Organizations

Getting Started

Issue	01
Date	2025-06-03

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Copyright © Huawei Cloud Computing 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 Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions

and other Huawei trademarks are the property 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 Cloud 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 Using Organizations to Manage Multiple Accounts..... 1
2 Using SCPs to Control Permissions of Member Accounts..... 8
3 Using Tag Policies to Standardize Resource Tags..... 13
4 Enabling Trusted Services to Provide Organization-wide Capabilities..... 17

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1 Using Organizations to Manage Multiple Accounts

Scenarios

The Organizations service helps you govern multiple accounts within your organization. If your enterprise has multiple branches, departments, or different service applications, you can use Organizations to build a hierarchical cloud resource structure that aligns with your own management and operational methods. By using this service, you can create an organization to consolidate and centrally manage multiple Huawei Cloud accounts that would otherwise be scattered.

The following describes how to create an organization and organizational units (OUs) and how to invite accounts to join an organization, so you can manage multiple accounts in a structured manner.

Procedure

Step	Description
Preparations	1. Sign up for a HUAWEI ID, enable Huawei Cloud services, and complete enterprise real-name authentication. 2. Enable Enterprise Center and become a master account. 3. Top up your account to ensure that the account is not frozen due to arrears.
Step 1: Create an Organization	Create an organization.
Step 2: Create OUs	Create multi-level OUs for the organization.
Step 3: Invite Accounts to Join Your Organization	(Organization management account) Invite other accounts to join the organization.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step	Description
Step 4: Move Accounts	Move member accounts to other OUs.

Preparations

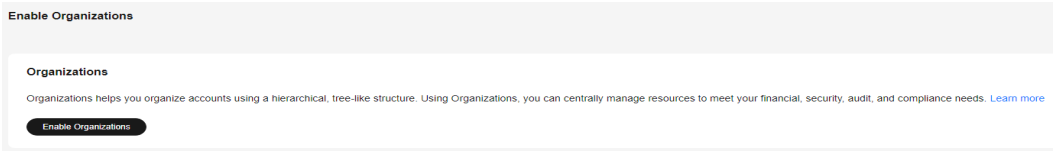
1. Sign up for a HUAWEI ID, enable Huawei Cloud services, and complete enterprise real-name authentication.
   a. Visit the Huawei Cloud official website and click **Sign Up** in the upper right corner.
   b. Complete the registration by following the instructions. For details, see Signing Up for a HUAWEI ID and Enabling Huawei Cloud Services.
      After the sign-up is complete, you will be redirected to your personal information page.
   c. Complete real-name authentication by following the instructions in Enterprise Real-Name Authentication.
2. Enable Enterprise Center and become a master account.
   Before creating an organization, you need to enable Enterprise Center and become an enterprise master account by following these steps:
   a. Access the Enterprise Center console.
   b. Click **Enable for Free**. The **Enable Enterprise Center** page is displayed.
   c. Select **I have read and agree to Huawei Cloud Enterprise Management Service Agreement** and click **Enable Now**.
      After you enable Enterprise Center, you will automatically become an enterprise master account.
3. Top up your account.
   Organizations is a free service. You will not be billed for using Organizations-related functions.
   Ensure that your account balance is sufficient. If your account is frozen due to arrears, you cannot perform any write operations on the Organizations console. For details about how to top up your account, see Topping Up an Account.

Step 1: Create an Organization

Step 1 Log in to the management console.

Step 2 Click in the upper left corner. In the service list, choose **Management & Governance** > **Organizations**.

Step 3 Click **Enable Organizations**.



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

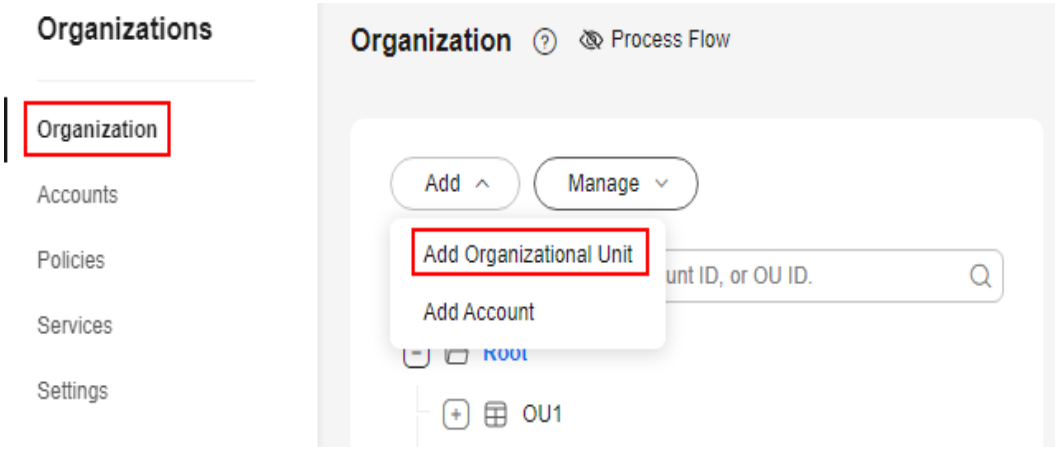
After the Organizations service is enabled, your organization and the root are automatically created, and your login account is defined as the management account.

