ALIBABA CLOUD

Alibaba Cloud

Resource Access Management
RAM User Management

Document Version: 20220429

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, 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 this document 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice 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.
Warning	A warning notice 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 restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	**Notice:** If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	**Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Overview of RAM users

This topic describes the basic concepts of Resource Access Management (RAM) users. This topic also describes the procedure, best practices, and limits of using RAM users.

What is a RAM user?

A physical identity that has a fixed ID and credential information. A RAM user represents a person or an application. A RAM user has the following characteristics:

- A RAM user can be created by an Alibaba Cloud account. In this case, the RAM user belongs to the Alibaba Cloud account. A RAM user can also be created by a RAM user or a RAM role that has administrative rights. In this case, the RAM user belongs to the Alibaba Cloud account that creates the RAM user or the RAM role.
- A RAM user does not own resources. Resource usage fees of the RAM user are billed to the Alibaba Cloud account to which the RAM user belongs. A RAM user does not receive individual bills and cannot make payments.
- Before RAM users can log on to the Alibaba Cloud Management Console or call operations, they must be authorized by Alibaba Cloud accounts. After RAM users are authorized, the RAM users can access resources that are owned by the Alibaba Cloud accounts.
- RAM users have independent passwords or AccessKey pairs for logon.
- An Alibaba Cloud account can create multiple RAM users. RAM users can be employees, systems, and applications within an enterprise.

You can create RAM users and authorize the RAM users to access different resources. If multiple users in your enterprise need to simultaneously access resources, you can use RAM to assign the least permissions to the users. This prevents the users from sharing the username and password or AccessKey pair of an Alibaba Cloud account and reduces the security risks.

Procedure

1. Log on to the RAM console by using an Alibaba Cloud account or a RAM user or a RAM role that has administrative rights.
2. Create a RAM user.

   For more information, see Create a RAM user.
3. Configure logon parameters.

   You can configure both logon passwords and AccessKey pairs for RAM users. For security reasons, we recommend that you configure only a logon password or an AccessKey pair for a RAM user to ensure security. If a RAM user is an application, the RAM user must call operations to access resources. In this case, you need to create only an AccessKey pair for the RAM user. If a RAM user is an employee, the RAM user must log on the Alibaba Cloud Management Console to access resources. In this case, you need to configure only a logon password for the RAM user.

   - Logon to the Alibaba Cloud Management Console

     You must enable logon to the Alibaba Cloud Management Console, configure a console logon password, and configure a password policy for the RAM user. You can also change the console logon password and enable multi-factor authentication (MFA) based on your business requirements. For more information, see Manage console logon settings for a RAM user, Configure a password policy for RAM users, Change the password of a RAM user, and Enable an MFA device for a RAM user.

> **Note** If user-based single sign-on (SSO) is enabled, you do not need to enable logon to the Alibaba Cloud Management Console for the RAM user. The RAM user can log on to the Alibaba Cloud Management Console by using user-based SSO. For more information, see Overview of user-based SSO.

- API calls

  You must create an AccessKey pair for the RAM user. For more information, see Create an AccessKey pair for a RAM user.

4. Grant permissions to the RAM user.

   You can grant different RAM users the permissions to access different resources. For more information, see Grant permissions to a RAM user.

5. Use the RAM user to log on to the Alibaba Cloud Management Console or call operations by using an AccessKey pair.

   For more information, see Log on to the Alibaba Cloud Management Console as a RAM user and API overview.

Best practices

Enterprises that have multiple Alibaba Cloud resources can use RAM to manage identities, user permissions, and resources. For more information, see Use RAM to manage user permissions and resources.

Limits

For more information about the limits of using RAM users, see Limits.

2.Basic operations

2.1. Create a RAM user

This topic describes how to create a Resource Access Management (RAM) user. A RAM user is an entity that you create in RAM to represent an O&M engineer or application. After you create a RAM user and grant the relevant permissions to the RAM user, the RAM user can access the required Alibaba Cloud resources.

Procedure

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Users**.
3. On the **Users** page, click **Create User**.
4. In the **User Account Information** section of the **Create User** page, configure the **Logon Name** and **Display Name** parameters.

