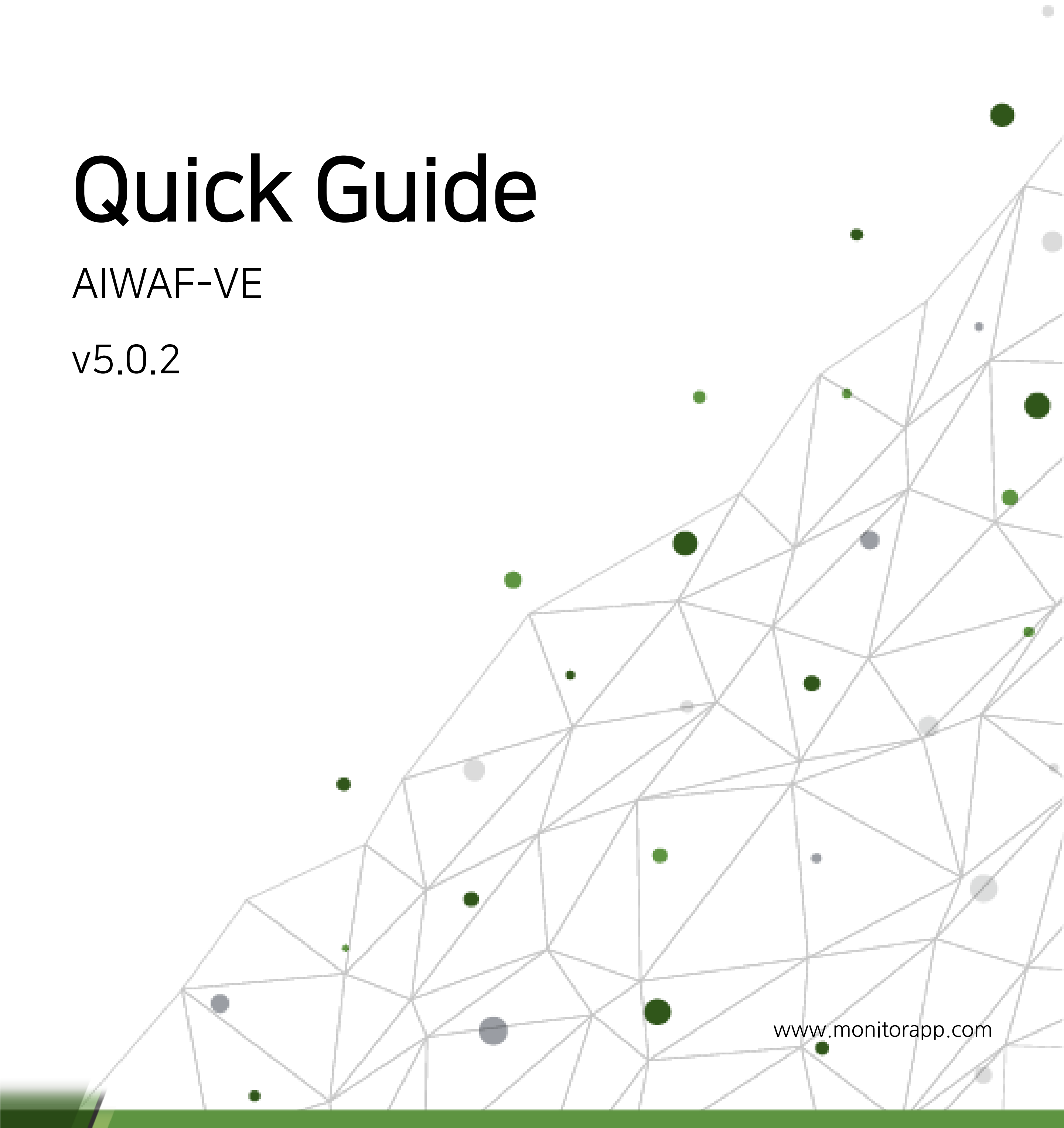
MONITORAPP

Quick Guide

AIWAF-VE

v5.0.2



www.monitorapp.com

Table of Contents

Overview for AIWAF-VE menu 3

Configuration of AIWAF-VE 4

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

Testing AIWAF-VE: Procedure for Test 21

Step 1: Redirect Test Traffic to AIWAF-VE: 21

Step 2: Send Sample Traffic to AIWAF-VE: 21

Step 3: Verify Attack Detection: 22

Contact us 23

Overview of AIWAF-VE menu

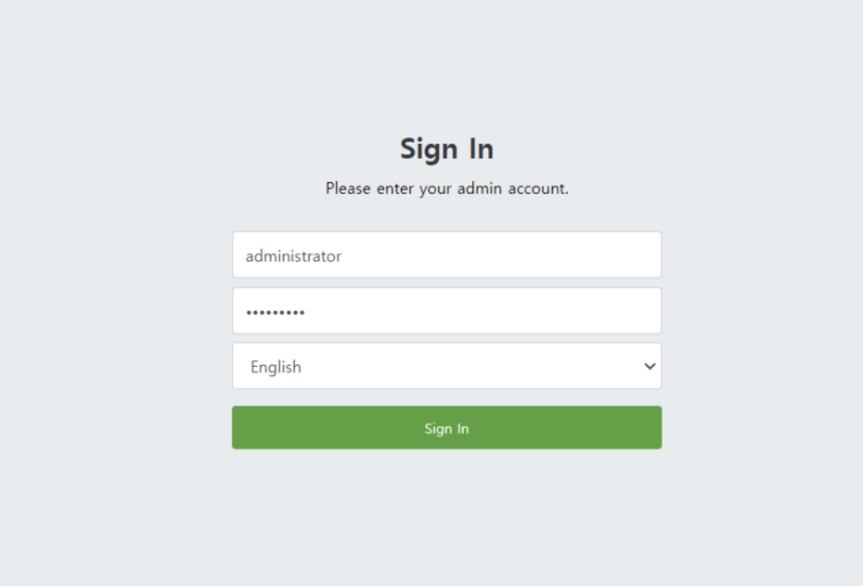
Menu	Description
Monitoring	Provides a centralized visual representation of web traffic, system information, detection counts, detection severity, and the detection log of your web server. It is a user interface that allows users to monitor and analyze real-time or historical data in a concise and easily 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

2. Access the Web User Interface (UI):



Sign In

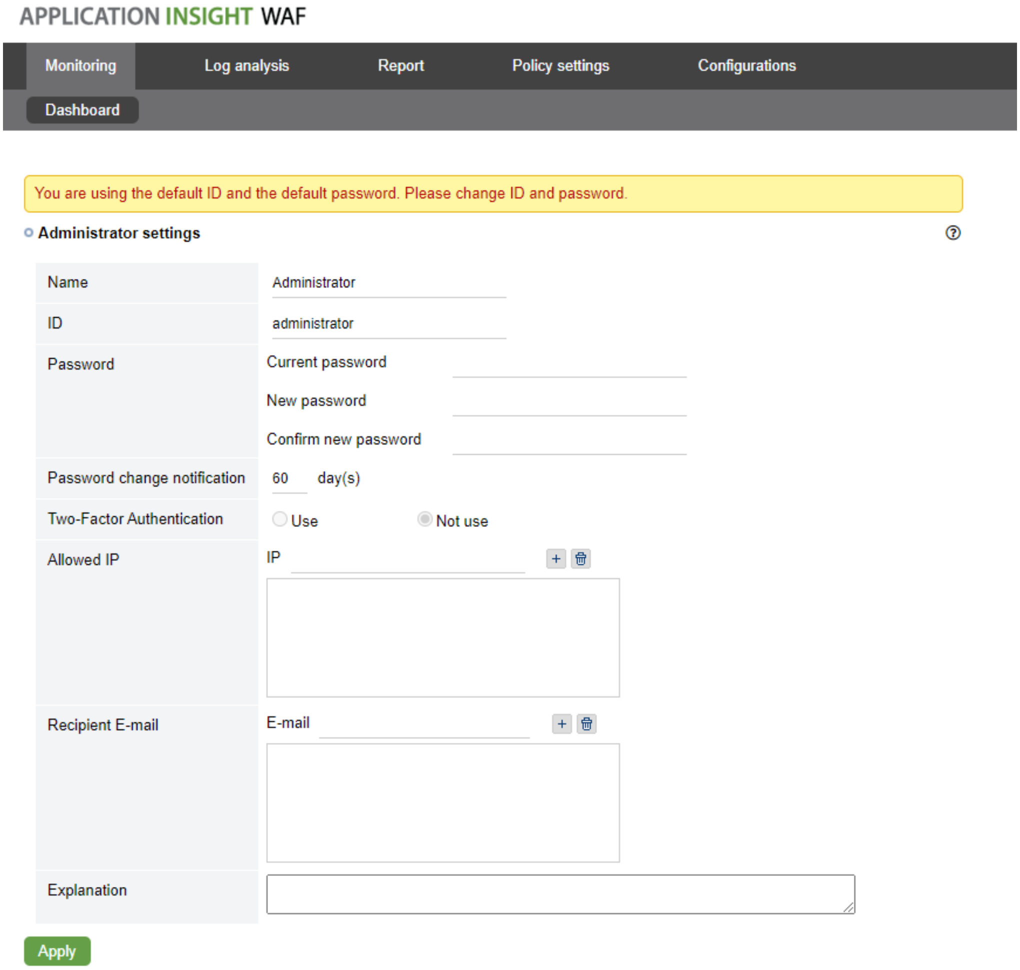
Please enter your admin account.

administrator

•••••••••

English

- 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 : **[_appleader]**)



