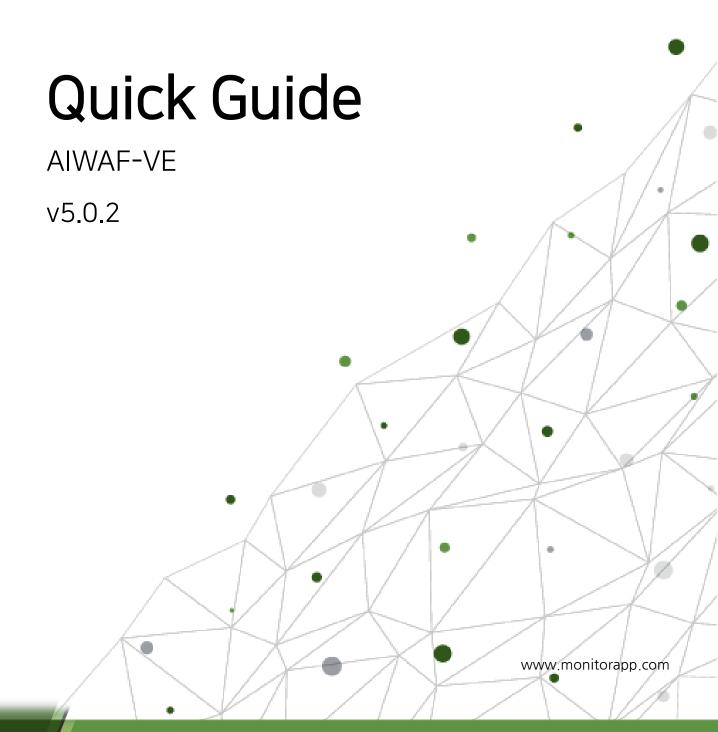
MONITOR PP



.

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 ✓ Sign In		
English ~		
English	administrator	
Sign In	English	~
	Sign In	

- Open your internet browser and access by entering the assigned IP from the instance as follows: 'https://[AIWAF-VE IP]:222'. (e.g., <u>https://192.168.10.110:222</u>)
- 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 ana	alysis	Report	Policy settings	Configura	tions	
ľ	Dashboard							
	You are using t	the default ID and	the default passv	vord. Please change	ID and password			
0	Administrato	r settings						(?)
	Name		Administrator					
	ID		administrator					
	Password		Current passwo	ord				
			New password					
			Confirm new pa	assword				
	Password ch	ange notification	60 day(s)					
	Two-Factor A	Authentication	Use	Not use				
	Allowed IP		IP		+ 🖶			
	Recipient E-r	mail	E-mail		+ 🖶			
	Explanation							
			L				/	
	Apply							

- 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.

Oconfigure Static IP (Optional):

APPLICATION IN:	SIGHT WAF							
Monitoring	Log analysis	Report	Policy settings	Configurations				
Administrator settings	System setti	ings NIC settings	Product settings	Log management	Service control			
Click menu title to move t	«	습 IP settings						0
 IP settings 		Туре	ODHCP	STATIC				
 Mail settings Telegram notification set 		IP	IP Version	● IPv4 ○ IPv6				
 Backup server settings 	ttings			✓ IP	Netmask	Gateway	+ 8	
Hostname settings								
 Time synchronization se 	ttings							
• Time zone settings								
 SNMP GET settings 		mgmt IP						
• SNMP TRAP settings		Netmask						
		Gateway						
		DNS 1						
		DNS 2						
							A	pply

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:

APPLICATION INSIGHT WAF

Monitoring	Log analysis	Report	Policy settings	Configurations			
Administrator settings	System settin	gs NIC settings	Product settings Lo	og management	Service control		
Click menu title to move t	« o the menu	Online update	License update				Apply
• License management		Use/Not use	 Use 	O Not use	9		
• HA settings		Activation Code	8characters	- 4charac - 4chara	- 4charac - 12characters	Check	
 Configurations synchron settings Program/Configuration b 		Server address	O IP: Domain:		Port:	443 🗲	
 National IP DB settings Whois settings 							Apply
 Open API settings 		☆ HA settings					0
		HA mode	Not use	⊖ Active-	Standby		
							Apply