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

5. In the **Access Mode** section, select an access mode.
   - **Console Access**: If you select this option, you must complete the logon security settings. These settings specify whether to use a system-generated or custom logon password, whether the password must be reset upon the next logon, and whether to enable multi-factor authentication (MFA).

     > **Note** If you select Custom Logon Password in the Console Password section, you must specify a password. The password must meet the complexity requirements. For more information about the complexity requirements, see Configure a password policy for RAM users.

   - **OpenAPI Access**: If you select this option, an AccessKey pair is automatically created for the RAM user. The RAM user can call API operations or use other development tools to access Alibaba Cloud resources.

     > **Note** To ensure the security of the Alibaba Cloud account, we recommend that you select only one access mode for the RAM user. This prevents the RAM user from using an AccessKey pair to access Alibaba Cloud resources after the RAM user leaves the organization.

6. Click **OK**.

What's next

- The created RAM user can be used to log on to the RAM console. For more information, see Log on to the Alibaba Cloud Management Console as a RAM user.
- You can attach policies to the RAM user. After you attach a policy, the RAM user can access the Alibaba Cloud resources that are specified in the policy. For more information, see Grant permissions to a RAM user.
- You can add the RAM user to RAM user groups and grant permissions to the RAM user groups. For

more information, see Add a RAM user to a RAM user group.

Related information

- CreateUser

2.2. Delete a RAM user

This topic describes how to delete a Resource Access Management (RAM) user. After a RAM user is deleted, the AccessKey pairs of the RAM user are deleted, the permissions of the RAM user are removed, and the multi-factor authentication (MFA) device and the DingTalk account of the RAM user are unbound from the RAM user.

Prerequisites

The RAM user is not used by systems or applications. Otherwise, a service failure may occur after the RAM user is deleted.

Procedure

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Users**.
3. On the **Users** page, find the RAM user that you want to delete and click **Delete** in the **Actions** column.
4. In the **Delete User** message, click **I fully understand the risks and confirm the deletion.**

Related information

- DeleteUser

2.3. View the basic information about a RAM user

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

Procedure

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Users**.
3. On the **Users** page, click the username of a specific RAM user.
4. In the **Basic Information** section of the page that appears, view information such as **Logon Name**, **Display Name**, and **UID**.

Related information

- GetUser

2.4. Modify the basic information about a RAM user

This topic describes how to modify the basic information, such as the logon name and display name, about a Resource Access Management (RAM) user.

Procedure

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Users**.
3. On the **Users** page, click the username of the specific RAM user whose information you want to modify.
4. In the **Basic Information** section, click **Modify Basic Information**.
5. In the **Modify Basic Information** panel, modify the basic information about the RAM user and click **OK**.

Related information

- UpdateUser

3.Logon management

3.1. Manage console logon settings for a RAM user

This topic describes how to enable console logon, and view, modify, or clear console logon settings for a Resource Access Management (RAM) user.

Enable console logon for a RAM user

You can enable console logon for a RAM user and configure parameters such as the logon password.

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Users**.
3. In the **User Logon Name/Display Name** column, click the username of ta specific RAM user.
4. In the **Console Logon Management** section of the **Authentication** tab, click **Enable Console Logon**.
5. In the **Modify Logon Settings** panel, configure the following parameters.
   - **Console Password Logon**: Select **Enabled**.
   - **Set Logon Password**: Select Automatically Generate Default Password or Custom Logon Password based on your business requirements.

     > **Note** We recommend that you save the password for subsequent use.

   - **Password Reset**: Set this parameter to specify whether to reset the password upon the next logon of the RAM user.
   - **Enable MFA**: Set this parameter to specify whether to enable multi-factor authentication (MFA) for the RAM user.

     > **Note** If you select Required, the page on which you can enable an MFA device automatically appears upon the next logon of the RAM user.

6. Click **OK**.

View console logon settings of a RAM user

After you enable console logon for a RAM user, you can view the console logon settings.

