😊 AWS Control Tower

AWS Control Tower is an Amazon Web Services (AWS) service designed to help organizations set up and govern a secure, multi-account AWS environment. It provides a straightforward and automated way to implement AWS best practices for security and compliance across an organization. Here are the main components and features of AWS Control Tower:

Key Components

1. **Landing Zone**:
    - A landing zone is a well-architected, multi-account AWS environment that adheres to AWS best practices. AWS Control Tower sets up this environment with foundational components such as centralized logging, cross-account security audits, and account baseline settings.
2. **Guardrails**:
    - Guardrails are pre-configured policies that enforce governance rules in your AWS environment. They help manage security, compliance, and operational practices. Guardrails come in two types:
        - **Preventive Guardrails**: These prevent actions that could lead to security vulnerabilities or non-compliance.
        - **Detective Guardrails**: These monitor and detect policy violations, providing alerts for remediation.
3. **Account Factory**:
    - The Account Factory in AWS Control Tower simplifies the provisioning of new AWS accounts. It allows for the creation of accounts with pre-configured settings and guardrails, ensuring they align with organizational policies from the start.
4. **Dashboard**:
    - The AWS Control Tower dashboard provides visibility into your multi-account environment. It shows the status of guardrails, compliance across accounts, and other key information. This centralized view helps administrators monitor and manage the environment effectively.
5. **Blueprints**:
    - Blueprints are configurations that define how AWS accounts and resources should be set up within the Control Tower environment. They include pre-configured roles, permissions, and resource configurations.

Features and Benefits

- **Centralized Governance**: Control Tower provides a single point of control for managing security and compliance across multiple AWS accounts. It integrates with AWS Organizations to facilitate centralized management.

- **Automated Account Provisioning**: The Account Factory streamlines the creation of AWS accounts, ensuring they are set up with consistent security and compliance settings.
- **Pre-configured Best Practices**: AWS Control Tower incorporates AWS best practices, making it easier for organizations to meet industry standards and regulatory requirements.
- **Ease of Use**: With an intuitive interface and automated workflows, AWS Control Tower reduces the complexity of managing a multi-account environment, making it accessible to organizations without extensive cloud governance expertise.
- **Scalability**: AWS Control Tower scales with your organization, allowing you to easily manage additional accounts and resources as your cloud footprint grows.

AWS Control Tower is especially useful for organizations looking to establish a standardized, secure, and compliant AWS environment quickly and efficiently. It reduces the overhead associated with managing multiple accounts and enforces a consistent governance framework

😄 Use Cases of AWS Control Tower:

AWS Control Tower is designed to simplify the management and governance of a multi-account AWS environment, making it a valuable tool for a variety of use cases. Here are some common scenarios where AWS Control Tower is particularly useful:

1. Enterprise Cloud Adoption

- **Centralized Governance and Compliance**: Large enterprises adopting AWS can use Control Tower to establish a well-architected, secure environment from the outset. It helps enforce governance policies across multiple business units or departments, ensuring compliance with industry regulations and internal standards.
- **Standardized Account Creation**: Enterprises can standardize the setup of new AWS accounts, ensuring each one is provisioned with the necessary security controls, compliance settings, and baseline configurations.

2. Startups and Small to Medium Businesses (SMBs)

- **Rapid and Secure Cloud Onboarding**: For startups and SMBs, AWS Control Tower provides a straightforward way to set up a secure AWS environment without needing deep expertise in cloud governance. It offers pre-configured best practices that help new businesses get started quickly while maintaining security and compliance.
- **Scalable Growth**: As these businesses grow, they can easily expand their AWS environment, creating new accounts and scaling resources while maintaining a consistent security posture.

3. Regulated Industries

- **Compliance with Regulatory Requirements**: Industries such as finance, healthcare, and government often have stringent compliance requirements. AWS Control Tower

helps organizations in these sectors implement and monitor compliance controls, ensuring that all AWS accounts adhere to necessary regulations and standards.

- **Audit Readiness**: Control Tower provides visibility into compliance across all accounts, making it easier to prepare for and respond to audits.

4. Decentralized Teams and Business Units

- **Autonomous Yet Governed Environments**: Organizations with decentralized teams or business units can use AWS Control Tower to provide autonomy in managing their AWS accounts while still enforcing global security and compliance policies. Each team can have the flexibility to manage its own resources, but within the guardrails set by the central IT or cloud governance team.
- **Resource Isolation and Cost Management**: By using separate AWS accounts for different teams or projects, organizations can achieve resource isolation and better manage costs. Control Tower facilitates the easy creation and management of these accounts.

5. Mergers and Acquisitions

- **Integrating Acquired Companies**: When companies are acquired, integrating their IT infrastructure into the existing environment can be challenging. AWS Control Tower provides a standardized way to bring the new company's AWS accounts into the existing governance framework, ensuring security and compliance alignment.

6. Multi-Cloud and Hybrid Cloud Strategies

- **Centralized Control in Hybrid Environments**: For organizations leveraging a hybrid cloud strategy, AWS Control Tower can help manage the AWS portion of their infrastructure in a consistent and secure manner. It allows for a unified approach to security and governance, even when some workloads remain on-premises or in other clouds.

7. Cloud Migration

- **Migrating to AWS**: Organizations migrating workloads from on-premises or other cloud providers to AWS can use Control Tower to establish a secure landing zone. This ensures that new AWS accounts are set up with the appropriate security controls and governance mechanisms, facilitating a smooth migration.

🤔 What are we doing in this Lab?

In this exercise, you are setting up an AWS Control Tower environment, also known as a "landing zone." The process involves configuring a multi-account AWS setup with governance and security controls according to AWS best practices. The steps include setting up organizational units (OUs) for different purposes, creating shared accounts for logging and auditing, and configuring access and identity management.

End Goal: The goal is to establish a secure and governed AWS environment where multiple accounts can be managed efficiently. This setup includes:

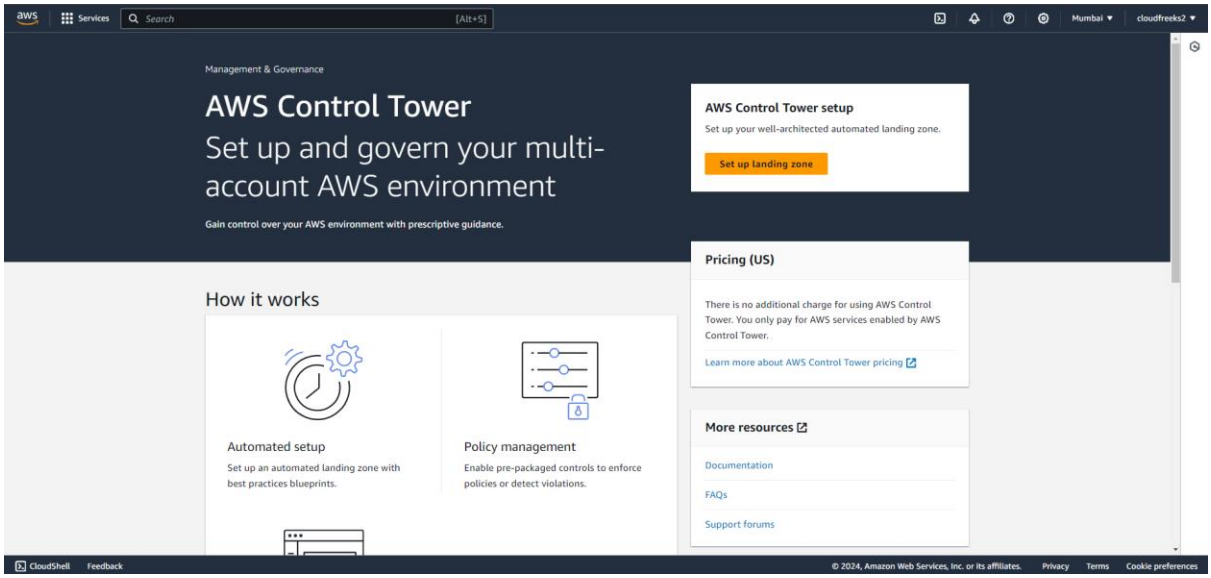
1. **Organizational Structure:** Creating OUs for shared and user-provisioned accounts.
2. **Shared Accounts:** Setting up management, log archive, and security audit accounts.
3. **Governance and Compliance:** Implementing preventive and detective controls to enforce and monitor policies.
4. **VPC Configuration:** Defining network settings for new accounts.
5. **User Access Management:** Managing federated access and user identities.

