ALIBABA CLOUD

Alibaba Cloud

Resource Access Management

Security Settings

Document Version: 20200910

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	Danger: Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Overview of security settings

This topic describes some basic concepts of security settings in the RAM console.

Password

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

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

For more information about how to set a password, see Change the password for an Alibaba Cloud account and Change the password for a RAM user.

Default domain name

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

For information about how to set a default domain name, see Manage the default domain name.

Domain alias

A custom domain name that can be used 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 domain alias can be used only after domain ownership verification. After verification, you can use the domain alias to replace the default domain name in all scenarios where the default domain name is required.

For information about how to set a domain alias, see Create and verify a domain alias.

AccessKey pair

An identity credential that consists of an AccessKey ID and 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 API 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 information about how to create an AccessKey pair, see Create an AccessKey pair for a RAM user.

Multi-factor authentication (MFA)

A simple best practice that adds an extra layer of protection on top of your username and password. Multi-factor authentication provides enhanced security for your account. If you log on to the Alibaba Cloud console with MFA enabled, you must enter the following information:

1. Username and password
2. Verification code provided by the MFA device

For information about how to set MFA, see Enable an MFA device for an Alibaba Cloud account and Enable an MFA device for a RAM user.

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 on a regular basis for added security. The password must be at least 6 characters in length, and must contain at least two of the following elements: letters, special characters, and digits.

Procedure

1. Log on to the RAM console with an 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 **Login Password** section of the **Security Settings** page, click **Change**.
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. Set a password policy for RAM users

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

Procedure

1. Log on to the RAM console by using an Alibaba Cloud account.
2. In the left-side navigation pane, click **Settings** under **Identities**.
3. On the **Security Settings** tab, click **Edit Password Rule**. In the Edit Password Rule pane, set the parameters.
   - **Password Length**: The password must be 8 to 32 characters in length.

     > **Note** To ensure account security, the password must be at least 8 characters in length.

   - **Required Elements in Password**: The available elements include lowercase letters, uppercase letters, digits, and special characters.

     > **Note** The password must contain the selected element or elements. To enhance account security, we recommend that you select at least two of the preceding elements.

   - **Minimum Different Characters in Password**: The value range is from 0 to 8. The default value is 0, which indicates that no limit is imposed on the number of unique characters in a

password.

- **Include Username in Password**: Select Allow or Do Not Allow.
  - Allow: A password can contain the username.
  - Do Not Allow: A password cannot contain the username.
- **Password Validity Period**: The value range is from 0 to 1095, in days. The default value is 0, which indicates that the password never expires.

  > **Note** The password validity period restarts if you reset the password.

- **Action After Password Expires**: You can specify whether to allow the RAM users to log on to the RAM console after their passwords expire. You can select one of the following options based on your business needs.
  - Deny Logon: If you select this option, the RAM users can log on to the console only after you reset the passwords by using your Alibaba Cloud account.
  - Allow Logon: If you select this option, the RAM users can change their passwords after the passwords expire. The RAM users can then use the new passwords to log on to the console.
- **Password History Check Policy**: You can prevent RAM users from reusing the previous *N* passwords. The value range is 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 (N) of allowed logon attempts. If you enter wrong passwords for N consecutive times, you are not allowed to log on to the account in the next hour. The value range is from 0 to 32. The default value is 0, which indicates 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**.

Result

The password settings apply to all the RAM users of your Alibaba Cloud account.

Related information

- SetPasswordPolicy

2.3. Change the password for a RAM user

This topic describes how to change the password for a RAM user of your Alibaba Cloud account.

Procedure

1. Log on to the RAM console with 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 username of the target RAM user.
4. On the **Authentication** tab, click **Modify Logon Settings**.

5. In the **Set Logon Password** section, select **Automatically Regenerate Default Password** or **Reset Custom Password**.

   > **Note** If you select the **Automatically Regenerate Default Password** option, save the generated new password for subsequent use.

6. If you select the **Reset Custom Password** option, 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 also change their passwords in the RAM 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 maintain security of your Alibaba Cloud resources.

3.2. Generate and download user credential reports

This topic describes how to generate and download a user credential report that contains the credential details of your Alibaba Cloud account and RAM users in the RAM console. The credential details include the passwords, AccessKey pairs, and multi-factor authentication (MFA) devices. You can use credential reports for compliance checks and auditing.

