Image Recognition

Service Overview

Issue 01

Date 2025-11-12

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 What Is Image Recognition?

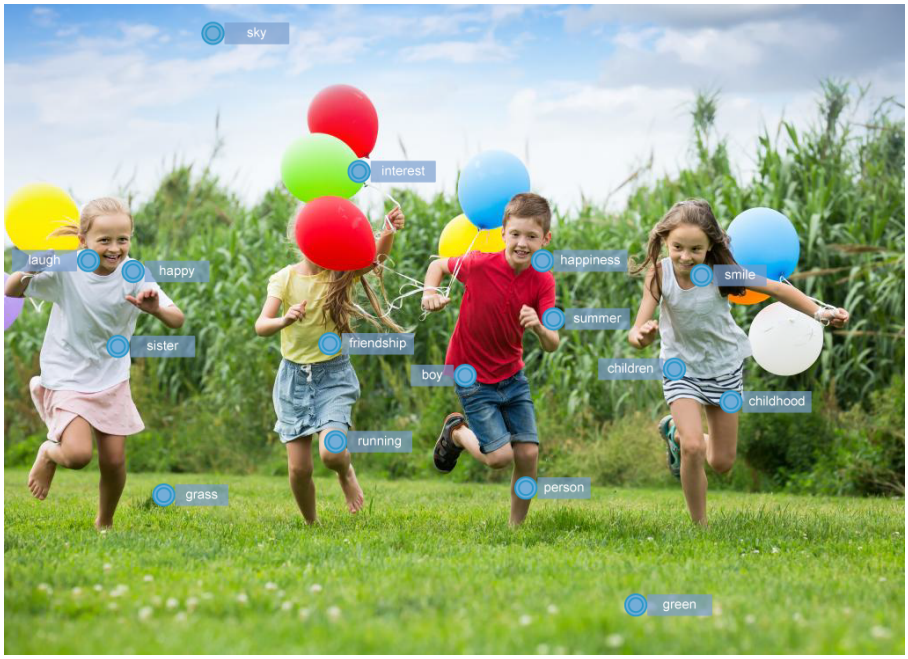
Image Recognition is a technology that uses computers to process, analyze, and understand images to identify objects in different modes, including Image Tagging.

Image Recognition provides services through open Application Programming Interfaces (APIs). You can obtain the inference result by accessing and calling APIs in real time. It helps you collect key data automatically and build an intelligent business system, thereby improving service efficiency.

Image Tagging

Image Tagging can recognize thousands of objects and hundreds of scenario tags in natural images, which have extensive semantic meanings because one image contains a wide variety of tags. It can intelligently and precisely understand image content and make intelligent album management, picture retrieval and classification, and scenario- or object-based advertising more intuitive.

Figure 1-1 Example of Image Tagging



2 Application Scenarios

Image Tagging

Image Tagging can be used in the following scenarios:

- Scenario analysis

  Image Tagging can accurately recognize video and image content, thereby improving retrieval efficiency and precision. It makes personalized recommendation and content retrieval and distribution more effective.

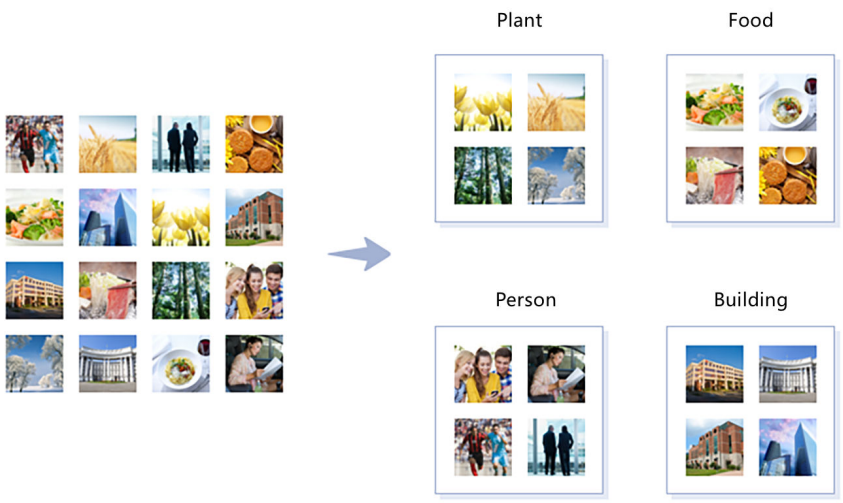
  Figure 2-1 Scenario analysis

- Smart albums

  A maximum of nearly 10,000 image tags can be recognized, such as plant, food, and work. This feature facilitates tag-based album management and improves user experience.

