

## **AWS Landing Zone Set up**

To set up control Tower you will need the following

- One AWS account which will be used as the master account ( **please use the same master account that has your AWS organization**)
- 2 email addresses that is not associated with any AWS account

It takes 60-90 minutes to launch an AWS Control Tower on a new AWS account. So I recommend you follow the below steps to deploy the control tower before our session.

### **Steps:**

1. Log in to the AWS Management Console of the account where you plan to deploy AWS Control Tower. This should be the same master account which you used for the AWS organization simulation.
2. Select the service **Control Tower** under **Management & Governance**.
3. Make sure you are in a control Tower supported region.
4. On the AWS Control Tower home page, select **Set up your landing zone** button.
5. Select the below options while leaving everything else as default:
  - a. **Home region** - Should be the default region you are using for Control Tower
  - b. Additional AWS Regions for governance - leave blank

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.

Search:

Region name	Region code
<input checked="" type="checkbox"/> US East (N. Virginia) <b>Home Region</b>	us-east-1
<input type="checkbox"/> Asia Pacific (Hyderabad)	ap-south-2
<input type="checkbox"/> Asia Pacific (Mumbai)	ap-south-1
<input type="checkbox"/> Europe (Milan)	eu-south-1
<input type="checkbox"/> Europe (Spain)	eu-south-2
<input type="checkbox"/> Middle East (UAE)	me-central-1
<input type="checkbox"/> Israel (Tel Aviv)	il-central-1
<input type="checkbox"/> Canada (Central)	ca-central-1

- c. **Region deny settings** select **Not enabled**

- d. **Foundational OU - Security**
- e. **Additional OU - Opt out of creating OU**

**Foundational OU**

To start a well-planned OU structure in your landing zone, AWS Control Tower sets up a Security OU for you. This OU contains two shared accounts: the log archive account, and the security audit account (also referred to as the audit account).

**Change OU name - *optional***  
"Security" is the default OU name for your shared accounts. OU names must be unique and can be edited after you set up your landing zone.

Security

**Additional OU**

To help set up a multi-account system, AWS Control Tower recommends you create a secondary OU when setting up your landing zone. This OU can be used to store any production or development accounts. You can create more OUs after setting up your landing zone.

☐ Create new OU - *recommended*

☒ Opt out of creating OU

Opt out of creating OU [Info](#)

**You have opted out of creating an additional OU during set up. You must register an organizational unit before provisioning new accounts.**

Cancel

Previous

Next

- 6. Configure shared accounts by providing 2 email IDs which will be used to set up the Log Archive account and the audit account. (This should be emails that have not been previously used for any AWS account before)

## Configure shared accounts [Info](#)

### Management account

The management account provides billing and management of your accounts and your landing zone. It relies on your existing AWS account email address.

\_\_\_\_\_?@gmail.com

### Log archive account

The log archive account is a repository of immutable logs of API activities and resource configurations from all accounts.

☒ **Create new account**

Create a new email address for the log archive account. This email address must not be in use for an existing AWS account.

☐ **Use existing account**

Enter the account ID for a log archive account that exists in your organization

#### Create account

\_\_\_\_\_'+log-archive@gmail.com

The log archive account email address must not be in use for an existing AWS account. It must be from 6 to 64 characters long.

#### Change account name - *optional*

Keep your log archive account name unique from your other account names. You cannot edit the name after setting up your landing zone.

Log Archive

### Audit account

The audit account is a restricted account. It allows your security and compliance teams to gain access to all accounts in the organization.

☒ **Create new account**

Create a new email address for the audit account. This email address must not be in use for an existing AWS account.

☐ **Use existing account**

Enter the account ID for a audit account that exists in your organization

#### Create account

\_\_\_\_\_?+audit@gmail.com

The audit account email address must not be in use for an existing AWS account. It must be from 6 to 64 characters long.

#### Change account name - *optional*

Keep your audit account name unique from your other account names. You cannot edit the name after setting up your landing zone.

Audit

- Under Additional configurations, leave defaults (Control Tower sets up access with IAM Identity Center, CloudTrail is Enabled and bucket retention for logging 1 year)

### Additional configurations

#### AWS account access configuration [Info](#)

Select how to manage access to your AWS accounts registered with AWS Control Tower. You can change this later.

☒ **AWS Control Tower sets up AWS account access with IAM Identity Center.**

Best if you are just getting started with AWS or if your access management structure works with [AWS Control Tower groups and permission sets](#). You can connect your external identity provider (IdP) in IAM Identity Center later.


☐ **Self-managed AWS account access with IAM Identity Center or another method.**

Best if you have custom requirements for managing AWS account access. AWS Control Tower will not manage account access. You must configure IAM Identity Center or another access method.

#### AWS CloudTrail configuration [Info](#)

AWS CloudTrail captures actions for AWS Control Tower as events. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket.

