

# Alibaba Cloud Resource Access Management

## User Guide

Issue: 20190816

## Legal disclaimer

---

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.



## Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 <b>Danger:</b> Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 <b>Warning:</b> Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 <b>Notice:</b> Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 <b>Note:</b> You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
<b>Bold</b>	It is used for buttons, menus, page names, and other UI elements.	Click OK.
Courier font	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[ ] or [a b]	It indicates that it is a optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<b><code>{}</code> or <code>{a b}</code></b>	It indicates that it is a required value, and only one item can be selected.	<code>swich {stand   slave}</code>



# Contents

---

Legal disclaimer.....	I
Generic conventions.....	I
<b>1 RAM users.....</b>	<b>1</b>
1.1 Overview of a RAM user.....	1
1.2 Create a RAM user.....	1
1.3 View basic information about a RAM user.....	2
1.4 Modify basic information about a RAM user.....	3
1.5 Grant permission to a RAM user.....	3
1.6 Remove permission from a RAM user.....	4
1.7 Log on to the console as a RAM user.....	4
1.8 Delete a RAM user.....	5
<b>2 RAM user groups.....</b>	<b>6</b>
2.1 Overview of a RAM user group.....	6
2.2 Create a RAM user group.....	6
2.3 Add RAM users to a group.....	7
2.4 Remove a RAM user from a group.....	7
2.5 View basic information about a RAM user group.....	7
2.6 Modify basic information about a RAM user group.....	8
2.7 Grant permission to a RAM user group.....	8
2.8 Remove permission from a RAM user group.....	9
2.9 Delete a RAM user group.....	9
<b>3 RAM roles.....</b>	<b>10</b>
3.1 Overview of a RAM role.....	10
3.2 Create a RAM role.....	13
3.2.1 Create a RAM role for a trusted Alibaba Cloud account.....	13
3.2.2 Create a RAM role for a trusted Alibaba Cloud service.....	14
3.2.3 Create a RAM role for a trusted IdP.....	14
3.3 View basic information about a RAM role.....	15
3.4 Grant permission to a RAM role.....	15
3.5 Remove permission from a RAM role.....	16
3.6 Edit the policy of a RAM role.....	16
3.7 Change the trusted entity of a RAM role.....	17
3.8 Assume a RAM role.....	19
3.9 Delete a RAM role.....	20
<b>4 Policies.....</b>	<b>21</b>
4.1 Policy overview.....	21
4.2 Policy models.....	22
4.3 View basic information about a policy.....	24
4.4 Custom policies.....	24



4.4.1 Create a custom policy.....	24
4.4.2 Modify a custom policy.....	25
4.4.3 Manage policy versions.....	25
4.4.4 Delete a custom policy.....	26
4.5 Manage policy references.....	27
4.6 Policy language.....	27
4.6.1 Policy elements.....	27
4.6.2 Policy structure and grammar.....	31
4.6.3 Policy check rules.....	35
<b>5 Security settings.....</b>	<b>41</b>
5.1 Overview of security settings.....	41
5.2 Passwords.....	42
5.2.1 Change the password for an Alibaba Cloud account.....	42
5.2.2 Set a password policy for RAM users.....	43
5.2.3 Change the password for a RAM user.....	44
5.3 Basic security settings.....	45
5.3.1 Check account security.....	45
5.3.2 Modify logon settings for a RAM user.....	46
5.3.3 Set a security policy for RAM users.....	47
5.3.4 Set a logon mask for an Alibaba Cloud account.....	48
5.4 Advanced settings.....	48
5.4.1 Manage the default domain name.....	48
5.4.2 Create a domain alias.....	49
5.5 Access keys.....	50
5.5.1 Create an access key for a RAM user.....	50
5.5.2 View basic information about an access key.....	51
5.5.3 Disable an access key.....	51
5.5.4 Delete an access key.....	51
5.6 Multi-factor authentication.....	52
5.6.1 Enable an MFA device for an Alibaba Cloud account.....	52
5.6.2 Disable an MFA device for an Alibaba Cloud account.....	54
5.6.3 Enable an MFA device for a RAM user.....	54
5.6.4 Disable an MFA device for a RAM user.....	56
<b>6 SSO management.....</b>	<b>57</b>
6.1 SSO overview.....	57
6.2 Application scenarios of SSO.....	59
6.3 User-based SSO.....	60
6.3.1 Overview of user-based SSO.....	60
6.3.2 Configure the SAML for user-based SSO.....	62
6.3.3 Configure the SAML of an IdP during user-based SSO.....	63
6.3.4 Implement user-based SSO by using AD FS.....	66
6.4 Identity providers.....	76
6.4.1 Create an identity provider.....	76
6.4.2 View basic information about an identity provider.....	76

6.4.3 Modify basic information about an identity provider.....	76
6.4.4 Delete an identity provider.....	77
6.5 Role-based SSO.....	77
6.5.1 Overview of role-based SSO.....	77
6.5.2 Configure the SAML for role-based SSO.....	80
6.5.3 Configure the SAML of an IdP during role-based SSO.....	81
6.5.4 SAML assertions for role-based SSO.....	83
6.5.5 Implement role-based SSO by using AD FS.....	86
6.5.6 Implement role-based SSO by using Azure Active Directory.....	99

# 1 RAM users

---

## 1.1 Overview of a RAM user

A RAM user is a RAM identity with a fixed ID and credential information. Specifically, a RAM user corresponds to an identity, which can be either a person or an application.

- An Alibaba Cloud account owner can create multiple RAM users (which correspond to employees, systems, or applications of their enterprise) under their account.
- RAM users do not own resources. Rather, the fees incurred by RAM users are billed to the Alibaba Cloud accounts to which they belong. RAM users do not receive individual bills and cannot make payments.
- RAM users are visible only to the corresponding Alibaba Cloud account to which they belong.
- RAM users have permissions for only the Alibaba Cloud resources under the Alibaba Cloud account to which they belong after they are authorized to operate on these resources.



**Note:**

Enterprises that have multiple Alibaba Cloud resources can use RAM to manage user permissions and resources. For more information, see [#unique\\_5](#).

## 1.2 Create a RAM user

A RAM user is an entity that you create in Alibaba Cloud to represent the person or application to interact with Alibaba Cloud. You can create a RAM user and grant it the relevant permissions to access the necessary Alibaba Cloud resources.

### Procedure

1. Log on to the [RAM console](#).
2. Choose Identities > Users.

3. Click **Create User**, and enter the logon name and display name.



**Note:**

You can click **Add User** to create multiple RAM users at a time.

4. Select an access mode. The available access modes are **Console Password Logon** and **Programmatic Access**.

- **Console Password Logon:** If you select this check box, you must also complete the basic security settings for logon, including deciding whether to automatically generate a password or customize the logon password, setting whether the user must reset the password upon the next logon, and setting whether to enable multi-factor authentication (MFA).
- **Programmatic Access:** If you select this check box, an access key is automatically created for the RAM user. The user can access Alibaba Cloud resources by calling an API action or by using a development tool.



**Note:**

We recommend that you set only one access mode for the user to maintain the security of your Alibaba Cloud account.

5. Click **OK**.

#### What's next

- You can add the RAM user to one or more RAM user groups and grant permission to the user as needed. For more information, see [#unique\\_7](#).
- You can also attach one or more policies to the RAM user to grant the user access permission. For more information, see [#unique\\_8](#).

## 1.3 View basic information about a RAM user

This topic describes how to view basic information about a RAM user, such as the username, the display name, and the user ID (UID).

#### Procedure

1. Log on to the [RAM console](#).
2. Choose **Identities > Users**.
3. In the **User Logon Name/Display Name** column, click the username of the target RAM user.

4. In the Basic Information section, view the user information.

## 1.4 Modify basic information about a RAM user

This topic describes how to modify basic information about a RAM user, such as the username and the display name.

### Procedure

1. Log on to the [RAM console](#).
2. Choose Identities > Users.
3. In the User Logon Name/Display Name column, click the username of the target RAM user.
4. In the Basic Information section, click Modify Basic Information.
5. Click OK.

## 1.5 Grant permission to a RAM user

This topic describes how to grant permission to a RAM user. A RAM user can access Alibaba Cloud resources after obtaining relevant permissions.

### Procedure

1. Log on to the [RAM console](#).
2. Choose Permissions > Grants.
3. Click Grant Permission.
4. In the Principal field, enter the username or the user ID, and click the target RAM user.



Note:

You can also enter keywords to search for a specific username.

5. In the Policy Name column, select the target policy and click OK.



Note:

You can click X to revoke your selection.

## 1.6 Remove permission from a RAM user

This topic describes how to remove permission from a RAM user when the RAM user no longer needs a permission or when the RAM user leaves your organization.

### Procedure

1. Log on to the [RAM console](#).
2. Choose Permissions > Grants.
3. In the Principal column, find the target RAM user and click Revoke Permission.
4. Click OK.

## 1.7 Log on to the console as a RAM user

This topic describes how to log on to the RAM console as a RAM user, including the address and method to log on to the console.

### Procedure

1. Log on to the [RAM console](#) as a RAM user.



#### Note:

To view the address that is used by a RAM user to log on to the console, use your Alibaba Cloud account to log on to the [RAM console](#). The address is displayed on the Overview page.

2. Enter the logon name and then click Next.

- Method 1: Use the default domain name to log on to the console. The format of the logon name for a RAM user is `<$ username >@<$ AccountAlias> . com`, for example, `username@company-alias.onaliyun.com`.



#### Note:

The logon name of a RAM user must be in the User Principal Name (UPN) format. All logon names listed in the RAM console use this

format. <\$username> represents the username of the RAM user. <\$AccountAlias>.onaliyun.com represents the default domain name.

- Method 2: Use the enterprise alias to log on to the console. The format of the logon name for a RAM user is <\$ username >@<\$ AccountAli as >, for example, username@company-alias.



Note:

<\$username> represents the username of the RAM user. <\$AccountAlias> represents the enterprise alias.

- Method 3: If you have set a domain alias, you can also use the domain alias to log on to the console. The format of the logon name for a RAM user is <\$ username >@<\$ DomainAlia s >, for example, username@example.com.



Note:

<\$username> represents the username of the RAM user. <\$DomainAlias> represents the domain alias.

3. Enter the logon password and click Log On.

## 1.8 Delete a RAM user

This topic describes how to delete a RAM user. You can delete a RAM user when the user leaves your organization. After a RAM user is deleted, the access key, multi-factor authentication (MFA) device, and permissions of the RAM user are also deleted.

### Procedure

1. Log on to the [RAM console](#).
2. Choose Identities > Users.
3. In the User Logon Name/Display Name column, select the target RAM user and click Delete.
4. Click OK.



Note:

Deleting an active RAM user may result in service failure. Exercise caution when performing this action.

## 2 RAM user groups

---

### 2.1 Overview of a RAM user group

A RAM user group is a type of identity in RAM. You can create RAM user groups to classify and organize RAM users under your Alibaba Cloud account. By classifying and organizing your RAM users, you can effectively manage permissions in the RAM console.

- If the responsibilities of a RAM user change, you only need to move the user to a RAM user group with the appropriate permissions. This action does not affect other RAM users.

For information about how to create a RAM user group, see [#unique\\_17](#).

- If the responsibilities of a RAM user group change, you only need to modify the policy attached to the user group. Changes to the policy apply to all RAM users in the group.

For information about how to grant permission to a RAM user group, see [#unique\\_18](#).

### 2.2 Create a RAM user group

This topic describes how to create a RAM user group. If you have multiple RAM users under your Alibaba Cloud account, you can create RAM user groups to classify and organize these RAM users for easier user and permission management.

#### Procedure

1. Log on to the [RAM console](#).
2. Choose Identities > Groups.
3. Click Create Group, and enter the group name, display name, and description.
4. Click OK.

#### What's next

You can attach one or more policies to the RAM user group. For more information, see [#unique\\_18](#).



## 2.3 Add RAM users to a group

This topic describes how to add RAM users to a RAM user group. After a RAM user is added to a group, the user shares the permissions of the group.

### Procedure

1. Log on to the [RAM console](#).
2. Choose Identities > Groups.
3. In the Group Name/Display Name column, find the target RAM user group and click Add Group Members.
4. In the Name column, select the target RAM users and click OK.



#### Note:

You can click X to revoke your selection.

## 2.4 Remove a RAM user from a group

This topic describes how to remove a RAM user from a RAM user group. You must remove a user from the specific RAM user group when the user leaves your organization or when permissions of the user change.

### Procedure

1. Log on to the [RAM console](#).
2. Choose Identities > Groups.
3. In the Group Name/Display Name column, click the name of the target RAM user group.
4. In the User Logon Name/Display Name column, find the target RAM user and click Remove from Group.
5. Click OK.

## 2.5 View basic information about a RAM user group

This topic describes how to view basic information about a RAM user group, such as the group name and the display name.

### Procedure

1. Log on to the [RAM console](#).

2. Choose Identities > Groups.
3. In the Group Name/Display Name column, click the name of the target RAM user group.
4. In the Group Basic Information section, view the group information.

## 2.6 Modify basic information about a RAM user group

This topic describes how to modify basic information about a RAM user group, such as the group name and the display name.

### Procedure

1. Log on to the [RAM console](#).
2. Choose Identities > Groups.
3. In the Group Name/Display Name column, click the name of the target RAM user group.
4. In the Group Basic Information section, click Modify Basic Information.
5. Click OK.

## 2.7 Grant permission to a RAM user group

This topic describes how to grant permission to a RAM user group. After you grant permission to a RAM user group, all users in this group share the permissions of the group.

### Procedure

1. Log on to the [RAM console](#).
2. Choose Permissions > Grants.
3. Click Grant Permission.
4. In the Principal field, enter the group name and click the target RAM user group.
5. In the Policy Name column, select the target policy and click OK.



**Note:**

You can click X to revoke your selection.

## 2.8 Remove permission from a RAM user group

This topic describes how to remove permission from a RAM user group.

### Procedure

1. Log on to the [RAM console](#).
2. Choose Permissions > Grants.
3. In the Principal column, find the target RAM user group and click Revoke Permission.
4. Click OK.

## 2.9 Delete a RAM user group

This topic describes how to delete a RAM user group. If a RAM user group is deleted, all users in the group and policies attached to the group are also deleted.

### Procedure

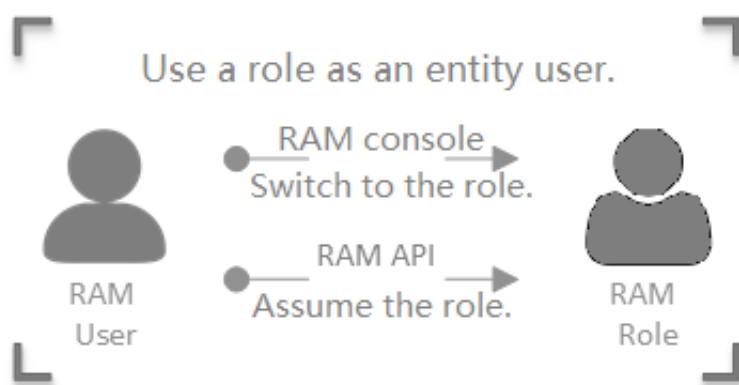
1. Log on to the [RAM console](#).
2. Choose Identities > Groups.
3. In the Group Name/Display Name column, select target RAM user group and click Delete.
4. Click OK.

## 3 RAM roles

### 3.1 Overview of a RAM role

A RAM role is a RAM identity that you can create in your Alibaba Cloud account. A role does not have standard long-term credentials such as a password or an access key. You must first specify a trusted entity that can assume a RAM role before you use the role.

#### Related concepts



#### RAM role

A virtual identity that you can create in your Alibaba Cloud account. The differences among RAM roles, entity users (Alibaba Cloud account, RAM users, or Alibaba Cloud services), and textbook roles are as follows:

- Entity users have specific logon passwords or access keys.
- A textbook role (or a traditionally defined role) indicates a permission set, similar to a policy in RAM. If such a role is granted to a user, the user has a set of permissions and can access the authorized resources.
- As virtual users, RAM roles have specific identities and can be granted a set of policies. However, RAM roles do not have standard long-term credentials (passwords or access keys). When an entity user wants to use a role, the user must assume the role to obtain the role token. Then, the user can use the role token to call Alibaba Cloud API actions.

#### ARN

The Alibaba Cloud Resource Name (ARN) of a RAM role. Each role has a unique ARN. For example, the ARN of the RAM role `devops` under an Alibaba Cloud account is `acs : ram :: 1234567890 : 12 : ****:`

`role / samplerole` . After you create a RAM role, you can click the role name and find its ARN on the Basic Information page.

<b>Trusted entity</b>	The trusted entity that can assume a RAM role. You must specify a trusted entity when you create a RAM role. Only trusted entities can assume RAM roles. The trusted entity can be an Alibaba Cloud account, Alibaba Cloud service, or identity provider (IdP).
<b>Policy</b>	A set of permissions that are described by using policy structure and grammar. Roles that are not attached to any policy can exist, but cannot access resources.
<b>Role assuming</b>	The method for entity users to obtain security tokens of RAM roles. By calling the <code>AssumeRole</code> action of STS, an entity user can obtain the security token of a role and use the token to access Alibaba Cloud service APIs.
<b>Identity switching</b>	The method by which entity users can switch from the logon identity to role identity in the RAM console. After logging on to the RAM console, an entity user can switch to a RAM role that the user can assume. The user can then use the role identity to operate Alibaba Cloud resources. When the user no longer needs the role identity, the user can switch back to its logon identity.
<b>Role token</b>	A temporary access key to a role identity. RAM roles do not have standard long-term credentials (passwords or access keys). When an entity user wants to use a role, the user must assume the role to obtain the role token. Then, the user can use the role token to call Alibaba Cloud API actions.

## Access to Alibaba Cloud resources by using a RAM role



1. The Alibaba Cloud account specifies a trusted entity that can assume the RAM role.
2. The trusted entity logs on to the console or calls an API action to assume the role and obtains a role token.
  - The trusted entity can assume the role by switching its identity in the console. For more information, see [#unique\\_29](#).
  - The trusted entity can assume the role by calling the AssumeRole action.



### Note:

An entity user can obtain a role token by assuming a RAM role and then use the token to access Alibaba Cloud resources.

3. The Alibaba Cloud account attaches a policy to the RAM role. For more information, see [#unique\\_30](#).



### Note:

A RAM role can have one or more policies attached. A RAM role without a policy cannot access Alibaba Cloud resources.

4. The trusted entity assumes the RAM role and uses a temporary STS token to access Alibaba Cloud resources.

## RAM role types

RAM roles are divided into the following types according to different trusted entities:

- **Alibaba Cloud account:** roles that RAM users can assume. The RAM users may belong to their own Alibaba Cloud accounts or other Alibaba Cloud accounts. Such roles provide solutions to cross-account access and temporary authorization.
- **Alibaba Cloud service:** roles that Alibaba Cloud services can assume. Such roles are used to authorize Alibaba Cloud services to operate resources as stand-alone applications.
- **IdP:** roles that users in an entrusted IdP can assume. Such roles are used to implement Single Sign On (SSO) to Alibaba Cloud.

## Application scenarios

- [#unique\\_31](#)
- [#unique\\_32](#)
- [#unique\\_33](#)

## 3.2 Create a RAM role

### 3.2.1 Create a RAM role for a trusted Alibaba Cloud account

This topic describes how to create a RAM role for a trusted Alibaba Cloud account.

You can create a RAM role for three types of trusted entities: trusted Alibaba Cloud accounts, trusted Alibaba Cloud services, and trusted identity providers (IdPs).

#### Procedure

1. Log on to the [RAM console](#).
2. In the left-side navigation pane, click RAM Roles.
3. Click Create RAM Role.
4. Select Alibaba Cloud Account and click Next.
5. Enter a RAM role name and description.
6. Select a trusted Alibaba Cloud account and click OK.



#### Note:

If you select Other Alibaba Cloud Account, you must enter the account ID.

## What's next

After you create a RAM role, you can click **Add Permissions to RAM Role** to grant permission to this role. For more information, see [#unique\\_30](#).

### 3.2.2 Create a RAM role for a trusted Alibaba Cloud service

This topic describes how to create a RAM role for a trusted Alibaba Cloud service.

You can create a RAM role for three types of trusted entities: trusted Alibaba Cloud accounts, trusted Alibaba Cloud services, and trusted identity providers (IdPs).

#### Procedure

1. Log on to the [RAM console](#).
2. In the left-side navigation pane, click **RAM Roles**.
3. Click **Create RAM Role**.
4. Select **Alibaba Cloud Service** and click **Next**.
5. Enter a RAM role name and description.
6. Select a trusted Alibaba Cloud service and click **OK**.



#### Note:

For more information about the trusted services, see the RAM console.

#### What's next

After you create a RAM role, you can click **Add Permissions to RAM Role** to grant permission to this role. For more information, see [#unique\\_30](#).

### 3.2.3 Create a RAM role for a trusted IdP

This topic describes how to create a RAM role for a trusted identity provider (IdP).

You can create a RAM role for three types of trusted entities: trusted Alibaba Cloud accounts, trusted Alibaba Cloud services, and trusted IdPs.

#### Procedure

1. Log on to the [RAM console](#).
2. In the left-side navigation pane, click **RAM Roles**.
3. Click **Create RAM Role**.
4. Select **IdP** and click **Next**.
5. Enter a RAM role name and description.



6. Select a trusted IdP and click OK.



Note:

In the Condition Keyword column, only the keyword `saml : recipient` (which is required and cannot be modified) is currently allowed.

#### What's next

After you create a RAM role, you can click **Add Permissions to RAM Role** to grant permission to this role. For more information, see [#unique\\_30](#).

## 3.3 View basic information about a RAM role

This topic describes how to view basic information about a RAM role, such as the role name, the date and time when the role was created, and the Alibaba Cloud Resource Name (ARN) of the role.

#### Procedure

1. Log on to the [RAM console](#).
2. In the left-side navigation pane, click **RAM Roles**.
3. In the **RAM Role Name** column, click the name of the target RAM role.
4. In the **Basic Information** section, view the role information.



Note:

The RAM role information can be viewed but cannot not be modified.

## 3.4 Grant permission to a RAM role

This topic describes how to grant permission to a RAM role. You can grant permission to a RAM role that you created for a trusted Alibaba Cloud account, Alibaba Cloud service, or identity provider (IdP).

#### Procedure

1. Log on to the [RAM console](#).
2. Choose **Permissions > Grants**.
3. Click **Grant Permission**.

4. In the Principal field, enter the role name and click the target RAM role.



Note:

You can also enter keywords to search for a specific RAM role.

5. In the Policy Name column, select the target policy and click OK.



Note:

You can click X to revoke your selection.

## 3.5 Remove permission from a RAM role

This topic describes how to remove permission from a RAM role when the RAM role no longer needs a permission.

### Procedure

1. Log on to the [RAM console](#).
2. Choose Permissions > Grants.
3. In the Principal column, find the target RAM role and click Revoke Permission.
4. Click OK.

## 3.6 Edit the policy of a RAM role

This topic describes how to edit the policy of a RAM role to change the trusted entity that assumes the role.

### Context

The `Principal` element specifies the trusted entity that assumes the role. You can change a trusted entity by modifying the `Principal` element.

### Procedure

1. Log on to the [RAM console](#).
2. In the left-side navigation pane, click RAM Roles.
3. In the RAM Role Name column, click the name of the target RAM role.
4. On the Trust Policy Management tab, click Edit Trust Policy.



Note:

For information about how to edit a policy, see [#unique\\_42](#).

5. Click OK.

## 3.7 Change the trusted entity of a RAM role

This topic describes how to change the trusted entity of a RAM role by modifying the policy attached to the role. The trusted entity of a RAM role can be an Alibaba Cloud account, an Alibaba Cloud service, or an identity provider (IdP).

### Change the trusted entity to an Alibaba Cloud account

If the `Principal` element contains a "RAM" field, the trusted entity is an Alibaba Cloud account, and the role can be assumed by RAM users under the trusted account.

