

Alibaba Cloud

Resource Access Management Security Settings

Document Version: 20220429

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 <code>cd /d C:/window</code> command to enter the Windows system folder. |
| <i>Italic</i> | Italic formatting is used for parameters and variables. | <code>bae log list --instanceid</code> <i>Instance_ID</i> |
| [] or [a b] | This format is used for an optional value, where only one item can be selected. | <code>ipconfig [-all -t]</code> |
| { } or {a b} | This format is used for a required value, where only one item can be selected. | <code>switch {active stand}</code> |

Table of Contents

| | |
|---|----|
| 1. Overview of security settings | 05 |
| 2. Passwords | 08 |
| 2.1. Change the password of an Alibaba Cloud account | 08 |
| 2.2. Configure a password policy for RAM users | 08 |
| 2.3. Change the password of a RAM user | 09 |
| 3. Basic security settings | 11 |
| 3.1. Check the security of an Alibaba Cloud account | 11 |
| 3.2. Generate and download user credential reports | 11 |
| 3.3. Manage console logon settings for a RAM user | 16 |
| 3.4. Configure security policies for RAM users | 18 |
| 4. Advanced settings | 20 |
| 4.1. View and modify the default domain name | 20 |
| 4.2. Create and verify a domain alias | 20 |
| 5. AccessKey pairs | 22 |
| 5.1. Create an AccessKey pair for a RAM user | 22 |
| 5.2. View the information about an AccessKey pair | 22 |
| 5.3. Rotate AccessKey pairs | 23 |
| 5.4. Disable an AccessKey pair | 23 |
| 5.5. Delete an AccessKey pair | 24 |
| 6. Multi-factor authentication | 25 |
| 6.1. What is multi-factor authentication | 25 |
| 6.2. Enable an MFA device for an Alibaba Cloud account | 26 |
| 6.3. Disable an MFA device for an Alibaba Cloud account | 27 |
| 6.4. Enable an MFA device for a RAM user | 28 |
| 6.5. Disable an MFA device for a RAM user | 30 |

1. Overview of security settings

This topic introduces some basic concepts of security settings in the Resource Access Management (RAM) console.

password

An identity credential that is used to log on to the Alibaba Cloud Management Console.

 **Note** We recommend that you change your password on a regular basis and keep your password confidential.

For more information, see [Change the password of an Alibaba Cloud account](#) and [Change the password of a RAM user](#).

default domain name

The domain name that is used to identify the Alibaba Cloud account. Alibaba Cloud assigns a **default domain name** to each Alibaba Cloud account. The format of the default domain name is `<AccountAlias>.onaliyun.com`. The default domain name can be used for RAM user logon and single sign-on (SSO) management.

For more information, see [View and modify the default domain name](#).

domain alias

A custom domain name that you can use to replace the default domain name. The custom domain name must be publicly resolvable. A domain alias is the alias of the default domain name.

 **Note** A custom domain can be used as a domain alias only after the ownership of the custom domain is verified. After the ownership is verified, you can use the domain alias to replace the default domain name in all scenarios in which the default domain name is required.

For more information, see [Create and verify a domain alias](#).

AccessKey pair

An identity credential that is used to verify access identities. Each AccessKey pair consists of an AccessKey ID and an AccessKey secret. You can use your AccessKey pair or Alibaba Cloud SDK to sign API requests that you send to Alibaba Cloud. The AccessKey ID and AccessKey secret are used for symmetric encryption and identity verification. After the identity is verified, you can manage Alibaba Cloud resources by calling operations.

The AccessKey ID is used to identify a user, and the AccessKey secret is used to encrypt and verify a signature string.

 **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.

For more information, see [Create an AccessKey pair for a RAM user](#).

multi-factor authentication (MFA)

MFA is an easy-to-use and effective authentication method. In addition to the username and password, MFA provides an extra layer of protection. MFA enhances the security of your account.