----End

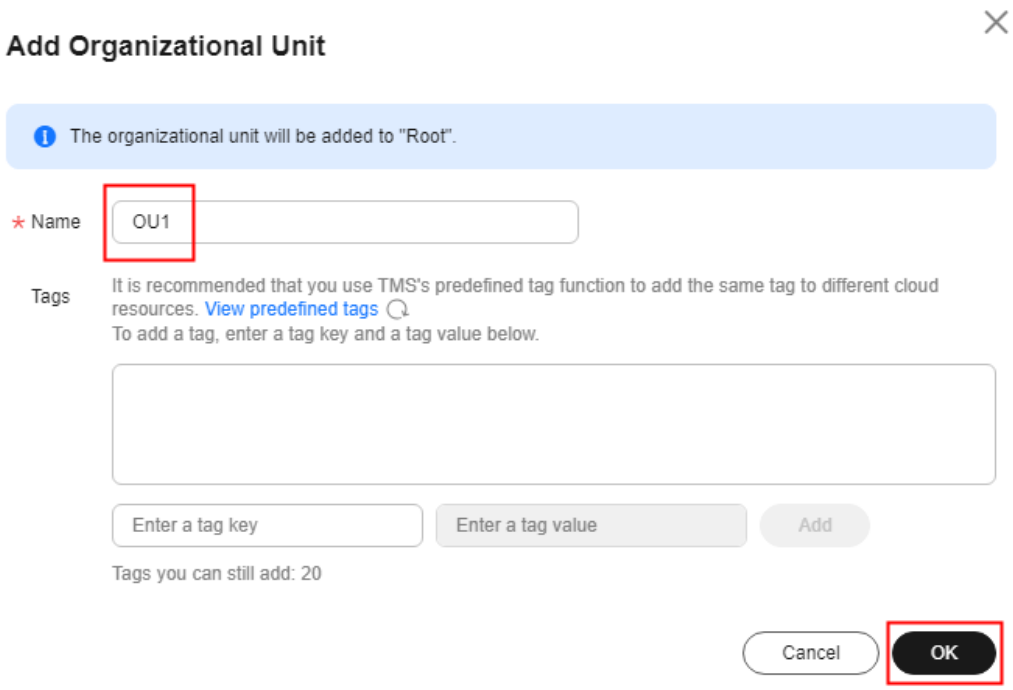
Step 2: Create OUs

You can create OUs and place your accounts in the OUs to group the accounts by a specific dimension, for example, by service scope, account owner, or application environment. The following provides an example of creating multi-level OUs. Up to five OU levels are supported.

Step 1 Access the Organizations console. On the **Organization** page, select the root OU, and choose **Add** > **Add Organizational Unit**.

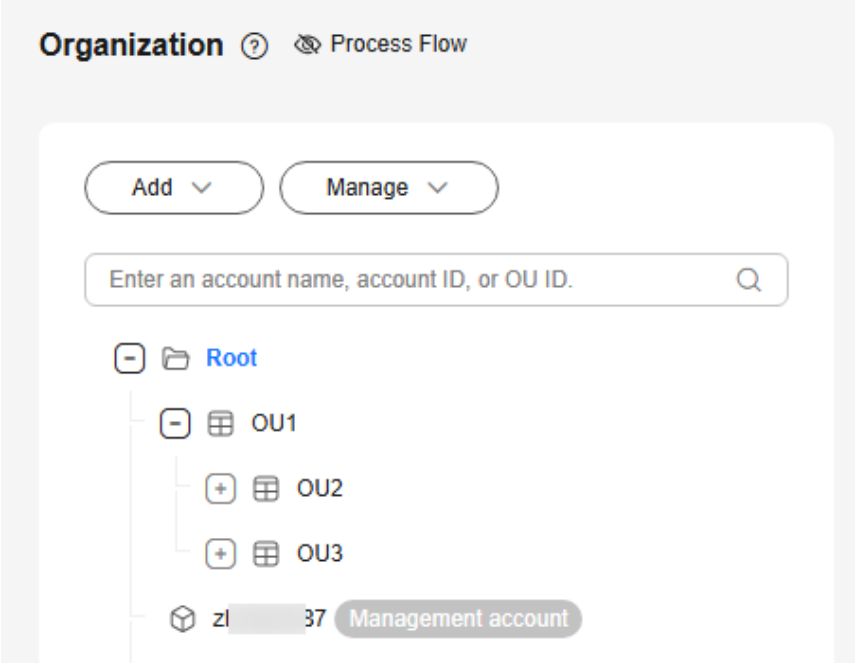


Step 2 Enter the OU name (**OU1** in this example) and click **OK** in the displayed dialog box.



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 3 Select **OU1** and repeat the preceding steps to create its child OUs (**OU2** and **OU3** in this example). The following figure shows the organizational structure.



----End

Step 3: Invite Accounts to Join Your Organization

Now that you have an organization, you can begin to populate it with accounts. In this step, you invite existing accounts to join as members of your organization. You can also create accounts in your organization, and the accounts will automatically become part of your organization. For details, see Creating an Account.

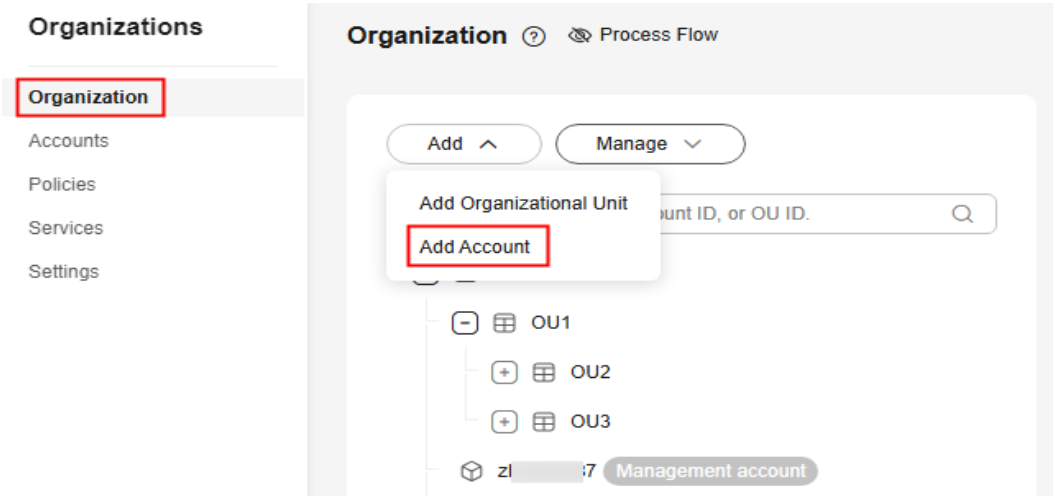
NOTE

The accounts you invite to join your organization must have completed enterprise or individual real-name authentication. For details, see Real-Name Authentication.