The outcome is a centralized system that provides secure, compliant, and scalable management of AWS resources across the organization.

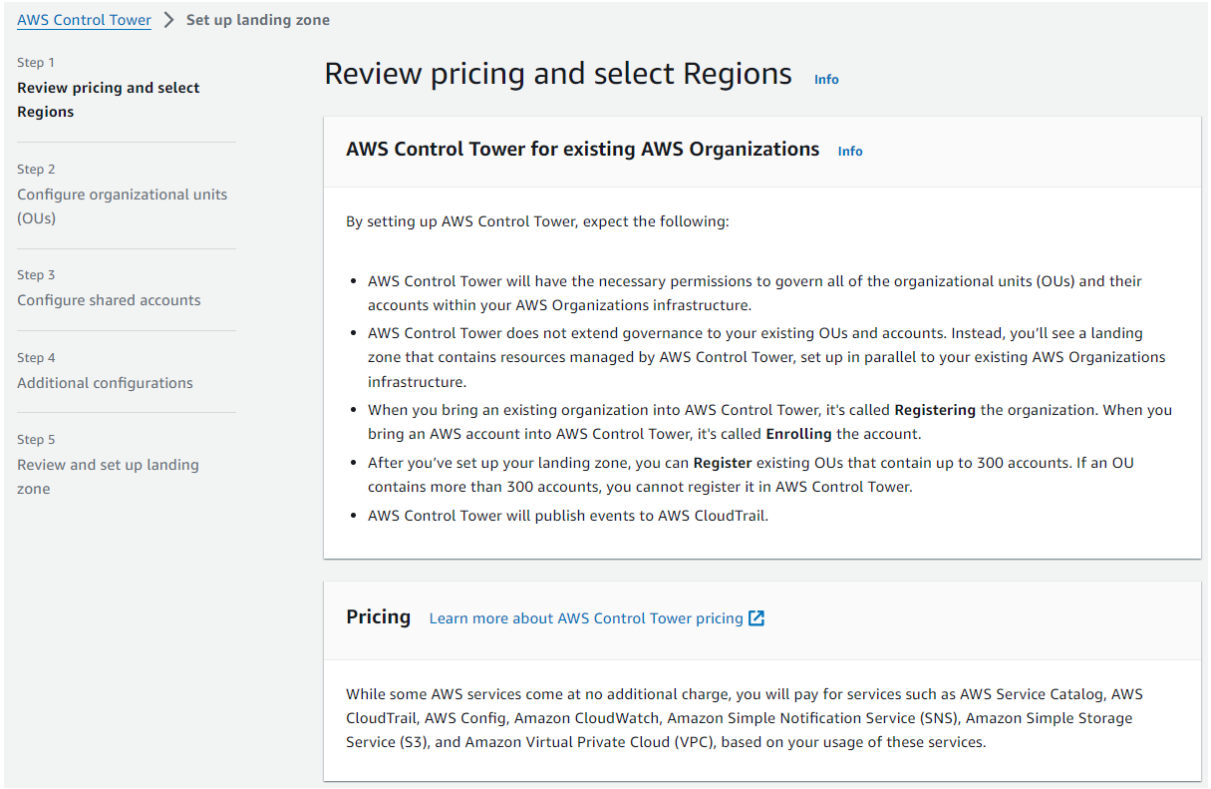
The end goal of setting up AWS Control Tower is to create a well-organized and secure environment in AWS where you can easily manage and control multiple AWS accounts. This setup ensures that all accounts follow the same security and governance rules, making it easier to keep things safe and compliant. It also simplifies the process of creating new accounts and managing them, so you can focus on building and running your applications without worrying about security and compliance details.

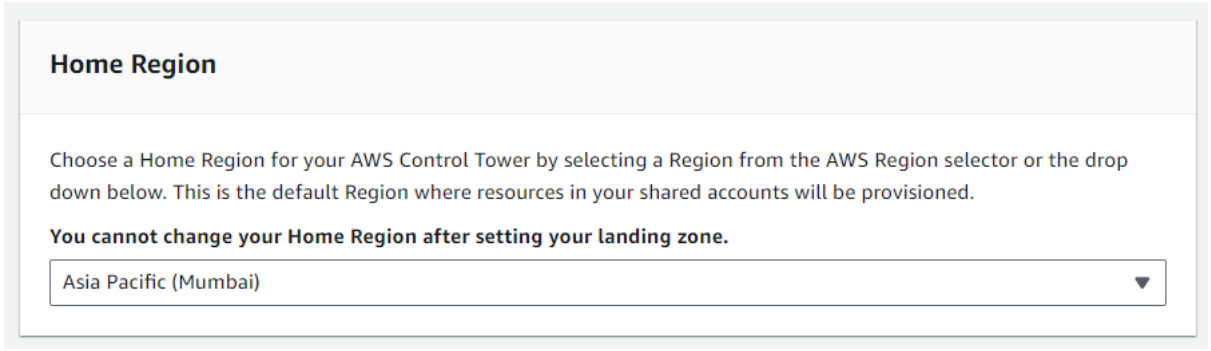
😄 To begin with the Lab:

1. In your AWS Console search for control tower and navigate to it. You will see that same page as shown below and you need to click on Set up Landing zone.



2. So, remember when we create our configuration in Control Tower, it's known as a landing zone, and that's the number of accounts and configurations that are applied (check in the snapshots). Here, AWS lets you know what to expect when you set up Control Tower. Essentially, Control Tower is going to have the ability to govern your resources across accounts and organizational units, but it's not going to take control of everything by default. So, you can extend that governance afterward.
3. Below are the snapshots of Step 1 from the control tower just keep those to default and click on next.