- 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

Monitoring	Log analysis	Report	Policy settings	Configurations	
Dashboard					
Click menu title to more	ve to the menu	☆ Time zone settin	gs		0
• IP settings		Current time	Tue Aug 22 8:45:	14 KST 2023	
• Mail settings		Time zone	Asia/Seoul	~	
• Telegram notification	settings				Apply
• Backup server setting	gs				, 46A
• Hostname settings					
• Time synchronization	n settings	☆ SNMP GET settin	igs		0
• Time zone settings					
• SNMP GET settings		SNMP MIBs list			
 SNMP TRAP settings 	5	Version	SNMPv2	○ SNMPv	3
		A			

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

APPLICATION INSIGHT WAF

Monitoring	Log analysis	Report	Policy settings	Configurations	
Administrator settings	System setting	s NIC settings	Product settings Lo	og management	Service control
	«				
Click menu title to move to	o the menu	☆ Language setting	5		0
 Language settings 					
		Language	English	~	
 License management 					
 HA settings 					Apply
 Configurations synchroni settings 	ization				
• Program/Configuration b	ackup	☆ License managem	ient		٢
 National IP DB settings 		Product license			

Language Setup: Configurations > System Settings > Language Settings

5. Update Signature and Geolocation DB:

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

APPLICATION I	NSIGHT WAF										
Monitoring	Log analysis	Report	Policy s	settings	Configurations						
Default settings	Admin policy	Domain policy	Policy test								
	×	습 Pattern upd	ate settings								
Click menu title to mo	ve to the menu	Pattern updat	e server								0
 Operation mode 		Server address		O IP:							
• User authentication				Domain:	api.monitorapp.com		Port:	443	*		
 System overload aut 	o bypass setting	Auto pattern up	date	⊙Use Ot	Not use						
 Log abridgement 											Apply
 Pattern detection mo 	de										Abbiy
 Path case sensitive 		Online patterr	n update								0
 Health check for prot servers 	lected web	The current patt	ern version	W.5.0.057.000	07_20230727_79f5fc5e30cf	6bc9be5a827dcd1	69051ccd	e6422c6052	20270ebd77112	89f425e1	
• Web server encoding	g settings	Latest pattern v	ersion	Check versi	on W.5.0.057.0007_20230	727_79f5fc5e30c	6bc9be5a	827dcd1690	051ccde6422c6)520270ebd7711289	f425e1
 Multiple decoding de 	tect setting										Pattern update
• Web shell solution in	terwork settings	1									
• Threat Intelligence(A	ICC) interwork	Offline pattern	1 update								0
setting		Upload pattern f	ile (Choose File	No file chosen						
 Passive mirror 											
 Passive Mirror VXLA 	N										Apply
 All policies response 	data logging										
 Custom page setup 		습 Auto Scalin	a mode setting								0
 Pattern update settin 	gs	A Auto adality	a more serring	-							U

- [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.

APPLICATION INS	SIGHT WAF				
Monitoring	Log analysis	Report Pa	blicy settings	Configurations	
Administrator settings	System settings	NIC settings Pro	oduct settings Lo	og management	Service control
Click menu title to move to	o the menu]			
 Language settings 	合	lational IP DB setting	5		
 License management HA settings 	N	ational IP DB automatic	updates		0
 Configurations synchron settings 	ization Au	omatic update	 Use 	◯ Not us	8
• Program/Configuration b	ackup				Apply
National IP DB settings	N	ational IP DB file upload	i		0
 Whois settings 	Th	e current national IP DB i	nformation: GeoIP2 0	Country database, Bu	ild Epoch: 2019-12-24
 Open API settings 	File	upload	Choose File	No file chosen	
					Apply
	公 1	Vhois settings			0

