# Structure of an AWS Control Tower Landing Zone

The structure of a landing zone in AWS Control Tower is as follows:

* **Root** – The parent that contains all other OUs in your landing zone.
* **Security OU** – This OU contains the Log Archive and Audit accounts. These accounts often are referred to as *shared accounts*. You can choose customized names for these shared accounts when you launch your landing zone. However, they cannot be renamed later.
* **Sandbox OU** – The Sandbox OU is created when you launch your landing zone, if you enable it. This and other registered OUs contain the enrolled accounts that your users work with to perform their AWS workloads.
* **AWS SSO directory** – This directory houses your AWS SSO users. It defines the scope of permissions for each AWS SSO user.
* **AWS SSO users** – These are the identities that your users can assume to perform their AWS workloads in your landing zone.

# What happens when you set up a landing zone

When you set up a landing zone, AWS Control Tower performs the following actions in your management account on your behalf:

* Creates three Organizations organizational units (OUs): Root, Security, and Sandbox (optional).
* Creates two shared accounts in the Security OU: the Log Archive account and the Audit account.
* Creates a cloud-native directory in AWS SSO, with preconfigured groups and single sign-on access.
* Applies 20 preventive guardrails to enforce policies.
* Applies six detective guardrails to detect configuration violations.
* Preventive guardrails are not applied to the management account.
* Except for the management account, guardrails are applied to the organization as a whole.

**Safely Managing Resources Within Your AWS Control Tower Landing Zone and Accounts**

* When you create your landing zone, a number of AWS resources are created. To use AWS Control Tower, you must not modify or delete these AWS Control Tower managed resources outside of the supported methods described in this guide. Deleting or modifying these resources will cause your landing zone to enter an unknown state. For details, see [Guidance for Creating and Modifying AWS Control Tower Resources](https://docs.aws.amazon.com/controltower/latest/userguide/best-practices.html#getting-started-guidance)
* When you enable guardrails with *strongly recommended* guidance, AWS Control Tower creates AWS resources that it manages in your accounts. Do not modify or delete resources created by AWS Control Tower. Doing so can result in the guardrails entering an unknown state. For more information, see [Guardrail Reference](https://docs.aws.amazon.com/controltower/latest/userguide/guardrails-reference.html).

When you set up your landing zone, the following AWS resources are created within your management account.

<https://docs.aws.amazon.com/controltower/latest/userguide/how-control-tower-works.html>

# What Are the Shared Accounts?

In AWS Control Tower, three shared accounts in your landing zone are provisioned automatically during setup: the management account, the log archive account, and the audit account.

**What is the management account?**

This is the account that you created specifically for your landing zone. This account is used for billing for everything in your landing zone. It's also used for Account Factory provisioning of accounts, as well as to manage OUs and guardrails.

**Note**: It is not recommended to run any type of production workloads from an AWS Control Tower management account. Create a separate AWS Control Tower account to run your workloads.

**What is the audit account?**

The audit account is a restricted account that's designed to give your security and compliance teams read and write access to all accounts in your landing zone. From the audit account, you have programmatic access to review accounts, by means of a role that is granted to Lambda functions only. The audit account does not allow you to log in to other accounts manually. For more information about Lambda functions and roles, see [Configure a Lambda function to assume a role from another AWS account](https://aws.amazon.com/premiumsupport/knowledge-center/lambda-function-assume-iam-role).

**What is the log archive account?**

This account works as a repository for logs of API activities and resource configurations from all accounts in the landing zone.

# Programmatic roles and trust relationships for the AWS Control Tower audit account

You can log into the audit account to review other accounts programmatically. The audit account does not allow you to log in to other accounts manually.

The audit account gives you programmatic access to other accounts, by means of some roles that are granted to AWS Lambda functions only. For security purposes, these roles have *trust relationships* with other roles, which means that the conditions under which the roles can be utilized are strictly defined.

