Alibaba Cloud
Resource Access Management

Quick Start

Issue: 20180930

MORE THAN JUST CLOUD | Alibaba Cloud

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.	⛔ **Danger:** 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.	⚠ **Warning:** 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.	📋 **Note:** 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.	📋 **Note:** You can use **Ctrl** + **A** to select all files.
>	Multi-level menu cascade.	**Settings** > **Network** > **Set network type**
Bold	It is used for buttons, menus, page names, and other UI elements.	Click **OK**.
`Courier font`	It is used for commands.	Run the `cd /d C:/windows` command to enter the Windows system folder.
`Italics`	It is used for parameters and variables.	`bae log list --instanceid` *`Instance_ID`*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *`[-all|-t]`*
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich` *`{stand | slave}`*

Contents

Legal disclaimer..I
Generic conventions..I
1 Introduction..1
2 Set up MFA (optional)..2
3 Create a RAM user..6
4 Create a RAM user group (optional)..12
5 Create a custom policy (optional)..13
6 Attach policies to a RAM user..17
7 Log on with a RAM user account..19
8 Limits..20

1 Introduction

This document lists the tasks you should perform to get started with Resource Access Management (RAM):

1. *Set up MFA (optional)*
2. *Ram initial setup*
3. *Create a RAM user*
4. *Create a RAM user group (optional)*
5. *Create a custom policy (optional)*
6. *Attach policies to a RAM user*
7. *Log on with a RAM user account*

2 Set up MFA (optional)

This document describes how to activate and use multi-factor authentication (MFA) to log on to the RAM console. With MFA, your account security will be improved.

Activate MFA for your primary account

Your primary account has full control over the resources under it. Once the logon password or access key of the primary account is disclosed, the assets under the account will face great security threats. To reduce the security threats, we strongly recommend that you bind MFA to your primary account.

Prerequisites

Make sure you have installed on your smartphone a virtual MFA application, preferably the Alibaba Cloud app.

You can also install Google Authenticator, which is also a common MFA application.

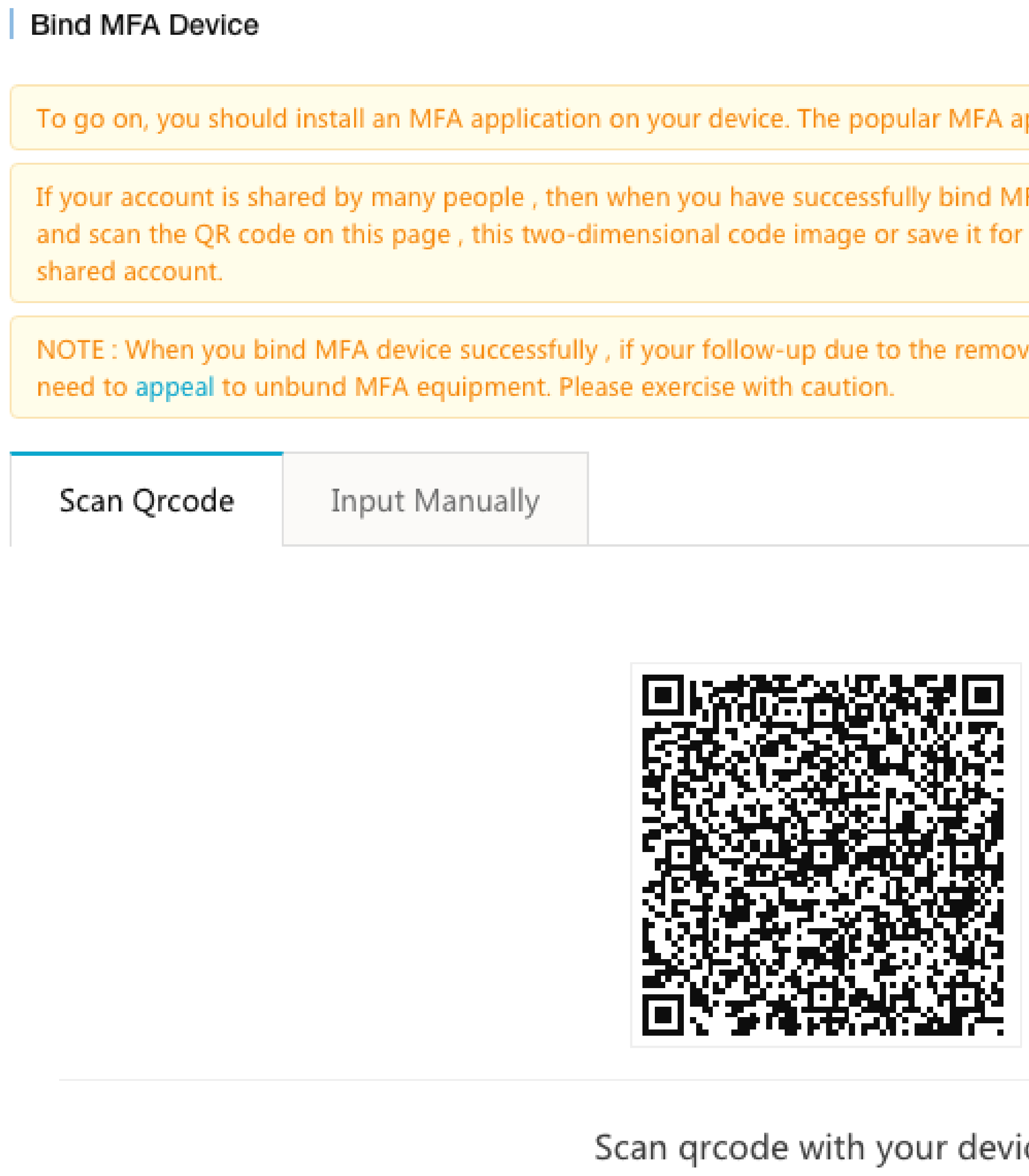
- iOS: Install Google Authenticator in App Store. The installation method can be found in *iOS-based Google Authenticator installation and use guide*.
- Android: Install Google Authenticator in Google Play. The installation method can be found in *Android-based Google Authenticator installation and use guide*.

