

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.

The screenshot shows the 'Specify user details' page in the AWS IAM console. On the left, a sidebar lists four steps: 'Specify user details' (selected), 'Set permissions', 'Review and create', and 'Retrieve password'. The main content area is titled 'Specify user details' and contains the following sections:

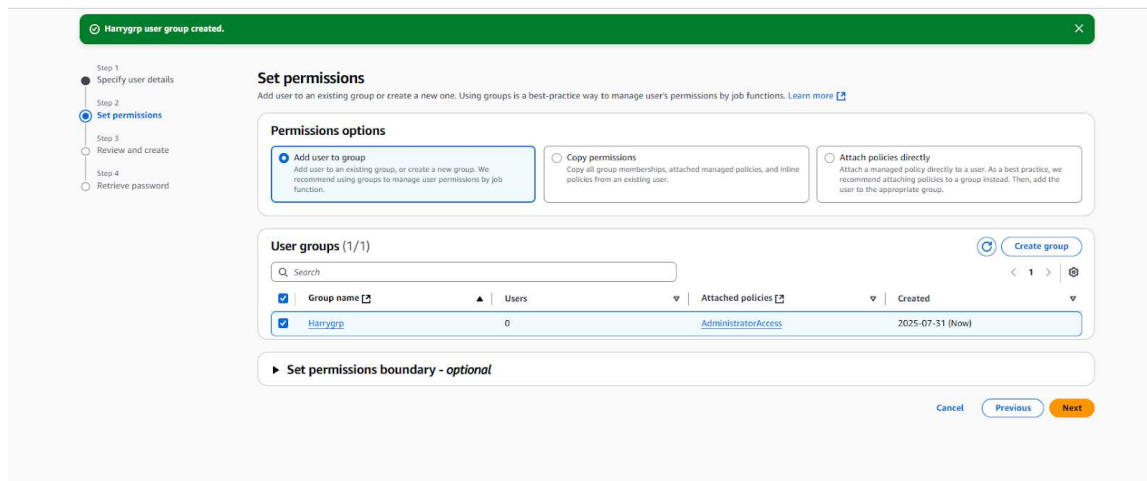
- User details:** A text input field for 'User name' containing the text 'Harry'. Below the field is a small note: 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and +, -, @, _ (hyphen)'.
- Provide user access to the AWS Management Console - optional:** A checkbox is checked. Below it is a link to 'manage their access in IAM Identity Center'.
- Are you providing console access to a person?:** A section with a 'User type' heading. It contains two radio buttons: 'Specify a user in Identity Center - Recommended' (unselected) and 'I want to create an IAM user' (selected). Below the radio buttons is a note: '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:** Two radio buttons: 'Autogenerated password' (unselected) and 'Custom password' (selected). Below the 'Custom password' option is a text input field for 'Enter a custom password for the user' containing 'xxxxxxxxxx'. To the right of the field are two bullet points: '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) = [!@#\$%^&*~+-]'. Below the field is a checkbox for 'Show password' which is unchecked.
- Users must create a new password at next sign-in - Recommended:** A checkbox is checked. Below it is a note: 'Users automatically get the IAMUserChangePassword policy to allow them to change their own password.'