The following policy indicates that the role can be assumed by any RAM user under the Alibaba Cloud account (123456789012\*\*\*\*):

```
{
  "Statement": [
    {
      "Action": "sts : AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "RAM": [
          "acs : ram :: 1234567890 12 ****: root"
        ]
      }
    ]
  },
  "Version": "1"
}
```

If you modify the `Principal` element as follows, the role can be assumed by the RAM user `testuser` under the Alibaba Cloud account (123456789012\*\*\*\*):

```
    "Principal": {
      "RAM": [
        "acs : ram :: 1234567890 12 ****: user /
testuser"
      ]
    }
```

### Change the trusted entity to an Alibaba Cloud service

If the `Principal` element contains a "Service" field, the trusted entity is an Alibaba Cloud service, and the role can be assumed by trusted Alibaba Cloud services under the current Alibaba Cloud account.

The following policy indicates that the role can be assumed by ECS under the current Alibaba Cloud account:

```
{
  "Statement": [
    {
      "Action": "sts : AssumeRole ",
      "Effect": "Allow ",
      "Principal": {
        "Service": [
          "ecs . aliyuncs . com "
        ]
      }
    }
  ],
  "Version": " 1 "
}
```

### Change the trusted entity to an IdP

If the `Principal` element contains a "Federated" field, the trusted entity is an IdP, and the role can be assumed by users under the trusted IdP.

The following policy indicates that the role can be assumed by users under the IdP ( `testprovid er` ) in the current Alibaba Cloud account (123456789012\*\*\*\*):

```
{
  "Statement": [
    {
      "Action": "sts : AssumeRole ",
      "Effect": "Allow ",
      "Principal": {
        "Federated": [
          "acs : ram :: 1234567890 12 ****: saml -
provider / testprovid er "
        ]
      },
      "Condition": {
        "StringEquals": {
          "saml : recipient ":" https :// signin .
alibabaclo ud . com / saml - role / sso "
        }
      }
    }
  ],
  "Version": " 1 "
}
```

```
}
```

## 3.8 Assume a RAM role

This topic describes how to assume a RAM role by using a RAM user under a trusted Alibaba Cloud account.

### Prerequisites



#### Note:

To maintain account security, a trusted Alibaba Cloud account is not allowed to assume RAM roles itself. RAM roles must instead be assumed by RAM users of the Alibaba Cloud account.

1. A RAM user is created. For information about how to create a RAM user, see [#unique\\_45](#).
2. An access key or a password is set for the RAM user.
  - For information about how to create an access key, see [#unique\\_46](#).
  - For information about how to set a password, see [#unique\\_47](#).
3. The system policy `AliyunSTSA ssumeRoleA ccess` is attached to the RAM user. For information about how to grant permission to a RAM role, see [#unique\\_30](#).

### Procedure

1. Log on to the [RAM console](#) as a RAM user.
2. Move the pointer over the account icon in the upper-right corner and click Switch Role.
3. On the displayed Switch Role page, enter the enterprise alias or the default domain name in the Enterprise Alias/Default Domain Name field and the RAM role name in the Role Name field. Then, click Switch.
4. Click Switch Back to Logon User to switch back to your logon identity.



#### Note:

After you switch to the logon identity, you will obtain the original permissions and lose the permissions associated with the RAM role.

### What's next

A RAM user can also assume a RAM role by calling an API action. After being granted the `AliyunSTSAssumeRoleAccess` policy, a RAM user can use its access key to call the [#unique\\_48](#) action of the Security Token Service (STS) to obtain the temporary security token of a role. Then, the user uses the token to access Alibaba Cloud APIs.

## 3.9 Delete a RAM role

This topic describes how to delete a RAM role when you no longer need it.

### Prerequisites



#### Note:

Before you delete a RAM role, make sure that no policy is attached to the role.

### Procedure

1. Log on to the [RAM console](#).
2. In the left-side navigation pane, click RAM Roles.
3. In the RAM Role Name column, select the target RAM role and click Delete.
4. Click OK.

## 4 Policies

---

### 4.1 Policy overview

You can manage access in Alibaba Cloud by creating policies and attaching them to RAM identities (RAM users, RAM user groups, or RAM roles) or Alibaba Cloud resources. A policy, when associated with an identity or an Alibaba Cloud resource, defines their permissions.

#### Permission

A statement within a policy that allows or denies access to a particular Alibaba Cloud resource.

- An Alibaba Cloud account (resource owner) controls all permissions.
  - Each Alibaba Cloud resource has only one owner. The owner must be an Alibaba Cloud account and has full resource control permissions.
  - The resource owner is not necessarily the resource creator. For example, if a RAM user has permission to create Alibaba Cloud resources, the resources created by this RAM user belong to the RAM user's Alibaba Cloud account. The RAM user is the resource creator, but is not the resource owner.
- By default, a RAM user has no permissions.
  - A RAM user is an operator and must be granted explicit permission before performing any operations.
  - A new RAM user has no operation permissions by default, and cannot perform operations on Alibaba Cloud resources through the console or APIs until being granted permission.
- A resource creator (RAM user) is not automatically granted permissions for the created resources.
  - A RAM user can create resources if the user is granted the resource creation permission.
  - However, the RAM user is not automatically granted any permissions for the created resources, unless the resource owner explicitly grants permission to the user.

## Policy

A set of permissions that are described by using policy structure and grammar. It can accurately describe the authorized resource sets, operation sets, and authorization conditions a user can be granted with. For information about structures and grammars supported by RAM, see [#unique\\_52](#).

In RAM, a policy is a resource entity that can be created, updated, deleted, and viewed by RAM users. RAM supports the following two types of policies:

- **System policy:** System policies are created by Alibaba Cloud and cannot be modified by users. The policies are automatically upgraded by Alibaba Cloud.
- **Custom policy:** If no system policy meets your requirements, you can create a custom policy as needed. You can also modify and delete a custom policy as needed.

You can attach one or more policies to RAM users, RAM user groups, or RAM roles. For more information, see [#unique\\_8](#), [#unique\\_18](#), and [#unique\\_30](#).

### Policies attached to RAM identities

You can attach one or more policies to RAM identities to grant necessary permissions to them.

- The attached policy can be either a system policy or a custom policy.
- If the attached policy is updated, the updates to the policy automatically take effect, and you do not need to attach the policy again.

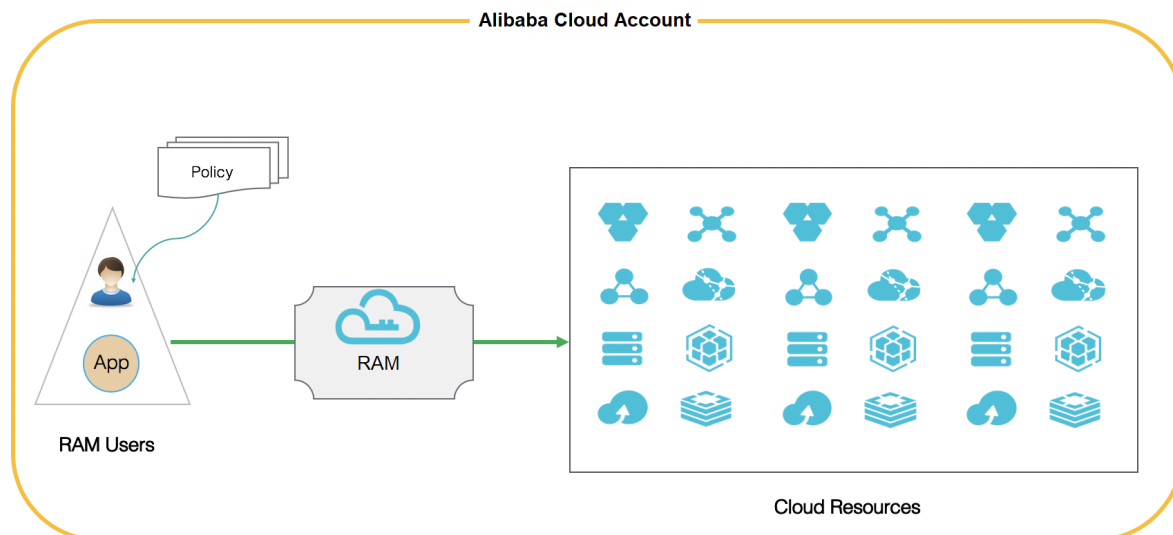
## 4.2 Policy models

Alibaba Cloud allows you to grant permission for an Alibaba Cloud account or for a resource group. You can select an appropriate model according to your specific requirements.

### Grant permission for an Alibaba Cloud account

Granting permission for an Alibaba Cloud account means that when you attach a policy to a RAM identity, all Alibaba Cloud resources under the account are included within the scope of the policy permissions.

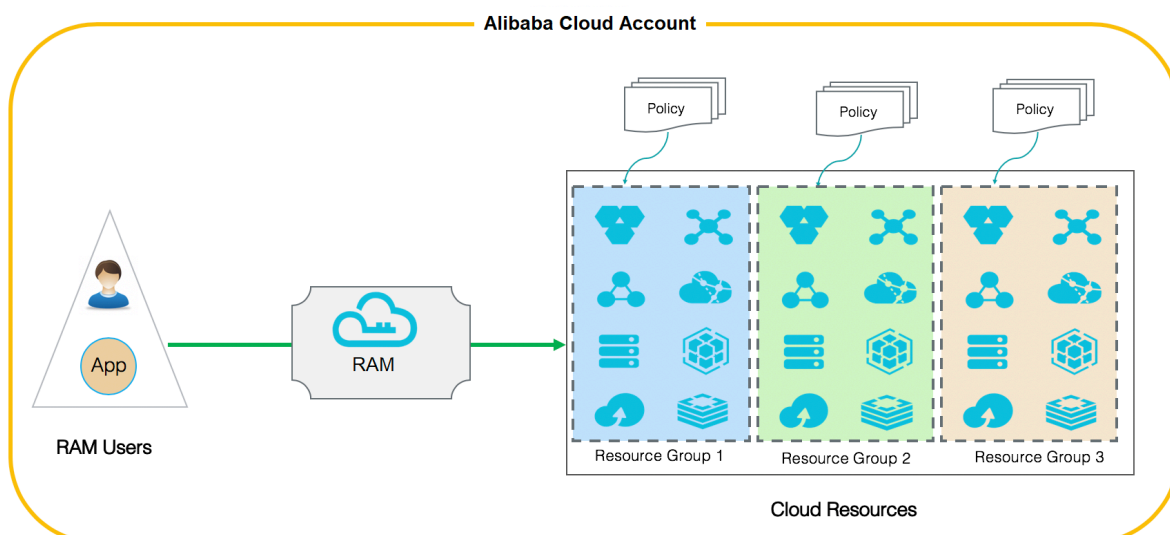




### Grant permission for a target resource group

Granting permission for a resource group means that when you attach a policy to a RAM identity, only the Alibaba Cloud resources within the target resource group are included within the scope of the policy permissions.

In detail, the RAM user with the `AdministratorAccess` system policy in a resource group is called administrator. By default, the resource group creator is assigned as administrator. The administrator is the entity that can add RAM users to the resource group and grant permission to the users in the resource group.



## 4.3 View basic information about a policy

This topic describes how to view basic information about a policy, such as the policy name, policy type, and the number of times the policy is referenced.

### Procedure

1. Log on to the [RAM console](#).
2. Choose Permissions > Policies.
3. Enter a policy name or description in the search box.
4. From the Policy Type drop-down list, select System Policy or Custom Policy.



#### Note:

System policies can be viewed but cannot be modified, whereas custom policies can be created and modified.

## 4.4 Custom policies

### 4.4.1 Create a custom policy

This topic describes how to create a custom policy. Custom policies provide more precise control than system policies.

### Prerequisites

Before you create a custom policy, we recommend that you read about the basic structure and grammar of a policy. For more information, see [#unique\\_52](#).

### Procedure

1. Log on to the [RAM console](#).
2. Choose Permissions > Policies.
3. Click Create Policy.
4. Enter a policy name and description.
5. Set the configuration mode.
  - If you set the configuration mode to Visualized, click Add Statement and configure the permission effect, actions, and resources as prompted.
  - If you set the configuration mode to Script, edit the policy according to [policy structure and grammar](#).
6. Click OK.

## 4.4.2 Modify a custom policy

This topic describes how to modify a custom policy. If the permissions of a RAM user are changed (added or removed), you must modify the corresponding policy attached to the user.

### Context

You may have the following requirements when modifying a policy:

- You still want to use the old policy after a period of time.
- You want to restore a previous policy version if the current version has incorrect modifications.

### Procedure

1. Log on to the [RAM console](#).
2. Choose Permissions > Policies.
3. From the Policy Type drop-down list, select Custom Policy.
4. In the Policy Name column, click the name of the target custom policy.



**Note:**

System policies and custom policies are available for use in Alibaba Cloud Resource Access Management (RAM). System policies can be viewed but cannot be modified, whereas custom policies can be created and modified.

5. On the Policy Document tab, click Modify Policy Document.



**Note:**

For information about how to modify a policy document, see [#unique\\_52](#).

6. Click OK.



**Note:**

After the modifications are completed, a new custom policy is automatically generated and used as a default policy.

## 4.4.3 Manage policy versions

This topic describes how to manage policy versions, such as viewing a policy version, setting the default policy version, and deleting a policy version.

### Context

- You can retain multiple versions for a policy.
- If you reach the maximum number of policy versions allowed, we recommend that you delete versions you no longer need to save space.
- Even if a policy has multiple versions, only one version is active. The active version is known as the default version.
- The default version can be viewed but cannot be deleted.

#### Procedure

1. Log on to the [RAM console](#).
2. Choose Permissions > Policies.
3. In the Policy Name column, click the name of the target policy.
4. On the Versions tab, you can:
  - Click View to view the policy version and the policy document.
  - Click Use This Version to set the policy version to the default version.
  - Click Delete to delete the policy version.

### 4.4.4 Delete a custom policy

This topic describes how to delete a custom policy. You can delete a custom policy when permissions in this policy change or when you no longer need this policy.

#### Prerequisites

- The policy has only one version, that is, the default version. If multiple versions exist, you must delete all of the versions except the default one.
- The policy is not referenced (that is, attached to a RAM user, RAM user group, or RAM role). If the policy is currently being referenced, remove related permissions in the policy. For more information, see [#unique\\_60](#).

#### Procedure

1. Log on to the [RAM console](#).
2. Choose Permissions > Policies.
3. From the Policy Type drop-down list, select Custom Policy.
4. In the Policy Name column, find the target custom policy and click Delete.
5. Click OK.

## 4.5 Manage policy references

This topic describes how to manage policy references, such as viewing and deleting policy references.

### Procedure

1. Log on to the [RAM console](#).
2. Choose Permissions > Policies.
3. In the Policy Name column, click the name of the target policy.
4. On the References tab, you can:
  - View the permission principal, the principal type, and actions.
  - Click Revoke Permission to delete the policy reference, that is, remove permission from a principal.

## 4.6 Policy language

### 4.6.1 Policy elements

This topic describes the elements of policies that are used in Alibaba Cloud Resource Access Management (RAM) to define a permission.

### Elements

Element	Description
Effect	Specifies whether the statement results in an allow or an explicit deny.  Valid values: <code>Allow</code>   <code>Deny</code>
Action	Describes the specific API action or actions that will be allowed or denied.
Resource	Specifies the object or objects that the statement covers.
Condition	Specifies when a policy takes effect.

### How to use a policy element

- Effect



Note:

If policies that apply to a request include an `Allow` statement and a `Deny` statement, the `Deny` statement trumps the `Allow` statement.

Example: `" Effect ": " Allow "`

- Action



**Note:**

In most cases, each Alibaba Cloud service has its own set of API actions. For more information, see [#unique\\_64](#).

**Format:** `< service - name > : < action - name >`

- `service - name` : the name of an Alibaba Cloud service
- `action - name` : `service` : the name of a relevant API action

Example: `" Action ": [ " oss : ListBucket s ", " ecs : Describe *", " rds : Describe *"]`

- Resource

**Format:** `acs : < service - name > : < region > : < account - id > : < relative - id >`

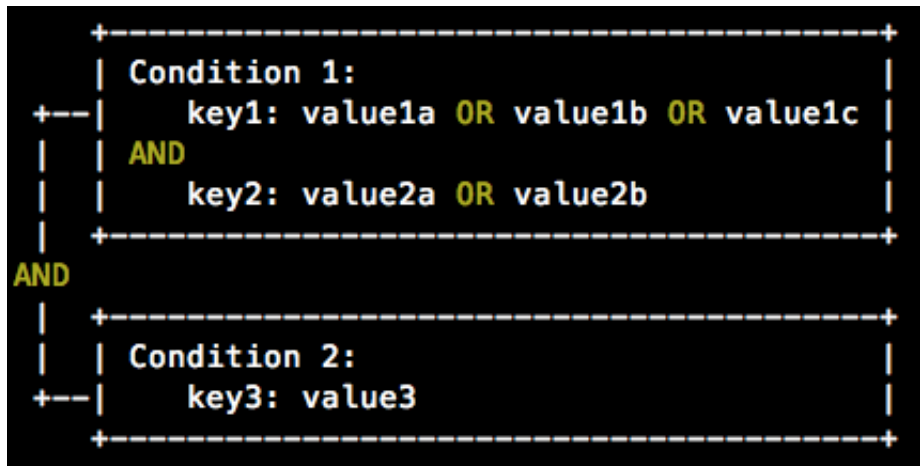
- `acs` : the abbreviation of Alibaba Cloud Service
- `service - name` : the name of an Alibaba Cloud service
- `region` : the region information. If this element is not supported, use an asterisk (\*).
- `account - id` : the Alibaba Cloud account ID, such as `1234567890 12 ****`. If no ID is required or available, it can be replaced with an asterisk (\*).
- `relative - id` : service-related resource description. Its meaning is specified by a specific Alibaba Cloud service. The `relative - id` element is similar to a file path. For example, `relative - id = " mybucket / dir1 / object1 . jpg "` indicates an OSS object.

Example: `" Resource ": [ " acs : ecs : *: *: instance / inst - 001 ", " acs : ecs : *: *: instance / inst - 002 ", " acs : oss : *: *: mybucket ", " acs : oss : *: *: mybucket /*"]`

## · Condition

A condition block can contain multiple conditions, and each condition can contain multiple key-value pairs.

Figure 4-1: Condition block



- Unless otherwise specified, all keys can have multiple values. When conditions are evaluated, if the condition value matches any of the corresponding values, the condition is satisfied.
- A condition is satisfied only if multiple conditions of the same action type are all satisfied.
- A condition block is satisfied only if all of its conditions are satisfied.

## Action type

The following types of actions are supported: string, numeric, date and time, Boolean, and IP address.

Action type	Supported type
String	<ul style="list-style-type: none"> <li>- StringEquals</li> <li>- StringNotEquals</li> <li>- StringEqualsIgnoreCase</li> <li>- StringNotEqualsIgnoreCase</li> <li>- StringLike</li> <li>- StringNotLike</li> </ul>

Action type	Supported type
Numeric	<ul style="list-style-type: none"> <li>- NumericEquals</li> <li>- NumericNotEquals</li> <li>- NumericLessThan</li> <li>- NumericLessThanEquals</li> <li>- NumericGreaterThan</li> <li>- NumericGreaterThanEquals</li> </ul>
Date and time	<ul style="list-style-type: none"> <li>- DateEquals</li> <li>- DateNotEquals</li> <li>- DateLessThan</li> <li>- DateLessThanEquals</li> <li>- DateGreaterThan</li> <li>- DateGreaterThanEquals</li> </ul>
Boolean	Bool
IP address	<ul style="list-style-type: none"> <li>- IpAddress</li> <li>- NotIpAddress</li> </ul>

### Condition key

- The format of common condition keys is as follows:

```
acs :< condition - key >
```

Condition key	Type	Description
acs : CurrentTime	Date and time	The date and time when the web server receives a request. This key is defined in ISO 8601 format, for example, 2012 - 11 - 11T23 : 59 : 59Z .
acs : SecureTransport	Boolean	Indicates whether a secure channel, such as HTTPS, is used to send a request.
acs : SourceIp	IP address	The IP address of the client that sends a request.



Condition key	Type	Description
<code>acs : MFAPresent</code>	Boolean	Indicates whether multi-factor authentication (MFA) is used during user logon.

- The format of Alibaba Cloud service-related condition keys is as follows:

```
< service - name > : < condition - key >
```

Condition key	Alibaba Cloud service	Type	Description	
<code>ecs : tag / &lt; tag - key &gt;</code>	ECS	String	The tag-key pair for ECS. This key can be customized.	
<code>rds : ResourceTag / &lt; tag - key &gt;</code>	RDS	String	The tag-key pair for RDS. This key can be customized.	
<code>oss : Delimiter</code>	OSS	String	The separator used by OSS to group object names.	
<code>oss : Prefix</code>	OSS	String	The prefix of an OSS object name.	

## 4.6.2 Policy structure and grammar

This topic describes the structure and grammar used to create or update policies in Alibaba Cloud Resource Access Management (RAM).

### Conventions used in a policy grammar

The conventions used in a policy grammar are as follows:

- Characters in a policy:

- The following characters are JSON tokens and are included in policies:

`{ } [ ] " , :`

- The following characters are special characters in the grammar and are not included in policies:

`= < > ( ) |`

- Use of characters:

- If an element allows multiple values, you can:

- Use a comma (,) as the delimiter to separate each value, and an ellipsis (...) to describe the remaining values. For example, [`< action_str ing >`, `< action_str ing >`, ...].

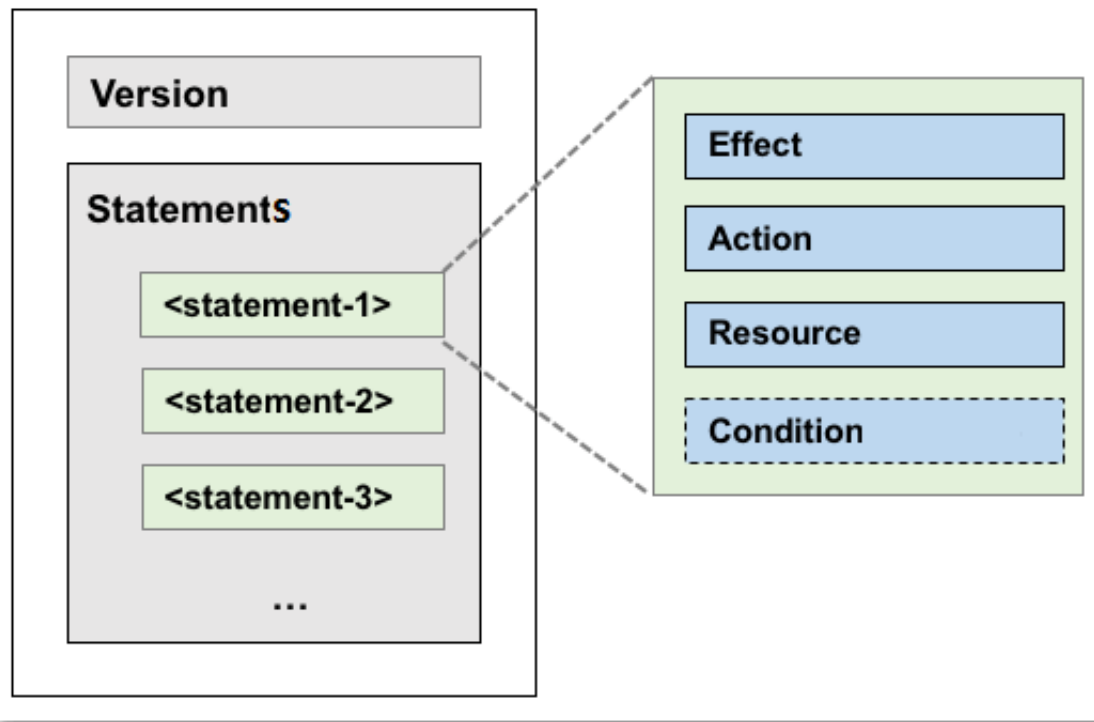
- Include only one value, for example, " Action ": [`< action_str ing >`] and " Action ": `< action_str ing >`.

- A question mark (?) following an element indicates that the element is optional, for example, `< condition_ block ?>`.
- A vertical bar (|) between elements indicates alternatives, for example, (" Allow " | " Deny ").
- Elements that must be text strings are enclosed in double quotation marks (""), for example, `< version_block > = " Version " : (" 1 ")`.

