

Control Center Operation Guide



Tencent Cloud

Copyright Notice

©2013–2023 Tencent Cloud. All rights reserved.

The complete copyright of this document, including all text, data, images, and other content, is solely and exclusively owned by Tencent Cloud Computing (Beijing) Co., Ltd. ("Tencent Cloud"); Without prior explicit written permission from Tencent Cloud, no entity shall reproduce, modify, use, plagiarize, or disseminate the entire or partial content of this document in any form. Such actions constitute an infringement of Tencent Cloud's copyright, and Tencent Cloud will take legal measures to pursue liability under the applicable laws.

Trademark Notice



This trademark and its related service trademarks are owned by Tencent Cloud Computing (Beijing) Co., Ltd. and its affiliated companies ("Tencent Cloud"). The trademarks of third parties mentioned in this document are the property of their respective owners under the applicable laws. Without the written permission of Tencent Cloud and the relevant trademark rights owners, no entity shall use, reproduce, modify, disseminate, or copy the trademarks as mentioned above in any way. Any such actions will constitute an infringement of Tencent Cloud's and the relevant owners' trademark rights, and Tencent Cloud will take legal measures to pursue liability under the applicable laws.

Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

Operation Guide

Landing Zone

- Viewing a Landing Zone
- Managing Departments
- Managing Core Accounts
- Configuring Financial Policies
- Managing Security Rules
- Managing Permissions
- Managing CloudAudit Log Shipping
- Managing Config Log Shipping
- Inviting Existing Accounts

Control Center Overview

Baselines

- Viewing Baselines
- Adding Baselines
- Configuring Baselines
 - Configuring a Contact Baseline
 - Configuring a CAM Password Policy Baseline
- Applying Baselines
- Deleting Baselines

Accounts

- Viewing Accounts
- Adding Accounts
- Inviting Accounts

Login Permissions

- Creating Permissions

Finance

- Viewing the Financial Structure
- Viewing Billing Overview

Security Rules

- Viewing Security Rules
- Managing Security Rules

Compliance Audit

Cloud Security Center

Operation Guide

Landing Zone

Viewing a Landing Zone

Last updated: 2023-08-15 16:52:04

Overview

In Tencent Cloud Control Center, a landing zone provides a top-level framework for enterprise cloud migration. It enables enterprises to rapidly establish a cloud environment aligned with best practices. If you haven't set up a landing zone, you can refer to the document for landing zone configuration. This document describes the resulting page after a landing zone is set up.

Prerequisites

You have logged in to the Tencent Cloud console and set up a landing zone.

Directions

Viewing existing configurations

In the Tencent Cloud console, go to the **Control Center** > [Landing zone](#) page. The configurations that have been set up are displayed on the left side of the page. You can click a configuration to view its setup history in detail.

The screenshot shows the 'Landing zone' page in the Tencent Cloud console. The page has a header with 'Landing zone' on the left, a 'Continue setup' button, and a 'Documentation' link. The main content area is divided into two columns. The left column, titled 'Configurations', is highlighted with a red border and contains three sections: 'Manage units' with an 'Admin account' button, 'Manage core accounts' with an 'Admin account' button, and 'Configure financial policy' with an 'Admin account' button. The right column, titled 'Manage departments', contains a blue information bar with an 'i' icon and the text 'You can go to [Accounts](#) to manage departments and accounts.' Below this, there are two rows of department information: 'Core account department' with the value 'core', and 'Business account department' with the value 'application'.

Continuing landing zone setup

Click **Continue setup** in the top-right corner to complete the setup of the landing zone.

Landing zone [Continue setup](#) [Documentation](#)

Configurations

Manage units
[Admin account](#)

Manage core accounts
[Admin account](#)

Configure financial policy
[Admin account](#)

Manage departments

i You can go to [Accounts](#) to manage departments and accounts.

Core account department	core
Business account department	application

Managing Departments

Last updated: 2023-08-14 09:55:13

Overview

Departments are an essential configuration for resource management within an enterprise. You can create departments to enable proper resource allocation, permission management, compliance auditing, and more. This document describes how to configure the departments within a landing zone.

Prerequisites

You have logged in to the Tencent Cloud console and gone to the **Control Center** > [Landing zone](#) page.

Directions

Automatically creating departments

Control Center automatically creates departments for your core accounts and business accounts based on best practices.

- Core account department: This is where members with administrative roles are placed.
- Business account department: This is where members engaged in specific business operations are placed.

Selecting an existing department

If you have created departments and don't need to use automatically generated ones, you can click

Note:

- If you need to modify departments, go to **Control Center** > **Accounts**.
- The Accounts menu is displayed in the left sidebar after a landing zone is set up.

- 1 Add configuration >
- 2 Preview >
- 3 Deployment result

Configurations [Add configuration](#)

- ✓ **Manage units**
[Admin account](#)
- 🕒 **Manage core accounts**
[Admin account](#)
- 🕒 **Configure financial policy**
[Admin account](#)

Manage departments

Create a department for core accounts

You can use this department for core accounts such as the logging account and security account.

Department name [Select department](#)

Create a department for business accounts

You can use this department for business accounts.

Department name [Select department](#)

- [Next: Preview](#)
- [Save draft](#)

Managing Core Accounts

Last updated: 2023-08-14 18:05:04

Overview

Core accounts are used to manage all log shipping and cloud security operations. You can either create new core accounts or select existing accounts as core accounts. This document describes how to configure core accounts in a landing zone.

Prerequisites

You have logged in to the Tencent Cloud console and gone to the **Control Center** > [Landing zone](#) page.

Directions

Creating a logging account

On the **Landing zone** page, select **Manage core accounts**. On the right side of the page, you can specify the detailed information for core accounts.

- Creation method:

Manage core accounts

Create logging account

A logging account ships and analyzes the logs of all accounts of the organization.

Join as

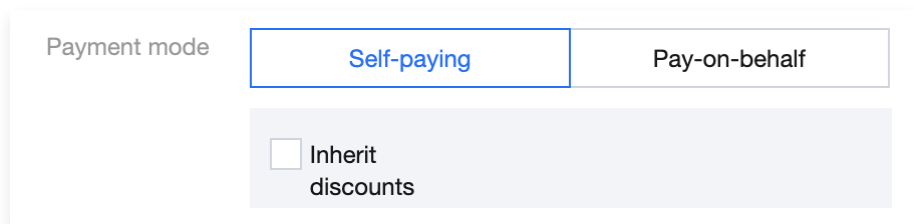
Account name

Payment mode

Inherit discounts

- Click **New account** and enter an account name. By default, the account name is **Logging account**.
- Click **Existing account** to select an existing account from the drop-down list as the **Logging account** for your department. The payment mode is inherited from the selected account.

- Payment mode:



Payment mode

Self-paying Pay-on-behalf

Inherit discounts

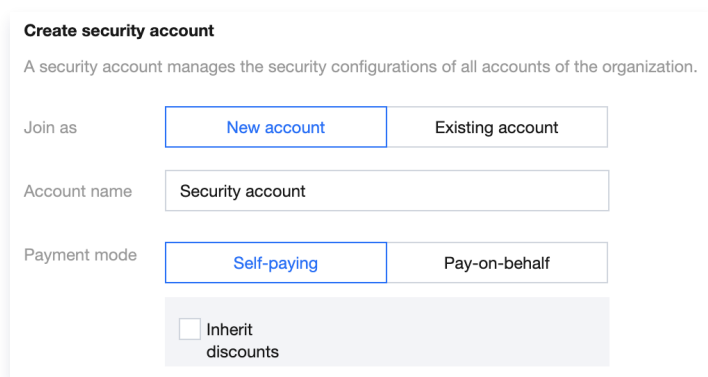
- Select **Self-paying** if you want to make the account responsible for its own payments. You can select **Inherit discounts** to let the account inherit contracted discounts from the admin account.
- Select **Pay-on-behalf** if you want to specify a corporate payer to make payments on the account's behalf.

Creating a security account

A security account enables unified management of security products, including the Cloud Security Center, within all accounts of your organization.

On the **Landing zone** page, select **Manage core accounts**. On the right side of the page, you can specify the detailed information for core accounts.

- **Creation method:**



Create security account

A security account manages the security configurations of all accounts of the organization.

Join as

New account Existing account

Account name

Security account

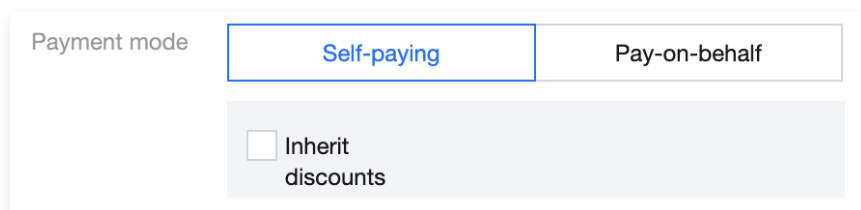
Payment mode

Self-paying Pay-on-behalf

Inherit discounts

- Click **New account** and enter an account name. By default, the account name is **Security account**.
- Click **Existing account** to select an existing account as the Security account from the drop-down list of your department. The payment mode is inherited from the selected account.

- **Payment mode:**



Payment mode

Self-paying Pay-on-behalf

Inherit discounts

- Select **Self-paying** if you want to make the account responsible for its own payments.

You can select Inherit discounts to inherit the contracted discounts from the admin account.

- Select **Pay-on-behalf** if you want to specify a corporate payer to make payments on the account's behalf.

Configuring Financial Policies

Last updated: 2023-08-14 18:05:39

Overview

Landing zones offer default financial policies and payment modes for accounts in Control Center. On the Landing zone page, you can view the financial policies and payment modes and manage other entities of the organization. This document describes how to configure enterprise financial policies in a landing zone.

Prerequisites

You have logged in to the Tencent Cloud console and gone to the **Control Center** > [Landing zone](#) page.

Directions

1. On the **Landing zone** page, select **Configure financial policy**.

← Landing zone
Documentation [🔗](#)

1 Add configuration >
 2 Preview >
 3 Deployment result

Configurations [Add configuration](#)

✔ Manage units

✔ Manage core accounts

✔ **Configure financial policy**

Configure financial policy

Configure financial policy

You can grant five financial permissions to an account.

Financial policy [View bills](#) [View balance](#) [Allocate funds](#) [Consolidated billing](#) [Invoice](#)

Configure payment mode

The admin account of the organization can pay on behalf of member accounts with the same enterprise identity and can configure discount inheritance for other entities of the organization. You can also create one admin account for each entity, which can pay on behalf of the entity's member accounts.

Current admin account

Entity

Entities of the organization

Entity	Payer account	Status	Operation
		● Configured	Configure Remove

Next: Preview
Save draft

- **Configure financial policy:** By default, five financial policies are supported. You can go to **Control Center > Finance** to modify these policies later.
- **Configure payment mode:** The organization admin account can pay on behalf of other accounts within the same entity as itself. It can also set other entities to inherit its discounts.
- **Entities of the organization:** The entities associated with the account are automatically displayed, including the current entity and other entities. To remove any other entities, click **Remove** in the **Operation** column.

! **Note:**

By default, the organization admin account pays on behalf of other accounts under its owner entity, and that entity cannot be modified or removed.

Managing Security Rules

Last updated: 2023-12-05 14:38:36

Overview

Control Center allows you to enable and manage security rules to ensure a more secure multi-account environment. This document describes how to configure security rules in a landing zone.

Prerequisites

You have logged in to the Tencent Cloud console and gone to the **Control Center** > [Landing zone](#) page.

Directions

1. On the **Landing zone** page, click **Add configuration**.

← Landing zone

1 Add configuration > 2 Preview > 3 Deployment result

Configurations [Add configuration](#)

✓ **Manage units**
Admin account

✓ **Manage core accounts**
Admin account

▼ **Completed (1)**

Configure financial policy
Admin account

Manage departments

Create a department for core accounts
You can use this department for core accounts such as the logging account and security account.

Department name [Select department](#)

Create a department for business accounts
You can use this department for business accounts.