AWS Control Tower
Set up landing zone
Step 1
Review pricing and select Regions
Step 2
Configure organizational units (OUs)
Step 3
Configure shared accounts
Step 4
Additional configurations
Step 5
Review and set up landing zone
Review pricing and select Regions
Info
AWS Control Tower for existing AWS Organizations
Info
By setting up AWS Control Tower, expect the following:
AWS Control Tower will have the necessary permissions to govern all of the organizational units (OUs) and their accounts within your AWS Organizations infrastructure.
AWS Control Tower does not extend governance to your existing OUs and accounts. Instead, you'll see a landing zone that contains resources managed by AWS Control Tower, set up in parallel to your existing AWS Organizations infrastructure.
When you bring an existing organization into AWS Control Tower, it's called Registering the organization. When you bring an AWS account into AWS Control Tower, it's called Enrolling the account.
After you've set up your landing zone, you can Register existing OUs that contain up to 300 accounts. If an OU contains more than 300 accounts, you cannot register it in AWS Control Tower.
AWS Control Tower will publish events to AWS CloudTrail.
Pricing
Learn more about AWS Control Tower pricing
While some AWS services come at no additional charge, you will pay for services such as AWS Service Catalog, AWS CloudTrail, AWS Config, Amazon CloudWatch, Amazon Simple Notification Service (SNS), Amazon Simple Storage Service (S3), and Amazon Virtual Private Cloud (VPC), based on your usage of these services.


Home Region
Choose a Home Region for your AWS Control Tower by selecting a Region from the AWS Region selector or the drop down below. This is the default Region where resources in your shared accounts will be provisioned.
You cannot change your Home Region after setting your landing zone.
Asia Pacific (Mumbai)

Select additional Regions for governance (1/29) Info

Select the AWS Regions to govern for your environment. **Review the Additional Regions for governance** help panel, because certain controls in AWS Control Tower are not available in all Regions. The home Region cannot be deselected.

We recommend that you expand your AWS Control Tower landing zone only into AWS Regions where you require workloads to run.

1 2 3 4

Region name	Region code	AWS Control Tower status	AWS Region status
Asia Pacific (Mumbai) Home Region	ap-south-1	Not governed	Active by default
Asia Pacific (Hyderabad)	ap-south-2	Not governed	Not active
Europe (Milan)	eu-south-1	Not governed	Not active
Europe (Spain)	eu-south-2	Not governed	Not active
Middle East (UAE)	me-central-1	Not governed	Active
Israel (Tel Aviv)	il-central-1	Not governed	Not active
Canada (Central)	ca-central-1	Not governed	Active by default
Europe (Frankfurt)	eu-central-1	Not governed	Active by default

Region deny setting Info

Select settings of the Region deny control for your landing zone. You cannot deny access to your home Region. This setting can be changed at a later time.

The Region deny setting enforces a control that prohibits access to AWS services and operations, by Region. It can be enabled for the landing zone and for individual OUs. For the landing zone, the configuration is based on the selections in the Additional Regions for governance table. It is enforced when you confirm your landing zone configurations. **Review the Region deny setting** help panel to understand how the Region deny control affects your landing zone and OUs.

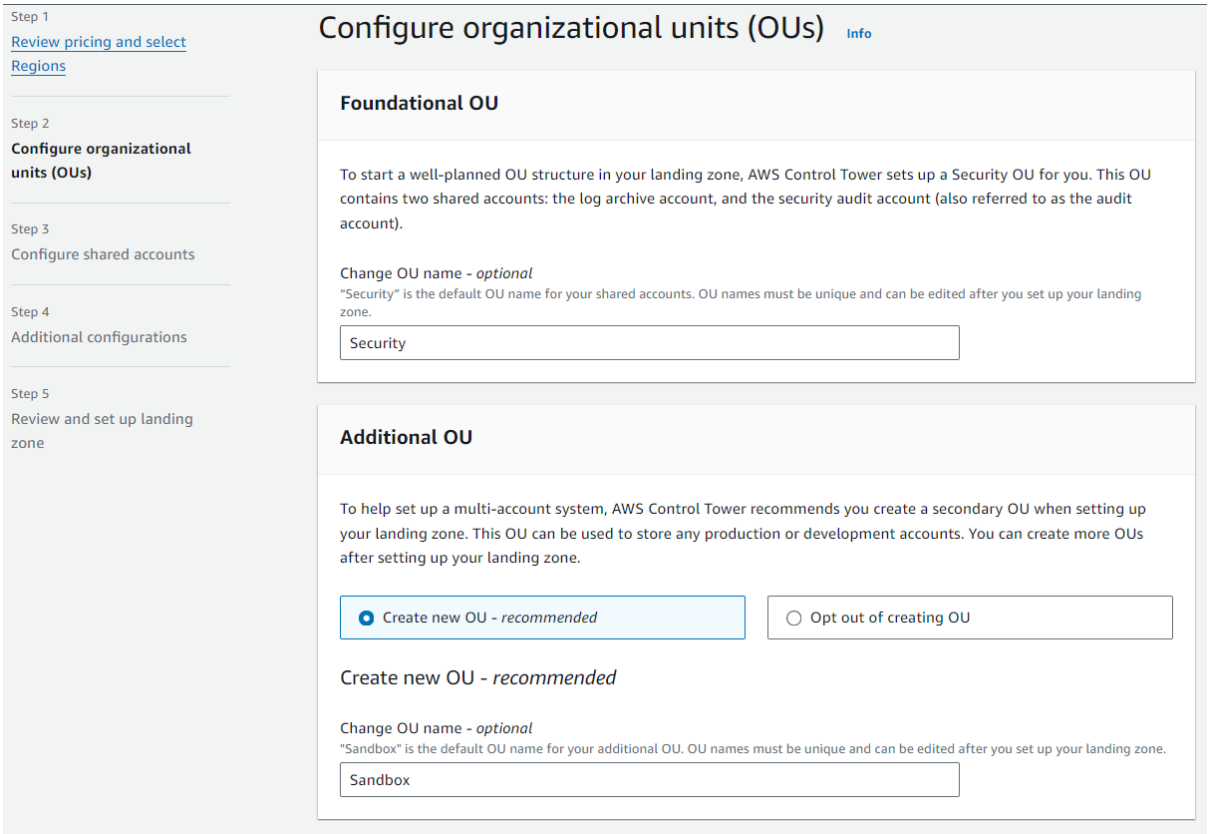
Before you enforce the Region deny control, be sure you do not have existing resources in Regions you want to deny, and Regions AWS Control Tower is not available in. You cannot access the resources in those Regions after the control is enforced.

