MONITORAPP

Quick Guide

AIWAF-VE for AWS Marketplace(BYOL/PAYG)

v5.0.2

Table of Contents

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. Subscribe AIWAF-VE BYOL or PAYG

- Subscribe AIWAF-VE **BYOL or PAYG** in the AWS Marketplace.

2. Access the Web User Interface (UI):
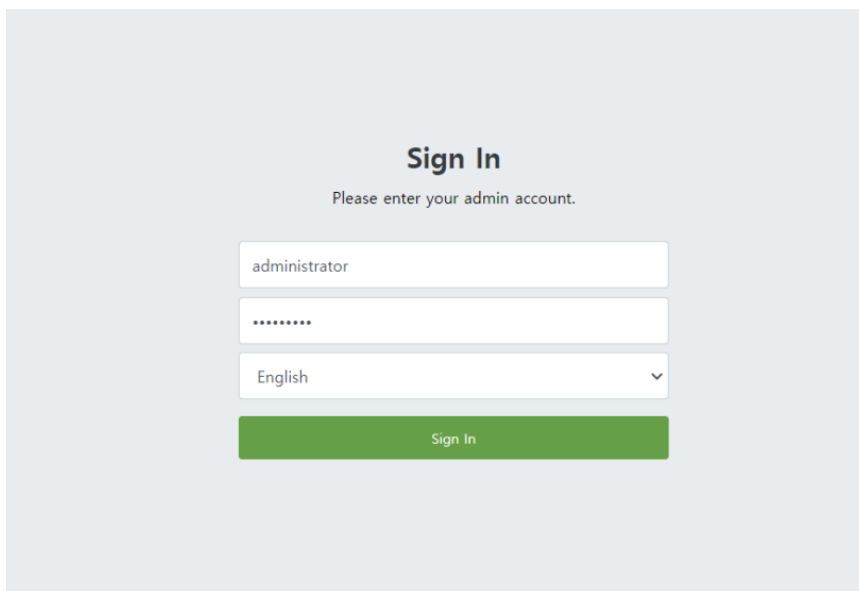
- Open your internet browser and access by entering the assigned IP from the AWS instance as follows: 'https://[AIWAF-VE IP]:222'. (e.g., https://192.168.10.110:222)
- Please change the language before sign in. (Supported languages: English, Japanese, Korean)
- Login with the provided ID and Password (ID: **administrator**, PW : **[instance ID*]**)
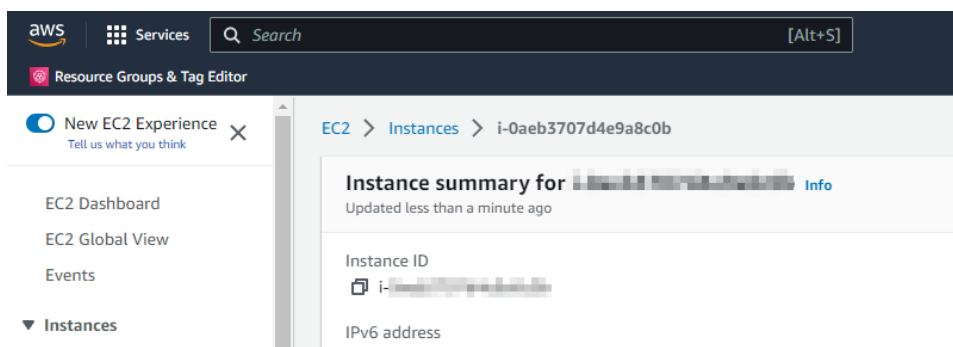
* The Password instanceID for the initial connection is not the alphabet instanceID, but the actual instanceID that you can find in the AWS Management Console for launching AIWAF- VE.

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**   ⑦

Name	Administrator
ID	administrator
Password	Current password _____ New password _____ Confirm new password _____
Password change notification	60 day(s)
Two-Factor Authentication	○ Use ● Not use
Allowed IP	IP _____ [+] [🗑]
Recipient E-mail	E-mail _____ [+] [🗑]
Explanation	

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.

