

Alibaba Cloud Web Application Firewall

User Guide

Issue: 20181212

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 due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information 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.
	This warning information 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 restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Note: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus, page names, and other UI elements.	Click OK .
Courier font	It is used for commands.	Run the <code>cd /d C:/windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is a optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	It indicates that it is a required value, and only one item can be selected.	<code>swich {stand / slave}</code>

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 Access WAF.....	1
1.1 Website configuration.....	1
1.2 Mark WAF back-to-origin flow.....	8
1.3 WAF deployment guide.....	9
1.4 Whitelist Alibaba Cloud WAF IP addresses.....	14
1.5 Perform redirect check with a local computer.....	16
1.6 Update HTTPS certificates.....	17
1.7 HTTPS advanced settings.....	21
1.8 Supported non-standard ports.....	23
1.9 Load balance across multiple origin IPs.....	24
1.10 Deploy WAF and Anti-DDoS Pro together.....	26
1.11 Deploy WAF and CDN together.....	27
2 Protection configuration.....	31
3 Protection reports.....	32
4 SDK solution.....	33
4.1 Access the WAF SDK.....	33
4.2 iOS integration manual.....	34
4.3 Android integration manual.....	39
5 Real-time log query and analysis.....	47
5.1 Billing method.....	47
5.2 Activate WAF Log Service.....	49
5.3 Log collection.....	50
5.4 Log Analyses.....	53
5.5 Log Reports.....	67
5.6 Fields in the log entry.....	79
5.7 Advanced settings.....	84
5.8 Export log entries.....	84
5.9 Grant log query and analysis permissions to a RAM user.....	86
5.10 Manage log storage.....	89

1 Access WAF

1.1 Website configuration

Website configuration describes the forwarding routes of the websites that are deployed with Alibaba Cloud WAF.

You can add a website configuration by using the [automatic](#) or [manual](#) method.

- Automatically create a website configuration. When you are creating a website configuration, WAF accesses your A record configurations in [Alibaba Cloud DNS](#) and lists all website domains and their origin server IP addresses. You can simply select the domains for which you want to enable WAF protection and let WAF do the rest of configurations. In this way, WAF also helps update the DNS settings to redirect web traffic to WAF for inspection.
- Manually create a website configuration. If no A record has been created in Alibaba Cloud DNS, you must manually create the website configuration. After that, you must log on to the DNS host's system to update the DNS settings to redirect web traffic to WAF for inspection.

For more information about how to update the DNS settings, see [WAF deployment guide](#).

**Note:**

The number of website configurations you can add to the Alibaba Cloud WAF instance depends on your subscription plan and the number of extra domains. For more information, see [Extra domain quota](#).

When your origin server addresses, protocol types, or ports change, or you want to configure the HTTPS advanced settings, you can [edit the website configuration](#).

For websites that do not need WAF protection any more, you can restore their DNS settings and [delete the website configuration](#).

Automatically add a website configuration

Prerequisites

- The domain to be protected is hosted at Alibaba Cloud DNS. Besides, its DNS settings must include at least one valid A record.

If you do not use Alibaba Cloud DNS, see [Website configuration](#) to manually add the website configuration.

- (For Mainland China region) The website is granted an ICP license by the Ministry of Industry and Information Technology (MIIT).
- (For HTTPS-enabled websites) You have access to a valid SSL certificate and private key of the website, or you have uploaded the certificate to Alibaba Cloud SSL Certificate Service.

Procedure

1. Log on to the [Alibaba Cloud WAF console](#).
2. On the top of the page, select the region: **Mainland China, International**.
3. On the **Management > Website Configuration** page, click **Add Domain**.

WAF automatically lists all domain names that have an A record configured in Alibaba Cloud DNS of the current Alibaba Cloud account. If no A record has been created in Alibaba Cloud DNS, the **Please choose your domain** page does not appear. In this case, we recommend that you manually create a website configuration. For more information, see [Website configuration](#).

Domain Name	Server address	Protocol type	HTTPS Certificate
<input type="checkbox"/> example.com	192.168.1.1	<input type="checkbox"/> HTTPS <input checked="" type="checkbox"/> HTTP	--
<input checked="" type="checkbox"/> example.com	192.168.1.1	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> HTTP	• No certificate verify certificate
<input type="checkbox"/> example.com	192.168.1.1	<input type="checkbox"/> HTTPS <input type="checkbox"/> HTTP	--

Total: 25 item(s), Per Page: 10 item(s) « < 1 2 3 > »

4. On the **Please choose your domain** page, check the **Domain Name** for which you want to enable WAF protection and the **Protocol Type**.
5. (Optional) If the protocol type includes **HTTPS**, you must verify certificate first to add the configuration.



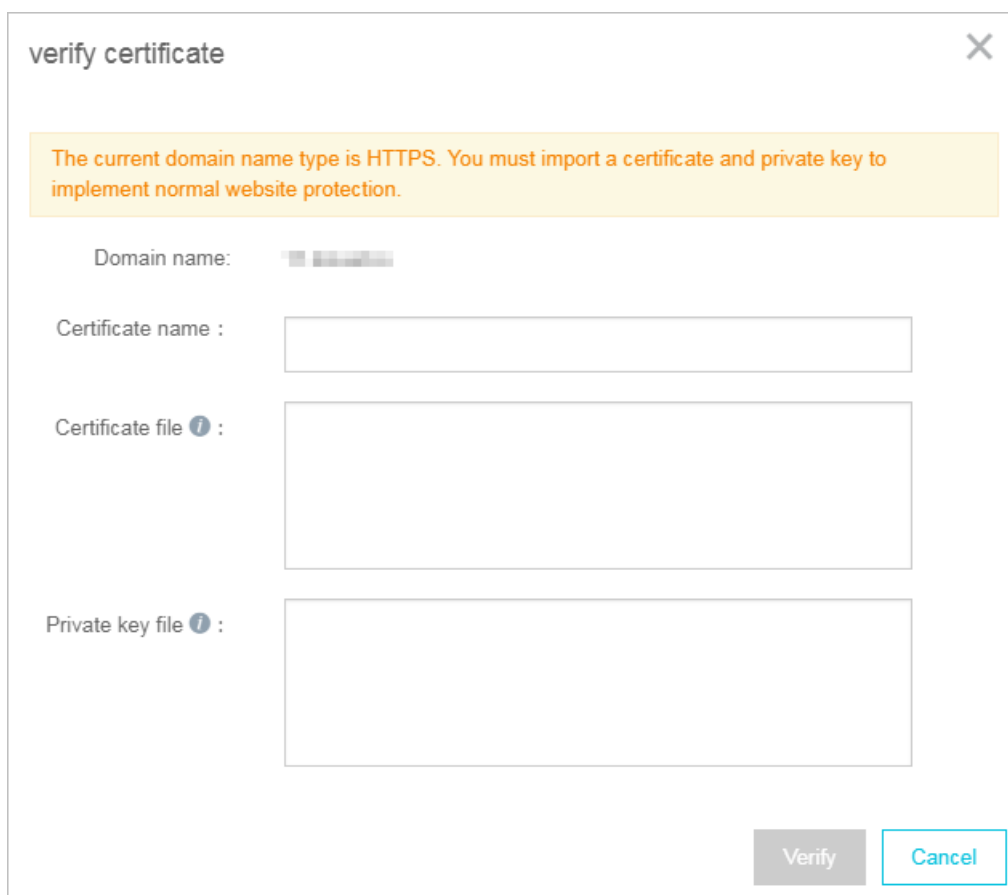
Note:

Alternatively, do not select **HTTPS** here, but edit the website configuration and upload the certificate after you create the configuration. For more information, see [Update HTTPS certificate](#).

- a. Click **Verify Certificate**.
- b. In the **Verify Certificate** dialog box, upload the certificate and private key.

- If the certificate has been hosted in the [Alibaba Cloud SSL Certificate Service console](#), you can click **Select existing certificate** in the **Verify Certificate** dialog box and select it to upload.
- Manual upload. Click **Manual upload**, enter the **Certificate name**, and paste the text content of the certificate and private key respectively to the **Certificate file** and **Private key file** boxes.

For more information, see [Update HTTPS certificate](#).



c. Click **Verify** to upload.

6. Click Add domain protection now.

After adding the website configuration, WAF automatically updates the DNS settings (CNAME record) of the domain name to redirect web requests to WAF for inspection. The whole process takes about 10 to 15 minutes.



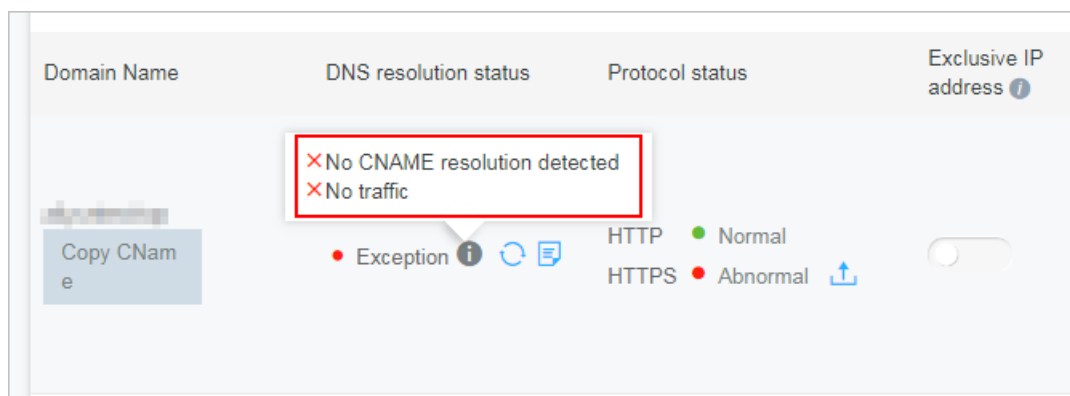
Note:

If you are prompted to manually change the DNS settings, you must perform [Step 2: Update DNS settings](#) to redirect web traffic to WAF.

7. On the **Management > Website Configuration** page, view the newly added domain name and its **DNS Resolution Status**.

- Normal indicates that Alibaba Cloud WAF has been successfully deployed for the website. Go on to perform [Step 3: Configure WAF protection policies](#).
- **Exception** indicates that you must wait for a while or check the DNS settings at your DNS service provider.

If the DNS settings are incorrect, perform [Step 2: Update DNS settings](#). For more information, see [DNS resolution status exception](#).



Manually add a website configuration

Prerequisites

- Obtain the domain name of the website to be protected.
- Obtain the origin server IP address or other type of address that is supposed to receive the WAF-returned traffic.
- Determine whether the website is deployed with CDN, DDoS protection, or other proxy services.
- (For Mainland China region) The website is granted an ICP license by the Ministry of Industry and Information Technology (MIIT).
- (For HTTPS-enabled websites) You have access to a valid SSL certificate and private key of the website, or you have uploaded the certificate to Alibaba Cloud SSL Certificate Service.




Procedure




1. Log on to the [Alibaba Cloud WAF console](#).
2. On the top of the page, select the region: **Mainland China**, **International**.
3. On the **Management > Website Configuration** page, click **Add Domain**.

WAF automatically lists all domain names that have an A record configured in Alibaba Cloud DNS of the current Alibaba Cloud account. If no A record has been created in Alibaba Cloud DNS, the **Please choose your domain page** does not appear.

4. (Optional) On the **Please choose your domain** page, click **Add other domain manually**.

5. In the task of **Fill in the website information**, complete the following configuration.

Configuration	Description
Domain name	<p>Enter the domain name to be protected.</p> <div>  Note: <ul style="list-style-type: none"> Supports wildcard domains, such as *.aliyun.com. When a wildcard domain is presented, all its associated subdomains are matched. If you add website configurations for an exact domain (for example, www.aliyun.com) and a wildcard domain (for example, *.aliyun.com) that matches the exact domain, the configuration for the exact domain takes priority. Does not support .edu domain names. If you want to use Alibaba Cloud WAF to protect domain names suffixed with .edu, submit a ticket to us. </div>
Protocol type	<p>Check the protocols used by the website. Optional values: HTTP, HTTPS.</p> <div>  Note: <ul style="list-style-type: none"> If your website is enabled with HTTPS, check HTTPS and see Update HTTPS certificate to upload a valid certificate and private key to let WAF inspect the HTTPS traffic. When HTTPS is checked, you can configure the Advanced settings to enable HTTPS force redirect or HTTP back-to-source to smooth the website access. For more information, see HTTPS advanced settings. </div>
Server address	<p>Enter the origin server address, which can be one or more IP addresses or other addressees, such as an OSS CNAME address. When the website is deployed with Alibaba Cloud WAF, WAF returns the inspected web requests to this address.</p> <ul style="list-style-type: none"> (Recommended) Check IP and enter the public IP address of the origin server, such as the ECS instance IP or the SLB instance IP. <div>  Note: </div>

Configuration	Description
	<ul style="list-style-type: none"> Multiple IP addresses are separated by commas. Up to 20 IP addresses can be added. If multiple IP addresses are presented, WAF performs health check and load balancing across them when returning the inspected web traffic. For more information, see Load balancing across multiple origin servers. Check Other addresses and enter the server address used to receive the WAF-returned traffic, such as an OSS CNAME address. <div>  Note: <ul style="list-style-type: none"> The server address (Other address) must not be same as the website domain name. If you enter an OSS CNAME address, after you create the website configuration, you must log on to the Alibaba Cloud OSS console to associate the custom domain (in this case, the domain to be protected) for the specified OSS CNAME address. For more information, see Associate a custom domain. </div>
Server port	<p>Specify the server port. When the website is deployed with Alibaba Cloud WAF, WAF returns the inspected web requests to this port.</p> <ul style="list-style-type: none"> When Protocol type includes HTTP, the default HTTP port is 80. When Protocol type includes HTTPS, the default HTTPS port is 443. If you want to specify other ports, click custom to add them. <div>  Note: For more information, see Supported non-standard ports. </div>
Any layer 7 proxy (e.g. Anti-DDoS/CDN) enabled?	<p>Check yes or no according to the actual condition. If any layer 7 proxy is deployed in front of Alibaba Cloud WAF, you must check yes. Otherwise, Alibaba Cloud WAF may not be able to obtain the real client IP address.</p>
Load balancing algorithm	<p>When multiple origin server addresses are specified, select the load balance method (IP HASH or Round-robin) for WAF to distribute traffic among these addresses.</p>
Flow Mark	<p>Enter an unoccupied Header Filed name and a custom Header Field Value to mark the web requests returned to the origin server by Alibaba Cloud WAF. WAF adds the specified header field into the inspected web requests for your web server to identify the WAF-returned traffic.</p> <div>  Note: </div>

Configuration	Description
	If the web request itself uses the specified header field, Alibaba Cloud WAF overwrites the original value with the specified value.

6. Click **Next** to complete the configuration.

When the website configuration is created, you can perform the following tasks:

- Follow the tutorial to perform the next task **Change DNS Record**. For more information, see [WAF deployment guide](#).
- (For HTTPS-enabled websites) Upload the HTTPS certificate and private key. For more information, see [Update HTTPS certificate](#).
- Go to the **Management > Website Configuration** page to view the newly added website configuration, and **Edit** or **Delete** it as you need.

Edit a website configuration

When your web server's configuration changes, such as server IP address changes, protocol type or port changes, or when you want to configure the HTTPS advanced settings, you can edit the website configuration.

Procedure

1. Log on to the [Alibaba Cloud WAF console](#).
2. On the top of the page, select the region: **Mainland China, International**.
3. On the **Management > Website Configuration** page, select the website configuration to be operated, and click **Edit**.
4. On the **Edit** page, complete the configuration by following [Step 5 in Manually add a website configuration](#).



Note:

The **Domain name** cannot be modified. If you want to associate another domain name, we recommend that you add a new website configuration and delete the unnecessary one.

5. Click **OK** to complete the procedure.

Delete a website configuration

If you want to disable Alibaba Cloud WAF for your website, you can restore the DNS to redirect traffic to your web servers, and delete the website configuration on the Alibaba Cloud WAF console.

Procedure

1. Log on to the [Alibaba Cloud WAF console](#).
2. On the top of the page, select the region: **Mainland China, International**.
3. On the **Management > Website Configuration** page, select the website configuration to be deleted, and click **Delete**.

**Note:**

You must restore the DNS settings before deleting the website configuration. Otherwise, the website may become inaccessible.

4. In the **Prompt message** dialog box, click **OK**.

1.2 Mark WAF back-to-origin flow

When you add a website domain configuration in Web Application Firewall for protection, you can set the flow mark for the website domain. When the traffic of the website domain passes through WAF, WAF adds the specified flow mark to the requests. Thus, the origin server can easily collect corresponding information.

According to the HTTP header field name and the field value that you specify in the flow mark, when the traffic passes through WAF, WAF adds the fields and values to the HTTP Header of all requests. By marking the traffic, you can easily identify traffic that are forwarded by WAF, and then configure precise origin server protection policies (Access Control), or analyze protection effects.

**Note:**

If the user-defined HTTP Header field that you specified as flow mark already exists in the request, WAF still overwrites the field value with the specified flow mark field value in the request.

Procedure

1. Log on to the [Alibaba Cloud WAF console](#).
2. On the top of the page, select the region: **Mainland China, International**.
3. Go to the **Management > Website Configuration** page, choose a domain configuration record, and click **Edit**.

