



DragonWAFTM

Ver. IIS 6

**INSTALLATION
GUIDE**

DragonWAFTM is a trademark of DragonSoft Security Associates
Copyright ©2010 DragonSoft Security Associates, All rights Reserved.

- I N D E X -

DragonWAF Web Server Application Firewall
.....03

System Requirements
.....05

DragonWAF Pre-install Check
To ensure optimal DragonWAF performance, the suggested security settings are crucial.
(Please make sure you remove other earlier DragonWAF versions before install a new one.)
.....06

Installation and Registration
.....11

Appendice

IIS Advance Configuration
.....15

DragonWAF Customer Support
.....18



DragonWAF Web Server Application Firewall

DragonWAF adopts a filtration technique to analyze hidden threats inside application layer of the web server, protect loss of important data. The malicious attacks against IIS Web Server are detected, recorded and filtered by DragonWAF from the source, DragonWAF records dates, attacker IP, attack patterns into a “diversified graph” analysis, facilitate better control on IIS Web Server security management.

DragonWAF Web Application Firewall fulfills

“Strengthened Security, Intrusion Prevention, Penetration Protection, Anti-Tampering”, shape new value on web security.

Intrusion Identification Technology including:

- SQL Injection
- Buffer Overflow
- HTTP Response Splitting
- Encoding Attack Prevention
- Keyword Strings Filtering
- Directory Traversal Prevention
- Directory Indexing Protection
- Customizable Warning Message
- More....coming soon

DragonWAF – Best Entrepreneurial Web Server Protection Solution

Over the years, frequent use of websites to spread information symbolize enterprise image significantly. The use of firewalls to combat against malicious intrusion and digging web vulnerability that cause website malfunction, loss of transaction records, customer information, bank records, web defacement, denial of service, phishing, botnet...is basic and common in web security.

In order to remedy what ordinary firewalls signature-based task on non-application layers, a specialized firewall for web site protection is formulated – WAF (Web Application Firewall).

DragonWAF strengthens overall website security in terms of “Website Protection” and “Filter Malicious Signature Patterns”, blocks known and unknown vulnerability attacks taking place on Web Servers, records malicious requests. It is your most powerful website protector.

System Requirements :

Processor : Intel Pentium 4 Celeron and above (No support 64 bit)

Memory : 1 GB and above

Hard Disc : 40 GB and above

Installation Device : CD / DVD ROM

Network : High-speed Ethernet Network Card / Wi-Fi Network Card

Firewall settings : Opening port 80 to 2-way traffic

Software Requirements :

Operating Systems : Windows 2003

IIS Versions : IIS 6

Web Browsers : IE 6.0 and above, FireFox 3.0 and above.

Correspondence Table of MS O.S. and IIS Versions

Operating Systems	MS-IIS Versions
Windows 2003 / 2003 R2	IIS 6
Windows Vista / 2008	IIS 7
Windows 2008	IIS 7.5

DragonWAF Pre-install Check

Just before DragonWAF installation, please check following IIS configuration for optimal state of web site security.

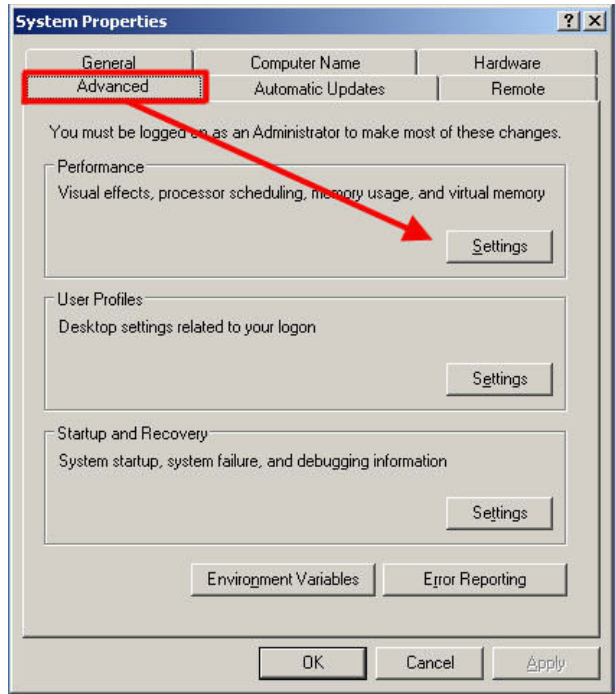
(Please make sure you remove other earlier DragonWAF versions before install a new one.)