Supported types

MFA devices are classified into various types. Alibaba Cloud supports the following two types of MFA devices:

- **Virtual MFA devices**

Time-based one-time cipher algorithm (TOTP) is a multi-factor authentication protocol that is widely used. Applications that support TOTP on devices such as mobile phones are called virtual MFA devices. For example, both the Alibaba Cloud app and the Google Authenticator app are virtual MFA devices. If you enable a virtual MFA device, you must enter the 6-digit verification code that is generated on the device when you log on to the Alibaba Cloud Management Console. This prevents unauthorized logon due to password theft.

- **U2F security keys**

Universal 2nd Factor (U2F) is a multi-factor authentication protocol that is widely used and hosted by the Fast Identity Online (FIDO) Alliance. For more information, visit [Fast Identity Online \(FIDO\) Alliance](#). The protocol is used to provide an efficient and universal multi-factor authentication method. A hardware device that supports Web Authentication is a U2F security key, such as YubiKey produced by Yubico. You can plug a U2F security key into a USB port on your computer. Then, you can complete multi-factor authentication by tapping the button on the device when you log on to the Alibaba Cloud Management Console. For more information, see [Web Authentication](#).

Usage notes

If you have enabled an MFA device, you must perform the following steps when you log on to the Alibaba Cloud Management Console:

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

For more information, see [Enable an MFA device for an Alibaba Cloud account](#) and [Enable an MFA device for a RAM user](#).

Limits

- Virtual MFA devices can be used when you log on to the Alibaba Cloud Management Console from a browser or the Alibaba Cloud app.
- U2F security keys have the following limits:
 - U2F security keys can be used only on computers with USB ports. If you log on to the Alibaba Cloud Management Console from a browser on a mobile device or from the Alibaba Cloud app, you cannot use U2F security keys. If you use a virtual machine or Remote Desktop Services, U2F authentication is not supported.
 - You can use U2F security keys only when you log on to the Alibaba Cloud Management Console by using the `signin.alibabacloud.com` domain name. If you use the `signin-intl.aliyun.com` domain name that was previously supported by Alibaba Cloud, U2F authentication is not supported.

- You can use U2F security keys in the following versions of browsers that support [Web Authentication \(WebAuthn\)](#):
 - Google Chrome 67 and later
 - Opera 54 and later
 - Mozilla Firefox 60 and later

 **Note** If you use Mozilla Firefox, you must manually enable the U2F feature by performing the following operations: Enter `about:config` in the address bar of your browser to go to the browser configuration page. On this page, search for `u2f` and set the `security.webauth.u2f` parameter to `true`. For more information, see the [Mozilla Firefox help documentation](#).

MFA for sensitive operations

MFA is required for sensitive operations. If a RAM user for which MFA is enabled wants to perform a sensitive operation in the Alibaba Cloud Management Console, risk control is triggered and the RAM user is required to pass MFA again. The RAM user can perform the sensitive operation only after the RAM user enters a valid MFA verification code.

Before you can implement MFA for sensitive operations for all RAM users, you must enable MFA for all RAM users. For more information, see [Configure security policies for RAM users](#).

2. Passwords

2.1. Change the password of an Alibaba Cloud account

This topic describes how to change the password of an Alibaba Cloud account. We recommend that you 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. Move the pointer over the profile picture in the upper-right corner of the RAM console, and click **Security Settings**.
3. In the **Login password** section of the **Security Settings** page, click **Modify**.
4. In the **Verify identity** step, select a verification method and click **Verify now**.
5. After your identity is verified, enter a **new password** and **confirm the password**.
6. Click **OK**.

2.2. 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

- [Set Password Policy](#)

2.3. 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. Basic security settings

3.1. Check the security of an Alibaba Cloud account

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](#) by using an Alibaba Cloud account.
2. On the **Overview** page, check the security items.
3. Click a security item, and click **Set Now**. On the page that appears, complete the security settings.