The following takes the Alibaba Cloud app as an example to describe the operation procedure.

Procedure

1. Log on to the Alibaba Cloud Console with your primary account. Choose Account Management > Security Settings to open the *Security Settings* page.
2. Under the **Virtual MFA** menu, click **Set** to enter the virtual MFA device binding procedure.
3. Complete the authentication through mailbox authentication, smartphone authentication, or security authentication. Then, go to the **Enable the Virtual MFA Device** page, as shown in the following figure.

Figure 2-1: Identity verification



Bind MFA Device

To go on, you should install an MFA application on your device. The popular MFA ap

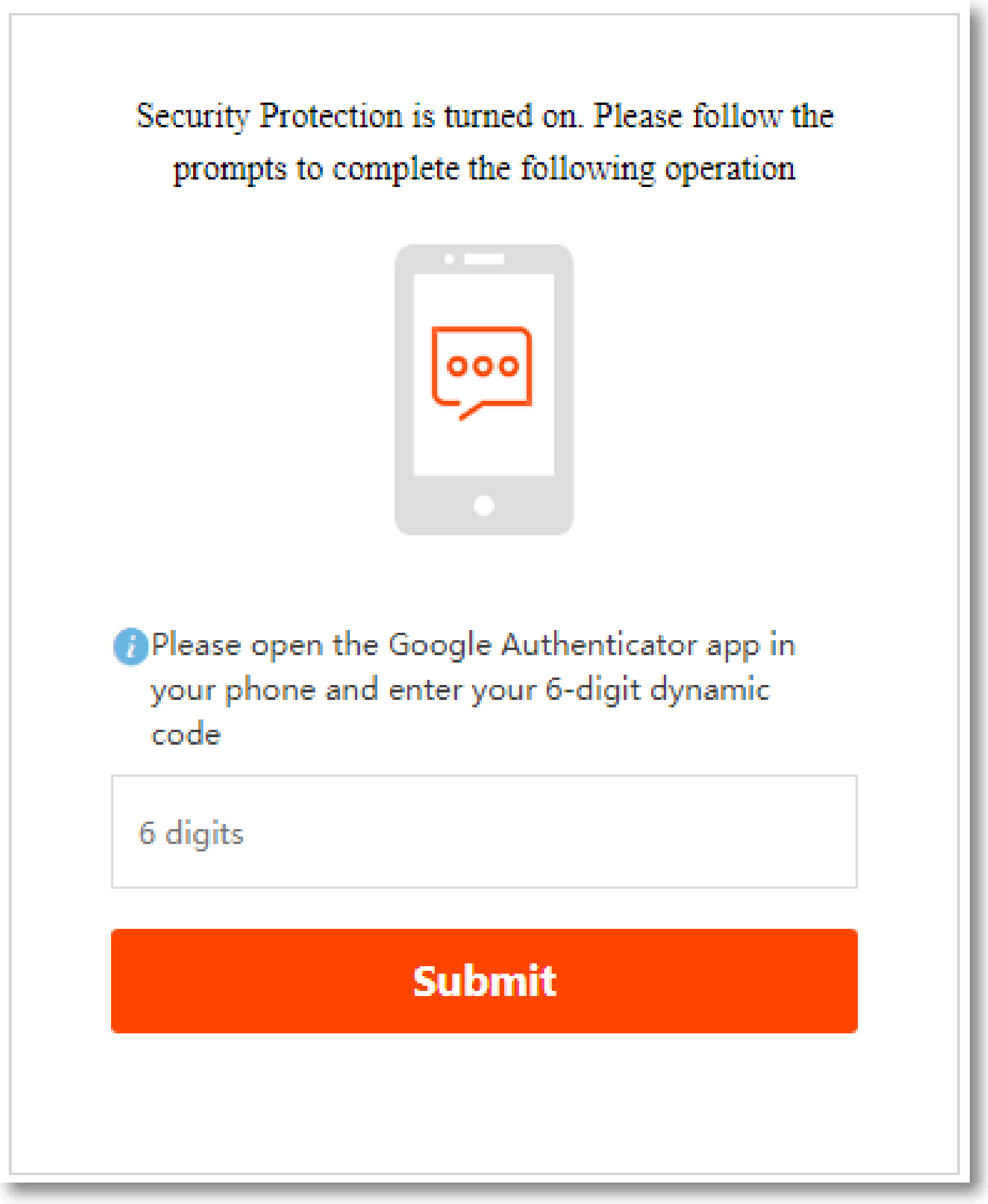
If your account is shared by many people , then when you have successfully bind MF and scan the QR code on this page , this two-dimensional code image or save it for shared account.