- [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

APPLICATION INSIGHT W	ΆF							
Monitoring Log analys	is Report	Policy settings	Configurations					
Default settings Admin policy	Domain policy Policy	y test						
Admin policy	Admin policy > Protecte	ed web server 🟠 Add	shortcut menu					
Protected web server Additional settings								Cert. Quick change Add rule
IP policy	- Use/Not use	All	∽ - Name		Certificate status	All 🗸	- Issued to	
IP Whitelist	- Protocol	All	 ✓ IP 		- Port		Host name	
IP Blacklist	 RX interface 	All	 TX interface 	All	 Explanation 			
DoS policy					_			
Session attack detection	(U)				Q Search			15 line(s) 🗸
Slow DoS attack detection	∎ رڻ Na	ame 🔻 🛛 Pro	tocol 🔻 RX/TX 🔻		Web se	rver information		Explanation Change
Slow Read attack detection								
Priority policy					There is no data.			
URL access rule								

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

Web server	
• Web server	
Use/Not use	Use ONot use
Name	CustomeName
Protocol	● HTTP ○ HTTPS
RX interface	eth0: 10.0.11.230 V 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'.

dd Web server		
URL http:// www.yourdomair	n.com / All(*)	
IP 192.168.0.100	Port 80 + 🖶	
Server Load Balancing Has	h 🗸	
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.

d Web server			
URL http:// www.yourdoma	in.com / All(*)		
IP	Port	+ 🖶	
Server Load Balancing Ha	ish 🗸		
DIP: 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 		
	Use/Not use	● Use O Not use	
2	Name	CustomeName	
	Protocol	● HTTP ○ HTTPS	
J.	RX interface	eth0: 10.0.11.230 V Port 80	
	TX interface	eth0: 10.0.11.230 🗸	
	Receive Allowed IPs other than RX interface IP list	IP:PORT: + 世	
	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 p	olicy > Protected web server 🗠 🏠 Add shortcut menu										
🕸 Suci	cessfully applied the p	oolicies. Do	o you want to app	oly the policies? To the Policies	cy management menu	pply policy Restored to the p	previous policies.			Cert. Quick change	Add rule
• Prot	/Not use ocol nterface	All All All	× ×	- Name - IP - TX interface	All v	Certificate status Port Explanation	All		 Issued to Host name 		
	ტ					Q Search				1	15 line(s) 🗸
• 4) Name 🔻	7	Protocol 🔻	RX/TX 🔻		Web serv	rer information			Explanation	Change
<u>ا</u>	CustomeName		HTTP	RX: eth0 10.0.11.230:80 TX: eth0 10.0.11.230	Host name: www.yourd - 192.168.0.100:80 - 192.168.0.101:80	Jomain.com					ľ
Total co	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

APPLICATION INSIGHT WAF

Monitoring	Log analysis	Report	Policy settings	Configurations					
Default settings	Admin policy	Domain policy Polic	y test						
Admin policy		Admin policy > Protect	ed web server (☆ A	dd shortcut menu					
Protected we	b server								
Additional se	ettings								Cert. Quick change Add rule
IP policy		- Use/Not use	All	 ✓ • Name 		Certificate status	All	✓ Issued to	
IP Whitelist		- Protocol	All	 ✓ 		- Port		Host name	
IP Blacklist		- RX interface	All	 TX interface 	All 🗸	 Explanation 			
DoS policy									15 line(s) 🗸
Session atta	ick detection	(b) (b)				Q Search			To line(s) 🗸
Slow DoS at	ttack detection	∎ (b) N	ame 🔻 🛛 F	Protocol 🔻 RX/TX 🔻		Web ser	rver information		Explanation Change
	attack detection				The	e is no data.			
Priority polic					Ther	e is nu uata.			
URL access	rule								

