



# DragonWAF (IIS6) Install Guide

網站應用程式防火牆 安裝手冊

## 目錄

DragonWAF 網站應用程式防火牆	2
軟硬體規格需求	4
DragonWAF (IIS6)安裝檢查項目	5
為確保網站安全設定一致性，強烈建議您於安裝前，確認本章節所有設定 ( 安裝 DragonWAF 所有版本前，請先確定您已移除其他版本 DragonWAF )	
安裝與註冊說明	11
( 附錄 )	
1. IIS 進階設定 適用設定規範	21
2. 多語系檔案/網頁名稱安全性建議	23



中 | 華 | 龍 | 網

台灣資安軟體之先驅與領導廠商

Copyright© DragonSoft Security Associates, Inc. All rights reserved



# DragonWAF (IIS6) Install Guide

## 網站應用程式防火牆 安裝手冊

### DragonWAF 網站應用程式防火牆

DragonWAF 採取過濾保護技術，分析 Web Server 網站應用層中潛藏的不安因素，保護重要資料避免外洩，當 DragonWAF 偵測到對 IIS Web Server 具有攻擊行為時進行，將過濾並偵測惡意行為的來源並將惡意行為資訊紀錄於系統，DragonWAF 防禦記錄採取了日期、對方 IP、類型匯入方式整合多種圖形的一種【多元圖形化】方式呈現分析，協助 IIS Web Server 安全狀況的控制與管理。

### DragonWAF 網站應用程式防火牆實現

「安全強化、阻擋入侵、防護滲透、阻絕竄改」讓您發現網站防禦新價值

提供以下入侵行為辨識技術

- ◆ SQL Injection -
- ◆ Buffer Overflow 過濾防護 -
- ◆ HTTP 指令過濾防護 -
- ◆ ShellCode 過濾防護 -
- ◆ Encoding Attack 過濾防護 -
- ◆ 關鍵字串過濾防護 -
- ◆ Directory Traversal 過濾防護 -
- ◆ 目錄保護功能 -
- ◆ 自訂警告訊息 -
- ◆ 更多.....新功能陸續追加中





# DragonWAF (IIS6) Install Guide

## 網站應用程式防火牆 安裝手冊

### DragonWAF 為企業最佳 Web Server 防護方案

近年資訊運用得頻繁，網站已是企業的一大象徵，面對運行惡意挖掘與弱點入侵，導致網站不正常的運作，藉由網站入侵取得企業網站文件包括、商品交易資料、客戶資料、銀行交易紀錄、惡意竄改網頁內容、阻斷網站服務、更可能將網站作為跳板，對外破壞竊取攻擊成為惡意人士幫凶，採用防火牆保護對外服務是基本也是常識。

但是一般防火牆僅能防護的大多是非應用層上的特徵行為，為了因應傳統防火牆的不足與問題，專屬保護網站的防火牆開始因應而生，也就是網站應用程式防火牆 WAF ( web Application Firewall ) 。

DragonWAF 能協助強化整體網站安全，「保護網站」與「過濾惡意特徵」阻擋已知的弱點攻擊與未知的弱點攻擊，於層出不窮的攻擊中保護 Web Server，並把惡意網站要求阻絕記錄，成為您網站安全、防禦縱深最強大的保護者。





# DragonWAF (IIS6) Install Guide

## 網站應用程式防火牆 安裝手冊

### 硬體規格需求：

處理器建議：Pentium 4 Celeron 以上 ( 不支援 64 位元處理器 )

記憶體建議：1 GB 以上記憶體

硬碟空間：40 GB 以上硬碟空間

安裝介面：CD / DVD ROM

網路介面：高速乙太網路卡 / 無線網卡

防火牆需求：安裝註冊時，請開放雙向 port 80 對外

### 軟體安裝需求：

作業系統：Windows Vista/ 7 / 2003/2008

IIS 版本支援：IIS 6/ IIS 7/ IIS 7.5

瀏覽器採用：IE 6.0 以上、FireFox 3.0 以上

若對本身 IIS 版本不確定，可參考微軟作業系統與 IIS 參照對應表如下

作業系統	IIS 版本對應
Windows 2003	IIS 6
Windows Vista/2008	IIS 7
Windows 7 / 2008 R2	IIS 7.5





