Alibaba Cloud
Resource Access Management

Security Settings

Issue: 20190919

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.	 Notice: 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]*

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

Contents

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_4 and #unique_5.

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_6.

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_7.

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_8.

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_9 and #unique_10.

2 Passwords

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.

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.

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.

3 Basic security settings

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_17.

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 `Automatica lly 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.

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_20.
4. Click OK.

 Note:

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

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.

4 Advanced settings

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_24.

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

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 >@<$ DomainAlia s >`. For more information, see #unique_24.

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 Access keys

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.

5.2 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.

5.3 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.

5.4 Delete an AccessKey pair

If you no longer need to access Alibaba Cloud resources by calling API operations or using other development tools, you can delete AccessKey pairs.

Prerequisites

Before deleting an AccessKey pair, you can query the time when the pair was last used to check whether the pair is being used. For more information about how to query the time when an AccessKey pair was last used, see #unique_32.

> Note:
> Use caution when you delete an AccessKey pair. If you delete an AccessKey pair that is being used by an app, system errors may occur on the app.

Procedure

1. Log on to the RAM console by using an Alibaba Cloud account.
2. In the left-side navigation pane, click Users under Identities.
3. In the User Logon Name/Display Name column, click the name of the target RAM user.
4. In the User AccessKeys section, click Delete.
5. In the check box that appears, select I am aware of the risk and confirm the deletion.
6. Click OK.

More information
#unique_33

6 Multi-factor authentication

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.

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.

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.

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 Retrieve 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.

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.

7 Best practices

7.1 Use RAM to maintain security of your Alibaba Cloud resources

This topic describes how to use RAM to apply access and security settings to your Alibaba Cloud resources so that you can better manage access permissions with fine-grained access control.

Prerequisites

An Alibaba Cloud account is created. If not, create one before proceeding. To create an Alibaba Cloud account, click Create a new Alibaba Cloud account.

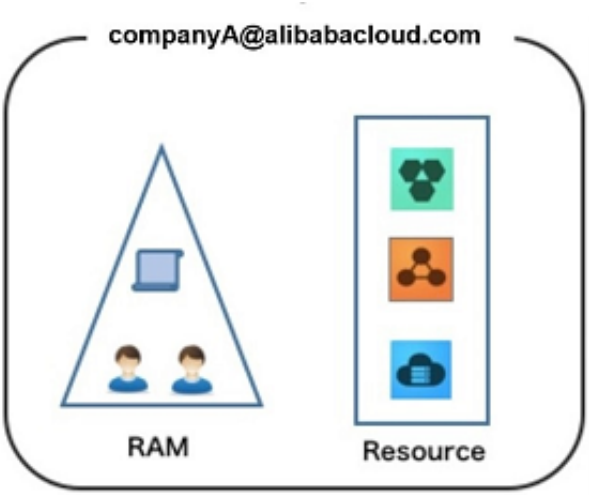
Scenario

When you migrate your business resources to the cloud, the traditional organizati onal structures and previous management methods of your resources may no longer meet your requirements. As a result, the migration of your resources may create higher security management issues as follows:

- The responsibilities of the RAM users are not clear.
- The Alibaba Cloud account owner does not want to share the access key with RAM users due to security risks involved.
- RAM users can access resources by using different methods, which is not unified and may mistakenly cause security risks.
- The resource access permissions of RAM users need to be frequently recalled when the users no longer require these permissions.

Solution

To resolve the preceding issues, you can use RAM to create RAM users and grant resource access permissions to RAM users. Specifically, you can use RAM to separate the access key of your Alibaba Cloud account from RAM users and grant minimum permissions to users as needed to maintain the security of your resources.



Security management solution

- Create independent RAM users.

  An enterprise needs only one Alibaba Cloud account. As a best practice, the Alibaba Cloud account is not used for daily tasks. However, multiple RAM users can be created under the account, and granted the necessary access permissions to resources as needed.

  For more information, see #unique_41.
- Separate console users from API users.

  We recommend that you do not create a logon password for console operations and an access key for API operations for a RAM user at the same time.

