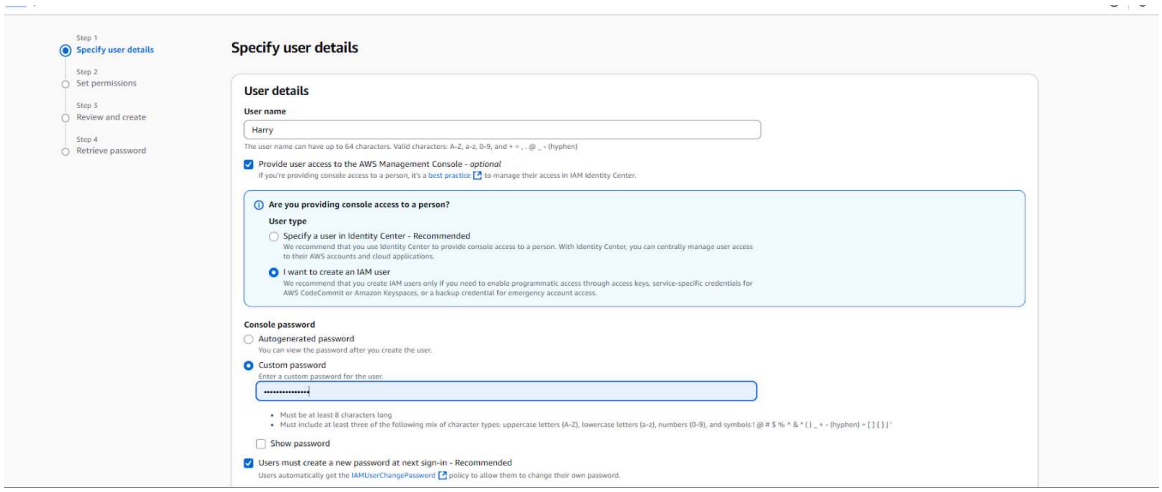
IAM User, Groups, Merged Groups, Roles, Policies

Step 1: Specify User Details

Console Steps

1. Go to the IAM Dashboard in the AWS Management Console.
2. Navigate to:
   Access management → Users → Add users
3. Enter the User name:
   e.g., `Harry`
   (User names may contain up to 64 characters with letters, numbers, and hyphens.)
4. Select AWS access options:
   - *Management Console access:*
     - Set custom password or let AWS generate one.
     - Decide whether to require a password reset at next sign-in (*recommended*).
5. Click Next.

