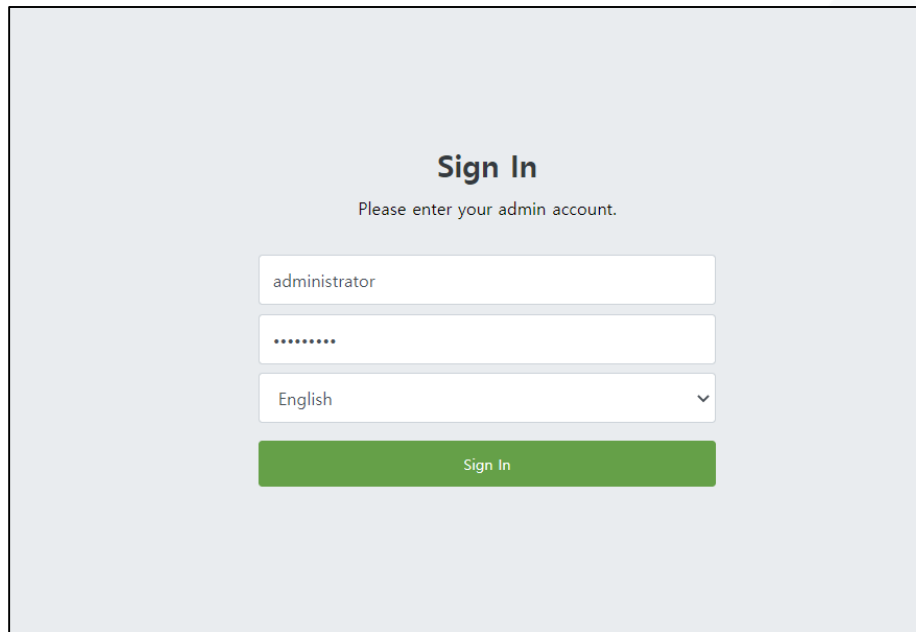


QuickStart Guide

AIWAF V5.0.2



- ❖ Access AIWAF-VE system with HTTPS protocol with port "222" for GUI service.



The screenshot shows a "Sign In" page with the following elements:

- Title: **Sign In**
- Instruction: Please enter your admin account.
- Username field: Contains the text "administrator".
- Password field: Contains seven dots ".....".
- Language dropdown: Shows "English" with a downward arrow.
- Sign In button: A green button with the text "Sign In".

- I. Set security setup as default
 - All types of protocols or ports have to be allowed for the instance.
- II. Access the GUI with web browser.
 - **https://[Public IP address]:222**
- III. Login the page.
 - ID: **administrator**
 - PW: **[instance id]**
- IV. Click "**LOGIN**" button

1

Access AIWAF GUI page

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ
HTTP	TCP	80	0.0.0.0/0
HTTP	TCP	80	:::0
SSH	TCP	22	0.0.0.0/0
Custom TCP Rule	TCP	222	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0
HTTPS	TCP	443	:::0

***** All ports for web services must be allowed in AWS security group *****

- ❖ Change default login account.

The screenshot shows the 'Administrator settings' page in the Application Insight WAF GUI. At the top, there is a navigation bar with tabs for 'Monitoring', 'Log analysis', 'Report', 'Policy settings', and 'Configurations'. Below this is a 'Dashboard' tab. A yellow warning banner at the top of the settings area reads: 'You are using the default ID and the default password. Please change ID and password.' The settings are organized into a table-like structure:

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="🗑️"/>
Recipient E-mail	E-mail <input type="text"/> <input type="button" value="+"/> <input type="button" value="🗑️"/>
Explanation	<input type="text"/>

An 'Apply' button is located at the bottom left of the settings area.

- I. Both ID and PW have to be changed
 - Cannot use the same ID & PW
- II. IP address to allow login also need to be set
 - It can be set as a range
- III. Click "**Apply**" button

- ❖ Configure the time zone.

