

Resource Governance Center

Getting Started

Issue 02
Date 2025-02-20



Copyright © Huawei Technologies Co., Ltd. 2025. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Preparations.....	1
2 Setting Up and Enabling a Landing Zone.....	2
3 Using Governance Policies to Manage Your Landing Zone.....	9

1 Preparations

Before using RGC, you need to prepare as described in the following sections:

Enabling Enterprise Center

Before enabling RGC, you need to enable Enterprise Center and become the management account of your organization. Do as follows:

- Step 1** Go to the Enterprise Center console.
- Step 2** Click **Enable for Free**. The **Enable Enterprise Center** page is displayed.
- Step 3** Select **I have read and agree to the HUAWEI CLOUD Enterprise Management Service Agreement** and click **Enable for Free**. Your account will become an enterprise master account. For details, see [Enabling Enterprise Center](#).

----End

2 Setting Up and Enabling a Landing Zone

Background

With RGC:

- You will have the necessary permissions to govern all of the organizational units (OUs) and member accounts in your organization.
- You need to set up a landing zone in RGC and determine which OUs and member accounts to govern in the landing zone. RGC does not extend governance to other existing OUs or member accounts in your organization.
- When existing OUs are governed by RGC, they are called registered OUs.
- After your landing zone is set up, you can still register existing OUs in RGC.

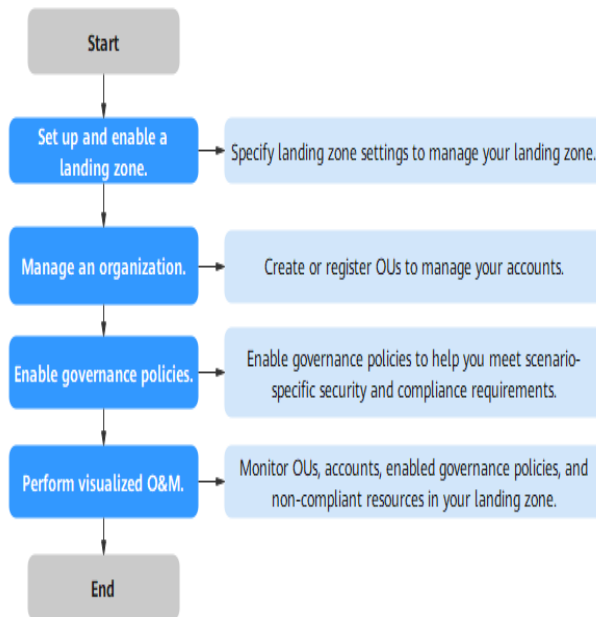
Prerequisites

The current account has enabled Enterprise Center. For details, see [Enabling Enterprise Center](#).

Getting Started

[Figure 2-1](#) shows the flowchart for using RGC.

Figure 2-1 Flowchart for using RGC



Setting Up a Landing Zone

- Step 1** Log in to Huawei Cloud using an enterprise master account.
- Step 2** Click ☰ and choose **Management & Governance > Resource Governance Center**.
- Step 3** Click **Enable**.

Figure 2-2 Enabling RGC



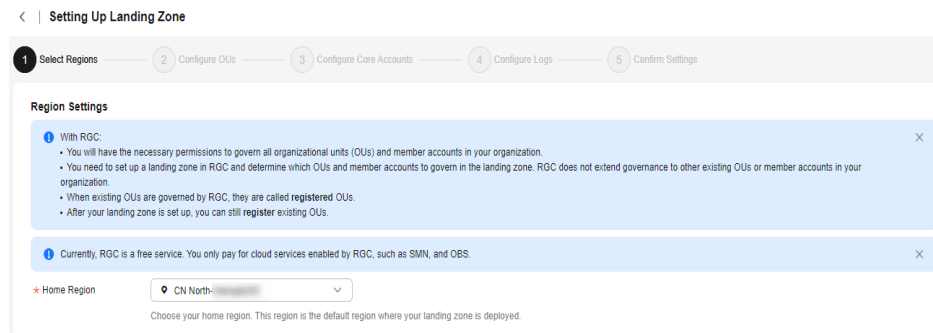
You have not set up a landing zone.

Resource Governance Center (RGC) helps you set up and govern a secure scalable multi-account cloud environment. With RGC and other Huawei Cloud services, such as Organizations, Config, and IAM Identity Center, you can establish a landing zone to centrally govern your resources.

Enable

- Step 4** Select the home region for RGC. The region will be the default region for your landing zone.

Figure 2-3 Selecting the home region



Step 5 Click **Next**.

