

# Quick Guide

AIWAF-VE

v5.0.2

# Table of Contents

<b>Overview for AIWAF-VE menu</b>	<b>3</b>
<b>Configuration of AIWAF-VE</b>	<b>4</b>
1. Subscribe AIWAF-VE BYOL or PAYG:	4
2. Access the Web User Interface (UI):	4
3. Register Your License(AIWAF-VE BYOL only):	6
4. Time Zone and Language Setting:	7
5. Update Signature and Geolocation DB:	8
6. Register Protected Web Servers:	9
6-1. Register HTTP Web Servers	9
6-2. Register HTTPS Web Servers	12
6-3. Apply Policy	16
6-4. Security Policy Block Mode Configuration	17
7. Complete Configuration:	20
<b>Testing AIWAF-VE: Procedure for Test</b>	<b>21</b>
Step 1: Redirect Test Traffic to AIWAF-VE:	21
Step 2: Send Sample Traffic to AIWAF-VE:	21
Step 3: Verify Attack Detection:	22
<b>Contact us</b>	<b>23</b>

## Overview of AIWAF-VE menu

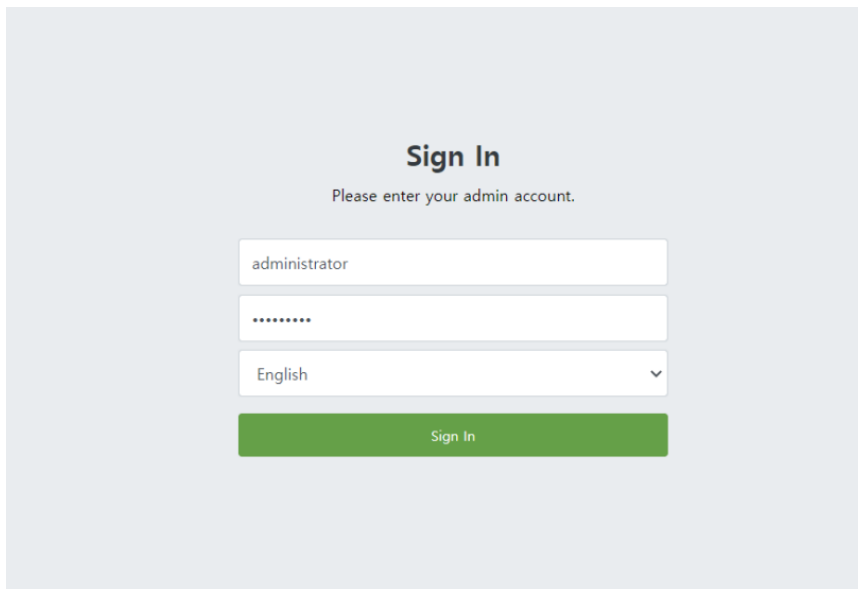
Menu	Description
Monitoring	Provides a centralized visual representation of web traffic, system information, detection counts, detection severity, and the detection log of your web server. It is a user interface that allows users to monitor and analyze real-time or historical data in a concise and easily understandable format.
Log analysis	Provides a platform for analyzing and interpreting detection log, audit log, and web server status log data. This menu is designed to assist users in gaining insights from large volumes of log entries, uncovering meaningful patterns, trends, anomalies, and security-related information.
Report	Generating, viewing, and managing various types of reports (detection log, web traffic, web accelerator, system, and policy settings) that summarize and present information from the registered domain. This menu provides a concise and organized overview of data, metrics, trends, and analysis results.
Policy settings	Configuring and managing the protected web server along with the security policies that govern the behavior of the AIWAF-VE. This menu empowers administrators to configure and fine-tune security policies, determining how the AIWAF-VE detects, prevents, and responds to potential threats targeting web servers.
Configurations	Offers various configurations for AIWAF-VE, including administrator, system, NIC, product settings, log management, and service control.

# Configuration of AIWAF-VE

## 1. Deploy the AIWAF-VE Image:

- Upload the downloaded AIWAF-VE image file (ova, vhd, vmdk) to your preferred environment and boot it up.
- Subscribe to the AIWAF-VE and allocate an instance according to the procedures of your CSP.

## 2. Access the Web User Interface (UI):



- Open your internet browser and access the GUI by entering the assigned IP for the instance as follows: **https://[AIWAF-VE IP]:222**.  
(e.g., if your assigned IP for the instance is 192.168.10.110, the URL is <https://192.168.10.110:222>)
- Please change the language before sign in. (Supported languages: English, Japanese, Korean)
- Login with the provided ID and Password (ID: **administrator**, PW : **\_appleader**)

## APPLICATION INSIGHT WAF

Monitoring | Log analysis | Report | Policy settings | Configurations

Dashboard

You are using the default ID and the default password. Please change ID and password.

### Administrator settings

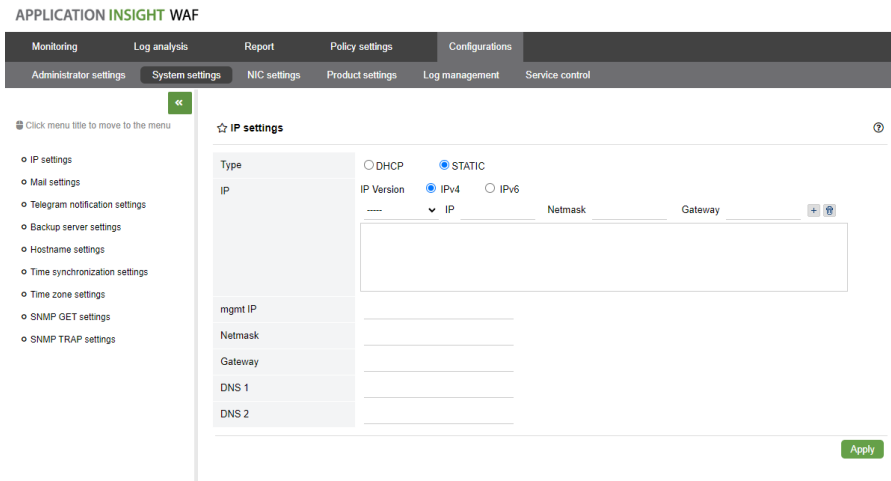
Name	Administrator
ID	administrator
Password	Current password
	New password
	Confirm new password
Password change notification	60 day(s)
Two-Factor Authentication	<input type="radio"/> Use <input checked="" type="radio"/> Not use
Allowed IP	IP <input type="text"/> <input type="button" value="+"/> <input type="button" value="🗑"/>
	<input type="text"/>
Recipient E-mail	E-mail <input type="text"/> <input type="button" value="+"/> <input type="button" value="🗑"/>
	<input type="text"/>
Explanation	<input type="text"/>