The AWS Control Tower stack set StackSet-AWSControlTowerBP-BASELINE-ROLES creates these programmatic-only, cross-account roles in the audit account:

* **aws-controltower-AdministratorExecutionRole**
* **aws-controltower-AuditAdministratorRole**
* **aws-controltower-ReadOnlyExecutionRole**
* **aws-controltower-AuditReadOnlyRole**

ReadOnlyExecutionRole: Note that this role allows the audit account to read objects in S3 buckets across the entire organization (in contrast to the SecurityAudit policy, which allows for metadata access only).

**aws-controltower-AdministratorExecutionRole:**

* Has administrator permissions
* Cannot be assumed from the console
* Can be assumed only by a role in the audit account – the aws-controltower-AuditAdministratorRole

**aws-controltower-AuditAdministratorRole:**

* Can be assumed by the AWS Lambda service only
* Has permission to perform read (Get) and write (Put) operations on S3 objects with names that start with the string **log**

**aws-controltower-ReadOnlyExecutionRole:**

* Cannot be assumed from the console
* Can be assumed only by another role in the audit account – the AuditReadOnlyRole

**aws-controltower-AuditReadOnlyRole:**

* Can be assumed by the AWS Lambda service only
* Has permission to perform read (Get) and write (Put) operations on S3 objects with names that start with the string **log**

# Getting started with AWS Control Tower

This getting started procedure is for AWS Control Tower central cloud administrators. Use this procedure when you're ready to set up your landing zone. From start to finish, it should take about half an hour. This procedure has a prerequisite and four steps.

## Prerequisite: Automated pre-launch checks for your management account

Before AWS Control Tower sets up the landing zone, it automatically runs a series of pre-launch checks in your account. There's no action required on your part for these checks, which ensure that your management account is ready for the changes that establish your landing zone. Here are the checks that AWS Control Tower runs before setting up a landing zone:

* The existing service limits for the AWS account must be sufficient for AWS Control Tower to launch. For more information, see [Limitations and quotas in AWS Control Tower](https://docs.aws.amazon.com/controltower/latest/userguide/limits.html).
* The AWS account must be subscribed to the following AWS services:
  + Amazon Simple Storage Service (Amazon S3)
  + Amazon Elastic Compute Cloud (Amazon EC2)
  + Amazon SNS
  + Amazon Virtual Private Cloud (Amazon VPC)
  + AWS CloudFormation
  + AWS CloudTrail
  + Amazon CloudWatch
  + AWS Config
  + AWS Identity and Access Management (IAM)
  + AWS Lambda

**Considerations for AWS Single Sign-On (SSO) customers**

* If AWS Single Sign-On (AWS SSO) is already set up, the AWS Control Tower home Region must be the same as the AWS SSO Region.
* AWS Control Tower does not manage the SSO directory if SSO has been set up with an external identity provider.
* AWS SSO can be installed only in the management account of an organization.

**Considerations for AWS Config and AWS CloudTrail customers**

* The AWS account cannot have trusted access enabled in the organization management account for either AWS Config or AWS CloudTrail.
* If you have an existing AWS Config Recorder, delivery channel or aggregation setup, you must remove these configurations so that AWS Control Tower can configure AWS Config on your behalf during landing zone launch. If you used AWS CloudFormation to create these AWS Config resources, ensure that you also use CloudFormation to remove the resources.
* If you are running ephemeral workloads from accounts in AWS Control Tower, you will see an increase in costs associated with AWS Config. Contact your AWS account representative for more specific information about managing these costs.
* When you enroll an account into AWS Control Tower, your account is governed by the AWS CloudTrail trail for the AWS Control Tower organization. If you have an existing deployment of a CloudTrail trail, you may see duplicate charges unless you delete the existing trail for the account before you enroll it in AWS Control Tower.

## Requirements for your shared account email addresses

If you're setting up your landing zone in a new AWS account, for information on creating your account and your IAM administrator, see [Setting up](https://docs.aws.amazon.com/controltower/latest/userguide/setting-up.html).

To set up your landing zone, AWS Control Tower requires two unique email addresses that aren't already associated with an AWS account. Each of these email addresses will serve as a collaborative inbox -- a shared email account -- intended for the various users in your enterprise that will do specific work related to AWS Control Tower. The email addresses are required for:

* **Audit account** – This account is for your team of users that need access to the audit information made available by AWS Control Tower. You can also use this account as the access point for third-party tools that will perform programmatic auditing of your environment to help you audit for compliance purposes.
* **Log archive account** – This account is for your team of users that need access to all the logging information for all of your enrolled accounts within registered OUs in your landing zone.

