

AWS WAF Managed Rules
"Rule Group Exceptions" Manual
Ver 1.0

Table of Contents

1. [Overview](#)
2. [Requirements](#)
3. [How to Enable "Rule Group Exceptions" Function](#)
4. [Using "Rule Group Exceptions" Function](#)
 - 4.1. [How to Check the Managed Rules List and Exception Setting Status](#)
 - 4.2. [How to Change the Action of Entire/Individual Rules of Managed Rules](#)
 - 4.3. [How to Check the Status of Operation of Action Change](#)
5. [Appendix](#)
 - 5.1. [Available Operations on the Managed Rules page](#)
 - 5.2. [Action Override](#)
 - 5.3. [Action](#)
 - 5.4. [Task](#)
 - 5.5. [Status](#)

1. Overview

AWS WAF Managed Rules "Rule Group Exceptions" function setting can be easily set on WafCharm management console, without accessing the AWS management console.

- What is "Rule Group Exceptions" function?
This function allows you to switch individual rules in AWS WAF Managed Rules to COUNT / BLOCK mode.
- What are AWS WAF Managed Rules?
It is a set of rules consisting of large number of rules, which can be purchased on AWS Marketplace. Please refer to the following link for more info on the rules provided by AWS Marketplace Sellers.
<https://aws.amazon.com/marketplace/solutions/security/waf-managed-rules>

2. Requirements

The following settings are required to start using Rule Group Exceptions function in WafCharm.

- 2.1 Subscribe to the Managed Rules provided by CSC from the following link.
[Cyber Security Cloud Managed Rules for AWS WAF -HighSecurity OWASP Set-](#)
- 2.2 Apply the above Managed Rules in the Web ACL registered to WafCharm.
- 2.3 Users on "Entry Plan" can not use WafCharm's rule group exception function.
You need to subscribe to "Business Plan" or above.

3. How to Enable "Rule Group Exceptions" Function

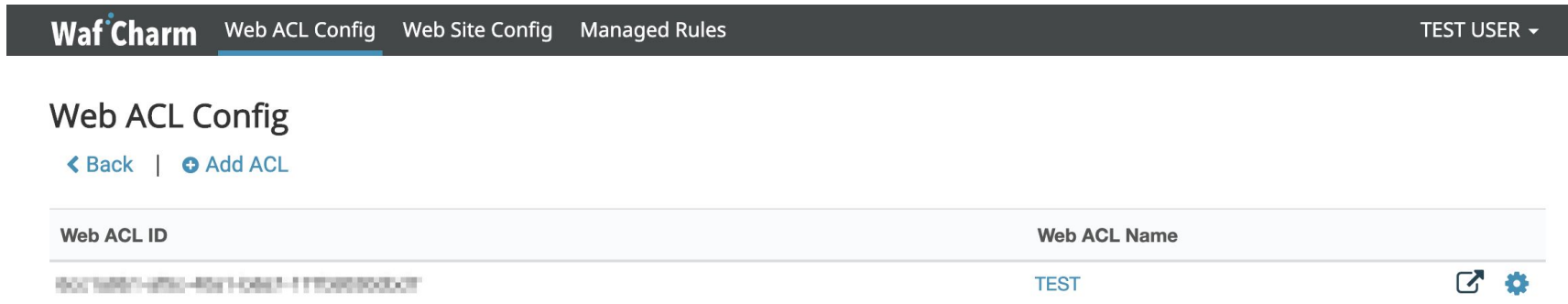
3.1 Web ACL Config Setting

3.1.1 Log in to WafCharm management console.

3.1.2 Open the Web ACL Config screen to which Managed Rules are applied.

3.1.3 Please refer to the following blog if you have not completed Web ACL Config registration.

[WafCharm Initial Setting Manual](#)



The screenshot displays the WafCharm management console interface. At the top, a dark navigation bar contains the WafCharm logo and menu items: Web ACL Config (highlighted), Web Site Config, and Managed Rules. On the right side of the navigation bar, it shows 'TEST USER' with a dropdown arrow. Below the navigation bar, the main content area is titled 'Web ACL Config'. Underneath the title, there are two links: '< Back' and '+ Add ACL'. A table below lists the Web ACL configurations. The table has two columns: 'Web ACL ID' and 'Web ACL Name'. The first row shows a long alphanumeric ID and the name 'TEST'. To the right of the 'TEST' name, there are two icons: a share icon and a gear icon.