3. Register Your License(AIWAF-VE BYOL only):

- If you are **BYOL user**, you need to register your license to start AIWAF-VE. PAYG user can skip this step and proceed to the next page.
- 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:

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

- Language Setup: **Configurations** > **System Settings** > **Language Settings**

5. Update Signature and Geolocation DB:

- You need to update the pattern signatures and geolocation database.
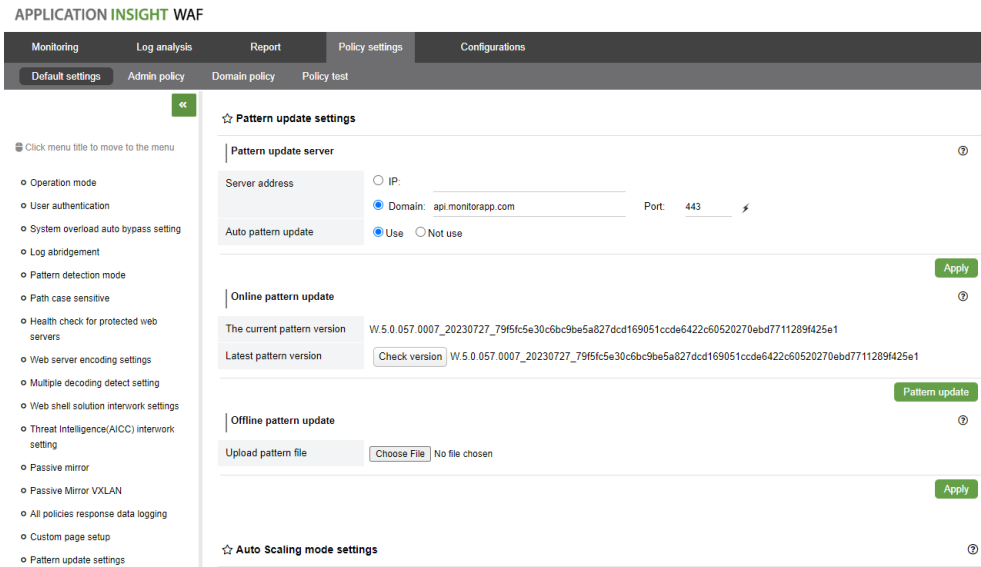
- [Signature Update] To access, go to: **Policy settings → Default settings → Pattern update settings → Online pattern update.**
- If the checkbox displays '**The current pattern version is the latest version**' it indicates that the latest pattern is applied.
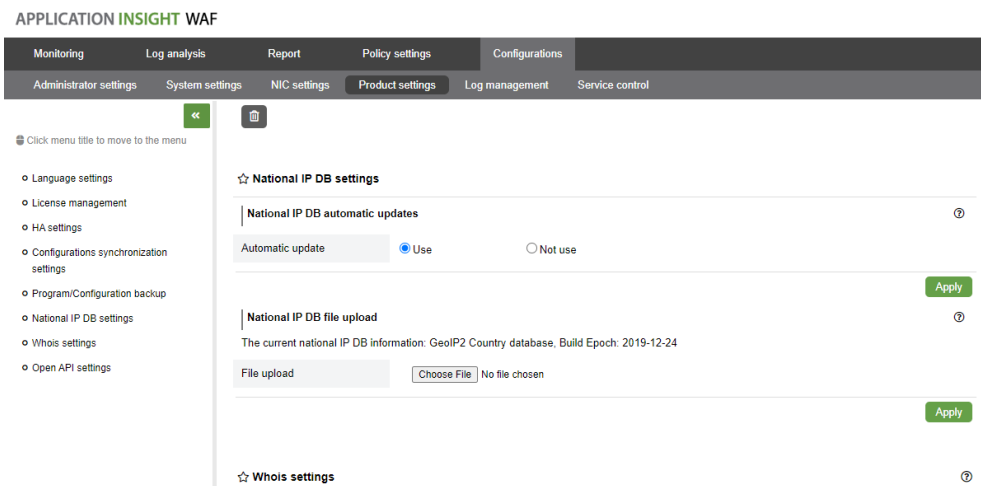
- [Geolocation Update] To update geolocation information, follow these steps: Go to **Configurations → Product settings → National IP DB settings**. Enable automatic updates '**Use**' and click '**Apply.**'
- Once you see the 'Completed' message, you can proceed to the next step.

