A day in the life of a control tower admin

Pre-requisite

- You must have already deployed the control tower environment and have access to the 3 accounts it creates.
- Use supported region: Oregon, Ohio, N.Virginia, Ireland
- Sign in URL (Email and password)

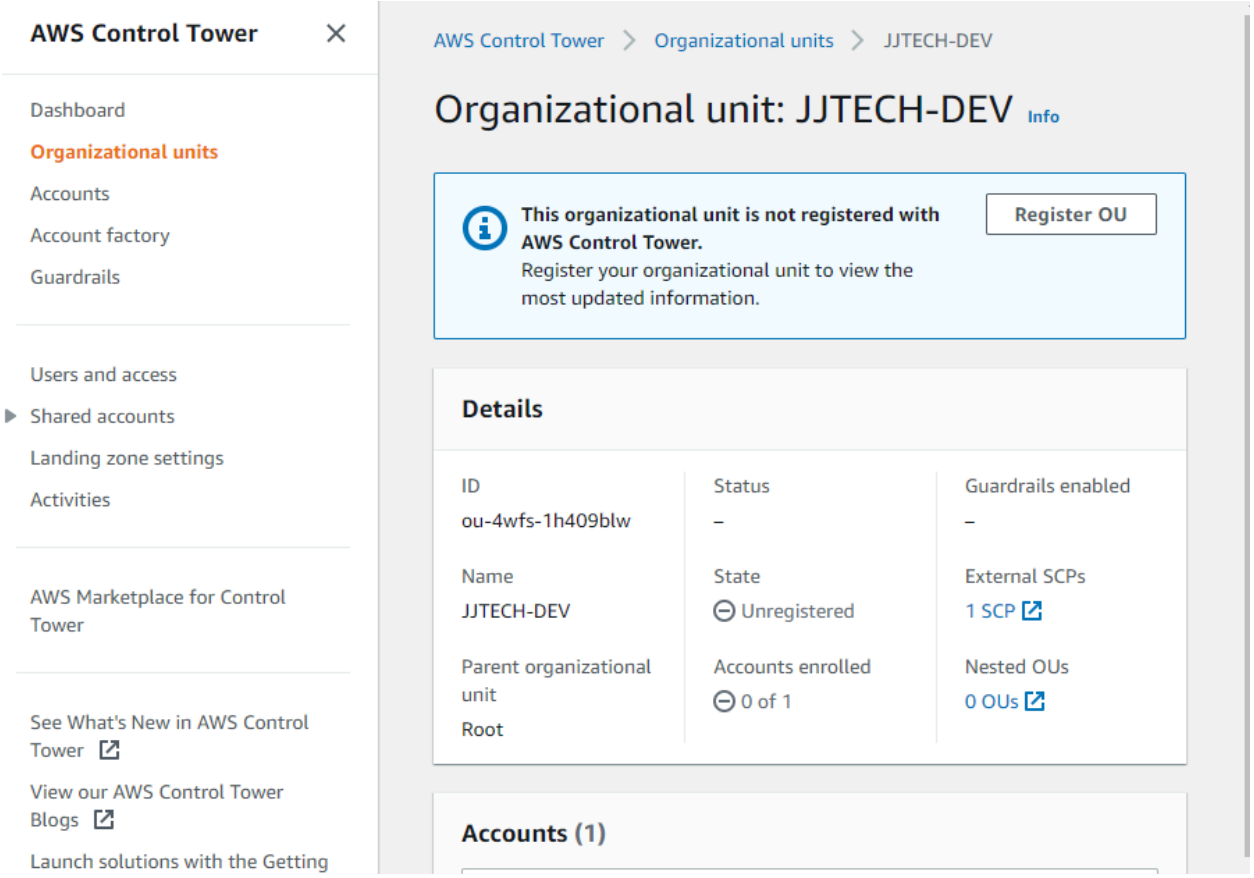
Lab 1: Explore the AWS Control Tower Console

