ALIBABA CLOUD

Alibaba Cloud

Web应用防火墙

Protection Lab

Document Version: 20220110

Alibaba Cloud

Legal disclaimer

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

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

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

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

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

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

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

Document conventions

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

Table of Contents

1.Configure account security

Web Application Firewall (WAF) supports the account security feature. The feature allows you to monitor user authentication-related endpoints, such as the endpoints used for registration and logon. The feature also allows you to detect account security events that may threaten user credentials. The events include dictionary attacks, brute-force attacks, spam user registration, weak password sniffing, and SMS flood attacks. This topic describes how to configure an account security rule and view account security reports.

Prerequisites

- A WAF instance of the **Pro** edition or higher is purchased. For more information, see Purchase a WAF instance.
- Your website is added to WAF. For more information, see Add a website.

Background information

Before you enable the account security feature, you must obtain the endpoint information that is required for configurations. The information includes the domain name, the URI to which user credentials are submitted, and the parameters that specify the username and password. Each WAF instance allows you to enable the account security feature for a maximum of three endpoints.

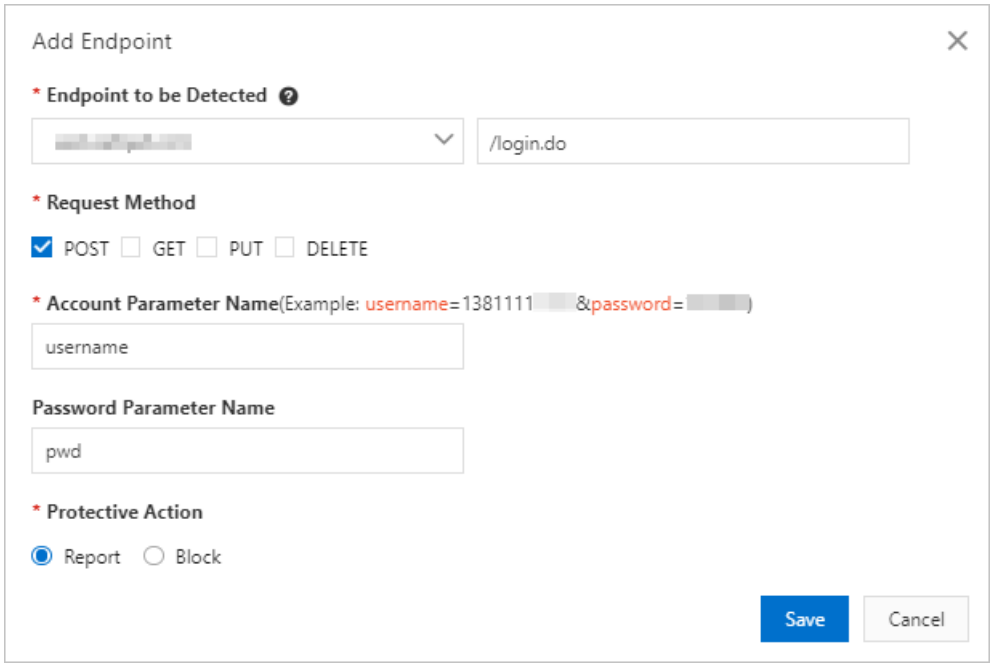
Add an endpoint

1. Log on to the Web Application Firewall console.
2. In the top navigation bar, select the resource group and region to which the WAF instance belongs. The region can be **Mainland China** or **International**.
3. In the left-side navigation pane, choose **Protection Lab > Account Security**.
4. On the **Account Security** page, click **Add Endpoint**.

   If this is the first time you go to the **Account Security** page, skip this step.

   > **Note** Each WAF instance allows you to enable the account security feature for a maximum of three endpoints. If three endpoints are added, **Add Endpoint** is dimmed.

5. Configure the parameters and click **Save**.



Parameter	Description
Endpoint to be Detected	Select the domain name for which you want to enable the account security feature. Then, enter the URI to which user credentials are submitted. Do not enter the URI of the logon page. For example, do not enter `/login.html`. Instead, enter the URI to which the username and password are submitted. **Note** If you have enabled the asset discovery feature of WAF and added the selected domain name to WAF, all the URIs that belong to the domain name are automatically listed. Select a URI from the drop-down list. For more information, see Asset discovery.
Request Method	Select the request method for the endpoint. Valid values: **POST**, **GET**, **PUT**, and **DELETE**.
Account Parameter Name	Enter the username.
Password Parameter Name	Enter the password. If passwords are not required to access the endpoint, you do not need to configure this parameter.
Protective Action	Select the action to manage requests that compromise account security. Valid values: ○ **Report** ○ **Block**

Configuration examples:

- Example 1: If the URI of the logon page is `/login.do` and the body of the POST request is `username=Jammy&pwd=123456`, set the **Account Parameter Name** parameter to `username` and

the **Password Parameter Name** parameter to `pwd`.

