# Smart Media Hosting

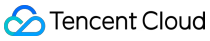
# Quick Start

# Product Documentation

## Copyright Notice



## Trademark Notice





## 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

# Quick Start
# Initiate request

Last updated：2026-01-07 11:03:06

This document describes how to make requests to the SMH service. The procedure is as follows.

## Overview

The SMH service's API is RESTful and supports CORS. You can use any programming library capable of initiating standard HTTPS requests to make requests to the SMH service, or directly initiate requests in the browser. For interfaces with a request body, the request body defaults to JSON format.

> Note:
> For security reasons, SMH does not support HTTP requests.

## Preparations

A Tencent Cloud account has been registered with identity verification completed.

- To register a Tencent Cloud account, click Register Tencent Cloud Account.
- To complete the identity verification, click Identity Verification.

## Operation Steps

### Step 1: Create an Access Token

When the SMH service is used, except for media library management performed through the console, requests to operate the access token itself, and read requests after enabling public read, all other requests require the use of an access token for authentication and identification of requests.

Since access tokens are prerequisites for all operations and require specifying granted permissions when requested, such operation requests must not be initiated from the client-side to prevent any privilege escalation. Therefore, requests to create access tokens require validation of the LibrarySecret, while business parties should not expose the LibrarySecret in client-side environments.

In the actual business architecture, the business backend first needs to complete login and authentication operations for the business frontend (such as username and password of a self-built user system, SMS verification login, WeChat login, mini-program login, and so on). After confirming that the request from the business frontend is from a legitimate user, based on the user's role in the business corresponding to the permissions in the SMH service, the business backend calls the SMH interface to generate an access

token and returns it to the business frontend. When the access token is generated, the user ID can also be attached to the request so that SMH can record the operator of subsequent operations.

Access tokens have a validity period, which defaults to 24 hours. You can specify a different validity period when generating an access token. When an access token is used to initiate a request, SMH automatically renews it, extending its validity to the default 24 hours or the specified duration. Therefore, provided that the interval between each user access to SMH is shorter than the default 24 hours or the validity period specified by you, the access token will remain valid.

To ensure the information security of your business and users, we also provide an interface to forcefully revoke access tokens. When a user changes their password, loses a device, or when you need to proactively disable access for a specific user, you can use this interface to forcefully revoke the access tokens of the specified user on specific devices or all devices.

For detailed instructions on the interfaces for generating and deleting access tokens, refer to Generating Access Tokens and Deleting Specified Access Tokens in the API documentation.

## Step 2: Initiate Request

You can refer to API Documentation to learn specific operational instructions and request parameters.