What's next

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

- **SubUser**: the number of RAM users.
- **SubUserBindMfa**: the number of RAM users for whom multi-factor authentication (MFA) is enabled.
- **SubUserWithUnusedAccessKey**: the number of RAM users that have unused AccessKey pairs.
- **RootWithAccessKey**: the number of created AccessKey pairs.
- **SubUserWithOldAccessKey**: the number of RAM users with AccessKey pairs that have existed for a long period of time.
- **SubUserPwdLevel**: the password strength of RAM users.
- **UnusedAkNum**: the number of unused AccessKey pairs.
- **OldAkNum**: the number of existing AccessKey pairs.
- **BindMfa**: indicates whether MFA is enabled for the Alibaba Cloud account.
- **Score**: the security score of the Alibaba Cloud account.

Note

- A low security score means that your Alibaba Cloud account is less vulnerable. In this case, we recommend that you complete relevant security settings to improve your account security.
- We recommend that you follow the best practices about how to use RAM. For more information, see [Use RAM to ensure security of the Alibaba Cloud resources of your enterprise](#).

3.2. Generate and download user credential reports

A user credential report contains the details of your Alibaba Cloud account and Resource Access Management (RAM) users. The details include logon passwords, AccessKey pairs, and multi-factor authentication (MFA) devices. User credential reports can be generated and downloaded in the RAM console. You can use the user credential reports for compliance checks and auditing.

Procedure

1. Log on to the [RAM console](#) by using your Alibaba Cloud account. You can also log on as a RAM user that is attached with the AliyunRAMFullAccess policy.
2. In the left-side navigation pane, click **Overview**.
3. In the **Security Check** section of the page that appears, click **Download User Credential Report**.
4. After the user credential report is generated, click **Download**.

 **Note** The time period required to generate the user credential report is affected by the number of RAM users within the current Alibaba Cloud account. If a long period of time is required to generate the report, you can click **Download Later**. A new user credential report in the CSV format can only be generated every four hours. When you send a request to download a report, RAM first checks whether a report has been generated within the last four hours. If the latest report is generated within the last four hours, the latest report is downloaded. If the latest report is generated four hours or more earlier, or if no previous report has been generated, RAM generates a new report.

Result

The following table describes the fields that are included in the user credential report.

| Field | Example | Description |
|--------------------|-------------------------------------|---|
| user | username@company-alias.onaliyun.com | The usernames of the Alibaba Cloud account and the RAM users. The value in the first row of the CSV file is <root>, which indicates the Alibaba Cloud account. The values in the remaining rows are the usernames of the RAM users within your Alibaba Cloud account, and the values are in the User Principal Name (UPN) format. |
| user_creation_time | 2019-11-11T12:33:18Z | The time at which the RAM users were created.  Note The time follows the ISO 8601 standard in the YYYY-MM-DDThh:mm:ssZ format. The time is displayed in UTC. |

| Field | Example | Description |
|-----------------|----------------------|---|
| user_last_logon | 2019-11-11T12:45:18Z | <p>The time at which the RAM users last logged on to the RAM console.</p> <p>Note The RAM users may log on to the RAM console by using passwords or single sign-on (SSO). If a RAM user has never logged on to the RAM console, the value of this field is a hyphen (-).</p> |
| password_exist | TRUE | <p>Indicates whether a password for logging on to the RAM console is available. Valid values: <code>TRUE</code> and <code>FALSE</code>.</p> <ul style="list-style-type: none"> The value for a RAM user is determined by the logon configurations of the RAM user. The value for an Alibaba Cloud account is <code>TRUE</code> and cannot be changed. <p>Note If you use a resource account that is created on the Resource Directory page of the Resource Management console, you can view the password. However, the password cannot be used to log on to the RAM console.</p> |
| password_active | N/A | <p>Indicates whether a password is active. Valid values: <code>TRUE</code>, <code>FALSE</code>, and <code>N/A</code>.</p> <ul style="list-style-type: none"> If the logon configurations for a RAM user are unavailable, the value for the RAM user is <code>N/A</code>. The value for an Alibaba Cloud account is <code>N/A</code>. |