# DragonWAF (IIS6) Install Guide

網站應用程式防火牆 安裝手冊

## DragonWAF 安裝檢查項目

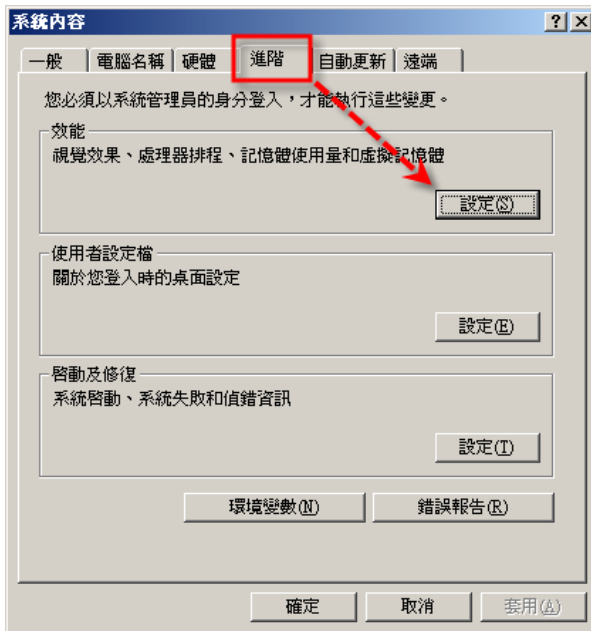
DragonWAF 在實施安裝前，請您先行檢查以下 IIS 設定選項，  
以為您網站設定更佳資安防護品質：

( 安裝 DragonWAF 所有版本前，請先確定您已移除 DragonWAF 其他版本 )

1. 作業系統 DEP 檢查 ( Date Execution Prevention 資料執行保護 )
2. 網頁服務延伸檢查 ( 所有未知的 ISAPI 擴充程式 )
3. IIS 防護網域設定檢查
4. IIS 5.0 隔離模式確認

### 1. 作業系統 DEP 檢查

請點選，我的電腦點選「右鍵」→「系統內容」→「進階」( 設定 )





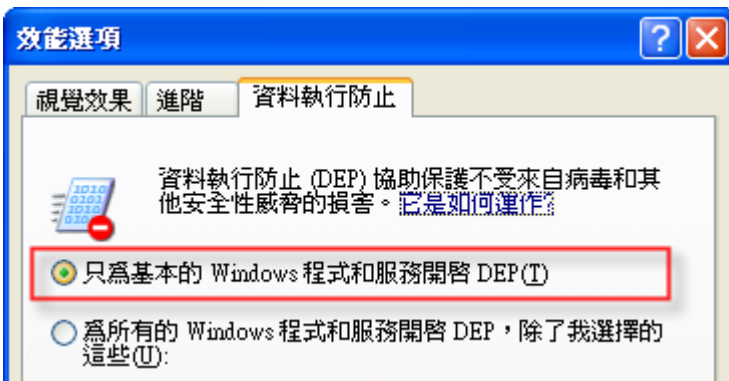
## DragonWAF (IIS6) Install Guide

### 網站應用程式防火牆 安裝手冊

作業系統 DEP 檢查 ( Date Execution Prevention 資料執行保護 ) ，主要為微軟作業系統提供於記憶體位置保護之功能，防範具惡意程式挾持與利用系統記憶體位置進行破壞，入侵等行為。

資料執行防止設定項目	
A	「只為基本的 Windows 程式和服務開啟 DEP(T)」
B	「為所有的 Windows 程式和服務開啟 DEP，除了我選擇的這些(U)」

為因應安裝需要，請檢查此處設定為「A」項目（如下圖）。  
之後 DragonWAF 將於安裝時引導您回復本項設定。





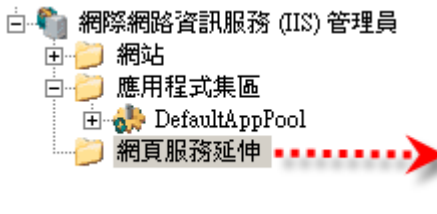
# DragonWAF (IIS6) Install Guide

## 網站應用程式防火牆 安裝手冊

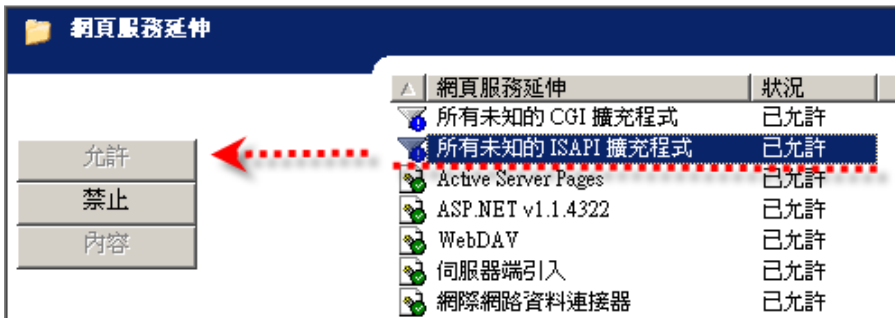
### 2. 網頁服務延伸檢查

請開啟您 IIS 主機中「網際網路資訊服務 (IIS) 管理員」  
您可以在「開始」→「程式集」→「系統管理工具」  
→「網際網路資訊服務 (IIS) 管理員」找到此項功能。

