

IAM- Identity Access Management

Aunthentication:

It means users entering their username and password.

Authorization:

It means what rights are given to the users to perform their operations.

IAM User:

An **IAM User** is an individual identity in AWS with specific **login credentials**.

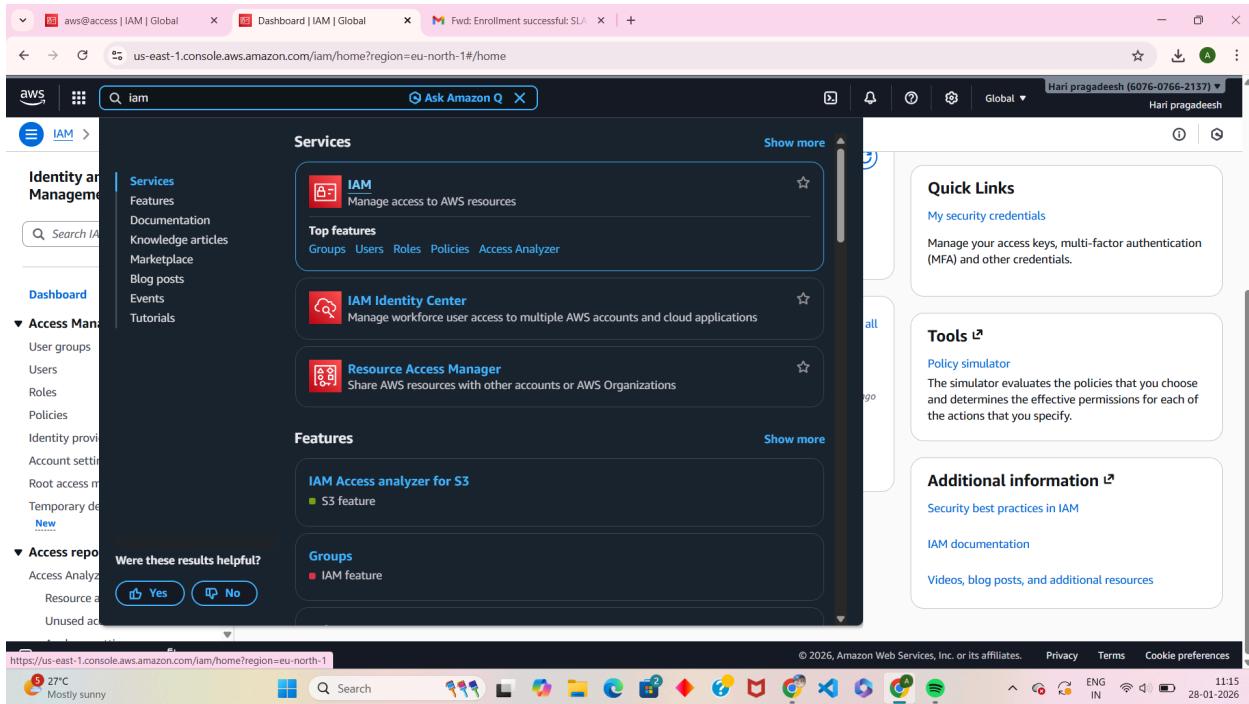
It represents a **person or application** and is given **permissions** to access AWS resources.

IAM Group:

