot shows the AWS IAM User groups page. The left sidebar has sections for Identity and Access Management (IAM) like Dashboard, Access Management (User groups, Users, Roles, Policies, Identity providers, Account settings, Root access management, Temporary delegation requests), Access reports (Access Analyzer, Resource analysis, Unused access, Analyzer settings, Credential report, Organization activity, Service control policies, Resource control policies), and CloudShell, Feedback, Console Mobile App links. The main content area is titled "User groups (0) Info" and says "A user group is a collection of IAM users. Use groups to specify permissions for a collection of users." It has a search bar and columns for Group name, Users, Permissions, and Creation time. A message at the bottom says "No resources to display". The top right shows MAITRI JAIN (2323-5110-5360) and Global dropdowns.

7. Click Create group.

The screenshot shows the "Create user group" page. The left sidebar is identical to the previous screenshot. The main content area has three sections: "Name the group" with a "User group name" input field (placeholder "Enter a meaningful name to identify this group.", note "Maximum 128 characters. Use alphanumeric and '-' characters."), "Add users to the group - Optional (1) Info" with a table showing one user "mjuser" (Last activity 29 minutes ago, Creation time 32 minutes ago), and "Attach permissions policies - Optional (111) Info" with a table showing three policies: "AccountManagementFromVercel" (AWS managed, None used), "AdministratorAccess" (AWS managed - job function, None used), and "AmazonS3FullAccess" (AWS managed, None used). The top right shows MAITRI JAIN (2323-5110-5360) and Global dropdowns.

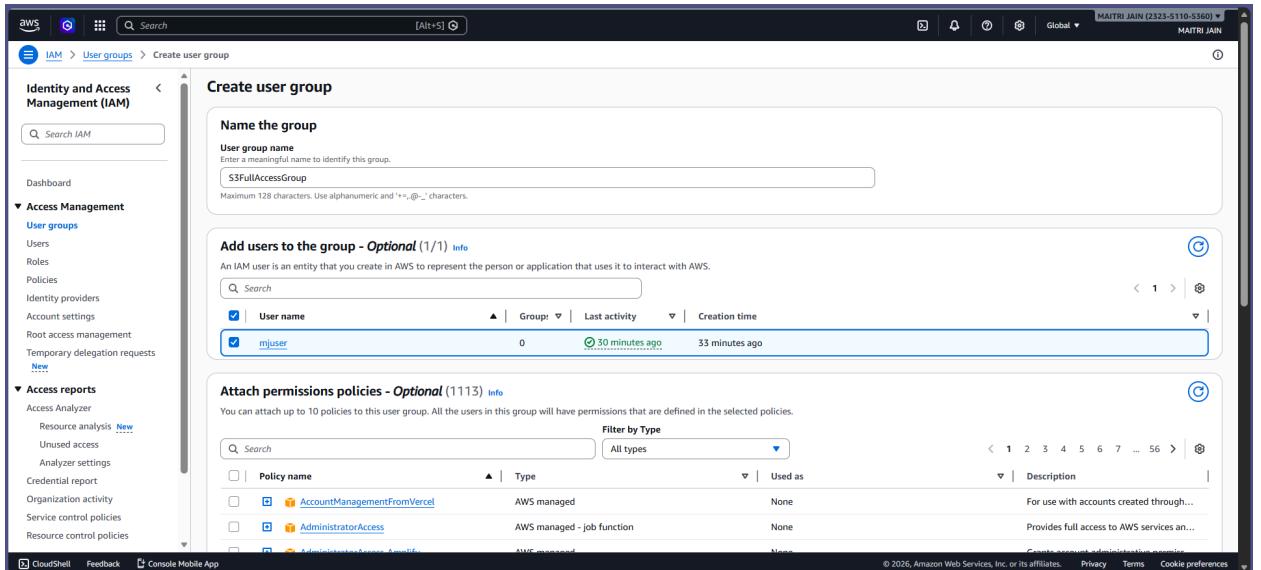
8. Enter group name S3FullAccessGroup.