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Users**.
3. In the **User Logon Name/Display Name** column, click the username of ta specific RAM user.
4. In the **Console Logon Management** section of the **Authentication** tab, view the console logon settings.
   - **Console Access**: indicates whether console logon is enabled.
   - **Last Console Logon**: indicates the last time that the RAM user logged on to the console.

- **Required to Enable MFA**: indicates whether MFA is required when the RAM user logs on to the console.
- **Reset Password at Next Logon**: indicates whether password resetting is required when the RAM user logs on to the console the next time.
- **Logon Method**: indicates that username-password logon is enabled for the RAM user. You can move the pointer over the icon to the right of the Logon Method parameter and click the link to log on to the console as the RAM user. You can also copy the link and paste the link to the address bar of your browser to log on to the console.

Modify console logon settings for a RAM user

After you enable console logon for a RAM user, you can modify console logon settings based on your business requirements. For example, you can disable console logon or modify the logon password.

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Users**.
3. In the **User Logon Name/Display Name** column, click the username of a specific RAM user.
4. In the **Console Logon Management** section of the **Authentication** tab, click **Modify Logon Settings**.
5. In the **Modify Logon Settings** panel, configure the following parameters.
   - **Console Password Logon**: Select **Disabled**.

     > **Note** If you select Disabled, you can still modify logon settings for the RAM user. However, the settings after modification do not take effect. The settings take effect only after you select **Enabled**.

   - **Set Logon Password**: Select Automatically Generate Default Password or Custom Logon Password based on your business requirements.

     > **Note** We recommend that you save the password for subsequent use.

   - **Password Reset**: Set this parameter to specify whether to reset the password upon the next logon of the RAM user.
   - **Enable MFA**: Set this parameter to specify whether to enable multi-factor authentication (MFA) for the RAM user.

     > **Note** If you select Required, the page on which you can enable an MFA device automatically appears upon the next logon of the RAM user.

6. In the **Modify Logon Settings** panel, click **OK**.

Clear console logon settings for a RAM user

You can clear console logon settings for a RAM user with a few clicks and disable console logon for the RAM user.

> **Notice** The console logon settings cannot be automatically restored after the settings are cleared. Proceed with caution.

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Users**.
3. In the **User Logon Name/Display Name** column, click the username of a specific RAM user.
4. In the **Console Logon Management** section of the **Authentication** tab, click **Remove Logon Settings**.
5. In the **Remove Logon Settings** message, click **OK**.

3.2. Configure a password policy for RAM users

This topic describes how to configure a password policy for the Resource Access Management (RAM) users of your Alibaba Cloud account. You can specify password complexity requirements, including the password length, validity period, and password history check.

Context

Your password is hashed by using Secure Hash Algorithm 256 (SHA-256) with a salt value. Alibaba Cloud does not save your password in plaintext. This ensures password security.

Procedure

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Settings**.
3. On the **Security Settings** tab of the page that appears, click **Edit**. In the panel that appears, configure the parameters.
   - **Password Length**: This parameter specifies the minimum length of passwords. The value ranges from 8 to 32.

     > **Note** To ensure account security, we recommend that you set this parameter to a value greater than or equal to 8.

   - **Required Elements in Password**: The available elements include Lowercase Letters, Uppercase Letter, Numbers, and Symbols.

     > **Note** To enhance account security, we recommend that you select at least two of the preceding elements.

   - **Minimum Different Characters in Password**: The value ranges from 0 to 8. The default value is 0, which indicates that no limits are imposed on the number of unique characters in a password.
   - **Include Username in Password**: The valid values are **Allow** and **Do Not Allow**. You can select one based on your business requirements.
     - **Allow**: A password can contain the username.
     - **Do Not Allow**: A password cannot contain the username.
   - **Password Validity Period**: The value ranges from 0 to 1095, in days. The default value is 0, which indicates that the password never expires.

> **Note** If you reset a password, the password validity period restarts.