Procedure

1. Log on to the RAM console by using an 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 required for generating the user credential report is affected by the number of RAM users under the current Alibaba Cloud account. If the generation of a report requires a long period of time, you can click **Download Later**. A new credential report in the comma-separated values (CSV) format can be generated only once every four hours. After you send a request to download a report, RAM checks whether a report has been generated within the past four hours. If the latest report is generated within the past four hours, the latest report is downloaded. If the latest report is generated four hours 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 username of the Alibaba Cloud user. 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 under the Alibaba Cloud account, and the values are in the User Principal Name (UPN) format.
user_creation_time	2019-11-11T12:33:18Z	The time when the Alibaba Cloud user was created. **Note** Specify the time in the ISO 8601 standard in the YYYY-MM-DDThh:mm:ssZ format. The time must be in UTC.

Field	Example	Description
user_last_logon	2019-11-11T12:45:18Z	The last time when the RAM user logged on to the RAM console. Note The RAM user may log on to the RAM console by using the password or single sign-on (SSO). If the RAM user has never logged on to the RAM console, the value of this field is `-`.
password_exist	TRUE	Indicates whether a password for logging on to the RAM console is available. Valid values are `TRUE` and `FALSE`. • The value for a RAM user is determined by the logon configurations of the RAM user. • The value for an Alibaba Cloud account is `TRUE`, and cannot be changed. Note If you are using 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.

Field	Example	Description
password_active	N/A	Indicates whether the password is active. Valid values are `TRUE`, `FALSE`, and `N/A`. • If the logon configurations for a RAM user are not available, the value for the RAM user is `N/A`. • The value for an Alibaba Cloud account is `N/A` and cannot be changed.
password_last_changed	2019-11-11T12:50:18Z	The time when the password was last changed. If the logon configurations for a RAM user are not available, the value for the RAM user is `N/A`. **Note** RAM records the changes that were made after April 5, 2016. If the 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.

Field	Example	Description
password_next_rotation	2019-11-13T12:50:18Z	The time when a new password must be set in compliance with the password rotation policy. • If the password is permanently valid and password rotation is not required, the value is `-`. • If the logon configurations for a RAM user are not available, the value for the RAM user is `N/A`. • The value for an Alibaba Cloud account is `N/A` and cannot be changed.
mfa_active	TRUE	Indicates whether to enable an MFA device. Valid values are `TRUE`, `FALSE`, and `N/A`. If the logon configurations for a RAM user are not available, the value for the RAM user is `N/A`.
access_key_1_exist	TRUE	Indicates whether the first AccessKey pair exists. Valid values are `TRUE` and `FALSE`.
access_key_1_active	TRUE	Indicates whether the first AccessKey pair is active. Valid values are `TRUE`, `FALSE`, and `N/A`. If no AccessKey pair has been created, the value is `N/A`.
access_key_1_last_rotated	2019-11-11T12:50:18Z	The time when the first AccessKey pair was created or last changed. If no AccessKey pair has been created, the value is `N/A`.

Field	Example	Description
access_key_1_last_used	2019-11-13T12:50:18Z	The time when the first AccessKey pair was last used. • If the AccessKey pair has not been used since RAM started to track this information, the value is `-`. • If no AccessKey pair has been created, the value is `N/A`. **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.
access_key_2_exist	TRUE	Indicates whether the second AccessKey pair exists. Valid values are `TRUE` and `FALSE`.
access_key_2_active	TRUE	Indicates whether the second AccessKey pair is active. Valid values are `TRUE`, `FALSE`, and `N/A`. If no AccessKey pair has been created, the value is `N/A`.

Field	Example	Description
access_key_2_last_rotated	2019-11-11T12:50:18Z	The time when the second AccessKey pair was created or last changed. If no AccessKey pair has been created, the value is `N/A`.
access_key_2_last_used	2019-11-13T12:50:18Z	The time when the second AccessKey pair was last used. • If the AccessKey pair has not been used since RAM started to track this information, the value is `-`. • If no AccessKey pair has been created, the value is `N/A`. **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.

Note A maximum of two AccessKey pairs can be created for each Alibaba Cloud user (Alibaba Cloud account user or RAM user) in the RAM console. Before this limit takes effect, more than two AccessKey pairs can be created. Therefore, an Alibaba Cloud 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 logon settings for a RAM user

This topic describes how to allow RAM users to log on to the RAM console, and how to modify or clear console logon settings for RAM users.