Figure 2-2 Smart album



- Object detection

  On the construction site, the customized object detection system can monitor whether onsite personnel wear the safety helmet in real time, which helps reduce security risks.

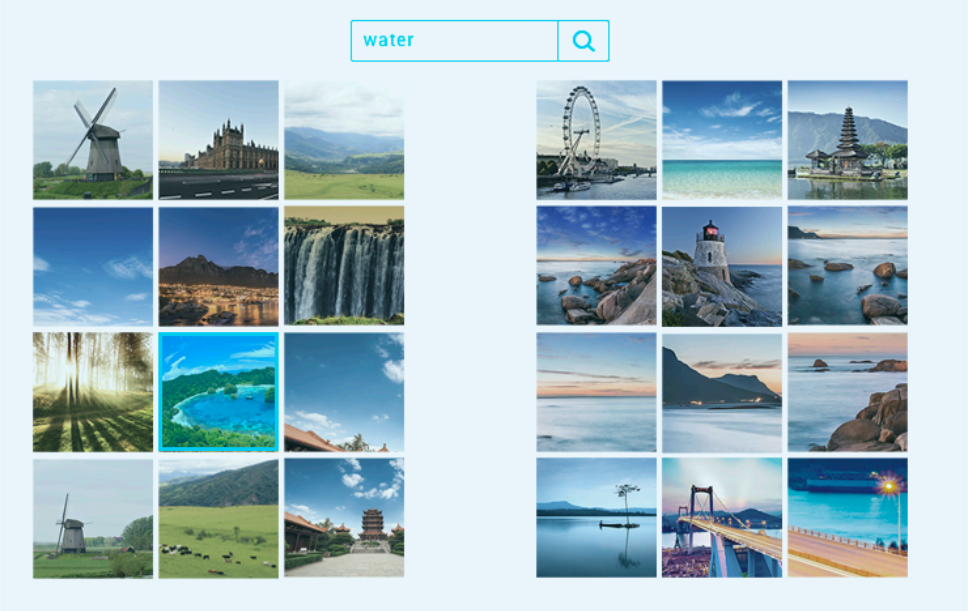
  Figure 2-3 Object detection

- Image search

  The image search technology helps you quickly search for the desired image matching the keyword or image you have entered.

Figure 2-4 Image search



3 Constraints

Before using Image Recognition, you need to read and understand the following constraints.

Image Tagging

- The service is available in the **CN-Hong Kong** region.
- Only images in PNG, JPEG, BMP, or WEBP format can be recognized.
- Each edge of the image must contain 15 to 4,096 pixels.
- The size of the Base64 encoded image cannot exceed 10 MB (the size of the original image cannot exceed 7.5 MB).

4 Related Services

IAM

Identity and Access Management (IAM) provides Image Recognition with the user authentication and authorization function. For more information about IAM, see the *Identity and Access Management User Guide*.

Cloud Eye

Cloud Eye monitors metrics of Image Recognition. You can learn about the service usage with the metrics in a timely manner. For more information about Cloud Eye, see the *Cloud Eye User Guide*.

Table 4-1 Image Recognition metrics

Metric Name	Description	Value Range	Monitoring Period (Raw Metric)
Successful Calls of Image Recognition	Number of successful calls to the service Unit: times/min	≥ 0 times/min	1 min
Failed Calls of Image Recognition	Number of failed calls to the service Unit: times/min	≥ 0 times/min	1 min

OBS

Object Storage Service (OBS) is a stable, secure, efficient, and ease-of-use cloud storage service. Most Image Recognition APIs require data processing. You can use OBS to batch process data to improve data processing efficiency on the cloud. Image Recognition APIs can be temporarily authenticated or anonymously and publicly authorized to obtain data from OBS for processing.

For more information about OBS, see the *Object Storage Service API Reference* and *Object Storage Service Developer Guide*.

5 Using Image Recognition

You can access Image Recognition on a web-based service management platform, that is, the management console, or using HTTPS-based APIs.

- You can subscribe to Image Recognition on the management console and view the number of successful and failed API calls.
- If you access Image Recognition through APIs, you need to integrate Image Recognition to a third-party system.

The procedure is as follows:

Step 1 Apply for a service.

You can apply for a service on the management console. For details about how to apply for a service, see "Applying for a Service" in the *Image Recognition API Reference*.

NOTE

You only need to apply for a service once.

Step 2 Obtain request authentication.