Enabled

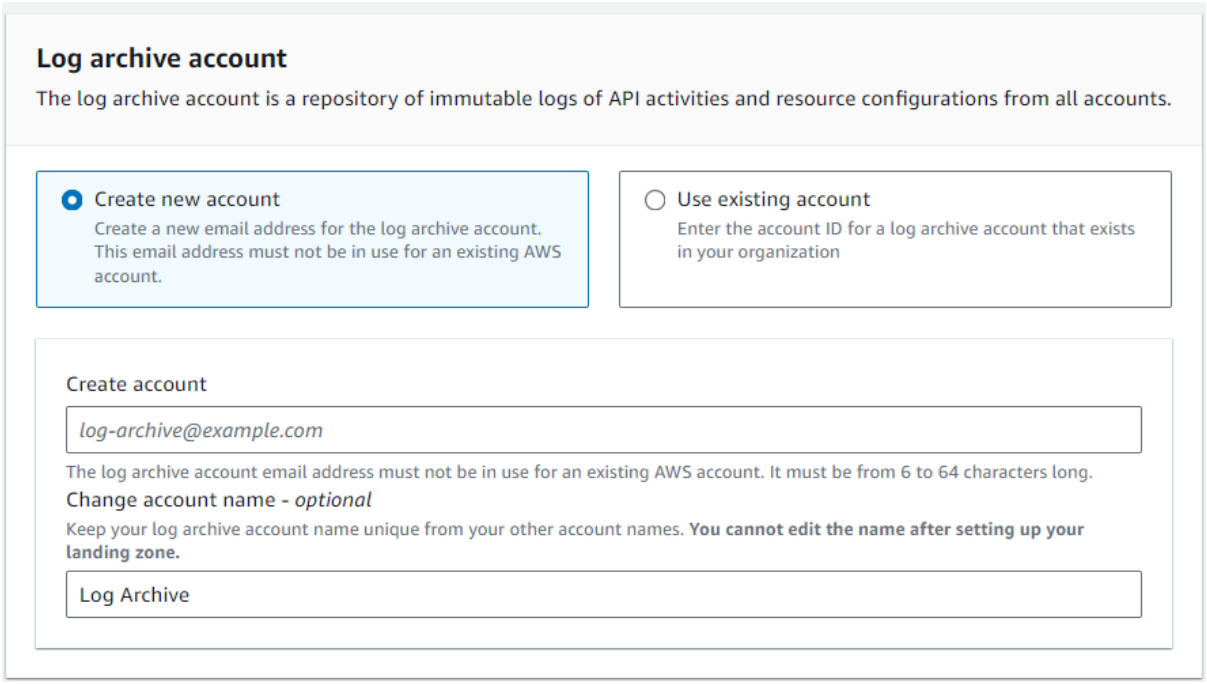
Not enabled

Cancel Next

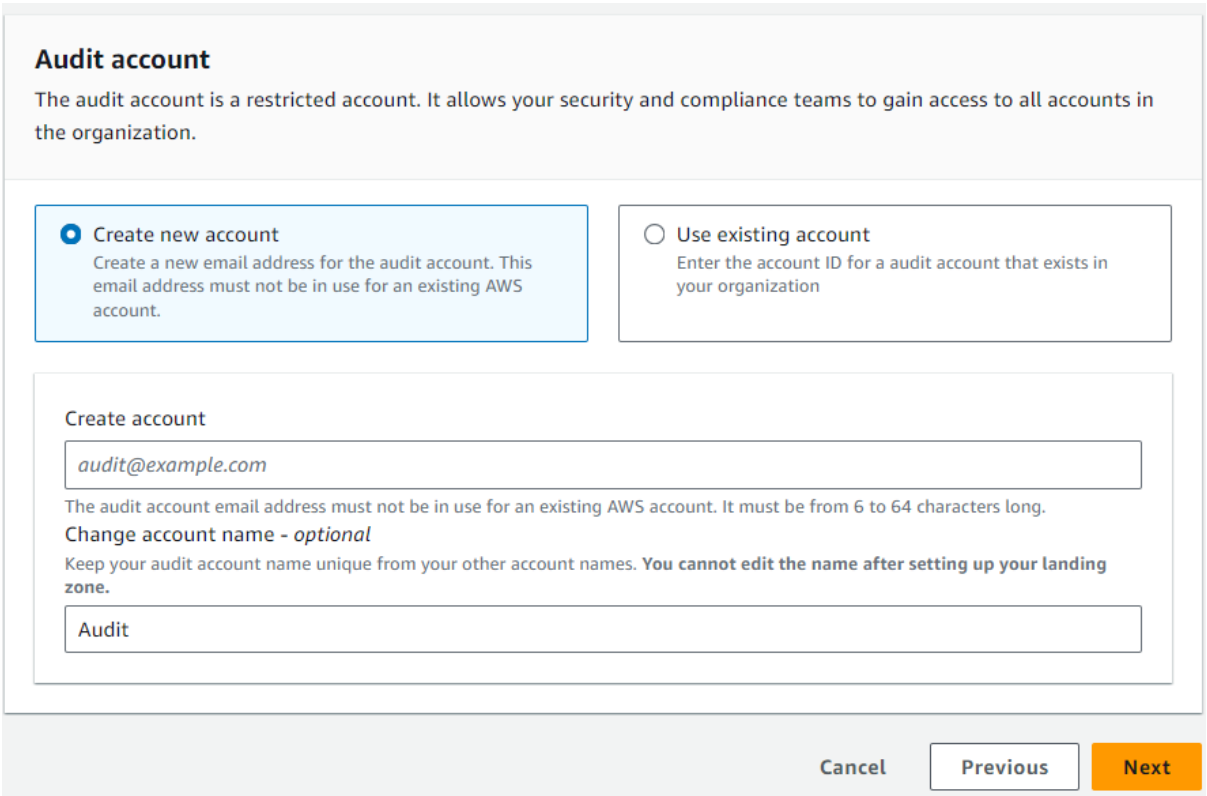
4. Now step 2 you will see that we can define the organizational unit structure. The foundational OU, which is called 'Security' as you can see below in the snapshot, is where we're going to have two shared accounts that will be the **log archive account** and the **security audit account**. Then, you can also create an additional OU if you wish to. This one's called 'Sandbox', and you can create an account there after setup, which you can then use for any kind of dev/test workloads. Let's just leave the defaults, and I'm going to click on 'Next'.



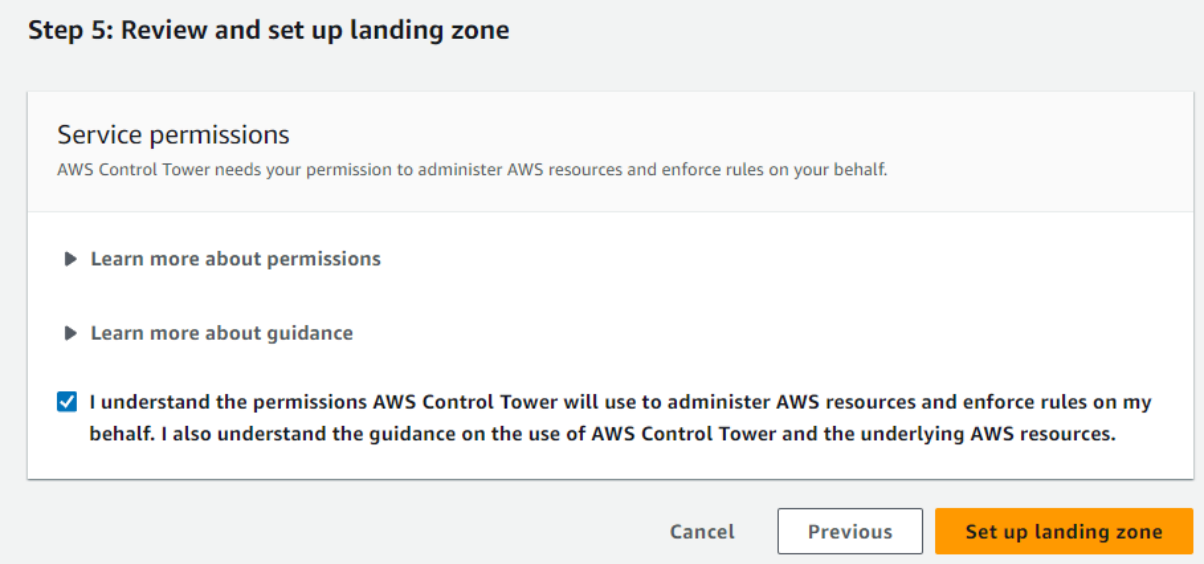
5. On the third step of the wizard, we can configure the shared accounts and the encryption settings.
6. Below you can see that it is creating two accounts or you can use 2 existing accounts if you have any.
7. If you are going with the option to create a new account then you need to give an email address.