Procedure

1. Log on to the RAM console with 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 username of the target RAM user.
4. In the **Console Logon Management** section of the **Authentication** tab, enable the RAM user to log on to the RAM console with a password, and modify or clear console logon settings based on your business needs.
   - **Enable Console Logon**: If console logon settings have not been specified for the RAM user, you can specify the following configuration items based on your business needs.
     - **Console Password Logon**: specifies whether the RAM user can use the password to log on to the console.

       > **Note**
       > - If you want to allow the RAM user to log on to the RAM console, select **Enabled**.
       > - If you want to keep the password, multi-factor authentication (MFA), and other logon settings while disallowing the RAM user to log on to the RAM console, select **Disabled**. If you select **Disabled**, you can modify logon settings for the RAM user. However, these settings do not take effect. These settings take effect only after you select **Enabled**.

     - **Set Logon Password**: specifies whether a default password or a custom password is used by the RAM user. The default password is automatically generated by the system. If you select the option of using a custom password, specify one before proceeding.

       > **Note** 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 the RAM user must enable MFA.

       > **Note** If you select Required, the page for enabling an MFA device automatically appears when the RAM user logs on to the console.

   - **Modify Logon Settings**: If console logon settings have been specified for the RAM user, you can click this button to modify the logon settings based on your business needs.
   - **Remove Logon Settings**: If console logon settings have been specified for the RAM user, you can click this button to clear the logon settings, including the password and MFA settings.

     > **Note** The console logon settings cannot be automatically recovered after they are cleared. Proceed with caution. You can enable the RAM user to log on to the RAM console later. In this case, you must specify the console logon settings again.

Related information

- CreateLoginProfile
- GetLoginProfile
- UpdateLoginProfile
- DeleteLoginProfile

3.4. Set security policies for RAM users

This topic describes how to use your Alibaba Cloud account to set security policies for RAM users.

Procedure

1. Log on to the RAM console by using an Alibaba Cloud account.
2. In the left-side navigation pane, click **Settings** under **Identities**.
3. On the **Security Settings** tab, click **Update RAM User Security Settings**. In the dialog box that appears, configure the following parameters:
   - **Save MFA Logon Status for 7 Days**: specifies whether to allow RAM users to keep the multi-factor authentication (MFA) devices logged on for seven days. By default, this parameter is set to Not Allowed.
   - **Manage Passwords**: specifies whether to allow RAM users to change their passwords.
   - **Manage AccessKey**: specifies whether to allow RAM users to change their AccessKey pairs.
   - **Manage MFA Devices**: specifies whether to allow RAM users to enable and disable MFA devices.
   - **Logon Session Valid For**: specifies the maximum duration of a logon session. The validity period is measured in hours.

     > **Note** If you log on to the Alibaba Cloud console by assuming a RAM role or using single sign-on (SSO), the maximum session duration is limited by the **Logon Session Valid For** parameter. For more information, see Assume a RAM role and SAML response for role-based SSO.

   - **Logon Address Mask**: specifies the IP addresses that can be used for password logon or SSO. By default, this parameter is unspecified, which indicates that logon from all IP addresses is allowed. If you use the password or SSO to log on to the Alibaba Cloud console, you can initiate access requests only from the IP addresses that are specified by the subnet masks. However, you can use AccessKey pairs to call API operations to access Alibaba Cloud resources from all IP addresses regardless of the subnet mask setting.
4. Click **OK**.

> **Note** The settings apply to all the RAM users of your Alibaba Cloud account.

Related information

- SetSecurityPreference

3.5. Set subnet masks for an Alibaba Cloud account

This topic describes how to set subnet masks for an Alibaba Cloud account to specify the IP addresses from which access is allowed. The subnet masks help you enhance account security.

Procedure

1. Log on to the RAM console with an 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 **Login Mask** section of the **Security Settings** page, click **Set**.
4. On the **Login Mask** page, specify one or more valid subnet masks.

   > **Note** If you want to specify more than one subnet mask, separate the masks with semicolons (;), for example, 192.168.0.0/16;10.0.0.0/8.