Apply

### ! NOTE

- After your first login, please change the **default ID** and **Password** and specify **Allowed access IPs** for the security.
- Password change menu location : Configurations → Administrator settings → click 'Change' button.

## Configure Static IP (Optional):

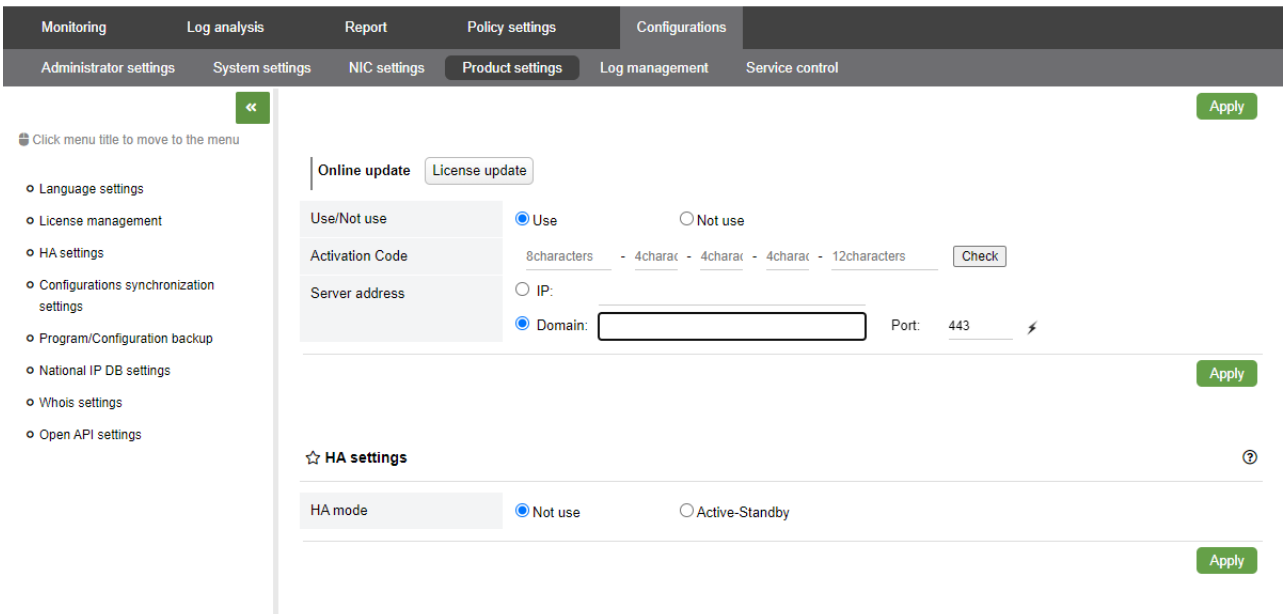


- If you are using a static IP, follow these steps: Go to **Configurations** → **System settings** → **IP settings**. Select 'STATIC,' enter the IP settings and gateway value, click **+**, and then click 'Apply' to complete the process.

## 3. Register Your License (for BYOL only):

\*If you are a PAYG (Pay-As-You-Go) user, you can skip the license installation step since your plan already includes the necessary license.

### APPLICATION INSIGHT WAF



- Access: **Configurations** → **Product settings** → **License management** → **Online update**.
- Choose your online update preference (enable/disable).
- Enter the Activation Code and click 'Check' to validate.
- Click 'Apply' to complete license registration.

## 4. Time Zone and Language Settings:

### APPLICATION INSIGHT WAF

The screenshot shows the 'Configurations' tab in the Application Insight WAF interface. The left sidebar contains a menu with options: IP settings, Mail settings, Telegram notification settings, Backup server settings, Hostname settings, Time synchronization settings, Time zone settings (selected), SNMP GET settings, and SNMP TRAP settings. The main content area is titled 'Time zone settings' and includes a 'Current time' field showing 'Tue Aug 22 8:45:14 KST 2023' and a 'Time zone' dropdown menu set to 'Asia/Seoul'. An 'Apply' button is visible. Below this, the 'SNMP GET settings' section is partially visible, showing 'SNMP MIBs list' and 'Version' options for SNMPv2 (selected) and SNMPv3.