## Policy structure

The policy structure includes the version number and a list of statements.

Each statement contains the following elements: effect, action, resource, and condition. The condition element is optional.



### Policy grammar

```

policy = {
    < version_block >,
    < statement_block >
}
< version_block > = " Version " : ( " 1 " )
< statement_block > = " Statement " : [ < statement >, < statement
>, ... ]
< statement > = {
    < effect_block >,
    < action_block >,
    < resource_block >,
    < condition_block ? >
}
< effect_block > = " Effect " : ( " Allow " | " Deny " )
< action_block > = ( " Action " | " NotAction " ) :
    ( "*" | [ < action_string >, < action_string >, ... ] )
< resource_block > = ( " Resource " | " NotResource " ) :
    ( "*" | [ < resource_string >, < resource_string >, ... ] )
< condition_block > = " Condition " : < condition_map >
< condition_map > = {
    < condition_type_string > : {
        < condition_key_string > : < condition_value_list >,
        < condition_key_string > : < condition_value_list >,
        ...
    },
    < condition_type_string > : {
        < condition_key_string > : < condition_value_list >,
        < condition_key_string > : < condition_value_list >,
        ...
    }, ...
}
< condition_value_list > = [ < condition_value >, < condition_value
>, ... ]

```

```
< condition_ value > = (" String " | " Number " | " Boolean ")
```

**Description:**

- The current policy version is 1.
- The policy can have multiple statements.
  - Each statement can be either `Allow` or `Deny` .

**Note:**

In a statement, both the action and resource elements can have multiple values.

- Each statement supports its own conditions.

**Note:**

A condition block can contain multiple conditions with different action types and logical combinations of these conditions.

- You can attach multiple policies to a RAM user. If policies that apply to a request include an `Allow` statement and a `Deny` statement, the `Deny` statement trumps the `Allow` statement.
- Element value:
  - If an element value is a number or Boolean, it must be enclosed by using double quotation marks (") such as strings.
  - If an element value is a string, characters such as the asterisk (\*) and question mark (?) can be used for fuzzy matching.

- The asterisk (\*) indicates any number (including zero) of allowed characters.

For example, `ecs : Describe *` indicates all ECS actions starting with `Describe` .

- The question mark (?) indicates one allowed character.

**Policy format check**

Policies are stored in RAM as JSON documents. When you create or update a policy, RAM first checks whether the JSON format is correct.

- For more information about the JSON grammar standards, see [RFC 7159](#).
- We recommend that you use tools such as JSON validators and editors to verify your policies to meet JSON grammar standards.


### 4.6.3 Policy check rules



This topic describes the policy check rules to help you better understand RAM policies.

#### Check rules

You can access Alibaba Cloud resources in RAM by using an Alibaba Cloud account, or as an authorized RAM user or RAM role.

RAM determines whether to allow access according to the rules described in the following table.

Access type	Rules
Alibaba Cloud account	<p>The Alibaba Cloud account is the resource owner and can access all Alibaba Cloud resources under the account.</p> <div> <b>Note:</b> Some Alibaba Cloud services, such as Log Service, support cross-account ACL authorization. If ACL authorization is successful, access is allowed even the Alibaba Cloud account is not the resource owner.</div>

Access type	Rules
RAM user	<ul style="list-style-type: none"> <li>• The Alibaba Cloud account has attached a policy with explicit allow effect to the RAM user.</li> <li>• The Alibaba Cloud account to which the RAM user belongs has permission to access specific Alibaba Cloud resources.</li> </ul> <div data-bbox="847 591 1433 871">  <b>Note:</b>  By default, a RAM user does not have any permissions to access Alibaba Cloud resources. The user can access Alibaba Cloud resources only when both of the preceding rules are met. </div> <p>For information about how to check the permissions of a RAM user, see <a href="#">Policy check rules for RAM users</a>.</p>
RAM role	<ul style="list-style-type: none"> <li>• The STS token of the RAM role has the required permissions.</li> </ul> <p>For more information about RAM role STS tokens, see <a href="#">#unique_67</a></p> <ul style="list-style-type: none"> <li>• The Alibaba Cloud account has attached a policy with explicit allow effect to the RAM role.</li> <li>• The Alibaba Cloud account to which the RAM role belongs has permission to access specific Alibaba Cloud resources.</li> </ul> <div data-bbox="847 1610 1433 1890">  <b>Note:</b>  By default, a RAM role does not have any permissions to access Alibaba Cloud resources. The role can access Alibaba Cloud resources only when all the preceding rules are met. </div> <p>For information about how to check the permissions of a RAM role, see <a href="#">Policy check rules for RAM roles</a>.</p>

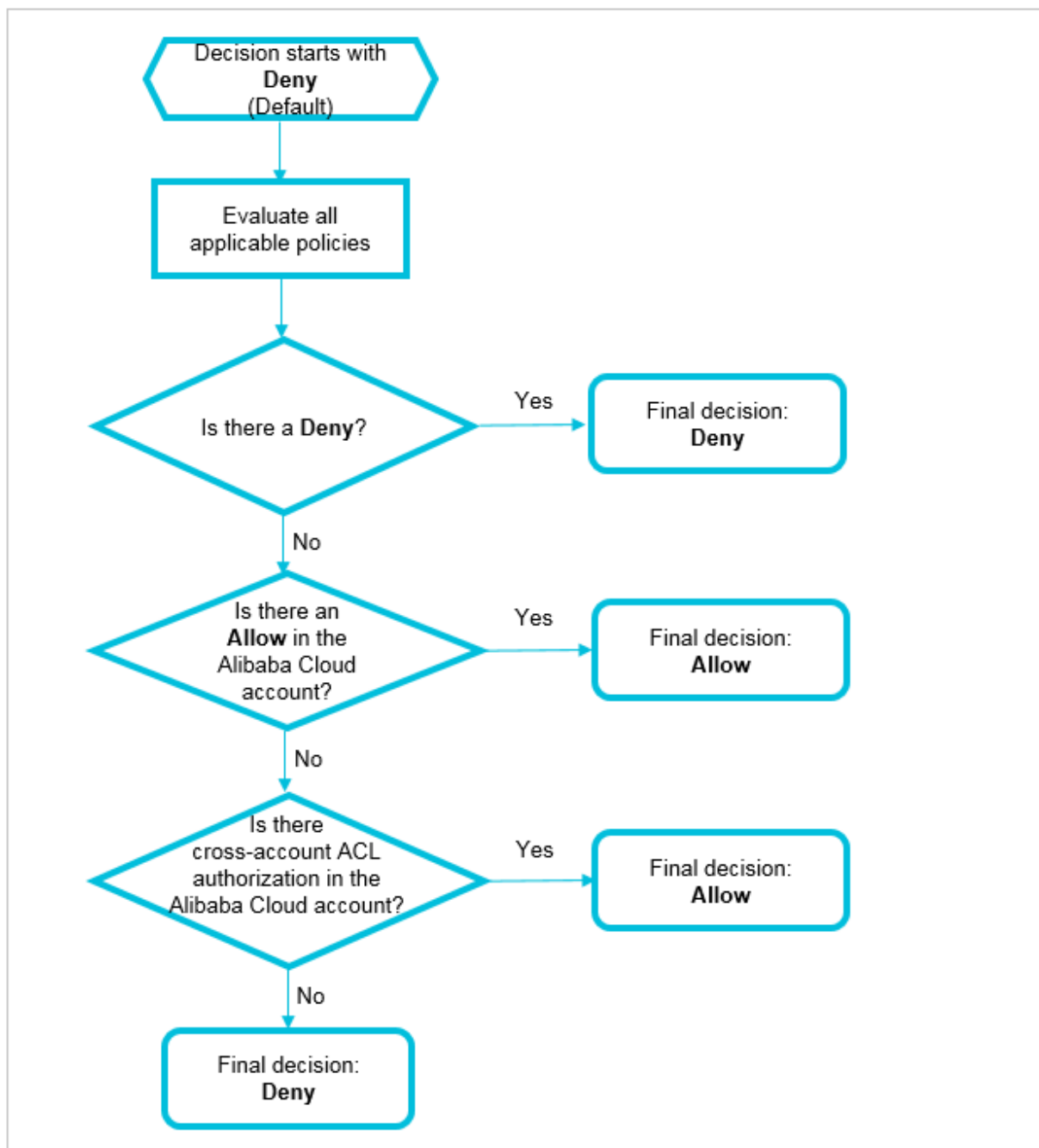
## Policy check rules for RAM users

By default, RAM users do not have resource access permissions unless they have been granted explicit permission by the Alibaba Cloud account.



### Note:

A policy can contain **Allow** and **Deny** statements. If policies that apply to a request include an **Allow** statement and a **Deny** statement, the **Deny** statement trumps the **Allow** statement.



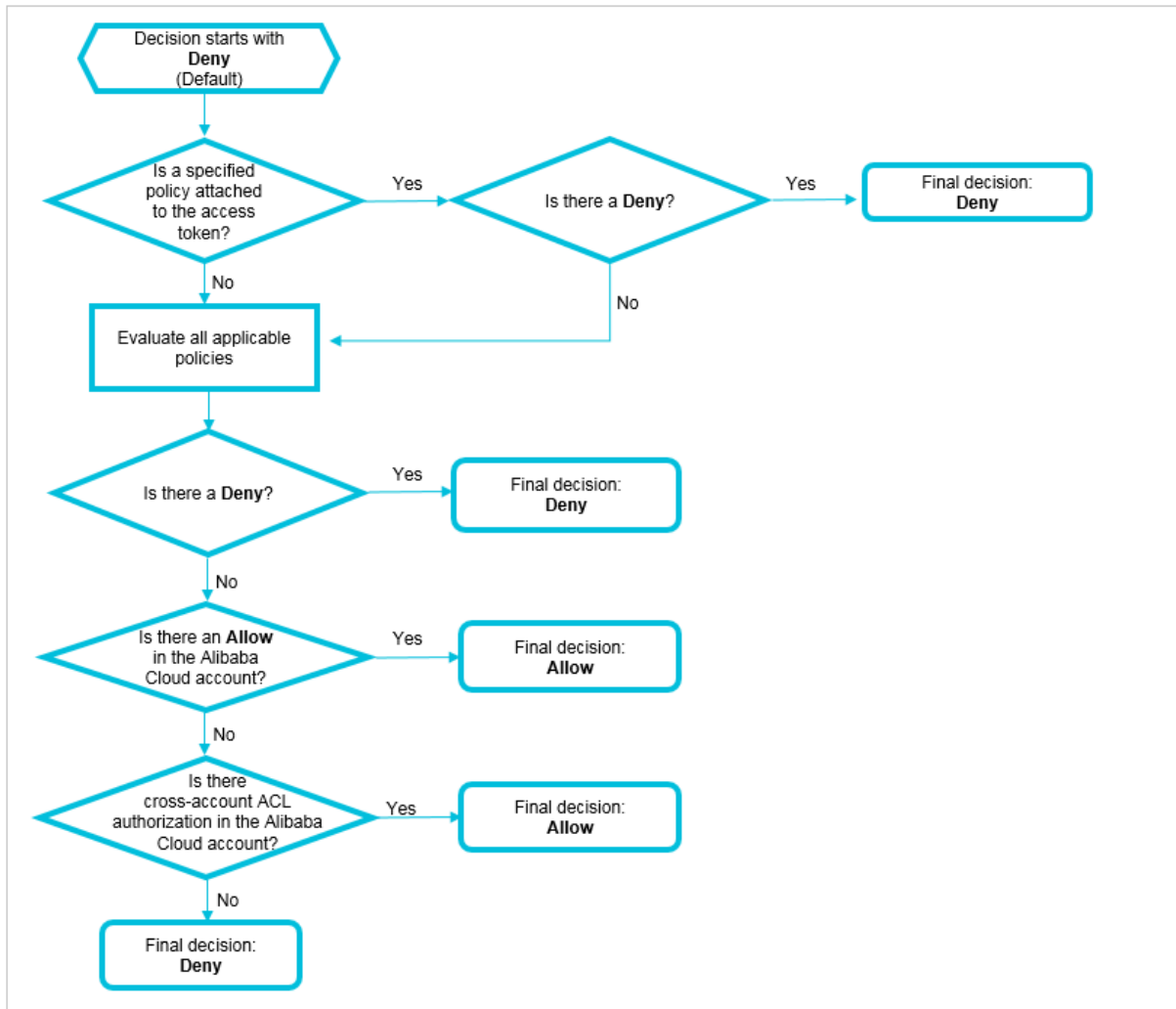
When you access Alibaba Cloud resources as a RAM user, the system checks the policies as follows:

1. Whether the policy attached to the RAM user has a `Deny` statement:
  - If yes, access is denied.
  - If no, go to the next step.
2. Whether the policy attached to the Alibaba Cloud account of the RAM user has an `Allow` statement:
  - If yes, access is allowed.
  - If no, go to the next step.
3. Whether the Alibaba Cloud account of the RAM user has cross-account ACL authorization:
  - If yes, access is allowed.
  - If no, access is denied.

#### Policy check rules for RAM roles

You can access Alibaba Cloud resources as a RAM role by using an STS token and calling the [#unique\\_48](#) action. The `Policy` parameter specifies the resource access permission or permissions.





When you access Alibaba Cloud resources as a RAM role, the system checks the policies as follows:

1. Whether a policy is attached to the STS token:

- If a policy is attached to the STS token, the system checks whether the policy has a **Deny** statement.
  - If yes, access is denied.
  - If no, the system checks the policy attached to the RAM role.
- If no policy is attached to the STS token, the system checks the policy attached to the RAM role.

2. Whether the policy attached to the RAM role has a **Deny** statement:

- If yes, access is denied.
- If no, go to the next step.

3. Whether the policy attached to the Alibaba Cloud account of the RAM role has an **Allow** statement:

- If yes, access is allowed.
- If no, go to the next step.

4. Whether the Alibaba Cloud account of the RAM role has cross-account ACL authorization:

- If yes, access is allowed.
- If no, access is denied.

## 5 Security settings

---

### 5.1 Overview of security settings

This topic describes some commonly used concepts that are relevant to security settings in the RAM console.

#### Password

An identity credential that is used by a user to log on to Alibaba Cloud.



**Note:**

We recommend that you change your password periodically and keep your password private.

For information about how to set a password, see [#unique\\_47](#) and [#unique\\_70](#).

#### Default domain name

A unique identifier of an Alibaba Cloud account that is used in scenarios such as RAM user logon and Single Sign On (SSO) management. Alibaba Cloud assigns a default domain name for each Alibaba Cloud account in the `< AccountAli as >. onaliyun . com` format.

For information about how to set a default domain name, see [#unique\\_71](#).

#### Domain alias

A custom domain name that can be used to replace the default domain name provided by the system.



**Note:**

A domain alias can be used only after domain ownership verification.

For information about how to set a domain alias, see [#unique\\_72](#).

#### Access key

The combination of an access key ID and an access key secret. You can use your access key or Alibaba Cloud SDK to sign API requests that you make to Alibaba Cloud.

The access key ID and access key secret are used together to sign programmatic Alibaba Cloud requests cryptographically. The access key ID is used to identify a user, whereas the access key secret is used to encrypt and verify a signature.



**Note:**

The access key secret is displayed only once when you first create it. We recommend that you save the access key secret for subsequent use.

For information about how to create an access key, see [#unique\\_46](#).

### Multi-factor authentication (MFA)

A simple best practice that adds an extra layer of protection on top of your username and password. When you log on to Alibaba Cloud with MFA enabled, the system requires the following two security factors:

1. Your username and password
2. Verification code provided by the MFA device

For information about how to set MFA, see [#unique\\_73](#) and [#unique\\_74](#).

## 5.2 Passwords

### 5.2.1 Change the password for an Alibaba Cloud account

This topic describes how to change the password for an Alibaba Cloud account. You can change your password periodically to protect your password. The password must have a minimum of six characters and must contain a minimum of two of the following character types: letters, special characters, and numbers.

#### Procedure

1. Log on to the [Alibaba Cloud console](#).
2. Move the pointer over the account icon and click Security Settings.
3. In the Login Password section of the Security Settings page, click Change.
4. On the Identity Verification page, select a verification method and click Verify now.
5. In the New Password field, enter a new password and confirm the password.
6. Click Submit.

## 5.2.2 Set a password policy for RAM users

You can set a password policy on your Alibaba Cloud account to specify the complexity requirements and expiration period for passwords of your RAM users.

### Procedure

1. Log on to the [RAM console](#).
2. Choose Identities > Settings.
3. On the Security Settings tab, click Edit Password Rule and set the relevant parameters.

- Password Length: The password must be 8 to 32 characters in length.
- Required Elements in Password: The required elements include lowercase letters, uppercase letters, numbers, and special characters.



**Note:**

To protect your Alibaba Cloud account, we recommend that you select a minimum of two of the preceding elements.

- Password Validity Period: The value range is from 0 to 1,095, in days. The default value is 0, indicating that the password never expires.



**Note:**

The password validity period changes if you reset the password.

- Action After Password Expires: Specifies whether to allow your RAM users to log on to the console after their passwords expire. The options are Deny Logon and Allow Logon.
  - If you select Deny Logon, your RAM users can log on to the console only after you reset the password by using your Alibaba Cloud account.
  - If you select Allow Logon, your RAM users can change their passwords after their passwords expire and log on to the console properly.
- Password History Check Policy: You can prevent RAM users from reusing a specified number of previous passwords. The value range is from 0 to 24. The

default value is 0 , indicating that RAM users are not prevented from reusing previous passwords.

- Password Retry Constraint Policy: The maximum number of permitted logon attempts in an hour. The value range is from 0 to 32. The default value is 0 , indicating that the logon attempts are not limited.



**Note:**

The number of logon attempts is reset to zero after you change the password.

4. Click OK.



**Note:**

The settings of the password policy apply to all RAM users under your Alibaba Cloud account.

### 5.2.3 Change the password for a RAM user

This topic describes how to change the password for a RAM user under your Alibaba Cloud account.

#### Procedure

1. Log on to the [RAM console](#).
2. Choose Identities > Users.
3. In the User Logon Name/Display Name column, click the username of the target RAM user.
4. On the Authentication tab, click Modify Logon Settings.
5. In the Set Logon Password section, select Reset Custom Password.
6. Enter a new password and click OK.



**Note:**

If your Alibaba Cloud account allows RAM users to manage their own passwords, the RAM users can change their passwords in the RAM console by clicking Security and clicking Change Password on the Password Management page.

## 5.3 Basic security settings

### 5.3.1 Check account security

This topic describes how to check the security of your Alibaba Cloud account. You can evaluate your account security based on a security report and complete relevant security settings to protect your account.

#### Procedure

1. Log on to the [RAM console](#).
2. On the Overview page, check the security items.
3. Click a security item and then click Set Now.
4. Complete the relevant security settings.

#### What's next

You can click Download Security Report to download a report that lists security information about your Alibaba Cloud account.

- SubUser: the number of RAM users under your Alibaba Cloud account
- SubUserBindMfa: whether a multi-factor authentication (MFA) device is enabled for RAM users under your Alibaba Cloud account
- SubUserWithUnusedAccessKey: the number of access keys that are not used by RAM users under your Alibaba Cloud account
- RootWithAccessKey: the number of access keys created by your Alibaba Cloud account
- SubUserWithOldAccessKey: the number of existing access keys of RAM users under your Alibaba Cloud account
- SubUserPwdLevel: the password complexity of RAM users under your Alibaba Cloud account
- UnusedAkNum: the number of access keys that are not used by your Alibaba Cloud account
- OldAkNum: the number of existing access keys of your Alibaba Cloud account
- BindMfa: whether an MFA device is enabled for your Alibaba Cloud account
- Score: the security score of your Alibaba Cloud account



Note:

- If your score is less than 60, we recommend that you complete relevant security settings to improve your account security.
- We recommend that you follow the best practices when you use RAM. For more information, see [#unique\\_81](#).

### 5.3.2 Modify logon settings for a RAM user

This topic describes how to modify logon settings for a RAM user.

#### Procedure

1. Log on to the [RAM console](#).
2. Choose Identities > Users.
3. In the User Logon Name/Display Name column, click the username of the target RAM user.
4. Click the Authentication tab.
5. In the Console Logon Management section, click Modify Logon Settings and modify the logon settings for the RAM user.
  - Console Password Logon: specifies whether the RAM user can log on to the console by using a password.
  - Set Logon Password: specifies whether to keep the current password unchanged, whether a default password is generated, or whether the RAM user needs to set a custom password.



#### Note:

If you select `Automatically Regenerate Default Password`, a new password is automatically generated. We recommend that you save the password for subsequent use.

- Password Reset: specifies whether the RAM user must reset the password upon the next logon.
- Enable MFA: specifies whether to enable multi-factor authentication (MFA).



#### Note:

If you select `Required`, the page for enabling an MFA device is automatically displayed when the RAM user logs on to the console.

6. Click OK.



### 5.3.3 Set a security policy for RAM users

This topic describes how to set a security policy for RAM users under your Alibaba Cloud account to better manage RAM user permissions.

#### Procedure

1. Log on to the [RAM console](#).
2. Choose Identities > Settings.
3. On the Security Settings tab, click Update RAM user security settings and set the relevant parameters.
  - **Save MFA Logon Status for 7 Days:** Specifies whether to save the multi-factor authentication (MFA) logon status for your RAM users. The default value is Not Allowed. If you select Allow, the MFA logon status is saved for seven days.
  - **Manage Passwords:** Specifies whether RAM users are allowed to change their own passwords.
  - **Manage AccessKey:** Specifies whether RAM users are allowed to manage their access keys.
  - **Manage MFA Devices:** Specifies whether RAM users are allowed to enable or disable an MFA device.
  - **Logon Session Valid For:** The validity period of the logon sessions. The unit is hours.
  - **Logon Address Mask:** Specifies which IP addresses cannot be used for logon. This parameter is left unspecified by default. That is, all IP addresses can be used for logon. If you specify this parameter, you cannot log on to the console by using a password or through Single Sign On (SSO). However, you can call API actions by using an access key. For information about how to set a logon mask, see [#unique\\_84](#).
4. Click OK.



#### Note:

The settings of the security policy apply to all RAM users under your Alibaba Cloud account.

### 5.3.4 Set a logon mask for an Alibaba Cloud account

This topic describes how to set a logon mask for an Alibaba Cloud account to specify the IP addresses that can be used for logon.

#### Procedure

1. Log on to the [Alibaba Cloud console](#).
2. Move the pointer over the account icon and click Security Settings.
3. In the Login Mask section of the Security Settings page, click Set.
4. On the Login Mask page, enter a correct mask.



#### Note:

If you need to configure multiple masks, separate the masks by using a semicolon (;), for example, 192.168.0.0/16;10.0.0.0/8.

5. Click Save.



#### Note:

After you set a logon mask for your Alibaba Cloud account, you cannot log on to the console by using a password or through Single Sign On (SSO). However, you can call API actions by using an access key.

## 5.4 Advanced settings

### 5.4.1 Manage the default domain name

This topic describes how to view or change the default domain name of an Alibaba Cloud account. Each Alibaba Cloud account has a default domain name, and the domain name can be used by its RAM users to log on to the RAM console. You can customize the logon name suffix by changing the default domain name.

#### Procedure

1. Log on to the [RAM console](#) by using your Alibaba Cloud account.
2. In the left-side navigation pane, click Identities, and click Settings.
3. Click the Advanced tab. In the Default Domain section, you can:
  - View the default domain name of your Alibaba Cloud account. The format of the default domain name is `<$ AccountAli as >. onaliyun . com`. By default, the `AccountAli as` is your Alibaba Cloud account ID. If you have

not specified an account alias, the format of the default domain name is <\$

AccountID >. onaliyun . com .

- Update the domain name. Click Update, enter an account alias, and then click OK.

#### What's next

RAM users then can use the updated domain name to log on to the [RAM console](#).

To log on to the RAM console as a RAM user by using the updated domain name, enter the logon name in the format of <\$ username >@<\$ AccountAli as >. onaliyun . com . For more information, see [#unique\\_88](#).

This also simplifies the procedure to configure the SAML for user-based SSO. For more information, see [Configure the SAML for user-based SSO](#).