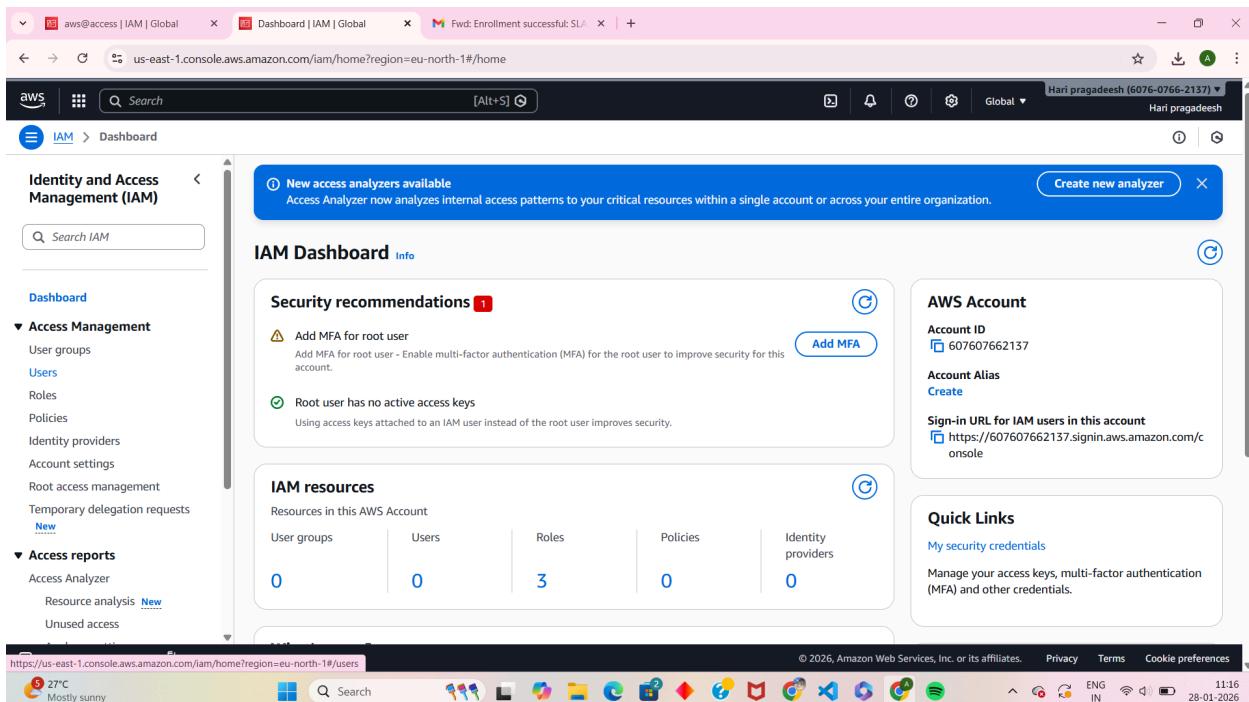
An **IAM Group** is a collection of IAM users.

Permissions are assigned to the **group**, and all users in the group automatically get those permissions.

Now we can see how to create IAM user in AWS



- In search bar enter IAM and click IAM



- Then the IAM dashboard will open.
- Then click users.

The screenshot shows the AWS IAM console with the 'Users' section selected. The left sidebar includes 'Access Management' (User groups, Users, Roles, Policies, Identity providers, Account settings, Root access management, Temporary delegation requests) and 'Access reports' (Access Analyzer, Resource analysis, Unused access). The main content area displays the 'Users (0)' page with a search bar and a table header for 'User name', 'Path', 'Group', 'Last activity', 'MFA', 'Password age', 'Console last sign-in', and 'Access summary'. A message states 'No resources to display'. The top navigation bar shows tabs for 'aws@access | IAM | Global', 'Create user | IAM | Global', and 'Fwd: Enrollment successful: SL...'.

Opened **Users** section in IAM

No IAM users created yet

Option available to **Create user**

The screenshot shows the 'Create user' wizard at Step 3: User details. The left sidebar shows steps: Step 3 (Review and create), Step 4 (Retrieve password). The main form has a 'User name' field containing 'loki'. Below it is a note: 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and +, ., @, _, - (hyphen)'. A checked checkbox says 'Provide user access to the AWS Management Console - optional'. Under 'Console password', the 'Autogenerated password' option is selected. A note says: 'You can view the password after you create the user.' Below is a 'Custom password' field with a note: 'Enter a custom password for the user.' A note below 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 ! @ # \$ % ^ & * () _ + - (hyphen) = [] { } | ^'. A checked checkbox says 'Users must create a new password at next sign-in - Recommended'. A note says: 'Users automatically get the IAMUserChangePassword policy to allow them to change their own password.' A callout box says: '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'.

Started creating a new IAM user

Entered user name: loki

Enabled AWS Management Console access

Selected auto-generated password

Enabled “User must change password at next sign-in”

The screenshot shows the AWS IAM 'Create user' wizard, Step 2: Set permissions. The left sidebar shows steps 1 through 4. Step 2, 'Set permissions', is selected and highlighted with a blue circle. The main content area is titled 'Set permissions' and contains the following options:

- Permissions options**
 - Add user to group**: 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](#)
 - 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.
- Get started with groups**: 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. [Learn more](#)

At the bottom right of the main content area are 'Cancel', 'Previous', and 'Next' buttons. The bottom of the screen shows the Windows taskbar with various pinned icons and system status information.

Selected Add user to group (best practice)

No group created yet

Permissions to be assigned using groups

The screenshot shows the 'Create user' process in the AWS IAM console. The user is at the 'Review and create' step, which is the final step before creating the user. The user details section shows a user named 'loki' with an auto-generated password type. The permissions summary section shows the attached policy 'IAMUserChangePassword'. The tags section is empty. At the bottom right, there are 'Cancel', 'Previous', and 'Create user' buttons.

