

# Resource Access Management

Quick Start

# Quick Start

## Procedure



## Activate multi-factor authentication (two-step authentication) for primary accounts

Your Alibaba Cloud account has full control permissions for all of the resources under it. If the logon password or access key of the primary account is disclosed, the security of all of the assets under the primary account is greatly threatened. To reduce this risk, we strongly recommend that you bind multi-factor authentication (MFA) to your primary account.

### Go to account security settings

Log on to [www.aliyun.com](http://www.aliyun.com), and then move the mouse pointer to your account displayed on the upper-right corner of the page and click **Security Settings**.

On the **Security Settings** page, click **Set** next to **Virtual MFA** to enable the VMFA device binding process.

#### Virtual MFA

After binding virtual MFA, you can use it for secondary verification when logging in.

 Not Set | [Set](#)

3. Enter your verification code sent either to your mobile phone or your email to verify your identity.

## Enable VMFA device binding process (start two-step authentication)

Go to the **Bind MFA Device** page to bind your MFA device.

To perform this operation, you must install an MFA application on your mobile phone. Alibaba Cloud ID Sec and Google Authenticator are two popular MFA applications. To install Google Authenticator, refer to [Google Authenticator Installation and Use Guide](#).

**Bind MFA Device**

To go on, you should install an MFA application on your device. The popular MFA apps are [Shenfenbao](#), Google Authenticator. See also [instruction of installing Google Authenticator](#).

If your account is shared by many people, then when you have successfully bind MFA, MFA unbound others will not be able to log on. The solution is to allow other people to install MFA application and scan the QR code on this page, this two-dimensional code image or save it for others to carry out the follow-up scan code. But security best practice, we recommend that you cancel many people shared account.

NOTE: When you bind MFA device successfully, if your follow-up due to the removal device MFA accounts, uninstall the application, the phone is lost, Brush and other causes can not be used, you need to [appeal](#) to unbind MFA equipment. Please exercise with caution.

Scan Qrcode    Input Manually



Scan qrcode with your device

Input the 2 set of code from your MFA app

Security code 1:  
Input security code please (6 digits)

Security code 2:  
Input security code please (6 digits)

Confirm to bind

Add a user in your MFA application.

We use Google Authenticator as an example. Open **Authenticator**, click **+** (**Add User**), and then click **Scan Barcode** to scan the code. If your mobile phone does not support this feature, you can click **Input Manually** to enter the MFA key yourself. )

After you have scanned the code, the user is added automatically and your MFA application will display a dynamic password for the account. Note that the dynamic password is updated every 30 seconds.

Acquire two consecutive passwords.

On the **Enable Virtual MFA Device** page, enter the consecutive passwords displayed in the MFA application, and then click **Confirm to bind** button, as shown in the following figure:

Input the 2 set of code from your MFA app

**Security code 1:**

**Security code 2:**

**Confirm to bind**

The MFA device is then successfully enabled.

## Logon process with MFA enabled (two-step authentication process)

Log on to the console with your user name and password.

After the password is verified, you also need to provide a dynamic verification code from the VMFA device, as shown in the following figure:

Verify virtual MFA device

To go on, you should install an MFA application on your device. The popular MFA apps are [Shenfenbao](#), [Google Authenticator](#). See also [instruction of installing Google Authenticator](#). ×

If you can not verify due to some reasons, you can [appeal](#) to unbind MFA. ×

\* Input security code please:

Remember this computer for 7 days

**Submit**

After you pass the two-step verification, you successfully log on to Alibaba Cloud.