- 1. DEP (Data Execution Prevention) check in operating system.**
- 2. Web Service Extensions (All Unknown ISAPI)**
- 3. IIS Domains Check**
- 4. IIS 5.0 Isolation Mode Check**

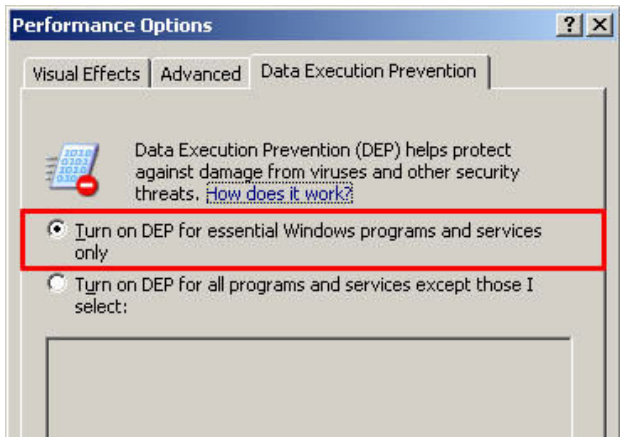
1. DEP (Data Execution Prevention) Setting in Operating System

Right click “My Computer”, choose “Properties”.

Find “Settings” in “Advanced” under “System Properties”

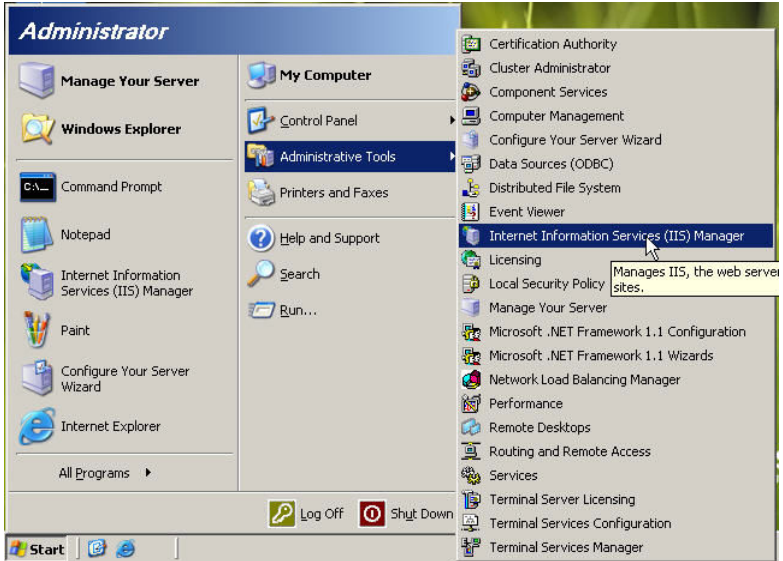


Go to “Data Execution Prevention”, choose “Turn on DEP for essential programs and services only”.

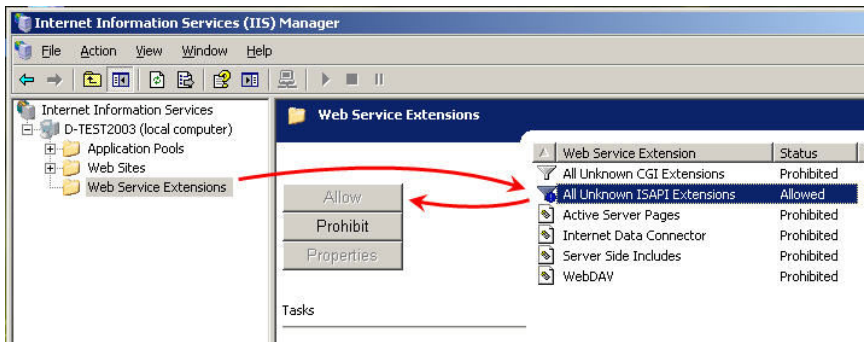


2. Web Service Extensions Check

Find “Web Service Extensions” in “Internet Information Services (IIS) Manager” as following:



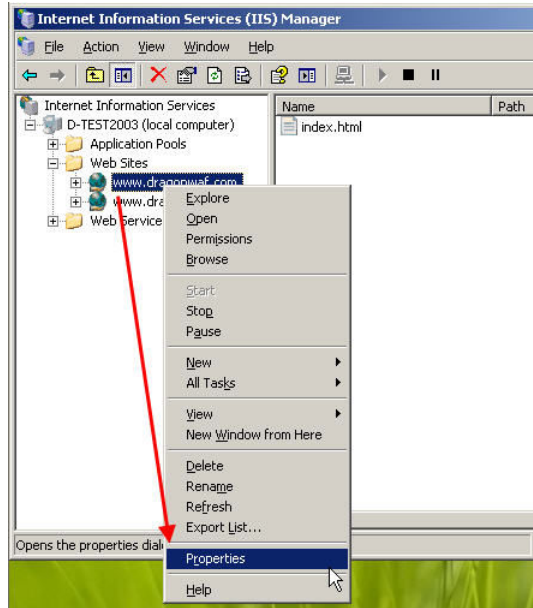
Locate “All Unknown ISAPI Extensions” under “Web Service Extensions”, Allow the service by clicking “Allow” button in the middle of the screen.



3. IIS Domains Check

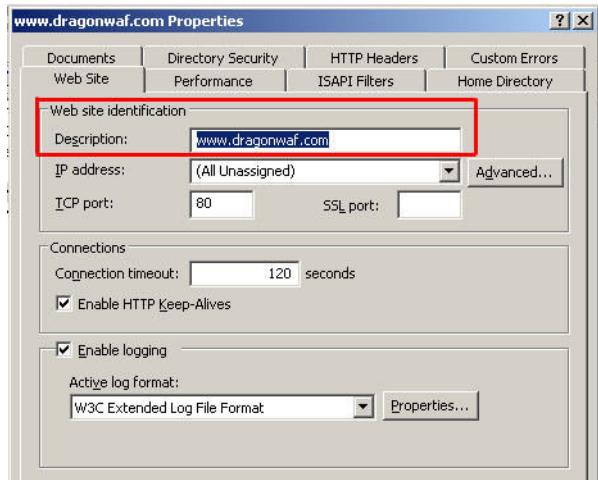
This is to ensure all domains are listed on IIS for DragonWAF to extract for activated protection.

Find “Web Sites” in “Internet Information Services (IIS) Manager”, right click on “Properties”.



Under “Web Site” tab, make sure domain name is given to “Description”. This will appear in DragonWAF website protection windows.

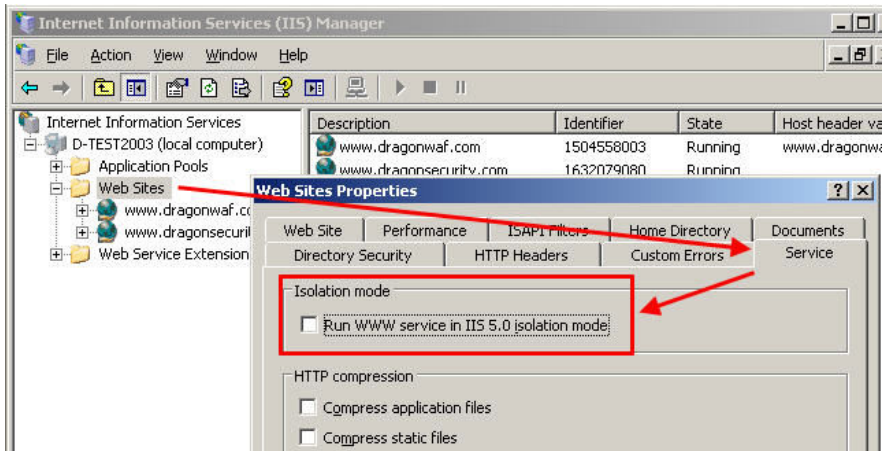
You may add more domains here before DragonWAF could offer protection.



4. IIS 5.0 Isolation Mode Check

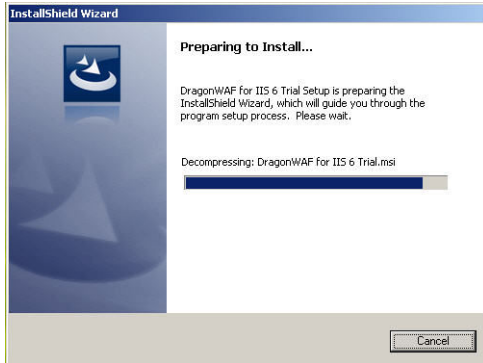
This is to ensure DragonWAF does not run under IIS 5.0 mode at all instead of IIS 6 that could affect certain IIS performance.