點選下方「網頁服務延伸檢查」



請確認右方「所有未知的 ISAPI 擴充程式」已設定為「已允許」  
(若未設置成已允許請點選左方設置，或點選右鍵進行狀態變更)





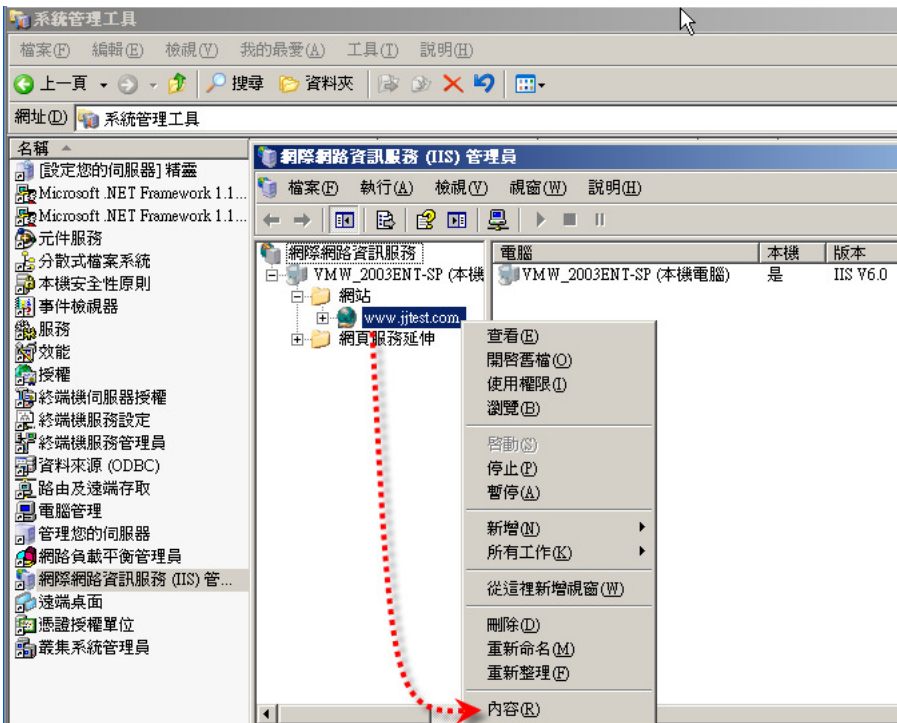
# DragonWAF (IIS6) Install Guide

## 網站應用程式防火牆 安裝手冊

### 3. IIS 防護網域設定檢查

請開啟您 IIS 主機中「網際網路資訊服務 (IIS) 管理員」  
您可以在「開始」→「程式集」→「系統管理工具」  
→「網際網路資訊服務 (IIS) 管理員」找到此項功能。

在要設定的網址列上，點選右鍵→「內容」





## DragonWAF (IIS6) Install Guide

### 網站應用程式防火牆 安裝手冊

DragonWAF 於進行產品註冊與網站防護時，需定義所需保護之網域名稱，故需要確認 IIS 主機，請於網站「說明」(下方紅框處)所輸入網域名稱。

網域名稱需為 DNS ( Domain Name System ) 可解析之網域名稱。  
或暫時替代 DNS 之解析設定方式，如本機 hosts 文件設定網址指向本機  
( 微軟作業系統預設位址為 %SystemRoot%\system32\drivers\etc\ )

The screenshot shows the 'www.jjtest.com 內容' dialog box in IIS6. The '網站識別碼' (Website Identification) section is expanded, and the '說明(S):' (Description) field is highlighted with a red rectangle and contains the text 'www.jjtest.com'. Other fields in this section include 'IP 位址(I):' (All unspecified), 'TCP 連接埠(T):' (80), and 'SSL 連接埠(L):'. The '連線' (Connections) section is also visible, showing '連線逾時時間(N):' (120 seconds) and checkboxes for '啟用 HTTP 的持續作用(K)' and '啟用記錄(E)'. The '現用的記錄格式(Y):' (Current log format) is set to 'W3C 擴充記錄檔案格式'.