Department name [Select department](#)

[Next: Preview](#) [Save draft](#)

2. In the pop-up window, select **Enable security rules** and click **Confirm**.

Add configuration ✕

Enable security rules

Configure multi-account security rules to evaluate the compliance of account resources.

Manage permissions

With the permission management capability, the enterprise administrator can log into with any account of the enterprise to view and manage resources.

Manage CloudAudit log shipping

Ship the operation logs of all the enterprise's accounts to a specified COS bucket to centrally manage and analyze logs and facilitate the operations of CloudAudit.

Manage Config log shipping

Ship the configuration logs of all the enterprise's accounts to a specified COS bucket so that changes made to resources can be viewed and managed easily.

Invite existing accounts

Invite existing accounts to the organization. An invitation will be sent to the invited account, which can join the organization after accepting the invitation.

3. In the **Enable security rules** list:

- Click **Enable** to enable a specific security rule. Then, the rule enters the **Enabled** state.
- Click **Disable** to disable a specific security rule. Secondary confirmation is required for disabling high-risk rules. Then, the rule enters the **Disabled** state.

Note:

Following best practices, Tencent Cloud classifies security rules into low-risk, medium-risk, and high-risk rules based on their risk level. You can enable security rules based on your needs.

← Landing zone Documentation

1 Add configuration > 2 Preview > 3 Deployment result

Configurations [Add configuration](#)

- Manage units
- Manage core accounts
- Enable security rules**
- Completed (1)

Enable security rules

Rule ID	Rule name	Description	Risk level	Status	Operation
cam-group-user-bound	Checks whether there are user group...	If a CAM user group exists at least one user, the ...	Low	Enabled	Disable
cam-user-policy-directly-bound	Checks whether there are policies dir...	If there are no authorized policies directly added ...	Low	Enabled	Disable
cam-user-risky-policy-bound	Checks whether specified high-risk p...	If no specified high-risk permission is authorized ...	Low	Enabled	Disable
cam-policy-in-use	Checks whether there are idle permis...	If each CAM policy is associated with at least on...	Low	Enabled	Disable
cam-user-login-check	Checks CAM user login permissions	If either the console login and access permission...	Low	Enabled	Disable
cam-user-ak-rotated	Checks whether the CAM user's key ...	If a user's key changes within a specified period ...	High	Enabled	Disable
cam-user-logged-in	Checks whether there are login activiti...	If CAM users have login activities during a specifi...	Medium	Enabled	Disable
cam-policy-admin-access-bound	Checks whether there are super admini...	If there are no super admin permissions (Adminis...	Low	Enabled	Disable
cam-account-login-mfa-enabled	Checks whether login protection MFA...	If login protection MFA is enabled in CAM, the ev...	High	Enabled	Disable
cam-account-action-mfa-enabled	Checks whether sensitive operation ...	If sensitive operation MFA is enabled in CAM, the...	High	Enabled	Disable
cam-user-group-bound	Checks whether a CAM sub-user is a...	If a CAM user is associated with at least one use...	Low	Enabled	Disable

- **High:** These are essential security rules and are enabled by default. Disabling them requires secondary confirmation.
- **Medium:** These are compliance rules and are enabled by default. You can disable them as needed.
- **Low:** These rules are optional and are enabled by default. You can disable them as needed.

4. Click **Next: Preview**. After confirming that the configured rules are correct, click **Apply**.

5. After the rules are applied, you can go to **Control Center > Security rules** and click **Manage security rules** to complete rule configuration under **Tencent Cloud Config**.

Security rules

Overview

Total rules 66

Violated rules 54

[Manage security rules](#)

Rule name



Rule name	Risk level	Status	Evaluation result	Creation time
Checks whether the CAM user's key changes wit...	High	Enabled	Compliant	2023-11-21 11:45:01
Checks whether the CAM user's key changes wit...	High	Enabled	Compliant	2023-11-21 11:45:31
Checks whether the CAM user's key changes wit...	High	Enabled	Compliant	2023-11-21 11:55:49
Checks whether the CAM user's key changes wit...	High	Enabled	Compliant	2023-11-22 10:44:41
Checks whether the CAM user's key changes wit...	High	Enabled	Compliant	2023-11-24 15:11:50
Checks whether the CAM user's key changes wit...	High	Enabled	Compliant	2023-11-24 17:37:31
Checks whether there are idle permission policies...	Low	Enabled	Non-compliant	2023-11-21 11:44:59
Checks whether there are idle permission policies...	Low	Enabled	Non-compliant	2023-11-21 11:45:29
Checks whether there are idle permission policies...	Low	Enabled	Non-compliant	2023-11-21 11:55:47
Checks whether there are idle permission policies...	Low	Enabled	Non-compliant	2023-11-22 10:44:39

Total items: 66

10 / page

⏪
⏩
4
/ 7 pages
⏪
⏩

Managing Permissions

Last updated: 2023-08-15 14:23:56

Overview

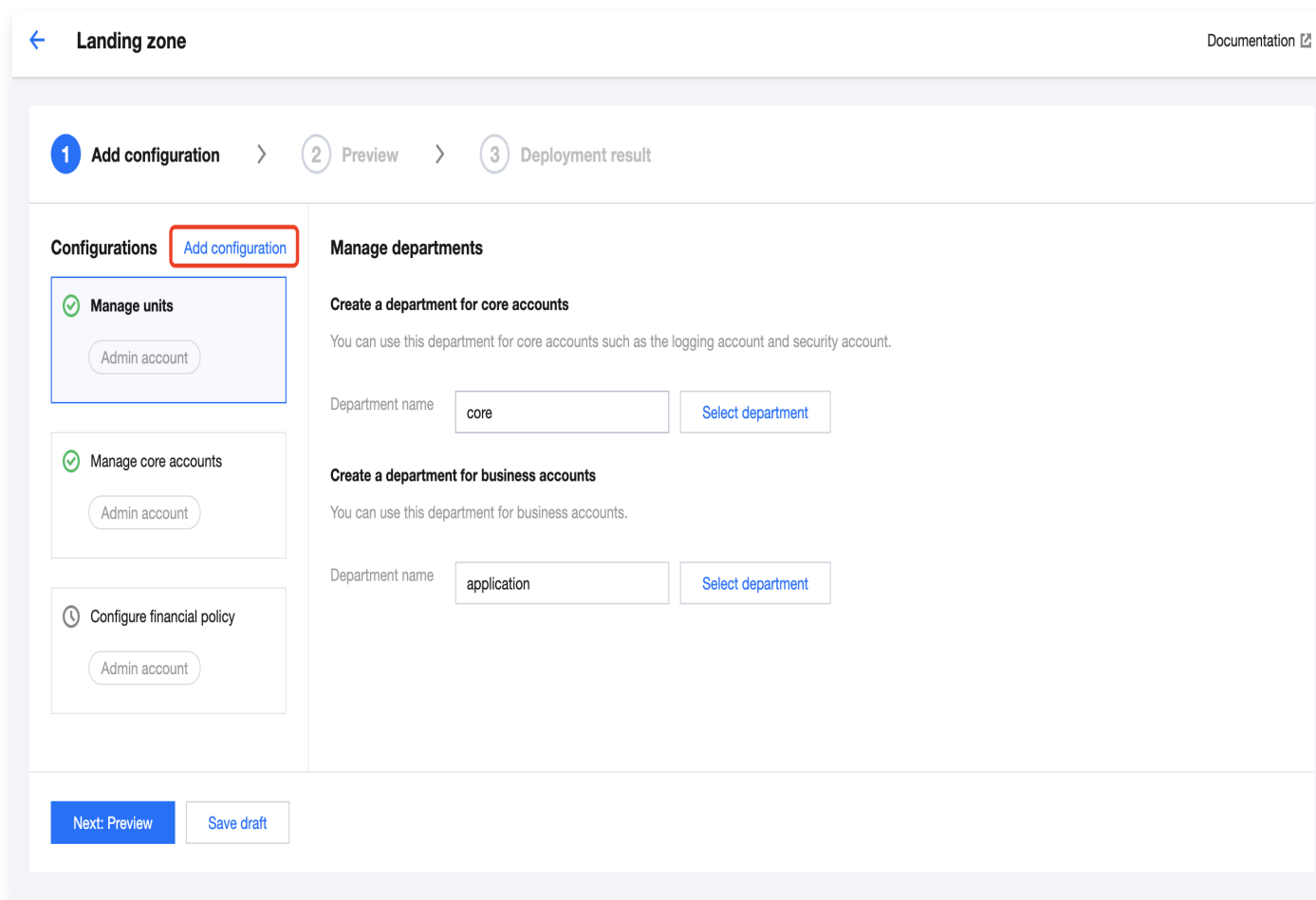
Through permissions management, enterprise administrators can easily log in to and manage resources in any account within the organization. This document describes how to configure permissions management in a landing zone.

Prerequisites

You have logged in to the Tencent Cloud console and gone to the **Control Center** > **Landing zone** page.

Directions

1. On the **Landing zone** page, click **Add configuration**.



2. In the **Add configuration** pop-up window, select **Manage permissions** and click **Confirm**.

Add configuration ✕

Manage permissions

With the permission management capability, the enterprise administrator can log into with any account of the enterprise to view and manage resources.

Manage CloudAudit log shipping

Ship the operation logs of all the enterprise's accounts to a specified COS bucket to centrally manage and analyze logs and facilitate the operations of CloudAudit.

Manage Config log shipping

Ship the configuration logs of all the enterprise's accounts to a specified COS bucket so that changes made to resources can be viewed and managed easily.

Invite existing accounts

Invite existing accounts to the organization. An invitation will be sent to the invited account, which can join the organization after accepting the invitation.

3. On the **Manage permissions** page that appears, all permissions associated with the account are displayed. A search box is provided for fuzzy search of permissions.

← Landing zone Documentation

1 Add configuration > 2 Preview > 3 Deployment result

Configurations [Add configuration](#)

- Manage units [Admin account](#)
- Manage core accounts [Admin account](#)
- Configure financial policy [Admin account](#)
- Manage permissions** [Admin account](#)

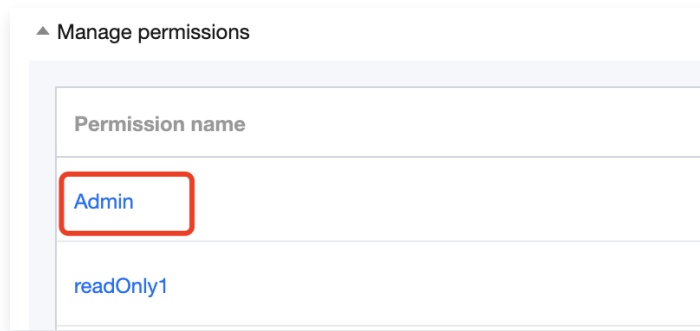
Manage permissions

Configure identities and permissions for member accounts.

Permission name	Note	Type
test001	test	Default

Total items: 1 10 / page 1 / 1 page

4. Click **Next: Preview** to go to the preview page.
5. When you click a specific **permission name**, you will be redirected to the **Unified member access** page where you can view detailed information about that permission.



