

Video Moderation System

Best Practices

Product Documentation



Copyright Notice

©2013-2024 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.

Contents

Best Practices

API Connection Guide

Preparations Before Connection

Configuration During Connection

Verification After Connection

Error Codes

CAM Authorization Guide

Overview

Configuring CAM for CMS

Enabling CAM for CMS

Configuring CAM for CMS

FAQs

Business Practices

Forum Comment Recognition

Album Content Recognition

Live Audio Stream Recognition

Live Room Content Recognition

Best Practices

API Connection Guide

Preparations Before Connection

Last updated : 2023-12-21 17:06:05

This document describes how to connect to and use VM.

Getting Account Information

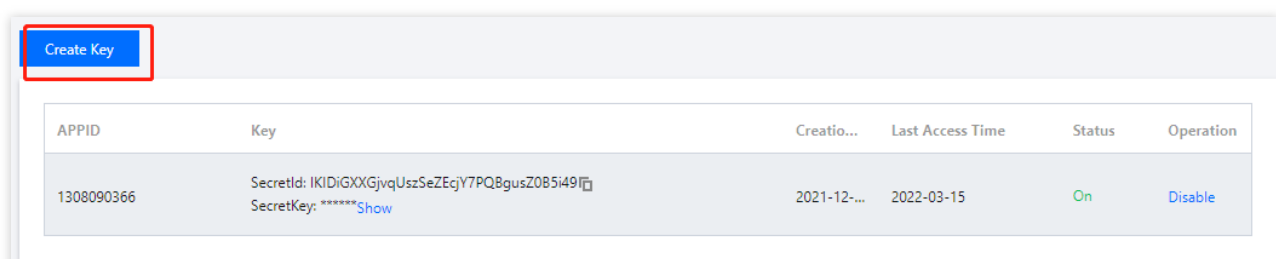
Getting Tencent Cloud account

Log in to the [Tencent Cloud console](#) to sign up and verify your identity as instructed in [Signing up for a Tencent Cloud Account](#). You can skip this step if you already have a Tencent Cloud account.

Getting Tencent Cloud API access key

Tencent Cloud uses `secretid` and `secretkey` to verify your identity and permissions. You can get the Tencent Cloud API access key in the following steps:

1. Go to the [TencentCloud API key management](#) page and select **CAM > API Key Management** on the left sidebar to enter the API key management page.
2. Click **Create Key** to create a key and save the `secretid` and `secretkey` for subsequent API calls. You can skip this step if you already have a Tencent Cloud key.



Configuring in Console

Activating service

Log in to the [CMS console](#) and click **Activate Now**. You will be gifted a free trial package of **600 minutes** (equivalent to **36,000 images** and **600 minutes of audio**) valid for **one month**.

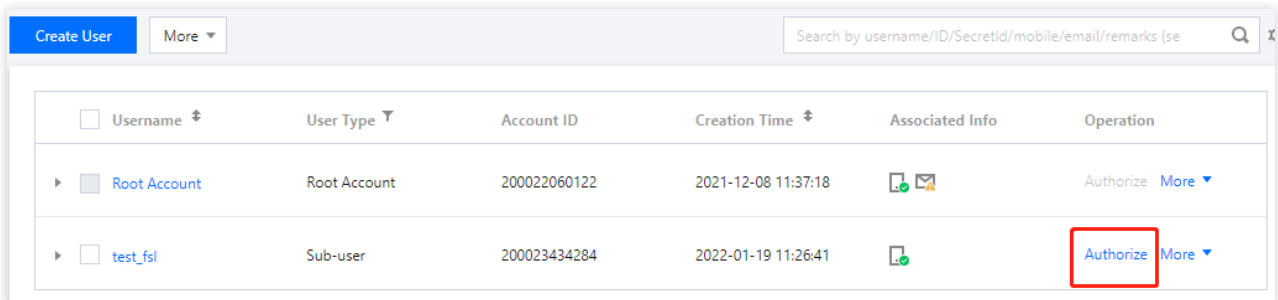
Configuring permission

If you want to call VM through a sub-account, you need to authorize it by assigning a policy in the following steps:

1. Log in to the [CAM console](#) and select **User > User List** on the left sidebar to enter the **User List** page.
2. On the **User List** page, find the target sub-account and click **Authorize** in the **Operation** column to pop up the **Associate Policy** window.

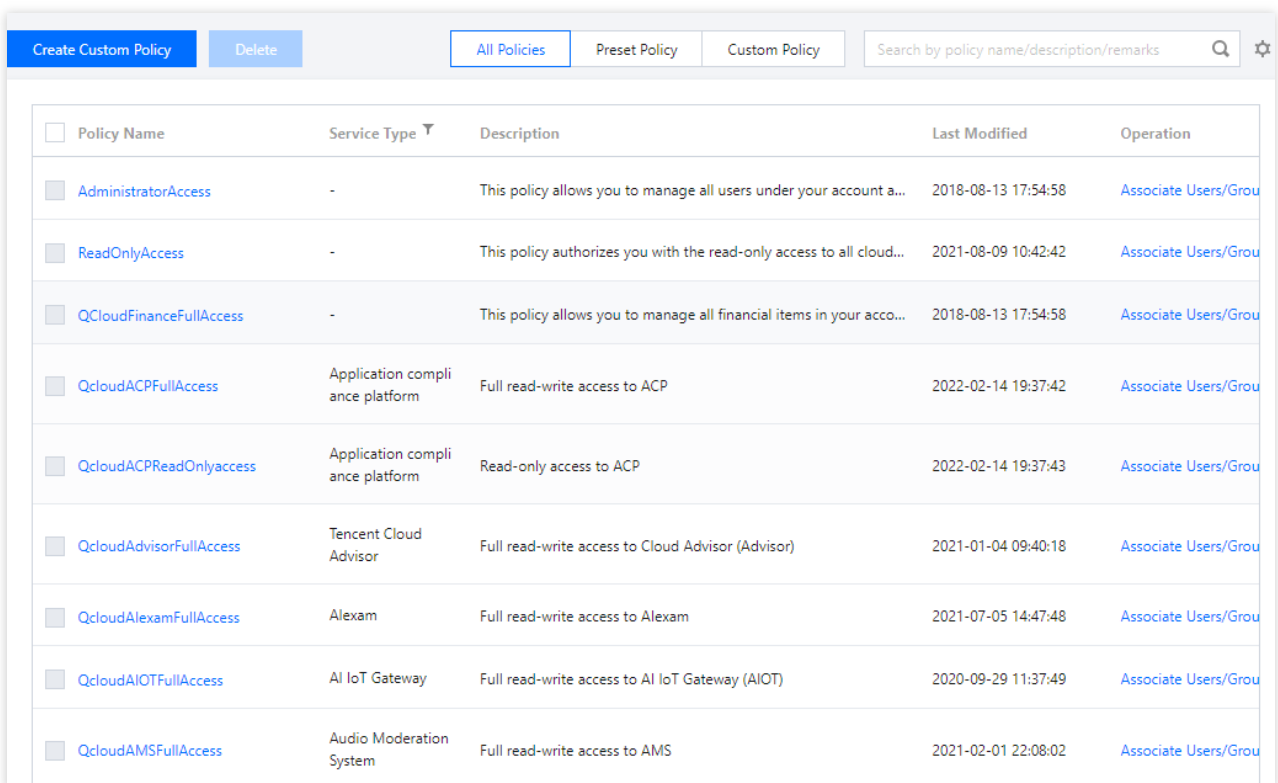
Note:

For more information on CAM, see [CAM Authorization Guide](#).



<input type="checkbox"/> Username	User Type	Account ID	Creation Time	Associated Info	Operation
<input checked="" type="checkbox"/> Root Account	Root Account	200022060122	2021-12-08 11:37:18		Authorize More
<input type="checkbox"/> test_fsl	Sub-user	200023434284	2022-01-19 11:26:41		Authorize More

3. In the **Associate Policy** pop-up window, select the `QcloudVMFullAccess` policy and click **OK**.



<input type="checkbox"/> Policy Name	Service Type	Description	Last Modified	Operation
<input checked="" type="checkbox"/> AdministratorAccess	-	This policy allows you to manage all users under your account a...	2018-08-13 17:54:58	Associate Users/Grou
<input checked="" type="checkbox"/> ReadOnlyAccess	-	This policy authorizes you with the read-only access to all cloud...	2021-08-09 10:42:42	Associate Users/Grou
<input checked="" type="checkbox"/> QCloudFinanceFullAccess	-	This policy allows you to manage all financial items in your acco...	2018-08-13 17:54:58	Associate Users/Grou
<input checked="" type="checkbox"/> QcloudACPFullAccess	Application compli ance platform	Full read-write access to ACP	2022-02-14 19:37:42	Associate Users/Grou
<input checked="" type="checkbox"/> QcloudACPReadOnlyaccess	Application compli ance platform	Read-only access to ACP	2022-02-14 19:37:43	Associate Users/Grou
<input checked="" type="checkbox"/> QcloudAdvisorFullAccess	Tencent Cloud Advisor	Full read-write access to Cloud Advisor (Advisor)	2021-01-04 09:40:18	Associate Users/Grou
<input checked="" type="checkbox"/> QcloudAlexamFullAccess	Alexam	Full read-write access to Alexam	2021-07-05 14:47:48	Associate Users/Grou
<input checked="" type="checkbox"/> QcloudAIOTFullAccess	AI IoT Gateway	Full read-write access to AI IoT Gateway (AIOT)	2020-09-29 11:37:49	Associate Users/Grou
<input checked="" type="checkbox"/> QcloudAMSFULLAccess	Audio Moderation System	Full read-write access to AMS	2021-02-01 22:08:02	Associate Users/Grou

Configuring custom policy (optional)

Note:

This step is optional. If you don't use a custom recognition policy, you can use the default policy (by leaving the `Biztype` field empty when calling APIs) for content recognition.