- Time zone Setup: Configurations > System Settings > Time zone Settings

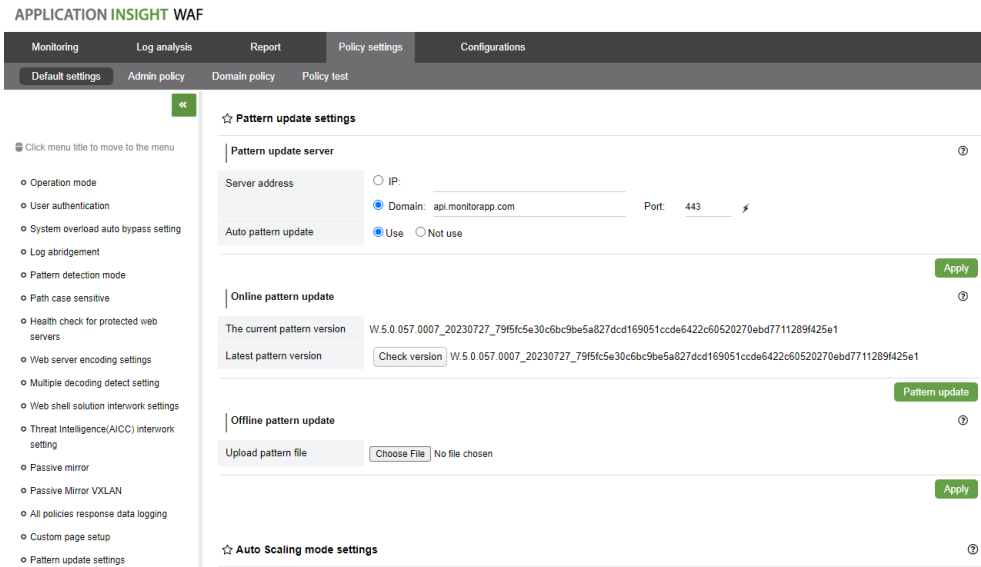
### APPLICATION INSIGHT WAF

The screenshot shows the 'Configurations' tab in the Application Insight WAF interface. The left sidebar contains a menu with options: Language settings (selected), License management, HA settings, Configurations synchronization settings, Program/Configuration backup, and National IP DB settings. The main content area is titled 'Language settings' and includes a 'Language' dropdown menu set to 'English'. An 'Apply' button is visible. Below this, the 'License management' section is partially visible, showing a 'Product license' field.

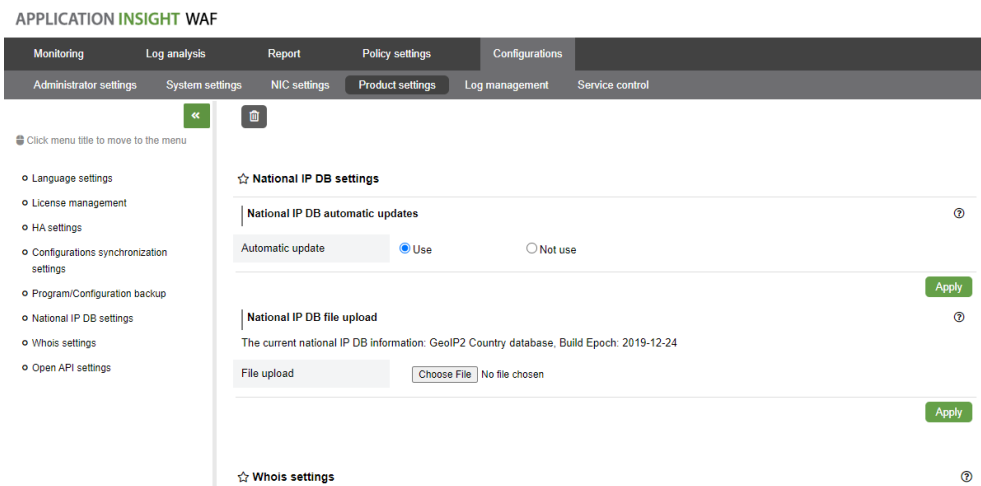
- Language Setup: Configurations > System Settings > Language Settings

## 5. Update Signature and Geolocation DB:

- You need to update the pattern signatures and geolocation database.



- [Signature Update] To access, go to: **Policy settings** → **Default settings** → **Pattern update settings** → **Online pattern update**.
- If the checkbox displays 'The current pattern version is the latest version' it indicates that the latest pattern is applied.



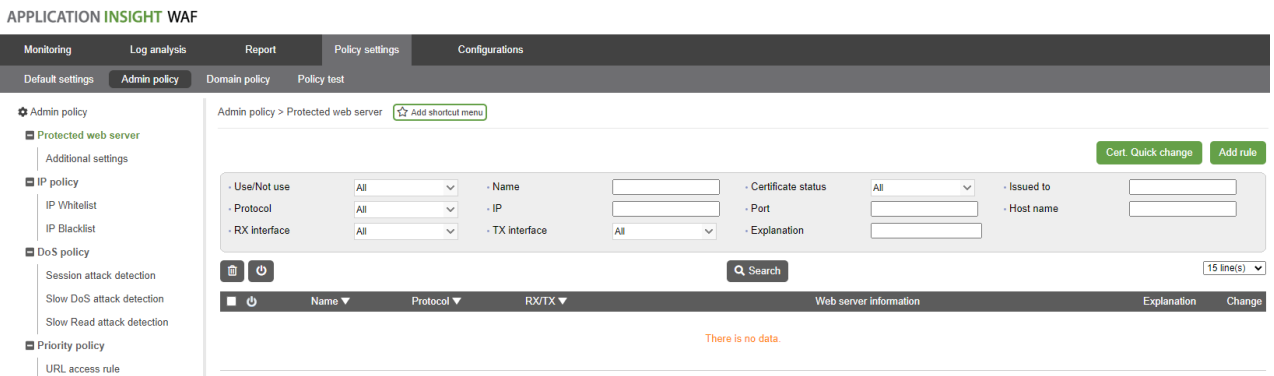
- [Geolocation Update] To update geolocation information, follow these steps: Go to **Configurations** → **Product settings** → **National IP DB settings**. Enable automatic updates 'Use' and click 'Apply.'
- Once you see the 'Completed' message, you can proceed to the next step.



