ALIBABA CLOUD

Alibaba Cloud

Web应用防火墙

Website Protection Settings

Document Version: 20220705

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
⚠ Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	⚠ Danger: Resetting will result in the loss of user configuration data.
🔔 Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	🔔 Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
📢 Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	📢 Notice: If the weight is set to 0, the server no longer receives new requests.
❓ Note	A note indicates supplemental instructions, best practices, tips, and other content.	❓ Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings> Network> Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Overview 06
2.Web security 10
2.1. Configure the protection rules engine feature 10
2.2. Configure the deep learning engine feature 14
2.3. Configure website tamper-proofing 16
2.4. Configure data leakage prevention 18
2.5. Configure the positive security model 22
3.Bot management 25
3.1. Scenario-specific configuration 25
3.1.1. Overview of scenario-specific configuration 25
3.1.2. Configure anti-crawler rules for websites 26
3.1.3. Configure anti-crawler rules for apps 30
3.1.4. Examples of using the scenario-specific configuration fe... 35
3.2. Configure the allowed crawlers function 38
3.3. Set a bot threat intelligence rule 39
3.4. Configure data risk control 42
3.5. Application protection 48
3.5.1. Overview of app protection 48
3.5.2. SDK integration guide (new) 50
3.5.2.1. Integrate the Anti-Bot SDK into Android apps 50
3.5.2.2. Integrate the Anti-Bot SDK into iOS apps 56
3.5.3. SDK integration guide (old) 63
3.5.3.1. Integrate the Anti-Bot SDK into Android application... 63
3.5.3.2. Integrate the Anti-Bot SDK into iOS applications 71
3.5.4. Configure application protection 77
4.Access control and throttling 82

4.1. Configure HTTP flood protection 82

4.2. Configure a blacklist 83

4.3. Configure scan protection 85

4.4. Create a custom protection policy 87

5.Whitelist 92

5.1. Configure a website whitelist 92

5.2. Configure a whitelist for web intrusion prevention 93

5.3. Configure a whitelist for Data Security 96

5.4. Configure a whitelist for Bot Management 97

5.5. Configure a whitelist for Access Control/Throttling 99

6.Fields in match conditions 102

7.Customize protection rule groups 106

8.Enable IPv6 traffic protection 114

9.Best practices for protection settings 116

9.1. Best practices for website protection 116

9.2. Best practices for the protection rules engine 125

9.3. Best practices for preventing HTTP flood attacks 129

9.4. Account security best practices 135

9.5. Best practices for using custom rule groups to provide en... 137

1.Overview

This topic describes the website protection features supported by Web Application Firewall (WAF).

Module	Feature	Description	Enabling method	Reference
Web Security	**RegEx Protection Engine**	The feature protects your websites against common web attacks based on built-in rule groups. The common web attacks include SQL injection, XSS, webshell upload, command injection, backdoor isolation, invalid file requests, path traversing, and common application attacks.	The feature is enabled by default after you add a domain name.	Configure the protection rules engine feature Best practices for the protection rules engine
	Protection Rule Group	The feature allows you to combine protection rules to create a custom rule group and apply the group to specific websites as needed. **Note** You can create a custom rule group for only **RegEx Protection Engine**.	You need to enable it after you add a domain name.	Customize protection rule groups Best practices for using custom rule groups to provide enhanced protection
	Big Data Deep Learning Engine	The feature is based on the deep neural network system of Alibaba Cloud. It classifies all web attack data and normal business data in the cloud and then creates a data model. This way, potential attacks can be blocked in real time.	You need to enable it after you add a domain name.	Configure the deep learning engine feature
	Website Tamper-proofing	The feature helps you lock specific web pages, such as those that contain sensitive information. When a locked web page is requested, the page cached in WAF is returned. This prevents the tampering of the web pages.	You need to enable it after you add a domain name.	Configure website tamper-proofing
	Data Leakage Prevention	The feature filters content, such as abnormal pages and keywords, returned from the servers to websites and masks sensitive information, such as identity card numbers, bank card numbers, phone numbers, and sensitive words. WAF then returns masked information or default error pages to visitors.	You need to enable it after you add a domain name.	Configure data leakage prevention

Module	Feature	Description	Enabling method	Reference
	Positive Security Model	The feature uses Alibaba Cloud machine learning algorithms to automatically analyze the normal network traffic of a website. It then generates security protection policies tailored for the website based on the collected data.	You need to enable it after you add a domain name.	Configure the positive security model
Bot Management	**Allowed Crawlers**	The feature maintains a whitelist for authorized search engines, such as Google, Bing, Baidu, Sogou and Yandex. The crawlers of these search engines are allowed to access specified domain names.	You need to enable it after you add a domain name.	Configure the allowed crawlers function
	Bot Threat Intelligence	The feature provides information about suspicious IP addresses of dialers, on-premises data centers, and malicious scanners based on the powerful computing capabilities of Alibaba Cloud. This feature also maintains a dynamic IP library of malicious crawlers and prevents crawlers from accessing your websites or specific directories.	You need to enable it after you add a domain name.	Set a bot threat intelligence rule
	Data Risk Control	The feature protects crucial website services, such as registrations, logons, campaigns, and forums, against fraud.	You need to enable it after you add a domain name.	Configure data risk control
	App Protection	The feature provides secure connections and anti-bot protection for native applications. This feature also identifies proxies, emulators, and requests with invalid signatures.	You need to enable it after you add a domain name.	Configure application protection
	HTTP Flood Protection	This feature helps you defend against HTTP flood attacks and provides protection policies in different modes.	The feature is enabled by default after you add a domain name.	Configure HTTP flood protection Best practices for preventing HTTP flood attacks

Module	Feature	Description	Enabling method	Reference
Access Control/Throttling	**IP Blacklist**	The feature blocks access requests from specified IP addresses, CIDR blocks, and IP addresses in specified regions.	You need to enable it after you add a domain name.	Configure a blacklist
	Scan Protection	The feature automatically blocks access requests that have specific characteristics. For example, if the source IP address of requests initiates multiple web attacks or targeted directory traversal attacks in a short period of time, WAF automatically blocks the requests. Source IP addresses are also blocked if they are from common scan tools or the Alibaba Cloud malicious IP library.	You need to enable it after you add a domain name.	Configure scan protection
	Custom Protection Policy	The feature allows you to customize ACL rules and configure rate limiting based on precise match conditions.	You need to enable it after you add a domain name.	Create a custom protection policy
Protection Lab	**Account Security**	The feature allows you to monitor user authentication-related interfaces, such as the endpoints used for registration and logon, and to detect events that may pose a threat to user credentials. These threats include credential stuffing, brute-force attacks, spam registration, weak password sniffing, and SMS flood attacks.	You need to enable it after you add a domain name.	Configure account security Account security best practices
	Website Whitelisting	After you configure a rule, requests that match the rule bypass all protection features and are directly forwarded to origin servers.	You need to enable it after you add a domain name.	Configure a website whitelist
	Whitelisting Rules in Web Intrusion Prevention	After you configure a rule, requests that match the rule bypass specified protection features, such as RegEx Protection Engine and Big Data Deep Learning Engine.	You need to enable it after you add a domain name.	Configure a whitelist for web intrusion prevention

Module	Feature	Description	Enabling method	Reference
Whitelists	**Whitelisting Rules in Data Security**	After you configure a rule, requests that match the rule bypass specified protection features, such as website tamper-proofing, data leak prevention, and account security.	You need to enable it after you add a domain name.	Configure a whitelist for Data Security
	Whitelisting Rules in Bot Management	After you configure a rule, requests that match the rule bypass specified protection features, such as bot threat intelligence, data risk control, intelligent algorithm, and application protection.	You need to enable it after you add a domain name.	Configure a whitelist for Bot Management
	Whitelisting Rules in Access Control/Throttling	After you configure a rule, requests that match the rule bypass specified protection features, such as HTTP flood protection, blacklist, scan protection, and custom protection policy.	You need to enable it after you add a domain name.	Configure a whitelist for Access Control/Throttling

2.Web security

2.1. Configure the protection rules engine feature

The protection rules engine feature uses built-in rules and automatically protects websites against common web attacks, such as SQL injections, XSS attacks, webshell uploads, command injections, backdoor isolations, invalid file requests, path traversals, and vulnerability exploits.

Prerequisites

-
-

Context

By default, the protection rules engine feature is enabled. After you add a website to Web Application Firewall (WAF), the feature protects the website.

The Alibaba Cloud security team accumulates a large number of basic protection rules to defend against web attacks. WAF uses these rules to protect your websites against common web attacks. You can specify a group of protection rules that are used by the protection rules engine feature based on your business requirements. WAF provides the following built-in protection rule groups based on the protection effects:

- **Medium rule group**: By default, this rule group is selected.
- **Loose rule group**: If you want to reduce the risk of blocking normal requests, we recommend that you select this rule group.
- **Strict rule group**: If you want WAF to block attacks in a strict way, we recommend that you select this rule group.

You can also create custom protection rule groups. For more information, see Customize protection rule groups.

Intelligent rule hosting

By default, **Intelligent Rule Hosting** is enabled. The intelligent rule hosting feature helps reduce the risk of blocking normal requests by the protection rules engine feature.

The feature automatically learns the pattern of historical traffic of your website by using intelligent algorithms and automatically identifies the protection rules that are not suitable for specific services or interfaces based on Alibaba Cloud threat intelligence. These protection rules may block normal requests or cause false positives for specific services or interfaces. Then, the feature adds the identified protection rules to the whitelist for web intrusion prevention. This helps reduce the risk of blocking normal requests or causing false positives and ensure protection performance. For more information about the whitelist for web intrusion prevention, see Configure the whitelist for web intrusion prevention. After the risk of blocking normal requests or causing false positives is eliminated, the protection rules engine feature automatically deletes the rules that are automatically added to the whitelist.

Procedure

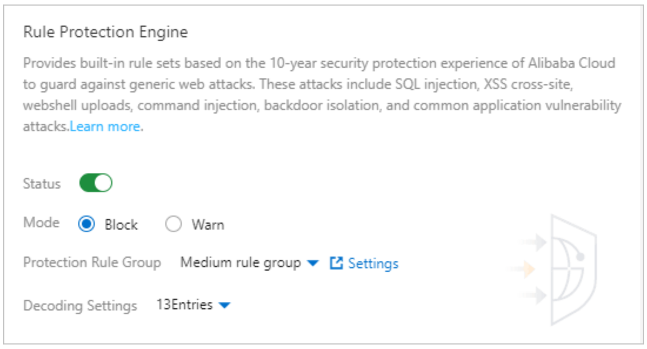
1.

2.

3.

4.

5. Click the **Web Security** tab, find the **Protection Rules Engine** section. The following table describes the parameters.



Rule Protection Engine

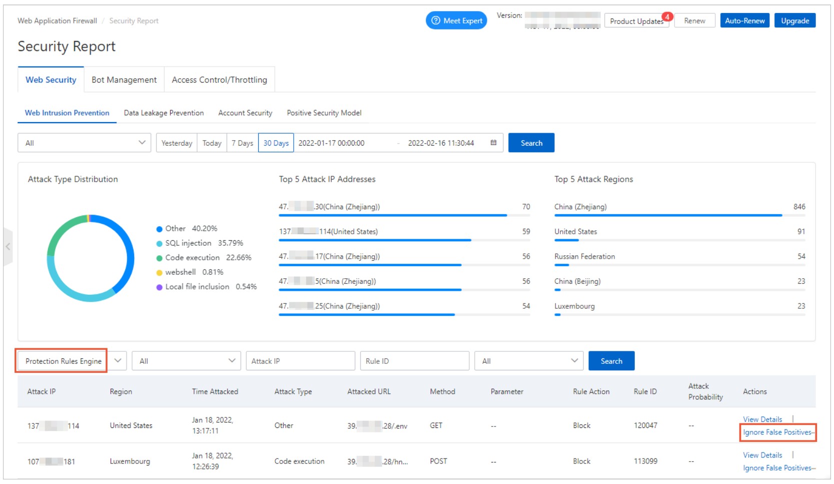
Provides built-in rule sets based on the 10-year security protection experience of Alibaba Cloud to guard against generic web attacks. These attacks include SQL injection, XSS cross-site, webshell uploads, command injection, backdoor isolation, and common application vulnerability attacks.Learn more.

Status

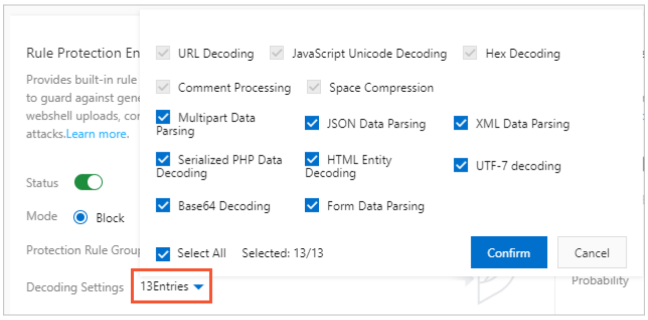
Mode ● Block ○ Warn

Protection Rule Group Medium rule group Settings

Decoding Settings 13Entries

Parameter	Description
Status	The switch that is used to enable or disable the protection rules engine feature. By default, the protection rules engine feature is enabled. The feature helps protect the websites that are added to WAF against common web attacks. To view the attacks blocked by the protection rules engine feature, navigate to **Security Report** and choose **Web Security > Web Intrusion Prevention**. If a normal request is blocked by a rule, find the rule and click **Ignore False Positives** in the Actions column. For more information, see View security reports on the Web Security tab.  Web Application Firewall / Security Report Meet Expert Version: [redacted] Product Updates 4 Renew Auto-Renew Upgrade Security Report Web Security Bot Management Access Control/Throttling Web Intrusion Prevention Data Leakage Prevention Account Security Positive Security Model All Yesterday Today 7 Days 30 Days 2022-01-17 00:00:00 - 2022-02-16 11:30:44 Search Attack Type Distribution: Other 40.20%; SQL injection 35.79%; Code execution 22.66%; webshell 0.81%; Local file inclusion 0.54% Top 5 Attack IP Addresses: 47.[redacted].30(China (Zhejiang)) 70; 137[redacted]114(United States) 59; 47.[redacted]17(China (Zhejiang)) 56; 47.[redacted]5(China (Zhejiang)) 56; 47.[redacted]25(China (Zhejiang)) 54 Top 5 Attack Regions: China (Zhejiang) 846; United States 91; Russian Federation 54; China (Beijing) 23; Luxembourg 23 Protection Rules Engine All Attack IP Rule ID All Search Attack IP | Region | Time Attacked | Attack Type | Attacked URL | Method | Parameter | Rule Action | Rule ID | Attack Probability | Actions 137[redacted]114 | United States | Jan 18, 2022, 13:17:11 | Other | 39.[redacted].28/.env | GET | -- | Block | 120047 | -- | View Details | Ignore False Positives··· 107[redacted]181 | Luxembourg | Jan 18, 2022, 12:26:39 | Code execution | 39.[redacted].28/hn... | POST | -- | Block | 113099 | -- | View Details | Ignore False Positives···
Mode	The action that you want to perform on requests when WAF detects attacks. Valid values: ○ **Block**: blocks requests. ○ **Warn**: triggers alerts but does not block requests.

Parameter	Description
Intelligent Rule Hosting	The switch that is used to enable or disable Intelligent Rule Hosting. By default, the intelligent rule hosting feature is enabled. The feature dynamically manages the whitelist for web intrusion prevention to reduce the risk of blocking normal requests. To view the number of rules that are automatically added to the whitelist, view **A total of xxx rules are optimized** in the **Protection Rules Engine** section. To view the rules, click **Click** to go to the **Web Intrusion Prevention - Whitelisting** page and set the rule source to **Intelligent Rule Hosting**. You can modify or delete the rules that are automatically added to the whitelist. After the risk is eliminated, the rules that are automatically added to the whitelist are deleted, Notice ○ If you modify a rule that is automatically added to the whitelist, the rule is automatically deleted after the risk is eliminated. ○ The rules that you manually add to the whitelist are not automatically deleted after the risk is eliminated.
Protection Rule Group	The protection rule group that you want to use. WAF allows you to create custom rule groups and provides the following built-in rule groups: ○ **Medium rule group**: detects common web application attacks in a standard way. By default, this rule group is used. ○ **Strict rule group**: detects web application attacks, such as path traversals, SQL injections, and command injections, in a strict way. ○ **Loose rule group**: detects common web application attacks in a loose way. If a high false positive rate exists when you apply the medium rule group or a large amount of uncontrollable user input, such as rich text editors and technical forums, is involved in your business, we recommend that you select the loose rule group. You can click **Settings** to go to the **Protection Rule Group** page. On this page, you can create custom rule groups. Then, select rules based on your business requirements. For more information, see Customize protection rule groups.

Parameter	Description
Decoding Settings	The data formats that you want the protection rules engine feature to decode and analyze. By default, the protection rules engine feature decodes and analyzes the request data in all formats. This ensures protection performance. If the protection rules engine feature blocks normal requests that contain data in specific formats, you can clear the formats to reduce the false positive rate. You can select the format that you want to decode or clear the format that you do not want to decode in the **Decode Settings** drop-down list. **Notice** You cannot clear the following formats: **URL Decoding**, **JavaScript Unicode Decoding**, **Hex Decoding**, **Comment Processing**, and **Space Compression**. Rule Protection En Provides built-in rule to guard against gene webshell uploads, cor attacks.Learn more. Status ● Mode ● Block Protection Rule Grou Decoding Settings 13Entries ▾ ☑ URL Decoding ☑ JavaScript Unicode Decoding ☑ Hex Decoding ☑ Comment Processing ☑ Space Compression ☑ Multipart Data Parsing ☑ JSON Data Parsing ☑ XML Data Parsing ☑ Serialized PHP Data Decoding ☑ HTML Entity Decoding ☑ UTF-7 decoding ☑ Base64 Decoding ☑ Form Data Parsing ☑ Select All Selected: 13/13 Confirm Cancel Probability

Query protection rules

You can use the following methods to query the latest protection rules that are added for the protection rules engine feature and query all protection rules that are included in the protection rules engine feature:

- Query the latest protection rules

  Log on to the . Go to the **Overview** page, find the **Vulnerabilities** section, and then click items in the section to view the latest protection rules.

  The **Vulnerabilities** section displays the updated protection rules that are provided by WAF to help you handle the latest security vulnerabilities disclosed on the Internet.

  You can click a rule to open the **Details of Emergency Vulnerability** panel. The panel displays the domain names that are affected by the vulnerability, the details of the vulnerability, and the information about protection rules.

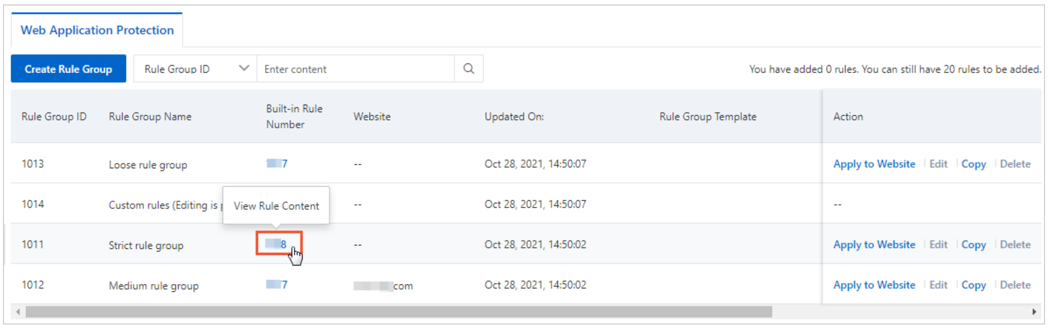
- Query all protection rules

  Log on to the . In the left-side navigation pane, choose **System Management > Protection Rule Group** and view all protection rules that are included in the protection rules engine feature.

  i. On the **Web Application Protection** tab, find **Strict rule group** and click the number in the **Built-in Rule Number** column.

     The strict rule group is a built-in rule group. The group contains all protection rules of the protection rules engine feature and cannot be modified.

> **Note** The number of protection rules of the protection rules engine feature dynamically changes. The number of protection rules that are displayed in the WAF console may be different from the number shown in the following figure.

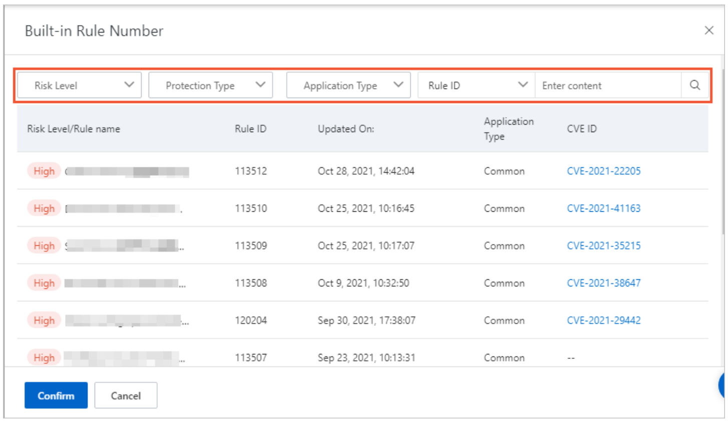


You have added 0 rules. You can still have 20 rules to be added.

Rule Group ID	Rule Group Name	Built-in Rule Number	Website	Updated On:	Rule Group Template	Action
1013	Loose rule group	[redacted]7	--	Oct 28, 2021, 14:50:07		Apply to Website | Edit | Copy | Delete
1014	Custom rules (Editing is		--	Oct 28, 2021, 14:50:07		--
1011	Strict rule group	[redacted]8	--	Oct 28, 2021, 14:50:02		Apply to Website | Edit | Copy | Delete
1012	Medium rule group	[redacted]7	[redacted]com	Oct 28, 2021, 14:50:02		Apply to Website | Edit | Copy | Delete

ii. In the **Built-in Rule Number** panel, query the protection rules that you want to view.

You can configure **Risk Level**, **Protection Type**, and **Application Type** to filter protection rules. You can also use **Rule ID** or **CVEID** to query a protection rule. You can obtain a rule ID on the **Overview** or **Security Report** page.



Risk Level/Rule name	Rule ID	Updated On:	Application Type	CVE ID
High [redacted]	113512	Oct 28, 2021, 14:42:04	Common	CVE-2021-22205
High [redacted]	113510	Oct 25, 2021, 10:16:45	Common	CVE-2021-41163
High [redacted]	113509	Oct 25, 2021, 10:17:07	Common	CVE-2021-35215
High [redacted]	113508	Oct 9, 2021, 10:32:50	Common	CVE-2021-38647
High [redacted]	120204	Sep 30, 2021, 17:38:07	Common	CVE-2021-29442
High [redacted]	113507	Sep 23, 2021, 10:13:31	Common	--

The rule list displays the following information: **Risk Level/Rule name**, **Rule ID**, **Updated On**, **Application Type**, **CVE ID**, **Protection Type**, and **Description**.

You can click a CVE ID to view the details about the vulnerability.

Related information

- Best practices for the protection rules engine
- Customize protection rule groups

2.2. Configure the deep learning engine feature

After you add a website to Web Application Firewall (WAF), you can enable the deep learning engine feature for your website. The deep learning engine is developed based on the deep neural network system of Alibaba Cloud. The feature performs classification training on all web attack data and normal business data in the cloud. This way, potential attacks can be blocked in real time.

Prerequisites

- A WAF instance is purchased. The instance must reside in the **Chinese mainland** and run the **Business** edition or higher.

  For more information, see Purchase a WAF instance.

-

Background information

Web attack methods keep evolving as the Internet develops. Traditional single-method protection no longer meets the security requirements of complex Internet services. Collaborative protection that uses multiple detection engines is more effective.

Based on massive operations data of Alibaba Cloud, the deep learning engine trains models for normal web applications and identifies abnormalities in these models. The engine also refines attack models from various web application attacks. The deep learning engine uses these models to detect zero-day vulnerabilities. When WAF is used to prevent web attacks, protected traffic is forwarded to the protection rules engine. Then, the traffic is forwarded to the deep learning engine. The two engines complement each other.

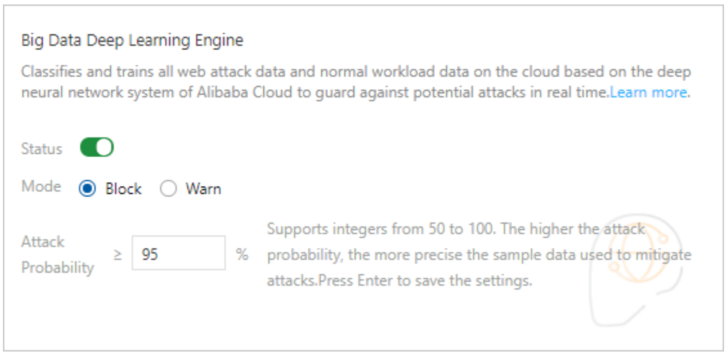
Scenarios

The deep learning engine scans for web requests that have weak attack characteristics rather than HTTP flood attacks. If you have more precise requirements on web attack protection, we recommend that you enable the deep learning engine.

The protection rules engine uses strong regular expression rules. The engine provides optimal protection against requests that have strong attack characteristics. The protection rules engine may fail to detect risks from requests that have weak attack characteristics, such as cross-site scripting (XSS) attacks. The engine may also fail to detect these attacks even in strict mode. In this case, you can enable the deep learning engine to identify and block requests that have weak attack characteristics and cannot be detected based on strict rules of the protection rules engine.

Procedure

1.
2.
3.
4.
5. Click the **Web Security** tab, find the **Deep Learning Engine** section, and configure following parameters.



Big Data Deep Learning Engine

Classifies and trains all web attack data and normal workload data on the cloud based on the deep neural network system of Alibaba Cloud to guard against potential attacks in real time.Learn more.

Status: enabled

Mode: ● Block ○ Warn

Attack Probability ≥ 95 %

Supports integers from 50 to 100. The higher the attack probability, the more precise the sample data used to mitigate attacks.Press Enter to save the settings.

Parameter	Description
Status	The switch that is used to enable or disable the deep learning engine. ⓘ **Note** After the deep learning engine is enabled, all requests that are destined for your website are checked by the engine. You can configure the whitelist in the Web Intrusion Prevention section. Then, the requests that match the rules specified in the whitelist can bypass the check. For more information, see Configure a whitelist for web intrusion prevention.
Mode	The action that you want to perform on requests when WAF detects attack requests. Valid values: ○ **Block**: blocks requests. ○ **Warn**: triggers alerts but does not block requests.
Attack Probability	The threshold value of the probability that a request is identified as an attack when the deep learning engine is used. The value is an integer within the range of 50 to 100. If the parameter value is large, the standard for determining that a request is an attack is strict, and the deep learning engine blocks real attacks in a more accurate manner. The engine may not block other risks. If the parameter value is small, the standard for determining that a request is an attack is not strict, and the deep learning engine blocks more suspicious requests. However, the engine may also block normal requests.

What's next

After you enable the deep learning engine, you can view the records of matched rules of the deep learning engine. To view the records, click **Security Report** and choose **Web Security** > **Web Intrusion Prevention**. For more information, see View Security Reports.

2.3. Configure website tamper-proofing

After you add a website to Web Application Firewall (WAF), you can enable the website tamper-proofing feature for the website. The feature helps you lock web pages that require protection, such as web pages that contain sensitive information. When a locked web page is requested, the page that is cached in WAF is returned. This way, malicious modification of web pages is prevented.

Prerequisites

- A WAF instance is purchased.

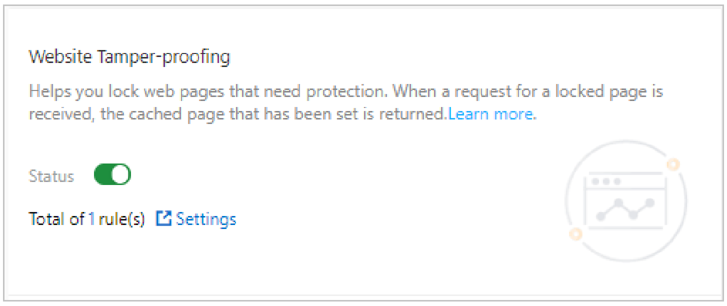
  For more information, see Purchase a WAF instance.

-

Procedure

1.
2.
3.
4.
5. Click the **Web Security** tab and find the **Website Tamper-proofing** section. Then, turn on **Status** and click **Settings**.

   > **Notice** After the website tamper-proofing feature is enabled, all requests that are destined for your website are checked by the feature. You can configure a data security rule. This way, the requests that meet the specified conditions in the rule can bypass the check. For more information, see Configure a whitelist for Data Security.

   Website Tamper-proofing

   Helps you lock web pages that need protection. When a request for a locked page is received, the cached page that has been set is returned.Learn more.

   Status

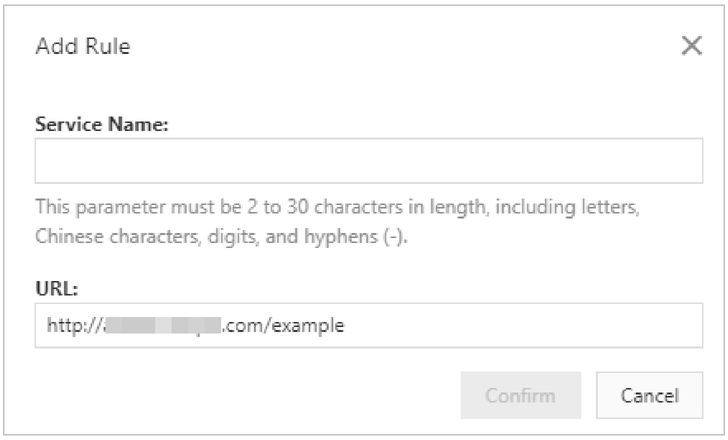
   Total of 1 rule(s) Settings

6. Create a website tamper-proofing rule.

   i. On the **Website Tamper-proofing** page, click **Add Rule**.

   ii. In the **Create Rule** dialog box, configure the **Service Name** and **URL** parameters for the web page that you want to protect.

   - **Service Name**: Specify the name of the service that is provided on the web page.
   - **URL**: Specify the exact path of the web page. The path must start with `http://` or `https://`. Wildcard characters or parameters are not supported. For example, you cannot specify `/*` or `/abc? xxx=`. The feature protects text data, HTML pages, and images in the specified path.

   Add Rule

   Service Name:

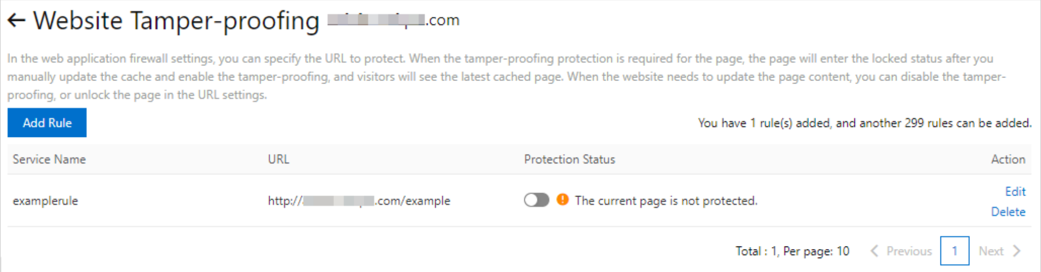
   This parameter must be 2 to 30 characters in length, including letters, Chinese characters, digits, and hyphens (-).

   URL:

   http://[redacted].com/example

   iii. Click **Confirm**.

By default, the rule is disabled after a website tamper-proofing rule is created. You can view the website tamper-proofing rule that you created in the rule list. The **Protection Status** switch of the rule is turned off.



← Website Tamper-proofing [redacted].com

In the web application firewall settings, you can specify the URL to protect. When the tamper-proofing protection is required for the page, the page will enter the locked status after you manually update the cache and enable the tamper-proofing, and visitors will see the latest cached page. When the website needs to update the page content, you can disable the tamper-proofing, or unlock the page in the URL settings.

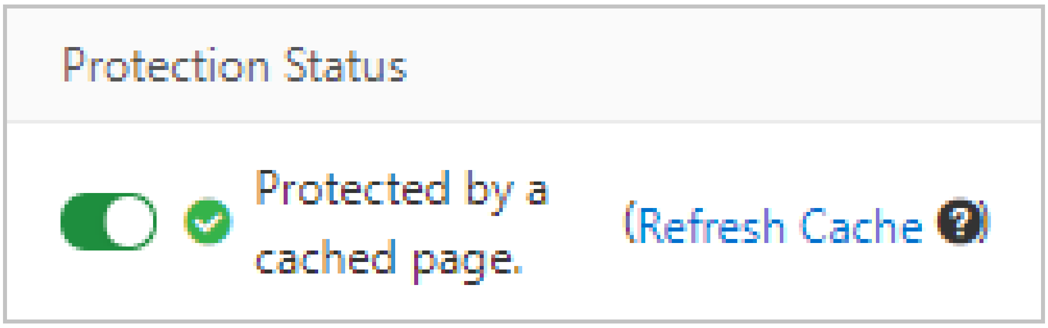
Add Rule

You have 1 rule(s) added, and another 299 rules can be added.

Service Name	URL	Protection Status	Action
examplerule	http://[redacted].com/example	The current page is not protected.	Edit Delete

Total : 1, Per page: 10 < Previous 1 Next >

7. Enable the rule. Find the rule that you want to enable in the rule list and turn on **Protection Status**.



   If you request the specified web page after you enable the rule, the page that is cached in WAF is returned.

8. (Optional)Update cached data. Find the rule that is enabled in the rule list and click **Refresh Cache** in the **Protection Status** column.

   > Notice If a protected web page is updated, click **Refresh Cache** to update the data that is cached in WAF. If you do not update the cached data when the protected page is updated, WAF returns the most recent page that is stored in the cache.

2.4. Configure data leakage prevention

After you add a website to Web Application Firewall (WAF), you can enable the data leakage prevention feature for the website. The feature filters content such as abnormal pages and keywords returned from servers, and masks sensitive information such as ID card numbers, phone numbers, bank card numbers, and sensitive words. WAF then returns the masked information or default response pages.

> Notice The data leakage prevention feature can process only data that is in the formats that are used in the Chinese mainland. The data includes ID card numbers, phone numbers, and bank card numbers.

Prerequisites

- A WAF instance is purchased. The instance meets the following requirements:
  - If the instance resides in the **Chinese mainland**, the instance must run the **Pro** edition or higher.

- If the instance resides **outside the Chinese mainland**, the instance must run the **Business** edition or higher.

  For more information, see Purchase a WAF instance.

-

Background information

WAF supports the data leakage prevention feature to comply with the following regulations required by the Cybersecurity Law of the People's Republic of China: Network operators shall adopt technological and other necessary measures to ensure the security of the personal information they collect, and prevent information leaks, damage or loss. In scenarios in which information leak, damage, or loss occurs, the network operators must take remedial measures at the earliest opportunity, notify users in a timely manner, and report the matter to the authority in compliance with the regulations. The data leakage prevention feature masks sensitive information such as phone numbers, ID card numbers, and bank card numbers in website content and triggers alerts when sensitive information is detected. You can also use the feature to block responses that contain a specific HTTP status code.

Features

Information maintained by a website may be leaked in the following scenarios: unauthorized access to a URL, such as unauthorized access to the backend management system, horizontal and vertical privilege escalation, and malicious crawlers that retrieve sensitive information from web pages. To prevent leaks of common sensitive information, the data leakage prevention feature provides the following capabilities:

- Detects and identifies personal information on web pages, masks the information, and triggers alerts to protect website data. Personal information includes but is not limited to ID card numbers, phone numbers, and bank card numbers.

  > **Notice** The data leakage prevention feature can process only data that is in the formats that are used in the Chinese mainland. The data includes ID card numbers, phone numbers, and bank card numbers.

- Masks sensitive server information, including web applications used by the website, the operating system, and the version of the server.
- Maintains a library that contains banned and sensitive keywords to detect and mask banned or sensitive website content, and trigger alerts.

How the data leakage prevention feature works

The feature detects whether a web page contains sensitive information, such as ID card numbers, phone numbers, and bank card numbers, based on the specified protection rules. If a rule is matched, WAF triggers alerts or masks the information based on the specified rule. The feature masks sensitive information by using asterisks (*).

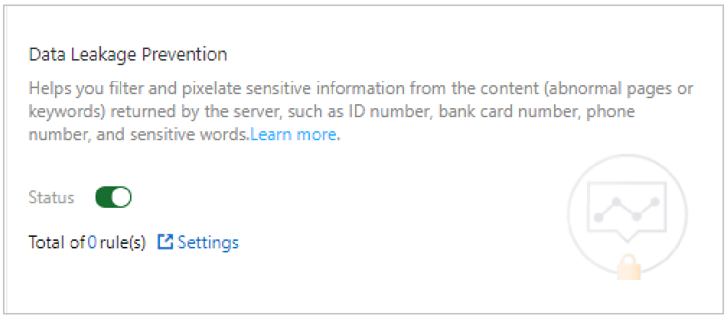
The feature allows you to set Content-Type to `text/*`, `image/*`, or `application/*` to protect web applications, native applications, and APIs.

Procedure

1.
2.
3.

4.
5. Click the **Web Security** tab and find the **Anti Sensitive Information Leakage** section. Then, turn on **Status** and click **Settings**.

> Notice
>
> - Before you configure protection rules, enable the data leakage prevention feature.
> - After the data leakage prevention feature is enabled, the feature checks all requests that are destined for your website. To allow the requests that match a whitelist rule to pass the check, you can configure the whitelist rule for Data Security. For more information, see Configure a whitelist for Data Security.



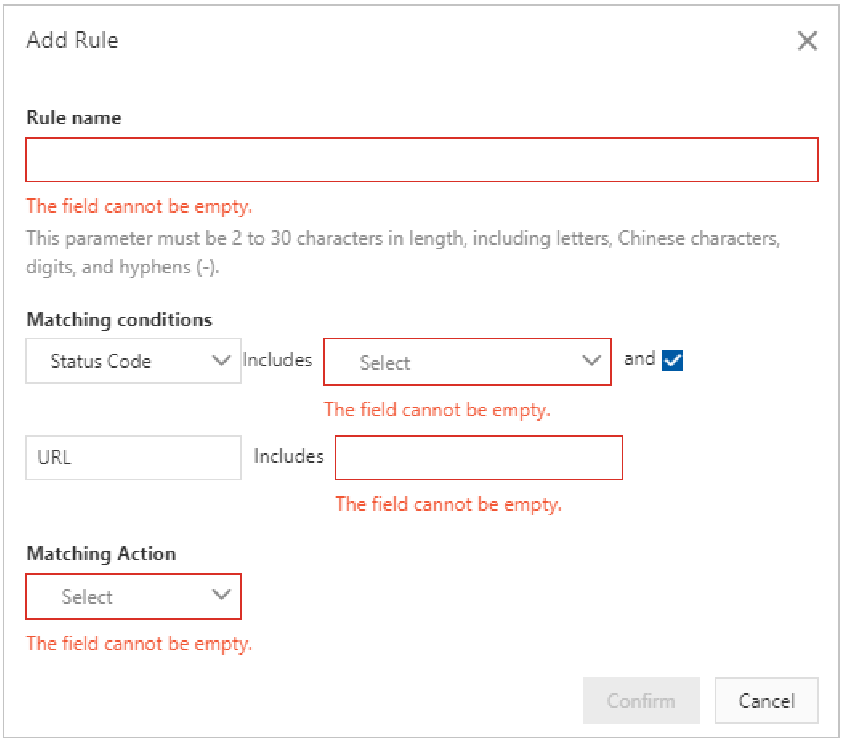
Data Leakage Prevention

Helps you filter and pixelate sensitive information from the content (abnormal pages or keywords) returned by the server, such as ID number, bank card number, phone number, and sensitive words.Learn more.

Status

Total of 0 rule(s) Settings

6. Create a data leakage prevention rule.
   1. On the **Anti Sensitive Information Leakage** page, click **Add Rule**.
   2. In the **Create Rule** dialog box, configure the following parameters.



Add Rule

Rule name

The field cannot be empty.

This parameter must be 2 to 30 characters in length, including letters, Chinese characters, digits, and hyphens (-).

Matching conditions

Status Code Includes Select and ☑

The field cannot be empty.

URL Includes

The field cannot be empty.

Matching Action

Select

The field cannot be empty.

Parameter	Description
Rule name	The name of the rule that you want to create.

Parameter	Description
Matching conditions	The types of information that you want to detect. Select a value from the drop-down list. Valid values: - **Status Code**: 400, 401, 402, 403, 404, 500, 501, 502, 503, 504, 405-499, and 505-599 - **Sensitive Info**: **ID Card**, **Credit Card**, **Telephone No.**, and **Default Sensitive Word** **Notice** The data leakage prevention feature can process only data that is in the formats that are used in the Chinese mainland. The data includes ID card numbers, phone numbers, and bank card numbers. You can select multiple values for Status Code and Sensitive Info. If you select **and**, you can specify the **URL** that you want to check. This way, WAF scans for sensitive information only on the specified page.
Matching Action	The action that you want to perform on the sensitive information that is detected. - If you set the match condition to **Status Code**, the following actions are supported: - **Warn**: triggers alerts when sensitive information is detected. - **Block**: blocks requests and returns the default page. This indicates that the requested website is blocked. - If you set the match condition to **Sensitive Info**, the following actions are supported: - **Warn**: triggers alerts when sensitive information is detected. - **Sensitive information filtering**: masks sensitive information in responses.

Sample configurations

- Mask sensitive information: Web pages may contain sensitive information, such as phone numbers and ID card numbers. You can create rules to mask sensitive information or trigger alerts when sensitive information is detected. The following example shows how to create a rule that masks phone numbers and ID card numbers.
    - Matching conditions: ID Card and Telephone No.
    - Matching Action: Sensitive information filtering

  After this rule takes effect, all phone numbers and ID card numbers on the website are masked.

  > **Notice** Phone numbers that must be provided to the public for business affairs, such as customer service and product hotlines, may also be masked by data leakage prevention rules.

- Block responses that contain specific HTTP status codes: You can create a rule to block or generate alerts when specific HTTP status codes are detected to prevent leaks of sensitive server information. The following example shows how to create a rule that blocks the HTTP 404 status code.
    - Matching conditions: 404
    - Matching Action: Block

  After this rule takes effect, if the requested page does not exist, the specified page that indicates that the requested website is blocked is returned.

- Mask specific sensitive information on specific pages: You can create rules to mask sensitive information or generate alerts when specific sensitive information, such as phone numbers or ID card numbers, is detected on specific pages. The following example shows how to create a rule that masks ID card numbers on the pages whose URLs contain `admin.php`.
    - Matching conditions: ID card numbers on pages whose URLs contain `admin.php`
    - Matching Action: Sensitive information filtering

  After this rule takes effect, the ID card numbers on the pages whose URLs contain admin.php are masked.

iii. Click **Confirm**.
After you create a data leakage prevention rule, the rule automatically takes effect. You can view new rules, and modify or delete rules in the rule list based on your business requirements.

What's next

After you enable the data leakage prevention feature, you can view the log data of the filtered or blocked requests that match data leakage prevention rules. To view the log data, go to the **Security Report** page, choose **Web Security** > **Data Leakage Prevention**, and view the relevant security report. For more information, see View Security Reports.

2.5. Configure the positive security model

After you add a website to Web Application Firewall (WAF), you can enable the positive security model for your website. The positive security model uses the machine learning algorithms developed by Alibaba Cloud to automatically learn the normal traffic of a website. The positive security model then generates custom protection rules for the website based on the learning results.