- **Action After Password Expires**: You can specify whether to allow the RAM users to log on to the Alibaba Cloud Management Console after their passwords expire. You can select **Deny Logon** or **Allow Logon** based on your business requirements.
  - **Deny Logon**: After the password expires, you cannot use the password to log on to the Alibaba Cloud Management Console. You can log on to the console only after you reset the password by using your Alibaba Cloud account or as a RAM user that has administrative rights.
  - **Allow Logon**: After the password expires, you can change the password as a RAM user and use the new password to log on to the Alibaba Cloud Management Console.
- **Password History Check Policy**: You can prevent RAM users from reusing the previous *N* passwords. The value ranges from 0 to 24. The default value is 0, which indicates that the RAM users can reuse previous passwords.
- **Password Retry Constraint Policy**: This parameter specifies the maximum number of password retries. If you enter the wrong passwords for the specified consecutive times, the account is locked for one hour. The value ranges from 0 to 32. The default value is 0, which indicates that the password retries are not limited.

> **Note** After you change the password, the number of password retries is reset to zero.

4. Click **OK**.

Result

The password policy applies to all RAM users of your Alibaba Cloud account.

Related information

- SetPasswordPolicy

3.3. Change the password of a RAM user

This topic describes how to change the password of a Resource Access Management (RAM) user that belongs to your Alibaba Cloud account. You can change your password on a regular basis for account security.

Procedure

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Users**.
3. On the **Users** page, click the username of a specific RAM user.
4. On the **Authentication** tab of the user details page, click **Modify Logon Settings**.
5. In the **Set Logon Password** section of the **Modify Logon Settings** panel, reset the logon password.
   - If you select **Keep Current Password Unchanged**, the password remains unchanged.
   - If you select **Automatically Regenerate Default Password** and click **OK**, the system generates a logon password. You must save the generated password for subsequent use.

- If you select **Reset Custom Password**, enter a new password and click **OK**.

  > **Note** The new password must meet the complexity requirements. For more information, see Configure a password policy for RAM users.

6. Click **Close**.

> **Note** If your Alibaba Cloud account allows RAM users to manage their passwords, the RAM users can change their passwords in the console.

Related information

- ChangePassword

3.4. Enable an MFA device for a RAM user

This topic describes how to enable a multi-factor authentication (MFA) device for a Resource Access Management (RAM) user. Virtual MFA devices and Universal 2nd Factor (U2F) security keys are two types of MFA devices. After you enable an MFA device, it provides higher security protection for the RAM user.

> **Note** You can enable only one type of MFA device for a RAM user.

Enable a virtual MFA device

Prerequisites

Before you can enable a virtual MFA device, you must download and install the Google Authenticator app on your mobile device. You can use one of the following methods to download the Google Authenticator app:

- For iOS, download the Google Authenticator app from the App Store.
- For Android, download the Google Authenticator app from your preferred app store.

> **Note** For Android, you must also download and install a quick response (QR) code scanner from an app store for Google Authenticator to identify QR codes.

Enabling methods

You can use one of the following methods to enable a virtual MFA device based on your business requirements:

- You can enable a virtual MFA device by using an Alibaba Cloud account or a RAM user that has administrative rights in the RAM console.
- If you have selected Required for Enable MFA when you create a RAM user, you are required to bind a virtual MFA device upon the logon of the RAM user. You can select **Virtual MFA Device** in the **Enable MFA Device** dialog box and go to .
- If a RAM user of your Alibaba Cloud account is allowed to manage its own virtual MFA device, the RAM user can enable the virtual MFA device in the RAM console. To enable a virtual MFA device, perform the following operations: Move the pointer over the profile picture in the upper-right corner of the console and click **Security Information Management**. On the **Virtual MFA Device** tab of the **Console Logon** page, click **Enable Virtual MFA Device** and go to .

Procedure

1. Log on to the RAM console by using your Alibaba Cloud account or a RAM user that has administrative rights.
2. In the left-side navigation pane, choose **Identities > Users**.
3. In the **User Logon Name/Display Name** column, click the username of the RAM user for which you want to enable a virtual MFA device.
4. On the page that appears, click the **Authentication** tab. Then, click the **Virtual MFA Device** tab.
5. Click **Enable Virtual MFA Device**.
6. On your mobile device, enable a virtual MFA device.