Dashboard	View summary of the Control Tower environment
Organizational units	Add/Delete/Register/Re-Register an OU
Accounts	View account details and state
Account factory	Edit Network configuration for new accounts and Enroll/Invite accounts
Guardrails	View details of each Guardrail
Users and access	View basic details for the AWS SSO integration
Shared accounts	Details for the shared accounts: Management, Log archive, and Audit
Landing zone settings	Version information for the Control Tower service

,

Lab 2: Enroll existing accounts and OUs to be governed by control tower

1. In the control Tower console select the account that is not enrolled my CT to enroll.
2. Click Go to OU and click on register OU to add the OU to the ones managed by CT


AWS Control Tower
Dashboard
Organizational units
Accounts
Account factory
Guardrails
Users and access
Shared accounts
Landing zone settings
Activities
AWS Marketplace for Control Tower
See What's New in AWS Control Tower
View our AWS Control Tower Blogs
Launch solutions with the Getting
AWS Control Tower > Organizational units > JJTECH-DEV
Info
Register OU

Organizational unit: JJTECH-DEV

This organizational unit is not registered with AWS Control Tower.
Register your organizational unit to view the most updated information.

Details

ID ou-4wfs-1h409blw	Status –	Guardrails enabled –
Name JJTECH-DEV	State ⊖ Unregistered	External SCPs 1 SCP
Parent organizational unit Root	Accounts enrolled ⊖ 0 of 1	Nested OUs 0 OUs

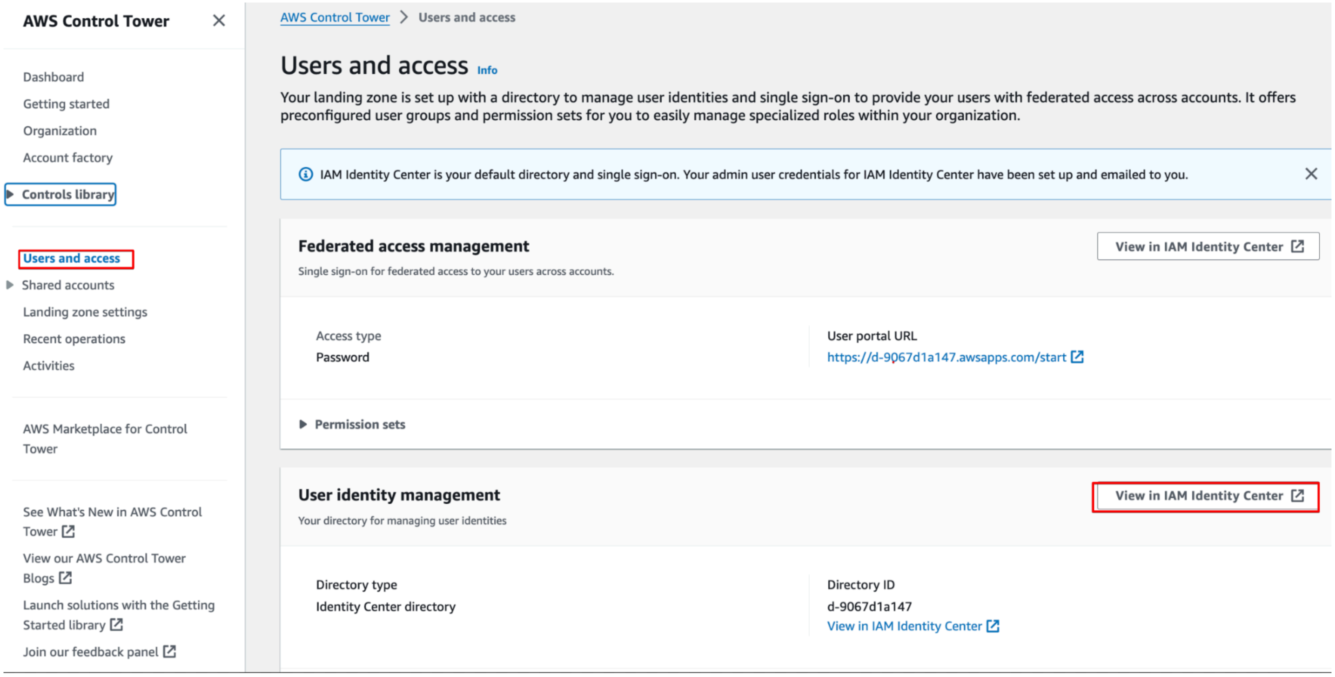
Accounts (1)