The screenshot shows the 'APPLICATION INSIGHT WAF' interface. The top navigation bar includes 'Monitoring', 'Log analysis', 'Report', 'Policy settings', and 'Configurations'. Below this, a secondary navigation bar lists 'Administrator settings', 'System settings' (highlighted with a red box), 'NIC settings', 'Product settings', 'Log management', and 'Service control'. On the left, a sidebar menu lists various settings categories, with 'Time zone settings' selected. The main content area is titled 'Time zone settings' and displays the current time as 'Fri Nov 13 14:39:40 KST 2020' and the time zone as 'Asia/Seoul'. Below this, there are sections for 'SNMP GET settings' and 'SNMP TRAP settings', each with an 'Apply' button.

- I. Access "**Configuration > System settings > Time zone settings**"
- II. Configure as a current location
 - If the location is wrong, system & detection logs are not shown.
- III. Click "**Apply**" button
- IV. Click "**Apply**" button in "**Time synchronization settings**"

❖ Download pattern file

The screenshot displays the 'APPLICATION INSIGHT WAF' configuration page. The 'Configurations' tab is active, and the 'Default settings' sub-tab is selected. The left sidebar contains a list of settings, with 'Pattern update settings' highlighted. The main content area shows the 'Pattern update settings' configuration. Under 'Pattern update server', the 'Domain' is set to 'api.monitorapp.com' and 'Port' is '443'. The 'Auto pattern update' option is set to 'Use'. Under 'Online pattern update', the 'Latest pattern version' is set to 'Check version'. Under 'Offline pattern update', the 'Upload pattern file' is set to 'Choose File'. The 'Auto Scaling mode settings' section is also visible, with 'Use/Not use' set to 'Not use'.

- I. Access "**Configuration > System settings > Time zone settings**"
- II. Configure as a current location
 - If the location is wrong, system & detection logs are not shown.
- III. Click "**Apply**" button
- IV. Click "**Apply**" button in "**Time synchronization settings**"

- ❖ Configure the Protected web server (HTTP)

The screenshot displays the 'Admin policy' configuration page for 'Protected web server' in the Application Insight WAF interface. The left sidebar shows a tree view with 'Protected web server' selected. The main content area includes a breadcrumb 'Admin policy > Protected web server', a search bar, and a table of rules. The table is currently empty, displaying 'There is no data.' The 'Add rule' button is highlighted with a red box.

APPLICATION INSIGHT WAF

Monitoring Log analysis Report Policy settings Configurations 2020-11-13 14:43

Default settings Admin policy Domain policy Policy test

Admin policy

Protected web server

Additional settings

IP policy

MAC Whitelist

IP Whitelist

IP Blacklist

DoS policy

Session attack detection

Slow DoS attack detection

Priority policy

URL access rule

National IP detection

User-defined rule

Block page manage

Admin policy > Protected web server Add shortcut menu

Cert. Quick change Add rule

User/Not use All Name HTTP/2 Use/Not use All 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
There is no data.					

- I. Access "Policy settings > Admin policy > Protected web server"
- II. Click "Add rule" button

❖ Configure the Protected web server (HTTP)

The screenshot displays the APPLICATION INSIGHT WAF configuration interface. The top navigation bar includes 'Monitoring', 'Log analysis', 'Report', 'Policy settings', and 'Configurations'. The 'Policy settings' tab is active, and the 'Admin policy' sub-tab is selected. The left sidebar shows a tree view of policy settings, with 'Protected web server' expanded. The main content area shows the configuration for a 'Web server' under 'Admin policy > Protected web server'. The 'Web server' section includes:

- Use/Not use:** Use Not use
- Name:** (empty text field)
- Protocol:** HTTP HTTPS
- RX interface:** eth0: 10.40.2.22 (dropdown menu) Port 80
- TX interface:** eth0: 10.40.2.22 (dropdown menu)
- Receive Allowed IPs other than RX interface IP list:** IP:PORT (text input field with '+' and '-' icons)
- Web server information:** Register new web server button
- Explanation:** (empty text area)

An 'Apply' button is located at the bottom left of the configuration area.