Step 6 Under **OU Settings**, configure the core OU. You have two options for **Core OU**:

- **Create:** A core OU will be preset in RGC to build a complete OU structure in the landing zone. This OU contains two core accounts: a log archive account and a security audit account (also called an "audit account").
The OU name must be unique. The default name of the core OU is **Security**. Once your landing zone is set up, the name of the core OU cannot be changed.
- **Skip:** No core OU will be created in RGC.

Figure 2-4 Configuring the core OU

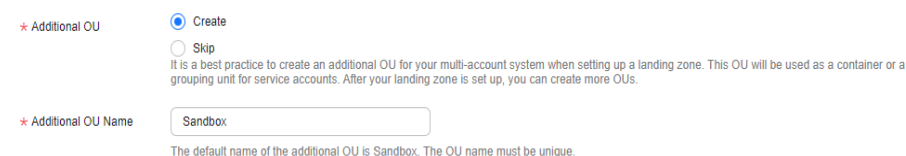


Step 7 Determine whether to create additional OUs.

To help set up a multi-account system, you are advised to create additional OUs when setting up a landing zone. Each OU functions as a container or grouping unit for service accounts. After your landing zone is set up, you can create more OUs. You have two options for **Additional OU**:

- **Create:** You will need to create an additional OU when you are setting up a landing zone. The OU name must be unique. The default name of the additional OU is **Sandbox**.
- **Skip:** There will be no other OUs except the preset core OU in your landing zone. You can create more OUs after your landing zone is set up.

Figure 2-5 Creating an additional OU

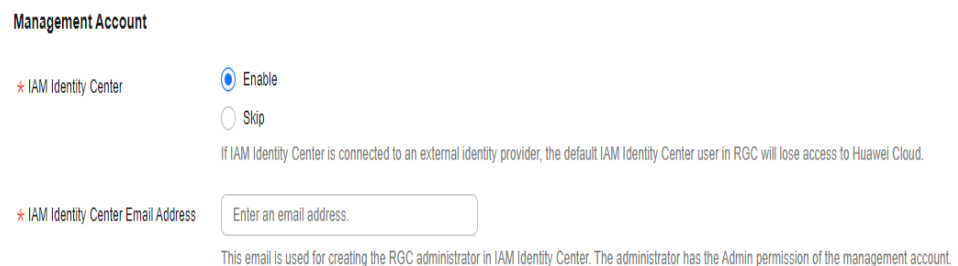


Step 8 Click **Next**.

Step 9 On the **Configure Core Accounts** page, configure the management account. You have two options for **IAM Identity Center**:

- **Enable:** You will need to enter the email address associated with the IAM Identity Center account. The email address of the management account must not be used for other IAM Identity Center users. It is used for creating the RGC administrator in IAM Identity Center. The administrator has the Admin permission.
- **Skip:** RGC will not create a user as the RGC administrator, any user groups, or permission sets in IAM Identity Center.

Figure 2-6 Configuring the management account



Management Account

* IAM Identity Center Enable Skip

If IAM Identity Center is connected to an external identity provider, the default IAM Identity Center user in RGC will lose access to Huawei Cloud.

* IAM Identity Center Email Address

This email is used for creating the RGC administrator in IAM Identity Center. The administrator has the Admin permission of the management account.

Step 10 Configure a log archive account. It is used to store logs of API activities and resource configurations from all accounts.

- Set **Account Type** to **Create new account**.
 - **Email Address:** Enter the email address of the log archive account. This email address cannot be currently used for any Huawei Cloud accounts. It can have a maximum of 64 characters.
 - **Account Name:** Specify a unique name for the log archive account. The name cannot be changed once your landing zone is set up. The account name can only contain digits, letters, underscores (_), and hyphens (-), and it cannot start with a digit. It can have 6 to 32 characters.
- Set **Account Type** to **Use existing account**.

The existing account you chose must belong to the organization of the management account, and an agency must have been set for the account. For details, see [Setting an Agency](#). If there are Config resources in the account, you must delete or modify them before enrolling the account in RGC when you are setting up a landing zone.

 - **Email Address:** Enter the email address of the log archive account. This email address cannot be currently used for any Huawei Cloud accounts. It can have a maximum of 64 characters.
 - **Account Name:** Enter the name of the account you have registered with Huawei Cloud.
 - **Account ID:** Enter the ID of the account you have registered with Huawei Cloud. The account ID cannot be the ID of the management account or of a member account in another organization.

Figure 2-7 Configuring a log archive account

Log Archive Account

* Account Type Create new account
 Use existing account
A log archive account is used to store logs of API activities and resource configurations from all accounts.

* Email Address
Enter an email address different from those used for existing Huawei Cloud accounts.