NOTE : When you bind MFA device successfully , if your follow-up due to the remov need to appeal to unbund MFA equipment. Please exercise with caution.

Scan qrcode with your devic

4. Open the **Alibaba Cloud app** in your smartphone and select**+** > **Sweep Code add**Sweep code. The user is automatically added upon completion of the sweep code, and the Alibaba Cloud app displays the dynamic password for your current account, update every 30 seconds.

Figure 2-2: Dynamic Password



Security Protection is turned on. Please follow the prompts to complete the following operation

Please open the Google Authenticator app in your phone and enter your 6-digit dynamic code

Note:

If your smart device does not support code sweep, then you can also select hand-to-hand information acquisition and manually enter it in the MFA application. How the MFA key is configured.

5. Enter mfa on the enable virtual MFA appliance page Apply the two consecutive sets of dynamic passwords displayed in, and then click OK to enable. as shown in the following figure.

   Figure 2-3: Enable virtual MFA Devices

So far, you have successfully enabled the MFA device.

Login process after opening MFA

After opening MFA, you can only log in to Ali cloud after completing two-step verification. The operation is as follows:

1. Enter your login user name and password first when you log on to the console.
2. After the password is verified, you also need to provide the dynamic verification code from the VMFA device, as shown in the figure below:

   Figure 2-4: Verify dynamic security verification code

In your mobile Alibaba Cloud app, get and enter the dynamic verification code for your login account, you can log in to Ali cloud.

3 Create a RAM user

Before creating a RAM user, ensure that you have finished *Ram initial setup* and have configured your enterprise alias, RAM user's logon password policy, and security policy.

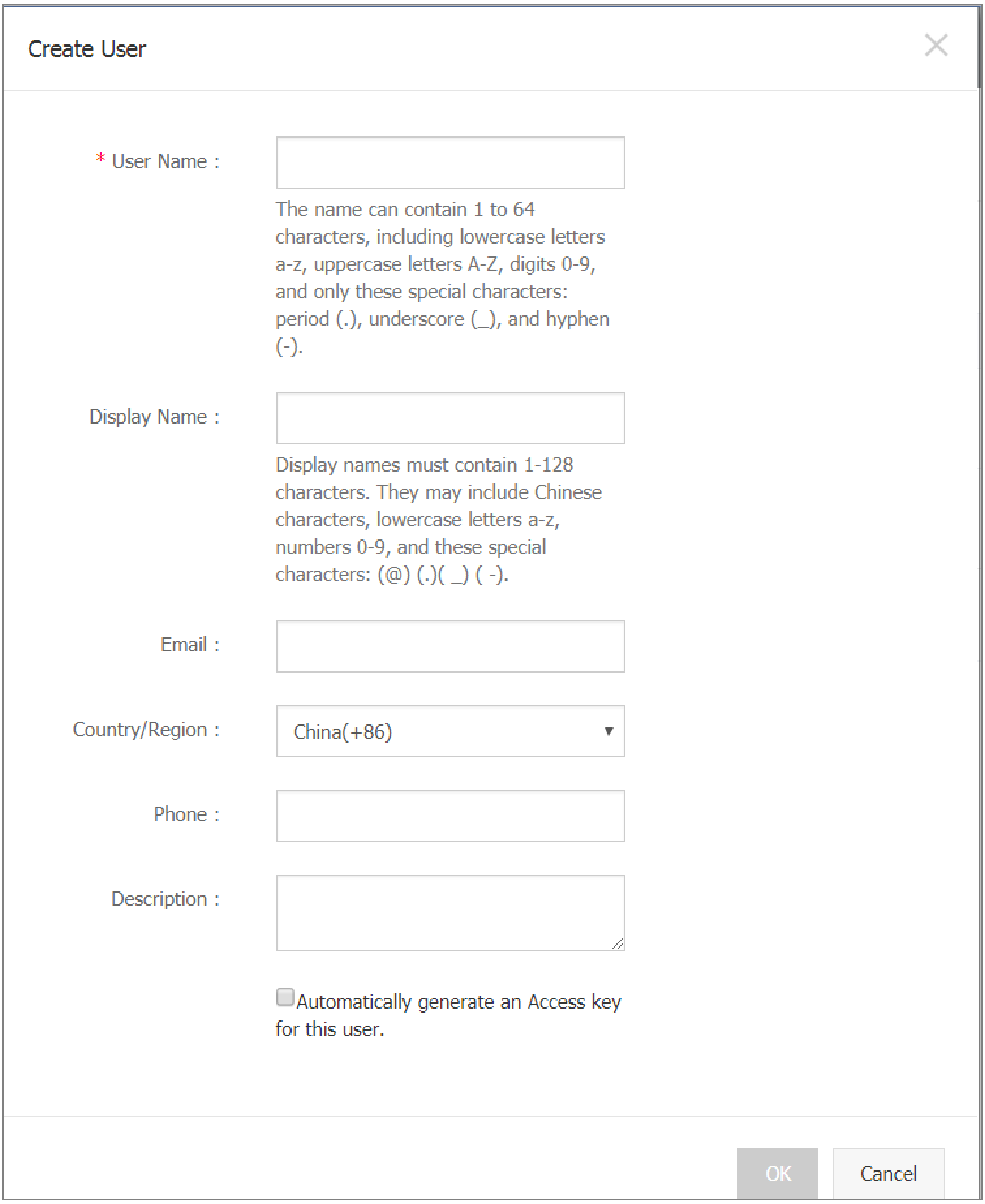
This document describes how to create a RAM user and how to configure the logon password (if the user needs to log on to the console) or the AccessKey (if the user needs to call the cloud service API through a program).