| Field | Example | Description |
|------------------------|----------------------|--|
| password_last_changed | 2019-11-11T12:50:18Z | <p>The time at which a password is last changed. If the logon configurations for a RAM user are unavailable, the value for the RAM user is N/A .</p> <div style="border: 1px solid #add8e6; padding: 5px; background-color: #e0f0ff;"> <p> Note RAM records the changes that were made after April 5, 2016. If a password was changed on this date or earlier, the value for this field is N/A . The user credential report may not include the changes that were made in an interval leading up to the report generation time. The interval is about 24 hours, but the actual time may vary based on the scenario.</p> </div> |
| password_next_rotation | 2019-11-13T12:50:18Z | <p>The time at which a new password must be configured in compliance with the password rotation policy.</p> <ul style="list-style-type: none"> • If the password is permanently valid and password rotation is not required, the value is a hyphen (-). • If the logon configurations for a RAM user are unavailable, the value for the RAM user is N/A . • The value for an Alibaba Cloud account is N/A . |
| mfa_active | TRUE | <p>Indicates whether an MFA device is enabled. Valid values: TRUE , FALSE , and N/A . If the logon configurations for a RAM user are unavailable, the value for the RAM user is N/A .</p> |
| access_key_1_exist | TRUE | <p>Indicates whether the first AccessKey pair exists. Valid values: TRUE and FALSE .</p> |

| Field | Example | Description |
|---------------------------|----------------------|---|
| access_key_1_active | TRUE | Indicates whether the first AccessKey pair is active. Valid values: <code>TRUE</code> , <code>FALSE</code> , and <code>N/A</code> . If no AccessKey pairs are created, the value is <code>N/A</code> . |
| access_key_1_last_rotated | 2019-11-11T12:50:18Z | The time at which the first AccessKey pair is created or last changed. If no AccessKey pairs are created, the value is <code>N/A</code> . |
| access_key_1_last_used | 2019-11-13T12:50:18Z | <p>The time at which the first AccessKey pair is last used.</p> <ul style="list-style-type: none"> If the AccessKey pair is not used since RAM started to track the AccessKey pair from the last usage, the value is a hyphen (<code>-</code>). If no AccessKey pairs are created, the value is <code>N/A</code>. <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p>Note RAM started to track the last usage time of AccessKey pairs from June 1, 2019. The user credential report may not include the usage records of the AccessKey pairs in an interval leading up to the report generation time. The interval is about two hours, but the actual time may vary based on the scenario.</p> </div> |
| access_key_2_exist | TRUE | Indicates whether the second AccessKey pair exists. Valid values: <code>TRUE</code> and <code>FALSE</code> . |
| access_key_2_active | TRUE | Indicates whether the second AccessKey pair is active. Valid values: <code>TRUE</code> , <code>FALSE</code> , and <code>N/A</code> . If no AccessKey pairs are created, the value is <code>N/A</code> . |
| access_key_2_last_rotated | 2019-11-11T12:50:18Z | The time at which the second AccessKey pair is created or last changed. If no AccessKey pairs are created, the value is <code>N/A</code> . |

| Field | Example | Description |
|------------------------|----------------------|--|
| access_key_2_last_used | 2019-11-13T12:50:18Z | <p>The time at which the second AccessKey pair was last used.</p> <ul style="list-style-type: none"> If the AccessKey pair is not used since RAM started to track the AccessKey pair from the last usage, the value is a hyphen (-). If no AccessKey pairs are created, the value is N/A . <p>Note RAM started to track the last usage time of AccessKey pairs from June 1, 2019. The user credential report may not include the usage records of the AccessKey pairs in an interval leading up to the report generation time. The interval is about two hours, but the actual time may vary based on the scenario.</p> |

Note A maximum of two AccessKey pairs can be created for each Alibaba Cloud account or RAM user in the RAM console. Before this limit takes effect, more than two AccessKey pairs can be created. Therefore, an Alibaba Cloud account or a RAM user may have more than two AccessKey pairs. The information about the additional AccessKey pairs is listed in the last columns of the CSV file. The names of these columns start with `additional_access_key_`.

3.3. 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 a 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 a 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**.