* Account Name
Enter a unique account name. The name cannot be changed once the log archive account is set up.

Step 11 Configure an audit account. The audit account has permission to access all member accounts in your organization. You are encouraged to strictly control the identity that uses this account.

- Set **Account Type** to **Create new account**.
 - **Alert Email:** Enter an email address for the audit account. It is used to receive alerts preset by RGC. This email address cannot be currently used for any Huawei Cloud accounts. It can have a maximum of 64 characters.
 - **Account Name:** Specify a unique name for the audit account. The name cannot be changed once your landing zone is set up. The account name can only contain digits, letters, underscores (_), and hyphens (-), and it cannot start with a digit. It can have 6 to 32 characters.
- Set **Account Type** to **Use existing account**.

The existing account you chose must belong to the organization of the management account, and an agency must have been set for the account. For details, see [Setting an Agency](#). If there are Config resources in the account, you must delete or modify them before enrolling the account in RGC when you are setting up a landing zone.

 - **Alert Email:** Enter an email address for the audit account. It is used to receive alerts preset by RGC. It can have a maximum of 64 characters.
 - **Account Name:** Enter the name of the account you have registered with Huawei Cloud.
 - **Account ID:** Enter the ID of the account you have registered with Huawei Cloud. The account ID cannot be the ID of the management account or of a member account in another organization.

Figure 2-8 Configuring an audit account

Audit Account

* Account Type Create new account
 Use existing account
The audit account has the permissions needed to access all member accounts in your organization. You are encouraged to strictly control the identity that uses this account.

* Alert Email
Enter an email address to receive preset RGC alarm notifications. It can have 6 to 36 characters.

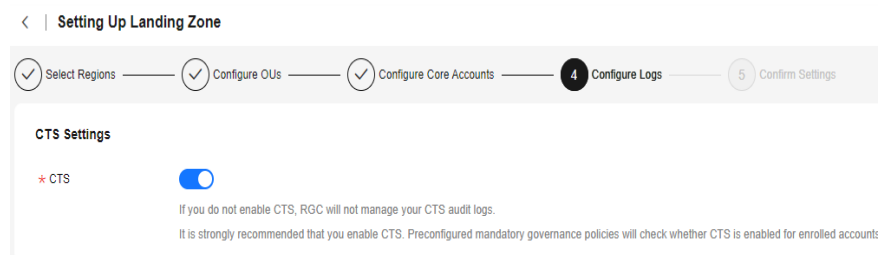
* Account Name
Enter a unique account name. The name cannot be changed once the audit account is set up.

Step 12 Click **Next**.

Step 13 Determine whether to enable CTS.

If you do not enable CTS, RGC will not manage your CTS audit logs. It is strongly recommended that you enable CTS. Preconfigured mandatory governance policies will check whether CTS is enabled for enrolled accounts.

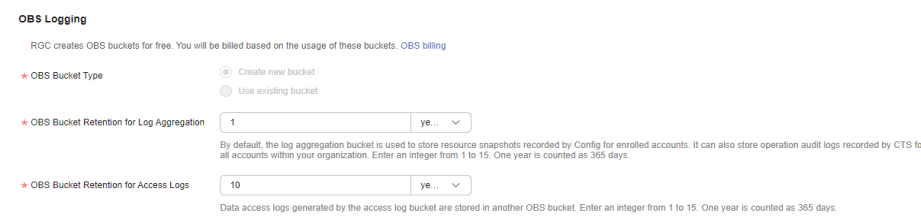
Figure 2-9 Enabling CTS



Step 14 Configure an OBS bucket for storing logs. You can create a new OBS bucket or use an existing one. If you chose to create a log archive account, you will also need to create an OBS bucket. Log data is encrypted with SSE-OBS, and the keys are created and managed by OBS.

- **Create new bucket:** If you choose this option, you need to configure a retention period for logs in the OBS bucket. Logs are automatically stored in the two default OBS buckets, and you cannot rename them.
 - **OBS Bucket Retention for Log Aggregation:** The default period is one year, but you can change this to up to 15 years.
This bucket is used to store operation audit logs recorded by CTS for all accounts in an organization and resource snapshots recorded by Config for managed accounts. It is stored in the bucket named **rgcservice-managed-audit-logs-*{Management account ID}***. ***{Management account ID}*** represents the actual ID of the management account.
 - **OBS Bucket Retention for Access Logs:** The default period is 10 years, but you can change this to up to 15 years.
The logs for accessing the log aggregation bucket are stored in the bucket **rgcservice-managed-access-logs-*{management account ID}***.
- **Use existing bucket:** If you choose this option, you need to enter the name of the OBS bucket created by the log archive account. If you use another bucket name, landing zone setup will fail. To ensure data security, you are advised to use a private OBS bucket.