   > **Note** The following example shows how to enable a virtual MFA device in the Google Authenticator app on your mobile device that runs iOS.

   i. Open the Google Authenticator app.

   ii. Click **Get started** and select one of the following methods to enable a virtual MFA device:

   - Tap **Scan a QR code** in the Google Authenticator app. Then, scan the QR code that is displayed on the **Scan the code.** tab in the RAM console. This method is recommended.
   - Tap **Enter a setup key**. Then, enter the account and key that you obtained from the **QR Information** tab in the RAM console, and tap **Add**.

7. In the RAM console, enter the two consecutive verification codes that are displayed in the Google Authenticator app. Then, click **Confirm Bind**.

   > **Note** 您还可以设置是否允许RAM用户**保存MFA验证状态7天**，如果为允许，则RAM用户使用MFA登录时，可以选中**记住这台机器，7天内无需再次验证**，就可以在7天内免MFA验证。关于具体的设置方法，请参见Configure security policies for RAM users。

Enable a U2F security key

Enabling methods

You can use one of the following methods to enable a U2F security key based on your business requirements:

- You can enable a U2F security key by using an Alibaba Cloud account or a RAM user that has administrative rights in the RAM console.
- If you have selected Required for Enable MFA when you create a RAM user, you are required to bind an MFA device upon the logon of the RAM user. You can select **U2F Security Key** in the **Enable MFA Device** dialog box and go to.
- If a RAM user of your Alibaba Cloud account is allowed to manage its own MFA device, the RAM user can enable a U2F security key in the RAM console. To enable a U2F security key, perform the following operations: Move the pointer over the profile picture in the upper-right corner of the console and click **Security Information Management**. On the **U2F Security Key** tab of the **Console Logon** page, click **Enable U2F Security Key** and go to .

Procedure

1. Log on to the RAM console by using your Alibaba Cloud account or a RAM user that has administrative rights.

2. In the left-side navigation pane, choose **Identities > Users**.
3. In the **User Logon Name/Display Name** column, click the username of the RAM user for which you want to enable a virtual MFA device.
4. On the page that appears, click the **Authentication** tab. Then, click the **U2F Security Key** tab.
5. Click **Enable U2F Security Key**.
6. On the **Bind U2F Security Key** page, bind the RAM user to the U2F security key.

> **Note** Before you perform the following operations, you must understand the limits on U2F security keys. For more information, see Limits.

   i. Plug the U2F security key into the USB port on your computer.
   ii. Tap the button of the U2F security key.
   iii. In the message that prompts you to obtain the U2F security key, click **OK**.
   iv. In the message indicating that the U2F security key is obtained, click **Confirm Bind**.

What's next

After you enable the MFA device and use the RAM user to log on the Alibaba Cloud Management Console again, the console prompts you to perform the following operations:

1. Enter the username and password of the RAM user.
2. Enter the verification code that is generated by the virtual MFA device. Alternatively, pass the U2F authentication.

> **Note**
> - If you want to change the type of MFA device that is bound to a RAM user, you must log on to the RAM console, disable the MFA device, and then bind the RAM user to another MFA device. For more information, see Disable an MFA device for a RAM user.
> - If the virtual MFA device is uninstalled before you disable the MFA device, or your U2F security key is lost, you cannot log on to the Alibaba Cloud Management Console. If this happens, you must use your Alibaba Cloud account or the RAM user that has administrative rights to log on to the RAM console and disable the MFA device. Then, bind the RAM user to an MFA device. For more information, see Disable an MFA device for a RAM user.

Related information

- BindMFADevice
-

3.5. Create an AccessKey pair for a RAM user

This topic describes how to create an AccessKey pair for a Resource Access Management (RAM) user. An AccessKey pair is a long-term credential for a RAM user. A RAM user can use an AccessKey pair to access Alibaba Cloud resources by calling API operations or by using other development tools.

Context

To ensure account security, we recommend that you create AccessKey pairs for RAM users instead of your Alibaba Cloud account.