- Reviewed user details
- Console password type: Auto-generated
- Password reset required at first login
- Attached policy: **IAMUserChangePassword**

The screenshot shows the AWS IAM 'Create user' wizard at Step 4: Retrieve password. A green success message box says 'User created successfully'. Below it, a note says 'You can view and download the user's password and email instructions for signing in to the AWS Management Console.' A 'View user' button is present. To the left, a vertical navigation path shows Step 1 (Specify user details), Step 2 (Set permissions), Step 3 (Review and create), and Step 4 (Retrieve password, which is highlighted). On the right, under 'Console sign-in details', there is a 'Console sign-in URL' (https://607607662137.signin.aws.amazon.com/console), a 'User name' (loki), and a 'Console password' field with a 'Show' link. Buttons for 'Email sign-in instructions', 'Download .csv file', and 'Return to users list' are at the bottom. The browser status bar shows the date as 28-01-2026.

IAM user **loki** created successfully

Confirmation message displayed

Option to view user details

This screenshot is identical to the one above, showing the AWS IAM 'Create user' wizard at Step 4: Retrieve password. It includes the success message, URL, and password fields. A download notification in the top right corner shows two files: 'loki_credentials (1).csv' (109 B) and 'jai_credentials.csv' (106 B), both from 28-01-2026. The browser status bar shows the date as 28-01-2026.

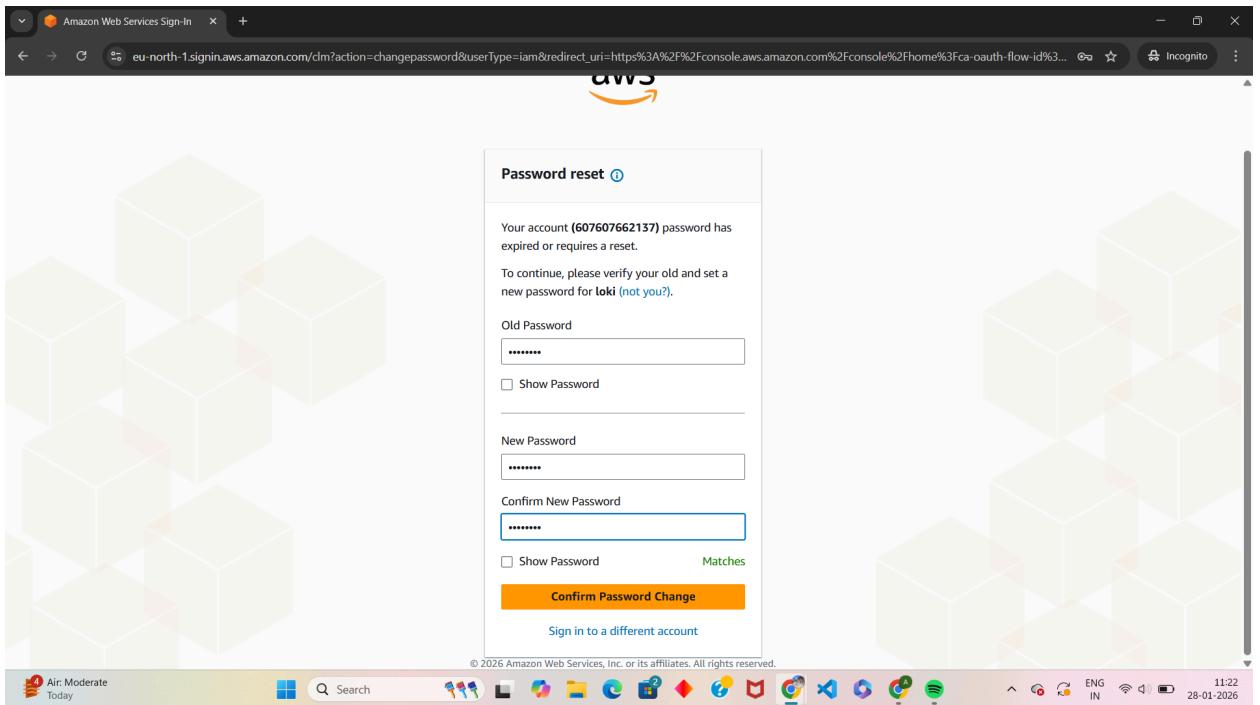
Credentials downloaded as **CSV file**

File contains username and password

Used for first-time login

The screenshot shows the AWS IAM 'Create user' page. At the top, there are three tabs: 'aws@access | IAM | Global', 'Create user | IAM | Global', and 'Fwd: Enrollment successful: SL/...'. The main content area displays a success message: 'User created successfully' and 'You can view and download the user's password and email instructions for signing in to the AWS Management Console.' A 'View user' button is present. To the left, a vertical navigation bar lists steps: Step 1 (Specify user details), Step 2 (Set permissions), Step 3 (Review and create), and Step 4 (Retrieve password), with Step 4 being the current active step. On the right, under 'Retrieve password', it says '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.' It shows a 'Copied' message next to 'Sign-in details' and provides a 'Console sign-in URL' (https://607607662137.signin.aws.amazon.com/console). It also lists 'User name' (loki) and 'Console password' (*****). Buttons for 'Email sign-in instructions' and 'Download .csv file' are available. The bottom of the screen shows a Windows taskbar with various icons and system status.