Prerequisites

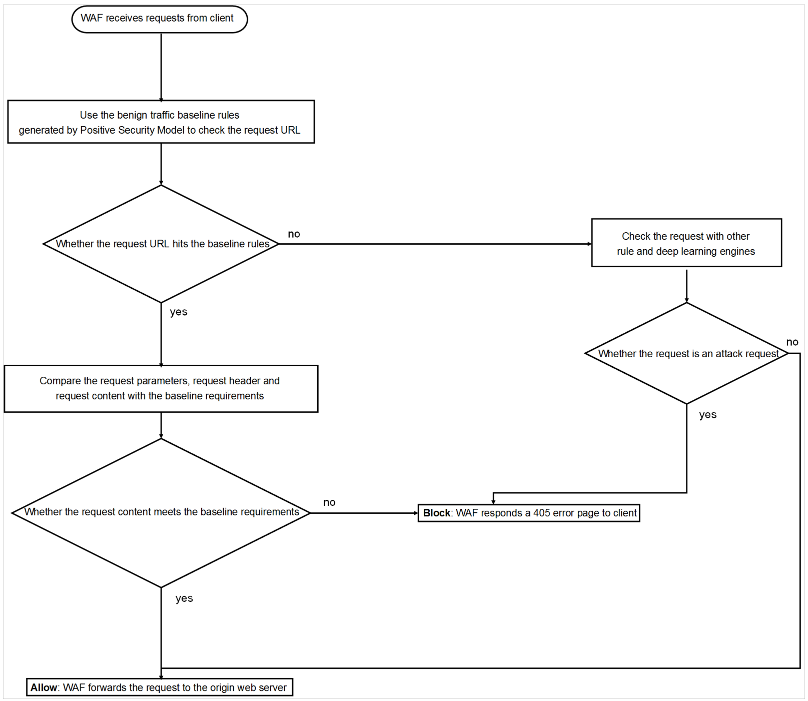
- A WAF instance is purchased. The instance runs the **Enterprise** edition or higher.

  For more information, see Purchase a WAF instance.

-

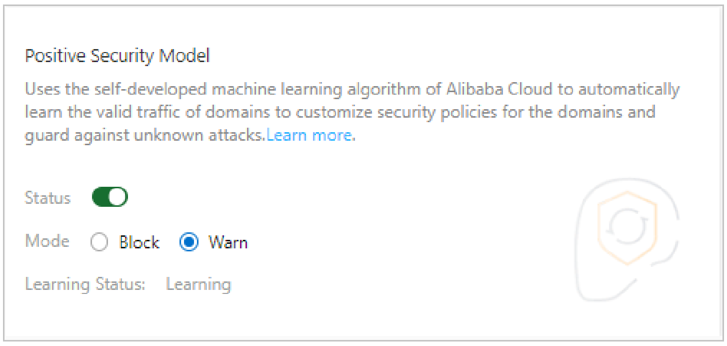
Background information

Traditional protection methods protect websites from attacks based on detection rules. The positive security model uses unsupervised learning to automatically learn the traffic of a website. Then, the positive security model uses the model built by machine learning algorithms to generate a standard security score and grade different requests. Based on the request scores, the positive security model defines the baseline traffic of the website and generates custom protection rules for the website. The positive security model collaborates with other protection modules of WAF to defend against attacks at different network layers.


WAF receives requests from client
Use the benign traffic baseline rules generated by Positive Security Model to check the request URL
Whether the request URL hits the baseline rules
no
Check the request with other rule and deep learning engines
yes
Whether the request is an attack request
no
Compare the request parameters, request header and request content with the baseline requirements
yes
Whether the request content meets the baseline requirements
no
Block: WAF responds a 405 error page to client
yes
Allow: WAF forwards the request to the origin web server

Procedure

1.
2.
3.
4.
5. On the **Web Security** tab, find the **Positive Security Model** section and configure the following parameters.



Positive Security Model

Uses the self-developed machine learning algorithm of Alibaba Cloud to automatically learn the valid traffic of domains to customize security policies for the domains and guard against unknown attacks.Learn more.

Status ●

Mode ○ Block ● Warn

Learning Status: Learning

Parameter	Description
Status	The switch that is used to enable or disable the positive security model.
Mode	The action that you want to perform on requests when WAF detects attacks. Valid values: ○ **Warn**: triggers alerts but does not block requests. ○ **Block**: blocks requests. **Note** By default, the positive security model is set to the Warn mode. In this mode, WAF reports the requests that match the protection rules but do not block the requests. Before you set the mode to Block, we recommend that you study the data in security reports and make sure that the protection rules do not cause false positives.

If this is the first time that you enable the positive security model for a website, WAF uses the model built by machine learning algorithms to automatically learn the historical traffic of the website. Then, WAF generates custom protection rules based on the learning results to protect the website. The time that is required to initially learn traffic varies based on the total amount of traffic. In most cases, WAF initially learns the traffic of a website and generates protection rules within about one hour. After WAF completes the learning process, WAF sends you a notification by using internal messages, text messages, or emails.

Notice If you disable the positive security model, the traffic learning results that are generated become invalid. If you enable the positive security model again, the positive security model needs to learn the traffic of your website again. If you upgrade your WAF instance, the learning results of the positive security model are not affected. If the traffic pattern of your website that is added to WAF changes, the learning results can no longer be used. We recommend that you configure the positive security model to learn the traffic of your website again. The traffic pattern change includes the change of the service type of your website.

3.Bot management

3.1. Scenario-specific configuration

3.1.1. Overview of scenario-specific configuration

The bot management module of Web Application Firewall (WAF) provides the scenario-specific configuration feature to protect your business from malicious crawlers. You can configure custom anti-crawler rules based on your business requirements.

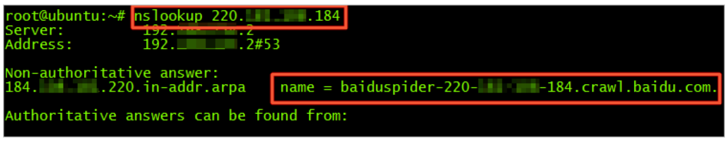
Background information

Malicious crawlers come in various types. Crawling methods keep changing to bypass anti-crawler rules that are configured by website administrators. Therefore, fixed rules cannot block all malicious crawlers. The methods that are used to block malicious crawlers vary based on your business requirements. Security experts are also required to deliver optimal protection.

If you need strong protection against malicious crawlers or have no security experts to configure anti-crawler rules, we recommend that you use the scenario-specific configuration feature that is provided by WAF. WAF provides IP address libraries of malicious crawlers and updates the IP address libraries of various public clouds and data centers in real time based on network-wide threat intelligence of Alibaba Cloud. This way, normal crawler requests are allowed and malicious crawler requests from the addresses in the IP address libraries are blocked.

Risks and characteristics of malicious crawlers

Normal crawler requests contain the `xxspider` keyword in the User-Agent field and have the following characteristics: low request rate, scattered URLs, and wide time range. To obtain the source IP address that initiates a crawler request, run a reverse `nslookup` or `tracert` command on the crawler request. For example, if you run the reverse nslookup command with the IP address of the Baidu crawler, you can obtain the source IP address of the crawler.



```
root@ubuntu:~# nslookup 220.[redacted].184
Server:         192.[redacted].2
Address:        192.[redacted].2#53

Non-authoritative answer:
184.[redacted].220.in-addr.arpa    name = baiduspider-220-[redacted]-184.crawl.baidu.com.

Authoritative answers can be found from:
```

Malicious crawlers may send a large number of requests to a specific URL or port of a domain name during a specific period of time. For example, HTTP flood attacks are disguised as crawlers or as requests from third parties to crawl sensitive information. A large number of malicious requests can cause increased CPU utilization, website access failures, and service interruptions.

Prerequisites

A WAF instance that runs Pro Edition or higher is purchased, and the bot management module is enabled.

References

Configure anti-crawler rules for websites

Configure anti-crawler rules for apps

Examples of using the scenario-specific configuration feature

3.1.2. Configure anti-crawler rules for websites

The bot management module of provides the scenario-specific configuration feature. This feature allows you to configure anti-crawler rules based on your business requirements and helps protect your business from malicious crawlers. This topic describes how to configure anti-crawler rules for websites.

Background information

The scenario-specific configuration feature allows you to configure anti-crawler rules based on your business requirements. You can use this feature together with intelligent algorithms to identify crawler traffic in a more precise manner. The feature can also automatically handle the crawler traffic that matches the configured anti-crawler rules. After you configure anti-crawler rules, you can verify the rules in a test environment. This prevents adverse effects on your websites or apps caused by inappropriate rule configurations or compatibility issues. The adverse effects include false positives and undesired protection results.

Prerequisites

- Subscription WAF instance: If your WAF instance runs the Pro, Business, or Enterprise edition, the **Bot Management** module is enabled. For more information, see Purchase a WAF instance.
-

Procedure

1.
2.
3.
4.
5. If you have not created an anti-crawler rule, click the **Bot Management** tab. In the **Scenario-specific Configuration** section, click **Start** to create an anti-crawler rule. If you have created an anti-crawler rule, click **Add** in the upper-right corner of the **Bot Management** tab to create an anti-crawler rule.

   Note You can create up to 50 **anti-crawler rules** for a domain name.

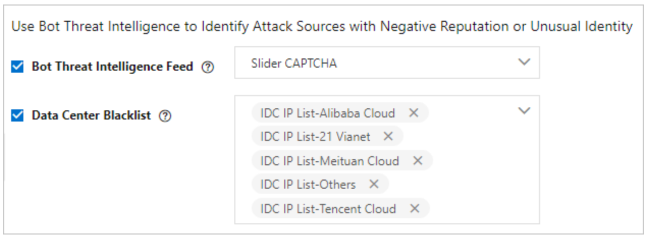
6. In the **Configure Scenarios** step, configure the basic information about the website that you want to protect and click **Next**.

Parameter	Description
Scenario	Specify the type of service scenarios in which you want to protect the domain name. Examples: logon, registration, and order placement.
Service Type	Select **Websites**. This way, WAF protects web pages and HTML5 pages. HTML5 apps are also protected. If the domain name of the website that you want to protect is accessed from a different domain name, you must select **Use Intermediate Domain Name**. Then, select the intermediate domain name from the drop-down list.

Parameter	Description
Traffic Characteristics	Add match conditions to identify traffic destined for the domain name of the website that you want to protect. To add a condition, you must specify the matching field, logical operator, and matching content. The matching field is a header field of HTTP requests. For more information about the matching fields, see Fields in match conditions. You can add up to five match conditions. **Notice** After you enter an IP address, you must press Enter.

7. In the **Configure Protection Rules** step, configure detailed settings for the anti-crawler rule and click **Next**.

Parameter	Description
Script-based Bot Block	If you turn on this switch, WAF performs JavaScript validation on clients. The traffic from non-browser tools that cannot run JavaScript code is blocked. This way, simple script-based attacks are blocked.
Dynamic Token Challenge	By default, the switch is turned off. If you turn on this switch, WAF performs signature verification on each request. Requests that fail signature verification are blocked. **Signature Verification Exception** is selected by default and cannot be deselected. Requests that do not contain signatures or requests that contain invalid signatures are detected. You can also select **Signature Timestamp Exception** and **WebDriver Attack**.
Intelligent Protection	If you turn on this switch, the intelligent protection engine analyzes access traffic and performs machine learning. Then, a blacklist or a protection rule is generated based on the analysis results and learned patterns. You can set the Protection Mode parameter to **Monitor** or **Slider CAPTCHA**. If you set the Protection Mode parameter to Monitor, the anti-crawler rule allows the traffic that matches the rule and records the traffic in security reports. If you set the Protection Mode parameter to Slider CAPTCHA, clients are required to pass slider CAPTCHA verification before they can access the protected domain name.
Bot Threat Intelligence Feed	If you turn on this switch, the threat intelligence library of Alibaba Cloud is used to identify the IP addresses that are frequently used to crawl content from Alibaba Cloud users. The clients that use these IP addresses are required to pass slider CAPTCHA verification before they can access the protected domain name.

Parameter	Description
Data Center Blacklist	If you turn on this switch, you must select libraries from the drop-down list. This way, WAF blocks access requests from IP addresses in the libraries to the protected domain name. The libraries contain known malicious IP addresses from the data centers of Alibaba Cloud and other mainstream cloud providers.  Use Bot Threat Intelligence to Identify Attack Sources with Negative Reputation or Unusual Identity ☑ Bot Threat Intelligence Feed: Slider CAPTCHA ☑ Data Center Blacklist: IDC IP List-Alibaba Cloud, IDC IP List-21 Vianet, IDC IP List-Meituan Cloud, IDC IP List-Others, IDC IP List-Tencent Cloud
IP Address Throttling	If you turn on this switch, you can configure throttling conditions to filter out the requests that are frequently initiated for crawling. This way, HTTP flood attacks are mitigated. You can configure throttling conditions for IP addresses. If the number of requests from the same IP address within the specified time period exceeds the threshold, WAF performs the specified action on subsequent requests. You can also configure the period during which the specified action is performed. The action can be Monitor, block, or Captcha. You can configure up to three throttling conditions. For more information, see Create a custom protection policy.
Custom Session-based Throttling	If you turn on this switch, you can configure custom throttling conditions to filter out the requests that are frequently initiated for crawling. This way, HTTP flood attacks are mitigated. You can configure throttling conditions for sessions. If the number of requests from the same session within the specified time period exceeds the threshold, WAF performs the specified action on subsequent requests. You can also configure the period during which the action is performed. The action can be Monitor, block, or Captcha. For more information, see Create a custom protection policy.

8. (Optional)In the **Verify Actions** step, test the effectiveness of the anti-crawler rule.

   This step is optional. To skip this step, you can click **Skip** in the lower-left corner. If this is your first time to configure an anti-crawler rule, we recommend that you complete this step before you publish the anti-crawler rule. This helps prevent the false positives that are caused by inappropriate configurations or compatibility issues.

   Test steps:

i. **Step 1: Enter a public IP address.**: Enter the public IP address of your test device, such as a computer or mobile phone. The test of the anti-crawler rule takes effect only for the public IP address. The test does not affect your business.

> **Notice** Do not enter the IP address that you obtain by running the **ipconfig** command. This command returns an internal IP address. If you want to obtain the public IP address of your test device, you can click Alibaba Network Diagnose Tool. On the page that appears, search for Local IP. The value of Local IP is the public IP address of your test device. You can also use a browser to search for the IP address of your test device.

ii. **Step 2: Select an action.**: Test the effectiveness of a protection action that you specify in the anti-crawler rule. WAF generates a test rule only for the specified IP address. The action can be **JavaScript Validation**, **Dynamic Token-based Authentication**, **Slider CAPTCHA Verification**, or **Block Verification**.

After you click **Start Test** for an action, WAF immediately delivers the test rule to the test device. In the dialog box that appears, WAF provides the test procedure, expected result, and demonstration. We recommend that you carefully read them.

After the test is complete, you can click **I Have Completed Test** to go to the next step. If the test result shows exceptions, you can click **Go Back** to optimize the anti-crawler rule. Then, perform the test again.

For more information about the exceptions that may occur during a test and the solutions to these exceptions, see FAQ.

9. In the **Preview and Publish Protection Rules** step, confirm the content of the anti-crawler rule and click **Publish**.

After the anti-crawler rule is published, the rule immediately takes effect.

> **Note** If this is your first time to create an anti-crawler rule, you cannot view the rule ID until the rule is published. The rule ID is displayed on the Bot Management tab of the **Security Report** page. You can use the ID of an anti-crawler rule to check for requests that match the rule in Log Service for WAF.

FAQ

Error	Cause	Solution
No valid test requests are detected. See WAF documentation or contact us to analyze the possible causes.	The test request fails to be sent or is not sent to WAF.	Make sure that the test request is sent to the IP address that maps the CNAME provided by WAF.
	The header fields in the test request do not match the header fields that you specify for **Traffic Characteristics** in the anti-crawler rule.	Modify the settings of Traffic Characteristics in the anti-crawler rule.
	The source IP address of the test request is different from the public IP address that you specify in the anti-crawler rule.	Use the correct public IP address. We recommend that you click Alibaba Network Diagnose Tool to obtain your public IP address.

Error	Cause	Solution
The test requests failed the verification. See WAF documentation or contact us to analyze the possible causes.	No real user access is simulated. For example, the debugging mode or automation tools are used.	Simulate real user access during the test.
	An incorrect service type is selected. For example, **Websites** is selected when you configure an anti-crawler rule for apps.	Change the value of the Service Type parameter.
	An intermediate domain name is used, but an incorrect intermediate domain name is selected in the anti-crawler rule.	Select **Use Intermediate Domain Name**. Then, select the correct intermediate domain name from the drop-down list.
	Compatibility issues occur in the frontend.	Contact customer service in the DingTalk group or submit a .
No verification is triggered. See WAF documentation or contact us to analyze the possible causes.	No test rules are generated.	Perform the test several times until the test rule is generated.
No valid test requests are detected or blocked. See WAF documentation or contact us to analyze the possible causes.	The test request fails to be sent or is not sent to WAF.	Make sure that the test request is sent to the IP address that maps the CNAME provided by WAF.
	The header fields in the test request do not match the header fields that you configure for **Traffic Characteristics** in the anti-crawler rule.	Modify the settings of Traffic Characteristics in the anti-crawler rule.
	The source IP address of the test request is different from the public IP address that you specify in the anti-crawler rule.	Use the correct public IP address. We recommend that you click Alibaba Network Diagnose Tool to obtain your public IP address.

What's next

Go to the **Bot Management** tab of the Security report page and view the protection results and the details of the requests that match the anti-crawler rule. Then, optimize the anti-crawler rule based on the protection results.

3.1.3. Configure anti-crawler rules for apps

The bot management module of Web Application Firewall (WAF) provides the scenario-specific configuration feature. You can use this feature to configure custom anti-crawler rules based on your business requirements and protect your business from malicious crawlers. This topic describes how to configure anti-crawler rules for apps.

Background information

The scenario-specific configuration feature allows you to configure anti-crawler rules based on your business requirements. You can use this feature together with intelligent algorithms to identify crawler traffic in a more precise manner. The feature can also automatically handle the crawler traffic that matches the configured anti-crawler rules. After you configure anti-crawler rules, you can verify the rules in a test environment. This prevents adverse effects on your websites or apps caused by inappropriate rule configurations or compatibility issues. The adverse effects include false positives and undesired protection results.

Prerequisites

- Subscription WAF instance: If your WAF instance runs the Pro, Business, or Enterprise edition, the **Bot Management** module is enabled. For more information, see Purchase a WAF instance.
-
- Anti-Bot SDK is integrated into the apps that you want to protect. For more information, see Integrate Anti-Bot SDK into apps.

Configure anti-crawler rules for apps

1.
2.
3.
4.
5. If you have not created an anti-crawler rule, click the **Bot Management** tab. In the **Scenario-specific Configuration** section, click **Start** to create an anti-crawler rule. If you have created an anti-crawler rule, click **Add** in the upper-right corner of the **Bot Management** tab to create an anti-crawler rule.

   > **Note** You can create up to 50 **anti-crawler rules** for a domain name.

6. In the **Configure Scenarios** step, configure the basic information about the scenario in which you want to protect apps and click **Next**.

Parameter	Description
Scenario	Specify the type of scenario in which you want to protect the apps. Examples: logon, registration, and order placement.
Service Type	Select **Apps** to protect native iOS and Android apps. **Note** HTML5 apps are not native iOS or Android apps. If you want to protect HTML5 apps, set the **Service Type** parameter to **Websites**.

Parameter	Description
Traffic Characteristics	Add match conditions to identify traffic destined for the apps that you want to protect. To add a match condition, you must specify the matching field, logical operator, and matching content. The matching field is a header field of HTTP requests. For more information about the fields in match conditions, see Fields in match conditions. You can specify up to five match conditions. **Notice** If you enter an IP address, you must press Enter.

7. In the **Configure Protection Rules** step, configure the anti-crawler rule and click **Next**.

Parameter	Description
Check Invalid App Signature	You can use this feature to detect and control requests that have invalid signatures or do not have signatures. You cannot disable this feature. You can configure **Action** to handle the requests that have invalid signatures or do not have signatures. If you set the Action parameter to Monitor, WAF allows these requests and records them in security reports and logs. If you set the Action parameter to Block, WAF blocks these requests.
Check Abnormal Device Behavior	After you enable this feature, WAF detects and controls the requests from the devices that have abnormal characteristics. The following characteristics of a device are considered abnormal characteristics: ○ **Use Simulators**: A simulator is used. ○ **Use Proxies**: A proxy is used. ○ **Use Rooted Device**: A rooted device is used. ○ **Debugging Mode**: The debugging mode is enabled. ○ **Hooking**: `Hooking` techniques are used. ○ **Multiboxing**: Multiple protected app processes run on the device at the same time. You can set the Action parameter to **Monitor** or **Block** based on your business requirements. .
Action	You can set this parameter to **Monitor** or **Block**. This setting takes effect for **Check Invalid App Signature** and **Check Abnormal Device Behaviors**.

Parameter	Description
IP Address Throttling	After you enable this feature, you can configure throttling conditions to filter abnormal requests. This way, HTTP flood attacks can be mitigated. You can specify throttling conditions for IP addresses. If the number of requests from an IP address within the specified time period exceeds the threshold, WAF performs the monitor or block action on subsequent requests. You can also specify the period during which the monitor or block action is performed. You can specify up to three conditions. For more information, see Create a custom protection policy.
Device Throttling	After you enable this feature, you can configure throttling conditions to filter abnormal requests. This way, HTTP flood attacks can be mitigated. You can specify throttling conditions for devices. If the number of requests from the same device within the specified time period exceeds the threshold, WAF performs the monitor or block action on subsequent requests. You can also specify the period during which the monitor or block action is performed. You can specify up to three conditions.
Custom Session-based Throttling	After you enable this feature, you can configure custom throttling conditions to filter abnormal requests. This way, HTTP flood attacks can be mitigated. You can specify throttling conditions for sessions. If the number of requests from the same session within the specified time period exceeds the threshold, WAF performs the monitor or block action on subsequent requests. You can also specify the period during which the monitor or block action is performed. You can specify up to three conditions. For more information, see Create a custom protection policy.

8. (Optional)In the **Verify Actions** step, check whether the anti-crawler rule is in effect.

   This step is optional. To skip this step, you can click **Skip** in the lower-left corner. Before you publish the rule, we recommend that you complete this step.

   Description:

   - **Step 1: Enter a public IP address.**: Enter the public IP address of your test device such as a mobile phone. During the test, the anti-crawler rule takes effect only for the public IP address. Therefore, the test does not affect your business.

     > Notice If you want to obtain the public IP address of your test device, you can click Alibaba Network Diagnose Tool. On the page that appears, search for Local IP. The value of Local IP is the public IP address of your test device. You can also use a browser to search for the IP address of your test device.

   - **Step 2: Verify the SDK signature.**: Click **Start Test** to verify that the SDK signature of the app is valid.

> **Note** Make sure that Anti-Bot SDK is integrated into the test device. If the Anti-Bot SDK is not integrated into the device, the signature verification fails, normal requests are blocked, and the test cannot be completed.

- **Step 3: Select an action.**: Check whether the Block action is in effect. After you click **Start Test**, WAF immediately delivers the anti-crawler rule to the test device. In the dialog box that appears, WAF provides the test procedure, expected result, and demonstration. We recommend that you carefully read them.

  After the test is complete, you can click **I Have Completed Test** to go to the next step. If the test result shows exceptions, you can click **Go Back** to optimize the anti-crawler rule. Then, perform the test again.

  For more information about the exceptions that may occur during a test and about the solutions to handle these exceptions, see FAQ.

9. In the **Preview and Publish Protection Rules** step, confirm the content of the anti-crawler rule and click **Publish**.

   After the anti-crawler rule is published, the rule immediately takes effect.

   > **Note** If this is your first time to create an anti-crawler rule, you cannot view the rule ID until the rule is published. The rule ID is displayed on the Bot Management tab of the **Security Report** page. You can use the ID of an anti-crawler rule to check for requests that match the rule in Log Service for WAF.

FAQ

Error	Cause	Solution
No valid test requests are detected. See WAF documentation or contact us to analyze the possible causes.	The test request fails to be sent or is not sent to WAF.	Make sure that the test request is sent to the IP address that maps the CNAME provided by WAF.
	The header fields in the test request do not match the header fields that you configure for **Traffic Characteristics** in the anti-crawler rule.	Modify the settings of Traffic Characteristics in the anti-crawler rule.
	The source IP address of the test request is different from the public IP address that you specify in the anti-crawler rule.	Use the correct public IP address. We recommend that you click Alibaba Network Diagnose Tool to obtain your public IP address.
The test requests failed the verification. See WAF	No real user access is simulated. For example, the debugging mode or automation tools are used.	Simulate real user access during the test.
	An invalid service type is selected. For example, you select **Websites** for protection.	Change the value of the Service Type parameter.

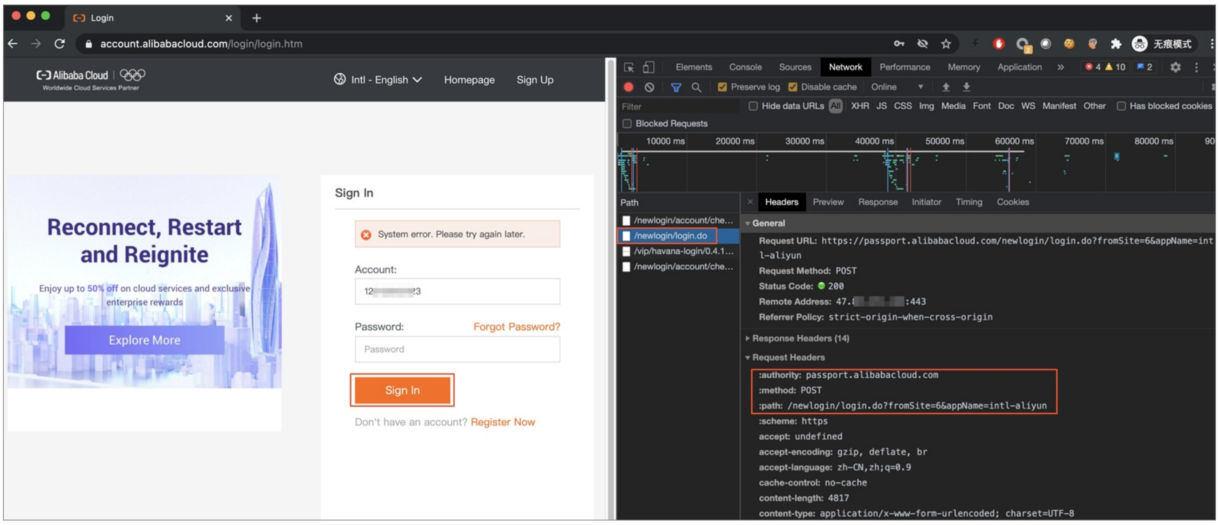
documentation or contact us to Error analyze the possible causes.	Cause	Solution
	An intermediate domain name is used, but an incorrect intermediate domain name is selected in the anti-crawler rule.	Select **Use an Intermediate Domain Name**, and then select the intermediate domain name from the drop-down list.
	Compatibility issues occur in the frontend.	Contact customer service in the DingTalk group or submit a .
No verification is triggered. See WAF documentation or contact us to analyze the possible causes.	No test rules are generated.	Perform the test several times until a test rule is generated.
No valid test requests are detected or blocked. See WAF documentation or contact us to analyze the possible causes.	The test request fails to be sent or is not sent to WAF.	Make sure that the test request is sent to the IP address that maps the CNAME provided by WAF.
	The header fields in the test request do not match the header fields that you configure for **Traffic Characteristics** in the anti-crawler rule.	Modify the settings of Traffic Characteristics in the anti-crawler rule.
	The source IP address of the test request is different from the public IP address that you specify in the anti-crawler rule.	Use the correct public IP address. We recommend that you click Alibaba Network Diagnose Tool to obtain your public IP address.
The test request is blocked. See WAF documentation or contact us to analyze the possible causes.	Some code may have logic issues when Anti-Bot SDK is integrated. As a result, requests contain invalid signatures. For example, the content of a signature does not match the actual request, or the request does not have a signature.	Check whether a signature issue occurs and fix the issue at the earliest opportunity. For more information, see App protection.
	Proxies are used, or you do not use a real device.	Use a real device to perform the test.

3.1.4. Examples of using the scenario-specific configuration feature

This topic provides examples on how to use the scenario-specific configuration feature.

Example 1: Configure an anti-crawler rule for the logon page of the Alibaba Cloud official website

After you click the Sign In button on the Alibaba Cloud official website, a logon request is sent, which uses the following header fields.



Sign In

System error. Please try again later.

Account: 12[redacted]3

Password: Forgot Password?

Sign In

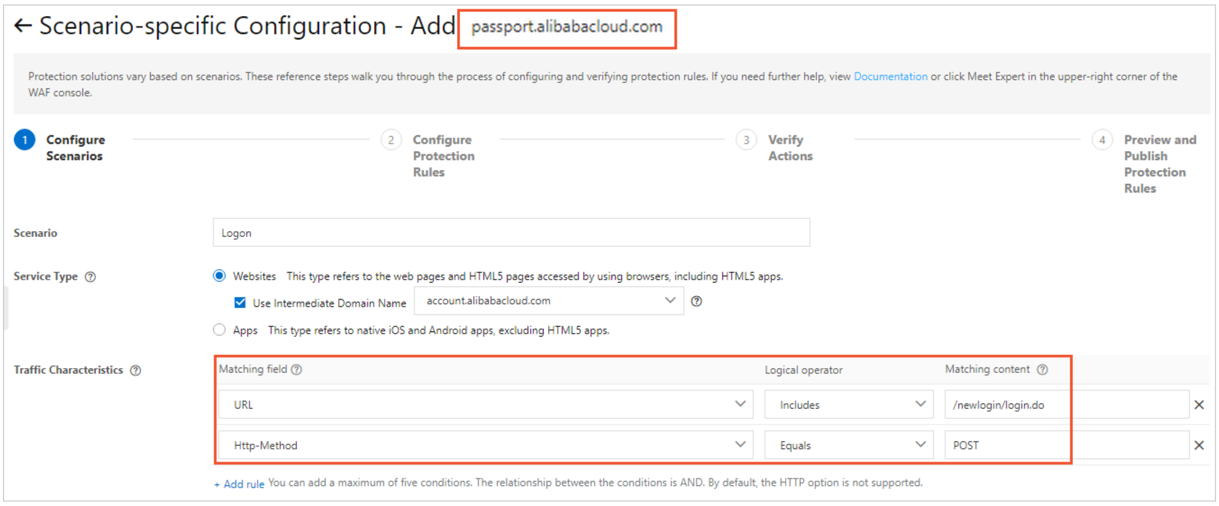
Don't have an account? Register Now

Request URL: https://passport.alibabacloud.com/newlogin/login.do?fromSite=6&appName=intl-aliyun
Request Method: POST
Status Code: 200
Remote Address: 47.[redacted]:443
Referrer Policy: strict-origin-when-cross-origin

Response Headers (14)

Request Headers
:authority: passport.alibabacloud.com
:method: POST
:path: /newlogin/login.do?fromSite=6&appName=intl-aliyun
:scheme: https
accept: undefined
accept-encoding: gzip, deflate, br
accept-language: zh-CN,zh;q=0.9
cache-control: no-cache
content-length: 4817
content-type: application/x-www-form-urlencoded; charset=UTF-8

The following figure shows the Scenario-specific Configuration page.



← Scenario-specific Configuration - Add passport.alibabacloud.com

Protection solutions vary based on scenarios. These reference steps walk you through the process of configuring and verifying protection rules. If you need further help, view Documentation or click Meet Expert in the upper-right corner of the WAF console.

1 Configure Scenarios — 2 Configure Protection Rules — 3 Verify Actions — 4 Preview and Publish Protection Rules

Scenario: Logon

Service Type: ● Websites This type refers to the web pages and HTML5 pages accessed by using browsers, including HTML5 apps.
☑ Use Intermediate Domain Name: account.alibabacloud.com
○ Apps This type refers to native iOS and Android apps, excluding HTML5 apps.

Traffic Characteristics:

Matching field	Logical operator	Matching content
URL	Includes	/newlogin/login.do
Http-Method	Equals	POST

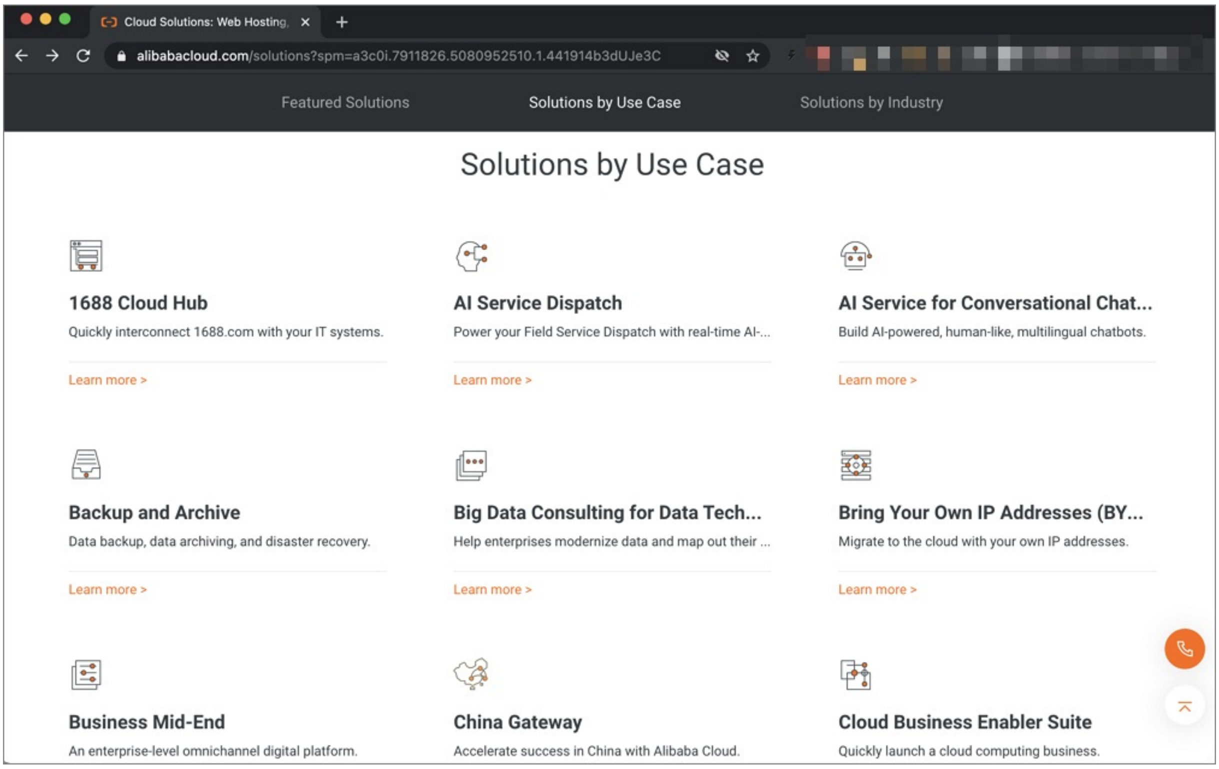
+ Add rule You can add a maximum of five conditions. The relationship between the conditions is AND. By default, the HTTP option is not supported.

You can configure an anti-crawler rule for the logon page based on the following description:

- If you click the Sign In button on the Alibaba Cloud official website, a logon request is sent. In this example, you must configure an anti-crawler rule to protect the logon page. Therefore, set the Scenario parameter to **Logon**.
- Set the Service Type parameter to **Websites** because the logon request is sent by a browser.
- The Sign In button is on the account.alibabacloud.com page. However, the logon request is sent to the passport.alibabacloud.com page. In this case, an intermediate domain name is used. Therefore, select **Use Intermediate Domain Name** and the **account.alibaba.com** domain name from the drop-down list. The anti-crawler rule is actually configured for the passport.alibabacloud.com domain name.
- The logon request includes /newlogin/login.do in the URL field and uses the POST method. You must add the required conditions for the Traffic Characteristics parameter.

Example 2: Configure an anti-crawler rule for the solution page of the Alibaba Cloud official website

The following figure shows the solution page at alibabacloud.com/solutions.



Cloud Solutions: Web Hosting,

alibabacloud.com/solutions?spm=a3c0i.7911826.5080952510.1.441914b3dUJe3C

Featured Solutions | Solutions by Use Case | Solutions by Industry

Solutions by Use Case

1688 Cloud Hub
Quickly interconnect 1688.com with your IT systems.
Learn more >

AI Service Dispatch
Power your Field Service Dispatch with real-time AI-...
Learn more >

AI Service for Conversational Chat...
Build AI-powered, human-like, multilingual chatbots.
Learn more >

Backup and Archive
Data backup, data archiving, and disaster recovery.
Learn more >

Big Data Consulting for Data Tech...
Help enterprises modernize data and map out their ...
Learn more >

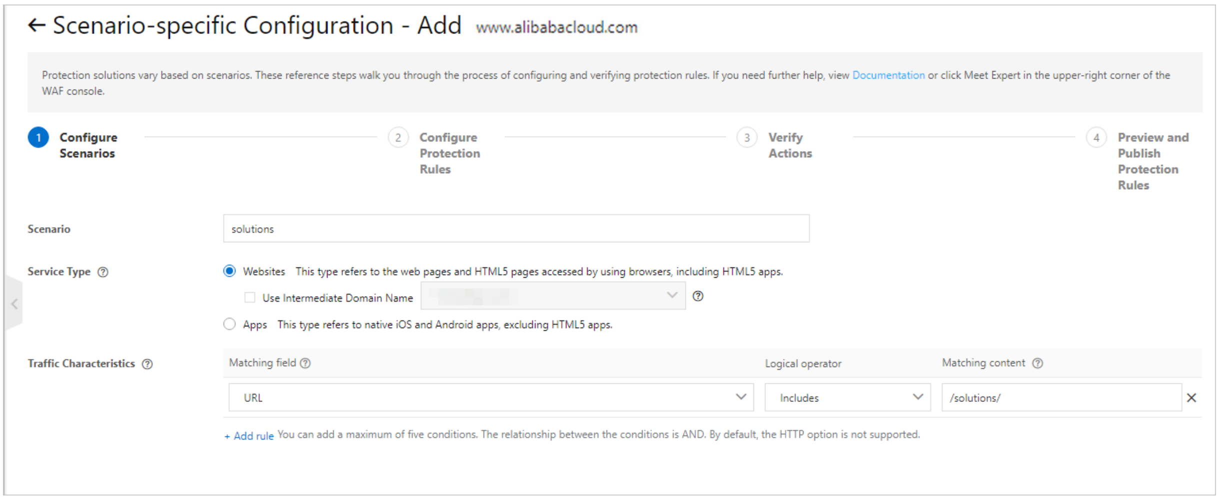
Bring Your Own IP Addresses (BY...
Migrate to the cloud with your own IP addresses.
Learn more >

Business Mid-End
An enterprise-level omnichannel digital platform.

China Gateway
Accelerate success in China with Alibaba Cloud.

Cloud Business Enabler Suite
Quickly launch a cloud computing business.

The following figure shows the Scenario-specific Configuration page.



← Scenario-specific Configuration - Add www.alibabacloud.com

Protection solutions vary based on scenarios. These reference steps walk you through the process of configuring and verifying protection rules. If you need further help, view Documentation or click Meet Expert in the upper-right corner of the WAF console.

1 Configure Scenarios — 2 Configure Protection Rules — 3 Verify Actions — 4 Preview and Publish Protection Rules

Scenario: solutions

Service Type ⓘ
● Websites This type refers to the web pages and HTML5 pages accessed by using browsers, including HTML5 apps.
□ Use Intermediate Domain Name ⓘ
○ Apps This type refers to native iOS and Android apps, excluding HTML5 apps.

Traffic Characteristics ⓘ

Matching field ⓘ	Logical operator	Matching content ⓘ
URL	Includes	/solutions/

+ Add rule You can add a maximum of five conditions. The relationship between the conditions is AND. By default, the HTTP option is not supported.

You can configure an anti-crawler rule for the solution page based on the following description:

- In this example, you must configure an anti-crawler rule to protect the subpages of alibabacloud.com/solutions. Therefore, set the Scenario parameter to **solutions**.
- Set the Service Type parameter to **Websites** because the solution page is visited by using a browser.
- If you want to visit a subpage of alibabacloud.com/solutions, a request whose URL is in the `/solutions/xxx` format is sent. Therefore, you must add the following conditions for the Traffic Characteristics parameter: `URLPath Includes /solutions/` and `Http-Method Equals GET`. You do not need to select **Use Intermediate Domain Name** because no intermediate domain names are used. You can add more conditions by using other header fields, such as User-Agent, Params, and Referer.

3.2. Configure the allowed crawlers function

The allowed crawlers function maintains a whitelist of authorized search engines, such as Google, Bing, Baidu, Sogou and Yandex. The crawlers of these search engines are allowed to access all pages on domain names.

Prerequisites

-
-

Background information

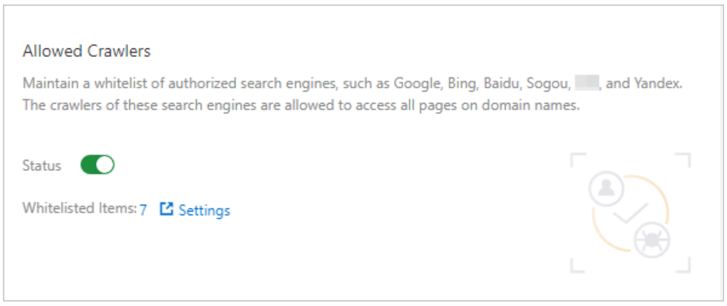
Rules defined in the function allow requests from specific crawlers to the target domain name based on the Alibaba Cloud crawler library. The Alibaba Cloud crawler library is updated in real time based on the analysis of network traffic that flows through Alibaba Cloud, and captures the characteristics of requests that are initiated from crawlers. The crawler library is updated dynamically and contains crawler IP addresses of mainstream search engines, including Google, Baidu, Sogou, Bing, and Yandex.

After you enable the allowed crawlers function, requests initiated from the crawler IP addresses of the authorized search engines are directly sent to the target domain names. The bot management module no longer detects these requests.

> **Note** To filter some requests from the crawler IP addresses, use the **Access Control/Throttling** module. For more information, see Create a custom protection policy.

Procedure

1.
2.
3.
4.
5. Click the **Bot Management** tab, find the **Allowed Crawlers** section. Then, turn on **Status** and click **Settings**.



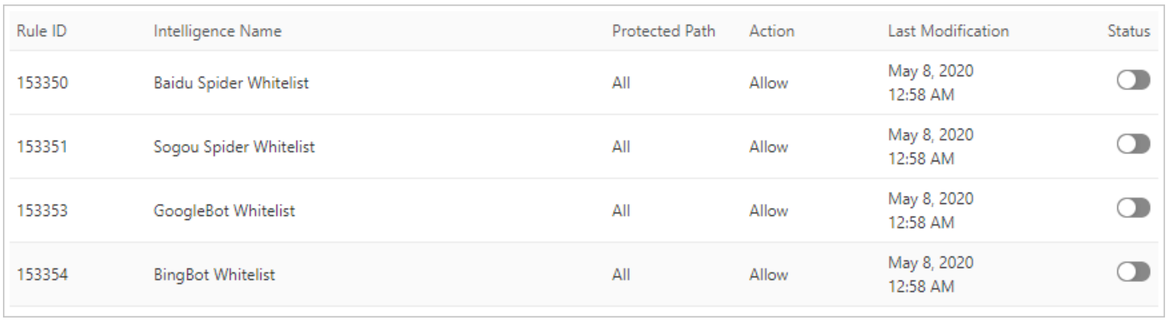
Allowed Crawlers

Maintain a whitelist of authorized search engines, such as Google, Bing, Baidu, Sogou, [redacted], and Yandex. The crawlers of these search engines are allowed to access all pages on domain names.

