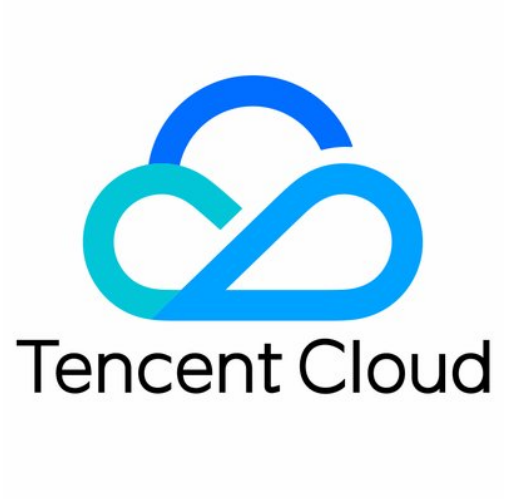
About Account

Account Security

Product Documentation



Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Account Security
Login Protection

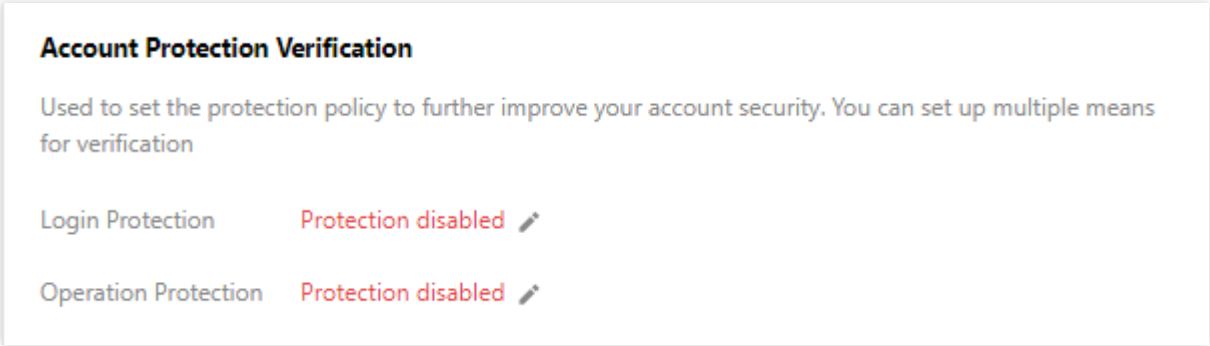
Last updated : 2020-05-08 17:32:16

Login protection is an additional layer of protection that Tencent Cloud provides for logins. An additional identity verification credential is required after the correct username and password are entered.

After login protection is enabled, you must verify your identity every time you log in to the Tencent Cloud website. This prevents others from logging in to your account even if they have cracked your password.

Enabling Login Protection

1. Log in to the Tencent Cloud Console and go to Security Settings page. Click the edit icon next to **Login Protection** to enable it.



2. Complete the identity authentication as prompted.
3. You will be able to enable **Login Protection** after you pass the identity authentication.

Login Protection Types

Log in to the Tencent Cloud Console and go to Security Settings. Go to **Account Protection Verification** > **Login Protection**, and select from the following accordingly:

Operation Protection Type	Description

Operation Protection Type	Description
Enable MFA	After entering your username and password in the login page, you will be redirected to the MFA verification page where you need to enter the correct MFA password before you can log in to your account.
Enable SMS verification	After entering your username and password in the login page, you will be redirected to the SMS verification page where you need to get a verification code on your phone and enter it correctly before you can log in to your account.
Do not enable	Secondary verification will not be required.

MFA Devices

Last updated : 2020-05-08 17:32:16

Multi-Factor Authentication (MFA) is a simple and effective security authentication method. It adds an additional layer of protection to strengthen the username and password credentials. An MFA device, also called a dynamic password card or token, is a device that enables this authentication method. Tencent Cloud currently offers two types of MFA devices: hardware MFA devices and virtual MFA devices.

Hardware MFA Devices

> Currently, hardware MFA devices are only available for beta users.

The figure below shows some examples of hardware MFA devices. The 6-digit dynamic authentication code displayed is updated every 30 seconds, and the serial number of the MFA device is on the back.