3.4. Configure security policies for RAM users

This topic describes how to use your Alibaba Cloud account to configure security policies for Resource Access Management (RAM) users.

Procedure

1. Log on to the **RAM console** by using an Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Settings**.
3. On the **Security Settings** tab, click **Modify RAM User Security Settings**.

4. In the **Modify RAM User Security Settings** panel, configure the parameters.
 - **Remember MFA for Seven Days:** specifies whether to allow RAM users to remember the multi-factor authentication (MFA) devices for seven days.
 - **Manage Passwords:** specifies whether to allow RAM users to change their passwords.
 - **Manage AccessKey Pairs:** specifies whether to allow RAM users to manage their AccessKey pairs.
 - **Manage MFA Devices:** specifies whether to allow RAM users to enable and disable MFA devices.
 - **MFA for RAM User Logons:** specifies whether MFA is required for all RAM users when the RAM users use usernames and passwords to log on to the Alibaba Cloud Management Console. If you set this parameter to Apply User-specific Configuration, user-specific settings are applied.

 **Note** If you select Enable for All Users for the MFA for RAM User Logons parameter, MFA for sensitive operations is enabled for all RAM users. If a RAM user wants to perform a sensitive operation in the Alibaba Cloud Management Console, risk control is triggered and the RAM user is required to pass MFA again. For more information, see [MFA for sensitive operations](#).

- **Manage DingTalk:** specifies whether RAM users can bind or unbind their DingTalk accounts.
- **Logon Session Validity Period:** specifies the validity period of a logon session. The validity period is measured in hours. Valid values: 1 to 24. Default value: 6.

 **Note** If you assume a RAM role or use single sign-on (SSO) to log on to the Alibaba Cloud Management Console, the validity period of your session is no greater than the value of the **Logon Session Validity Period** parameter. For more information, see [Assume a RAM role](#) and [SAML response for role-based SSO](#).

- **Logon Address Mask:** specifies the IP addresses from which you can log on to the Alibaba Cloud Management Console by using a password or SSO. By default, this parameter is left empty, which indicates that logon from all IP addresses is allowed. If you enter IP addresses in this field, console logons, including password-based and SSO-based logon, from these IP addresses are limited. However, API calls that are initiated from these IP addresses by using AccessKey pairs are not limited. You can enter up to 25 IP addresses. If you enter more than one IP address, separate the IP addresses with semicolons (;). The total length of the IP addresses can be a maximum of 512 characters.

5. Click **OK**.

 **Note** The settings take effect on all the RAM users of your Alibaba Cloud account.

Related information

- [SetSecurityPreference](#)

4. Advanced settings

4.1. View and modify the default domain name

Each Alibaba Cloud account has a default domain name. Resource Access Management (RAM) users can use this default domain name as the suffix of their logon name to log on to the Alibaba Cloud Management Console. This topic describes how to view and modify 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, choose **Identities > Settings**.
3. On the page that appears, click the **Advanced** tab to view and modify the default domain name in the **Default Domain** section.
 - View the information about the default domain name. The information includes the domain name, status, and the time when the default domain name was created. The default domain name is in the `<AccountAlias>.onaliyun.com` format. `<AccountAlias>` indicates the account alias. The default value of AccountAlias is the ID of your Alibaba Cloud account. In this case, the default domain name is `<AccountID>.onaliyun.com`.
 - Modify the default domain name. To modify the default domain name, click **Edit**. In the Edit default domain panel, specify an account alias and click **OK**.

What's next

The RAM users of your Alibaba Cloud account can use the default domain name to log on to the [RAM console](#). To log on to the RAM console, specify the logon name in the format of `<UserName>@<AccountAlias>.onaliyun.com`. For more information, see [Log on to the Alibaba Cloud Management Console as a RAM user](#).

You can use the default domain name to simplify the procedure of configuring SAML-based single sign-on (SSO). For more information, see [Configure the SAML settings of Alibaba Cloud for user-based SSO](#).