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

Web server	
• Web server	
Use/Not use	● Use O Not use
Name	CustomeNameHTTPS
Protocol	OHTTP OHTTPS
RX interface	eth0: 10.0.11.230 V Port 443
TX interface	eth0: 10.0.11.230 🗸
Receive Allowed IPs other than RX interface IP list	IP:PORT + 1
Web server information	Register new web server
Explanation	
Apply	

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

*If you do not use SSL offload, you	ı do not distinguish w	whether a URL has a path.	
JRL https:// www.yourdomain2.com	/ All(*)		
P 192.168.0.100	Port 443 +	- 🗑	
Server Load Balancing Hash	~		
	Replace response) data	
Select the other protected web server Not Use	✓ Web	eb server Not Use 🗸	
Certificate file Choose File No	o file chosen	Automatic register Certificate file format (pfx)	
Private key file Choose File No	o file chosen	Certificate verify	
-	Server		
SSL Connection priority OClient			
	Server HTTP/2 Suppo	ort	
Extension function		ort Block pageThe 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 o	do not distinguish	whether a URL ha	is a path.	*
URL https:// www.yourdomain2.com	/ All(*)		kup	
IP	Port -	+ ⊕		
Server Load Balancing Hash	~			
IP: 192.168.0.100 Port IP: 192.168.0.101 Port	: 443 : 443			
HTTP Service port Select the other protected web serverNot Use		e data eb server <u>Not Us</u>	e 🗸	
Certificate file Choose File No Private key file Choose File No		Certificate		e format (pfx)
SSL Connection priority OClient	Server			
Extension function	erver HTTP/2 Supp	ort		
Not-allowed SSL Version OSSL I	handshake denied	Block page	The default block page \checkmark	Create log
	a			Add Close