- Console sign-in URL copied
- User can log in using provided credentials
- Password must be changed after first login

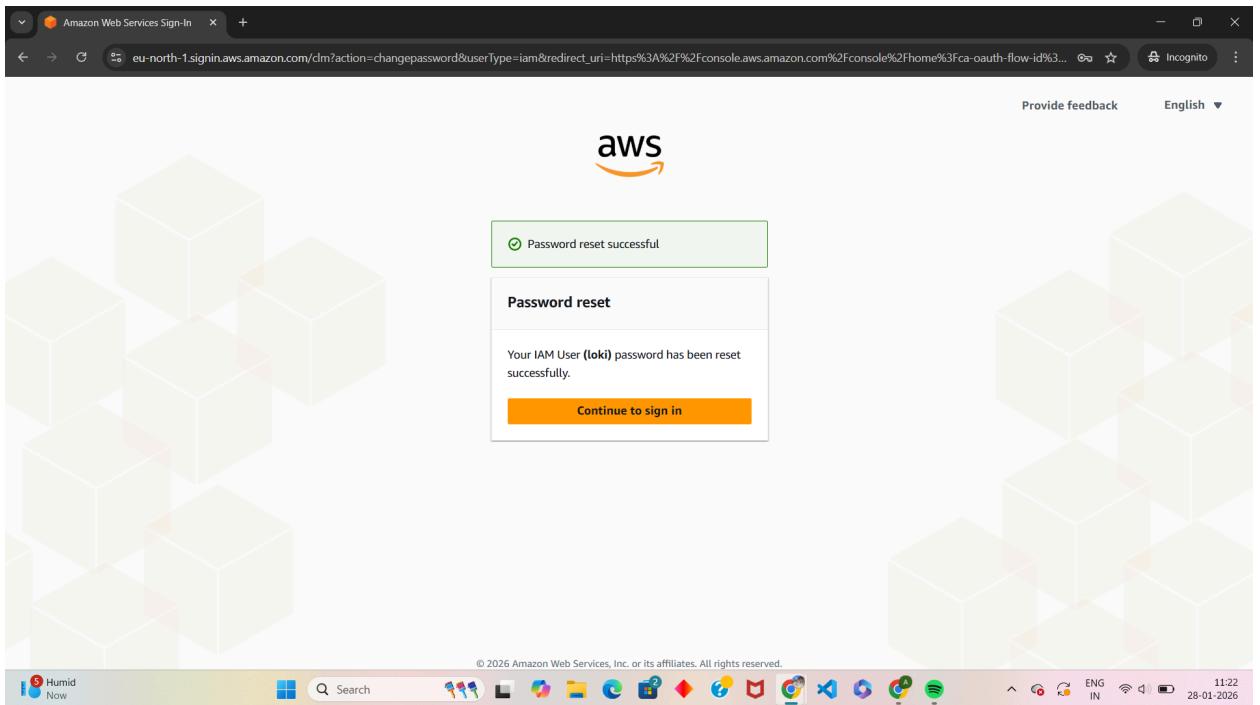


IAM user **loki** is signing in for the first time

AWS forces password reset (temporary password expired)