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

Administrator settings

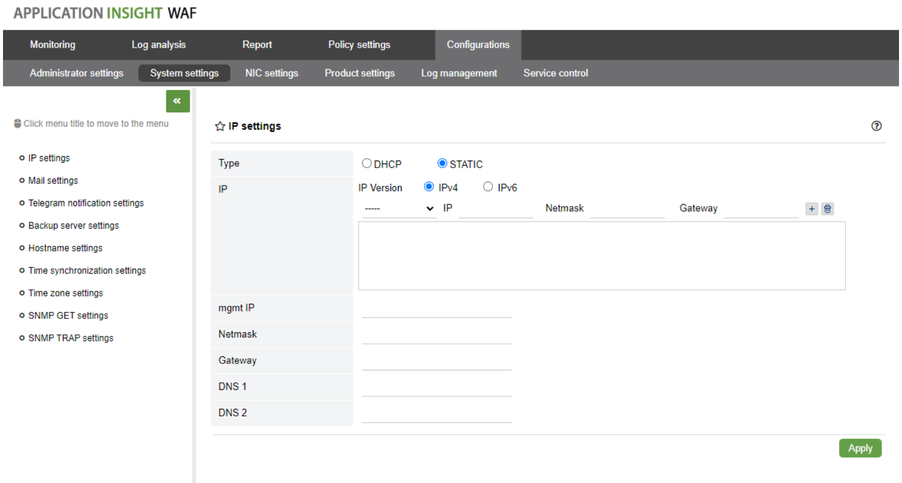
Name	Administrator
ID	administrator
Password	Current password New password Confirm new password
Password change notification	60 day(s)
Two-Factor Authentication	○ Use ● Not use
Allowed IP	IP
Recipient E-mail	E-mail
Explanation	

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):

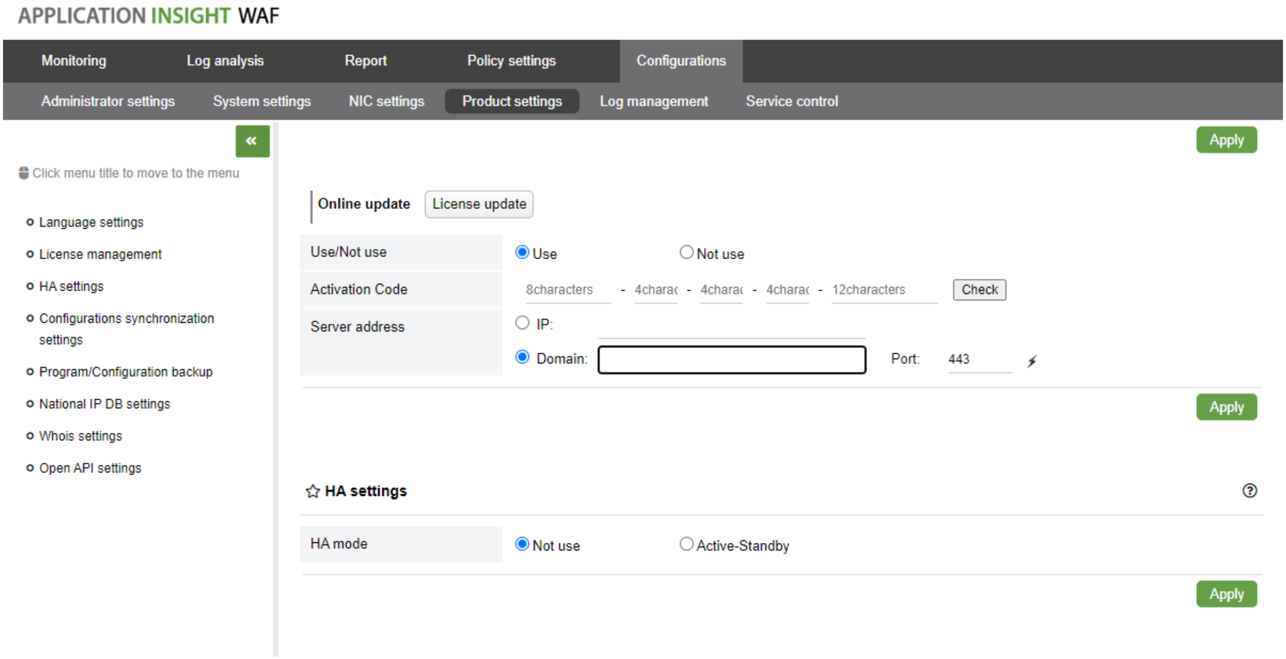


☆ IP settings

Type	○ DHCP ● STATIC
IP	IP Version ● IPv4 ○ IPv6 ----- IP Netmask Gateway + 🗑
mgmt IP	
Netmask	
Gateway	
DNS 1	
DNS 2	

- 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:



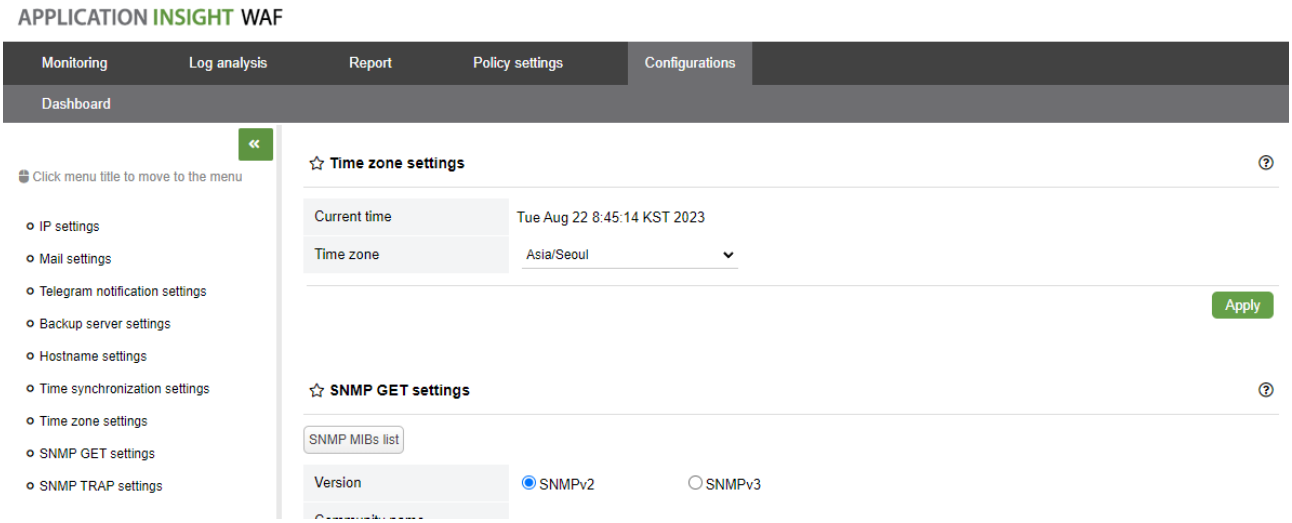
Use/Not use	● Use ○ Not use
Activation Code	8characters - 4charac - 4charac - 4charac - 12characters
Server address	○ IP: ● Domain: Port: 443

☆ HA settings

HA mode	● Not use ○ Active-Standby

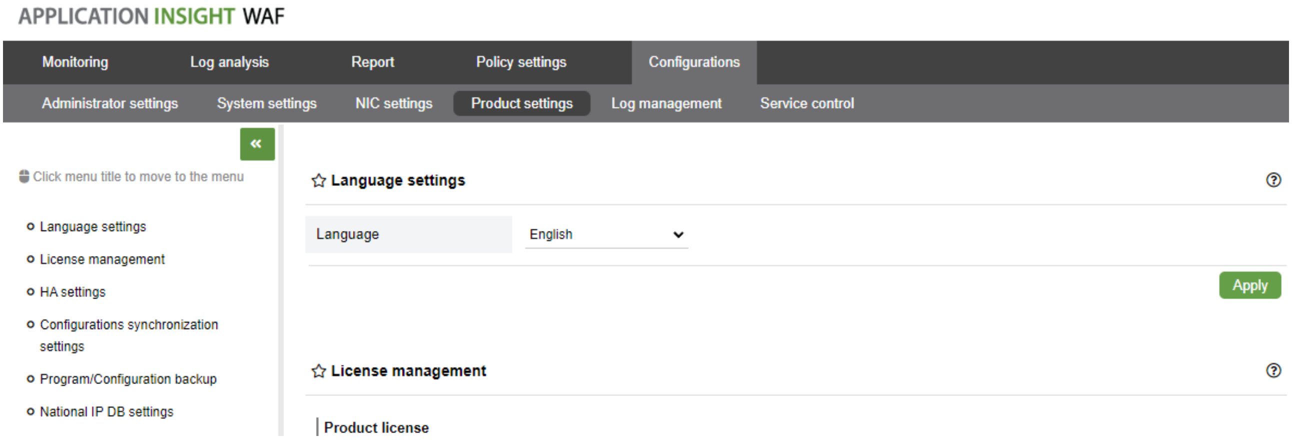
- Access: **Configurations** → **Product settings** → **License management** → **Online update.**
- Choose your online update preference (enable/disable).
- Enter the Activation Code and click '**Check**' to validate.
- Click '**Apply**' to complete license registration.