Procedure

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Users**.
3. On the **Users** page, click the username of a specific RAM user.
4. In the **User AccessKeys** section, click **Create AccessKey Pair**.
5. In the **Create AccessKey Pair** dialog box, view the AccessKey ID and AccessKey secret.

   You can click **Download CSV File** to download the AccessKey pair or click **Copy** to copy the AccessKey pair.
6. Click **Close**.

> **Note**
>
> - The AccessKey secret is displayed only when you create an AccessKey pair, and is unavailable for subsequent queries. We recommend that you save the AccessKey secret for subsequent use.
> - If the AccessKey pair is disclosed or lost, you must create another AccessKey pair. You can create a maximum of two AccessKey pairs.

Related information

- CreateAccessKey

3.6. Log on to the Alibaba Cloud Management Console as a RAM user

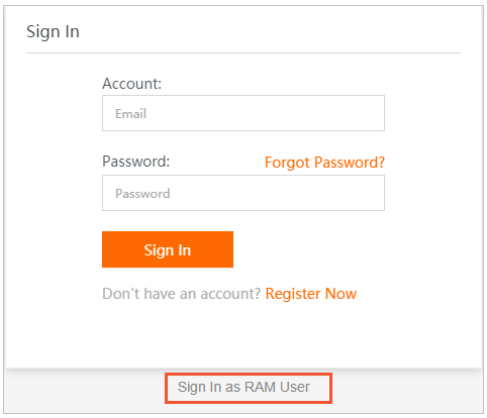
This topic describes how to log on to the Alibaba Cloud Management Console as a Resource Access Management (RAM) user. This topic also describes the logon portals and methods that you can use to log on to the console as a RAM user.

Logon portals

RAM provides the following logon portals for RAM users:

- Common logon portals

- Access the logon page of the International site (alibabacloud.com) and click **Sign In as RAM User**.



- Go to the logon page of the Alibaba Cloud Management Console for a RAM user.

- Logon portal for an Alibaba Cloud account

  Log on to the RAM console by using your Alibaba Cloud account. In the left-side navigation pane, click **Overview**. In the **Account Management** section of the page that appears, view the logon URL of RAM users.Example: `https://signin.alibabacloud.com/example.onaliyun.com/login.htm`. RAM users can use this logon URL to log on to the Alibaba Cloud Management Console.

- Logon portal for a RAM user

  Add the `username` parameter to the logon URL of a RAM user. On the page that appears, click **Next** and enter the password of the RAM user to log on to the Alibaba Cloud Management Console. You do not need to enter the username of the RAM user. The value of the `username` parameter is in the User Principal Name (UPN) format. The username of a RAM user is the logon name that is displayed in the RAM console. For example, you can use `https://signin.alibabacloud.com/login.htm?username=Alice@example.onaliyun.com` to log on to the Alibaba Cloud Management Console as a RAM user named Alice@example.onaliyun.com.

Log on to the Alibaba Cloud Management Console by using the username and password of a RAM user

The following section provides an example on how to log on to the Alibaba Cloud Management Console as a RAM user by using a common logon portal.

1. Log on to the Alibaba Cloud Management Console as a RAM user.
2. On the **RAM User Logon** page, enter the username of the RAM user and click **Next**.
   - Logon name 1: default domain name. The format of the logon name of the RAM user is `<UserName>@<AccountAlias>.onaliyun.com`. Example: username@company-alias.onaliyun.com.

     > **Note** `<UserName>` indicates the username of the RAM user. `<AccountAlias>.onaliyun.com` indicates the default domain name. For more information, see Terms and View and modify the default domain name.

   - Logon name 2: the account alias. The format of the logon name of the RAM user is `<UserName>@<AccountAlias>`. Example: username@company-alias.

> **Note** `<UserName>` indicates the username of the RAM user. `<AccountAlias>` indicates the account alias. For more information, see Terms and View and modify the default domain name.

- Logon name 3: the domain alias. If you configured a domain alias, you can use this logon name. The format of the logon name of the RAM user is `<UserName>@<DomainAlias>`. Example: username@example.com.

  > **Note** `<UserName>` indicates the username of the RAM user. `<DomainAlias>` indicates the domain alias. For more information, see Terms and Create and verify a domain alias.