Old password entered

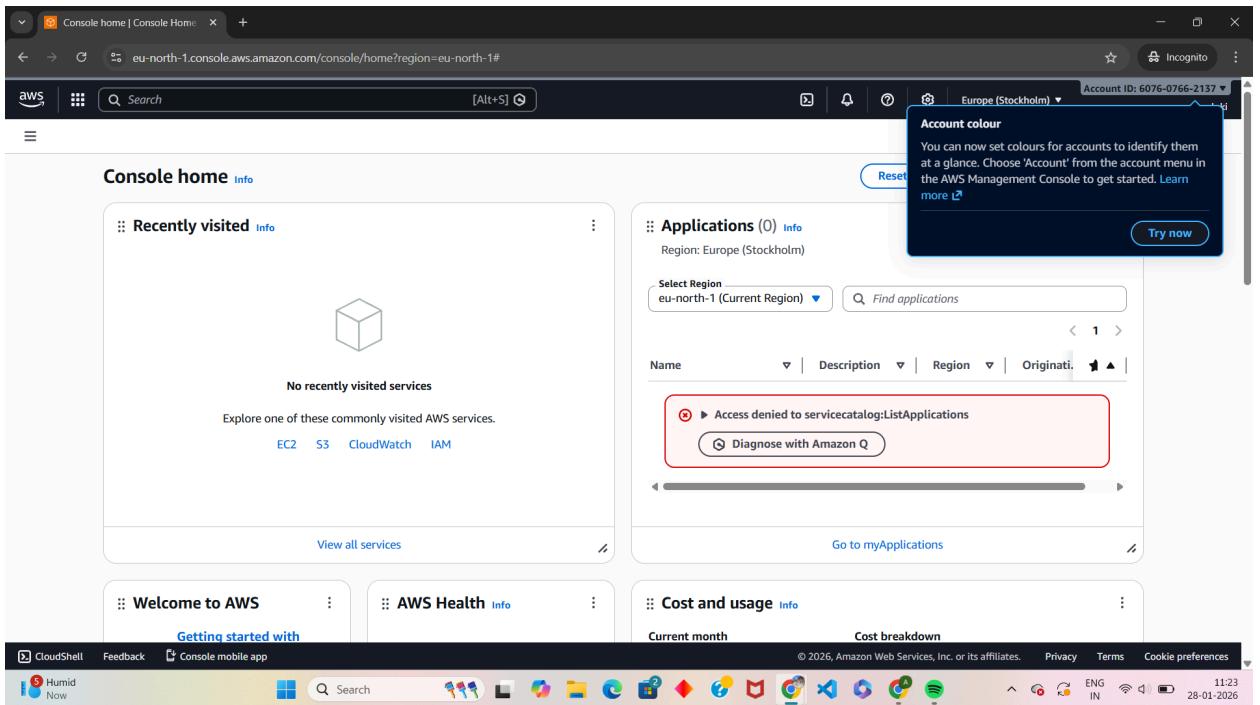
New password and confirm password entered



Password reset completed successfully

IAM user **loki** password updated

User can continue to AWS Console

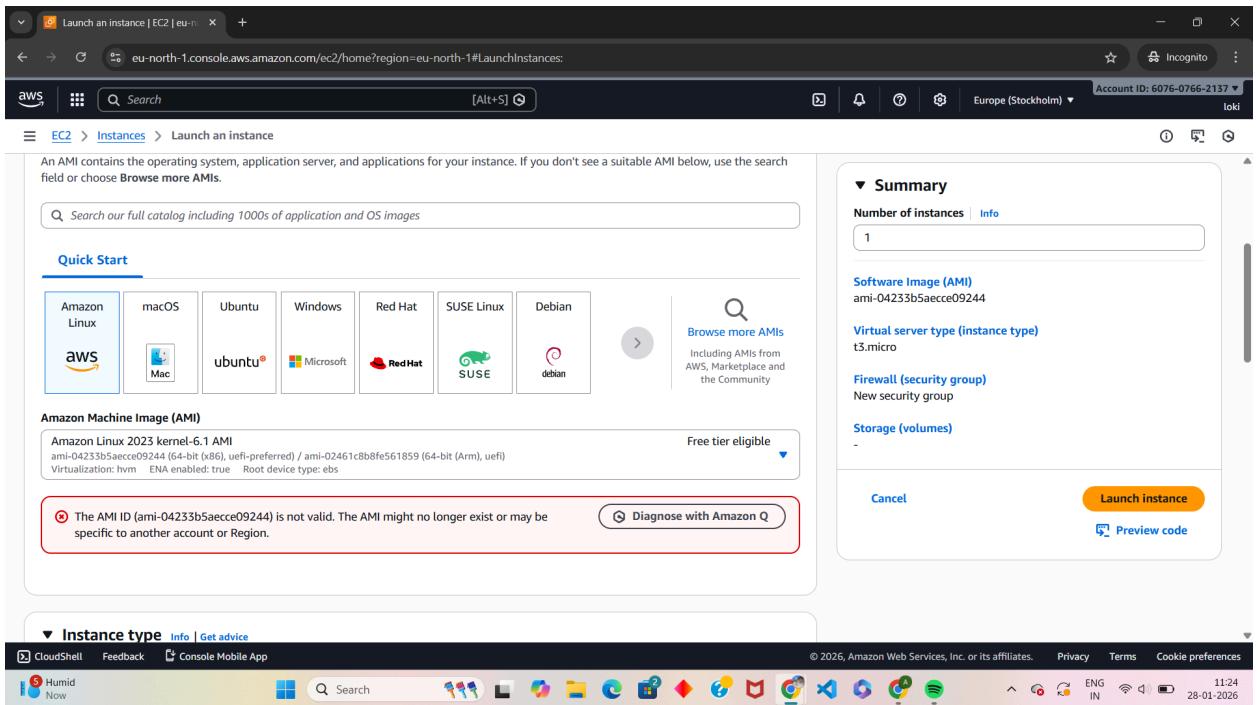


User logged into AWS Console

Region selected: **Europe (Stockholm)**

Access denied error shown for some services

Indicates **insufficient IAM permissions**



- User tried to launch an EC2 instance
- AMI ID error displayed
- Access issue due to **missing EC2 permissions**
- Shows need for EC2 policy assignment