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

protected web server Not Use ✓ Verificate file Choose File monitorapp23_server.crt Automatic register Certificate file format (pfx) Private key file Choose File monitorapp23_key.pem Certificate verify Verificate file Choose File monitorapp23_key.pem Certificate verify Verificate verify Client Server Extension function Verify Server HTTP/2 Support Not-allowed SSL Version OSL handshake denied Block page The default block page Create log Encryption algorithm preference settings © Client Server(AlWAF) [Client SSL Automatic selection of versions and algorithms] Client Encryption algorithms Client Encryption algorithms === All Select == CCDHE-RSA-AES256-SHA Maximum Allowable Protocol Client Encryption algorithms === All Select == ECDHE-RSA-AES256-SHA DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA OHE-RSA-AES256-SHA DHE-RSA-CAMELLIA256-SHA DHE-RSA-CAMELLIA256-SHA DHE-RSA-CAMELLIA256-SHA	elect the other		
Private key file Choose File monitorapp23_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 ✓ ✓ Maximum Allowable Protocol TLSv1.0 ✓ Maximum Allowable Protocol TLSv1.4 □ == All Select == □ == All Select == □ ECDHE-RSA-AES256-SHA □ DHE-RSA-AES256-SHA □ DHE-RSA-AES256-SHA □ DHE-RSA-AES256-SHA	orotected web server Not Use 🗸 We	b server Not Use 🗸	
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 Client Intervention algorithm preference settings Client SSL Automatic selection of versions and algorithms] Client SSL version Minimum Allowable Protocol TLSv1.0 V Maximum Allowable Protocol TLSv1.3 V Client Encryption algorithms = = All Select == ECDHE-RSA-AES256-SHA ECDHE-RSA-AES256-SHA DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA			nat (pfx)
SSL Connection priority Client ● Server Extension function ✓ Verify Server HTTP/2 Support Not-allowed SSL Version ○ SSL handshake denied ● Block page he 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 [LSv1.3 ✓ ○ Client Encryption algorithms ○ == All Select == ○ [Client Encryption algorithms ○ == All Select == ○ ECDHE-RSA-AES256-SHA ○ [DHE-RSA-AES256-SHA ○ DHE-RSA-AES256-SHA ○ DHE-RSA-AES256-SHA ○	Private key file Choose File monitorapp23_key.pem	Certificate verify	
Extension function Verify Server HTTP/2 Support Not-allowed SSL Version OSSL handshake denied OBlock page The default block page Create log Encryption algorithm preference settings Client Server(AIWAF) [Client SSL Automatic selection of versions and algorithms] [Client SSL Automatic selection of versions and algorithms] Client SSL version Minimum Allowable Protocol TLSv1.0 V Maximum Allowable Protocol TLSv1.3 V Client Encryption algorithms $ = = All Select == II Select == ECDHE-RSA-AES256-SHA DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA $			
Extension function Verify Server HTTP/2 Support Not-allowed SSL Version OSSL 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 V Maximum Allowable Protocol TLSv1.3 V [Client Encryption algorithms] [Client Encryption algorithms [Client SSL-AES256-SHA] [Client SSL-AES256-SHA] [Client-RSA-AES256-SHA] [Client-RSA-AES256-SHA	SL Connection priority OClient OServer		
Not-allowed SSL Version SSL handshake denied Image: Block page The default block page Create log Encryption algorithm preference settings Image: Client Server(AlWAF) [Client SSL Automatic selection of versions and algorithms] Client SSL version Minimum Allowable Protocol TLSv1.0 Maximum Allowable Protocol TLSv1.3 Image: Client SSL version Minimum Allowable Protocol TLSv1.0 Maximum Allowable Protocol TLSv1.3 Image: Client SSL version Image: Client SSL version Image: Client SSL version Maximum Allowable Protocol TLSv1.3 Image: Client SSL version Image: Client SSL version Image: Client SSL version Image: Client SSL version Client Encryption algorithms Image: Client SSL version Image: Client SSL version Image: Client SSL version Image: Second Se		ort	
Encryption algorithm preference settings Client SEL Automatic selection of versions and algorithms] Client SSL version Minimum Allowable Protocol TLSv1.0 Client SSL version Minimum Allowable Protocol TLSv1.0 Client Encryption algorithms $= All Select == ECDHE-RSA-AES256-SHA$ $DHE-RSA-AES256-SHA$ $DHE-RSA-AES256-SHA$		-	Create log
[Client SSL Automatic selection of versions and algorithms] Client SSL version Minimum Allowable Protocol TLSv1.3 ✓ Client Encryption algorithms = = All Select == ECDHE-RSA-AES256-SHA DHE-RSA-AES256-SHA	-		
Client SSL version Minimum Allowable Protocol TLSv1.0 V Maximum Allowable Protocol TLSv1.3 V Client Encryption algorithms = = All Select == ECDHE-RSA-AES256-SHA DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA	31 - 5 - 1		
TLSv1.3 Client Encryption algorithms == All Select == ECDHE-RSA-AES256-SHA DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA Add DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA Add DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA Add DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA 			
Client Encryption algorithms = = All Select == ECDHE-RSA-AES256-SHA DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA		TLSv1.0 Maximum Allowable Protocol	
== All Select == Image: Constraint of the select and the select an			
Image: Second	lient Encryption algorithms		_
DHE-RSA-AES256-SHA			
DHE-KSA-AES250-SHA			
	DHE-KSA-AES250-SHA		
AECDH-AES256-SHA			

- 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	>
protected web server Not Use 🗸 Web server Not Use 🗸	1
Certificate file Choose File No file chosen Automatic register Certificate file format (pfx) Private key file Cr Automatic selection of versions and algorithms I X	
SSL Connection priority Cipherscan Extension function Please enter server information. Not-allowed SSL Versio Please enter both IP and domain information for accurate scan Encryption algorithm p results when use Multi-domain	
[Client SSL Automatic s IP https:// 8.8.8 Client SSL version Domain https:// www.google.com : [443]	
TLSv1.3 ✓ Client Encryption algor Search □ == All Select == ECDHE-RSA-AES25 □ BECDHE-RSA-AES25 □ BECDHE-RSA-AES25	
DHE-RSA-AES256-5 Dedee	

- 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.