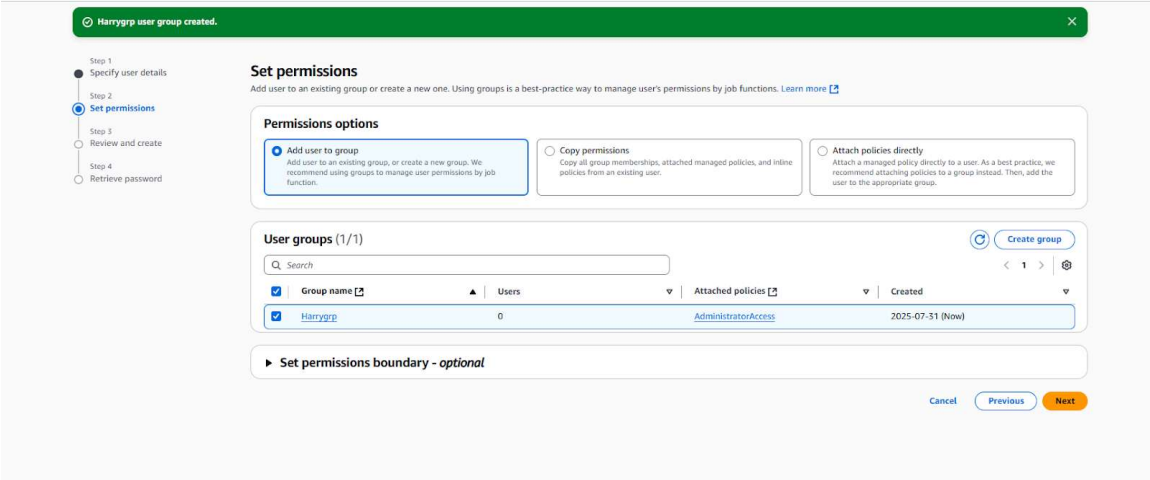


Step 2: Set Permissions

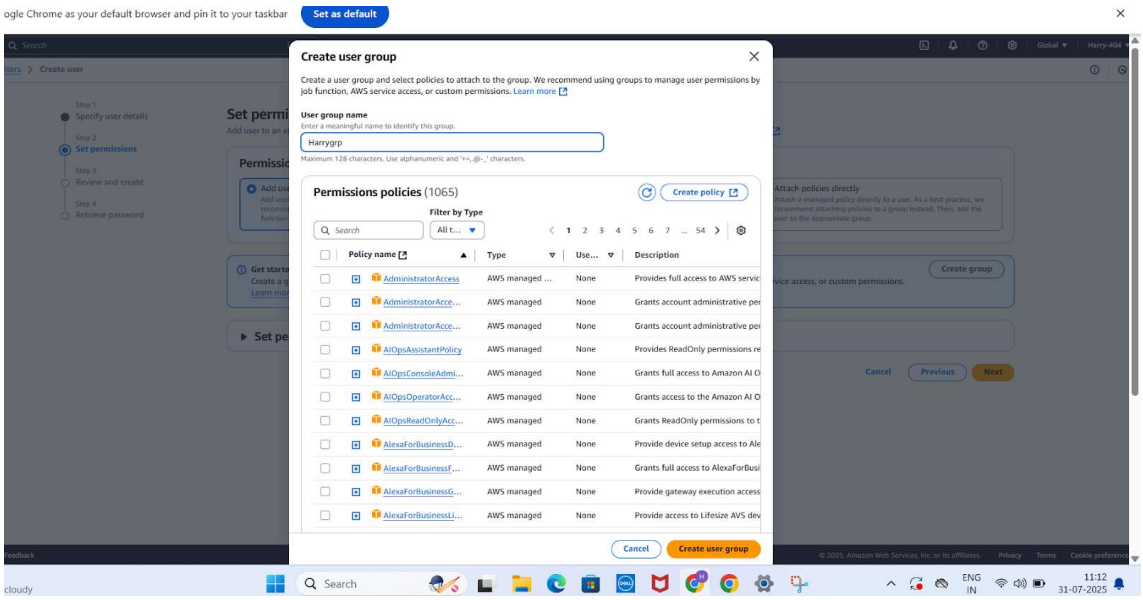
Console Steps

1. Add user to a group:
   - *Best practice is to use groups for permissions.*

2. Create new group (if needed):
    - Group name: `Harrygrp`
    - Attach permission policies (e.g., `AdministratorAccess`)
    - Click Create group
3. Select the group (e.g., `Harrygrp`) and add the user.
4. Click Next.