4.2. Create and verify a domain alias

This topic describes how to create and verify a domain alias for an Alibaba Cloud account. A domain alias is an alias of your default domain name. After you create and verify a domain alias, Resource Access Management (RAM) users of the Alibaba Cloud account can use this domain alias to log on to the RAM console.

Prerequisites

You own a domain name that is publicly resolvable.

Procedure

1. Create a domain alias in the RAM console.
 - i. Log on to the [RAM console](#) by using your Alibaba Cloud account.
 - ii. In the left-side navigation pane, choose **Identities > Settings**.

- iii. On the Settings page, click the **Advanced** tab.
 - iv. In the **Domain Alias** section, click **Create Domain Alias**.
 - v. In the **Create Domain Alias** panel, specify **Domain Name** and click **OK**.
 - vi. Copy the verification code.
2. Add a TXT record in the system of your DNS service provider.

If you use Alibaba Cloud DNS, configure the TXT record in the Alibaba Cloud DNS console. You must enter the verification code that you copied in Step in the **Value** field. For more information, see [Add DNS records](#).

A screenshot of the Alibaba Cloud DNS console showing a form for adding a TXT record. The form includes the following fields:

- Type:** A dropdown menu set to "TXT- Text".
- Host:** A text input field with the placeholder "Enter ...".
- ISP Line:** A dropdown menu set to "Default - Return to the default value when the query is not m...".
- * Value:** A text input field containing the verification code "aliyun-site-verification=409b99b2-014b-419a-affe-b5544273-...". This field is highlighted with a red rectangular border.
- * TTL:** A dropdown menu set to "10 minute(s)".

3. Log on to the RAM console to verify the ownership of the domain name.
 - i. In the left-side navigation pane, choose **Identities > Settings**.
 - ii. In the **Domain Alias** section of the **Advanced** tab, click **Domain Ownership Verification**.
 - iii. In the **Verify Domain Ownership** message, view the verification result and click **OK**.

What's next

The RAM users of your Alibaba Cloud account can use the default domain name to log on to the [RAM console](#). The logon name of a RAM user follows the format of `<UserName>@<DomainAlias>`. For more information, see [Log on to the Alibaba Cloud Management Console as a RAM user](#).

You can use the domain alias to simplify the procedure of configuring SAML-based single sign-on (SSO). For more information, see [Configure the SAML settings of Alibaba Cloud for user-based SSO](#).

5. AccessKey pairs

5.1. 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](#)

5.2. View the information about an AccessKey pair

This topic describes how to view the information about an AccessKey pair. The information includes the AccessKey ID, status, time when the AccessKey pair was last used, and time when the AccessKey pair was created.

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 of the page that appears, view the information about AccessKey pairs.

 **Note** The AccessKey secret is displayed only when you create an AccessKey pair. The AccessKey secret is unavailable for subsequent queries.

5.3. Rotate AccessKey pairs

You can create a maximum of two AccessKey pairs for each RAM user. If you have used an AccessKey pair for more than three months, we recommend that you rotate the AccessKey pair in a timely manner. This reduces the probability of AccessKey pair leak.

Procedure

1. Create an AccessKey pair for rotation. For more information, see [Create an AccessKey pair for a RAM user](#).
2. Update all applications and systems to use the new AccessKey pair.

 **Note** If you want to check whether the new or original AccessKey pair is in use, perform the following steps: Log on to the [RAM console](#) and go to the details page of the required user. In the **User AccessKeys** section, find the new and original AccessKey pairs. View the values in the **Last Used** column.

3. Disable the original AccessKey pair. For more information, see [Disable an AccessKey pair](#).
4. Confirm that your applications and systems are properly running.
 - If the applications and systems are properly running, the update succeeds. You can delete the original AccessKey pair.
 - If an application or system stops running, you must enable the original AccessKey pair, and repeat Step 2 to Step 4 until the update succeeds.
5. Delete the original AccessKey pair. For more information, see [Delete an AccessKey pair](#).

What's next

We recommend that you regularly rotate AccessKey pairs.