Status

Whitelisted Items: 7 Settings

6. In the **Allowed Crawlers** list, find the target rule by **Intelligence Name**, and turn on **Status**.



Rule ID	Intelligence Name	Protected Path	Action	Last Modification	Status
153350	Baidu Spider Whitelist	All	Allow	May 8, 2020 12:58 AM	○
153351	Sogou Spider Whitelist	All	Allow	May 8, 2020 12:58 AM	○
153353	GoogleBot Whitelist	All	Allow	May 8, 2020 12:58 AM	○
153354	BingBot Whitelist	All	Allow	May 8, 2020 12:58 AM	○

The default rules only allow crawler requests from the following search engines: Google, Bing, Baidu, Sogou and Yandex. You can enable the **Legit Crawling Bots** rule to allow requests from all search engine crawlers.

3.3. Set a bot threat intelligence rule

Bot threat intelligence provides information about suspicious IP addresses used by dialers, on-premises data centers, and malicious scanners. This function also maintains an IP address library of malicious crawlers and prevents crawlers from accessing all pages under your domain name or specific directories.

Prerequisites

-
-

Background information

Bot threat intelligence rules can block requests from crawlers that are recorded in the Alibaba Cloud crawler library. The Alibaba Cloud crawler library is updated in real time based on the analysis of network traffic that flows through Alibaba Cloud. It can effectively detect IP addresses of malicious crawlers and provide the characteristics of requests that are initiated from the crawlers.

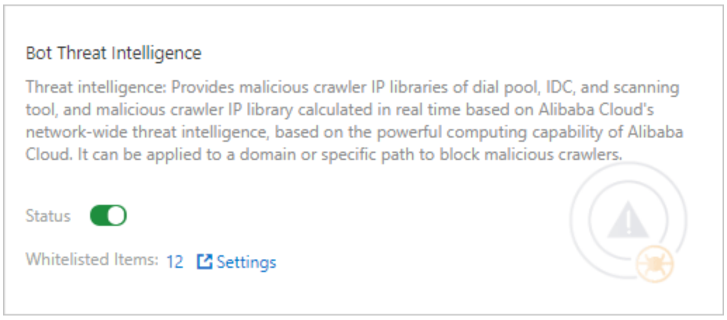
Note The Alibaba Cloud crawler library covers public clouds and on-premises data centers.

You can set a bot threat intelligence rule that chooses different actions to manage different requests based on the type of the threat intelligence library. For example, you can set a rule that blocks certain requests, or requires JavaScript verification or CAPTCHA verification to verify certain requests. You can also use a bot threat intelligence rule to protect important endpoints against certain threats. This helps you minimize the negative impacts on the services.

Procedure

1.
2.
3.
4.
5. Click the **Bot Management** tab, find the **Bot Threat Intelligence** section. Then, turn on **Status** and click **Settings**.

> **Note** After the bot threat Intelligence function is enabled, all requests destined for your website are checked by the function. You can configure a Bot Management rule so that the requests that match the rule bypass the check. For more information, see Configure a whitelist for Bot Management.



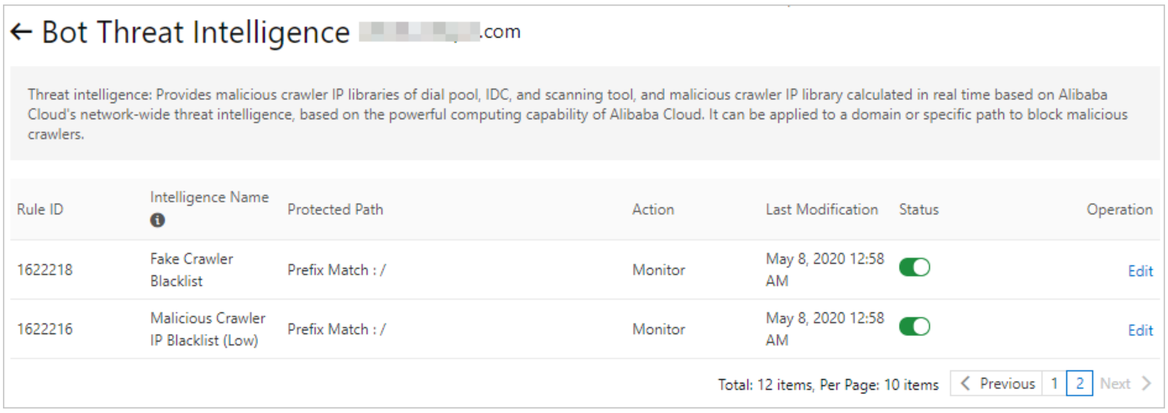
Bot Threat Intelligence

Threat intelligence: Provides malicious crawler IP libraries of dial pool, IDC, and scanning tool, and malicious crawler IP library calculated in real time based on Alibaba Cloud's network-wide threat intelligence, based on the powerful computing capability of Alibaba Cloud. It can be applied to a domain or specific path to block malicious crawlers.

Status: On

Whitelisted Items: 12 Settings

6. In the **Bot Threat Intelligence** rule list, find the threat intelligence library you want to use by **Intelligence Name**, and turn on **Status**.



← Bot Threat Intelligence [redacted].com

Threat intelligence: Provides malicious crawler IP libraries of dial pool, IDC, and scanning tool, and malicious crawler IP library calculated in real time based on Alibaba Cloud's network-wide threat intelligence, based on the powerful computing capability of Alibaba Cloud. It can be applied to a domain or specific path to block malicious crawlers.

Rule ID	Intelligence Name	Protected Path	Action	Last Modification	Status	Operation
1622218	Fake Crawler Blacklist	Prefix Match : /	Monitor	May 8, 2020 12:58 AM	On	Edit
1622216	Malicious Crawler IP Blacklist (Low)	Prefix Match : /	Monitor	May 8, 2020 12:58 AM	On	Edit

Total: 12 items, Per Page: 10 items < Previous 1 2 Next >

The following table lists the bot threat intelligence libraries that WAF supports.

Intelligence library	Description
Malicious Scanner Fingerprint Blacklist	This library contains characteristics of common scanners.
Malicious Scanner IP Blacklist	This library contains malicious IP addresses that are dynamically updated based on the source IP addresses of scan attacks detected on Alibaba Cloud.
Credential Stuffing IP Blacklist	This library contains malicious IP addresses that are dynamically updated based on the source IP addresses of credential stuffing and brute-force attacks detected on Alibaba Cloud.
Fake Crawler Blacklist	This library identifies crawlers that use the User-Agent of authorized search engines, such as BaiduSpider, to disguise as authorized programs. **Notice** Before you enable this library, make sure that you have configured a whitelist of crawlers. Otherwise, false positives may occur. For more information, see Configure the allowed crawlers function.

Intelligence library	Description
Malicious Crawler Blacklist	This library contains malicious IP addresses that are dynamically updated based on the source IP addresses of crawlers detected on Alibaba Cloud. This library is categorized into three severity levels: low, medium, and high. A higher severity indicates more IP addresses in the library and a higher false positive rate. **Note** We recommend that you set up two-factor authentication, such as CAPTCHA and JavaScript verification, for the high-severity library. In scenarios where two-factor authentication cannot be implemented, we recommend that you set threat intelligence rules based on the low-severity library.
IDC IP List	This library contains IP addresses of public clouds and on-premises data centers, including Alibaba Cloud, Tencent Cloud, Meituan Open Services, and 21Vianet. Attackers typically use CIDR blocks of public clouds or on-premises data centers to deploy crawlers or as proxies to access sites. Regular users rarely access sites in this way.

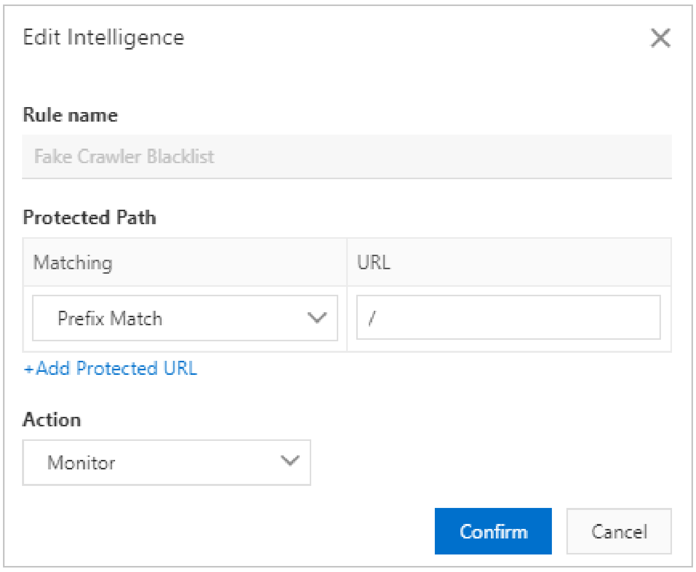
After you enable the default rule, requests initiated from IP addresses in the threat intelligence library to any directory of the protected domain name trigger the **Monitor** action. This action allows the requests to the destination directories and records the events.

If you need to modify the default rule, such as the protected URL or action, see the following step on how to customize a threat intelligence rule.

7. (Optional)Customize a threat intelligence rule.

   i. Find the target rule and click **Edit** in the Actions column.

   ii. In the **Edit Intelligence** dialog box that appears, set the following parameters.



Edit Intelligence

Rule name: Fake Crawler Blacklist

Protected Path

Matching	URL
Prefix Match	/

Action: Monitor

Parameter	Description

Parameter	Description
Protected Path	The **URL** that you want to protect, such as /abc, /login/abc, or forward slash (/) that indicates all directories. You also need to select a value for **Matching**. Valid values: ■ **Precise Match**: The destination URL must be an exact match of the protected URL. ■ **Prefix Match**: The prefix of the destination URL matches the protected URL. ■ **Regex Match**:The destination URL matches the specified regular expression. You can click **Add Protected URL** to add more URLs. You can add up to 10 URLs.
Action	The action to be performed after the match conditions of the rule are met. Valid values: ■ **Monitor**: allows the request to the destination directory and records the event. ■ **Block**: blocks the request. ■ **JavaScript Validation**: requires JavaScript verification. Requests are forwarded to the destination directory only after they pass the verification. ■ **Captcha**: requires CAPTCHA verification on the client side. Requests are forwarded to the destination directory only after they pass the verification. **Note** CAPTCHA only supports synchronous requests. To verify asynchronous requests, such as Ajax requests, contact the Alibaba Cloud security team. If you cannot determine whether the protected URL supports CAPTCHA, we recommend that you create a custom protection policy, such as an ACL rule, to run a test. For more information, see Create a custom protection policy. ■ **Strict Captcha**: requires CAPTCHA verification on the client side. Requests are forwarded to the destination directory only after they pass the verification. CAPTCHA verification has a stricter standard to verify visitor identities.

iii. Click **Confirm**.

3.4. Configure data risk control

After you add a website to Web Application Firewall (WAF), you can enable data risk control for the added website. Data risk control is used to protect crucial website services against attacks. These services include registrations, logons, campaigns, and forums. You can customize data risk control rules based on your business requirements.

Background information

The data risk control feature is based on Alibaba Cloud big data. This feature uses industry engines for risk decision-making and is integrated with human-machine identification technologies to protect crucial services against attacks in various scenarios. To use data risk control, you need only to add your website to WAF. You do not need to configure servers or clients.

Data risk control is suitable for a wide range of scenarios. These scenarios include spam user registration, SMS flood attacks, dictionary attacks, brute-force attacks, auto-purchase bots, promotion abuse, snatcher bots, vote manipulation, and spam.

Compatibility

Data risk control is suitable only for web pages or HTML5 environments. In some cases, the JavaScript plug-in that is inserted into web pages may be incompatible with the web pages. This results in errors in slider CAPTCHA verification. The following web pages may encounter compatibility issues:

- Static web pages that you can visit by using their URLs and web pages to which you can be redirected by modifying `location.href`, or by using the `window.open` method or the anchor tag `<a>`. The static web pages include HTML details pages, shared pages, website homepages, and documents.
- Web pages where you rewrite and commit code and web pages where you submit custom requests, such as when you submit forms, rewrite XMLHttpRequest (XHR), and send custom Ajax requests.
- Web pages whose code makes use of webhooks.

After you enable data risk control, we recommend that you select the warn mode and use data risk control together with the Log Service for WAF feature. This allows you to run a compatibility test. For more information, see Overview of the Log Service for WAF feature.

To protect native apps, we recommend that you use the Anti-Bot SDK. For more information, see Configure application protection.

Prerequisites

- A WAF instance is purchased. The instance meets the following requirements:
  - The instance is deployed in the **Chinese mainland**.
  - **Bot Management** is enabled.

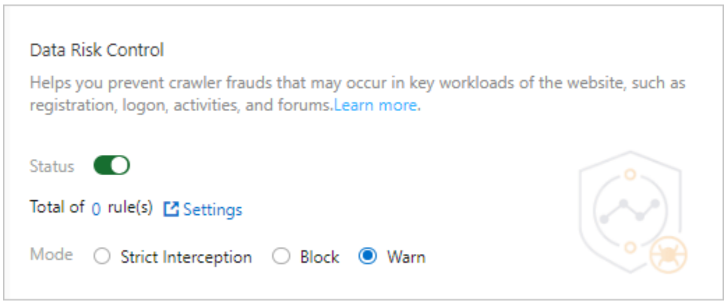
  For more information, see Purchase a WAF instance.
-

> **Notice** WAF provides the scenario-specific configuration feature. You can configure anti-crawler rules based on your business requirements to precisely protect your business from malicious crawlers. If you want to protect your website against malicious crawlers, we recommend that you use the scenario-specific configuration feature. For more information, see Overview of scenario-specific configuration. After you configure the anti-crawler rules, you no longer need to configure data risk control rules. This is because the two types of rules can both prevent malicious crawlers. Alibaba Cloud no longer provides updates or maintenance for the data risk control feature.

Procedure

1.
2.
3.

4.
5. Click the **Bot Management** tab, find the **Data Risk Control** section, and then click **Settings**.



Data Risk Control

Helps you prevent crawler frauds that may occur in key workloads of the website, such as registration, logon, activities, and forums.Learn more.

Status

Total of 0 rule(s) Settings

Mode ○ Strict Interception ○ Block ● Warn

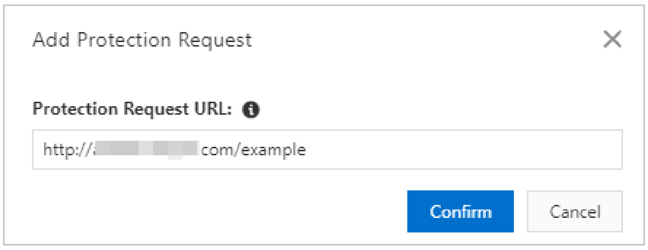
Parameter	Description
Status	The switch that you use to enable or disable data risk control. After you enable data risk control for a website, WAF inserts a JavaScript plug-in into specified or all web pages of the website. Reactive elements on the web pages are returned to users as compressed files that are not in the GZIP format. No further configurations are required, regardless of whether your website uses non-standard ports. Note ◦ If you want to configure the Mode parameter and protection rules, you must enable data risk control. ◦ After data risk control is enabled, all requests that are destined for your website are checked. You can configure a whitelist for the bot management module. This way, the requests that match the rule bypass the check. For more information, see Configure a whitelist for Bot Management.
Mode	The mode for data risk control. Valid values: ◦ **Strict Interception**: If WAF detects that your website is under attack, requests are required to pass strict multi-factor authentication. ◦ **Block**: If WAF detects that your website is under attack, requests are required to pass multi-factor authentication. ◦ **Warn**: If WAF detects that your website is under attack, requests are forwarded to your website. However, logs that are related to the requests are generated. You can view the detailed information in risk reports. Note By default, the Mode parameter is set to the Warn mode. In this mode, data risk control does not block requests. However, WAF inserts a JavaScript plug-in into static web pages to analyze client behavior.

6. Add a data risk control rule.

   i. On the **Data Risk Control** page, click the **Protection Request** tab and click **Add Protection Request**.

ii. In the **Add Protection Request** dialog box, enter the URL that you want to protect in the **Protection Request URL** field.

For more information, see Introduction to a protected URL.



Add Protection Request

Protection Request URL:

http://[redacted]com/example

iii. Click **Confirm**.

A newly added URL takes effect in about 10 minutes. You can view the newly added URL in the URL list. You can also modify or delete the URL based on your business requirements.

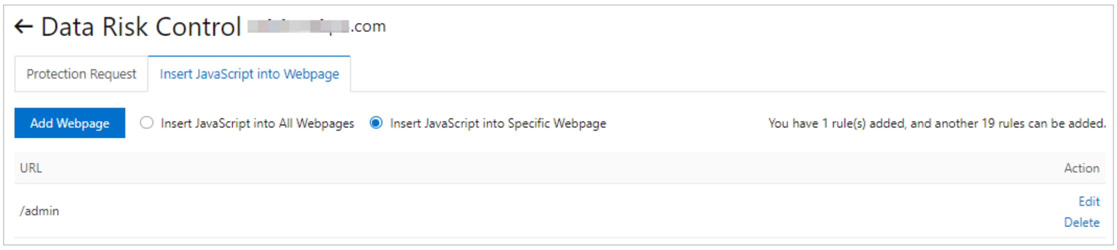
7. (Optional)Specify the web pages into which you want to insert the JavaScript plug-in.

Some code of web pages may be incompatible with the JavaScript plug-in. In this case, we recommend that you insert the JavaScript plug-in into only the pages that are compatible with the plug-in.

> **Note** If the JavaScript plug-in is inserted only into the pages that are compatible with the plug-in, data risk control may fail to obtain all user behavior. This compromises the effectiveness of data risk control.

i. On the **Data Risk Control** page, click the **Insert JavaScript into Webpage** tab.

ii. Select **Insert JavaScript into Specific Webpage** and click **Add Webpage**.



← Data Risk Control [redacted].com

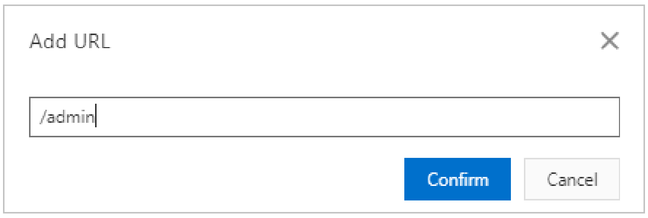
○ Insert JavaScript into All Webpages ● Insert JavaScript into Specific Webpage

You have 1 rule(s) added, and another 19 rules can be added.

URL	Action
/admin	Edit Delete

> **Note** You can add a maximum of 20 URL paths for the web pages.

iii. In the **Add URL** dialog box, enter the URL paths of the web pages into which you want to insert the JavaScript plug-in and click **Confirm**. The URL paths must start with a forward slash (/).



Add URL

/admin

After you add the URL paths, data risk control inserts the JavaScript plug-in into all the web pages in the URL paths.

After data risk control is enabled, you can use the Log Service for WAF feature to view the protection results. For more information, see View protection results.

Introduction to a protected URL

A protected URL is the endpoint that is used to perform service operations. A protected URL is different from the URL of a web page. For example, you have a registration page whose URL is `www.aliyundoc.com/new_user`. The endpoint that you can use to obtain verification codes is `www.aliyundoc.com/getsmscode`, whereas the endpoint that you can use to register is `www.aliyundoc.com/register.do`.

In this example, you must add `www.aliyundoc.com/getsmscode` and `www.aliyundoc.com/register.do` as protected URLs. This way, WAF can protect the URLs from SMS flood attacks and spam user registration. If you add `www.aliyundoc.com/new_user` as a protected URL, common users are also required to pass slider CAPTCHA verification. This impairs user experience.

When you configure a protected URL, take note of the following items:

- Protected URLs support exact match and do not support fuzzy match.

  For example, if you add `www.aliyundoc.com/test` as a protected URL, data risk control filters only the requests that are sent to this URL. Data risk control does not filter the requests that are sent to the subdirectories of this URL.

- Data risk control protects traffic based on website directories.

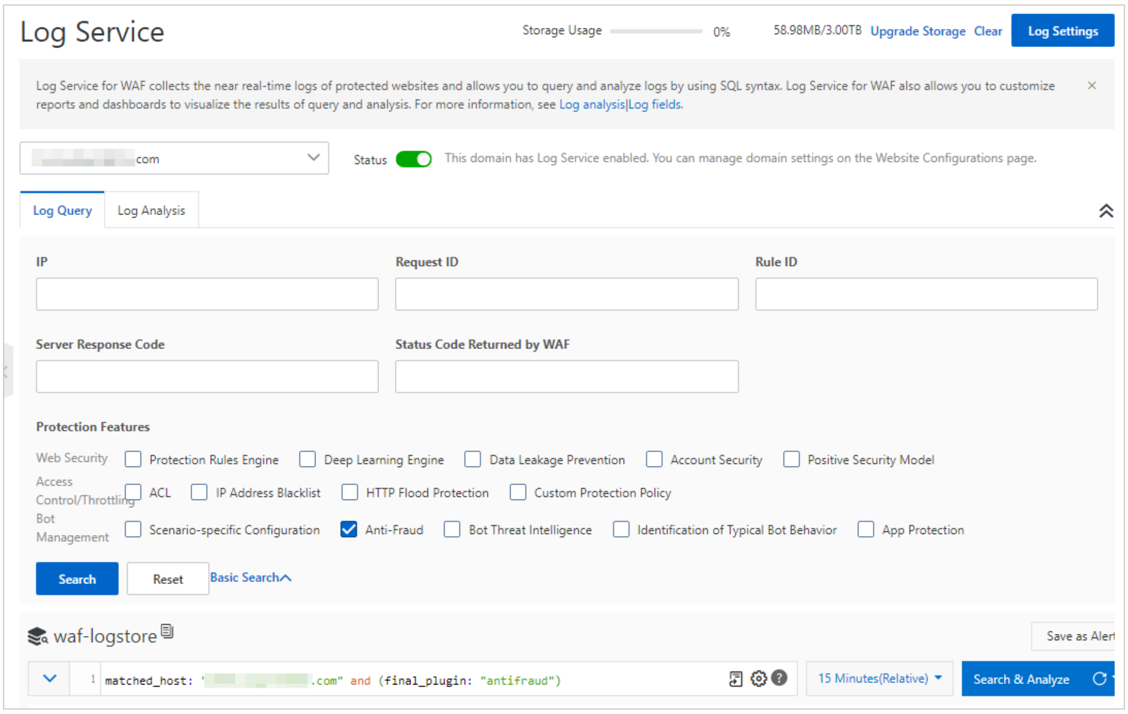
  If you add `www.aliyundoc.com/book/*` as a protected URL, data risk control filters the requests that are sent to the web pages in all the subdirectories of `www.aliyundoc.com/book`. We recommend that you do not configure data risk control to monitor the entire website. If you add `www.aliyundoc.com/*` as a protected URL, common users are required to pass slider CAPTCHA verification before they can visit the website homepage. This impairs user experience.

- Requests that are sent to a protected URL always trigger slider CAPTCHA verification. Make sure that common users cannot directly request a protected URL. Common users are required to pass multi-factor authentication before they can visit the protected URL.
- Data risk control does not apply to websites that support API operations. API calls are machine actions and cannot pass the slider CAPTCHA verification of data risk control. However, if a common user clicks a button on a page to call an API operation, data risk control still works.

View protection results

You can use the Log Service for WAF feature to view the protection results.

After log collection is enabled for a domain name, you can search for the protection results by selecting the **Anti-Fraud** option in the **Advanced Search** section on the **Log Query** tab. For more information, see Query and analyze logs.



Log Service for WAF collects the near real-time logs of protected websites and allows you to query and analyze logs by using SQL syntax. Log Service for WAF also allows you to customize reports and dashboards to visualize the results of query and analysis. For more information, see Log analysis|Log fields.

[redacted].com

Status: on. This domain has Log Service enabled. You can manage domain settings on the Website Configurations page.

Protection Features

- Web Security: □ Protection Rules Engine □ Deep Learning Engine □ Data Leakage Prevention □ Account Security □ Positive Security Model
- Access Control/Throttling: □ ACL □ IP Address Blacklist □ HTTP Flood Protection □ Custom Protection Policy
- Bot Management: □ Scenario-specific Configuration ☑ Anti-Fraud □ Bot Threat Intelligence □ Identification of Typical Bot Behavior □ App Protection

```
matched_host: '[redacted].com" and (final_plugin: "antifraud")
```

Examples

User Tom has a website whose domain name is `www.aliyundoc.com`. Common users can register as website members at `www.aliyundoc.com/register.html`. Tom notices that attackers can use malicious scripts to submit registration requests and create accounts. The accounts that are created by attackers are used to participate in prize draws that are held by the website. The registration requests are highly similar to normal requests, and the request rate is maintained at a normal level. In this case, the HTTP flood protection policy cannot identify this type of malicious request.

Configuration example

Tom adds the website to WAF and enables data risk control for the `www.aliyundoc.com` domain name. The URL of the most crucial registration service is `www.aliyundoc.com/register.html`. Therefore, Tom adds this URL as a protected URL.

Protection results

After the configurations take effect, data risk control inserts a JavaScript plug-in into all web pages of the website. This allows Tom to monitor and analyze the behavior of each user who visits `www.aliyundoc.com`. The web pages into which a JavaScript plug-in is inserted include the homepage and subpages. Then, data risk control determines whether the behavior of each user is normal. Data risk control also determines whether a source IP address is malicious based on the big data reputation library of Alibaba Cloud.

When a user sends a registration request to `www.aliyundoc.com/register.html`, WAF determines whether the user is an attacker based on the user behavioral and environmental data that is generated from the time the user visits the website to the time the user submits the registration request. For example, if a user directly submits a registration request and does not perform other operations before the request is submitted, the request is identified as suspicious.

- If data risk control determines that a request is from a normal user based on the past behavior of the user, the user can register accounts without verification.
- If data risk control identifies a request as suspicious, or the source IP address has a record that the source IP address is used to send malicious requests, slider CAPTCHA verification is triggered to verify the identity of the user. Only a user that passes the verification can register accounts.

  If slider CAPTCHA verification captures suspicious user behavior, such as the use of scripts to simulate real user behavior to pass slider CAPTCHA verification, data risk control uses other verification methods to verify the user identity until the user passes verification. Then, the user is identified as a normal user. If the user fails the verification, data risk control blocks the request.

During this process, data risk control is enabled for the entire website (`www.aliyundoc.com`). Data risk control inserts a JavaScript plug-in into all web pages of the website to analyze user behavior. However, protection and verification are required only for `www.aliyundoc.com/register.html` to which users submit registration requests. Data risk control is triggered only when a registration request is submitted.

3.5. Application protection

3.5.1. Overview of app protection

Web Application Firewall (WAF) provides the app protection feature that allows you to use SDKs to protect native apps. This feature ensures trusted communications and provides anti-bot protection.

Security issues resolved by app protection

App protection is developed by Alibaba Group engineers who have years of experience defending against online attackers, exploiters, and unauthorized speculators. Apps that are integrated with Anti-Bot SDK can provide the same trusted communications as Alibaba apps, such as Tmall, Taobao, and Alipay. The apps are protected against online attackers, exploiters, and unauthorized speculators based on the library of malicious device fingerprints accumulated by Alibaba Group.

App protection provides solutions to the following security issues of native apps:

- Spam user registration, dictionary attacks, and brute-force attacks
- HTTP flood attacks against apps
- SMS flood attacks
- Promotion abuse and snatcher bots
- Auto-purchase bots
- Brushing, such as, brushing for air tickets or hotel reservations
- Crawling for valuable information, such as price, credit, financing, and fiction information
- Vote manipulation
- Spam and malicious comments

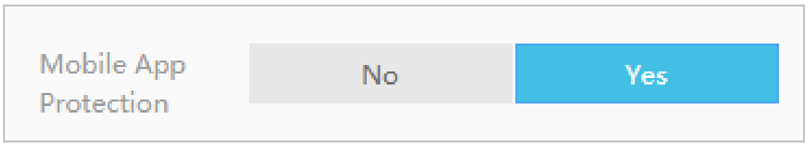
Procedure to enable app protection

The following steps show how to enable app protection:

1. Enable the app protection feature in the WAF console.

App protection is a value-added service provided by WAF. You must enable the app protection feature to use it. To enable the app protection feature, you can use one of the following methods:

- If WAF is not activated, activate WAF and set **Mobile App Protection** to Yes on the WAF buy page. For more information, see Purchase a WAF instance.

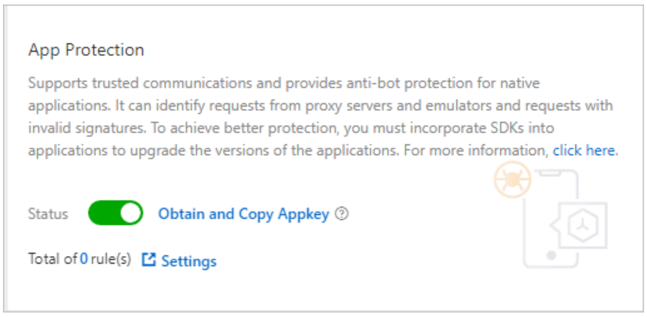


Mobile App Protection No [✓ Yes]

- If WAF is activated, upgrade the WAF instance and set **Mobile App Protection** to Yes on the Upgrade/Downgrade page. For more information, see Renewal and upgrade.

2. Log on to the console and choose **Protection Settings > Website Protection**. On the Bot Management tab of the Website Protection page, turn on **App Protection**. Then, configure app protection policies for the API that you want to protect. You can also turn on Version Protection based on your business requirements. For more information, see Configure application protection.

   After you turn on **App Protection**, you can click **Obtain and Copy Appkey** to obtain the `app key`. The app key is used in the integration code to send an SDK initialization request.



App Protection

Supports trusted communications and provides anti-bot protection for native applications. It can identify requests from proxy servers and emulators and requests with invalid signatures. To achieve better protection, you must incorporate SDKs into applications to upgrade the versions of the applications. For more information, click here.

Status ● Obtain and Copy Appkey

Total of 0 rule(s) Settings

3. Contact WAF technical support to obtain the Anti-Bot SDK package and integrate the package into your app.

   For more information about how to integrate the package into your app, see the following topics:

   - Integrate the Anti-Bot SDK into Android apps
   - Integrate the Anti-Bot SDK into iOS apps

   > **Note** SDK integration may take one or two man-days.

4. Add the domain name of your app to WAF. For more information, see Add a domain name.
5. Change the Domain Name System (DNS) record of the domain name to resolve the domain name to the CNAME assigned by WAF. For more information, see Change a DNS record.
6. Use your app to send test requests, and debug errors and exceptions based on the responses and log data. Make sure that Anti-Bot SDK is integrated into your app.
7. Release the latest version of your app.

   > **Notice** After you release the latest version of your app, we recommend that you push app updates to all devices. Otherwise, earlier versions of your app are still vulnerable to security risks.

3.5.2. SDK integration guide (new)

3.5.2.1. Integrate the Anti-Bot SDK into Android apps

This topic describes how to integrate the Anti-Bot SDK into Android apps. In this topic, Anti-Bot SDK is referred to as SDK. Before you can enable the app protection feature for your Android apps, you must integrate the SDK into your Android apps.

Limits

Your Android apps must use Android **16** or later. If the API version is earlier than 16, the SDK cannot work as expected.

Prerequisites

- The app protection feature is purchased and enabled.

  For more information, see Procedure to enable app protection.

- The SDK for Android apps is obtained.

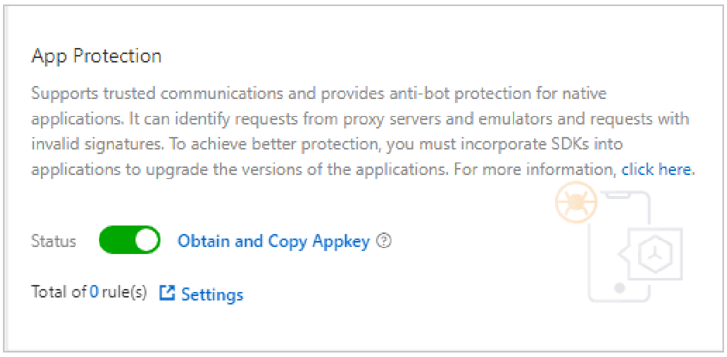
  After you purchase the app protection feature, you can contact technical support in the DingTalk service group to obtain the SDK. You can also submit a to obtain the SDK.

  The SDK for Android apps contains an **AAR** file, which is named in the following format: *AliTigerTally_X.Y.Z.aar*. *X.Y.Z* indicates the version number of the file.

- The SDK authentication key, namely the `app key`, is obtained.

  To obtain the app key, log on to the and choose **Protection Settings > Website Protection**. On the Bot Management tab of the Website Protection page, turn on **App Protection** and click **Obtain and Copy Appkey**. The SDK authentication key is used to send SDK initialization requests. The key must be included in the integration code.

  > **Note** Each Alibaba Cloud account has a unique `app key`, which can be used for all the domain names in your WAF instance. You can use the `app key`, regardless of whether you integrate the SDK into Android apps or iOS apps.

  App Protection

  Supports trusted communications and provides anti-bot protection for native applications. It can identify requests from proxy servers and emulators and requests with invalid signatures. To achieve better protection, you must incorporate SDKs into applications to upgrade the versions of the applications. For more information, click here.

  Authentication key example:

```
****OpKLvM6zliu6KopyHIhmneb_****u4ekci2W8i6F9vrgpEezqAzEzj2ANrVUhvAXMwYzgY_****vc51aEQlRo
vkRoUhRlVsf4IzO9dZp6nN_****Wz8pk2TDLuMo4pVIQvGaxH3vrsnSQiK****
```

Background information

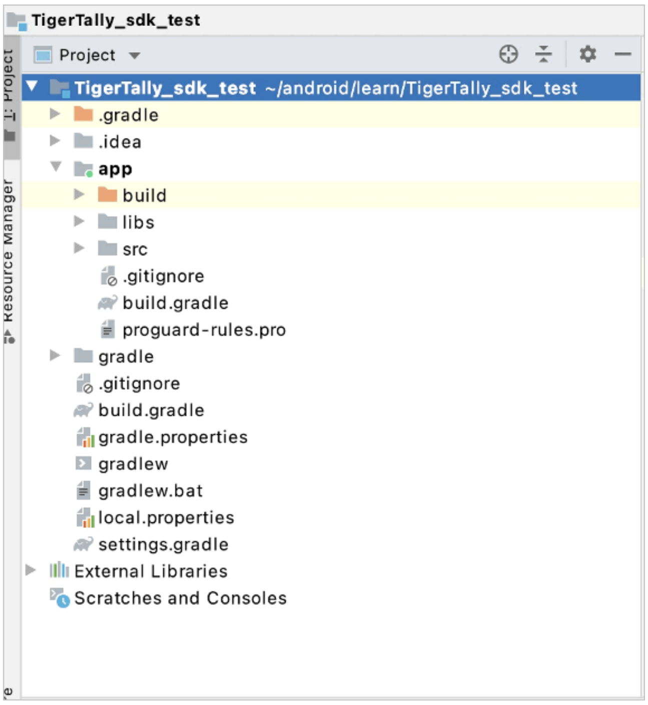
The SDK is used to sign requests that are sent by apps. Web Application Firewall (WAF) verifies the signatures in the requests to identify risks in app services and block malicious requests.

(Optional) Create a test Android project

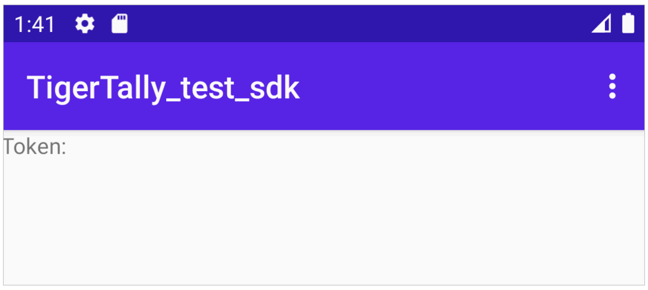
You can integrate the SDK into a real Android project. You can also integrate the SDK into a test Android project to familiarize yourself with the integration operations before you integrate the SDK into a real Android project.

In this example, use Android Studio to create a test Android project.

The following figure shows a test project named *TigerTally_sdk_test*.



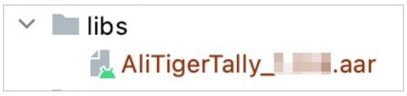
Before you integrate the SDK into apps, make sure that the test project runs as expected.



Token:

Procedure

1. Use Android Studio to open the test project and enter the file directory.
2. Reference the AAR file.
   i. Copy the *AliTigerTally.aar* file to the *libs* directory. You can also drag the file to the directory.



ii. Open the **build.gradle** file and modify the configurations based on the following descriptions:

- Add the *libs* directory as a source of dependencies.

```
repositories{
   flatDir {
     dirs 'libs'
   }
}
```

- Add a compilation dependency.

> **Notice** You must replace the version number (X.Y.Z) in the following code with the version number of the AAR file that you obtain.

```
dependencies {
  compile(name: 'AliTigerTally_X.Y.Z', ext: 'aar')
}
```

iii. Click **Sync Now** to synchronize the modifications to the project.

3. Reference an SO file.

If an SO file is included in the project, skip this step. Otherwise, add the following configuration to the **build.gradle** file:

```
android {
    defaultConfig {
    ndk {
        abiFilters 'arm64-v8a', 'x86', "armeabi-v7a"
        //abiFilters "armeabi-v7a"
      }
    }
}
```

4. Apply for the following permissions for apps.

Permission	Required	Description
android.permission.INTERNET	Yes	Connects to the Internet.
android.permission.ACCESS_NETWORK_STATE	No	Obtains the network status of a device.
android.permission.ACCESS_WIFI_STATE	No	Obtains the Wi-Fi connection status of a device.

Permission	Required	Description
android.permission.READ_PHONE_STATE	No	Reads the status and identity of a device. **Notice** You must dynamically apply for this permission for Android 6.0 or later apps.
android.permission.BLUETOOTH	No	Obtains the Bluetooth permissions of a device.
android.permission. READ_EXTERNAL_STORAGE	No	Reads the external storage of a device. **Notice** You must dynamically apply for this permission for Android 6.0 or later apps.
android.permission.CHANGE_NETWORK_STATE	No	Changes the network status of a device.

5. Add the integration code.

   i. Specify a user ID.

   Function:

```
int setAccount(String account);
```

   Description: specifies a user ID in requests. This way, you can configure WAF protection policies in a more efficient manner.

   Parameter: <account>, which specifies the user ID. Data type: string. We recommend that you enter a masked user ID.

   Return value: a value that indicates whether the setting is successful. Data type: int. The value *0* indicates that the setting is successful. The value *-1* indicates that the setting failed.

   Sample code:

```
final String account="account";
TigerTallyAPI.setAccount(account); // If the logon user is a guest, you do not need
to call this function. You can directly call the initialization function.
```

ii. Initialize the SDK.

Function:

```
int init(Context context, String appkey, int type);
```

Description: initializes the SDK and performs one-time information collection. One-time information collection allows you to collect terminal information for one time. If you want to collect terminal information again, call the `init` function.

One-time information collection supports two modes: full data collection and collection of data excluding sensitive fields. The sensitive fields include imei, imsi, simSerial, wifiMac, wifiList, and bluetoothMac of a user. To collect the sensitive fields, you must obtain permissions.

> **Note** Before a user agrees on the privacy policy of the apps, we recommend that you use the second mode. After a user agrees on the privacy policy of the apps, we recommend that you use the first mode. Full data collection helps identify risks.

Parameters:

- <context>: specifies the context that is passed to the apps.
- <appkey>: specifies the SDK authentication key. Data type: string.
- <type>: specifies the collection mode. Data type: CollectType. Valid values:
  - *DEFAULT*: full data collection.
  - *NO_GRANTED*: collection of data excluding sensitive fields.

Return value: a value that indicates whether the initialization is successful. Data type: int. The value *0* indicates that the initialization is successful. The value *-1* indicates that the initialization failed.

Sample code:

```
final String appkey="your_appkey";
// Collect full data.
int ret = TigerTallyAPI.init(this.getApplicationContext(), appkey, TigerTallyAPI.Co
llectType.DEFAULT);
// Collect data excluding sensitive fields.
int ret = TigerTallyAPI.init(this.getApplicationContext(), appkey, TigerTallyAPI.Co
llectType.NOT_GRANTED);
Log.d("AliSDK", "ret:" + ret);
```

iii. Sign request data.

Function:

```
String vmpSign(int signType, byte[] input);
```

Description: signs the input data and returns the signature string.

Parameters:

- <signType>: specifies the signature algorithm. Data type: int. Set the value to 1, which indicates that the default signature algorithm is used.
- <input>: specifies the data to be signed. Data type: byte[].

  In most cases, the data to be signed is the entire body of a request. If the POST request body is empty or a GET request body is used, enter `null` or a byte[] array that is converted from an empty string. Example: `"".getBytes("UTF-8")` .

Return value: the signature string. Data type: string.

Sample code:

> ⓘ **Note** In the following sample code, the signature string is defined as *wToken*.

```
String request_body = "i am the request body, encrypted or not!";
String wToken = null;
try {
    wToken = TigerTallyAPI.vmpSign(1, request_body.getBytes("UTF-8"));
} catch (UnsupportedEncodingException e) {
    e.printStackTrace();
}
Log.d("AliSDK", "wToken:" + wToken);
```

iv. Add the signature string to the HTTP header.

For example, if your project uses the `HttpURLConnection` class, you can add the content of the signature string *wToken* to the objects of the `HttpURLConnection` class.

Sample code:

```
String request_body = "i am the request body, encrypted or not!";
new Thread(new Runnable() {
    @Override
    public void run() {
        try {
            URL url = new URL("https://www.aliyundoc.com");
            HttpURLConnection conn = (HttpURLConnection) url.openConnection();
            conn.setReadTimeout(5000);
            conn.setRequestMethod("POST");
            // set wToken info to header
            conn.setRequestProperty("wToken", wToken);
            OutputStream os = conn.getOutputStream();
            // set request body info
            byte[] requestBody = request_body.getBytes("UTF-8");
            os.write(requestBody);
            os.flush();
            os.close();
            int code = conn.getResponseCode();
            Log.d("respCode", Integer.toString(code));
        } catch (MalformedURLException e) {
            e.printStackTrace();
        } catch (UnsupportedEncodingException e) {
            e.printStackTrace();
        } catch (ProtocolException e) {
            e.printStackTrace();
        } catch (IOException e) {
            e.printStackTrace();
        }
    };
    }).start();
```

v. Send requests that use the new HTTP header to the server of apps.

WAF receives requests that are destined for the server, parses the signature string *wToken* to identify and block malicious requests, and then forwards normal requests to the server.

Obfuscate code

If you use ProGuard to obfuscate code, you can use `-keep` to configure the functions of the SDK. This helps prevent the functions of the SDK from being removed.

Sample code:

```
-keep class com.aliyun.TigerTally.* {*;}
```

3.5.2.2. Integrate the Anti-Bot SDK into iOS apps

This topic describes how to integrate Anti-Bot SDK into iOS apps. In this topic, Anti-Bot SDK is referred to as SDK. Before you can enable the app protection feature for your iOS apps, you must integrate the SDK into your iOS apps.