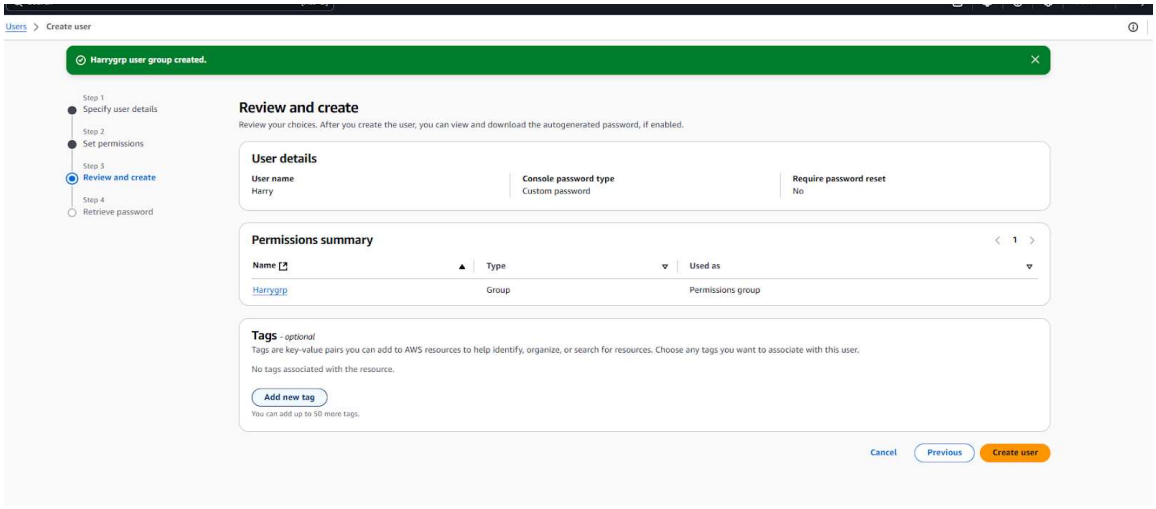
After Setting permission like also including user in group review and create user:

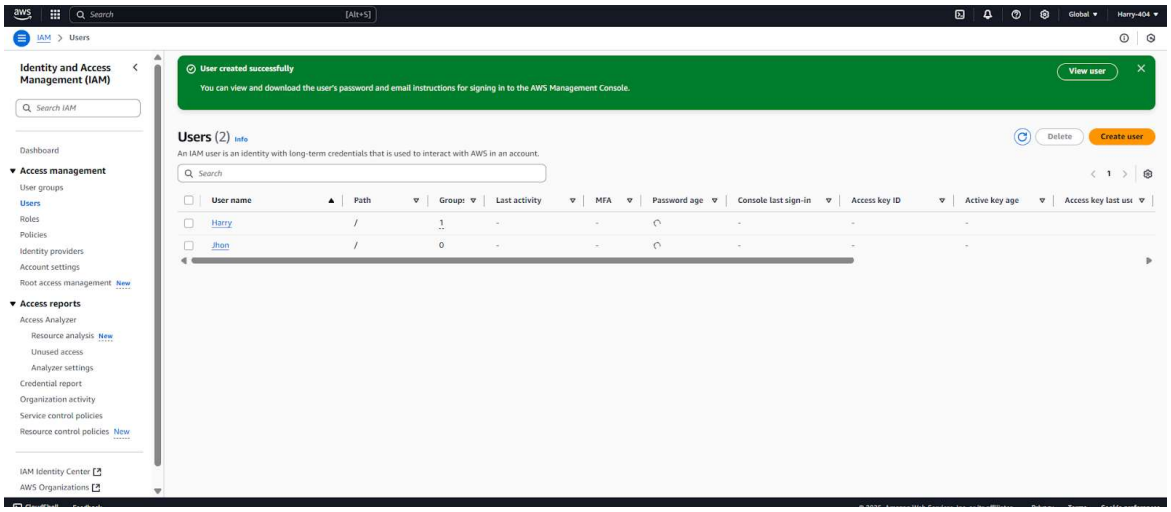


Step 3: Review and Create

Console Steps

1. Review the configuration:
    - User name
    - Assigned groups and their attached policies
    - Console password and reset preference
2. *Add tags if necessary* (optional, for resource management).
3. Click Create user.



