

# **Cloud Access Management Security Setting Policy Product Documentation**



## Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

## Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

## 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.

# Security Setting Policy

Last updated : 2021-06-07 09:42:09

## Basic Principles

### 1. Enable MFA protection

To strengthen account security, we recommend that you bind MFA for all accounts. We also recommend enabling login and operation protection for root accounts and sub-accounts. For the accounts that support login with e-mail, we strongly recommend enabling MFA secondary verification. This will require a secondary verification for account login and sensitive operations. For related settings, see [Setting Security Protection for Collaborators](#), and [Setting Security Protection for Sub-Users](#).

### 2. Access Tencent Cloud with a sub-account

Do not use the root account identity credentials to access Tencent Cloud, and **never** share identity credentials with anyone. Create a sub-account for all users that access Tencent Cloud, and grant management permissions as necessary. For information about the related settings, see [User Types](#).

### 3. Use groups to grant permissions

Define groups according to the job responsibilities, and grant management permissions to the group as necessary. Then, assign the users to the corresponding groups. In this way, when you modify the permissions for the group, the permissions of the users associated with the group will change accordingly. Additionally, when there are organizational changes and people move around, you only need to update the group the user belongs to. For more information, see [User Groups](#).

### 4. Grant least privilege

Granting least privilege is a standard security principle where you grant only the permissions required to perform a task. Any additional unnecessary permissions should not be granted. For example, if a user only uses CDN Service, access permission for other services (such as COS read and write permissions) should not be granted.

### 5. Manage users, permissions, and resources with different sub-accounts

We do not recommend managing users, permissions, and resources with the same account. Designate different sub-accounts to manage users, permissions and resources respectively.

### 6. Rotate credentials regularly

We recommend you or one of your CAM users change the login password or API key regularly. This way, if one of your credentials is compromised, the time it can be used to access your resources is limited.

For information about setting passwords for root accounts, see [Account Password](#).

For more information about setting passwords for sub-accounts, see [Resetting Login Passwords for Sub-Users](#).

## **7. Delete unnecessary certificates and permissions**

Delete certificates that the user does not need, and permissions that the user no longer needs. Minimize the security risks caused by compromised access credentials.

## **8. Use policy conditions to enhance security**

Define the conditions under which your policies will take effect as precisely as possible to limit access and strengthen security. For example, write conditions to specify the server users must perform operations on. The time period can also be specified.

For more information, see [Element References - Condition](#).