If your business scenarios require a custom recognition policy for video content, you can configure one in **Policy Management** in the following steps:

1. Log in to the [CMS console](#) and select **VM > Policy Management** on the left sidebar to enter the **Policy Management** page.
2. On the **Policy Management** page, click **Create Policy** in the top-left corner to enter the **Create Policy** page.
3. Enter the policy information based on your business scenario, reserve the `Biztype` field as an API input parameter, and click **Next**.

← Create Policy

1 Basic Information > 2 Policy Configuration > 3 Custom Library > 4 Creation Completed

* Policy name

* Biztype name ⓘ

* Service template ⓘ

* Industry

* Use industry template ☐ Yes ☒ No

Next

Parameter description:

Parameter	Description
Policy Name	Text description of the policy, which can contain up to 30 letters, digits, and underscores.
Biztype Name	Specific policy number used for API calls, which can contain 3–32 letters, digits, and underscores and must be unique.
Associate Service Template	Currently, only the default template can be used for configuration.
Industry Category	Category of the industry scenario involved in the policy.
Use Industry	It will be displayed only when Industry Category is set. You can select whether to use

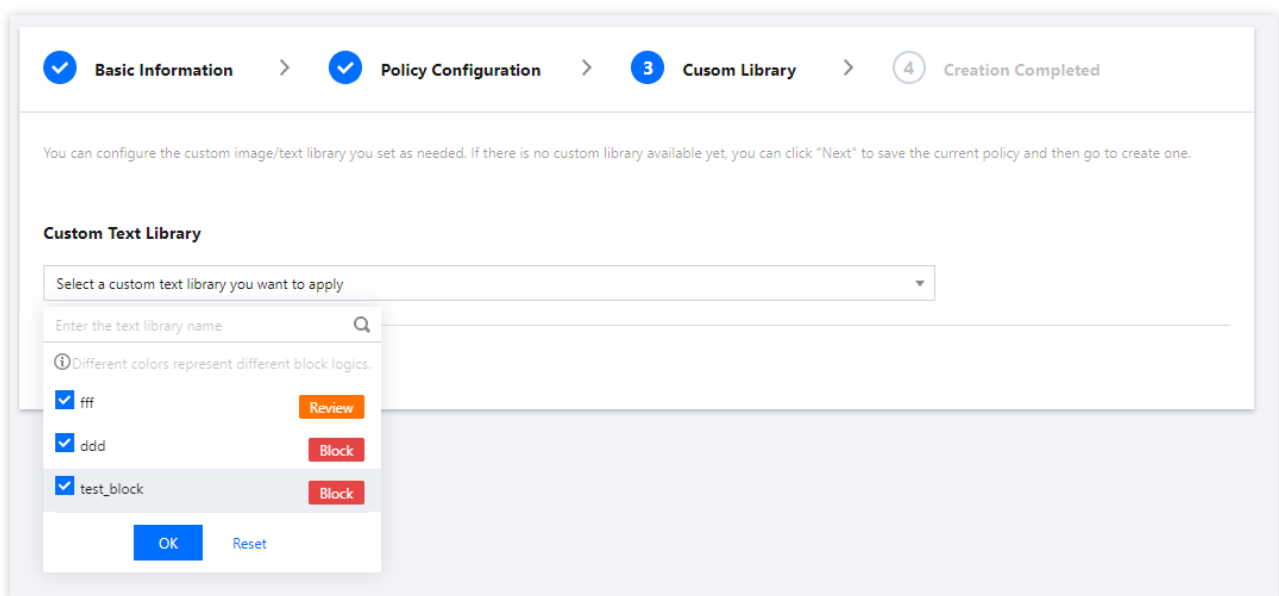
Template	Tencent Cloud's preset industry templates for recognition.
----------	--

4. On the **Recognition Policy Configuration** page, select whether to recognize different types of content based on your business needs and click **Next**.

5. You can choose to associate a custom dictionary you configured in the drop-down list and click **Next**.

Note:

Different colors in a custom dictionary represent different blocking logics, where red represents "blocked", yellow represents "suspected", and green represents "allowed".



6. After confirming that everything is correct, click **Complete**.

Note:

You can pass in the `Biztype` of a custom policy as an API input parameter to use the policy for video content recognition.

Configuration During Connection

Last updated : 2023-12-21 17:06:05

Online Debugging with API Explorer

Tencent Cloud API Explorer is an automated tool suitable for interactive UIs. It is easy to use with no additional configuration required but not suitable for repeated and continuous use.

This tool provides various capabilities such as online call, signature verification, SDK demo generation, and quick API search, greatly improving the efficiency of using TencentCloud API. You can use it to debug VM parameters online as instructed in Request Structure.

API Connection Through SDK

To improve your connection experience and reduce your connection costs, we recommend you use the companion SDK 3.0, a companion tool for the TencentCloud API 3.0 platform. It unifies parameter calls and features the same SDK usage, API call methods, error codes, and returned packet formats for different programming languages.

Verification After Connection

Last updated : 2023-12-21 17:06:05

After completing the API connection, you can verify whether VM is connected to successfully as detailed below.

Connection Success

If the `Response` doesn't have the `Error` field and the business parameters are returned normally, VM is connected to successfully as shown below:



```
{
  "Response": {
    "DataId": "123",
    "Extra": "xx",
    "BizType": "0",
    "RiskDetails": [
      {
        "Level": 2,
        "Label": "RiskAccount"
      }
    ]
  },
}
```

```
"DetailResults": [
  {
    "LibName": "Porn",
    "Score": 72,
    "Label": "Porn",
    "LibId": "12",
    "Suggestion": "Review",
    "Keywords": [
      "Porn"
    ],
    "LibType": 0
  },
  {
    "LibName": "Porn",
    "Score": 0,
    "Label": "",
    "LibId": "1",
    "Suggestion": "Block",
    "Keywords": [
      "Porn"
    ],
    "LibType": 2
  }
],
"Label": "Ad",
"Score": 87,
"RequestId": "x2123-123123-123",
"Suggestion": "Block",
"Keywords": [
  "Friend me for coupons"
]
}
```

Connection Failure

If the `Response` contains the `Error` field, the connection failed. The following is an example of failure caused by signature verification :



```
{
  "Response": {
    "Error": {
      "Code": "AuthFailure.SignatureFailure",
      "Message": "The provided credentials could not be validated. Please che",
    },
    "RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
  }
}
```

`Code` in `Error` indicates the error code, while `Message` indicates the specific error information. For more information, see [Error Codes](#). If you cannot identify the cause of the connection error, [submit a ticket](#) for assistance on a 24/7 basis.

Error Codes

Last updated : 2023-12-21 17:06:05

Common Error Codes

Error Code	Description
ActionOffline	The API is deactivated.
AuthFailure.InvalidAuthorization	The <code>Authorization</code> in the request headers doesn't meet Tencent Cloud standards.
AuthFailure.InvalidSecretId	Invalid key (not TencentCloud API key type).
AuthFailure.MFAFailure	MFA failure .
AuthFailure.SecretIdNotFound	The key does not exist. Check whether the key has been deleted or disabled in the console, and if not, check whether the key is correctly entered. Note that there shall be no space before or after the key.
AuthFailure.SignatureExpire	Signature expired. The timestamp and server time cannot differ by more than five minutes. Make sure that your current local time matches the standard time.
AuthFailure.SignatureFailure	Invalid signature. The signature calculation is incorrect. Make sure that you have followed the signature calculation steps as described in the signature algorithm document in the calling method.
AuthFailure.TokenFailure	Incorrect token.
AuthFailure.UnauthorizedOperation	The request is not authorized. For more information, see the authentication description in the CAM documentation .
DryRunOperation	DryRun Operation. It means that the request would have succeeded, but the DryRun parameter was used.
FailedOperation	The operation failed.
InternalError	Internal error.
InvalidAction	The API does not exist.

