







eCloudX WAF

Quick Guide

Table of Contents

Table of Contents	2
1. eCloudX WAF main menu overview	3
2. Getting Started	4
2.1. Getting Started with Web Operations System	4
2.2. Getting Started with Web Traffic Analytics.....	5

1. eCloudX WAF main menu overview

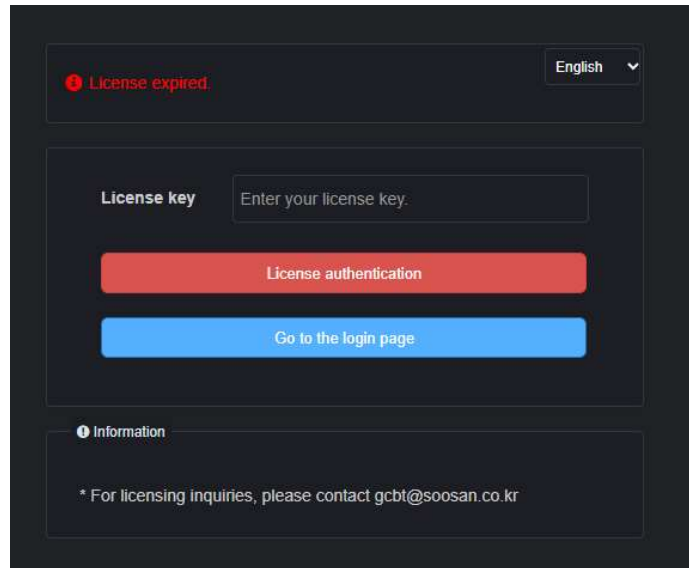
Main Menu	Features
 Dashboard	Monthly attacks on web applications, web traffic security threat index, resource usage. Provide real-time monitoring by day. One can customize the view of the dashboard.
 Log/Statistics	More detailed information is here than dashboard. You can review or search logs such as detection, system resource, traffic, audit logs. And more.
 Policies	Define and generate web application control policies. View patterns, Black list, control bots. And specific policies.
 Webserver	Manage protected web servers and certificates. Register web servers to be protected. Register certificate to decrypt HTTPS traffic.
 System	Provide WAF management features. Information on WAF device, alarms, system backup, and restore. Log collection.
 Administrator	Manage administrator accounts and policy groups.

2. Getting Started

2.1. Getting Started with Web Operations System

Once the installation process is complete, access administer page by entering the following URL in the web browser.

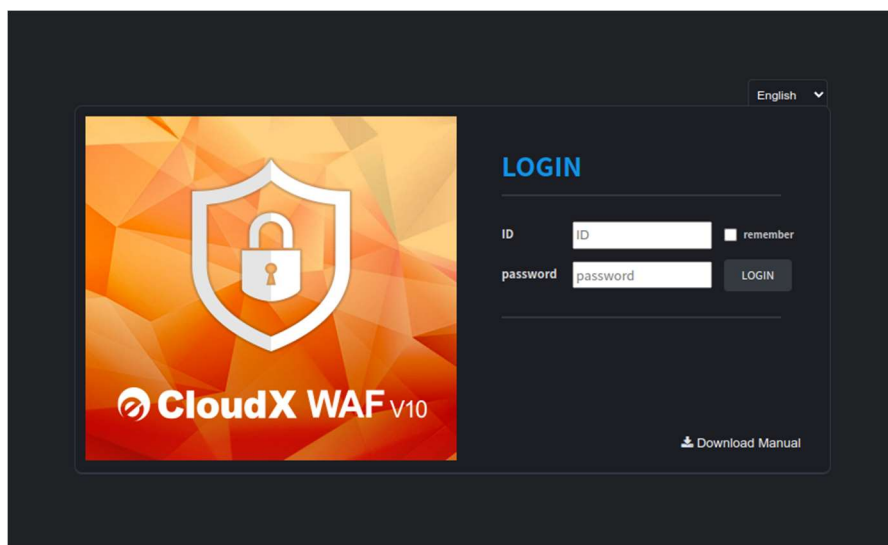
[https://\[eCloudX WAF management IP\]:8443/](https://[eCloudX WAF management IP]:8443/)



The screenshot shows a dark-themed web interface. At the top, there is a red warning banner that says "License expired" with a red exclamation mark icon. To the right of the banner is a language dropdown menu set to "English". Below the banner is a form for entering a license key. It has a label "License key" and a text input field with the placeholder text "Enter your license key.". Below the input field are two buttons: a red button labeled "License authentication" and a blue button labeled "Go to the login page". At the bottom of the form, there is an "Information" section with a small icon and the text "* For licensing inquiries, please contact gcbt@soosan.co.kr".