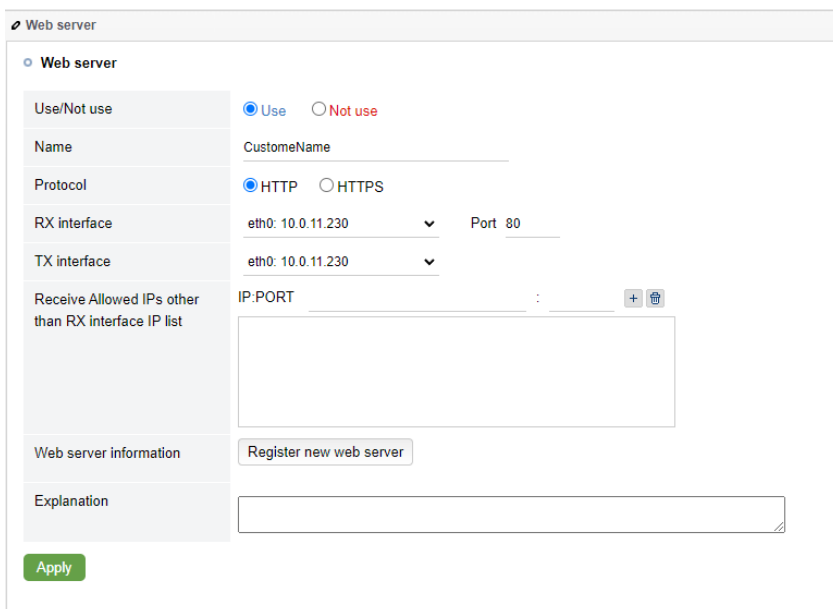
## 6. Register Protected Web Servers:

- HTTP and HTTPS (page #11) have separate registration procedures for protected websites. Follow the relevant procedure based on the website's protocol.

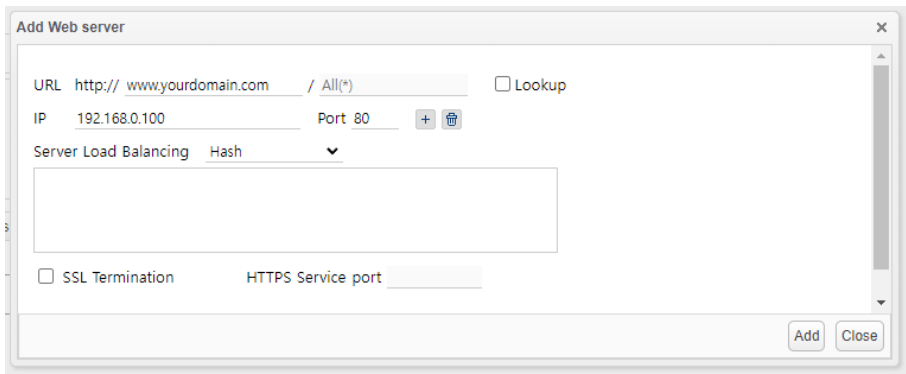
### 6-1. Register HTTP Web Servers



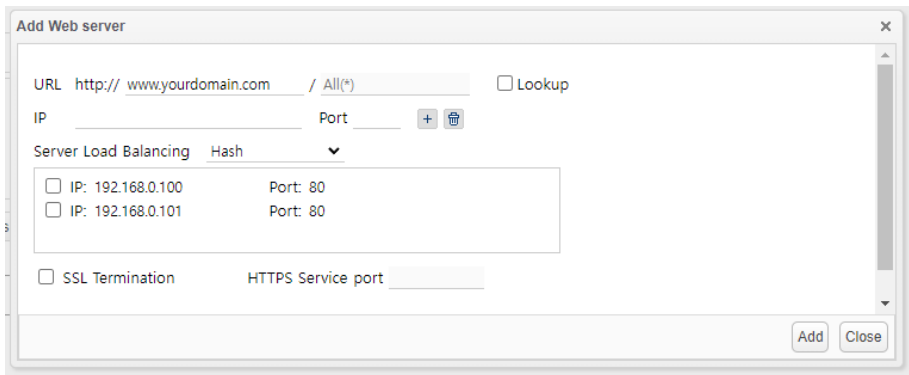
- To access, go to **Policy settings** → **Admin policy** → **Protected web server**, then click 'Add rule'.  
 ✓ No need for changes as HTTP is set as the default configuration.



- Enter a custom name for the web server registration and then click 'Register new web server'.



- Put your **protected URL**, **IP address** and **Port number** and click '+'
- For servers with dynamic IP, use Lookup option for alias registration.



- Once you have confirmed that the entered value is applied correctly, click '**Add**' to continue.

**Web server**

**Web server**

Use/Not use:  Use  Not use

Name: CustomName

Protocol:  HTTP  HTTPS

RX interface: eth0: 10.0.11.230 Port: 80

TX interface: eth0: 10.0.11.230

Receive Allowed IPs other than RX interface IP list: IP:PORT

Web server information: Register new web server

www.yourdomain.com 192.168.0.100:80, 192.168.0.101:80

Explanation:

[Apply](#)

- After verifying the entered web server information, click '**APPLY**' to finalize the web server registration.

Admin policy > Protected web server [Add shortcut menu](#)

Successfully applied the policies. Do you want to apply the policies? [To the Policy management menu](#) [Apply policy](#) [Restored to the previous policies.](#) [Cert. Quick change](#) [Add rule](#)

Use/Not use	All	Name		Certificate status	All	Issued to	
Protocol	All	IP		Port		Host name	
RX interface	All	TX interface	All	Explanation			

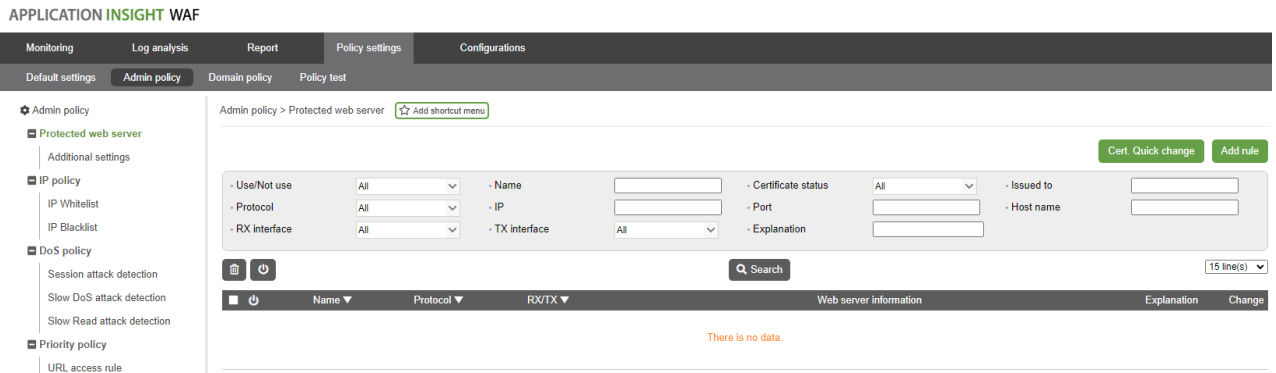
[Search](#) 15 line(s)