Binding a hardware MFA device

1. Log in to the Tencent Cloud Console, click the account name in the top-right corner, and click **Security Settings**.
2. Go to **Basic Settings** > **MFA Device** and click **Bind**.
3. Complete the identity authentication as prompted on the authentication window that pops up.
4. Select a hardware MFA device, enter the serial number and authentication code, and bind the device as prompted.
5. Click **Submit** to complete the binding of the hardware MFA device.

Unbinding a hardware MFA device

1. Log in to the Tencent Cloud Console, click the account name in the top-right corner, and click **Security Settings**.
2. Go to **Basic Settings** > **MFA Device** and click **Unbind**.
3. Click **Confirm** in the pop-up box.
4. Complete the identity authentication as prompted on the authentication window that pops up.
5. Complete the unbinding.

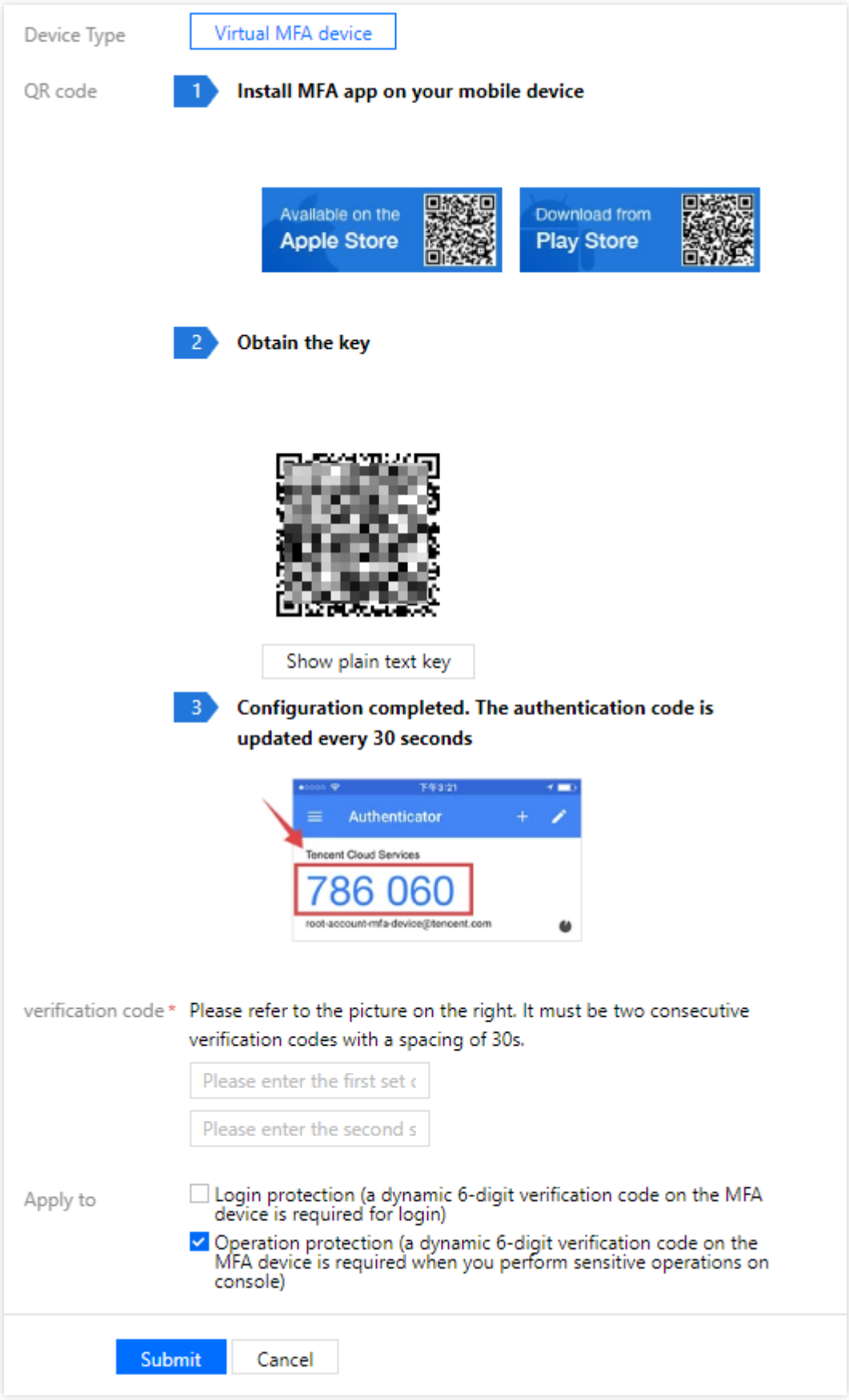
Virtual MFA Device

A virtual MFA device is an application program that generates dynamic authentication codes. It is compliant with the time-based one-time password (TOTP) standard as defined in RFC 6238. Tencent Cloud's virtual MFA devices are supported by the Tencent Cloud Assistant mini program.

Binding a virtual MFA device

1. Log in to the Tencent Cloud Console, click the account name in the top-right corner, and click **Security Settings**.
2. Go to **Basic Settings** > **MFA Device** and click **Bind**.
3. Complete the identity authentication as prompted on the authentication window that pops up.

4. Select a virtual MFA device and bind it as prompted.



5. Click **Submit** to complete the binding of the virtual MFA device.

Unbinding a virtual MFA device

1. Log in to the Tencent Cloud Console, click the account name in the top-right corner, and click **Security Settings**.
2. Go to **Basic Settings** > **MFA Device** and click **Unbind**.
3. Click **Confirm** in the pop-up box.
4. On the authentication page that pops up, enter the 6-digit dynamic authentication code and click **OK** to complete the unbinding.

Logging out from All Devices

Last updated : 2020-06-10 10:35:28

If your account is logged in on multiple devices, or you suspect that your account has been compromised, you can log out of your account from all devices including the current one.

1. Log in to the Tencent Cloud Console, enter the Security Settings page, go to **Login Status Management** and click **Log out from All Devices**.