Step 2: Set Permissions

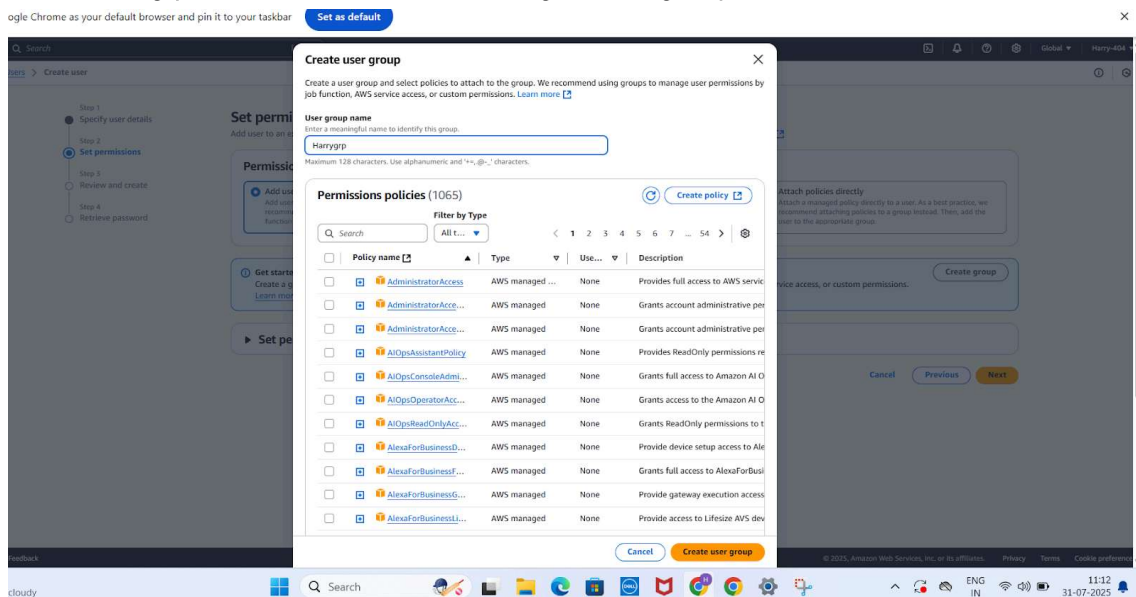
Console Steps

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.

The screenshot shows the 'Review and create' step of the AWS IAM 'Create user' process. A green banner at the top states 'Harrygrp user group created.' On the left, a progress bar shows four steps: 'Specify user details', 'Set permissions', 'Review and create' (which is highlighted), and 'Retrieve password'. The main content area is titled 'Review and create' and includes a sub-header 'Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.'

The 'User details' section contains three fields: 'User name' with the value 'Harry', 'Console password type' set to 'Custom password', and 'Require password reset' set to 'No'.

The 'Permissions summary' section shows a table with one entry: 'Harrygrp' (Name), 'Group' (Type), and 'Permissions group' (Used as).

The 'Tags - optional' section explains that tags are key-value pairs for AWS resources and provides an 'Add new tag' button. It notes that up to 50 tags can be added.

At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Create user'.

The screenshot shows the AWS IAM 'Users' page. A green banner at the top states 'User created successfully' and provides instructions on how to view and download the user's password and email instructions for signing in. Below the banner, the page title is 'Users (2)' with an 'Info' link. A sub-header explains that an IAM user is an identity with long-term credentials used to interact with AWS.

A search bar is present above a table listing the users. The table has columns for 'User name', 'Path', 'Groups', 'Last activity', 'MFA', 'Password age', 'Console last sign-in', 'Access key ID', 'Active key age', and 'Access key last use'.

User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key age	Access key last use
Harry	/	1	-	-	∞	-	-	-	-
jhon	/	0	-	-	∞	-	-	-	-

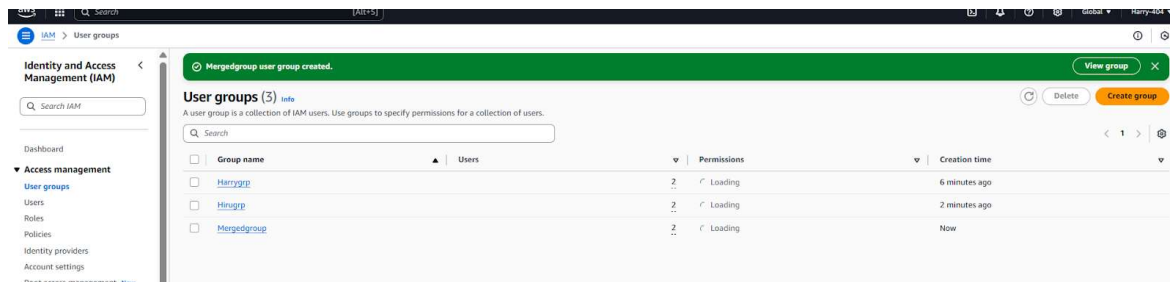
At the top right of the table, there are buttons for 'Delete' and 'Create user'.

Extra: Creating More Groups and Merged Groups

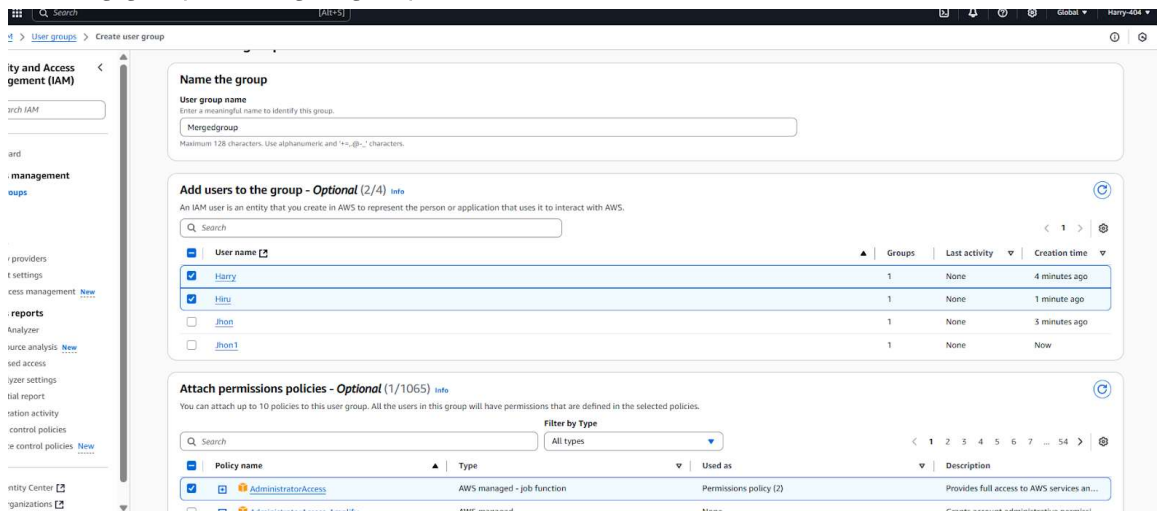
You can create multiple user groups and assign users to more than one group if needed.