6. After confirming that the preview is correct, click **Apply**.

Managing CloudAudit Log Shipping

Last updated: 2023-08-15 14:27:15

Overview

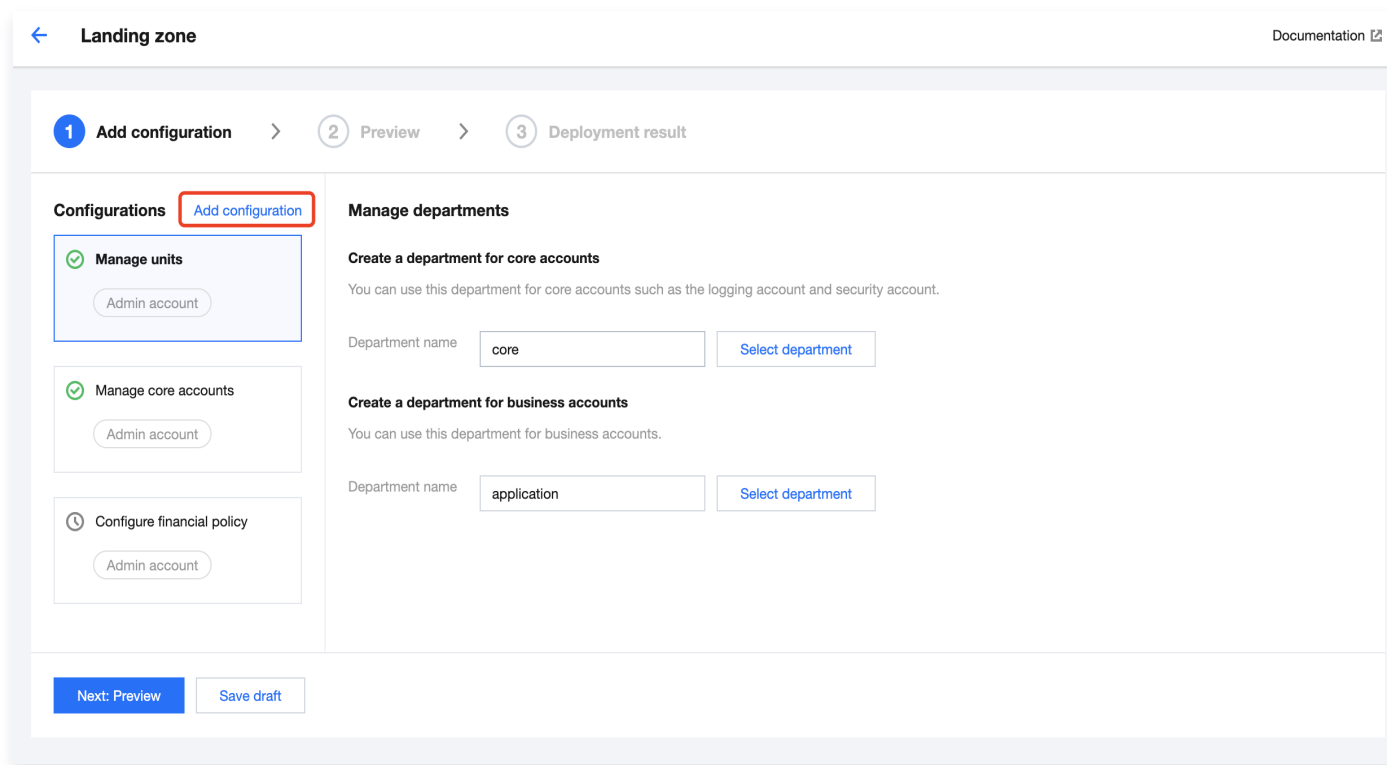
You can set to ship the operation logs of all accounts within the organization to a designated Cloud Object Storage (COS) bucket. This facilitates centralized management and analysis of logs and audit of account operations. This document describes how to set CloudAudit log shipping in a landing zone.

Prerequisites

You have logged in to the Tencent Cloud console and gone to the **Control Center** > [Landing zone](#) page.

Directions

1. On the **Landing zone** page, click **Add configuration**.



2. In the **Add configuration** pop-up window, select **Manage CloudAudit log shipping** and click **Confirm**.

Add configuration ×

Manage CloudAudit log shipping

Ship the operation logs of all the enterprise's accounts to a specified COS bucket to centrally manage and analyze logs and facilitate the operations of CloudAudit.

Manage Config log shipping

Ship the configuration logs of all the enterprise's accounts to a specified COS bucket so that changes made to resources can be viewed and managed easily.

Invite existing accounts

Invite existing accounts to the organization. An invitation will be sent to the invited account, which can join the organization after accepting the invitation.

ConfirmCancel

3. On the **Configure CloudAudit log shipping** page that appears, provide CloudAudit log information, including basic information, managed events, and shipping method.

- **Tracking set:** Enter a name for the tracking set, which must be 3 to 128 characters long and contain uppercase letters, lowercase letters, numbers, and underscores (_).
- **Event type:** The default value is Write only. You can change it to Read only or All.
- **Destination:** Create a COS bucket for log shipping, specify the region where the bucket is located, and name the bucket.

Configure CloudAudit log shipping (core account required)

After successful configuration, the system will create a CloudAudit tracking set under the admin account of the organization to ship the CloudAudit logs of all member accounts.

Basic information

Tracking set *
3-128 characters; only supports letters, digits, and -

Tracked regions All regions


Managed events

Event type * Write Read All

Event name * All events

Shipping method

Destination * Ship events to a COS bucket

COS bucket **New bucket**
Logs will be shipped to the COS bucket you create, which will incur COS storage costs. For the billing details, see [COS Billing Overview](#) 

Region *

-251241628
Max 50 characters; can only contain lowercase letters, digits, and -; cannot start or end with -

Log file prefix *
3-40 characters; can only contain letters and digits.

4. Click **Next: Preview** to go to the preview page.

5. After confirming that the preview is correct, click **Apply**.

Managing Config Log Shipping

Last updated: 2023-08-15 17:53:04

Overview

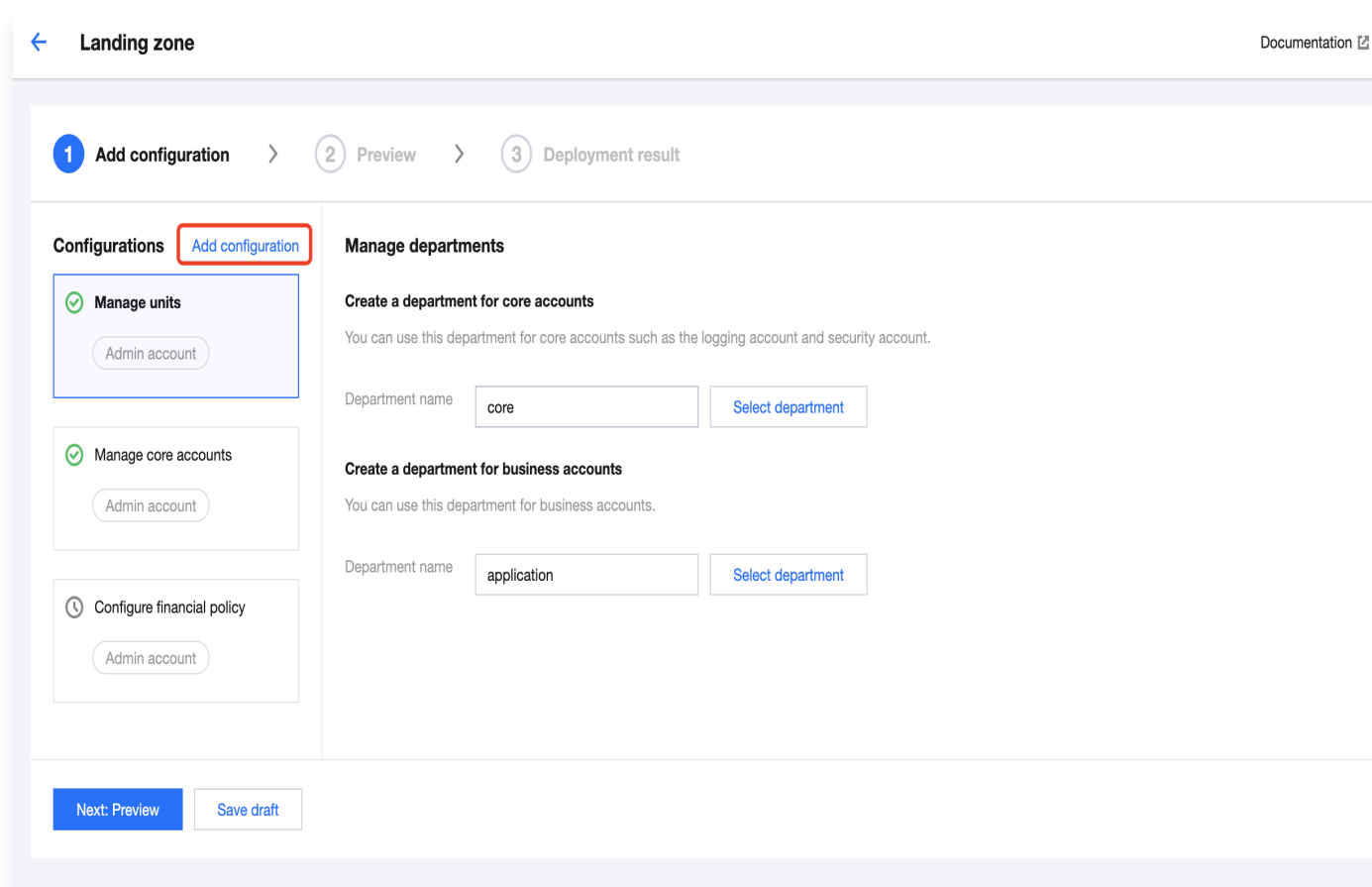
You can configure to ship the Config logs of all accounts to a designated Cloud Object Storage (COS) bucket for centralized monitoring and management of resource change records within the enterprise. This document describes how to configure Config log shipping.

Prerequisites

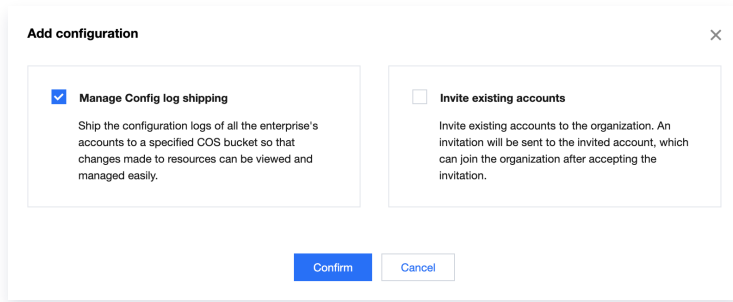
You have logged in to the Tencent Cloud console and gone to the **Control Center** > [Landing zone](#) page.

Directions

1. On the **Landing zone** page, click **Add configuration**.

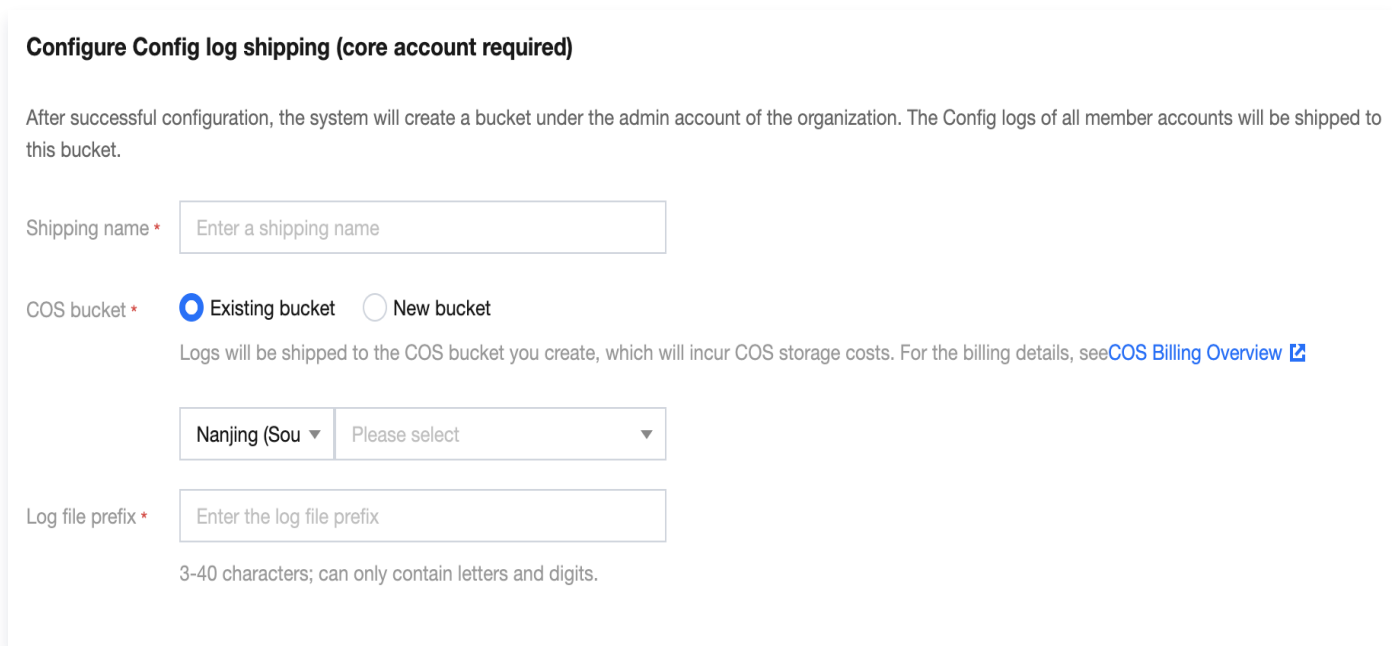


2. In the **Add configuration** pop-up window, select **Manage Config log shipping** and click **Confirm**.



The dialog box titled "Add configuration" contains two sections. The first section, "Manage Config log shipping", has a checked checkbox and a description: "Ship the configuration logs of all the enterprise's accounts to a specified COS bucket so that changes made to resources can be viewed and managed easily." The second section, "Invite existing accounts", has an unchecked checkbox and a description: "Invite existing accounts to the organization. An invitation will be sent to the invited account, which can join the organization after accepting the invitation." At the bottom are "Confirm" and "Cancel" buttons.