3. The blue progress bar will confirm when registration is completed.

Lab 3: Create AWS account using Account factory in control tower

Lab 4: Creating, Users, Groups and permission sets,

1. Log into the master account and navigate to the control tower dashboard.
2. Go to the users and access section. Under "**User identity management"** select "**View in IAM Identity Center**". This will take you to the Identity Center console where you will manage SSO access to your AWS accounts and cloud application.


AWS Control Tower
Dashboard
Getting started
Organization
Account factory
Controls library
Users and access
Shared accounts
Landing zone settings
Recent operations
Activities
AWS Marketplace for Control Tower
See What's New in AWS Control Tower
View our AWS Control Tower Blogs
Launch solutions with the Getting Started library
Join our feedback panel
AWS Control Tower > Users and access
Info
View in IAM Identity Center
Permission sets
View in IAM Identity Center
View in IAM Identity Center

Users and access

Your landing zone is set up with a directory to manage user identities and single sign-on to provide your users with federated access across accounts. It offers preconfigured user groups and permission sets for you to easily manage specialized roles within your organization.

IAM Identity Center is your default directory and single sign-on. Your admin user credentials for IAM Identity Center have been set up and emailed to you.

Federated access management

Single sign-on for federated access to your users across accounts.

Access type
Password

User portal URL
https://d-9067d1a147.awsapps.com/start

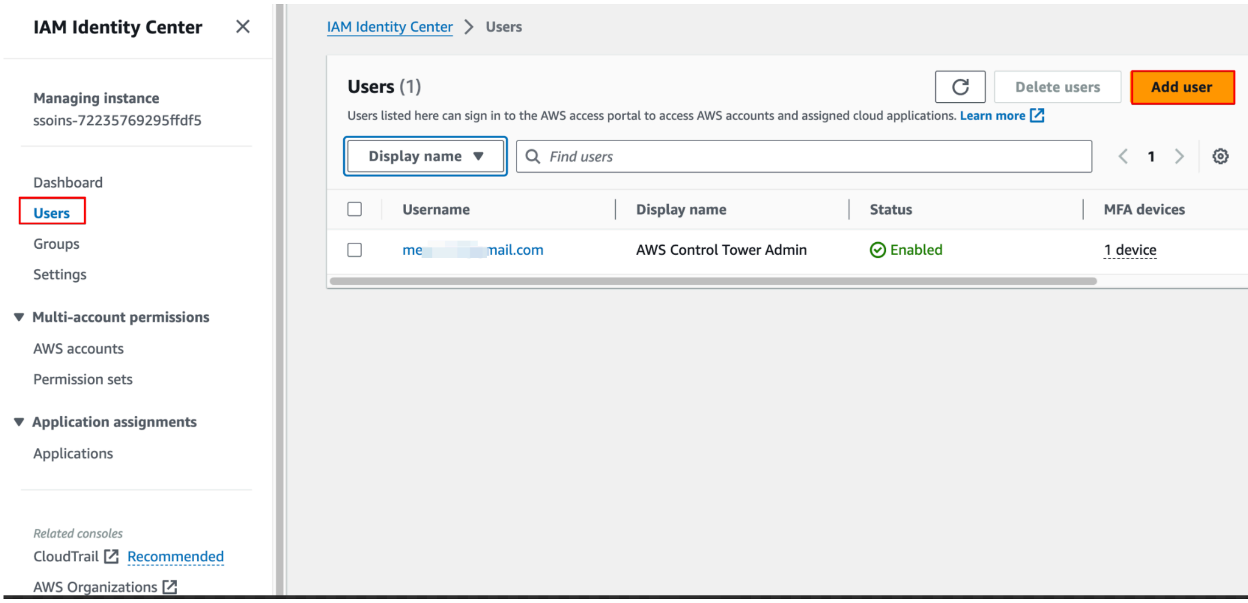
User identity management

Your directory for managing user identities

Directory type
Identity Center directory

Directory ID
d-9067d1a147

3. **Create a new SSO account for an External Auditor who will need read-only access to all your existing accounts and add user to Group.**
    a. In the Identity Center dashboard, select Users and click on Add user

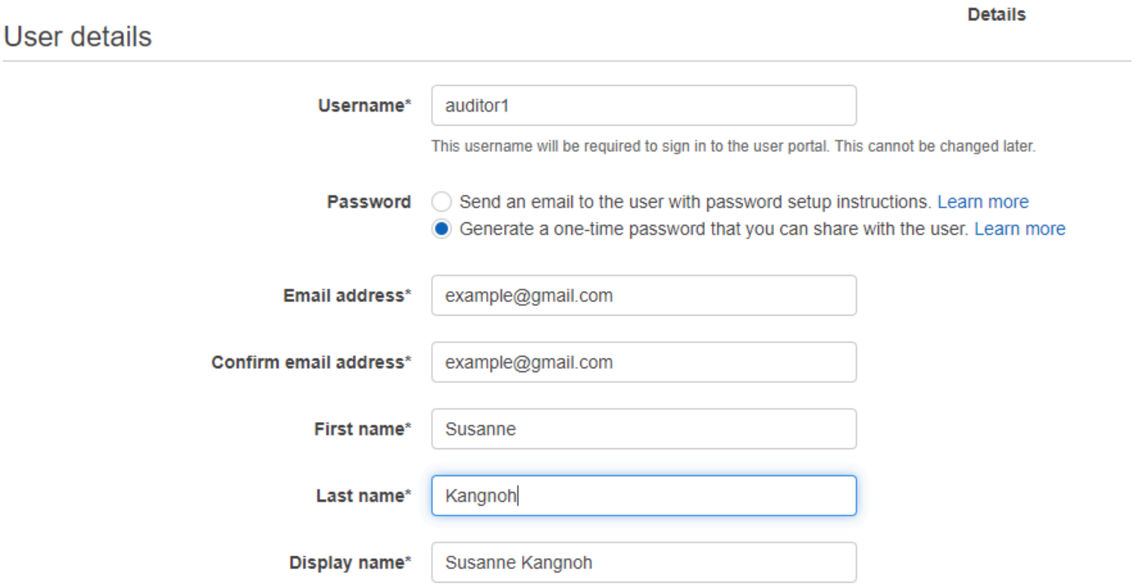


Users (1)

Users listed here can sign in to the AWS access portal to access AWS accounts and assigned cloud applications. Learn more

□	Username	Display name	Status	MFA devices
□	me[redacted]mail.com	AWS Control Tower Admin	Enabled	1 device

b. Complete the basic information about the user.
Select the option to **generate a one-time password** to share with the user



User details

Username*	auditor1
	This username will be required to sign in to the user portal. This cannot be changed later.
Password	○ Send an email to the user with password setup instructions. Learn more ● Generate a one-time password that you can share with the user. Learn more
Email address*	example@gmail.com
Confirm email address*	example@gmail.com
First name*	Susanne
Last name*	Kangnoh
Display name*	Susanne Kangnoh