5. Click **Save**.

   > **Note** If you use the password or single sign-on (SSO) to log on to the Alibaba Cloud console, you can initiate access requests only from the IP addresses that are specified by the subnet masks. You can also use AccessKey pairs to call API operations to access Alibaba Cloud resources.

4.Advanced settings

4.1. Manage the default domain name

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. This topic describes how to change the default domain name to customize the logon name suffix of RAM users for easy identification.

Procedure

1. Log on to the RAM console by using an Alibaba Cloud account.
2. In the left-side navigation pane, click **Settings** under **Identities**.
3. Click the **Advanced** tab. On this tab, you can view and update the **Default Domain** parameter.
   - View the **Default Domain** parameter. The format of the **Default Domain** parameter is `<AccountAlias>.onaliyun.com`. The default value of the *AccountAlias* element is your Alibaba Cloud account ID. If you have not created an account alias, the format of the **Default Domain** parameter is `<AccountID>.onaliyun.com`.
   - Update the **Default Domain** parameter. To update the parameter, click **Update**. In the **Update Domain** pane, specify an account alias, and click **OK**.

What's next

RAM users can then 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, specify the logon name in the format of `<username>@<AccountAlias>.onaliyun.com`. For more information, see Log on to the console as a RAM user.

The use of default domain names simplifies the procedure to configure SAML for user-based 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, RAM users of the Alibaba Cloud account can use this domain alias to log on to the RAM console.

Prerequisites

The domain alias must be publicly resolvable. Before the domain alias can be used, you must verify that you own the domain alias.

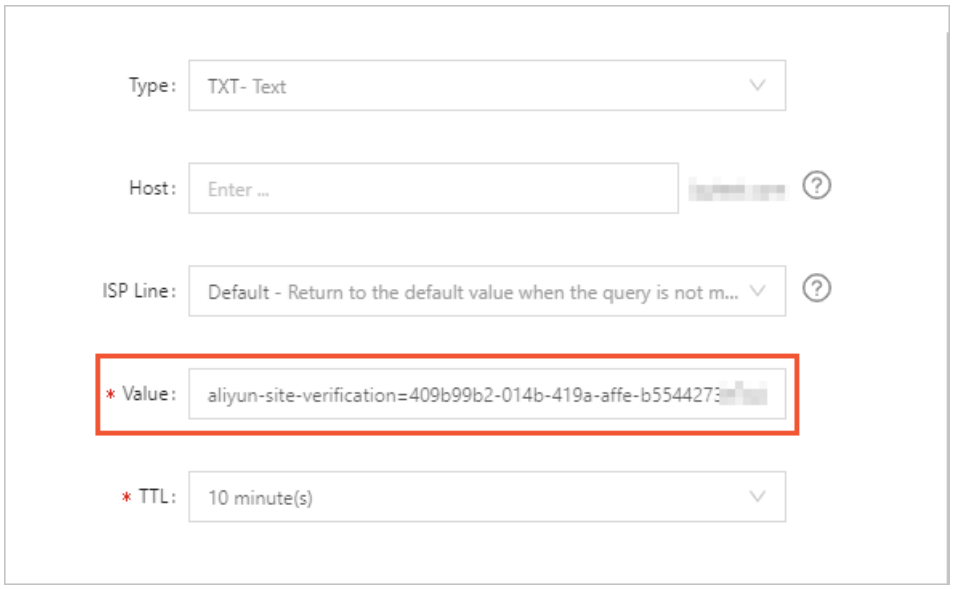
Procedure

1. Create a domain alias in the RAM console.
   i. Log on to the RAM console with your Alibaba Cloud account.
   ii. In the left-side navigation pane, click **Settings** under **Identities**.
   iii. On the **Advanced** tab, click **Create Domain Alias**.

iv. Set the **Domain Name** parameter.

v. Click **OK** and then copy the verification code.

2. Add a TXT record in the system at your DNS hosting provider. If you use the Alibaba Cloud DNS service, configure the TXT record, as shown in the following figure. Note that you must enter the verification code in the **Value** field. For more information, see Add DNS records.



3. Log on to the RAM console to verify that you own the domain name.

i. In the left-side navigation pane, click **Settings** under **Identities**.

ii. On the **Advanced** tab, click **Domain Ownership Verification**.

iii. Click **OK**.

What's next

After the domain alias is created, the RAM users of your Alibaba Cloud account can use the domain alias 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 console as a RAM user.