InvalidParameter	Incorrect request parameter (such as parameter format and type).
InvalidParameterValue	Invalid parameter value.
InvalidRequest	The multipart format of the request body is incorrect.
IpInBlacklist	The IP address is in the blocklist.
IpNotInWhitelist	The IP address is not in the allowlist.
LimitExceeded	The quota limit is exceeded.
MissingParameter	A parameter is missing.
NoSuchProduct	The product does not exist.
NoSuchVersion	The API version does not exist.
RequestLimitExceeded	The request rate limit is exceeded.
RequestLimitExceeded.IPLimitExceeded	The IP frequency limit is exceeded.
RequestLimitExceeded.UinLimitExceeded	The frequency limit of the root account is exceeded.
RequestSizeLimitExceeded	The request packet size exceeds the limit.
ResourceInUse	The resource is in use.
ResourceInsufficient	Insufficient resource.
ResourceNotFound	The resource does not exist.
ResourceUnavailable	The resource is unavailable.
ResponseSizeLimitExceeded	The response packet size exceeds the limit.
ServiceUnavailable	The service is temporarily unavailable.
UnauthorizedOperation	Unauthorized operation.
UnknownParameter	Unknown parameter. An undefined parameter can cause an error.
UnsupportedOperation	Unsupported operation.
UnsupportedProtocol	Unsupported HTTP(S) request protocol. Only GET and POST requests are supported.
UnsupportedRegion	Unsupported region.

Business Error Codes

Error Code	Description
InternalServerError.ErrTextTimeOut	The request timed out.
InvalidParameter.ErrAction	Incorrect action.
InvalidParameter.ErrTextContentLen	The text in the request is too long.
InvalidParameter.ErrTextContentType	The text type is incorrect. The text must be Base64-encoded.
InvalidParameterValue.ErrTextContentLen	The text in the request exceeds the length limit.
InvalidParameterValue.ErrTextContentType	The format of the text in the request is incorrect. The text must be Base64-encoded.
UnauthorizedOperation.Unauthorized	The API is not authorized.

CAM Authorization Guide

Overview

Last updated : 2023-12-21 17:06:05

Cloud Access Management (CAM) is a user and permission management system provided by Tencent Cloud for the refined management of access to CMS and its specific APIs. Currently, CMS supports **service-level authorization** and console operations. For more information, see [CAM-Enabled Products](#).

Note:

You can skip this section if you don't need to manage access to CMS resources for sub-accounts. This will not affect your understanding and use of the other sections of the document.

Use Cases

If you have multiple businesses under your Tencent Cloud account which need to be managed separately, you can create sub-users/collaborators in CAM and assign them to the admins of different businesses.

CAM enables you to configure different access permissions for your partners or employees and specify which operations they can perform and which resources they can access, thus implementing least privilege management.

If you have set up an account management system based on the private network, you can connect CAM to your existing authentication system to grant your employees and partners access to Tencent Cloud services and resources.

Configuring CAM for CMS

Enabling CAM for CMS

Last updated : 2023-12-21 17:06:05

Creating Sub-user

A root account/admin user can create one or more sub-user accounts for team members and bind permission policies to them. The CAM authorization feature of CMS supports three creation methods: **quick creation, custom creation, and import from WeChat/WeCom.**

Quick creation is easy and fast, but the permission policies that can be bound are relatively fixed.

Custom creation is complex, but it supports batch creation and refined permission policy management.

Import from WeChat/WeCom makes it easier to connect an existing organizational structure or configure permission policies for external members.

For how to create a sub-user, see [Creating Sub-user](#).

Creating Collaborator

An admin user can set the **Tencent Cloud accounts** of other team members as collaborators and grant them access to cloud resources and bind permission policies to them. For detailed directions, see [Creating Collaborator](#).

Configuring CAM for CMS

Last updated : 2023-12-21 17:06:05

Step 1. Log in to the CAM console

After creating a sub-user/collaborator, you can click **Username** on the **User List** management page in the [CAM console](#) to disable or enable the console access for the current user in **User Details**.

Note:

The sub-user/collaborator denied access to the console will not be able to log in to the Tencent Cloud console with the current account, but they can still log in to the Tencent Cloud console with their own accounts; in other words, access grant/revocation by the current account does not affect their use of their own Tencent Cloud account.

Step 2. Grant API access (programming access)

You can configure and manage API access keys as instructed in [Root Account Access Key Management](#) and [Access Key](#).

Note:

Your API key represents your account identity and granted permissions, **which is equivalent to your login password**. Do not disclose it to others.

Step 3. Authorize a sub-user/collaborator

Grant access to CMS services

CAM allows you to grant sub-users/collaborators the access permissions of specific CMS services. It can be combined with access method authorization (console/API access) for refined permission management.

Policy authorization process

1. Log in to the [console](#) with the root account or a sub-user/collaborator with admin permissions and enter the **User List** page.
2. On the **User List** page, select the target sub-user/collaborator and click **Authorize** to pop up the **Associate Policy** page.

<input type="checkbox"/> Username ↕	User Type ▼	Account ID	Creation Time ↕	Associated Info	Operation
▶ <input type="checkbox"/> Root Account	Root Account	200022060122	2021-12-08 11:37:18		Authorize More ▼
▶ <input type="checkbox"/> test_fsl	Sub-user	200023434284	2022-01-19 11:26:41		Authorize More ▼

3. On the **Associate Policy** page, configure the access permissions of CMS services for the sub-user/collaborator as needed.

Note:

Currently, you can configure **full access/read-only access** to the AMS, VM, IMS, and TMS services under CMS.

Create Custom Policy

Delete

All Policies

Preset Policy

Custom Policy

Search by policy name/description/remarks

<input type="checkbox"/> Policy Name	Service Type	Description	Last Modified	Operation
<input type="checkbox"/> AdministratorAccess	-	This policy allows you to manage all users under your account a...	2018-08-13 17:54:58	Associate Users/Grou
<input type="checkbox"/> ReadOnlyAccess	-	This policy authorizes you with the read-only access to all cloud...	2021-08-09 10:42:42	Associate Users/Grou
<input type="checkbox"/> QCloudFinanceFullAccess	-	This policy allows you to manage all financial items in your acco...	2018-08-13 17:54:58	Associate Users/Grou
<input type="checkbox"/> QcloudACPFullAccess	Application compli ance platform	Full read-write access to ACP	2022-02-14 19:37:42	Associate Users/Grou
<input type="checkbox"/> QcloudACPReadOnlyaccess	Application compli ance platform	Read-only access to ACP	2022-02-14 19:37:43	Associate Users/Grou
<input type="checkbox"/> QcloudAdvisorFullAccess	Tencent Cloud Advisor	Full read-write access to Cloud Advisor (Advisor)	2021-01-04 09:40:18	Associate Users/Grou
<input type="checkbox"/> QcloudAlexamFullAccess	Alexam	Full read-write access to Alexam	2021-07-05 14:47:48	Associate Users/Grou
<input type="checkbox"/> QcloudAIOTFullAccess	AI IoT Gateway	Full read-write access to AI IoT Gateway (AIOT)	2020-09-29 11:37:49	Associate Users/Grou
<input type="checkbox"/> QcloudAMSFullAccess	Audio Moderation System	Full read-write access to AMS	2021-02-01 22:08:02	Associate Users/Grou
<input type="checkbox"/> QcloudAntiDDoSFullAccess	Anti-DDoS	Full read-write access to Anti-DDoS	2021-04-26 22:45:45	Associate Users/Grou

4. Click **OK**.

Description of CAM policies for CMS services

The preset policies for CMS services are as listed below:

Service	Preset Policy	Permission Description

TMS	QcloudTMSFullAccess	Full access
	QcloudTMSReadOnlyAccess	Read-Only access
IMS	QcloudIMSFullAccess	Full access
	QcloudIMSFullAccess	Read-Only access
AMS	QcloudAMSFullAccess	Full access
	QcloudAMSReadOnlyAccess	Read-Only access
VM	QcloudVMFullAccess	Full access
	QcloudVMReadOnlyAccess	Read-Only access

Note:

The above preset policies can be used to associate different access permissions of the corresponding CMS services with a sub-user/collaborator. After you assign a preset policy to a sub-user/collaborator as instructed in [Authorization Management](#), the sub-user/collaborator can access or use the corresponding service according to the permissions granted by the policy.

Notes

By default, a root account is the resource owner and has full access to all resources under it, while a sub-user/collaborator does not have access to any resources. **A resource creator does not automatically possess the access to the created resource** and should be authorized by the resource owner instead.