3. On the **Configure Config log shipping** page that appears, configure the following parameters as needed.



Configure Config log shipping (core account required)

After successful configuration, the system will create a bucket under the admin account of the organization. The Config logs of all member accounts will be shipped to this bucket.

Shipping name *


COS bucket * Existing bucket New bucket

Logs will be shipped to the COS bucket you create, which will incur COS storage costs. For the billing details, see [COS Billing Overview](#)

Log file prefix *


3-40 characters; can only contain letters and digits.

- **Shipping name:** This refers to the service name for Config log shipping.
- **COS bucket:** You can select an existing bucket in the corresponding region or create a new bucket. If you create a new bucket, specify the bucket region and name the bucket.
- If any shipping configurations exist, you can view the existing information in the list.

← Landing zone Documentation 

1 Add configuration > 2 Preview > 3 Deployment result

Configurations Add configuration

Invite existing accounts 
[Admin account](#)

▼ **Completed (7)**

Manage units
[Admin account](#)

Manage core accounts
[Admin account](#)


Configure financial policy
[Admin account](#)









Manage permissions
[Admin account](#)

Manage CloudAudit log shipping
[Admin account](#)

Manage Config log shipping
[Admin account](#)

Manage CloudAudit log shipping

 You can go to [Compliance audit](#), to view more details.

Name	Tracked regions	Tracked resource types	Application scope	COS bucket	CLS log topic	Log file prefix	Logging status
	All regions	All resource types	All accounts		-		Enable
	All regions	All resource types	All accounts		-		Enable
	All regions	All resource types	All accounts	-	Query and analysis		Enable

4. After confirming that the information is correct, click **Next: Preview**.

5. After confirming that the preview is correct, click **Apply**.

Inviting Existing Accounts

Last updated: 2023-08-17 11:49:44

Overview

You can invite an existing Tencent Cloud account to join your organization for centralized management. Control Center will send a confirmation email to the invited account, and the account can join the organization after confirmation. This document describes how to invite existing accounts to join your organization.

Prerequisites

You have logged in to the Tencent Cloud console and gone to the **Control Center** > [Landing zone](#) page.

Directions

1. On the **Landing zone** page, click **Add configuration**.

The screenshot shows the 'Landing zone' page in the Tencent Cloud console. The page title is 'Landing zone' with a back arrow on the left and a 'Documentation' link on the right. A progress bar at the top indicates three steps: 1. Add configuration (active), 2. Preview, and 3. Deployment result. The main content area is divided into two columns. The left column, titled 'Configurations', contains three items: 'Manage units' (with a green checkmark and an 'Add configuration' button highlighted in red), 'Manage core accounts' (with a green checkmark), and 'Configure financial policy' (with a clock icon). Each item has an 'Admin account' button below it. The right column, titled 'Manage departments', contains two sections: 'Create a department for core accounts' and 'Create a department for business accounts'. Each section has a description and a form with a 'Department name' input field and a 'Select department' button. The 'core' department is selected in the first section, and 'application' is selected in the second. At the bottom of the page, there are two buttons: 'Next: Preview' and 'Save draft'.

2. In the **Add configuration** pop-up window, select an existing account and click **Confirm**.

Add configuration ×

Invite existing accounts
Invite existing accounts to the organization. An invitation will be sent to the invited account, which can join the organization after accepting the invitation.

Confirm Cancel

3. On the **Invite existing accounts** page that appears, click **Add**.

Invite existing accounts

Invite an existing account to join the organization. An invitation (valid for 14 days) will be sent to the invitee, which will become a member of the organization only if they accept the invitation.

Add

Account ID	Account name	Payment mode	Department	Operation
None				

Total items: 010 ▼ / page

⏪ ⏩ 1 / 1 page ⏪ ⏩

4. On the **Invite account** page that appears on the right side, enter the member account information and then click **Confirm**.

ⓘ Note:

The entity used by a member account for identity verification must be the current entity.

Invite account ✕

Account ID *

You can only invite an account with the same enterprise identity.

Account name *

The name must be unique across the organization. It should be 1-25 characters long and can only contain letters, digits, Chinese characters, and characters @、&、_[]-;

Financial permissions Finance management

View bills View balance
 Allocate funds Consolidated billing Invoice

Department [New department](#)

Payment mode Self-paying Pay-on-behalf

Inherit discounts

Allow quit Allow the account to quit the organization

5. After the member account is successfully added, you can view it in the list and remove it as needed.

Invite existing accounts

Invite an existing account to join the organization. An invitation (valid for 14 days) will be sent to the invitee, which will become a member of the organization only if they accept the invitation.

[Add](#)

Account ID	Account name	Payment mode	Department	Operation
		Self-paying		Remove

Total items: 1

10 / page

1 / 1 page

6. After confirming that the member account information is correct, click **Next: Preview**.

7. After confirming that the preview is correct, click **Apply**.

Note:

Consent from the invited account is required. The invitation email is valid for 14 days.

Control Center Overview

Last updated: 2023-08-15 17:54:50

Overview Modules

The [Overview](#) page of the Control Center console comprises six modules: Organization overview, Security rules, Finance, Related services, User guides, and Best practices.

The screenshot displays the 'Overview' page of the Control Center console. The page is divided into six main modules arranged in a grid. The 'Organization overview' module shows 3 Departments, 3 Accounts, 1 Entity, and 4 Permissions. The 'Security rules' module shows 29 Rule templates and 0 Total rules. The 'Finance' module shows a 2023-07 Total spend of 0 CNY, with a 0.0% change from last month. The 'Related services' module lists Account management, Cloud Access Management, CloudAudit, Tencent Cloud Config, and Cloud Security Center. The 'User guides' and 'Best practices' modules are also visible.

Module	Item	Value
Organization overview	Departments	3
	Accounts	3
	Entities	1
	Permissions	4
Security rules	Rule templates	29
	Total rules	0
Finance	2023-07 Total spend	0 CNY
	Change from last month	0.0%
Related services	Account management	1
	Cloud Access Management	1
User guides	Paid-on-behalf accounts	0
	Self-paying accounts	3

Organization overview

The **Organization overview** module displays the number of departments, accounts, entities, and permissions within the organization that the current account belongs to. For information about operations, see [Viewing Accounts](#).

Organization overview[View all accounts](#)

Departments

3

Accounts

3

Entities

1

Permissions

4

Security rules

The **Security rules** module displays the total number of security rules and that of enabled security rules. For information about operations, see [Viewing Security Rules](#).

Security rules

Rule templates

29

Total rules

0

Finance

The **Finance** module shows the total expenses and cost breakdown information for the current month. By clicking an account name, you can view the details of the account. The module also displays the number of paid-on-behalf accounts and self-paying accounts within the organization.

Finance

2023-07 Total spend

0 CNY From last month ↑ 0.0%

Billing details



Paid-on-behalf accounts	0	Self-paying accounts	3
-------------------------	---	----------------------	---

Related services

The **Related services** module displays other services relevant to Control Center, such as Account management, Cloud Access Management, CloudAudit, Tencent Cloud Config, and Cloud Security Center. By clicking a service name, you will be directed to the respective service page.

Related services

- Account management
- Cloud Access Management
- CloudAudit
- Tencent Cloud Config
- Cloud Security Center

User guides

The **User guides** module displays the operations documentation for Control Center. By clicking a user guide, you will be directed to the corresponding document.

Best practices

The **Best practices** module displays the best practices for using Control Center.

Baselines

Viewing Baselines

Last updated: 2023-08-15 17:55:23

Overview

Through baseline management, you can add and configure common baselines, including identity permissions, network, security, and finance. Once configured, these baselines can be applied to specific accounts to enhance delivery efficiency. This document describes the features provided on the baselines page.

Directions

Log in to the Tencent Cloud console and go to the **Control Center > Baselines** page.

Baseline	Description	Category	Baseline status	Dependency	Application his...	Operation
Configure financial policy	Configure the default financial policy for the enterprise and s...	Finance manag...	Configured	-	All accounts	Details
Manage permissions	With the permission management capability, the enterprise a...	Permission man...	Configured	-	All accounts	Details

Baseline operations

- To add baselines, click **Add baseline**. For more information, see [Adding Baselines](#).
- You can delete the baselines that have been added. For more information, see [Deleting Baselines](#).
- To apply configured baselines to member accounts, click **Apply baselines**. For more information, see [Applying Baselines](#).
- To configure a specific baseline, click **Configure** for the baseline in the list. After you complete the configuration, the baseline status will change to Configured. For more information, see [Configuring Baselines](#).

Adding Baselines

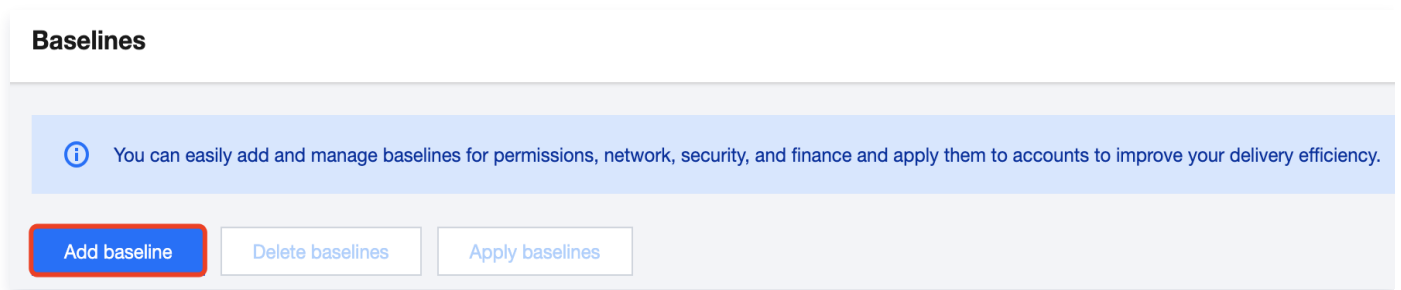
Last updated: 2023-08-15 18:00:59

Overview

This document describes how to add baselines.

Directions

1. Log in to the Tencent Cloud console and go to the **Control Center** > [Baselines](#) page.
2. Click **Add baseline**.



3. Select the baselines you want to add, such as contacts and message subscriptions. Click **Confirm** to add the selected baselines.

Add baseline ✕

VPC

The VPC baseline helps you easily create a private network and configure the IP address range, routing table, and gateway.

security group

A security group functions as a virtual firewall. It allows you to control inbound and outbound requests for instances to enhance security.