The screenshot shows the AWS IAM console interface. On the left, a sidebar navigation includes 'Identity and Access Management (IAM)', 'Dashboard', 'Access Management' (with 'User groups' selected), 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings', 'Root access management', 'Temporary delegation requests', and 'Access reports' (with 'Resource analysis' selected). The main content area is titled 'Create user group' under 'User groups'. It has two sections: 'User group name' (containing 'aws@access') and 'Add users to the group - Optional (2/2)'. The 'Add users to the group' section lists 'jai' and 'loki' with their respective activity status ('Now' and '4 minutes ago'). Below this is the 'Attach permissions policies - Optional (1111)' section, which is currently empty. The bottom of the screen shows the Windows taskbar with various pinned icons.

Created a new IAM group named **aws@access**

Selected users **jai** and **loki**

Users added to the group

The screenshot shows the AWS IAM console interface for creating a user group. The left sidebar navigation includes 'Identity and Access Management (IAM)', 'Dashboard', 'Access Management' (with 'User groups' selected), 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings', 'Root access management', 'Temporary delegation requests', 'Access reports', 'Access Analyzer', 'Resource analysis', and 'Unused access'. The main content area has two sections: 'Add users to the group - Optional (2/2)' and 'Attach permissions policies - Optional (1/1111)'. In the 'Add users to the group' section, users 'jai' and 'loki' are listed. In the 'Attach permissions policies' section, a search for 'ec2fu' finds the 'AmazonEC2FullAccess' policy, which is described as providing full access to Amazon EC2 via AWS managed policies. The bottom of the screen shows the Windows taskbar with various pinned icons.

Searched for EC2 policy

Selected **AmazonEC2FullAccess**

Policy attached to the user group

Group provides full EC2 access

The screenshot shows the AWS IAM User Groups page. A success message at the top states "aws@access user group created." The main table displays one user group:

Group name	Users	Permissions	Creation time
aws@access	2	Defined	Now

The left sidebar shows the navigation menu for IAM, including "User groups", which is currently selected. Other options like "Users", "Roles", and "Policies" are also listed.

IAM user group **aws@access** created

Group contains **2 users**

Permissions status shown as **Defined**

Identity and Access Management (IAM)

aws@access Info

Summary

User group name: aws@access | Creation time: January 28, 2026, 11:27 (UTC+05:30) | ARN: arn:aws:iam::607607662137:group/aws@access

Users (2) | Permissions | Access Advisor

Users in this group (2)

User name	Groups	Last activity	Creation time
jai	1	None	2 minutes ago
loki	1	6 minutes ago	8 minutes ago

- Opened **aws@access** group details
- Shows group ARN and creation time
- Lists users **jai** and **loki**

Identity and Access Management (IAM)

loki Info

Summary

ARN: arn:aws:iam::607607662137:user/loki | Console access: Enabled without MFA | Access key 1: Create access key

Created: January 28, 2026, 11:19 (UTC+05:30) | Last console sign-in: Today

Permissions | Groups (1) | Tags | Security credentials | Last Accessed

Permissions policies (2)

Policy name	Type	Attached via
AmazonEC2FullAccess	AWS managed	Group aws@access
IAMUserChangePassword	AWS managed	Directly

IAM user **loki** summary page

Console access enabled (without MFA)

Policies attached:

- **AmazonEC2FullAccess** (via group)
- **IAMUserChangePassword** (direct)

User now has EC2 permissions

The screenshot shows the 'Add permissions' step of the IAM user configuration process. The user 'loki' is selected. The 'Permissions options' section is open, showing three choices: 'Add user to group' (unchecked), 'Copy permissions' (unchecked), and 'Attach policies directly' (checked). Below this, the 'Permissions policies' section lists 's3ful' as a search result, with a checkbox next to it. The checkbox is checked, indicating the selection of the 'AmazonS3FullAccess' policy. The 'Next Step' button is visible at the bottom right.