4. Time Zone and Language Settings:



Current time	Tue Aug 22 8:45:14 KST 2023
Time zone	Asia/Seoul
Version	● SNMPv2 ○ SNMPv3

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

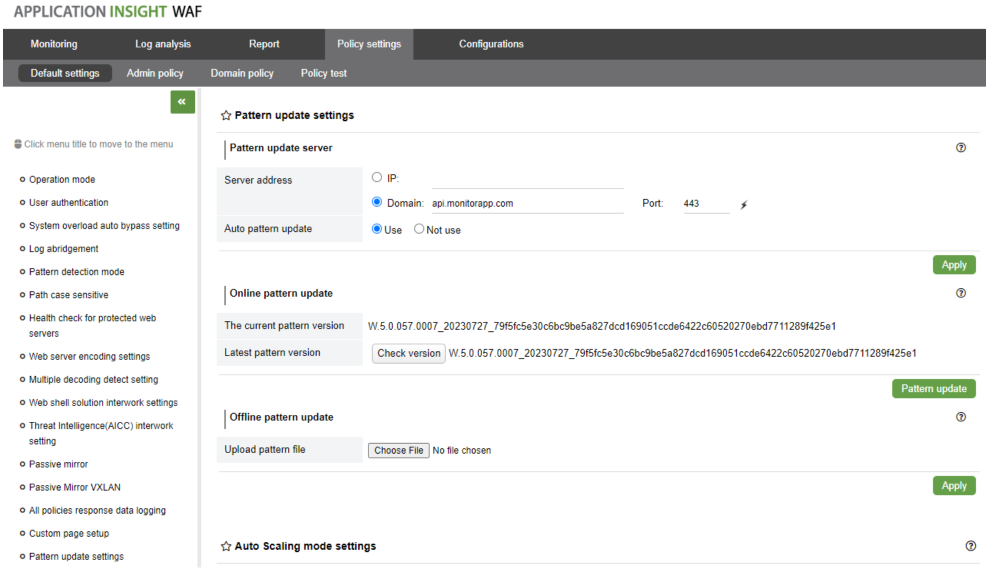


Language	English

- Language Setup: Configurations > System Settings > Language Settings

5. Update Signature and Geolocation DB:

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



☆ Pattern update settings

Pattern update server

Server address	○ IP: ● Domain: api.monitorapp.com Port: 443
Auto pattern update	● Use ○ Not use

Apply

Online pattern update

The current pattern version	W.5.0.057.0007_20230727_79f5fc5e30c6bc9be5a827dcd169051ccde6422c60520270ebd7711289f425e1
Latest pattern version	Check version W.5.0.057.0007_20230727_79f5fc5e30c6bc9be5a827dcd169051ccde6422c60520270ebd7711289f425e1

Pattern update

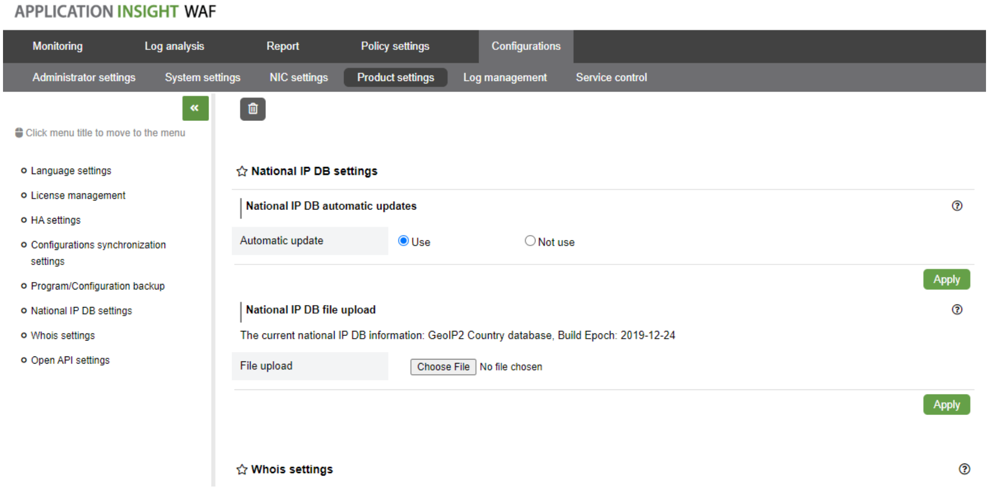
Offline pattern update

Upload pattern file	Choose File No file chosen

Apply

☆ Auto Scaling mode settings

- [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.



☆ National IP DB settings

National IP DB automatic updates

Automatic update	● Use ○ Not use

Apply

National IP DB file upload

The current national IP DB information: GeoIP2 Country database, Build Epoch: 2019-12-24

File upload	Choose File No file chosen

Apply

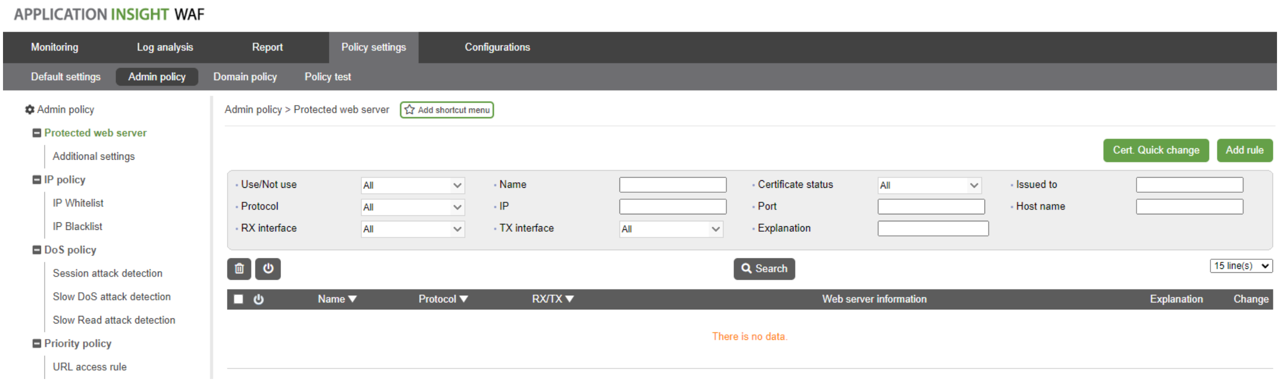
☆ Whois settings

- [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.

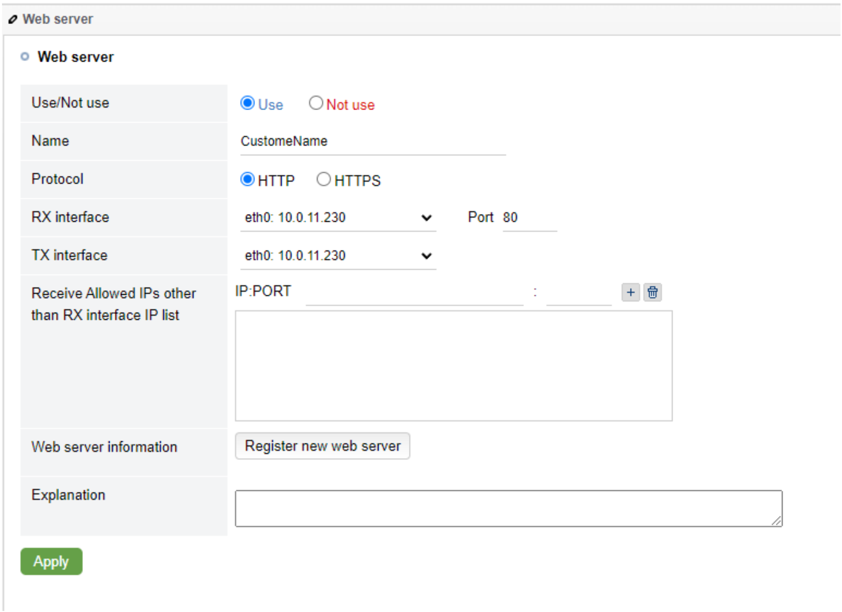
6. Register Protected Web Servers:

- 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.

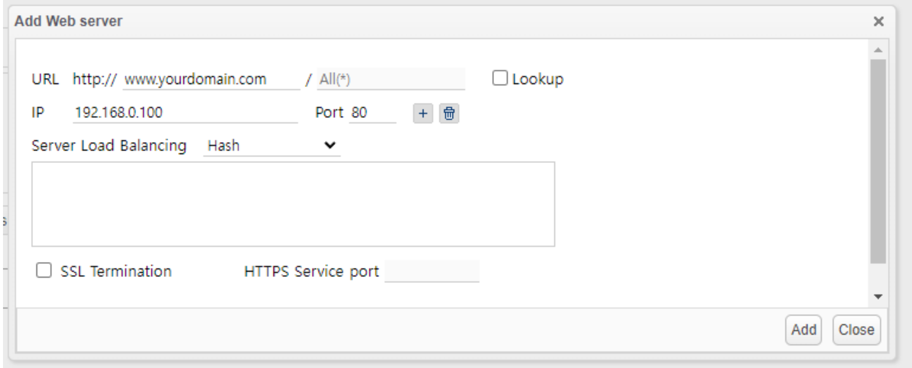

Web server

Web server

Use/Not use	● Use ○ Not use
Name	CustomeName
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
Explanation	

Apply

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



Add Web server

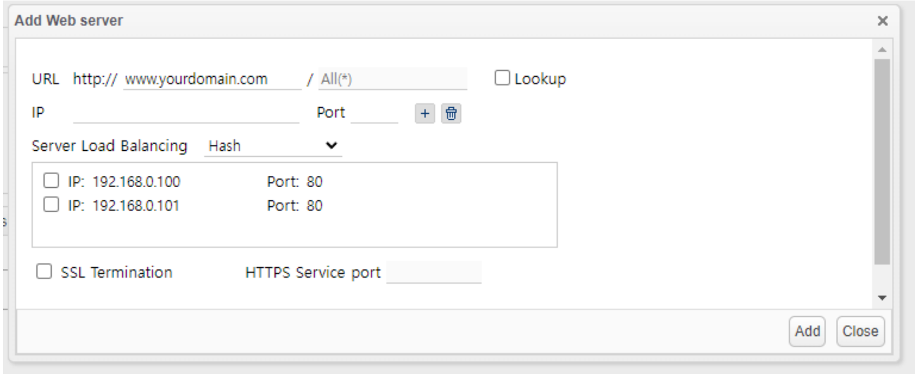
URL http:// www.yourdomain.com / All(*) □ Lookup