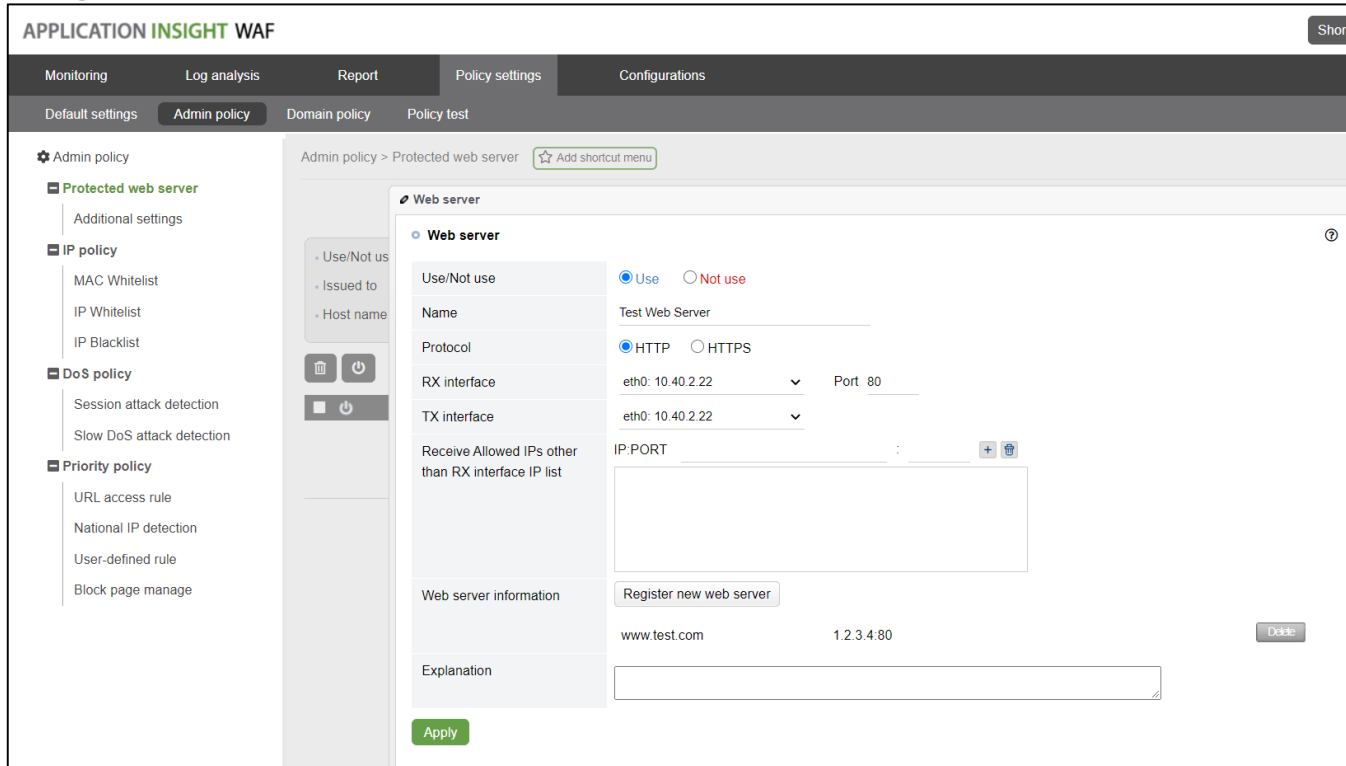
- III. Select protocol with **"HTTP"** and insert port for web server
 - The 3 options should be .matched
- IV. Click **"Register new web server"** button

❖ Configure the Protected web server (HTTP)

The screenshot displays the 'Web server' configuration page. On the left, a sidebar lists various configuration options: 'Use/Not use', 'Name', 'Protocol', 'RX interface', 'TX interface', 'Receive Allowed IPs other than RX interface IP list', 'Web server information', and 'Explanation'. The main area shows the 'Web server' configuration with radio buttons for 'Use' (selected) and 'Not use', and 'Protocol' set to 'HTTP'. An 'Add Web server' dialog box is open, showing the following fields: 'URL' (http:// www.test.com / All(*) with a 'Lookup' checkbox), 'IP' (1.2.3.4) and 'Port' (80) with '+' and '-' icons, 'Server Load Balancing' set to 'Hash', a large empty text box, and 'SSL Termination' (unchecked) with an 'HTTPS Service port' field. 'Add' and 'Close' buttons are at the bottom right of the dialog. An 'Apply' button is at the bottom left of the main configuration area.