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
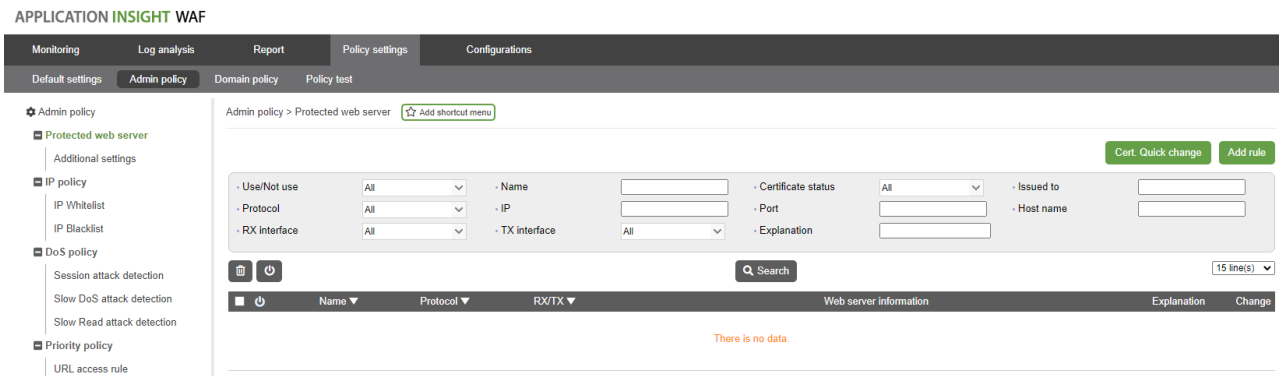
- To access, go to **Policy settings** → **Admin policy** → **Protected web server**, then click '**Add rule**'.
    - ✓ No need for changes as HTTP is set as the default configuration.
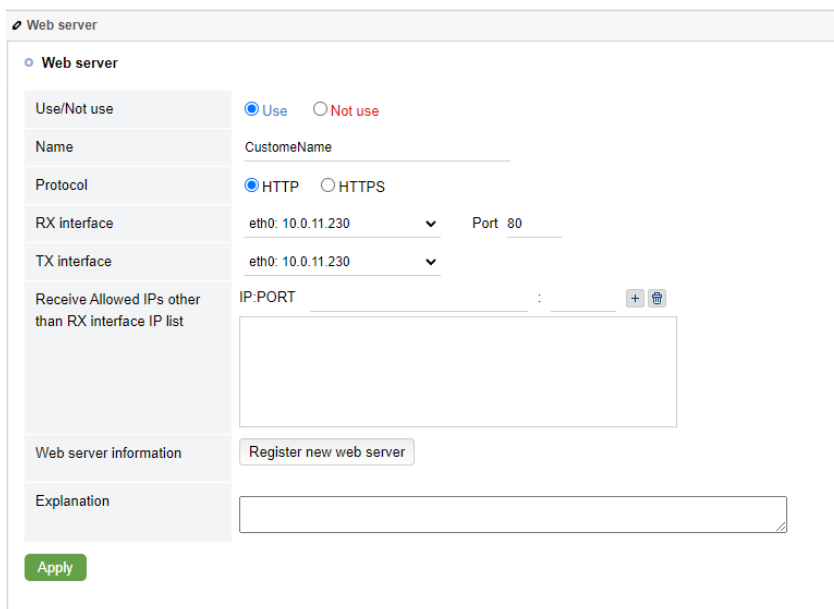
- Enter a custom name for the web server registration and then click '**Register new web server**'.
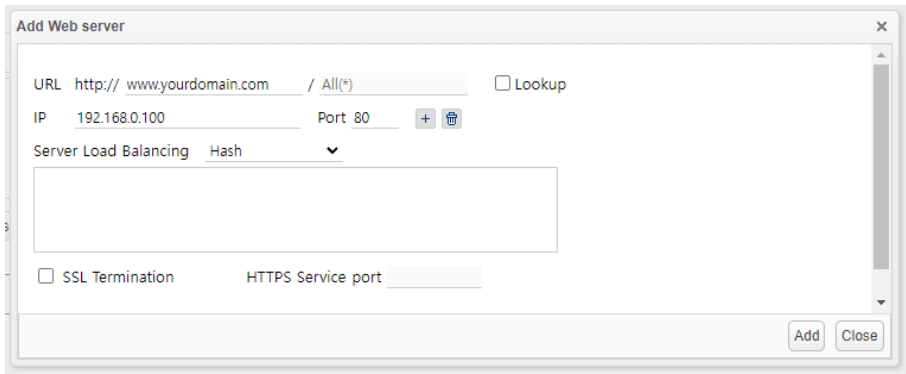
- Put your **protected URL**, **IP address** and **Port number** and click '**+**'
- For servers with dynamic IP, use Lookup option for alias registration.
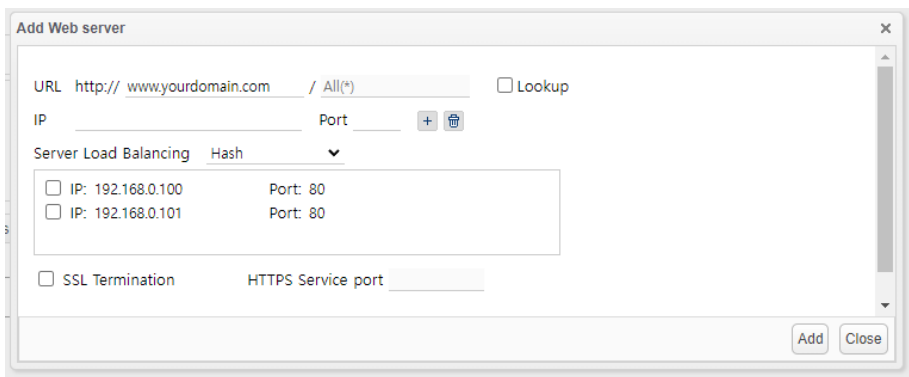
- Once you have confirmed that the entered value is applied correctly, click '**Add**' to continue.