## 5.4.2 Create a domain alias

This topic describes how to create a domain alias for an Alibaba Cloud account. A domain alias is an additional domain name that points to your default domain name. RAM users under your Alibaba Cloud account can use your domain alias that can be resolved on the Internet to log on to the RAM console.

#### Procedure

1. Log on to the [RAM console](#) by using your Alibaba Cloud account.
2. In the left-side navigation pane, click Identities, and click Settings.
3. Click the Advanced tab, and click Create Domain Alias.
4. Enter a domain alias.
5. Click OK.
6. Click Domain Ownership Verification to verify the domain ownership.



#### Note:

Before you perform domain ownership verification, make sure that you have added a TXT record for the domain alias in the system of your domain service provider. After you add a domain alias, a random code is generated for domain ownership verification. Copy the verification code, and then click Domain Ownership Verification to verify the domain ownership.

#### What's next

After the domain alias is created, the RAM users under your Alibaba Cloud account can use the domain alias to log on to the [RAM console](#).

To log on to the RAM console as a RAM user by using the domain alias, enter the logon name in the format of <\$ username >@<\$ DomainAlias >. For more information, see [#unique\\_88](#).

The use of domain aliases also simplifies the procedure to configure the SAML for user-based SSO. For more information, see [Configure the SAML for user-based SSO](#).

## 5.5 Access keys

### 5.5.1 Create an access key for a RAM user

This topic describes how to create an access key for a RAM user. An access key is a long-term credential for a RAM user. With an access key, a RAM user can access Alibaba Cloud resources by calling API actions or by using development tools.

#### Procedure

1. Log on to the [RAM console](#).
2. Choose Identities > Users.
3. In the User Logon Name/Display Name column, click the name of the target RAM user.
4. In the User AccessKeys section, click Create AccessKey.



#### Note:

You must enter a verification code if you are creating an access key for the first time.

5. Click OK.



#### Note:

- The access key secret is displayed only once when you first create it. We recommend that you save the access key secret for subsequent use.
- If the access key is mistakenly disclosed or lost, you must create a new one. Currently, you can create a maximum of two access keys.

## 5.5.2 View basic information about an access key

This topic describes how to view basic information about an access key, such as the access key ID, access key status, the latest time when the access key was used, and the date and time when the access key was created.

### Procedure

1. Log on to the [RAM console](#).
2. Choose Identities > Users.
3. In the User Logon Name/Display Name column, click the username of the target RAM user.
4. In the User AccessKeys section, view the access key information.



#### Note:

The access key secret is displayed only once when you first create it.

## 5.5.3 Disable an access key

This topic describes how to disable an access key for a RAM user when the user's permission changes or when the user no longer needs to access Alibaba Cloud resources by calling API actions.

### Procedure

1. Log on to the [RAM console](#).
2. Choose Identities > Users.
3. In the User Logon Name/Display Name column, click the username of the target RAM user.
4. In the User AccessKeys section, click Disable.
5. Click OK.



#### Note:

To enable the access key, click Enable.

## 5.5.4 Delete an access key

This topic describes how to delete an access key of a RAM user when the user no longer needs to access Alibaba Cloud resources by calling API actions or by using development tools.

### Prerequisites

The access key to be deleted is not being used by another RAM user.



**Note:**

Deleting an access key that is currently in use may cause service failure. Exercise caution when performing this action.

#### Procedure

1. Log on to the [RAM console](#).
2. Choose Identities > Users.
3. In the User Logon Name/Display Name column, click the username of the target RAM user.
4. In the User AccessKeys section, click Delete.
5. Click OK.

## 5.6 Multi-factor authentication

### 5.6.1 Enable an MFA device for an Alibaba Cloud account

This topic describes how to enable a multi-factor authentication (MFA) device for your Alibaba Cloud account with the Google Authenticator app. After an MFA device is enabled, it provides additional security protection for your Alibaba Cloud account.

#### Procedure

1. Log on to the [Alibaba Cloud console](#).
2. Move the pointer over the account icon and click Security Settings.
3. In the Account Protection section, click Edit.



**Note:**

Virtual MFA is now renamed TOTP.

4. On the displayed page, select a scenario and select TOTP.
5. Click Submit.
6. On the displayed page, click Verify now.
7. Enter the verification code and click Submit.

## 8. Download and install Google Authenticator on your mobile phone.



**Note:**

If you already installed Google Authenticator, click Next.

- For iOS: Install Google Authenticator from the App Store.
- For Android: Install Google Authenticator from the Google Play Store.



**Note:**

You need to install a QR code scanner from the Google Play Store for Google Authenticator to identify QR codes.

## 9. After you install Google Authenticator, go back to the Identity Verification page and click Next.

## 10. Open Google Authenticator and tap BEGIN SETUP.

- Tap Scan barcode and scan the QR code on the Identity Verification page.
- Tap Manual entry, enter the username and key, and then tap the check mark (✓) icon.



**Note:**

You can obtain the username and key by moving the pointer over Scan failed on the Identity Verification page.

## 11. On the Identity Verification page, enter the 6-digit verification code obtained from Google Authenticator and click Next.



**Note:**

The verification code is refreshed at an interval of 30 seconds.

## What's next

When you log on to Alibaba Cloud with MFA enabled, the system requires the following two security factors:

1. Your username and password
2. Verification code provided by the MFA device



**Note:**

- The MFA settings for your Alibaba Cloud account does not affect the logon of users under the account.
- Before you uninstall or remove an MFA device, you must first log on to the Alibaba Cloud console to disable the MFA device.

## 5.6.2 Disable an MFA device for an Alibaba Cloud account

This topic describes how to disable the multi-factor authentication (MFA) device for your Alibaba Cloud account. After you disable the MFA device, you only need to enter your password when you log on to Alibaba Cloud next time.

### Procedure

1. Log on to the [Alibaba Cloud console](#).
2. Move the pointer over the account icon and click Security Settings.
3. In the Account Protection section, click Edit.



#### Note:

Virtual MFA is now renamed TOTP.

4. In the TOTP section, click Turn off.
5. Click Submit.
6. Open Google Authenticator.
7. On the Identity Verification page, enter the 6-digit verification code obtained from Google Authentication and click Submit.

## 5.6.3 Enable an MFA device for a RAM user

This topic describes how to enable a multi-factor authentication (MFA) device for a RAM user with the Google Authenticator app. After an MFA device is enabled, it provides additional security protection for your Alibaba Cloud account.

### Procedure

1. Log on to the [RAM console](#) by using your Alibaba Cloud account.



#### Note:

- If you selected Required for Enable MFA when you modify the logon settings of a RAM user, the user can go to step 5 when the user logs on to the RAM console.
- If you allow a RAM user under your Alibaba Cloud account to manage its own MFA device, the user can also enable an MFA device in the RAM console. The



procedure is as follows: Click Security. In the left-side navigation pane, click MFA Device Management. Then, click Enable MFA Device.

2. Choose Identities > Users.
3. In the User Logon Name/Display Name column, click the username of the target RAM user.
4. In the MFA Device section, click Enable the device.
5. Download and install Google Authenticator on your mobile phone.
  - For iOS: Install Google Authenticator from the App Store.
  - For Android: Install Google Authenticator from the Google Play Store.



**Note:**

You need to install a QR code scanner from the Google Play Store for Google Authenticator to identify QR codes.

6. Open Google Authenticator and tap BEGIN SETUP.
  - Tap Scan barcode and scan the QR code displayed on the Scan the code tab in the console.
  - Tap Manual entry, enter the username and key, and then tap the check mark (✓) icon.



**Note:**

You can obtain the username and key from the Retrieval manually enter information tab in the console.

7. On the Scan the code tab, enter the two consecutive verification codes obtained from Google Authenticator and click Enable.



**Note:**

The verification code is refreshed at an interval of 30 seconds.

## What's next

When a RAM user logs on to the RAM console with MFA enabled, the system requires the following two security factors:

1. Username and password of the RAM user
2. Two consecutive verification codes provided by the MFA device

**Note:**

Before you uninstall or remove an MFA device from a RAM user, you must first log on to the Alibaba Cloud console to disable the MFA device.

## 5.6.4 Disable an MFA device for a RAM user

This topic describes how to disable the multi-factor authentication (MFA) device for a RAM user under your Alibaba Cloud account.

### Procedure

1. Log on to the [RAM console](#) by using your Alibaba Cloud account.

**Note:**

If you allow a RAM user under your Alibaba Cloud account to manage its own MFA device, the user can also disable an MFA device in the RAM console. The procedure is as follows: Click Security. In the left-side navigation pane, click MFA Device Management. Then, click Disable MFA Device.

2. Choose Identities > Users.
3. In the User Logon Name/Display Name column, click the username of the target RAM user.
4. In the MFA Device section, click Disable the virtual MFA device.
5. Click OK.

## 6 SSO management

---

### 6.1 SSO overview

This topic describes the concepts and methods of Single Sign On (SSO), also known as identity federation. Enterprises can implement SSO to their Alibaba Cloud accounts by using SAML 2.0.

#### Concepts

Identity provider (IdP)	<p>A RAM entity that provides identity management services. IdPs are generally classified into the following types:</p> <ul style="list-style-type: none"><li>· Locally deployed IdPs, such as Microsoft Active Directory Federation Service (AD FS) and Shibboleth</li><li>· Cloud-based IdPs, such as Azure AD, Google G Suite, Okta, and OneLogin</li></ul>
Service provider (SP)	<p>An application that uses the identity management function of an IdP to provide users with specific services. An SP uses the user information provided by an IdP. In some identity systems (such as OpenID Connect) that do not comply with the SAML protocol, SP is known as relying party, which means the relying party of an IdP.</p>
Security Assertion Markup Language 2.0 (SAML 2.0)	<p>A protocol for enterprise-level user identity authentication. It can be used to achieve communication between an SP and an IdP. SAML 2.0 is a standard that enterprises can use to implement enterprise-level SSO.</p>
SAML assertion	<p>A core element in the SAML protocol to describe the authentication request and response. For example, specific properties of a user are contained in the authentication response assertion.</p>
Trust	<p>A mutual trust mechanism between an SP and an IdP. It is usually implemented by using public and private keys. An SP obtains SAML metadata of an IdP in a trusted way. The metadata includes the public key</p>

for verifying the SAML Assertion issued by the IdP. The SP can use the public key to verify the assertion integrity.

## Methods of SSO

Enterprises can implement SSO with Alibaba Cloud through SAML 2.0-based IdPs (for example, AD FS). Alibaba Cloud offers the following two SAML 2.0-based SSO methods:

- **User-based SSO:** The RAM user that you can use to log on to Alibaba Cloud can be determined through a SAML assertion. After logon, you can use the RAM user to access Alibaba Cloud. For more information, see [#unique\\_103](#).
- **Role-based SSO:** The RAM role that you can use to log on to Alibaba Cloud can be determined through SAML assertions. After logon, you can use the role specified in the SAML assertion to access Alibaba Cloud. For more information, see [#unique\\_104](#).

## Comparison between role-based SSO and user-based SSO

SSO method	Supports SSO initiated by SP?	Supports SSO initiated by IdP?	Supports logon with your RAM account and password?	Supports association of one IdP and multiple Alibaba Cloud accounts?	Supports multiple IdPs?
User- based SSO	Yes	Yes	No	No	No
Role-based SSO	No	Yes	Yes	Yes	Yes



**Note:**

For more information, see [#unique\\_105](#).

## 6.2 Application scenarios of SSO

This topic describes the application scenarios of two SSO methods supported by Alibaba Cloud: role-based SSO and user-based SSO.

### Role-based SSO

Application scenarios:

- You do not want to create or manage users on Alibaba Cloud to avoid user synchronization and reduce costs.
- You want to implement SSO to Alibaba Cloud and manage some users on Alibaba Cloud. The users managed on Alibaba Cloud can be used to test new features of Alibaba Cloud and log on to Alibaba Cloud if your network or identity provider (IdP) encounters exceptions.
- You want to manage the operation permissions on Alibaba Cloud according to the user groups in your local IdP or a specific user attribute. Then, you can manage user permissions by grouping users in your local IdP or changing the attribute of a user.
- You have multiple Alibaba Cloud accounts and only one IdP. You want to implement SSO to multiple Alibaba Cloud accounts by configuring your IdP only once.
- You have multiple IdPs and only one Alibaba Cloud account. You want to implement SSO from multiple IdPs to one Alibaba Cloud account by configuring IdPs in the Alibaba Cloud account.
- You want to implement SSO by using the console or by calling APIs.

### User-based SSO

Application scenarios:

- You want to initiate logon from Alibaba Cloud, not from your IdP.
- Some of your Alibaba Cloud services cannot be accessed by roles (that is, through STS). For more information about Alibaba Cloud services that can be accessed by roles, see [#unique\\_64](#).
- Your IdP does not support complex configuration of attributes.
- You want to simplify IdP configuration.

## 6.3 User-based SSO

### 6.3.1 Overview of user-based SSO

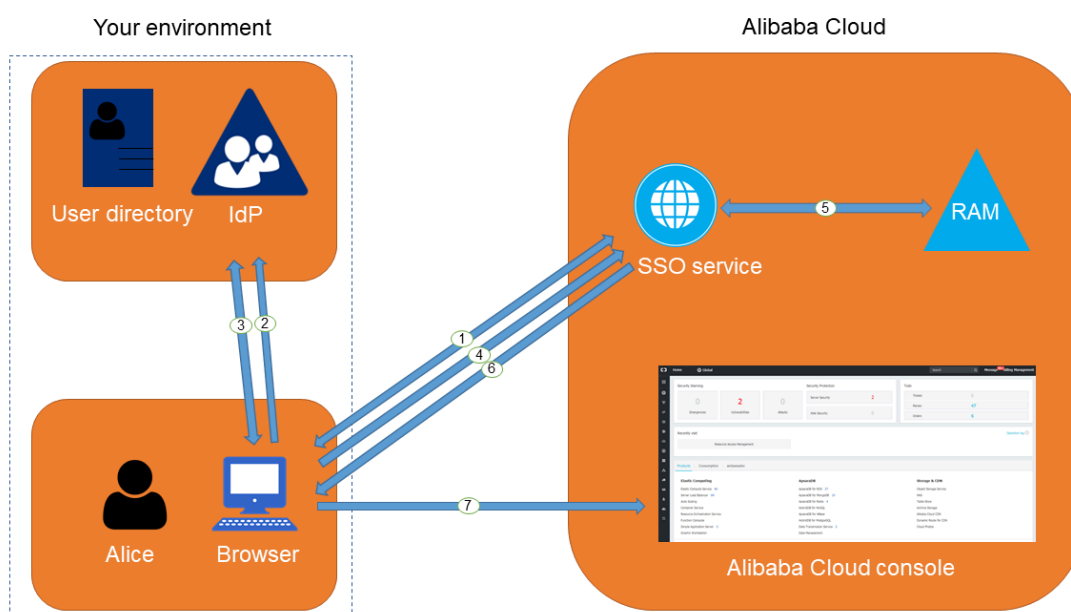
This topic describes the scenario, process, and configuration of user-based Single Sign On (SSO).

#### Scenario

In scenarios where Alibaba Cloud and the identity management system of an enterprise work together to perform user-based SSO, Alibaba Cloud is the service provider (SP) and the enterprise system is the identity provider (IdP). User-based SSO allows an employee in the enterprise to access Alibaba Cloud as a RAM user.

#### User-based SSO process

Figure 6-1: Process



As shown in the preceding figure, after the administrator configures user-based SSO, the employee (Alice) can log on to Alibaba Cloud after the following steps are completed:

1. Alice logs on to the Alibaba Cloud console through a browser, and Alibaba Cloud returns an SAML authentication request to the browser.
2. The browser forwards the SAML authentication request to the IdP.
3. The IdP prompts Alice to log on and returns an SAML response to the browser.

4. The browser forwards the SAML response to the SSO service.
5. Through the SAML mutual trust configuration, the SSO service verifies the digital signature in the SAML response to check the authenticity of the SAML assertion, and then matches the identity of the RAM user according to the value of `NameID` in the SAML assertion.
6. The SSO service returns the URL of the Alibaba Cloud console to the browser.
7. The browser redirects to the Alibaba Cloud console.

**Note:**

In step 1, the employee does not necessarily have to log on to Alibaba Cloud. Instead, the employee can click the link on the IdP portal to send an SAML authentication request to the IdP and access the Alibaba Cloud console.

### User-based SSO configuration

Before you use user-based SSO, you must set configurations to establish trust between Alibaba Cloud and your IdP.

1. To make sure your IdP is trusted by Alibaba Cloud, you must configure the IdP in the Alibaba Cloud console.

For more information, see [Configure the SAML of an account](#).

2. To make sure Alibaba Cloud is trusted by the IdP, you must configure Alibaba Cloud as a trusted SAML SP and configure an SAML assertion in your IdP.

For more information, see [#unique\\_109](#).

3. After the IdP and Alibaba Cloud are configured, you must create RAM users to match your IdP through SDK, CLI, or logging on to the RAM console.

For more information, see [#unique\\_45](#).

The processes of configuring an SAML assertion and an SAML SP vary according to the IdP system. For more information about how to implement user-based SSO from Microsoft Active Directory Federation Service (AD FS) to Alibaba Cloud, see [#unique\\_110](#).

## 6.3.2 Configure the SAML for user-based SSO

This topic describes how to configure the metadata for user-based Single Sign On (SSO) according to SAML 2.0 to establish trust between your identity provider (IdP) and Alibaba Cloud.

### Prerequisites

A default domain name, a domain alias, or an auxiliary domain name is set to simplify SAML SSO. For more information, see [#unique\\_71](#) and [#unique\\_72](#).

### Procedure

1. Log on to the [RAM console](#).
2. In the left-side navigation pane, click SSO.
3. Click the User-based SSO tab.
4. In the SSO Settings section, click Modify to modify the SSO settings as needed.

- SSO Status: You can enable or disable the SSO function as needed.



#### Note:

This setting applies to all RAM users under your Alibaba Cloud account.

- The SSO function is disabled by default. If the SSO function is disabled, RAM users can use their passwords for logon, and all SSO settings do not take effect.
- If you enable the SSO function, RAM users cannot use their passwords for logon. They must log on to an IdP for identity authentication. If the SSO function is disabled later, the page for logon by using passwords is automatically displayed.
- Metadata File: You can click Upload to upload the metadata file provided by your IdP.



#### Note:



The metadata file, usually in XML format, is provided by an IdP. It contains the IdP's logon service address and X.509 public key certificate that is used to verify the validity of the SAML assertion issued by the IdP.

- **Auxiliary Domain: (Optional)** You can turn on or turn off this function as needed.
  - If you turn on this function, you can set an auxiliary domain name and use it as the suffix of the `NameID` element in the SAML assertion.
  - If you turn off this function, you can only use the default domain name or domain alias of your Alibaba Cloud account as the suffix of the `NameID` element in the SAML assertion.

For more information about values of the `NameID` element, see [#unique\\_109](#).



**Note:**

If you set a domain alias and an auxiliary domain name at the same time, only the domain alias or the default domain name can be used as the suffix of the `NameID` element.

### What's next

You can migrate or synchronize data from your IdP to Alibaba Cloud or Alibaba Cloud RAM by using either of the following methods:

- Log on to the [RAM console](#) and create RAM users that match the users in your IdP.
- Use a RAM SDK to write a program or use Alibaba Cloud command line interface (CLI) to customize a solution.

## 6.3.3 Configure the SAML of an IdP during user-based SSO

This topic describes how to configure the SAML of an identity provider (IdP) during user-based Single Sign On (SSO). You can configure Alibaba Cloud as a trusted SAML service provider (SP), and configure an SAML assertion in the IdP.

### Procedure

1. Obtain the SAML SP metadata URL from Alibaba Cloud.
  - a) Log on to the [RAM console](#) by using your Alibaba Cloud account.
  - b) In the left-side navigation pane, click SSO.
  - c) Click the User-based SSO tab.
  - d) Copy the SAML SP metadata URL.

2. Create an SAML SP in your IdP and then configure Alibaba Cloud as the relying party by using one of the following methods:

- Copy and paste the SAML SP metadata URL of Alibaba Cloud into your IdP.
- If your IdP does not support URL configuration, click Copy next to SAML Service Provider Metadata URL to download an XML file. Then, when you create an SAML SP, you can upload the XML file.
- If you fail to upload an XML file to your IdP, configure the following parameters:
  - `Entity ID` : The value of the `entityID` attribute in the `md` : `EntityDesc` `riptor` element of the metadata XML file.
  - `ACS URL` : The value of the `Location` attribute in the `md` : `AssertionC` `onsumerSer` `vice` element of the metadata XML file.
  - `RelayState` : Optional. If the `RelayState` parameter is available in your IdP, you can set this parameter to the URL to be directed after SSO succeeds. If this parameter is left unspecified, the home page of the Alibaba Cloud console is directed after SSO succeeds.



Note:

Only the URL in the `*. console . aliyun . com` or `*. console . alibabacloud . com` domain can be set for `RelayState`.

### What's next

After you configure Alibaba Cloud as a trusted SAML SP, you need to configure an SAML assertion in the IdP.

Alibaba Cloud uses a User Principal Name (UPN) to locate a RAM user. Therefore, the SAML response generated by the IdP must contain the UPN of the RAM user. Alibaba Cloud resolves the `NameID` element in the SAML assertion, then matches the `NameID` element to the UPN of the corresponding RAM user, so that user-based SSO can be implemented.

If you configure the SAML assertion issued by the IdP, you must map the UPN of the target RAM user to the `NameID` element in the SAML assertion. The `NameID` element must contain one of the following suffixes:

- The domain alias of your Alibaba Cloud account, for example, `< username >@< domain_ali as >`. Here, the `<username>` sub-element is the username of a

RAM user, and the `< domain_alias >` sub-element is the domain alias. For information about how to set a domain alias, see [#unique\\_72](#).

- The auxiliary domain name that is set for user-based SSO, for example, `< username >@< auxiliary_ domain >`. Here, the `<username>` sub-element is the username of a RAM user, and the `< auxiliary_ alias >` sub-element is the auxiliary domain name. For information about how to set an auxiliary domain name, see [Set an auxiliary domain name](#).



**Note:**

If you set a domain alias and an auxiliary domain name at the same time, only the domain alias can be used as the suffix of the `NameID` element.

- The default domain name of your Alibaba Cloud account, for example, `< username >@< default_domain >`. Here, the `<username>` sub-element is the username of a RAM user, and the `< default_domain >` sub-element is the default domain name. For information about how to set a default domain name, see [#unique\\_71](#).



**Note:**

You can use the default domain name of your Alibaba Cloud account as the suffix of the `NameID` element regardless of whether you set a domain alias or an auxiliary domain name.

Assume that you have a RAM user named `Alice`, and the default domain name of your Alibaba Cloud account is `example . onaliyun . com`.

- If you set the domain alias of your Alibaba Cloud account to `example . com`, the `NameID` element in the SAML assertion is `Alice @ example . onaliyun . com` or `Alice @ example . com`.
- If you do not have a domain alias and set the auxiliary domain name to `example2 . com`, the `NameID` element in the SAML assertion is `Alice @ example . onaliyun . com` or `Alice @ example2 . com`.
- If you set the domain alias of your Alibaba Cloud account to `example . com` and the auxiliary domain name to `example2 . com`, the `NameID` element in the SAML assertion is `Alice @ example . onaliyun . com` or `Alice @ example . com`.

### 6.3.4 Implement user-based SSO by using AD FS

This topic provides an example of how to implement user-based Single Sign On (SSO) from AD FS to Alibaba Cloud, detailing the end-to-end SSO process from an enterprise identity provider (IdP) to Alibaba Cloud.

#### Notes

This topic uses Windows Server 2012 R2 as an example to describe how to implement user-based SSO from AD FS to Alibaba Cloud.

#### Prerequisites

Microsoft AD is properly configured and the following server roles are configured on Windows Server 2012 R2:

- DNS server: resolves and sends identity authentication requests to the correct Federation Service.
- Active Directory Domain Service (AD DS): creates, queries, and modifies objects such as domain users and domain devices.
- Active Directory Federation Service (AD FS): configures the identity federation relying party and performs SSO authentication for the configured relying party.