  - To allow an application to access cloud resources only through APIs, you only need to create an access key for the application.
  - To allow an employee to operate on cloud resources only through the console, you only need to set a logon password for the employee.

  For more information, see #unique_41.
- Create RAM users and group them.

  If your Alibaba Cloud account has multiple RAM users, you can group RAM users with same responsibilities and grant permissions to the group as needed.

  For more information, see #unique_42.
- Grant the minimum permissions to different RAM user groups.

  You can attach proper system policies to RAM users or user groups as needed. You can also create custom policies for fine-grained permission management. In

this way, by granting the minimum permissions to different RAM users and user groups, you can better manage the RAM users' operations on the cloud resources.

For more information, see #unique_43.

- Configure strong password policies.

  You can configure password policies with custom conventions regarding the minimum length, mandatory characters, and validation period, for RAM users in the RAM console. If a RAM user is allowed to change their logon password, the user must create a strong logon password and rotate the password or access key on a regular basis.

  For more information, see #unique_44.

- Enable an MFA device for your Alibaba Cloud account.

  You can enable a multi-factor authentication (MFA) device for your Alibaba Cloud account to enhance the account security. 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 more information, see #unique_9.

- Enable SSO for RAM users.

  After Single Sign On (SSO) is enabled, all the internal accounts of your enterprise will be authenticated. Then, users can log on to Alibaba Cloud to access corresponding resources only by using an internal account.

  For more information, see #unique_45.

- Do not share the access key of your Alibaba Cloud account.

  Your Alibaba Cloud account has full control permissions over resources under it, and its access keys have the same permissions as logon passwords. However, access keys are used for programmatic access whereas logon passwords are used to log on to the console. Therefore, to avoid information leaks due to misuse of an access key, we recommend that you do not share or use the access key of your Alibaba Cloud account.

  Instead, create a RAM user and grant this user the relevant permissions.

  For more information, see #unique_8.

- Specify operation conditions to enhance security.

  You can specify the operational conditions that a RAM user must meet before they can use your cloud resources. For example, you can specify that the RAM user must use a secure channel (such as SSL), use a specified source IP address, or operate within a specified period of time.

  For more information, see #unique_46.
- Manage permissions of your cloud resources.

  By default, all your resources are under your Alibaba Cloud account. A RAM user can use the resources but do not own the resources. This allows you to easily manage the instances or data created by RAM users.

  - For an existing RAM user that you no long require, you can remove all of its corresponding permissions by simply removing the RAM user account.
  - For a RAM user that requires a permission, you need to first create the RAM user , set the logon password or access key for it, and then grant the RAM user the relevant permissions as needed.

  For more information, see #unique_47.
- Use STS to grant temporary permissions to RAM users.

  The Security Token Service (STS) is an extended authorization service of RAM. You can use STS to grant temporary permissions to RAM users and specify the permission and automatic expiration time of the tokens as needed.

  For more information, see #unique_48

Result

After migrating your services to the cloud, you can use the preceding solutions to ensure you manage your cloud-based resources effectively and keep your Alibaba Cloud account and all business assets secure.

What to do next

You can use RAM to categorize your O&M requirements and assign tasks to different engineers as needed. For more information, see #unique_49.