Web ACL ID	Web ACL Name
860274857-4756-4547-0487-117098000007	TEST

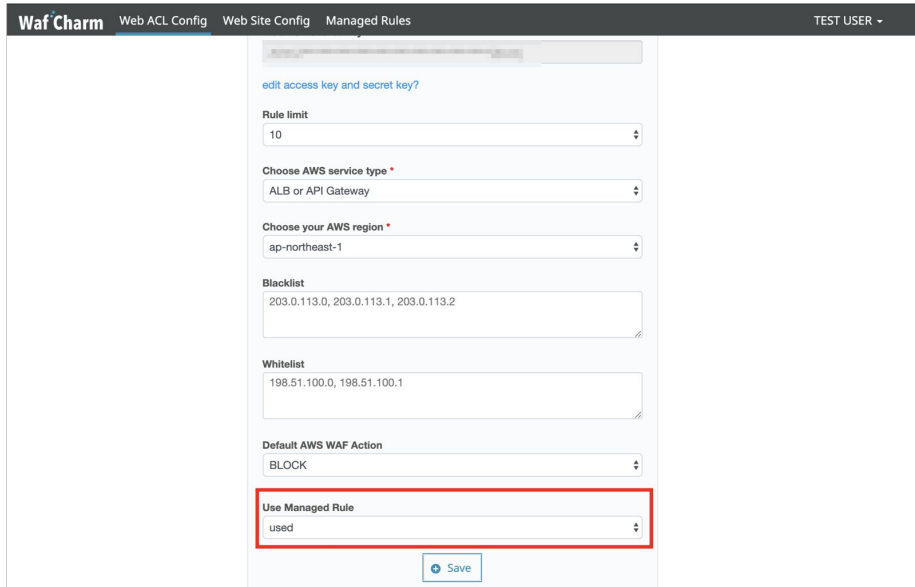
3.2 Enabling "Rule Group Exceptions" Function

3.2.1 Open the Edit screen of Web ACL Config.

3.2.2 Change "Use Managed Rule" from "unused" to "used".

3.2.3 Click "Save".

*Settings can be changed at any time.



The screenshot shows the Waf Charm interface with the following configuration details:

- Waf Charm** | Web ACL Config | Web Site Config | Managed Rules | TEST USER
- edit access key and secret key?
- Rule limit**: 10
- Choose AWS service type**: ALB or API Gateway
- Choose your AWS region**: ap-northeast-1
- Blacklist**: 203.0.113.0, 203.0.113.1, 203.0.113.2
- Whitelist**: 198.51.100.0, 198.51.100.1
- Default AWS WAF Action**: BLOCK
- Use Managed Rule**: used (highlighted with a red box)
- Save** button

Enabled "Rule Group Exceptions" Function

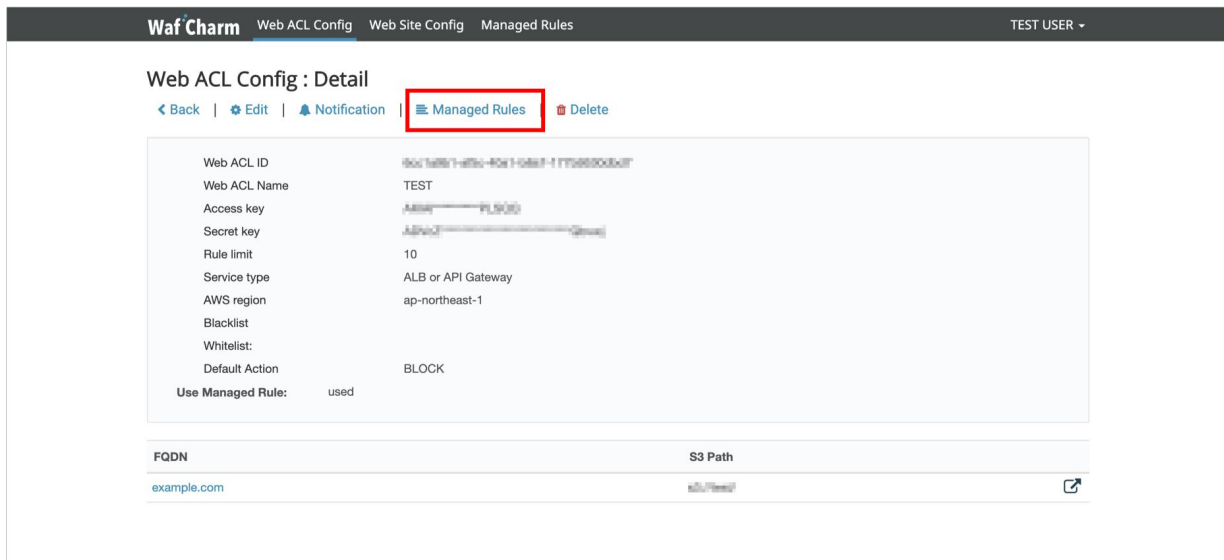
The rule group exception function is now ready to use.