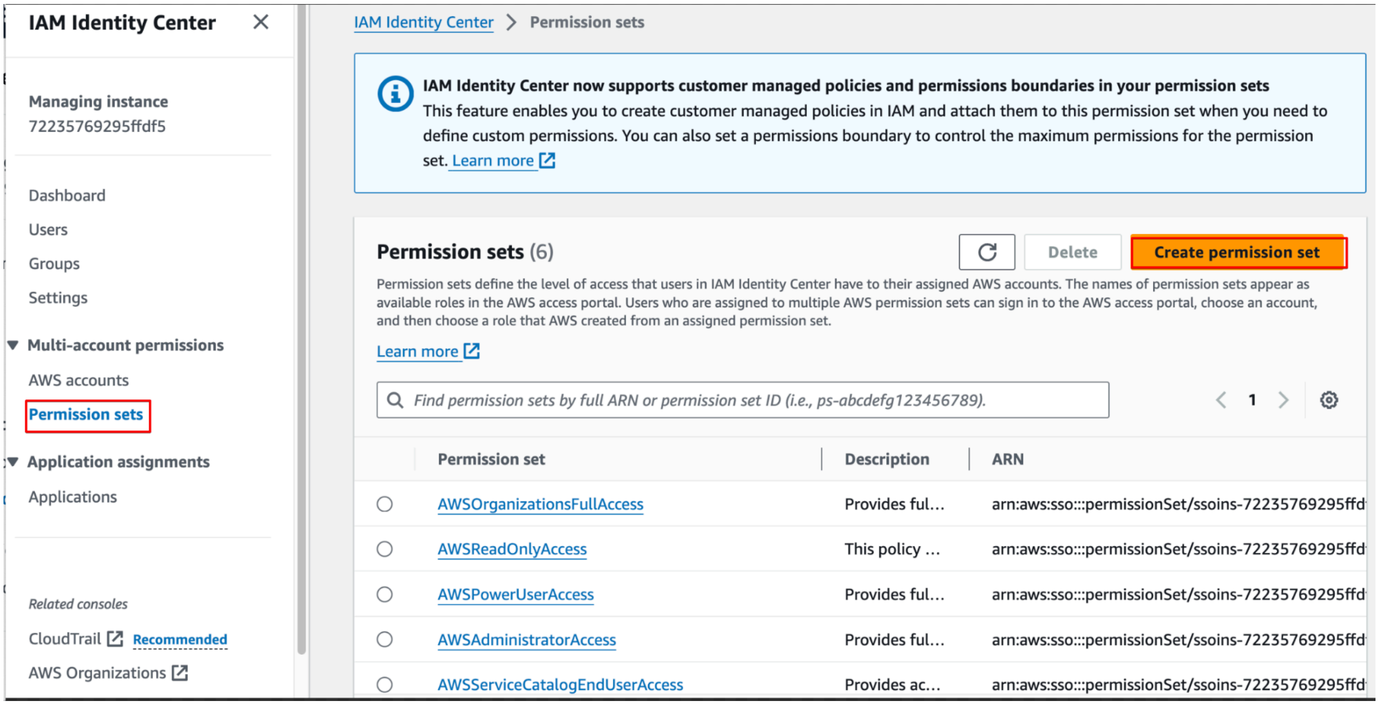
c. Click Next to add a user to Groups. Select the preconfigured group **AWSSecurityAuditors**. This group already has the permissions that will grant read-only access to users.

d. Copy details and share with the user.

e. Test this by logging in as auditor and you will notice the only permission set available to access the account is the AWSReadonlyaccess.. Log into any service and you will see that the user cannot create any resources.

4. **Create a custom permission set for a Developer with access to carry development work in a particular AWS account.**

   a. In the Identity Center console, under Multi-account permissions,. Select **Permission Sets** and click on create permission set.



IAM Identity Center now supports customer managed policies and permissions boundaries in your permission sets
This feature enables you to create customer managed policies in IAM and attach them to this permission set when you need to define custom permissions. You can also set a permissions boundary to control the maximum permissions for the permission set. Learn more

