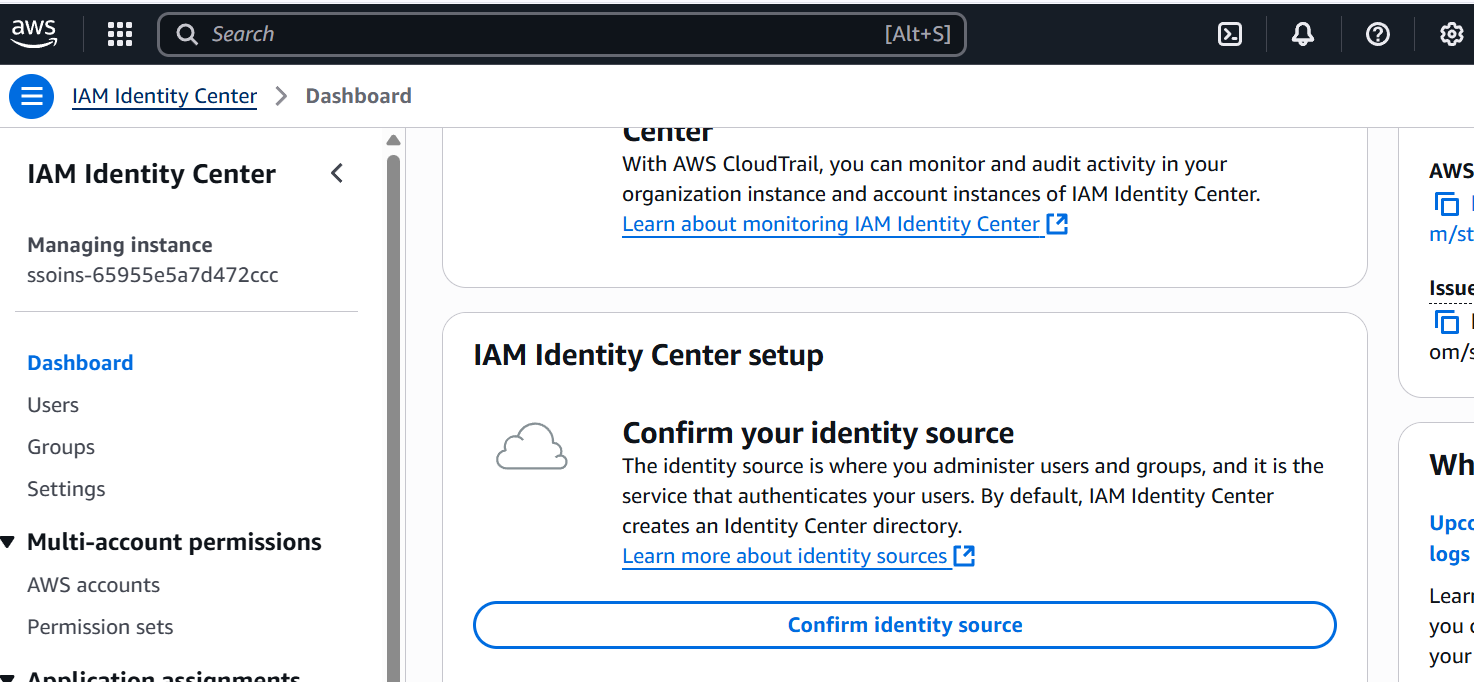
**Step 1: Enable IAM Identity Center (SSO)**