## Procedure

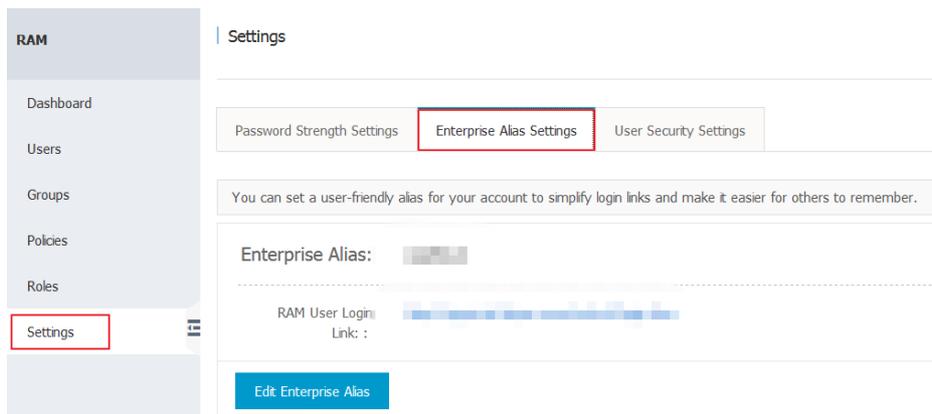


# Initialize RAM Configuration

Log on to [www.aliyun.com](http://www.aliyun.com) with your Alibaba Cloud account and activate the Resource Access Management (RAM) service. You can then log on to the RAM console to set your enterprise alias, RAM user logon password strength, and RAM user MFA logon configuration.

## Set your enterprise alias

Setting an RAM enterprise alias for your Alibaba Cloud account makes it easier for RAM users to remember the logon portal. For security reasons, the RAM user logon portal is different from the primary account logon portal. When logging on to the RAM portal, RAM users must provide the enterprise alias of the primary account as well as their own usernames and passwords.



## Set RAM user logon password strength

You can specify a minimum logon password strength for all RAM users. When any users reset their passwords, the new password cannot be weaker than this setting allows.

The screenshot shows the 'Settings' page in the RAM console. The left sidebar has 'Settings' highlighted. The main content area is titled 'Settings' and has three tabs: 'Password Strength Settings' (highlighted with a red box), 'Enterprise Alias Settings', and 'User Security Settings'. Below the tabs, there is a message: 'You can set user login password modification rules to improve your security level.' A 'User Security Level' progress bar is shown. The settings include:

- Password Length: 8 to 32 characters.
- Password Must Contain:
  - Lowercase Letters
  - Uppercase Letters
  - Number
  - Special Characters
- Password Validity Period: 15 day(s) (max 1,095 days, 0 indicates the password never expires)
- Password Expiration:  If checked, it means the user cannot log in.
- Password History Check Policy: Doesn't allow passwords used more than 0 times previously (max 24. 0 means previous passwords are not checked)
- Password Attempt Limit Policy: Maximum number of incorrect password attempts within one hour: 0 time(s) (max 32, 0 indicates no password attempt limit is enabled)

A 'Save Changes' button is at the bottom.

## Set RAM user security settings

You can specify whether RAM users can reset their passwords, accesskeys or MFAs. You can also specify whether to store MFA logon status for 7 days on devices that are used for logon.

The screenshot shows the 'Settings' page in the RAM console. The left sidebar has 'Settings' highlighted. The main content area is titled 'Settings' and has three tabs: 'Password Strength Settings', 'Enterprise Alias Settings', and 'User Security Settings' (highlighted with a red box). Below the tabs, there are four settings:

- Allow MFA login status to be saved on login (for 7 days).
- Allow independent password management
- Allow independent Access key management
- Allow independent MFA device management

A 'Save Changes' button is at the bottom.

## Procedure



## Create a RAM user

Log on to the Alibaba Cloud console, and then click **Resource Access Management** from the left-side navigation bar to open the RAM console.

On the RAM console, click **Users**.

On the **User Management** page, click **New user**.

In the **Create User** window, enter a login name and fill in the other details, and then click **OK**.

## Set a logon password for the user (if required)

Log on to the Alibaba Cloud console, and then click **Resource Access Management** from the left-side navigation bar to open the RAM console.

On the RAM console, click **Users** to open the **User Management** page.

On the **User Management** page, click a user.

On the **User Details** page, click **Enable Console Login** and set an initial password for the selected user in the pop-up window. You can also specify that the user must change this password at his or her first logon.

