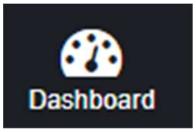
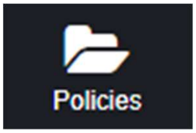
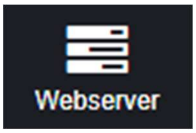
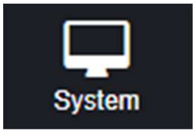
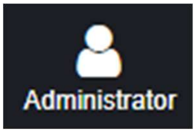
eCloudX WAF

Quick Guide

Table of Contents

1. eCloudX WAF main menu overview

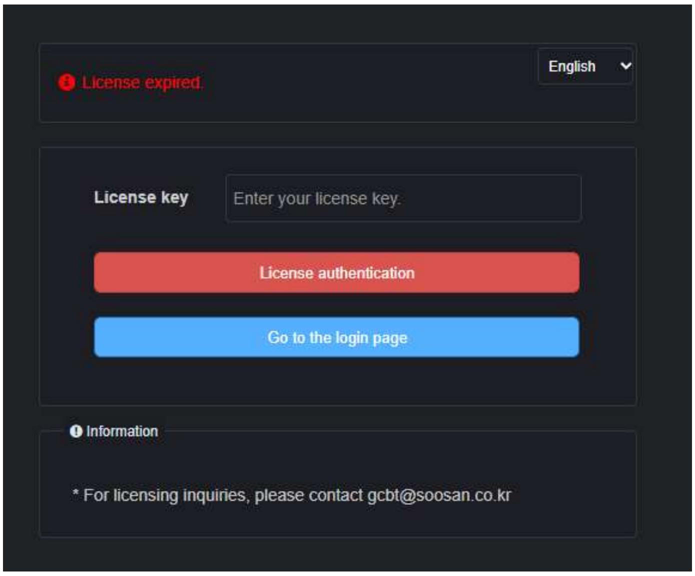
Main Menu	Features
 Dashboard	Monthly attacks on web applications, web traffic security threat index, resource usage. Provide real-time monitoring by day. One can customize the view of the dashboard.
Log/Statistics	More detailed information is here than dashboard. You can review or search logs such as 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/



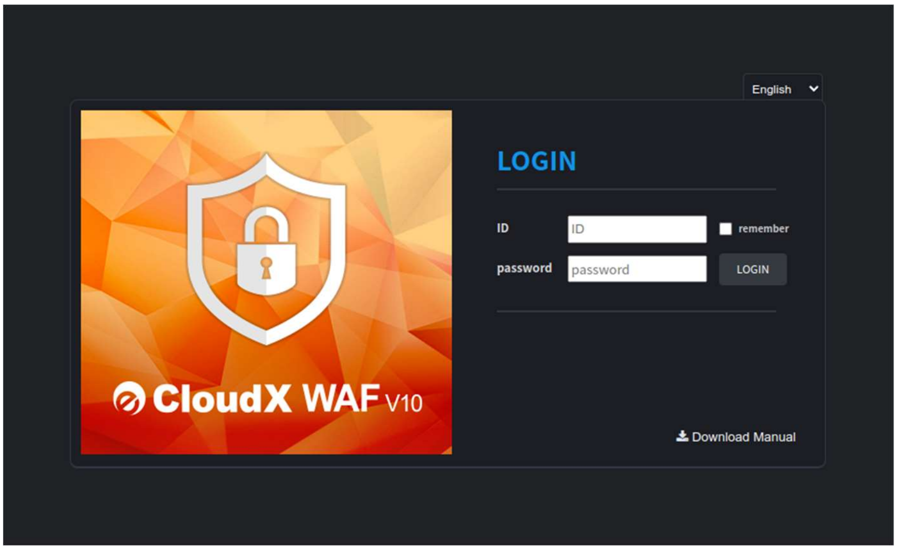
License expired.

License key: Enter your license key.