You can use the domain alias to simplify the procedure of configuring user-based 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 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 only for RAM users and do not create AccessKey pairs for your Alibaba Cloud account.

Procedure

1. Log on to the RAM console by using an 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 the target RAM user.
4. In the **User AccessKeys** section, click **Create AccessKey**.
5. 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 a new one. You can create a maximum of two AccessKey pairs.

Related information

- CreateAccessKey

5.2. View the basic information about AccessKey pairs

This topic describes how to view the basic information about AccessKey pairs, including the AccessKey ID, status, last usage time, and creation time.

Procedure

1. Log on to the RAM console with 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 username of the target RAM user.
4. In the **User AccessKeys** section, view the basic information about AccessKey pairs.

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

5.3. Rotate AccessKey pairs

This topic describes how to rotate AccessKey pairs. You can create up to 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 to prevent against the leakage of AccessKey pairs.

Procedure

1. Create a new 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 AccessKey pair is in use, follows these steps: Log on to the RAM console. Go to the details page of the target user. Find the new and original AccessKey pairs in the **User AccessKeys** section. View the values in the **Last Used** column for the AccessKey pairs. You can determine whether the new or original AccessKey pair is in use based on the column values.

3. Disable the original AccessKey pair. For more information, see Disable an AccessKey pair.
4. Confirm that your applications and systems are working.
   - If the applications and systems are working, the update is successful. Then, you can delete the original AccessKey pair.
   - If an application or system stops working, you must re-enable the original AccessKey pair, and then repeat step 2 to step 4 until the update is successful.
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 RAM user. You can disable AccessKey pairs of a RAM user if the permissions required by the RAM user change or if the RAM user no longer needs to access Alibaba Cloud resources by calling API operations.

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. On the **Users** page, click the username of the target RAM user in the **User Logon Name/Display Name** column.
4. In the **User AccessKeys** section, find the target AccessKey pair and click **Disable**.

> Note To re-enable the AccessKey pair, click Enable.

5. Click OK.

Related information

- UpdateAccessKey

5.5. Delete an AccessKey pair

This topic describes how to delete an AccessKey pair for a RAM user. You can delete AccessKey pairs for a RAM user if the RAM user no longer needs to access Alibaba Cloud resources by calling API operations or using other development tools.

Prerequisites

Before you delete an AccessKey pair, you can query the last usage time of the pair to check whether the pair is in use. For information about how to query the last usage time, see View the basic information about AccessKey pairs.

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

Procedure

1. Log on to the RAM console with 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 username of the target RAM user.
4. In the User AccessKeys section, click Delete.
5. In the dialog box that appears, select I am aware of the risk and confirm the deletion.
6. Click OK.

Related information

- DeleteAccessKey

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. This topic uses the Google Authenticator app as an example to explain the detailed procedure. After you enable an MFA device, it provides additional security protection for your Alibaba Cloud account.

Procedure

1. Log on to the Alibaba Cloud console with an 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 now renamed TOTP.

4. On the **Turn on Account Protection** page, select scenarios, select the TOTP verification method, and then click **Submit**.
5. In the **Verify identity** step of the **Identity Verification** page, select a verification method.
6. Click **Verify now**, enter the verification code, and then click **Submit**.
7. Download and install Google Authenticator on your mobile phone. After you install Google Authenticator, go back to the **Install the application** step of the **Identity Verification** page and click **Next**.
   - For iOS, install the Google Authenticator app from the App Store.
   - For Android, install the Google Authenticator app from the Google Play Store.

   > **Note** For Android, you must install a QR code scanner from the Google Play Store for Google Authenticator to identify QR codes.

8. Open the Google Authenticator app and tap **BEGIN SETUP**.
9. Select a method to enable the MFA device from the following available options.
   - (Recommended) Tap **Scan barcode** in the Google Authenticator app, and scan the QR code in the **Enable the MFA** step of the **Identity Verification** page in the Alibaba Cloud console.
   - Tap **Manual entry**, enter the username and key, and then tap the √ icon in the Google Authenticator app.

   > **Note** You can find the username and key by moving the pointer over **Scan failed** in the **Enable the MFA** step of the **Identity Verification** page.

10. In the **Enable the MFA** step of the **Identity Verification** page, enter the dynamic verification code in the Google Authenticator app, and click **Next** to complete the account protection settings.