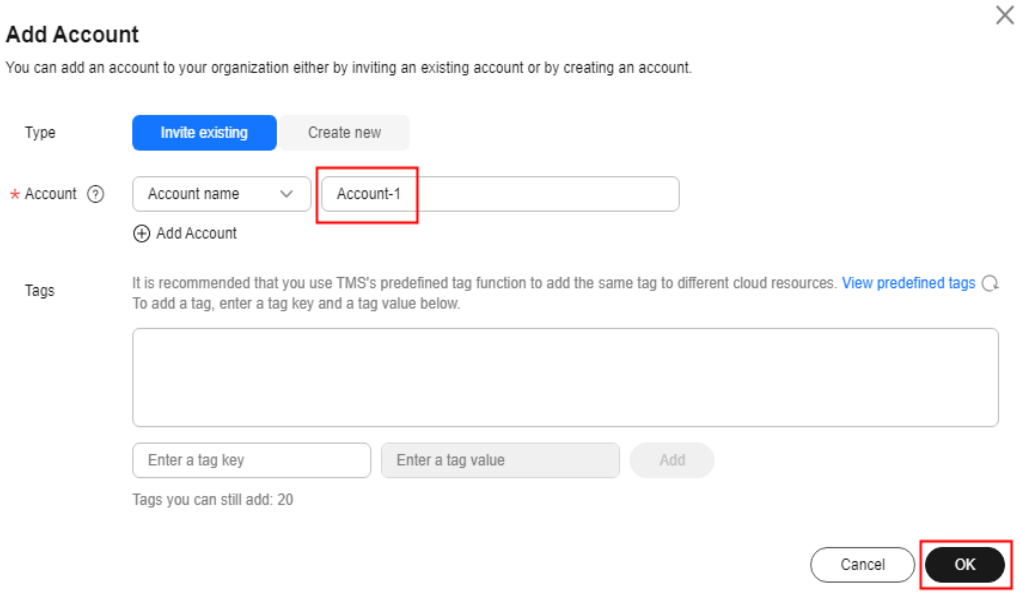
The original accounting relationship (master-member association) of invited accounts will remain unchanged.

Step 1 Access the Organizations console. On the **Organization** page, choose **Add** > **Add Account**.

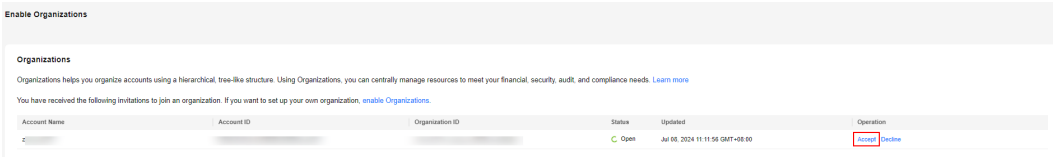
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.



Step 2 In the displayed dialog box, enter the name of the account you are inviting, for example, **Account-1**. Click **OK**. An invitation to join the organization will be sent to the account.



Step 3 Switch to the account **Account-1**, access the Organizations console, and click **Accept**. **Account-1** will join the organization.



Step 4 Repeat the preceding steps to invite more accounts to join the organization.

----End

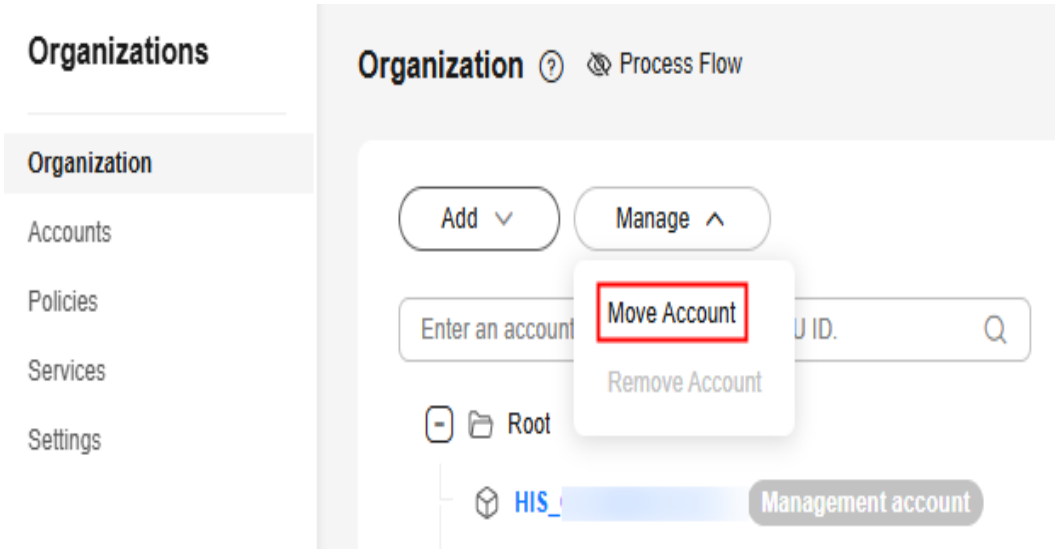
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 4: Move Accounts

By default, invited member accounts are placed under the organization root. You can log in as the organization management account to move the accounts to other OUs, so you can manage them more effectively.

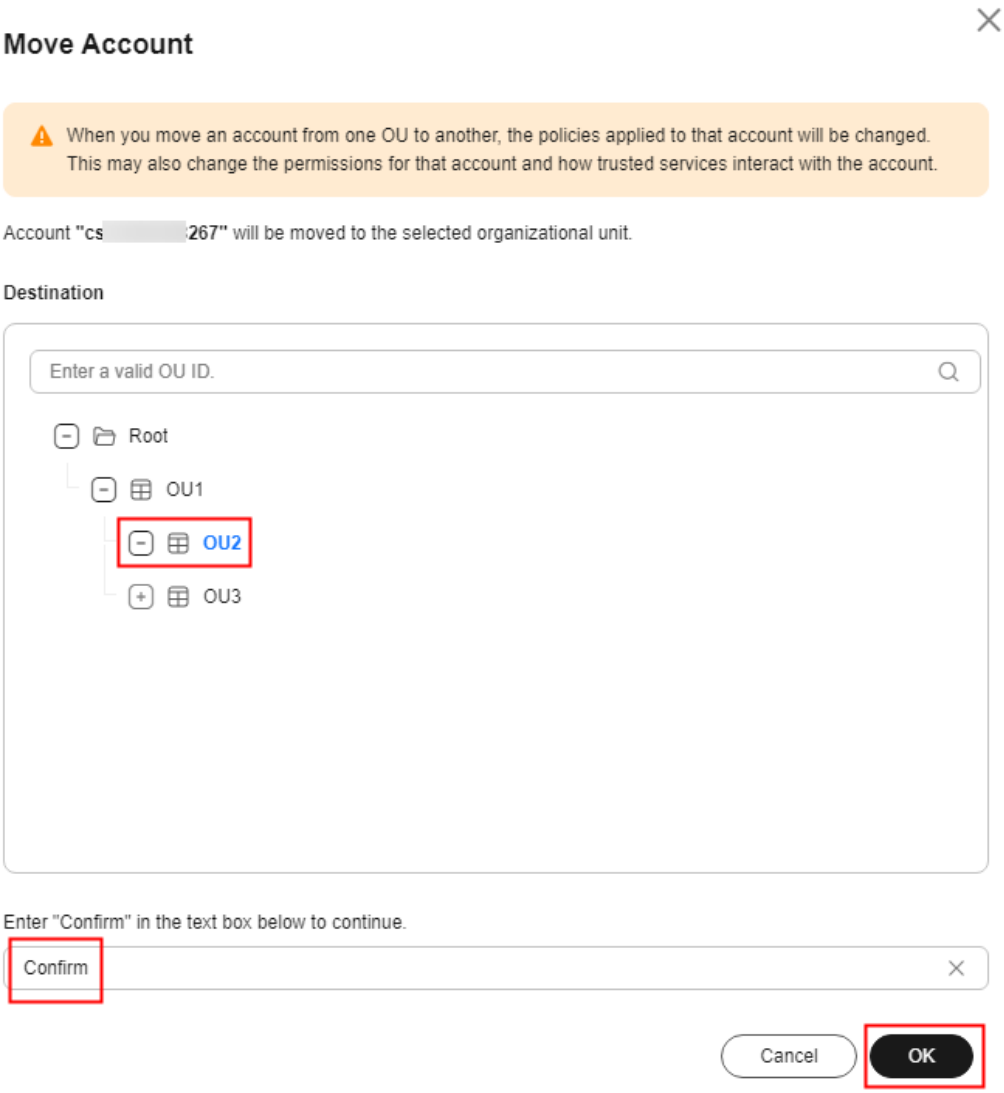
Step 1 Log in to the Huawei Cloud console using the organization management account.