Create a RAM user

To create a RAM user, follow these steps.

1. From the left navigation pane of the *RAM console*, click **Users**.
2. Click **Create User** in the upper right corner to open the Create User dialog box.
3. After entering user information, click **OK**.

Figure 3-1: Create a user



Create User

* User Name :

The name can contain 1 to 64 characters, including lowercase letters a-z, uppercase letters A-Z, digits 0-9, and only these special characters: period (.), underscore (_), and hyphen (-).

Display Name :

Display names must contain 1-128 characters. They may include Chinese characters, lowercase letters a-z, numbers 0-9, and these special characters: (@) (.)(_) (-).

Email :

Country/Region : China(+86)

Phone :

Description :

□ Automatically generate an Access key for this user.

Now, you have created a RAM user.

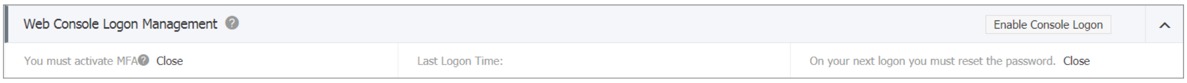
Create a logon password

To allow a RAM user's access to the management console, create a logon password for the user.

Procedure

1. From the left navigation pane of the RAM console, click **Users**.
2. On the User Management page, select the target user (which can be searched by **User Name**) and click the user name or the corresponding **Manage** in the Actions column to open the User Details page.
3. In the **Web Console Logon Management** area, click **Enable Console Logon**.