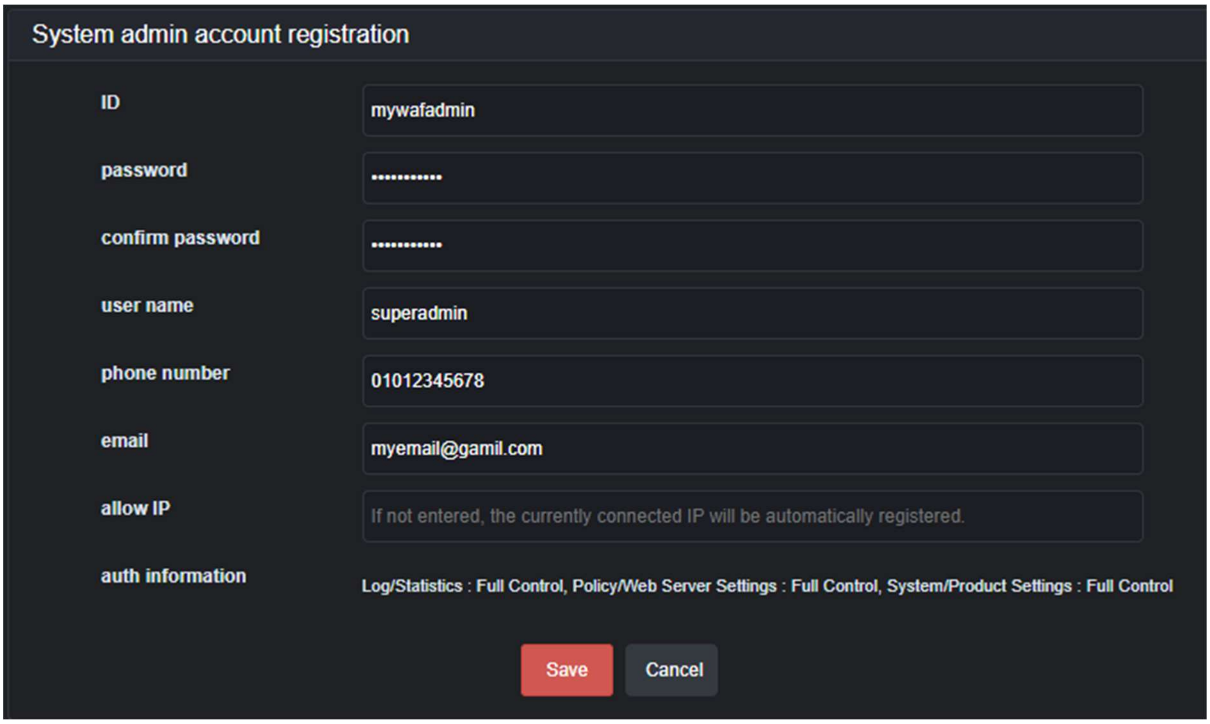
Information

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

For BYOL, enter the license key.
For licensing inquiries, please contact gcbt@soosan.co.kr.



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



System admin account registration

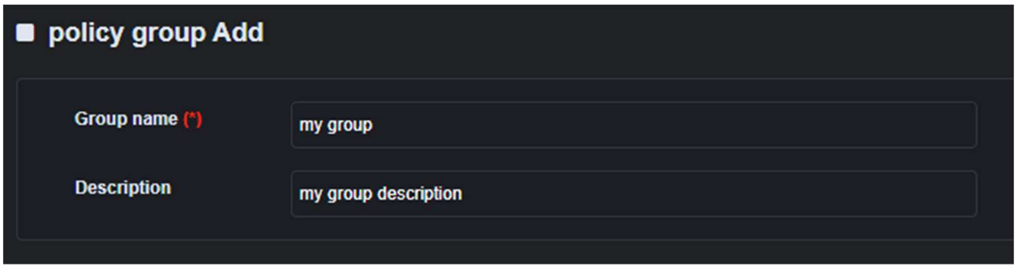
ID	mywafadmin
password	•••••••••••
confirm password	•••••••••••
user name	superadmin
phone number	01012345678
email	myemail@gamil.com
allow IP	If not entered, the currently connected IP will be automatically registered.
auth information	Log/Statistics : Full Control, Policy/Web Server Settings : Full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