4. Using "Rule Group Exceptions" Function

4.1 How to Check the Managed Rules List and Exception Setting Status

4.1.1 Switch to Managed Rules screen

Switch to Managed Rules screen by clicking "Managed Rules".



The screenshot shows the Waf Charm interface with the 'Managed Rules' tab selected. The 'Managed Rules' link in the navigation bar is highlighted with a red box. The main content area displays the configuration details for a Web ACL named 'TEST'.

Property	Value
Web ACL ID	50c7a8b1-4f5c-40d1-0d87-17709000b0f7
Web ACL Name	TEST
Access key	AKIAI4478143260247L5UJLQ
Secret key	AKIAI4478143260247L5UJLQ
Rule limit	10
Service type	ALB or API Gateway
AWS region	ap-northeast-1
Blacklist	
Whitelist	
Default Action	BLOCK
Use Managed Rule:	used

FQDN	S3 Path
example.com	s3://test/

4.1 How to Check the Managed Rules List and Exception Setting Status

4.1.2 Managed Rules Screen

On the following screen, you can check the list of rules in Managed Rules.

For details on links inside the yellow box below, please refer to the appendix.

[\(Available Operations on the Managed Rules page\)](#)

*For the first time users of Rule Group Exceptions function, the "Action Override" status in the red box below is "Checking". Since it is checking the status of our Managed Rules applied to your AWS WAF, please wait until the status is reflected. (About 10 minutes)

WafCharm Web ACL Config Web Site Config Managed Rules TEST USER ▾

Managed Rules

Web ACLs > Web ACL: TEST

[Edit](#) [Waiting Tasks](#) [Completed Tasks](#) [Refresh Status](#)

Rule Group Section

Managed Rule Group Name	Action Override
Cyber Security Cloud Managed Rules for AWS WAF -HighSecurity OWASP Set-	Checking

Individual Rules Section

No	Rule Id	Name	Attack Type	Field Type	Action Override	Action
1	804646-048-470442-1417044444-78	bad_useragent-header-001	bad_useragent	header	No	🛑 BLOCK
2	444444-1183-4800-4042-444444444444	bad_useragent-header-002	bad_useragent	header	No	🛑 BLOCK

4.1 How to Check the Managed Rules List and Exception Setting Status

4.1.3 Managed Rules Screen (After confirming the status of our Managed Rules)

You can check the status of our managed rules applied to your AWS WAF in the following screen. After confirming the status of our Managed Rules applied to your AWS WAF, the current status will be reflected in "Action Override" in the red box as shown below.

Waf Charm Web ACL Config Web Site Config Managed Rules TEST USER ▾

Managed Rules

Web ACLs > Web ACL: TEST

[Edit](#) [Waiting Tasks](#) [Completed Tasks](#) [Refresh Status](#)

Rule Group Section

Managed Rule Group Name	Action Override
Cyber Security Cloud Managed Rules for AWS WAF -HighSecurity OWASP Set-	No override

Individual Rules Section

No	Rule Id	Name	Attack Type	Field Type	Action Override	Action
1	arn:aws:wafv2:us-east-1:123456789012:rulegroup/rg-012345678901	bad_useragent-header-001	bad_useragent	header	No	⊞ BLOCK
2	arn:aws:wafv2:us-east-1:123456789012:rulegroup/rg-012345678901	bad_useragent-header-002	bad_useragent	header	No	⊞ BLOCK

4.1 How to Check the Managed Rules List and Exception Setting Status

4.1.4 AWS WAF status on AWS Management Console

You can check the state of "Action" on AWS Management Console as shown below, and confirm that it matches the one on the Managed Rules screen.