0	Web server		
(Web server		
	Use/Not use	Use ONot use	
	Name	CustomeNameHTTPS	
	Protocol	OHTTP OHTTPS	
	RX interface	eth0: 10.0.11.230 V Port 443	
	TX interface	eth0: 10.0.11.230 V	
	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	Deiele
	Explanation		
	Apply		

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

6-3. Apply Policy

Monitoring	Log analysis	Report	Policy settings	Configurations	
Default settings	Admin policy	Domain policy	Policy test		
Admin policy N		Admin policy	슈 Add shortcut menu		
Protected web	server N	Policy apply/ca	naal		(?)
Additional set	tings		ncer		()
IP policy			Policy		Changed items
IP Whitelist		Protected we	eb server	1 (Case(s) Q
IP Blacklist		IP Whitelist		0 (Case(s)
DoS policy		IP Blacklist		0 (Case(s)
Session attac	k detection	Session atta	ck detection	0 (Case(s)
Slow DoS atta		Slow DoS at	tack detection	0 (Case(s)
		Slow Read a	ttack detection	0 (Case(s)
	tack detection	URL access	rule	0 (Case(s)
Priority policy		National IP d	letection	0 (Case(s)
URL access r	ule	User Manage	ement	0 (Case(s)
National IP de	etection	User-defined	l rule	0 (Case(s)
User-defined	rule	Block page r	nanage	0 (Case(s)
Block page m	anage	Default SSL		0 (Case(s)
URL Rewriting	policy	Health-check	URL	0 0	Case(s)
URL Rewritin		URL Rewritin	ng request rule	0 (Case(s)
	g response rule	URL Rewritin	ng response rule	0 (Case(s)
		URL Encrypt	ion policies	0 0	Case(s)
URL Encryption	policies	API policies		0 (Case(s)
API policies		Apply policy	Restored to the previous poli	cies	
test			- reaction to the provides poil		-
hoiiang		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

Monitoring	Log analysis	Report	Policy settings	Configurations				
Default settings	Admin policy	Domain policy Po	olicy test					
Click menu title to move	to the menu	☆ Operation mode						0
		Operation mode	O Policy by	oypass O Detection mode	Block mode			
 Operation mode User authentication 		Bypass target	Request	✓ Header name:Value	: All headers a	are applied if there are no +	• 🖶	
 System overload auto I 	bypass setting			est/Response] Content-Type:application				
 Log abridgement 				est/Response] Content-Type:application				
• Pattern detection mode	e			est/Response] Content-Type:application est/Response] Content-Type:application			•	
• Path case sensitive								
 Health check for protect servers 	cted web		URL Path	HTTP • ://	80 /	?	+ 🖶	
• Web server encoding s	settings							
• Base64 decoding dete	ct setting							
• Multiple decoding dete	ct setting							
• Web shell solution inter	rwork settings		URL extensi	sion + 🖶				
 Threat Intelligence(AIC setting 	C) interwork							
• Passive mirror								
• Passive Mirror VXLAN								
• All policies response da	ata logging							
 Custom page setup 		Detection mode targe	ts URL HTT	TP 🗸 ://	: 80 /	?	+ 🖶	
• Pattern update settings	5							
 Auto Scaling mode set 	tings							
• Policy synchronization	settings							
• Backup/Restore policy								
								Apply

• 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								
Monitoring Log	g analysis	Report	Policy	/ settings 🛚	Co	onfigurations		
Default settings 🛤 🛛 Ad	min policy	Domain policy	Policy test					
Apply policy/Cancel 🚊	«	☆ Operation mo	de _{NEW}					
Do you want to apply the policy?	-	Operation mode		O Policy b	/pass	O Detection mode	Block mode	
Apply policy Restored to the previous policie	s.	Bypass target			st/Response]	ader name:Value	n/vnd.ms.wms-hdr.asfv1	ers are applied if th
Click menu title to move to the menu						Content-Type:application Content-Type:application	-	
Operation mode N	- 11							
• User authentication	- 11			URL Path	HTTP ¥	://	80 /	
 System overload auto bypass 								

• 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

Monitoring	Log analysis	Report	Policy settings N	Configurations	
Default settings N	Admin policy	Domain policy	Policy test		
 Domain management Domain policy 	nt	Policy apply	r/cancel		0
Default				Changed items 0 Case(s)	

- <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).)