These accounts are created in the **Security** OU when you create your landing zone. As a best practice, we recommend that when you need to perform some action in these accounts, you should use an AWS SSO user with the appropriately scoped permissions.

For the sake of clarity, this User Guide always refers to the shared accounts by their default names: **log archive** and **audit**. As you read this document, remember to substitute the customized names you give to these accounts initially, if you choose to customize them. You can view your accounts with their customized names on the **Account details** page.

**Note**

We are changing our terminology regarding the default names of some AWS Control Tower organizational units (OUs) to align with the AWS multi-account strategy. You may notice some inconsistencies while we are making a transition to improve the clarity of these names. The Security OU was formerly called the Core OU. The Sandbox OU was formerly called the Custom OU.

### Expectations for landing zone configuration

The process of setting up your AWS Control Tower landing zone has multiple steps. Certain aspects of your AWS Control Tower landing zone are configurable. Other choices are "one-way doors" that cannot be changed after setup.

**Key items to configure during setup**

* You can select your top-level OU names during setup, and you also can change OU names after you've set up your landing zone. By default, the top-level OUs are named **Security** and **Sandbox**. For more information, see [Guidelines to set up a well-architected environment](https://docs.aws.amazon.com/controltower/latest/userguide/aws-multi-account-landing-zone.html#guidelines-for-multi-account-setup).
* During setup, you can select customized names for your shared accounts, called **log archive** and **audit** by default, but you cannot change these names after setup. (This is a one-time selection.)

**Configuration choices that cannot be undone**

* You cannot change your home Region after you've set up your landing zone.
* After you select any Region for governance by AWS Control Tower, you cannot unselect the Region to remove it from governance.
* If you're provisioning Account Factory accounts with VPCs, VPC CIDRs can't be changed after they are created.

## Configure and launch your landing zone

Before you launch your AWS Control Tower landing zone, determine the most appropriate home Region. For more information, see [Administrative Tips for Landing Zone Setup](https://docs.aws.amazon.com/controltower/latest/userguide/best-practices.html#tips-for-admin-setup).

**Important**

Changing your home Region after you have deployed your AWS Control Tower landing zone requires the assistance of AWS Support. This practice is not recommended.

AWS Control Tower has no APIs or programmatic access. To configure and launch your landing zone, perform the following series of steps.

**Prepare: Navigate to the AWS Control Tower console**

1. Open a web browser, and navigate to the AWS Control Tower console at <https://console.aws.amazon.com/controltower>.
2. In the console, verify that you are working in your desired home Region for AWS Control Tower. Then choose **Set up your landing zone**.

**Step 1. Review pricing and select your AWS Regions.**

Be sure you've correctly designated the AWS Region that you select for your home Region. After you've deployed AWS Control Tower, you can't change the home Region.

In this section of the setup process, you can add any additional AWS Regions that you require. You can add more Regions at a later time, if needed. After you add a Region into governance by AWS Control Tower, you cannot remove it from governance.

**To select additional AWS Regions to govern**

* The panel shows you the current Region selections. Open the dropdown menu to see a list of additional Regions available for governance. Check the box next to each Region to bring into governance by AWS Control Tower. Your home Region selection is not editable.

**Step 2. Configure your organizational units (OUs).**

If you accept the default names of these OUs, there's no action you need to take for setup to continue. To change the names of the OUs, enter the new names directly in the form field.

* **Foundational OU** – AWS Control Tower relies upon a **Foundational OU** that is initially named the **Security OU**. You can change the name of this OU during initial setup and afterward, from the OU details page. This **Security OU** contains your two shared accounts, which by default are called the **log archive** account and the **audit** account.
* **Additional OU** – AWS Control Tower can set up one or more **Additional OUs** for you. We recommend that you provision at least one **Additional OU** in your landing zone, besides the **Security OU**. If this Additional OU is intended for development projects, we recommend that you name it the **Sandbox OU**, as given in the [Guidelines to set up a well-architected environment](https://docs.aws.amazon.com/controltower/latest/userguide/aws-multi-account-landing-zone.html#guidelines-for-multi-account-setup). If you already have an existing OU in AWS Organizations, you may see the option to skip setting up an Additional OU in AWS Control Tower.