IP 192.168.0.100 Port 80

Server Load Balancing Hash

□ SSL Termination HTTPS Service port

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



Add Web server

URL http:// www.yourdomain.com / All(*) □ Lookup

IP Port

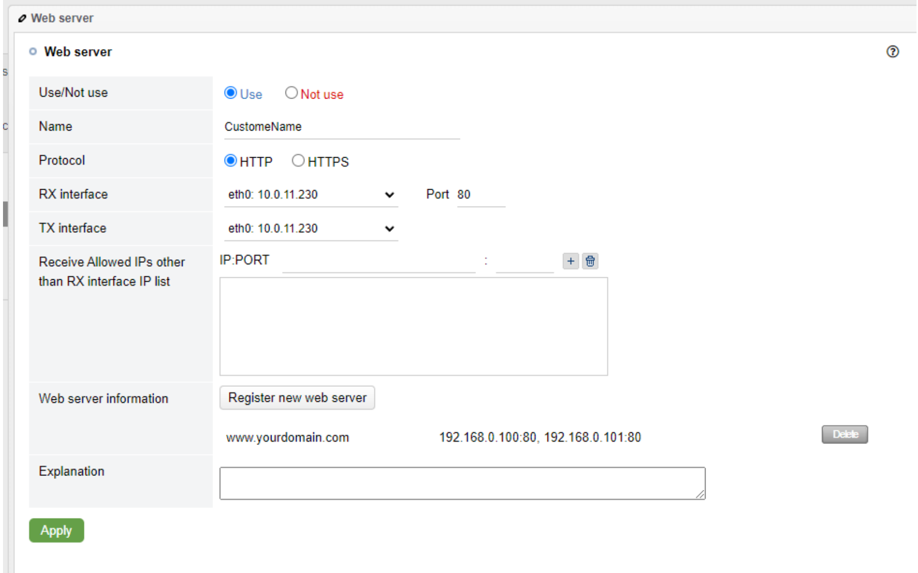
Server Load Balancing Hash

□ IP: 192.168.0.100 Port: 80

□ IP: 192.168.0.101 Port: 80

□ SSL Termination HTTPS Service port

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

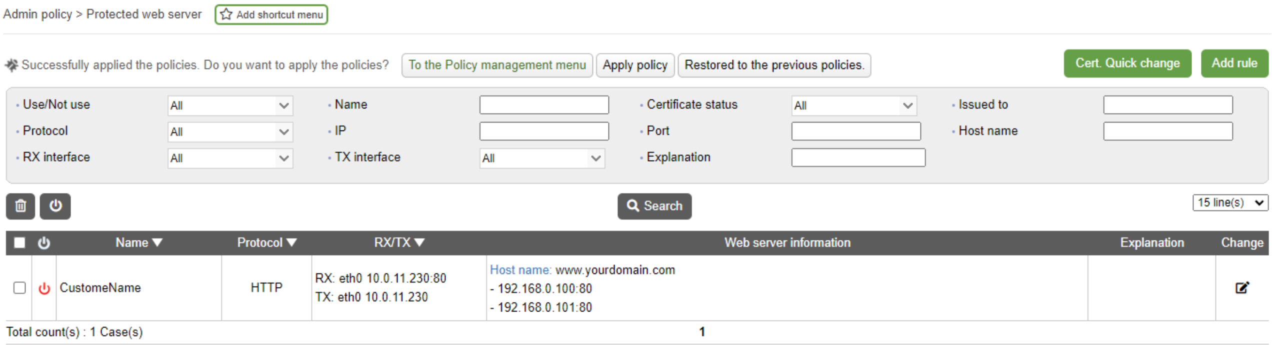


Web server

○ Web server

Use/Not use	● Use ○ Not use
Name	CustomeName
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 Delete
Explanation	

- 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

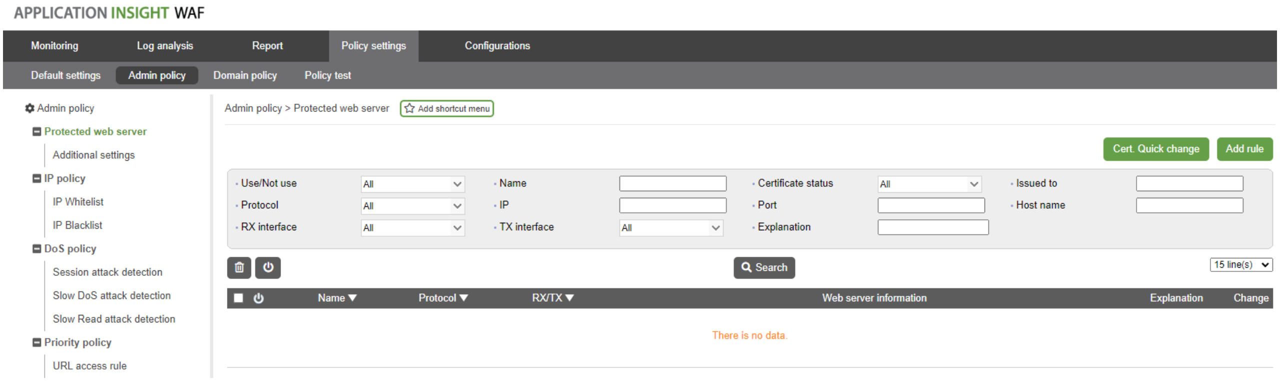
Use/Not use	All	Name		Certificate status	All	Issued to	
Protocol	All	IP		Port		Host name	
RX interface	All	TX interface	All	Explanation			

☐	⏻	Name ▼	Protocol ▼	RX/TX ▼	Web server information	Explanation	Change
☐	⏻	CustomeName	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		✎

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

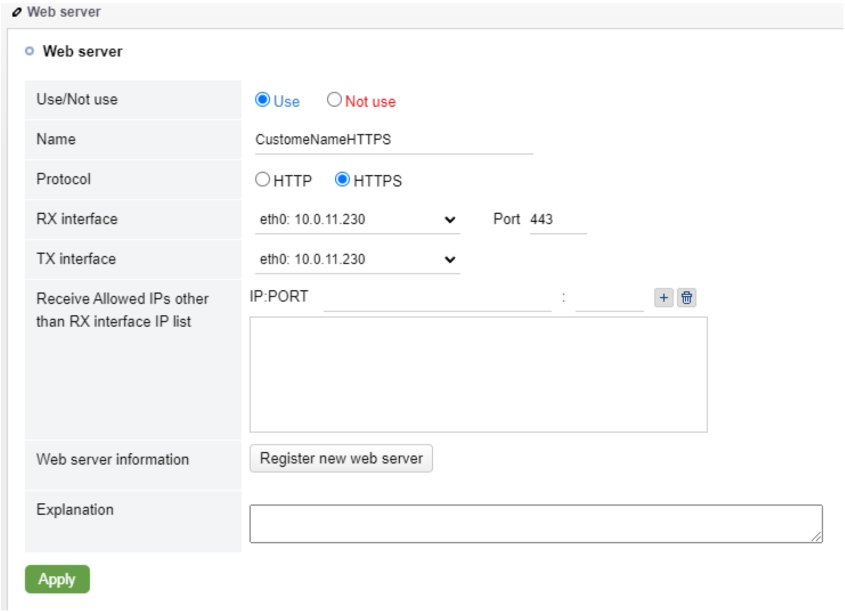


Use/Not use	All	Name		Certificate status	All	Issued to	
Protocol	All	IP		Port		Host name	
RX interface	All	TX interface	All	Explanation			

□	⏻	Name ▼	Protocol ▼	RX/TX ▼	Web server information	Explanation	Change

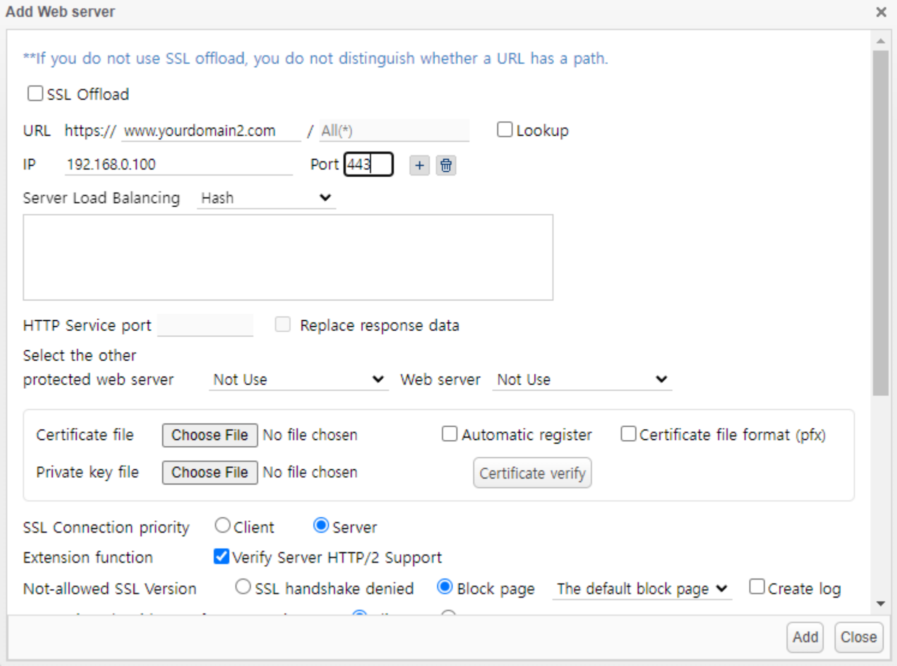
There is no data.

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



Use/Not use	● Use ○ Not use
Name	CustomeNameHTTPS
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
Explanation	

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



Add Web server

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

☐ SSL Offload

URL https:// www.yourdomain2.com / All(*) ☐ Lookup

IP 192.168.0.100 Port 443

Server Load Balancing Hash

HTTP Service port ☐ Replace response data

Select the other protected web server Not Use Web server Not Use

Certificate file Choose File No file chosen ☐ Automatic register ☐ Certificate file format (pfx)

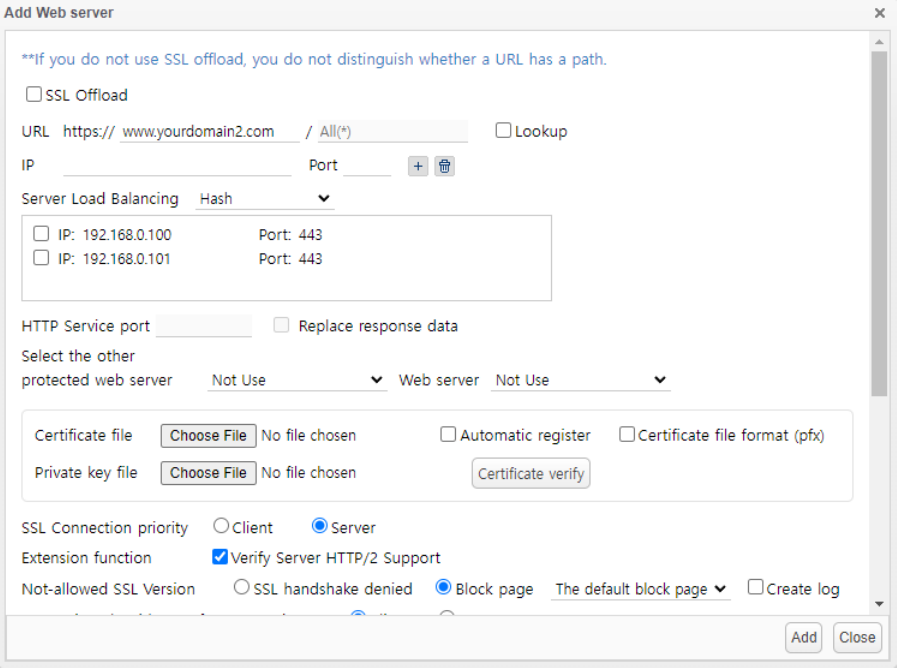
Private key file Choose File No file chosen Certificate verify

SSL Connection priority ○ Client ● Server

Extension function ☑ Verify Server HTTP/2 Support

Not-allowed SSL Version ○ SSL handshake denied ● Block page The default 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.