**Note:**

You can also specify flow mark when adding a new website domain configuration record.

4. In the Flow Mark configuration item, enter the Header field name and the field value.

**Note:**

Do not specify a user-defined HTTP Header field that has already been used. Otherwise, the value of this field in the request is overwritten by the flow mark field value by WAF.

Flow Mark:	<input type="text" value="Header Field"/>
	<input type="text" value="Header Field Value"/>
<p>Note: If the user-defined header field already has a value, the value is overwritten with the WAF flow mark value. If the header field is already used, the field is overwritten with the flow mark field setting</p>	

5. Click **OK**. After the configuration takes effect, WAF adds the specified HTTP header fields and values when forwarding requests to the website domain.

1.3 WAF deployment guide

Deploying Alibaba Cloud WAF for a website indicates updating the DNS records (CNAME or A type) after the website configuration is created, to redirect web requests to WAF for inspection.

You can use a [CNAME record](#) or [A record](#) to redirect web traffic. We recommend that you use CNAME. Using CNAME supports node switch or even redirecting traffic back to source in case of node failure or machine failure, which improves your business's availability and failure recovery capacity.

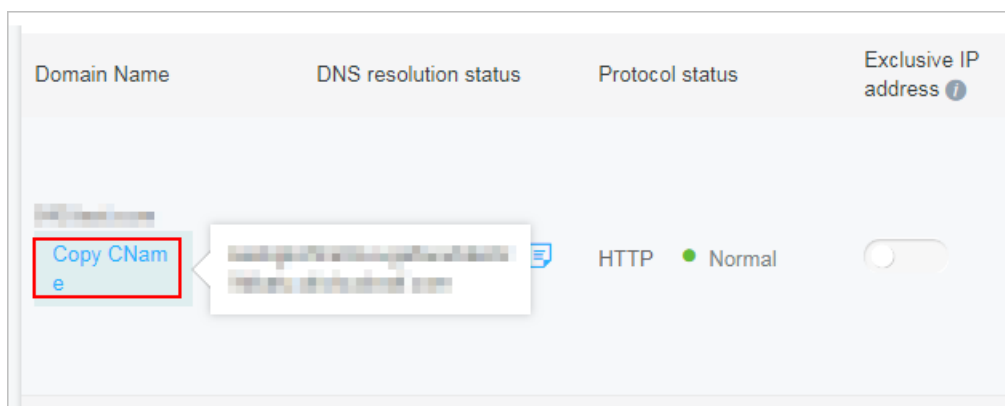
The following content applies to deploying Alibaba Cloud WAF exclusively for the website, that is, the website does not use CDN, DDoS protection, and other proxy services. For other scenarios, see the following documents:

- [Deploy Alibaba Cloud WAF and CDN together](#): explains how to deploy CDN and WAF together for your website.
- [Deploy Alibaba Cloud WAF and DDoS protection together](#): explains how to deploy DDoS protection and WAF together for your website.

(Recommended) Edit CNAME record to deploy WAF

Prerequisites

- Website configuration is successfully created. For more information, see [Website configuration](#).
- Obtain the WAF CNAME address.
 1. Log on to the [Alibaba Cloud WAF console](#).
 2. On the top of the page, select the region: **Mainland China, International**.
 3. On the **Management > Website Configuration** page, move the pointer onto the domain name you want to operate. You will see the **Copy CName** button.



4. Click **Copy CName** to copy the WAF CNAME address to the clipboard.

**Note:**

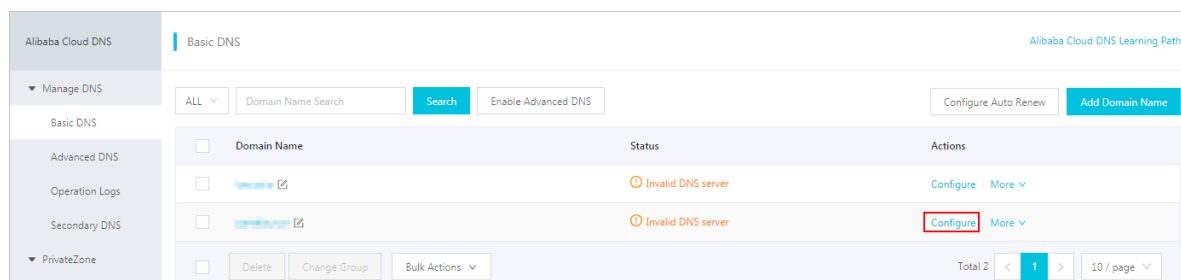
If you want to update A record to redirect web traffic to WAF, you can ping this CNAME address to obtain the corresponding WAF IP address. For more information, see [WAF deployment guide](#). In general, the WAF IP address seldom changes.

- You have permissions to update the domain's DNS settings in its DNS host's system.
- (Optional) Whitelist Alibaba Cloud WAF IP addresses. If your origin web server has enabled non-Alibaba Cloud security software (such as Fortinet FortiGate), you must whitelist WAF IP addresses in the software to prevent legitimate traffic returned by WAF from being blocked. For more information, see [Whitelist Alibaba Cloud WAF IP addresses](#).
- (Optional) Perform redirect check with a local computer. Perform a redirect check to guarantee that all configuration is correct, before you change the DNS settings. This helps avoid business interruption due to incorrect configuration. For more information, see [Perform redirect check with a local computer](#).

Procedure

The following steps explain how to update the **CNAME** record in **Alibaba Cloud DNS**. If your domain is hosted in Alibaba Cloud DNS, follow these steps. Otherwise, you must log on to your DNS host's system to do the modification.

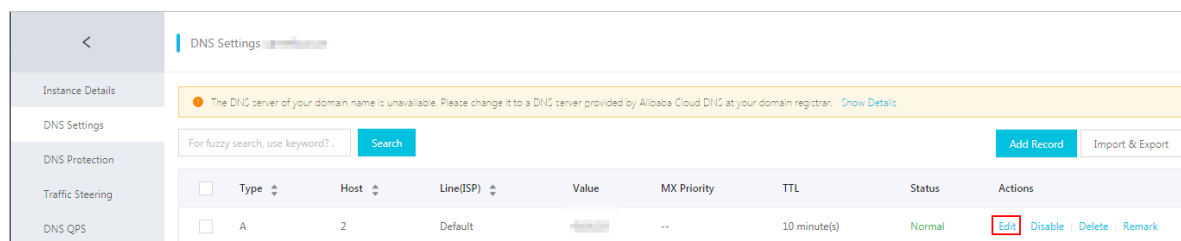
1. Log on to the [Alibaba Cloud DNS console](#).
2. Select the domain to be operated and click **Configure**.



3. Select the **Host** (hostname) to be operated and click **Edit**.

Take `abc.com` as an example. You can select hostname as follows:

- **www**: matches the subdomain starting with `www`, in this case `www.abc.com`.
- **@**: matches the root domain, in this case `abc.com`.
- *****: matches a wildcard domain name that includes both the root domain and all subdomains, in this case `blog.abc.com`, `www.abc.com`, `abc.com`, and so on.



4. In the **Edit Record** dialog box, do the following:

- **Type**: Select **CNAME**.
- **Value**: Enter the WAF CNAME address.
- Leave other settings as they are. We recommend that you set TTL value to 10 minutes. The larger the TTL value, the slower the DNS propagation.

Notes about editing DNS records:

- For a hostname, the CNAME record is unique. You must edit it to the WAF CNAME address.
- Different record type conflicts with each other. For example, for a hostname, the CNAME record cannot coexist with an A record, MX record, or TXT record. If you cannot change the record type directly, you can first delete the conflicting records and add a new CNAME record.

**Note:**

The whole process of deleting and adding must be performed in a short time. Otherwise, your domain becomes inaccessible.

- If the MX record is being used, you can use an A record to redirect web traffic to WAF. For more information, see [WAF deployment guide](#).

Edit Record

Type: CNAME- Canonical name

Host: www

ISP Line: Default - Return to the default value when the query is not ...

* Value: aliyundunwaf.com

* TTL: 10 minute(s)

Cancel OK

5. Click **OK** to complete the DNS settings and wait for the DNS change to take effect.
6. (Optional) Verify the DNS settings. You can ping the domain or use [DNS Check](#) to validate whether the DNS change is effective.

**Note:**

It takes a certain time for the setting to be in effect. If the validation fails, wait for about 10 minutes and re-validate it again.

7. Check the DNS resolution status.
 - a. Log on to the [Alibaba Cloud WAF console](#).
 - b. On the **Management > Website Configuration** page, check the **DNS resolution status** of the domain name.
 - **Normal:** Alibaba Cloud WAF has been successfully deployed and the web traffic is being monitored by WAF.

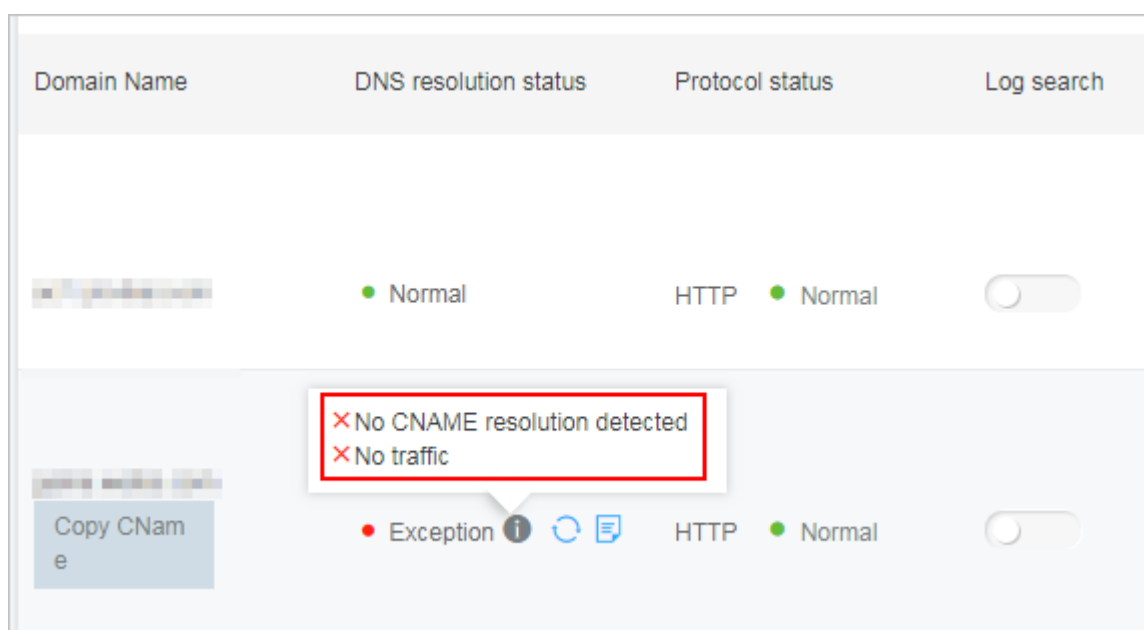
- **Exception:** With the exception messages of **NO CNAME resolution detected**, **No traffic**, or **DNS check failed**, the DNS settings might be incorrect.

In this case, check the DNS settings. If you confirm that the DNS settings are correct, wait for an hour and refresh the DNS resolution status. For more information, see [DNS resolution status exception](#).



Note:

The exception here indicates that WAF is not properly deployed. Your website access is not affected.



Protect the origin

When the origin server IP address is exposed, attackers may exploit it to bypass Alibaba Cloud WAF and start direct-to-origin attacks. To prevent such attacks, we recommend that you configure the ECS security group or SLB whitelist to block all web requests that do not come from Alibaba Cloud WAF's IP addresses. For more information, see [Protect your origin server](#).

Edit A record to deploy WAF

The A record method is same as the CNAME one, except the following differences.

- **Prerequisites:** After obtaining the WAF CNAME address, do the following to obtain the associated WAF IP address.
 1. In a Windows operating system, open the cmd command line tool.
 2. Run the following command: `ping "copied WAF Cname address"`.

3. In the result, view the WAF IP address.

- **Procedure:** In step 4 editing record, do the following:

- **Type:** Select **A**.
- **Value:** Enter the WAF IP address.
- Leave other settings as they are.

1.4 Whitelist Alibaba Cloud WAF IP addresses

When a website is deployed with Alibaba Cloud WAF, all web traffic is redirected to WAF for inspection, and WAF returns the inspected traffic to origin server.

From the origin server's perspective, all web requests arrive from a limited quantity of WAF IP addresses, which is suspicious. If the origin server has been installed with a security software such as FortiGate, the security software may trigger a blocking action against WAF IP address and web traffic returned by WAF. Therefore, you must whitelist all WAF IP addresses in the security software in origin server to avoid normal business interruption.



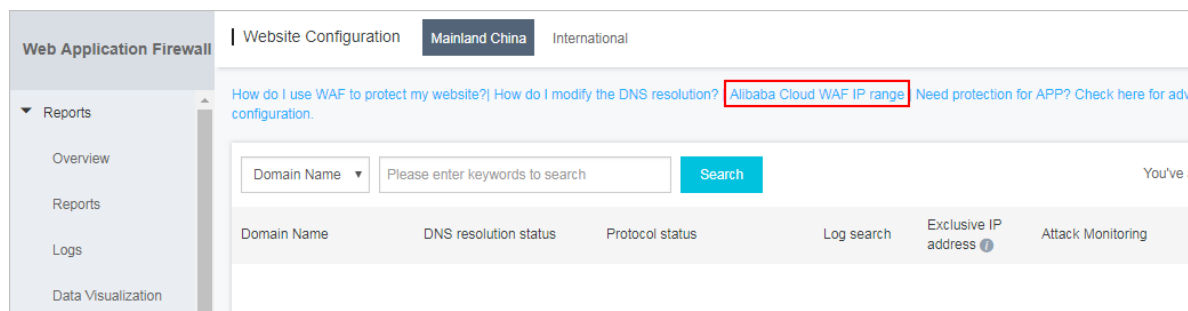
Note:

We recommend that you uninstall other security software in origin server after Alibaba Cloud WAF is deployed.

Procedure

You can view the IP addresses of Alibaba Cloud WAF in the Alibaba Cloud WAF console. The procedure is as follows.

1. Log on to the [Alibaba Cloud WAF console](#).
2. On the top of the page, select the region: **Mainland China**, **International**.
3. Go to the **Management > Website Configuration** page.
4. Click **Alibaba Cloud WAF IP range** to view and copy all WAF IP addresses.



From origin server's perspective, web requests from the Alibaba Cloud WAF IP addresses are more concentrated and in a very high frequency. The security software in origin server may determine that Alibaba Cloud WAF IP addresses are starting attacks, and trigger a blocking action against them. If Alibaba Cloud WAF IP addresses are blocked, the real client cannot get a response. Therefore, you must whitelist Alibaba Cloud WAF IP addresses once your website is deployed with WAF. Otherwise, normal web access may be affected, which leads to web pages cannot be opened or respond slowly.

We recommend that after deploying Alibaba Cloud WAF, you only allow web requests originate from WAF and block other requests to guarantee normal web business access and avoid direct-to-origin attacks. If the origin server IP address is disclosed, an attacker can bypass WAF to directly attack your origin server. For more information, see [Protect your origin server](#).

1.5 Perform redirect check with a local computer

When you have created a website configuration in Alibaba Cloud WAF for your website and are going to update the DNS settings to redirect web traffic to WAF for inspection, we recommend that you perform a redirect check with a local computer to make sure that WAF can handle the traffic. Redirect check requires you to modify the local hosts file to make your local machine look directly at your Alibaba Cloud WAF instance. Therefore, you can test whether the WAF instance works properly.

Modify the local hosts file

Modify the local `hosts` file ([What is the hosts file?](#)) to forward local requests to WAF. For Windows systems, the procedure is as follows:

1. Open the `hosts` file with Notepad. The `hosts` file locates in the `C:\Windows\System32\drivers\etc\hosts` directory.
2. In the last line, add the following content: `WAF_IP_address Domain_name_protected`.

Suppose that you have created a website configuration for `www.aliyundemo.cn`, and Alibaba Cloud WAF assigns the following CNAME address to it: `xxxxxxxxxwmqvixt8vedyneaepztpuqu.alicloudwaf.com`.

- a. Open the cmd command-line tool in Windows, and run the following command to obtain the WAF IP address: `ping xxxxxxxxxxxwmqvixt8vedyneaepztpuqu.alicloudwaf.com`. You can view the WAF IP address in the response.

```
C:\Users\ali-22031774>ping 111.77.42.195
Pinging 111.77.42.195 with 32 bytes of data:
Reply from 111.77.42.195: bytes=32 time=2ms TTL=106
Reply from 111.77.42.195: bytes=32 time=4ms TTL=106
Reply from 111.77.42.195: bytes=32 time=4ms TTL=106
Reply from 111.77.42.195: bytes=32 time=4ms TTL=106
```

- b. Add the following line to *hosts*. The IP address is the WAF IP address obtained in the previous step, and the domain name is the protected domain name.

```
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
0.0.0.0 cert.bandicam.com
#       ::1            localhost
111.77.42.195 www.aliyundemo.cn
```

3. Save changes to *hosts*. Ping the protected domain name in cmd.

```
C:\Users\ali-22031774>ping www.aliyundemo.cn
Pinging www.aliyundemo.cn [111.77.42.195] with 32 bytes of data:
Reply from 111.77.42.195: bytes=32 time=2ms TTL=106
Reply from 111.77.42.195: bytes=32 time=4ms TTL=106
Reply from 111.77.42.195: bytes=32 time=4ms TTL=106
Reply from 111.77.42.195: bytes=32 time=4ms TTL=106
```

If WAF works properly, the IP address you see will be the WAF IP address configured in the previous step. If the origin IP address is displayed, try refreshing the local DNS cache. In Windows, you can run `ipconfig/flushdns` in cmd.