Name	Protocol	RX/TX	Web server information	Explanation	Change
CustomName	HTTP	RX: eth0 10.0.11.230:80 TX: eth0 10.0.11.230	Host name: www.yourdomain.com - 192.168.0.100:80 - 192.168.0.101:80		<a href="#">Change</a>

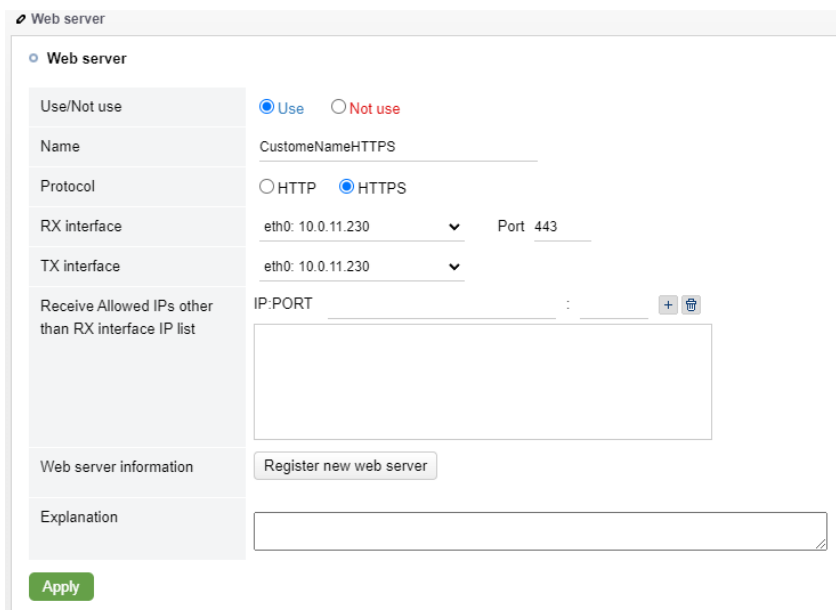
Total count(s) : 1 Case(s) 1

- In the 'Protected web server' menu, you can see the registered web server.

## 6-2. Register HTTPS Web Servers



- Access: Policy settings → Admin policy → Protected web server → Click 'Add rule'



- Enter a custom name, ensure 'HTTPS' is checked, and then click 'Register new web server'.

## Configuration

\*\*If you do not use SSL offload, you do not distinguish whether a URL has a path.

SSL Offload

URL   Lookup

IP  Port

Server Load Balancing

HTTP Service port   Replace response data

Select the other  
protected web server   Web server

Certificate file  No file chosen  Automatic register  Certificate file format (pfx)

Private key file  No file chosen

SSL Connection priority  Client  Server

Extension function  Verify Server HTTP/2 Support

Not-allowed SSL Version  SSL handshake denied  Block page    Create log

- Put your **protected URL, IP address** and **Port number** and click '+'
- For servers with dynamic IP, use Lookup option for alias registration.

\*\*If you do not use SSL offload, you do not distinguish whether a URL has a path.

SSL Offload

URL   Lookup

IP  Port

Server Load Balancing

IP: 192.168.0.100 Port: 443

IP: 192.168.0.101 Port: 443

HTTP Service port   Replace response data

Select the other  
protected web server   Web server

Certificate file  No file chosen  Automatic register  Certificate file format (pfx)