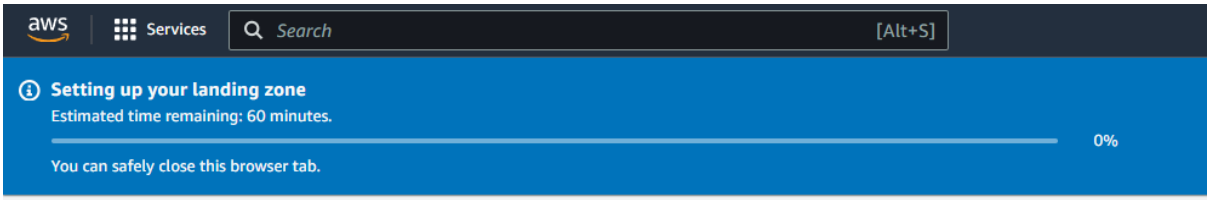
8. Same for the Audit account you need to provide the email address or you can go with the existing account instead.



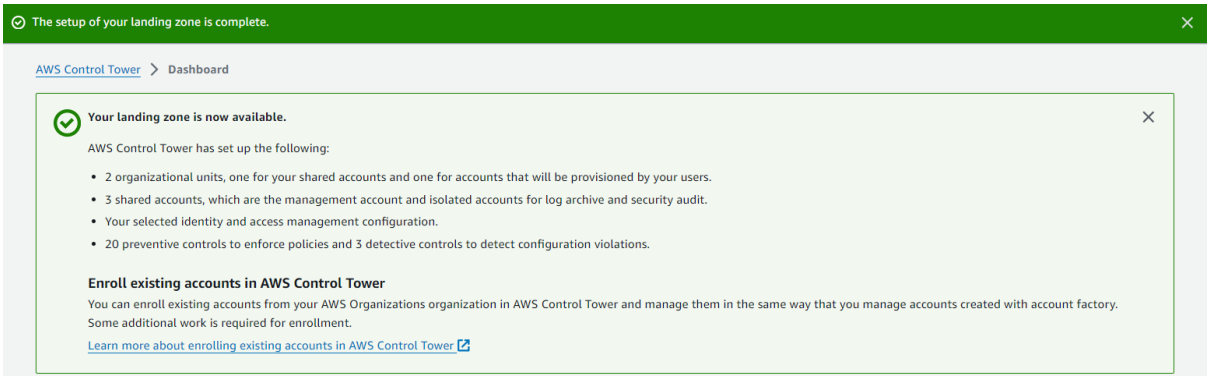
9. Once you have given the emails you can move to step 4 and keep the settings to default then move to the review page. Here you can check your details once again and check the box then click on Set up Landing zone.



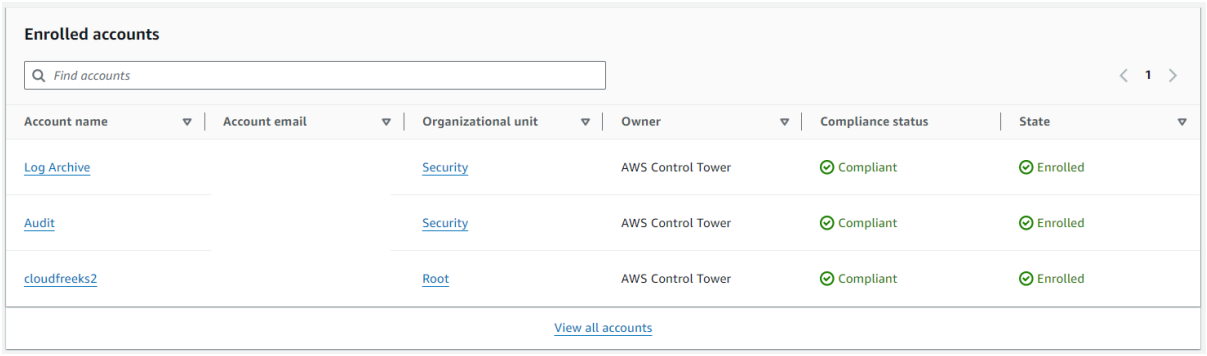
10. Now it will take some time to set up the control tower. As you can see below it will take 60 minutes.



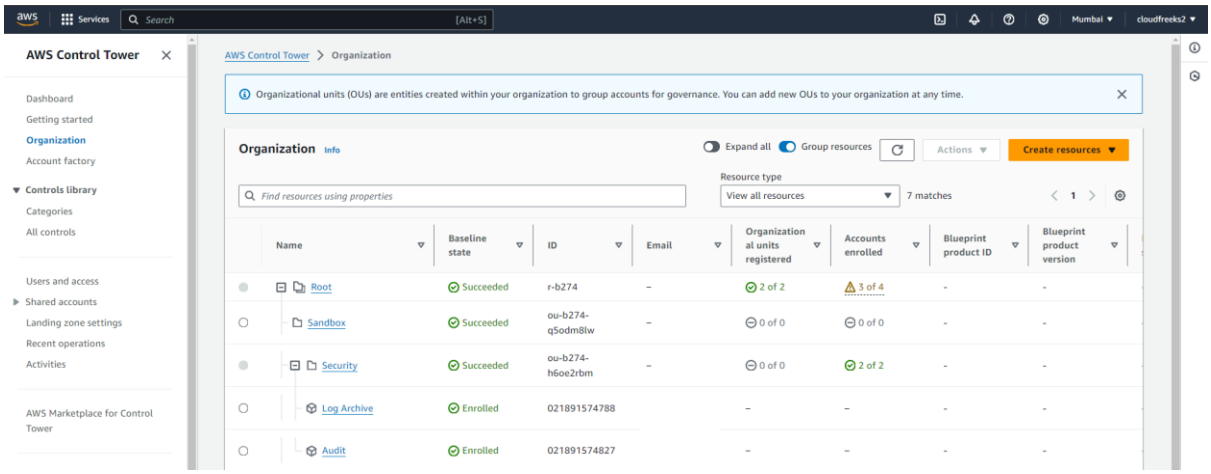
11. After 60 minutes you can see that our landing zone is now available to us. Also, the AWS Control tower has set up the following.
    - 2 organizational units, one for your shared accounts and one for accounts that will be provisioned by your users.
    - 3 shared accounts, which are the management account and isolated accounts for log archive and security audit.
    - Your selected identity and access management configuration.
    - 20 preventive controls to enforce policies and 3 detective controls to detect configuration violations.



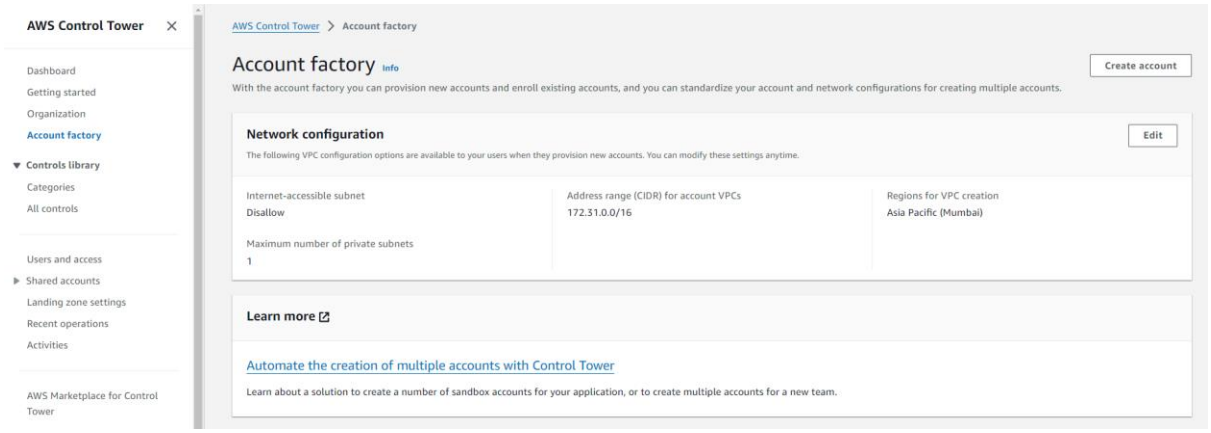
12. Now scroll down to the bottom of the dashboard and here you will see three enrolled accounts. So, you can see that the last account is the root account where I have created the control tower which is why it has the OU as the root, along with that it has created two more accounts which have been created from scratch.