Step 2 Access the Organizations console. On the **Organization** page, select the account you want to move, and choose **Manage** > **Move Account**.



Step 3 Select the OU (**OU2** in this example) you choose to hold the account, and enter "Confirm" in the text box. Then, click **OK**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.



Step 4 Repeat the preceding steps to move more accounts to other OUs.

----End

Follow-up Operations

After you create an organization, you can add, delete, modify, and query OUs and member accounts at any time. If you no longer need the organization, you can choose to delete it. The following links are for your reference:

- Managing Organizations
- Managing OUs
- Managing Accounts

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

2 Using SCPs to Control Permissions of Member Accounts

Scenarios

Service control policies (SCPs) are a type of organization policy that you can use to manage permissions in your organization. The organization management account can use SCPs to limit which permissions can be assigned to member accounts to ensure that they stay within your organization's access control guidelines. SCPs can be attached to an organization, OUs, and member accounts. Any SCP attached to an organization or OU affects all the accounts within the organization or under the OU.

The following describes how to create a service control policy (SCP) and attach it to a member account.

Procedure

Step	Description
Preparations	1. Create an organization and add a member account to the organization. 2. Top up your account to ensure that the account is not frozen due to arrears.
Step 1: Enable the SCP Type and Create an SCP	Enable the SCP type and create a custom SCP.
Step 2: Attach the SCP	Attach the SCP to the member account.
Step 3: Test the SCP Effect	Use the member account to test the SCP effect.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Preparations

1. Create an organization and add one or more member accounts to the organization. For details, see **Using Organizations to Manage Multiple Accounts**.
2. Top up your account.

   Organizations is a free service. You will not be billed for using Organizations-related functions.

   Ensure that your account balance is sufficient. If your account is frozen due to arrears, you cannot perform any write operations on the Organizations console. For details about how to top up your account, see Topping Up an Account.

Step 1: Enable the SCP Type and Create an SCP

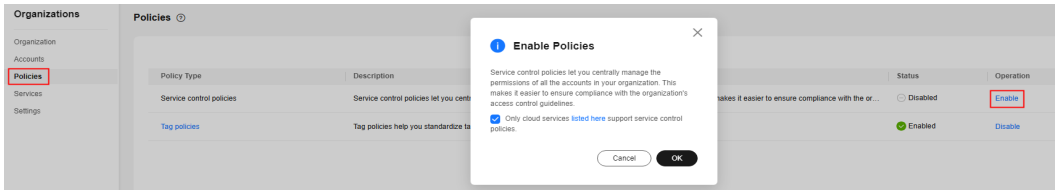
If you want to prevent a member account in your organization from deleting RAM resource shares, you can create an SCP similar to the example SCP provided below.

The following example only focuses on key parameter settings. You can retain the default values of other parameters. For more information about SCPs, see Creating an SCP.

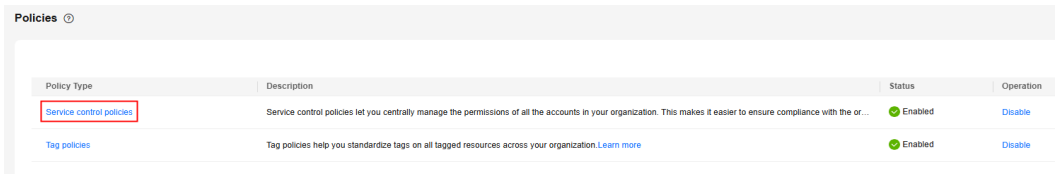
Step 1 Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

Step 2 In the navigation pane, choose **Policies**. On the displayed page, locate **Service control policies** and click **Enable** in the **Operation** column.

Step 3 In the displayed dialog box, select the check box and click **OK**.



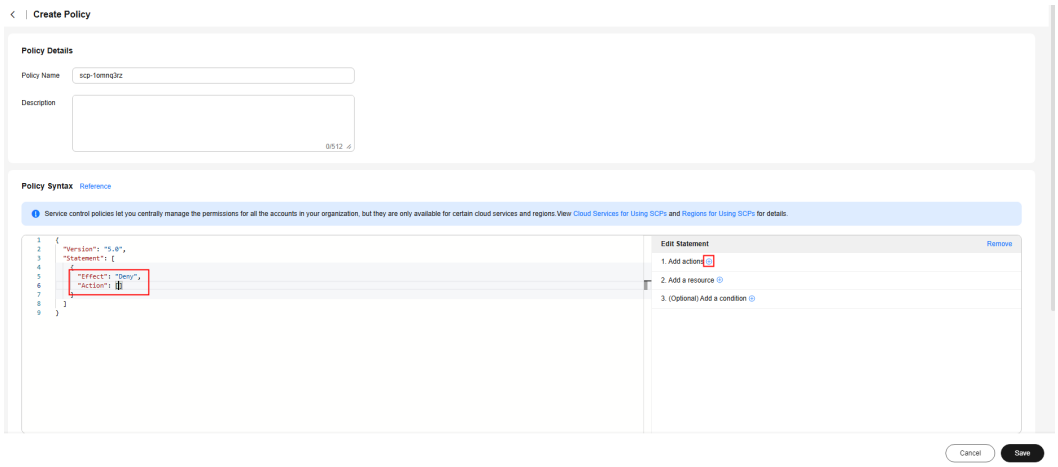
Step 4 Click **Service control policies**. The **Service control policies** page is displayed.