The screenshot displays the AWS Management Console interface for configuring a Web ACL. The left sidebar shows the navigation menu with 'Web ACLs' selected. The main content area is split into two panels. The left panel, titled 'Web ACLs', shows a list of Web ACLs with a filter set to 'Asia Pacific (Tokyo)'. The right panel, titled 'Rules', shows a table of rules with columns for Order, Rule, Type, and Action. A red box highlights the rule 'Cyber Security Cloud Managed Rules for AWS WAF - HighSecurity OWASP Set-' with a 'No override' action. Below the table, there is a section for 'Default action' and a section for 'The following rules within the rule group will be overridden to count'.

Order	Rule	Type	Action
1	[Redacted]	Regular	Count requests
2	[Redacted]	Regular	Count requests
3	[Redacted]	Regular	Count requests
4	[Redacted]	Regular	Count requests
5	[Redacted]	Regular	Count requests
6	Cyber Security Cloud Managed Rules for AWS WAF - HighSecurity OWASP Set-	Group	No override

Rule group name	Status
Cyber Security Cloud Managed Rules for AWS WAF - HighSecurity OWASP Set-	0 rule(s) excluded

4.2 How to Change the Action of Entire/Individual Rules of Managed Rules

4.2.1 Changing the Action (Edit Screen)

Click "Action" in the "Action Override" rules section & click "Update".

- In case of BLOCK, set "Action Override" to "No"
- In case of COUNT, set "Action Override" to "to Count"

- * It takes about 10 minutes to reflect the setting.
- * The Managed Rules screen on the right does not show all the rules in our Managed Rules, but is a pick-up of rules that is considered better controlled by the user.
- * If you would like us to change some sort of rule's action other than the right rules, please let [us](#) know.

The screenshot shows the 'Managed Rules' interface in WebCharm. At the top, there are navigation tabs: 'Web ACL Config', 'Web Site Config', and 'Managed Rules'. Below this, there's a section for 'Managed Rules' with a breadcrumb 'Web ACL > Web ACL TEST' and links for 'Edit', 'Waiting Tasks', 'Completed Tasks', and 'Refresh Status'. A 'Rule Group Section' is visible, showing 'Managed Rule Group Name' as 'Cyber Security Cloud Managed Rules for AWS WAF - HighSecurity OWASP Set' and an 'Action Override' dropdown set to 'No'. The main part of the screen is a table of 'Individual Rule Section' with columns: 'No', 'Rule Id', 'Rule Name', 'Attack Type', 'Field Type', 'Action Override', and 'Action'. The 'Action Override' column contains dropdown menus, and the 'Action' column contains icons for different actions like 'BLOCK' and 'COUNT'. A red box highlights the 'Action Override' dropdown for rule 1, which is set to 'to Count'. Another red box highlights the 'Update' button at the bottom right of the table.