APPLICATION INSIGHT WAF

Monitoring Log analysis	Report Policy settings • Configurations	
Default settings Admin policy	Domain policy Policy test	
Domain management Domain policy	Applied URL SelNot use All SelNot use	▼ · Risk [All ▼] Search
Default	Batch change use/not use of policies Use v Apply · Batch change action of policies Detect v Apply	Policy status summary view
	Vulnerability attack detection	× A V
	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)
	E 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)
	\boxplus Vulnerable page access detection	Rule 1Count(s) Detect 1Count(s) Block 0Count(s)
	① System file access detection	Rule 1Count(s) Detect 1Count(s) Block 0Count(s)
	equal Web server vulnerability detection	Rule 1Count(s) Detect 1Count(s) Block 0Count(s)
	\oplus 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					V & *
SQL injection				Rule 1Count(s)	Detect 1Count(s) Block 0Count(s)
Add rule					View header Apply
🔲 😃 🛛 Rule name	Client IP	Server URL	Unused patterns S	chedule 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
				Rule 1Count(s)	Detect 1Count(s) Block 0Count(s
🗆 Caalija faraani				Dulo (Count/o)	Datast (Count/s) Dissle (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 poli	icies. Do you want to apply	the policies? Apply policy	Restored to th	e previous policies.			
Applied URL		Rule name		Use/Not use All	Action Al	Mail All	•
- Batch change use/not use o	of policies Use 🗸 Ap	• Batch change ac	tion of policies	Detect			
Vulnerability attack detection	new						
□ SQL injection 🛛							Rule 10
Add rule							
🔲 😃 Rule name	Client IP		Server URL		Unused patterns	Schedule	Ехр
SQL Injection	All IPs	All URLs			0 Case(s)	Always	
Total count(s) : 1 Case(s)							

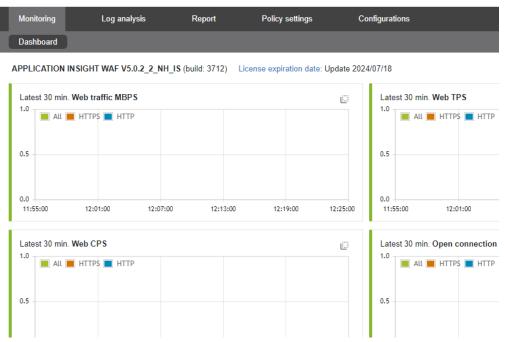
• Similar to saving other modifications, click on 'Apply policy' at the top to save your changes.

Applied URL V SerNot use All Action All	✓ Mail All	✓ Risk All	▼ Search	
Batch change use/not use of policies Use			Policy status	summary view
Vulnerability attack detection				♥ & ≈
B SQL injection		Rule 1Count(s)	Detect 0Count(s)	Block 1Count(s)
EDAP 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)
I Malicinuc file unlead detection	Dula 1Count/c)	Allow 0Count(c)	Detect 1Count(c)	Plack (Count/c)

- 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



• 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 sta	tus log						
C All Delete	C All Delete								
Period : 2023-08-16 12:	Period : 2023-08-16 12:51 ~ 2023-08-16 13:21 ×								
• Period O Today	\bigcirc 1 week	○ 1 month	8-16 🔢 12 🗸 : 51 🗸 ~	2023-08-16 📑 13 🗸 : 21 🗸					
Search Q Down	nload 皆 🛛 Char	rt 诀 🛛 Pivot Chart 诀							
Auto Refresh 5 se	C. 🗸								
Attack domain: 0Coun	nt(s) Attacker(Orig	gin IP): 0Count(s)(0Count(s)) Attack count: 0Case(s)	1					
Time	Client IP	Origin IP Serve	r 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.