Figure 2-10 Configuring the OBS bucket retention for logging

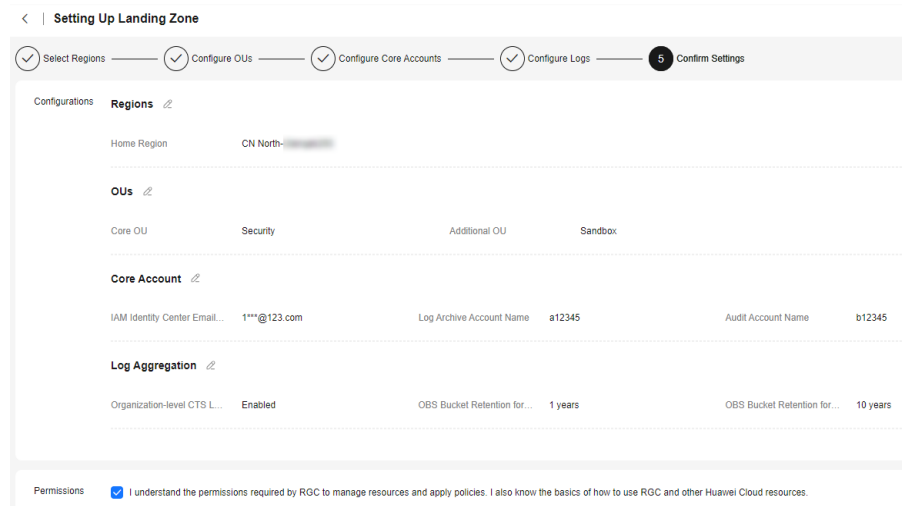


Step 15 Review and confirm the landing zone settings, and then select the checkbox **I understand the permissions required by RGC to manage resources and apply**

policies. I also know the basics of how to use RGC and other Huawei Cloud resources.

You can log in to the IAM console, choose **Identity Policies** in the navigation pane. On the displayed page, search for **RGCServiceAgencyPolicy** to view the permissions used by RGC to manage resources and enforce policies.

Figure 2-11 Confirming the landing zone settings



Step 16 Click **Set Up Landing Zone**.

NOTICE

The email address you configured for audit account alerts will receive a subscription confirmation email from the regions governed in RGC. If you want your audit account to receive such emails, click the confirmation link in each email from each region.

----End

Important Notes

- You also need to deploy and manage existing OUs and member accounts. For details, see [Organization Management](#).
- After your landing zone is set up, all preventive governance policies will be attached to the OU that the core account belongs to.
- After your landing zone is set up, the bucket policies **AllowCtsAccessBucket** and **AllowConfigAccessBucket** will be configured for the OBS bucket that stores logs. For details about the bucket policies, go to the OBS console.
- After your landing zone is set up, the object read permission will be configured for the OBS bucket that stores logs so that the core account has permission to view logs in the bucket.

3 Using Governance Policies to Manage Your Landing Zone

RGC provides multiple types of governance policies. Mandatory governance policies are automatically applied to OUs created in RGC. You can use the management account to enable strongly recommended or elective governance policies as needed.

You need to register the OUs created in an organization before applying governance policies to them.

Preventive governance policies apply to all member accounts in the OUs, regardless of their enrollment status. Detective governance policies apply only to enrolled accounts.

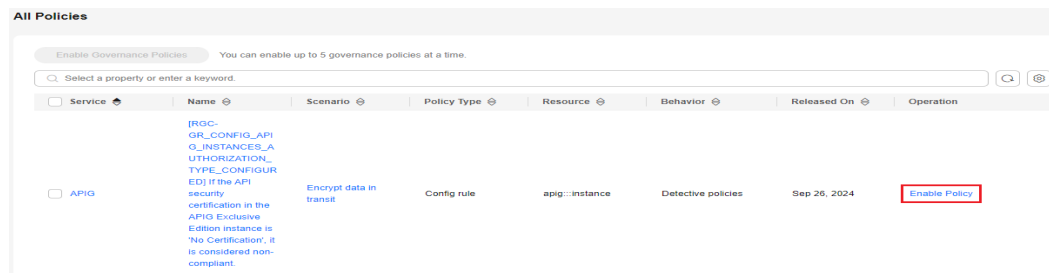
Constraints

- You can only manually enable or disable strongly recommended and elective governance policies.
- Governance policies cannot be attached to the root OU, core OU, or any unregistered OUs.