- V. Input Domain, server IP and port information and click "+"
 - If one of the options have to be matched
- VI. Click **"Add"** button

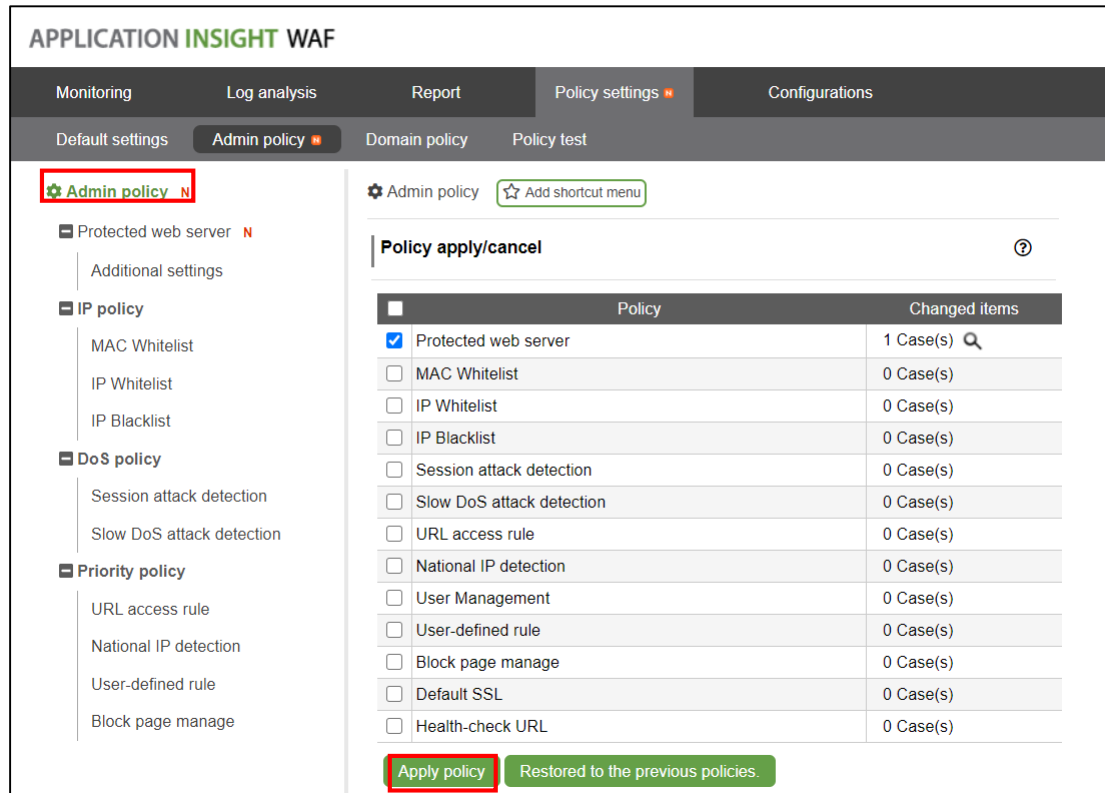
❖ Configure the Protected web server (HTTP)



The screenshot displays the APPLICATION INSIGHT WAF interface. The top navigation bar includes Monitoring, Log analysis, Report, Policy settings, and Configurations. The left sidebar shows the Admin policy menu with options like Protected web server, IP policy, DoS policy, and Priority policy. The main content area is titled "Admin policy > Protected web server" and shows a "Web server" configuration form. The form includes fields for Name (Test Web Server), Protocol (HTTP selected), RX interface (eth0: 10.40.2.22), TX interface (eth0: 10.40.2.22), and a text area for "Receive Allowed IPs other than RX interface IP list". A "Web server information" section shows "www.test.com" and "1.2.3.4:80". An "Explanation" text area is at the bottom. A green "Apply" button is located at the bottom left of the form.