#### Example configuration

The configuration details used in the example are as follows:

- The default domain name of the Alibaba Cloud account: `secloud . onaliyun . com`.
- The RAM user under the Alibaba Cloud account: `alice`. The User Principal Name (UPN) of the RAM user is `alice @ secloud . onaliyun . com`.
- The AD FS of the on-premises Microsoft AD: `adfs . secloud . club`.
- The domain name of the on-premises Microsoft AD: `secloud . club`. The NETBIOS is `secloud`.
- The UPN of the RAM user (Alice) in Microsoft AD: `alice @ secloud . club`. The RAM user can also use `secloud \ alice` for intra-domain logon.

## Configure AD FS as a trusted SAML IdP in RAM

1. Enter the following URL in your browser:

```
https://adfs.secloud.club/Federation/Metadata/2007-06/FederationMetadata.xml
```

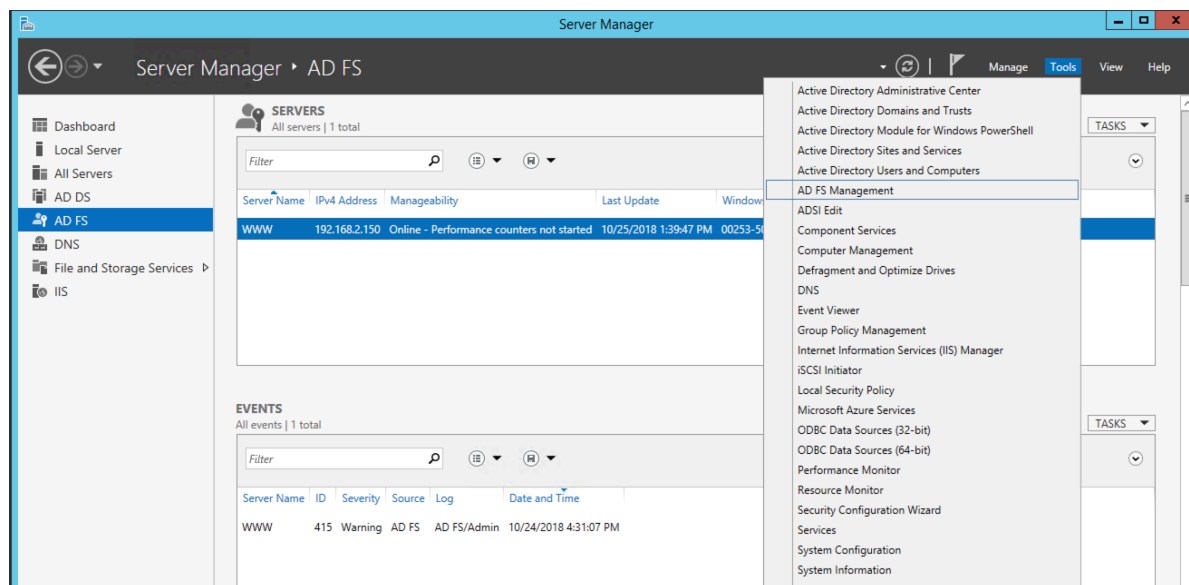
2. Download the metadata file in XML format.
3. In the RAM console, use the metadata file for SSO configuration.

For more information, see [#unique\\_113](#).

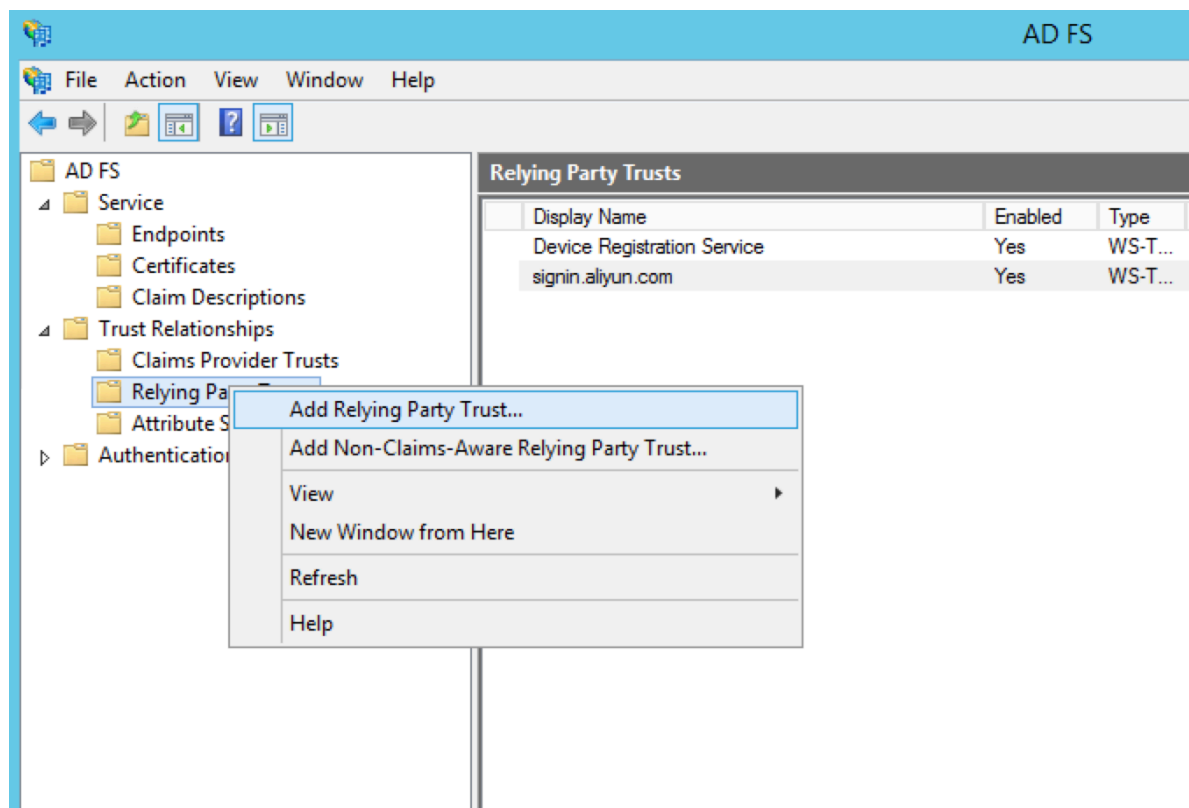
## Configure Alibaba Cloud as a trusted SAML SP in AD FS

In AD FS, SAML SP is called relying party. To configure Alibaba Cloud as a trusted SP, follow these steps:

1. On the Server Manager page, choose Tools > AD FS Management.



## 2. Select Add Relying Party Trust.



### 3. Set the SAML metadata of Alibaba Cloud for the relying party.

To view the SAML metadata URL, log on to the [RAM console](#), click SSO in the left-side navigation pane, and click User-based SSO. You can enter the metadata URL when configuring the AD FS relying party.

The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar says 'Add Relying Party Trust Wizard'. The main area is titled 'Select Data Source'. On the left, there is a 'Steps' pane with the following steps: Welcome (selected), Select Data Source (current), Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main content area has the instruction: 'Select an option that this wizard will use to obtain data about this relying party:'. There are three radio button options: 1. 'Import data about the relying party published online or on a local network' (selected). Description: 'Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.' Input field: 'Federation metadata address (host name or URL):' with the value 'https://signin.alibabacloud.com/saml/SpMetadata.xml?tenantID=58167'. Example text: 'Example: fs.contoso.com or https://www.contoso.com/app'. 2. 'Import data about the relying party from a file'. Description: 'Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.' Input field: 'Federation metadata file location:' with a 'Browse...' button. 3. 'Enter data about the relying party manually'. Description: 'Use this option to manually input the necessary data about this relying party organization.' At the bottom right are buttons: '< Previous', 'Next >', and 'Cancel'.

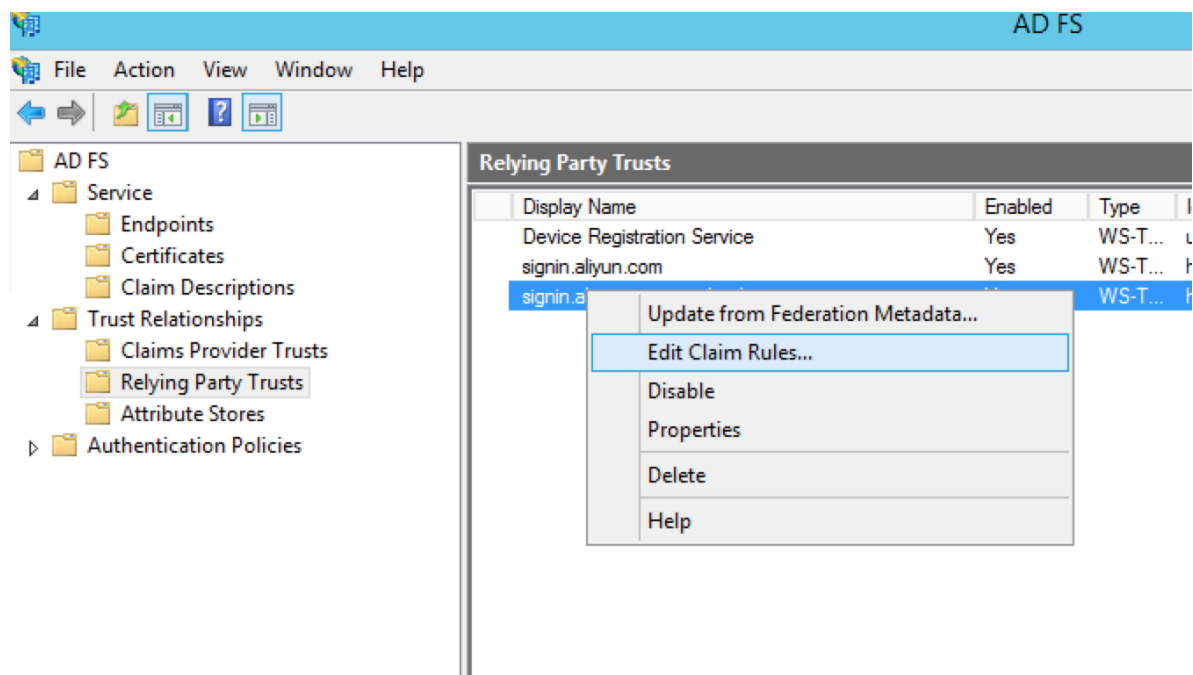
After the relying party is configured, Alibaba Cloud sends a request to authenticate RAM users under the Alibaba Cloud account whose default domain name is `secloud.onaliyun.com` to AD FS `adfs.secloud.club`. AD FS receives the request from Alibaba Cloud, authenticates the user, and sends a response to Alibaba Cloud.

#### Configure the SAML assertion attributes for the Alibaba Cloud SP

We recommend that you set the value of the `NameID` field in the SAML assertion to the UPN of the RAM user, so that Alibaba Cloud can locate the correct RAM user according to the SAML response.

You must set the UPN in the AD to the `NameID` in the SAML assertion. The procedure is as follows:

1. Right-click the display name of the relying party and select Edit Claim Rules.



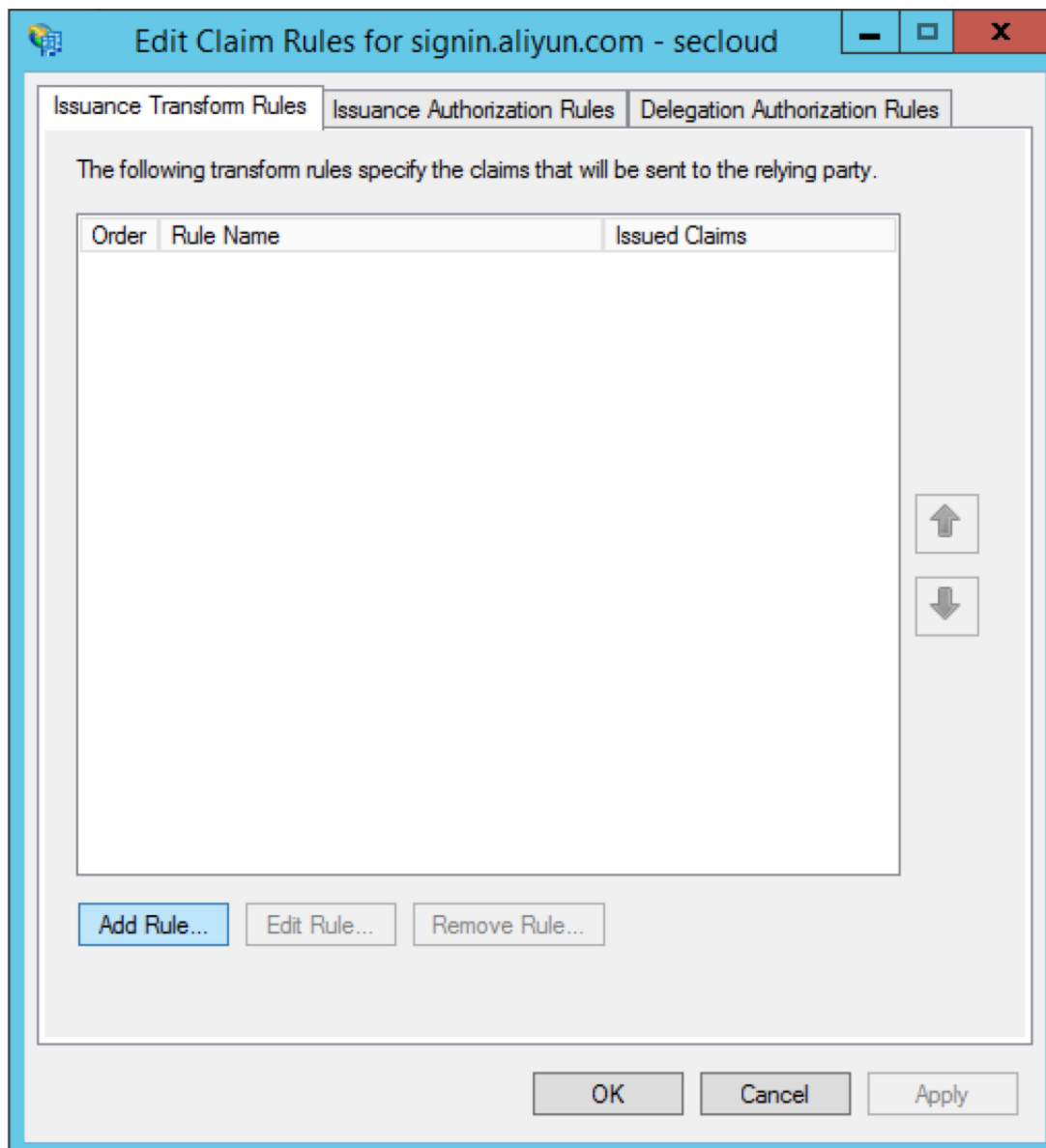
2. Click Issuance Transform Rules to add a rule.



Note:



Issuance Transform Rules indicates how to transform a known user attribute and issue it as an attribute in the SAML assertion. You must issue the UPN of a user in Microsoft AD as a `NameID` . This means that a new rule is required.



### 3. From the Claim rule template drop-down list, select Transform an Incoming Claim.

**Add Transform Claim Rule Wizard**

**Select Rule Template**

**Steps**

- Choose Rule Type
- Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Transform an Incoming Claim

Claim rule template description:

Using the Transform an Incoming Claim rule template you can select an incoming claim, change its claim type, and optionally change its claim value. For example, you can use this rule template to create a rule that will send a role claim with the same claim value of an incoming group claim. You can also use this rule to send a group claim with a claim value of "Purchasers" when there is an incoming group claim with a value of "Admins". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited. For more information on the sources of incoming claims, click Help.

< Previous   Next >   Cancel

### 4. Select Edit Rule.



#### Note:

In this example, the domain name of the UPN in the Alibaba Cloud account is

secloud . onaliyun . com , and the domain name of the UPN in Microsoft AD

is `secloud . club` . If you directly map the UPN in Microsoft AD to the `NameID` , Alibaba Cloud cannot match the correct user.

To solve this problem, use one of the following methods:

- a. Method 1: Set the domain name of Microsoft AD to the domain alias of your Alibaba Cloud account.

If the domain name `secloud . club` of Microsoft AD is registered in a DNS on the Internet, you can set `secloud . club` to the domain alias of RAM. For information about how to set a domain alias, see [#unique\\_72](#).

After the settings are completed, map the UPN to the `NameID` on the Edit Rule page.

**Edit Rule**

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Rule template: Transform an Incoming Claim

Incoming claim type:

Incoming name ID format:

Outgoing claim type:

Outgoing name ID format:

☒ Pass through all claim values

☐ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value:

☐ Replace incoming e-mail suffix claims with a new e-mail suffix

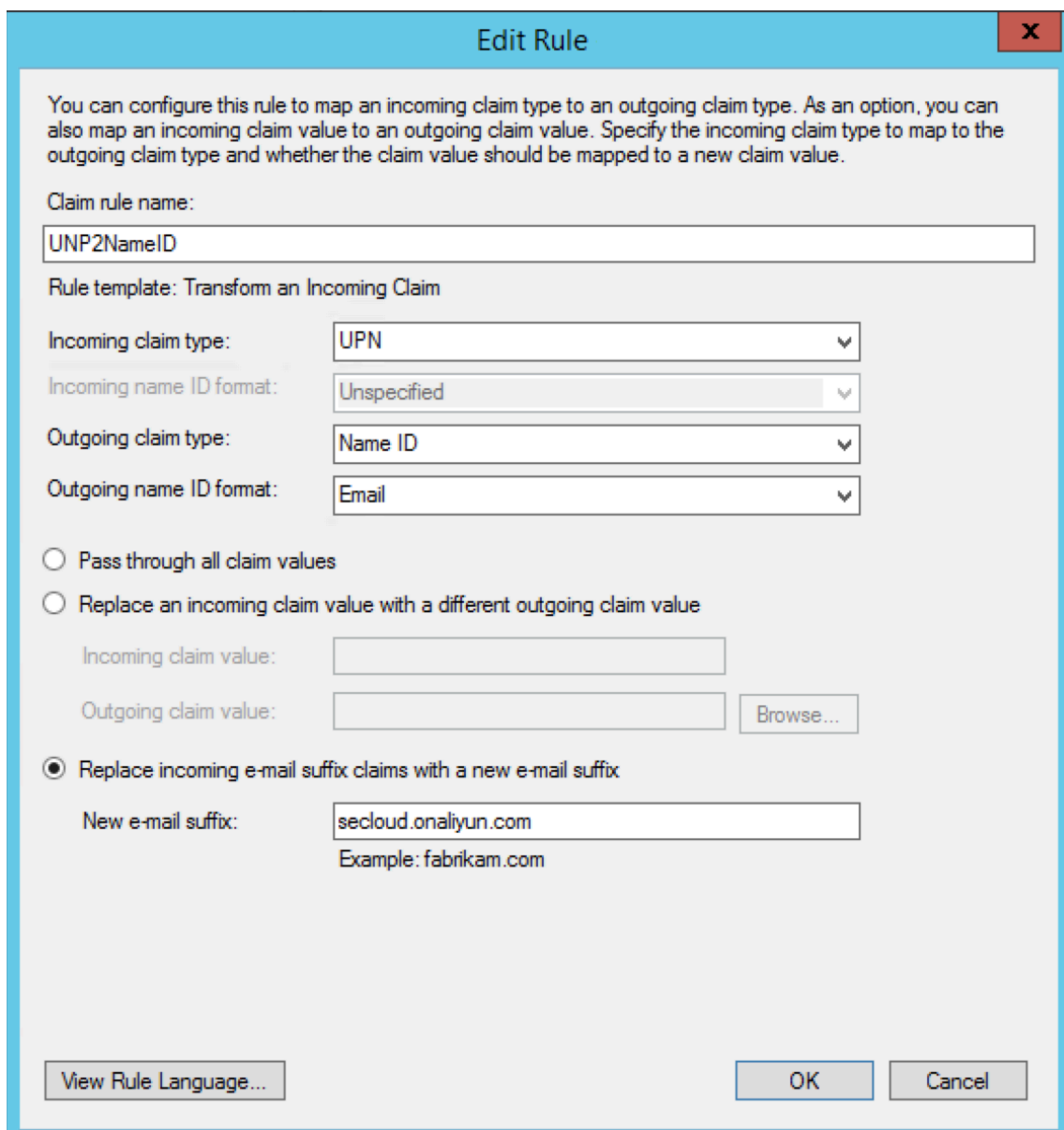
New e-mail suffix:

Example: fabrikam.com

**b. Method 2: Transform the domain names in AD FS.**

If the domain name `secloud . club` is an intranet domain name of an enterprise, Alibaba Cloud cannot verify the domain ownership of the enterprise. RAM can only use the default domain name `secloud . onaliyun . com`.

In this case, in the SAML assertion issued by AD FS to Alibaba Cloud, you must replace the domain name suffix `secloud . club` of the UPN with `secloud . onaliyun . com`.



**Edit Rule**

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Rule template: Transform an Incoming Claim

Incoming claim type:

Incoming name ID format:

Outgoing claim type:

Outgoing name ID format:

☐ Pass through all claim values

☐ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value:

☒ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

**c. Method 3: Set the domain name of Microsoft AD to an auxiliary domain name.****Note:**

You can configure auxiliary domain by modifying SSO settings on the User-based SSO tab.

If the domain name `secloud . club` is an intranet domain name of an enterprise, Alibaba Cloud cannot verify the domain ownership of the enterprise. In this case, you can set `secloud . onaliyun . com` to the auxiliary domain name. For information about how to set an auxiliary domain name, see [Set an auxiliary domain name](#).

After the settings are completed, map the UPN to the `NameID` on the Edit Rule page.

**Edit Rule**

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Rule template: Transform an Incoming Claim

Incoming claim type:

Incoming name ID format:

Outgoing claim type:

Outgoing name ID format:

☒ Pass through all claim values

☐ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value:

☐ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

## 6.4 Identity providers

### 6.4.1 Create an identity provider

This topic describes how to create an identity provider (IdP). You must create an IdP before you use role-based Single Sign On (SSO).

#### Procedure

1. Log on to the [RAM console](#).
2. In the left-side navigation pane, click SSO.
3. On the Role-based SSO tab, click Create IdP.
4. Enter an IdP name and description.
5. In the Metadata File section, click Upload to upload a metadata file.



#### Note:

The metadata file, usually in XML format, is provided by an IdP. It contains the logon service address of the IdP, the public key for verifying the SAML assertion, and the assertion format.

6. Click OK.

### 6.4.2 View basic information about an identity provider

This topic describes how to view basic information about an identity provider (IdP), such as the IdP name and the Alibaba Cloud Resource Name (ARN) of the IdP.

#### Procedure

1. Log on to the [RAM console](#).
2. In the left-side navigation pane, click SSO.
3. On the Role-based SSO tab, click the name of the target IdP.
4. In the IdP Information section, view the IdP information.

### 6.4.3 Modify basic information about an identity provider

This topic describes how to modify basic information about an identity provider (IdP), such as the IdP description and the metadata file.

#### Procedure

1. Log on to the [RAM console](#).
2. In the left-side navigation pane, click SSO.

3. On the Role-based SSO tab, click the name of the target IdP.
4. In the IdP Information section, click Modify.



Note:

The IdP name cannot be modified.

5. Click OK.

## 6.4.4 Delete an identity provider

This topic describes how to delete an identity provider (IdP) that you no longer need. After you delete your IdP, you cannot perform Single Sign On (SSO) between your enterprise and Alibaba Cloud RAM.

### Procedure

1. Log on to the [RAM console](#).
2. In the left-side navigation pane, click SSO.
3. On the Role-based SSO tab, find the target IdP and click Delete.
4. Click OK.

## 6.5 Role-based SSO

### 6.5.1 Overview of role-based SSO

This topic describes the scenario, process, and configuration of role-based Single Sign On (SSO).