Verify WAF forwarding

Once the changes in the hosts file are effective, you can access the protected domain name from your local computer. If WAF is configured correctly, the website is expected to be normally accessed.

In addition, you can verify the protection effect by constructing some simple attack commands. For example, you can add `/? alert(xss)` to the URL to construct a Web attack request for testing. As you try to access `www.aliyundemo.cn/? alert(xss)`,

1.6 Update HTTPS certificates

To let Alibaba Cloud WAF inspect HTTPS traffic for your web business, you must include HTTPS in the protocol type in [website configuration](#), and upload a valid HTTPS certificate to WAF. If the certificate changes, you must update the certificate in the Alibaba Cloud WAF console in a timely manner.

Context

If you have uploaded the certificate file to [Alibaba Cloud SSL Certificate Service](#) for integrated management, then in the following steps, you can reuse it directly instead of uploading it again.

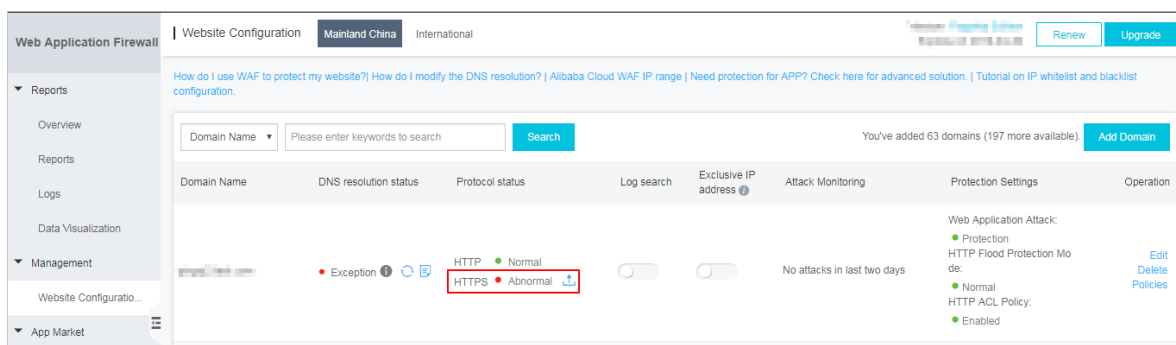
Otherwise, you must have the certificate and private key files prepared, to complete the following operations.

In general, the following files are required:

- *.crt (Public key) or *.pem (Certificate)
- *.key (Private key)

Procedure

1. Log on to the [Alibaba Cloud WAF console](#).
2. On the top of the page, select the region: **Mainland China, International**.
3. On the **Management > Website Configuration** page, locate the domain name to be operated, and click the Update Certificate button (↕) next to the **HTTPS Protocol Status**.



4. In the **Update Certificate** dialog box, select an **Upload method**.
 - If the HTTPS certificate to be uploaded is hosted in [Alibaba Cloud SSL Certificate Service](#), you can check **Select existing certificate** and select it for upload.

Update certificate

The current domain name type is HTTPS. You must import a certificate and private key to implement normal website protection.

Upload method :

☐ Manual upload
☒ Select existing certificate

Certificate :

Select an existing certificate or ma...

You can upload and manage your certificates in [SSL Certificates Service](#).

Save

Cancel

- Manual upload. Click **Manual upload**, enter a **Certificate name**, and paste the text context of the certificate file and private key file respectively to the **Certificate file** and **Private key file** boxes.



Note:

- For certificates in general formats, such as PEM, CER, and CRT, you can open the certificate file directly by using a text editor tool to copy the text content. For certificates in other formats, such as PFX and P7B, convert the certificate file to the PEM format, and then copy the text content from the converted certificate file.
- If the HTTPS certificate has multiple certificate files, such as a certificate chain file, merge the text contents from the multiple certificate files and paste them into the **Certificate file** box.

Example of the text content of a certificate file:

```
-----BEGIN CERTIFICATE-----
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx8ixZJ4krc+1M+
j2kcubVpse2
cgHdj4v8H6jUz9Ji4mr7vMNS6dXv8PUkl/qoDeNGCNdyTS5NIL5ir+g92cL8IGOk
jgvhlqt9vc
65Cgb4mL+n5+DV9uOyTZTW/MojmlgfUekC2xiXa54nxJf17Y1TADGSbyJbsC0Q9
nIrHsPl8YKk
vRWvIAqYxXZ7wRwWWmv4TMxFhWRiNY7yZIo2ZUhl02SIDNggIEeg==
-----END CERTIFICATE-----
```

Example of the text content of a private key file:

```
-----BEGIN RSA PRIVATE KEY-----
DADTPZoOhd9WtZ3UKHJTRgNQmioPQn2bqdKHop+B/dn/4VZL7Jt8zSDGM9sTMThL
yvsmLQKBgQ
```

```
Cr+ujntC1kN6pGBj2Fw2l/EA/W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQra6ZdwBcQJ
aiygoIYo
aMF2EjRwc0qwHaluq0C15f6ujSoHh2e+D5zdmkTg/3NKNjqNv6xA2gYpinVDz
FdZ9Zujxvuh9o
4Vqf0YF8bv5UK5G04RtKadOw==
-----END RSA PRIVATE KEY-----
```

Update certificate

The current domain name type is HTTPS. You must import a certificate and private key to implement normal website protection.

Upload method :

☒ Manual upload
 ☐ Select existing certificate

Domain name:

Certificate name :

Certificate file

Private key file

Save

Cancel

5. Click **Save** to complete the procedure.

Result

The HTTPS protocol status displays as **Normal**.

Web Application Firewall

Website Configuration

Mainland China

International

How do I use WAF to protect my website? | How do I modify the DNS resolution? | Alibaba Cloud WAF IP range | Need protection for APP? Check here for advanced solution. | Tutorial on IP whitelist and blacklist configuration.

Domain Name

Please enter keywords to search

Search

You've added 63 domains (197 more available).

Add Domain

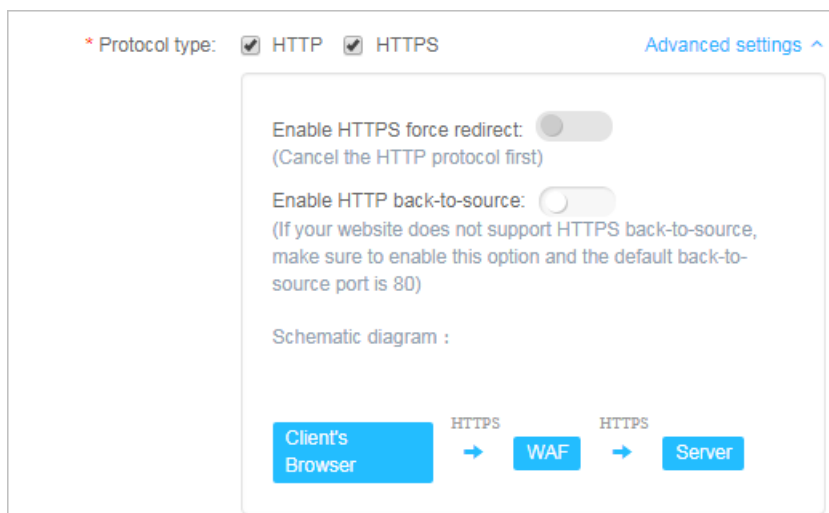
Domain Name	DNS resolution status	Protocol status	Log search	Exclusive IP address	Attack Monitoring	Protection Settings	Operation
	Exception	<div>HTTP Normal</div> <div>HTTPS Normal</div>			No attacks in last two days	Web Application Attack: <ul style="list-style-type: none"> Protection HTTP Flood Protection Mode: <ul style="list-style-type: none"> Normal HTTP ACL Policy: <ul style="list-style-type: none"> Enabled 	<a>Edit <a>Delete <a>Policies

1.7 HTTPS advanced settings

Alibaba Cloud WAF provides convenient HTTPS options to help you implement HTTP back-to-source and HTTPS force redirect without re-constructing the origin.

Procedure

1. Log on to the [Alibaba Cloud WAF console](#).
2. On the top of the page, select the region: **Mainland China**, **International**.
3. On the **Management > Website Configuration** page, locate the domain name to be operated, and click **Edit**.
4. Check **HTTPS** under **Protocol type**, and expand the **Advanced settings** menu.



- **Enable HTTP back-to-source**

You can enable an HTTP communication between Alibaba Cloud WAF and origin server by enabling **HTTP back-to-source**. By doing this, WAF returns the inspected traffic to the default port of 80 of your origin server.



Note:

Using HTTP back-to-source does not require any modification on origin server or any HTTPS configuration. However, you must make sure that you **upload the correct certificate and private key to Alibaba Cloud WAF**. You can apply for a certificate for free in Alibaba Cloud SSL Certificate Service.

* Protocol type: ☒ HTTP ☒ HTTPS [Advanced settings ^](#)

Enable HTTPS force redirect: ☐
(Cancel the HTTP protocol first)

Enable HTTP back-to-source: ☒
(If your website does not support HTTPS back-to-source, make sure to enable this option and the default back-to-source port is 80)

Schematic diagram :

```
graph LR
    Client[Client's Browser] -- HTTPS --> WAF[WAF]
    WAF -- HTTP --> Server[Server]
```

- **Enable HTTPS force redirect**

If you want to force clients to use HTTPS to access your sites, you can enable **HTTPS force redirect**.

**Note:**

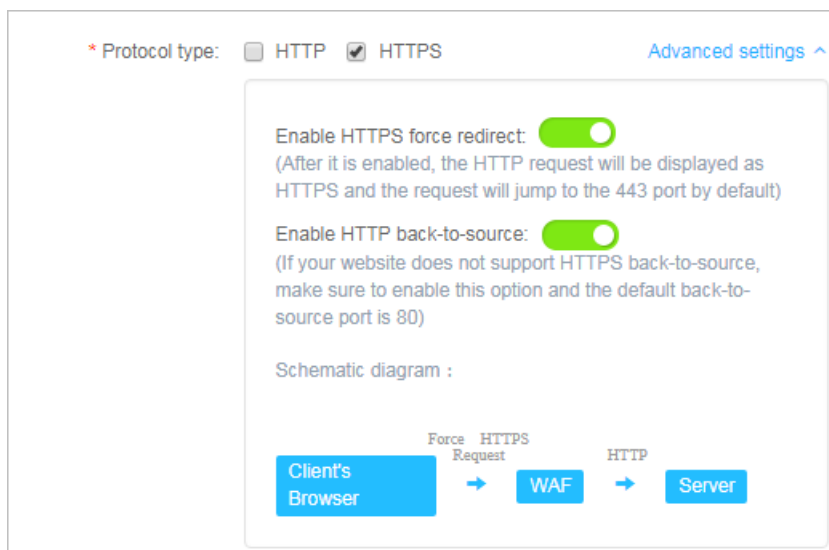
You must cancel the HTTP protocol to enable HTTPS force redirect.

When HTTPS force redirect is enabled, some Web browsers that support HSTS (HTTP Strict Transport Security) will be forced to use HTTPS for a period of time. Therefore, you must make sure that the origin server supports HTTPS.

Confirm

Explorers that support HSTS will be forced to use HTTPS for a period of time, please make sure the origin supports HTTPS.

When HTTPS force redirect is enabled, all HTTP requests will be displayed as HTTPS and forwarded to port 443.



1.8 Supported non-standard ports

Alibaba Cloud WAF returns web traffic to the following ports of origin server by default: port 80 and 8080 for HTTP connection and port 443 and 8443 for HTTPS connection. You can specify other ports with the Business or Enterprise subscription plan. This topic explains the maximum number of ports you can specify and the custom ports you can use.

Maximum number of ports

For each Alibaba Cloud WAF subscription, the maximum number of different ports you can specify in all website configurations is as follows:

- Business plan: You can specify **a maximum of 10 different ports**, including port 80, 8080, 443, and 8443.
- Enterprise plan: You can specify **a maximum of 50 different ports**, including port 80, 8080, 443, and 8443.

Supported ports



Note:

Alibaba Cloud WAF only inspects web traffic that requests the supported ports. When a client requests an unsupported port (for example, 4444), the request will be discarded.

- For the Business or Enterprise subscription plan of Alibaba Cloud WAF, the following **HTTP** ports are supported:
80, 81, 82, 83, 84, 88, 89, 800, 808, 1000, 1090, 3333, 3501, 3601, 5000, 5222, 6001, 6666, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016,

7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7070, 7081, 7082, 7083, 7088, 7097, 7777, 7800, 8000, 8001, 8002, 8003, 8008, 8009, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8081, 8082, 8083, 8084, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8106, 8181, 8334, 8336, 8800, 8686, 8888, 8889, 8999, 9000, 9001, 9002, 9003, 9080, 9200, 9999, 10000, 10001, 10080, 12601, 86, 9021, 9023, 9027, 9037, 9081, 9082, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 48800, 87, 97, 7510, 9180, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 28080, 33702

- For the Business or Enterprise subscription plan of Alibaba Cloud WAF, the following **HTTPS** ports are supported:

443, 4443, 5443, 6443, 7443, 8443, 9443, 8553, 8663, 9553, 9663, 18980

1.9 Load balance across multiple origin IPs

You can specify a maximum of 20 origin IP addresses in a website configuration.

When multiple origin IP addresses are specified, WAF performs load balance across them when returning the inspected web traffic. WAF also performs health check on all origin IPs. When one IP is inaccessible, WAF stops assigning requests to that IP until it can be accessed again.

Suppose you have three origin IPs: 1.1.1.1, 2.2.2.2, and 3.3.3.3. You can configure your website as follows.



Note:

If you have other layer-7 proxies enabled together with WAF, such as DDoS protection or CDN, make sure that you select **yes** for **Any layer 7 proxy (e.g. Anti-DDoS/CDN) enabled?** in website configuration

* Domain name:

It supports top-level domain names (e.g. test.com) and second-level domain names (e.g. www.test.com). They have no impact on each other. Please fill in your actual domain name.

* Protocol type: ☒ HTTP ☐ HTTPS

* Server address: ☒ IP ☐ Other addresses

Please separate up to 20 IPs with commas (","), Line breaks are not allowed.

* Server port: HTTP 80 [Custom](#)

Any layer 7 proxy (e.g. Anti-DDoS/CDN) enabled?: ☐ yes ☒ no [i](#)

Load balancing algorithm: ☒ IP HASH ☐ Round-robin

Flow Mark:

Note: If the user-defined header field already has a value, the value is overwritten with the WAF flow mark value. If the header field is already used, the field is overwritten with the flow mark filed setting

When multiple origin IPs are specified, select a load balancing algorithm, such as IP HASH or Round-robin.

**Note:**

If you use IP hash, make sure that the origin IP addresses are discrete. Otherwise, load balancing may not work properly.

1.10 Deploy WAF and Anti-DDoS Pro together

Alibaba Cloud WAF and Anti-DDoS Pro are fully compatible. You can use the following architecture to deploy WAF and Anti-DDoS Pro together: Anti-DDoS Pro (entry layer, DDoS attack protection) > WAF (intermediate layer, web attack protection) > Origin.

Procedure

1. Create a website configuration for your website in Alibaba Cloud WAF.
 - **Server address:** Check **IP** and enter the public IP address of the ECS instance/Server Load Balancer instance or external server IP address.
 - **Any layer 7 proxy (e.g. Anti-DDoS/CDN) enabled?:** Check **yes**.

For more information, see [Website configuration](#).

2. Create a web service access configuration for your website in Anti-DDoS Pro. The procedure is as follows:

1. On the **Access > Web Service** page, click **Add Domain**.
2. In the **Fill in the domain name information** task, do the following:
 - **Domain name:** Enter the domain name to be protected.
 - **Protocol:** Check the supported protocol.
 - **Origin IP/Domain:** Check **Origin site domain** and enter the WAF CNAME address.



Note:

For more information about how to view the WAF CNAME address, see [WAF deployment guide](#).

The screenshot shows a multi-step configuration wizard. The first step, 'Fill in the domain name information', is highlighted in blue. The subsequent steps are 'Please choose Instance and ISP', 'Modify DNS resolution', and 'Change Origin IP'. Under the 'Line' section, there is a 'Domain Name' field with a placeholder 'Please enter the domain name to protect'. Below this is a red note: 'Note: If a wildcard domain is added, please also add its top-level domain in another type. For example, after you add the *.taobao.com wildcard domain, you must add its top-level domain, taobao.com, in another rule. The top-level domain and sub-level domain must be configured separately.' There are four protocol checkboxes: HTTP, HTTPS, websocket, and websockets. Under 'Origin IP/Domain', there are two radio buttons: 'Origin site IP' and 'Origin site domain', with the latter selected and highlighted by a red box. Below this is a text field with the placeholder 'Please key in origin site domain'. A link 'What to do after source IP exposed?' is present. At the bottom is a 'Next' button.