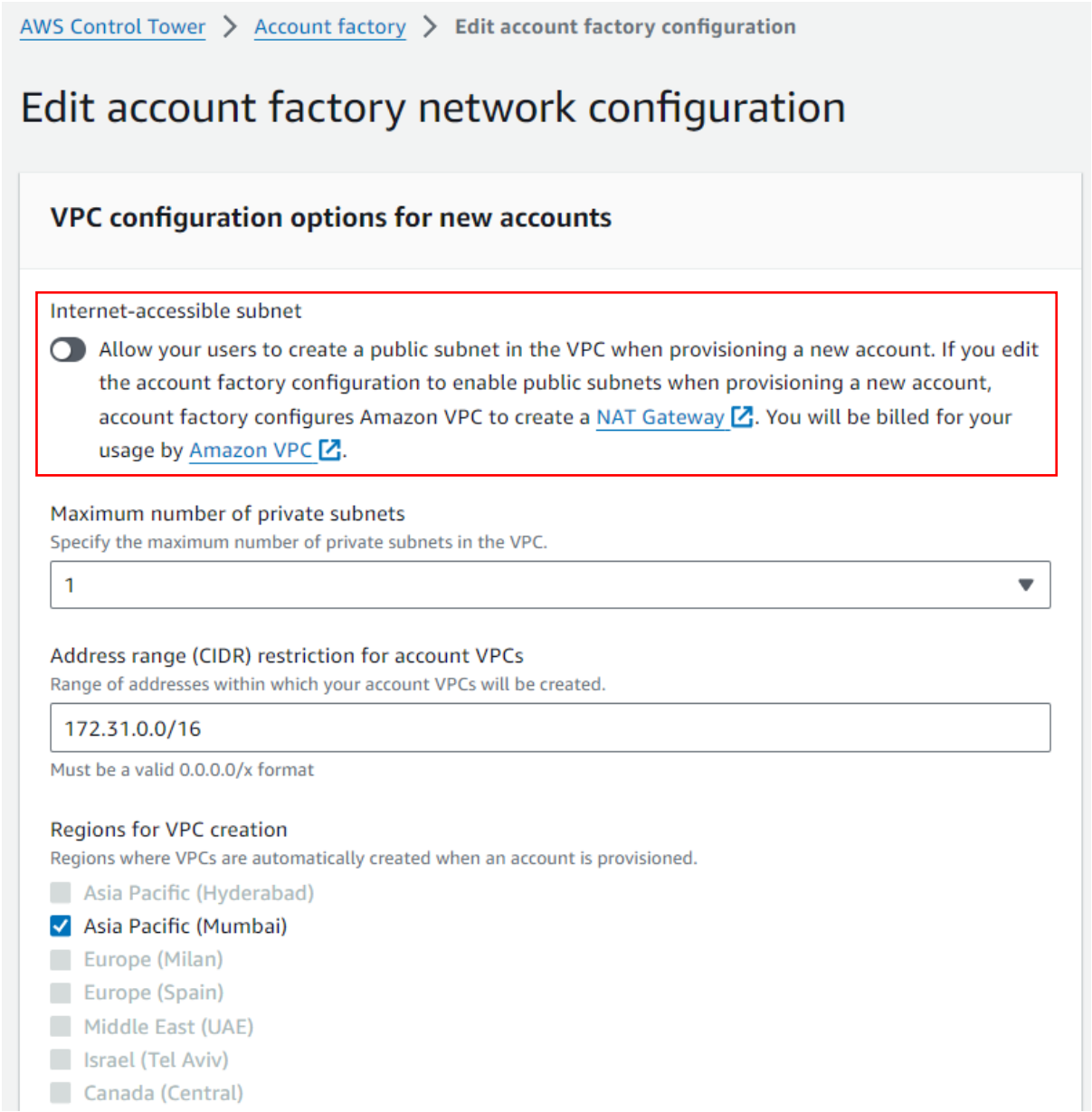


13. Now if you go to Organization, you will see the accounts related to AWS Control Tower.

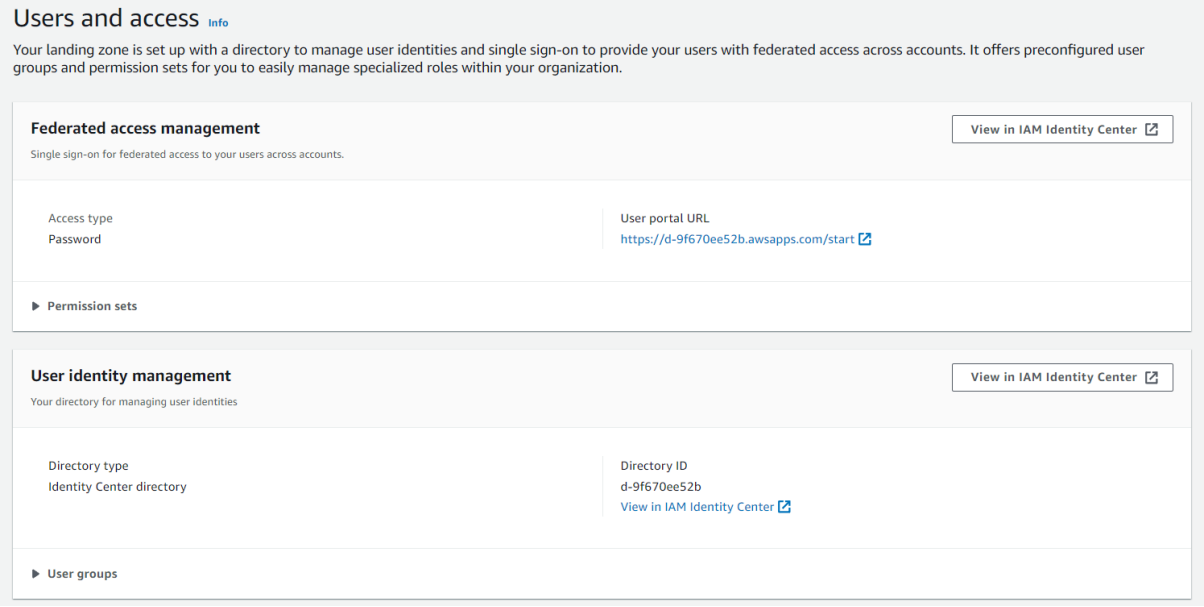


14. Now if you go to Account Factory here, we can see the VPC configuration options that are available for users when they provision new accounts. So, what this is, it defines what is allowed to be created in a VPC that's controlled by Control Tower. So, we can choose to enable internet-accessible subnets (that's disabled by default), the number of private subnets they're allowed to have, and so on. Now, I've only got the one region that's enabled at this stage, so you can see the others are all grayed out here. You can also enroll accounts, so you can either enroll accounts that already exist and bring them under the control of Control Tower, or you can create a new account.

