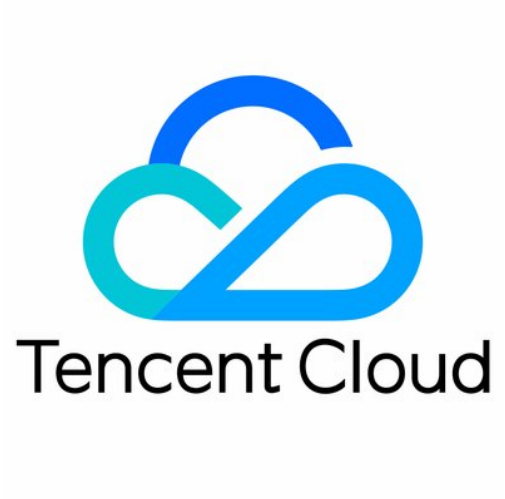
Captcha

FAQs

Product Documentation



Contents

FAQs

Billing

Last updated：2024-12-26 14:11:11

How do I check the fees incurred?

1. Both the client and server sides have completed the necessary code integration. **The earlier version** of the Captcha will be billed based on the number of server-side ticket verifications. **The new version** , 202412 - (TJNCaptcha-global.js), will be billed based on the number of verifications initiated after users respond to a verification query. To view verification frequency trends or the number of ticket verifications, log in to the Captcha console, and in the left sidebar, choose **CAPTCHA** > **CAPTCHA Statistics** .
2. Log in to the console and go to **Cost Center** -> **Bills** -> **Bill Details** to view the details of the generated bills.

I am already using the Captcha service, why are no fees deducted?

Please check whether the client and server have integrated to the Captcha service as required. After TenDI Captcha is integrated into the business client, the business server needs to verify the CAPTCHA ticket. For more information, please see Integration to Ticket Verification (Web and App).

Note:

If ticket verification is not integrated, the black market can easily forge verification results, which defeats the purpose of human verification via CAPTCHAs.

Feature

Last updated：2024-01-02 15:46:48

FAQs about use limits

What is the QPS limit for TenDI Captcha? What is the business impact when the limit is exceeded? Can the limit be changed?

1. **Queries Per Second** (QPS) is limited to 1,000 for ticket verification.
2. When QPS exceeds 1,000 for the ticket verification API calls, **an error is returned** (RequestLimitExceeded).
3. To change the limit, submit a ticket or contact us.

FAQs about features

How does TenDI Captcha block unusual requests?

During the verification, ten security protection mechanisms are used to defend against malicious activities of the black market. For more information, please see "Multi-dimensional defense" in Overview.

Why can't TenDI Captcha effectively block unusual requests?

If you want to block more malicious requests from the black market, you can log in to the Captcha console, select the CAPTCHA to configure, and click **Security configuration**. On the CAPTCHA details page, select the **Security configuration** tab, and change the risk control level to "Strict". Then, TenDI Captcha will block unusual verification requests with stricter risk control policies.

Does TenDI Captcha support multiple languages?

TenDI Captcha supports 23 languages. You can configure the language in the following ways:
1. Log in to the Captcha console, select the CAPTCHA to configure, and click "Appearance configuration". On the CAPTCHA details page, select the **Appearance configuration** tab, and set the prompt language to "Adaptive" (which means the prompt language changes with the browser language).
2. Configure relevant parameters during client integration. For more information, please see Web Client Integration.

Does the prompt language first match the system language or the browser language if it is set as "Adaptive"?

TenDI Captcha matches the browser language first.

Does TenDI Captcha support private deployment?

TenDI Captcha does not support private deployment.

FAQs about usage

Why are users prompted "Too many attempts. Try again later" after they correctly answer the verification questions?

Possible reasons and solutions are as follows:
The user is in an unusual environment and deemed suspicious by the policies. They can wait for 10-20 minutes or change the network environment and try again.
The user is malicious or in a malicious environment and is blocked by the policies. TenDI Captcha ensures secure verification using multi-dimensional policy models consisting of user environments, verification history, and device fingerprints.
Check whether the CaptchaAppId used for the business client integration belongs to a CAPTCHA created by the console. For how to create a valid CaptchaAppId, please see Operation Guide.
If this problem is reported by multiple users, the policies may be too strict. You can log in to the Captcha console, select the CAPTCHA in use, and click **Security configuration**. On the CAPTCHA details page, select the **Security configuration** tab, and change the risk control level to "Loose".