CAM password policy

Configure password rules including minimum length, complexity, and expiration period to reduce the risk of leakage.

Confirm Cancel

4. The added baselines appear in the **Baselines** list. Click **Configure** to set a specific baseline before you can use it.

- For information about how to configure the contact baseline, see [Configuring a Contact Baseline](#).
- For information about how to configure the CAM password policy baseline, see [Configuring a CAM Password Policy Baseline](#).

Note

- For baselines with dependencies, the system will automatically select and add the dependencies along with the baselines.
- When deleting a baseline with dependencies, you must delete the dependencies first. For example, if a message subscription baseline depends on a contact baseline, you must delete the message subscription baseline before deleting the contact baseline.

Configuring Baselines

Configuring a Contact Baseline

Last updated: 2023-08-15 18:03:39

Overview

You can add contacts for an account in a contact baseline. The added contacts will receive account notifications.

Prerequisites

You have added the contact baseline. For directions on adding baselines, see [Adding Baselines](#).

Directions

1. Go to the **Control Center** > [Baselines](#) page and click **Configure** for the contact baseline.

Baselines

You can easily add and manage baselines for permissions, network, security, and finance and apply them to accounts to improve your delivery efficiency.

[Add baseline](#) [Delete baselines](#) [Apply baselines](#)


Baseline	Description	Category	Baseline status	Dependency	Application history	Operation
Configure financial policy	Configure the default financial policy for the enterprise and set the paye...	Finance management	Configured	-	All accounts	Details
Manage permissions	With the permission management capability, the enterprise administrato...	Permission manage...	Configured	-	All accounts	Details
Manage CloudAudit log shipping	Ship the operation logs of all the enterprise's accounts to a specified C...	Compliance audit	Configured	-	All accounts	Details
Manage Config log shipping	Ship the configuration logs of all the enterprise's accounts to a specifi...	Compliance audit	Configured	Manage core accounts	All accounts	Details
Contacts	Add contacts for new accounts to receive notifications. Tencent Cloud ...	Message	Configured	-	0	Configure Delete

2. On the **Baseline/Contacts** page, click **Add contact**. In the pop-up window, enter the contact information.

Baselines/Contacts

Add contacts for receiving notifications.

Add contact

Contact name	Mobile number	Email	Remarks	Operation
 No contacts yet				

Total items: 0

10 / page 1 / 1 page

3. Click Add.

Configuring a CAM Password Policy Baseline

Last updated: 2023-08-15 18:04:03

Overview

You can configure CAM password policies in the corresponding baseline to strengthen password security and mitigate the risk of account breaches.

Prerequisites

You have added the CAM password policy baseline. For directions on adding baselines, see [Adding Baselines](#).

Directions

1. Go to the **Control Center** > [Baselines](#) page and click **Configure** for the CAM password policy baseline.
2. On the **Baselines/CAM password policy** page, configure the password policy for sub-user login.

← Baselines/CAM password policy

ⓘ The password policy you configure on this page only applies to sub-users logging in using passwords. It does not apply to collaborators or sub-users who log in by scanning the QR code with Weixin. After a password expires, the sub-user will be unable to log in (including via QR code scan) and must reset the password. For improved account security, we will not tell users the password rules when they reset passwords. You can download the rules and send them to your sub-users.

Must include • Digits Lowercase letters Uppercase letters Special characters (not including spaces)

Minimum length • characters
The minimum password length. The default is 8 characters. You can set it to up to 32 characters.

Expiration period • days
The expiration period for a password, after which it must be reset. The default value is 0, which means the password will never expire. You can set it to up to 365 days.

Reuse limit •
The number of previous passwords to prevent reusing. The default value is 1, which means a new password cannot be identical to the last one. The maximum value allowed is 24. If you set this to 0, no reuse limit will be set.

Retry limit • /hour
The number of retry attempts allowed. The default value is 10. The smallest value allowed is 1. After the limit is reached, the account will be locked for one hour.

- **Must include:** Select the types of characters you want sub-users to include in their passwords.
- **Minimum length:** Click the **plus** or **minus** sign to adjust the minimum length of passwords, or enter the desired length in the numeric text box.
- **Expiration period:** Click the **plus** or **minus** sign to set the number of days until a password expires, or enter the desired number of days to expiration in the numeric text box. If the expiration period is set to 0, passwords will never expire.

- **Reuse limit:** Click the **plus or minus sign** to set the number of previous passwords that cannot be reused, or enter the desired number in the numeric text box. If this parameter is set to 0, the system does not check if a new password is identical to previous ones.
 - **Retry limit:** Click the **plus or minus sign** to set the password retry count, or enter the desired retry count in the numeric text box. By default, up to 10 retries are allowed in an hour. If the retry count is exceeded, the account will be locked for one hour automatically.
3. After you set all parameters, click **Update**. If you click **Reset**, the parameters will be restored to default values.

Applying Baselines

Last updated: 2023-08-15 18:04:25

Overview

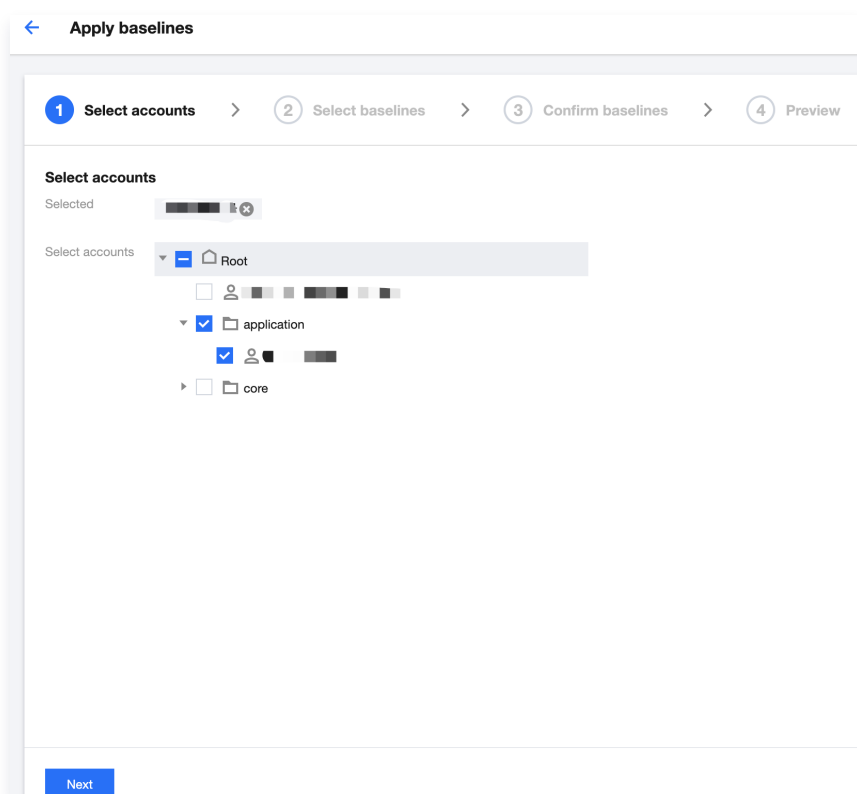
By applying baselines, you can rapidly configure baselines for accounts and streamline the process of associating baselines with accounts.

Prerequisites

You have configured baselines. For more information, see [Configuring Baselines](#).

Directions

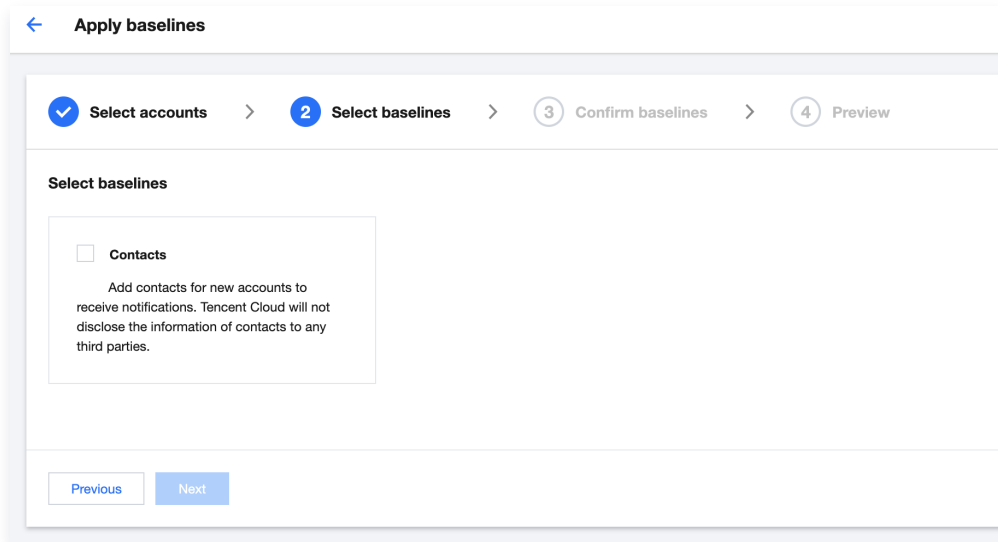
1. On the **Control Center** > [Baselines](#) page, click **Apply baselines**.
2. On the page that appears, select the accounts to which you want to apply the baselines. You can select either individual accounts or an entire department.



3. Click **Next** and select the baseline(s) you want to apply.

Note:

You can only select baselines that have been configured.



4. Click **Next** to go to the **Confirm baselines** page, where you can modify the baselines. For more information, see [Configuring Baselines](#).
5. Click **Next** to go to the **Preview** page and verify whether the information about the baselines to be applied is correct.
6. If the information is correct, click **Apply**. A message appears in the top-right corner of the page, indicating that the baselines are applied successfully.

Deleting Baselines

Last updated: 2023-08-15 18:05:25

Overview

This document describes how to delete a baseline.

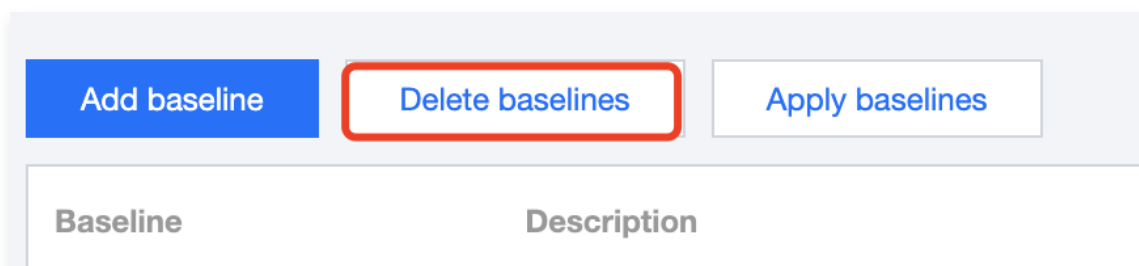
Prerequisites

You have added baselines other than default baselines.

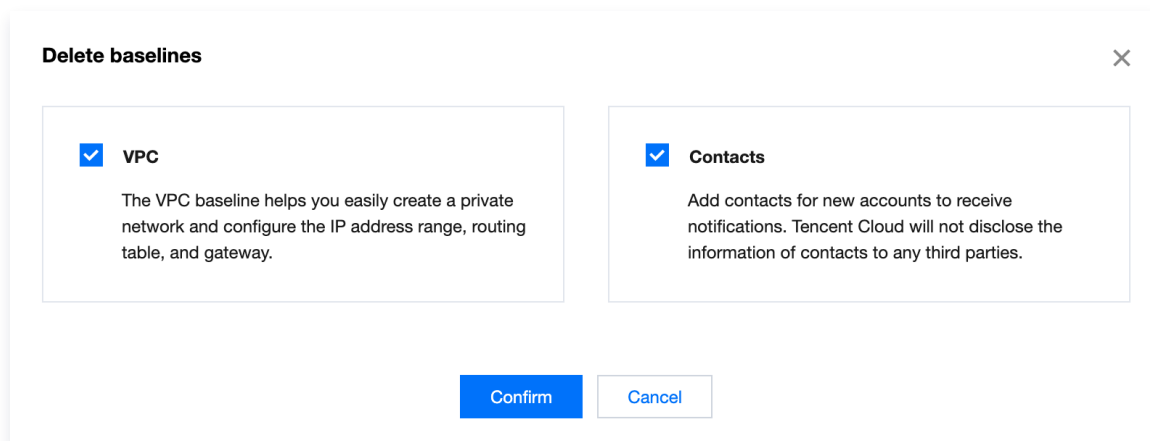
Directions

Deleting multiple baselines at a time

1. On the **Control Center** > **Baselines** page, click **Delete baselines**.



2. On the page that appears, select the baselines you want to delete, then click **Confirm**.



Note:
Default baselines cannot be deleted.