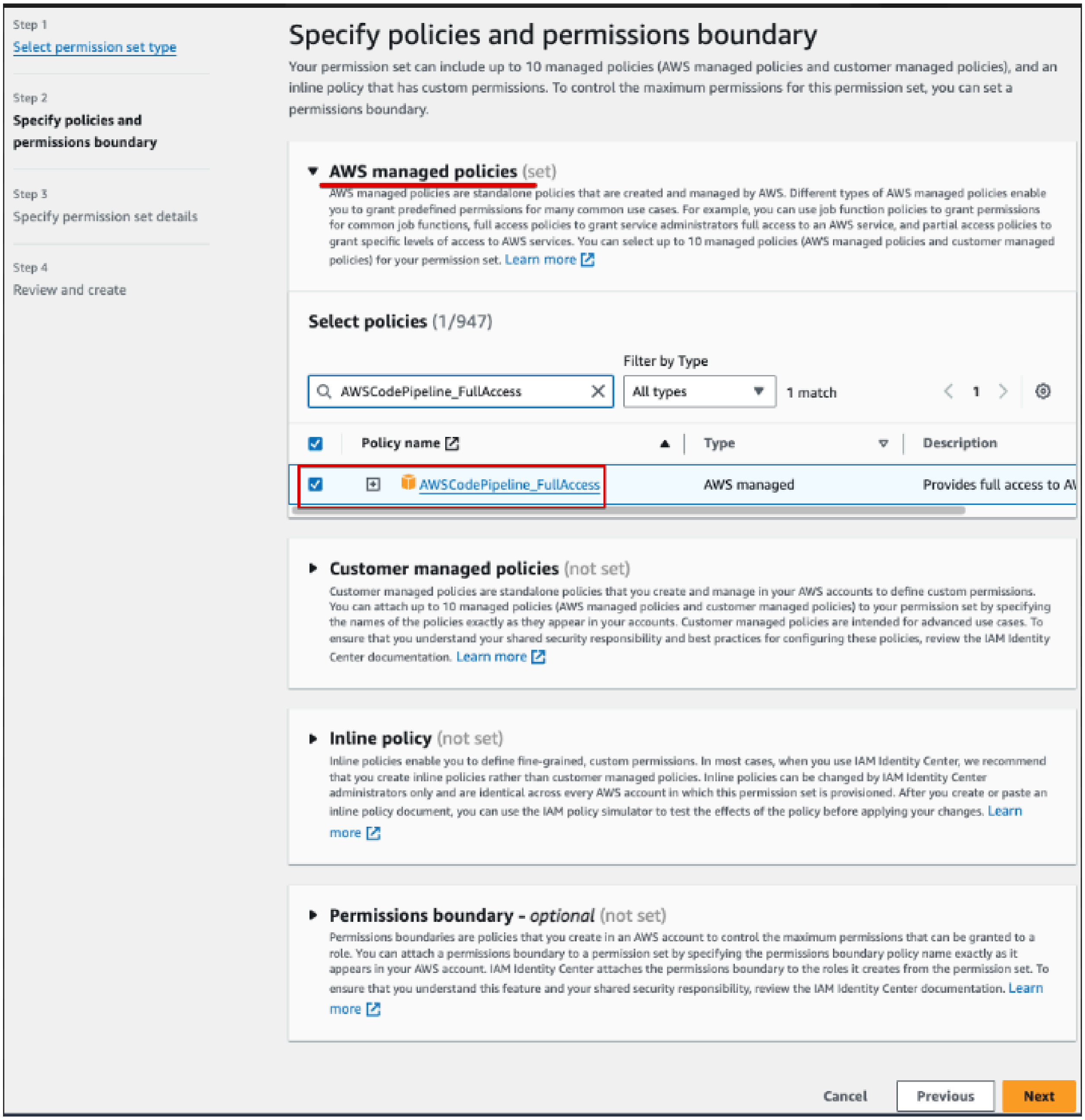
Permission sets (6)

Permission sets define the level of access that users in IAM Identity Center have to their assigned AWS accounts. The names of permission sets appear as available roles in the AWS access portal. Users who are assigned to multiple AWS permission sets can sign in to the AWS access portal, choose an account, and then choose a role that AWS created from an assigned permission set.