A policy is a syntax rule that defines and describes one or more permissions. There are two policy types: **preset policy** and **custom policy**.

Note:

A preset policy is a set of common permissions that are frequently used by users, such as super admin and full resource access. Preset policies cover a wide range of operation objects at a coarse operation granularity. They are preset by the system and cannot be edited by users.

A custom policy is a set of user-defined permissions that describes resource management in a more refined way. It allows fine-grained permission division and can flexibly meet your differentiated permission management needs. You can set user permissions by selecting a policy in the policy list for association, reusing the existing user policy, or adding the user to a group to get the permissions of the group.

For how to create a custom policy, see [Creating Custom Policy](#).

For how to configure a policy for a user/user group, see [Authorization Management](#).

Step 4. Configure and manage CAM

CAM needs to be properly configured and continuously managed to maximize its value. For the security suggestions on the configuration and management of CAM, see [Security Setting Policy](#).

FAQs

Last updated : 2023-12-21 17:06:05

How do I set a sub-user/collaborator as admin?

You can grant the sub-user/collaborator the admin permissions by assigning them the preset **AdministratorAccess** policy as instructed in **Configuring Policy for User/User Group**. The policy allows the authorized account to manage all users and their permissions, financial information, and Tencent Cloud service assets under the root account.

How does a sub-user/collaborator get account management permission?

You can grant the sub-user/collaborator the account management permission by assigning them the preset **QcloudCamFullAccess** policy as instructed in [Authorization Management](#). The policy allows you to manage all users and their permissions in the account.

You can also grant the sub-user/collaborator read-only access to CAM by assigning them the preset **QcloudCamReadOnlyAccess** policy.

How does a sub-user/collaborator get the same data viewing permission as the root account?

We recommend you assign the preset **QcloudCamReadOnlyAccess** policy to the sub-user/collaborator as instructed in [Authorization Management](#) to grant them read-only access to CAM. When they log in to the console, a user selection box will be displayed on the corresponding pages, and the default option is the current sub-account, which has the same data permissions as the root account.

Note:

You can also grant a sub-user/collaborator the same data viewing permission as the root account by setting them as admin. We recommend you follow the principle of least privilege when doing so.

How do I access the financial information with a root account or financial admin account?

Root account: log in to the Tencent Cloud console and click [Billing Center > Bills](#) to view the package usage and billing details.

Financial admin account: you need to grant the sub-user/collaborator **financial admin permissions**, console access, and **QCloudFinanceFullAccess** as instructed in [Authorization Management](#), so that they can manage the financial information in the account and view the package usage and billing details in [Billing Center - Bills](#) in the Tencent Cloud console.

How do I restrict the access IPs of sub-users/collaborators?

You can set login restrictions for sub-users/collaborators in the CAM console, so that they can log in to the Tencent Cloud console only in secure environments. Specifically, you can restrict suspicious logins (from unusual login

locations or 30 days after the last successful login) and allow/forbid login from specified IPs. For detailed directions, see [Login Restrictions](#).

Business Practices

Forum Comment Recognition

Last updated : 2023-12-21 17:32:27

You can directly call the **TextModeration** API to recognize forum comments (such as shopping website reviews, community replies, and video comments).

Note:

Before calling the API, make sure that the current account **has at least the access permission of TMS**. For more information on how to configure the permission, see [CAM Authorization Guide](#).

If you cannot access the TMS service, you will need to activate the service/check the billing information (for root account) or request the corresponding permission from the admin or root account (for sub-account/collaborator).

Step 1. Configure a custom dictionary (optional)

The custom dictionary is used to configure the personalized recognition content. You can skip this step if you don't need to configure a custom library.

1. Log in to the [CMS console](#) and select **TMS > Custom Library Management > Custom Dictionary** on the left sidebar to enter the **Custom Dictionary** page.
2. On the **Custom Dictionary** page, click **Add Dictionary** in the top-left corner to pop up the **Create Dictionary** window.
3. In the **Create Dictionary** pop-up window, configure a custom library based on your business needs.

Create a Text Library

* Text library

Enter the text library name

Moderation suggestion ⓘ

☒ Block ☐ Review

Matching mode

☒ Exact matching ⓘ ☐ Fuzz

OK

Cancel

4. Click **OK**.

5. On the **Custom Dictionary** page, select the target dictionary and click **Manage** in the **Operation** column to enter the dictionary content management page.



Custom Library Management

Preset Text Library

Custom Text Library

ⓘ Before using Text Moderation, please assign CMS with the required permissions to access your data in CAM.

Add a Text Library

Text library	Moderation sugges... ⌵	Matching mode ⌵	Associated policy	Last modified
	Block	Exact matching	None	

6. On the dictionary content management page, click **Add Sample** in the top-left corner to pop up the **Add Sample** window.

7. In the **Add Sample** pop-up window, select the recognition details, enter keywords, and click **OK**.

Note:

Recognition Details: violation type that corresponds to the recognition model.

Keywords: each keyword can contain **up to 20 characters**, and **a maximum of 500 keywords separated by line breaks can be batch submitted** at a time.

Add Samples

Moderation suggestion *

Please select a content category ▼

Keyword *

Press 'Enter' key to separate multiple keywords in newlines. Up to 50 time

1. One keyword per line; up to 100 chars per keyword

2. Paste multiple keywords (up to 500) to add them in a batch

3. You can add up to 2,000 keywords to the library.

OK

Cancel

8. On the **Custom Dictionary** page, select the target dictionary and click



in the **Operation** column to enable or disable it.

Note:

After the dictionary is disabled, samples in it will not be used to match and recognize image content.

9. After configuring the custom dictionary, you can associate it with the policy created in [Configure a task policy](#).

Step 2. Configure a task policy (optional)

You can skip this step if you use the preset default policy. The default policy is developed by TenDI based on models for multiple industries. It is suitable for most content security requirements.

1. Log in to the [CMS console](#) and select **TMS > Policy Management** on the left sidebar to enter the **Policy Management** page.
2. On the **Policy Management** page, click **Create Policy** in the top-left corner to enter the **Create Policy** page.
3. On the **Create Policy** page, set the relevant policy information, including the policy name, Biztype name, associated service template (**not required currently**), and industry category (select whether to use TenDI's preset industry templates for recognition), and click **Next**.

← **Create Policy**

1 **Basic Information** > 2 **Policy Configuration** > 3 **Custom Library** >

* Policy name

* Biztype name ⓘ

* Service template ⓘ

* Industry

* Use industry template ☐ Yes ☒ No

Next

4. Configure the recognition policy, select whether to recognize different types of risky content based on your business needs, enter relevant information, and click **Next**.
5. Configure the custom library, select whether to configure the custom dictionary, enter relevant information, and click **Next**.
6. After the creation is completed, you can view the policy configuration information on this page. After confirming it, click **Complete**.

Step 3. Create a task and get the recognition result (optional)

After completing the above steps, you can call the **TextModeration** API to create a comment recognition task as instructed below:

Make sure that the text to be recognized meets the [file format requirements](#) of the API.

Enter the input parameters as instructed in the [API documentation](#).

If the task is created successfully, the API will return the detailed recognition result, and you can refer to [Text Content Recognition Sample](#) for more information on sample response parameters. If task creation failed, the API will return an error code, and you can refer to [Business Error Codes](#) and [Common Error Codes](#) for troubleshooting.

Note:

When connecting to the service, you can use API Explorer for online debugging.

Album Content Recognition

Last updated : 2023-12-21 17:32:27

For image content, after [activating IMS](#), you can directly call the **ImageModeration** API to batch recognize images in albums (such as Qzone album).

