

Cloud Access Management

Glossary

Product Documentation



Copyright Notice

©2013–2026 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

 Tencent Cloud

All trademarks associated with Tencent Cloud and its services are owned by the Tencent corporate group, including its parent, subsidiaries and affiliated companies, as the case may be. 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.

Glossary

Last updated: 2025-08-12 15:15:49

Policy

A syntactic rule that defines one or more permissions. A root account performs authorization by associating policies with users/user groups. An admin or any sub-account that is granted the policy management permission can also create, update and delete policies, or associate policies with users/user groups.

Login credentials

Login username and password. After you log in to Tencent Cloud console with the username and password, you can access resources with the scope of permissions through the console.

Multi-factor authentication (MFA)

An additional layer of security protection on top of the login credentials. If you have bound an MFA device in the security information settings, you can choose to enable login and operation protections.

Access certificates

TencentCloud API keys (SecretId and SecretKey), including individual API keys and project keys. For most services, individual API keys are used to access TencentCloud APIs. For some services, such as COS, project keys are used to access TencentCloud APIs.

Root account

When you apply for a Tencent Cloud account, a root account is created by the system which you can use to log in to Tencent Cloud services. A root account is the entity used to bill your usage of Tencent Cloud resources. A root account has full access to all the resources under it by default.

Identity credentials

Credentials used to verify the identity of a user, including login credentials and access certificates. You must keep the credentials safe.

Permission

An authorization to allow some users to perform certain operations or access certain resources or prohibit some users from doing so. By default, a root account has full access to all the resources under the account, while a sub-account does not have access to any resources under the root account.

User group

A group of users (sub-accounts) who fulfill the same function. You can create multiple user groups as needed, and associate the user groups with specific policies to grant them different permissions.

Sub-account

An entity created by the root account. It has an ID and identity credentials and has the permission to log in to Tencent Cloud console. A sub-account does not own any resource by default, and must be authorized by its root account to use the resources. A root account can create multiple sub-accounts.

Role

A virtual identity with a collection of permissions. It is used to grant permissions to role entities for them to access services and resources and perform operations in Tencent Cloud. Those permissions are granted to a role, instead of a user or user group.

For more information, see [Basic Concepts](#).

Role entity

An object allowed to have the permissions associated with a role. You can edit role entities by adding or deleting objects to allow them to assume roles to access your Tencent Cloud resources or prohibit them from doing so.

For more information, see [Basic Concepts](#).

Permission policy

A JSON file on permissions in which you can define which operations a role can perform and what resources a role can access. This file should conform to the CAM policy language rule.

Trust policy

A JSON file on permissions in which you can define which objects can assume a role and what conditions need to be met before an object assumes a role. This file should conform to the CAM policy language rule.