VII. Click **"Apply"** button

- ❖ Configure the Protected web server (HTTP)



APPLICATION INSIGHT WAF

Monitoring Log analysis Report Policy settings **Configurations**

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

Admin policy N

- Protected web server N
 - Additional settings
- IP policy
 - MAC Whitelist
 - IP Whitelist
 - IP Blacklist
- DoS policy
 - Session attack detection
 - Slow DoS attack detection
- Priority policy
 - URL access rule
 - National IP detection
 - User-defined rule
 - Block page manage

Admin policy ☆ Add shortcut menu

Policy apply/cancel ?

<input type="checkbox"/>	Policy	Changed items
<input checked="" type="checkbox"/>	Protected web server	1 Case(s) 🔍
<input type="checkbox"/>	MAC Whitelist	0 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"/>	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)

Apply policy Restored to the previous policies.

- VIII. Access **"Policy settings > Admin policy"**
- IX. Click **"Apply policy"** button

- ❖ Configure the Protected web server (HTTPS)

The screenshot displays the 'Protected web server' configuration page in the Application Insight WAF Admin console. The left sidebar shows a navigation menu with 'Protected web server' highlighted. The main content area includes a breadcrumb trail 'Admin policy > Protected web server' and an 'Add shortcut menu' button. Below this, there are several configuration fields: 'User/Not use' (All), 'Name' (text input), 'HTTP/2 Use/Not use' (All), 'Certificate status' (All), 'Issued to' (text input), 'Protocol' (All), 'IP' (text input), 'Port' (text input), 'Host name' (text input), 'RX interface' (All), 'TX interface' (All), and 'Explanation' (text input). A green 'Add rule' button is visible in the top right corner. Below the configuration fields is a search bar and a table with columns for Name, Protocol, RX/TX, Web server information, Explanation, and Change. The table currently displays 'There is no data.'

- I. Access "Policy settings > Admin policy > Protected web server"
- II. Click "Add rule" button

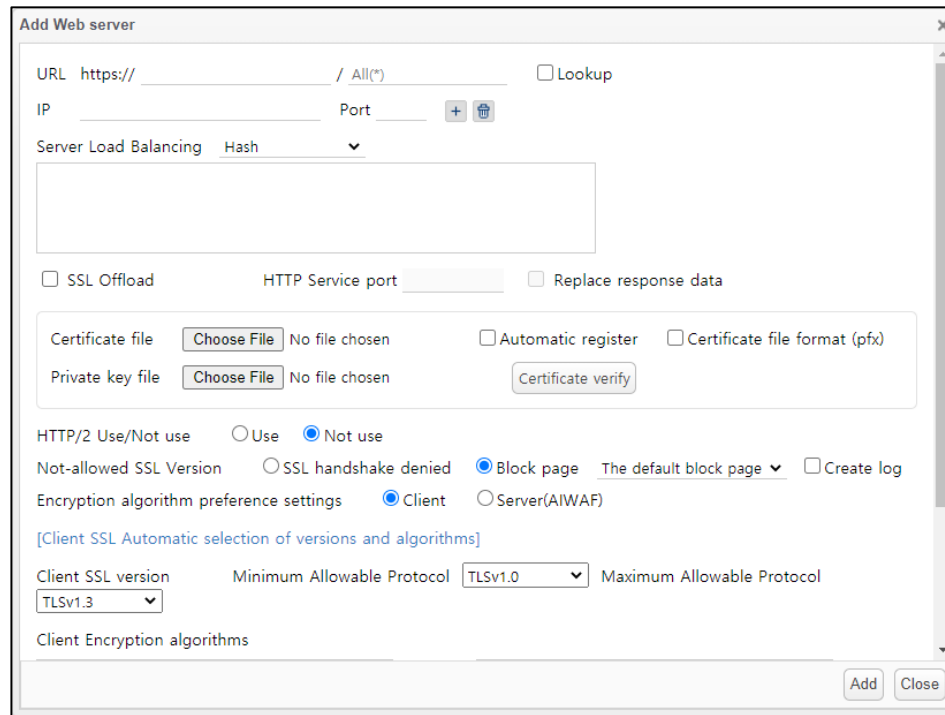
❖ Configure the Protected web server (HTTPS)