Note:

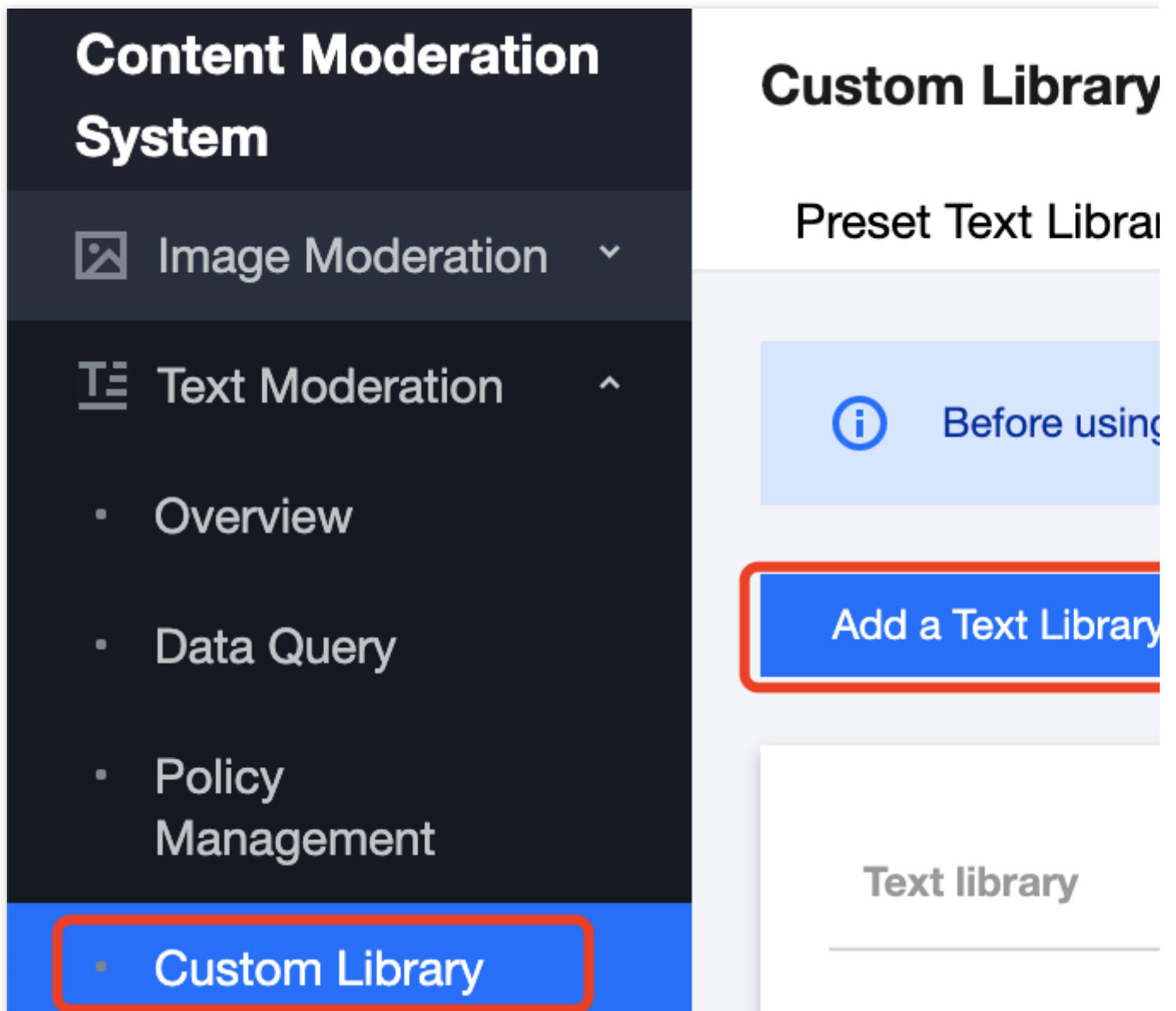
Before calling the API, make sure that the current account **has at least the access permission of IMS**. For more information on how to configure the permission, see [CAM Authorization Guide](#).

If you cannot access the service, you will need to activate the service/check the billing information (for root account) or request the corresponding permission from the admin or root account (for sub-account/collaborator).

Step 1. Configure a custom dictionary (optional)

The custom dictionary is used to configure the personalized recognition content. You can skip this step if you don't need to configure a custom library.

1. Log in to the [CMS console](#) and select **IMS > Custom Library Management > Custom Dictionary** on the left sidebar to enter the **Custom Dictionary** page.
2. On the **Custom Dictionary** page, click **Add Dictionary** in the top-left corner to pop up the **Create Dictionary** window.



3. In the **Create Dictionary** pop-up window, configure a custom library based on your business needs.

Create a Text Library

* Text library

Enter the text library name

Moderation suggestion ⓘ

☒ Block ☐ Review

Matching mode

☒ Exact matching ⓘ ☐ Fuzz

OK

Cancel

4. Click **OK**.

5. On the **Custom Dictionary** page, select the target dictionary and click **Manage** in the **Operation** column to enter the dictionary content management page.



Custom Library Management

Preset Text Library

Custom Text Library

ⓘ Before using Text Moderation, please assign CMS with the required permissions to access your data in CAM.

Add a Text Library

Text library	Moderation sugges... ⌵	Matching mode ⌵	Associated policy	Last modified
	Block	Exact matching	None	

6. On the dictionary content management page, click **Add Sample** in the top-left corner to pop up the **Add Sample** window.

7. In the **Add Sample** pop-up window, select the recognition details, enter keywords, and click **OK**.

Note:

Recognition Details: violation type that corresponds to the recognition model.

Keywords: each keyword can contain **up to 20 characters**, and **a maximum of 500 keywords separated by line breaks can be batch submitted** at a time.

Add Samples

Moderation suggestion *

Please select a content category ▼

Keyword *

Press 'Enter' key to separate multiple keywords in newlines. Up to 50 time

1. One keyword per line; up to 100 chars per keyword

2. Paste multiple keywords (up to 500) to add them in a batch

3. You can add up to 2,000 keywords to the library.

OK

Cancel

8. On the **Custom Dictionary** page, select the target dictionary and click



in the **Operation** column to enable or disable it.

Note:

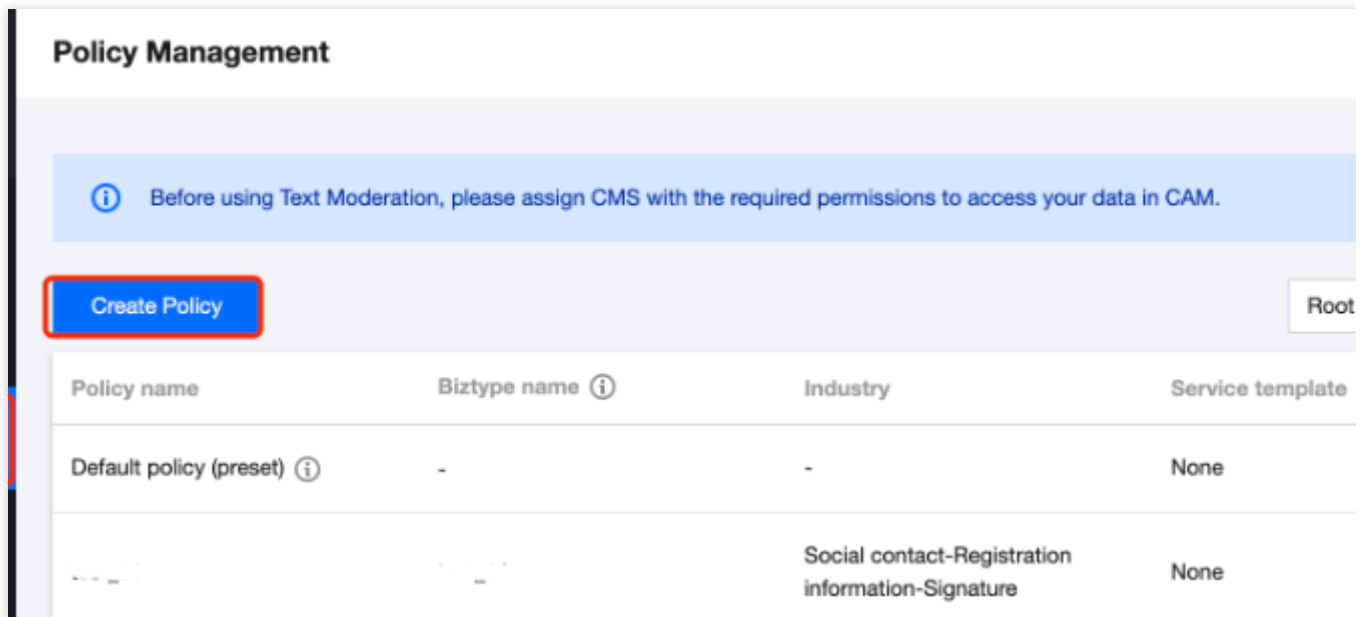
After the dictionary is disabled, samples in it will not be used to match and recognize image content.

9. After configuring the custom dictionary, you can associate it with the policy created in Configure a task policy.

Step 2. Configure a task policy (optional)

You can skip this step if you use the preset default policy. The default policy is developed by TenDI based on models for multiple industries. It is suitable for most content security requirements.

1. Log in to the [IMS console](#) and select **IMS > Policy Management** on the left sidebar to enter the **Policy Management** page.
2. On the **Policy Management** page, click **Create Policy** in the top-left corner to enter the **Create Policy** page.



3. On the **Create Policy** page, set the relevant policy information, including the policy name, Biztype name, associated service template (**not required currently**), and industry category (select whether to use TenDI's preset industry templates for recognition), and click **Next**.

The screenshot shows the 'Create Policy' page with a back arrow and the title 'Create Policy'. Below the title is a progress bar with three steps: '1 Basic Information' (active), '2 Policy Configuration', and '3 Custom Library'. The 'Basic Information' section contains three required fields:

- * Policy name: Enter a policy name
- * Biztype name: Enter a Biztype name
- * Industry: Select an industry (dropdown menu)

At the bottom left of the form is a 'Next' button.