The screenshot displays the 'User Details' page for a user named 'appserver'. The page is organized into several sections:

- Basic Information:** Includes fields for Login Name (appserver), Display Name, and Creation Time (2017-03-06 19:38:02). There is an 'Edit Basic Information' button.
- Web Console Login Management:** Features a red-bordered button labeled 'Enable Console Login'. Below it, there are fields for 'You must activate MFA' (with a 'Close' button) and 'Last Logon Time'. A note states 'On your next login you must reset the password.' with a 'Close' button.
- MFA Device:** A table with columns: Type, Introduction, Enabling Status, and Operation. It lists a 'VMFA Device' with the introduction 'Application calculates a 6-digit verification code using the TOTP standard algorithm.', an 'Enabling Status' of 'Not Enabled', and an 'Operation' button labeled 'Enable VMFA Device'.
- User Access Key:** A table with columns: AccessKey ID, Status, Creation Time, and Operation. There is a 'Create Access Key' button.

## Create AccessKeys for the user (if required)

Log on to the Alibaba Cloud console, and then click **Resource Access Management** from the left-side navigation bar to open the RAM console.

On the RAM console, click **Users** to open the **User Management** page.

On the **User Management** page, click a user.

On the **User Details** page, click **Create Access Key**.

In the pop-up window, click **Save Access Key Information** to save the access key.

**Note:**

1. An AccessKeySecret can only be viewed or downloaded during access key creation process. For security reasons, you cannot view or download it once the access key has been created. If an access key is lost, you must create a new one. The newly created access key represents the same user identity as the old one. Different access keys for the same RAM user are equivalent.
2. It is recommended that you change application access keys regularly to avoid any risk of access key disclosure.

For information on how to grant permissions to RAM users, refer to [RAM User Authorization](#).

## Procedure



## Create a custom authorization policy

Access the RAM console and click **Policies**. Two policy options, **System Policy** and **Custom Policy**, are available on **Policy Management** page.

Alibaba Cloud currently provides multiple system authorization policies for user selection. These authorization policies only provide coarse-grained access control capabilities. For example, you can grant read-only permission or all permissions to specific cloud products. If you require finer-grained authorization, you can create custom authorization policies for access control. For example, you can grant the user B read-only permission for all of the objects in `oss://sample_bucket/b/`, and prevent access by IP addresses from outside your company network (your company network IP address can be acquired by searching "My IP" using the search engine).

**Note:**

Before creating custom authorization policies, you must understand the basic structure and syntax of the authorization policy language. For more details, refer to [Authorization Policy](#)

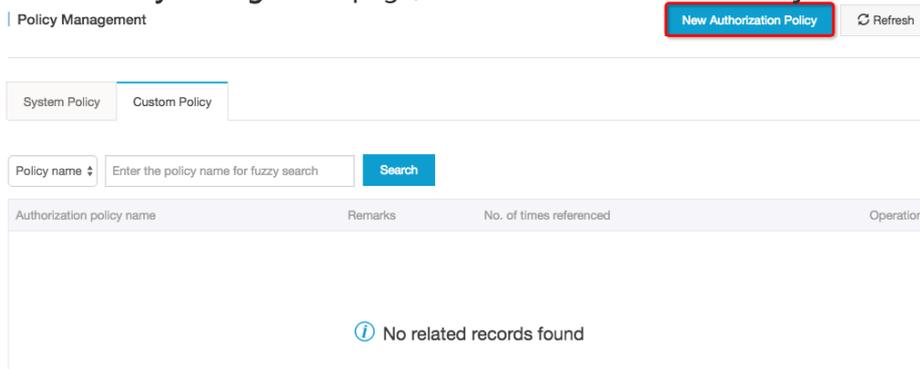
## Language Description.

After learning the authorization policy language, you can easily create custom authorization policies on the RAM console. This process is as follows:

- i. Log on to the Alibaba Cloud console, and then click **Resource Access Management** from the left-side navigation bar to open the RAM console.