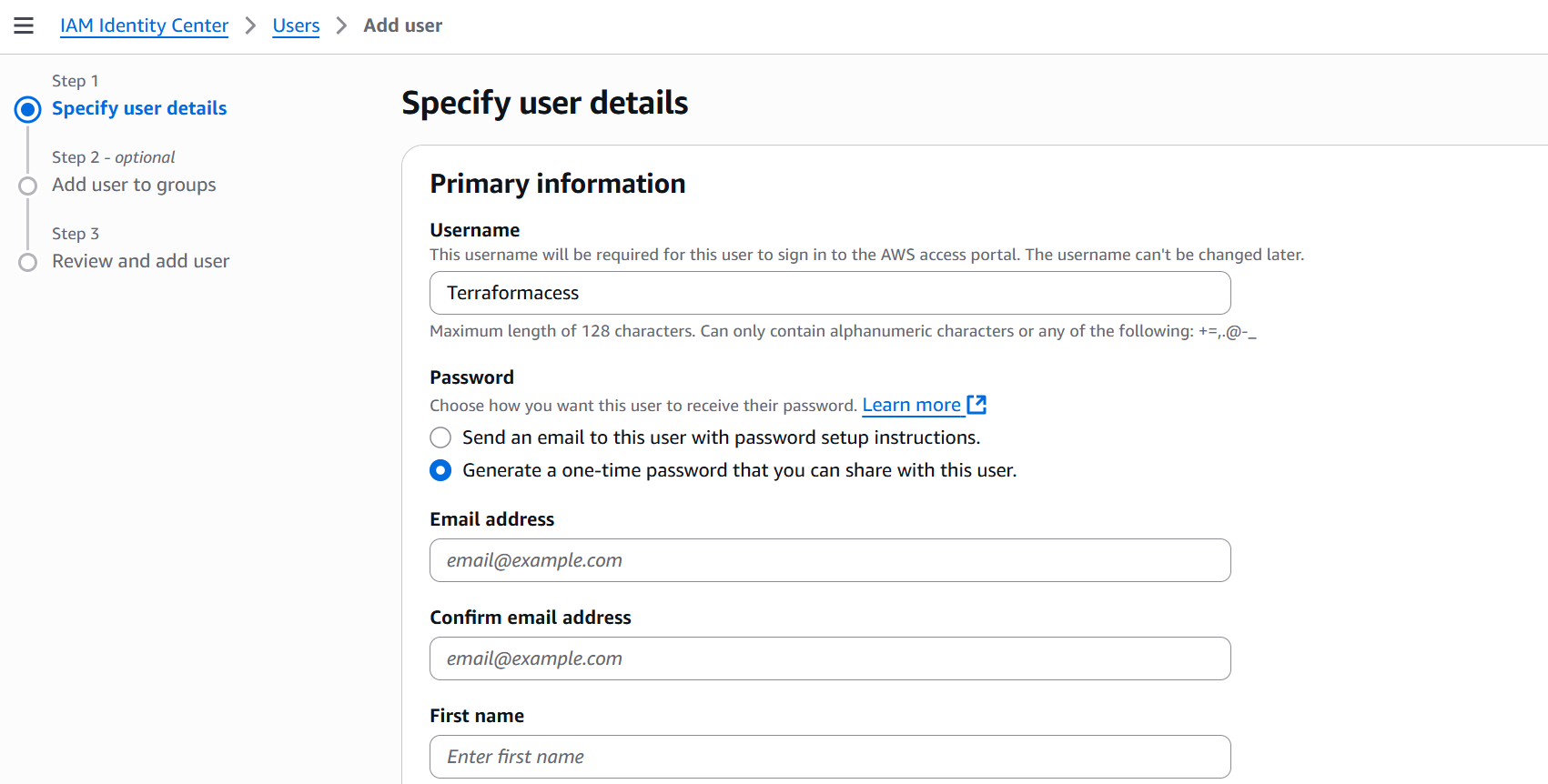
1. **Login to AWS Console** with an admin account.
2. Go to [**IAM Identity Center**](https://console.aws.amazon.com/singlesignon/).
3. If not already enabled:
   * Click **Enable** to set up IAM Identity Center (SSO).
4. Choose an **identity source**:
   * You can use the default **AWS IAM Identity Center directory**.