#### Scenario

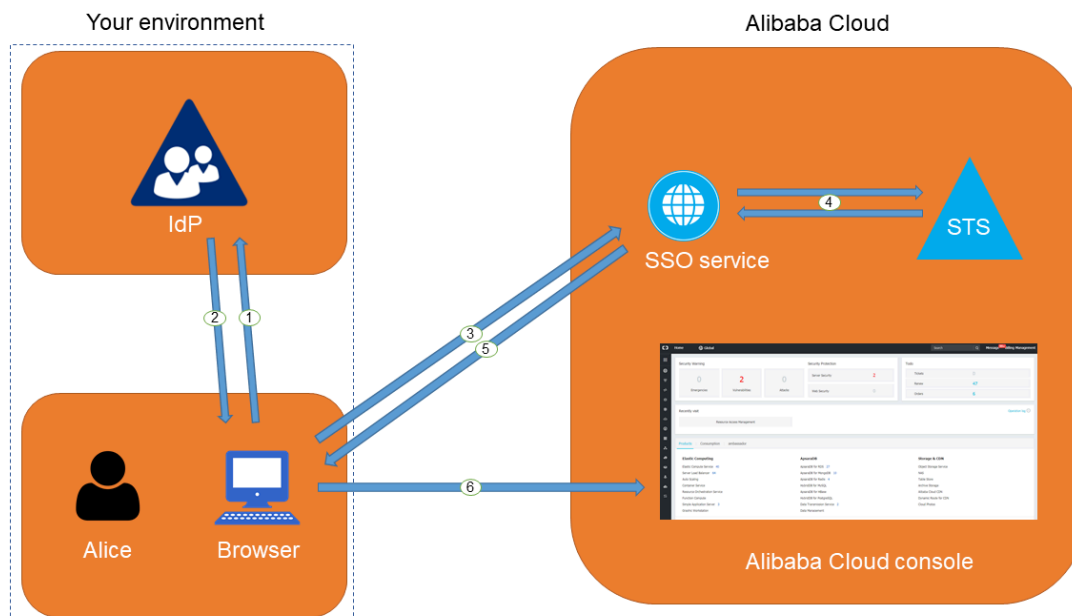
In scenarios where Alibaba Cloud and the identity management system of an enterprise work together to perform role-based SSO, Alibaba Cloud is the service provider (SP) and the enterprise system is the identity provider (IdP). Through role-based SSO, the enterprise can manage users in the local IdP without synchronizing users from your IdP to Alibaba Cloud, and the enterprise employee can log on to Alibaba Cloud by using a specific RAM role.

#### Role-based SSO process

Through role-based SSO, you can access Alibaba Cloud either by logging on to the Alibaba Cloud console or by using a program.

## Access Alibaba Cloud through the console

Figure 6-2: Process



As shown in the figure, after the administrator configures role-based SSO, the employee (Alice) can log on to Alibaba Cloud after the following steps are completed:

1. Alice uses the browser to select Alibaba Cloud as the target service on the login page of the IdP.

For example, if the IdP is Microsoft Active Directory Federation Service (AD FS), the log on URL will be `https://ADFSServiceName/adfs/ls/IdpInitiatedSignOn.aspx`.

**Note:**

Some IdPs require users to log on first and then select an SSO application that represents Alibaba Cloud.

2. The IdP generates a SAML response to the browser.
3. The browser redirects to the page of the SSO service, and forwards the SAML response.



4. The SSO service uses the SAML response to request an STS token from the Alibaba Cloud STS service, and generates a URL that can log on to the Alibaba Cloud console with the STS token.

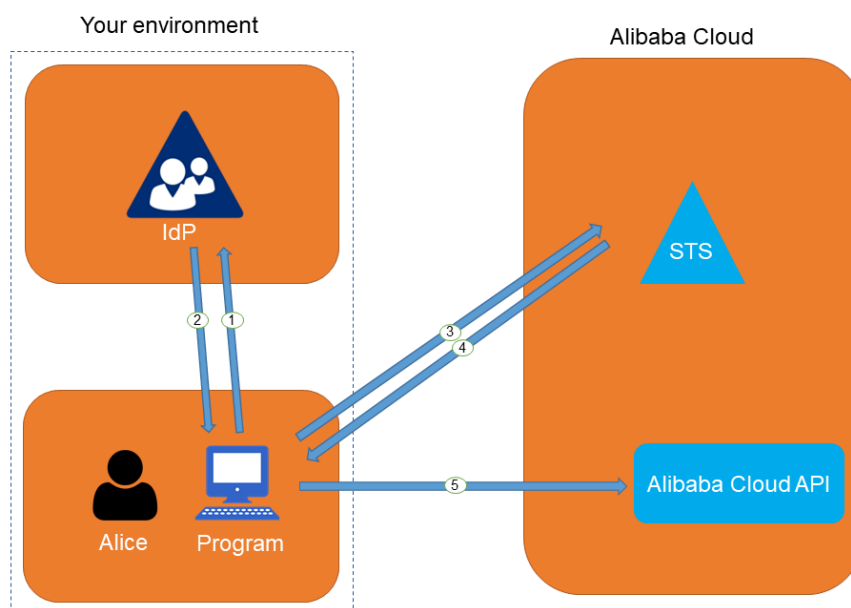
**Note:**

If the SAML response contains attributes that map to multiple RAM roles, the user is prompted to select a role firstly.

5. The SSO service returns the URL to the browser.
6. The browser redirects to the URL, and logs on to the Alibaba Cloud console with the specific RAM role.

Access Alibaba Cloud through a program

Figure 6-3: Process



As shown in the figure, the employee (Alice) can log on to Alibaba Cloud after the following steps are completed:

1. Alice initiates an authentication request to the IdP through a program.
2. The IdP generates a SAML response that contains the user's SAML assertion, and returns the SAML response to the program.
3. The program calls the [#unique\\_122](#) API action of the Alibaba Cloud STS service, and forwards the information including the ARN of an Alibaba Cloud IdP, the ARN of the role to be assumed, and the SAML assertion obtained from the IdP.

4. The STS service verifies the SAML assertion and returns an STS token to the program.
5. The program calls an Alibaba Cloud API action with the STS token.

### Configure role-based SSO

Before you use role-based SSO, you must set configurations to establish trust between Alibaba Cloud and your IdP.

1. To make sure your IdP is trusted by Alibaba Cloud, you must configure the IdP in the Alibaba Cloud console.

For more information, see [#unique\\_123](#).

2. You must use a program or log on to the RAM console to create RAM roles and grant permissions to them.

For more information, see [#unique\\_124](#).

3. To make sure Alibaba Cloud is trusted by the IdP, you must configure Alibaba Cloud as a trusted SAML SP and configure SAML assertions in your IdP.

For more information, see [#unique\\_125](#).

The processes of configuring SAML assertions and an SAML SP vary according to the IdP system. For more information about how to implement role-based SSO from AD FS to Alibaba Cloud, see [#unique\\_126](#).

## 6.5.2 Configure the SAML for role-based SSO

This topic describes how to configure the metadata for role-based Single Sign On (SSO) according to SAML 2.0, to establish trust between your identity provider (IdP) and Alibaba Cloud.

### Procedure

1. Log on to the [RAM console](#).
2. In the left-side navigation pane, click SSO.
3. On the Role-based SSO tab, click Create IdP.
4. Enter an IdP name and description.
5. In the Metadata File section, click Upload to upload a metadata file.



Note:

The metadata file, usually in XML format, is provided by an IdP. It contains the logon service address of the IdP, the public key for verifying the SAML assertion, and the assertion format.

6. Click OK.

### What's next

After you create an IdP in RAM, you must create one or more RAM roles with the trusted entity type set to IdP, to establish an association between the IdP and Alibaba Cloud.

Click Create RAM Role to navigate to the page for creating RAM roles. For more information about how to create a RAM role, see [#unique\\_124](#).

## 6.5.3 Configure the SAML of an IdP during role-based SSO

This topic describes how to configure the SAML of an identity provider (IdP) during role-based Single Sign On (SSO). You can configure Alibaba Cloud as a trusted SAML service provider (SP), and configure SAML assertions in the IdP.

### Procedure

1. Obtain the SAML SP metadata URL `https://signin.alibabacloud.com/saml-role/sp-metadata.xml`.
  - a) Log on to the [RAM console](#) by using your Alibaba Cloud account.
  - b) In the left-side navigation pane, click SSO.
  - c) On the Role-based SSO tab, copy the SAML SP metadata URL.

2. Create an SAML SP in your IdP and configure Alibaba Cloud as the relying party by using one of the following methods:

- Copy and paste the SAML SP metadata URL of Alibaba Cloud into your IdP.
- If your IdP does not support URL configuration, click Copy next to SAML Service Provider Metadata URL to download an XML file. Then, when you create an SAML SP, you can upload the XML file.
- If you fail to upload an XML file to your IdP, configure the following parameters:
  - Entity ID : `urn : alibaba : cloudcomputing : international`
  - ACS URL : `https :// signin . alibabacloud . com / saml - role / sso`
  - RelayState : Optional. If the RelayState parameter is available in your IdP, you can set this parameter to the URL to be directed after SSO succeeds. If this parameter is left unspecified, the home page of the Alibaba Cloud console is directed after SSO succeeds.



**Note:**

Only the URL in the `*. console . aliyun . com` or `*. console . alibabacloud . com` domain can be set for RelayState .

### What's next

After you configure Alibaba Cloud as a trusted SAML SP, you must configure SAML assertions in your IdP.

Alibaba Cloud resolves an SAML assertion to determine a RAM role. Therefore, the SAML assertions generated by your IdP must contain the necessary information of the RAM role.

For more information about SAML assertions, see [#unique\\_129](#).

## 6.5.4 SAML assertions for role-based SSO

This topic describes the mandatory attribute elements in SAML assertions issued by your identity provider (IdP) for role-based SSO.

### Scenario

During SAML 2.0-based SSO, after the identity of a user is verified, your IdP generates an authentication response and sends it to Alibaba Cloud through a browser or a program. This response contains an SAML assertion that complies with the HTTP POST Binding for SAML 2.0 standard.

Alibaba Cloud uses the SAML assertion to determine the logon status and identity of the user. Therefore, the SAML assertion must contain elements that are required by Alibaba Cloud.

### Common elements in SAML 2.0

- **Issuer**

The value of the **Issuer** element must match the **EntityID** in the IdP metadata file uploaded in the IdP created in Alibaba Cloud.

- **Signature**

The SAML assertion in Alibaba Cloud must be used as a signature. The **Signature** element must contain information such as the signature value and signature algorithm.

- **Subject**

The **Subject** element must contain the following sub-elements:

- Only one **NameID** sub-element. You must specify the value of **NameID** according to SAML 2.0. But note that Alibaba Cloud does not determine a logon identity according to the value of **NameID**.
- Only one **SubjectConfirmation** sub-element with a **SubjectConfirmationData** sub-element. The **SubjectConfirmationData** sub-element must contain the following attributes:
  - **NotOnOrAfter** : specifies the validity of an SAML assertion.
  - **Recipient** : Alibaba Cloud checks whether it is the recipient of the SAML assertion according to the value of the **Recipient** element. Therefore, you

`must set Recipient to https://signin.alibabacloud.com/saml-role/sso.`

The following is an example of the `Subject` element:

```
< Subject >
  < NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"> administrator </ NameID >

  < SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    < SubjectConfirmationData NotOnOrAfter="2019-01-01T00:01:00.000Z" Recipient="https://signin.alibabacloud.com/saml-role/sso"/>
  </ SubjectConfirmation >
</ Subject >
```

- `Conditions`

The `Conditions` element must contain an `AudienceRestriction` sub-element. The `AudienceRestriction` sub-element can contain multiple `Audience` sub-elements, and the value of an `Audience` sub-element must be `urn:alibaba:cloudcomputing:international`.

The following is an example of the `Conditions` element:

```
< Conditions >
  < AudienceRestriction >
    < Audience > urn:alibaba:cloudcomputing:international
  </ Audience >
  </ AudienceRestriction >
</ Conditions >
```

### Custom elements required by Alibaba Cloud

The `AttributesStatement` element in an SAML assertion must contain the following `Attribute` sub-elements required by Alibaba Cloud:

- A mandatory `Attribute` element with the `Name` attribute set to `https://www.aliyun.com/SAML-Role/Attributes/Role`

This element contains one or more `AttributeValue` sub-elements that list the role can be assumed by the user in your IdP. The value of the `AttributeValue`

**sub-element** is a comma-delimited pair of role ARN and IdP ARN. You can obtain the role ARN and IdP ARN in the RAM console.

- To obtain the role ARN, go to the RAM Roles page and click the name of the target RAM role.
- To obtain the IdP ARN, go to the SSO page. On the Role-based SSO tab, click the name of the target IdP.

If the sub-element contains multiple pairs, the user is asked to select which role to assume during login through the console.

The following is an example of the **Role** sub-element:

```
< Attribute    Name =" https :// www . aliyun . com / SAML - Role /
Attributes / Role ">
  < AttributeV  alue > acs : ram ::$ account_id : role / role1 , acs
: ram ::$ account_id : saml - provider / provider1 </ AttributeV
alue >
  < AttributeV  alue > acs : ram ::$ account_id : role / role2 , acs
: ram ::$ account_id : saml - provider / provider1 </ AttributeV
alue >
</ Attribute >
```



**Note:**

The value of \$ **account\_id** is the Alibaba Cloud account ID that defines the RAM role and IdP.

- A mandatory **Attribute** element with the **Name** attribute set to **https :// www . aliyun . com / SAML - Role / Attributes / RoleSessionName**

This element contains only one **AttributeV alue** sub-element that is used to display user information in the RAM console and ActionTrail logs. If you want multiple users to assume one role, use a unique **RoleSessionName** value, such as the user ID and email address for different users.

The value in the **AttributeV alue** sub-element must be 2 to 64 characters in length, and include only letters, digits, commas (,), periods (.), hyphens (-), underscores (\_), plus signs (+), equal signs (=), and at signs (@).

The following is an example of the **RoleSessionName** sub-element:

```
< Attribute    Name =" https :// www . aliyun . com / SAML - Role /
Attributes / RoleSessionName ">
  < AttributeV  alue > user_id </ AttributeV  alue >
```

```
</ Attribute >
```

- Optional, an `Attribute` element with the `Name` attribute set to `https://www.aliyun.com/SAML-Role/Attributes/SessionDuration`

This element contains only one `AttributeV alue` sub-element that specifies the logon duration. If the logon is initiated through the console, the `AttributeV alue` sub-element represents the number of seconds for the session. If the logon is initiated through the program, the `AttributeV alue` sub-element represents the STS token validity.

The value of `AttributeV alue` is an integer representing the logon duration, in seconds. The value can range from 900 seconds (15 minutes) to 3600 seconds (1 hour). If this sub-element does not exist, the logon duration is one hour.

The following is an example of the `SessionDuration` sub-element:

```
< Attribute   Name =" https:// www . aliyun . com / SAML - Role /
  Attributes / SessionDur ation ">
  < AttributeV alue > 1800 </ AttributeV alue >
</ Attribute >
```

### 6.5.5 Implement role-based SSO by using AD FS

This topic provides an example of how to implement role-based Single Sign On (SSO) from AD FS to Alibaba Cloud, detailing the end-to-end identity SSO process from an enterprise identity provider (IdP) to Alibaba Cloud.

#### Scenario

You use Active Directory (AD) to manage your users and use AD FS to configure enterprise applications such as Alibaba Cloud. Your AD administrator manages the access permissions on Alibaba Cloud accounts according to users' AD groups. In this example, you have two Alibaba Cloud accounts (Account1 and Account2), and the permissions managed by your AD administrator are Admin and Reader. You have a user named Alice. The AD groups of Alice are Aliyun-<account-id>-ADFS-Admin and Aliyun-<account-id>-ADFS-Reader. You want to implement SSO from AD FS to Account1 and Account2.

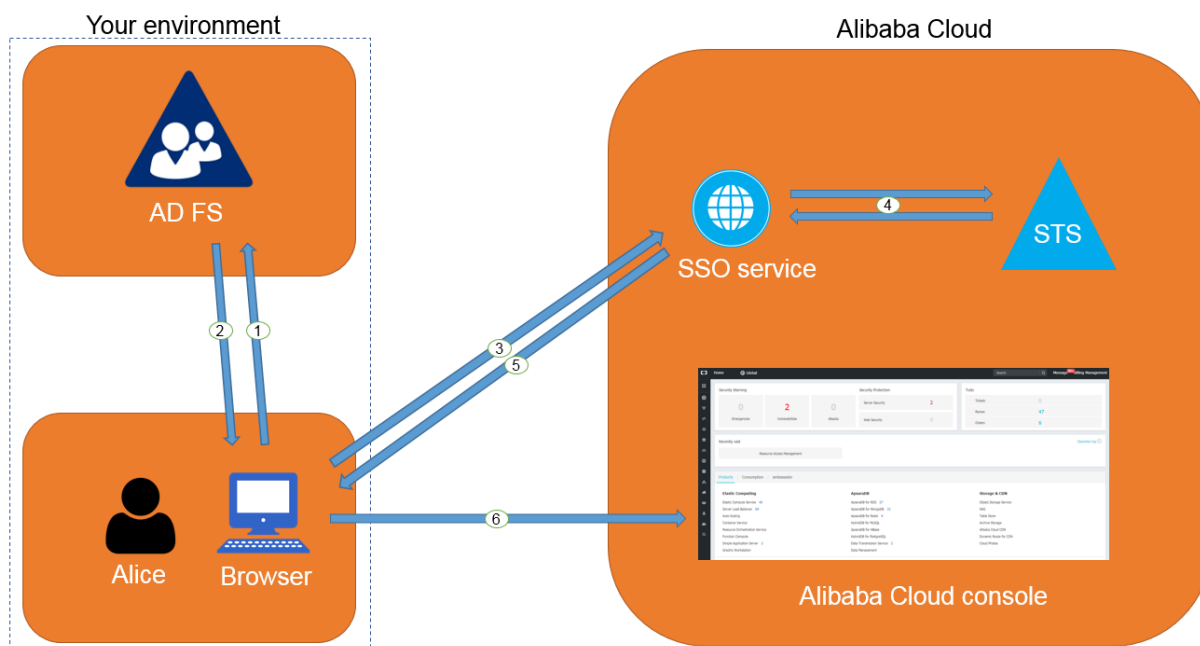


#### Note:

In the preceding groups, <account-id> is the account ID of Account1 or Account2. Therefore, Alice belongs to four AD groups, which correspond to the Admin and Reader permissions respectively.



The following figure shows the basic SSO process through the console.



After the AD administrator has completed role-based SSO configurations, Alice can log on to the Alibaba Cloud console by following the steps in the preceding figure. For more information, see [#unique\\_104](#).

The preceding SSO process shows that users of an enterprise can be authenticated with no need to provide Alibaba Cloud usernames and passwords during login.

## Configurations

To implement role-based SSO, the administrator must configure Alibaba Cloud and AD FS by following these steps:

- Configure AD FS as a trusted SAML IdP in Alibaba Cloud:
  1. Create an IdP named `ADFS` under `Account1` in the Alibaba Cloud RAM console, and configure the corresponding metadata file. The metadata file of your AD FS can be obtained from `https://<ADFS - server>/federation/metadata/2007-06/federationmetadata.xml`.



**Note:**

In the preceding URL, <ADFS-server> is the server domain name or IP address of your AD FS.

For more information, see [#unique\\_123](#).

2. Create two RAM roles named ADFS-Admin and ADFS-Reader under Account1, select `ADFS` you have created as the trusted entity, and attach the `AdministratorAccess` and `ReadOnlyAccess` policies to these two RAM roles respectively. For more information, see [#unique\\_132](#).
3. Create an IdP and two RAM roles under Account2 as described in the preceding steps, and attach policies to these two RAM roles.



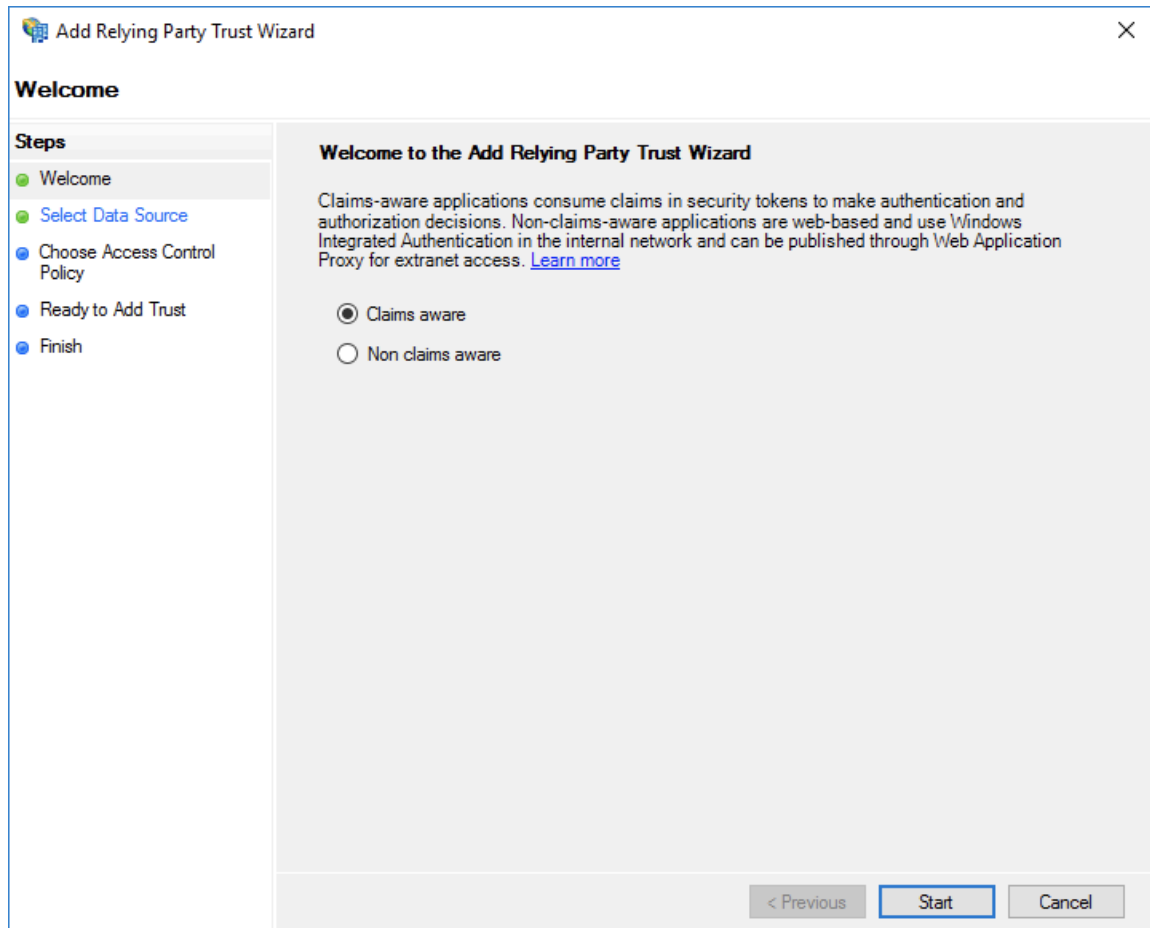
**Note:**

After the configurations are completed, your Alibaba Cloud accounts (Account1 and Account2) will trust the user identity and role information in the SAML requests sent from your AD FS.

- Configure Alibaba Cloud as a trusted SAML SP in AD FS.

In AD FS, SAML SP is also known as a relying party. To set Alibaba Cloud as a trusted SAML SP in AD FS, follow these steps:

1. On the Server Manager page, choose Tools > AD FS Management.
2. Select Add Relying Party Trust.



3. Set the SAML SP metadata of Alibaba Cloud for the relying party. The metadata URL is `https://signin.alibabacloud.com/saml-role/sp-metadata.xml`.

**Add Relying Party Trust Wizard**

**Select Data Source**

**Steps**

- Welcome
- Select Data Source
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

☒ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

☐ Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

☐ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

< Previous   Next >   Cancel

4. Complete the configurations as prompted.

- Configure the SAML assertion attributes for the Alibaba Cloud SP.

The SAML assertion issued by your AD FS must contain the attributes such as `NameID`, `Role`, and `RoleSessionName`. Your AD FS can provide these attributes by issuing transform rules.