The screenshot shows the 'Admin policy' configuration page for 'Protected web server' in the 'APPLICATION INSIGHT WAF' interface. The page is divided into several sections:

- Navigation:** Monitoring, Log analysis, Report, Policy settings, Configurations.
- Sub-navigation:** Default settings, Admin policy (selected), Domain policy, Policy test.
- Left Sidebar (Admin policy):**
 - Protected web server
 - Additional settings
 - IP policy
 - MAC Whitelist
 - IP Whitelist
 - IP Blacklist
 - DoS policy
 - Session attack detection
 - Slow DoS attack detection
 - Priority policy
 - URL access rule
 - National IP detection
 - User-defined rule
 - Block page manage
- Main Content Area (Admin policy > Protected web server):**
 - Web server configuration:**
 - Use/Not use: Use Not use
 - Name:
 - Protocol: HTTP HTTPS
 - RX interface: eth0: 10.40.2.22 (dropdown) Port: 443
 - TX interface: eth0: 10.40.2.22 (dropdown)
 - Receive Allowed IPs other than RX interface IP list: IP:PORT (input field with + and - icons)
 - Web server information: Register new web server button
 - Explanation:
 - Buttons: Apply (green)

- III. Select protocol with **"HTTP"** and insert port for web server
 - The 3 options should be .matched
- IV. Click **"Register new web server"** button

❖ Configure the Protected web server (HTTPS)

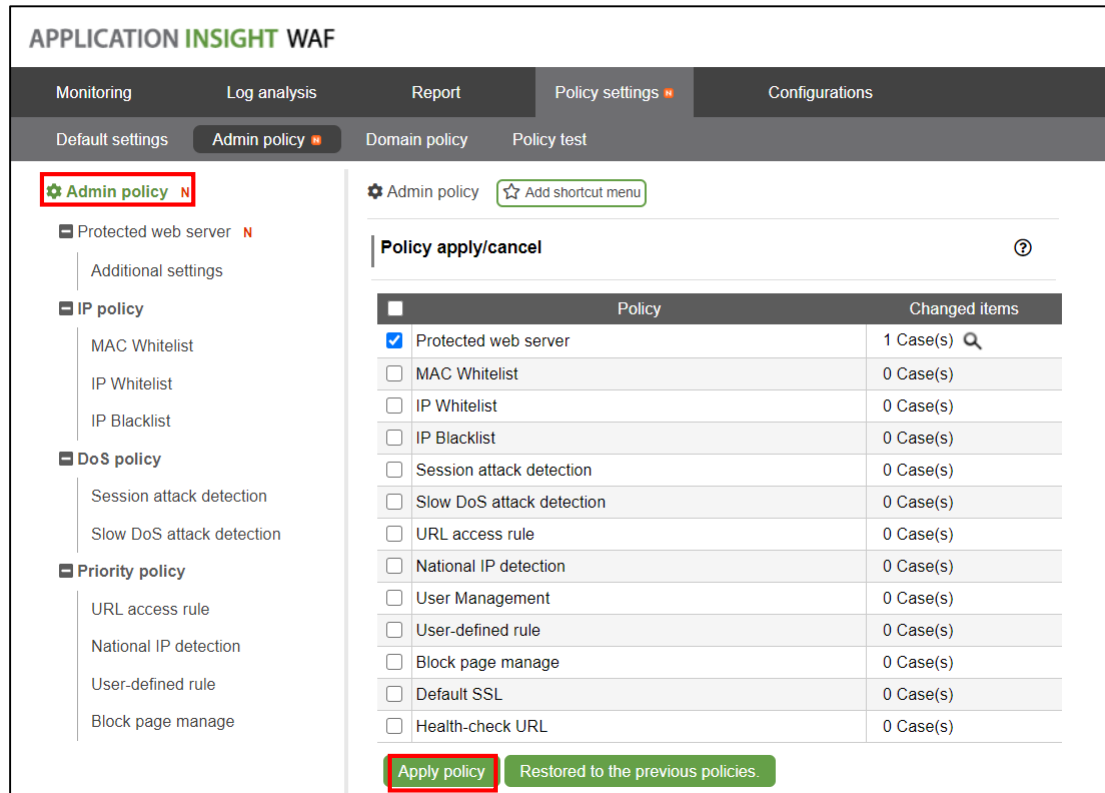


The screenshot shows the 'Add Web server' configuration window. It includes the following elements:

- URL:** https:// / All(*) with a Lookup checkbox.
- IP:** A text field followed by a **Port** field, a **+** button, and a trash icon.
- Server Load Balancing:** A dropdown menu set to 'Hash'.
- SSL Offload:** SSL Offload, **HTTP Service port** field, and Replace response data.
- Certificate file:** No file chosen, Automatic register, Certificate file format (pfx).
- Private key file:** No file chosen, .
- HTTP/2 Use/Not use:** Use, Not use.
- Not-allowed SSL Version:** SSL handshake denied, Block page, **The default block page** dropdown, Create log.
- Encryption algorithm preference settings:** Client, Server(AIWAF).
- [Client SSL Automatic selection of versions and algorithms]**
- Client SSL version:** dropdown.
- Minimum Allowable Protocol:** dropdown.
- Maximum Allowable Protocol:** A text field.
- Client Encryption algorithms:** A text area.
- Buttons:** and .

- V. Input Domain, server IP and port information and click "+"
 - If one of the options have to be matched
- VI. Upload web server's certification & key file.
 - CRT, PEM, PFX, etc. types are supported
 - Certifications file should be decrypted.
 - In case of PEM & CRT type, certification have to be started "Server > Chain > Root"
- VII. Click "**Add**" button
 - SSL versions and encryption algorithms can be selected manually.

- ❖ Configure the Protected web server (HTTPS)



APPLICATION INSIGHT WAF

Monitoring Log analysis Report Policy settings **Configurations**

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

Admin policy N

- Protected web server N
 - Additional settings
- IP policy
 - MAC Whitelist
 - IP Whitelist
 - IP Blacklist
- DoS policy
 - Session attack detection
 - Slow DoS attack detection
- Priority policy
 - URL access rule
 - National IP detection
 - User-defined rule
 - Block page manage

Admin policy ☆ Add shortcut menu

Policy apply/cancel ?

<input type="checkbox"/>	Policy	Changed items
<input checked="" type="checkbox"/>	Protected web server	1 Case(s) 🔍
<input type="checkbox"/>	MAC Whitelist	0 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"/>	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)

Apply policy Restored to the previous policies.

- VIII. Access **"Policy settings > Admin policy"**
- IX. Click **"Apply policy"** button

❖ Configure the Protected web server (HTTPS)

The screenshot displays the 'APPLICATION INSIGHT WAF' configuration page. The top navigation bar includes 'Monitoring', 'Log analysis', 'Report', 'Policy settings', and 'Configurations'. Under 'Policy settings', 'Default settings' is selected. The left sidebar lists various configuration categories, with 'Operation mode' expanded. The main content area shows the 'Operation mode' configuration. Three radio buttons are present: 'Policy bypass', 'Detection mode', and 'Block mode'. The 'Block mode' radio button is selected and highlighted with a red box. Below the radio buttons, there is a 'Bypass target' section with a table of headers and their values. The table has columns for 'Request', 'Header name', and 'Value'. The rows are:

Request	Header name	Value
<input type="checkbox"/>	[Request/Response]	Content-Type:application/vnd.ms.wms-hdr.asfv1
<input type="checkbox"/>	[Request/Response]	Content-Type:application/x-mms-framed
<input type="checkbox"/>	[Request/Response]	Content-Type:application/x-wms-getcontentinfo
<input type="checkbox"/>	[Request/Response]	Content-Type:application/x-wms-LogStats

Below the table, there are fields for 'URL Path' (set to 'HTTP // : 80 / ?') and 'URL extension'. At the bottom, there is a 'Detection mode targets' section with a field for 'URL' (set to 'HTTP // : 80 / ?').