Limits

Your iOS apps must use iOS **9.0** or later. If the API version is earlier than 9.0, the SDK cannot work as expected.

Prerequisites

- The app protection feature is purchased and enabled.

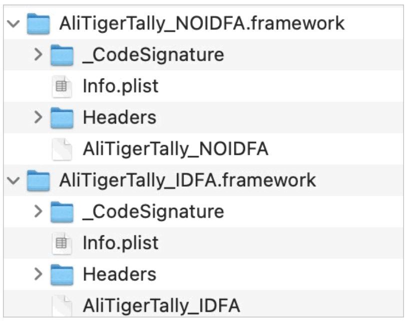
  For more information, see Procedure to enable app protection.

- The SDK for iOS apps is obtained.

  After you purchase the app protection feature, you can contact technical support in the DingTalk service group to obtain the SDK. You can also submit a to obtain the SDK.

  The SDK has two versions: Identifier for Advertising (IDFA) version and non-IDFA version. The two versions use the following SDK files:

  - *AliTigerTally_IDFA.framework*
  - *AliTigerTally_NOIDFA.framework*

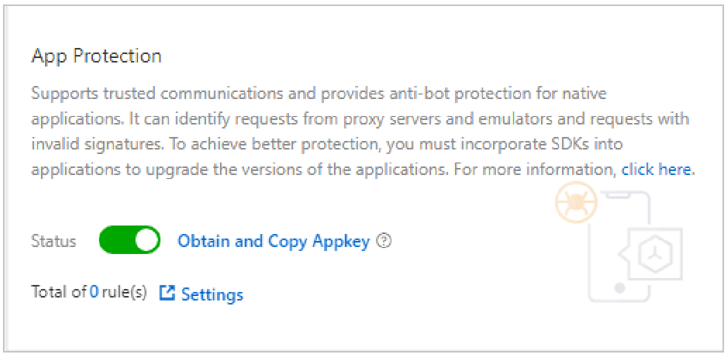
  AliTigerTally_NOIDFA.framework
  _CodeSignature
  Info.plist
  Headers
  AliTigerTally_NOIDFA
  AliTigerTally_IDFA.framework
  _CodeSignature
  Info.plist
  Headers
  AliTigerTally_IDFA

  If you use the IDFA version, we recommend that you integrate the SDK of the AliTigerTally_IDFA version into your iOS apps. If you use the non-IDFA version, we recommend that you integrate the SDK of the AliTigerTally_NOIDFA version into your iOS apps.

- The SDK authentication key, namely the `app key`, is obtained.

  To obtain the app key, log on to the and choose **Protection Settings > Website Protection**. On the Bot Management tab of the Website Protection page, turn on **App Protection** and click **Obtain and Copy Appkey**. The SDK authentication key is used to send SDK initialization requests. The key must be included in the integration code.

  > **Note** Each Alibaba Cloud account has a unique `app key`, which can be used for all the domain names in your WAF instance. You can use the `app key`, regardless of whether you integrate the SDK into Android apps or iOS apps.



App Protection

Supports trusted communications and provides anti-bot protection for native applications. It can identify requests from proxy servers and emulators and requests with invalid signatures. To achieve better protection, you must incorporate SDKs into applications to upgrade the versions of the applications. For more information, click here.

Status Obtain and Copy Appkey

Total of 0 rule(s) Settings

Authentication key example:

```
****OpKLvM6zliu6KopyHIhmneb_****u4ekci2W8i6F9vrgpEezqAzEzj2ANrVUhvAXMwYzgY_****vc51aEQlRo
vkRoUhRlVsf4IzO9dZp6nN_****Wz8pk2TDLuMo4pVIQvGaxH3vrsnSQiK****
```

Background information

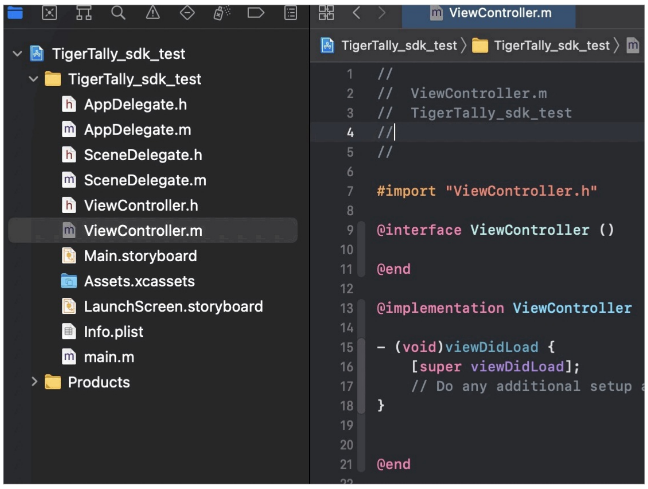
The SDK is used to sign requests that are sent by apps. Web Application Firewall (WAF) verifies the signatures in the requests to identify risks in app services and block malicious requests.

(Optional) Create a test iOS project

You can integrate the SDK into a real iOS project. You can also integrate the SDK into a test iOS project to familiarize yourself with the integration operations before you integrate the SDK into a real iOS project.

The following example shows how to use Xcode to create a test iOS project.

The following figure shows a test project named *TigerTally_sdk_test*.

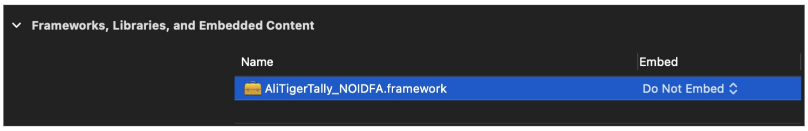


- TigerTally_sdk_test
  - TigerTally_sdk_test
    - AppDelegate.h
    - AppDelegate.m
    - SceneDelegate.h
    - SceneDelegate.m
    - ViewController.h
    - ViewController.m
    - Main.storyboard
    - Assets.xcassets
    - LaunchScreen.storyboard
    - Info.plist
    - main.m
  - Products

```
//
//  ViewController.m
//  TigerTally_sdk_test
//
//

#import "ViewController.h"

@interface ViewController ()

@end

@implementation ViewController

- (void)viewDidLoad {
    [super viewDidLoad];
    // Do any additional setup a
}


@end
```

Procedure

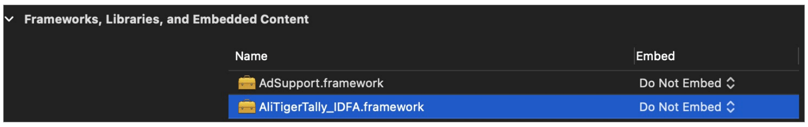
1. Use Xcode to open the test iOS project and enter the file directory.
2. Copy the SDK to the project.
   - The following figure shows the SDK of the non-IDFA version.



Frameworks, Libraries, and Embedded Content

Name	Embed
AliTigerTally_NOIDFA.framework	Do Not Embed

- The following figure shows the SDK of the IDFA version.

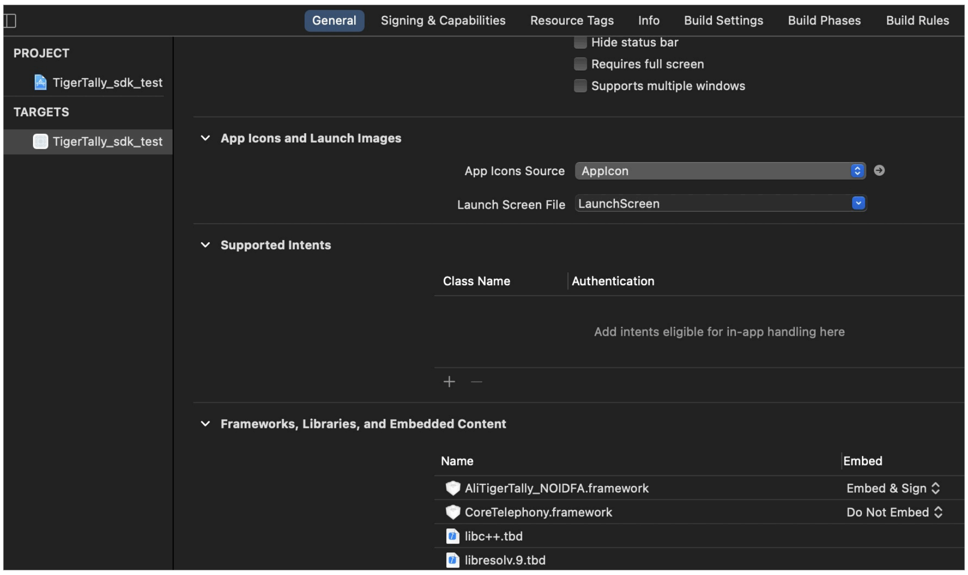


Frameworks, Libraries, and Embedded Content

Name	Embed
AdSupport.framework	Do Not Embed
AliTigerTally_IDFA.framework	Do Not Embed

3. Add dependency libraries to the project.

Dependency library	Non-IDFA	IDFA
libc++.tbd	Required	Required
CoreTelephony.framework	Required	Required
libresolv.9.tbd	Required	Required
AdSupport.framework	Not required	Required



App Icons and Launch Images

App Icons Source: AppIcon

Launch Screen File: LaunchScreen

Supported Intents

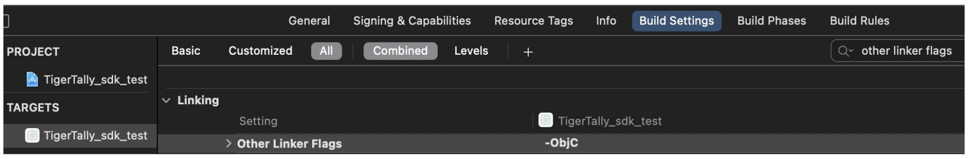
Class Name	Authentication

Add intents eligible for in-app handling here

Frameworks, Libraries, and Embedded Content

Name	Embed
AliTigerTally_NOIDFA.framework	Embed & Sign
CoreTelephony.framework	Do Not Embed
libc++.tbd	
libresolv.9.tbd	

4. Open **Build Settings** and add **-ObjC** to the **Other Linker Flags** option.



Linking

Setting	TigerTally_sdk_test
Other Linker Flags	-ObjC

5. Add the integration code.

i. Add a header file.

Sample code:

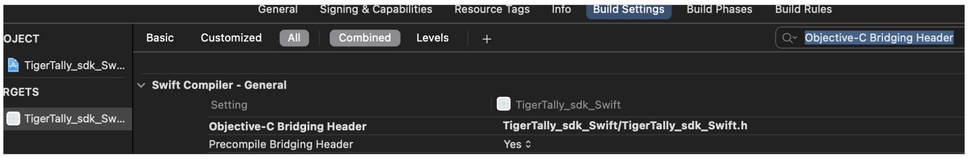
- Objective-C

```
// Non-IDFA version
#import <AliTigerTally_NOIDFA/AliTigerTally.h>
// IDFA version
#import <AliTigerTally_IDFA/AliTigerTally.h>
```

- Swift

```
// Create a header file.
#ifndef TigerTally_sdk_Swift_h
#define TigerTally_sdk_Swift_h
// Non-IDFA version
#import <AliTigerTally_NOIDFA/AliTigerTally.h>
// IDFA version
#import <AliTigerTally_IDFA/AliTigerTally.h>
#endif /* TigerTally_sdk_Swift_h */
```

You must add the header file that you create to the **Objective-C Bridging Header** option on **Build Settings**.



Objective-C Bridging Header TigerTally_sdk_Swift/TigerTally_sdk_Swift.h

Precompile Bridging Header Yes

ii. Specify a user ID.

Function:

```
-(void)setAccount:(NSString*)account
```

Description: configures a user ID in requests. This way, you can configure WAF protection policies in a more efficient manner.

Parameter: <account> which specifies the user ID. Data type: NSString*. We recommend that you enter a masked user ID.

Return value: none.

Sample code:

- Objective-C

```
// testAccount indicates an example of the user ID string.
//If the logon user is a guest, you do not need to call this function. You can di
rectly call the initialization function.
[[AliTigerTally sharedInstance] setAccount:@"testAccount"];
```

- Swift

```
// testAccount indicates an example of the user ID string.
//If the logon user is a guest, you do not need to call this function. You can di
rectly call the initialization function.
AliTigerTally.sharedInstance().setAccount("testAccount")
```

iii. Initialize the SDK.

Function:

```
-(bool)initialize:(NSString*)appKey
```

Description: initializes the SDK and performs one-time information collection. One-time information collection allows you to collect terminal information for one time. If you want to collect terminal information again, call the initialize function.

Interface parameter: <appKey> specifies the SDK authentication key. Data type: NSString*.

Return value: A value that indicates whether the initialization is successful. Data type: bool. The value true indicates that the initialization is successful. The value false indicates that the initialization failed.

Sample code:

- Objective-C

```
NSString *appKey=@"****OpKLvM6zliu6KopyHIhmneb_****u4ekci2W8i6F9vrgpEezqAzEzj2ANr
VUhvAXMwYzgY_****vc51aEQlRovkRoUhRlVsf4IzO9dZp6nN_****Wz8pk2TDLuMo4pVIQvGaxH3vrsn
SQiK****";
if([[AliTigerTally sharedInstance]initialize:appKey]){
    NSLog(@"The initialization is successful.");
 }else{
     NSLog(@"The initialization failed.");
}
```

- Swift

```
let binit = AliTigerTally.sharedInstance().initialize("****OpKLvM6zliu6KopyHIhmne
b_****u4ekci2W8i6F9vrgpEezqAzEzj2ANrVUhvAXMwYzgY_****vc51aEQlRovkRoUhRlVsf4IzO9dZ
p6nN_****Wz8pk2TDLuMo4pVIQvGaxH3vrsnSQiK****")
if(binit){
    NSLog("The initialization is successful.");
}else{
    NSLog("The initialization failed.");
}
```

iv. Sign request data.

Function:

```
-(NSString*)vmpSign:(NSData*)inputBody
```

Description: signs the input data and returns the signature string.

Parameter: <inputBody> which specifies the data body to be signed. Data type: NSData*.

Return value:

- Normal return results: A signature string is returned. Data type: NSString*.

- Abnormal return results

Return result	Description	Solution
`you must call initialize`	The `initialize` function is not called.	Call the `initialize` function to initialize the SDK. Then, call the `vmpSign` function.
`you must input body`	The data body to be signed is not specified.	When you call the `vmpSign` function, specify the data body <inputBody> to be signed.
`NULL`	The initialization is not complete, and request data failed to be signed.	Call the `vmpSign` function again. If this issue repeatedly occurs, contact technical support in the DingTalk service group. You can also submit a to contact technical support.

Sample code:

> ⓘ **Note** In the following sample code, the signature string is defined as *wToken*.

- Objective-C

```
if(![[AliTigerTally sharedInstance]initialize:@"xxxxxxxxxxxxxxxxxxxxx"])
{
        NSLog(@"The initialization failed.");
        return;
}
NSString *signBody =@"hello";
NSString *wToken= [[AliTigerTally sharedInstance] vmpSign:[signBody dataUsingEnco
ding:NSUTF8StringEncoding]];
NSLog(@"wToken== %@",wToken);
```

- Swift

```
if(!AliTigerTally.sharedInstance().initialize("xxxxxxxxxxxxxxxxxxxxx")){
    NSLog("The initialization failed.");
   return
}
let signBody = "hello"
var token = AliTigerTally.sharedInstance().vmpSign(signData)
NSLog(token);
```

v. Add the signature string to the header and send requests to the server of your iOS apps.

The signature string is submitted to the server for business-critical events, such as client logon request events. WAF receives requests that are destined for the server, parses the signature string *wToken* to identify and block malicious requests, and then forwards normal requests to the server.

Sample code:

- Objective-C

```
NSURL * url = [NSURL URLWithString:@"https://xxxxxx/test?id=123"];
NSMutableURLRequest *request=[NSMutableURLRequest requestWithURL:url cachePolicy:
NSURLRequestUseProtocolCachePolicy timeoutInterval:10];
[request setValue: wToken forHTTPHeaderField: @"wToken"];
request.HTTPMethod=@"post";
request.HTTPBody=[signBody dataUsingEncoding:NSUTF8StringEncoding];
NSURLSessionDataTask *dataTask = [[NSURLSession sharedSession] dataTaskWithReques
t:request completionHandler:^(NSData * _Nullable data, NSURLResponse * _Nullable
response, NSError * _Nullable error) {
    if(error){
        NSLog(@"The data fails to be sent.%@", error);
    }else
    {
        NSLog(@"The data is sent.");
    }
}];
[dataTask resume];
```

- Swift

```
guard let url = URL(string: "https://xxxxxx/test?id=123") else { return }
var request = URLRequest(url: url)
request.httpMethod = "POST"
request.addValue(token, forHTTPHeaderField: "wToken")
let session = URLSession.shared
session.dataTask(with: request) { (data, response, error) in
    if let data = data {
        do {
            print("OK")
        } catch {
            print("ERROR")
            print(error)
        }
    }
}.resume()
}
```

3.5.3. SDK integration guide (old)

3.5.3.1. Integrate the Anti-Bot SDK into Android applications

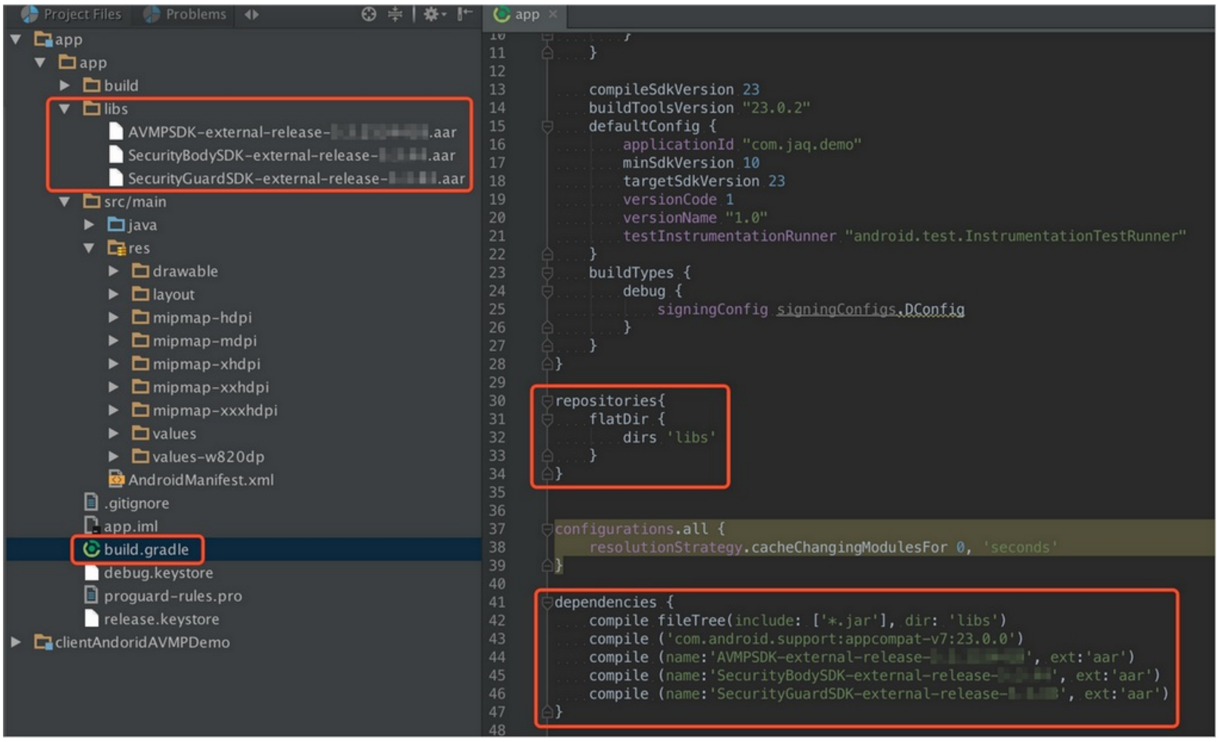
This topic describes how to integrate the Anti-Bot SDK into Android applications.

SDK files for Android applications

Contact Alibaba Cloud technical support to obtain the SDK package, and decompress it on your local machine. The following table describes the files contained in the *sdk-Android* folder.

File name	Description
SecurityGuardSDK-xxx.aar	The main framework.
AVMPSDK-xxx.aar	The virtual machine engine plug-in.
SecurityBodySDK-xxx.aar	The bot recognition plug-in.
yw_1222_0335_mwua.jpg	The configuration file of the virtual machine.

Configure an Android project



```
    }

    compileSdkVersion 23
    buildToolsVersion "23.0.2"
    defaultConfig {
        applicationId "com.jaq.demo"
        minSdkVersion 10
        targetSdkVersion 23
        versionCode 1
        versionName "1.0"
        testInstrumentationRunner "android.test.InstrumentationTestRunner"
    }
    buildTypes {
        debug {
            signingConfig signingConfigs.DConfig
        }
    }
}

repositories{
    flatDir {
        dirs 'libs'
    }
}


configurations.all {
    resolutionStrategy.cacheChangingModulesFor 0, 'seconds'
}

dependencies {
    compile fileTree(include: ['*.jar'], dir: 'libs')
    compile ('com.android.support:appcompat-v7:23.0.0')
    compile (name:'AVMPSDK-external-release-[redacted]', ext:'aar')
    compile (name:'SecurityBodySDK-external-release-[redacted]', ext:'aar')
    compile (name:'SecurityGuardSDK-external-release-[redacted]', ext:'aar')
}
```

1. Import the AAR files from the decompressed SDK package to Android Studio. Copy all the AAR files from the sdk-Android folder to the *libs* directory of the Android application project.

   > Note If the *libs* directory does not exist in the current project, manually create a folder named *libs* in the specified path.

2. Modify the configurations. Open the *build.gradle* file of the project and modify the configuration as follows.

   - Add the *libs* directory as the source for searching dependencies.

```
repositories{
   flatDir {
     dirs 'libs'
   }
}
```

- Add compilation dependencies.

  > Note The versions of the AAR files in this example may be different from those of the files you downloaded.

```
dependencies {
  compile fileTree(include: ['*.jar'], dir: 'libs')
  compile ('com.android.support:appcompat-v7:23.0.0')
  compile (name:'AVMPSDK-external-release-xxx', ext:'aar')
  compile (name:'SecurityBodySDK-external-release-xxx', ext:'aar')
  compile (name:'SecurityGuardSDK-external-release-xxx', ext:'aar')
}
```

3. Add the JPG configuration file from the decompressed SDK package to the *drawable* directory. Copy the *yw_1222_0335_mwua.jpg* configuration file in the *sdk-Android* folder to the *drawable* directory of the Android application project.

   > Note If the *drawable* directory does not exist in the project, create a folder named *drawable* in the specified path.

4. Remove redundant application binary interfaces (ABIs) because they require SO files. Currently, the Anti-Bot SDK only provides SO files for the following ABIs: armeabi, armeabi-v7a, and arm64-v8a.

   > Warning Therefore, you must filter out redundant ABIs. Otherwise, the application may crash.

   i. In the *libs* directory of the Android application project, delete all CPU architecture files other than *armeabi*, *armeabi-v7a*, and *arm64-v8a*, including *x86*, *x86_64*, *mips*, and *mips64*. Keep the *armeabi*, *armeabi-v7a*, and *arm64-v8a* folders only.

ii. As shown in the following sample code, add filter rules to the *build.gradle* configuration file of the application project. Architectures specified by abiFilters are included in the Android application package (APK) file.

> **Note** In this example, abiFilters only specifies the armeabi architecture. You can also specify the armeabi-v7a and arm64-v8 architectures as needed.

```
defaultConfig{
  applicationId "com.xx.yy"
  minSdkVersion xx
  targetSdkVersion xx
  versionCode xx
  versionName "x.x.x"
  ndk {
    abiFilters "armeabi"
    // abiFilters "armeabi-v7a"
    // abiFilters "arm64-v8a"
  }
}
```

> **Note** If you keep the SO files of the armeabi architecture only, you can significantly reduce the size of the application without affecting its compatibility.

5. Grant permissions to the application.

   - If you use an Android Studio project and AAR files to integrate the SDK, required permissions are already specified in the AAR files. You do not need to grant permissions to the application in the project.
   - If you use an Eclipse project, you must add the following permissions to the *AndroidMenifest.xml* file:

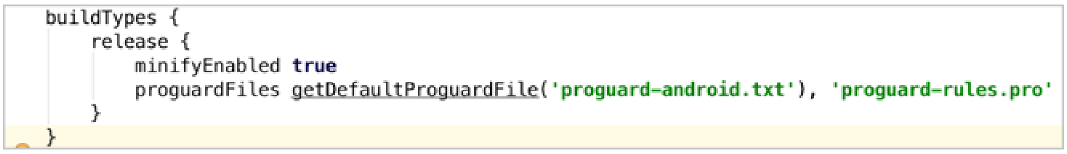
```
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
<uses-permission android:name="android.permission.WRITE_SETTINGS" />
```

6. Add ProGuard configurations.

> **Note** If you need to use ProGuard to obfuscate code, you must add ProGuard configurations. Methods to configure ProGuard in Android Studio and Eclipse are different.

   - Android Studio

If you have set the proguardFiles parameter and the minifyEnabled parameter is set to true in the *build.gradle* file, the *proguard-rules.pro* file is used to obfuscate code.



```
    buildTypes {
        release {
            minifyEnabled true
            proguardFiles getDefaultProguardFile('proguard-android.txt'), 'proguard-rules.pro'
        }
    }
```

- Eclipse

  If you have configured ProGuard in the *project.properties* file, such as adding the `proguard.config=proguard.cfg` statement to the *project.properties* file, ProGuard is used to obfuscate code.

  > Note Obfuscation configurations are specified in the *proguard.cfg* file.

Add keep rules

To guarantee that certain classes are not obfuscated, you must add the following rules to the ProGuard configuration file.

```
-keep class com.taobao.securityjni.**{*;}
-keep class com.taobao.wireless.security.**{*;}
-keep class com.ut.secbody.**{*;}
-keep class com.taobao.dp.**{*;}
-keep class com.alibaba.wireless.security. **{*;}
```

Call the SDK

Step 1: Import packages

```
import com.alibaba.wireless.security.jaq.JAQException;
import com.alibaba.wireless.security.jaq.avmp.IJAQAVMPSignComponent;
import com.alibaba.wireless.security.open.SecurityGuardManager;
import com.alibaba.wireless.security.open.avmp.IAVMPGenericComponent;
```

Step 2: Initialize the SDK

Endpoints: `boolean initialize();`

Function: Initializes the SDK.

Parameters: None.

Responses: Boolean values. If the initialization is successful, true is returned. If the initialization fails, false is returned.

Sample code

```
IJAQAVMPSignComponent jaqVMPComp = SecurityGuardManager.getInstance(getApplicationContext()
).getInterface(IJAQAVMPSignComponent.class);
boolean result = jaqVMPComp.initialize();
```

Step 3: Sign requests

Endpoints: `byte[] avmpSign(int signType, byte[] input);`

Function: Signs the input data by using the Ali Virtual Machine Protect (AVMP) technique, and returns a signature string.

Parameters

Parameter	Type	Required	Description
signType	int	Yes	The algorithm used to sign requests. Set the value to `3`.
input	byte[]	No	The data to be signed, which is typically the entire request body. **Note** If the request body is empty, for example, an empty POST or GET request body, enter null or the value of the Bytes parameter, such as "".getBytes("UTF-8").

Responses: A signature string of the byte[] data type.

Sample code: When the client sends data to the server, it must call the avmpSign method to sign the entire request body. A wToken signature string is returned.

```
int VMP_SIGN_WITH_GENERAL_WUA2 = 3;
String request_body = "i am the request body, encrypted or not!" ;
byte[] result = jaqVMPComp.avmpSign(VMP_SIGN_WITH_GENERAL_WUA2, request_body.getBytes("UTF-
8"));
String wToken = new String(result, "UTF-8");
Log.d("wToken", wToken);
```

Step 4: Add wToken to the protocol header

Add the content of the wToken field to the object of the HttpURLConnection class.

Sample code

```
String request_body = "i am the request body, encrypted or not!" ;
URL url = new URL("http://www.aliyundoc.com");
HttpURLConnection conn = (HttpURLConnection) url.openConnection();
conn.setRequestMethod("POST");
// set wToken info to header
conn.setRequestProperty("wToken", wToken);
OutputStream os = conn.getOutputStream();
// set request body info
byte[] requestBody = request_body.getBytes("UTF-8");
os.write(requestBody);
os.flush();
os.close();
```

Step 5: Send data to the server

Send data with the modified protocol header to the server of the application. Anti-Bot Service captures the data and parses the wToken to identify risks.

> **Warning** The signed request body must be the same as the original request body that is sent by the client. The string encoding format, spaces, special characters, and parameter sequence of the signed request body must be the same as those of the original request body sent by the client. Otherwise, the request fails to pass signature verification.

Error codes

Errors may occur when you call the initialize and avmpSigni methods. If an error occurs or the SDK fails to generate a signature string, use the keyword `SecException` to search for relevant information in the log data.

The following table describes common error codes.

Error code	Description
1901	The error code returned because the parameters are invalid. Check the parameters.
1902	The error code returned because the image file is invalid. The APK signature used to retrieve the image file is not the same as that of the application. Use the APK signature of the application to generate a new image.
1903	The error code returned because the format of the image file is invalid.
1904	Upgrade the image version. The AVMP signature function only supports v5 images.
1905	The error code returned because the specified image file cannot be found. Make sure that the image file is in the *res\drawable* directory, and AVMP images are in the *yw_1222_0335_mwua.jpg* file.

Error code	Description
1906	The error code returned because the AVMP signature of the image does not have the required bytecode. Check whether the image is invalid.
1907	The error code returned because the initialization of AVMP failed. Try again later.
1910	The error code returned because the AVMP instance is invalid. Possible causes include: ● The InvokeAVMP method was called after the AVMP instance had been destroyed. ● The version of the bytecode of the image does not match the SDK.
1911	The error code returned because the bytecode of the encrypted image does not have the required export function.
1912	The error code returned because the system failed to call AVMP. Contact Alibaba Cloud technical support.
1913	The error code returned because the InvokeAVMP method was called after the AVMP instance had been destroyed.
1915	The error code returned because the memory resources of the AVMP instance are insufficient. Try again later.
1999	The error code returned because an unknown error occurred. Try again later.

Verify the integration

Take the following steps to verify that the Anti-Bot SDK has been correctly integrated into the application.

1. Convert the packaged APK file into a ZIP file by modifying the file name extension, and decompress the file on your local machine.
2. Go to the *libs* directory of the project, and make sure that the folder only contains the *armeabi*, *armeabi-v7a*, and *arm64-v8a* sub-folders.

   > **Note** If any other architecture file exists, delete it. For more information, see Configure an Android project.

3. Go to the *res/drawable* directory of the project, and make sure that the *yw_1222_0335_mwua.jpg* file exists and its size is not 0.
4. Print the log, and make sure that the correct signature information can be generated after the avmpSign method is called.

> ⓘ **Note** If signature information cannot be generated, see the error codes and descriptions to troubleshoot.

FAQ

Why is the key image incorrectly optimized after shrinkResources is set to true?

In Android Studio, if shrinkResources is set to true, resource files that are not referenced in the code may be optimized during project compilation. After shrinkResources is set to true, JPG files in the Anti-Bot SDK may not work as expected. If the size of the *yw_1222_0335.jpg* configuration file in the packaged APK is 0 KB, it indicates that the image file has been optimized.

Solutions

1. Create a directory named *raw* in the *res* directory of the project, and create a file named *keep.xml* in the raw directory.
2. Add the following content to the *keep.xml file*:

```
<? xml version="1.0" encoding="utf-8"? >
<resources xmlns:tools="http://schemas.android.com/tools"
tools:keep="@drawable/yw_1222_0335.jpg,@drawable/yw_1222_0335_mwua.jpg" />
```

3. After you add the content, compile the project APK again.

3.5.3.2. Integrate the Anti-Bot SDK into iOS applications

This topic describes how to integrate the Anti-Bot SDK into iOS applications.

SDK files for iOS applications

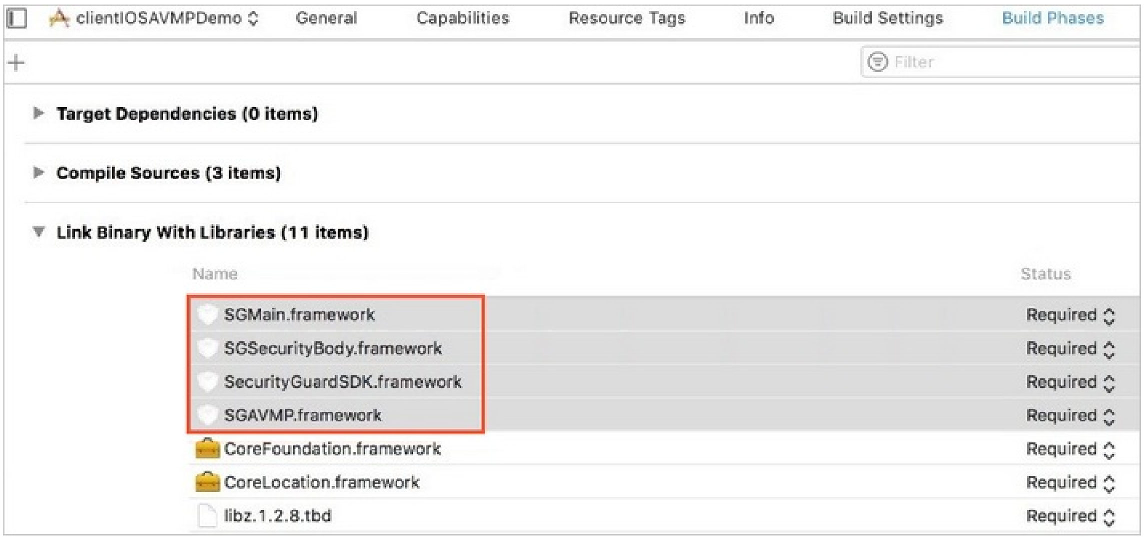
Contact Alibaba Cloud technical support to obtain the SDK package, and decompress it on your local machine. The following table describes the files contained in the *sdk-iOS* folder.

File name	Description
SGMain.framework	The main framework.
SecurityGuardSDK.framework	The basic security plug-in.
SGSecurityBody.framework	The bot recognition plug-in.
SGAVMP.framework	The virtual machine engine plug-in.
yw_1222_0335_mwua.jpg	Configuration files.

Configure an iOS project

1. Import the SDK dependency files. Import the following four .framework files extracted from the SDK package to the dependency library in an iOS project. The dependency library locates in the **Link Binary With Libraries** menu on the **Build Phases** tab.
    - *SGMain.framework*
    - *SecurityGuardSDK.framework*

- *SGSecurityBody.framework*
- *SGAVMP.framework*



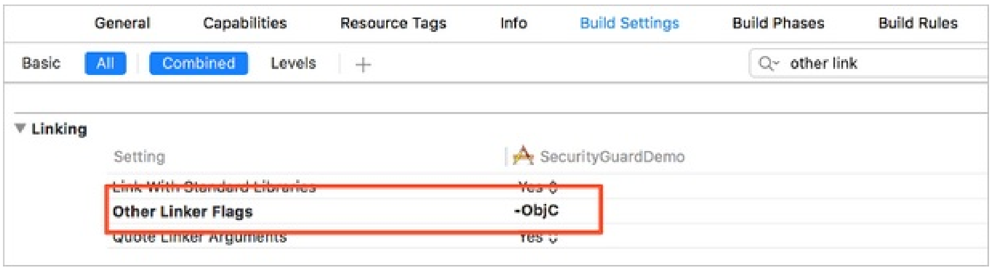
▶ Target Dependencies (0 items)

▶ Compile Sources (3 items)

▼ Link Binary With Libraries (11 items)

Name	Status
SGMain.framework	Required
SGSecurityBody.framework	Required
SecurityGuardSDK.framework	Required
SGAVMP.framework	Required
CoreFoundation.framework	Required
CoreLocation.framework	Required
libz.1.2.8.tbd	Required

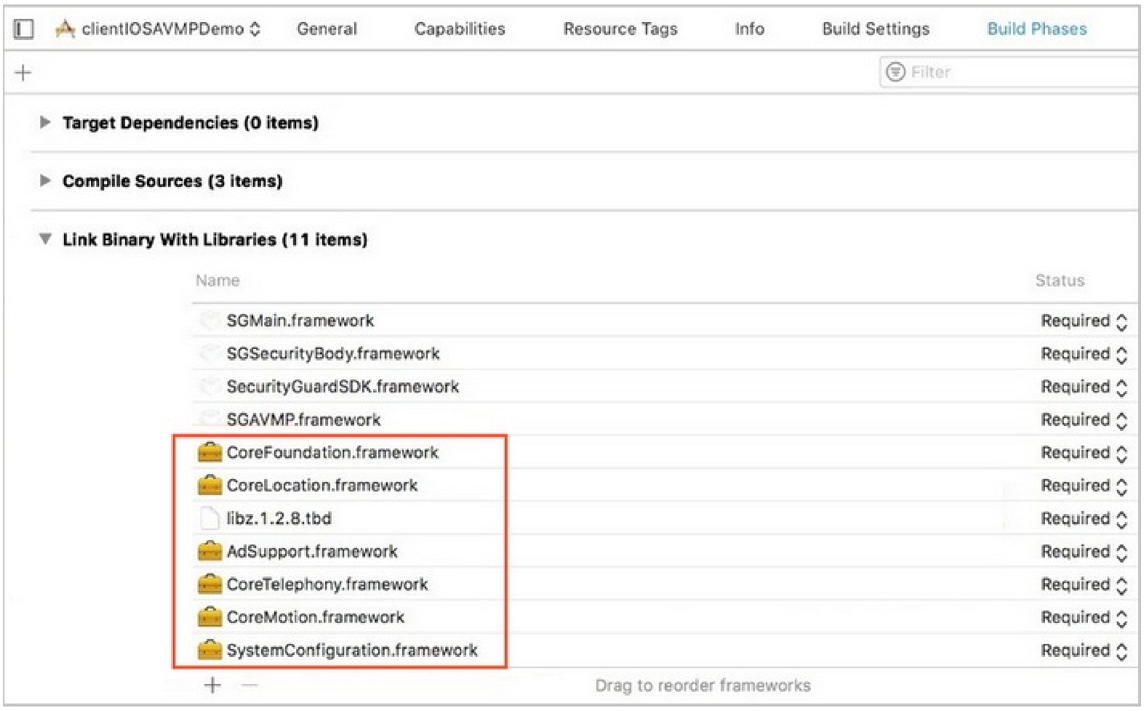
2. Add link options. On the **Build Settings** tab, choose **Linking** > **Other Linker Flags** to set the value to **-ObjC**.



▼ Linking

Setting	SecurityGuardDemo
Link With Standard Libraries	Yes
Other Linker Flags	-ObjC
Quote Linker Arguments	Yes

3. Import system dependency files. Import these files to the dependency library of an iOS project:
   - *CoreFoundation.framework*
   - *CoreLocation.framework*
   - *AdSupport.framework*
   - *CoreTelephony.framework*
   - *CoreMotion.framework*
   - *SystemConfiguration.framework*



Target Dependencies (0 items)

Compile Sources (3 items)

Link Binary With Libraries (11 items)

Name	Status
SGMain.framework	Required
SGSecurityBody.framework	Required
SecurityGuardSDK.framework	Required
SGAVMP.framework	Required
CoreFoundation.framework	Required
CoreLocation.framework	Required
libz.1.2.8.tbd	Required
AdSupport.framework	Required
CoreTelephony.framework	Required
CoreMotion.framework	Required
SystemConfiguration.framework	Required

Drag to reorder frameworks

4. Import the configuration file. Add the *yw_1222_0335_mwua.jpg* configuration file in the SDK package to the *mainbundle* directory.

> Notice When the application integrates multiple targets, make sure to add the `yw_1222_0335_mwua.jpg` configuration file to the correct target membership.

Call the SDK

Step 1: Initialize the SDK

Endpoint: `+ (BOOL) initialize;`

Function: Initializes the SDK.

Parameters: None.

Responses: Boolean. YES is returned if the initialization is successful. NO is returned if the initialization fails.

Call methods: `[JAQAVMPSignature initialize];`

Sample code

```
static BOOL avmpInit = NO;
- (BOOL) initAVMP{
  @synchronized(self) { // just initialize once
    if(avmpInit == YES){
      return YES;
    }
    avmpInit = [JAQAVMPSignature initialize];
    return avmpInit;
  }
}
```

Step 2: Sign the request

Endpoints: `+ (NSData*) avmpSign: (NSInteger) signType input: (NSData*) input;`

Function: Signs the input data by using the AVMP technique, and returns a signature string.

> **Warning** The signed request body must be the same as the request body that is sent by the client. That is, the string coding format, spaces, special characters, and parameter sequence of the signed request body must be the same as those of the request body sent by the client. Otherwise, signature verification may fail.

Request parameters

Parameter	Type	Required	Description
signType	NSInteger	Yes	The algorithm used to sign the request. Set the value to `3`.
input	NSData*	No	The data to be signed, which is typically the entire request body. **Note** If the request body is empty, for example, an empty POST or GET request body, enter null or the value of the Bytes parameter.

Responses: A signature string is returned.

Call methods: `[JAQAVMPSignature avmpSign: 3 input: request_body];`

Sample code

> **Note** When the client sends data to the server, you must call the avmpSign operation to sign the entire request body. Then, you will obtain a wToken signature string.

```
# define VMP_SIGN_WITH_GENERAL_WUA2 (3)
- (NSString*) avmpSign{
  @synchronized(self) {
    NSString* request_body = @"i am the request body, encrypted or not!" ;
    if(![ self initAVMP]){
      [self toast:@"Error: init failed"];
        return nil;
    }
    NSString* wToken = null;
    NSData* data = [request_body dataUsingEncoding:NSUTF8StringEncoding];
    NSData* sign = [JAQAVMPSignature avmpSign: VMP_SIGN_WITH_GENERAL_WUA2 input:data];
    if(sign == nil || sign.length <= 0){
      return nil;
    }else{
      wToken = [[NSString alloc] initWithData:sign encoding: NSUTF8StringEncoding];
      return wToken;
    }
  }
}
```

If the request body is empty, you must call the avmpSign operation to generate the wToken signature string. When you call this operation, set the value of the second parameter to null. Examples:

```
NSData* sign = [JAQAVMPSignature avmpSign: VMP_SIGN_WITH_GENERAL_WUA2 input:null];
```

Step 3: Add wToken to the protocol header

Sample code

```
#define VMP_SIGN_WITH_GENERAL_WUA2 (3)
-(void)setHeader
{ NSString* request_body = @"i am the request body, encrypted or not!" ;
  NSData* body_data = [request_body dataUsingEncoding:NSUTF8StringEncoding];
  NSString* wToken = nil;
  NSData* sign = [JAQAVMPSignature avmpSign: VMP_SIGN_WITH_GENERAL_WUA2 input:body_data];
  wToken = [[NSString alloc] initWithData:sign encoding: NSUTF8StringEncoding];
  NSString *strUrl = [NSString stringWithFormat:@"http://www.aliyundoc.com/login"];
  NSURL *url = [NSURL URLWithString:strUrl];
  NSMutableURLRequest *request =
    [[NSMutableURLRequest alloc]initWithURL:url cachePolicy:NSURLRequestReloadIgnoringCache
Data timeoutInterval:20];
  [request setHTTPMethod:@"POST"];
  // set request body info
  [request setHTTPBody:body_data];
  // set wToken info to header
  [request setValue:wToken forHTTPHeaderField:@"wToken"];
  NSURLConnection *mConn = [[NSURLConnection alloc]initWithRequest:request delegate:self st
artImmediately:true];
  [mConn start];
  // ...
}
```

Step 4: Send data to the server

Send the data with the modified protocol header to Alibaba Cloud Security, which analyzes the wToken for risk identification and malicious request interception, and then forwards valid requests to the origin server.