- `NameID`

Follow these steps to configure the Windows account name of AD to be the `NameID` in the SAML assertion:

1. Right-click the display name of the relying party and select Edit Claim Rules.
2. Click Issuance Transform Rules.



**Note:**

Issuance Transform Rules indicates how to transform a known user attribute and issue it as an attribute in the SAML assertion. You must issue the

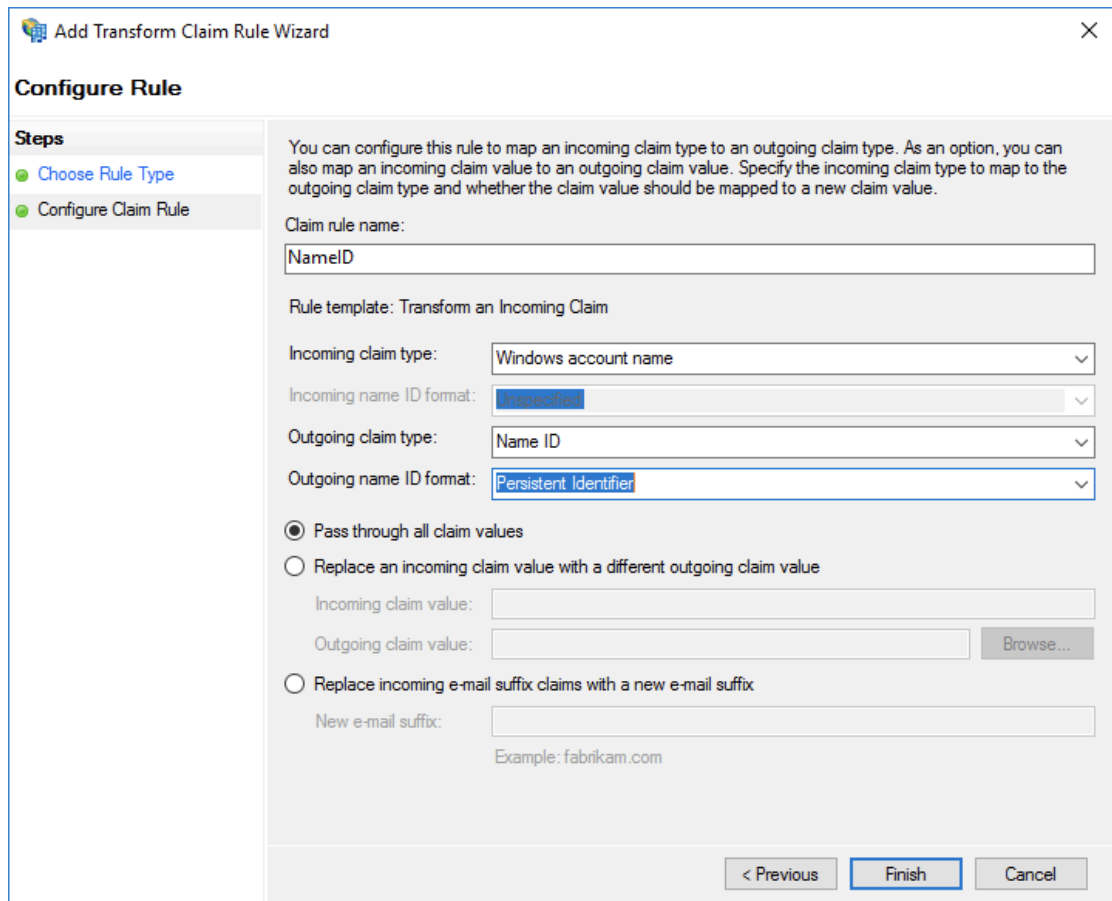
Windows account name of a user in AD as a `NameID` . This means that a new rule is required.

3. Select Transform an Incoming Claim from the Claim rule template drop-down list.

The screenshot shows the 'Add Transform Claim Rule Wizard' dialog box. The title bar says 'Add Transform Claim Rule Wizard' with a close button. The main heading is 'Select Rule Template'. On the left, under 'Steps', there are two items: 'Choose Rule Type' (marked with a green dot) and 'Configure Claim Rule' (marked with a blue dot). The main area contains the following text: 'Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.' Below this is a section 'Claim rule template:' with a dropdown menu showing 'Transform an Incoming Claim'. Underneath is a section 'Claim rule template description:' with a text box containing the following text: 'Using the Transform an Incoming Claim rule template you can select an incoming claim, change its claim type, and optionally change its claim value. For example, you can use this rule template to create a rule that will send a role claim with the same claim value of an incoming group claim. You can also use this rule to send a group claim with a claim value of "Purchasers" when there is an incoming group claim with a value of "Admins". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited.' At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

4. Configure the claim rule as follows, and click Finish.

- Claim rule name: NameID
- Incoming claim type: Windows account name
- Outgoing claim type: Name ID
- Outgoing name ID format: Persistent Identifier
- Pass through all claim values: Selected



**Add Transform Claim Rule Wizard** [X]

**Configure Rule**

**Steps**

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Rule template: Transform an Incoming Claim

Incoming claim type:

Incoming name ID format:

Outgoing claim type:

Outgoing name ID format:

☒ Pass through all claim values  
☐ Replace an incoming claim value with a different outgoing claim value  
     Incoming claim value:   
     Outgoing claim value:    
☐ Replace incoming e-mail suffix claims with a new e-mail suffix  
     New e-mail suffix:   
     Example: fabrikam.com

< Previous   **Finish**   Cancel

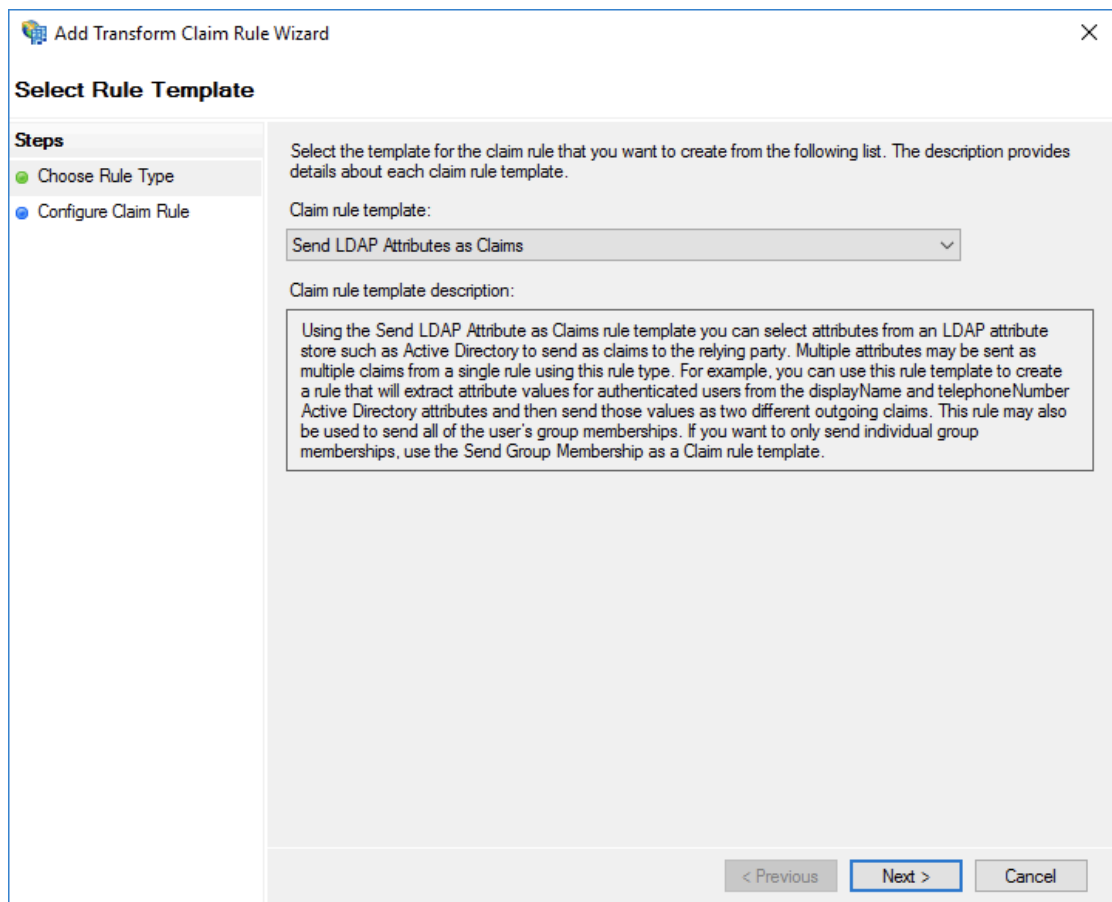
After the configurations are completed, AD FS will send the required `NameID` format to Alibaba Cloud. The following is an example:

```
< NameID    Format =" urn : oasis : names : tc : SAML : 2 . 0 :
          nameid - format : persistent ">
          YourDomain \ rolessouse    r
</ NameID >
```

- RoleSessionName

Follow these steps to configure the UPN of AD to the RoleSessionName in the SAML assertion:

1. Click Add Transform Claim Rule.
2. Select Send LDAP Attributes as Claims from the Claim rule template drop-down list.



3. Configure the claim rule as follows, and click Finish.

- Claim rule name: RoleSessionName
- Attribute store: Active Directory
- LDAP Attribute: User-Principal-Name (You can select other attributes, such as Email, as needed.)
- Outgoing Claim Type: https://www.aliyun.com/SAML-RoleAttributes/RoleSessionName

Add Transform Claim Rule Wizard

### Configure Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	User-Principal-Name	v.aliyun.com/SAML-Role/Attributes/RoleSessionName
*		

< Previous   **Finish**   Cancel

After the configurations are completed, AD FS will send the required

`RoleSessionName` format to Alibaba Cloud. The following is an example:

```
< Attribute Name = " https :// www . aliyun . com / SAML - Role /
Attributes / RoleSessionName ">
  < AttributeValue > rolessouser@example.com <
  AttributeValue >
</ Attribute >
```



- Role

Follow these steps to transform the user's AD group membership into the role name of Alibaba Cloud by using custom rules:

1. Click Add Transform Claim Rule.
2. Select Send Claims Using a Custom Rule from the Claim rule template drop-down list and click Next.

**Add Transform Claim Rule Wizard**

**Select Rule Template**

**Steps**

- Choose Rule Type
- Configure Claim Rule**

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Send Claims Using a Custom Rule

Claim rule template description:

Using a custom rule, you can create rules that can't be created with a rule template. Custom rules are written in the AD FS claim rule language. Capabilities that require custom rules include:

- Sending claims from a SQL attribute store
- Sending claims from an LDAP attribute store using a custom LDAP filter
- Sending claims from a custom attribute store
- Sending claims only when 2 or more incoming claims are present
- Sending claims only when an incoming claim value matches a complex pattern
- Sending claims with complex changes to an incoming claim value
- Creating claims for use only in later rules

< Previous   **Next >**   Cancel

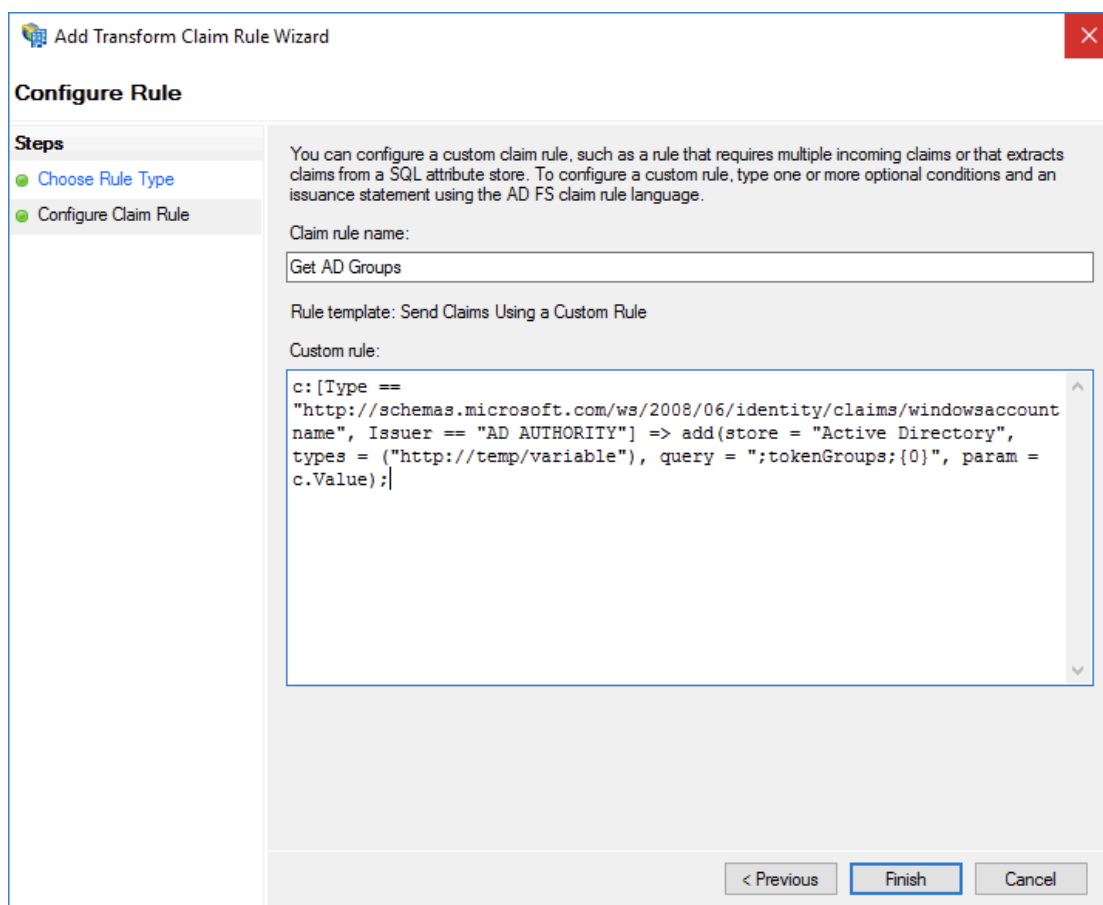
3. Configure the claim rule as follows, and click Finish.

■ Claim rule name: Get AD Groups

■ Custom rule:

```
c :[ Type ==
" http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"] => add ( store = "Active Directory",
types = (" http://temp/variable"), query = ";
tokenGroups;{ 0 }", param =
```

```
c . Value );
```



**Add Transform Claim Rule Wizard**

**Configure Rule**

**Steps**

- Choose Rule Type
- Configure Claim Rule

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.

Claim rule name:  
Get AD Groups

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccount
name", Issuer == "AD AUTHORITY"] => add(store = "Active Directory",
types = ("http://temp/variable"), query = ";tokenGroups;{0}", param =
c.Value);
```

< Previous Finish Cancel



#### Note:

This rule is used to obtain the user's AD group membership and save it to `http://temp/variable`.

- Click Add Transform Claim Rule.
- Repeat the preceding steps and click Finish.

■ Claim rule name: Role

■ Custom rule:

```
c :[ Type == " http :// temp / variable ", Value =~ "(? i
)^ Aliyun -([\ d ]+)"
=> issue ( Type = " https :// www . aliyun . com / SAML -
Role / Attributes / Role ",
Value = RegExRepla ce ( c . Value , " Aliyun -([\ d ]+)-
(.+)", " acs : ram ::
```

```
$ 1 : role /$ 2 , acs : ram ::$ 1 : saml - provider / ADFS
"));
```

**Add Transform Claim Rule Wizard**

**Configure Rule**

**Steps**

- Choose Rule Type
- Configure Claim Rule

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.

Claim rule name:

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
c:[Type == "http://temp/variable", Value =~ "(?i)^Aliyun-([\d]+)"]
=> issue(Type = "https://www.aliyun.com/SAML-Role/Attributes/Role",
Value = RegexReplace(c.Value, "Aliyun-([\d]+)-(.)", "acs:ram::
$1:role/$2,acs:ram::$1:saml-provider/ADFS"));
```

< Previous Finish Cancel



#### Note:

According to this rule, if the user's AD group contains Aliyun-<account-id>-ADFS-Admin or Aliyun-<account-id>-ADFS-Reader, an SAML attribute will be generated and sent to Alibaba Cloud to match the RAM role ADFS-Admin or ADFS-Reader.

After the configurations are completed, your IdP will return a required SAML assertion to Alibaba Cloud. The following is an example:

```
< Attribute Name = " https :// www . aliyun . com / SAML - Role /
Attributes / Role ">
  < AttributeV alue > acs : ram ::< account - id >: role / ADFS
- Admin , acs : ram ::< account - id >: saml - provider / ADFS </
AttributeV alue >
</ Attribute >
```

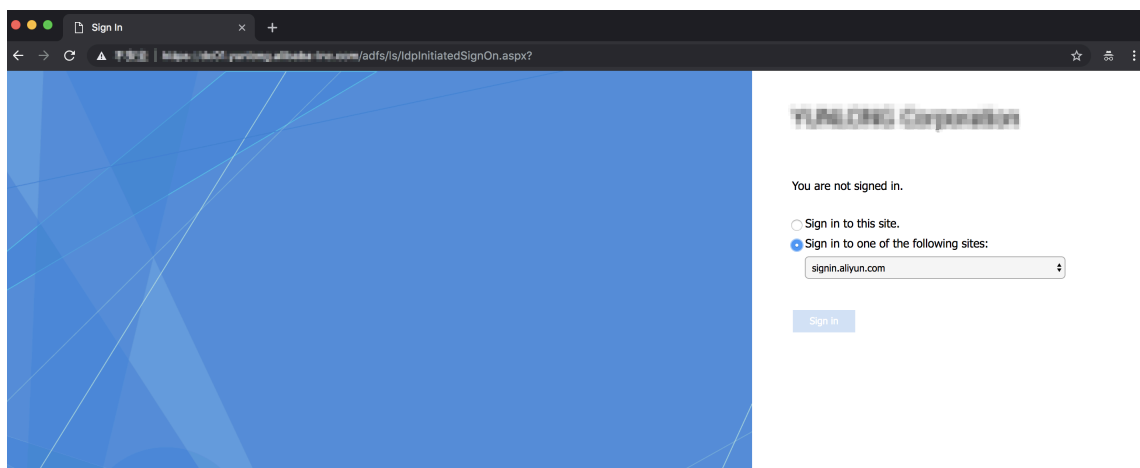
## Verification

- 1. Log on to the AD FS SSO portal (URL: `https://<ADFS-server>/adfs/ls/IdpInitiatedSignOn.aspx`), select Alibaba Cloud application, and enter the username and password.



### Note:

In the preceding URL, <ADFS-server> is the server domain name or IP address of your AD FS. If the URL does not work, run the PowerShell `Set-AdfsProperties -EnableIdpInitiatedSignonPage $True`.



- 2. On the Alibaba Cloud role-based SSO page, select the target role and click Sign In.



### Note:

If your user belongs to only one AD group, the user can log on to Alibaba Cloud with no need of selecting a role.

Alibaba Cloud SAML SSO Homepage

Role-based SSO

Please select a role

Account : 987654321054

☐ Admin

☐ Reader

Account : 123456789012

☐ Admin

☐ Reader

Sign In

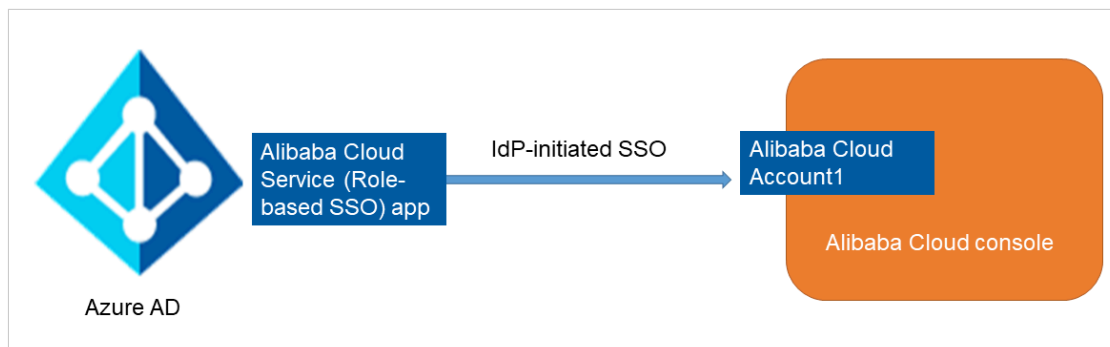
## 6.5.6 Implement role-based SSO by using Azure Active Directory

This topic provides an example of how to implement role-based Single Sign On (SSO) to Alibaba Cloud from Azure Active Directory (Azure AD), detailing the end-to-end identity SSO process from a cloud identity provider (IdP) to Alibaba Cloud. After implementing role-based SSO, you can better manage your Azure AD users who have access to Alibaba Cloud, enable your users to automatically log on to Alibaba Cloud with their Azure AD accounts, and manage your accounts in the Azure portal.

### Scenario

You use Azure AD to manage your users and configure enterprise applications such as Alibaba Cloud. In this example, you have an Alibaba Cloud account (Account1) and a user named u2. You want u2 to implement SSO from Azure AD to Account1.

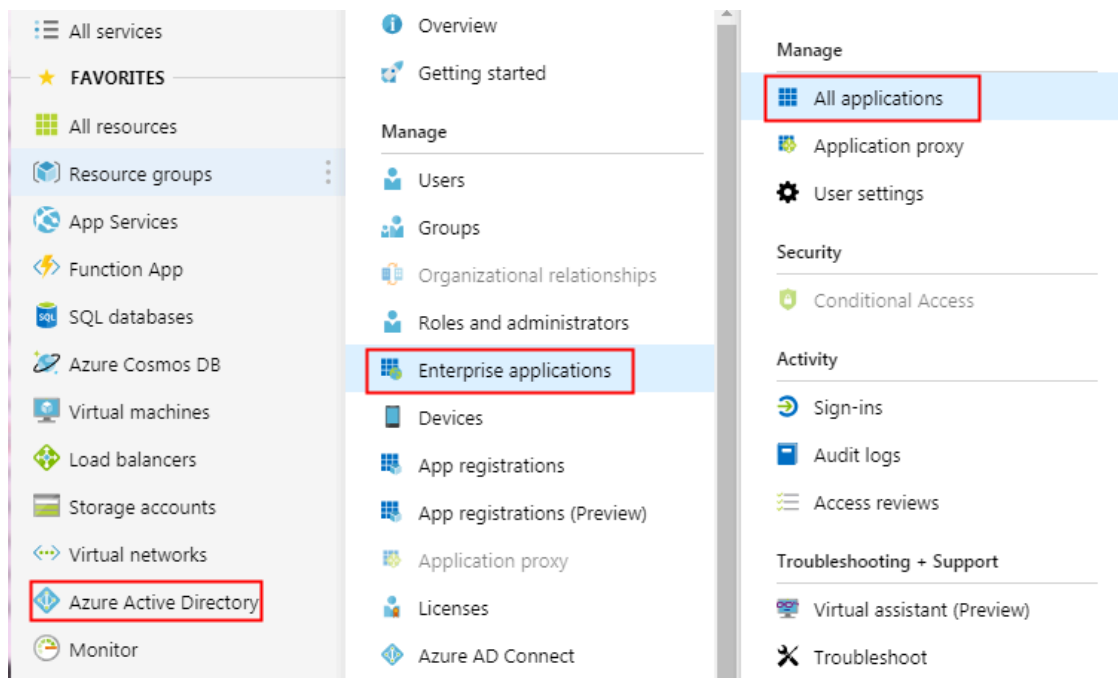
The following figure shows the basic SSO process.