	Permission set	Description	ARN
○	AWSOrganizationsFullAccess	Provides ful…	arn:aws:sso:::permissionSet/ssoins-72235769295ffd
○	AWSReadOnlyAccess	This policy …	arn:aws:sso:::permissionSet/ssoins-72235769295ffd
○	AWSPowerUserAccess	Provides ful…	arn:aws:sso:::permissionSet/ssoins-72235769295ffd
○	AWSAdministratorAccess	Provides ful…	arn:aws:sso:::permissionSet/ssoins-72235769295ffd
○	AWSServiceCatalogEndUserAccess	Provides ac…	arn:aws:sso:::permissionSet/ssoins-72235769295ffd

b. Under "Permission set type" Select **custom permission set**., and click on next

c. In **"**Specify policies and permissions boundary**"**,
Select the option to attach an AWS managed policy and attach the policy **AWSCodePipelineFullAccess**.



Step 1
Select permission set type

Step 2
Specify policies and permissions boundary

Step 3
Specify permission set details

Step 4
Review and create

Specify policies and permissions boundary

Your permission set can include up to 10 managed policies (AWS managed policies and customer managed policies), and an inline policy that has custom permissions. To control the maximum permissions for this permission set, you can set a permissions boundary.

▼ **AWS managed policies** (set)

AWS managed policies are standalone policies that are created and managed by AWS. Different types of AWS managed policies enable you to grant predefined permissions for many common use cases. For example, you can use job function policies to grant permissions for common job functions, full access policies to grant service administrators full access to an AWS service, and partial access policies to grant specific levels of access to AWS services. You can select up to 10 managed policies (AWS managed policies and customer managed policies) for your permission set. Learn more

Select policies (1/947)

Search: AWSCodePipeline_FullAccess — Filter by Type: All types — 1 match

☑	Policy name	Type	Description
☑	AWSCodePipeline_FullAccess	AWS managed	Provides full access to AW

▶ **Customer managed policies** (not set)

Customer managed policies are standalone policies that you create and manage in your AWS accounts to define custom permissions. You can attach up to 10 managed policies (AWS managed policies and customer managed policies) to your permission set by specifying the names of the policies exactly as they appear in your accounts. Customer managed policies are intended for advanced use cases. To ensure that you understand your shared security responsibility and best practices for configuring these policies, review the IAM Identity Center documentation. Learn more

▶ **Inline policy** (not set)

Inline policies enable you to define fine-grained, custom permissions. In most cases, when you use IAM Identity Center, we recommend that you create inline policies rather than customer managed policies. Inline policies can be changed by IAM Identity Center administrators only and are identical across every AWS account in which this permission set is provisioned. After you create or paste an inline policy document, you can use the IAM policy simulator to test the effects of the policy before applying your changes. Learn more

▶ **Permissions boundary** - *optional* (not set)

Permissions boundaries are policies that you create in an AWS account to control the maximum permissions that can be granted to a role. You can attach a permissions boundary to a permission set by specifying the permissions boundary policy name exactly as it appears in your AWS account. IAM Identity Center attaches the permissions boundary to the roles it creates from the permission set. To ensure that you understand this feature and your shared security responsibility, review the IAM Identity Center documentation. Learn more

d. Under “specify permission set details” enter **name** e.g **DevTeam** and other other details for
e. Next through, review and create Permission Set.