**Step 3. Configure your shared accounts.**

In this section of the setup process, the panel shows the default selections for the names of your shared AWS Control Tower accounts. These accounts are an essential part of your landing zone. **Do not move or delete these shared accounts**, although you can choose customized names for them during setup.

You must provide unique email addresses for your log archive and audit accounts, and you can verify the email address that you previously provided for your management account. Choose the **Edit** button to change the editable default values.

**About the shared acccounts**

* **The management account** – The AWS Control Tower management account is part of the Root level. The management account allows for AWS Control Tower billing. The account also has administrator permissions for your landing zone. You cannot create separate accounts for billing and for administrator permissions in AWS Control Tower.

The email address shown for the management account is not editable during this phaase of setup. It is shown as a confirmation, so you can check that you're editing the correct management account, in case you have multiple accounts.

* **The two shared accounts** – You can choose customized names for these two accounts, and you must supply a unique email address for each account. Remember that the email addresses must not already have associated AWS accounts.

**To configure the shared accounts, fill in the requested information.**

1. At the console, select a name for the account initially called the **log archive** account. Many customers decide to keep the default name for this account.
2. Provide a unique email address for this account.
3. Select a name for the account initially called the **audit** account. Many customers choose to call it the **Security** account.
4. Provide a unique email address for this account.

**Step 4. Review and set up the landing zone**

The next section in the setup shows you the permissions that AWS Control Tower requires for your landing zone. Choose a checkbox to expand each topic. You'll be asked to agree to these permissions, which may affect multiple accounts, and to agree to the overall **Terms of Service**.

**To finalize**

1. At the console, review the **Service permissions**, and when you're ready, choose **I understand the permissions AWS Control Tower will use to administer AWS resources and enforce rules on my behalf**.
2. To finalize your selections and initialize launch, choose **Set up landing zone**.

This series of steps starts the process of setting up your landing zone, which can take about thirty minutes to complete. During setup, AWS Control Tower creates your Root level, the Security OU, and the shared accounts. Other AWS resources are created, modified, or deleted.

**Important**

The email address you provided for the audit account will receive **AWS Notification - Subscription Confirmation** emails from every AWS Region supported by AWS Control Tower. To receive compliance emails in your audit account, you must choose the **Confirm subscription** link within each email from each AWS Region supported by AWS Control Tower.

## Next steps

Now that your landing zone is set up, it's ready for use.

To learn more about how you can use AWS Control Tower, see the following topics:

* For recommended administrative practices, see [Best Practices](https://docs.aws.amazon.com/controltower/latest/userguide/best-practices.html).
* You can set up AWS SSO users and groups with specific roles and permissions. For recommendations, see [Recommendations for Setting Up Groups, Roles, and Policies](https://docs.aws.amazon.com/controltower/latest/userguide/best-practices.html#roles-recommendations).
* To begin enrolling organizations and accounts from your AWS Organizations deployments, see [Govern existing organizations and accounts](https://docs.aws.amazon.com/controltower/latest/userguide/importing-existing.html).
* Your end users can provision their own AWS accounts in your landing zone using Account Factory. For more information, see [Permissions for Configuring and Provisioning Accounts](https://docs.aws.amazon.com/controltower/latest/userguide/account-factory.html#configure-provision-new-account).
* To assure [Compliance Validation for AWS Control Tower](https://docs.aws.amazon.com/controltower/latest/userguide/compliance-program-info.html), your central cloud administrators can review log archives in the Log Archive account, and designated third-party auditors can review audit information in the Audit (shared) account, which is a member of the Security OU.
* To learn more about the capabilities of AWS Control Tower, see [Related information](https://docs.aws.amazon.com/controltower/latest/userguide/related-information.html).
* From time to time, you may need to update your landing zone to get the latest backend updates, the latest guardrails, and to keep your landing zone up-to-date. For more information, see [Configuration update management in AWS Control Tower](https://docs.aws.amazon.com/controltower/latest/userguide/configuration-updates.html).
* If you encounter issues while using AWS Control Tower, see [Troubleshooting](https://docs.aws.amazon.com/controltower/latest/userguide/troubleshooting.html).