Find “Web Sites” in “Internet Information Services (IIS) Manager”, right click on “Properties”. Under “Service” tab, make sure “Isolation Mode” is unticked, as shown in below:



Installation and Registration

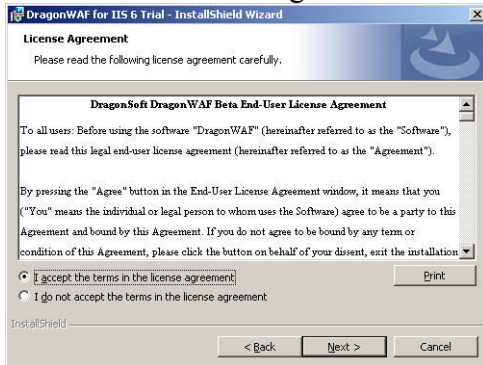
1. Run InstallShield Wizard



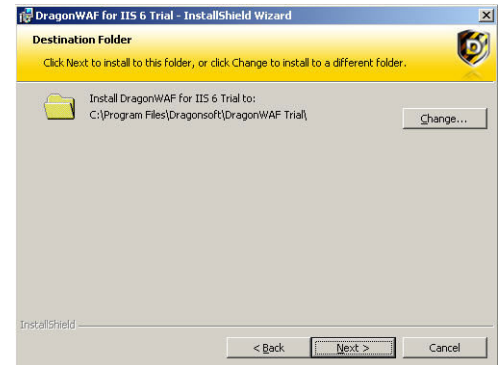
2. Welcome



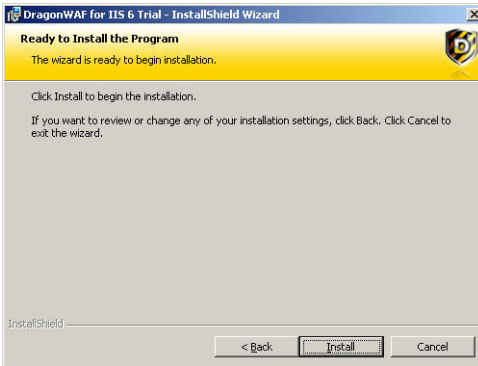
3. End-user License Agreement



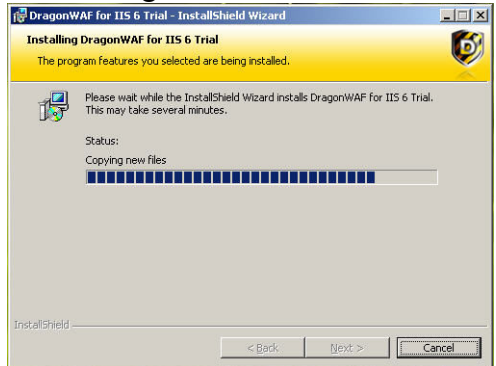
4. Select destination folder



5. Confirm to start installation



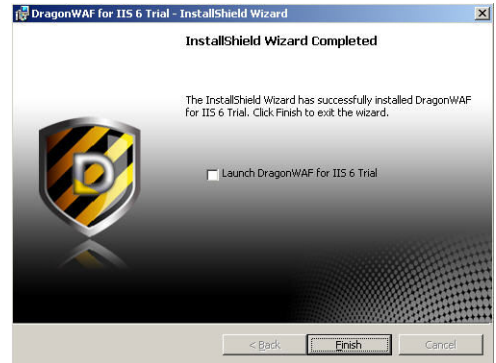