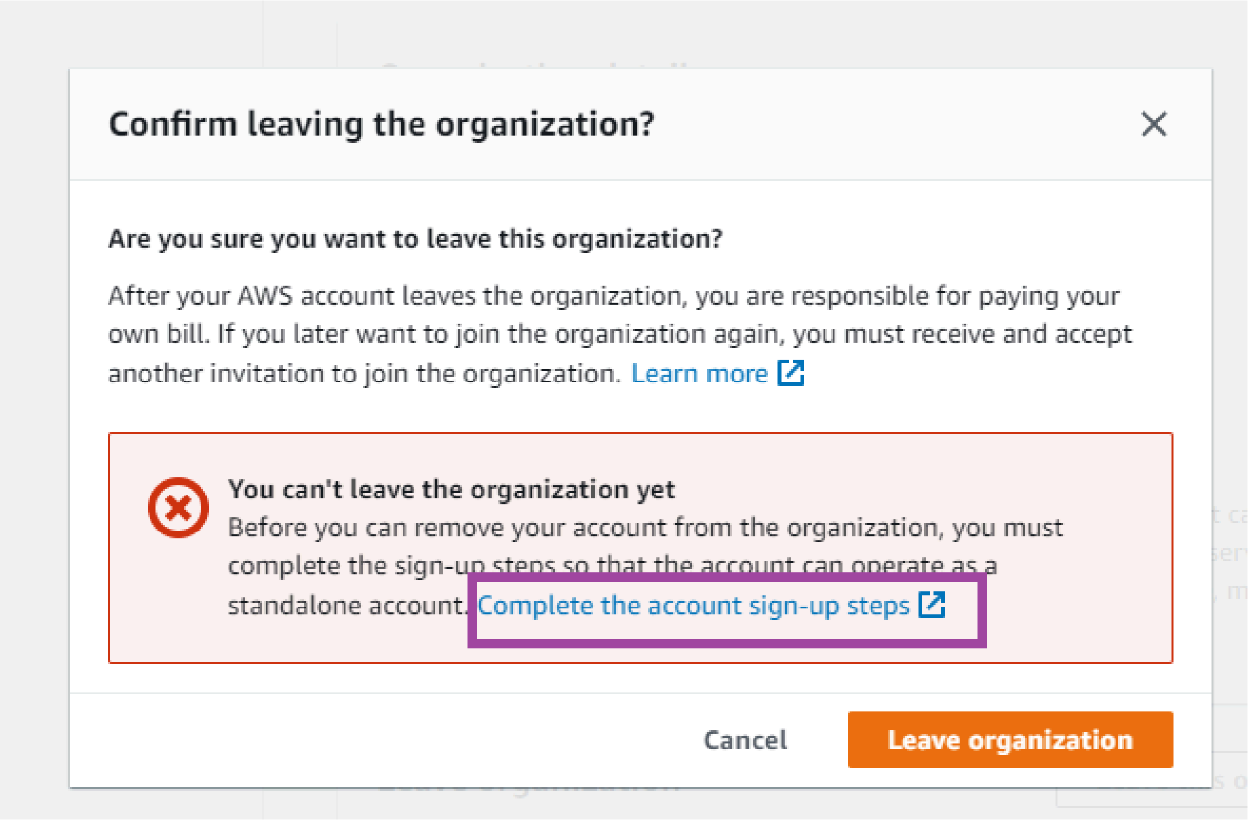
f. Go to the Identity Center Console, Navigate to the Groups and create a Group named **DevOpsAdmin**
g. Create a new user and assign to the group created above
h. To grant users access to a specific AWS account:
    i. Navigate to the AWS account screen, select the account to grant permissions to and click on Assign users and click on next
    ii. In the Select users or group screen, choose group and select the DevOpsAdmin Group.
    iii. Select the Permission sets created above and click on Finish.
    iv. Test this by logging in as the user user created in g above and test the permissions.

CLEAN UP(Students will do cleanup on their own by following the below steps) !!

To clean up this lab, you will need to remove the accounts from the AWS organization and close the account

Remove Account from Organization

1. Log into the account you want to remove from the organization as a root user.
2. Navigate to the AWS Organization and select the leave organization. You will let the prompt below. Click on complete the account sign-up-steps



Confirm leaving the organization?

Are you sure you want to leave this organization?

After your AWS account leaves the organization, you are responsible for paying your own bill. If you later want to join the organization again, you must receive and accept another invitation to join the organization. Learn more

You can't leave the organization yet

Before you can remove your account from the organization, you must complete the sign-up steps so that the account can operate as a standalone account. Complete the account sign-up steps

3. Complete the payment details step and leave the organization.

Close AWS Account

1. Login as root in the AWS account
2. Click on the My Account and close account