You can use either of the following authentication methods when calling APIs:

- Token authentication: Requests are authenticated using tokens. For details, see Authentication > Token-based Authentication in the *Image Recognition API Reference*.
- AK/SK-based authentication: Requests are encrypted using the access key ID (AK) and secret access key (SK). AK/SK authentication provides higher security. For details, see Authentication > AK/SK-based Authentication in the *Image Recognition API Reference*.

Step 3 Call an API.

Image Recognition delivers services through APIs. For details about how to call Image Recognition APIs, see the *Image Recognition API Reference*.

Step 4 View service usage.

- You can view the total number of API calls on the Image Recognition management console.

----End

6 Metrics

Description

This chapter describes metrics reported by Image Recognition to Cloud Eye as well as their namespaces, list, and dimensions. You can follow the instructions on the Cloud Eye console or use APIs provided by Cloud Eye to query the metrics of Image Recognition.

Namespace

SYS.IRS

Monitoring Metrics

Table 6-1 Monitoring metrics supported by the service

Metric ID	Metric Name	Description	Value Range	Unit	Conversion Rule	Monitored Object (Dimension)	Monitoring Period (Raw Metric)
successful_call_times_of_service	Successful Calls of Image Recognition	Number of successful calls to the service	≥ 0	Times/min	N/A	API	1 min
failed_call_times_of_service	Failed Calls of Image Recognition	Number of failed calls to the service	≥ 0	Times/min	N/A	API	1 min

Dimension

Table 6-2 Dimension description

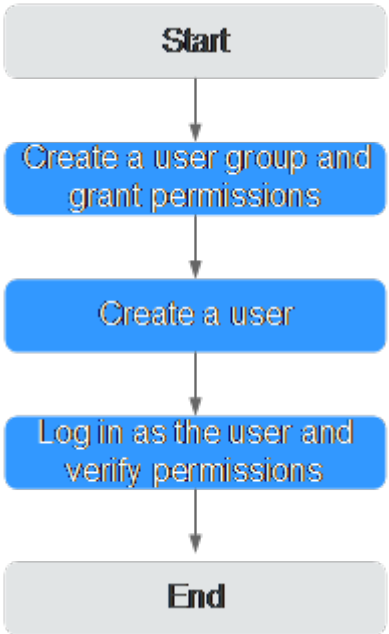
Key	Value
call_of_interface	API

7 (Optional) Authorizing Subaccounts to Use Image Recognition

This section describes how to grant the **Tenant Guest** permission of Image Recognition and the **OBS Buckets Viewer** permission of OBS to a user group, and add users to the user group. In this way, subaccounts have corresponding operation rights. The operation process is shown in **Figure 7-1**.

Authorization Process

Figure 7-1 Process for authorizing subaccounts to use Image Recognition



NOTE

For details about the Tenant Guest permission and how to apply for the permission, see **Permissions Policies** and **Creating a User Group and Assigning Permissions** in the *Identity and Access Management User Guide*.

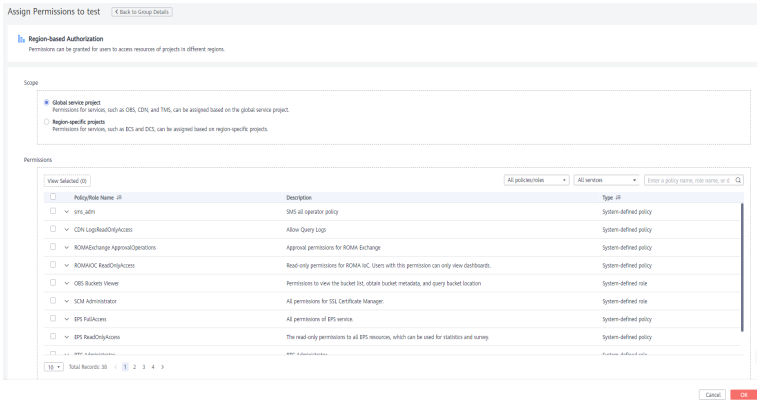
Step 1: Create a User Group and Grant Permissions.

User groups facilitate centralized user management and streamlined permission management. Users in the same user group have the same permissions. Users created in IAM inherit permissions from the groups they belong to. To create a user group and grant it permissions, perform the following steps:

1. Log in to Huawei Cloud using an account.
2. On the management console, mouse over the username on the upper right corner and then choose **Identity and Access Management**.
3. On the IAM console, choose **User Groups** in the navigation pane. Then click **Create User Group**.
4. Enter a user group name, and click **OK**.