Deleting individual baselines

1. On the **Control Center** > **Baselines** page, click **Delete** in the **Operation** column for the

baseline you want to delete.

Baseline	Description	Category	Baseline status	Dependency	Application his...	Operation
Configure financial policy	Configure the default financial policy for the enterprise and s...	Finance manag...	Configured	-	All accounts	Details
Manage permissions	With the permission management capability, the enterprise a...	Permission man...	Configured	-	All accounts	Details
CAM password policy	Configure password rules including minimum length, comple...	Security	Configured	-	0	Configure Delete

2. In the pop-up window, click **Confirm**.

Are you sure you want to delete this baseline?

The application data of this baseline will be deleted as well.

[Confirm](#) [Cancel](#)

Accounts

Viewing Accounts

Last updated: 2023-08-15 18:09:01

Overview

After you set up a landing zone, you can configure multi-account scenarios by using the accounts feature to minimize delivery costs. This document describes the elements on the Accounts page.

Directions

Log in to the Tencent Cloud console and go to the **Control Center** > [Accounts](#) page where you can view the following information.

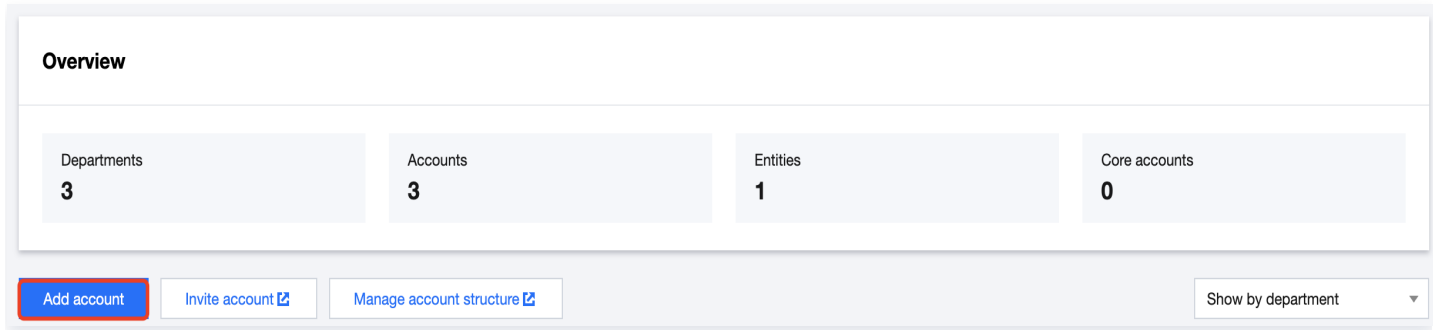
Viewing account statistics

Overview			
Departments	Accounts	Entities	Core accounts
3	3	1	0

- **Departments:** The real-time number of departments within the organization, including the root node.
- **Accounts:** The real-time number of all accounts (including admin accounts) within the organization. Accounts that have been invited but have not yet accepted the invitation are excluded.
- **Entities:** The current number of authenticated entities.
- **Core accounts:** The number of core accounts under the organization.

Adding accounts

To add member accounts under the organization, click **Add account**. For more information, see [Adding Accounts](#).



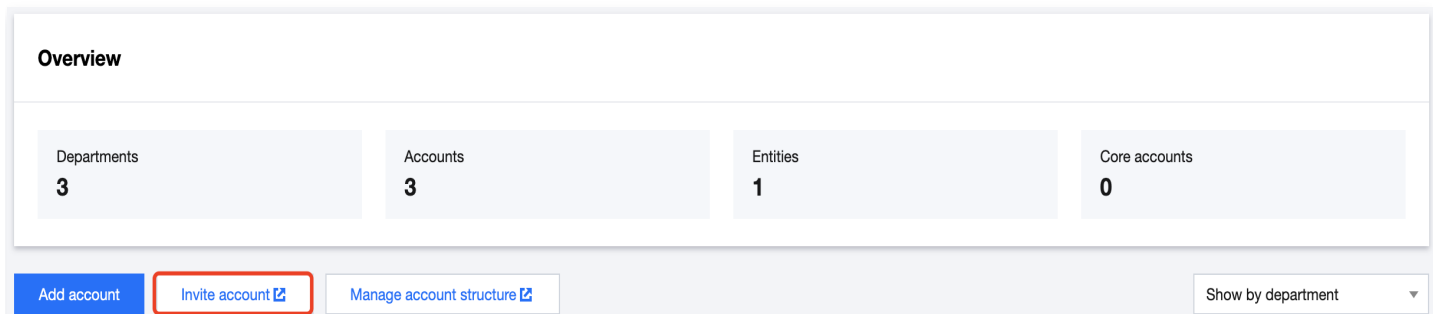
Overview

Departments 3	Accounts 3	Entities 1	Core accounts 0
-------------------------	----------------------	----------------------	---------------------------

[Add account](#) [Invite account](#) [Manage account structure](#) Show by department ▾

Inviting accounts

To invite accounts, click **Invite account** to go to the member account management page. For more information, see [Adding Organization Members](#).



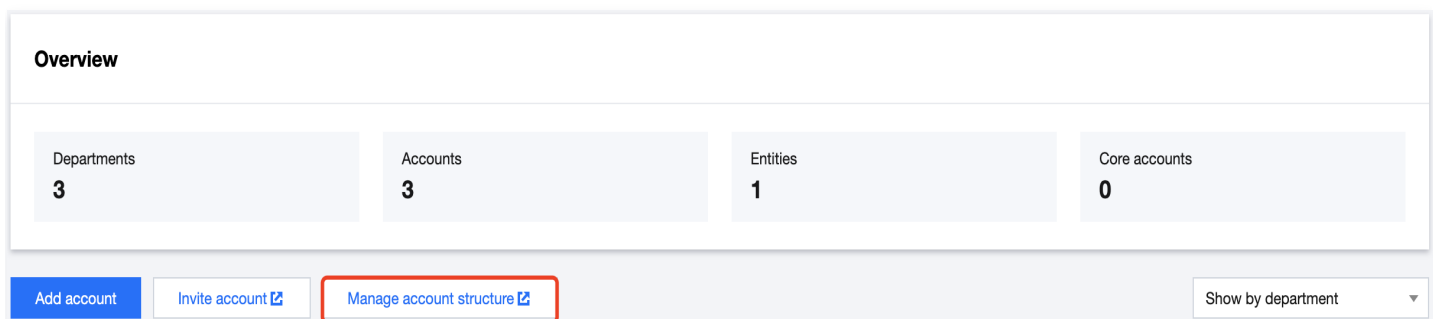
Overview

Departments 3	Accounts 3	Entities 1	Core accounts 0
-------------------------	----------------------	----------------------	---------------------------

[Add account](#) [Invite account](#) [Manage account structure](#) Show by department ▾

Managing accounts

To manage accounts, click **Manage account structure** to go to the department management page. For more information, see [Department Management](#).



Overview

Departments 3	Accounts 3	Entities 1	Core accounts 0
-------------------------	----------------------	----------------------	---------------------------

[Add account](#) [Invite account](#) [Manage account structure](#) Show by department ▾

Account display mode

Accounts can be displayed by department or by member. By default, accounts are displayed by department. You can click **Show by department** to open the drop-down list and select the other display mode.

The screenshot shows the Tencent Cloud Control Center interface for account management. At the top, there are buttons for 'Add account', 'Invite account', and 'Manage account structure'. A dropdown menu in the top right corner is set to 'Show by department'. The main content area is titled 'Root' and shows a table of accounts. The table has the following columns: 'Account ID', 'Member account name', 'Payment mode', 'Financial permissions', and 'Operation'. A single account is listed with 'Self-paying' payment mode and 'Finance management(5)' permissions. The 'Operation' column contains a link 'Apply baselines'. Below the table, it shows 'Total items: 1' and a pagination control for '10 / page' and '1 / 1 page'.

- **Show by department**

You can click the **account name** of a member account to view account details.

- **Show by member**

You can click the **account ID** of a member account to view account details.

Viewing financial permissions

To view the financial permissions of a member account, hover over **Financial management** for the member account. In the pop-up window, click the **specific permissions** you want to view.

Root

Creation time 2023-07-07 Accounts 1

- Finance management
- View bills [↗](#)
- View balance [↗](#)
- Allocate funds [↗](#)
- Consolidated billing [↗](#)
- Invoice [↗](#)

Account ID	Member account name	Payment mode	Operation
██████████	██████████ ..	Self-paying	Finance management(5) Apply baselines

Total items: 1

10 / page

[◀](#) 1 / 1 page [▶](#)

Applying baselines

To add baselines to a member account, click **Apply baseline** for the member account. On the page that appears, you can add baselines for the member. For more information about baseline configuration, see [Applying Baselines](#).

Adding Accounts

Last updated: 2023-08-15 18:09:19

Overview

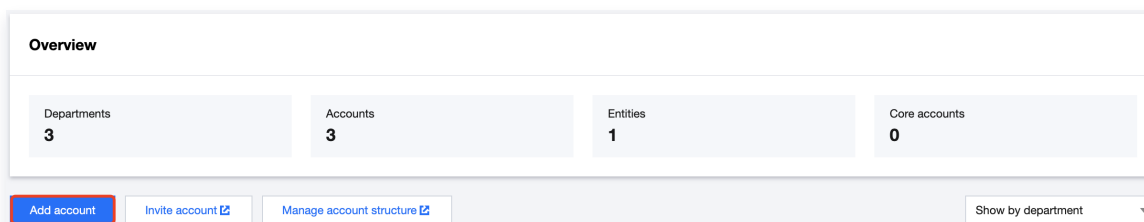
This document describes how to add accounts.

Prerequisites

You have configured account baselines. For more information, see [Viewing Baselines](#).

Directions

1. Log in to the Tencent Cloud console and go to the **Control Center** > **Accounts** page.
2. Click **Add account**.



3. On the **Accounts/Add account** page, configure basic account information.

- **Account name:** An account name is the unique identifier of an account within the department and can be modified later.
- **Add baseline:** You can select pre-configured account baselines.

- Entity: You can select the current entity or another entity.

Note:

If you select another entity, the new account will become active only after it has been reviewed and approved by the admin account of the selected entity. The account will use the entity for identity verification.

- Financial permissions: The View bills and View balance options are required. Other options, including Allocate funds, Consolidated billing, and Invoice, are optional.
- Payment mode: You can select Self-paying or Pay-on-behalf.
- Department: Select the department to which the account belongs. You can modify this parameter later.