Error code

Errors may occur when you call the initialize and avmpSign operations. If the system fails to generate a valid signature string, see the information about security guard errors in the console.

The following table lists the common error codes and their descriptions.

Error code	Description
1901	The error code returned because the parameters are invalid. Check the parameters.
1902	The error code returned because the image file is invalid. The image may not match the bundle ID.
1903	The error code returned because the format of the image file is invalid.
1904	Upgrade the image version. The AVMP signature function only supports v5 images.
1905	The error code returned because the specified image file cannot be found. Make sure that the yw_1222_0335_mwua.jpg image file has been correctly added to the project.
1906	The error code returned because the AVMP signature of the image does not have the required bytecode. Check whether the image is invalid.
1907	The error code returned because the initialization of AVMP failed. Try again later.
1910	The error code returned because the AVMP instance is invalid. Possible causes include: • The AVMP instance is destroyed before InvokeAVMP is called. • The version of the bytecode of the image does not match the SDK.
1911	The byteCode of the encrypted image does not have the corresponding export function.
1912	The error code returned because the system failed to call AVMP. Contact Alibaba Cloud technical support.
1913	The error code returned because the InvokeAVMP method was called after the AVMP instance had been destroyed.

Error code	Description
1915	The error code returned because the memory resources of the AVMP instance are insufficient. Try again later.
1999	The error code returned because an unknown error occurred. Try again later.

3.5.4. Configure application protection

Application protection provides secure connections and anti-bot protection for native applications. This function identifies proxies, emulators, and requests with invalid signatures. This topic describes how to configure and enable application protection in the Web Application Firewall (WAF) console after you integrate the Anti-Bot SDK into an application.

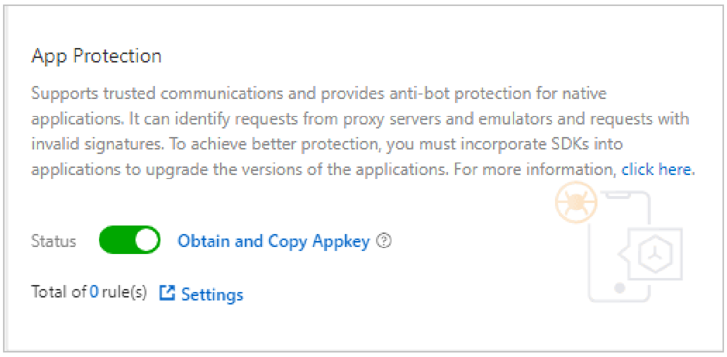
Prerequisites

-
- You have integrated the Anti-Bot SDK into the target application. For more information, see Overview of app protection.

Procedure

1.
2.
3.
4.
5. Click the **Bot Management** tab, find the **App Protection** section, and then click **Settings**.

   > ⓘ **Note** After application protection is enabled, all service requests are checked by the function. You can configure a Bot Management rule so that the requests that match the rule bypass the check. For more information, see Configure a whitelist for Bot Management.

   App Protection

   Supports trusted communications and provides anti-bot protection for native applications. It can identify requests from proxy servers and emulators and requests with invalid signatures. To achieve better protection, you must incorporate SDKs into applications to upgrade the versions of the applications. For more information, click here.

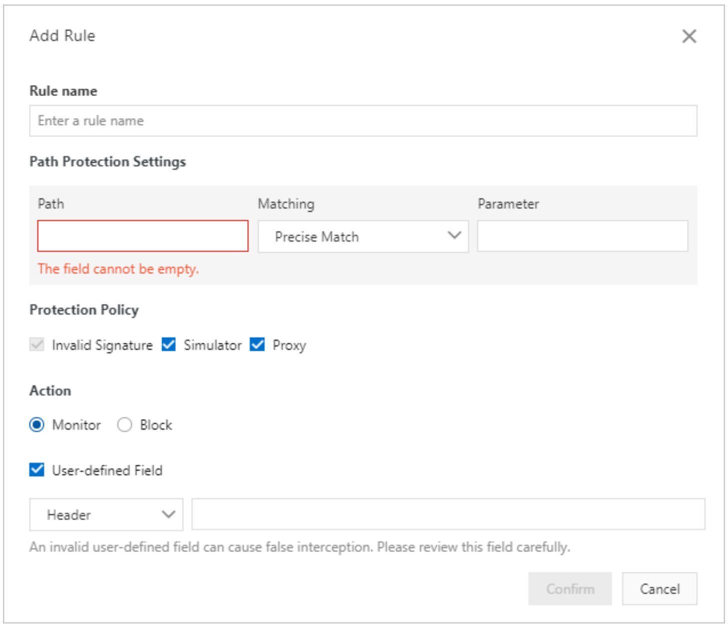
   Status ● Obtain and Copy Appkey

   Total of 0 rule(s) Settings

6. Create a path protection rule.

   i. On the **App Protection** page, find the **Interface Protection** section, and click **Add Rule**.

   ii. In the **Add Rule** dialog box that appears, set the following parameters.



Add Rule

Rule name

Enter a rule name

Path Protection Settings

Path	Matching	Parameter
	Precise Match	

The field cannot be empty.

Protection Policy

☑ Invalid Signature ☑ Simulator ☑ Proxy

Action

● Monitor ○ Block

☑ User-defined Field

Header

An invalid user-defined field can cause false interception. Please review this field carefully.

Note In the test phase, we recommend that you set **Path** to a forward slash (`/`) and **Matching** to **Prefix Match** to match all paths. You can set **Action** to **Monitor**. If the target domain name is a test domain name, you can set Action to **Block**. This allows you to debug the application without affecting your online workloads.

Parameter	Description
Rule Name	The name of the rule that you want to create.

Parameter	Description
Path Protection Settings	The path that you need to protect. The following parameters are required: - **Path**: The path that you need to protect. A forward slash (/) indicates all paths. Note Signature verification may fail when the body of a POST request exceeds 8 KB. We recommend that you disable SDK protection for API operations that do not require protection, for example, the API operation that is used to upload large images. If you do need to enable SDK protection for an API operation, use a user-defined field. - **Matching**: **Prefix Match**, **Precise Match**, and **Regular Expression Match** are supported. If you set the value to Prefix Match, all endpoints under the specified path are considered matches. If you set the value to Precise Match, only the specified path is considered a match. If you set the value to Regular Expression Match, paths specified by the regular express are considered matches. - **Parameter**: The parameters that need to be matched if the protected path contains invariable parameters. WAF can use these parameters to filter endpoints more precisely. The parameters are the parts following the question mark (?) in the request URL. Example: The protected URL contains `domain name/? action=login&name=test` . In this case, set **Path** to a forward slash (/), **Matching** to Prefix Match, and **Parameter** to name, login, name=test, and action=login.
Protection Policy	Protection policy that you want to use. - **Invalid Signature**: This policy is selected by default and cannot be cleared. The system checks whether the signatures of requests sent to the specified path are correct. The rule is matched if a signature is incorrect. - **Simulator**: If this policy is selected, the system checks whether the user uses an emulator to initiate requests to the specified path. The rule is matched if a request is initiated from an emulator. - **Proxy**: If this policy is selected, the system checks whether the user uses a proxy to initiate requests to the specified path. We recommend that you select this option. The rule is matched if a request is initiated from a proxy.

Parameter	Description
Action	The action to be performed on requests that match the rule. ■ **Monitor**: records the request but does not block the request. ■ **Block**: blocks the request and returns a 405 HTTP status code. **Notice** Before the SDK integration or debugging is completed, do not set Action to Block for domain names used in a production environment. Otherwise, valid requests may be blocked because the SDK is not properly integrated into the application. In the test phase, you can set Action to Monitor to debug the SDK-integrated application based on log data.
User-defined Field	When a user-defined field is used, the system verifies the request signature based on the specified request field and field value. By default, the system verifies the signature based on the request body. The verification may fail if the length of the request body exceeds 8 KB. In this case, you can specify a user-defined field to replace the default field for signature verification. If you select User-defined Field, you can choose Header, Parameter, or Cookie, and then specify the field that is used to verify the request signature. For example, you can choose **Cookie** and then enter DG_ZUID. This replaces the default body field with the DG_ZUID field in the request cookie as the field used for signature verification.

iii. Click **Confirm**.

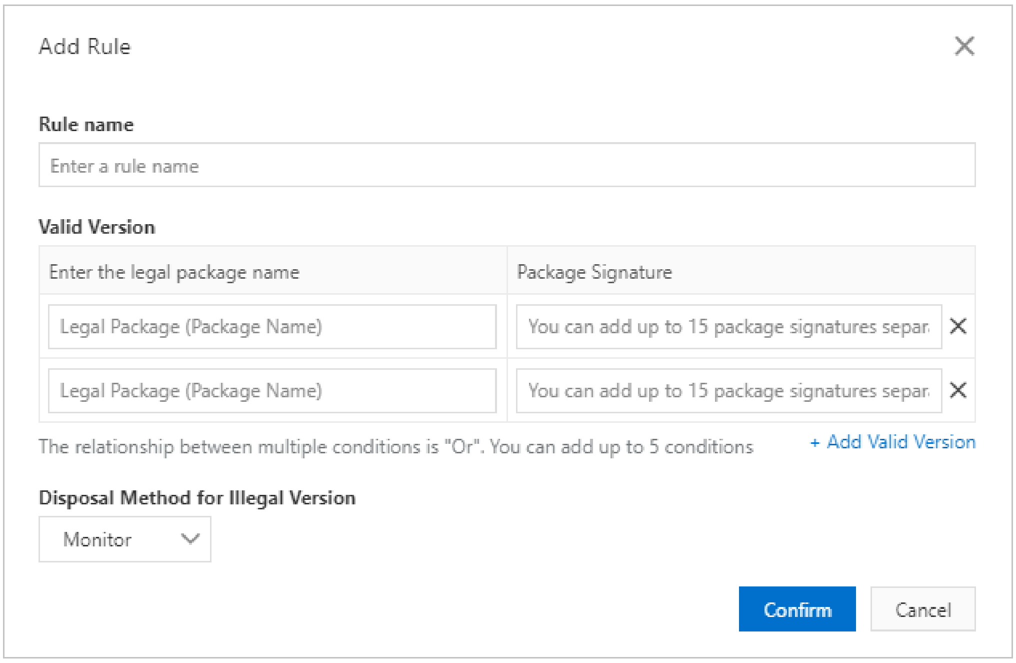
7. Enable version protection.

   You can configure version protection to block requests from non-official applications. You can also use this function to verify the validity of an application.

   > **Note** A version protection policy is required only when you need to verify the validity of an application.

   i. On the **App Protection** page, find the **Version Protection** section and turn on **Allow Specified Version Requests**.

   ii. In the **Add Rule** dialog box that appears, set the following parameters.


Add Rule

Rule name

Enter a rule name

Valid Version

Enter the legal package name	Package Signature
Legal Package (Package Name)	You can add up to 15 package signatures separ
Legal Package (Package Name)	You can add up to 15 package signatures separ

The relationship between multiple conditions is "Or". You can add up to 5 conditions

+ Add Valid Version

Disposal Method for Illegal Version

Monitor

Confirm Cancel

Parameter	Description
Rule Name	The name of the rule that you want to create.
Valid Version	The valid versions of an application. - **Enter the legal package name**: Enter the name of the valid application package, for example, *com.aliyundemo.example*. - **Package Signature**: Contact Alibaba Cloud technical support to obtain the package signature. This parameter is optional if the package signature does not need to be verified. In this case, the system verifies only the package name. Notice The **Package Signature** is not the signature of the application certificate. Click **Add Valid Version** to add more valid versions. You can add a maximum of five valid versions. Package names must be unique. Currently, both iOS and Android applications are supported. You can enter multiple valid versions to match the package names.
Disposal Method for Illegal Version	- **Monitor**: records the request but does not block the request. - **Block**: blocks the request and returns a 405 HTTP status code.

iii. Click **Confirm**.

8. Enable application protection. In the **App Protection** section, turn on **Status**.

> Note We recommend that you integrate the Anti-Bot SDK into the application, debug the application, and release the new version before you enable application protection to make sure that the protection settings take effect.

4.Access control and throttling

4.1. Configure HTTP flood protection

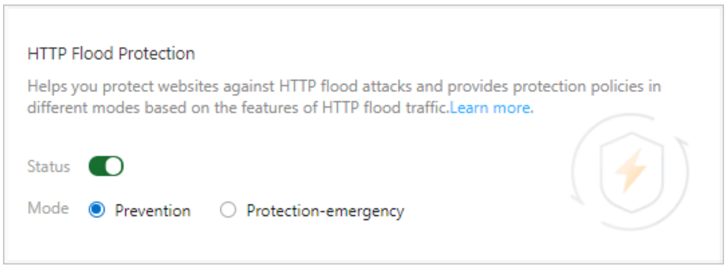
After you add a website to Web Application Firewall (WAF), HTTP flood protection is enabled by default and protects your website against HTTP flood attacks. When HTTP flood attacks are blocked, the 405 Method Not Allowed error code is returned. You can adjust HTTP flood protection policies as needed.

Prerequisite

-
-

Procedure

1.
2.
3.
4.
5. On the **Access Control/Throttling** tab, find the **HTTP Flood Protection** section and configure the following parameters.



HTTP Flood Protection

Helps you protect websites against HTTP flood attacks and provides protection policies in different modes based on the features of HTTP flood traffic.Learn more.

Status

Mode ● Prevention ○ Protection-emergency

Parameter	Description
Status	Enable or disable HTTP flood protection. By default, HTTP flood protection is enabled after you add a website to WAF. **Note** After HTTP flood protection is enabled, all requests destined for your website are checked by this function. You can configure a **Access Control/Throttling** rule so that requests that match the rule bypass the check. For more information, see Configure a whitelist for Access Control/Throttling.

Parameter	Description
Mode	The protection mode. Valid values: ○ **Protection**: This mode blocks only suspicious requests and maintains a low false positive rate. We recommend that you apply this mode when no abnormal traffic is detected on the website to avoid false positives. ○ **Protection-emergency**: This mode effectively blocks HTTP flood attacks but maintains a high false positive rate. You can apply this mode if the Protection mode fails to block HTTP flood attacks, the website responds slowly, and indicators such as traffic, CPU, and memory are abnormal. **Note** The Protection-emergency mode is applicable to web pages and HTML5 pages. This mode is not suitable for APIs or native applications because a large number of false positives may occur. We recommend that you create custom protection policies for API and native applications scenarios. For more information, see Create a custom protection policy.

References

- If you find that the **Protection-emergency** mode cannot block a large number of attacks, we recommend that you check whether the attacks come from back-to-origin IP addresses of WAF. If the origin server is directly attacked, you can change the settings to allow only requests from the back-to-origin IP addresses of WAF. For more information, see Configure protection for an origin server.
- If you need to reinforce protection and maintain a low false positive rate, we recommend that you use the custom protection policy. For more information, see Create a custom protection policy.

4.2. Configure a blacklist

After you add a website to Web Application Firewall (WAF), you can enable the blacklists feature. This feature blocks access requests from specified IP addresses, Classless Inter-Domain Routing (CIDR) blocks, and IP addresses in specified regions. You can specify either an IP address blacklist or a region blacklist based on your requirements.

Background information

WAF supports both IP address and region blacklists.

- An IP address blacklist blocks access requests from specified IP addresses and CIDR blocks.
- A region blacklist blocks the access requests from administrative regions in China or countries and areas outside China.

Prerequisites

- A WAF instance is purchased. The instance runs the **Pro**, **Business**, **Enterprise** or **Exclusive**.

> Notice WAF instances of the **Pro** and **Business** edition support only the **IP Address Blacklist** feature and do not support the **Region Blacklist** feature.
>
> To use the **Region Blacklist** feature, your WAF instance must run the **Enterprise** or **Exclusive** edition.

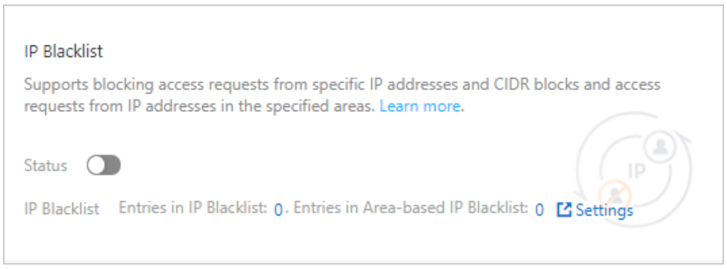
For more information, see Purchase a WAF instance.

-

Procedure

1.
2.
3.
4.
5. On the **Access Control/Throttling** tab, find the **Blacklists** section. Then, turn on **Status** and click **Settings**.

   > Note If you specify an IP address blacklist, all requests destined for your website are checked by this blacklist. You can also configure the whitelist for **Access Control/Throttling** to allow requests that match rules to bypass the check. For more information, see Configure a whitelist for Access Control/Throttling.

   IP Blacklist

   Supports blocking access requests from specific IP addresses and CIDR blocks and access requests from IP addresses in the specified areas. Learn more.

   Status

   IP Blacklist Entries in IP Blacklist: 0. Entries in Area-based IP Blacklist: 0 Settings

6. On the **Blacklists** page, configure **Blacklists** and **Region Blacklist**.
   - **Blacklists**: Enter IP addresses that you want to block and click **Save** in the lower part of the page. Separate multiple IP addresses with commas (,). You can add a maximum of 200 IP addresses.
   - **Region Blacklist**: Select the administrative regions that you want to block from the **Inside China** tab and countries and areas from the **Outside China** tab. Then, click **Save** in the lower part of the page.

     After the blacklists feature is enabled, all the access requests from IP addresses and regions in the blacklists are blocked.

References

- If you need more precise access control based on blacklists, we recommend that you use a custom protection policy. For more information, see Create a custom protection policy.
- If you want to allow access requests from specified IP addresses, we recommend that you configure the whitelist for **Access Control/Throttling**. For more information, see Configure a whitelist for Access Control/Throttling.

4.3. Configure scan protection

After you add a website to Web Application Firewall (WAF), you can enable the scan protection feature for your website. After the scan protection feature is enabled, access requests from specific IP addresses are automatically blocked. These IP addresses include source IP addresses that initiate high-frequency web attacks and malicious directory traversal attacks, and IP addresses defined in common scanners or the Alibaba Cloud malicious IP library.

Prerequisites

- A WAF instance is purchased. The instance runs the **Pro** edition or higher.

  > **Notice** WAF instances of the Pro edition support only default scan protection policies. You cannot configure custom scan protection policies for WAF instances of the Pro edition. If you need to configure custom policies for **Blocking IPs Initiating High-frequency Web Attacks** and **Directory Traversal Prevention**, the instance must run the **Business** edition or higher.

  For more information, see Purchase a WAF instance.

-

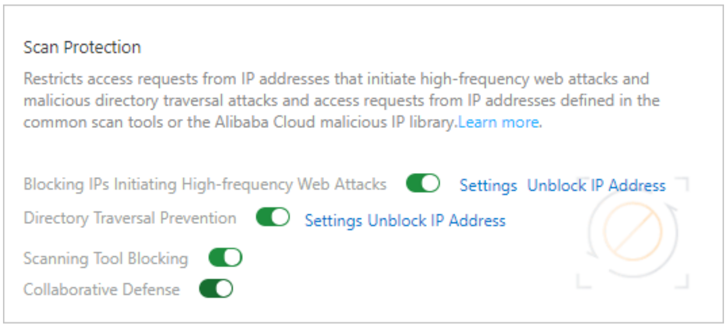
Background information

The scan protection feature provides the following scan protection policies:

- **Blocking IPs Initiating High-frequency Web Attacks**: automatically blocks client IP addresses that initiate multiple web attacks within a short period of time. You can configure custom scan protection policies and manually unblock a blocked IP address.
- **Directory Traversal Prevention**: automatically blocks client IP addresses that initiate multiple directory traversal attacks in a short period of time. You can configure custom scan protection policies and manually unblock a blocked IP address.
- **Scanning Tool Blocking**: automatically blocks access requests from IP addresses defined in common scanners. The scanners include sqlmap, AWVS, Nessus, AppScan, WebInspect, Netsparker, Nikto, and RSAS.
- **Collaborative Defense**: automatically blocks access requests from IP addresses defined in the Alibaba Cloud malicious IP library.

Procedure

1.
2.
3.
4.
5. On the **Access Control/Throttling** tab, find the **Scan Protection** section and configure the following settings:



Scan Protection

Restricts access requests from IP addresses that initiate high-frequency web attacks and malicious directory traversal attacks and access requests from IP addresses defined in the common scan tools or the Alibaba Cloud malicious IP library.Learn more.

Blocking IPs Initiating High-frequency Web Attacks ● Settings Unblock IP Address

Directory Traversal Prevention ● Settings Unblock IP Address

Scanning Tool Blocking ●

Collaborative Defense ●

> ⓘ **Note** By default, all requests destined for your website are checked by the scan protection feature when any policy in this section is enabled. If you want requests that match specific conditions to bypass the check, configure the whitelist for **Access Control/Throttling**. For more information, see Configure a whitelist for Access Control/Throttling.

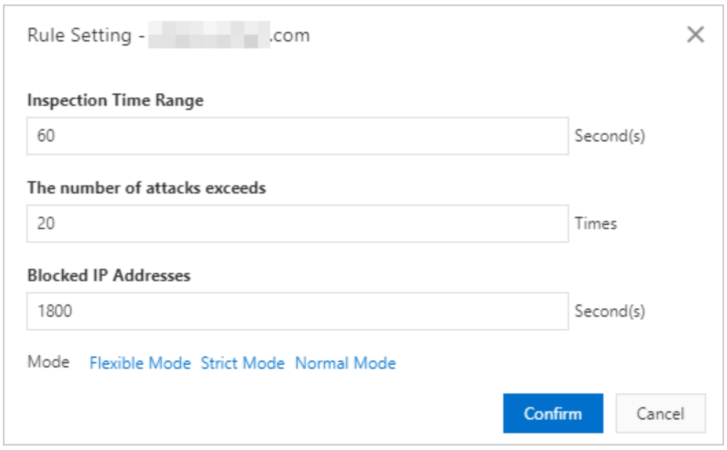
- **Blocking IPs Initiating High-frequency Web Attacks**: You can enable or disable it.

  Configure the protection policy.

  a. Turn on Blocking IPs Initiating High-frequency Web Attacks.

  b. Click **Settings**.

  c. In the **Rule Setting** dialog box, specify the following parameters: **Inspection Time Range**, **The number of attacks exceeds**, and **Blocked IP Addresses**.

  Rule Setting - [redacted].com

  Inspection Time Range: 60 Second(s)

  The number of attacks exceeds: 20 Times

  Blocked IP Addresses: 1800 Second(s)

  Mode: Flexible Mode Strict Mode Normal Mode

  If the number of web attacks initiated from a client IP address in the specified inspection time range exceeds a specific number, the access requests from this IP address are blocked during the specified blocking period.

  > ⓘ **Note** We recommend that you select a built-in configuration mode from **Flexible Mode**, **Strict Mode**, and **Normal Mode** in the **Mode** section. You can modify the parameters based on your requirements.

  d. Click **Confirm**.

  You can click **Unblock IP Address** to unblock IP addresses that are blocked by the policy.

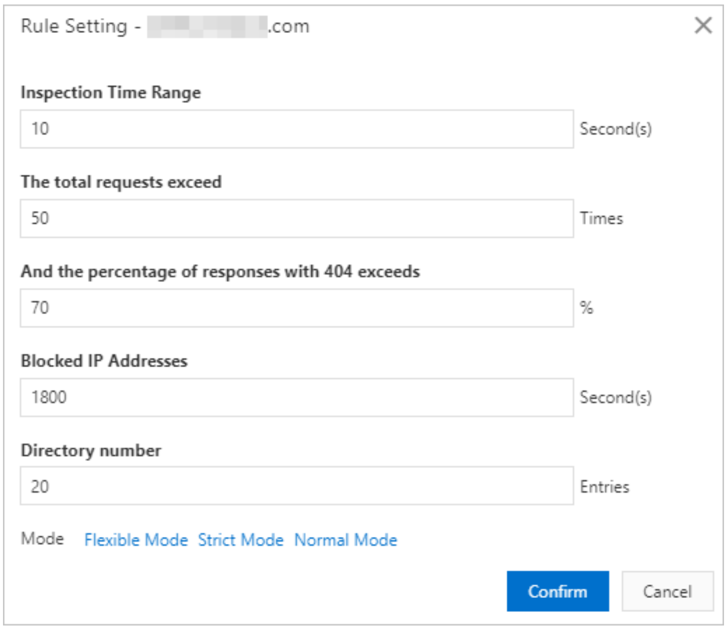
- **Directory Traversal Prevention**: You can enable or disable it.

  Configure the protection policy.

a. Turn on Directory Traversal Prevention.

b. Click **Settings**.

c. In the **Rule Setting** dialog box, specify the following parameters: **Inspection Time Range**, **The total requests exceed**, **And the percentage of responses with 404 exceeds**, **Blocked IP Addresses**, and **Directory number**.



Rule Setting - [redacted].com

Inspection Time Range

10 Second(s)

The total requests exceed

50 Times

And the percentage of responses with 404 exceeds

70 %

Blocked IP Addresses

1800 Second(s)

Directory number

20 Entries

Mode Flexible Mode Strict Mode Normal Mode

If the total number of requests initiated from a client IP address in the specified inspection time range exceeds a specific number and the proportion of the requests for which the HTTP status code 404 is returned to the total requests exceeds a specific proportion, or the number of directories to which requests are sent within the specified inspection time range exceeds a specific number, the access requests from this IP address are blocked during the specified blocking period.

> **Note** We recommend that you select a built-in configuration mode from **Flexible Mode**, **Strict Mode**, and **Normal Mode** in the **Mode** section. You can modify the parameters based on your requirements.

d. Click **Confirm**.

You can click **Unblock IP Address** to unblock IP addresses that are blocked by the policy.

- **Scanning Tool Blocking**: You can enable or disable it.

  After you enable Scanning Tool Blocking, the behavior of common scanners is automatically detected. If an access request meets the characteristics of scanning, this request is always blocked. If you disable Scanning Tool Blocking, scanning behavior is no longer blocked.

- **Collaborative Defense**: You can enable or disable it.

  After you enable Collaborative Defense, all access requests from the IP addresses in the Alibaba Cloud malicious IP library are blocked.

4.4. Create a custom protection policy

After you add a website to Web Application Firewall (WAF), you can enable the custom protection policy feature to protect the website. This feature allows you to customize access control list (ACL) rules based on precise match conditions and configure rate limiting. Custom protection policies can be tailored for different scenarios, such as hotlink protection and website backend protection.

Prerequisites

-
-

Background information

The custom protection policy feature is implemented by using custom protection rules. Custom protection rules include ACL rules and HTTP flood protection rules.

- An ACL rule filters requests based on precise match conditions such as client IP addresses, request URLs, and common request headers.
- An HTTP flood protection rule filters requests based on the precise match conditions and rate limiting you have configured.

Limits

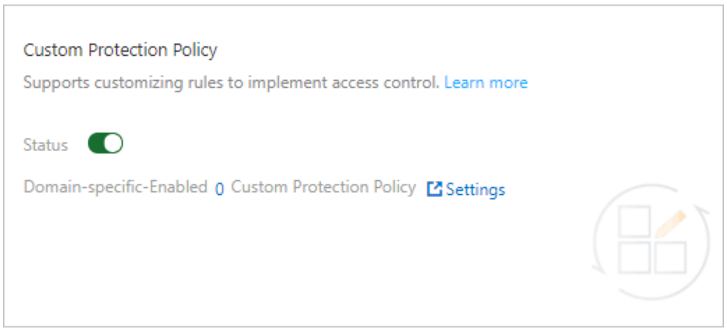
The number and specifications of custom rules that can be configured vary based on the editions of subscription WAF instances.

Specification	Description	Pro edition	Business edition	Enterprise edition and higher
Number of custom protection rules	The maximum number of custom protection rules that you can create.	200 per domain name	200 per domain name	200 per domain name
Advanced match fields	The advanced match fields other than IP addresses and URLs that you can specify in custom protection rules.	Not supported	Supported	Supported
Rate limiting	The rate limiting settings in a custom protection policy. The settings define an HTTP flood protection rule.	Not supported	Supported	Supported
Custom statistical objects	The custom statistical objects other than IP addresses and sessions that can be used to configure rate limiting.	Not supported	Supported	Supported

Procedure

1.
2.
3.
4.
5. Click the **Access Control/Throttling** tab and find the **Custom Protection Policy** section. Then,

turn on **Status** and click **Settings**.



Custom Protection Policy

Supports customizing rules to implement access control. Learn more

Status

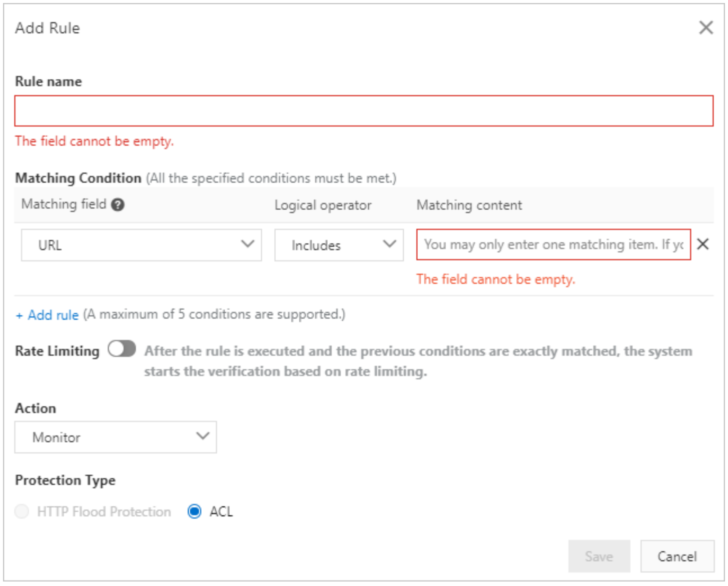
Domain-specific-Enabled 0 Custom Protection Policy Settings

Note When the custom protection policy feature is enabled, all requests destined for your website are checked by the feature. You can configure a whitelist rule for Access Control/Throttling to allow requests that match the whitelist rule to bypass the check. For more information, see Configure a whitelist for Access Control/Throttling.

6. Create a custom protection rule.

   i. On the **Custom Protection Policy** page, click **Create Custom Protection Policy**.

   ii. In the **Create Rule** dialog box, configure the following parameters.



Add Rule

Rule name

The field cannot be empty.

Matching Condition (All the specified conditions must be met.)

Matching field	Logical operator	Matching content
URL	Includes	You may only enter one matching item. If yo
		The field cannot be empty.

+ Add rule (A maximum of 5 conditions are supported.)

Rate Limiting After the rule is executed and the previous conditions are exactly matched, the system starts the verification based on rate limiting.

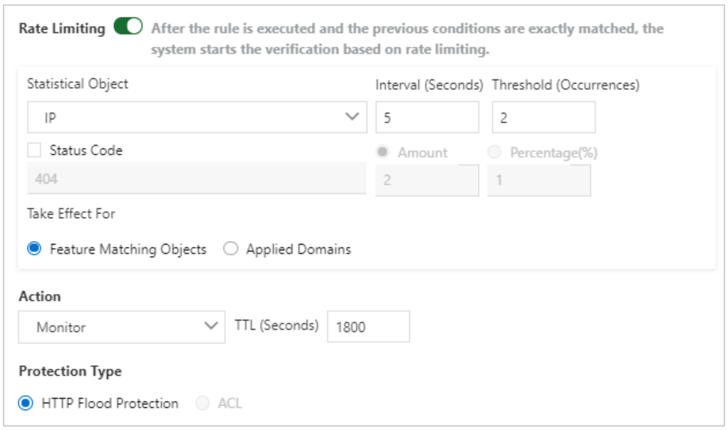
Action

Monitor

Protection Type

○ HTTP Flood Protection ● ACL

Parameter	Description
Rule name	The name of the rule that you want to create.
Matching Condition	The match conditions of the rule. The rule is triggered only when match conditions are met. Click **Add rule** to add more conditions. You can add a maximum of five conditions. If you specify multiple match conditions, the rule is triggered only after all the match conditions are met. For more information about conditions, see Fields in match conditions.

Parameter	Description
Rate Limiting	Enables or disables rate limiting. WAF starts calculating the request rate only when match conditions are met. When you enable rate limiting, you must configure the parameters to collect statistics.  Rate Limiting: on. After the rule is executed and the previous conditions are exactly matched, the system starts the verification based on rate limiting. Statistical Object: IP Interval (Seconds): 5 Threshold (Occurrences): 2 □ Status Code: 404 ● Amount: 2 ○ Percentage(%): 1 Take Effect For: ● Feature Matching Objects ○ Applied Domains Action: Monitor TTL (Seconds): 1800 Protection Type: ● HTTP Flood Protection ○ ACL For more information about rate limiting parameters, see Rate limiting parameters.
Action	The action to be performed after the rule is triggered. Valid values: - **Monitor**: triggers alerts but does not block requests. - **Block**: blocks requests. - **CAPTCHA**: redirects requests to another page to implement CAPTCHA verification. - **Strict Captcha**: redirects requests to another page to implement strict CAPTCHA verification. - **JavaScript Validation**: triggers JavaScript verification. If you enable **Rate Limiting**, you must specify **TTL (Seconds)** during which the action takes effect. **Note** A certain latency may exist in the statistical process because WAF collects data from multiple servers in a cluster to calculate the request rate.
Protection Type	The type of the rule. This parameter is automatically set based on the status of **Rate Limiting**. - If rate limiting is enabled, the value is set to **HTTP Flood Protection**. - If rate limiting is disabled, the value is set to **ACL**.

The following table describes the rate limiting parameters.

Parameter	Description
Statistical Object	The object based on which the request rate is calculated. Valid values: ■ **IP**: calculates the number of requests from a specific IP address. ■ **Session**: calculates the number of requests transmitted over a specific session. ■ **Custom-Header**: calculates the number of requests with the same specified header content. ■ **Custom-Param**: calculates the number of requests with the same specified parameter content. ■ **Custom-Cookie**: calculates the number of requests with the same specified cookie content.
Interval (Seconds)	The time period during which the number of requests is calculated.
Threshold (Occurrences)	The maximum number of requests that are allowed from the object during the specified time period. If this limit is exceeded, rate limiting is triggered.
Status Code	The HTTP status code. After the detection logic takes effect, the number or percentage of the specified **Status Code** within the specified time period is calculated. Select either the amount or the percentage. ■ **Amount**: the maximum number of the specified HTTP status codes. ■ **Percentage (%)**: the maximum percentage of the requests for which the specified HTTP status code is returned in the total requests.
Take Effect For	The objects to which rate limiting is applied. Valid values: ■ **Feature Matching Objects**: Only requests that meet the **match conditions** of the protection rule are calculated. ■ **Applied Domains**: All requests that are destined for the domain name are calculated.

iii. Click **Save**.

After a custom protection rule is created, it is automatically enabled. You can view, disable, edit, or delete the rule in the rule list based on your business requirements.

Related information

- Fields in match conditions

5.Whitelist

5.1. Configure a website whitelist

After you add a website to Web Application Firewall (WAF), you can configure a website whitelist to allow trusted access requests of the website to be directly routed to the origin server. Trusted access requests include requests from trusted vulnerability scan tools and trusted authenticated third-party system endpoints.

Prerequisites

-
-

Background information

WAF provides multiple detection modules. If a website is added to WAF, all requests to this website are automatically detected by the modules that are enabled. To directly route trustworthy requests to your origin server, you can configure a website whitelist that allows the requests to bypass all detection modules of WAF.

You can also configure a whitelist for a specific detection module. This allows trusted access requests to bypass the detection of the specific detection module. You can configure the following types of whitelists:

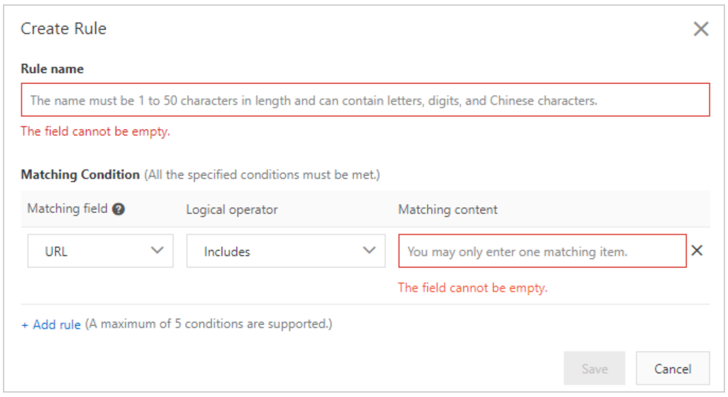
- Whitelist for Web Intrusion Prevention: Trusted access requests are not detected by RegEx Protection Engine or Big Data Deep Learning Engine.
- Whitelist for Data Security: Trusted access requests are not detected by Data Leakage Prevention, Website Tamper-proofing, or Account Security.
- Whitelist for Bot Management: Trusted access requests are not detected by Bot Threat Intelligence, Data Risk Control, Intelligent Algorithm, or App Protection.
- Whitelist for Access Control/Throttling: Trusted access requests are not detected by HTTP Flood Protection, IP Blacklist, Scan Protection, or Custom Protection Policy.

> **Note** We recommend that you create a whitelist for a specific detection module as required. A whitelist with more precise rules improves website security. A whitelist for a detection module provides better security protection than a website whitelist.

Procedure

1.
2.
3.
4.
5. In the upper-right corner, click **Website Whitelist**.
6. Create a website whitelist.
   i. On the **Website Whitelist** page, click **Create Rule**.

ii. In the **Create Rule** dialog box, configure the following parameters.



Create Rule

Rule name

The name must be 1 to 50 characters in length and can contain letters, digits, and Chinese characters.

The field cannot be empty.

Matching Condition (All the specified conditions must be met.)

Matching field	Logical operator	Matching content
URL	Includes	You may only enter one matching item. The field cannot be empty.

+ Add rule (A maximum of 5 conditions are supported.)

Parameter	Description
Rule name	Specify a name for the rule.
Matching Condition	Specify match conditions for the rule. Click **Add rule** to add more match conditions. A maximum of five match conditions are allowed. If you specify multiple match conditions, the rule is triggered only after all the match conditions are met. For more information about match conditions, see Fields in match conditions.

iii. Click **Save**.

After you create rules for the whitelist, the rules are automatically enabled. You can view created rules in the rule list. You can also disable, edit, or delete rules as required.

References

Fields in match conditions

5.2. Configure a whitelist for web intrusion prevention

After you add a website to Web Application Firewall (WAF), you can configure a whitelist for web intrusion prevention. If the requests that are destined for the website meet specific conditions, the Protection Rules Engine and Big Data Deep Learning Engine do not detect the requests. Web intrusion prevention may block normal access requests based on specific rules. You can use a whitelist to allow this type of requests.

Prerequisites

-
-

Background information

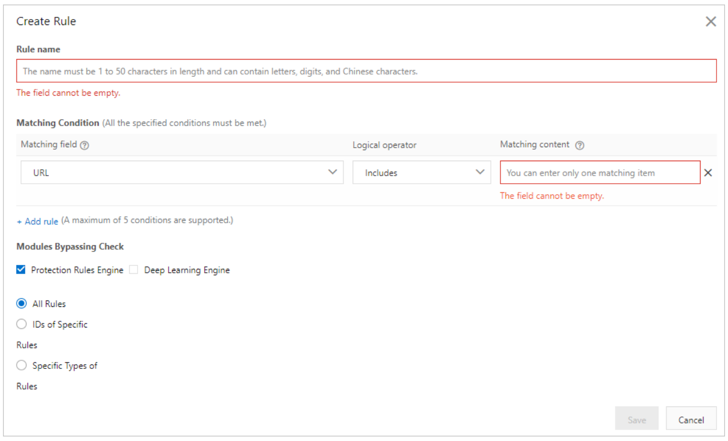
Web intrusion prevention protects your website against common web attacks and zero-day vulnerabilities. Web intrusion prevention provides the following protection features:

- Protection Rules Engine
- Big Data Deep Learning Engine

After you enable the preceding protection features, normal access requests may be blocked. If normal access requests are blocked by the protection features, you can configure a whitelist. Then, the protection features do not detect the requests that meet specific conditions. We recommend that you configure a whitelist based on your business requirements.

Procedure

1.
2.
3.
4.
5.
6. Create a whitelist rule for web intrusion prevention.
    i. On the **Web Intrusion Prevention - Whitelisting** page, click **Create Rule**.
    ii. In the **Create Rule** dialog box, configure the following parameters.



Create Rule

Rule name

The name must be 1 to 50 characters in length and can contain letters, digits, and Chinese characters.

The field cannot be empty.

Matching Condition (All the specified conditions must be met.)

Matching field: URL

Logical operator: Includes

Matching content: You can enter only one matching item

The field cannot be empty.

+ Add rule (A maximum of 5 conditions are supported.)

Modules Bypassing Check

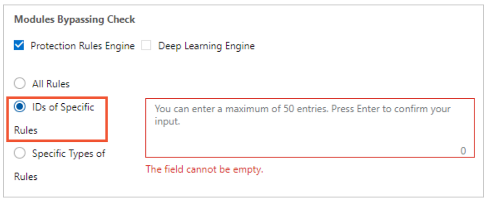
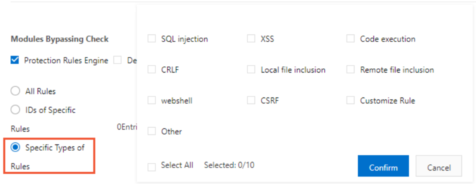
☑ Protection Rules Engine □ Deep Learning Engine

● All Rules

○ IDs of Specific Rules

○ Specific Types of Rules

Parameter	Description
Rule name	The name of the rule that you want to create. The name must be 1 to 50 characters in length and can contain letters and digits.
Matching Condition	The condition based on which requests are allowed. Click **Add rule** to add more conditions. You can add a maximum of five conditions. If you specify multiple conditions, the rule is matched only if all the conditions are met. For more information about conditions, see Fields in match conditions.

Parameter	Description
Modules Bypassing Check	The protection feature that does not detect requests if the requests meet the specified conditions. Valid values: **Protection Rules Engine** and **Big Data Deep Learning Engine**. If you select **Protection Rules Engine**, **All Rules** is automatically selected. In this case, all rules in the protection rules engine are skipped for requests. You can specify the rules or rule types that you want to skip based on your business requirements. To specify the rules or rule types, perform the following steps: a. Select **Protection Rules Engine**. b. (Optional)If you want to skip specific rules, select **IDs of Specific Rules** and enter the IDs of the rules.  Modules Bypassing Check ☑ Protection Rules Engine ☐ Deep Learning Engine ○ All Rules ● IDs of Specific Rules You can enter a maximum of 50 entries. Press Enter to confirm your input. 0 The field cannot be empty. ○ Specific Types of Rules To view the IDs of rules, you can click **Create Rule Group** on the **Protection Rule Group** page. The Create Rule Group page displays all protection rules that are included in WAF. For more information, see Customize protection rule groups. Press Enter each time you enter a rule ID. You can enter a maximum of 50 rule IDs. **Note** You can also create a whitelist rule on the **Security Report** page. On the **Web Intrusion Prevention** tab of the page, find the rule ID that you want to manage and click **Ignore False Positives** in the Actions column. After you click **Ignore False Positives**, WAF automatically generates a whitelist rule based on the characteristics of attack requests. You do not need to manually configure conditions or query rule IDs. For more information, see View security reports on the Web Security tab. c. (Optional)If you want to skip specific types of rules, select **Specific Types of Rules**, select the rule types, and then click **Confirm**.  Modules Bypassing Check ☑ Protection Rules Engine ☐ De ○ All Rules ○ IDs of Specific Rules 0Entri ● Specific Types of Rules ☐ SQL injection ☐ XSS ☐ Code execution ☐ CRLF ☐ Local file inclusion ☐ Remote file inclusion ☐ webshell ☐ CSRF ☐ Customize Rule ☐ Other ☐ Select All Selected: 0/10

iii. Click **Save**.