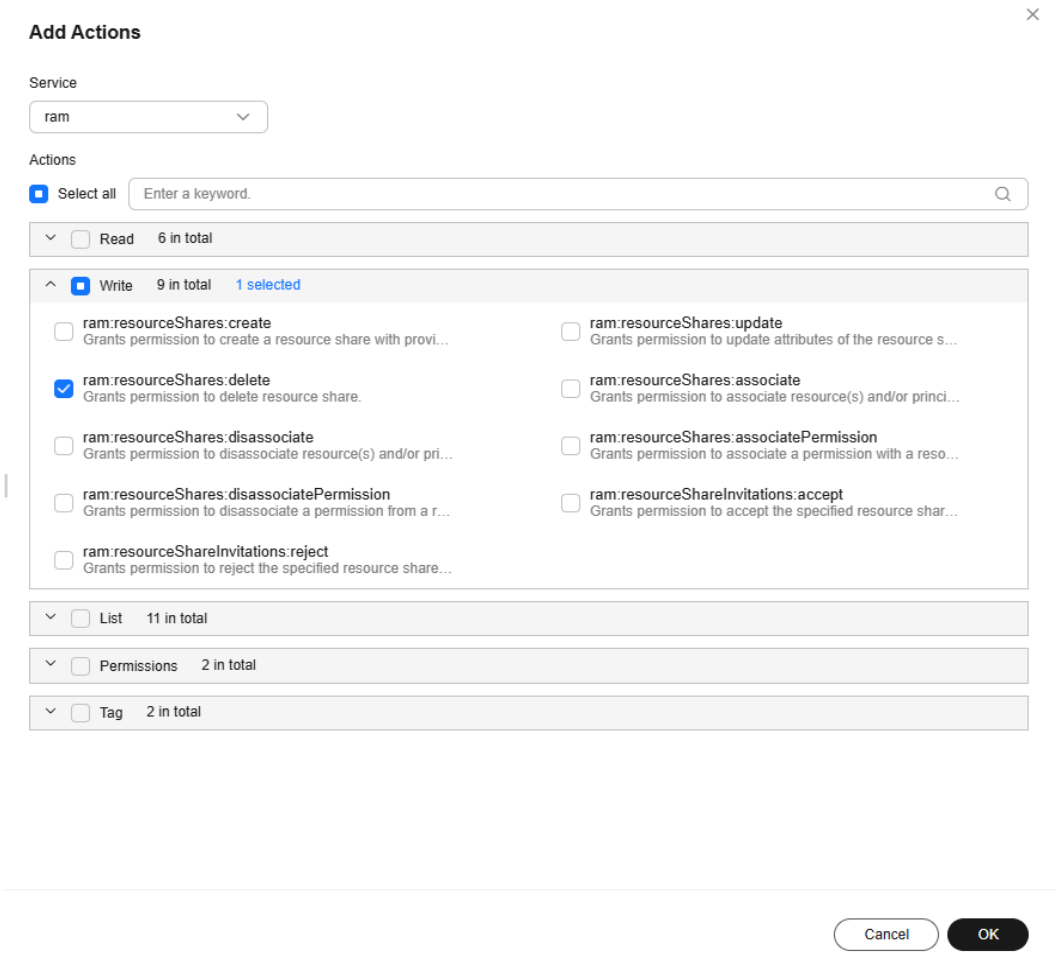
Step 5 Click **Create**. The **Create Policy** page is displayed.

Step 6 Under **Policy Syntax**, click "Effect" or "Action" in the policy statement, and then click the plus sign (+) next to **Add actions** in the policy editor on the right pane.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

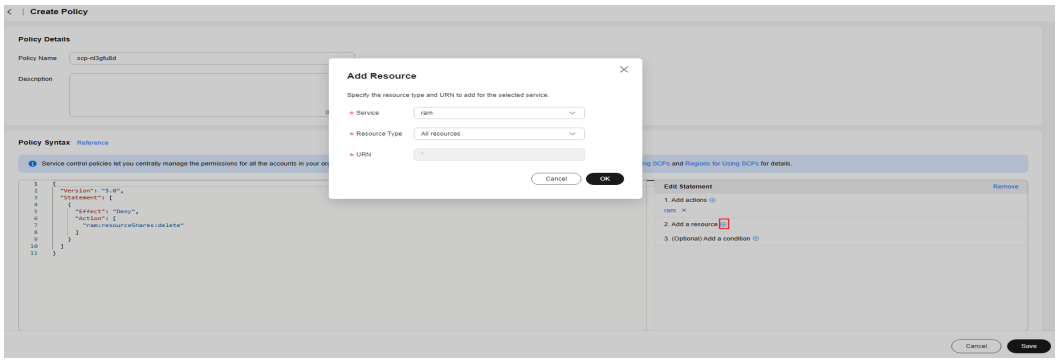


Step 7 In the displayed dialog box, select the action **ram:resourceShares:delete**. Then, click **OK**.



Step 8 Click the plus sign (+) next to **Add resources**. In the displayed dialog box, set **Service** to **ram** and **Resource Type** to **All resources**, and click **OK**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.



The final policy content is as follows:

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:resourceShares:delete"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Step 9 Click **Save** in the lower right corner of the page.

----End

Step 2: Attach the SCP

If you attach the SCP to a member account, the member account cannot delete any resource shares.

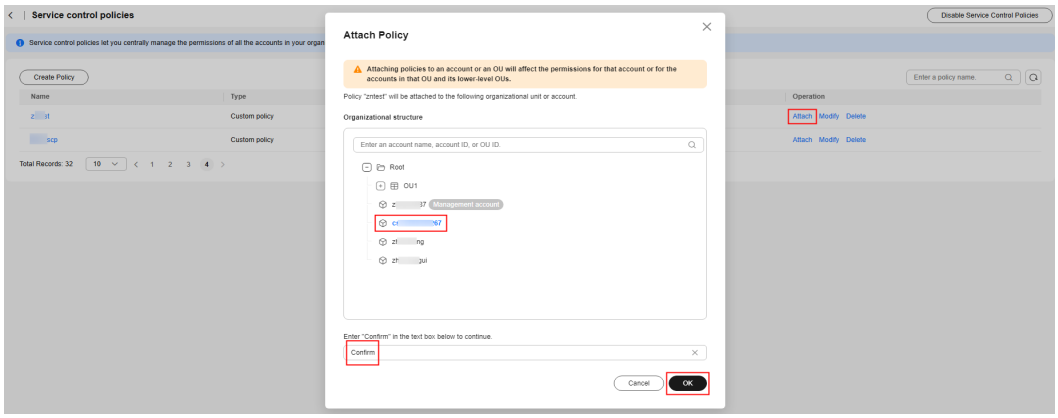
Step 1 In the SCP list, locate the SCP you created and click **Attach** in the **Operation** column.