# Limitations and quotas in AWS Control Tower

This chapter covers the AWS service limitations and quotas that you should keep in mind as you use AWS Control Tower. If you're unable to set up your landing zone due to a service quota issue, contact [AWS Support](https://aws.amazon.com/premiumsupport/).

## Limitations in AWS Control Tower

This section describes known limitations and unsupported use cases in AWS Control Tower.

* Nested OUs are not displayed in the AWS Control Tower console.
* Creation of nested OUs from the AWS Control Tower console is not supported.
* Email addresses of shared accounts in the Security OU can be changed, but you must update your landing zone to see these changes in the AWS Control Tower console.
* A limit of 5 SCPs per OU applies to OUs in your AWS Control Tower landing zone.
* Existing OUs with over 300 accounts cannot be registered or re-registered in AWS Control Tower.

## Quotas for Integrated Services

Each AWS service has its own quotas and limits. You can find the quotas for each service in its documentation. For more information, see the related links:

* **AWS CloudFormation** – [AWS CloudFormation Quotas](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cloudformation-limits.html)
* **AWS CloudTrail** – [Quotas in AWS CloudTrail](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/WhatIsCloudTrail-Limits.html)
* **Amazon CloudWatch** – [CloudWatch Quotas](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch_limits.html)
* **AWS Config** – [AWS Config Quotas](https://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html#limits_config)
* **AWS Identity and Access Management** – [Quotas for IAM Entities and Objects](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_iam-limits.html)
* **AWS Lambda** – [AWS Lambda Quotas](https://docs.aws.amazon.com/lambda/latest/dg/limits.html)
* **AWS Organizations** – [Quotas for AWS Organizations](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_reference_limits.html)
* **Amazon Simple Storage Service** – [Bucket Restrictions and Quotas](https://docs.aws.amazon.com/AmazonS3/latest/dev/BucketRestrictions.html)
* **AWS Service Catalog** – [AWS Service Catalog Default Service Quotas](https://docs.aws.amazon.com/servicecatalog/latest/adminguide/limits.html)
* **AWS Single Sign-On** – [Quotas in AWS SSO](https://docs.aws.amazon.com/singlesignon/latest/userguide/limits.html)
* **Amazon Simple Notification Service** – [Amazon Simple Notification Service (Amazon SNS) Quotas](https://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html#limits_sns)
* **AWS Step Functions** – [Quotas](https://docs.aws.amazon.com/step-functions/latest/dg/limits.html)

## Administrative Tips for Landing Zone Maintenance

* You can make your own log buckets in the log archive account, but it is not recommended. Be sure to leave the buckets created by AWS Control Tower. Note that your Amazon S3 access logs must be in the same AWS Region as the source buckets. For buckets you create, you do not have access to use s3:PutEncryptionConfiguration, s3:PutBucketLogging, or s3:PutBucketPolicy on those buckets because of restrictions created by mandatory guardrails.
* By keeping your workloads and logs in the same AWS Region, you reduce the cost that would be associated with moving and retrieving log information across regions.
* The VPC created by AWS Control Tower is limited to the AWS Regions in which AWS Control Tower is available. Some customers whose workloads run in non-supported regions may want to disable the VPC that is created with your Account Factory account. They may prefer to create a new VPC using the AWS Service Catalog portfolio, or to create a custom VPC that runs in only the required Regions.
* The VPC created by AWS Control Tower is not the same as the default VPC that is created for all AWS accounts. In regions where AWS Control Tower is supported, AWS Control Tower deletes the default AWS VPC when it creates the AWS Control Tower VPC.
* If you delete your default VPC in your home AWS Region, it's best to delete it in all other AWS Regions.

## Sign in as a Root User

Certain administrative tasks require that you must sign in as a root user. You can sign in as a root user to an AWS account that was created by account factory in AWS Control Tower.