4. Configure the recognition policy, select whether to recognize different types of risky content based on your business needs, and click **Next**.
5. Configure the custom library, select whether to configure the custom dictionary, and click **Next**.
6. After the creation is completed, you can view the policy configuration information on this page. After confirming it, click **Complete**.

Step 3. Create a task and get the recognition result

After completing the above steps, you can call the **ImageModeration** API to create an album recognition task as instructed below:

Make sure that the images meet the [file format requirements](#) of the API.

Enter the input parameters as instructed in the [API documentation](#).

If the task is created successfully, the API will return the detailed recognition result, and you can refer to [Image Content Recognition Sample](#) for more information on sample response parameters. If task creation failed, the API will return an error code, and you can refer to [Business Error Codes](#) and [Common Error Codes](#) for troubleshooting.

Note:

When connecting to the service, you can use API Explorer for online debugging.

Live Audio Stream Recognition

Last updated : 2023-12-21 17:32:27

After activating [AMS](#), you can directly call **AMS** APIs to recognize audio stream content (such as game live streaming, radio, and voice chat).

Note:

Before calling the API, make sure that the current account **has at least the access permission of AMS**. For more information on how to configure the permission, see [CAM Authorization Guide](#).

If you cannot access the service, you will need to activate the service/check the billing information (for root account) or request the corresponding permission from the admin or root account (for sub-account/collaborator).

Step 1. Configure a global task template (optional)

Task templates are used to manage how files are processed for recognition tasks. You can skip this step if the default template is used.

Note:

Currently, only the default template can be edited for template configuration.

1. Log in to the [CMS console](#) and select **AMS > Service Management** on the left sidebar to enter the **Service Management** page.
2. On the service management page, click **View Details**, and the details of the default template will be displayed on the right.

Template name	Associated policy	Last modified
default	dddd、test_01、test01...(4 in total)	2021-12-21 18:00:03

3. On the specific information page, click **Edit** in the top-right corner to enter the template editing page.

Service Management	Template Details	
<div>Template name</div> <div>default</div> <div>Total items: 1</div>	Basic information	
	Template name	default
	Associated policy	test_01、 default
	COS configuration	
	COS description	The video will be stored in the specified COS bucket. The video moderation service is authorized to read the content from the bucket. If the service cannot read the content, the video will be marked as Reference document for COS bucket creation .
	COS bucket name	tianyu-content-moderation-1308090366
	COS region	ap-singapore
	COS object prefix	segment-
	Image moderation configuration	
	Screenshot interval	15s
	Audio moderation configuration	
	Service status	Enabled
	Audio or video clip duration	15s
	Callback address	http://baidu.com
	Full callback	Enabled

4. On the template editing page, set the configuration information, including template name, audio stream or large file segment duration (15s, 30s, or 60s), optional callback address (to which risky content can be returned), and full callback for live streaming switch (on/off). You can customize the template configuration based on your business and storage needs.

Basic information

* Template name

default

Image moderation configuration

* Screenshot interval

☐ 1 second ☐ 5 seconds ☐ 10 seconds ☒ 15 seconds

Audio moderation configuration

* Service status

☒ Enabled ☐ Close

* Audio or video clip duration

☒ 15s ☐ 30s ☐ 60s

Callback address
(optional)

http://baidu.com

* Full callback

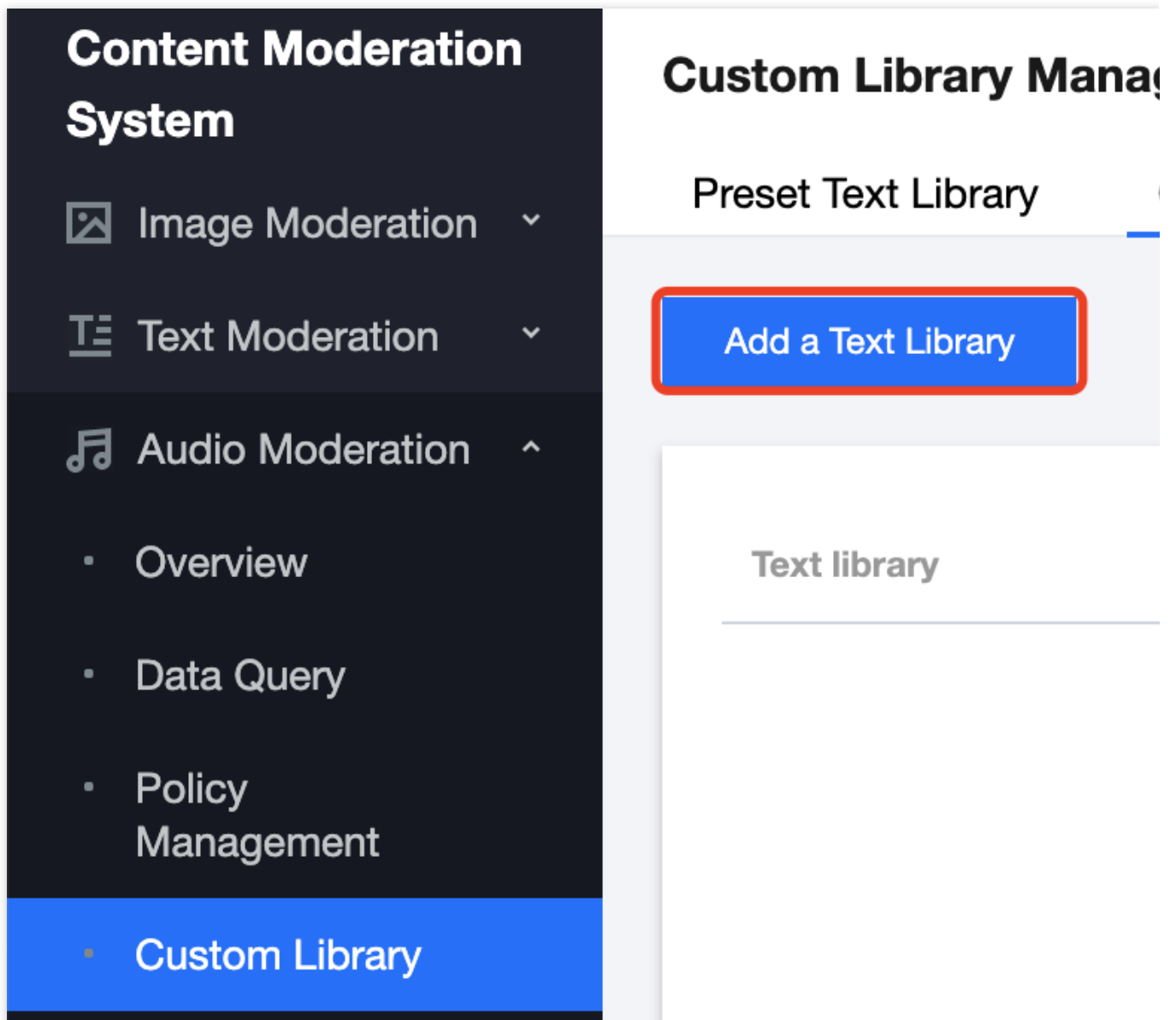
☒ Enabled

5. Click **Save** to save the current template, **which will take effect immediately for all AMS services under the account.**

Step 2. Configure a custom library (optional)

The custom library is used to configure the personalized recognition content. You can skip this step if you don't need to configure a custom library.

1. Log in to the [CMS console](#) and select **AMS > Custom Library Management > Custom Dictionary** on the left sidebar to enter the **Custom Dictionary** page.
2. On the **Custom Dictionary** page, click **Add Dictionary** to pop up the **Create Dictionary** window.



3. In the **Create Dictionary** pop-up window, configure a custom library based on your business needs.

Create a Text Library

* Text library

Enter the text library name

Moderation suggestion ⓘ

☒ Block ☐ Review

Matching mode

☒ Exact matching ⓘ ☐ Fuzzy

OK

Cancel

4. Click **OK**.

5. On the **Custom Dictionary** page, select the target dictionary and click **Manage** in the **Operation** column to enter the dictionary content management page.

Text library	Moderation sugges... ⌵	Matching mode ⌵	Associated policy	Last modified
---	Block	Exact matching	None	2022-01-19 10:49:1
■	Review	Exact matching	None	2022-01-19 10:26:2

6. On the dictionary content management page, click **Add Sample** in the top-left corner to pop up the **Add Sample** window.

7. In the **Add Sample** pop-up window, select the recognition details, enter keywords, and click **OK**.

Note:

Recognition Details: violation type that corresponds to the recognition model.