After you create the whitelist rule, the whitelist rule is automatically enabled. You can view, disable, edit, or delete the rule in the rule list based on your business requirements.

Notice By default, a whitelist rule is permanently valid after you create it. If you no longer need a whitelist rule, you can disable or delete it.

References

Fields in match conditions

5.3. Configure a whitelist for Data Security

After you add a website to Web Application Firewall (WAF), you can configure a whitelist for Data Security to allow trusted access requests of the website to bypass the detection of Website Tamper-proofing, Data Leakage Prevention, and Account Security. This whitelist is used to allow access requests that are blocked by mistake.

Prerequisites

-
-

Background information

Data Security protects your website against page content leaks and tampering to ensure the integrity and confidentiality of website data. It provides the following detection modules:

- Website Tamper-proofing
- Data Leakage Prevention
- Account Security

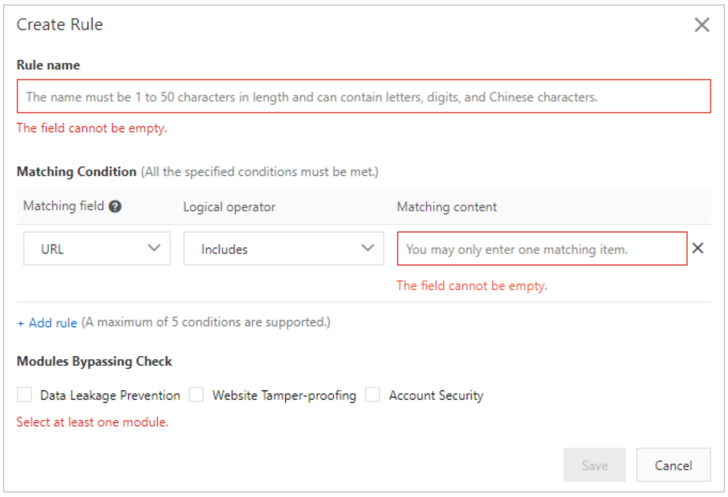
After the preceding detection modules are enabled, normal access requests may be blocked by mistake. In this case, you can configure a whitelist to allow trusted access requests to bypass the detection of a specific module in Data Security.

We recommend that you specify rules for the whitelist as precisely as possible to ensure that only trusted access requests are allowed.

Procedure

1.
2.
3.
4.
5.
6. Create the whitelist for Data Security.
    i. On the **Data Security Control - Whitelisting** page, click **Create Rule**.

ii. In the **Create Rule** dialog box, configure the following parameters.



Create Rule

Rule name

The name must be 1 to 50 characters in length and can contain letters, digits, and Chinese characters.

The field cannot be empty.

Matching Condition (All the specified conditions must be met.)

Matching field	Logical operator	Matching content
URL	Includes	You may only enter one matching item.

The field cannot be empty.

+ Add rule (A maximum of 5 conditions are supported.)

Modules Bypassing Check

□ Data Leakage Prevention □ Website Tamper-proofing □ Account Security

Select at least one module.

Parameter	Description
Rule name	Specify a name for the rule.
Matching Condition	Specify match conditions for the rule. Click **Add rule** to add more match conditions. A maximum of five match conditions are allowed. If you specify multiple match conditions, the rule is triggered only after all the match conditions are met. For more information about match conditions, see Fields in match conditions.
Modules Bypassing Check	Select the detection modules to bypass after the match conditions are met. Valid Values: ▪ **Data Leakage Prevention** ▪ **Website Tamper-proofing** ▪ **Account Security**

iii. Click **Save**.

After you create rules for the whitelist, the rules are automatically enabled. You can view created rules in the rule list. You can also disable, edit, or delete rules as required.

References

Fields in match conditions

5.4. Configure a whitelist for Bot Management

After you add a website to Web Application Firewall (WAF), you can configure a whitelist for Bot Management to allow trusted access requests of the website to bypass the detection of Bot Threat Intelligence, Data Risk Control, Intelligent Algorithm, and App Protection. This whitelist is used to allow access requests that are blocked by mistake.

Prerequisites

-
-

Background information

Bot Management protects web applications, native applications, and APIs from malicious crawlers. It provides the following detection modules:

- Allowed Crawlers
- Bot Threat Intelligence
- Data Risk Control
- App Protection
- Intelligent Algorithm

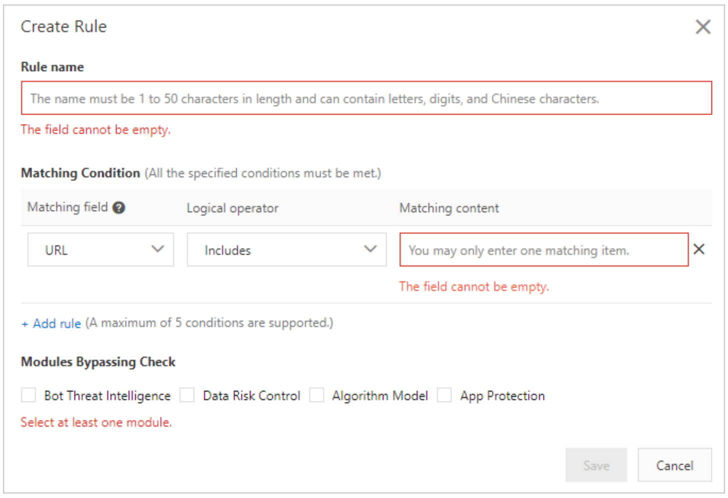
After the preceding detection modules but Allowed Crawlers are enabled, normal access requests may be blocked by mistake. In this case, you can configure a whitelist to allow trusted access requests to bypass the detection of a specific module in Bot Management.

We recommend that you specify rules for the whitelist as precisely as possible to ensure that only trusted access requests are allowed.

Procedure

1.
2.
3.
4.
5.
6. Create a whitelist for Bot Management.
   i. On the **Bot Management - Whitelist** page, click **Create Rule**.

ii. In the **Create Rule** dialog box, configure the following parameters.



Create Rule

Rule name

The name must be 1 to 50 characters in length and can contain letters, digits, and Chinese characters.

The field cannot be empty.

Matching Condition (All the specified conditions must be met.)

Matching field	Logical operator	Matching content
URL	Includes	You may only enter one matching item. The field cannot be empty.

+ Add rule (A maximum of 5 conditions are supported.)

Modules Bypassing Check

□ Bot Threat Intelligence □ Data Risk Control □ Algorithm Model □ App Protection

Select at least one module.

Parameter	Description
Rule name	Specify a name for the rule.
Matching Condition	Specify match conditions for the rule. Click **Add rule** to add more match conditions. A maximum of five match conditions are allowed. If you specify multiple match conditions, the rule is triggered only after all the match conditions are met. For more information about match conditions, see Fields in match conditions.
Modules Bypassing Check	Select the detection modules to bypass after the match conditions are met. Valid Values: - **Bot Threat Intelligence** - **Data Risk Control** - **Algorithm Model** - **App Protection**

iii. Click **Save**.

After you create rules for the whitelist, the rules are automatically enabled. You can view created rules in the rule list. You can also disable, edit, or delete rules as required.

References

Fields in match conditions

5.5. Configure a whitelist for Access Control/Throttling

After you add a website to Web Application Firewall (WAF), you can configure a whitelist for Access Control/Throttling to allow trusted access requests of the website to bypass the detection of HTTP Flood Protection, IP Blacklist, Scan Protection, and Custom Protection Policy. This whitelist is used to allow access requests that are blocked by mistake.

Prerequisites

-
-

Background information

Access Control/Throttling provides custom access control policies and traffic management policies at the application layer to ensure website accessibility. It provides the following detection modules:

- HTTP Flood Protection
- IP Blacklist
- Scan Protection
- Custom Protection Policy

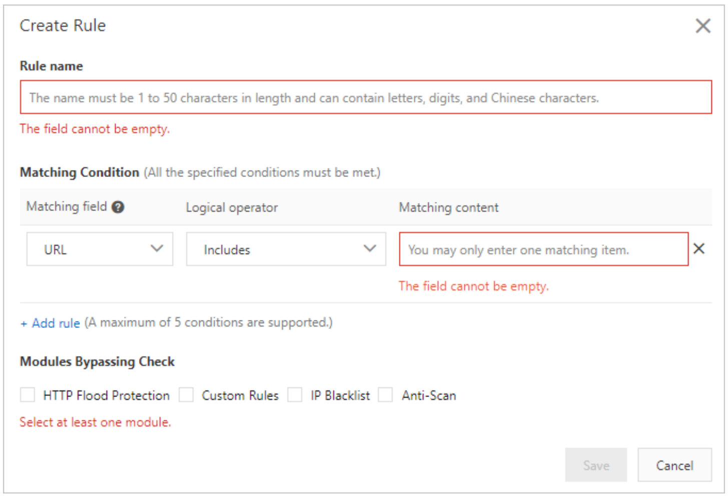
After the preceding detection modules are enabled, normal access requests may be blocked by mistake. In this case, you can configure a whitelist to allow trusted access requests to bypass the detection of a specific module in Access Control/Throttling.

We recommend that you specify rules for the whitelist as precisely as possible to ensure that only trusted access requests are allowed.

Procedure

1.
2.
3.
4.
5.
6. Create a whitelist for Access Control/Throttling.
   i. On the **Access Control/Throttling - Whitelisting** page, click **Create Rule**.

ii. In the **Create Rule** dialog box, configure the following parameters.



Create Rule

Rule name

The name must be 1 to 50 characters in length and can contain letters, digits, and Chinese characters.

The field cannot be empty.

Matching Condition (All the specified conditions must be met.)

Matching field	Logical operator	Matching content
URL	Includes	You may only enter one matching item. The field cannot be empty.

+ Add rule (A maximum of 5 conditions are supported.)

Modules Bypassing Check

□ HTTP Flood Protection □ Custom Rules □ IP Blacklist □ Anti-Scan

Select at least one module.

Parameter	Description
Rule name	Specify a name for the rule.
Matching Condition	Specify match conditions for the rule. Click **Add rule** to add more match conditions. A maximum of five match conditions are allowed. If you specify multiple match conditions, the rule is triggered only after all the match conditions are met. For more information about match conditions, see Fields in match conditions.
Modules Bypassing Check	Select the detection modules to bypass after the match conditions are met. Valid Values: ■ **HTTP Flood Protection** ■ **Custom Rules** ■ **IP Blacklist** ■ **Anti-Scan**

iii. Click **Save**.

After you create rules for the whitelist, the rules are automatically enabled. You can view created rules in the rule list. You can also disable, edit, or delete rules as required.

References

Fields in match conditions

6.Fields in match conditions

You must add match conditions to rules when you configure a whitelist and customize protection policies for Web Application Firewall (WAF). This topic describes the fields that you can use in the match conditions and their descriptions.

Match conditions and actions

In the WAF console, you can customize rules for whitelists and protection policies. A custom rule consists of match conditions and actions. When you create a rule, you must specify the match fields, logical operators, and match content to add match conditions. You also need to select an action that is triggered when requests match the conditions you specify.

- Match conditions

  Each match condition consists of a match field, logical operator, and match content. The match content does not support regular expressions. You can add a maximum of five match conditions to a custom rule, and the logical relation among the conditions is AND. The custom rule works only when all the match conditions are met.

- Action

  When you configure a whitelist rule, you must select features for Modules Bypassing Check so that requests that meet match conditions bypass the corresponding checks. When you configure custom protection policies, you must select an action that is triggered for requests that meet match conditions. For more information, see the following topics:

  - Configure a website whitelist
  - Configure a whitelist for web intrusion prevention
  - Configure a whitelist for Access Control/Throttling
  - Configure a whitelist for Bot Management
  - Configure a whitelist for Data Security
  - Create a custom protection policy

Supported match fields

The following table lists the match fields that are supported in match conditions.

Match field	Edition	Logical operator	Description
IP	Pro edition or higher	Has and Does not have	The source IP address of an access request. You can enter IP addresses or CIDR blocks, for example, 1.1.1.1/24. Note You can enter a maximum of 50 IP addresses or CIDR blocks. Separate them with commas (,).

Match field	Edition	Logical operator	Description
URL	Pro edition or higher	- Includes and Does not include - Equals and Does not equal - URI Path Match - Regular Expression	The URL of an access request.
Referer	Pro edition or higher	- Includes and Does not include - Equals and Does not equal - Length equals, Length more than, and Length less than - Does not exist	The URL of the source page from which the access request is redirected.
User-Agent	Pro edition or higher	- Includes and Does not include - Equals and Does not equal - Length equals, Length more than, and Length less than	The browser information of the client that initiates access requests. The information includes the browser, rendering engine, and version.
Params	Pro edition or higher	- Includes and Does not include - Equals and Does not equal - Length equals, Length more than, and Length less than	The parameter part in the request URL, usually the part that follows the question mark (?) in the URL. For example, in `www.abc.com/index.html?action=login` , `action=login` is the parameter part.

Match field	Edition	Logical operator	Description
Cookie	Business edition or higher	• Includes and Does not include • Equals and Does not equal • Length equals, Length more than, and Length less than • Does not exist	The cookie information in an access request.
Content-Type	Business edition or higher	• Includes and Does not include • Equals and Does not equal • Length equals, Length more than, and Length less than	The HTTP content type (MIME) in the response.
Content-Length	Business edition or higher	Value less than, Value equals, and Value more than	The number of bytes in the response.
X-Forwarded-For	Business edition or higher	• Includes and Does not include • Equals and Does not equal • Length equals, Length more than, and Length less than • Does not exist	The actual IP address of the client that initiates access requests. X-Forwarded-For (XFF) is an HTTP header field. It is used to identify the originating IP address of a client that connects to the server through an HTTP proxy or a Server Load Balancer (SLB) instance. XFF is only included in the access requests that are forwarded by the HTTP proxy or SLB instance.
Post-Body	Business edition or higher	• Includes and Does not include • Equals and Does not equal	The content of an access request.
Http-Method	Business edition or higher	Equals and Does not equal	The request method, such as GET, POST, DELETE, PUT, and OPTIONS.

Match field	Edition	Logical operator	Description
Header	Business edition or higher	• Includes and Does not include • Equals and Does not equal • Length equals, Length more than, and Length less than • Does not exist	The header of an access request, which is used to customize the HTTP header.
URLPath	Business edition or higher	• Includes and Does not include • Equals and Does not equal • URI Path Match • Regular Expression	The URL path of an access request.

Logical operators

Logical operator	Description
Has and Does not have	Whether the match field has the match content.
Includes and Does not include	Whether the match field includes the match content.
Equals and Does not equal	Whether the match field equals the match content.
Length equals, Length more than, and Length less than	The length of the match field is equal to, greater than, or less than that of the match content.
Does not exist	The match field does not exist.
Value less than, Value equals, and Value more than	The value of the match field is less than, equal to, or greater than that of the match content.
URI Path Match	The prefix of the match field contains the match content.
Regular Expression	The match field matches the regular expression defined in the match content.

7.Customize protection rule groups

You can use the protection rules provided by Web Application Firewall (WAF) to customize your rule groups for a specific protection feature, such as Protection Rules Engine, also known as web application protection. If default protection rule groups do not meet your business requirements, we recommend that you customize protection rule groups to protect your website.

Prerequisites

- A WAF instance is purchased. The instance must meet the following requirements:
  - The instance uses the subscription billing method.
  - If the instance is deployed **in mainland China**, the instance must be of the **Business** edition or higher.
  - If the instance is deployed **outside mainland China**, the instance must be of the **Enterprise** edition or higher.

  For more information, see Purchase a WAF instance.
-

Context

Only the **Protection Rules Engine** feature supports custom protection rule groups. For more information about **Protection Rules Engine**, see Configure the protection rules engine feature.

Use a custom rule group

Before you can use a custom rule group, you must complete the following steps:

1. Create a rule group: Create a custom rule group for a specific protection feature.
2. Apply the rule group: Apply the created rule group to your website.

Create a rule group

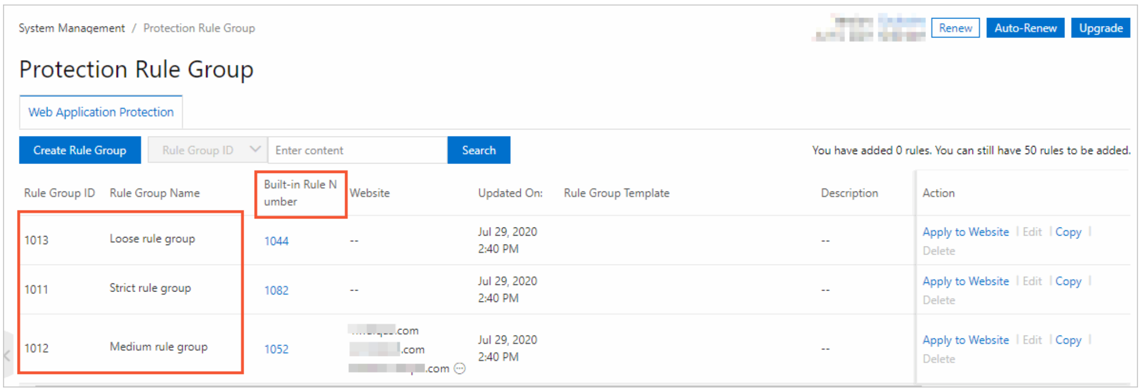
1.
2.
3.
4. (Optional)On the **Protection Rule Group** page, click the tab of the protection feature for which you want to create a custom rule group.

   > **Note** You can skip this step because only the **web application protection** feature supports custom protection rule groups. The **Web Application Protection** tab automatically appears.

   The tab displays default and custom rule groups.

   - Default rule group: Default rule groups are **Loose rule group**, **Medium rule group**, and **Strict rule group**.

You can click a value in the **Built-in Rule Number** column to view information about the built-in rules of the default rule group.



System Management / Protection Rule Group

[redacted] Renew Auto-Renew Upgrade

Protection Rule Group

Web Application Protection

Create Rule Group | Rule Group ID | Enter content | Search

You have added 0 rules. You can still have 50 rules to be added.

Rule Group ID	Rule Group Name	Built-in Rule Number	Website	Updated On:	Rule Group Template	Description	Action
1013	Loose rule group	1044	--	Jul 29, 2020 2:40 PM		--	Apply to Website | Edit | Copy | Delete
1011	Strict rule group	1082	--	Jul 29, 2020 2:40 PM		--	Apply to Website | Edit | Copy | Delete
1012	Medium rule group	1052	[redacted].com [redacted].com [redacted].com	Jul 29, 2020 2:40 PM		--	Apply to Website | Edit | Copy | Delete

Note Default rule groups cannot be edited or deleted.

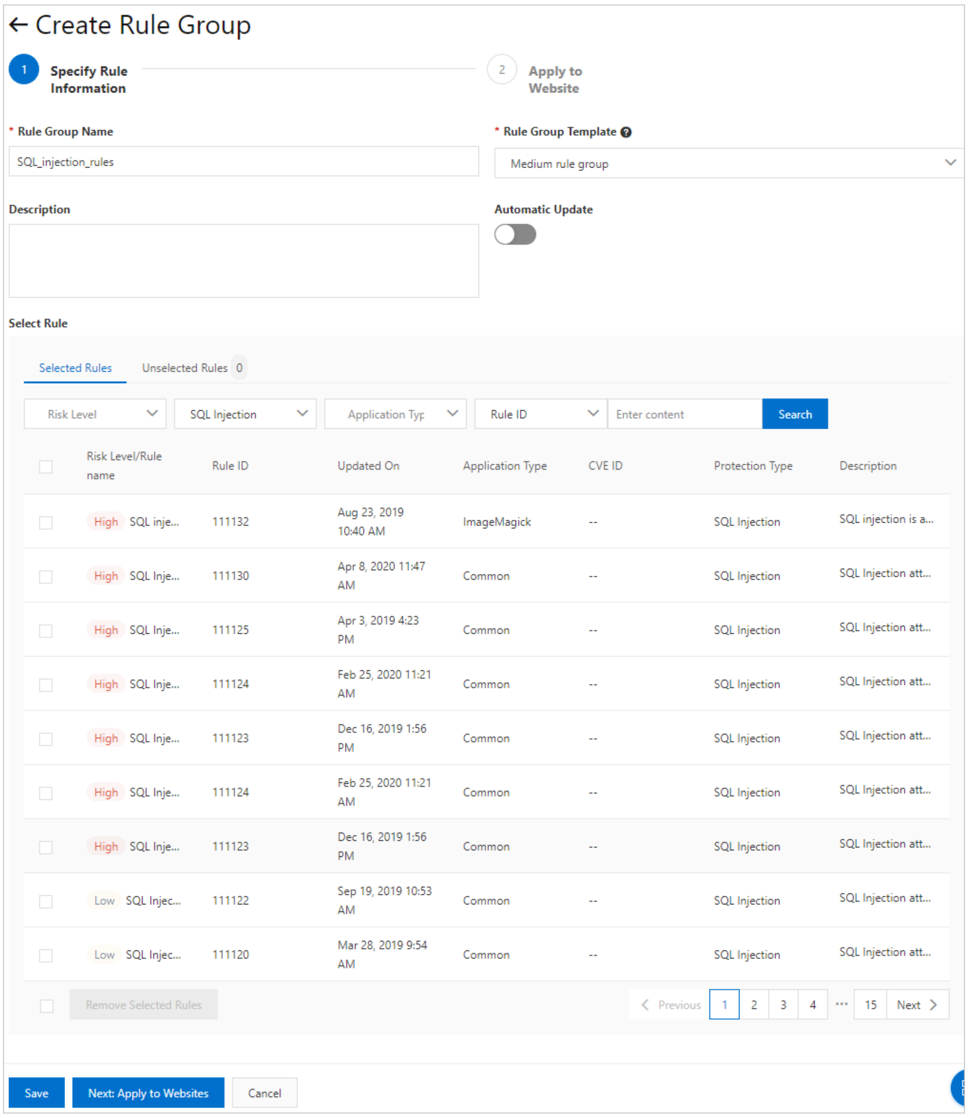
- Custom rule group: You can create a custom rule group on the **Protection Rule Group** page.

5. Click **Create Rule Group**.

   Note You can create a maximum of 10 rule groups for the web application protection feature.

6. Complete the **Create Rule Group** wizard.

   i. **Specify rule information**. Configure the following parameters and click **Next: Apply to Websites**.



← Create Rule Group

1 Specify Rule Information — 2 Apply to Website

* Rule Group Name: SQL_injection_rules

* Rule Group Template: Medium rule group

Description:

Automatic Update: ○ Off

Select Rule

□	Risk Level/Rule name	Rule ID	Updated On	Application Type	CVE ID	Protection Type	Description
□	High SQL inje...	111132	Aug 23, 2019 10:40 AM	ImageMagick	--	SQL Injection	SQL injection is a...
□	High SQL Inje...	111130	Apr 8, 2020 11:47 AM	Common	--	SQL Injection	SQL Injection att...
□	High SQL Inje...	111125	Apr 3, 2019 4:23 PM	Common	--	SQL Injection	SQL Injection att...
□	High SQL Inje...	111124	Feb 25, 2020 11:21 AM	Common	--	SQL Injection	SQL Injection att...
□	High SQL Inje...	111123	Dec 16, 2019 1:56 PM	Common	--	SQL Injection	SQL Injection att...
□	High SQL Inje...	111124	Feb 25, 2020 11:21 AM	Common	--	SQL Injection	SQL Injection att...
□	High SQL Inje...	111123	Dec 16, 2019 1:56 PM	Common	--	SQL Injection	SQL Injection att...
□	Low SQL Injec...	111122	Sep 19, 2019 10:53 AM	Common	--	SQL Injection	SQL Injection att...
□	Low SQL Injec...	111120	Mar 28, 2019 9:54 AM	Common	--	SQL Injection	SQL Injection att...

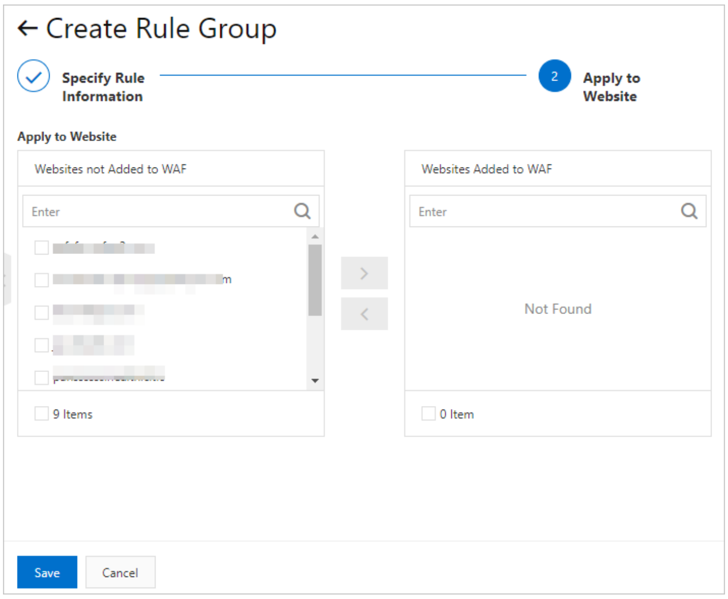
Parameter	Description
Rule Group Name	Enter a name for the rule group. The name is used to identify the rule group. We recommend that you enter an informative name.
Rule Group Template	Select a rule group template from which you want to select rules for the rule group. Valid values: ■ **Strict rule group** ■ **Medium rule group** ■ **Loose rule group** Different rule group templates contain different rules. After you select the rule group template and turn on Automatic Update, each time a rule in the rule group template is updated, the rule is also updated in the created rule group.
Description	Enter a description for the rule group.

Parameter	Description
Automatic Update	If you turn on this switch, each time a rule in the rule group template is updated, the rule is also updated in the created rule group. **Note** Some custom rule groups do not support the automatic update feature. In this case, we recommend that you create custom rule groups to replace these rule groups.
Select Rule	Specify rules for the rule group. The **Selected Rules** tab lists all rules in the rule group template that you select. You must select rules that are not applicable or may cause false positives, and click **Remove Selected Rules**. You can use the filter or search feature to find the rules that you want to remove. You can filter rules by **Protection Type**, **Application Type**, or **Risk Level**. You can also enter the name or ID of a rule to search for the rule. ■ **Risk Level**: indicates the risk level of web attacks. Valid values: **High**, **Medium**, and **Low**. ■ **Protection Type**: indicates the type of web attacks. Valid values: **SQL Injection**, **Cross-site Script**, **Code Execution**, **Local File Inclusion**, **Remote File Inclusion**, **Webshell**, and **Others**. ■ **Application Type**: indicates the type of the protected web application. Valid values: **Common**, **Wordpress**, **Dedecms**, **Discuz**, **Phpcms**, **Ecshop**, **Shopex**, **Drupal**, **Joomla**, **Metinfo**, **Struts2**, **Spring Boot**, **Jboss**, **Weblogic**, **Websphere**, **Tomcat**, **Elastic Search**, **Thinkphp**, **Fastjson**, **ImageMagick**, **PHPwind**, **phpMyAdmin**, and **Others**.

Note If you do not want to immediately apply a rule group after you create it, click **Save** to complete the wizard. If you want to apply the rule group later, you can edit the rule group again.

ii. (Optional)**Apply the created rule group to a website**. To do this, you must select the website from the **Websites not Added to WAF** section and add the website to the **Websites Added to WAF** section.

> **Notice** You can apply only one rule group to a website.



iii. Click **Save**.

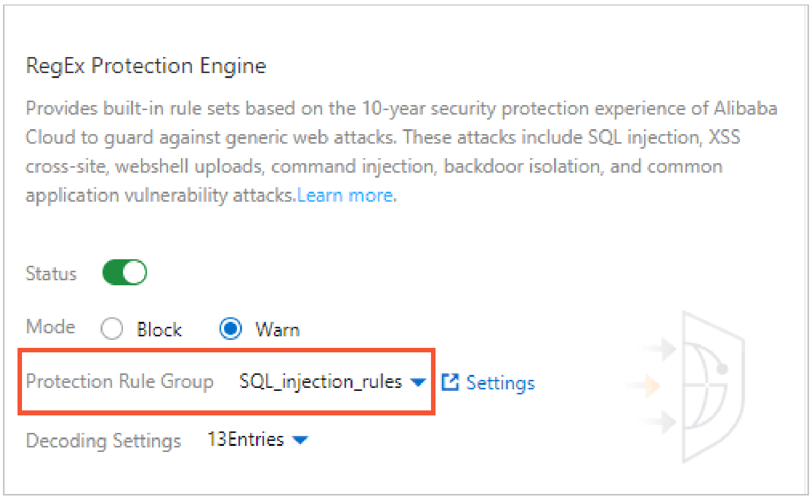
You can view the created rule group in the rule group list and select the website to which you want to apply the rule group. For more information, see Apply the rule group.

After the rule group is created, you can view the time when the rule group was created in the **Updated On:** column on the **Protection Rule Group** page and determine whether to update the rule group.

Apply the rule group

After you create a custom rule group, you can apply it by using one of the following methods:

- On the **Protection Rule Group** page, apply the rule group to a website. The following procedure is provided for this scenario.
- On the **Website Protection** page, select the rule group from the Protection Rule Group drop-down list in the Protection Rules Engine card.



RegEx Protection Engine

Provides built-in rule sets based on the 10-year security protection experience of Alibaba Cloud to guard against generic web attacks. These attacks include SQL injection, XSS cross-site, webshell uploads, command injection, backdoor isolation, and common application vulnerability attacks.Learn more.

Status: on

Mode: ○ Block ● Warn

Protection Rule Group: SQL_injection_rules Settings

Decoding Settings: 13Entries

For more information, see Configure the protection rules engine feature.

1.

2.

3.

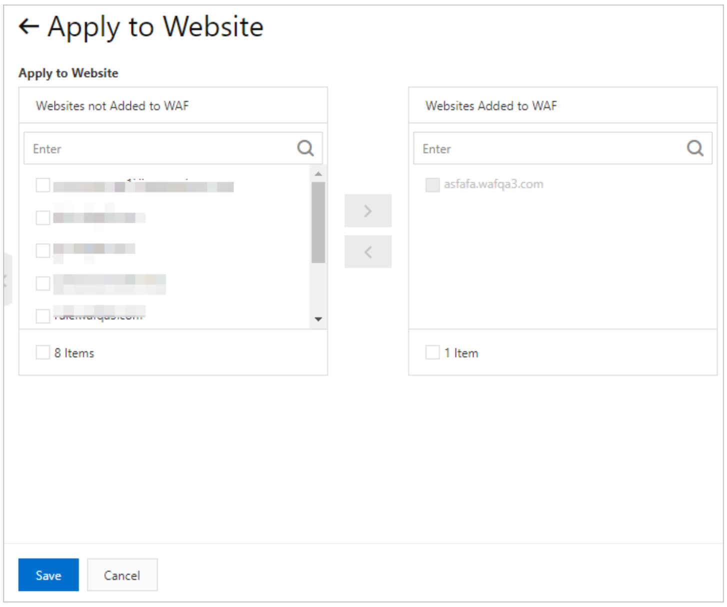
4. (Optional)On the **Protection Rule Group** page, click the tab of the protection feature for which you want to apply a rule group.

   > Note You can skip this step because only the **web application protection** feature supports custom protection rule groups. The **Web Application Protection** tab automatically appears.

5. In the rule group list, find the rule group that you want to apply and click **Apply to Website** in the Action column.

6. On the **Apply to Website** page, select the website to which you want to apply the rule group from the **Websites not Added to WAF** section, add the website to the **Websites Added to WAF** section, and then click **Save**.

   > Notice You must apply one rule group to each website.

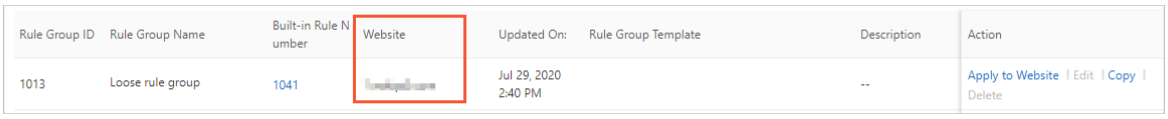


← Apply to Website

Apply to Website

Websites not Added to WAF	Websites Added to WAF
Enter	Enter
□ [redacted]	□ asfafa.wafqa3.com
□ [redacted]	
□ [redacted]	
□ [redacted]	
□ [redacted]	
□ 8 Items	□ 1 Item

After the rule group is applied, you can view the website in the **Website** column in the rule group list.



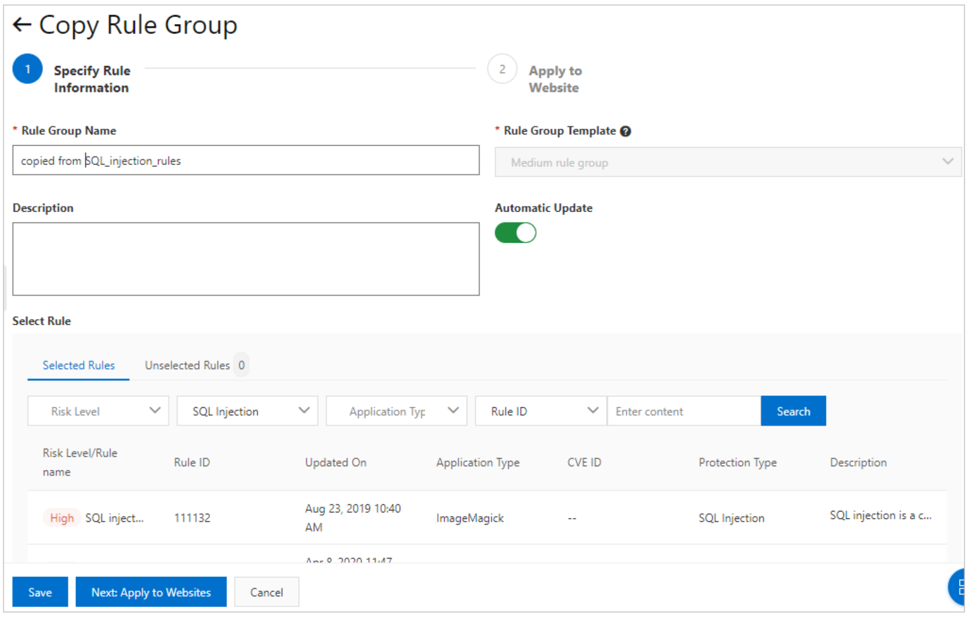
Rule Group ID	Rule Group Name	Built-in Rule Number	Website	Updated On:	Rule Group Template	Description	Action
1013	Loose rule group	1041	[redacted]	Jul 29, 2020 2:40 PM		--	Apply to Website | Edit | Copy | Delete

What to do next

You can perform the following operations to manage the created rule group on the **Protection Rule Group** page:

- **Copy**: allows you to copy the configurations of the rule group.

  The following figure shows the Copy Rule Group page. On this page, you can change the settings for **Rule Group Name**, **Description**, and **Automatic Update**. However, you cannot change the setting for **Rule Group Template** or the rule settings. If you want to change the rule settings, we recommend that you copy the rule group and change the rule settings in the copied rule group.



← Copy Rule Group

1 Specify Rule Information — 2 Apply to Website

* Rule Group Name: copied from SQL_injection_rules

* Rule Group Template: Medium rule group

Description:

Automatic Update: On

Select Rule

Selected Rules | Unselected Rules 0

Risk Level | SQL Injection | Application Typ | Rule ID | Enter content | Search

Risk Level/Rule name	Rule ID	Updated On	Application Type	CVE ID	Protection Type	Description
High SQL inject...	111132	Aug 23, 2019 10:40 AM	ImageMagick	--	SQL Injection	SQL injection is a c...
		Apr 8, 2020 11:47				

- **Edit**: allows you to change the name, description, and rule settings of the rule group. Default rule groups cannot be edited.
- **Delete**: allows you to delete the rule group. Default rule groups cannot be deleted.

  Before you delete a custom rule group, make sure that it is not applied to a website. If the rule group is applied to a website, apply a different rule group to the website before you delete the rule group.

8.Enable IPv6 traffic protection

After you add your website to Web Application Firewall (WAF), you can enable the IPv6 traffic protection feature for the website with a few clicks. This feature protects your website against attacks that originate from IPv6 sources.

Prerequisites

- A subscription WAF instance is purchased. The WAF instance runs the Business, Enterprise, or Exclusive edition. For more information, see Purchase a WAF instance.
- The WAF instance resides in mainland China.

> Note IPv6 traffic protection is not supported for WAF instances that reside outside mainland China.

- Your website is added to WAF. For more information, see Add a domain name.

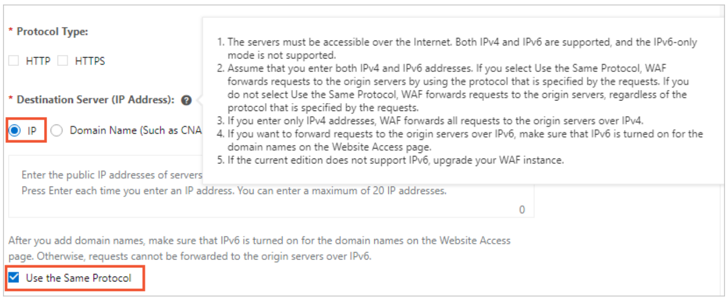
Context

After IPv6 traffic protection is enabled, the Canonical Name (CNAME) that is automatically generated by WAF is resolved in two channels. Take note of the following resolution rules:

- Resolution requests from IPv4 clients are resolved to a protection cluster for IPv4 addresses.
- Resolution requests from IPv6 clients are resolved to a protection cluster for IPv6 addresses.

Two-channel resolution allows WAF to detect and block threats that originate from IPv4 and IPv6 sources. Only normal traffic is forwarded to origin servers.

In addition, you can enable the feature of forwarding requests to origin servers over IPv6. To enable this feature, you must configure back-to-origin IPv4 and IPv6 addresses and select **Use the Same Protocol**. This way, WAF forwards requests to origin servers based on the protocol that is specified in the requests. For more information, see Add a domain name.



* Protocol Type:

□ HTTP □ HTTPS

* Destination Server (IP Address):

● IP ○ Domain Name (Such as CNA

1. The servers must be accessible over the Internet. Both IPv4 and IPv6 are supported, and the IPv6-only mode is not supported.
2. Assume that you enter both IPv4 and IPv6 addresses. If you select Use the Same Protocol, WAF forwards requests to the origin servers by using the protocol that is specified by the requests. If you do not select Use the Same Protocol, WAF forwards requests to the origin servers, regardless of the protocol that is specified by the requests.
3. If you enter only IPv4 addresses, WAF forwards all requests to the origin servers over IPv4.
4. If you want to forward requests to the origin servers over IPv6, make sure that IPv6 is turned on for the domain names on the Website Access page.
5. If the current edition does not support IPv6, upgrade your WAF instance.

Enter the public IP addresses of servers
Press Enter each time you enter an IP address. You can enter a maximum of 20 IP addresses.

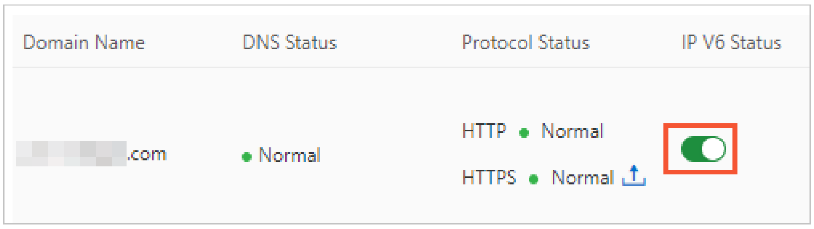
0

After you add domain names, make sure that IPv6 is turned on for the domain names on the Website Access page. Otherwise, requests cannot be forwarded to the origin servers over IPv6.

☑ Use the Same Protocol

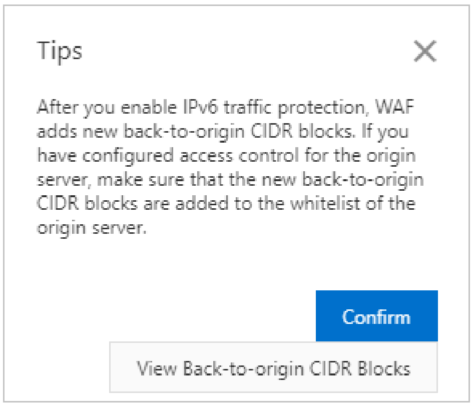
Procedure

1.
2.
3.
4. In the **domain name list**, find the domain name that you want to manage, and turn on the **IPv6** switch in the **Quick Access** column.



Domain Name	DNS Status	Protocol Status	IP V6 Status
[redacted].com	● Normal	HTTP ● Normal HTTPS ● Normal	

5. In the **Tips** message, click **OK**.



Tips

After you enable IPv6 traffic protection, WAF adds new back-to-origin CIDR blocks. If you have configured access control for the origin server, make sure that the new back-to-origin CIDR blocks are added to the whitelist of the origin server.

What's next

After IPv6 is enabled, WAF uses new back-to-origin Classless Inter-Domain Routing (CIDR) blocks to forward the requests from the IPv6 clients to origin servers.

To ensure that origin servers can receive the requests forwarded by WAF, you must configure the origin servers to allow the requests from the new back-to-origin CIDR blocks of WAF. This applies especially when you have configured the origin servers to allow requests from only the back-to-origin CIDR blocks of WAF. If you do not configure the origin servers to allow the requests from the new back-to-origin CIDR blocks of WAF, access from IPv6 clients may encounter errors or fail. For more information, see Allow access from back-to-origin CIDR blocks of WAF and Configure protection for an origin server.

9.Best practices for protection settings

9.1. Best practices for website protection

If this is the first time you add a domain name to WAF, we recommend that you learn more about website protection. This topic describes how to select protection modules and configure protection policies of WAF from the perspective of different roles to meet business requirements in different scenarios. By reading this topic, you can understand the protection logic of WAF.

Prerequisites

Your website configurations are added to WAF. For more information, see Add a domain name.

Usage notes

All the descriptions in this topic are based on the fact that you have enabled the recommended website protection features. If you have not enabled such features, enable and configure them based on the feature descriptions.

Unless otherwise specified, the recommended website protection features are configured on the **Website Protection** page. Perform the following operations to go to the **Website Protection** page:

1.
2.
3.
4.

Overview

This topic provides the recommended website protection features based on roles and business requirements. You can decide which features to enable based on your business requirements.

- I am new to WAF. I am unsure of my security needs
- I am an O&M engineer. I require reliable services and convenient troubleshooting
- I am a security engineer. I need to comprehensively prevent web intrusion
- I want to achieve the strongest protection and radically block attacks
- My website is often crawled and is at risk of data breach or tampering

I am new to WAF. I am unsure of my security needs

You may have purchased a WAF instance based on a need for classified protection or the intention to improve the security level of your enterprise. In either case, you can add your website configurations to WAF and then use the default protection settings of WAF. The default protection settings are sufficient to protect your website from the majority of basic web threats.