No	Rule Id	Rule Name	Attack Type	Field Type	Action Override	Action
1	v183a29-248-4283-8213-88730443a78	bad_useragent-header-001	SQL_Compromised	Header	to Count	⬇️ COUNT
2	v5a23279-37182-4939-4971-322541912428	bad_useragent-header-002	SQL_Compromised	Header	to Count	⬇️ COUNT
3	8a6e6e6e-652-2441-4732-244782783a3a	cookie-qp-001	COOKIE	Body	No	⊖ BLOCK
4	93154989-2311-4498-4970-29202899823	cookie-qp-001	COOKIE	QP	No	⊖ BLOCK
5	821674a6-3141-4a43-4a43-4a434a434a43	dupcal-multi-001	SQL_INJECT	MULTI	No	⊖ BLOCK
6	00981748-2343-4232-4970-71920712087	dupcal-multi-002	SQL_INJECT	MULTI	No	⊖ BLOCK
7	4218103a-e163-4388-4341-47111e4a4a47	joorls-ur-001	SQL_INJECT	URI	No	⊖ BLOCK
8	21920207-1322-4718-4a43-148992024a48	joorls-ur-001	SQL_INJECT	URI	No	⊖ BLOCK
9	a77a1a4a-1648-4882-4882-4882770a48870a	noop-body-001	SQL_INJECT	Body	No	⊖ BLOCK
10	8234432a-1422-4238-4238-42387950049493	noop-qp-001	SQL_INJECT	QP	No	⊖ BLOCK
11	8a1a1a1a-1234-4321-4321-432143214321	oracle-multi-001	SQL_INJECT	MULTI	No	⊖ BLOCK
12	078a1a1a-0782-4321-4321-432107820782	oscommand-body-001	OS_COMMAND	Body	No	⊖ BLOCK
13	8a1a1a1a-8a1a-4321-4321-43218a1a1a1a	oscommand-qp-001	OS_COMMAND	QP	No	⊖ BLOCK
14	811a1a1a-811a-4321-4321-4321811a1a1a	pathtraversal-body-001	PATH_TRAVERSAL	Body	No	⊖ BLOCK
15	8a1a1a1a-8a1a-4321-4321-43218a1a1a1a	pathtraversal-qp-001	PATH_TRAVERSAL	QP	No	⊖ BLOCK
16	8a1a1a1a-8a1a-4321-4321-43218a1a1a1a	pathtraversal-ur-001	PATH_TRAVERSAL	URI	No	⊖ BLOCK
17	8a1a1a1a-8a1a-4321-4321-43218a1a1a1a	sql-body-001	SQL	Body	No	⊖ BLOCK
18	8a1a1a1a-8a1a-4321-4321-43218a1a1a1a	sql-body-002	SQL	Body	No	⊖ BLOCK
19	8a1a1a1a-8a1a-4321-4321-43218a1a1a1a	sql-qp-001	SQL	QP	No	⊖ BLOCK
20	8a1a1a1a-8a1a-4321-4321-43218a1a1a1a	sql-qp-002	SQL	QP	No	⊖ BLOCK
21	8a1a1a1a-8a1a-4321-4321-43218a1a1a1a	sql-ur-001	SQL	URI	No	⊖ BLOCK
22	8a1a1a1a-8a1a-4321-4321-43218a1a1a1a	stuts-multi-001	SQL_INJECT	MULTI	No	⊖ BLOCK
23	8a1a1a1a-8a1a-4321-4321-43218a1a1a1a	stuts-multi-002	SQL_INJECT	MULTI	No	⊖ BLOCK
24	8a1a1a1a-8a1a-4321-4321-43218a1a1a1a	stuts-multi-003	SQL_INJECT	MULTI	No	⊖ BLOCK
25	8a1a1a1a-8a1a-4321-4321-43218a1a1a1a	suspicious_access-ur-001	SUSPICIOUS_ACCESS	URI	No	⊖ BLOCK
26	8a1a1a1a-8a1a-4321-4321-43218a1a1a1a	suspicious_access-ur-002	SUSPICIOUS_ACCESS	URI	No	⊖ BLOCK
27	8a1a1a1a-8a1a-4321-4321-43218a1a1a1a	suspicious_access-ur-003	SUSPICIOUS_ACCESS	URI	No	⊖ BLOCK
28	8a1a1a1a-8a1a-4321-4321-43218a1a1a1a	tomcat-multi-001	SQL_INJECT	MULTI	No	⊖ BLOCK
29	8a1a1a1a-8a1a-4321-4321-43218a1a1a1a	xss-body-001	XSS	Body	No	⊖ BLOCK
30	8a1a1a1a-8a1a-4321-4321-43218a1a1a1a	xss-qp-001	XSS	QP	No	⊖ BLOCK
31	8a1a1a1a-8a1a-4321-4321-43218a1a1a1a	xss-ur-001	XSS	URI	No	⊖ BLOCK
32	8a1a1a1a-8a1a-4321-4321-43218a1a1a1a	xss-ur-001	XSS	URI	No	⊖ BLOCK
33	8a1a1a1a-8a1a-4321-4321-43218a1a1a1a	rails-header-001	SQL	Header	No	⊖ BLOCK

4.2 How to Change the Action of Entire/Individual Rules of Managed Rules

4.2.2 Checking the Status on Managed Rules Screen

After changing the "Action" of our Managed Rules on the AWS Management Console, it takes about 10 minutes to reflect it on the Managed Rules screen below.