Add Web server

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

☐ SSL Offload

URL https:// www.yourdomain2.com / All(*) ☐ Lookup

IP Port

Server Load Balancing Hash

☐ 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 Not Use Web server Not Use

Certificate file Choose File No file chosen ☐ Automatic register ☐ Certificate file format (pfx)

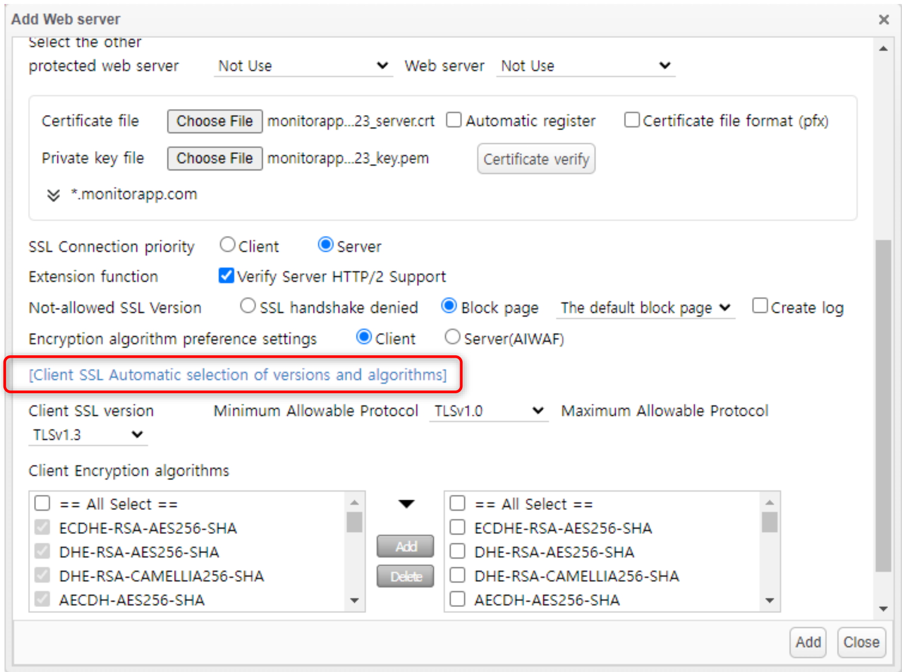
Private key file Choose File No file chosen Certificate verify

SSL Connection priority ○ Client ● Server

Extension function ☑ Verify Server HTTP/2 Support

Not-allowed SSL Version ○ SSL handshake denied ● Block page The default 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.



Add Web server ×

Select the other protected web server: Not Use | Web server: Not Use

Certificate file: Choose File monitorapp...23_server.crt □ Automatic register □ Certificate file format (pfx)

Private key file: Choose File monitorapp...23_key.pem Certificate verify

*.monitorapp.com

SSL Connection priority: ○ Client ● Server

Extension function: ☑ Verify Server HTTP/2 Support

Not-allowed SSL Version: ○ SSL handshake denied ● Block page The default block page □ Create log

Encryption algorithm preference settings: ● Client ○ Server(AIWAF)

[Client SSL Automatic selection of versions and algorithms]

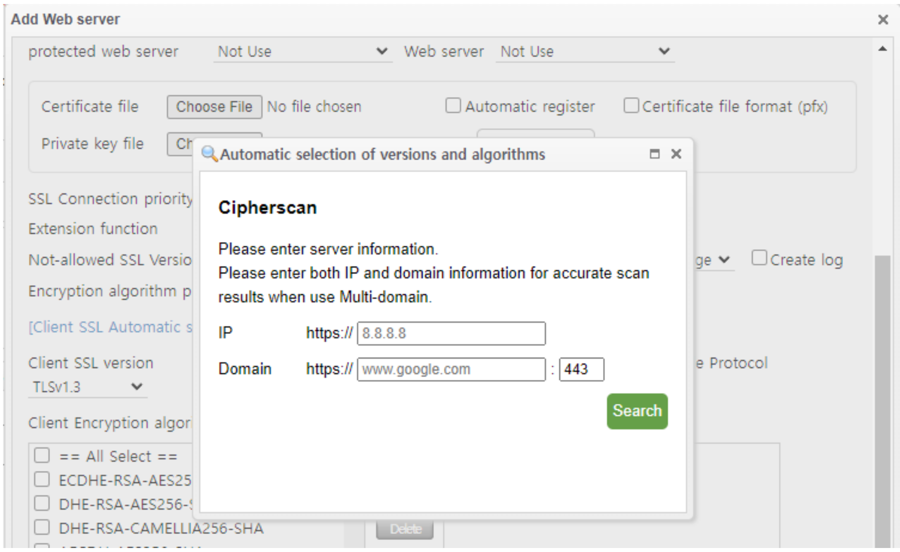
Client SSL version: Minimum Allowable Protocol TLSv1.0 Maximum Allowable Protocol TLSv1.3

Client Encryption algorithms

□ == All Select ==		□ == All Select ==
☑ ECDHE-RSA-AES256-SHA	Add	□ ECDHE-RSA-AES256-SHA
☑ DHE-RSA-AES256-SHA	Delete	□ DHE-RSA-AES256-SHA
☑ DHE-RSA-CAMELLIA256-SHA		□ DHE-RSA-CAMELLIA256-SHA
☑ AECDH-AES256-SHA		□ AECDH-AES256-SHA

Add Close

- 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.



Add Web server ×

Automatic selection of versions and algorithms

Cipherscan

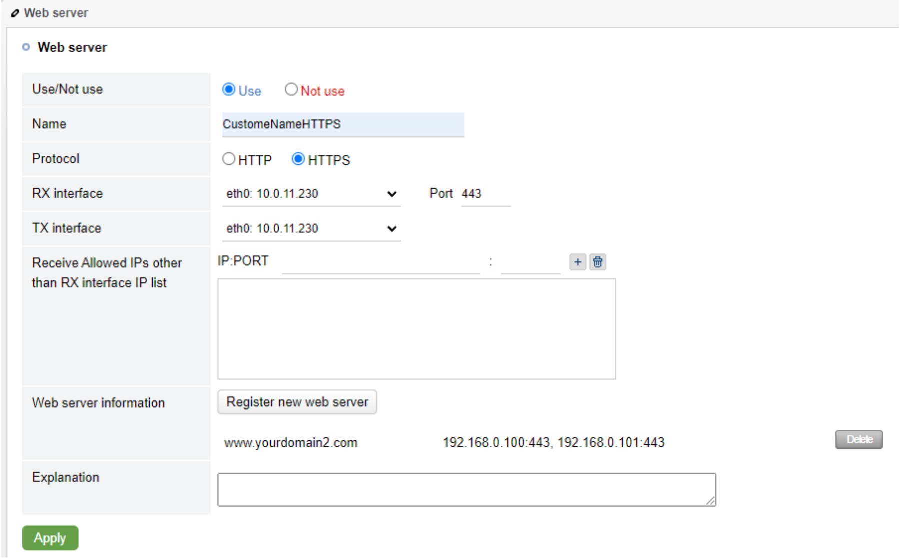
Please enter server information.
Please enter both IP and domain information for accurate scan results when use Multi-domain.

IP https:// 8.8.8.8

Domain https:// www.google.com : 443

Search

- 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.