Private key file  No file chosen

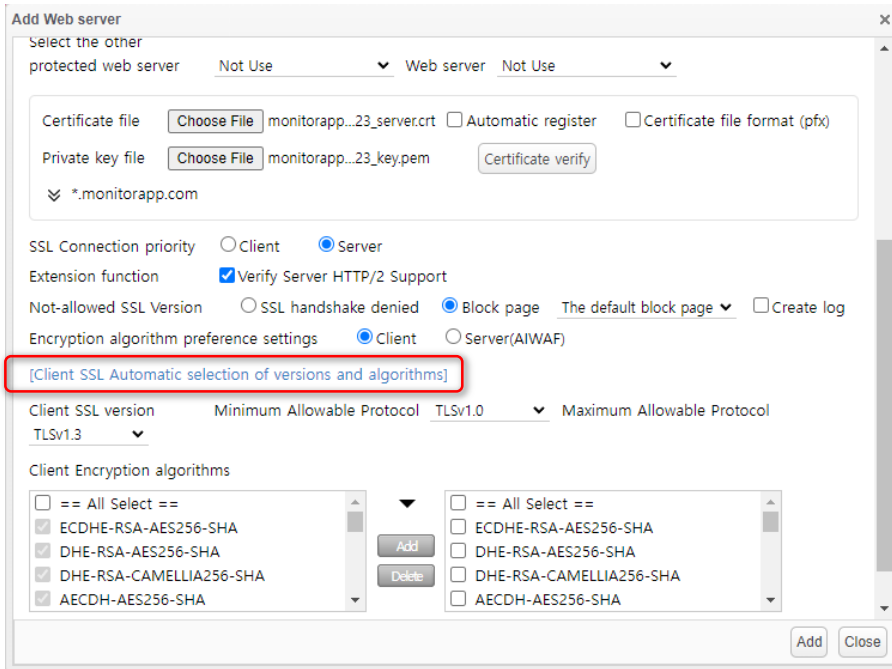
SSL Connection priority  Client  Server

Extension function  Verify Server HTTP/2 Support

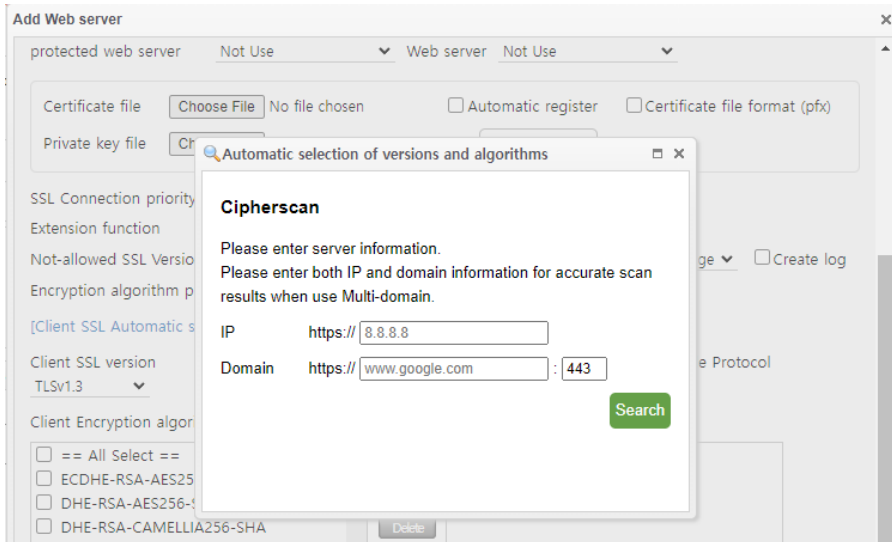
Not-allowed SSL Version  SSL handshake denied  Block page    Create log

- Verify the registered IP address and port number.
- Register the '**Certificate file**', '**Private key file**' and click '**Certificate verify**' to proceed.

# Configuration



- Once you've confirmed the certificate file and private key, proceed with the detailed configuration of the web server, including SSL/TLS versions and cipher suites, if necessary.
- Additionally, for **[Client SSL Automatic selection of versions and algorithms]**, input the domain and IP to scan the cipher suite of the web server you are registering.



- Enter the IP and domain information. The web server scanning will automatically select the SSL version and algorithms for the web server.
- After completing the previous steps,, click 'Add' to register web server information.

Web server

Web server

Use/Not use  Use  Not use

Name CustomNameHTTPS

Protocol  HTTP  HTTPS

RX interface eth0: 10.0.11.230 Port 443

TX interface eth0: 10.0.11.230

Receive Allowed IPs other than RX interface IP list IP:PORT : + -

Web server information Register new web server

www.yourdomain2.com 192.168.0.100:443, 192.168.0.101:443 Details

Explanation

Apply

- Once you've reviewed the provided information, click '**Apply**' to complete the process.

## 6-3. Apply Policy

APPLICATION INSIGHT WAF

Monitoring Log analysis Report Policy settings **Admin policy** Configurations

Default settings **Admin policy** Domain policy Policy test

**Admin policy**

- Protected web server
  - Additional settings
- IP policy
  - IP Whitelist
  - IP Blacklist
- DoS policy
  - Session attack detection
  - Slow DoS attack detection
  - Slow Read attack detection
- Priority policy
  - URL access rule
  - National IP detection
  - User-defined rule
  - Block page manage
- URL Rewriting policy
  - URL Rewriting request rule
  - URL Rewriting response rule
- URL Encryption policies
- API policies
  - test
  - hoiiann

**Admin policy** Add shortcut menu

**Policy apply/cancel**

Policy	Changed items
<input checked="" type="checkbox"/> Protected web server	1 Case(s)
<input type="checkbox"/> IP Whitelist	0 Case(s)
<input type="checkbox"/> IP Blacklist	0 Case(s)
<input type="checkbox"/> Session attack detection	0 Case(s)
<input type="checkbox"/> Slow DoS attack detection	0 Case(s)
<input type="checkbox"/> Slow Read attack detection	0 Case(s)
<input type="checkbox"/> URL access rule	0 Case(s)
<input type="checkbox"/> National IP detection	0 Case(s)
<input type="checkbox"/> User Management	0 Case(s)
<input type="checkbox"/> User-defined rule	0 Case(s)
<input type="checkbox"/> Block page manage	0 Case(s)
<input type="checkbox"/> Default SSL	0 Case(s)
<input type="checkbox"/> Health-check URL	0 Case(s)
<input type="checkbox"/> URL Rewriting request rule	0 Case(s)
<input type="checkbox"/> URL Rewriting response rule	0 Case(s)
<input type="checkbox"/> URL Encryption policies	0 Case(s)
<input type="checkbox"/> API policies	0 Case(s)

Apply policy Restored to the previous policies.

**Restore policy**

- After registering the web server, configuring its details, and making changes to various policies, remember to click '**Apply policy**' in the Admin policy section of the upper-level menu to implement the changes. Otherwise, the changes will not be applied. (Previous policies will be backed up.)
- To access: **Policy settings** → **Admin policy** → **Policy apply/cancel** → click '**Apply policy**'.



## 6-4. Security Policy Block Mode Configuration

### APPLICATION INSIGHT WAF

The screenshot shows the 'Operation mode' configuration page. At the top, there are tabs for 'Monitoring', 'Log analysis', 'Report', 'Policy settings', and 'Configurations'. Below these are sub-tabs for 'Default settings', 'Admin policy', 'Domain policy', and 'Policy test'. A left sidebar lists various settings like 'Operation mode', 'User authentication', etc. The main area is titled 'Operation mode' and has three radio buttons: 'Policy bypass', 'Detection mode', and 'Block mode' (which is selected). Below this is a 'Bypass target' section with a table of headers to bypass. The table has columns for 'Request' (all '[Request/Response]') and 'Header name:Value'. The headers listed are 'Content-Type: application/vnd.ms.wms-hdr.asfv1', 'Content-Type: application/x-mms-framed', 'Content-Type: application/x-wms-getcontentinfo', and 'Content-Type: application/x-wms-LogStats'. Below the table are fields for 'URL Path' (set to 'HTTP://:80/?') and 'URL extension'. At the bottom, there is a 'Detection mode targets' section with a similar URL field. An 'Apply' button is in the bottom right corner.