4. After configuring the information, click **Add**.

Inviting Accounts

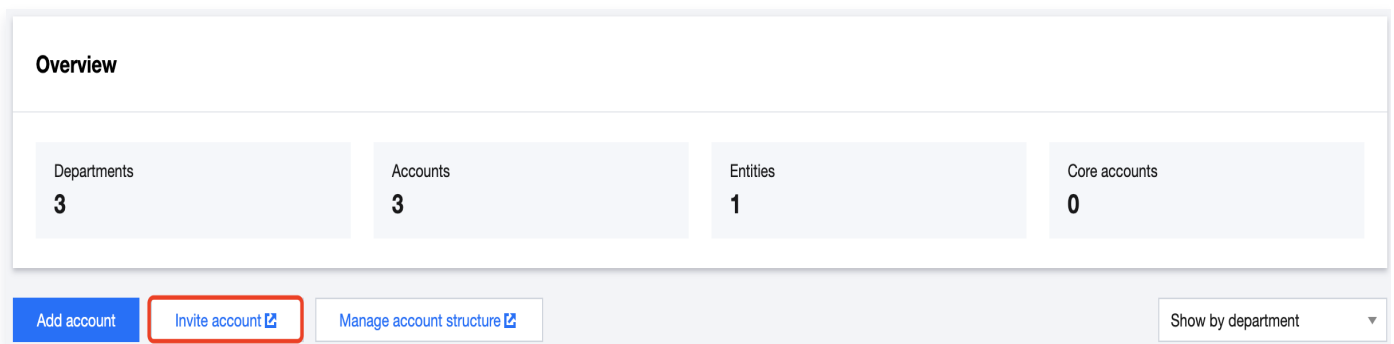
Last updated: 2023-08-15 18:09:36

Overview

This document describes how to invite accounts.

Directions

1. Log in to the Tencent Cloud console and go to the **Control Center** > **Accounts** page. Click **Invite account**.



2. On the page that appears, select **Invite member** as the adding method. For more information about the configuration, see [Adding Members](#).

Adding method

Create member
Create a Tencent Cloud root account and add it to the organization

Invite member
Invite a Tencent Cloud root account that is in use to join the organization

Account ID *

You can invite a Tencent Cloud account that has the same verified identity as yours.

Member name *

It can only contain 1-25 letters, digits, Chinese characters, and symbols (@, & _ [] - ;).

Member finance authorization

- View bills
- View balance
- Allocate funds
- Consolidate bills
- Invoice
- Inherit offer
- Cost Analysis

Payment mode

Self-pay Pay-on-behalf

Department

Root

Active quitting supported If this option is enabled, the member account can actively quit the organization.

The invited account must either accept or reject the invitation within 15 days; otherwise, the invitation will expire.

Login Permissions

Creating Permissions

Last updated: 2023-08-15 18:09:59

Overview

On the Login Permissions page, you can view the list of permissions for enterprise internal accounts that are currently available for unified login. You can also customize login permissions by creating permissions. This document describes the product features for setting up login permission.

Prerequisites

You have configured **Manage identities and permissions** in the landing zone settings.

Directions

1. Log in to the Tencent Cloud console and go to the **Control Center** > [Login permissions](#) page.
2. To refine permission authorization, click **Create permission** to go to the **Account management** > **Unified member access** page. For more information about how to create a permission, see [Creating Member Login Permissions](#).

Login permissions

 The administrator of the organization can create permissions and grant them to member accounts. Up to 20 custom permissions can be created.

[Create permission](#) 

[Authorize members](#) 

[View authorization](#) 

Finance

Viewing the Financial Structure

Last updated: 2023-08-15 18:10:24

Overview

On the **Finance** page, you can view the financial structure of your organization so that you can adjust the financial structure of your cloud account as needed. This document describes operations related to the financial structure.

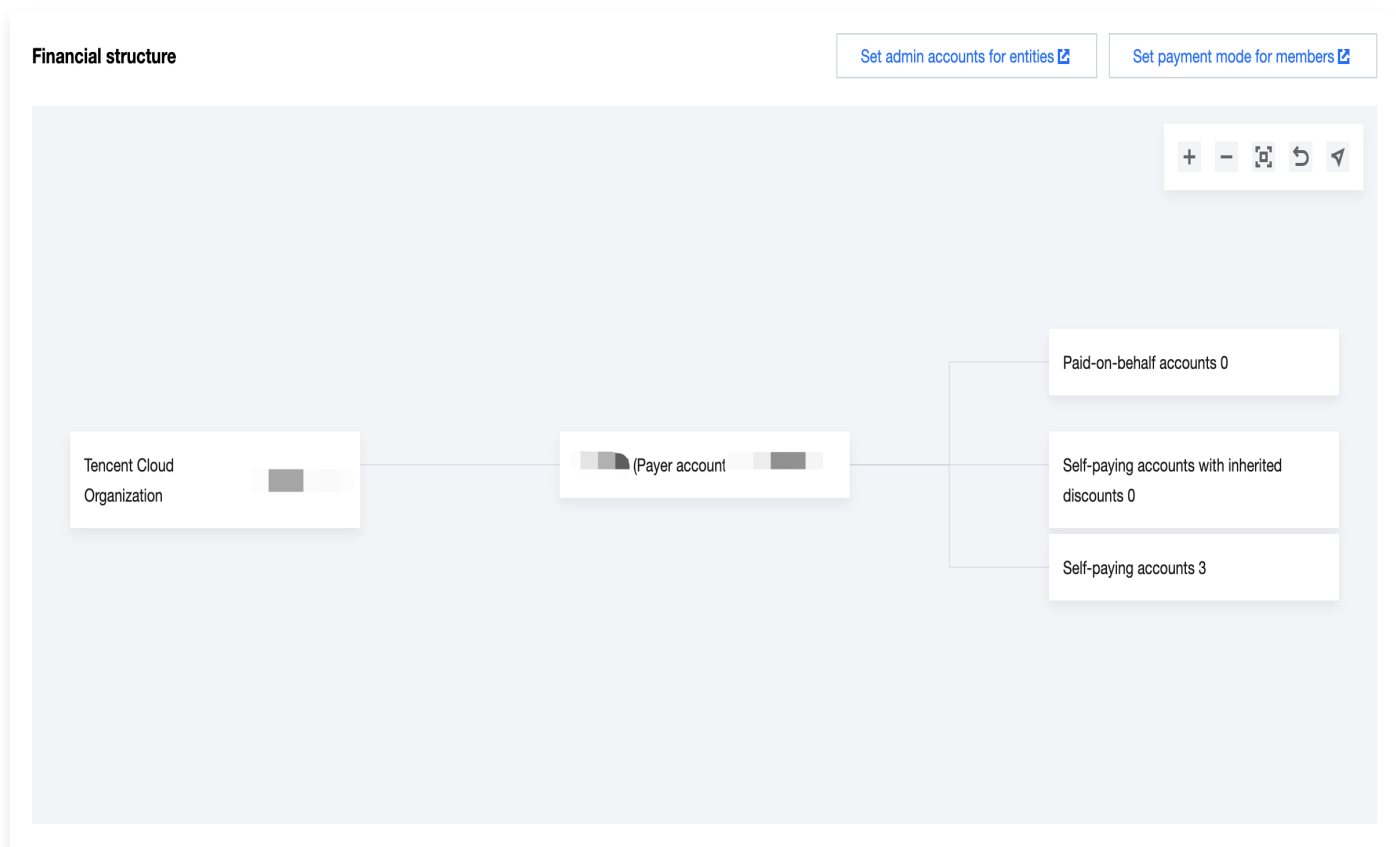
Prerequisites

You have configured financial policies in the landing zone.

Directions

Browse the financial structure

1. Log in to the Tencent Cloud console and go to the **Control Center** > **Finance** page.



2. In the top-right corner of the **Financial structure** page, there are five buttons



, which are Zoom In, Zoom Out, Full Screen, Undo, and Navigate, from left to right.

- Zoom In: You can click this button to enlarge the page and view the structure in detail.
- Zoom Out: You can click this button to shrink the page to view the overall structure.
- Full Screen: You can click this button to display the financial structure in full-screen mode.
- Undo: You can click this button to reverse zoom actions.
- Navigate: You can click this button to open the navigation window to quickly locate specific positions in the structure.

Setting admin accounts for entities

To configure the authenticated entity and admin account, click **Set admin accounts for entities** in the top-right corner of the **Financial structure** page to go to the **Account management > Verified entity management** page. For more information about configuration, see [Organization Verified Entity Management](#).

Setting payment mode for members

To manage the payment mode for member accounts, click **Set payment mode for members** in the top-right corner of the **Financial structure** page to go to the **Account management > Member account management** page. For more information about configuration, see [Organization Fund Allocation Mode](#).

Viewing Billing Overview

Last updated: 2023-08-15 18:10:45

Overview

The billing overview presents a summary of the historical billing data for all accounts within your organization. The data can be aggregated by member or by product.

Prerequisites

You have configured financial policies in the landing zone.

Directions

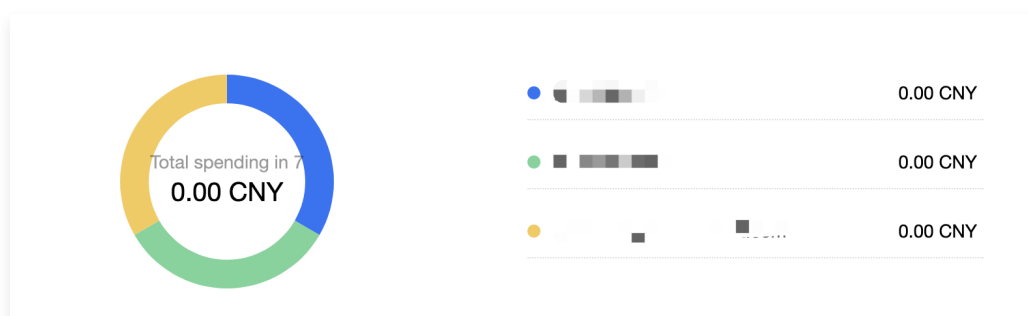
Log in to the Tencent Cloud console and go to the **Control Center** > **Finance** page to view the billing overview.

Note:

By default, billing data is aggregated by member. You can click **Group by member** to switch to the desired aggregation method.

• Group by member

- Total expenses: This shows the total expenses for all members managed under the organization in the current month (excluding those who joined or left in the current month).

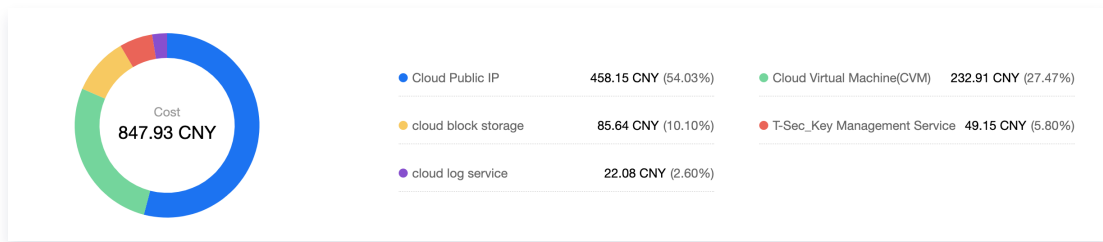


- Member billing list: Below the total expenses, you can view the billing expenses for each member in the current month.

Account ID	Member account name	Month	Spend	Ratio
[blurred]	[blurred]	[blurred]	[blurred]	[blurred]

• **Group by product**

- **Total expenses:** This is the total expenses for all products managed by TCO in the current month (excluding those that joined or left in the current month).



Security Rules

Viewing Security Rules

Last updated: 2023-12-05 14:34:39

Overview

In Control Center, you can view and configure security rules to ensure security in a multi-account environment. This document describes the key elements on the security rules page.

Prerequisites

You have completed the configuration of **Enable security rules** in the landing zone.

Directions

Overview

In the **Overview** section on the **Control Center > Security rules** page, you can view the total number of rules and the number of violated rules.

Overview

Total rules 66 Violated rules 54

- **Total rules:** This parameter represents the total number of security rules created within the organization, including both enabled and disabled rules.
- **Violated rules:** This parameter represents the number of rules that are violated.

Viewing rule evaluation results

1. On the **Control Center > Security rules** page, click a specific rule name to go to the rule details page.

Security rules

Overview

Total rules 66 Violated rules 54

[Manage security rules](#)

Rule name	Risk level	Status	Evaluation result
Checks whether the CAM user's key changes wit...	High	Enabled	Compliant

2. View the basic information and evaluation results of the rule.

3. You can click the **Resource ID/name** of a resource to view its details. For more information about resource configuration, see [Viewing Resource Details](#) .