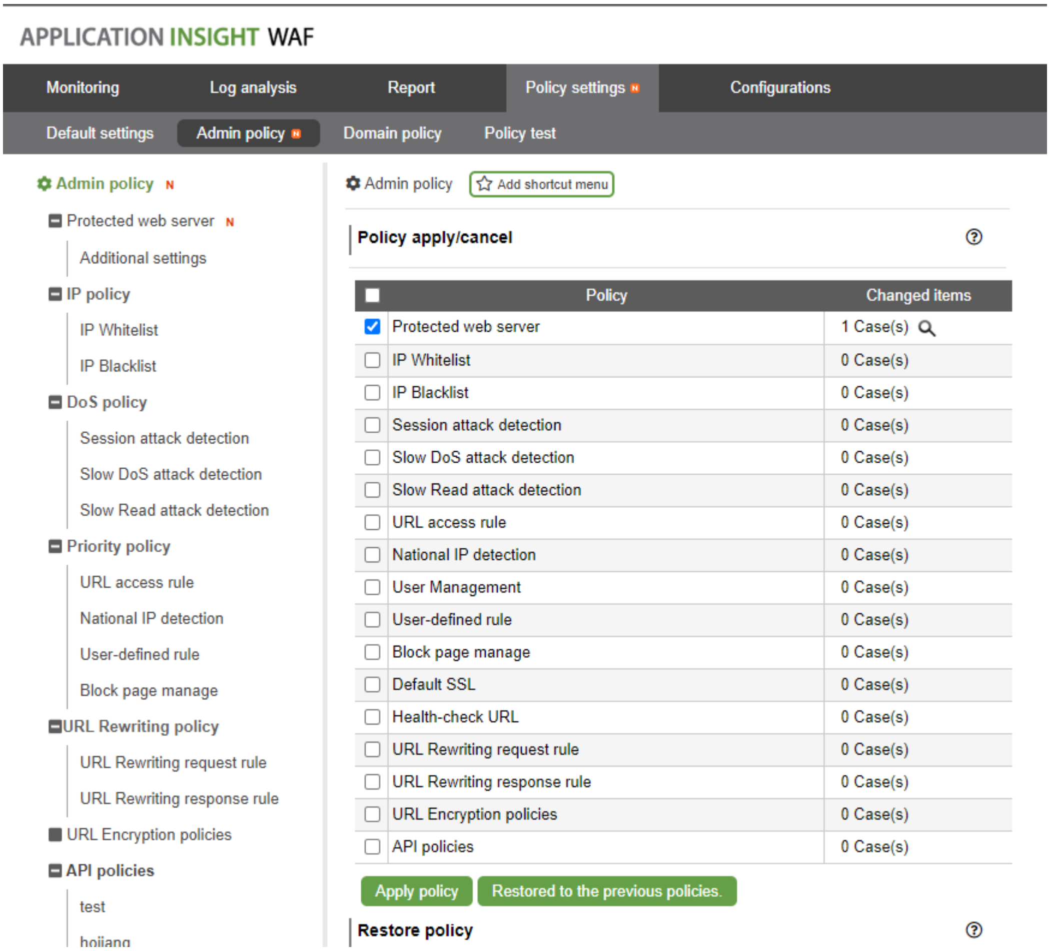
Web server

Web server

Use/Not use	● Use ○ Not use
Name	CustomeNameHTTPS
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 Delete
Explanation	

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

6-3. Apply Policy



- Admin policy N
  - ⊟ Protected web server N
    - 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
    - hojiang

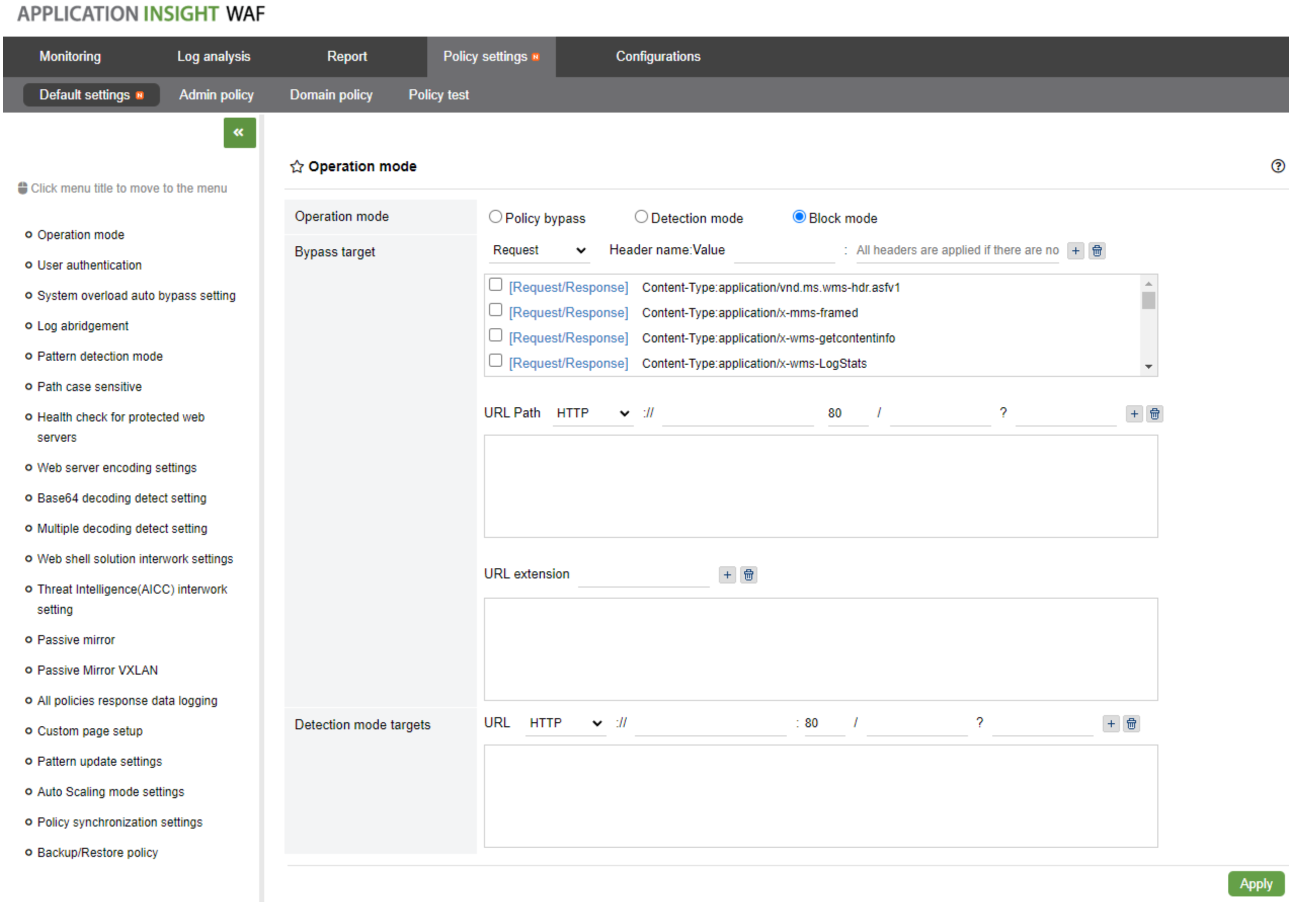
Policy apply/cancel

□	Policy	Changed items
☑	Protected web server	1 Case(s)
□	IP Whitelist	0 Case(s)
□	IP Blacklist	0 Case(s)
□	Session attack detection	0 Case(s)
□	Slow DoS attack detection	0 Case(s)
□	Slow Read attack detection	0 Case(s)
□	URL access rule	0 Case(s)
□	National IP detection	0 Case(s)
□	User Management	0 Case(s)
□	User-defined rule	0 Case(s)
□	Block page manage	0 Case(s)
□	Default SSL	0 Case(s)
□	Health-check URL	0 Case(s)
□	URL Rewriting request rule	0 Case(s)
□	URL Rewriting response rule	0 Case(s)
□	URL Encryption policies	0 Case(s)
□	API policies	0 Case(s)

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 polic**y'.

6-4. Security Policy Block Mode Configuration


APPLICATION INSIGHT WAF
Monitoring
Log analysis
Report
Policy settings
Configurations
Default settings
Admin policy
Domain policy
Policy test
«
Click menu title to move to the menu
Operation mode
User authentication
System overload auto bypass setting
Log abridgement
Pattern detection mode
Path case sensitive
Health check for protected web servers
Web server encoding settings
Base64 decoding detect setting
Multiple decoding detect setting
Web shell solution interwork settings
Threat Intelligence(AICC) interwork setting
Passive mirror
Passive Mirror VXLAN
All policies response data logging
Custom page setup
Pattern update settings
Auto Scaling mode settings
Policy synchronization settings
Backup/Restore policy
Apply

☆ Operation mode

Operation mode: ○ Policy bypass ○ Detection mode ● Block mode

Bypass target: Request Header name:Value : All headers are applied if there are no

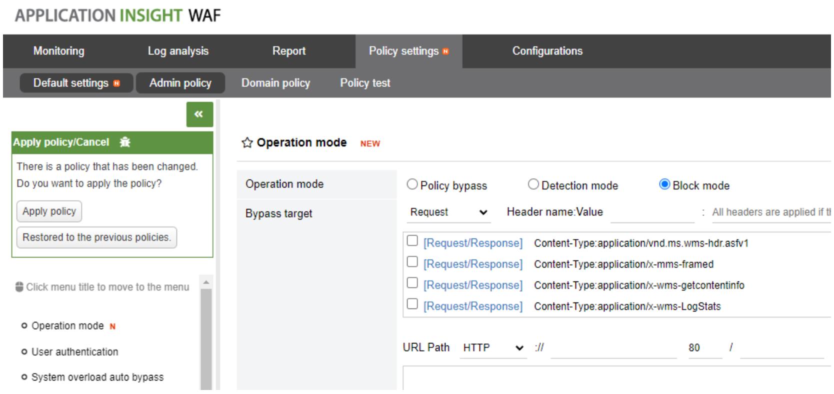
□ [Request/Response] Content-Type:application/vnd.ms.wms-hdr.asfv1
□ [Request/Response] Content-Type:application/x-mms-framed
□ [Request/Response] Content-Type:application/x-wms-getcontentinfo
□ [Request/Response] Content-Type:application/x-wms-LogStats

URL Path HTTP :// 80 / ?

URL extension

Detection mode targets: URL HTTP :// : 80 / ?

- 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.



Apply policy/Cancel

There is a policy that has been changed. Do you want to apply the policy?

Apply policy

Restored to the previous policies.