WafCharm [Web ACL Config](#) [Web Site Config](#) [Managed Rules](#) TEST USER ▾

Managed Rules

[Web ACLs](#) > [Web ACL: TEST](#)

[Edit](#) [Waiting Tasks](#) [Completed Tasks](#) [Refresh Status](#)

Rule Group Section

Managed Rule Group Name	Action Override
Cyber Security Cloud Managed Rules for AWS WAF -HighSecurity OWASP Set-	No override

Individual Rules Section

No	Rule Id	Name	Attack Type	Field Type	Action Override	Action
1	arn:aws:wafv2:us-east-1:123456789012:managed-rule-groups/123456789012/bad-useragent-header-001	bad_useragent-header-001	bad_useragent	header	to Count	📊 COUNT
2	arn:aws:wafv2:us-east-1:123456789012:managed-rule-groups/123456789012/bad-useragent-header-002	bad_useragent-header-002	bad_useragent	header	to Count	📊 COUNT
3	arn:aws:wafv2:us-east-1:123456789012:managed-rule-groups/123456789012/cookie-body-001	cookie-body-001	cookie	body	No	🚫 BLOCK
4	arn:aws:wafv2:us-east-1:123456789012:managed-rule-groups/123456789012/cookie-qs-001	cookie-qs-001	cookie	qs	No	🚫 BLOCK

4.2 How to Change the Action of Entire/Individual Rules of Managed Rules

4.2.3 AWS Management Console Status

You can also confirm the result of "Action" change on the AWS Management Console. The AWS Management Console reflects the rules that you want to be in COUNT mode in Managed Rules. (Please refer to the red box below)

The screenshot shows the AWS Management Console interface for configuring Web ACLs. The left sidebar contains navigation options for AWS WAF, AWS Shield, and AWS FMS. The main content area is titled 'Web ACLs' and includes a 'Filter' dropdown set to 'Asia Pacific (Tokyo)'. Below the filter is a list of rules, with one rule selected. The right-hand pane shows the configuration for the selected rule, including a table of rules and a summary of the rule group's status.

Order	Rule	Type	Action
1	[Redacted]	Regular	Count requests
2	[Redacted]	Regular	Count requests
3	[Redacted]	Regular	Count requests
4	[Redacted]	Regular	Count requests
5	[Redacted]	Regular	Count requests
6	Cyber Security Cloud Managed Rules for AWS WAF - HighSecurity OWASP Set-	Group	No override

Rule group name	Status
Cyber Security Cloud Managed Rules for AWS WAF - HighSecurity OWASP Set-	2 rule(s) excluded

4.3 How to Check the Status of Operation of Action Change

4.3.1 Checking the status of operation

By clicking the "Waiting Tasks", you can check the current status of pending tasks.

Waiting Tasks Screen

Waf Charm [Web ACL Config](#) [Web Site Config](#) [Managed Rules](#) TEST USER ▾

Managed Rules

[Web ACLs](#) > [Web ACL: TEST](#)

[Edit](#) [Waiting Tasks](#) [Completed Tasks](#) [Refresh Status](#)

Target	Rule ID	Name	Task	Status	Accepted
Group		Cyber Security Cloud Managed Rules for AWS WAF -HighSecurity OWASP Set-	Refresh Status	Waiting	2019-06-05 10:20:57 +0900

4.3 How to Check the Status of Operation of Action Change

4.3.2 Operation Completion Status Confirmation

By clicking the "Completed Tasks", you can confirm the status of completed tasks.

Completed Tasks Screen

WafCharm Web ACL Config Web Site Config Managed Rules TEST USER ▾

Managed Rules

Web ACLs > Web ACL: TEST

[Edit](#) [Waiting Tasks](#) [Completed Tasks](#) [Refresh Status](#)

Target	Rule ID	Name	Task	Status	Accepted	Completed
Rule	11904489-0001-4000-8010-407804000170	bad_useragent-header-001	Update to Override to Count	Success	2019-06-05 12:07:45 +0900	2019-06-05
Rule	11904489-0001-4000-8010-407804000170	bad_useragent-header-002	Update to Override to Count	Success	2019-06-05 12:07:45 +0900	2019-06-05

Using "Rule Group Exceptions" Function

That's it on how to use the rule group exceptions function.

5. Appendix

5.1 Available Operations on the Managed Rules Page

Detailed explanation of the following menu provided on the Managed Rules page.