Keywords: each keyword can contain up to 20 characters, and a maximum of 500 keywords separated by line breaks can be batch submitted at a time.

Add Samples

Moderation suggestion *

Please select a content category ▼

Keyword *

Press 'Enter' key to separate multiple keywords in newlines. Up to 5 time

1. One keyword per line; up to 100 chars per keyword
2. Paste multiple keywords (up to 500) to add them in a batch
3. You can add up to 2,000 keywords to the library.

OK

Cancel

8. On the **Custom Dictionary** page, select the target dictionary and click



in the **Operation** column to enable or disable it.

Note:

After the custom dictionary is enabled, custom violation results will be returned in preference to the default dictionary.

After the dictionary is disabled, samples in it will not be used to match and recognize image content.

9. After configuring the custom dictionary, you can associate it with the policy created in [Configure a task policy](#).

Step 3. Configure a task policy (optional)

You can skip this step if you use the preset default policy. The default policy is developed by TenDI based on models for multiple industries. It is suitable for most content security requirements.

1. Log in to the [CMS console](#) and select **AMS > Policy Management** on the left sidebar to enter the **Policy Management** page.


2. On the **Policy Management** page, click **Create Policy** in the top-left corner to enter the **Create Policy** page.

Content Moderation System

- Image Moderation
- Text Moderation
- Audio Moderation
 - Overview
 - Data Query
- Policy Management**

Policy Management

Create Policy

Policy name	Biztype name
	default

Total items: 1

3. On the **Create Policy** page, set the relevant policy information, including the policy name, Biztype name, associated service template (not required currently), and industry category (select whether to use TenDI's preset industry templates for recognition), and click **Next**.

1 Basic Information

2 Policy Configuration

3 Custom Library

4 Creation

* Policy name

Enter a policy name

* Biztype name ⓘ

Enter a Biztype name

* Service template ⓘ

Select a service template

* Industry

Select an industry

Next

4. Configure the recognition policy, select whether to recognize different types of risky content based on your business needs, and click **Next**.

5. Configure the custom library and select whether to configure the custom dictionary you set. If there is no custom library, you can click **Next** to save the current policy and go to the **Configure a custom dictionary** step.
6. After the creation is completed, you can view the policy configuration information on this page. After confirming it, click **Complete**, and then the policy can be used in API calls.

Step 4. Create an AMS task

After completing the above steps, you can call the **CreateAudioModerationTask** API to create an audio stream recognition task as instructed below:

Make sure that the audio meets the [file format requirements](#) of the API.

Enter the input parameters as instructed in the [API documentation](#).

If the task is created successfully, you can use the task query API to query task details, and you can refer to the [example of creating audio recognition task](#) for more information on sample response parameters. If task creation fails, the API will return an error code, and you can refer to [Business Error Codes](#) and [Common Error Codes](#) for troubleshooting.

Note:

When connecting to the service, you can use API Explorer for online debugging.

Step 5. Get the AMS task result

After creating the audio recognition task, you can call the **DescribeTaskDetail** API to query the details of the task as instructed below:

Enter the input parameters as instructed in the [API documentation](#).

If the API call is successful, you will receive the response output from the API, including the task details. You can refer to the [example of viewing task details](#) for more information on sample response parameters.

Live Room Content Recognition

Last updated : 2023-12-21 17:32:27

After activating [VM](#), you can directly call **VM** APIs to batch recognize video stream content (such as live rooms and video meetings).

Note:

Before calling the API, make sure that the current account **has at least the access permission of VM**. For more information on how to configure the permission, see [CAM Authorization Guide](#).

If you cannot access the service, you will need to activate the service/check the billing information (for root account) or request the corresponding permission from the admin or root account (for sub-account/collaborator).

Step 1. Configure a policy (optional)

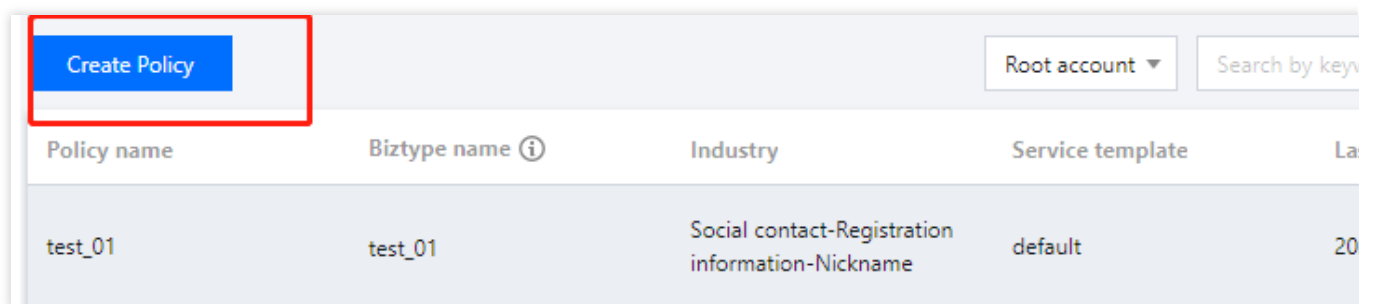
We recommend you configure a recognition policy based on your business needs for a personalized user experience.

Note:

You can skip this step if you use the preset default policy of Tencent Cloud CMS.

The default policy is developed by TenDI based on models for multiple industries. It is suitable for most content security requirements.

1. Log in to the [CMS console](#) and select **VM > Policy Management** on the left sidebar.
2. On the **Policy Management** page, click **Create Policy** to enter the **Create Policy** page.



Create Policy				
Root account ▼		Search by key		
Policy name	Biztype name ⓘ	Industry	Service template	La
test_01	test_01	Social contact-Registration information-Nickname	default	20

3. On the **Policy Configuration** page, enter the relevant information of the policy and click **Next**.

1

Basic Information

>

2

Policy Configuration

>

3

Custom Library

*Policy name

test1

*Biztype name ⓘ

test333

*Service template ⓘ

default

▼

*Industry

Game

▼

*Use industry template

☐ Yes ☒ No

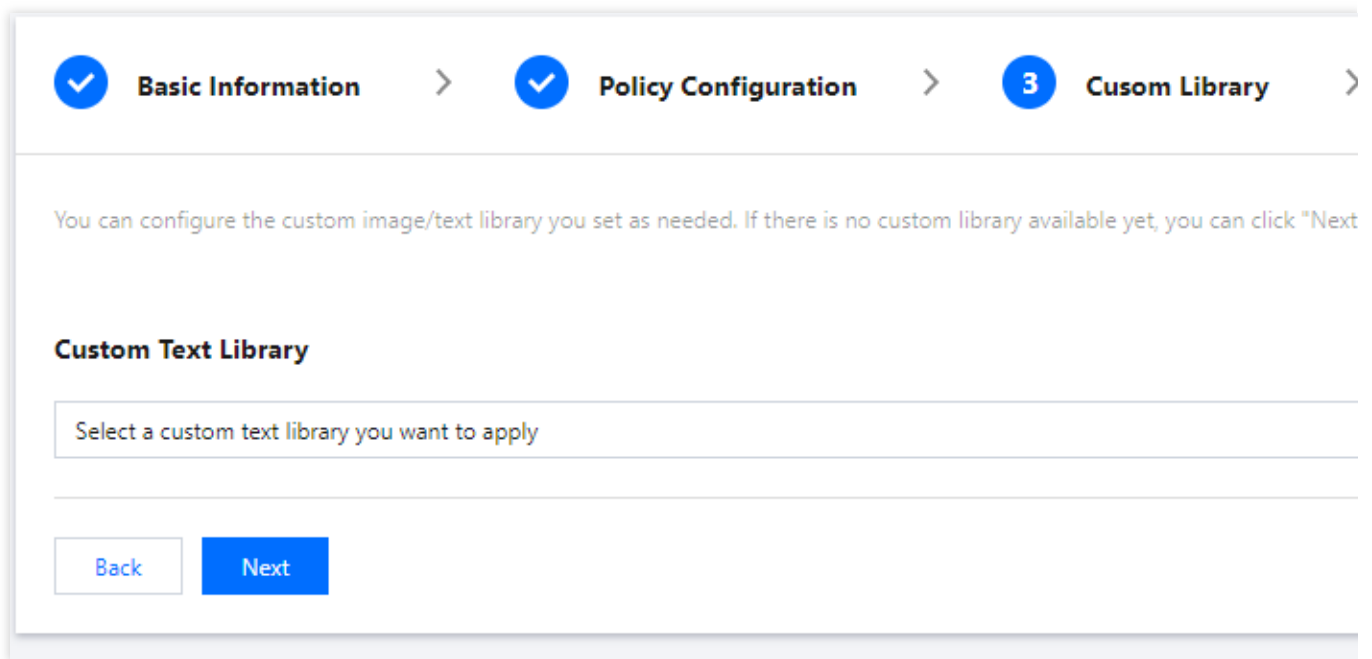
Next

Parameter description:

Parameter	Description
Policy Name	Text description of the policy, which can contain up to 30 letters, digits, and underscores.
Biztype Name	Specific policy number used for API calls, which can contain 3–32 letters, digits, and underscores and must be unique.
Associate Service Template	Currently, only the default template can be used for configuration.
Industry Category	Category of the industry scenario involved in the policy.
Use Industry Template	It will be displayed only when Industry Category is set. You can select whether to use Tencent Cloud's preset industry templates for recognition.