3. Enter the logon password and click **Log On**.
4. Optional. If you enable multi-factor authentication (MFA), enter the verification code that is provided by the virtual MFA device or configure settings to pass the Universal 2nd Factor (U2F) authentication.

   For more information, see multi-factor authentication (MFA) and Enable an MFA device for a RAM user.

4.Authorization management

4.1. Grant permissions to a RAM user

After a Resource Access Management (RAM) user is granted the relevant permissions, the RAM user can access the required Alibaba Cloud resources. This topic describes how to grant permissions to a RAM user.

Method 1: Grant permissions to a RAM user on the Users page

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Users**.
3. On the **Users** page, find the RAM user to which you want to grant permissions and click **Add Permissions** in the **Actions** column.
4. In the **Add Permissions** panel, grant permissions to the RAM user.
   i. Select the authorization scope.
      - **Alibaba Cloud Account**: The authorization takes effect on the current Alibaba Cloud account.
      - **Specific Resource Group**: The authorization takes effect on a specific resource group.

      > **Note** If you select Specific Resource Group for Authorized Scope, make sure that the required cloud service supports resource groups. For more information, see Alibaba Cloud services that support resource groups.

   ii. Specify the principal.

      The principal is the RAM user to which permissions are to be granted. By default, the current RAM user is specified. You can also specify another RAM user.

   iii. Select policies.

      > **Note** You can attach a maximum of five policies to a RAM user at a time. If you need to attach more than five policies to a RAM user, perform the operation multiple times.

5. Click **OK**.
6. Click **Complete**.

Method 2: Grant permissions to a RAM user on the Grants page

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Permissions > Grants**.
3. On the **Grants** page, click **Grant Permission**.
4. On the **Grant Permission** page, grant permissions to a RAM user.

i. Select the authorization scope.
   - **Alibaba Cloud Account**: The authorization takes effect on the current Alibaba Cloud account.
   - **Specific Resource Group**: The authorization takes effect on a specific resource group.

   > **Note** If you select Specific Resource Group for Authorized Scope, make sure that the required cloud service supports resource groups. For more information, see Alibaba Cloud services that support resource groups.

ii. Specify the principal.

   The principal is the RAM user to which permissions are to be granted.

iii. Select policies.

   > **Note** You can attach a maximum of five policies to a RAM user at a time. If you need to attach more than five policies to a RAM user, perform the operation multiple times.

5. Click **OK**.
6. Click **Complete**.

Related information

- AttachPolicyToUser

4.2. View the permissions of a RAM user

This topic describes how to view the permissions of a Resource Access Management (RAM) user. The permissions include the permissions that are granted to the RAM user and the permissions that the RAM user inherits from RAM user groups.

View the permissions that are granted to a RAM user

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Users**.
3. On the **Users** page, click the username of a specific RAM user.
4. Click the **Permissions** tab.
5. Click the **Individual** tab and view the permissions that are granted to the RAM user.

View the permissions that a RAM user inherits from RAM user groups

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Users**.
3. On the **Users** page, click the username of a specific RAM user.
4. Click the **Permissions** tab.
5. Click the **Group Permissions** tab and view the permissions that the RAM user inherits from RAM user groups.

4.3. Revoke permissions from a RAM user

If a Resource Access Management (RAM) user no longer needs specific permissions or the RAM user leaves your organization, you can revoke the permissions from the RAM user. This topic describes how to revoke permissions from a RAM user.

Method 1: Revoke permissions from a RAM user on the Users page

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Users**.
3. On the **Users** page, click the username of a specific RAM user.
4. On the page that appears, click the **Permissions** tab, find the policy that you want to detach from the RAM user, and then click **Remove Permission** in the **Actions** column.
5. In the message that appears, click **OK**.

Method 2: Revoke permissions from a RAM user on the Grants page

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Permissions > Grants**.
3. On the **Grants** page, find the RAM user from which you want to revoke permissions and click **Revoke Permission** in the **Actions** column.
4. Click **OK**.

Related information

- DetachPolicyFromUser