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

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

6-2. Register HTTPS Web Servers
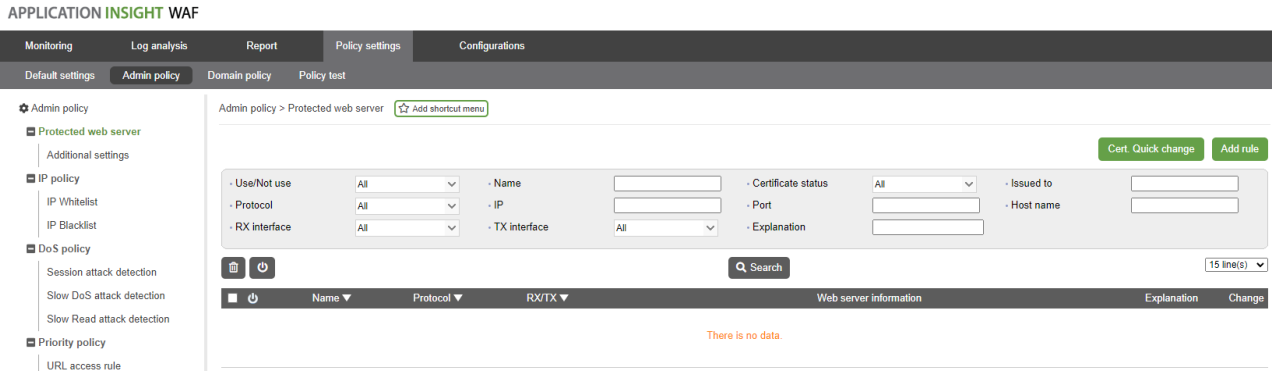
- Access: **Policy settings** → **Admin policy** → **Protected web server** → Click '**Add rule**'
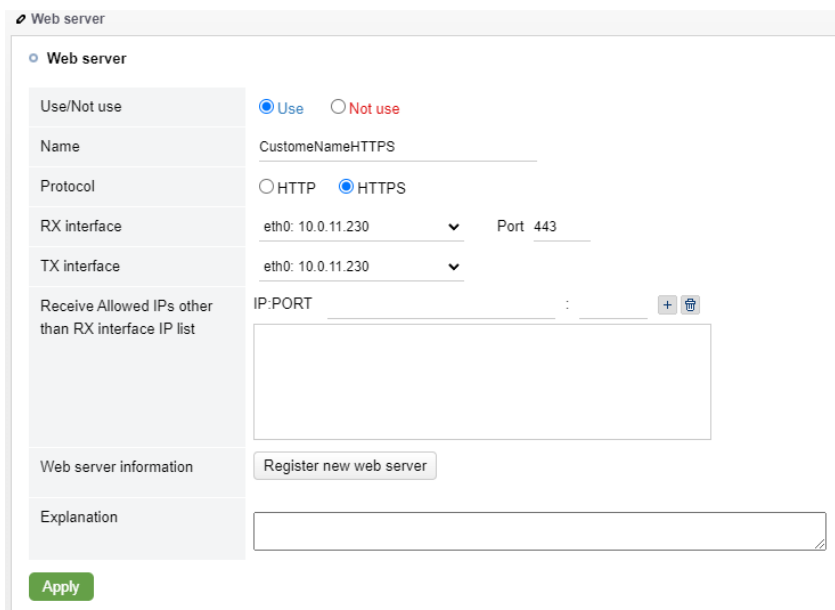
- Enter a custom name, ensure '**HTTPS**' is checked, and then click '**Register new web server**'.