3. Click **Next**.

4. Complete the **Please choose Instance and ISP Line** task.

3. Update the DNS settings of your domain name. Log on to the DNS host's system and add a CNAME record to redirect web traffic to the Anti-DDoS Pro CNAME address.

For more information, see [Access Anti-DDoS Pro through a CNAME record](#).

Result

All web requests to your website are redirected to Anti-DDoS Pro for cleanup and then redirected to WAF for inspection before they reach your origin server.

1.11 Deploy WAF and CDN together

You can deploy Alibaba Cloud WAF and CDN (Content Delivery Network) together to speed up your website and protect against web attacks at the same time. We recommend that you use the following architecture: CDN (entry layer, website speed up) > WAF (intermediate layer, web attacks protection) > Origin.



Note:

Most CDN providers do not defend against HTTP Flood attacks, which result to accesses to HTTP Flood-attacked domain names are intercepted at the CDN layer. We recommend that you do not deploy WAF and CDN together for domain names that are frequently targeted by HTTP Flood attacks.

Procedure

Suppose you use Alibaba Cloud CDN. Follow these steps to deploy WAF and CDN together:

1. See [Get started with Alibaba Cloud CDN](#) to implement a CDN for your domain name.
2. Create a website configuration in Alibaba Cloud WAF.
 - **Domain name:** Enter the CDN-enabled domain name. Wildcard is supported.
 - **Server address:** Enter the public IP address of the ECS/Server Load Balancer instance, or the external server IP address of the origin server.
 - **Any layer 7 proxy (e.g. Anti-DDoS/CDN) enabled?:** Check **yes**.

For more information, see [Website configuration](#).

* Domain name:

It supports top-level domain names (e.g. test.com) and second-level domain names (e.g. www.test.com). They have no impact on each other. Please fill in your actual domain name.

* Protocol type: ☒ HTTP ☐ HTTPS

* Server address: ☒ IP ☐ Other addresses

Please separate up to 20 IPs with commas (","), Line breaks are not allowed.

* Server port: HTTP 80 [Custom](#)

Any layer 7 proxy (e.g. Anti-DDoS/CDN) enabled?: ☒ yes ☐ no [?](#)

Load balancing algorithm: ☒ IP HASH ☐ Round-robin

Flow Mark:

Note: If the user-defined header field already has a value, the value is overwritten with the WAF flow mark value. If the header field is already used, the field is overwritten with the flow mark field setting

3. When the website configuration is successfully created, WAF generates a dedicated CNAME address for it.



Note:

For more information about how to view the WAF CNAME address, see [WAF deployment guide](#).

4. Modify the CDN configuration to change the origin site address to the WAF CNAME address.
 - a. Log on to the [Alibaba Cloud CDN console](#).
 - b. Go to the **Domain Names** page, select the domain to be configured, and click **Configure**.
 - c. Under **Origin site settings**, click **Modify**.
 - d. Modify origin site information.
 - **Type**: Select **Origin Site**.
 - **Origin site address IP**: Enter the WAF CNAME address.
 - **Use the same protocol as the back-to-source protocol**: Select **Enable**.

Back-to-Source Settings

Origin Site Information [How to set priorities for multiple origins?](#)

Type ☐ OSS domain name ☐ IP ☒ Origin Site

Origin Site Address Domain

Name	Priority
<input type="text" value="www.example.com"/>	Main

Add

Port ☒ Port 80 ☐ Port 443

Back-to-source method


Use the same protocol ☒ Enable ☐ Close

as the back-to-source protocol Please make sure your origin site supports http or https protocol

Back-to-source method ☒ Follow ☐ Http ☐ Https

Contact Us

- e. Under **Back-to-Source Settings**, make sure that **Back-to-Source host** is disabled.

Back-to-Source Settings			
Configuration Item	Description	Current Configuration	
Origin site settings	This specifies the resource's back-to-source address and port. Domain name and IP addresses are supported for origin sites. We recommend that you use an OSS origin site		Modify
Use the same protocol as the back-to-source protocol	The back-to-source protocol must be the same as the protocol the client uses to access resources. Note: The origin site must support port 443	Not enabled	
Acceleration regions	Different charges apply for overseas and domestic acceleration. You cannot change between them currently.	Mainland China	
Private Bucket Back-to-Source	Supports the acceleration of private OSS origin site content	Not enabled	Modify
Back-to-Source host	Customize the web server domain name a CDN node needs to access during the back-to-source process.	Not enabled	Modify

After the operation is complete, the traffic goes through CDN, and the dynamic content continues to be checked and protected by WAF.

2 Protection configuration

3 Protection reports

4 SDK solution

4.1 Access the WAF SDK

WAF SDK is a programming package designed specifically for native Apps. It offers security protection such as trusted communications, anti-fake-orders detection, and so on. WAF SDK can effectively identify high-risk mobile phones, ModemPOOLs, and other characteristics.

Scenarios

After accessing the SDK, your App can get the same trusted communication technologies as the clients such as Tmall, Taobao, and Alipay. WAF SDK also shares Alibaba Group's fingerprint database of malicious devices against black/grey industries and econnoisseurs, and fundamentally resolves the security issues at the App end.

WAF SDK can resolve the following **native App** side issues:

- Malicious registration, account credential enumeration attacks, and brute-force attacks
- Large volume traffic HTTP flood attacks against Apps
- Malicious attacks against SMS/CAPTCHA interfaces
- Bonus hunting and red envelopes snatching
- Seckill and time-and-purchase-limited goods
- Malicious check and brush votes (such as air tickets or hotel booking information)
- Value consulting crawls (such as price, credit information, financing, and fiction)
- Machine voting
- Spams and malicious comments

How to access WAF SDK

Follow these steps to access WAF SDK:

1. Log on to the [Web Application Firewall console](#).
2. Go to the **Management > Website Configuration** page, and add the App domain to the protection list to enable WAF protection for it. For more information, see [Set up WAF console](#).
3. At your DNS service provider, add a CNAME record by using the WAF-generated Cname address as the record value. For more information, see [Update DNS settings](#).
4. Integrate the SDK components provided by WAF on your App. This operation usually takes 1-2 days.

**Note:**

The SDK integration does not require any modification on the server side. WAF can filter out malicious traffic and only send the valid request back to the origin. The pressure of malicious requests is also handled by WAF.

For more information about how to integrate the SDK components on your App, see the following documents:

- [iOS integration manual](#)
- [Android integration manual](#)

5. Contact WAF support to help test your integrated App.
6. Release a new version of your App to enable the SDK protection.

4.2 iOS integration manual

This document describes the procedure to connect to WAF SDK by using an iOS App.

Download the SDK package

Download and unzip the WAF SDK package. The following files are included in the *sdk-ios* folder:

The description of these files is as follows:

Name	Description
<i>SGMain.framework</i>	Main framework SDK
<i>SecurityGuardSDK.framework</i>	Basic security plugin
<i>SGSecurityBody.framework</i>	Man/machine identification plugin
<i>SGAVMP.framework</i>	Virtual machine plugin
<i>yw_1222_0335_mwua.jpg</i>	Configuration file

Procedure

Follow these steps to configure a project:

1. Add Framework. Add the four *.framework* files provided by WAF SDK to the project's dependent libraries.

2. Add link options.
3. Add system dependent libraries.
4. Import configuration file. Add the `yw_1222_0335_mwua.jpg` configuration file of the SDK to `mainbundle`.

When the application integrates multiple targets, make sure to add the `yw_1222_0335_mwua.jpg` configuration file to the correct Target Membership.

Coding process

1. Initialize SDK

Interface definition

```
+ (BOOL) initialize;
```

Interface description

- Function: Initializes SDK.
- Parameter: N/A.
- Return value: BOOL type. YES if the initialization is successful, and NO if the initialization fails.

Call method

```
[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;
    }
}
```

2. Sign the request data

Interface definition

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

Interface description

Use the avmp technology to sign the input data, and return the signature string.



Note:

The signed request body must be identical to the request body sent out from the client. For example, the encoding format, spaces, special characters, and order of parameters in the request bodies must be the same. Otherwise, the verification may fail.

Parameters:

Name	Type	Required	Description
signType	NSInteger	Yes	Algorithm used by the signature. Currently, it is a fixed value. Enter 3.
input	NSData*	No	Data to be signed, which is generally the entire request body. If the request body is empty, then enter null for this parameter.

Return value: NSData* type. The signature string is returned.

Call method

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

Sample code

When the client sends data to the server, it must call the avmpSign interface to sign the entire body data and obtain the signature string (the wToken).

```
# 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 = nil;
    NSData* data = [request_body dataUsingEncoding:NSUTF8String
encoding];
    NSData* sign = [JAQAVMPSignature avmpSign: VMP_SIGN_W
ITH_GENERAL_WUA2 input:data];
    if(sign == nil || sign.length <= 0){
        return nil;
    }else{
        wToken = [[NSString alloc] initWithData:sign encoding:
NSUTF8StringEncoding];
        return wToken;
    }
}
}
}

```

**Note:**

Even if the request body is empty, the client still must call the avmpSign interface to generate the wToken. In this case, directly import null as the second parameter. The sample code is as follows:

```

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

```

3. Put the wToken in the protocol header

The sample code is as follows:

```

#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:NSUTF8String
encoding];

    NSString* wToken = nil;
    NSData* sign = [JAQAVMPSignature avmpSign: VMP_SIGN_WITH_GENERAL_WUA2
input:body_data];
    wToken = [[NSString alloc] initWithData:sign encoding: NSUTF8String
encoding];
    NSString *strUrl = [NSString stringWithFormat:@"http://www.xxx.com
/login"];
    NSURL *url = [NSURL URLWithString:strUrl];
    NSMutableURLRequest *request =
        [[NSMutableURLRequest alloc] initWithURL:url cachePolicy:
NSURLRequestReloadIgnoringCacheData 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 startImmediately:true];
[mConn start];
// ...
}
```

4. Send data to the server

Send the data with the modified protocol header to WAF. Upon receiving the request, WAF parses the wToken for risk identification, and then blocks malicious requests and forwards only the valid requests to the origin.

Error codes

The preceding `initialize` and `avmpsign` interfaces may encounter exceptions. If you encounter an exception or error when generating the signature string, you can search “SG Error” in the console.

Common errors and descriptions are listed in the following table:

Error Code	Meaning
1901	Incorrect parameter. Enter the correct parameter.
1902	Image file error. It generally indicates that the apk signature used to retrieve the image file is inconsistent with the current application's apk signature. Use the current application's apk to generate the image file. In iOS, it may be caused by inconsistent BundleIDs.
1903	Incorrect image format.
1904	Upgrade to the latest images. AVMP signature function only supports v5 images.
1905	Unable to find the image file. Make sure that the <code>yw_1222_0335_mwua.jpg</code> image file is added into the project.
1906	byteCode corresponding to the AVMP signature is missing in the image. Check if the image is correct.
1907	Failed to initialize AVMP. Try again later.
1910	Invalid avmpInstance instance. Probable causes are: <ul style="list-style-type: none"> • <code>InvokeAVMP</code> is called after AVMPInstance is destroyed. • The image's byteCode version does not match with that of the SDK.
1911	The encrypted image's byteCode does not have the corresponding export function.

1912	AVMP call failed. Submit a ticket for further assistance.
1913	InvokeAVMP is called after AVMPInstance is destroyed.
1915	Insufficient AVMP memory. Try again later.
1996	Unknown error. Try again

4.3 Android integration manual

This document describes the process of connecting to the WAF SDK using the Android app.

Download the SDK package

Download and unzip the WAF SDK package. In the *sdk-Android* folder, you can see the following files:



Note:

The *aar* file version numbers may be different.

The description of these files is as follows (xxx is the version number):

File	Description
<i>SecurityGuardSDK-xxx.aar</i>	Main framework SDK
<i>AVMP SDK-xxx.aar</i>	Virtual machine plugin
<i>SecurityBodySDK-xxx.aar</i>	Man/machine identification plugin
<i>yw_1222_0335.jpg</i>	Mainframe configuration file
<i>yw_1222_0335_mwua.jpg</i>	Virtual machine engine configuration file

Procedure

Follow these steps to configure the project:

1. Import the *aar* files of the SDK to Android Studio. Copy all *aar* files from the SDK to the project's *libs* directory. If the *libs* directory does not exist, create one.
2. Open this Module's *build.gradle* file, and add the following configuration to it (as shown in ③ and ④).
 - Use the *libs* directory as the source for searching dependencies.

```
repositories{
```

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

- Add compilation dependencies.

**Note:**

The *aar* file version numbers here may be different with those of the files downloaded by you.

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

3. Import the *jpg* file into the *drawable* folder. Move the *yw_1222_0335_mwua.jpg* and *yw_1222_0335.jpg* files from the SDK directory to the Android application project's *drawable* directory.

**Note:**

If the *drawable* directory does not exist by default, create one.

4. Filter out ABI to remove redundant SO architectures. Currently, WAF SDK only provides SO in the *armeabi* architecture. Therefore, you must filter the exported ABIs. Otherwise, it may cause an App crash. The procedure is as follows:
 - a. Go to the Android project's *lib* directory, and delete all CPU architecture folders apart from the *armeabi* folder, which include *armeabi-v7a*, *x86*, *x86_64*, *arm64-v8a*, *mips*, and *mips64*. Make sure you keep only the *armeabi*, *armeabi-v7a*, and *arm64-v8a* folders.
 - b. Add a filter rule in the project's *build.gradle* configuration file. Architectures specified by *abiFilters* are included in the APK. The sample code is as follows:

**Note:**

The *armeabi* architecture is specified in the following sample. You can also specify the *armeabi-v7a* or *arm64-v8a* architecture.

```
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:**

Keeping only the SO in the armeabi architecture can remarkably reduce the App size without affecting the App's compatibility.

下图显示了手机淘宝App的ABI情况。可以看出，手机淘宝App只有armeabi架构的目录。

5. Add App permission.

- For an Android Studio project that uses the aar method integration, additional permission configuration is not necessary, because the relevant permissions are already specified in the aar files.
- For an Eclipse project, you must add the following permission configuration to the *AndroidManifest.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 configuration.
- If you have used Proguard for obfuscation, then you must add the ProGuard configuration. Based on different access methods, the ProGuard configuration is divided into two types, which are Eclipse and AndrodStudio respectively.

- Android Studio**

If `proguardFiles` is configured in `build.gradle` and `minifyEnabled` is enabled, it means that the `proguard-rules.pro` configuration file is used for obfuscation, as shown in the following figure.

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

- **Eclipse**

If the proguard configuration is specified in `project.properties` (for example, the `project.properties` contains the following statement `proguard.config=proguard.cfg`), it means that proguard is used for obfuscation. Obfuscation configuration in the `proguard.cfg` file is shown in the following figure.



Add keep rules

To make sure that certain classes are not obfuscated, you must add the following rules in 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. **{*;}
```

Coding process

1. Import SDK

```
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;
;
```

2. Initialize SDK.

- Interface definition: `boolean initialize();`
- Interface description:

- Function: Initialize SDK.
- Parameter: N/A.
- Return value: Boolean type. Return value: Boolean type. True if the initialization is successful, and False if the initialization fails.
- Sample code:

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

3. Sign the request data

- Interface definition: `byte[] avmpSign(int signType, byte[] input);`
- Interface description:
 - Function: Use the avmp technology to sign the input data, and return the signature string.
 - Parameters:

Parameter Name	Type	Required	Description
signType	int	Yes	Algorithm used by the signature. Currently, it is a fixed value. Enter 3.
input	byte[]	No	Data to be signed, which is generally the entire request body. If the request body is empty, then enter null for this parameter.

- Return value: byte[] type. The signature string is returned.
- Sample code: When the client sends data to the server, it must call the avmpSign interface to sign the entire body data and obtain the signature string (the wToken).

```
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);
```

4. Put the wToken in the protocol header Add the wToken field's content to the HttpURLConnection class object. The sample code is as follows:

```
String request_body = "i am the request body, encrypted or not!" ;
URL url = new URL("http://www.xxx.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();
```

5. Send data to the server. Send the data with the modified protocol header to the App's self-owned server. WAF captures the data and parses the wToken for risk identification.



Note:

The signed request body must be exactly the same as the request body sent from client.

Error code

The preceding `initialize` and `avmpsign` interfaces may encounter exceptions. If you encounter an exception or error when generating the signature string, search "SecException" for related information in the log.

Common errors are listed as follows:

Error Code	Meaning
1901	Incorrect parameter. Enter the correct parameter.
1902	Image file error. It generally indicates that the apk signature used to retrieve the image file is inconsistent with the current application's apk signature. Use the current application's apk to generate the image file. In iOS, it may be caused by inconsistent BundleIDs.
1903	Incorrect image format.
1904	Upgrade to new version images. AVMP signature function only supports v5 images.
1905	Unable to find the image file. Make sure that the image file is in the <code>res\drawable</code>

	directory. The AVMP image is <code>yw_1222_0335_mwua.jpg</code> .
1906	byteCode corresponding to the AVMP signature is missing in the image. Check if the image used is correct.
1907	Failed to initialize AVMP. Try again later.
1910	Invalid avmpInstance instance. Probable causes are: InvokeAVMP is called after AVMPInstance is destroyed. The image's byteCode version does not match with that of the SDK.
1911	The encrypted image's byteCode does not have the corresponding export function.
1912	AVMP calling fails. Submit a ticket for further assistance.
1913	This error occurs when calling InvokeAVMP after AVMPInstance is destroyed.
1915	AVMP calling out of memory. Try again later.
1999	Unknown error. Try again later.