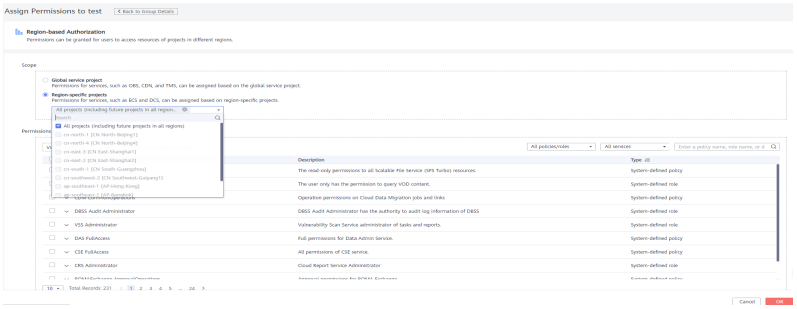
   The user group is displayed in the user group list.
5. In the row of the created user group, click **Manage Permissions** in the **Operation** column. The **Permissions Assigned** tab page is displayed. Click **Assign**. Select **Global service project** for **Scope**. Select **Tenant Guest** and click **OK**. See **Figure 7-2**.

   Figure 7-2 Global service configuration

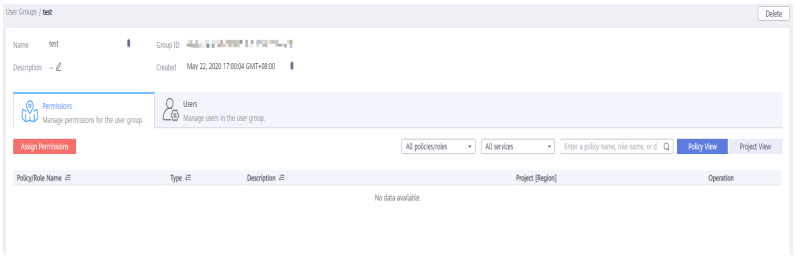
6. In the row of the user group you created, click **Manage Permissions** in the **Operation** column. The **Permissions Assigned** tab page is displayed. Click **Assign**. Set **Scope** to **Region-specific projects** and select **All projects (including future projects in all regions)**. Select **Tenant Guest** and click **OK**. See **Figure 7-3**.

   Figure 7-3 Region-specific service configuration

7. Return to the user group list, click **Manage Permissions** under the **Operation** column in the row that contains the newly created user group. On the **Permissions** tab page, view the configured permissions. See **Figure 7-4**.

Figure 7-4 Permissions Management



Step 2: Create an IAM User

IAM users can be created for employees or applications of an enterprise. Each IAM user has their own security credentials, and inherits permissions from the groups it is a member of. To create an IAM user, perform the following steps:

1. In the navigation pane of the IAM console, choose **Users**. Then click **Create User**.
2. Set user information and click **Next**. For details about the parameters, see **Creating an IAM User**.
3. On the next page, set a password type, an email address, and a mobile number, and click **OK**.
4. Add users to user groups so that the users inherit permissions from the groups to which they belong. For details about how to add users, see **Adding Users to a User Group**.

Step 3: Log In and Verify Permissions

After the user is created, use the username and identity credential to log in to HUAWEI CLOUD, and verify that the user has the permissions.

1. On the HUAWEI CLOUD login page, click **IAM User Login**.
2. Enter the account name, username, and password, and click **Log In**.
   - The account name is the name of the Huawei Cloud account that created the IAM user.
   - The username and password are those set by the account when creating the IAM user.
   - If the login fails, contact the entity owning the account to verify the username and password. Alternatively, you can reset the password.
3. Changes the region. After successful login, switch to a region where the user has been granted permissions on the management console. The default region is CN-Hong Kong.
4. Select **Image Recognition** from **Service List**. If OBS authorization, service enabling, and API calling can be properly performed on the service management page, the authorization has taken effect.

8 Security

8.1 Shared Responsibilities

Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system for different regions and industries based on Huawei's unique software and hardware advantages, laws, regulations, industry standards, and security ecosystem.

Unlike traditional on-premises data centers, cloud computing separates operators from users. This approach not only enhances flexibility and control for users but also greatly reduces their operational workload. For this reason, cloud security cannot be fully ensured by one party. Cloud security requires joint efforts of Huawei Cloud and you, as shown in **Figure 8-1**.