← Checks whether there are idle permission policies in CAM

Basic information

Rule name Checks whether there are idle permission policies in CAM Risk level Low
 Creation time 2023-11-21 11:44:59 Application scope All accounts

Evaluation result

Resource type	Resource ID/name	Evaluation result	Account	Evaluation time
QCS::CAM::Policy CAM - Policy	[Redacted]	Compliant	[Redacted]	2023-11-24 13:30:49
QCS::CAM::Policy CAM - Policy	[Redacted]	Non-compliant	[Redacted]	2023-11-24 13:30:48
QCS::CAM::Policy CAM - Policy	[Redacted]	Compliant	[Redacted]	2023-11-24 13:30:48
QCS::CAM::Policy CAM - Policy	[Redacted]	Compliant	[Redacted]	2023-11-24 13:30:49
QCS::CAM::Policy CAM - Policy	[Redacted]	Compliant	[Redacted]	2023-11-24 13:30:48
QCS::CAM::Policy CAM - Policy	[Redacted]	Non-compliant	[Redacted]	2023-11-21 13:31:18

Total items: 6

10 / page 1 / 1 page

Managing Security Rules

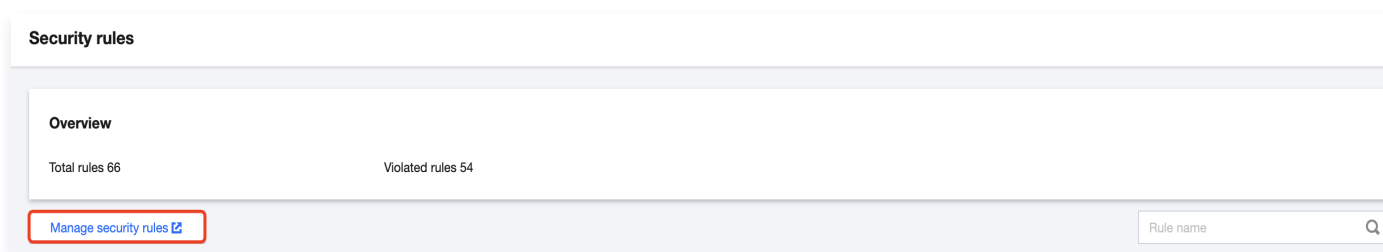
Last updated: 2023-12-05 14:35:19

Overview

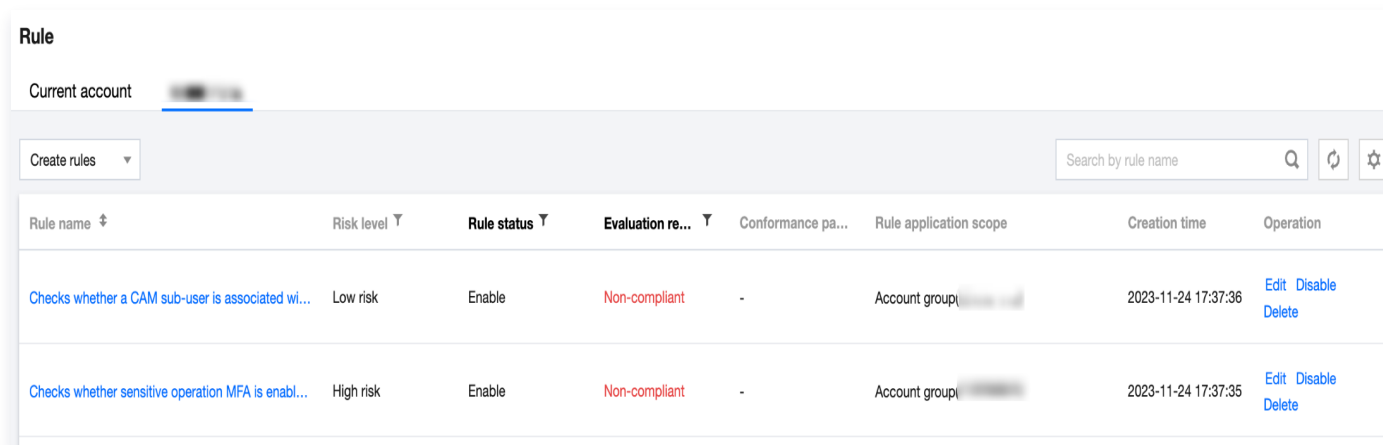
In Tencent Cloud Config, you can configure more security rule settings, such as creating new hosting rules, enabling or disabling rules, and searching for specific rules.

Directions

1. On the **Control Center > Security rules** page, click **Manage security rules** to open the **Tencent Cloud Config > Rule** page.



2. Click the top account bar and select the Account group.



3. On the **Tencent Cloud Config > Rule** page, you can perform various operations such as creating, editing, and enabling or disabling rules. For detailed instructions, see [Viewing Rule List](#).

Compliance Audit

Last updated: 2023-08-15 18:11:13

Overview

The compliance audit feature in Control Center allows you to track the destinations of Config logs and CloudAudit logs. This document describes how to use this feature.

Prerequisites

1. You have logged in to the Tencent Cloud console.
2. You have set up Config log shipping or CloudAudit log shipping in the landing zone. If not, see [Managing CloudAudit Log Shipping](#) or [Managing Config Log Shipping](#) for instructions.

Directions

Viewing log destinations

In the Tencent Cloud console, go to the **Control Center** > [Compliance audit](#) page where you can view the destinations of Config logs and CloudAudit logs in their respective lists.

Compliance audit

Config log shipping

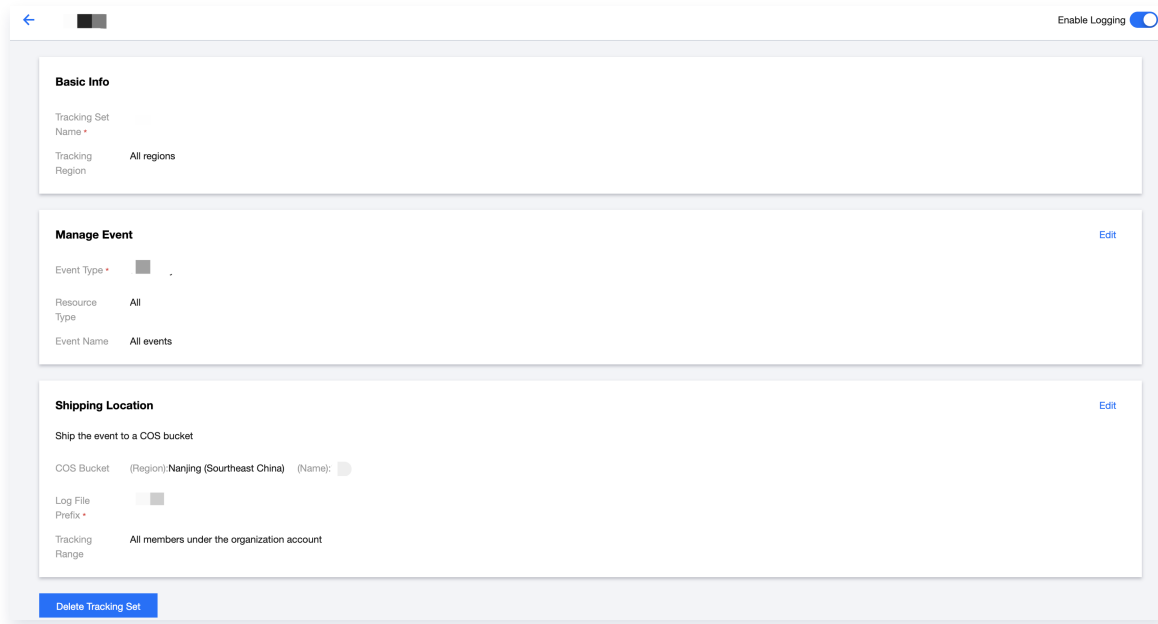
Shipping name	Bucket	Log file prefix	Status	Application scope
			Enable	All accounts

CloudAudit log shipping

Name	Tracked regions	Tracked resource t...	Application scope	COS bucket	CLS log topic	Log file prefix	Logging status
	All regions	All resource types	All accounts		-		Enable
	All regions	All resource types	All accounts		-		Enable
	All regions	All resource types	All accounts	-	Query and analysis		Enable

Managing the CloudAudit log shipping tracking set

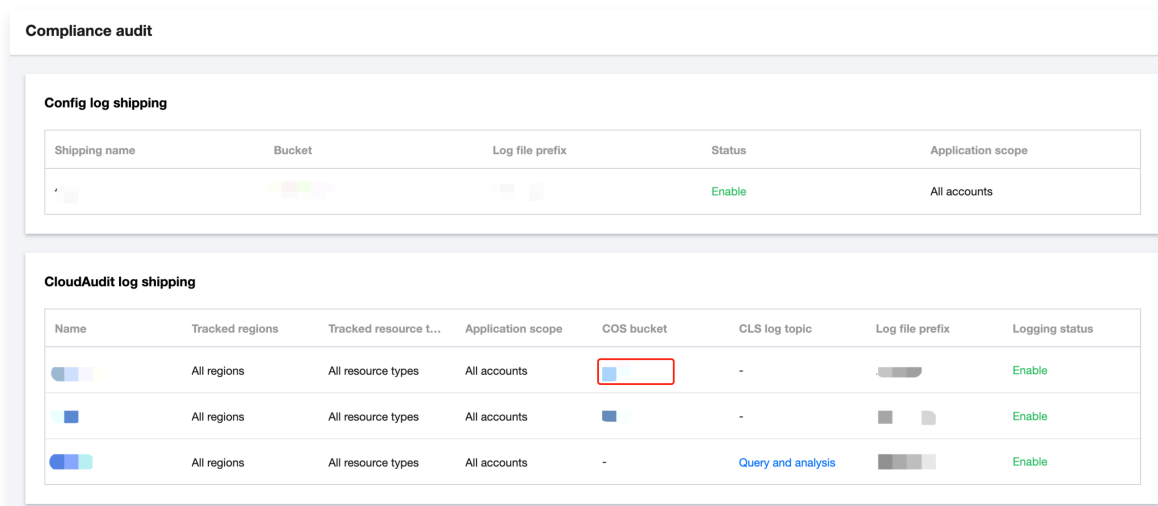
1. Click the **shipping name** in the CloudAudit log shipping list to open the **CloudAudit** > **Tracking set** page.
2. On the page that appears, you can view, edit, and delete the tracking set.



Managing CloudAudit log shipping COS buckets

A bucket is like a "container" for storing objects, and it has no upper limit for storage capacity. Objects are stored in buckets in a flat structure with no folders or directories. You can choose to store objects in one or multiple buckets.

1. Click the target **Cloud Object Storage (COS) bucket** in the CloudAudit log shipping list to open the **COS > Bucket List** page.



2. On the page that appears, you can manage buckets. For more information, see [Bucket Overview](#).

Managing CLS topics

A topic is the basic unit for collecting, storing, retrieving, and analyzing logs. You can manage the relevant topics in the compliance audit module.

1. Click **Query and analysis** for the target Cloud Log Service (CLS) topic in the CloudAudit log

shipping list to open the **CLS > Log Topic** page.

2. On the page that appears, you can view detailed information about the topic. For more information about the configuration, see [Managing Log Topic](#).

Cloud Security Center

Last updated: 2023-08-15 18:11:31

Overview

Cloud Security Center (CSC) is a one-stop security management platform provided by Tencent Cloud. CSC ensures security throughout your business operations by offering proactive threat detection, real-time incident response, and post-incident root cause analysis.

Prerequisites

You have set up a landing zone.

Directions

1. Log in to the Tencent Cloud console and go to the [Control Center](#) page. Click **Security center** in the left-side menu to open the **Security center > Multi-account management** page.
2. On the page that appears, you can submit tickets and create organizations. For more information, see [Multi-account Management](#).