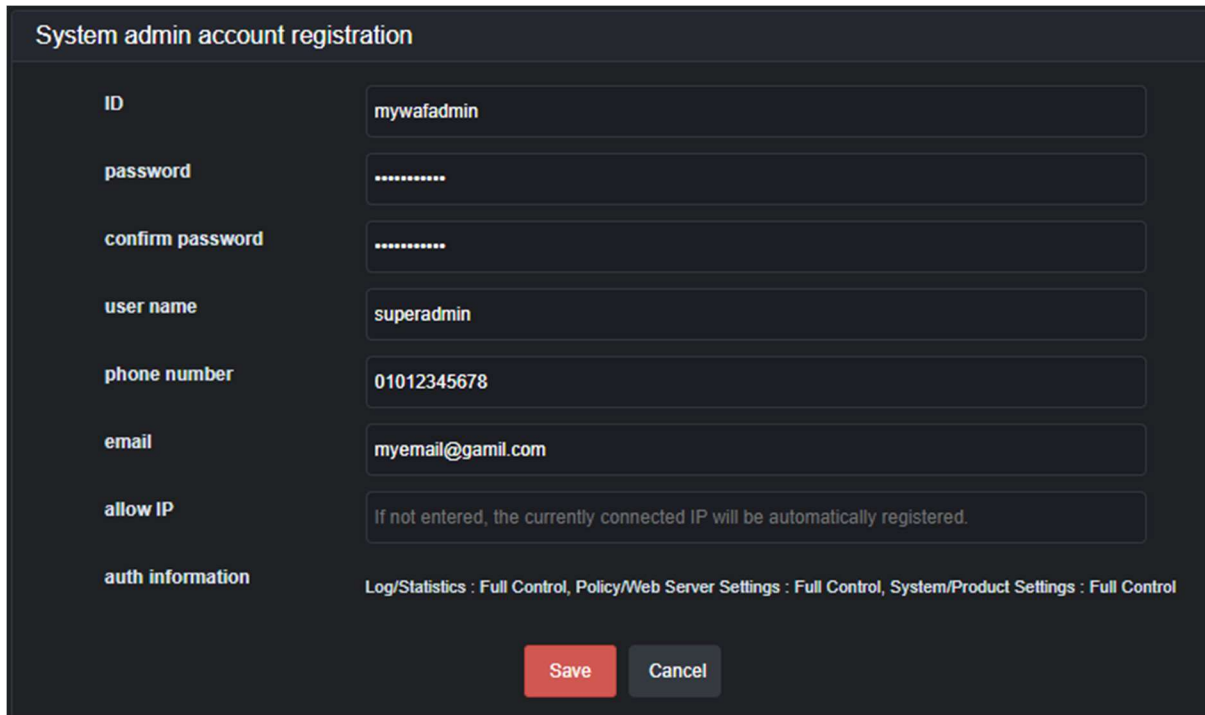
For BYOL, enter the license key.

For licensing inquiries, please contact gcbt@soosan.co.kr.



The screenshot shows the login page of the eCloudX WAF V10. On the left, there is a large orange and red graphic with a white shield icon containing a padlock. Below the graphic, it says "CloudX WAF V10". On the right, there is a "LOGIN" section with two input fields: "ID" and "password". The "ID" field has a "remember" checkbox next to it. Below the input fields is a "LOGIN" button. At the bottom right of the login section, there is a link that says "Download Manual" with a download icon.

Enter your ID and password, which are initially set to **admin** and **[Instance ID]** during installation.



The image shows a 'System admin account registration' form. It contains the following fields and values:

Field	Value
ID	mywafadmin
password	*****
confirm password	*****
user name	superadmin
phone number	01012345678
email	myemail@gamil.com
allow IP	If not entered, the currently connected IP will be automatically registered.
auth information	Log/Statistics : Full Control, Policy/Web Server Settings : Full Control, System/Product Settings : Full Control

At the bottom of the form are two buttons: 'Save' (red) and 'Cancel' (grey).

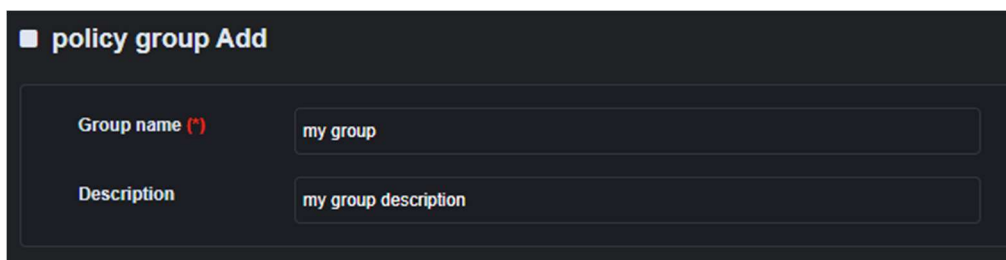
Register system admin account. After you register for a new system admin account, you need to log in again.