- **Huawei Cloud**: Huawei Cloud is responsible for infrastructure security, including security and compliance, regardless of cloud service categories. The infrastructure consists of physical data centers, which house compute, storage, and network resources, virtualization platforms, and cloud services Huawei Cloud provides for you. In PaaS and SaaS scenarios, Huawei Cloud is responsible for security settings, vulnerability remediation, security controls, and detecting any intrusions into the network where your services or Huawei Cloud components are deployed.
- **Customer**: As our customer, your ownership of and control over your data assets will not be transferred under any cloud service category. Without your explicit authorization, Huawei Cloud will not use or monetize your data, but you are responsible for protecting your data and managing identities and access. This includes ensuring the legal compliance of your data on the cloud, using secure credentials (such as strong passwords and multi-factor authentication), and properly managing those credentials, as well as monitoring and managing content security, looking out for abnormal account behavior, and responding to it, when discovered, in a timely manner.

Figure 8-1 Huawei Cloud shared security responsibility model

Cloud security responsibilities are determined by control, visibility, and availability. When you migrate services to the cloud, assets, such as devices, hardware, software, media, VMs, OSs, and data, are controlled by both you and Huawei Cloud. This means that your responsibilities depend on the cloud services you select. As shown in **Figure 8-1**, customers can select different cloud service types (such as IaaS, PaaS, and SaaS services) based on their service requirements. As control over components varies across different cloud service categories, the responsibilities are shared differently.

- In on-premises scenarios, customers have full control over assets such as hardware, software, and data, so tenants are responsible for the security of all components.
- In IaaS scenarios, customers have control over all components except the underlying infrastructure. So, customers are responsible for securing these components. This includes ensuring the legal compliance of the applications, maintaining development and design security, and managing vulnerability remediation, configuration security, and security controls for related components such as middleware, databases, and operating systems.
- In PaaS scenarios, customers are responsible for the applications they deploy, as well as the security settings and policies of the middleware, database, and network access under their control.
- In SaaS scenarios, customers have control over their content, accounts, and permissions. They need to protect their content, and properly configure and protect their accounts and permissions in compliance with laws and regulations.

9 Billing

Billing Modes

The pay-per-use and yearly/monthly package billing modes are available.

You can use the price calculator provided by Image Recognition to quickly calculate the price for purchasing your desired APIs. For details, see **Image Recognition Pricing Details**.

- **Pay-per-use**

  Image Recognition adopts tiered pricing based on the number of API calls. The tiered API calls are accumulated by calendar month. After a calendar month ends, the API calls are cleared. .

  NOTE

  - An API call is counted only when it is successfully called. Remaining free API calls at the end of the month do not roll over to subsequent months.
  - Billing rule: tiered pricing based on the number of API calls. The tiered API calls are accumulated by calendar month and settled by the end of each month. After a calendar month ends, the API calls are cleared.
  - Billing cycle: hourly. Bills are generally issued within 1 hour after each billing period ends, depending on how fast the system can process them.

- **Yearly/Monthly**

  You can also purchase a discount resource package for a better price. However, if your usage exceeds the package quota, subsequently used resources will be billed on a pay-per-use basis. For more information about pricing, see **Product Pricing Details**. Compared with the pay-per-use mode, this mode provides a larger discount. You can enjoy higher discounts for longer use. Yearly/Monthly packages are recommended for long-term users.

NOTE

- After you determine the required duration and API calls, Image Recognition automatically calculates the fees you need to pay. Packages are paid in full, take effect immediately upon payment, and become unavailable upon expiration. Currently, you cannot specify the date when the package takes effect. For example, if you purchase a one-year discount package on January 1, the package automatically expires on January 1 in the next year. The validity period will not be extended and the fees cannot be refunded even though you have not made any API calls in the year.
- Packages can be subscribed to multiple times and can be used together.
- The fees for API calls can be deducted from the discount package quota only when the API calls are made within the validity period of the discount package. The excess part is billed in pay-per-use mode.

  The fees for API calls beyond the discount package quota are settled in pay-per-use mode according to tiered pricing.

Overdue Payment

In pay-per-use mode, API fees are deducted every hour. If your account balance is insufficient to pay for the expense occurred in the last hour, your account will be in arrears, and APIs have a **grace period and retention period**.

If you top up your account within the retention period, the APIs will be available and billed from the original expiration date.

NOTE

If your account is in arrears, some operations will be restricted. You are advised to top up your account as soon as possible. The restricted operations are as follows:

- API calls purchased in pay-per-use mode cannot be used.
- Remaining API calls in a discount package can still be used, but the package cannot be subscribed again or renewed.
- Services cannot be subscribed.

Renewal

You can renew a resource package upon its expiration, or you can set auto-renewal rules for a resource package. For details about renewal operations, see **Renewal Management**.

Expiration

- After a yearly/monthly package expires, you will be billed for subsequently used resources on a pay-per-use basis.
- If the account is not topped up or the resource package is not renewed before the retention period expires, your data will be deleted and cannot be recovered.