6. Installing



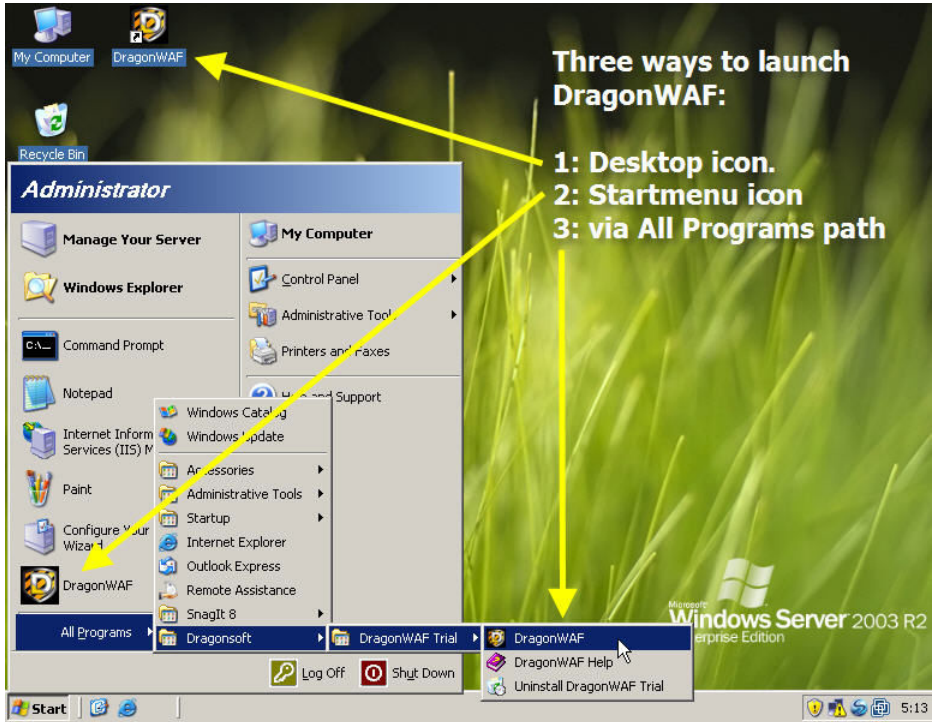
7. Service installed successfully



8. Finished installation



Run DragonWAF program:



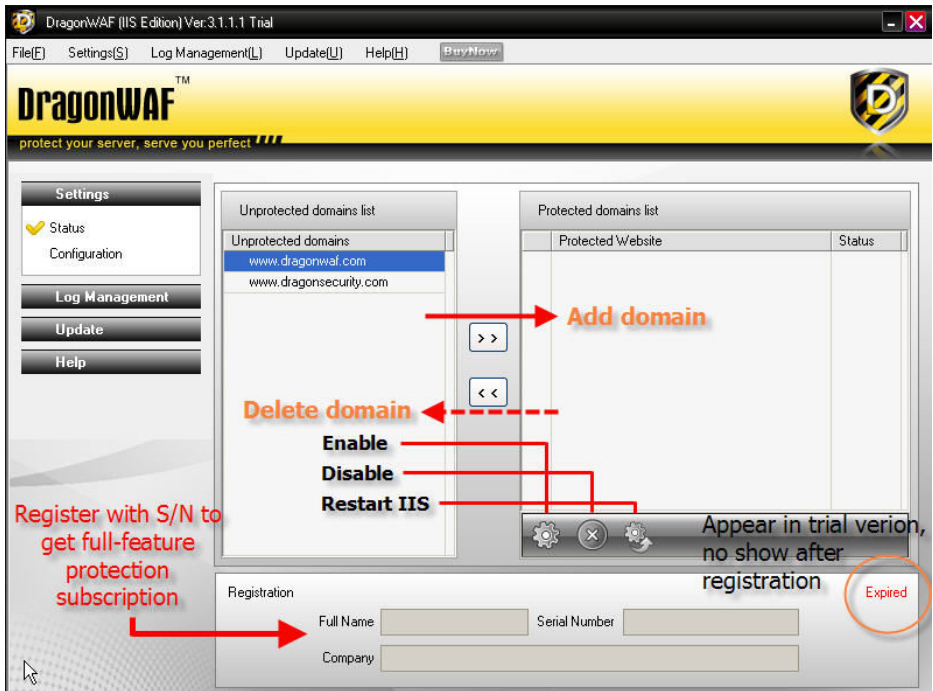
A window will pop up, asking for a domain to be protected.



Select one to activate as default, add more in program UI.



A list of domains appears on starting page, you may add list up to the limit of authorized domain counts.



Note: You must register with given S/N license key(s) to get full-feature protection subscription from DragonSoft.