- To access, go to **Policy settings** → **Default settings** → **Operation mode**
- The default operation mode of AIWAF-VE is 'Detection.' Click on 'Block' and press 'Apply' to proceed.

### APPLICATION INSIGHT WAF

This screenshot is similar to the previous one but includes a confirmation dialog box on the left. The dialog box has a green header 'Apply policy/Cancel' and contains the text: 'There is a policy that has been changed. Do you want to apply the policy?'. It has two buttons: 'Apply policy' (which is highlighted in green) and 'Cancel'. Below the dialog box, the 'Operation mode' configuration is visible, showing that 'Block mode' is still selected. The 'Apply' button at the bottom right of the main configuration area is also visible.

- When making changes, you'll see the 'Apply policy/Cancel' box on the left. Select 'Apply policy' to save and apply the modified settings.

## APPLICATION INSIGHT WAF

- To apply the blocking policy completely, you need to change the **Detect** setting to **Block** for each individual security policy per domain.
- To access, go to **Policy settings** → **Domain policy**
- Click '**Default**' to manage each security policy. (The default page refers to the basic rule settings applied to the web pages users have registered(5-1, 5-2).)

## APPLICATION INSIGHT WAF

- All default rules are set to '**Detect**'. Please click on the rule you want to change.

# Configuration

Vulnerability attack detection

SQL injection Rule 1 Count(s) Detect 1 Count(s) Block 0 Count(s)

Add rule  View header

<input type="checkbox"/>	Rule name	Client IP	Server URL	Unused patterns	Schedule	Explanation	Action	Log	Mail	Risk	Change
<input type="checkbox"/>	SQL Injection	All IPs	All URLs	0 Case(s)	Always						

Total count(s) : 1 Case(s)

LDAP injection Rule 1 Count(s) Detect 1 Count(s) Block 0 Count(s)

Cross site script Rule 1 Count(s) Detect 1 Count(s) Block 0 Count(s)

Cookie forgery Rule 1 Count(s) Detect 1 Count(s) Block 0 Count(s)

- The green shield below the Action on the right side of the security rule represents the 'Detect' mode. Clicking on it will change it to 'Block'.
- To apply the changes, please click the 'Apply' button.

Successfully applied the policies. Do you want to apply the policies?

Applied URL  Rule name  Use/Not use  Action  Mail

Batch change use/not use of policies   Batch change action of policies

Vulnerability attack detection new

SQL injection Rule 1C

Add rule

<input type="checkbox"/>	Rule name	Client IP	Server URL	Unused patterns	Schedule	Exp
<input type="checkbox"/>	SQL Injection	All IPs	All URLs	0 Case(s)	Always	

Total count(s) : 1 Case(s)

- Similar to saving other modifications, click on 'Apply policy' at the top to save your changes.

Applied URL  Rule name  Use/Not use  Action  Mail  Risk  Search

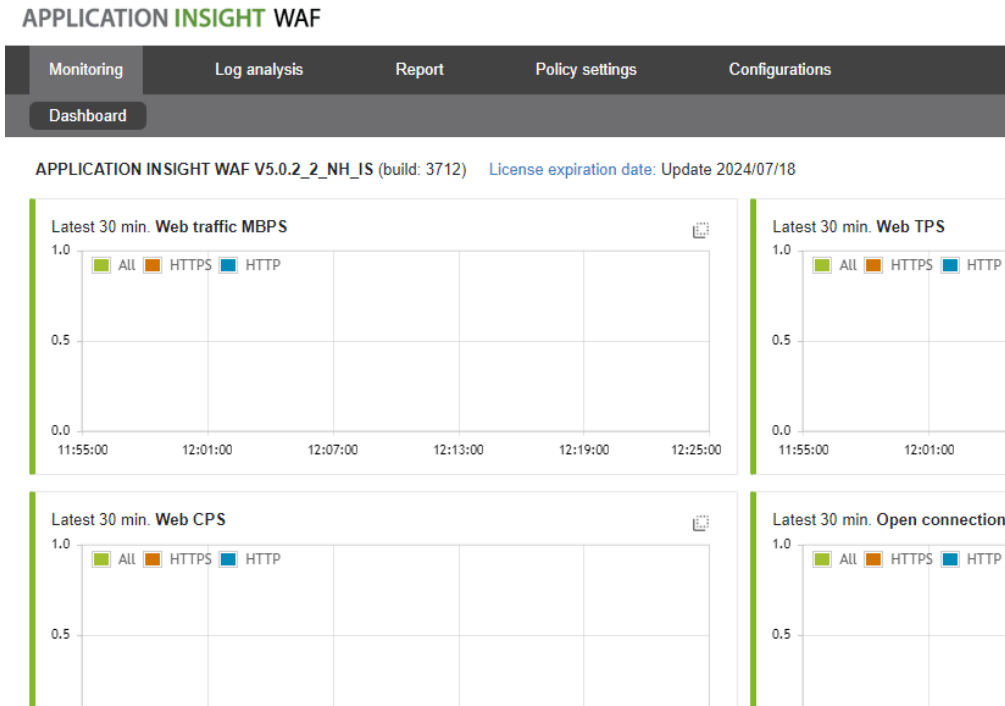
Batch change use/not use of policies   Batch change action of policies

Vulnerability attack detection

SQL injection	Rule 1 Count(s)	Detect 0 Count(s)	Block 1 Count(s)	
LDAP injection	Rule 1 Count(s)	Detect 1 Count(s)	Block 0 Count(s)	
Cross site script	Rule 1 Count(s)	Detect 1 Count(s)	Block 0 Count(s)	
Cookie forgery	Rule 1 Count(s)	Detect 1 Count(s)	Block 0 Count(s)	
CSRF detection	Rule 1 Count(s)	Detect 1 Count(s)	Block 0 Count(s)	
Malicious file upload detection	Rule 1 Count(s)	Allow 0 Count(s)	Detect 1 Count(s)	Block 0 Count(s)

- You'll notice that the SQL injection security rule has been switched from 'Detect' to 'Block'.
- You can refer to page 22 to review actual log data (detection, blocking data).