   Figure 3-2: Enable console logon

   Web Console Logon Management

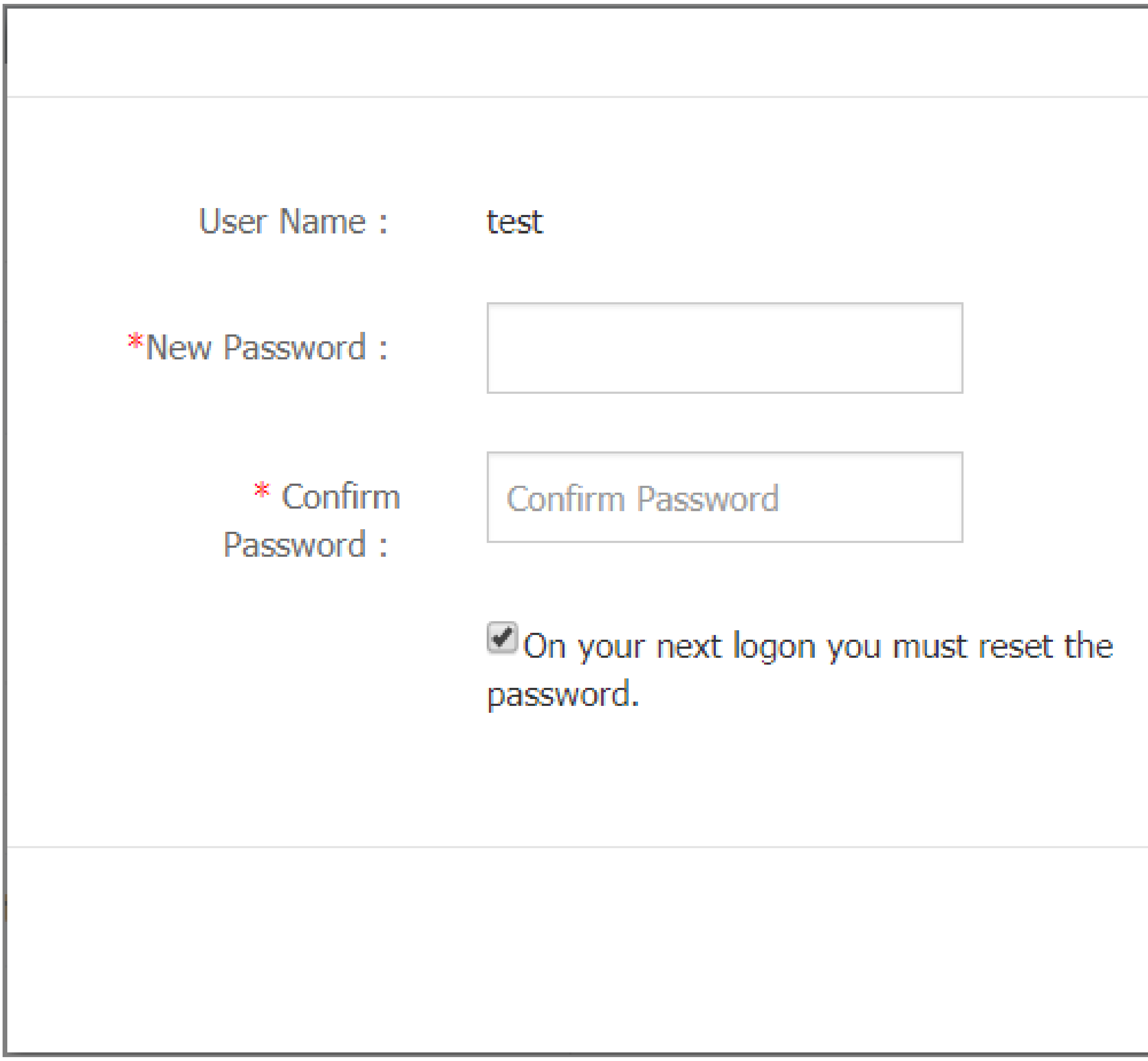
   You must activate MFA Close

   Last Logon Time:

   On your next logon you must reset the password. Close

4. In the displayed dialog box, set an initial password for the user. You can also specify that the user must change this password at next logon.

Figure 3-3: Set a logon password



User Name : test

*New Password :

* Confirm Password : Confirm Password

☑ On your next logon you must reset the password.

Now, you have set the logon password for the RAM user.

- To log on for testing as a RAM user, see *Log on with a RAM user account*.
- To manage the RAM user logon password, perform steps 1 through 3. In the **Web Console Logon Management** area, click **Reset Password** or **Disable Console Logon**.

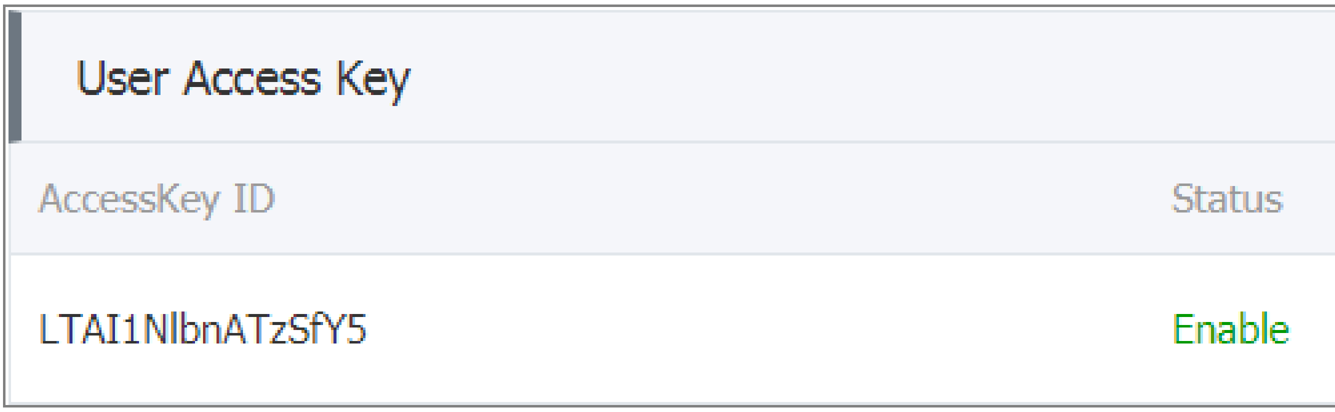
Create an AccessKey

To allow a RAM user to call the cloud service API through a program, create an AccessKey for the user.

Procedure

1. From the left navigation pane of the RAM console, click **Users**.
2. Select the target user (which can be queried by **User Name**). Click the user name or **Manage** to open the User Details page.
3. In the **User Access Key** area, click **Create Access Key**.