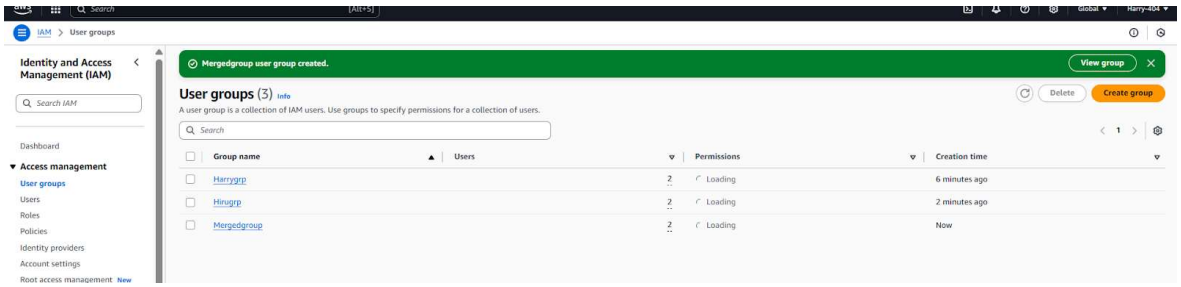


Extra: Creating More Groups and Merged Groups

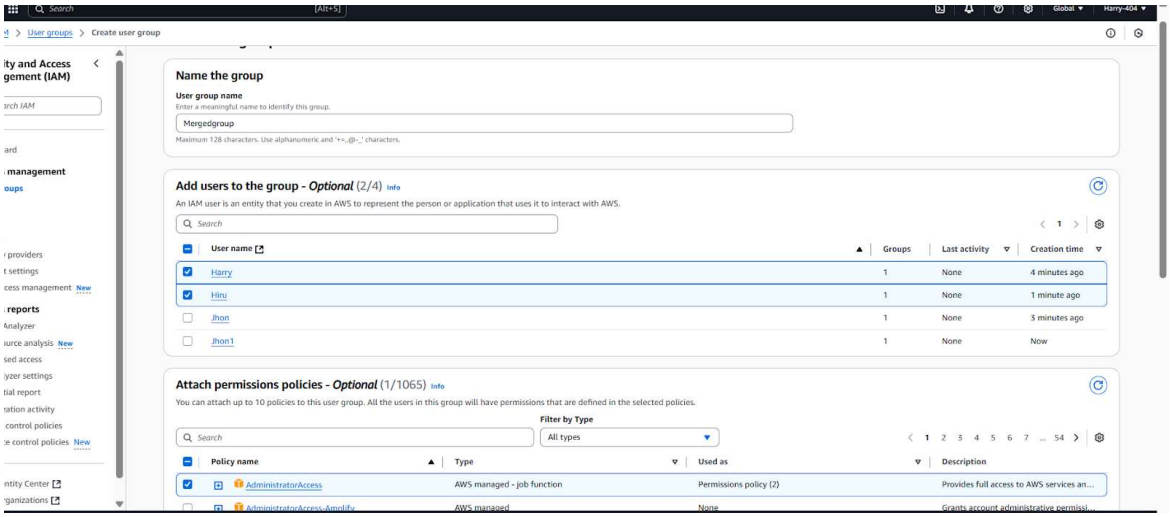
You can create multiple user groups and assign users to more than one group if needed.

Console Steps

1. Go to IAM > User Groups > Create Group
2. Enter group name (e.g., `Mergedgroup`)
3. Select users to add
4. Attach desired permission policies
5. Create the group