APPLICATION INSIGHT WAF

Step 3: Verify Attack Detection:

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

APPLICATION IN	ISIGHT WAF								
Monitoring	Log analysis	Report	Policy settings	Configurations					
Detection log view	Audit log view	View web server sta	tus log						
C ^{AII} Delete									
Period : 2023-08-16 12:	51 ~ 2023-08-16 13:21	×							
• Period O Today	O1week ○	1 month 💿 2023-08	3-16 📑 12 🗸 : 51 🗸 -	2023-08-16 📑 13 🗸 : 21 🗸					
Search Q Dow	nload 皆 🛛 Chart 🕻	Pivot Chart 🔇							
Auto Refresh 5 se	ec. 🗸								
Attack domain: 0Cour	Attack domain: 0Count(s) Attacker(Origin IP): 0Count(s)(0Count(s)) Attack count: 0Case(s)								
Time	Client IP C	Drigin IP Serve	IP Domain	Detection type					
				There is no da					

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

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

Monitoring	Log analysi	s Re	eport i	Policy settings	Configurations						
Detection log vie	w Audit log vi	ew View w	eb server status lo	g							
C ^{AII} Delete											
Period : 2023-08-2	2 10:52 ~ 2023-08-	22 12:06 ×									
• Period O To	oday O1 week	\bigcirc 1 month	0 2023-08-22	10 V : 52 V	~ 2023-08-22	06 🗸 🛛 View only pa	ttern detection mode logs 🗌 🕓 Show	only interest logs			•
Search Q	Download 🖹 🛛 C	ihart 🚯 🛛 Piv	ot Chart 🕓						C Appl	y searc	h filter
_											
Auto Refresh	5 sec. 🗸								Search [15 line(s	s) 🗸
Auto Refresh		Origin IP): 1Cour	nt(s)(0Count(s)) A	Attack count: 10Cas	e(s)				Search [15 line(s	s) 🗸
_		Origin IP): 1Cour Origin IP	nt(s)(0Count(s)) A Server IP	Attack count: 10Cas Domain	e(s) Detection type	Rule name	URL	Risk	Search [;) V
Attack domain: 10	Count(s) Attacker(Rule name SQL Injection	URL http://example.com/				
Attack domain: 10 Time 08-22 10:52:40	Count(s) Attacker(Client IP	Origin IP	Server IP	Domain	Detection type			Risk		Mail	ß
Attack domain: 10 Time 08-22 10:52:40 08-22 10:52:32	Count(s) Attacker(Client IP	Origin IP ? None	Server IP 3.38.96.49	Domain Default	Detection type SQL injection	SQL Injection	http://example.com/	Risk	Action	Mail	ه م
Attack domain: 1C Time 08-22 10:52:40 08-22 10:52:32 08-22 10:52:12	Count(s) Attacker(Client IP [•] 112.216.3.62 [•] 112.216.3.62	Origin IP ? None ? None ? None	Server IP 3.38.96.49 3.38.96.49	Domain Default Default	Detection type SQL injection SQL injection	SQL Injection SQL Injection	http://example.com/ http://example.com/	Risk	Action	Mail	බ ර ර
Attack domain: 10 Time 08-22 10:52:40 08-22 10:52:32 08-22 10:52:12 08-22 10:52:12	Count(s) Attacker(Client IP [•] 112.216.3.62 [•] 112.216.3.62 [•] 112.216.3.62	Origin IP ? None ? None ? None ? None	Server IP 3.38.96.49 3.38.96.49 3.38.96.49 3.38.96.49	Domain Default Default Default	Detection type SQL injection SQL injection Directory access detect	SQL Injection SQL Injection Directory Access	http://example.com/ http://example.com/ http://example.com/	Risk F	Action	Mail	බ ර ර ර

• 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).



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.