Managed Rules

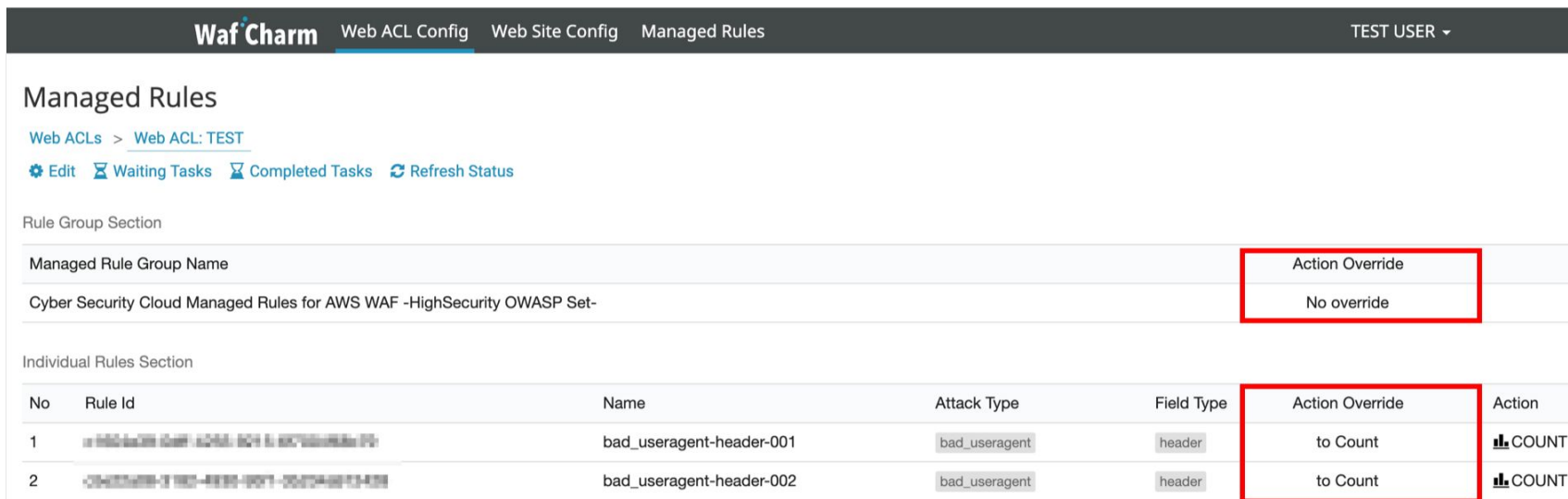
[Web ACLs](#) > [Web ACL: TEST](#)

[Edit](#) [Waiting Tasks](#) [Completed Tasks](#) [Refresh Status](#)

Title	Role
Edit	Used to change the "Action" of individual or entire rules of Managed Rules.
Waiting Tasks	You can check the list of currently pending tasks.
Completed Tasks	You can check the list of completed tasks.
Refresh Status	Used to match the status with our Managed Rules on the AWS Management Console. If you change the "Action" of our Managed Rules on the AWS Management Console side, please click here to match the status.

5.2 Action Override

Detailed explanation of "Action Override" in "Rule Group Section" and "Individual Rules Section".



The screenshot displays the Waf Charm interface. At the top, there is a navigation bar with "Waf Charm" on the left and "Web ACL Config", "Web Site Config", and "Managed Rules" in the center. On the right side of the navigation bar, it says "TEST USER" with a dropdown arrow. Below the navigation bar, the main content area is titled "Managed Rules". Underneath this title, there is a breadcrumb "Web ACLs > Web ACL: TEST" and a row of action buttons: "Edit", "Waiting Tasks", "Completed Tasks", and "Refresh Status".

The interface is divided into two sections:

- Rule Group Section:** This section contains a table with two columns: "Managed Rule Group Name" and "Action Override". The first row shows "Cyber Security Cloud Managed Rules for AWS WAF -HighSecurity OWASP Set-" and "No override". The "Action Override" cell in this row is highlighted with a red border.
- Individual Rules Section:** This section contains a table with columns: "No", "Rule Id", "Name", "Attack Type", "Field Type", "Action Override", and "Action". There are two rows of data. The first row has "1" in the "No" column, a rule ID, "bad_useragent-header-001" in the "Name" column, "bad_useragent" in the "Attack Type" column, "header" in the "Field Type" column, "to Count" in the "Action Override" column, and "COUNT" in the "Action" column. The second row has "2" in the "No" column, a rule ID, "bad_useragent-header-002" in the "Name" column, "bad_useragent" in the "Attack Type" column, "header" in the "Field Type" column, "to Count" in the "Action Override" column, and "COUNT" in the "Action" column. The "Action Override" cells in both rows of this section are highlighted with a red border.