Appendice

IIS Advance Configuration

IP Input Prevention

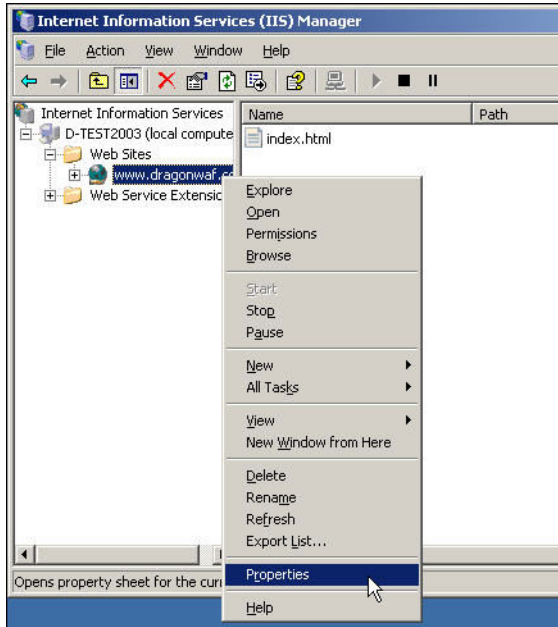
Most webmasters do not notice the IP input attack method, DragonWAF provides higher web security by means of IP input prevent setting. (Note: Except for websites that authenticate financial transactions with other parties using IP addresses)

Go to “Internet Information Services (IIS) Manager” option as shown in following :

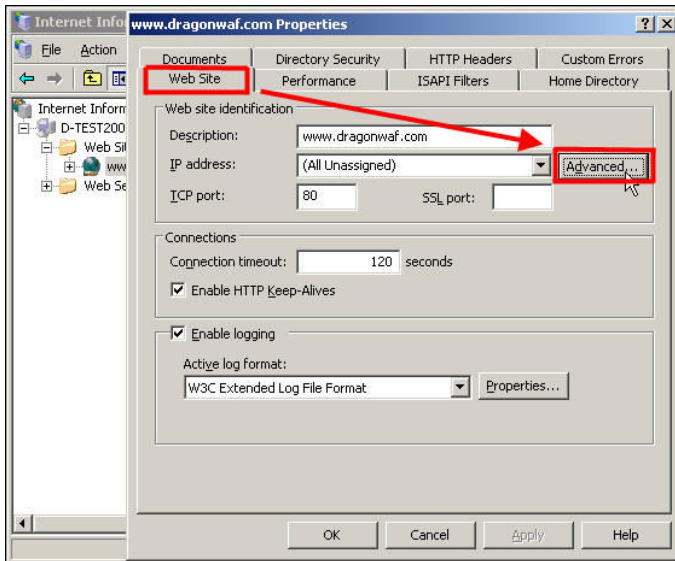


Go to “Properties” under IIS websites as shown below.

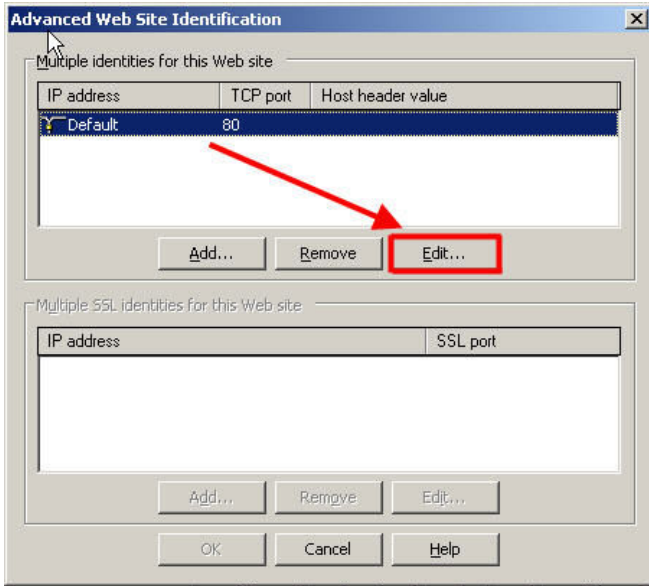
DragonWAF INSTALLATION GUIDE



Go to “Web Site” tab, click on “Advanced” next to IP address.



Select “Default” identity, click on “Edit”.



Type in website domain on your IIS server to complete.



DragonWAF Customer Support

The purchase of DragonWAF series products include one year full license use and customer support by means of :

1. Telephone, facsimines and email consulting
2. Module update service

Please contact us for product support when you encounter any questions during the use of DragonWAF. DragonSoft Service department is standing by to handle your questions :

Customer Service Line : +886-(2)-25077677

Facsimiles : +886-(2)-25010035

Customer Service email : dragonwaf_en@dragonsoft.com



DragonWAF™ is a registered trade mark of DragonSoft Security Associates. Other products and names are DragonSoft's trade marks and properties. This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.