FAQ: Secret key image is optimized away due to specifying shrinkResources.

In Android Studio, if you specify `shrinkResources` to be `True`, then resource files that are not referenced in the code are optimized away during project compilation.

As a result, the two `jpg` files provided in the SDK cannot work normally. In the following figure, the file size of `yw_1222_0335.jpg` is 0 KB, which means the image is optimized away.

Resolution

Create a `raw` folder under the project's `res` directory, and then create a `keep.xml` file in the `raw` folder. Enter 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"
/>
```

After that, re-compile the project apk.

Test and validation

Follow these steps to check if your App is correctly integrated with WAF SDK:

1. Change the suffix of the compressed apk file to zip, and decompress this zip file.
2. Locate the project's *lib* directory, and make sure that it contains only the *armeabi* folder. If you find folders for other architectures, delete them. For more information, see [Procedure step 4](#).
3. Locate the project's *res/drawable* directory, and make sure that the *yw_1222_0335.jpg* and *yw_1222_0335_mwua.jpg* files are there, and the file sizes are not 0.
4. Print the log, and make sure that the correct signature information is generated after the **avmpSign** interface is called. If the signature information cannot be generated, check the log for error codes.

5 Real-time log query and analysis

5.1 Billing method

Web Application Firewall (WAF) Log Service is billed based on the log storage period and the log storage size of your choice.

WAF Log Service is activated on a subscription basis.

**Note:**

To activate WAF Log Service, you must buy a WAF subscription.

In the WAF purchase page, enable Activate Log Service and select the log storage period and the log storage size. Then, the price is automatically calculated based on the **log store specification** of your choice and the **validity** of the WAF instance.

Log storage specification

The detailed pricing for each log storage specification for WAF Log Service is shown in the following table.

Log storage period	Log storage size	Recommended scenarios	For International region instances		For Mainland China region instances	
			Monthly subscription	Yearly subscription	Monthly subscription	Yearly subscription
180 days	3 TB	Average daily QPS is up to 80.	450	5,400	225	2,700
	5 TB	Average daily QPS is up to 120.	750	9,000	375	4,500
	10 TB	Average daily QPS is up to 260.	1,500	18,000	750	9,000
	20 TB	Average daily QPS is up to 500.	3,000	36,000	1,500	18,000
	50 TB	Average daily QPS is up to 1,200.	7,500	90,000	3,000	36,000

Log storage period	Log storage size	Recommended scenarios	For International region instances		For Mainland China region instances	
			Monthly subscription	Yearly subscription	Monthly subscription	Yearly subscription
	100 TB	Average daily QPS is up to 2,600.	15,000	180,000	7,500	90,000
360 days	5 TB	Average daily QPS is up to 60.	750	9,000	375	4,500
	10 TB	Average daily QPS is up to 120.	1,500	18,000	750	9,000
	20 TB	Average daily QPS is up to 260.	3,000	36,000	1,500	18,000
	50 TB	Average daily QPS is up to 600.	7,500	90,000	3,000	36,000
	100 TB	Average daily QPS is up to 1,200.	15,000	180,000	7,500	90,000

Upgrade storage capacity

If you have no log storage left, a notification appears to remind you to expand the storage size. You can expand the log storage size at any time.



Note:

If log storage is full, WAF stops writing new log entries to the exclusive logstore in Log Service. A log entry stored in the logstore is deleted based on the specified period. If the WAF Log Service instance expires and you do not renew it within seven days, all log entries in the logstore are deleted.

Validity

The validity of the WAF Log Service instance is based on your WAF subscription.

- **Buy:** When you buy a WAF subscription and enable Log Service, the price of Log Service is calculated based on the validity of the subscription.

- **Upgrade:** When you enable Log Service by upgrading an existing WAF subscription, the price of Log Service is calculated based on the remaining validity of the existing WAF instance. The remaining validity is accurate to minutes.

Service expiration

If your WAF instance expires, WAF Log Service expires at the same time.

- When the service expires, WAF stops writing log entries to the exclusive logstore in Log Service.
- The log entries recorded by WAF Log Service are retained within seven days after the service expires. If you renew the service within seven days after the service expires, you can continue to use WAF Log Service. Otherwise, all stored WAF log entries are deleted.

5.2 Activate WAF Log Service

After purchasing a Web Application Firewall instance, you can activate the real-time log query and analysis service for your websites on the App Management page in the console.

Scope

With WAF Log Service, you can collect multiple log entries in real time from your websites that are protected by WAF. You can also perform real-time log query and analysis and display results in dashboards. WAF Log Service fully meets the business protection needs and operational requirements of your websites. You can select the log storage period and the log storage size as needed when enabling WAF Log Service.



Note:

At the moment, WAF Log Service is only available to WAF subscription instances (Pro, Business, or Enterprise edition).

Benefits

The WAF real-time log query and analysis service has the following benefits:

- **Simple configuration:** You can easily configure the service to collect log entries that record visits to and attacks on your websites.
- **Real-time analysis:** Integrated with Log Service, the WAF console provides the real-time log analysis service and the out-of-the-box report center. You can know almost everything about visits to and attacks on your websites.

- **Real-time alarms:** Near real-time monitoring and alerts based on specific indicators are available to ensure timely responses to critical business exceptions.
- **Collaboration:** This service is used with real-time computing, cloud storage, visualization, and other data solutions to discover more data value.

Enable WAF Log Service

1. Log on to the [Web Application Firewall console](#).
2. Choose **App Market > App Management**, and select the region where your WAF instance is located.
3. Click **Upgrade** in Real-time Log Query and Analysis Service.
4. On the page that is displayed, enable **Log Service**, select the log storage period and the log storage size, and then click **Buy Now**.



Note:

For more information about the billing of WAF Log Service, see [WAF Log Service Billing methods](#).

5. Return to the WAF console and choose **App Market > App Management**, and then click **Authorize** in Real-time Log Query and Analysis Service.
6. Click **Agree** to authorize WAF to write log entries to your exclusive logstore.

WAF Log Service is then enabled and authorized.
7. Return to the WAF console and choose **App Market > App Management** and then, click **Configure** in Real-time Log Query and Analysis Service.
8. On the **Log Service** page, select the domain name of your website that is protected by WAF, and turn on the **Status** switch on the right to enable WAF Log Service.

Log Service collects all web log recorded by WAF in real time. These log entries can be queried and analyzed in real time.

5.3 Log collection

You can enable the Web Application Firewall (WAF) log collection feature for a specified domain in the WAF console.

Prerequisites

- Buy a WAF instance and protect the [domain using WAF](#).
- Enable Log Service.

Context

Log Service collects log entries that record visits to and attacks on websites that are protected by **Alibaba Cloud WAF**, and supports real-time log query and analysis. The query results are displayed in dashboards. You can timely perform analytical investigation on visits to and attacks on your websites and help security engineers to develop protection strategies.

Procedure

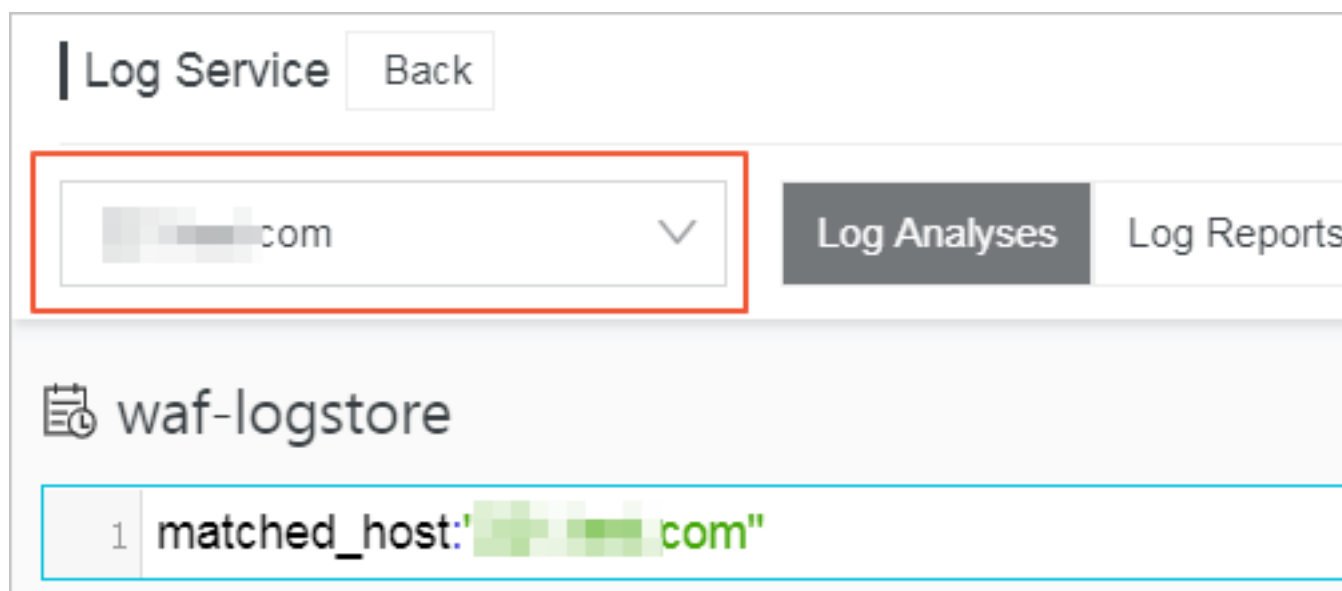
1. Log on to the [Web Application Firewall console](#).
2. Choose **App Market > App Management**, and click Real-time Log Query and Analysis Service.



Note:

If you are configuring the WAF log collection feature for the first time, click **Authorize** and follow the instructions on the authorization page to authorize WAF to write all log entries to your exclusive logstore.

3. Select the domain and turn on the **Status** switch on the right to enable the log collection feature.



The WAF log collection feature has now been enabled for the domain. Log Service automatically creates an exclusive logstore for your account. WAF automatically writes log entries to the exclusive logstore. The following [Default configuration](#) table describes the default configuration of the exclusive logstore.

Table 5-1: Default configuration

Default configuration item	Description
Project	<p>A project is created by default. The project name format is determined by the region of your WAF instance.</p> <ul style="list-style-type: none">• If the WAF instance is created in Mainland China, the project name is <code>waf-project-Your Alibaba Cloud account ID-cn-hangzhou</code>.• If the WAF instance is created in other regions, the project name is <code>waf-project-Your Alibaba Cloud account ID-ap-southeast-1</code>.
Logstore	<p>A logstore <code>waf-logstore</code> is created by default.</p> <p>All log entries collected by the WAF log collection feature are saved in this logstore.</p>
Region	<ul style="list-style-type: none">• If the WAF instance is created in Mainland China, the project is saved in the Hangzhou region by default.• If the WAF instance is created in other regions, the project is saved in the Singapore region by default.
Shard	<p>Two shards are created by default with the Automatic shard splitting feature enabled.</p>
Dashboard	<p>Three dashboards are created:</p> <ul style="list-style-type: none">• Access Center• Operation Center• Security Center <p>For more information about dashboards, see WAF Log Service—Log Reports.</p>

Limits and instructions

- Other data cannot be written to the exclusive logstore.

Log entries generated by WAF are stored in the exclusive logstore. You cannot write other data to this logstore by using API, SDK or other methods.

**Note:**

The exclusive logstore has no special limits in query, statistics, alerts, streaming consumption and other functions.

- Basic configurations, such as the storage period of log entries, cannot be modified.
- The exclusive logstore is not billed.

To use the exclusive logstore, you must enable Log Service for your account. The exclusive logstore is not billed.

**Note:**

When your Log Service is overdue, the WAF log collection feature is suspended until you pay the bills in a timely manner.

- Do not delete or modify the configurations of the project, logstore, index, and dashboards, which are created by Log Service by default. Log Service updates the WAF log query and analysis service on an irregular basis. The index of the exclusive logstore and the default reports are also updated automatically.
- If you want to use the WAF log query and analysis service with a RAM user, you must grant the required Log Service permissions to the RAM user. For more information about how to grant permissions, see [Grant log query and analysis permissions to a RAM user](#).

5.4 Log Analyses

The Real-time Log Query and Analysis Service page in the Web Application Firewall (WAF) console is integrated with the **Log Analyses** feature and the **Log reports** feature. After [enabling the WAF log collection feature](#) for a domain, you can perform real-time query and analysis, view or edit dashboards, and set up monitoring and alarms in the Real-time Log Query and Analysis Service page.

Procedure

1. Log on to the [Web Application Firewall console](#), and choose **App Market > App Management**.
2. Click on the Real-time Log Query and Analysis Service area to open the **Log Service** page.
3. Select the domain and check that the **Status** switch on the right is turned on.
4. Click **Log Analyses**.

The current page is integrated with the **Querying and analyzing** page. A query statement is automatically inserted. For example, `matched_host: "www.aliyun.com"` is used to query all log entries that is related to the domain in the statement.

5. Enter a query and analysis statement, select a log time range, and then click **Search & Analysis**.

More operations

The following operations are available in the Log Analyses page.

- **Customize query and analysis**

Log Service provides rich query and analysis syntax for querying log entries in a variety of complex scenarios. For more information, see the [Custom query and analysis](#) in this topic.

- **View the distribution of log entries by time period**

Under the query box, you can view the distribution of log entries that are filtered by time period and query statement. A histogram is used to indicate the distribution, where the horizontal axis indicates the time period, and the vertical axis indicates the number of log entries. The total number of the log entries in the query results is also displayed.



Note:

You can hold down the left mouse button and drag the histogram to select a shorter period. The `time picker` automatically updates the time period, and the query results are also updated based on the updated time period.

- **View raw log entries**

In the **Raw Logs** tab, each log entry is detailed in a single page, which includes the time when the log entry is generated, the content, and the properties in the log entry. You can click **Display Content Column** to configure the display mode (**Full Line** or **New Line**) for long strings in the Content column. You can click **Column Settings** to display specific fields, or click the Download Log button to download the query results.

Additionally, you can click a value or a property name to add a query criterion to the query box. For example, if you click the value GET in the `request_method: GET` field, the query statement in the query box is updated to:

<The original query statement> and request_method: GET

The screenshot shows the 'waf-logstore' interface. At the top, a search bar contains the query: `matched_host:"10.10.10.10" and request_method: GET`. Below the search bar, there are tabs for 'Raw Logs', 'LiveTail', and 'Graph'. The 'Raw Logs' tab is selected, showing a table of log entries. The first entry is highlighted, showing details such as `__source__: log_service`, `__topic__: waf_access_log`, `acl_action: pass`, `body_bytes_sent: 96`, `cc_action: none`, `cc_phase: -`, `content_type: -`, `host: 10.10.10.10`, `http_cookie: __cfduid=d2da07745b6d4f434ce22244e72fec09a1543457409; acw_tc=7837b11715438308768321524e47a48a2a189df5277c32b16a9b52d044f; http_referer: http://maomao.test.com/; http_user_agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.110 Safari/537.36; http_x_forwarded_for: -; https: false`, `matched_host: 10.10.10.10`, `real_client_ip: 10.10.10.14`, `region: cn`, `remote_addr: 10.10.10.14`, `remote_port: 10431`, `request_length: 592`, and `request_method: GET`.

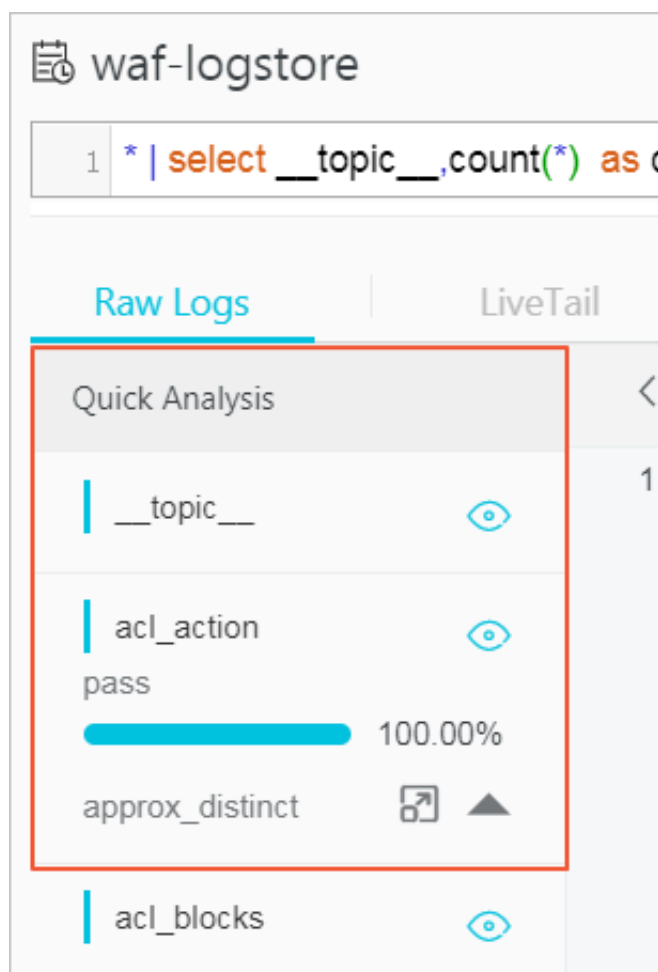
- **View analysis graphs**

Log Service enables you to display the analysis results in graphs. You can select the graph type as needed in the **Graph** tab. For more information, see [Analysis graph](#).

The screenshot shows the 'waf-logstore' interface with the 'Graph' tab selected. The search bar contains the query: `* | select __topic__.count(*) as count group by __topic__ order by count desc limit 10`. Below the search bar, there are tabs for 'Raw Logs', 'LiveTail', and 'Graph'. The 'Graph' tab is selected, showing a bar chart visualization. The chart has a title 'waf_access_log' and a y-axis labeled 'count'. The chart shows a single bar with a value of 3. Below the chart, there are 'Drilldown Configurations' and a table with columns 'waf_access_log' and 'count'. The table has one row with the value 3.

- **Perform quick analysis**

The Quick Analysis feature in the **Raw Logs** tab provides you with an one-click interactive experience, which gives you a quick access to the distribution of log entries by a single property within a specified time period. This feature can reduce the time used for indexing key data. For more information, see [Quick analysis](#) in the following section.



Customize query and analysis

The log query statement consists of the query (Search) and the analysis (Analytics). These two parts are divided by a vertical bar (|):

```
$Search | $Analytics
```

Type	Description
Query (Search)	A keyword, a fuzzy string, a numerical value, a range, or other criteria can be used in the query criteria. A combined condition can also be used. If the statement is empty or only contains an asterisk (*), all log entries are displayed.
Analysis (Analytics)	Performs computing and statistics to the query results or all log entries.



Note:

Both the query part and the analysis part are optional.

- When the query part is empty, all log entries within the time period are displayed. Then, the query results are used for statistics.
- When the analysis part is empty, only the query results are returned without statistics.

Query syntax

The query syntax of Log Service supports **full-text index** and **field search**. You can enable the New Line display mode, syntax highlighting, and other features in the query box.

- **Full text index**

You can enter keywords without specifying properties to perform the query by using the full-text index. You can enter the keyword with double quotation marks (") surrounded to query log entries that contain the keyword. You can also add a space or `and` to separate keywords.

Examples

- **Multiple-keywords query**

The following statements can be used to query all log entries that contain `www.aliyun.com` and `error`.