We recommend that you browse the **Overview** and **Security report** pages in the Web Application Firewall console to understand the security situations of your business and the attacks it may face. For more information, see the following topics:

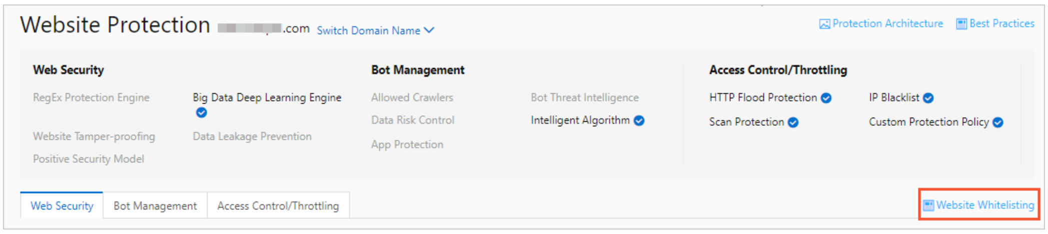
- View Protection History on the WAF Overview Page
- View Security Reports

I am an O&M engineer. I require reliable services and convenient troubleshooting

We recommend that you enable the following website protection features after you add your website configurations to WAF:

- **Website Whitelisting**: You can configure a whitelist to allow requests that meet the specific conditions without the need to perform a check.

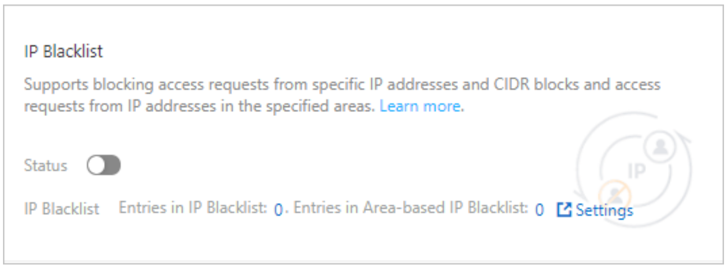
  Operations: On the **Website Protection** page, click **Website Whitelisting** in the upper-right corner. On the Website Whitelisting page, create a whitelist. For more information, see Configure a website whitelist.

  To implement more precise protection, you can also configure a whitelist for a specific protection module. For more information, see the following topics:

  - Whitelist for Web Intrusion Prevention: Trusted access requests are not detected by RegEx Protection Engine or Big Data Deep Learning Engine.
  - Whitelist for Data Security: Trusted access requests are not detected by Data Leakage Prevention, Website Tamper-proofing, or Account Security.
  - Whitelist for Bot Management: Trusted access requests are not detected by Bot Threat Intelligence, Data Risk Control, Intelligent Algorithm, or App Protection.
  - Whitelist for Access Control/Throttling: Trusted access requests are not detected by HTTP Flood Protection, IP Blacklist, Scan Protection, or Custom Protection Policy.

- **IP Blacklist**: This feature allows you to configure an IP address blacklist to block requests from IP addresses and CIDR blocks that are irrelevant to your business and from IP addresses in specific regions. For example, if a local government forum is accessed only by local IP addresses, you can add IP addresses from other regions to a regional blacklist. If your website does not have users outside China, you can add all the regions outside China to a regional blacklist.

  IP Blacklist

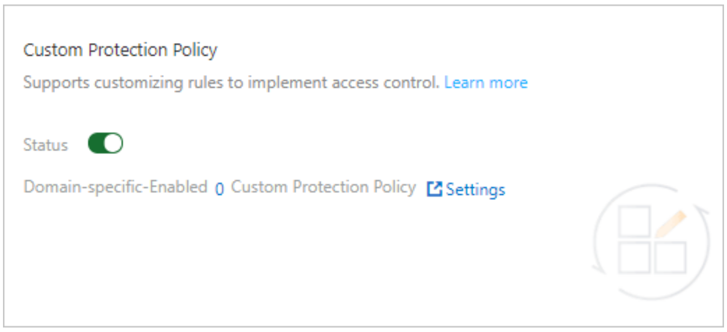
  Supports blocking access requests from specific IP addresses and CIDR blocks and access requests from IP addresses in the specified areas. Learn more.

  Status

  IP Blacklist Entries in IP Blacklist: 0. Entries in Area-based IP Blacklist: 0 Settings

  Operations: On the **Website Protection** page, click the **Access Control/Throttling** tab. Find the **IP Blacklist** card and configure the required parameters. For more information, see Configure a blacklist.

- **Custom Protection Policy**: This feature allows you to customize access control lists (ACLs) or throttling policies. For example, you can allow access to an API only from specific IP addresses or user agents and configure an upper limit for specific types of requests. You can also use this feature to defend against HTTP flood attacks, crawler attacks, and some special web attacks.



Custom Protection Policy

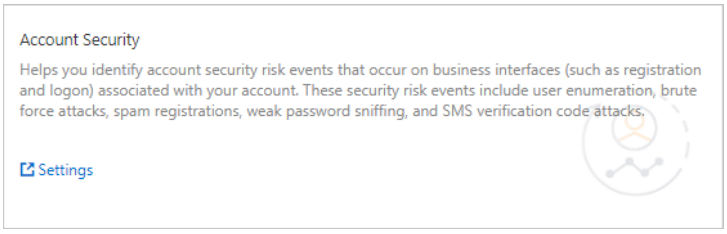
Supports customizing rules to implement access control. Learn more

Status

Domain-specific-Enabled 0 Custom Protection Policy Settings

Operations: On the **Website Protection** page, click the **Access Control/Throttling** tab. Find the **Custom Protection Policy** card and configure the required parameters. For more information, see Create a custom protection policy.

- **Account Security**: This feature allows you to monitor user authentication-related interfaces, such as the interfaces used for registration and logon, to detect events that may pose a threat to user credentials. These threats include credential stuffing, brute-force attacks, account registrations launched by bots, weak password sniffing, and SMS interface abuse.



Account Security

Helps you identify account security risk events that occur on business interfaces (such as registration and logon) associated with your account. These security risk events include user enumeration, brute force attacks, spam registrations, weak password sniffing, and SMS verification code attacks.

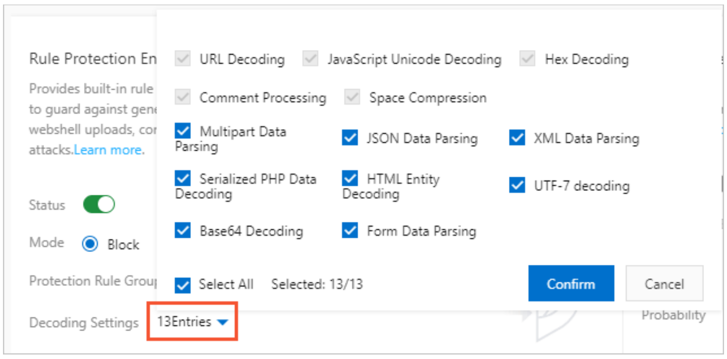
Settings

Operations: On the **Website Protection** page, click the **Web Security** tab. In the **Data Security** section, find **Account Security**. In the Account Security card, click **Settings** and configure the required parameters. For more information, see Configure account security.

I am a security engineer. I need to comprehensively prevent web intrusion

We recommend that you enable the following website protection features after you add your website configurations to WAF:

- **Decoding Settings**: This feature allows you to specify a decoding method for the WAF engine based on your business coding scheme to maximize protection for your website. A proper decoding method allows the WAF engine to effectively identify traffic and achieve precise prevention. WAF uses all the 13 decoding methods by default. You can filter out unnecessary methods to avoid unnecessary parsing and false blocking.



Rule Protection En
Provides built-in rule to guard against gene webshell uploads, cor attacks.Learn more.

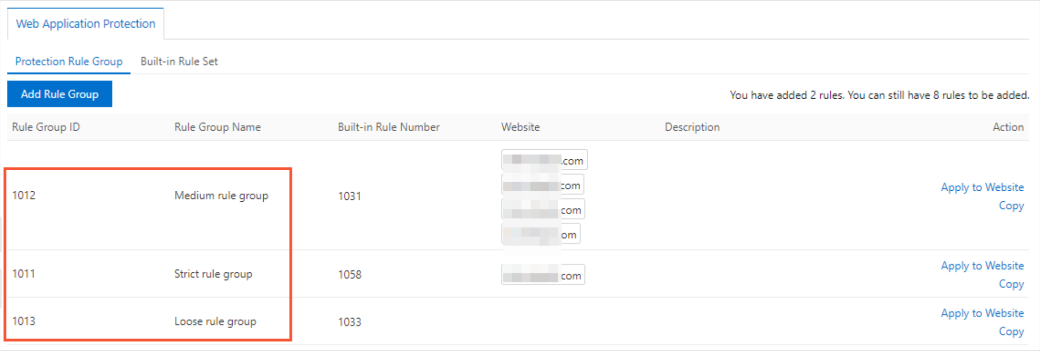
Status
Mode ● Block
Protection Rule Grou
Decoding Settings 13Entries

☑ URL Decoding ☑ JavaScript Unicode Decoding ☑ Hex Decoding
☑ Comment Processing ☑ Space Compression
☑ Multipart Data Parsing ☑ JSON Data Parsing ☑ XML Data Parsing
☑ Serialized PHP Data Decoding ☑ HTML Entity Decoding ☑ UTF-7 decoding
☑ Base64 Decoding ☑ Form Data Parsing
☑ Select All Selected: 13/13

Operations: On the **Website Protection** page, click the **Web Security** tab. In the **Web Intrusion Prevention** section, find **RegEx Protection Engine**. In the RegEx Protection Engine card, specify **Decoding Settings**. For more information, see Configure the protection rules engine feature.

- **Protection Rule Group**: This feature allows you to select protection rules from a built-in protection rule set based on the form, framework, and middleware of your business system. You can use these rules to customize a rule group to prevent web attacks and apply the rule group to your website. We recommend that you use this feature to configure web intrusion prevention policies for your website. If you want to configure prevention policies for a single URL, we recommend that you use the Custom Protection Policy feature.

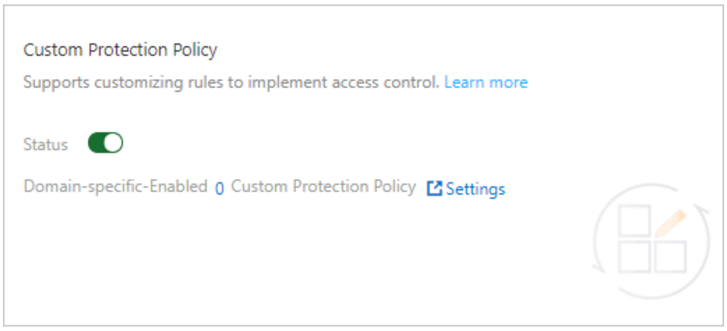
  Operations: Log on to the Web Application Firewall console and choose **System Management > Protection Rule Group**. On the Protection Rule Group page, customize the rule group for web attack prevention and apply the rule group to your website. For more information, see Customize protection rule groups.



You have added 2 rules. You can still have 8 rules to be added.

Rule Group ID	Rule Group Name	Built-in Rule Number	Website	Description	Action
1012	Medium rule group	1031	[redacted].com [redacted]com [redacted]com [redacted]om		Apply to Website Copy
1011	Strict rule group	1058	[redacted]com		Apply to Website Copy
1013	Loose rule group	1033			Apply to Website Copy

- **Custom Protection Policy**: This feature allows you to customize access control lists (ACLs) or throttling policies. For example, you can allow access to an API only from specific IP addresses or user agents and configure an upper limit for specific types of requests. You can also use this feature to defend against HTTP flood attacks, crawler attacks, and some special web attacks.

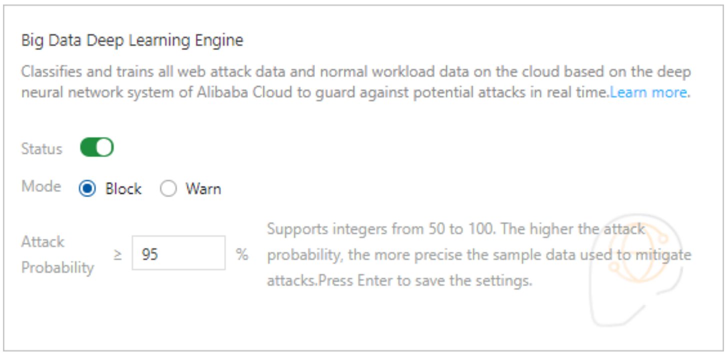


Custom Protection Policy
Supports customizing rules to implement access control. Learn more

Status
Domain-specific-Enabled 0 Custom Protection Policy

Operations: On the **Website Protection** page, click the **Access Control/Throttling** tab. Find the **Custom Protection Policy** card and configure the required parameters. For more information, see Create a custom protection policy.

- **Big Data Deep Learning Engine** (**Warn** mode): The Big Data Deep Learning Engine is trained based on the intelligence of hundreds of millions of samples generated on the cloud every day. This makes up for the weaknesses of the RegEx Protection Engine, especially in terms of defense against deformed or unknown attacks. We recommend that you enable the Big Data Deep Learning Engine in **Warn** mode. Then, observe the anomalies that are detected by the engine over a period of one to two weeks. If the engine works properly, switch to the **Block** mode.



Big Data Deep Learning Engine

Classifies and trains all web attack data and normal workload data on the cloud based on the deep neural network system of Alibaba Cloud to guard against potential attacks in real time.Learn more.

Status: On

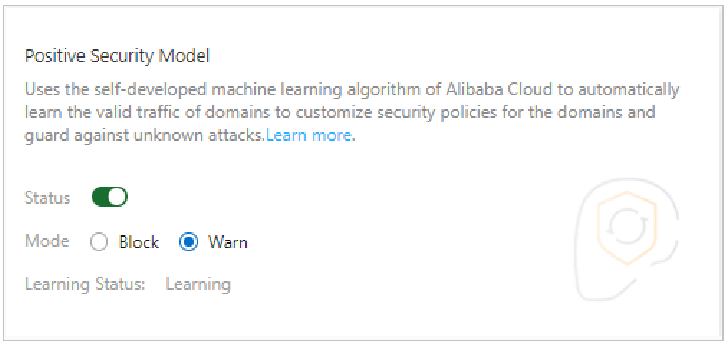
Mode: ● Block ○ Warn

Attack Probability ≥ 95 %

Supports integers from 50 to 100. The higher the attack probability, the more precise the sample data used to mitigate attacks.Press Enter to save the settings.

Operations: On the **Website Protection** page, click the **Web Security** tab. In the **Web Intrusion Prevention** section, find **Big Data Deep Learning Engine**. In the Big Data Deep Learning Engine card, turn on **Status** and set **Mode** to **Warn**. For more information, see Configure the deep learning engine feature.

- **Positive Security Model** (**Warn** mode): The positive security model is built based on the learning of the traffic in the current domain name. The model specifies the types and lengths of request parameters and whether the parameters are required. After the model is built, if a request does not match the characteristics described in the model, an alert is generated. The positive security model in **Warn** mode allows you to effectively detect anomalies and threats to your business. If the detected requests are useless to your business, you can enable the **Block** mode.



Positive Security Model

Uses the self-developed machine learning algorithm of Alibaba Cloud to automatically learn the valid traffic of domains to customize security policies for the domains and guard against unknown attacks.Learn more.

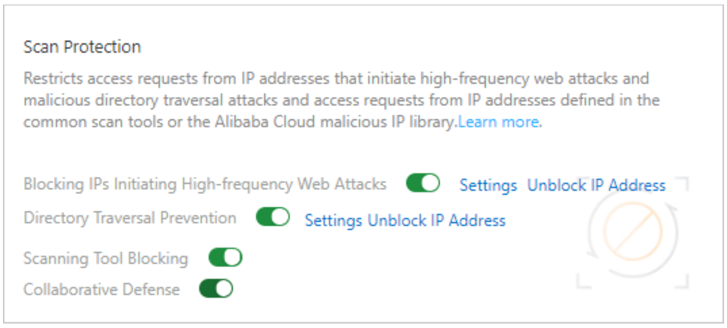
Status: On

Mode: ○ Block ● Warn

Learning Status: Learning

Operations: On the **Website Protection** page, click the **Web Security** tab. In the **Advanced protection** section, find **Positive Security Model**. In the Positive Security Model card, turn on **Status** and set **Mode** to **Warn**. For more information, see Configure the positive security model.

- **Scan Protection** (**Blocking IPs Initiating High-frequency Web Attacks**, **Directory Traversal Prevention**, **Scanning Tool Blocking**, and **Collaborative Defense**): This feature helps reduce the threats generated by your scanner from multiple dimensions, such as intelligence, scanner features, and scan behavior.



Scan Protection

Restricts access requests from IP addresses that initiate high-frequency web attacks and malicious directory traversal attacks and access requests from IP addresses defined in the common scan tools or the Alibaba Cloud malicious IP library.Learn more.

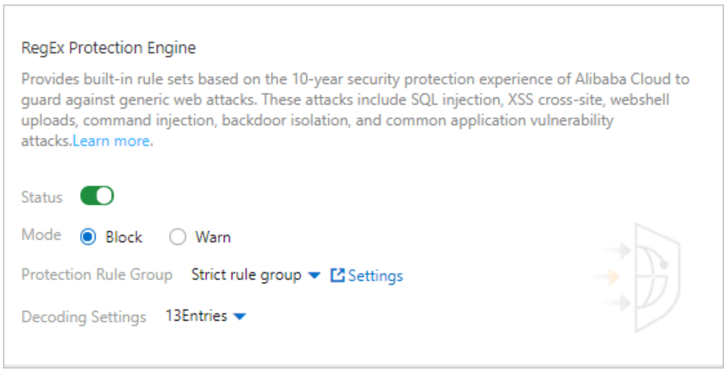
Blocking IPs Initiating High-frequency Web Attacks ● Settings Unblock IP Address
Directory Traversal Prevention ● Settings Unblock IP Address
Scanning Tool Blocking ●
Collaborative Defense ●

Operations: On the **Website Protection** page, click the **Access Control/Throttling** tab. In the **Scan Protection** card, enable all functions and specify appropriate thresholds. For more information, see Configure scan protection.

I want to achieve the strongest protection and radically block attacks

We recommend that you enable the following website protection features after you add your website configurations to WAF:

- **RegEx Protection Engine** (**Strict rule group**)



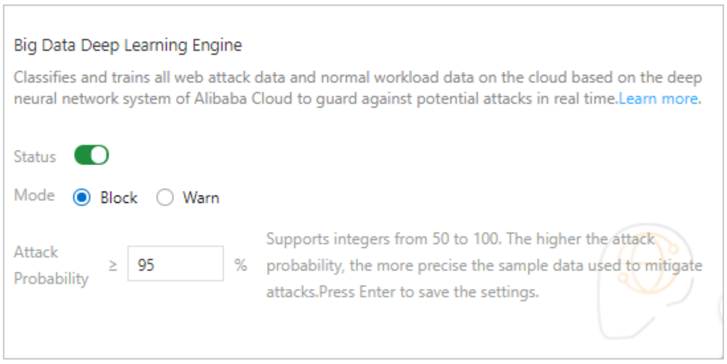
RegEx Protection Engine

Provides built-in rule sets based on the 10-year security protection experience of Alibaba Cloud to guard against generic web attacks. These attacks include SQL injection, XSS cross-site, webshell uploads, command injection, backdoor isolation, and common application vulnerability attacks.Learn more.

Status ●
Mode ● Block ○ Warn
Protection Rule Group Strict rule group ▾ Settings
Decoding Settings 13Entries ▾

Operations: On the **Website Protection** page, click the **Access Control/Throttling** tab. In the **Web Intrusion Prevention** section, find **RegEx Protection Engine**. In the RegEx Protection Engine card, set **Protection Rule Group** to **Strict rule group**. For more information, see Create a custom protection policy.

- **Big Data Deep Learning Engine** (**Block** mode): The Big Data Deep Learning Engine is trained based on the intelligence of hundreds of millions of samples generated on the cloud every day. This makes up for the weaknesses of the RegEx Protection Engine, especially in terms of defense against deformed or unknown attacks. To achieve the strongest protection, we recommend that you enable the **Block** mode.



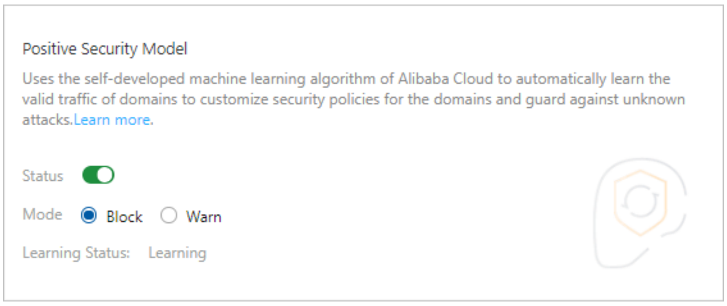
Big Data Deep Learning Engine

Classifies and trains all web attack data and normal workload data on the cloud based on the deep neural network system of Alibaba Cloud to guard against potential attacks in real time.Learn more.

Status ●
Mode ● Block ○ Warn
Attack Probability ≥ 95 % Supports integers from 50 to 100. The higher the attack probability, the more precise the sample data used to mitigate attacks.Press Enter to save the settings.

Operations: On the **Website Protection** page, click the **Web Security** tab. In the **Web Intrusion Prevention** section, find **Big Data Deep Learning Engine**. In the Big Data Deep Learning Engine card, turn on **Status** and set **Mode** to **Block**. For more information, see Configure the deep learning engine feature.

- **Positive Security Model** (**Block** mode): The positive security model is built based on the learning of the traffic in the current domain name. The model specifies the types and lengths of request parameters and whether the parameters are required. After the model is built, if a request does not match the characteristics described in the model, an alert is generated. To achieve the strongest protection, we recommend that you enable the **Block** mode.



Positive Security Model

Uses the self-developed machine learning algorithm of Alibaba Cloud to automatically learn the valid traffic of domains to customize security policies for the domains and guard against unknown attacks.Learn more.

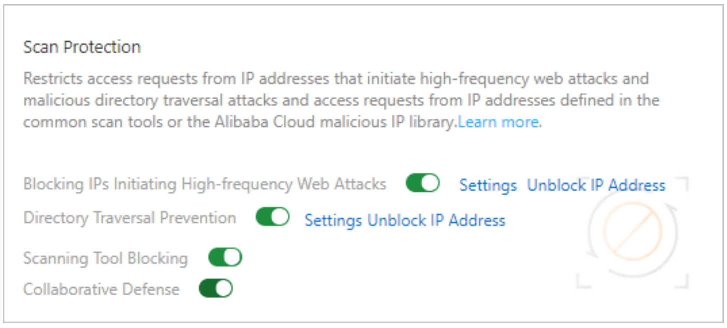
Status

Mode ● Block ○ Warn

Learning Status: Learning

Operations: On the **Website Protection** page, click the **Web Security** tab. In the **Advanced Protection** section, find **Positive Security Model**. In the Positive Security Model card, turn on **Status** and set **Mode** to **Block**. For more information, see Configure the positive security model.

- **Scan Protection** (**Blocking IPs Initiating High-frequency Web Attacks**, **Directory Traversal Prevention**, **Scanning Tool Blocking**, and **Collaborative Defense**): This feature helps reduce the threats generated by your scanner from multiple dimensions, such as intelligence, scanner features, and scan behavior.



Scan Protection

Restricts access requests from IP addresses that initiate high-frequency web attacks and malicious directory traversal attacks and access requests from IP addresses defined in the common scan tools or the Alibaba Cloud malicious IP library.Learn more.

Blocking IPs Initiating High-frequency Web Attacks Settings Unblock IP Address

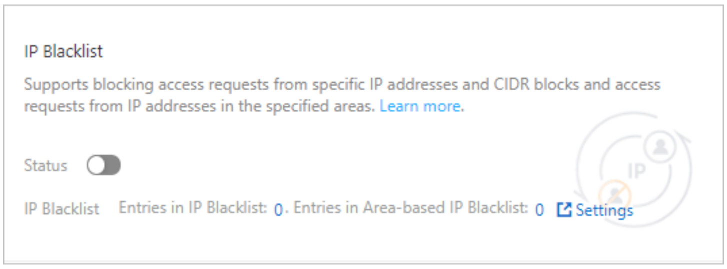
Directory Traversal Prevention Settings Unblock IP Address

Scanning Tool Blocking

Collaborative Defense

Operations: On the **Website Protection** page, click the **Access Control/Throttling** tab. In the **Scan Protection** card, enable all functions and specify appropriate thresholds. For more information, see Configure scan protection.

- **IP Blacklist**: This feature allows you to configure an IP address blacklist to block requests from IP addresses and CIDR blocks that are irrelevant to your business and from IP addresses in specific regions. For example, if a local government forum is accessed only by local IP addresses, you can add IP addresses from other regions to a regional blacklist. If your website does not have users outside China, you can add all the regions outside China to a regional blacklist.



IP Blacklist

Supports blocking access requests from specific IP addresses and CIDR blocks and access requests from IP addresses in the specified areas. Learn more.

Status ○

IP Blacklist Entries in IP Blacklist: 0. Entries in Area-based IP Blacklist: 0 Settings

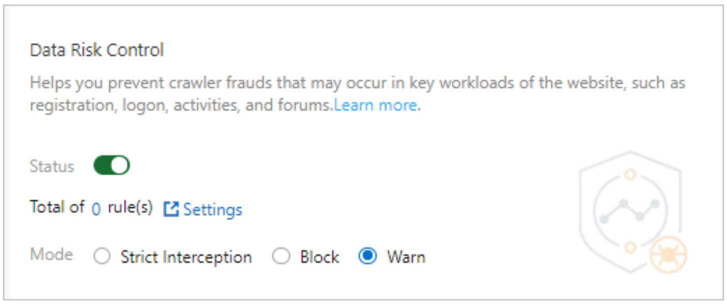
Operations: On the **Website Protection** page, click the **Access Control/Throttling** tab. Find the **IP Blacklist** card and configure the required parameters. For more information, see Configure a blacklist.

My website is often crawled and is at risk of data breach or tampering

We recommend that you enable the following website protection features after you add your website configurations to WAF:

- **Data Risk Control**: This feature is best suited for defending against bot traffic that is generated by scripts or automated tools and destined for specific APIs for logon, registration, and order placing.

  > **Note** Data risk control depends on JavaScript plug-ins and is applicable only to web pages. Do not use this feature in applications. If you are not sure whether this feature is suitable for your API, submit a ticket or contact the technical support by using DingTalk.

  Data Risk Control

  Helps you prevent crawler frauds that may occur in key workloads of the website, such as registration, logon, activities, and forums.Learn more.

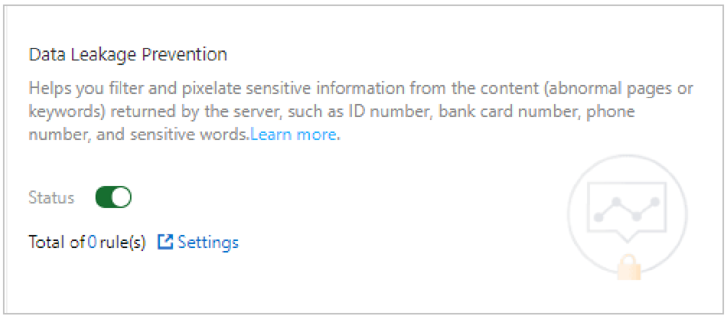
  Status ●

  Total of 0 rule(s) Settings

  Mode ○ Strict Interception ○ Block ● Warn

  Operations: On the **Website Protection** page, click the **Bot Management** tab. In the **Data Risk Control** card, configure the required parameters. For more information, see Configure data risk control.

- **Data Leakage Prevention**: This feature allows you to filter sensitive information in the returned content, such as abnormal pages and keywords, from the server. The sensitive information includes ID numbers, bank card numbers, telephone numbers, and sensitive words.

  Data Leakage Prevention

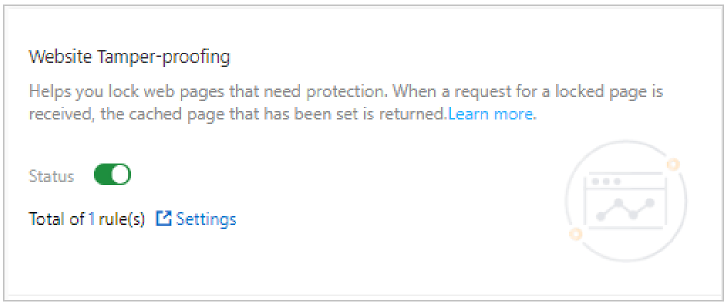
  Helps you filter and pixelate sensitive information from the content (abnormal pages or keywords) returned by the server, such as ID number, bank card number, phone number, and sensitive words.Learn more.

  Status ●

  Total of 0 rule(s) Settings

  Operations: On the **Website Protection** page, click the **Web Security** tab. In the **Data Security** section, find **Data Leakage Prevention**. In the Data Leakage Prevention card, configure the required parameters. For more information, see Configure data leakage prevention.

- **Website Tamper-proofing**: This feature allows you to lock specified web pages to avoid content tampering. When a locked web page receives a request, a cached page you have preconfigured is returned.

  Website Tamper-proofing

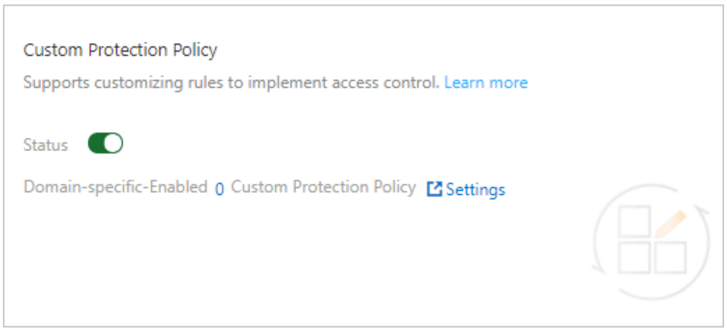
  Helps you lock web pages that need protection. When a request for a locked page is received, the cached page that has been set is returned.Learn more.

  Status

  Total of 1 rule(s) Settings

  Operations: On the **Website Protection** page, click the **Web Security** tab. In the **Data Security** section, find **Website Tamper-proofing**. In the Website Tamper-proofing card, configure the required parameters. For more information, see Configure website tamper-proofing.

- **Custom Protection Policy**: You can enable JavaScript verification for frequently crawled static web pages at one click to block most scripts and automated programs. You can also use fine-grained frequency control to enable slider verification for sessions from which access requests are initiated at an abnormally high frequency.

  Custom Protection Policy

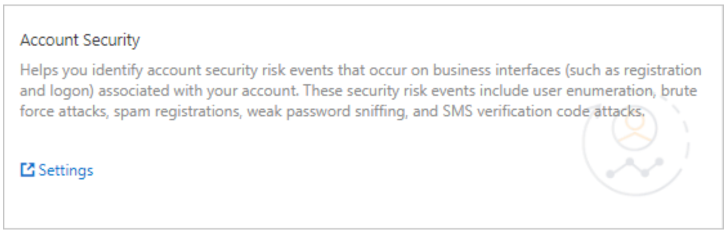
  Supports customizing rules to implement access control. Learn more

  Status

  Domain-specific-Enabled 0 Custom Protection Policy Settings

  Operations: On the **Website Protection** page, click the **Access Control/Throttling** tab. Find the **Custom Protection Policy** card and configure the required parameters. For more information, see Create a custom protection policy.

- **Account Security**: This feature allows you to monitor user authentication-related interfaces, such as the interfaces used for registration and logon, to detect events that may pose a threat to user credentials. These threats include credential stuffing, brute-force attacks, account registrations launched by bots, weak password sniffing, and SMS interface abuse.

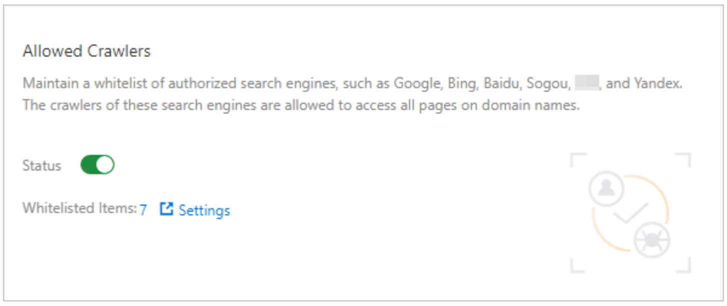
  Account Security

  Helps you identify account security risk events that occur on business interfaces (such as registration and logon) associated with your account. These security risk events include user enumeration, brute force attacks, spam registrations, weak password sniffing, and SMS verification code attacks.

  Settings

  Operations: On the **Website Protection** page, click the **Web Security** tab. In the **Data Security** section, find **Account Security**. In the Account Security card, click **Settings** and configure the required parameters. For more information, see Configure account security.

- **Allowed Crawlers**: This feature maintains a whitelist of authorized search engines, such as Google, Bing, Baidu, Sogou and Yandex. The crawlers of these search engines are allowed to access the specified domain names.



Allowed Crawlers

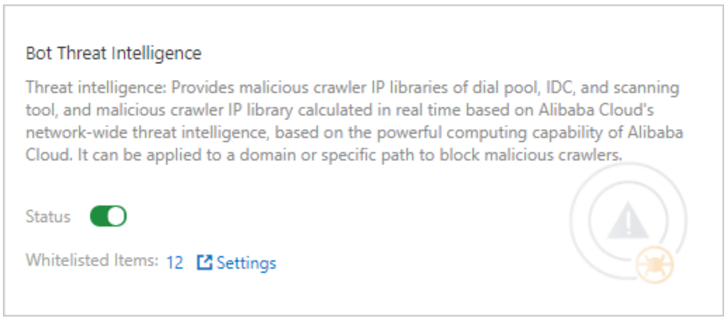
Maintain a whitelist of authorized search engines, such as Google, Bing, Baidu, Sogou, [redacted], and Yandex. The crawlers of these search engines are allowed to access all pages on domain names.

Status

Whitelisted Items: 7 Settings

Operations: On the **Website Protection** page, click the **Bot Management** tab. In the **Allowed Crawlers** card, configure the required parameters. For more information, see Configure the allowed crawlers function.

- **Bot Threat Intelligence**: This feature provides information about suspicious IP addresses used by dialers, data centers, and malicious scanners. This feature also maintains an IP address library of malicious crawlers and prevents crawlers from accessing your website or specific directories.



Bot Threat Intelligence

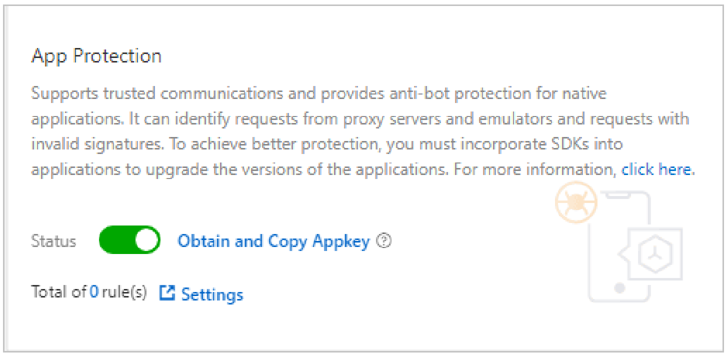
Threat intelligence: Provides malicious crawler IP libraries of dial pool, IDC, and scanning tool, and malicious crawler IP library calculated in real time based on Alibaba Cloud's network-wide threat intelligence, based on the powerful computing capability of Alibaba Cloud. It can be applied to a domain or specific path to block malicious crawlers.

Status

Whitelisted Items: 12 Settings

Operations: On the **Website Protection** page, click the **Bot Management** tab. In the **Bot Threat Intelligence** card, configure the required parameters. For more information, see Set a bot threat intelligence rule.

- **App Protection**: This feature provides secure connections and anti-bot protection for native apps and can identify proxies, emulators, and requests with invalid signatures.



App Protection

Supports trusted communications and provides anti-bot protection for native applications. It can identify requests from proxy servers and emulators and requests with invalid signatures. To achieve better protection, you must incorporate SDKs into applications to upgrade the versions of the applications. For more information, click here.

Status Obtain and Copy Appkey

Total of 0 rule(s) Settings

Operations: On the **Website Protection** page, click the **Bot Management** tab. In the **App Protection** card, configure the required parameters. For more information, see Configure application protection.

9.2. Best practices for the protection rules engine

This topic describes best practices for the protection rules engine provided by Web Application Firewall (WAF).

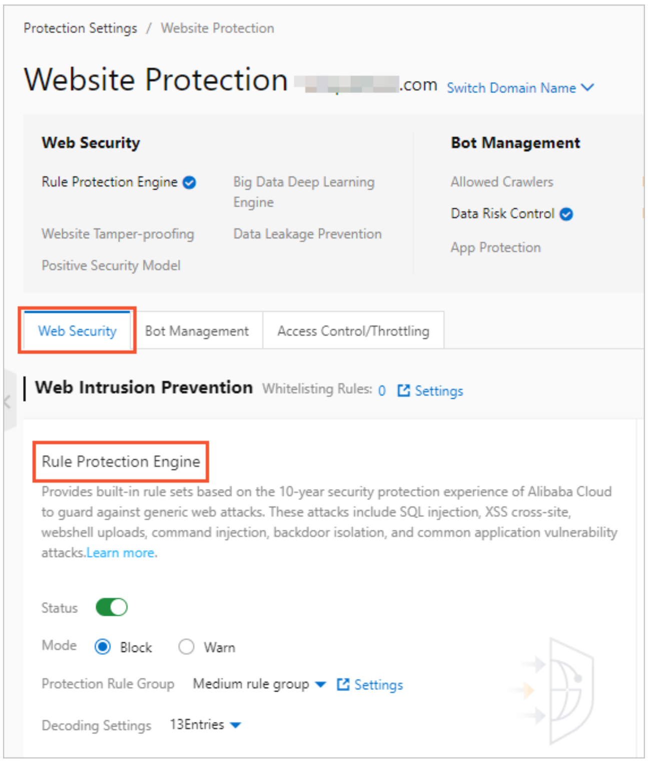
Scenarios

WAF protects your website against web attacks, such as SQL injections, XSS attacks, remote code executions, and webshell attacks. For more information about web attacks, see Definitions of common web vulnerabilities.

> Note WAF cannot defend against server intrusions caused by host security issues, such as unauthorized access to ApsaraDB for Redis or ApsaraDB RDS for MySQL.

Configure protection policies

By default, **Protection Rules Engine** is enabled and Protection Rule Group is set to Medium rule group after you add your website to WAF. This blocks common attacks. You can go to the **Website Protection** page to view the status of **Protection Rules Engine** and configure protection policies. For more information, see Configure the protection rules engine.



Provides built-in rule sets based on the 10-year security protection experience of Alibaba Cloud to guard against generic web attacks. These attacks include SQL injection, XSS cross-site, webshell uploads, command injection, backdoor isolation, and common application vulnerability attacks.Learn more.

Status: On

Mode: ● Block ○ Warn

Protection Rule Group: Medium rule group Settings

Decoding Settings: 13Entries

Protection status description

- **Status**: Turn on or off the switch to enable or disable the protection rules engine. This engine is enabled by default.
- **Mode**: Select the action that you want WAF to take on requests when WAF detects attacks. Valid values:
  - **Block**: WAF automatically blocks requests and logs attacks in the backend.
  - **Warn**: WAF does not block requests but logs attacks in the backend.
- **Protection Rule Group**: Select a group of protection rules that you want to apply. Valid values:

  - **Medium rule group**: blocks common web application attacks in a standard way. These attacks can bypass protection policies.
  - **Strict rule group**: blocks web application attacks in a strict way. These attacks can bypass complex protection policies.
  - **Loose rule group**: blocks common web application attacks.

> **Note** These settings take effect only when you enable the protection rules engine.

If you use WAF Business or Enterprise in mainland China or WAF Enterprise outside mainland China, you can customize protection rule groups. The custom rule groups combine all protection rules provided by WAF and provide specific protection policies for your website. For more information, see Customize protection rule groups.

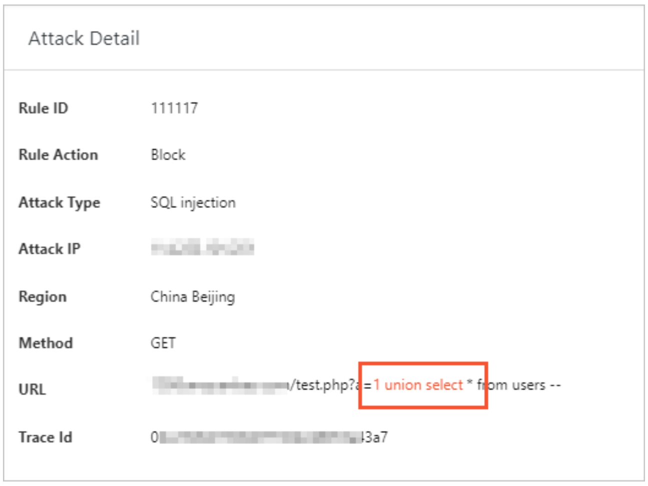
Recommended configurations

- If you are not clear about the characteristics of your business traffic, we recommend that you set Mode to **Warn**. After one or two weeks, analyze the attack logs in this mode.
  - If the attack logs show that normal traffic is not blocked, you can set Mode to **Block**.
  - If the attack logs show that normal traffic is blocked, you can contact Alibaba Cloud security experts to resolve the issue.
- If you add phpMyAdmin and development technology forums to WAF for protection, WAF may block normal traffic. If this occurs, we recommend that you contact Alibaba Cloud security experts to resolve the issue.
- We recommend that you take note of the following points:
  - Do not pass raw SQL statements or JavaScript code in the HTTP requests for your normal business.
  - Do not use special keywords, such as UPDATE or SET, in the paths for normal business URLs. For example, do not use `www.example.com/abc/update/mod.php?set=1` .
  - Do not use a browser to upload files that exceed 50 MB. We recommend that you upload the files by using OSS or other methods. For more information, see Get started with OSS.

View protection effects

After you enable the protection rules engine, you can view its protection records. To view the records, click **Security report**. On the page that appears, click **Web Security** and view the report on the **Web Intrusion Prevention** tab. For more information, see View Security Reports.

The **Web Intrusion Prevention** tab provides charts that display attack records over the last 30 days. The section below the charts lists specific attack records. You can select **Regular Protection**, find an attack record, and click **View Details** to view the attack details. The following figure shows an SQL injection request that is blocked by WAF.