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

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

- 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.

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

6-3. Apply 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 polic**y'.

6-4. Security Policy Block Mode Configuration

- 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.

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

- <u>To apply the blocking policy completely</u>, 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).)

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

- 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.

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

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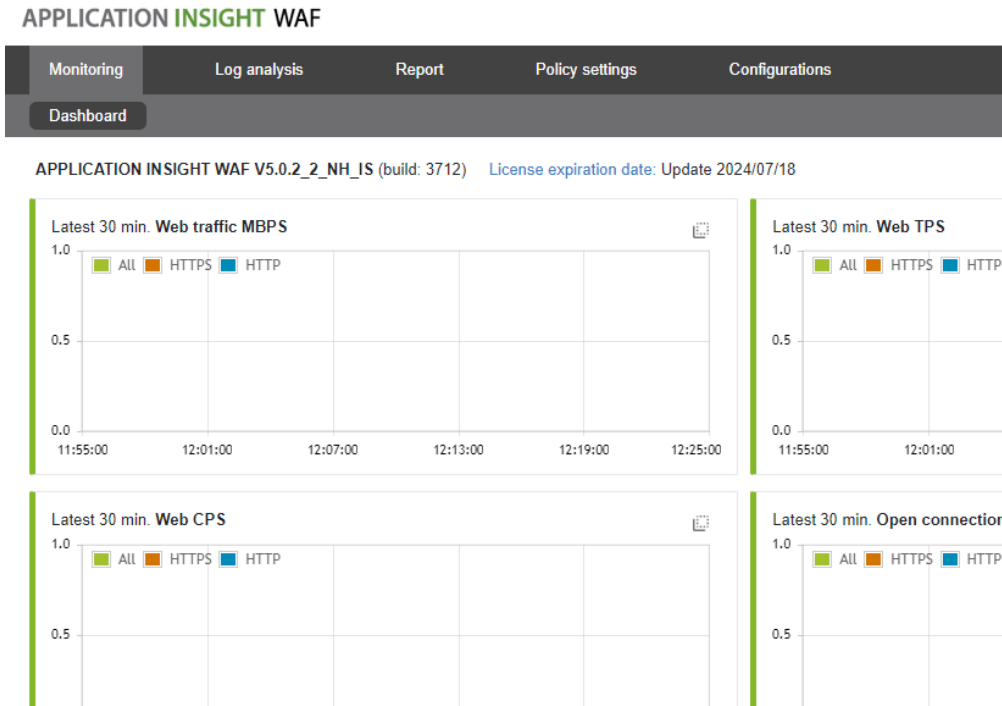
- Your configuration is now set. You can monitor web traffic at **Monitoring → Dashboard.**

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.

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

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

- 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

Copyright © 2023 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.