```
www.aliyun.com error OR www.aliyun.com and error.
```

- **Criteria query**

The following statement can be used to search for all log entries that contain `www.aliyun.com`, `error` or `404`.

```
www.aliyun.com and (error or 404)
```

- **Prefix query**

The following statement can be used to query all log entries that contain `www.aliyun.com` and start with `failed_`.

```
www.aliyun.com and failed_*
```

**Note:**

An asterisk (*) can be added as a suffix, but it cannot be added as a prefix. For example, the statement cannot be `*_error`.

- **Field search**

You can perform a more accurate query based on specified fields.

The field search supports comparison queries for fields of numeric type. The format is `field name:value` or `field name>=value`. Moreover, you can perform combination queries using `and` or `or`, which can be used in combination with the full text index.

**Note:**

The log entries that record access, operation, and attack on the domain name in WAF Log Service can also be queried by fields. For more information about the meaning, type, format, and other information of the fields, see [Fields in the WAF log entries](#).

Examples

- **Multiple-fields query**

The following statement can be used to query all log entries that record the HTTP flood attack on the `www.aliyun.com` domain and are intercepted by WAF .

```
matched_host: www.aliyun.com and cc_blocks: 1
```

If you want to query all log entries that record access from a specific client whose IP address is `1.2.3.4` to `www.aliyun.com`, and access is blocked by the 404 error, you can use the following statement.

```
real_client_ip: 1.2.3.4 and matched_host: www.aliyun.com and  
status: 404
```

**Note:**

In this example, the `matched_host`, `cc_blocks`, `real_client_ip`, and `status` fields are the fields defined in the WAF log.

- **Numeric fields query**

The following statement can be used to query all log entries where the response time exceeds five seconds.

```
request_time_msec > 5000
```

Range query is also supported. For example, you can query all log entries where the response time exceeds five seconds and is no more than 10 seconds.

```
request_time_msec in (5000 10000]
```

**Note:**

The following query statement has the same function.

```
request_time_msec > 5000 and request_time_msec <= 10000
```

- **Field existence query**

You can perform a query based on the existence of a field.

- The following statement can be used to search for all log entries where the `ua_browser` field exists.

```
ua_browser: *
```

- The following statement can be used to search for all log entries where the `ua_browser` field does not exist.

```
not ua_browser: *
```

For more information about the query syntax that is supported by Log Service, see [Index and query](#).

Syntax for analysis

You can use the SQL/92 syntax for log analysis and statistics.

For more information about the syntax and functions supported by Log Service, see [Syntax description](#).



Note:

- The `from table name` part that follows the SQL standard syntax can be omitted from the analysis statement. In WAF Log Service, `from log` can be omitted.
- The first 100 results are returned by default, and you can modify the number of results that are returned by using the [LIMIT syntax](#).

Examples of query and analysis

Time-based log query and analysis

Each WAF log entry has a `time` field, which is used to represent the time when the log entry is generated. The format of the value in this field is `<year>-<month>-<day>T<hour>:<minute>:<second>+<time zone>`. For example, `2018-05-31T20:11:58+08:00` is 20:11:58 UTC+8 (Beijing Time), May 15, 2018.

In addition, each log entry has a built-in field `__time__`, which is also used to indicate the time when the log entry is generated. This field is used for calculation when performing statistics. The format of this field is a *Unix timestamp*, and the value of this field indicates the number of seconds that have elapsed since 00:00:00 Coordinated Universal Time (UTC), January 1, 1970. Therefore, if you want to display a calculated result, you must convert the format first.

- **Select and display the time**

You can query the log based on the `time` field. For example, you can search for the last 10 log entries that record the HTTP flood attacks on `www.aliyun.com` and are intercepted by WAF. Then, you can display the time field, the source IP field, and the client field.

```
matched_host: www.aliyun.com and cc_blocks: 1
| select time, real_client_ip, http_user_agent
  order by time desc
```

```
limit 10
```

waf-logstore

```
1 matched_host: [REDACTED] .com and cc_blocks:1
2 | select time, real_client_ip, http_user_agent
3   order by time desc
4 | limit 10
```

3.2

0

12-03

12-03

Raw Logs

LiveTail

Graph

Chart type:



Drilldown Configurations

time +

No drilldown configurations available. Click the (+) icon in the table header to add.

2018-12-03T17:54:42+08:00

2018-12-03T17:54:37+08:00

2018-12-03T17:54:27+08:00

- **Calculate using time.**

You can use the `__time__` field to calculate using time. For example, you can calculate the number of days that have elapsed since the domain suffered a HTTP flood attack.

```
matched_host: www.aliyun.com and cc_blocks: 1
round((to_unixtime(now()) - __time__)/86400, 1) as "days_passed",
real_client_ip, http_user_agent
order by time desc
limit 10
```



Note:

In this example, `round((to_unixtime(now()) - __time__)/86400, 1)` is used to calculate the number of days that have elapsed since the domain had a HTTP flood attack. First, use `now()` to get the current time, and convert the current time into a Unix timestamp using `to_unixtime`. Then, subtract the converted time with the value of the built-in field `__time__` to get the number of seconds that have elapsed. Finally, divide it by 86400 (the total number of seconds in a day) and apply the `round(data, 1)` function to keep one decimal place. The result is the number of days that have elapsed since each attack log entry is generated.

The screenshot shows the WAF logstore interface. At the top, there's a search bar with the query: `matched_host: www.aliyun.com and cc_blocks:1`. Below the search bar, there's a table with 4 columns: `time`, `days_passed`, `real_client_ip`, and `http_user_agent`. The table contains 3 rows of data. The first row shows a time of 2018-12-03T17:54:42+08:00, days_passed of 0.7, and a user agent of Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.110 Safari/537.36. The second row shows a time of 2018-12-03T17:54:37+08:00, days_passed of 0.7, and a user agent of Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.110 Safari/537.36. The third row shows a time of 2018-12-03T17:54:37+08:00, days_passed of 0.7, and a user agent of Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.110 Safari/537.36. The interface also includes a 'Search & Analysis' button and a 'Log Entries: 3' status.

- **Perform group statistics based on a specific time**

You can query the log based on the trend of HTTP flood attacks on the domain within a specified time period.

```
matched_host: www.aliyun.com and cc_blocks: 1
| select date_trunc('day', __time__) as dt, count(1) as PV
group by dt
```

```
order by dt
```

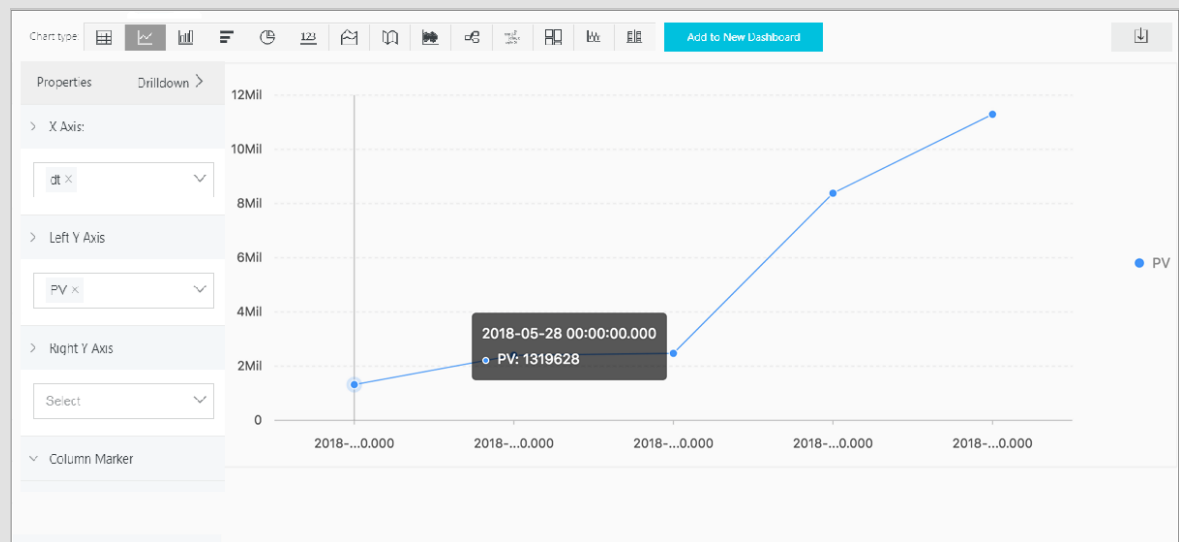
**Note:**

In this example, the built-in field `__time__` is used by the `date_trunc('day', ...)` function to align the time of the entries by day. Each log entry is assigned to a group based on the day when the log entry is generated. The total number of log entries in each group is counted using `count(1)`. Then, these entries are ordered by the group. You can use other values for the first parameter of the `date_trunc` function to group the log entries based on other time units, such as `second`, `minute`, `hour`, `week`, `month`, and `year`. For more information about this function, see [Date and time functions](#).

dt +	PV +
2018-12-03 00:00:00.000	3

**Note:**

You can also display the results with a line chart.



- **Perform group statistics based on time.**

If you want to analyze the log based on time using more flexible groupings, complex calculations are required. For example, you can query the log based on the trend of HTTP flood attacks on the domain within every five minutes.

```
matched_host: www.aliyun.com and cc_blocks: 1
| select from_unixtime(__time__ - __time__ % 300) as dt,
      count(1) as PV
  group by dt
 order by dt
```

```
limit 1000
```

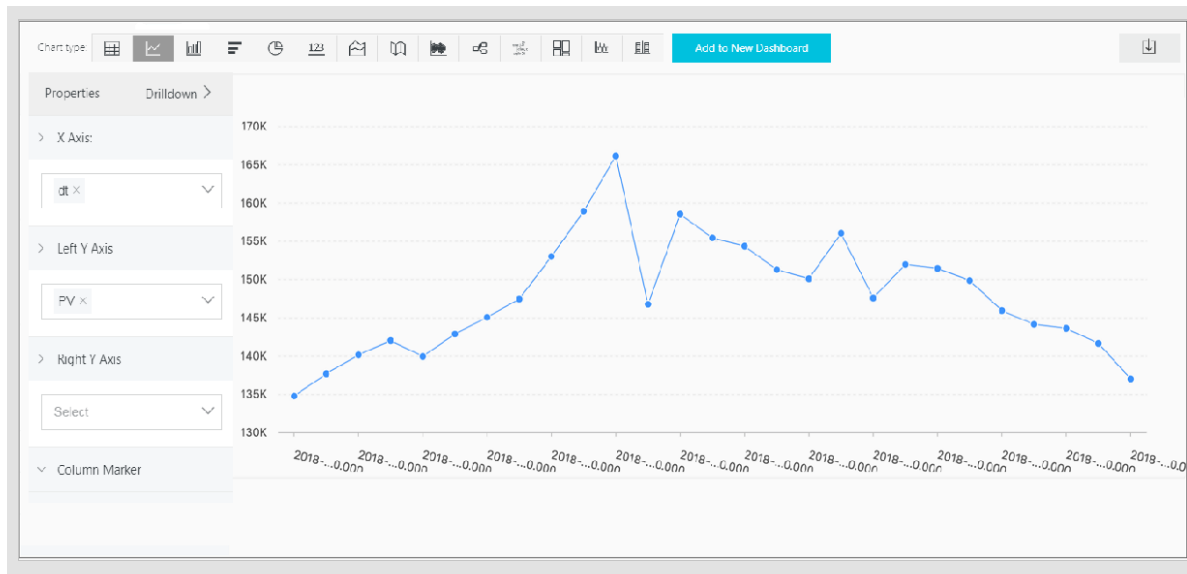
**Note:**

In this example, the built-in field is used for aligning the time by using the formula `__time__ - __time__ % 300`, and the `from_unixtime` function converts the format of the result. Then, each entry is assigned to a group that indicates a time period of five minutes (300 seconds), and the total number of log entries in each group is counted using `count(1)`. Finally, the query results are ordered by group and the first 1,000 results are returned, which include the log entries that are generated within 83 hours before the specified time period.

dt ↕↑	PV ↕↑
2018-05-31 21:30:00.000	134795
2018-05-31 21:35:00.000	137691
2018-05-31 21:40:00.000	140171
2018-05-31 21:45:00.000	142037
2018-05-31 21:50:00.000	139958
2018-05-31 21:55:00.000	142906
2018-05-31 22:00:00.000	145093
2018-05-31 22:05:00.000	147474

**Note:**

You can also display the results with a line graph.



The `date_parse` and `date_format` functions are used to convert the time format. For more information about the functions that can be used to parse the time field, see [Date and time functions](#).

Client IP address-based log query and analysis

The WAF log contains the field `real_client_ip`, which reflects the real client IP address. In cases where the user accesses your website through a proxy server, or the IP address in the request header is wrong, you cannot get the real IP address of the user. However, the `remote_addr` field forms a direct connection to the client, which can be used to get the real IP address.

- **Classify attackers by country**

You can query the log based on the distribution of HTTP flood attackers by country.

```
matched_host: www.aliyun.com and cc_blocks: 1
| SELECT ip_to_country(if(real_client_ip='', remote_addr,
  real_client_ip)) as country,
      count(1) as "number of attacks"
  group by country
```

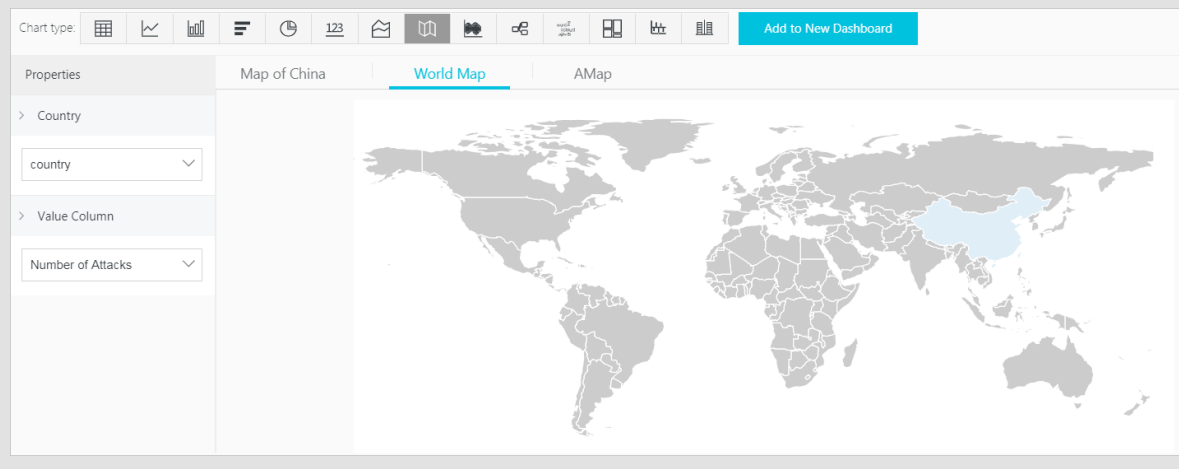


Note:

In this example, the function `if(condition, option1, option2)` returns the real client IP address. If `real_client_ip` is `-`, the function returns the value of `remote_addr`. Otherwise, the function returns `real_client_ip`. Then, use the `ip_to_country` to get the country information from the IP address of the client.

**Note:**

You can also display the results with a world map.



- **Distribution of visitors by province**

If you want to get the distribution of visitors by province, you can use the `ip_to_province` function to get the province information from the IP addresses.