Step 2 Select the member account you want to attach the SCP to and enter "Confirm" in the text box. Then, click **OK**.

NOTICE

The SCP will be applied within 30 minutes.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.



----End

Step 3: Test the SCP Effect

Perform the following steps to test the SCP Effect:

Step 1 Log in to the management console as the member account with the SCP attached and access the RAM console.

Step 2 Try to delete a resource share. If an error message is displayed, the SCP has been applied.

----End

Follow-up Operations

If you want to use SCPs to impose more complex permission control, see the following references:

- For details about SCPs, see SCP Principles and SCP Syntax, where there are also descriptions and examples of global condition keys and operators available for policy statements.
- For details about the services that support SCPs, see Cloud Services for Using SCPs. For details about actions, resource types, and service-level condition keys supported by cloud services, see Actions Supported by SCP-based Authorization.
- For details about SCP examples, see Example SCPs.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

3 Using Tag Policies to Standardize Resource Tags

Scenarios

Tag policies are a type of policy that can help you standardize tags across resources in your organization's accounts. In a tag policy, you specify tagging rules applicable to resources when they are tagged. Untagged resources and tags that are not defined in the tag policy are not evaluated for compliance with the tag policy.

To standardize the usage of tags in your organization, you can create a tag policy to formulate tag rules.

The following describes how to create a tag policy and attach it to a member account.

Procedure

Step	Description
Preparations	1. Create an organization and add a member account to the organization. 2. Top up your account to ensure that the account is not frozen due to arrears.
Step 1: Enable the Tag Policy Type and Create a Tag Policy	Enable the tag policy type and create a tag policy.
Step 2: Attach the Tag Policy	Attach the tag policy to a member account.
Step 3: Test the Tag Policy Effect	Use the member account to test the tag policy effect.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Preparations

1. Create an organization and add one or more member accounts to the organization. For details, see **Using Organizations to Manage Multiple Accounts**.
2. Top up your account.

   Organizations is a free service. You will not be billed for using Organizations-related functions.

   Ensure that your account balance is sufficient. If your account is frozen due to arrears, you cannot perform any write operations on the Organizations console. For details about how to top up your account, see Topping Up an Account.

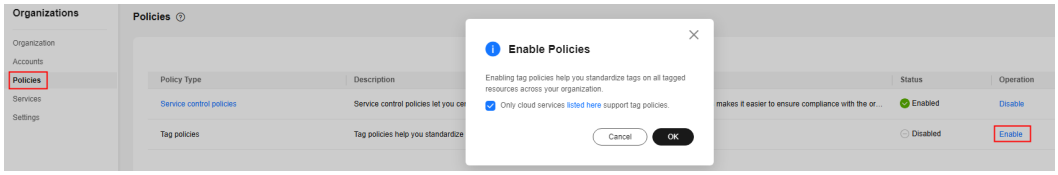
Step 1: Enable the Tag Policy Type and Create a Tag Policy

The following example only focuses on key parameter settings. You can retain the default values of other parameters. For more information about creating tag policies, see Creating a Tag Policy.

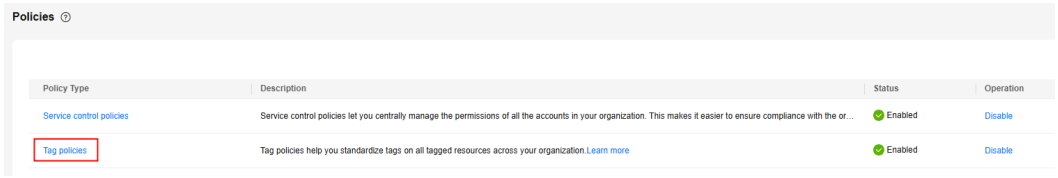
Step 1 Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

Step 2 On the **Policies** page, locate **Tag policies**, and click **Enable** in the **Operation** column.

Step 3 In the displayed dialog box, select the check box and click **OK**.



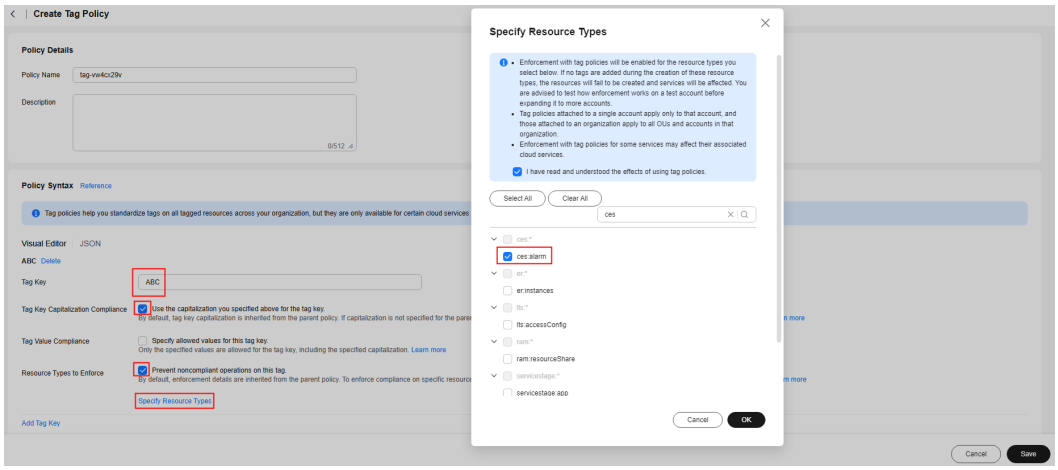
Step 4 Click **Tag policies**. The list of tag policies is displayed.



Step 5 Click **Create Policy**. The **Create Tag Policy** page is displayed.

Step 6 Set parameters for the tag policy based on the table below, and retain the default values for other parameters.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.



Parameter	Example	Setting
Tag Key	**ABC**	Enter the key (**ABC** in this example) for the tag you want to define in the tag policy. The tag policy will apply only to tags with this tag key.
Tag Key Capitalization Compliance	**Selected**	Use the capitalization you specified for the tag key for compliance check. If you select this option, tag keys in all uppercase characters like **ABC** are considered compliant, and those in all lowercase characters like **abc** or both uppercase and lowercase characters (such as **Abc**) are considered non-compliant. The tag policy will prevent you from adding any non-compliant tags to your resources.
Resource Types to Enforce	**ces:alarm**	Specify resource types to enforce the tag policy. Select the **Prevent noncompliant operations on this tag.** option and click **Specify Resource Types**. In the displayed dialog box, read and confirm the effects of using tag policies. Then, select resource types and click **OK**.