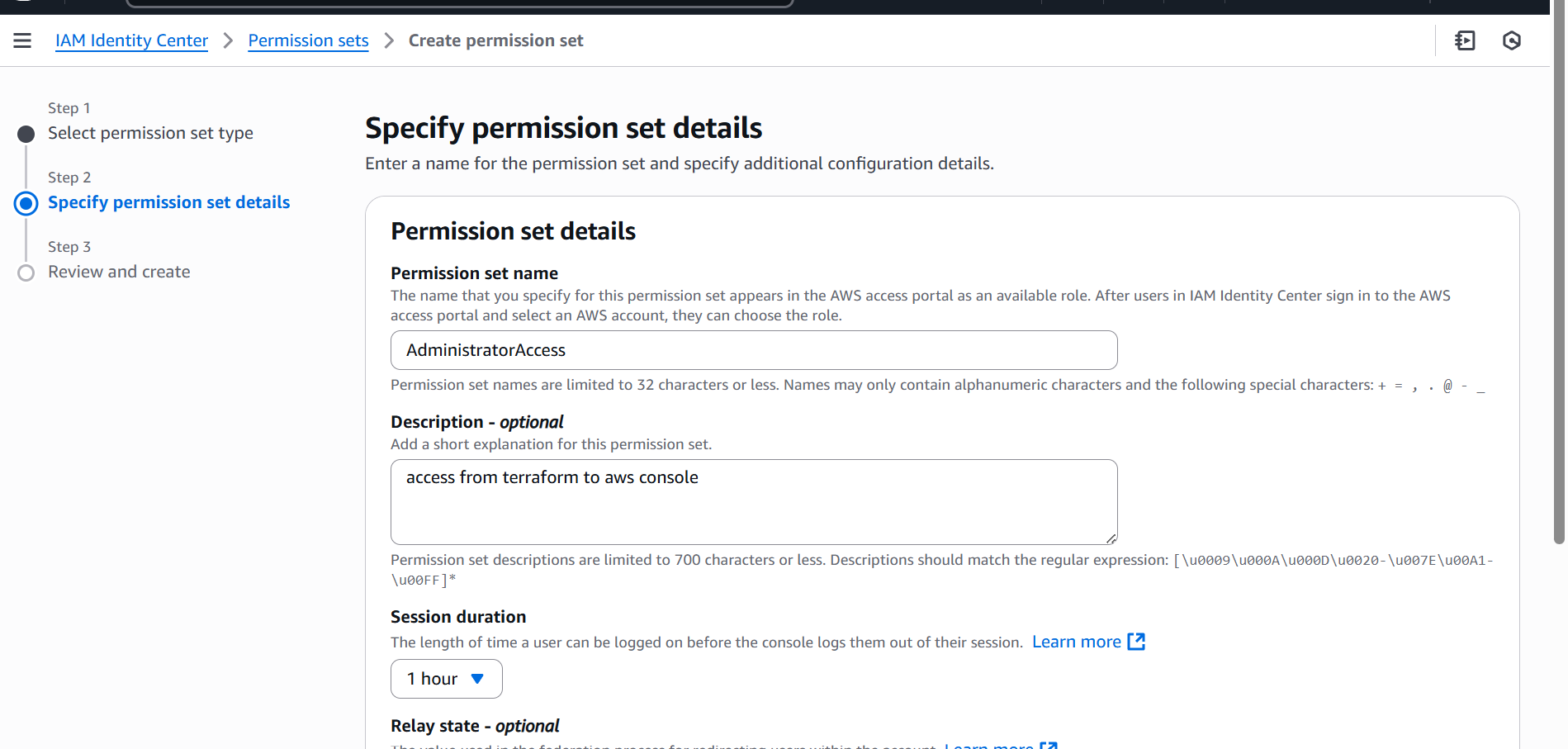
* + Or integrate with an external IdP like Okta or Azure AD