9. Attach AmazonS3FullAccess policy.



The screenshot shows the 'Create user group' interface in the AWS IAM console. On the left, the navigation sidebar includes 'Identity and Access Management (IAM)', 'Dashboard', and sections for 'Access Management' (User groups, Roles, Policies), 'Access reports' (Access Analyzer, Resource analysis, Unused access, Analyzer settings, Credential report, Organization activity, Service control policies, Resource control policies), and 'New' (Temporary delegation requests). The main area is titled 'Create user group' and contains three tabs: 'Name the group', 'Add users to the group - Optional (1/1)', and 'Attach permissions policies - Optional (1113)'. The 'Name the group' tab has a 'User group name' input field containing 'S3FullAccessGroup'. The 'Add users to the group' tab shows a single user named 'mjuiser' selected. The 'Attach permissions policies' tab shows a list of policies, with 'AmazonS3FullAccess' selected and highlighted in blue. A search bar at the top is set to 's3'. The bottom of the screen displays standard AWS footer links: CloudShell, Feedback, Console Mobile App, Privacy, Terms, and Cookie preferences.

Policy name	Type	Used as	Description
<input checked="" type="checkbox"/>  AmazonS3FullAccess	AWS managed	Permissions policy (1)	Provides full access to all buckets via ...
<input type="checkbox"/>  AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	None	Provides AWS Lambda functions permi...
<input type="checkbox"/>  AmazonS3OutpostsFullAccess	AWS managed	None	Provides full access to Amazon S3 on ...
<input type="checkbox"/>  AmazonS3OutpostsReadOnlyAccess	AWS managed	None	Provides read only access to Amazon S...
<input type="checkbox"/>  AmazonS3ReadOnlyAccess	AWS managed	None	Provides read only access to all bucket...
<input type="checkbox"/>  AmazonS3TablesFullAccess	AWS managed	None	Provides full access to all S3 table bu...
<input type="checkbox"/>  AmazonS3TablesLakeFormationServiceRole	AWS managed	None	This managed policy grants AWS Lake ...
<input type="checkbox"/>  AmazonS3TablesReadOnlyAccess	AWS managed	None	Provides read only access to all S3 tabl...
<input type="checkbox"/>  AWSBackupServiceRolePolicyForS3Backup	AWS managed	None	Policy containing permissions necessar...
<input type="checkbox"/>  AWSBackupServiceRolePolicyForS3Restore	AWS managed	None	Policy containing permissions necessar...
<input type="checkbox"/>  AWSQuickSetupSSMDeploymentS3BucketR...	AWS managed	None	This policy grants permissions for listi...
<input type="checkbox"/>  QuickSightAccessForS3StorageManagemen...	AWS managed	None	Policy used by QuickSight team to acc...
<input type="checkbox"/>  S3UnlockBucketPolicy	AWS managed	None	Provides access required to unlock a S...



The screenshot shows the 'Create user group' interface in the AWS IAM console, identical to the previous one but with a different policy selected. The 'Attach permissions policies' tab now shows the 'AdministratorAccess' policy selected and highlighted in blue. The other policies listed are 'AccountManagementFromVercel', 'AdministratorAccess', and 'AdministratorAccess - job function'. The rest of the interface remains the same, including the 'Name the group' and 'Add users to the group' sections.

Policy name	Type	Used as	Description
<input type="checkbox"/>  AccountManagementFromVercel	AWS managed	None	For use with accounts created through...
<input type="checkbox"/>  AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services an...
<input type="checkbox"/>  AdministratorAccess - job function	AWS managed	None	Provides full access to AWS services an...

10. Create the group.

The screenshot shows the AWS IAM User Groups page. A green success message at the top states "S3FullAccessGroup user group created." The main table displays one user group named "S3FullAccessGroup". The table has columns for Group name, Users, Permissions, and Creation time. The "Permissions" column shows "Defined" and "Now".

11. Open IAM → Users → (your username).

12. Click Add user to group.

13. Select S3FullAccessGroup.

The screenshot shows the AWS IAM User page for the user "mjuser". Under the "Permissions" tab, it lists two attached policies: "AmazonS3FullAccess" and "IAMUserChangePassword", both of which are AWS managed policies attached directly via the group "S3FullAccessGroup".

14. Click Add.

Result: IAM user and user group were successfully created, and S3 Full Access permission was assigned to the user through the group.

Conclusion: IAM groups help manage permissions efficiently and securely by assigning policies to groups instead of individual users.