Creating group or merged group



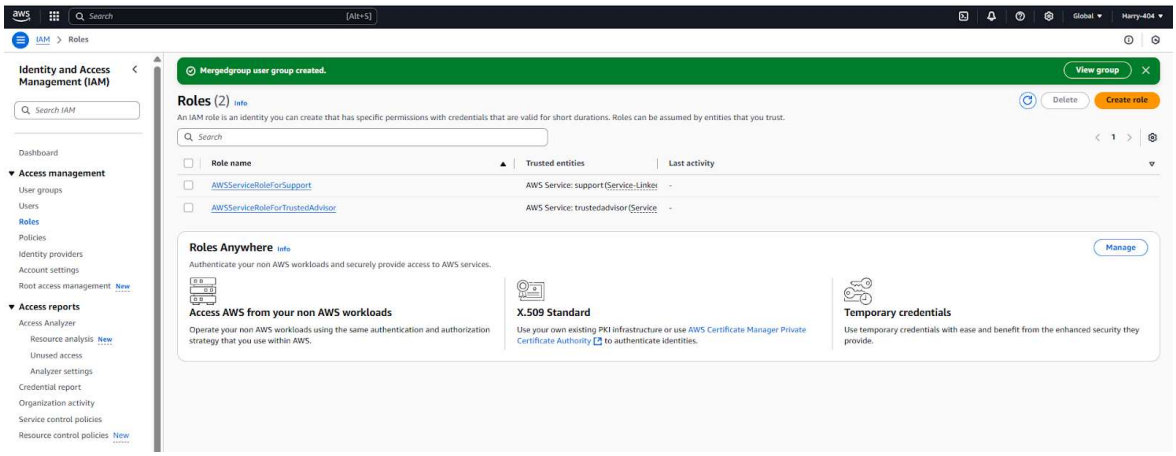
Step 4 (Optional): Managing Roles

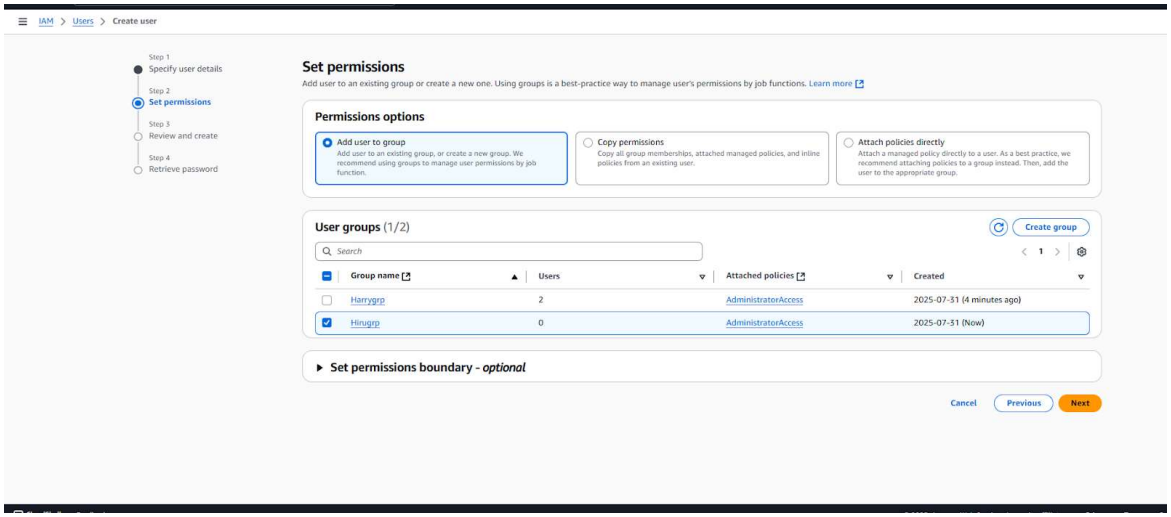
Roles are different from users/groups; they're for permissions that can be assumed temporarily.

Console Steps

- Go to Roles → Create Role
- Select trusted entity (e.g., AWS service, another account)
- Attach policies as needed

- Name the role and finish creation





Step 5: Create and Attach Custom Policies

You can create custom policies in AWS IAM to precisely tailor permissions for users or groups. This step is in addition to using AWS-managed policies and is especially valuable for organizations requiring fine-grained access controls.

Console Steps

1. Navigate to the IAM Dashboard:
    - Go to IAM > Policies.
2. Create Policy:
    - Click Create policy.
    - Choose Visual editor or JSON:

- Visual Editor: Select a service, choose actions, and specify resources.
- JSON: Paste your custom policy document.

Summary Table

Resource	Console Steps Summary
User	Add Users
Group	User Groups > Create Group
Policy	Attach via wizard
Add to group	Select in UI
Role	Roles > Create Role