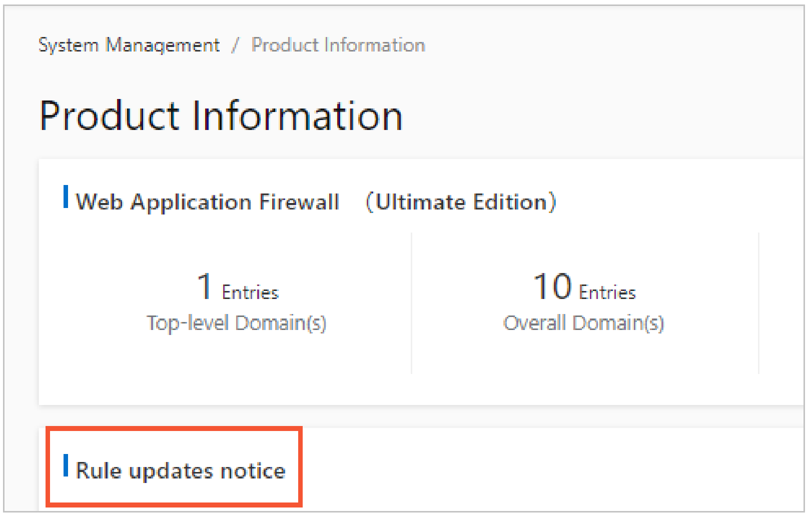
Attack Detail

Rule ID	111117
Rule Action	Block
Attack Type	SQL injection
Attack IP	[redacted]
Region	China Beijing
Method	GET
URL	[redacted]/test.php?a=1 union select * from users --
Trace Id	0[redacted]3a7

> Note If you find that WAF blocks normal traffic, we recommend that you configure a whitelist for the blocked URLs in the **Web Intrusion Prevention** section and then contact Alibaba Cloud security experts to find a solution. For more information, see Configure a whitelist for web intrusion prevention.

View rule updates

WAF updates protection rules and releases protection bulletins in a timely manner to fix known and zero-day vulnerabilities. To view **Rule updates notice**, go to the **Product Information** page. For more information, see View product information.



System Management / Product Information

Product Information

Web Application Firewall (Ultimate Edition)

1 Entries
Top-level Domain(s)

10 Entries
Overall Domain(s)

Rule updates notice

> Note Web attacks have more than one proof of concept (POC). Alibaba Cloud security experts conduct a thorough analysis of vulnerability principles to ensure that published web protection rules cover all disclosed and undisclosed vulnerabilities.

9.3. Best practices for preventing HTTP flood attacks

This topic describes common types of HTTP flood attacks and how to defend against them by using protection policies offered by WAF.

Overview

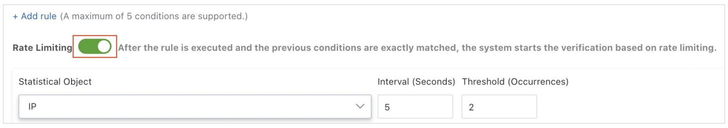
You can determine which protection policies to use based on the attack type.

- Volumetric and high-rate HTTP flood attacks
- Attacks from regions outside China and public clouds
- Malformed packets
- API abuse
- Malicious scans
- App attacks
- Malicious crawlers

Volumetric and high-rate HTTP flood attacks

In volumetric HTTP flood attacks, a zombie server sends requests at a higher frequency than a normal server does. To prevent such attacks, the most effective measure is to limit the request rate of request sources. WAF provides the **Rate Limiting** function for this purpose. You can configure this function from the **Custom Protection Policy** page. For more information, see Create a custom protection policy.

You can configure a rule, as shown in the following figure. The rule blocks all IP addresses that initiate more than 1,000 requests in a 30 second interval to any path under the domain name. The blocking period lasts for 10 hours. This rule is used to protect small and medium-sized websites.

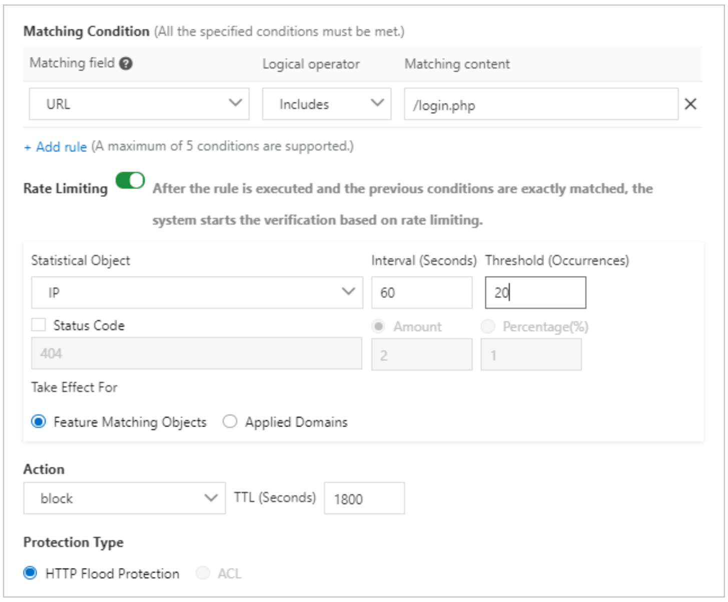


+ Add rule (A maximum of 5 conditions are supported.)

Rate Limiting ● After the rule is executed and the previous conditions are exactly matched, the system starts the verification based on rate limiting.

Statistical Object	Interval (Seconds)	Threshold (Occurrences)
IP	5	2

You can modify the protected path, adjust the threshold, and select the optimal action to best suit your protection requirements. For example, to prevent credential stuffing on logon endpoints, you can set **Matching field** to URL and **Matching content** to `/login.php` , and block IP addresses that send more than 20 requests to access the path within 60 seconds.



Matching Condition (All the specified conditions must be met.)

Matching field	Logical operator	Matching content
URL	Includes	/login.php

+ Add rule (A maximum of 5 conditions are supported.)

Rate Limiting After the rule is executed and the previous conditions are exactly matched, the system starts the verification based on rate limiting.

Statistical Object	Interval (Seconds)	Threshold (Occurrences)
IP	60	20
□ Status Code	● Amount	○ Percentage(%)
404	2	1

Take Effect For

● Feature Matching Objects ○ Applied Domains

Action

block TTL (Seconds) 1800

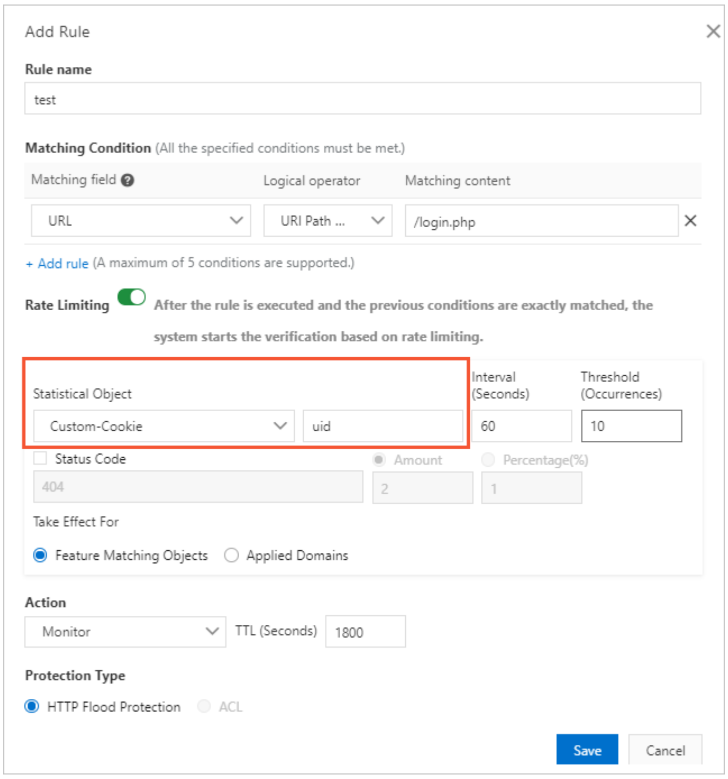
Protection Type

● HTTP Flood Protection ○ ACL

Note the following points when you configure HTTP flood protection policies:

- **Captcha** and **Strict Captcha** in the **Action** drop-down list aim to verify whether requests originate from a human or an automation script. You can use these two actions to protect common and HTML5 web pages, but not native apps or APIs. To protect the native apps and APIs, set **Action** to **block**.
- You can configure whitelist policies for APIs or IP addresses that may be mistakenly blocked by HTTP flood protection on the **Access Control/Throttling** tab. For more information, see Configure a whitelist for Access Control/Throttling.
- Do not select the **Protection-emergency** mode for native apps or APIs in the **HTTP Flood Protection** section.

If you have purchased an instance of the WAF Enterprise edition, you can configure rate limiting by using custom statistical objects, IP addresses, and sessions. Blocking IP addresses may affect NAT. You can use cookies or parameters that identify users as statistical objects. In the following example, the request rate is calculated based on the cookie that is used to identify the user, and Captcha is used to verify the requests. Assume that the cookie format is as follows: `uid=12345` .



Add Rule

Rule name

test

Matching Condition (All the specified conditions must be met.)

Matching field	Logical operator	Matching content
URL	URI Path ...	/login.php

+ Add rule (A maximum of 5 conditions are supported.)

Rate Limiting After the rule is executed and the previous conditions are exactly matched, the system starts the verification based on rate limiting.

Statistical Object		Interval (Seconds)	Threshold (Occurrences)
Custom-Cookie	uid	60	10

□ Status Code: 404 ● Amount: 2 ○ Percentage(%): 1

Take Effect For

● Feature Matching Objects ○ Applied Domains

Action

Monitor TTL (Seconds) 1800

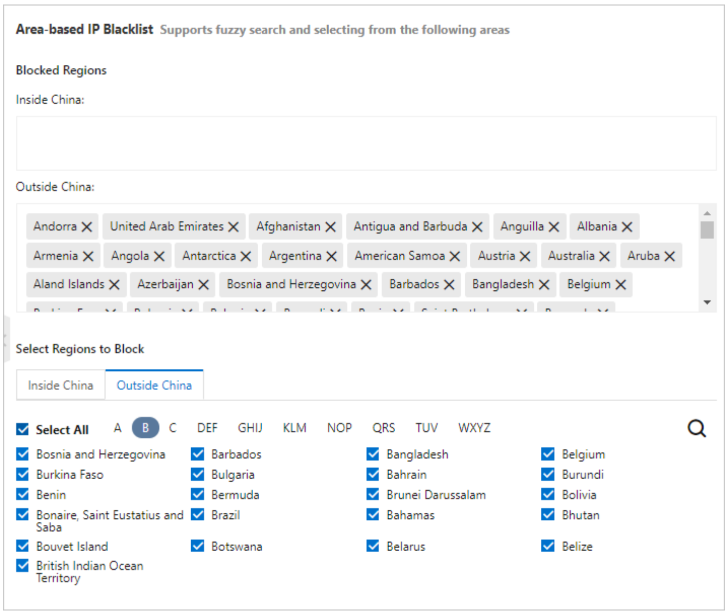
Protection Type

● HTTP Flood Protection ○ ACL

Attacks from regions outside China and public clouds

A large portion of HTTP flood attacks originate from regions outside China, on-premises data centers, and public clouds.

If your website targets users inside China, you can block requests from regions outside China to mitigate this type of attack. WAF provides the **Area-based IP Blacklist** function for this purpose. For more information, see Configure a blacklist



Area-based IP Blacklist Supports fuzzy search and selecting from the following areas

Blocked Regions

Inside China:

Outside China:

Andorra ✕ United Arab Emirates ✕ Afghanistan ✕ Antigua and Barbuda ✕ Anguilla ✕ Albania ✕
Armenia ✕ Angola ✕ Antarctica ✕ Argentina ✕ American Samoa ✕ Austria ✕ Australia ✕ Aruba ✕
Aland Islands ✕ Azerbaijan ✕ Bosnia and Herzegovina ✕ Barbados ✕ Bangladesh ✕ Belgium ✕

Select Regions to Block

Inside China | Outside China

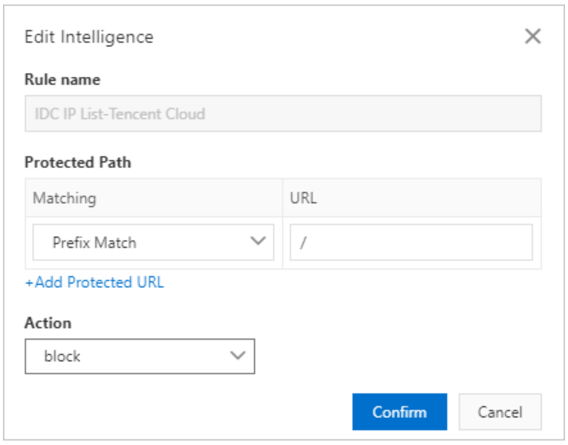
☑ Select All A B C DEF GHIJ KLM NOP QRS TUV WXYZ

☑ Bosnia and Herzegovina	☑ Barbados	☑ Bangladesh	☑ Belgium
☑ Burkina Faso	☑ Bulgaria	☑ Bahrain	☑ Burundi
☑ Benin	☑ Bermuda	☑ Brunei Darussalam	☑ Bolivia
☑ Bonaire, Saint Eustatius and Saba	☑ Brazil	☑ Bahamas	☑ Bhutan
☑ Bouvet Island	☑ Botswana	☑ Belarus	☑ Belize
☑ British Indian Ocean Territory			

If you need to block the crawler IP addresses of common IP libraries, such as the CIDR blocks of Alibaba Cloud, Tencent Cloud, and on-premises data centers, you can use the **Bot Threat Intelligence** function on the **Bot Management** tab.

> **Note** Many crawlers are deployed on ECS instances. Users do not access your services by using the source IP addresses of public clouds or on-premises data centers.

Example: You can use the following bot threat intelligence rule to block accesses from the crawler IP addresses of Tencent Cloud. For more information, see Set a bot threat intelligence rule.



Edit Intelligence

Rule name: IDC IP List-Tencent Cloud

Protected Path

Matching	URL
Prefix Match	/

Action: block

Malformed packets

Malicious requests in HTTP flood attacks are specially crafted and contain malformed packets. Malformed packets have the following features:

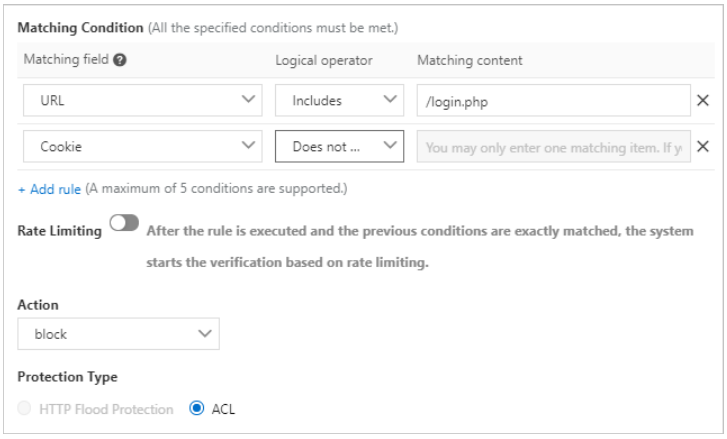
- Abnormal or malformed User-Agent string: has characteristics of automation tools (such as Python), is in an incorrect format (such as `Mozilla///`), or is impossible to be used in normal requests (such as `www.example.com`). If abnormal or malformed User-Agent strings are detected, block the requests.

- Unusual User-Agent string: Promotional HTML5 pages that target WeChat users are supposed to be accessed through WeChat. It is unusual if the User-Agent string indicates that the request is sent from a Windows desktop browser, such as Microsoft Internet Explorer 6.0. If unusual User-Agent strings are detected, block the requests.
- Abnormal referer field: If a request does not have a referer field or has a referer field that identifies the addresses of illegitimate websites, block the request. However, when a user visits your homepage or your website for the first time, the request may not contain the referer field. If a URL can only be accessed by using redirects, you can decide whether to block the URL based on the referer field.
- Abnormal cookie: Similar to the referer field, a normal request contains cookies that identify the requested websites, unless it is the first time for the user to visit your website. Malicious requests in HTTP flood attacks typically do not contain any cookie information. You can block access requests without cookies.
- Missing HTTP headers: Normal requests contain authorization headers while malicious requests do not.
- Incorrect request methods: If an API has only received POST requests before but is now overwhelmed by GET requests, you can block these GET requests.

You can analyze the features of requests and set Protection Type to **ACL** from the **Custom Protection Policy** page to block malicious requests. For more information, see Create a custom protection policy.

Configuration examples:

- Example 1: Block requests that do not contain cookies.



Matching Condition (All the specified conditions must be met.)

Matching field	Logical operator	Matching content
URL	Includes	/login.php
Cookie	Does not ...	You may only enter one matching item. If y

+ Add rule (A maximum of 5 conditions are supported.)

Rate Limiting After the rule is executed and the previous conditions are exactly matched, the system starts the verification based on rate limiting.

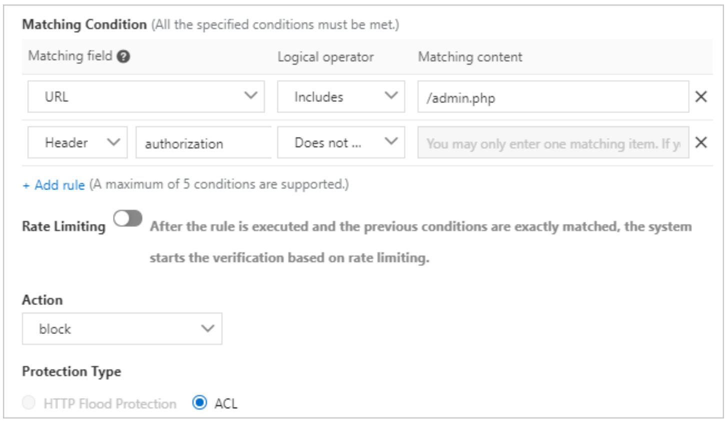
Action

block

Protection Type

○ HTTP Flood Protection ● ACL

- Example 2: Block requests that do not contain authorization headers.



Matching Condition (All the specified conditions must be met.)

Matching field	Logical operator	Matching content
URL	Includes	/admin.php
Header authorization	Does not ...	You may only enter one matching item. If y

+ Add rule (A maximum of 5 conditions are supported.)

Rate Limiting After the rule is executed and the previous conditions are exactly matched, the system starts the verification based on rate limiting.

Action

block

Protection Type

○ HTTP Flood Protection ● ACL

API abuse

We recommend that you use the data risk control function to protect important APIs from attacks. These APIs include logon, registration, voting, and SMS verification APIs.

Data risk control injects a JavaScript snippet into your website and collects information about user behaviors and environment variables to determine whether requests originate from a human or an automation script. Data risk control makes decisions based on CAPTCHA rather than the request rate or the source IP address. The function mitigates low-frequency attacks very effectively.

> **Notice** Data risk control checks whether requests contain authentication parameters required by all normal requests to identify malicious requests. The function is not suitable for environments where JavaScript is not supported, such as APIs and native apps. To prevent false positives, we recommend that you test data risk control in the test environment before you enable it. Alternatively, you can use the observation mode and contact engineers before you enable the prevention mode.

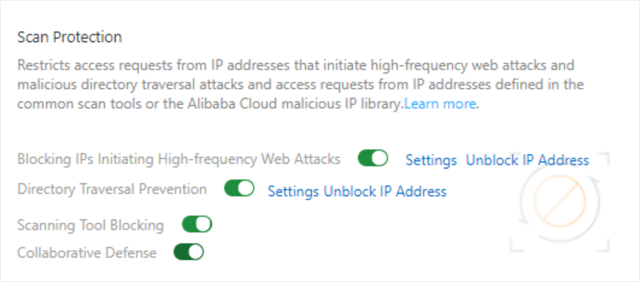
For more information, see Configure data risk control.

Malicious scans

A large number of malicious scans pose a serious threat to the performance of your servers. Apart from rate limiting, you can also use the **Scan Protection** function to enhance security. Scan protection supports the following settings:

- **Blocking IPs Initiating High-frequency Web Attacks**: automatically blocks client IP addresses that initiate high-frequency web attacks.
- **Directory Traversal Prevention**: automatically blocks client IP addresses that initiate multiple directory traversal attacks in a short period of time.
- **Scanning Tool Blocking**: automatically blocks access requests from IP addresses defined in the common scan tools or the Alibaba Cloud malicious IP library.
- **Collaborative Defense**: automatically blocks access requests from IP addresses defined in the Alibaba Cloud malicious IP library.

For more information, see Configure scan protection.



Scan Protection

Restricts access requests from IP addresses that initiate high-frequency web attacks and malicious directory traversal attacks and access requests from IP addresses defined in the common scan tools or the Alibaba Cloud malicious IP library.Learn more.

Blocking IPs Initiating High-frequency Web Attacks ● Settings Unblock IP Address

Directory Traversal Prevention ● Settings Unblock IP Address

Scanning Tool Blocking ●

Collaborative Defense ●

App attacks

In addition to the preceding measures, you can also use SDK to enhance protection.

After you integrate the SDK with your app, all incoming requests are verified before they are sent to your server. The device information and request signature are combined to determine whether the requests are from legitimate apps. Requests that do not originate from official apps are automatically blocked. This ensures that only valid requests are served. You do not need to analyze the patterns of invalid requests.

To use the SDK, you must enable **App Protection**. For more information, see Configure application protection.

Malicious crawlers

For informational websites that offer services such as credit reports, apartment rentals, airline tickets, and e-book reading, malicious crawlers can significantly increase the bandwidth usage and server workload, and even cause data leaks. If the preceding measures cannot prevent against malicious crawlers, we recommend that you enable and use the **Bot Management** feature for more effective protection. For more information, see Configure a whitelist for Bot Management.

9.4. Account security best practices

Web Application Firewall (WAF) provides an account security feature that helps you identify account risks. This topic describes how to protect interfaces in different scenarios. You can follow the instructions in this topic to better protect interfaces on which user authentication is performed.

Context

WAF supports the account security feature that detects account risks. This feature monitors interfaces related to user authentication, such as registration and logon interfaces, and detects risks on these interfaces. These risks include credential stuffing, brute-force attacks, spam registration, weak password sniffing, and SMS interface abuse. After interfaces are added to WAF, you can view detection results in WAF security reports. For more information, see Configure account security.

Use verification services to protect common and HTML5 web pages

Verification services are the easiest and most effective approaches to protect interfaces. The integration of verification services into your business typically requires minor code changes. It may take one or two business days to modify the code.

Common verification methods can block direct calls launched from simple tools or scripts. However, due to the adaptation of attack methods and tools, the common verification methods can be easily bypassed. We recommend that you use professional verification services to better protect interfaces against attacks.

Use SDK signatures to protect native apps

Verification services may be unsuitable for native apps. Alibaba Cloud provides an SDK solution for native apps. The solution collects the information about the hardware and environment of a mobile device, calculates signatures, and verifies signatures of requests. This ensures that only requests from verified apps are directed to the origin server. Requests sent from scripts, automated programs, simulators, and other unverified sources are blocked.

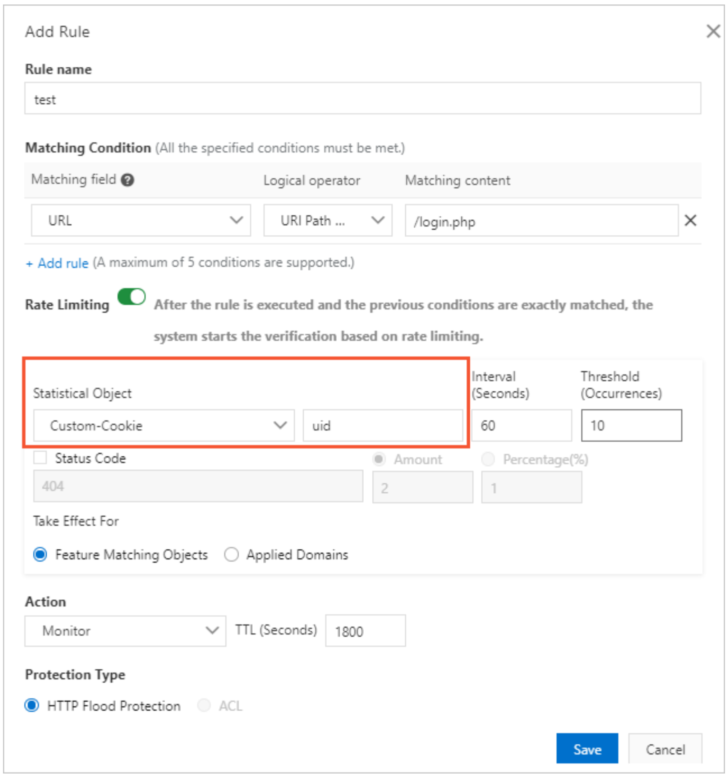
> **Note** To use the SDK solution, you must enable **App Protection** in the WAF console. For more information, see App protection overview.

Configure frequency control to block attack sources

Frequency control helps you identify requests that contain a common field among a large number of requests. You can specify the maximum occurrences of the common field. The source of the requests is blocked when the maximum occurrences are exceeded. Traditional protection methods typically block malicious IP addresses. Malicious requests sent from proxies or rotating IP addresses may contain the same token, for example, the same UID, in their cookies. In this case, you can configure the maximum occurrences based on the cookies to block malicious accounts.

WAF provides **Rate Limiting** for this purpose. You can configure rate limiting on the **Custom Protection Policy** page, as shown in the following figure. For more information, see Create a custom protection policy.

> **Note** All WAF editions allow you to use IP addresses and sessions as statistical objects. WAF Enterprise allows you to use more objects, such as custom cookies, custom headers, and custom parameters.



Add Rule

Rule name: test

Matching Condition (All the specified conditions must be met.)

Matching field	Logical operator	Matching content
URL	URI Path ...	/login.php

+ Add rule (A maximum of 5 conditions are supported.)

Rate Limiting: on. After the rule is executed and the previous conditions are exactly matched, the system starts the verification based on rate limiting.

Statistical Object		Interval (Seconds)	Threshold (Occurrences)
Custom-Cookie	uid	60	10

□ Status Code: 404 ● Amount: 2 ○ Percentage(%): 1

Take Effect For: ● Feature Matching Objects ○ Applied Domains

Action: Monitor TTL (Seconds): 1800

Protection Type: ● HTTP Flood Protection ○ ACL

Analyze suspicious requests

Malicious requests have certain common characteristics. The following examples describe common characteristics among malicious requests.

- Incomplete HTTP headers. Malicious requests may exclude certain fields, such as Referer, Cookie, or Content-Type.
- Abnormal User-Agent values. User-Agent headers used in requests that target Java or Python-based websites are found in requests sent to common websites. User-Agent headers used in requests initiated from desktop browsers are found in requests sent to WeChat mini programs. In these cases, requests that contain abnormal User-Agent headers may be malicious.
- Missing cookies. Typically, multiple cookies are used in an application. Common cookies include SessionID, userid, deviceid, and lastvisit. However, crawlers may include only one or two cookies that are required for retrieving information and exclude other cookies that identify users.

- Abnormal parameters. Similar to missing cookies, some parameters are not required for crawlers to retrieve information. Crawlers may exclude or repeatedly submitted these parameters in requests.
- Suspicious fields. Suspicious fields may be contained in email addresses, phone numbers, and account information.

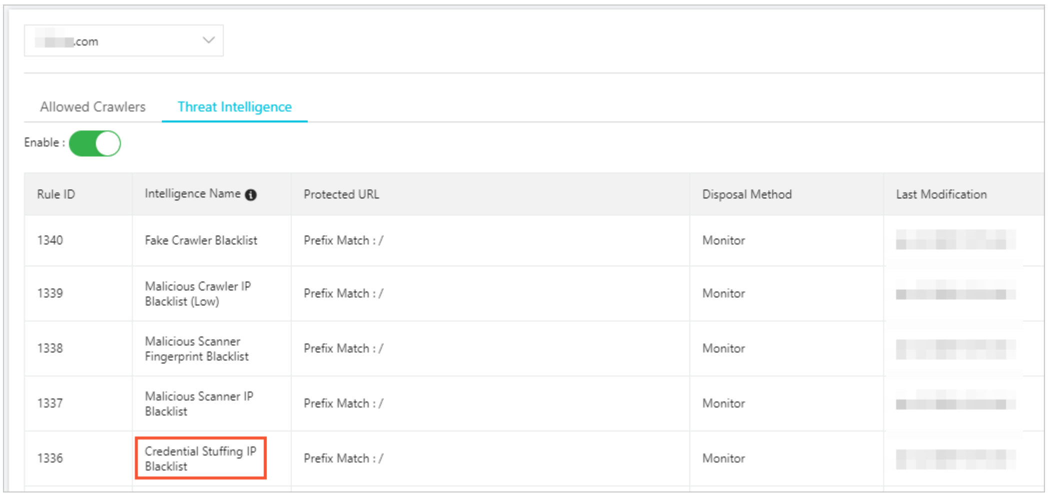
We recommend that you use the Log Service of WAF feature to query logs. This feature allows you to analyze request characteristics, such as top IP addresses and the proportion of requests with certain characteristics to total requests.

> **Note** To use the Log Service of WAF feature, you must enable **Log Service** from the WAF console. For more information, see Enable Log Service for WAF.

Enable credential stuffing and bot threat intelligence

WAF provides a **Bot Management** feature. This feature uses algorithms and identifies malicious IP addresses from credential stuffing attacks detected by Alibaba Cloud. A credential stuffing IP address blacklist is created and updated dynamically. You can use the **Bot Threat Intelligence** function from the Bot Management tab to set the credential stuffing IP address blacklist to the Monitor, Block, or Captcha mode. For more information, see Set a bot threat intelligence rule.

> **Note** You must enable the **Bot Management** feature before you can use the **Bot Threat Intelligence** function.



[redacted].com

Enable : ●

Rule ID	Intelligence Name	Protected URL	Disposal Method	Last Modification
1340	Fake Crawler Blacklist	Prefix Match : /	Monitor	[redacted]
1339	Malicious Crawler IP Blacklist (Low)	Prefix Match : /	Monitor	[redacted]
1338	Malicious Scanner Fingerprint Blacklist	Prefix Match : /	Monitor	[redacted]
1337	Malicious Scanner IP Blacklist	Prefix Match : /	Monitor	[redacted]
1336	Credential Stuffing IP Blacklist	Prefix Match : /	Monitor	[redacted]

9.5. Best practices for using custom rule groups to provide enhanced protection

If you find that RegEx Protection Engine of WAF blocks normal requests to your website, you can customize protection rule groups to avoid this issue.

Prerequisites

- A WAF instance is purchased. The instance must meet the following requirements:
  - The instance uses the subscription billing method.

  - If the instance is deployed **in mainland China**, the instance must be of the **Business** edition or higher.
  - If the instance is deployed **outside mainland China**, the instance must be of the **Enterprise** edition or higher.

  For more information, see Purchase a WAF instance.

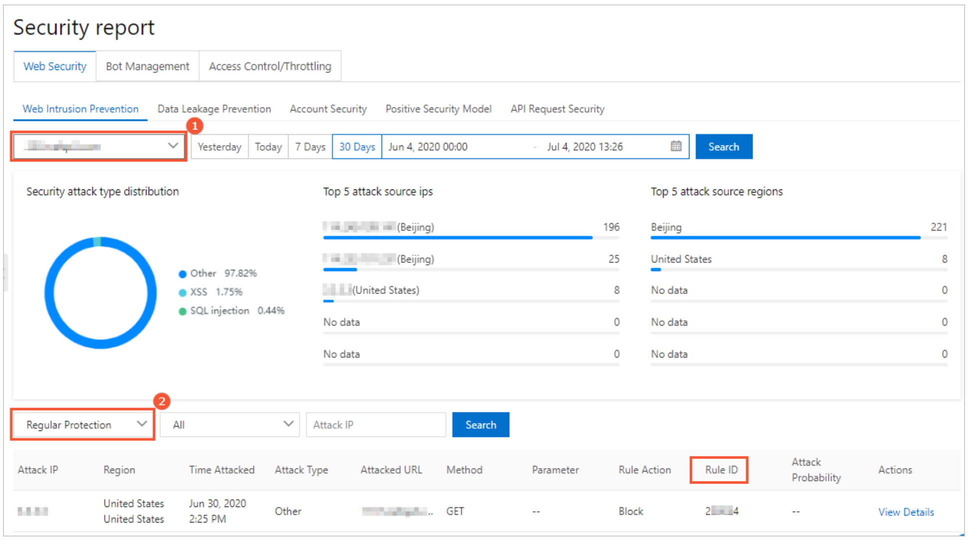
-

Context

To address this issue, you must identify the protection rule that causes the issue, create a custom rule group for the affected domain name, and then remove the protection rule from the custom rule group.

Procedure

1.
2.
3.
4. Identify the ID of the protection rule that causes false positives.
   i. On the **Web Security** tab, click **Web Intrusion Prevention**, select the target domain name, and select **Regular Protection** in the lower part of the page to view attack records.



[redacted]

Jun 4, 2020 00:00 - Jul 4, 2020 13:26

Top 5 attack source ips

[redacted] (Beijing)	196
[redacted] (Beijing)	25
[redacted] (United States)	8
No data	0
No data	0

Top 5 attack source regions

Beijing	221
United States	8
No data	0
No data	0
No data	0

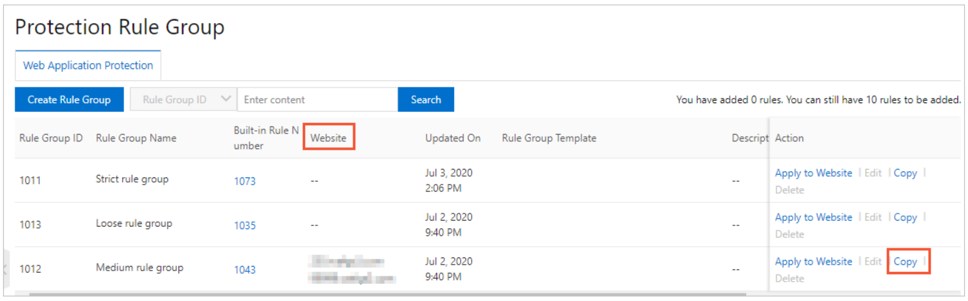
Attack IP	Region	Time Attacked	Attack Type	Attacked URL	Method	Parameter	Rule Action	Rule ID	Attack Probability	Actions
[redacted]	United States United States	Jun 30, 2020 2:25 PM	Other	[redacted]..	GET	--	Block	2[redacted]4	--	View Details

   ii. In the attack record list, find the false positive record and record the rule ID. You can search for the record by using the attack IP address.

5.
6. Create a custom rule group and remove the protection rule from the rule group.

i. In the rule group list on the **Web Application Protection** tab, find the rule group that applies to the affected domain name.

> **Note** To find the rule group, search for the affected domain name in the **Website** column.



Protection Rule Group

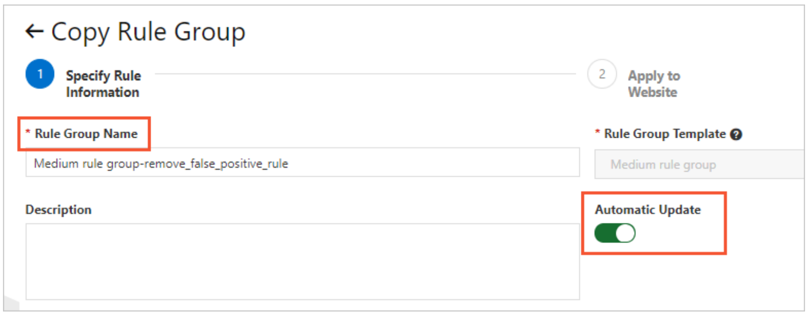
Web Application Protection

You have added 0 rules. You can still have 10 rules to be added.

Rule Group ID	Rule Group Name	Built-in Rule Number	Website	Updated On	Rule Group Template	Descript	Action
1011	Strict rule group	1073	--	Jul 3, 2020 2:06 PM		--	Apply to Website | Edit | Copy | Delete
1013	Loose rule group	1035	--	Jul 2, 2020 9:40 PM		--	Apply to Website | Edit | Copy | Delete
1012	Medium rule group	1043	[redacted]	Jul 2, 2020 9:40 PM		--	Apply to Website | Edit | Copy | Delete

ii. Click **Copy** in the Action column. Assume that the **Medium rule group** causes the issue.

iii. On the **Copy Rule Group** page, modify **Rule Group Name**, turn on **Automatic Update**, and click **Save**. You can change the rule group name to medium rule group-remove false positive rule.



← Copy Rule Group

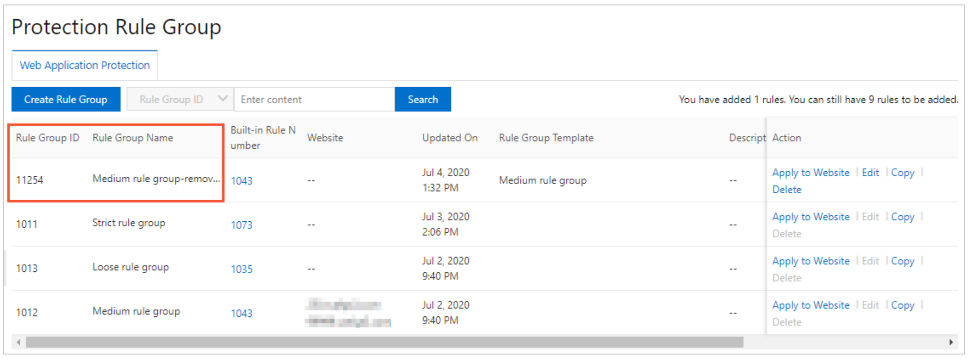
* Rule Group Name: Medium rule group-remove_false_positive_rule

* Rule Group Template: Medium rule group

Description:

Automatic Update: ●

After you copy the rule group, you can view it in the rule group list.



Protection Rule Group

Web Application Protection

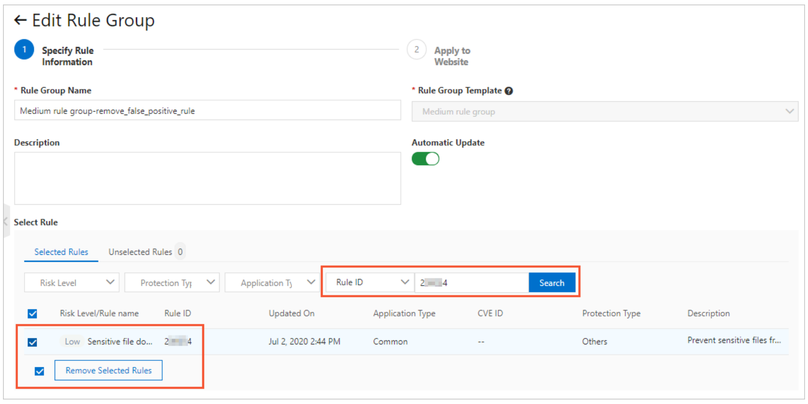
You have added 1 rules. You can still have 9 rules to be added.

Rule Group ID	Rule Group Name	Built-in Rule Number	Website	Updated On	Rule Group Template	Descript	Action
11254	Medium rule group-remov...	1043	--	Jul 4, 2020 1:32 PM	Medium rule group	--	Apply to Website | Edit | Copy | Delete
1011	Strict rule group	1073	--	Jul 3, 2020 2:06 PM		--	Apply to Website | Edit | Copy | Delete
1013	Loose rule group	1035	--	Jul 2, 2020 9:40 PM		--	Apply to Website | Edit | Copy | Delete
1012	Medium rule group	1043	[redacted]	Jul 2, 2020 9:40 PM		--	Apply to Website | Edit | Copy | Delete

iv. Find the rule group that you copy and click **Edit** in the Action column.

v. On the **Edit Rule Group** page, search for the rule that causes false positives by using the **rule ID**, select the rule, and then click **Remove Selected Rules**.

> **Note** Before you remove a protection rule from a custom rule group, make sure that you select the exact rule that blocks normal requests.



← Edit Rule Group

* Rule Group Name: Medium rule group-remove_false_positive_rule

* Rule Group Template: Medium rule group

Description:

Automatic Update: on

Select Rule

Rule ID: 2[redacted]4 Search

☑	Risk Level/Rule name	Rule ID	Updated On	Application Type	CVE ID	Protection Type	Description
☑	Low Sensitive file do...	2[redacted]4	Jul 2, 2020 2:44 PM	Common	--	Others	Prevent sensitive files fr...

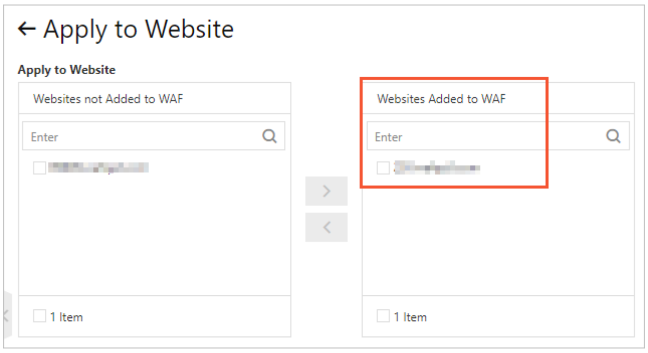
☑ Remove Selected Rules

vi. Click **Save**.

7. Apply the custom rule group to your website.

   i. Find the rule group that you copy and click **Apply to Website** in the Action column.

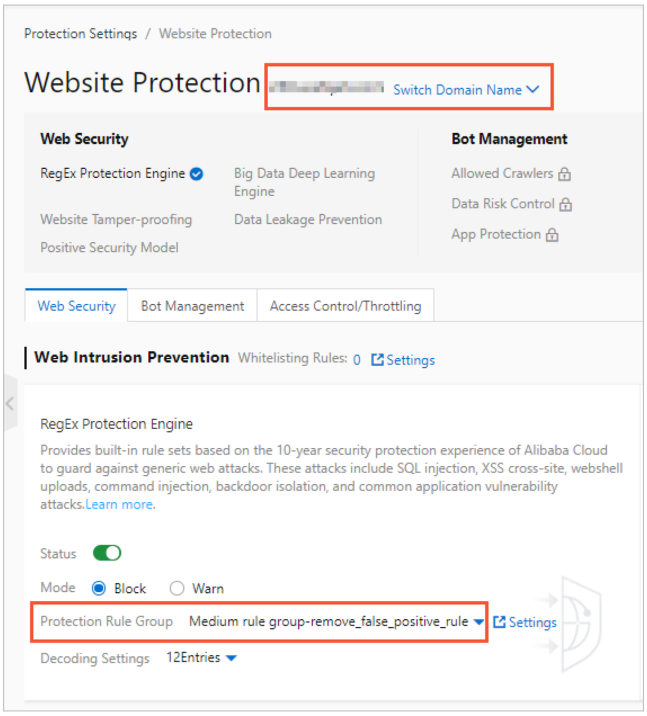
   ii. On the **Apply to Website** page, add the affected domain name to the **Websites Added to WAF** section and click **Save**.



← Apply to Website

Apply to Website

After you apply the custom rule group, you can go to the **Website Protection** page and view the **RegEx Protection Engine** settings. The **Protection Rule Group** changes to the custom rule group that you apply. For more information, see Configure the protection rules engine feature.



Protection Settings / Website Protection

Website Protection [redacted] Switch Domain Name

Web Security

RegEx Protection Engine ✓

Big Data Deep Learning Engine

Website Tamper-proofing

Data Leakage Prevention

Positive Security Model

Bot Management

Allowed Crawlers

Data Risk Control

App Protection

Web Security | Bot Management | Access Control/Throttling

Web Intrusion Prevention Whitelisting Rules: 0 Settings

RegEx Protection Engine

Provides built-in rule sets based on the 10-year security protection experience of Alibaba Cloud to guard against generic web attacks. These attacks include SQL injection, XSS cross-site, webshell uploads, command injection, backdoor isolation, and common application vulnerability attacks.Learn more.

Status: On

Mode: ● Block ○ Warn

Protection Rule Group: Medium rule group-remove_false_positive_rule Settings

Decoding Settings: 12Entries

When the website receives the same access requests again, WAF does not block the requests.

> **Note** If the requests are still blocked, make sure you identify the correct ID of the protection rule that causes false positives and remove this rule from the custom rule group.