```
matched_host: www.aliyun.com and cc_blocks: 1
| SELECT ip_to_province(if(real_client_ip='', remote_addr,
    real_client_ip)) as province,
        count (1) as "number of attacks"
    group by province
```

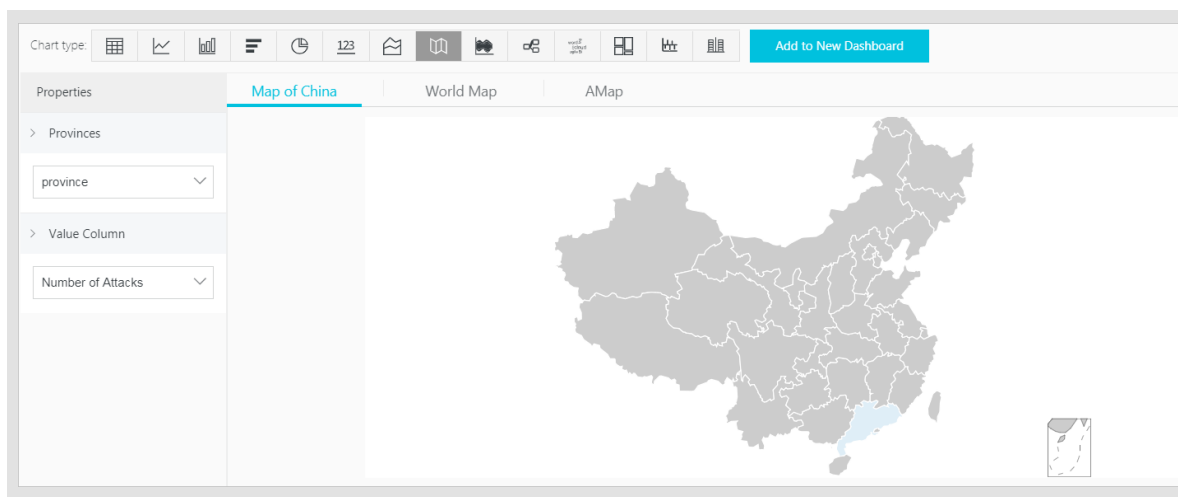
**Note:**

In this example, the `ip_to_province` function is used to get the country information from the real IP address of the client. If the IP address is not in the Mainland of China, the function returns the province or state of the IP address in the country field. However, if you choose to display the results with a map of China, IP addresses that are not in the Mainland of China are not displayed.

province +	Number of Attacks +
广东省	3

**Note:**

You can also display the results with a map of China.



- **Heat map that indicates the distribution of attackers**

You can use the `ip_to_geo` function to get the geographic information (the latitude and the longitude) from the real IP addresses of the clients. This information can be used to generate a heat map to indicate the density of attacks.

```
matched_host: www.aliyun.com and cc_blocks: 1
| SELECT ip_to_geo(if(real_client_ip='', remote_addr, real_client_ip)) as geo,
          count (1) as "number of attacks"
  group by geo
 limit 10000
```



Note:

In this example, the `ip_to_geo` function is used to get the latitude and the longitude from the real IP addresses of the clients. The first 10,000 results are returned.

Select Amap and click **Show Heat Map**.

The `ip_to_provider` function can be used to get the IP provider name, and the `ip_to_domain` function can be used to determine whether the IP is a public IP or a private IP. For more information about the functions that can be used to resolve IP addresses, see [IP functions](#).

5.5 Log Reports

The **Log Reports** page is integrated with the **Dashboard** page of Log Service. On this page, you can view default dashboards. You can filter business and security data about your website by modifying the time range or adding filters.

View reports

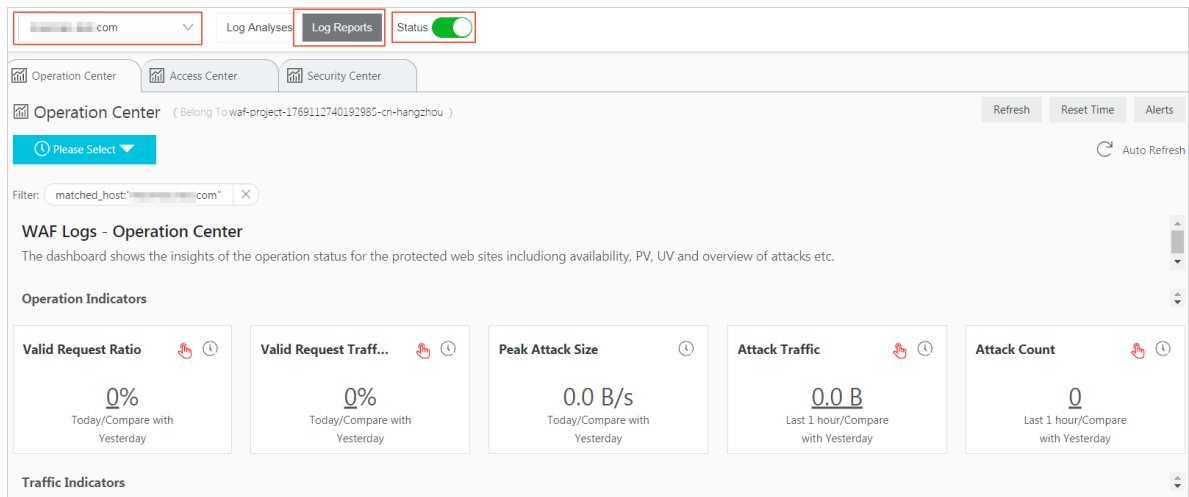
1. Log on to the [Web Application Firewall console](#), and choose **App Market > App Management**.
2. Click the Real-time Log Query and Analysis Service area to open the **Log Service** page.

3. [DO NOT TRANSLATE]

4. Select a domain and check that the **Status** switch on the right is turned on.

5. Click **Log Reports**.

The page that appears is integrated with the **Dashboard** page of Log Service. A **filter** is automatically added to display all log entries that are recorded for the domain you selected. In this example, the filter is `matched_host: www.aliyun.com`.

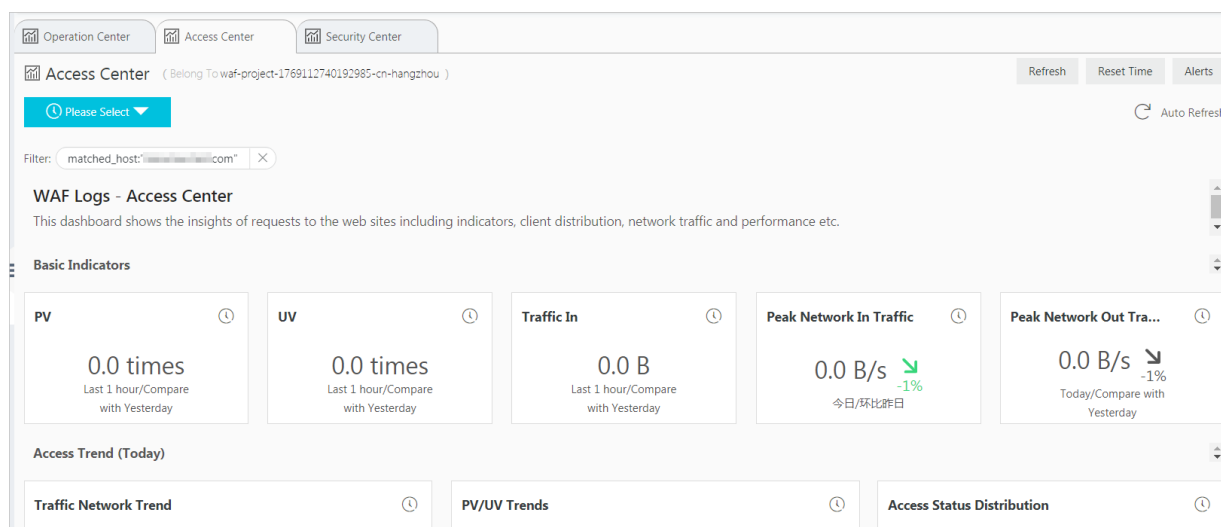


After you enable the WAF log collection feature, Log Service creates three dashboards by default: the Operation Center, Access Center, and Security Center.

**Note:**

For more information about the default dashboards, see [Default dashboards](#).

Dashboard	Description
Operation Center	Displays operation details such as the proportion of valid requests and the statistics of attacks, traffic details such as the peak of both inbound and outbound throughput and the number of requests received, operation trends, attack overview, and other information.
Access Center	Displays basic access details such as the number of page views (PV) and the number of unique visitors (UV), the access trend, the distribution of visitors, and other information.
Security Center	Displays basic index information of attacks, attack types, attack trend, attacker distribution, and other information.



Note:

Dashboards displays various reports using the layout that is predefined in WAF Log Service. The following table describes the graph types supported for reports. For more information about the graph types supported by Log Service, see [Graph description](#).

Type	Description
Number	Graphs of this type display important metrics, such as the valid request ratio and the peak of attacks.
Line chart and area chart	Graphs of these types display the trend of important metrics within a specified time period, such as the trend of inbound throughput and the trend of attack interceptions.
Map	Graphs of this type display the geographical distribution of visitors and attackers, for example, by country. Heat maps are also supported to illustrate the distribution of attackers.
Pie chart	Graphs of this type display a distribution, such as the distribution of attackers and the distribution of client types.
Table	Graphs of this type display a table that contains information, such as information of attackers.
Map	Graphs of this type display the geographical distribution of data.


Time selector

The data in all graphs on the dashboard page are generated based on different time ranges. If you want to unify the time ranges, configure the **time selector**.

1. On the **Log Reports** page, click **Please Select** and

2. select a time range in the pane that appears. You can select a relative time, a time frame, or customize a time range.

**Note:**

- After you set a time range, the time range is applied to all reports.
- If you set a time range, a temporary view is generated on the current page. When you view reports next time, the default time range is used.
- To change the time range for a single report in the dashboard, click  in the upper-right corner.

Time

×

> Relative

1Minute

5Minutes

15Minutes

1Hour

4Hours

1Day

Today

1Week

30Days

Custom

> Time Frame

1Minute

15Minutes

1Hour

4Hours

1Day

1Week

30Days

Today

Yesterday

The Day before Yesterday

This Week

Previous Week

This Month

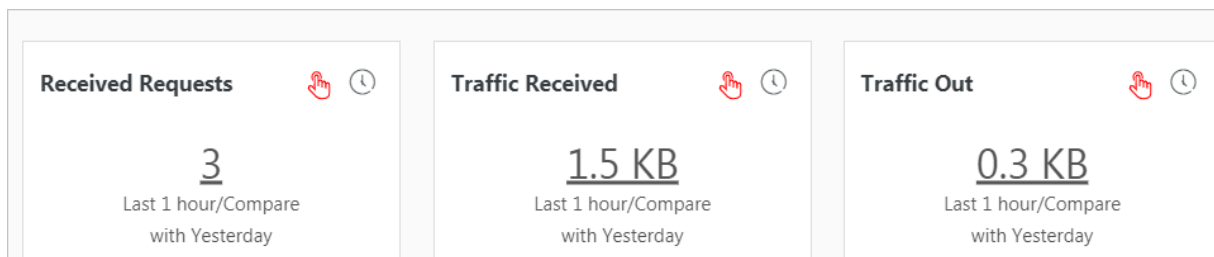
This Quarter


Custom

▽ Custom

Data drilldown

The drilldown operation is enabled for some graphs on the dashboard page, which provides you a quick access to the detailed data.



The drilldown operation is available for graphs marked with a  icon in the upper-right

corner. You can click a number with an underline to view the detailed underlying data. For example, to quickly find the domains that are attacked and the number of attacks, click the number in the **Attacked Hosts** graph of the **Security Center** report.



Note:

Alternatively, switch to the **Raw Log** tab to find the relevant log entries.

Description of values in default dashboards

- **Operation Center:** Displays operation details such as the proportion of valid requests and the statistics of attacks, traffic details such as the peak of both inbound and outbound throughput and the number of requests received, the operation trend, the attack overview, and other information.

Graph	Type	Default time range	Description	Example
Valid Request Ratio	Single value	Today (time frame)	Displays the percentage of valid requests in all requests. A valid request is a request that is neither an attack nor a request that is blocked by a 400 error.	95%
Valid Request Traffic Ratio	Single value	Today (time frame)	Displays the percentage of the traffic generated by valid requests in the	95%

Graph	Type	Default time range	Description	Example
			traffic generated by all requests.	
Peak Attack Size	Single value	Today (time frame)	Displays the peak of attack traffic, which is measured in Bps.	100 B/s
Attack Traffic	Single value	1 hour (relative)	Displays the total attack traffic, which is measured in B.	30 B
Attack Count	Single value	1 hour (relative)	The total number of attacks.	100
Peak Network In	Single value	Today (time frame)	Displays the peak inbound throughput, which is measured in KB/s.	100 KB/s
Peak Network Out	Single value	Today (time frame)	Displays the peak outbound throughput, which is measured in KB/s.	100 KB/s
Received Requests	Single value	1 hour (relative)	Displays the total number of valid requests.	7,800
Received traffic	Single value	1 hour (relative)	Displays the total inbound traffic that is generated by valid requests, which is measured in MB.	1.4 MB
Traffic Out	Single value	1 hour (relative)	Displays the total outbound traffic that is generated by valid requests, which is measured in MB.	3.8 MB
Network Traffic In And Attack	Area chart	Today (time frame)	Displays the trends of throughput generated by valid requests and attacks, which is measured in Kbit/s.	-

Graph	Type	Default time range	Description	Example
Request And Interception	Line chart	Today (time frame)	Displays the trends of valid requests and requests that are intercepted, which is measure in Kbit/h.	-
Access Status Distribution	Flow chart	Today (time frame)	Displays the trends of requests with different status codes (404, 304, 200, and other status codes), which is measured in Kbit/h.	-
Attack Source (World)	World map	1 hour (relative)	Displays the distribution of attackers by country.	-
Attack Source (China)	Map of China	1 Hour (Relative)	Displays the distribution of attackers in China by province.	-
Attack Type	Pie chart	1 hour (relative)	Displays the distribution of attacks by attack type .	-
Attacked Hosts	Tree map	1 hour (relative)	Displays the domains that are attacked and the number of attacks.	-

- **Access center:** Displays basic access details such as the number of PV and the number of UV, the access trend, the distribution of visitors, and other information.

Graph	Type	Default time range	Description	Example
PV	Single value	1 hour (relative)	Displays the total number of PV.	100,000
UV	Single value	1 hour (relative)	Displays the total number of UV.	100
Traffic In	Single value	1 hour (relative)	Displays the total inbound traffic, which is measured in MB.	300 MB
Peak Network In Traffic	Single value	Today (time frame)	Displays the peak inbound throughput,	0.5 KB/s

Graph	Type	Default time range	Description	Example
			which is measured in KB/s.	
Peak Network Out Traffic	Single value	Today (time frame)	Displays the peak outbound throughput, which is measured in KB/s.	1.3 KB/s
Traffic Network Trend	Area chart	Today (time frame)	Displays the trends of inbound and outbound throughput, which are measured in KB/s.	-
PV/UV Trends	Line chart	Today (time frame)	Displays the trends of PV and UV, which is measured in Kbit/h.	-
Access Status Distribution	Flow chart	Today (time frame)	Displays the trends of requests with different status codes (404, 304, 200, and other status code), which is measured in Kbit/h.	-
Access Source	World map	1 hour (relative)	Displays the distribution of attackers by country.	-
Traffic In Source (World)	World map	1 hour (relative)	Displays the distribution (by country) of inbound traffic from requests.	-
Traffic In Source (China)	Map of China	1 hour (relative)	Displays the distribution (by province) of inbound traffic from requests in China.	-
Access Heatmap	Amap	1 hour (relative)	Displays the heat map that indicates the source distribution of requests by geographical position.	-
Network Provider Source	Pie chart	1 hour (relative)	Displays the source distribution of requests by Internet service provider that provides	-

Graph	Type	Default time range	Description	Example
			network for the source, such as China Telecom , China Unicom, China Mobile, and universities.	
Referer	Table	1 hour (relative)	Displays the first 100 referer URLs which the hosts are most often redirected from, and displays the information of hosts and redirection frequency.	-
Mobile Client Distribution	Pie chart	1 hour (relative)	Displays the distribution of requests from mobile clients, by client type.	-
PC Client Distribution	Pie chart	1 hour (relative)	Displays the distribution of requests from PC clients, by client type.	-
Request Content Type Distribution	Pie chart	1 hour (relative)	Displays the distribution of request sources by content type, such as HTML, form, JSON, and streaming data.	-
Accessed Sites	Tree map	1 Hour (Relative)	Displays the addresses of 30 domains that are visited most.	-
Top Clients	Table	1 hour (relative)	Displays the information of 100 clients that visit your domains most. The information includes the client IP address, the region and city, network information, the request method, inbound traffic , the number of incorrect accesses, the number of attacks, and other information.	-

Graph	Type	Default time range	Description	Example
URL With Slowest Response	Table	1 hour (relative)	Displays the information of 100 URLs that have the longest response times. The information includes the website address, the URL, the average response time, the number of accesses, and other information.	-

- **Security Center:** Displays basic details of attacks, attack types, the attack trend, the distribution of attackers, and other information.

Chart	Type	Default time range	Description	Example
Peak Attack Size	Single value	1 hour (relative)	Displays the peak of the throughput when your website is suffering attacks, which is measured in Bps.	100 B/s
Attacked Hosts	Single value	Today (time frame)	Displays the number of domains that are attacked.	3
Source Country Of Attack	Single value	Today (time frame)	Displays the number of countries that are attack sources.	2
Attack Traffic	Single value	1 hour (relative)	Displays the total amount of traffic that is generated by attacks, which is measured in B.	1 B
Attacker UV	Single value	1 hour (relative)	Displays the number of unique clients that are attack sources.	40
Attack type distribution	Flow chart	Today (time frame)	Displays the distribution of attacks by attack type.	-


Chart	Type	Default time range	Description	Example
Intercepted Attack	Single value	1 hour (relative)	Displays the number of attacks that are intercepted by WAF.	100
HTTP flood attack Interception	Single value	1 hour (relative)	Displays the number of HTTP flood attacks that are intercepted by WAF.	10
Web Attack Interception	Single value	1 hour (relative)	Displays the number of Web application attacks that are intercepted by WAF.	80
Access Control Event	Single value	1 hour (relative)	Displays the number of requests that are intercepted by the HTTP ACL policies of WAF.	10
HTTP flood attack (World)	World map	1 hour (relative)	Displays the distribution of HTTP flood attackers by country.	-
HTTP flood attack (China)	China map	1 hour (relative)	Displays the distribution of HTTP flood attackers by province in China.	-
Web Attack (World)	World map	1 Hour (Relative)	Displays the distribution of Web application attacks by country.	-
Web Attack (China)	Map of China	1 hour (relative)	Displays the distribution of Web application attacks by province in China.	-
Access Control Attack (World)	World Map	1 hour (relative)	Displays the distribution by country of requests that are intercepted by the HTTP ACL policies of WAF.	-
Access Control Attack (China)	Map of China	1 Hour (Relative)	Displays the distribution by province in China of requests that are intercepted by the HTTP ACL policy of WAF.	-

Chart	Type	Default time range	Description	Example
Attacked Hosts	Tree map	1 hour (relative)	Displays the websites that are attacked most.	-
HTTP flood attack Strategy Distribution	Pie chart	1 hour (relative)	Displays the distribution of security policies being activated for HTTP flood attacks.	-
Web Attack Type Distribution	Pie chart	1 hour (relative)	Displays the distribution of Web attacks by attack type.	-
Top Attackers	Table	1 hour (relative)	Displays IP addresses, provinces, and network providers of the first 100 clients that launch the recent attacks, and displays the number of attacks and the amount of traffic generated by these attacks.	-
Attacker Referer	Table	1 Hour (Relative)	Displays the information in referers of attack requests, which includes referer URLs, referer hosts, and the number of attacks.	-

5.6 Fields in the log entry

WAF keeps detailed log entries for your domains, including access requests and attack logs. Each log entry contains dozens of fields. You can perform query and analysis based on specific fields.

Field	Description	Example
__topic__	The topic of the log entry. The value of this field is waf_access_log, which cannot be changed.	waf_access_log
acl_action	The action generated by the WAF HTTP ACL policy to the request, such as pass, drop, and captcha.	pass

Field	Description	Example
	 Note: If the value is null or –, it indicates that the action is pass.	
acl_blocks	Indicates whether the request is blocked by the HTTP ACL policy. <ul style="list-style-type: none"> If the value is 1, the request is blocked. If the value is not 1, the request is passed. 	1
antibot	The type of the Anti-Bot Service protection strategy that applies, which includes: <ul style="list-style-type: none"> ratelimit: Frequency control sdk: APP protection intelligence: Algorithmic model acl: HTTP ACL policy blacklist: Blacklist 	ratelimit
antibot_action	The action performed by the Anti-Bot Service protection strategy, which includes: <ul style="list-style-type: none"> challenge: Verifying using an embedded JavaScript script drop: Blocking report: Logging the access event captcha: Verifying using a slider captcha 	challenge
block_action	The type of the WAF protection that is activated, which includes: <ul style="list-style-type: none"> tmd: Protection against HTTP flood attacks waf: Protection against Web application attacks acl: HTTP ACL policy geo: Blocking regions antifraud: Risk control for data antibot: Blocking Web crawlers 	tmd

Field	Description	Example
body_bytes_sent	The size of the body in the access request, which is measured in Bytes.	2
cc_action	Protection strategies against HTTP flood attacks, such as none, challenge, pass, close, captcha, wait, login, and n.	close
cc_blocks	Indicates whether the request is blocked by the CC protection. <ul style="list-style-type: none"> If the value is 1, the request is blocked. If the value is not 1, the request is passed. 	1
cc_phase	The CC protection strategy that is activated, which can be seccookie, server_ip_blacklist, static_whitelist, server_header_blacklist, server_cookie_blacklist, server_args_blacklist, or qps_overmax.	server_ip_blacklist
content_type	The content type of the access request.	application/x-www-form-urlencoded
host	The source website.	api.aliyun.com
http_cookie	The client-side cookie, which is included in the request header.	k1=v1;k2=v2
http_referer	The URL information of the request source, which is included in the request header. - indicates no URL information.	http://xyz.com
http_user_agent	The User Agent field in the request header, which contains information such as the client browser and the operating system.	Dalvik/2.1.0 (Linux; U; Android 7.0; EDI-AL10 Build/HUAWEIEDISON-AL10)
http_x_forwarded_for	The X-Forwarded-For (XFF) information in the request header, which identifies the original IP address of the client that connects to the Web server using a HTTP proxy or load balancing.	-

Field	Description	Example
https	Indicates whether the request is an HTTPS request. <ul style="list-style-type: none"> true: the request is an HTTPS request. false: the request is an HTTP request. 	true
matched_host	The matched domain name (extensive domain name) that is protected by WAF. If no domain has been matched, the value is <code>-</code> .	*.aliyun.com
querystring	The query string in the request.	title=tm_content%3Darticle&pid=123
real_client_ip	The real IP address of the client. If the system cannot get the real IP address, the value is <code>-</code> .	1.2.3.4
region	The information of the region where the WAF instance is located.	cn
remote_addr	The IP address of the client that sends the access request.	1.2.3.4
remote_port	The port of the client that sends the access request.	23713
request_length	The size of the request, measured in Bytes.	123
request_method	The HTTP request method used in the access request.	GET
request_path	The relative path of the request. The query string is not included.	/news/search.php
request_time_msec	The request time, which is measured in microseconds.	44
request_traceid	The unique ID of the access request that is recorded by WAF.	7837b117154103869434 37009ea1f0
server_name	The name of the found host. If no host is found, the value is <code>default</code> .	api.abc.com
server_protocol	The response protocol and the version number of the origin server.	HTTP/1.1

Field	Description	Example
status	The status of the HTTP response to the client returned by WAF.	200
time	The time when the access request occurs.	2018-05-02T16:03:59+08:00
ua_browser	The information of the browser that sends the request.	ie9
ua_browser_family	The family of the browser that the sent the request.	internet explorer
ua_browser_type	The type of the browser that the sent the request.	web_browser
ua_browser_version	The version of the browser that sends the request.	9.0
ua_device_type	The type of the client device that sends the request.	computer
ua_os	The operating system used by the client that sends the request.	windows_7
ua_os_family	The family of the operating system used by the client.	windows
upstream_addr	A list of origin addresses, separated by commas. The format of an address is <code>IP:Port</code> .	1.2.3.4:443
upstream_ip	The origin IP address that corresponds to the access request. For example, if the origin server is an ECS instance, the value of this field is the IP address of the ECS instance.	1.2.3.4
upstream_response_time	The time that the origin site takes to respond to the WAF request, which is measured in seconds. "-" indicates the timeout of the request.	0.044
upstream_status	The response status that WAF receives from the origin server. "-" indicates that no response is received. The reason can be the response timeout, or the request being blocked by WAF.	200

Field	Description	Example
user_id	Alibaba Cloud account ID.	12345678
waf_action	The action from the Web attack protection policy. <ul style="list-style-type: none">If the value is block, the attack is blocked.If the value is bypass or other values, the attack is ignored.	block
web_attack_type	The Web attack type such as xss, code_exec, webshell, sqli, lfilei, rfilei, and other.	xss

5.7 Advanced settings

If you click Advanced Settings on the page of WAF log query and analysis service, you will be redirected to the Log Service console. Then you can set advanced features for Log Service. For example, you can set alarms and notifications, real-time log collection and consumption, shipping log data, or provide visual representations with other products.

Procedure


1. Log on to the [Web Application Firewall console](#), choose **App Market > App Management**.
2. Click the Real-time Log Query and Analysis Service area to open the **Log Service** page.
3. Click **Advanced Settings** in the upper-right corner.
4. In the dialog box that appears, click **Go** to open the Log Service console.
5. In the Log Service console, you can set the following advanced features for log projects and logstores:
 - [Real-time log collection and consumption](#)
 - [Shipping log data to other Alibaba Cloud storage services in real time](#)
 - [Providing visual representations with other products](#)

5.8 Export log entries

The WAF log query and analysis service enables you to export log query results to a local file.

You can export the log entries on the current page to a CSV file, or export all log entries to a TXT file.

Procedure

1. Log on to the [Web Application Firewall console](#) and choose **App Market > App Management**.
2. Click the log query and analysis service area to open the **Log Service** page.
3. On the **Raw Logs** tab of the **Log Service** page, click the download button  on the right.



Note:

The download button does not appear if no result is found for a query.

4. In the **Download Log** dialog box that appears, select **Download Log in Current Page** or **Download all logs in the CLI console**.
 - **Download Log in Current Page** : Click **OK** to download the raw log entries on the current page to a CSV file.
 - **Download all logs in the CLI console**
 1. For more information about installing the command-line interface (CLI), see the [CLI guide](#).
 2. Go to the [Security Management](#) page, and find the AccessKey ID and AccessKey Secret of the current user.
 3. Click **Copy Command** and paste the command into CLI, replace the `AccessID` obtained in step 2 and `AccessKey` obtained in step 2 with the AccessKey ID and AccessKey Secret of the current user, and then run the command.

Log Download

☐ Download Log in Current Page ☒ Download all logs in the CLI console

1. Install the command line tool

For information about the command line tool installation, see:[Documentation](#)

2. View the AccessID and AccessKey of the current user

Address:[Security information management](#)

3. Use the command line tool