5.2.1 About "Action Override" in Rule Group Section

- The Rule Group Section allows you to set the action of the entire Managed Rules.
 - The following actions can be selected.

Action Override	Action when detected
No override	BLOCK
Override to count	COUNT

5.2.2 About "Action Override" in Individual Rules Section

- The Individual Rules Section allows you to set the action of individual rules.
 - The following actions can be selected.

Action Override	Action when detected
No	BLOCK
to Count	COUNT

5.3.1 Action Override Combination Pattern

Example: If you select "Override to count" for the "Action Override" in the Rule Group Section, the "Action" will be "COUNT", even if the "Action" of Individual Rules Section is set to "No".

Rule Group Section Action Override	Individual Rules Section Action Override	Action
No override	No	BLOCK
No override	to Count	COUNT
Override to count	No	COUNT
Override to count	to Count	COUNT

5.4 Task

When you update “Action Override”, WafCharm executes instructions to AWS WAF asynchronously as “Task”, so you can check the execution status in the red box below.

WafCharm			Web ACL Config	Web Site Config	Managed Rules	TEST USER ▾		
Managed Rules								
Web ACLs > Web ACL: TEST								
Edit Waiting Tasks Completed Tasks Refresh Status								
Target	Rule ID	Name	Task	Status	Accepted	Completed		
Rule	arn:aws:wafv2:us-east-1:123456789012:webacl/TEST/arn:aws:wafv2:us-east-1:123456789012:webacl/TEST/bad_useragent-header-001	bad_useragent-header-001	Update to Override to Count	Success	2019-06-05 12:07:45 +0900	2019-06-05		
Rule	arn:aws:wafv2:us-east-1:123456789012:webacl/TEST/arn:aws:wafv2:us-east-1:123456789012:webacl/TEST/bad_useragent-header-002	bad_useragent-header-002	Update to Override to Count	Success	2019-06-05 12:07:45 +0900	2019-06-05		

Task	Details
Update to Override to Count	Change to COUNT mode
Update to No Override	Change to BLOCK mode
Refresh Status	Get Managed Rules Status on AWS Management Console

5.5 Status

The status of the "Task" is shown in the red box below.

WafCharm [Web ACL Config](#) [Web Site Config](#) [Managed Rules](#) TEST USER ▾

Managed Rules

[Web ACLs](#) > [Web ACL: TEST](#)

[Edit](#) [Waiting Tasks](#) [Completed Tasks](#) [Refresh Status](#)

Target	Rule ID	Name	Task	Status	Accepted	Completed
Rule	1504488-001-4250-8175-8788488479	bad_useragent-header-001	Update to Override to Count	Success	2019-06-05 12:07:45 +0900	2019-06-05
Rule	1504488-001-4250-8175-8788488479	bad_useragent-header-002	Update to Override to Count	Success	2019-06-05 12:07:45 +0900	2019-06-05

The "Status" is set according to the processing status. Status types are described on the next page.

5.5.1 Status Type (1/2)

Status	Meaning	Countermeasure
Success	Success	-
Failed(Permission error)	Insufficient permissions	Please refer to the following page for the IAM settings for permissions. https://www.wafcharm.com/en/blog/aws-iam-setting-for-wafcharm/
Failed(Managed Rule not found)	Managed Rules are not attached to the Web ACL.	<ol style="list-style-type: none">1. Make sure that our Managed Rules are attached to the Web ACL.2. Please check the requirements for using it.

5.5.1 Status Type (2/2)

Status	Meaning	Countermeasure
Failed(Unknown error happened)	Failure due to unknown error	<ol style="list-style-type: none">1. Please try again if the Rule Group Exception function can be used.2. If the situation does not improve with Step 1, please contact WafCharm support. wafcharm-support@cscloud.co.jp
Failed(Max retry was over)	Failure due to retry processing reaching its upper limit	<ol style="list-style-type: none">1. Please try again if the Rule Group Exception function can be used.2. If the situation does not improve with Step 1, please contact WafCharm support. wafcharm-support@cscloud.co.jp

For any questions or concerns, please contact WafCharm Support at:

wafcharm-support@cscloud.co.jp

Waf Charm