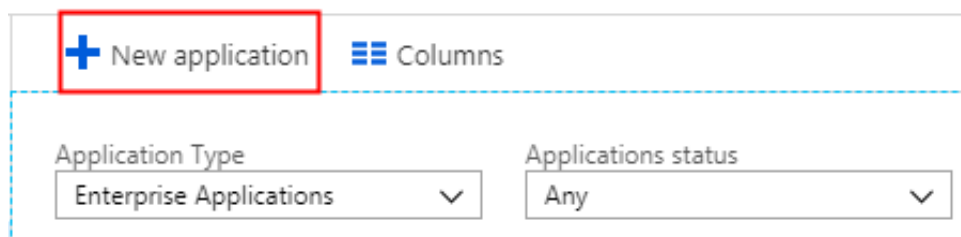
## Configurations

To implement role-based SSO, you must configure Azure AD and Alibaba Cloud by following these steps:

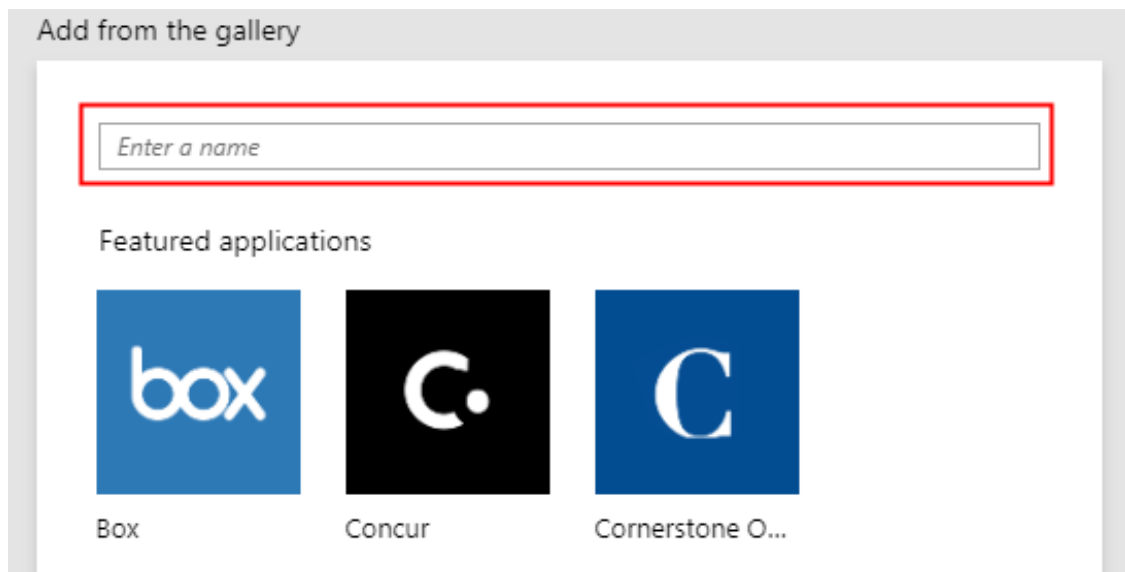
- Add Alibaba Cloud role-based SSO from Azure AD gallery:
  1. Log on to the [Azure portal](#).
  2. In the left-side navigation pane, choose Azure Active Directory > Enterprise applications > All applications.



3. Click New application.



4. On the displayed page, enter Alibaba Cloud Service (Role-based SSO) in the search box, press Enter, and select Alibaba Cloud Service (Role-based SSO).



5. On the displayed page, click Add.




Name ⓘ  
Alibaba Cloud Service (Role-based SSO)

Publisher ⓘ  
Alibaba Group

Single Sign-On Mode ⓘ  
SAML-based sign-on

URL ⓘ  
<https://www.aliyun.com>

Logo ⓘ  


[Read our step-by-step Alibaba Cloud Service \(Role-based SSO\) integration tutorial](#)

**Add**

6. On the Alibaba Cloud Service (Role-based SSO) page, click Properties in the left-side navigation pane, and copy and save the object ID for subsequent use.

Overview

Getting started

Deployment Plan

Manage

Properties

Owners

Users and groups

Single sign-on

Provisioning

Self-service

Security

Conditional Access

Permissions

Token encryption (Preview)

Activity

Sign-ins

Audit logs

Troubleshooting + Support

Virtual assistant (Preview)

Troubleshoot

New support request

Save Discard Delete


Name ⓘ

Alibaba Cloud Service (Role-based SSO)

Homepage URL ⓘ

https://www.aliyun.com

Logo ⓘ



User access URL ⓘ

Select a file

Application ID ⓘ

Object ID ⓘ

Terms of Service Url ⓘ

Privacy Statement Url ⓘ

Reply Url ⓘ

User assignment required? ⓘ

Yes

No

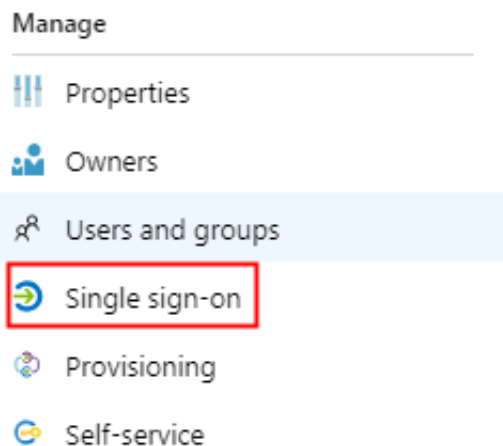
Visible to users? ⓘ

Yes

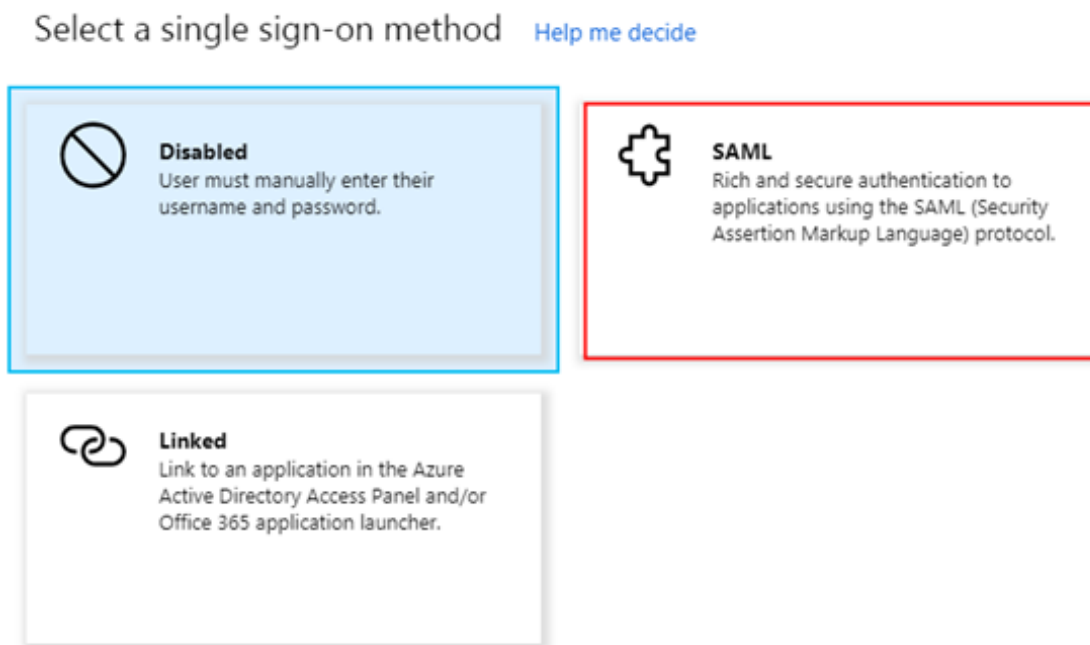
No

- Enable Azure AD SSO in Azure AD:

1. In the Azure portal, choose Azure Active Directory > Enterprise applications > All applications.
2. In the NAME column, click Alibaba Cloud Service (Role-based SSO).
3. On the displayed page, select Single sign-on from the left-side navigation pane.



4. In the Select a single sign-on method section, click SAML.



5. On the Set up Single Sign-On with SAML page, follow these steps:

- a. In the upper-left corner, click Upload metadata file to integrate Azure AD with Alibaba Cloud role-based SSO, and click Save.



**Note:**

You can obtain the metadata file from the URL `https://signin.alibabacloud.com/saml-role/sp-metadata.xml`.

- b. In the User Attributes & Claims section, click the Edit icon.

2

User Attributes & Claims



- c. Click Add new claim. In the Name field, enter `Role`. In the Namespace field, enter `https://www.aliyun.com/SAML-Role/Attributes`. Set Source to Attribute, select `user.assignedroles` from the Source attribute drop-down list, and click Save.

* Name	<input type="text" value="Role"/>	✓
Namespace	<input type="text" value="https://www.aliyun.com/SAML-Role/Attributes"/>	
Source	<input checked="" type="radio"/> Attribute <input type="radio"/> Transformation	
* Source attribute	<input type="text" value="user.assignedroles"/>	▼

- d. Repeat the preceding step to add a new claim with Name set to `RoleSessionName` and Source attribute set to `user:userprincipalname`, and click Save.

**Note:**

You can also enter `https://www.aliyun.com/SAML-Role/Attributes` in the Namespace field.

- e. In the SAML Signing Certificate section, click Download to download the federation metadata XML for subsequent use.

**3** SAML Signing Certificate

Status	Active
Thumbprint	D0AA08B5D8EC8CC9FC24AD03C8D808CF2B3C848D
Expiration	4/9/2022, 9:33:27 AM
Notification Email	1406281081@qq.com
App Federation Metadata Url	<a href="https://login.microsoftonline.com/878f14...">https://login.microsoftonline.com/878f14...</a>
Certificate (Base64)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>
Federation Metadata XML	<a href="#">Download</a>

- f. In the Set up Alibaba Cloud Service (Role-based SSO) section, copy the URLs as needed.

**4** Set up Alibaba Cloud Service (Role-based SSO)

You'll need to configure the application to link with Azure AD.

Login URL	<a href="https://login.microsoftonline.com/878f14...">https://login.microsoftonline.com/878f14...</a>
Azure AD Identifier	<a href="https://sts.windows.net/878f1420-238a-4...">https://sts.windows.net/878f1420-238a-4...</a>
Logout URL	<a href="https://login.microsoftonline.com/commo...">https://login.microsoftonline.com/commo...</a>

[View step-by-step instructions](#)

- Configure role-based SSO in Alibaba Cloud:

- Log on to the Alibaba Cloud [RAM console](#) by using Account1.
- In the left-side navigation pane, select SSO.
- On the Role-based SSO tab, click Create IdP.
- On the displayed page, enter `AAD` in the IdP Name field, enter a description in the Note field, click Upload to upload the federation metadata file you downloaded before, and click OK.
- After the IdP is successfully created, click Create RAM Role.
- In the RAM Role Name field, enter `AADrole`, select `AAD` from the Select IdP drop-down list, and click OK.



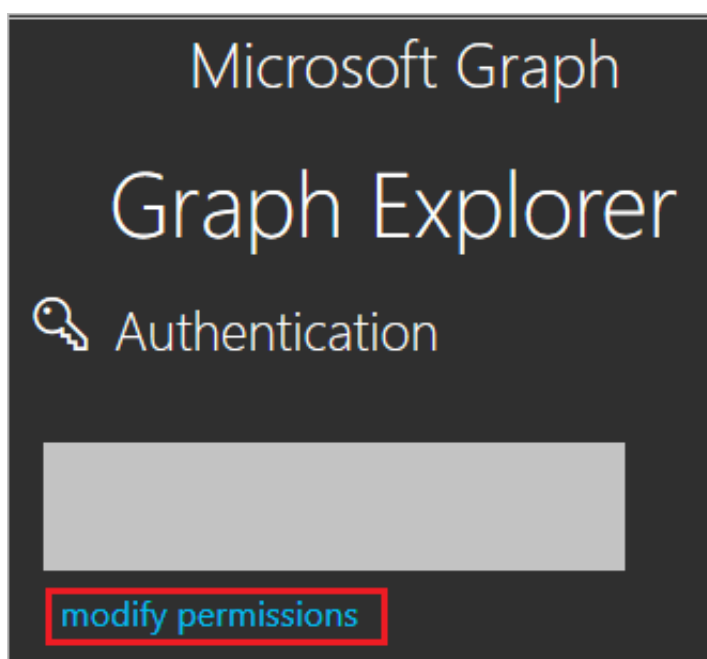
Note:

You can grant permission to the role as needed. After creating the IdP and the corresponding role, we recommend that you save the ARNs of the IdP and the role for subsequent use. You can obtain the ARNs on the IdP information page and the role information page.

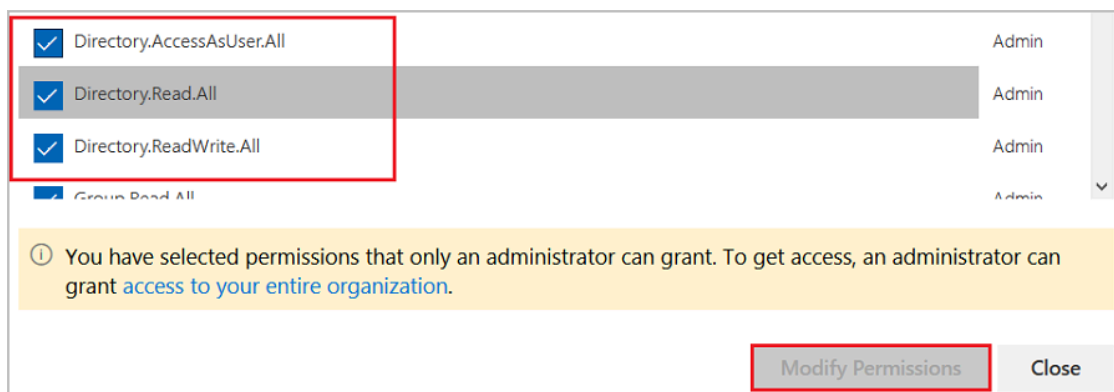
- Associate the Alibaba Cloud RAM role (AADrole) with the Azure AD user (u2):

To associate the RAM role with the Azure AD user, you must create a role in Azure AD by following these steps:

1. Log on to the [Azure AD Graph Explorer](#).
2. Click modify permissions to obtain required permissions for creating a role.



3. Select the following permissions from the list and click Modify Permissions, as shown in the following figure.



Note:

After permissions are granted, log on to the Graph Explorer again.

4. On the Graph Explorer page, select GET from the first drop-down list and beta from the second drop-down list. Then enter `https://graph.microsoft.com/beta/servicePrincipals` in the field next to the drop-down lists, and click Run Query.

The screenshot shows the Microsoft Graph Explorer interface. At the top, there are two dropdown menus: the first is set to 'GET' and the second is set to 'beta'. To the right of these is a text input field containing the URL 'https://graph.microsoft.com/beta/servicePrincipals'. A 'Run Query' button is located to the right of the URL field. Below the input fields, there are two tabs: 'Request Body' and 'Request Headers'. The 'Request Body' tab is selected. Below the tabs is a large empty box for the request body. A green status bar indicates a successful request: 'Success - Status Code 200, 1706ms'. Below the status bar, there are two tabs: 'Response Preview' and 'Response Headers'. The 'Response Preview' tab is selected. The response preview shows a JSON object with the following structure:

```
{
  "@odata.context": "https://graph.microsoft.com/beta/$metadata#servicePrincipals",
  "@odata.nextLink": "https://graph.microsoft.com/beta/servicePrincipals?$skiptoken=...",
  "value": [
    {
      "id": "...",
      "deletedDateTime": null,
      "accountEnabled": true,
      "appDisplayName": "Substrate Instant Revocation Pipeline",
      "appId": "..."
    }
  ]
}
```



Note:

If you are using multiple directories, you can enter `https://graph.microsoft.com/beta/contoso.com/servicePrincipals` in the field of the query.

5. In the Response Preview section, extract the `appRoles` property from the 'Service Principal' for subsequent use.

```
"appRoles": [
  {
    "allowedMemberTypes": [
      "User"
    ],
    "description": "msiam_access",
    "displayName": "msiam_access",
    "id": "41be2db8-48d9-4277-8e86-f6d22d35****",
    "isEnabled": true,
    "origin": "Application",
    "value": null
  }
],
```



#### Note:

You can locate the `appRoles` property by entering `https://graph.microsoft.com/beta/servicePrincipals/<objectId>` in the field of the query. Note that the `objectId` is the object ID you have copied from the Azure AD Properties page.

6. Go back to the Graph Explorer, change the method from GET to PATCH, paste the following content into the Request Body section, and click Run Query:

```
{
  " appRoles ": [
    {
      " allowedMem berTypes ":[
        " User "
      ],
      " descriptio n ": " msiam_acce ss ",
      " displayNam e ": " msiam_acce ss ",
      " id ": " 41be2db8 - 48d9 - 4277 - 8e86 - f6d22d35 ****",
      " isEnabled ": true ,
      " origin ": " Applicatio n ",
      " value ": null
    },
    { " allowedMem berTypes ": [
      " User "
    ],
      " descriptio n ": " Admin , AzureADPro d ",
      " displayNam e ": " Admin , AzureADPro d ",
      " id ": " 68adae10 - 8b6b - 47e6 - 9142 - 6476078cdb ce ",
```



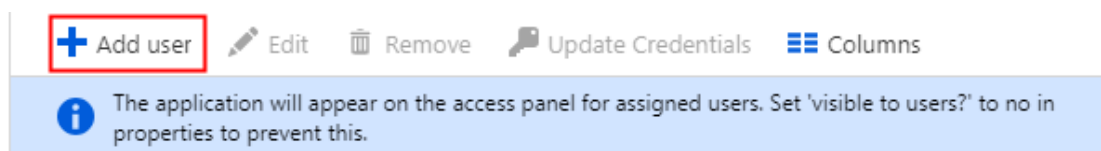
```
    " isEnabled ": true ,
    " origin ": " ServicePrincipal ",
    " value ": " acs : ram :: 1871250227 22 ****: role / aadrole
, acs : ram :: 1871250227 22 ****: saml - provider / AAD "
  }
]
}
```

**Note:**

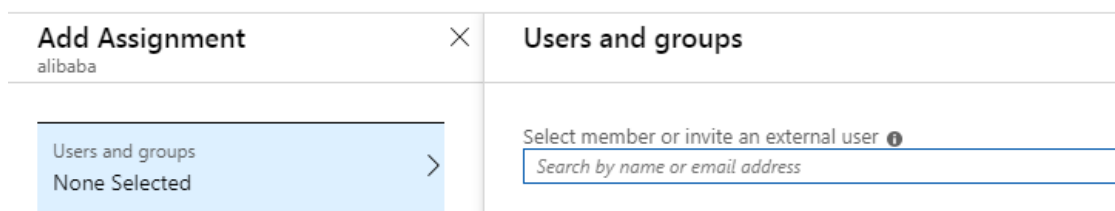
The `value` is the ARNs of the IdP and the role you created in the RAM console. Here, you can add multiple roles as needed. Azure AD will send the value of these roles as the claim value in SAML response. However, you can only add new roles after the `msiam_access` part for the patch operation. To

smooth the creation process, we recommend that you use an ID generator, such as GUID Generator, to generate IDs in real time.

7. After the 'Service Principal' is patched with the required role, attach the role with the Azure AD user (u2) by following these steps:
  - a. In the Azure portal, choose Azure Active Directory > Enterprise applications > All applications.
  - b. In the NAME column, click Alibaba Cloud Service (Role-based SSO).
  - c. On the displayed page, select Users and groups from the left-side navigation pane.
  - d. In the upper-left corner, click Add user.



- e. On the Users and groups tab, select u2 from the user list, and click Select. Then, click Assign.



- f. View the assigned role and test role-based SSO.

First 100 shown, to search all users & groups, enter a display name.		
DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
 u2	User	Admin,AzureADProd



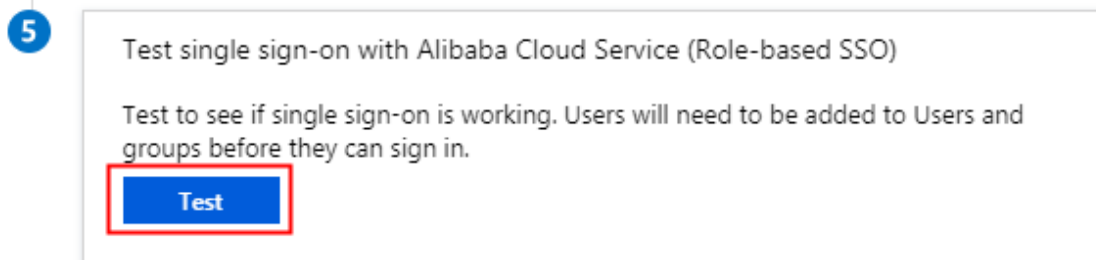
#### Note:

After you assign the user (u2), the created role is automatically attached to the user. If you have created multiple roles, you need to attach the appropriate role to the user as needed. If you want to implement role-based SSO from Azure AD to multiple Alibaba Cloud accounts, repeat the preceding steps.

## Test role-based SSO

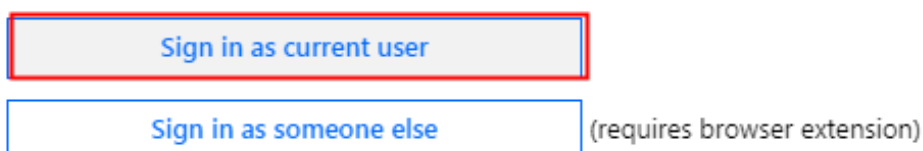
After the preceding configurations are completed, test role-based SSO by following these steps:

1. In the Azure portal, go to the Alibaba Cloud Service (Role-based SSO) page, select Single sign-on, and click Test.

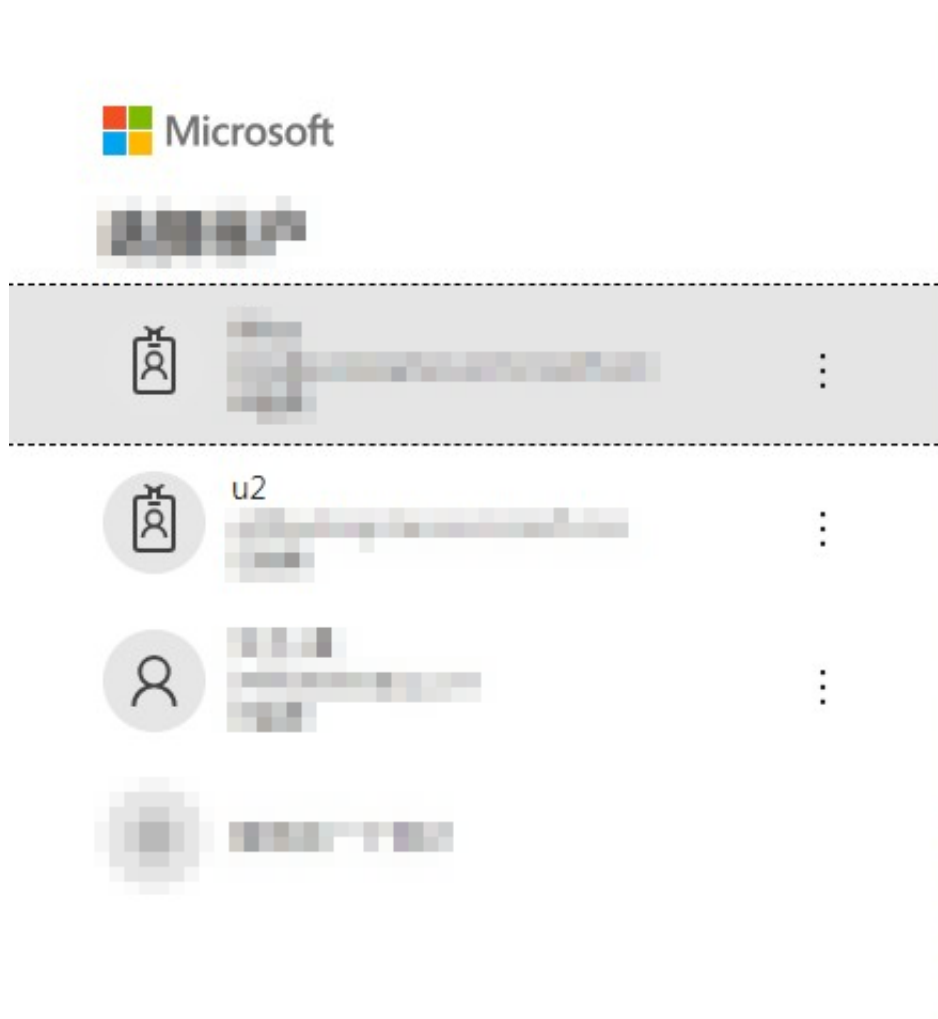


2. Click Sign in as current user.

Please make sure you have configured Alibaba Cloud Service (Role-based SSO) before testing.



3. On the account selection page, select u2.



The following page is displayed, indicating that role-based SSO is successful.