```
aliyunlog log get_log_all --project="waf-project-1769112740192985-cn-hangzhou" --logstore="waf-logstore" --query="" --from_time="2018-11-04 11:30:31 CST" --to_time="2018-12-04 11:30:31 CST" --region-endpoint="cn-hangzhou.log.aliyuncs.com" --jmes-filter="join('\n', map(&to_string(@), @))" --access-id="【AccessID obtained in step 2】" --access-key="【AccessKey obtained in step 2】" >> /downloaded_data.txt
```

Copy Command

4. Modify the AccessID and AccessKey in the command

After the command is executed, the search result is automatically downloaded to

OK Cancel

All raw log entries recorded by WAF are automatically downloaded and saved to the **download_data.txt** file in the directory where the command is run.

5.9 Grant log query and analysis permissions to a RAM user

If you want to use the WAF log query and analysis service with a RAM user, you must grant required permissions to the RAM user using the Alibaba Cloud account.

Context

The following permissions are required for enabling and using the WAF log query and analysis service.

Operation	Required account type and permissions
Enable Log Service (the service remains enabled after this operation)	Alibaba Cloud account
Authorize WAF to write log data to the exclusive logstore in Log Service in real-time (the authorization remains valid after this operation)	<ul style="list-style-type: none"> Alibaba Cloud account RAM user that has the <code>AliyunLogFullAccess</code> permission RAM user that has specific permissions
Use the log query and analysis service	<ul style="list-style-type: none"> Alibaba Cloud account RAM user that has the <code>AliyunLogFullAccess</code> permission RAM user that has specific permissions

Grant permissions to RAM users as required.

Scenario	Permission	Procedure
Grant permissions on all Log Service operations to a RAM user.	<code>AliyunLogFullAccess</code>	For more information, see RAM users .
Grant the log viewing permission to a RAM user after you enable the WAF log query and analysis service and complete the authorization on the Alibaba Cloud account.	<code>AliyunLogReadOnlyAccess</code>	For more information, see RAM users .
Grant the RAM user permissions on enabling and using the WAF log query and analysis service. This RAM user is not granted other administrative permissions on Log Service.	Custom authorization policy	For more information, see the following procedure.

Procedure

1. Log on to the [RAM console](#).
2. On the **Policies** page, select the **Custom Policy** tab.
3. In the upper-right corner of the page, click **Create Authorization Policy**.

4. Click **Create Authorization Policy**. In the template, specify the **Authorization Policy Name**, and then enter the following in the **Policy Content** field.

**Note:**

Replace `${Project}` and `${Logstore}` in the following policy content with the names of the exclusive project and logstore in WAF Log Service.

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": "log:GetProject",
      "Resource": "acs:log:*:*:project/${Project}",
      "Effect": "Allow"
    },
    {
      "Action": "log:CreateProject",
      "Resource": "acs:log:*:*:project/*",
      "Effect": "Allow"
    },
    {
      "Action": "log:ListLogStores",
      "Resource": "acs:log:*:*:project/${Project}/logstore/*",
      "Effect": "Allow"
    },
    {
      "Action": "log:CreateLogStore",
      "Resource": "acs:log:*:*:project/${Project}/logstore/*",
      "Effect": "Allow"
    },
    {
      "Action": "log:GetIndex",
      "Resource": "acs:log:*:*:project/${Project}/logstore/${Logstore}",
      "Effect": "Allow"
    },
    {
      "Action": "log:CreateIndex",
      "Resource": "acs:log:*:*:project/${Project}/logstore/${Logstore}",
      "Effect": "Allow"
    },
    {
      "Action": "log:UpdateIndex",
      "Resource": "acs:log:*:*:project/${Project}/logstore/${Logstore}",
      "Effect": "Allow"
    },
    {
      "Action": "log:CreateDashboard",
      "Resource": "acs:log:*:*:project/${Project}/dashboard/*",
      "Effect": "Allow"
    },
    {
      "Action": "log:UpdateDashboard",
      "Resource": "acs:log:*:*:project/${Project}/dashboard/*",
      "Effect": "Allow"
    }
  ]
}
```

```

    },
    {
      "Action": "log:CreateSavedSearch",
      "Resource": "acs:log:*:*:project/${Project}/savedsearch/*",
      "Effect": "Allow"
    },
    {
      "Action": "log:UpdateSavedSearch",
      "Resource": "acs:log:*:*:project/${Project}/savedsearch/*",
      "Effect": "Allow"
    }
  ]
}

```

5. Click **Create Authorization Policy**.
6. Go to the **Users** page, find the RAM user, and then click **Authorize**.
7. Add the authorization policy that you created and click **OK**.

This RAM user can enable and use the WAF log query and analysis service, and cannot use other features of Log Service.

5.10 Manage log storage

After WAF Log Service is activated, log storage is allocated for your WAF Log Service based on the specified log storage size. You can view the usage of the log storage on the **Log Service** page in the Web Application Firewall console.

View the usage of the log storage

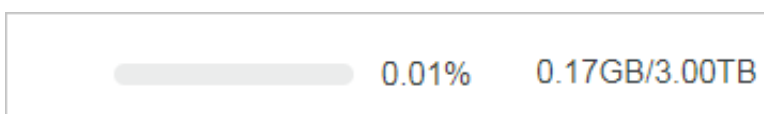
You can view the usage of the log storage that is generated by the WAF log query and analysis service at any time.



Note:

It takes two hours for changes in the storage usage to be updated in the console. You need to upgrade the log storage when only a little log storage space is available.

1. Log on to the [Web Application Firewall console](#).
2. Choose **App Market > App Management**, select the region where your WAF instance is located, and then click Real-time Log Query and Analysis Service.
3. At the top of the **Log Service** page, view the usage of log storage.



Upgrade log storage

To upgrade the log storage size, click **Upgrade Storage** at the top of the **Log Service** page.



Note:

If log storage is full, new log data cannot be written to the exclusive logstore. We recommend that you upgrade log storage before log storage is full.

Clear log storage

You can delete all log entries in the log storage as needed. For example, you can delete the log entries generated during the test phase to make full use of the log storage by recording only log entries that is generated during the production phase.

Click **Clear** at the top of the **Log Service** page, and click Confirm to delete all log entries in the log storage.



Note:

Log entries that are deleted cannot be restored. Delete log entries with caution.



Note:

You can clear the log storage for only a limited number of times.