Step 7 Click **Save** in the lower right corner.

----End

Step 2: Attach the Tag Policy

After a tag policy is bound to a member account, the member account must comply with the tag specifications defined by the tag policy when adding tags to related resources.

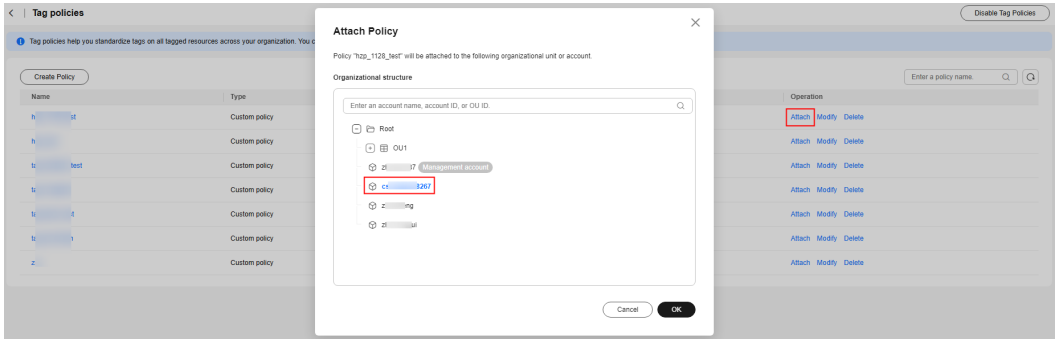
Step 1 In the tag policy list, locate the tag policy you created and click **Attach** in the **Operation** column.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 2 In the displayed dialog box, select the member account you want to attach the tag policy to and click **OK**.

NOTICE

The SCP will be applied within 30 minutes.



----End

Step 3: Test the Tag Policy Effect

Perform the following steps to test the tag policy effect.

Step 1 Log in to the management console as the member account with the tag policy attached. Access the Cloud Eye console, create an alarm rule, and add a tag to the alarm rule to check whether the tag policy is in effect.

1. If you add the tag **ABC** to the alarm rule, the operation will be successful.
2. If you add tag **abc** to the alarm rule, an error will be displayed, indicating that the tag is non-compliant. In this case, you need to modify the tag and try again until it becomes compliant.

CAUTION

If you try to add tags that do not comply with the tag policy during resource creation, the operation will be blocked by the tag policy, and the resources will not be created.

If you try to add tags that do not comply with the tag policy to ongoing resources, the operation will be blocked by the tag policy, but the resources will not be affected.

----End

Follow-up Operations

For details about other operations on tag policies, see Managing Tag Policies.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4 Enabling Trusted Services to Provide Organization-wide Capabilities

Scenarios

A trusted service is a Huawei Cloud service that is entrusted by Organizations to provide organization-wide capabilities. The management account can enable a cloud service as a trusted service with Organizations. Each trusted service has access to the information about the OUs and member accounts in your organization and also can manage the entire organization.

The following uses Config as an example to describe how to use a trusted service, including how to enable trusted access and create an organization compliance rule of Last Login Check.

Procedure

Step	Description
Preparations	1. Create an organization and add a member account to the organization. 2. Enable the resource recorder of Config. 3. Top up your account to ensure that the account is not frozen due to arrears.
Step 1: Enable Trusted Access	Enable trusted access for Config.
Step 2: Create Organization Rules	Use organization-wide capabilities to create organization rules in Config.

Preparations

1. Create an organization and add multiple member accounts to the organization. For details, see **Using Organizations to Manage Multiple Accounts**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

2. Enable the resource recorder so that the organization rule to be created can apply to the resources collected by the resource recorder.
3. Top up your account.

   Organizations is a free service. You will not be billed for using Organizations-related functions.

   Ensure that your account balance is sufficient. If your account is frozen due to arrears, you cannot perform any write operations on the Organizations console. For details about how to top up your account, see Topping Up an Account.

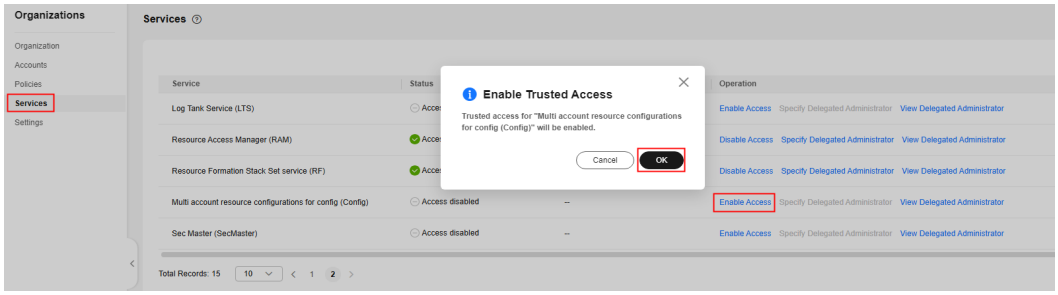
Step 1: Enable Trusted Access

Step 1 Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

Step 2 In the navigation pane, choose **Services**.

Step 3 On the **Services** page, locate Config and click **Enable Access** in the **Operation** column.

Step 4 Click **OK** in the displayed dialog box.



----End

Step 2: Create Organization Rules

As Config is now a trusted service with Organizations, you can use organization-wide capabilities in Config. This step provides an example of how to use Config to create organization rules.

The following example only focuses on key parameter settings. You can retain the default values of other parameters. For details about Config organization rules, see Organization Rules.