> Note The verification code in the Google Authenticator app is refreshed every 30 seconds.

What's next

If you log on to the Alibaba Cloud console with MFA enabled, you must enter the following information:

1. Username and password of the RAM user
2. Verification code provided by the MFA device

> Note
> - The MFA settings for your Alibaba Cloud account do not apply to your RAM users.
> - Before you uninstall or remove an MFA device, you must log on to the Alibaba Cloud console and disable the MFA device. Otherwise, a logon failure may occur.

Related information

- BindMFADevice

6.2. Disable an MFA device for an Alibaba Cloud account

This topic describes how to disable a multi-factor authentication (MFA) device for an Alibaba Cloud account. This topic uses the Google Authenticator app as an example to explain the detailed procedure.

Procedure

1. Log on to the Alibaba Cloud console with an 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 now renamed TOTP.

4. Click **Turn off** next to **Account Protect settings**.
5. Open the Google Authenticator app.
6. On the **Identity Verification** page in the console, enter the dynamic verification code that is obtained from the Google Authentication app, and click **Submit**.

6.3. Enable an MFA device for a RAM user

This topic takes the Google Authenticator app as an example to describe how to enable a multi-factor authentication (MFA) device for a RAM user. 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 an Alibaba Cloud account.

   > Note
   > - If you have selected Required for Enable MFA when modifying the logon settings of a RAM user, the RAM user needs to go to step 5 when the RAM user logs on to the RAM console.
   > - If you allow a RAM user of your Alibaba Cloud account to manage its own MFA device, the RAM user can enable an MFA device in the RAM console. The procedure is as follows: Move the pointer over the profile picture in the upper-right corner of the console, and click **Security**. In the left-side navigation pane, click **MFA Device Management**. On the page that appears, click **Enable MFA Device**.

2. In the left-side navigation pane, click **Users** under **Identities**.
3. In the **User Logon Name/Display Name** column, click the username of the target RAM user.
4. On the **Authentication** tab, click **Enable the Virtual MFA Device**.
5. Download and install the Google Authenticator app on your mobile device.
   - For iOS, install the Google Authenticator app from the App Store.
   - For Android, install the Google Authenticator app from the Google Play Store.

   > Note For Android, you must install a QR code scanner from the Google Play Store for Google Authenticator to identify QR codes.

6. Open the Google Authenticator app.
7. Select a method to enable the MFA device from the following available options.
   - Recommended. Tap **BEGIN SETUP** > **Scan barcode** in the Google Authenticator app, and scan the QR code that is displayed on the **Scan the code** tab in the RAM console.
   - Tap **BEGIN SETUP** > **Manual entry**, enter the username and key, and then tap the check sign (√) in the Google Authenticator app.

   > Note You can obtain the username and key from the **Retrieve manually enter information** tab in the console.

8. Enter the two consecutive verification codes that are obtained from the Google Authenticator app, and click **Enable**.

   > Note The verification code in the Google Authenticator app is refreshed at an interval of 30 seconds.

What's next

When a RAM user logs on to the RAM console with the MFA device enabled, the RAM user must enter the following information:

1. Username and password of the RAM user

2. Verification code provided by the MFA device

> **Note** Before you uninstall or remove an MFA device, you must log on to the Alibaba Cloud console and disable the MFA device. Otherwise, a logon failure may occur.

Related information

- BindMFADevice

6.4. Disable an MFA device for a RAM user

This topic describes how to disable a multi-factor authentication (MFA) device for a RAM user of your Alibaba Cloud account.

Procedure

1. Log on to the RAM console by using an Alibaba Cloud account.

   > **Note** If you allow a RAM user to manage its own MFA device, the RAM user can disable the MFA device in the RAM console. The procedure is as follows: Log on to the console as a RAM user, move the pointer over the profile picture in the upper-right corner of the console, and then click **Security**. In the left-side navigation pane, click **MFA Device Management**. On the page that appears, click **Disable MFA Device**.

2. In the left-side navigation pane, click **Users** under **Identities**.
3. On the **Users** page, click the name of the target RAM user in the **User Logon Name/Display Name** column.
4. On the **Authentication** tab, click **Disable the Virtual MFA Device**.
5. Click **OK**.

Related information

- UnbindMFADevice