Enabling a Governance Policy

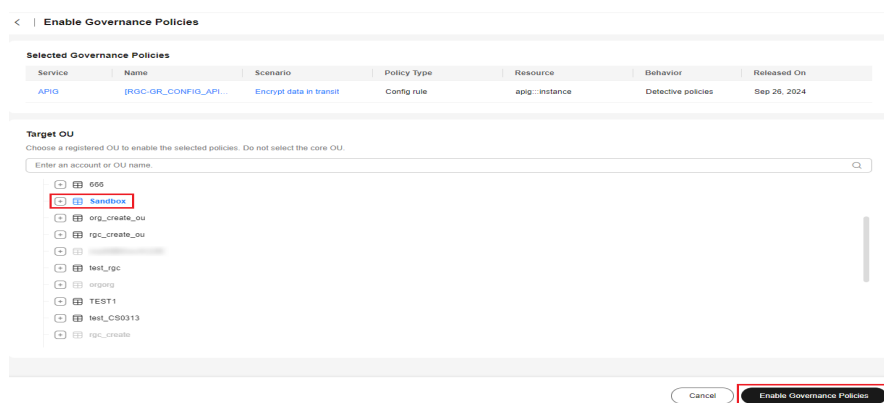
- Step 1** Log in to Huawei Cloud using the management account, and navigate to the RGC console.
- Step 2** Choose **Governance Policy Library > All Policies**. In the policy list, locate the governance policy you want to enable.
- Step 3** Click **Enable Policy** in the **Operation** column.

Figure 3-1 Enabling governance policies



Step 4 Select an OU that you want to enable this policy for.

Figure 3-2 Selecting an OU



Step 5 Click **Enable Governance Policies** in the lower right corner. This may take several minutes.

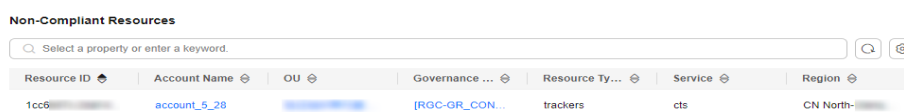
----End

Viewing How a Governance Policy Is Applied

- Step 1** Log in to Huawei Cloud using the management account, and navigate to the RGC console.
- Step 2** On the **Dashboard** page, view details of **OUs and Accounts**, **Enabled Governance Policies**, **Non-Compliant Resources**, **Registered OUs**, and **Enrolled Accounts** in your landing zone.
- Step 3** Under **Non-Compliant Resources**, click an account name to view the details about non-compliant resources.

You can use the management account to handle the non-compliant resources.

Figure 3-3 Non-compliant resources

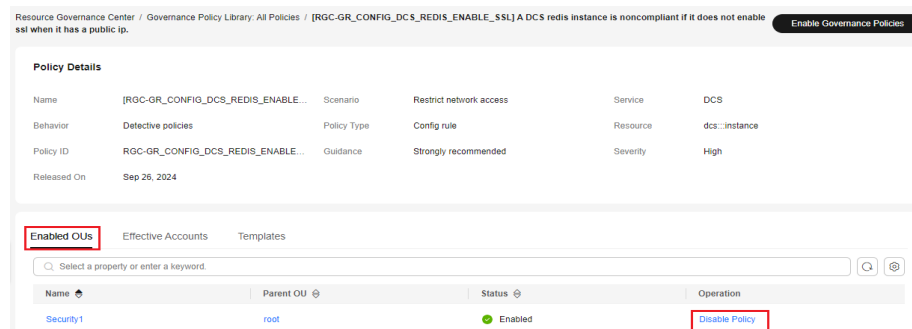


----End

Disabling a Governance Policy

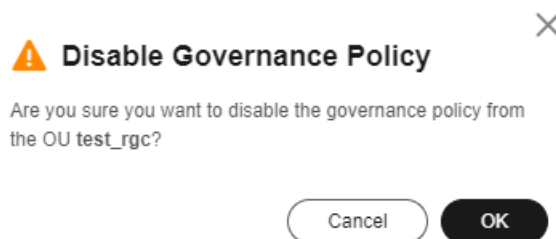
- Step 1** Log in to Huawei Cloud using the management account, and navigate to the RGC console.
- Step 2** Choose **Governance Policy Library > All Policies**. In the policy list, locate the governance policy you want to disable.
- Step 3** Click the policy name. The policy details are displayed.
- Step 4** On the **Enabled OUs** page, choose the OU that you want to disable this policy from.

Figure 3-4 Disabling a governance policy



- Step 5** Click **Disable Policy** in the **Operation** column.
- Step 6** Click **OK**. This may take several minutes.

Figure 3-5 Disabling a governance policy



----End