How can I grant permission to sub-accounts to use TenDI Captcha?

1. Log in to the Cloud Access Management console with your primary account, and click **Policies** on the left navigation pane to enter the policy management page.
2. Search for the QcloudCaptchaFullAccess policy, click "Associate User/User Group", select the users/user groups to associate in the "Select Users" box, and click **OK**.

Integration

Last updated：2024-12-23 17:49:12

Non-standard integration issues

What issues will occur if the Captcha JS is not dynamically loaded?

1. Integration method: When the Captcha on Web/App clients is integrated, dynamic loading of JavaScript is not used. Instead, alternative methods are employed to skip the loading process.
2. Security risks: If the above methods are used, CAPTCHAs cannot be updated and consequently some legitimate requests rather than malicious requests might be blocked, and errors might be reported in the frontend.
3. Solution: Dynamically introduce the Captcha JS. For more information, please see Web Integration.

What issues will occur if ticket verification is not integrated?

1. Integration method: The client integrates to Captcha, but the server does not.
2. Security risks: If ticket verification is not integrated, the black market can easily forge verification results, which defeats the purpose of human verification via CAPTCHAs.
3. Solution: Integrate the server to ticket verification. For more information, please see Integration to Ticket Verification (Web and App).

Web and App integration issues

During the test, the prompt "Too many attempts. Try again later." was displayed. How do I resolve this issue?

This is because the Captcha service blocks suspected malicious users. You may have frequently and intensively accessed the Captcha service of the same scenario in the same network environment, resulting in small-scale risk control blocking. Solutions:
Perform the test again after 10-20 minutes.
Change the IP or device and try again.
Log in to the Captcha console, go to the **Security Configuration** page of the verification, and adjust the malicious request blocking level to **Loose**.

Android uses the Web frontend HTML5 method for integration. During the debugging process, a blank background pops up first and then the CAPTCHA page. How do I change that?

During the debugging process, normally, the webview is called first to load the webpage and then the CAPTCHA page pops up.
If the blank background pops up first and then the CAPTCHA page, the reasons are as follows:
The time of loading the Captcha JS results in a white screen.
The page has no content, so the loaded webview is displayed. In this case, it is necessary to display the webview after the ready event is triggered.
Therefore, Android needs to load the page without displaying it, wait for the ready callback, and then display the page after being notified to do so. For ready configuration instructions, see Web Integration - Create Captcha Object.

```
options={ready: function(size){
// Communicate with Android
}}
new TencentCaptcha(appId, callback, options);
```

What should I do when CAPTCHAs are not completely displayed on the app?

CAPTCHAs are displayed in the center based on the width and height of the container. CAPTCHAs may be truncated if the width of the container is too wide, causing the incomplete display of the CAPTCHAs. In this case, you need to adjust the pop-up window. In addition, random loading of other webviews may also cause truncation.

Server Integration Issues

Verifying What Risk Types Are Included in Return Values of the Captcha Ticket API?

EvilBitmap Field Description

EvilBitmap is a decimal int type value that needs to be converted to a binary value for use. Each binary bit represents a major category of risk control interception policy.

Binary Bit	Major Category of Risk Control Interception Policy	Example
0	Second-level dial proxy IP address exception	EvilBitmap returns 34, which is converted to the binary value 100010. The first and fifth binary bits of it are 1, indicating the corresponding risk control interception policies are IP address short-term aggregation exception + Data parameter exception.
1	IP address short-term aggregation exception (multiple verifications in a short time)	
2	CaptchaAppId + IP address short-term aggregation exception (multiple verifications in a short time)	
3	CaptchaAppId + IP address + Device short-term aggregation exception (multiple verifications in a short time)	
4	Traffic feature exception (for example, TCP protocol	

	stack information exception)	
5	Data parameter exception (for example, browser parameter exception)	
6	Honeypot exception (Execute the logic that should not be executed.)	
7	Behavior clustering exception	

DeviceRiskCategory Field Description

Code	Risk Type	Description
101	Comprehensive score risk	-
201	Malicious request risk	Suspected use of tools to initiate malicious requests.
301	Emulator risk	Suspected use of emulators
401	Device tampering risk	Suspected tampering of device hardware information.
501	Suspected black market risk	Suspected use of black and gray market devices.
601	Behavior risk	Suspected use of automated operations.
701	Browser risk	Suspected tampering of browsers.