2.2. Getting Started with Web Traffic Analytics

Now we need a policy that defines how to protect the webserver to WAF to analyze and control web traffic.

Before you add a policy, add a policy group.

Administrator -> Policy Group -> policy group add



The image shows a 'policy group Add' form. It contains the following fields and values:

Field	Value
Group name (*)	my group
Description	my group description

Register policy group.

Please note that the following description assumes the webserver uses HTTPS.

Register certificate.

Webserver -> Certificate -> Certificate -> Certificate Addition

The screenshot shows a web form titled "Certificate Addition". It contains several input fields and radio button options. The "Name" field is filled with "soosan". The "Description" field is filled with "certificate for soosan". Under "Authentication type", the "Server (Default)" radio button is selected. Under "Certificate type", the "CRT" radio button is selected. There are five "Upload" buttons for "CRT file", "Key file", "Broker file1", "Broker file2", and "Root file". The "CRT file" and "Key file" buttons show file names "soosan.co.kr.crt" and "soosan.co.kr.key" respectively, each with a delete icon. The other three buttons show the text "Please upload your file" with a delete icon. A "Password" field at the bottom has the placeholder text "Please enter certificate password".

Name (*)	soosan
Description (*)	certificate for soosan
Authentication type	<input checked="" type="radio"/> Server (Default) <input type="radio"/> Client (mTLS) <input type="radio"/> CA (mTLS)
Certificate type	<input checked="" type="radio"/> CRT <input type="radio"/> DER <input type="radio"/> PKCS#7 <input type="radio"/> PKCS#12 <input type="radio"/> PEM <input type="radio"/> JKS
CRT file (*)	<input type="button" value="Upload"/> soosan.co.kr.crt ✕
Key file (*)	<input type="button" value="Upload"/> soosan.co.kr.key ✕
Broker file1	<input type="button" value="Upload"/> Please upload your file ✕
Broker file2	<input type="button" value="Upload"/> Please upload your file ✕
Root file	<input type="button" value="Upload"/> Please upload your file ✕
Password	<input type="text" value="Please enter certificate password"/>

Register the certificate by type accordingly.

Register web server to protect.

Webserver -> Target Server -> Target Server -> Add

Toggle the button in line with "IP" label to change "HTTP" to "HTTPS".

■ Target Server Modification

Domain	<input type="text" value="gw.soosan.co.kr"/>	Policy <input checked="" type="checkbox"/>	Bypass <input type="checkbox"/>
IP	<input type="text" value="10.200.137.42"/>	<input type="text" value="443"/>	HTTPS <input type="button" value="v"/> IPv6 <input type="checkbox"/>
Name	<input type="text" value="gw_soosan_443"/>		
Comment	<input type="text" value="my server comment"/>		
ACL	<input type="text" value="Basic Security Policy"/> <input type="button" value="v"/>		
File / Script	<input type="text" value="Basic Security Policy"/> <input type="button" value="v"/>		
Policy group	<input type="text" value="my group"/> <input type="button" value="v"/>		
Block page	<input type="text" value="Block page select"/> <input type="button" value="v"/>		
SNI	<input type="text" value="Please enter SNI"/> <input type="button" value="Add"/> <input type="text" value="gw.soosan.co.kr"/> <input type="button" value="x"/>		
Server certificates	<input type="text" value="soosan"/> <input type="button" value="v"/>		
TLS version	<input type="text" value="TLSv1.0"/> <input type="button" value="v"/>		
Cipher Suite Level	<input type="text" value="Enable All"/> <input type="button" value="v"/>		
Client certificates	<input type="text" value="Client certificates select"/> <input type="button" value="v"/>		
CA certificates	<input type="text" value="CA certificates select"/> <input type="button" value="v"/>		
SSL off loading	<input type="checkbox"/>	SSL off loading port	<input type="text" value="0"/> <input type="button" value="v"/> HTTP 1.1

Fill in the form according to the server settings and certificate type.

- Domain : target server domain
- IP : target server IP
- Name : target server name
- Comment : target server comment
- ACL : set to "Basic Policy"
- File / Script : set to "Basic Policy"
- Policy group : set to policy group you generated
- SNI : enter you SNI and click "Add"
- Server certificates : set to certificate you registered
- TLS version : TLS version. If you select a lower TLS version, it also supports the upper TLS version.
- Cipher suite level : set cipher suite level of certificate

Toggle on "Policy" and set your HTTPS port on left of that button.

Save it. And click "Apply Policies"