Figure 3-4: Create AccessKey



User Access Key

AccessKey ID	Status
LTAI1NlbnATzSfY5	Enable

4. After an AccessKey is created, click **Save Access Key Information** to save the AccessKey.

Note:

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

Now, you have created an AccessKey for the RAM user. To manage the user's AccessKey, perform steps 1 through 3. In the **User Access Key** area, **Disable** or **Delete** an existing AccessKey.

Follow-up operations

For a RAM user that has been created, assign the user an appropriate permission for accessing resources based on the user's responsibilities, before performing operations.

- For details about how to attach policies to a RAM user, see *Attach policies to a RAM user*.
- To create a fine-grained custom authorization policy, see *Create a custom policy (optional)*create a custom policy.

4 Create a RAM user group (optional)

Procedure

1. In the RAM console, click**Groups** > **Create Group**.

   Figure 4-1: Create a group

2. In the **Create Group** dialog box, enter **Group Name** (mandatory) and **Description** (optional) and then click **OK**.

5 Create a custom policy (optional)

At present, Alibaba Cloud offers a variety of system authorization policies for users. These authorization policies only provide coarse-grained access control capabilities, for example, read-only permissions or all permissions at a cloud product level.

If you have more fine-grained authorization requirements, for example, to authorize the user Bob to perform read-only operations on all objects only in `oss://samplebucket/bob/` and to 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), then you can perform access control by creating a custom authorization policy.

This document describes, taking user Bob for example, how to create a custom authorization policy, helping you better understand and use RAM for fine-grained access control.

The limit for log groups is: a maximum of 4096 logs or 10 MB space

Prerequisite

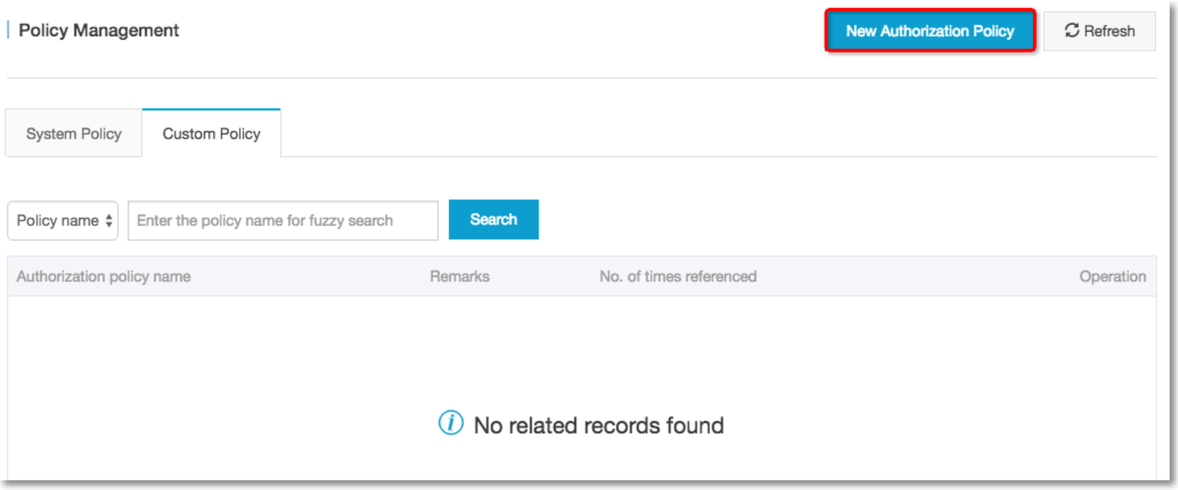
Before creating custom authorization policies, you must understand the basic structure and syntax of the authorization policy language. For more details, see *Attach policies to a RAM user*.

RAM supports the authorization of the API granularity, at the finest. That is, the operation permissions in the authorization policy can be as fine as each API. Before creating custom authorization policies, you must understand the authorization granularity and method supported by related products. For more details, see *Attach policies to a RAM user*.

Operation steps

1. In the RAM console, click **Policies** from the left-side navigation pane. On the **Policy Management** page, you can view the existing systems and custom policies through the **System Policy** and **Custom Policy** subpages, respectively.