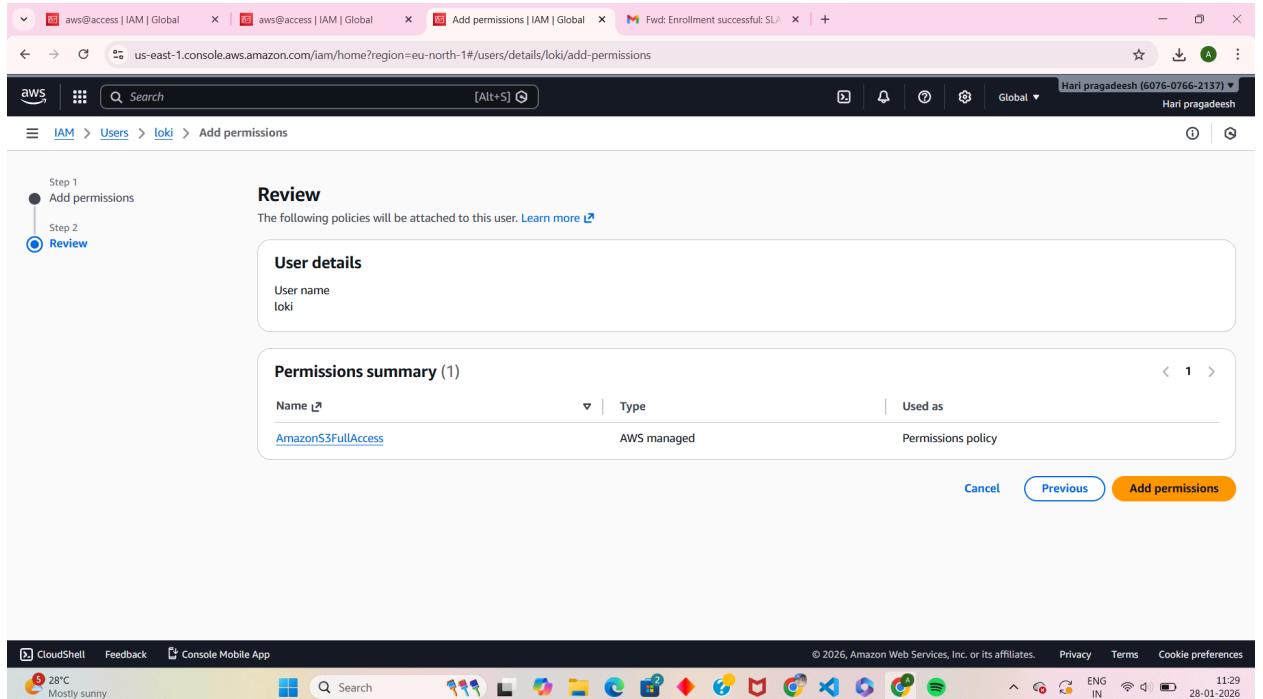
Opened IAM user **loki**

Selected **Attach policies directly**

Searched for S3 policy

Selected **AmazonS3FullAccess**

Proceeded to next step



The screenshot shows the AWS IAM 'Add permissions' review step. The top navigation bar includes tabs for 'aws@access | IAM | Global', 'aws@access | IAM | Global', 'Add permissions | IAM | Global', and 'Fwd: Enrollment successful: SLA'. The main content area is titled 'Review' and shows the following details:

- User details:** User name: loki
- Permissions summary (1):**

Name	Type	Used as
AmazonS3FullAccess	AWS managed	Permissions policy

At the bottom right, there are buttons for 'Cancel', 'Previous', and 'Add permissions'.

- Review page before attaching policy
- User name: **loki**
- Policy to be attached: **AmazonS3FullAccess**
- Clicked **Add permissions**

The screenshot shows the AWS IAM User details page for a user named 'loki'. The top navigation bar includes tabs for 'aws@access | IAM | Global' and 'aws@access | IAM | Global' (selected), along with a message 'Fwd: Enrollment successful: SU'. The main content area displays the 'loki' user's summary, including ARN (arn:aws:iam::607607662137:user/loki), creation date (January 28, 2026, 11:19 (UTC+05:30)), and access information (Console access Enabled without MFA, Last console sign-in Today). Below this, the 'Permissions' tab is selected, showing three policies attached: 'AmazonEC2FullAccess' (via group, AWS managed), 'AmazonS3FullAccess' (direct, AWS managed), and 'IAMUserChangePassword' (direct, AWS managed). The bottom of the screen shows the Windows taskbar with various pinned icons.

IAM user loki permissions page

Policies attached:

- AmazonEC2FullAccess (via group)
- AmazonS3FullAccess (direct)
- IAMUserChangePassword (direct)

User now has EC2 and S3 access

The screenshot shows the AWS IAM Users page. On the left, there's a sidebar with 'Identity and Access Management (IAM)' selected. The main area displays a table titled 'Users (2/2)'. The table has columns for User name, Path, Group, Last activity, MFA, Password age, Console last sign-in, and Account. Two users are listed: 'jai' and 'loki'. Both users belong to group '1'. Their last activity was 8 minutes ago. The password age is 5 minutes for jai and 8 minutes for loki. The console last sign-in was 8 minutes ago for both. There are buttons for 'Create user' and 'Delete' at the top right.