8 FAQ

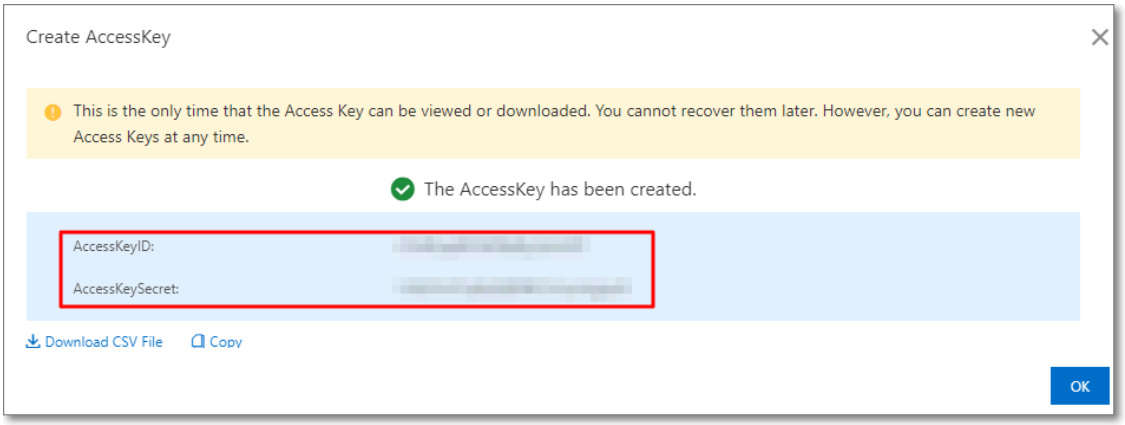
8.1 FAQ about AccessKey pairs

This topic describes FAQ about AccessKey pairs.

What information is displayed when I create an AccessKey pair for the first time?

When you create an AccessKey pair for the first time, the following information is displayed:

- AccessKey ID
- AccessKey secret



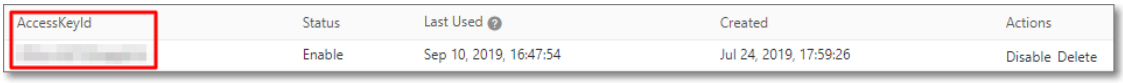
What information can be viewed after I create an AccessKey pair?

After creating an AccessKey pair, you can query the basic information of the AccessKey pair. For more information, see #unique_32.

Note:
You can only view the basic information of the AccessKey pair, such as the AccessKey ID, status, creation time, and the time when the pair was last used.

Can I view the AccessKey ID after I create an AccessKey pair?

After creating an AccessKey, you can query the AccessKey ID.

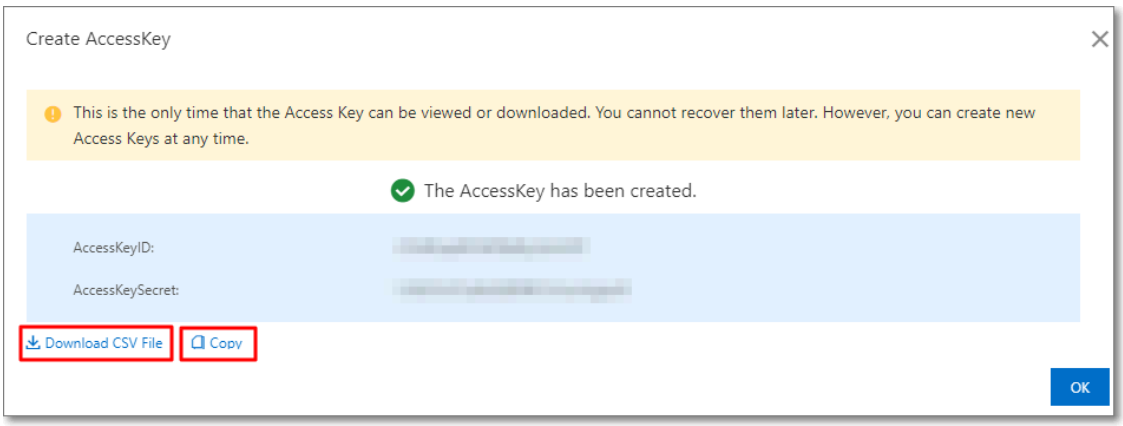


Can I view the AccessKey secret after I create an AccessKey pair?

The AccessKey secret is only displayed when you create an AccessKey pair, and is unavailable for subsequent queries. We recommend that you save the AccessKey secret for subsequent use.

How can I view the AccessKey secret?

When creating an AccessKey pair, you can manually save the AccessKey pair information to an on-premises device by using either of the following two methods:



- Click Download CSV file to download an excel that contains the AccessKey pair information to an on-premises device. The information includes the status, AccessKey ID, and AccessKey secret.
- Click Copy to save the AccessKey ID and AccessKey secret to an on-premises device.

How can I check whether the AccessKey pair is in use?

You can view the time when the AccessKey pair was last used to check whether the pair is in use.

Note:
Use caution when you delete an AccessKey pair. If the AccessKey pair is being used by an app, system errors may occur on the app.