Figure 5-1: Custom authorization policy



Policy Management

New Authorization Policy

Refresh

System Policy

Custom Policy

Policy name

Enter the policy name for fuzzy search

Search

Authorization policy name	Remarks	No. of times referenced	Operation

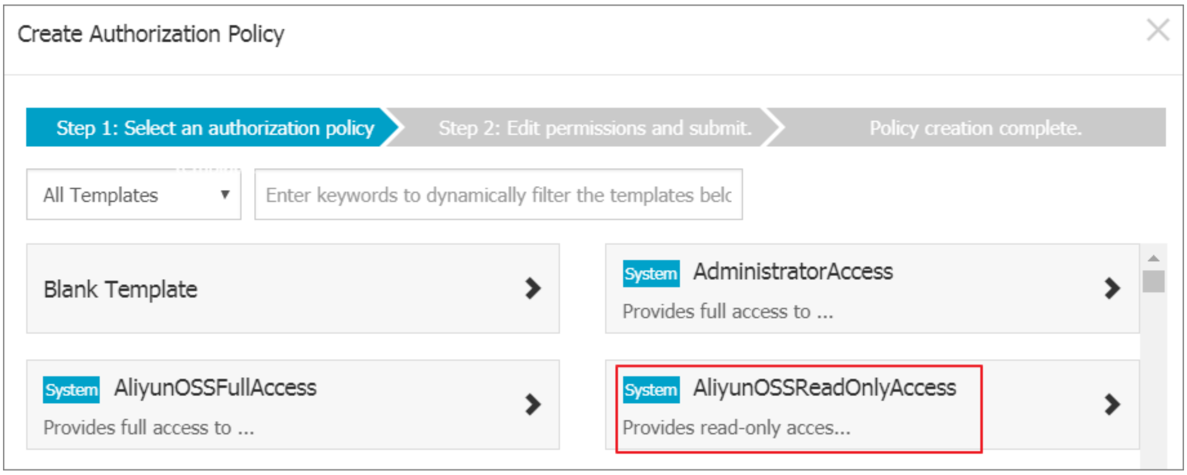
No related records found

2. Click **Create Authorization Policy** to go to the **Create Authorization Policy** page.
3. Select the policy template.

Note:

You can select a blank template, but it is recommended that you use a similar existing system policy as a template for editing. The policy AliyunOSSReadOnlyAccess (the read-only permission for all OSS resources under the account) is used as the template here.

Figure 5-2: Create an authorization policy



Create Authorization Policy

Step 1: Select an authorization policy

Step 2: Edit permissions and submit.

Policy creation complete.

All Templates

Enter keywords to dynamically filter the templates belc

Blank Template

System AdministratorAccess

Provides full access to ...

System AliyunOSSFullAccess

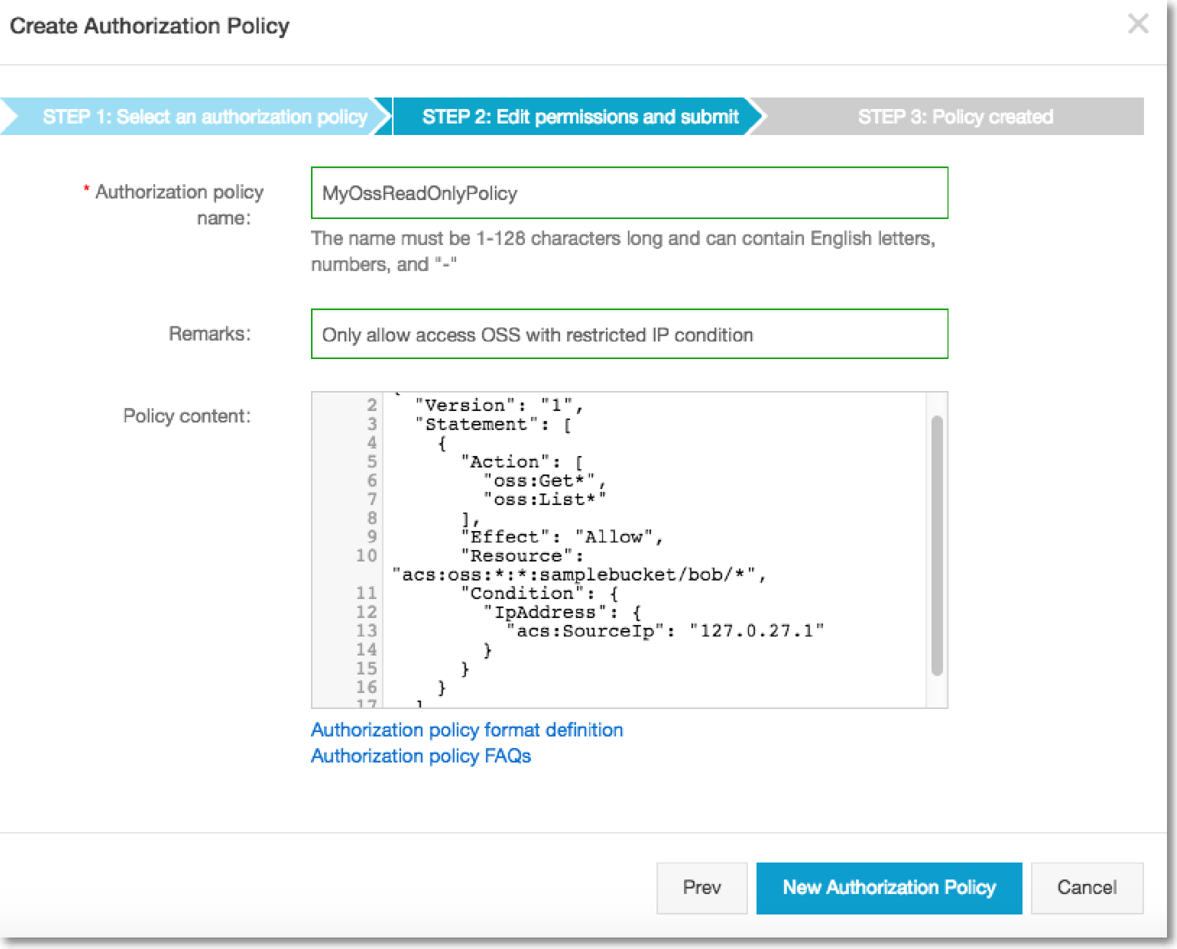
Provides full access to ...