User name	Path	Group	Last activity	MFA	Password age	Console last sign-in	Acc
jai	/	1	-	-	5 minutes	-	-
loki	/	1	8 minutes ago	-	8 minutes	8 minutes ago	-

- Displayed list of IAM users
- Users shown: **jai** and **loki**
- Both users belong to one group
- Shows last activity and password age

The screenshot shows the same AWS IAM Users page as before, but with a modal dialog box in the foreground. The dialog is titled 'Delete 2 users?' and contains a message: 'Delete 2 users permanently? This will also delete all their user data, security credentials and inline policies.' It lists the two selected users: 'loki' (last activity 9 minutes ago) and 'jai' (last activity -). Below the list is a note: 'Note: Recent activity usually appears within 4 hours. Data is stored for a maximum of 365 days, depending when your region began supporting this feature. [Learn more](#)' and a warning: 'To avoid accidental deletions, we ask you to provide additional written consent.' A text input field contains the word 'confirm'. At the bottom of the dialog are 'Cancel' and 'Delete users' buttons.

Selected users **jai** and **loki**

Delete users confirmation popup opened

Shows last activity details

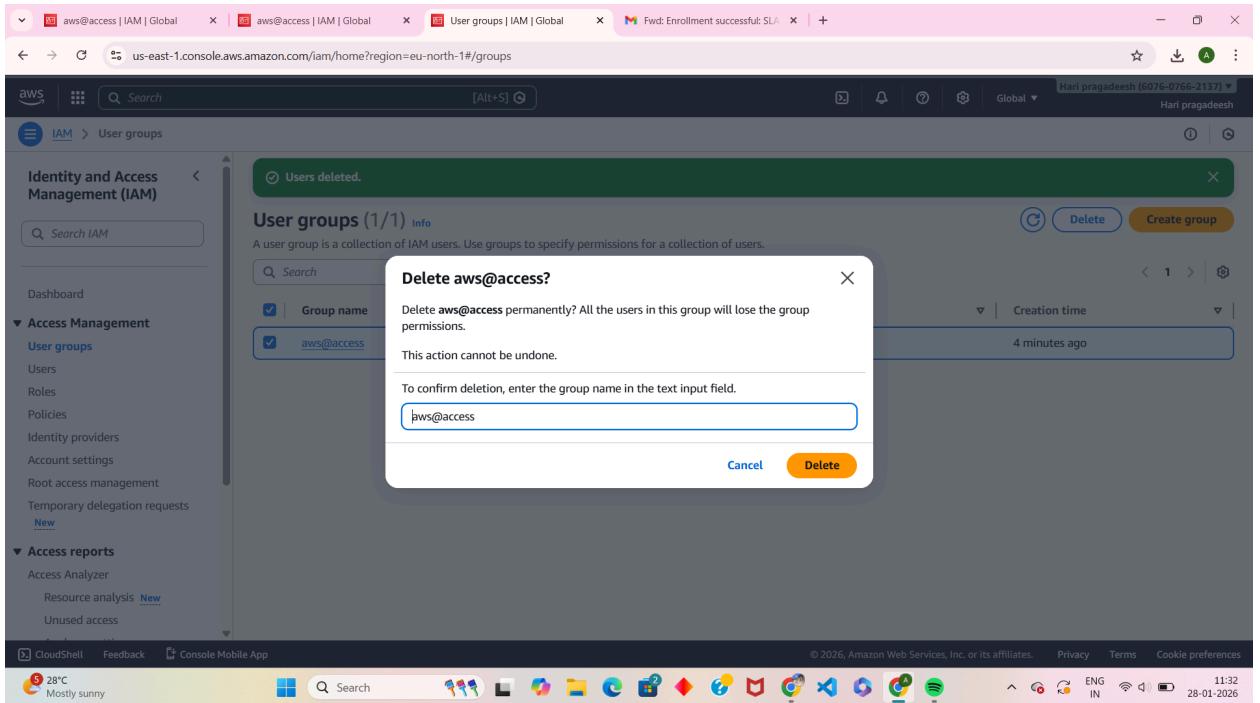
Typed **confirm** to proceed

The screenshot shows the AWS IAM User Groups page. At the top, there is a green confirmation message: "Users deleted." Below this, the title "User groups (1/1) Info" is displayed. A sub-instruction says "A user group is a collection of IAM users. Use groups to specify permissions for a collection of users." There is a search bar and a table with one row. The table columns are "Group name", "Users", "Permissions", and "Creation time". The single entry is "aws@access", which has 2 users, defined permissions, and was created 4 minutes ago. On the left sidebar, under "Access Management", "User groups" is selected. The bottom of the screen shows the standard AWS navigation bar with links like CloudShell, Feedback, and Console Mobile App.

Confirmation message: **Users deleted**

IAM Users list is now empty

Users removed permanently from account



Group name entered correctly

Ready to delete **aws@access** group

This removes all group permissions