☆ Operation mode

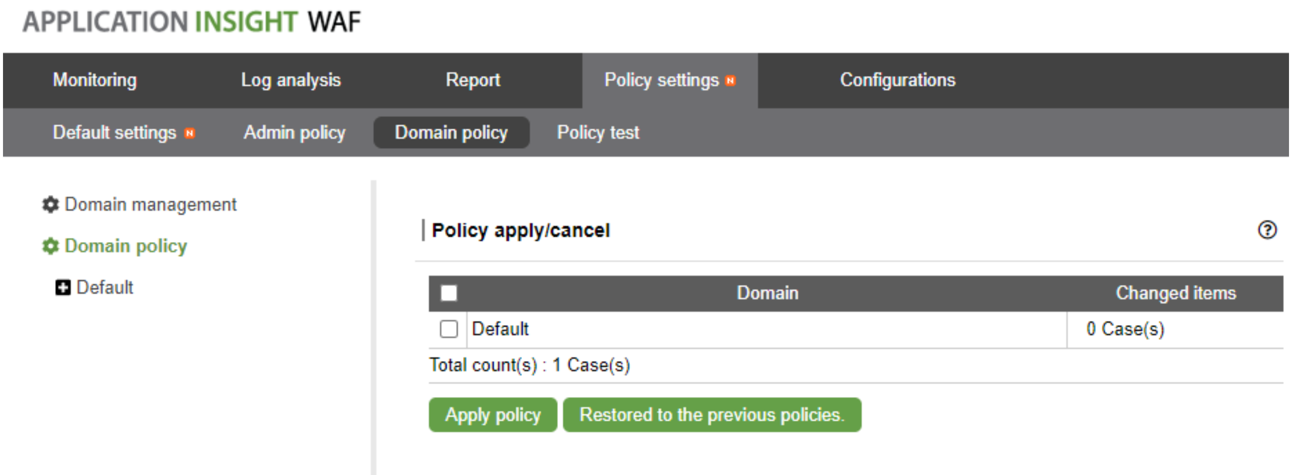
Operation mode: ○ Policy bypass ○ Detection mode ● Block mode

Bypass target: Request Header name:Value : All headers are applied if t

□ [Request/Response] Content-Type:application/vnd.ms.wms-hdr.asfv1
□ [Request/Response] Content-Type:application/x-mms-framed
□ [Request/Response] Content-Type:application/x-wms-getcontentinfo
□ [Request/Response] Content-Type:application/x-wms-LogStats

URL Path HTTP :// 80 /

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

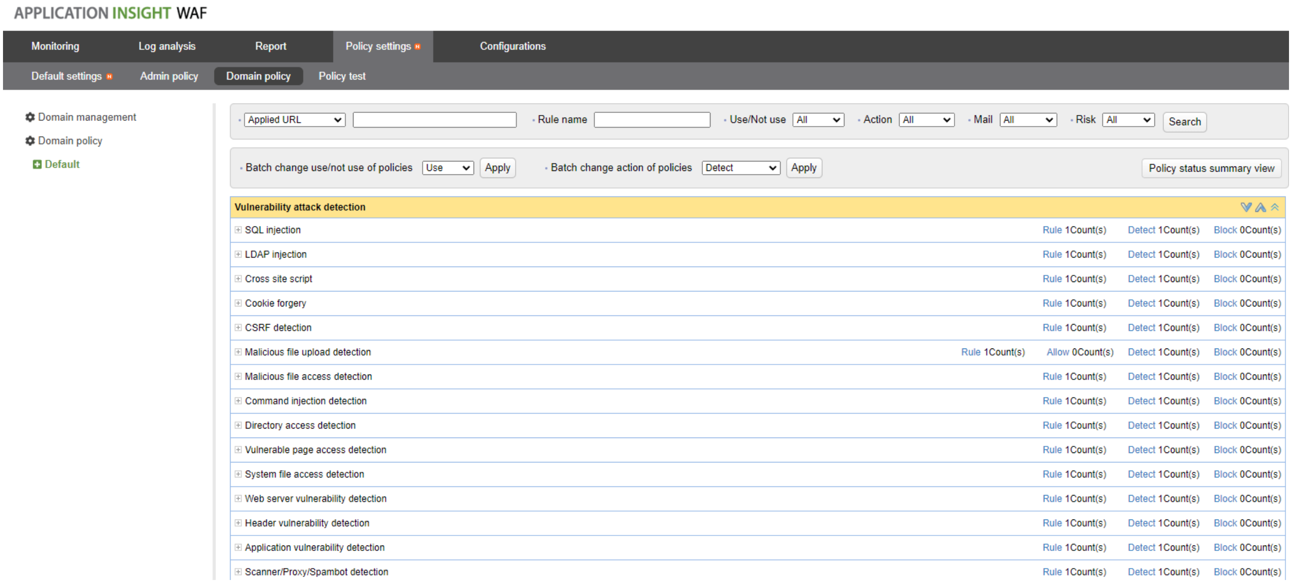


Policy apply/cancel

☐	Domain	Changed items
☐	Default	0 Case(s)

Total count(s) : 1 Case(s)

- 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).)

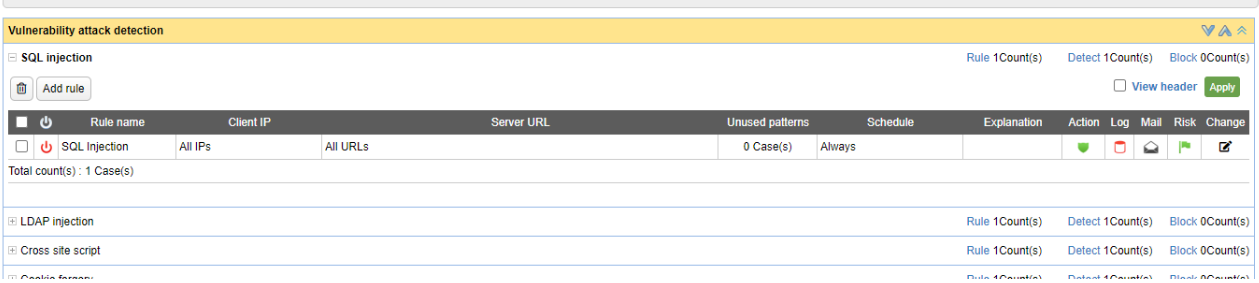


· Applied URL · Rule name · Use/Not use All · Action All · Mail All · Risk All

· Batch change use/not use of policies Use · Batch change action of policies Detect

Vulnerability attack detection				
SQL injection	Rule 1Count(s)		Detect 1Count(s)	Block 0Count(s)
LDAP injection	Rule 1Count(s)		Detect 1Count(s)	Block 0Count(s)
Cross site script	Rule 1Count(s)		Detect 1Count(s)	Block 0Count(s)
Cookie forgery	Rule 1Count(s)		Detect 1Count(s)	Block 0Count(s)
CSRF detection	Rule 1Count(s)		Detect 1Count(s)	Block 0Count(s)
Malicious file upload detection	Rule 1Count(s)	Allow 0Count(s)	Detect 1Count(s)	Block 0Count(s)
Malicious file access detection	Rule 1Count(s)		Detect 1Count(s)	Block 0Count(s)
Command injection detection	Rule 1Count(s)		Detect 1Count(s)	Block 0Count(s)
Directory access detection	Rule 1Count(s)		Detect 1Count(s)	Block 0Count(s)
Vulnerable page access detection	Rule 1Count(s)		Detect 1Count(s)	Block 0Count(s)
System file access detection	Rule 1Count(s)		Detect 1Count(s)	Block 0Count(s)
Web server vulnerability detection	Rule 1Count(s)		Detect 1Count(s)	Block 0Count(s)
Header vulnerability detection	Rule 1Count(s)		Detect 1Count(s)	Block 0Count(s)
Application vulnerability detection	Rule 1Count(s)		Detect 1Count(s)	Block 0Count(s)
Scanner/Proxy/Spambot detection	Rule 1Count(s)		Detect 1Count(s)	Block 0Count(s)

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



Vulnerability attack detection

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

Add rule — □ View header Apply

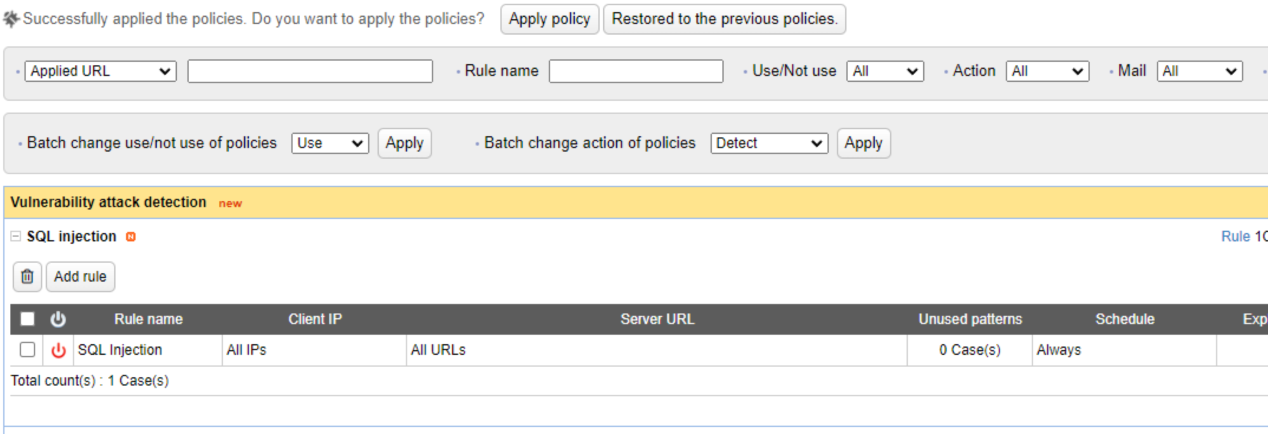
□	⏻	Rule name	Client IP	Server URL	Unused patterns	Schedule	Explanation	Action	Log	Mail	Risk	Change
□	⏻	SQL Injection	All IPs	All URLs	0 Case(s)	Always		🟩		✉	⚑	✎

Total count(s) : 1 Case(s)

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

⊞ Cross site script — Rule 1Count(s) Detect 1Count(s) Block 0Count(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? Apply policy Restored to the previous policies.