- Example 2: If the parameters that specify user credentials are included in the URI of a GET request, such as `/login.do?username=Jammy&pwd=123456`, set the **Request Method** parameter to **GET**. Keep other settings the same as those in Example 1.
- Example 3: If passwords are not required to access the endpoint, such as a registration endpoint, configure the **Account Parameter Name** parameter. You do not need to configure the **Password Parameter Name** parameter.
- Example 4: If a mobile number is required to access the endpoint, enter the mobile number for the account parameter. For example, the URI is `/sendsms.do?mobile=1381111****`. In this example, set the **Endpoint to be Detected** parameter to `/sendsms.do` and the **Account Parameter Name** parameter to `mobile`. You do not need to configure the **Password Parameter Name** parameter.

After you add the endpoint, WAF automatically dispatches detection tasks. If the network traffic of the endpoint meets the account security rule, account security events are reported within a few hours.

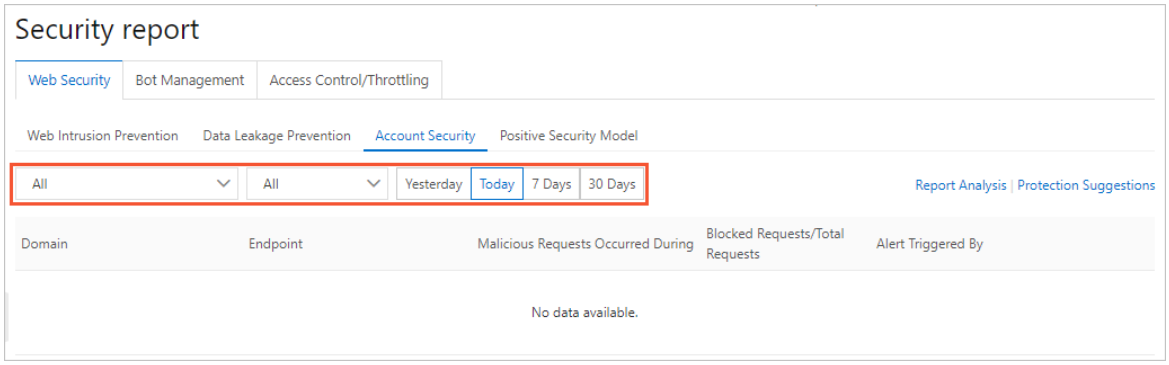
> **Note** After you enable the account security feature, all requests that are destined for your website are checked by using the account security rule. You can configure a whitelist to allow the requests that meet the account security rule to bypass the check. For more information, see Configure a whitelist for Data Security.

View account security reports

If you want to view account security reports, find the endpoint on the **Account Security** page, and click **View Report** in the Actions column. You can also view account security reports on the **Security Report** page.

The following procedure describes how to view account security reports on the **Security Report** page.

1. Log on to the Web Application Firewall console.
2. In the top navigation bar, select the resource group and region to which the WAF instance belongs. The region can be **Mainland China** or **International**.
3. In the left-side navigation pane, click **Security Report**.
4. On the **Web Security** tab, click **Account Security** and select the domain name, URI, and time range for which you want to check account security events. You can select **Yesterday**, **Today**, **7 Days**, or **30 Days** for the time range.



The following table describes the fields in an account security report.

Field	Description
Endpoint	The URI for which account security events are detected.
Domain	The domain name to which the URI belongs.
Malicious Requests Occurred During	The time range during which account security events are detected.
Blocked Requests	The number of requests that are blocked based on WAF protection rules during the time range displayed in the **Malicious Requests Occurred During** field. The WAF protection rules refer to the effective rules of different protection modules, such as the Protection Rules Engine, custom protection policy (ACL), HTTP flood protection, and region blacklist. The proportion of blocked requests indicates the account security status of the endpoint.
Total Requests	The total number of requests that are sent to the endpoint during the time range displayed in the **Malicious Requests Occurred During** field.
Alert Triggered By	The reason why the alert is triggered. The following list describes the possible reasons: ◦ A request fits the behavior model of dictionary attacks or brute-force attacks. ◦ The traffic baseline of the endpoint is abnormal during the specified time range. ◦ A large number of requests that are sent to the endpoint match the rules that are described in the threat intelligence library during the specified time range. ◦ Weak passwords are detected in a large number of requests that are sent to the endpoint during the specified time range. In this case, dictionary attacks and brute-force attacks may occur.

References

The account security feature only detects account risks. We recommend that you select suitable solutions based on your business requirements to safeguard your business. For more information, see Account security best practices.