- X. Access "Policy settings > Default settings > Operation mode"
- XI. Change operation mode to "Block mode"
- XII. Click "Apply policy" button

APPLICATION INSIGHT WAF

Monitoring Log analysis Report Policy settings Configurations

Default settings Admin policy Domain policy Policy test

Domain management

Domain policy

Default

Applied URL Rule name Use/Not use All Action All

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

Vulnerability attack detection

- SQL injection
- LDAP injection
- Cross site script
- Cookie forgery
- CSRF detection
- Malicious file upload detection
- Malicious file access detection
- Command injection detection
- Directory access detection
- Vulnerable page access detection

- I. Access "Policy settings > Domain policy > Default"

The screenshot shows the 'APPLICATION INSIGHT WAF' interface. The top navigation bar includes 'Monitoring', 'Log analysis', 'Report', 'Policy settings', and 'Configurations'. Under 'Policy settings', there are sub-tabs for 'Default settings', 'Admin policy', 'Domain policy', and 'Policy test'. The 'Domain policy' sub-tab is selected, showing a left sidebar with 'Domain management', 'Domain policy', and 'Default' (highlighted with a green plus icon). The main content area has a form with 'Applied URL' and 'Rule name' fields. Below this, there are 'Batch change use/not use of policies' (set to 'Use') and 'Batch change action of policies' (partially visible as 'Bl'). A yellow header 'Vulnerability attack detection' is followed by a list of rules: SQL injection, LDAP injection, Cross site script, Cookie forgery, CSRF detection, Malicious file upload detection, Malicious file access detection, Command injection detection, Directory access detection, and Vulnerable page access detection. A modal dialog box titled 'Batch change action of policies' is overlaid on the list, showing a question mark icon, the text 'Action : Block', and the question 'Do you want to change the status?' with 'Ok' and 'Cancel' buttons.

II. Change **“Batch change action of policies”** options to **“Block”**

5

Configure policies

APPLICATION INSIGHT WAF

Monitoring | Log analysis | Report | Policy settings | Configurations

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

- Domain management
- Domain policy
 - Default**

Applied URL: [dropdown] [input] | Rule name: [input]

Batch change use/not use of policies: [Use] [dropdown] [Apply] | Batch change action of policies: [Block]

Vulnerability attack detection

- SQL injection
- LDAP injection
- Cross site script
- Cookie forgery
- CSRF detection
- Malicious file upload detection
- Malicious file access detection
- Command injection detection
- Directory access detection
- Vulnerable page access detection

Batch change action of policies

The policy with the action other than detect/block except from the changed target.
(Page forgery detection, Error page cloaking, Comment cloaking, Web accelerator, POST request approval, Header cloaking)

Ok

III. Click **"Ok"** button

The screenshot shows the 'APPLICATION INSIGHT WAF' interface. The top navigation bar includes 'Monitoring', 'Log analysis', 'Report', 'Policy settings', and 'Configurations'. The 'Policy settings' section is active, with sub-tabs for 'Default settings', 'Admin policy', 'Domain policy', and 'Policy test'. The 'Domain policy' sub-tab is selected, showing a 'Domain management' sidebar with 'Domain policy' and 'Default' options. The main content area displays a confirmation message: 'Successfully applied the policies. Do you want to apply the policies?' with 'Apply policy' and 'Restored to the previous policies.' buttons. Below this are input fields for 'Applied URL', 'Rule name', and 'Use/Not use' (set to 'All'). There are also buttons for 'Batch change use/not use of policies' (set to 'Use') and 'Batch change action of policies' (set to 'Block'). A list of policies is shown under the heading 'Vulnerability attack detection new', including SQL injection, LDAP injection, Cross site script, Cookie forgery, CSRF detection, Malicious file upload detection, Malicious file access detection, Command injection detection, Directory access detection, and Vulnerable page access detection.

IV. Click **“Apply policy”** button to apply all



THANK YOU

MONITORAPP | **APPLICATION INSIGHT**