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



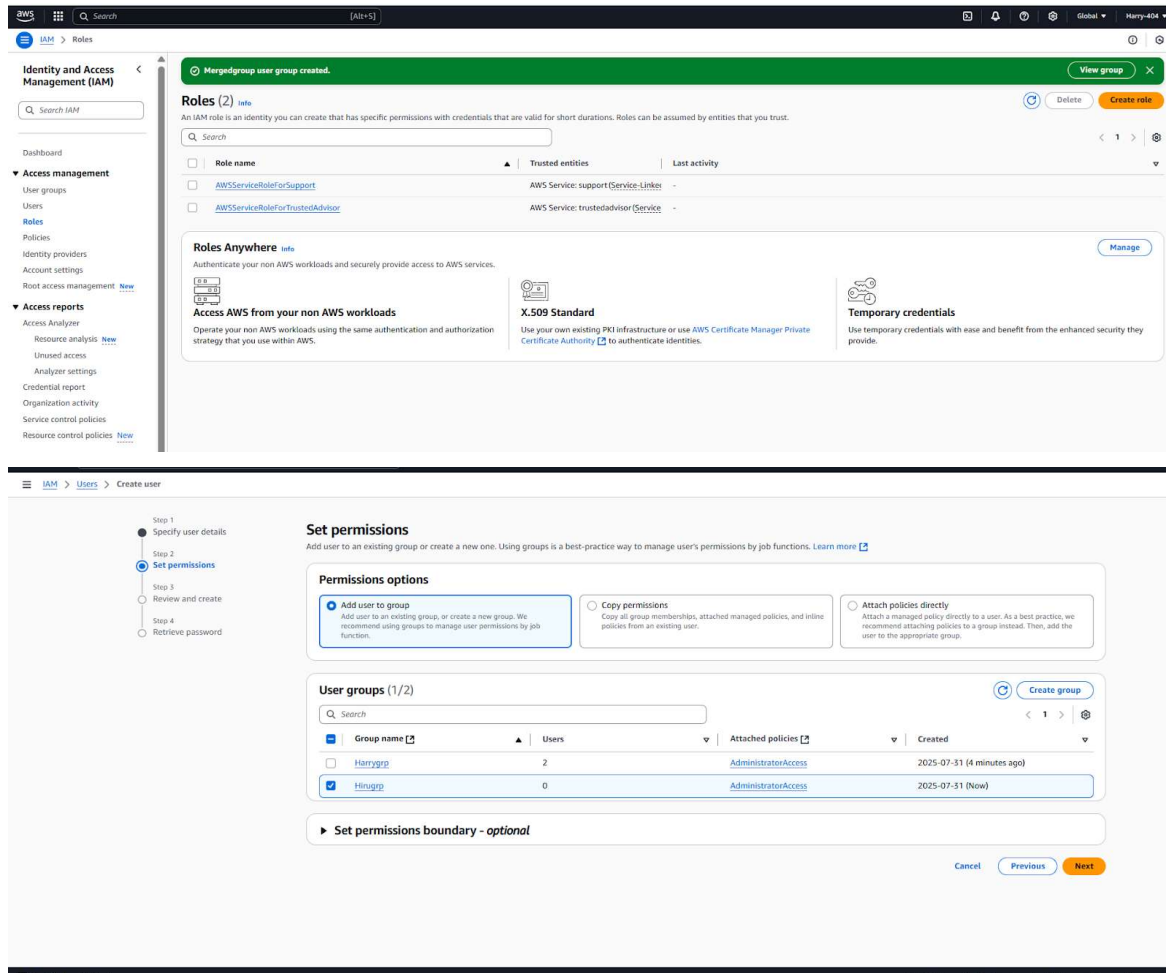
Step 4 (Optional): Managing Roles

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