In an organization-level CloudTrail, AWS Control Tower aggregates information from all accounts into the organization trail and delivers the logged information to a specified Amazon S3 bucket. The file path contains the organization ID as a prefix.

 If you do not enable organization-level CloudTrails, AWS Control Tower will not manage your AWS CloudTrail logs. You can change this setting when you update your landing zone.

AWS Control Tower strongly recommends that every organization or account establish AWS CloudTrail logging. You can create a custom trail that is not managed by AWS Control Tower, or you can select Enabled. A mandatory detective control detects whether enrolled accounts have enabled CloudTrail logging [Learn more about AWS CloudTrail](#)

☒ Enabled

☐ Not enabled

#### Log configuration for Amazon S3 - optional [Info](#)

In these two fields, enter numbers that represent lifecycle retention times for the Amazon S3 logging bucket and the access logging bucket.

Amazon S3 bucket retention for logging

Format for logging

years ▼

Years must be expressed as integers from 1 to 15, with values up to 2 decimal places. Durations less than 1 year are expressed as days.

Amazon S3 bucket retention for access logging

Format for access logging

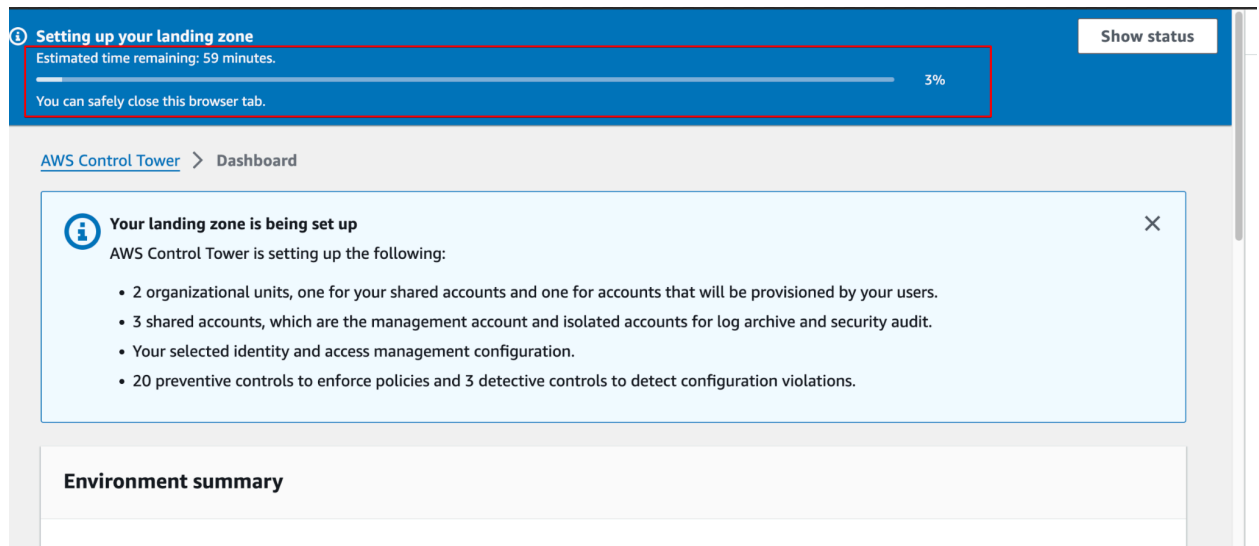
years ▼

Years must be expressed as integers from 1 to 15, with values up to 2 decimal places. Durations less than 1 year are expressed as days.

- Review the Control Tower configuration  
Expand **Learn more about permissions** under **Service permissions** to review the roles used to launch the AWS Control Tower service.
- Check “ **I understand the permissions AWS Control Tower will use to administer AWS resources and enforce rules on my behalf**”.

click on **Set up Landing Zone**".

10. You will be redirected to the **AWS Control Tower Dashboard**. The launch progress is shown in the blue bar on top of the Dashboard.




11. In a few minutes, you will receive an email with subject **Invitation to join AWS IAM Identity Center** to the master account email address. Make sure to open the email and click on **Accept invitation**.
12. The email you received also contains a User **portal URL**. Book mark this link as we will use it for handson.
13. On selecting **Accept Invitation**, you will be redirected to the **AWS Identity Center** page and from where you set **New Password** to your master account. Repeat Password and Update User to proceed.
14. Wait for the blue progress bar with **% complete** to disappear on top of the AWS Control Tower dashboard. **Note:** It is normal to see the progress staying at 99% for 15-20 minutes


Once all steps are completed, you should see the below screen when you connect to the User portal URL.

Single Sign-OnMFA devices | Sign out


Search




AWS Account (3)

**Audit**

#107463430110 | controltowerchild2@gmail.com


**ControlTowerMaster**

#322518508435 | controltowermaster1@gmail.com

**Log Archive**

#281445011069 | controltowerchild1@gmail.com

[Terms of Use](#)

Powered by 

You are all set!!