On the RAM console, click **Policies**.

On the **Policy Management** page, click **New Authorization Policy**.



Select an authorization policy among the templates provided, which including a blank template, system templates and custom templates such as AliyunOSSReadOnlyAccess. You can then edit your policy based on the template, as shown in the following figure:

Create Authorization Policy
✕

STEP 1: Select an authorization policy
STEP 2: Edit permissions and submit
STEP 3: Policy created

\* Authorization policy name:

The name must be 1-128 characters long and can contain English letters, numbers, and "-"

Remarks:

Policy content: 

```

2  "Version": "1",
3  "Statement": [
4    {
5      "Action": [
6        "oss:Get*",
7        "oss:List*"
8      ],
9      "Effect": "Allow",
10     "Resource":
11     "acs:oss:*:*:samplebucket/bob/*",
12     "Condition": {
13       "IpAddress": {
14         "acs:SourceIp": "127.0.27.1"
15       }
16     }
17   }

```

[Authorization policy format definition](#)  
[Authorization policy FAQs](#)

Prev
New Authorization Policy
Cancel

Custom policy example:

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "oss:Get*",
        "oss:List*"
      ],
      "Resource": [
        "acs:oss:*:*:samplebucket/bob/*"
      ]
    }
  ],
  "Condition": {
    "IpAddress": {
      "acs:SourceIp": "127.0.27.1"
    }
  }
}
```

Once finish all the settings, click **New Authorization Policy** to complete creating the custom authorization policy.

If you attach this custom authorization policy to the user B, B will have read-only permission for all of the objects in `oss://samplebucket/bob/` as long as they access the objects from your company network (in this example, 121.0.27.1).

## Procedure



## RAM user authorization

### Grant permissions to a RAM user directly (using `AttachPolicyToUser`)

Log on to the Alibaba Cloud console, and then click **Resource Access Management** from the left-side navigation bar to open the RAM console.

On the RAM console, click **Users**.

On the **User Management** page, click **Authorization** next to the user to whom you want to grant permissions.

In the **Edit Authorization Policy** window, click an authorization policy and move it to the selected authorization policy field.

Click **OK**.

## Grant permissions to the group to which a user belongs (using `AttachPolicyToGroup`)

Create a user group (if you already have a group, go directly to step 2).

- a. Go to the RAM console and click **Groups**.
- b. Click **New Group**. In the pop-up window, specify a group name and remarks. Click **OK**.
- c. Add a user to the user group. You can do this through user management or group management.

Attach an authorization policy to the group.

- a. Go to the RAM console and click **Groups**.
- b. On the **Group Management** page, click **Authorization** next to the group that you want to attach an authorization policy to.
- c. In the pop-up window, select an authorization policy and move it from the selected policy field, and then click **OK**.

## System authorization policies and custom authorization policies

System authorization policies are a group of general authorization policies provided by RAM to meet your coarse-grained authorization needs. For example, you can use them to authorize a RAM user to manage orders (`AliyunBSSFullAccess`), ECS resources (`AliyunECSFullAccess`), or all sub-users and their permissions (`AliyunRAMFullAccess`).

In RAM Authorization Policy Management, you can view all the system authorization policies that are

supported by RAM.

If these authorization policies do not meet your needs, you can create custom authorization policies. For details, refer to [Create a Customer Authorization Policy](#).

## Procedure



## RAM user login

The RAM user login endpoint URL is different from the primary account login endpoint URL. You can find your RAM user login URL in the dashboard tab of the RAM web console.

RAM Overview

Welcome to Resource Access Management (RAM)

---

RAM User Login Link: <http://signin-intl.aliyun.com/>

User Overview

You have ( 24 ) users(s)

Group Overview

You have ( 2 ) group(s)

Permission Policy Overview

You have ( 3 ) custom policy(ies)

Role Overview

You have ( 11 ) role(s)

Operations Guide

1. Manage authorization policies.
2. Create and authorize groups.
3. Create users and add them to groups.
4. Authorization complete.