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



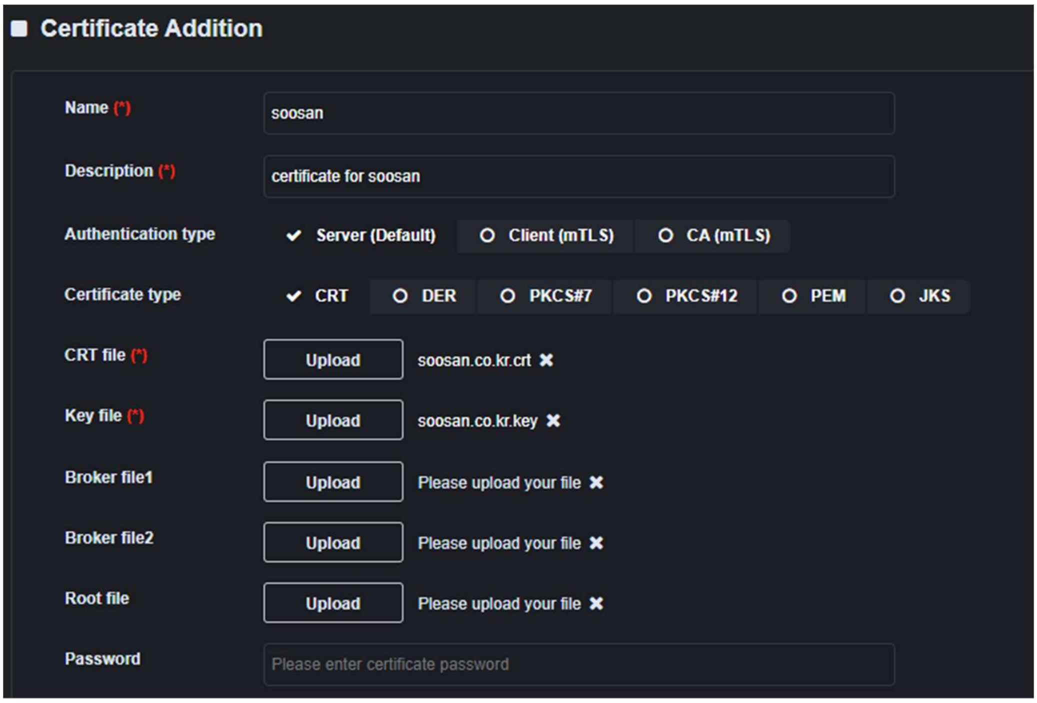
policy group Add

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



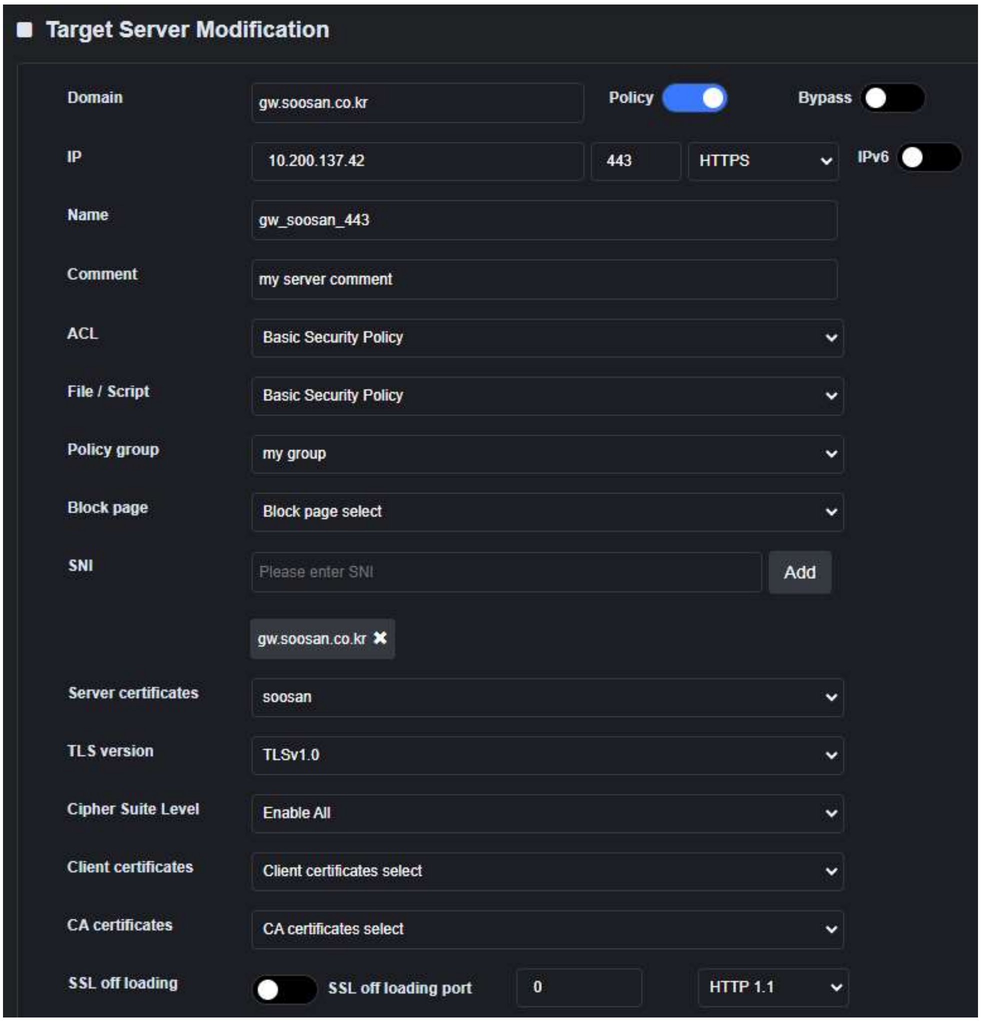
Certificate Addition

Name (*)	soosan
Description (*)	certificate for soosan
Authentication type	✓ Server (Default) ○ Client (mTLS) ○ CA (mTLS)
Certificate type	✓ CRT ○ DER ○ PKCS#7 ○ PKCS#12 ○ PEM ○ JKS
CRT file (*)	Upload soosan.co.kr.crt ✖
Key file (*)	Upload soosan.co.kr.key ✖
Broker file1	Upload Please upload your file ✖
Broker file2	Upload Please upload your file ✖
Root file	Upload Please upload your file ✖
Password	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	gw.soosan.co.kr	Policy ●	Bypass ○
IP	10.200.137.42	443 HTTPS	IPv6 ○
Name	gw_soosan_443		
Comment	my server comment		
ACL	Basic Security Policy		
File / Script	Basic Security Policy		
Policy group	my group		
Block page	Block page select		
SNI	Please enter SNI	Add	
	gw.soosan.co.kr ✖		
Server certificates	soosan		
TLS version	TLSv1.0		
Cipher Suite Level	Enable All		
Client certificates	Client certificates select		
CA certificates	CA certificates select		
SSL off loading	○ SSL off loading port 0	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.
- Ciper suite level : set ciper suite level of certificate

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

Save it. And click “Apply Policies”