2. Click **Log out Now** as prompted.

Products that support MFA

Last updated : 2020-04-16 11:04:17

Here is a list of products and operations that support MFA verification.

Account-Related Operations

The following account-related operations are supported:

- Deregistering an account
- Associating an account
- Disassociating an account
- Binding a token
- Unbinding a token
- Modifying the email login password
- Modifying the recovery mobile number
- Managing login status
- Resetting the email login password
- Viewing an API key in plaintext
- Setting operation protection
- Setting login protection

Billing-Related Operations

The following billing-related operations are supported:

- Bill verification

CAM

The following CAM-related operations are supported:

- Creating a sub-user
- Creating a role in the console
- Deleting a project key
- Viewing an API key in plaintext
- Getting a temporary token for MFA authentication
- Querying a project key
- Querying all user groups
- Modifying a virtual token
- Modifying a hardware token

- Setting operation protection
- Unbinding a sub-user login method
- Unbinding a virtual sub-account token
- Unbinding a sub-account token

CVM

The following CVM-related operations are supported:

- Rolling back a snapshot
- Binding a key pair
- Deleting a snapshot policy
- Deleting a snapshot
- Querying the VNC URL of an instance
- Unmounting a cloud disk
- Getting a VNC login token
- Modifying a cloud disk renewal flag
- Modifying a instance renewal flag
- Modifying the VPC of an instance
- Restarting an instance
- Reinstalling an instance
- Resetting a password
- Adjusting an instance configuration
- Shutting down an instance
- Switching system reinstallation parameters
- Switching instance configuration adjustment parameters
- Switching instance termination parameters
- Terminating a cloud disk
- Terminating an instance

Image-Related Operations

The following image-related operations are supported:

- Creating an image
- Deleting an image

Message Center

The following Message Center-related operations are supported:

- Modifying the message subscription recipient

VPC

The following VPC-related operations are supported:

- Creating a routing policy
- Deleting a routing policy
- Deleting a route table
- Disabling subnet routing
- Enabling subnet routing
- Replacing a routing policy
- Modifying the associated route table

CDN

The following CDN-related operations are supported:

- Deleting a domain name
- Deactivating a domain name

Operation Protection

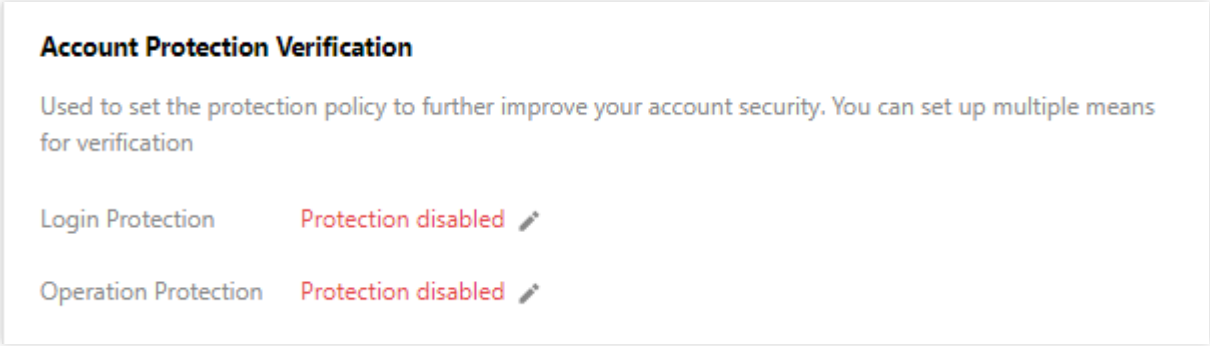
Last updated : 2020-05-08 17:32:17

Operation protection is an additional layer of protection that Tencent Cloud provides for sensitive operations. After operation protection is enabled, you will need to complete identity authentication before performing sensitive operations.

A verification code is often used for secondary confirmation when you perform sensitive operations in the console.

Enabling Operation Protection

1. Log in to the Tencent Cloud Console and go to Security Settings page. Click the edit icon next to **Operation Protection** to enable it.



2. Complete the identity authentication as prompted.
3. You will be able to enable **Operation Protection** after you pass the identity authentication.

Operation Protection Types

Log in to the Tencent Cloud Console and go to Security Settings. Go to **Account Protection Verification** > **Operation Protection**, and select from the following accordingly:

Operation Protection Type	Description
Enable MFA	To perform an operation in the console, you must enter the correct MFA password on the identity authentication page; otherwise, the operation cannot be performed.

Operation Protection Type	Description
Enable SMS verification	To perform an operation in the console, you must enter the verification code received on your phone on the identity authentication page; otherwise, the operation cannot be performed.
Do not enable	Secondary verification will not be required.

Account Cancellation

Last updated : 2020-07-08 14:22:01

Account Cancellation

Once an account has been cancelled, it cannot be restored. In order to ensure that your account assets, cloud resources, account information, and so on, are not affected, backup all data under your account before you apply to cancel your account.

Account Cancellation Process

1. Go to the Account Center

Go to **Account Center >Security Settings**. In the account cancellation module, select **Cancel**.

2. Confirm the application to cancel the account

Before submitting the application, read the notes carefully.

3. Verify mobile number

Verify your recovery mobile number. You cannot proceed to the next step before a successful verification.

4. Upload basic information materials

Users that have already undergone identity verification must upload the documents needed to verify their identity. Users that have not verified their identity do not need to perform this step and can proceed directly to the cancellation application review stage.
Documents needed for identity verified personal users:

- Passport or driver’s license.

> Above scans must be in **color**.

Documents needed for identity verified enterprise users:

- Business identification.

Above scans must be in **color**.

5. Review of the cancellation application

The review of the account cancellation application takes approximately 3 business days. You will be notified of the results through your secure phone number or email address. If you need to modify your secure phone number or email address, go to **Account Center** > **Security Settings**.

6. Successful account cancellation

When the account has been cancelled successfully, you will be notified by SMS and email. After the account is cancelled, you will no longer be able to use this account to log in to the Tencent Cloud website.

Account Password

Last updated : 2019-09-02 14:56:38

Your account password is an important credential ensuring the security of your account. Please keep it safe and change it regularly if possible.

Password Best Practices

1. Change your password at least once every 90 days.
2. Do not re-use any of your last three passwords.

Password Complexity Requirements

The password must be a combination of 8-20 characters including at least one of each of the following: letter, number and special character (such as / or _, but excluding spaces).

Email Login Security Rules

1. The password can only be entered incorrectly up to three times each day per account.
2. After three failed attempts, you must enter a verification code to log in.
3. After 10 failed attempts, your account will be locked for 24 hours, starting from the first time an incorrect password was entered.