## 7. Complete Configuration:



- Your configuration is now set. You can monitor web traffic at **Monitoring** → **Dashboard**.

## Testing AIWAF-VE: Procedure for Test

If you're looking to conduct a test with AIWAF-VE, follow these steps. Please note that the client (visitor) for this test scenario is designed around the Windows OS.

### Step 1: Redirect Test Traffic to AIWAF-VE:

To direct test client (visitor) traffic to AIWAF-VE, adjust the DNS information using the procedure below. In an actual network setting, you would typically modify the A record or CNAME of the domain name server. However, in this example, we're outlining a process that involves changing the contents of the hosts file.

- Launch Notepad as a Windows administrator.
- In Notepad, navigate to File and choose Open.
- Locate the hosts file path and open it using Notepad.
- Windows hosts file path: **C:\Windows\System32\drivers\etc\hosts**
- Register the IP of AIWAF-VE along with the domain name of the protected web server.
- Example: **[AIWAF-VE IP] [Domain] (e.g., 192.168.10.110 www.yourdomain.com)**
- Save the hosts file.

### Step 2: Send Sample Traffic to AIWAF-VE:

Generate sample detection traffic from the client (visitor) PC to AIWAF-VE.

- Open an internet browser.
- Enter the following values in the URL address input:  
URL: **http://www.yourdomain.com/?monitorapp=monitorapp**

## Step 3: Verify Attack Detection:

Check if the attack is logged in AIWAF-VE's detection log.

**APPLICATION INSIGHT WAF**

Monitoring | Log analysis | Report | Policy settings | Configurations

Detection log view | Audit log view | View web server status log

[All Delete](#)

Period : 2023-08-16 12:51 ~ 2023-08-16 13:21 [×](#)

Period  Today  1 week  1 month  2023-08-16  :  ~ 2023-08-16  :

[Search](#) [Download](#) [Chart](#) [Pivot Chart](#)

Auto Refresh ▼

Attack domain: 0Count(s) | Attacker(Origin IP): 0Count(s)(0Count(s)) | Attack count: 0Case(s)

Time	Client IP	Origin IP	Server IP	Domain	Detection type
There is no data					

- Navigate to: Web UI > **Log analysis** > **Detection log view**.
- This procedure provides a concise way to test AIWAF-VE. For more detailed instructions and assistance, consult our user manual or reach out to our support team.

## Step 3: Verify Attack Detection:

Check if the attack is logged in AIWAF-VE's detection log.

APPLICATION INSIGHT WAF

Monitoring | Log analysis | Report | Policy settings | Configurations

Detection log view | Audit log view | View web server status log

All Delete

Period: 2023-08-16 12:51 ~ 2023-08-16 13:21

Period: Today | 1 week | 1 month | 2023-08-16 | 12 | 51 | 2023-08-16 | 13 | 21

Search | Download | Chart | Pivot Chart

Auto Refresh 5 sec.

Attack domain: 0Count(s) | Attacker(Origin IP): 0Count(s)(0Count(s)) | Attack count: 0Case(s)

Time	Client IP	Origin IP	Server IP	Domain	Detection type
There is no data					

- Navigate to: Web UI > Log analysis > Detection log view.

### \*Example of Detection Log View(using quick guide's policy setup)

APPLICATION INSIGHT WAF

Monitoring | Log analysis | Report | Policy settings | Configurations

Detection log view | Audit log view | View web server status log

All Delete

Period: 2023-08-22 10:52 ~ 2023-08-22 12:06

Period: Today | 1 week | 1 month | 2023-08-22 | 10 | 52 | 2023-08-22 | 12 | 06

View only pattern detection mode logs | Show only interest logs

Search | Download | Chart | Pivot Chart | Apply search filter

Auto Refresh 5 sec. Search 15 line(s)

Attack domain: 1Count(s) | Attacker(Origin IP): 1Count(s)(0Count(s)) | Attack count: 10Case(s)

Time	Client IP	Origin IP	Server IP	Domain	Detection type	Rule name	URL	Risk	Action	Mail
08-22 10:52:40	112.216.3.62	None	3.38.96.49	Default	SQL injection	SQL Injection	http://example.com/	High	Block	Mail
08-22 10:52:32	112.216.3.62	None	3.38.96.49	Default	SQL injection	SQL Injection	http://example.com/	High	Block	Mail
08-22 10:52:12	112.216.3.62	None	3.38.96.49	Default	Directory access detect...	Directory Access	http://example.com/	Low	Alert	Mail
08-22 10:52:12	112.216.3.62	None	3.38.96.49	Default	System file access det...	System File Access	http://example.com/	Low	Alert	Mail
08-22 10:52:09	112.216.3.62	None	3.38.96.49	Default	Character set limits det...	CHARSET	http://example.com/	Low	Alert	Mail
08-22 10:52:09	112.216.3.62	None	3.38.96.49	Default	Cross site script	Cross-Site Scripting	http://example.com/	Low	Alert	Mail

- You can confirm the detection and blocking results below the 'Action'. In this case, SQL injection has been successfully blocked (indicated by a red shield icon), and other attacks have been detected (indicated by a green shield icon).

## Additional Resources

MONITORAPP offers further resources more in-depth information and support.

- **Support Contact:** +1-909-957-1335
- **Email:** [support@monitorapp.com](mailto:support@monitorapp.com)

Copyright © 2024 MONITORAPP, Inc

This user manual is protected by copyright law. Reproduction, public transmission, distribution, translation, or transformation of all or part of this user manual, whether in electronic media or machine-readable form, is prohibited.