5.4. Disable an AccessKey pair

This topic describes how to disable an AccessKey pair of a Resource Access Management (RAM) user. If the permissions required by a RAM user change or if the RAM user no longer needs to access Alibaba Cloud resources by calling API operations, you can disable an AccessKey pair of the 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 **User AccessKeys** section of the page that appears, find the specific AccessKey pair and click **Disable** in the **Actions** column.

 **Note** To re-enable the AccessKey pair, click **Enable** in the **Actions** column.

5. Click **OK**.

Related information

- [UpdateAccessKey](#)

5.5. Delete an AccessKey pair

This topic describes how to delete an AccessKey pair for a Resource Access Management (RAM) user. If a RAM user no longer needs to access Alibaba Cloud resources by calling API operations or using other development tools, you can delete an AccessKey pair of the RAM user.

Prerequisites

Before you delete an AccessKey pair, you can query the time when the AccessKey pair was last used to determine whether the AccessKey pair is in use. For information about how to query the time when an AccessKey pair was last used, see [View the information about an AccessKey pair](#).

 **Notice** If you delete an AccessKey pair that is being used, system errors may occur. Proceed with caution.

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 of the page that appears, find the specific AccessKey pair and click **Delete** in the **Actions** column.
5. Click **OK**.

Related information

- [DeleteAccessKey](#)

6. Multi-factor authentication

6.1. What is multi-factor authentication

Multi-factor authentication (MFA) is an easy-to-use and effective authentication method. In addition to username password authentication, MFA provides an extra layer of protection. MFA enhances security for your account.

Types of MFA devices

MFA devices are classified into various types. Alibaba Cloud supports the following two types of MFA devices:

- **Virtual MFA devices**

Time-based one-time cipher algorithm (TOTP) is a multi-factor authentication protocol that is widely used. Applications that support TOTP on devices such as mobile phones are called virtual MFA devices. For example, both the Alibaba Cloud app and the Google Authenticator app are virtual MFA devices. If you enable a virtual MFA device, you must enter the 6-digit verification code that is generated on the device when you log on to the Alibaba Cloud Management Console. This prevents unauthorized logon due to password theft.

- **U2F security keys**

Universal 2nd Factor (U2F) is a multi-factor authentication protocol that is widely used and hosted by the Fast Identity Online (FIDO) Alliance. For more information, visit [Fast Identity Online \(FIDO\) Alliance](#). The protocol is used to provide an efficient and universal multi-factor authentication method. A hardware device that supports Web Authentication is a U2F security key, such as YubiKey produced by Yubico. You can plug a U2F security key into a USB port on your computer. Then, you can complete multi-factor authentication by tapping the button on the device when you log on to the Alibaba Cloud Management Console. For more information, see [Web Authentication](#).

Usage notes

If you have enabled an MFA device, you must perform the following steps when you log on to the Alibaba Cloud Management Console:

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

For more information, see [Enable an MFA device for an Alibaba Cloud account](#) and [Enable an MFA device for a RAM user](#).

Limits

- Virtual MFA devices can be used when you log on to the Alibaba Cloud Management Console from a browser or the Alibaba Cloud app.
- U2F security keys have the following limits:
 - U2F security keys can be used only on computers with USB ports. If you log on to the Alibaba Cloud Management Console from a browser on a mobile device or from the Alibaba Cloud app, you cannot use U2F security keys. If you use a virtual machine or Remote Desktop Services, U2F authentication is not supported.

- You can use U2F security keys only when you log on to the Alibaba Cloud Management Console by using the `signin.alibabacloud.com` domain name. If you use the `signin-intl.aliyun.com` domain name that was previously supported by Alibaba Cloud, U2F authentication is not supported.
- You can use U2F security keys in the following versions of browsers that support [Web Authentication \(WebAuthn\)](#):
 - Google Chrome 67 and later
 - Opera 54 and later
 - Mozilla Firefox 60 and later

 **Note** If you use Mozilla Firefox, you must manually enable the U2F feature by performing the following operations: Enter `about:config` in the address bar of your browser to go to the browser configuration page. On this page, search for `u2f` and set the `security.webauth.u2f` parameter to `true`. For more information, see the [Mozilla Firefox help documentation](#).