System AliyunOSSReadOnlyAccess

Provides read-only acces...

4. Edit your policy based on the selected template.
5. Once finishing all the settings, click **New Authorization Policy** to complete creating the custom authorization policy.

Figure 5-3: New authorization policy



Create Authorization Policy

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

* Authorization policy name: MyOssReadOnlyPolicy

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

Remarks: Only allow access OSS with restricted IP condition

Policy content:

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

Authorization policy format definition
Authorization policy FAQs

Here, the **Authorization policy name**, **Remarks**, and **Policy content** are modified. The highlighted part of the **Policy content** is the added fine-grained authorization content. The code sample is:

~~~~
```json
{
"Version": "1",
"Statement": [
{
"Effect": "Allow",
"Action": [
"oss:Get*",
"oss:List*"
],
"Resource": [
"acs:oss:*:*:samplebucket/bob/*"
],
"Condition": {
"IpAddress": {
"acs:SourceIp": "121.0.27.1"
}
}
~~~~

~~~
}
]
}

```
~~~

Subsequent operation

Next, simply authorize the policy created in this document to user Bob, and Bob will have the read-only permission for the objects in `oss://samplebucket/bob/`, allowing access of the IP address (121.0.27.1) only from your company network.

Assign the authorization policy to the RAM user. For details, see *Attach policies to a RAM user*.

6 Attach policies to a RAM user

There are two methods for authorizing a RAM user:

- *Attach policies to a RAM user directly*
- *Authorization for user group to which the user belongs*

Both of these methods can achieve the purpose of granting a RAM user the permission for accessing related resources.

Background

System authorization policies are a group of general authorization policies that meet coarse-granularity authorization requirements. 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).

You can view all the system authorization policies that are supported by RAM in *Authorization Policy Management*.

If none of these authorization policies meet your needs, you can customize a finer-granularity authorization policy. For details, see *Create a custom policy (optional)*.

Attach policies to a RAM user directly

Use AttachPolicyToUser to attach policies to a RAM user directly.

The operation procedure is as follows:

1. Click **Users** in the left navigation pane of the RAM console.
2. On the Users page, click **Authorize** next to the user (which can be searched by user name) to whom you want to grant permissions.
3. In the **Edit User-Level Authorization** window, click an authorization policy and move it to the selected authorization policy field.
   - Optional Authorization Policy Name from left Select the policy you want in the list, click the right arrow (that is, authorization) adds it to the list of selected Authorization Policy names.
   - Instead, click the left arrow to deselect the policy in the list of selected Authorization Policy names.

   Figure 6-1: Edit a personal authorization policy

Authorization for user group to which the user belongs

Through the chain. Authorize the user group to which the user belongs.

Before using this method, make sure that the authorized user is already in the user group that you want to authorize.

Operation steps

1. In the ram console, click Group Management in the left navigation bar.
2. Locate the user group to which you want to authorize the user, and click the authorization button for this user group.
3. In the Edit Group Authorization Policy Dialog Box, add an Authorization Policy (search by keyword), and click Determine.

Subsequent operation

- For direct grant of RAM Permissions for users, you can go to the personal authorization Policies tab of the user authorization Policies Sub-page View permissions, or disauthorize.
- For grant of RAM Permissions for user-owned user groups, you can go to the group Authorizat ion Policy Management Sub-page to view the permissions or disauthorize.

7 Log on with a RAM user account

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

Logon entry

After logging on to the *RAM console*, query the logon link on the **Dashboard** page.)

Logon information

RAM user logon requires an enterprise alias, a sub-user name, and a password.

The enterprise alias is the one you have configured in *Ram initial setup*. If you have not configured the enterprise alias, the default enterprise alias is your cloud account ID (which can be queried through**Account Management** > **Security Settings**.

8 Limits

Resource	Limit
Users in an Alibaba Cloud account	100
Groups in an Alibaba Cloud account	50
Groups a RAM user can join	5
AccessKeys a RAM user can create	2
Virtual MFA devices in use for a RAM user	1
Virtual MFA devices in an Alibaba Cloud account	100
Custom policies in an Alibaba Cloud account	200
Versions of a custom policy that can be stored	5
Authorization policies attached to a user	5
Authorization policies attached to a group	5
Characters for a user name	64
Characters for a group name	64
Characters for an authorization policy name	128
Characters for a role name	64
Roles	100
Characters for an alias	3-64
Characters for a custom authorization policy	2048