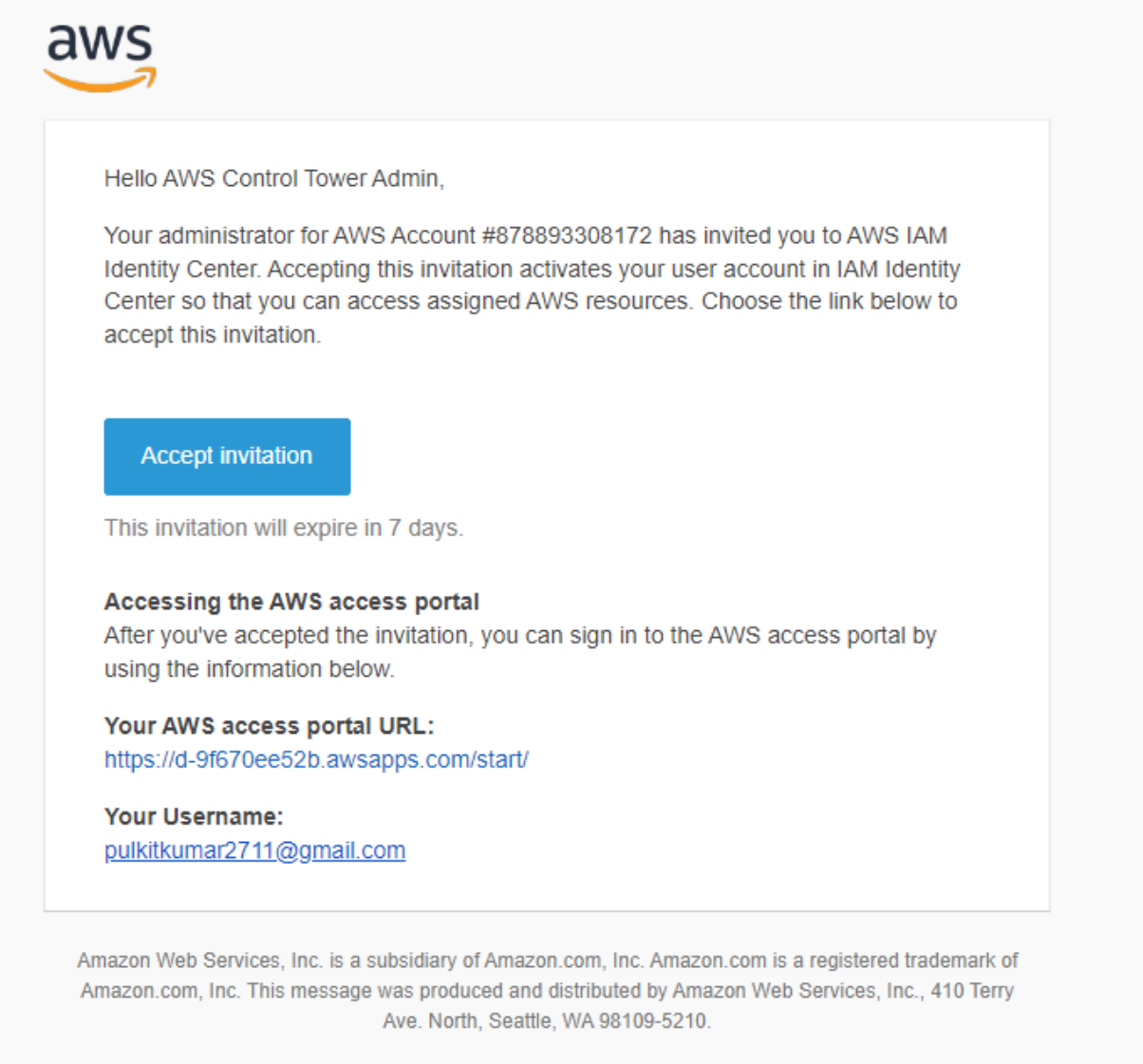




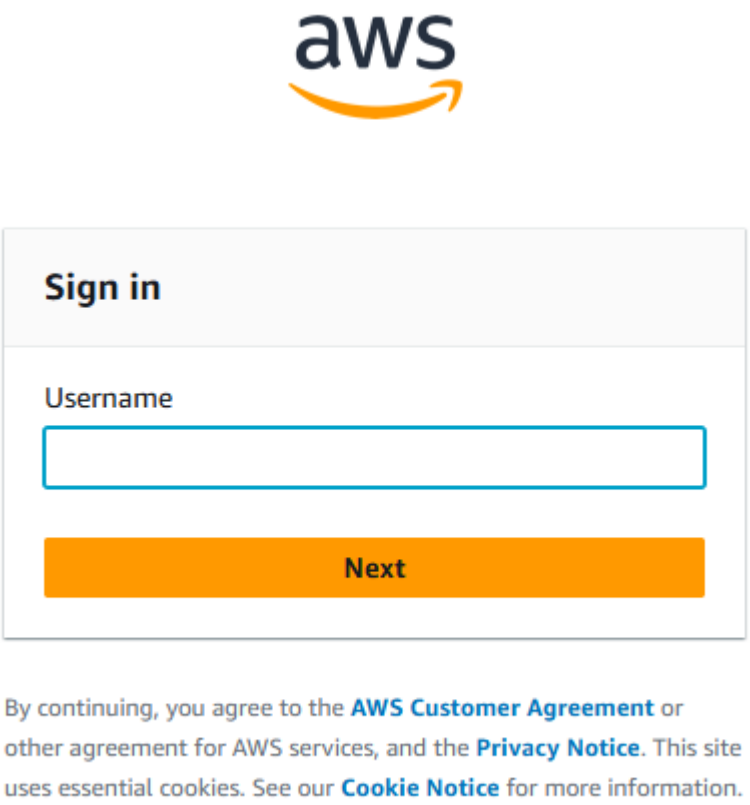
15. In users and access you can see your federated access management and the user identity management.
16. Also, you can see the User portal URL here, you can open this URL in another browser and open login with your Admin user.
17. The details regarding the Login will be mailed to you by AWS. So, check your email for that.