6.2. Enable an MFA device for an Alibaba Cloud account

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

Prerequisites

The Google Authenticator app is downloaded and installed 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.

Procedure

1. Log on to the [Alibaba Cloud Management Console](#) by using your Alibaba Cloud account.
2. Move the pointer over the profile picture in the upper-right corner of the console, and click **Security Settings**.
3. In the **Account Protection** section of the **Security Settings** page, click **Edit**.

 **Note** MFA is renamed Time-based One-time Password (TOTP).

4. On the **Turn on Account Protection** page, select scenarios and the **TOTP** verification method. Then, click **Submit**.
5. On the **Identity Verification** page, select a verification method.
6. In the **Install the application** step, click **Next**.

7. 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 and scan the QR code that is displayed in the **Enable the MFA** step of the Alibaba Cloud Management Console. This method is recommended.
 - Tap **Enter a setup key**, enter an account and the key of the account, and then tap **Add**.

 **Note** In the **Enable the MFA** step of the Alibaba Cloud Management Console, move the pointer over **Scan failed** to view the account and key.

8. In the **Enable the MFA** step of the Alibaba Cloud Management Console, enter the dynamic verification code that is displayed in the Google Authenticator app. Then, click **Next** to complete the account protection settings.

 **Note** Verification codes in the Google Authenticator app are updated at an interval of 30 seconds.

What's next

If you use the Alibaba Cloud account to log on to the Alibaba Cloud Management Console after you enable the virtual MFA device, you are prompted to enter the following verification information:

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

Note

- The virtual MFA device that is enabled for an Alibaba Cloud account does not affect the logon of the RAM users that belong to the Alibaba Cloud account.
- Before you uninstall your application that is used for MFA or unbind a virtual MFA device, you must log on to the Alibaba Cloud Management Console and disable the virtual MFA device. Otherwise, a logon failure may occur.

Related information

- [BindMFADevice](#)

6.3. Disable an MFA device for an Alibaba Cloud account

If you no longer need a multi-factor authentication (MFA) device that is enabled for an Alibaba Cloud account or you want to change the MFA device, you can disable the MFA device for the Alibaba Cloud account. This topic uses the Google Authenticator app as an example to describe how to disable an MFA device for an Alibaba Cloud account.

Procedure

1. Log on to the [Alibaba Cloud Management Console](#) by using your Alibaba Cloud account.
2. Move the pointer over the profile picture in the upper-right corner of the console, and click **Security Settings**.
3. In the **Account Protection** section of the **Security Settings** page, click **Edit**.

 **Note** MFA is renamed TOTP.

4. Click **Turn off** in the **Account Protect settings** section.
5. On the Identity Verification page in the Alibaba Cloud Management Console, enter the dynamic verification code that is displayed in the Google Authentication app, and click **Submit**.

6.4. 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](#)
-

6.5. Disable an MFA device for a RAM user

If you no longer require a multi-factor authentication (MFA) device enabled for a Resource Access Management (RAM) user, or you want to change the type of the MFA device that is bound to a RAM user, you can disable the MFA device for the RAM user by using your Alibaba Cloud account or a RAM user that has administrative rights.

Procedure

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

 **Note** If a RAM user of your Alibaba Cloud account is allowed to manage its own MFA device, the RAM user can disable the MFA device in the RAM console. To disable an 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 Security Management page, click **Disable Virtual MFA Device**. You can also click **Disable U2F Security Key** on the **U2F Security Key** tab.

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 disable an MFA device.
4. On the page that appears, click the **Authentication** tab.
 - On the tab, click the **Virtual MFA Device** tab and click **Disable Virtual MFA Device**. The virtual MFA device is disabled.
 - On the tab, click the **U2F Security Key** tab and click **Disable U2F Security Key**. The U2F security key is disabled.
5. Click **OK**.

Related information

- [UnbindMFADevice](#)