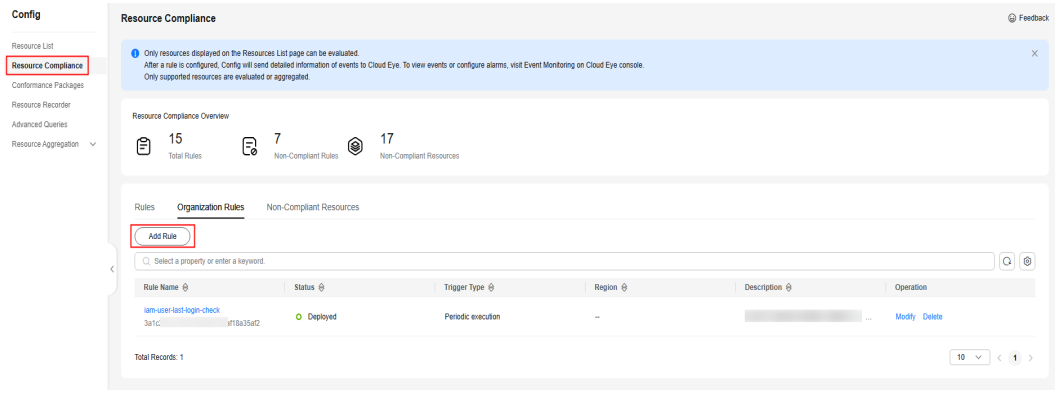
Step 1 Log in to the management console as an organization administrator or the delegated administrator of Config.

Step 2 Click ☰ in the upper left corner. In the service list, choose **Management & Governance** > **Config**.

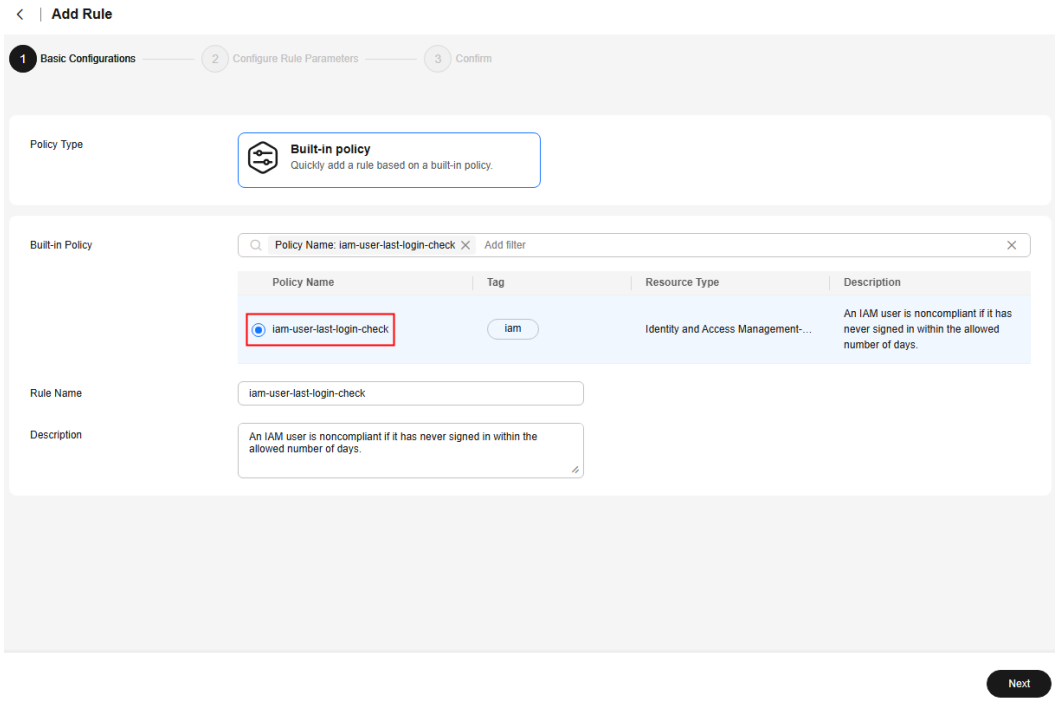
Step 3 In the navigation pane, choose **Resource Compliance**.

Step 4 Under **Organization Rules**, click **Add Rule**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

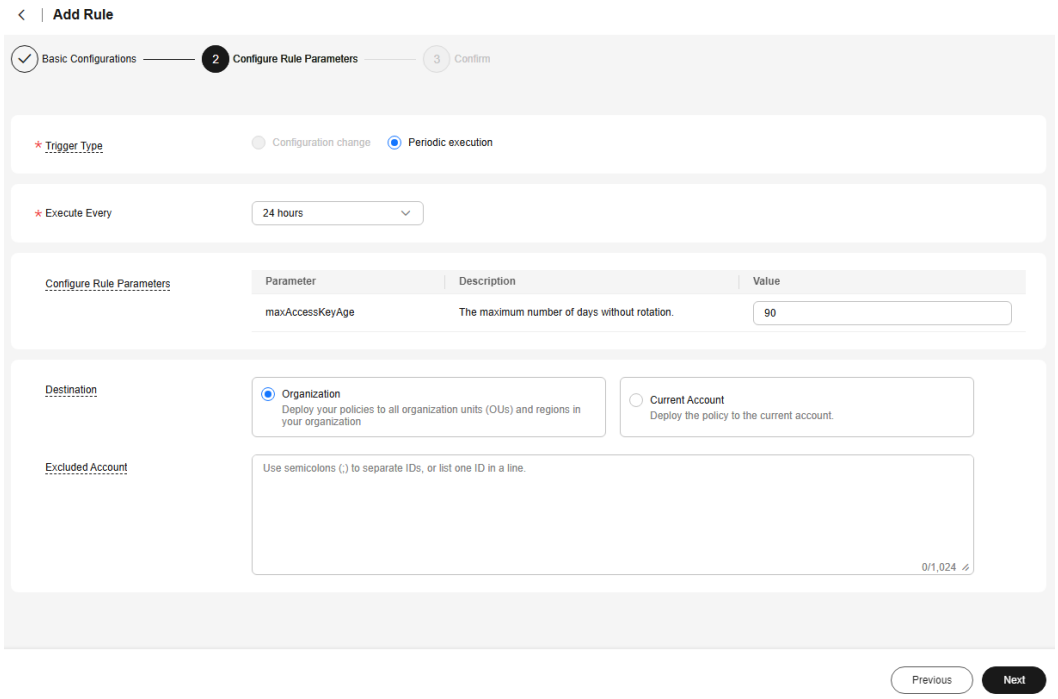


Step 5 On the **Basic Configurations** page, select the **iam-user-last-login-check** policy and click **Next**.



Step 6 On the **Configure Rule Parameters** page, retain the default value **Organization** for **Destination**, and click **Next**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.



Step 7 On the **Confirm** page, review and confirm the rule parameter settings, and click **Submit**.

NOTE

The organization rule you created will appear in the rule list of every member account in the organization. The rule name will have the prefix "Org-".

Only the account that created the rule can modify and delete it. The member accounts can evaluate the rule, view the result, and access the details.

----End

Follow-up Operations

For more information about trusted services integrable with Organizations and how to specify a delegated administrator, see Managing Trusted Services.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.