**You must sign in as a root user to perform the following actions:**

* Change certain account settings, including the account name, root user password, or email address. For more information, see [Updating and Moving Account Factory Accounts with AWS Service Catalog](https://docs.aws.amazon.com/controltower/latest/userguide/account-factory.html#updating-account-factory-accounts).
* To change or enable your [AWS Support plan](https://docs.aws.amazon.com/controltower/latest/userguide/troubleshooting.html#getting-support).
* To [close an AWS Account](https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/close-account.html).
* For more information about actions that require root login credentials, please see [AWS Tasks that Require AWS Root Login Credentials](https://docs.aws.amazon.com/general/latest/gr/aws_tasks-that-require-root.html).

## Recommendations for Setting Up Groups, Roles, and Policies

As you set up your landing zone, it's a good idea to decide ahead of time which users will require access to certain accounts and why. For example, a security account should be accessible only to the security team, the management account should be accessible only to the cloud administrators' team, and so forth.

**Recommended Restrictions**

You can restrict the scope of administrative access to your organizations by setting up an IAM role or policy that allows administrators to manage AWS Control Tower actions only. The recommended approach is to use the IAM Policy arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy. With the AWSControlTowerServiceRolePolicy role enabled, an administrator can manage AWS Control Tower only. Be sure to include appropriate access to AWS Organizations for managing your preventive guardrails, and SCPs, and access to AWS Config, for managing detective guardrails, in each account.

When you're setting up the shared audit account in your landing zone, we recommend that you assign the AWSSecurityAuditors group to any third-party auditors of your accounts. This group gives its members read-only permission. An account must not have write permissions on the environment that it is auditing, because it can violate compliance with Separation of Duty requirements for auditors.

## Guidance for Creating and Modifying AWS Control Tower Resources

We recommend the following practices as you create and modify resources in AWS Control Tower. This guidance might change as the service is updated.

**General Guidance**

* Do not modify or delete resources created by AWS Control Tower in the management account or in the shared accounts. Modification of these resources can require an update to your landing zone.
* Do not modify or delete the AWS Identity and Access Management (IAM) roles created within the shared accounts in the Security organizational unit (OU). Modification of these roles can require an update to your landing zone.
* For more information about the resources created by AWS Control Tower, see [What Are the Shared Accounts?](https://docs.aws.amazon.com/controltower/latest/userguide/how-control-tower-works.html#what-shared)
* Do not disallow usage of any AWS Regions through either SCPs or AWS STS. Doing so will break AWS Control Tower.
* In general, AWS Control Tower performs a single action at a time, which must be completed before another action can begin. For example, if you attempt to provision an account while the process of enabling a guardrail is already in operation, account provisioning will fail.

**AWS Organizations Guidance**

* Do not use AWS Organizations to update service control policies (SCPs) attached to an OU that is registered with AWS Control Tower. Doing so could result in the guardrails entering an unknown state, which will require you to re-enable affected guardrails in AWS Control Tower. Instead, you can create new SCPs and attach those to the OUs rather than editing the SCPs that AWS Control Tower has created.
* Moving individual accounts into AWS Control Tower, from outside of a registered OU, causes drift that must be repaired. See [Types of Governance Drift](https://docs.aws.amazon.com/controltower/latest/userguide/drift.html" \l "governance-drift).
* If you use AWS Organizations to create, invite, or move accounts within an organization registered with AWS Control Tower, those accounts are not enrolled by AWS Control Tower and those changes are not recorded. If you need access to these accounts through SSO, see [Member Account Access](http://aws.amazon.com/premiumsupport/knowledge-center/organizations-member-account-access/).
* If you use AWS Organizations to move an OU into an organization created by AWS Control Tower, the external OU is not registered by AWS Control Tower.
* Nested OUs are not accessible in AWS Control Tower, because AWS Control Tower displays only the top-level OUs.
* If you use AWS Organizations to rename an account or OU that was created by AWS Control Tower, you must repair your landing zone so that the new name is displayed by AWS Control Tower.
* If you use AWS Organizations to delete an OU that was created by AWS Control Tower, you also must delete the OU in AWS Control Tower. It cannot be used to contain accounts. You will not be able to provision a new account to this OU using Account Factory