· Applied URL · Rule name · Use/Not use All · Action All · Mail All

· Batch change use/not use of policies Use Apply · Batch change action of policies Detect Apply

Vulnerability attack detection new

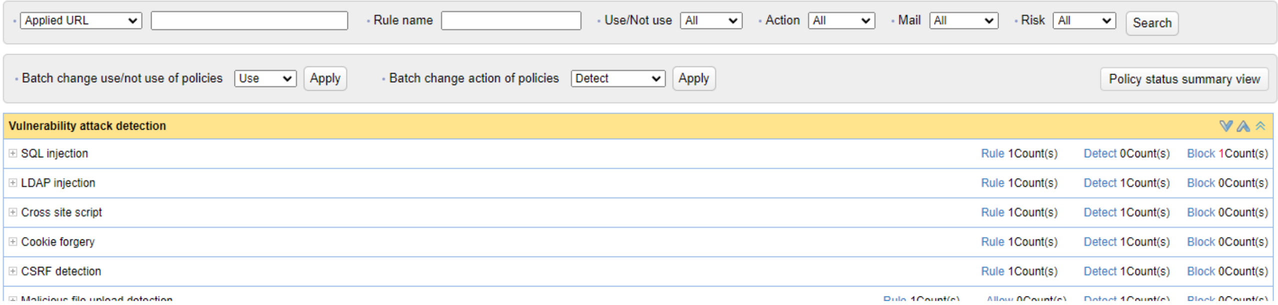
⊟ SQL injection — Rule 1C

Add rule

□	⏻	Rule name	Client IP	Server URL	Unused patterns	Schedule	Exp
□	⏻	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 All · Action All · Mail All · Risk All Search

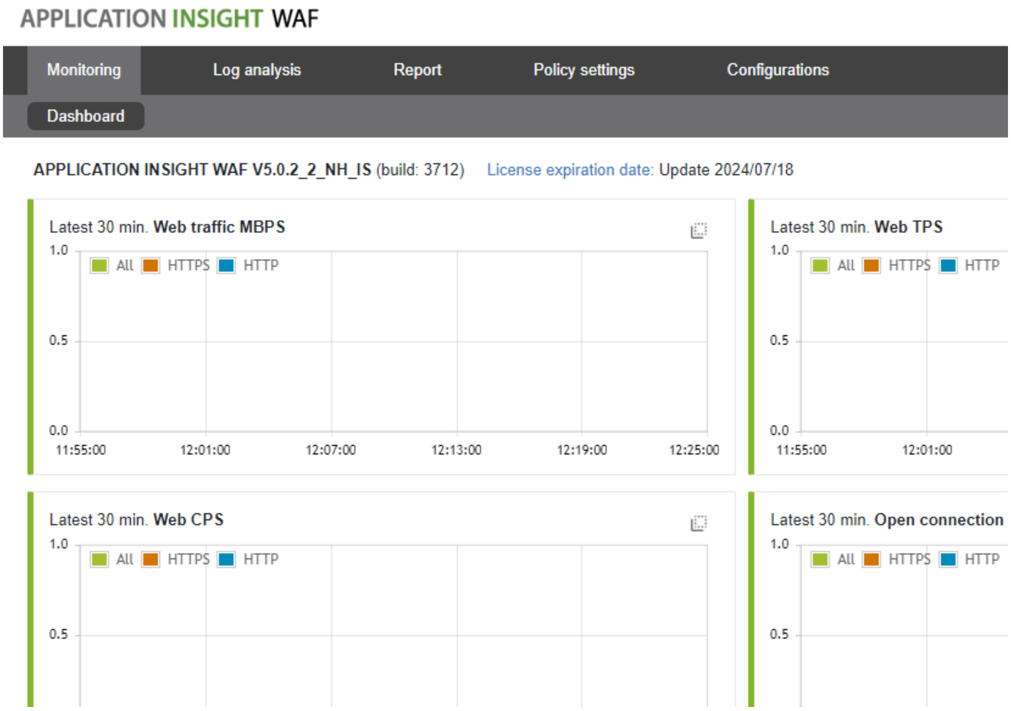
· Batch change use/not use of policies Use Apply · Batch change action of policies Detect Apply — Policy status summary view

Vulnerability attack detection

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



APPLICATION INSIGHT WAF V5.0.2_2_NH_IS (build: 3712) License expiration date: Update 2024/07/18

- 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.

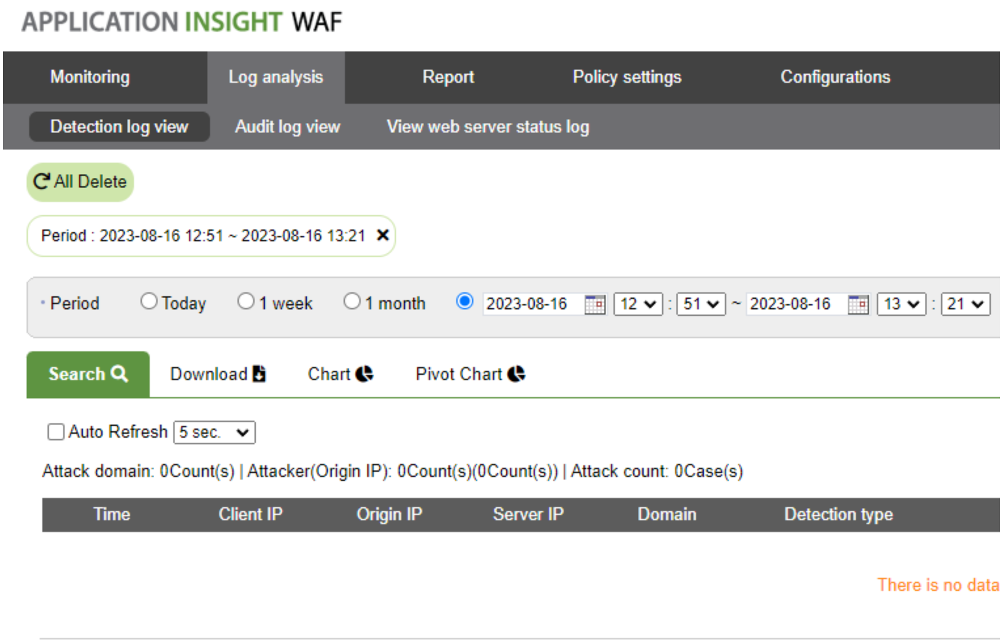
Step 2: Send Sample Traffic to AIWAF-VE:

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.



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

☐ Auto Refresh 5 sec.

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

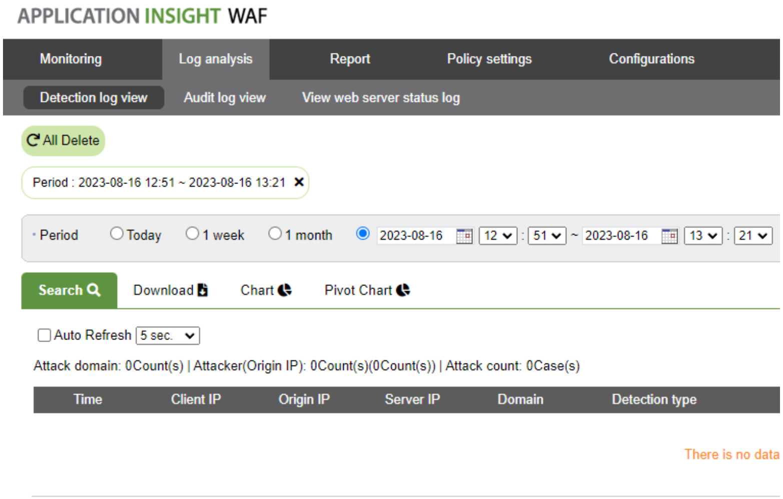
Time	Client IP	Origin IP	Server IP	Domain	Detection type

There is no data

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



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

□ Auto Refresh 5 sec.

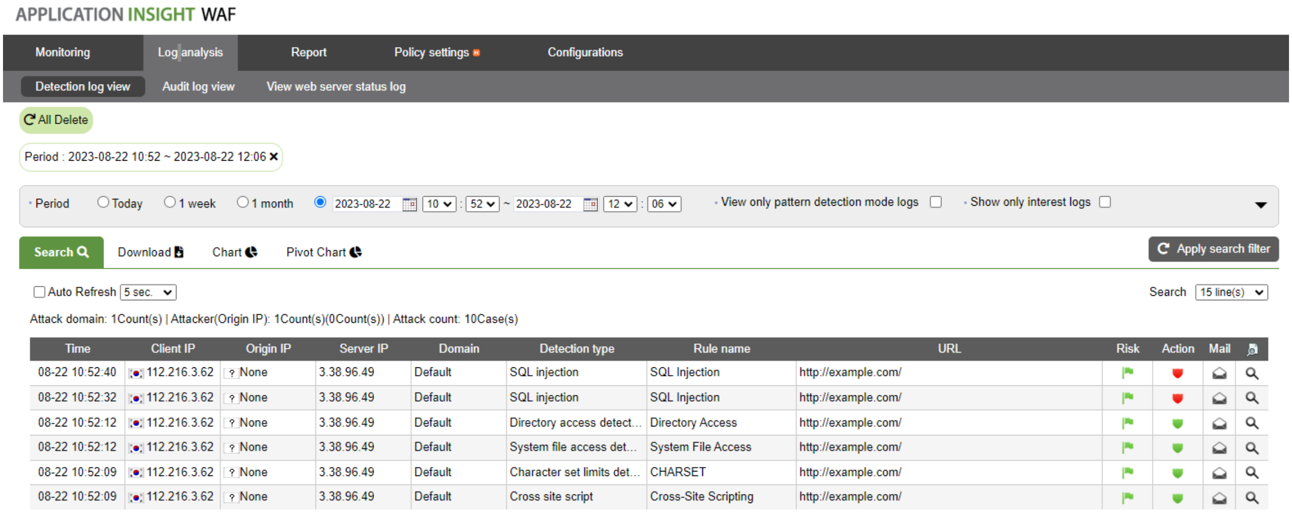
Attack domain: 0Count(s) | Attacker(Origin IP): 0Count(s)(0Count(s)) | Attack count: 0Case(s)

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)



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 □

□ 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/	⚑	🟥	✉	🔍
08-22 10:52:32	112.216.3.62	? None	3.38.96.49	Default	SQL injection	SQL Injection	http://example.com/	⚑	🟥	✉	🔍
08-22 10:52:12	112.216.3.62	? None	3.38.96.49	Default	Directory access detect...	Directory Access	http://example.com/	⚑	🟩	✉	🔍
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/	⚑	🟩	✉	🔍
08-22 10:52:09	112.216.3.62	? None	3.38.96.49	Default	Character set limits det...	CHARSET	http://example.com/	⚑	🟩	✉	🔍
08-22 10:52:09	112.216.3.62	? None	3.38.96.49	Default	Cross site script	Cross-Site Scripting	http://example.com/	⚑	🟩	✉	🔍

- 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