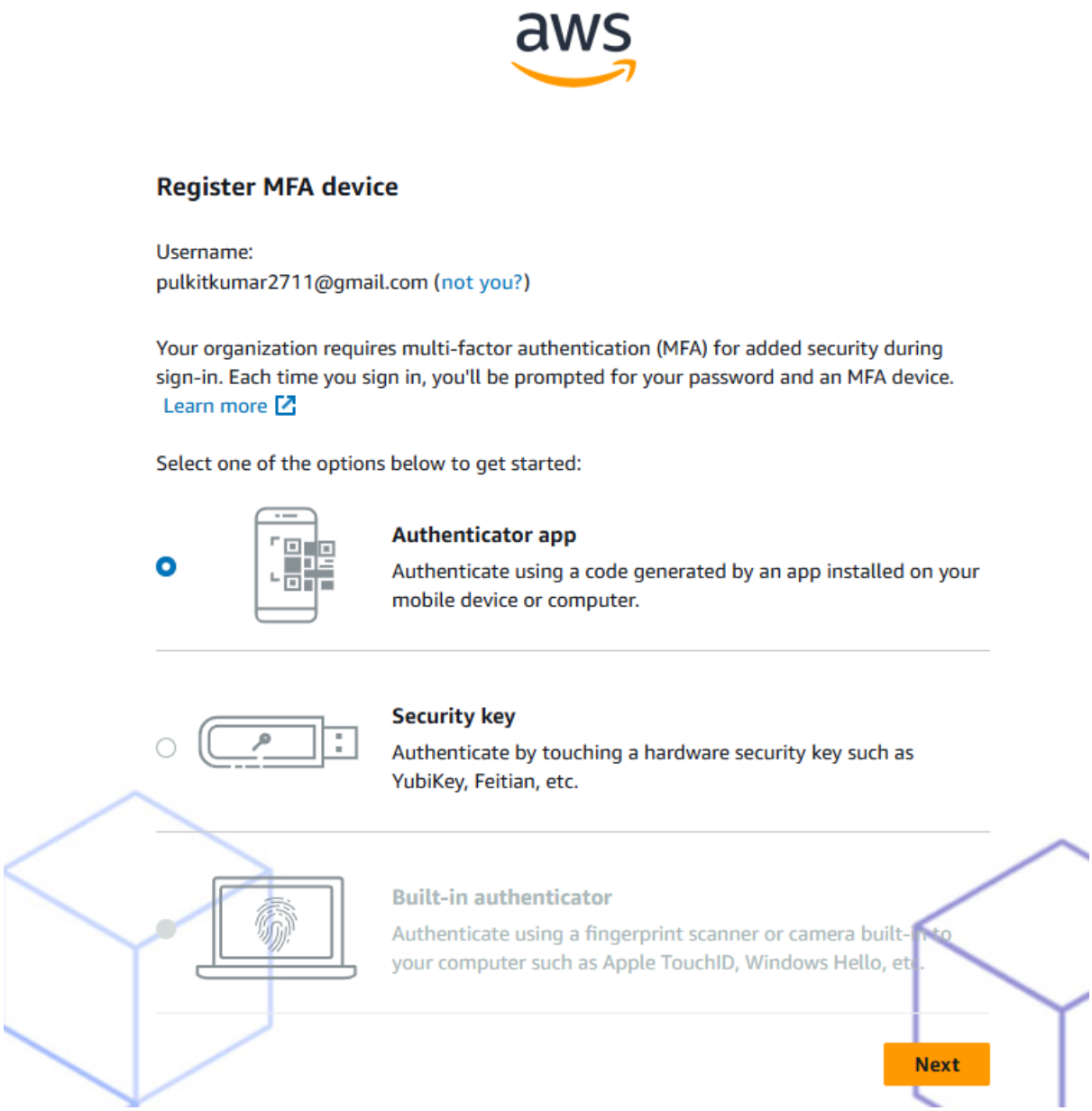
18. First you need to go to the email and accept the invitation then you have to create a password. Now copy the URL.



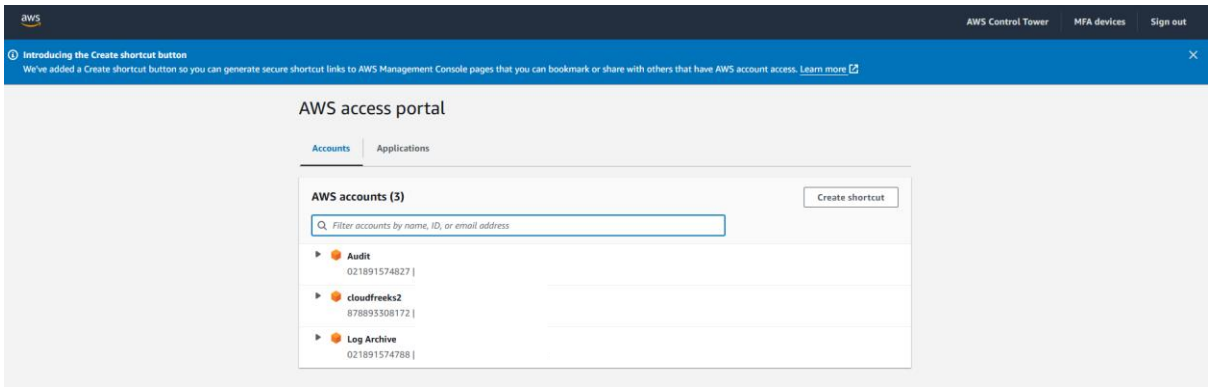
19. Now paste this URL into another browser and you will see it is asking you for a username. Now you need to give your username which AWS has provided you in the email.



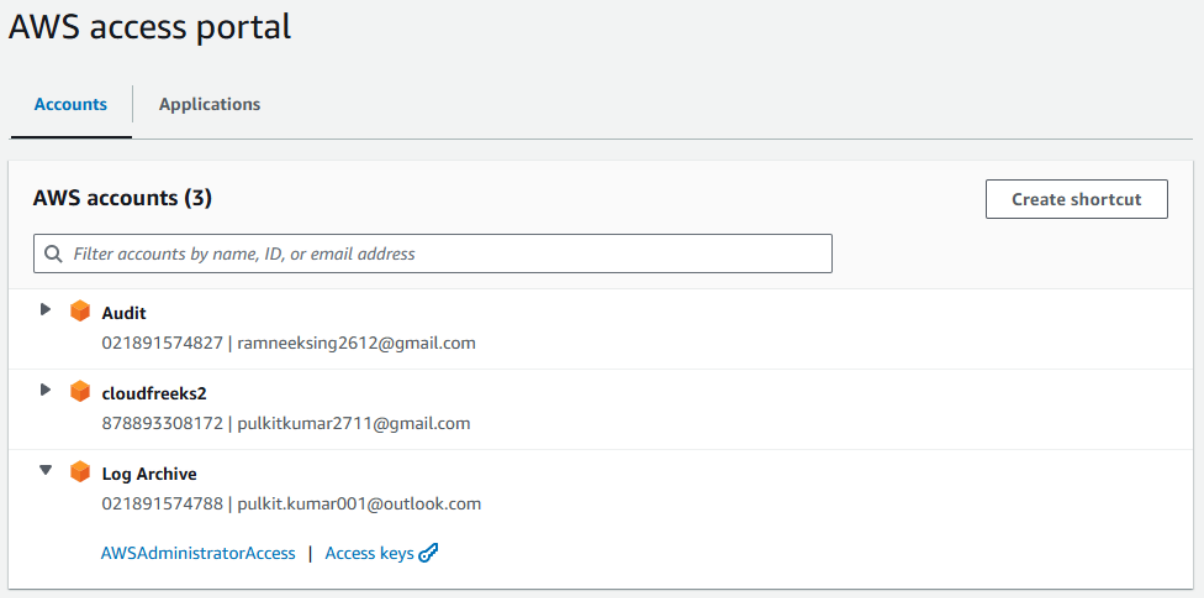
20. Below you can see that it is also asking you to enable the MFA. Do and it and move forward.



21. Once you have logged in you will be on the same page as shown below and you have ability to login into any of the three-account shown below.



22. Let’s say you want to go into the Log archive account so you need to expand it and you’ll have two options either get the access keys or you can click on AWS Administrator access and go to the management console.



23. Once you are in the account then just go to S3. As it is the Log Archive account in the S3 it has buckets regarding the log which you can check yourself.