**Step 2: Create Users and Assign Access**

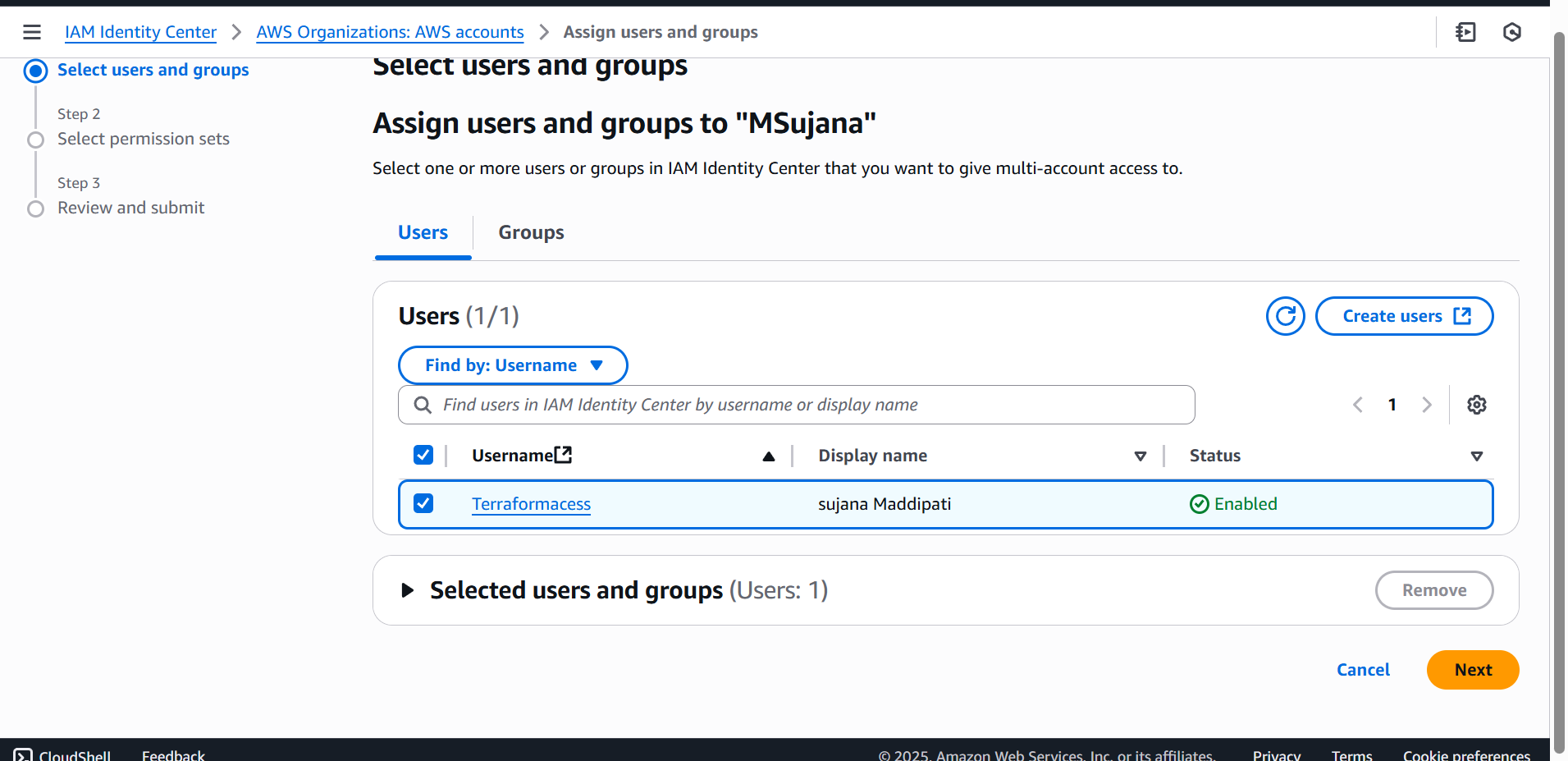
1. **Create a user** under **IAM Identity Center → Users**.
   * Example: [sujana@example.com](mailto:sujana@example.com)



1. Go to **Permission sets** → Click **Create permission set**.
   * Example: TerraformAccessSet
   * Choose policies like AdministratorAccess or create a custom one.



1. **Assign user access**:
   * Go to **AWS Accounts** → select your account.
   * Choose “Assign users or groups” → Add your user.
   * Assign the created permission set (e.g., TerraformAccessSet).



Configure AWS CLI with SSO:

Step 1:

aws configure sso - - profile <name of the profile>

Example values:

SSO session name: aws-sso-session

SSO start URL: https://<your-org>.awsapps.com/start

SSO region: ap-south-1

AWS account ID + Role name (assigned via permission set)

Step 2:

aws sso login --profile 04-aws-sso

terraform init , terraform plan, terraform apply

**📌 Notes**

* Login is valid temporarily, and may need renewal with aws sso login
* Very secure; best for organizations and teams