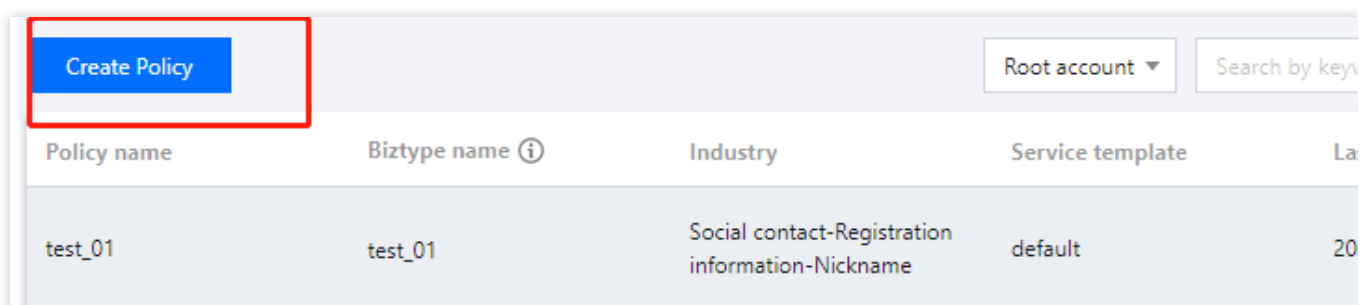
4. On the **Recognition Policy Configuration** page, configure recognition policies for audio and captured images, select whether to recognize different types of content based on your business needs, and click **Next**.

5. On the **Custom Library Configuration** page, select a custom dictionary for content recognition in the **Custom Dictionary** drop-down list. If there are no custom libraries, you can click **Next** or save the current policy and go to [Step 3. Configure a custom dictionary](#).



6. On the **Creation Completion** page, you can view the policy configuration information. After confirming it, click **Complete**.

7. The policy just created will be displayed in the list on the right of the **Policy Management** page.



Policy name	Biztype name ⓘ	Industry	Service template	La
test_01	test_01	Social contact-Registration information-Nickname	default	20

Step 2. Configure a global task template (optional)

Task templates are used to manage how files are processed for recognition tasks.

Note:

You can skip this step if the default template is used.

1. Log in to the [CMS console](#) and select **VM > Service Management** on the left sidebar.
2. On the service management page, click **View Details** to enter the template details page.

Note:

Currently, only the default template can be edited for template configuration.

Template name	Associated policy	Last modified
default	test_01、 default(2 in total)	2022-01-27 14:57:03
Total items: 1		20

3. On the template details page, click **Edit** in the top-right corner to modify parameters.

Basic information

* Template name

default

Audio moderation configuration

* Audio or video clip duration

☐ 15s ☒ 30s ☐ 60s

Callback address
(optional)

Enter a callback URL

* Full callback

☒ Enabled

Parameter description:

Parameter	Description
Template Name	Text description of the template, which can contain up to 30 letters, digits, and underscores.
Screencapture Interval	Set the time interval for screencapturing the video file, which can be 1s, 5s, 10s, 15s, or 30s (default).
Service Status	Select whether to recognize audio at the same time.

	Enable: yes. Disable: no.
Audio Stream or Large File Segment Duration	Set the time length for audio stream or large file segmentation, which can be 15s, 30s (default), or 60s.
Callback Address	The risky content can be returned to this optional address (if entered).
Enable Full Callback for Live Streaming	Set whether to enable full callback for live streaming. Enable: both normal and non-compliant video content will be returned to the callback address. Disable: only the non-compliant video content will be returned to the callback address.

4. Click **Save** to save the current template, which will take effect immediately for all VM services under the account.

Step 3. Configure a custom dictionary (optional)

You can configure a custom dictionary.

Note:

You can skip this step if you don't need to configure a custom dictionary.

1. Log in to the [CMS console](#) and select **VM > Custom Library Management > Custom Dictionary** on the left sidebar.
2. On the **Custom Dictionary** page, click **Add Dictionary** to pop up the **Create Dictionary** window.

Preset Text Library		Custom Text Library		
<div>Add a Text Library</div>		<div>Text library name</div>		
Text library	Moderation su... ▼	Matching mode ▼	Associated policy	Last modified
fff	Review	Exact matching	None	2021-12-23 18:59:38
ddd	Block	Exact matching	None	2021-12-23 18:59:21
test_block	Block	Exact matching	test_01	2021-12-13 16:36:03
Total items: 3				10 ▼

3. In the **Create Dictionary** pop-up window, configure a custom library based on your business needs.

Create a Text Library

*Text library

Enter the text library name

Moderation suggestion ⓘ

☒ Block ☐ Review

Matching mode

☒ Exact matching ⓘ ☐ Fuzzy matching ⓘ

OK

Cancel

Parameter description:

Parameter	Description
Dictionary Name	Text description of the dictionary, which can contain up to 32 letters, digits, and underscores.

Handling Suggestion	<p>You can select Non-compliant or Suspected.</p> <p>Non-compliant: the information is identified as non-compliant information</p> <p>Suspected: the information may be non-compliant and requires manual recognition</p>
Match Mode	<p>You can select Exact match or Fuzzy match.</p> <p>Exact match: it exactly matches the entered text</p> <p>Fuzzy match: it detects variants of the entered keyword to fuzzily match similar words such as split words, homographs, homophones, upper and lower cases, and numbers in words</p>

4. Click **OK**.

5. The dictionary just created will be displayed in the list below the **Custom Dictionary** tab.

Note:

Different colors in a custom dictionary represent different blocking logics, where red represents "non-compliant", and orange represents "suspected".

Text library	Moderation su... ▼	Matching mode ▼	Associated policy	Last modified
fff	Review	Exact matching	None	2021-12-23 18:59:38
ddd	Block	Exact matching	None	2021-12-23 18:59:21
test_block	Block	Exact matching	test_01	2021-12-13 16:36:03
Total items: 3				10 ▼

6. On the **Custom Dictionary** page, select the dictionary just created and click **Manage** in the **Operation** column to enter the dictionary management page.

Text library	Moderation su... ▼	Matching mode ▼	Associated policy	Last modified
fff	Review	Exact matching	None	2021-12-23 18:59:38
ddd	Block	Exact matching	None	2021-12-23 18:59:21
test_block	Block	Exact matching	test_01	2021-12-13 16:36:03
Total items: 3				10 ▼

- On the dictionary management page, click **Add Sample** to pop up the **Add Sample** window.
- In the **Add Sample** pop-up window, select the handling suggestion, enter keywords, and click **OK**.

Add Samples

Moderation suggestion *

Please select a content category ▼

Keyword *

Press 'Enter' key to separate multiple keywords in newlines. Up to 500 keywords can be submit time

1. One keyword per line; up to 100 chars per keyword

2. Paste multiple keywords (up to 500) to add them in a batch

3. You can add up to 2,000 keywords to the library.

OK

Cancel

Parameter description:

Parameter	Description
Handling Suggestion	Violation type that corresponds to the recognition model.

Keyword	Keywords are separated by line breaks, and each keyword can contain up to 20 letters. You can add up to 500 keywords at a time. You can add up to 2,000 keywords in total.
---------	--

Note:

After configuring the custom dictionary, you can associate it with the policy created in [Step 1. Configure a policy](#).

Step 4. Create a VM task

After completing the above steps, you can call the **CreateVideoModerationTask** API to create a video live room recognition task as instructed below:

Make sure that the video meets the [file format requirements](#) of the API.

Enter the input parameters as instructed in the [API documentation](#).

If the task is created successfully, you can use the task query API to query task details, and you can refer to the [example of creating video recognition task](#) for more information on sample response parameters. If task creation fails, the API will return an error code, and you can refer to [Business Error Codes](#) and [Common Error Codes](#) for troubleshooting.

Note:

When connecting to the service, you can use API Explorer for online debugging.

Step 5. Get the VM task result

After creating the video recognition task, you can call the **DescribeTaskDetail** API to query the details of the task as instructed below:

Enter the input parameters as instructed in the [API documentation](#).

If the API call is successful, you will receive the response output from the API, including the task details. You can refer to the [example of viewing task details](#) for more information on sample response parameters.