# DragonWAF (IIS6) Install Guide

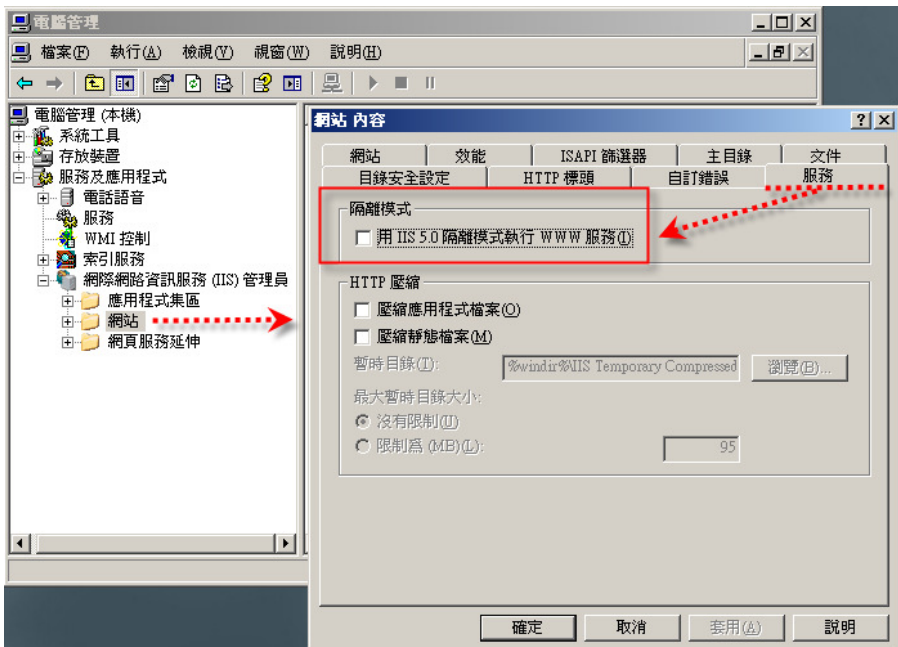
## 網站應用程式防火牆 安裝手冊

### 4. IIS 5.0 隔離模式確認

請您於桌面選擇「我的電腦」右鍵→「電腦管理」→「服務與應用程式」→「網際網路資訊服務 (IIS) 管理員」→「網站」右鍵→「網站內容」→分頁「服務」下方：

請確認「隔離模式」中

用 IIS 5.0 隔離模式執行 WWW 服務 (I) 為「不勾選」狀態



當您做好以上檢查後，您就可以開始進行系統安裝與註冊。





## DragonWAF (IIS6) Install Guide

網站應用程式防火牆 安裝手冊

### 安裝與註冊說明

請點選 DragonWAF 安裝程式，將自動執行以下安裝程序：

DragonWAF 安裝歡迎畫面



接下來，請選擇安裝目的地資料夾，點選面中「下一步」進行授權合約確認，請您詳細閱讀授權合約後（如下圖），如同意本授權規範，請點選「我接受該授權合約中的條款(A)」後，繼續安裝流程。



中 | 華 | 龍 | 網

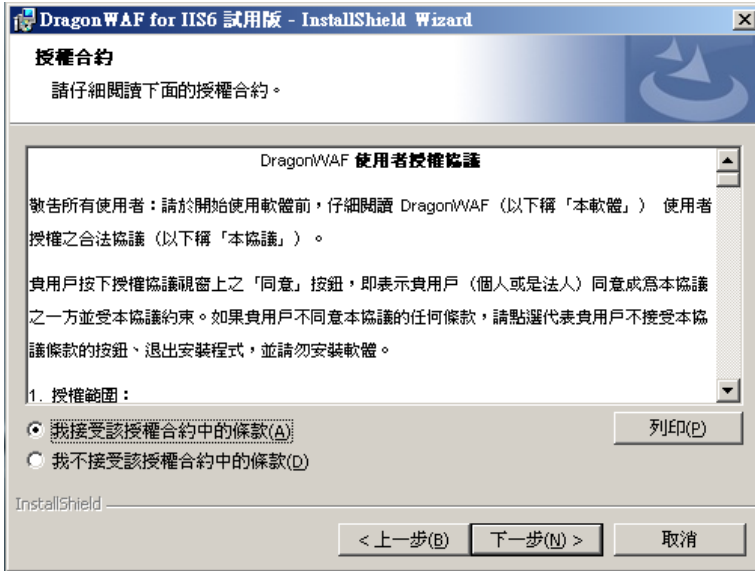
台灣資安軟體之先驅與領導廠商

Copyright© DragonSoft Security Associates, Inc. All rights reserved

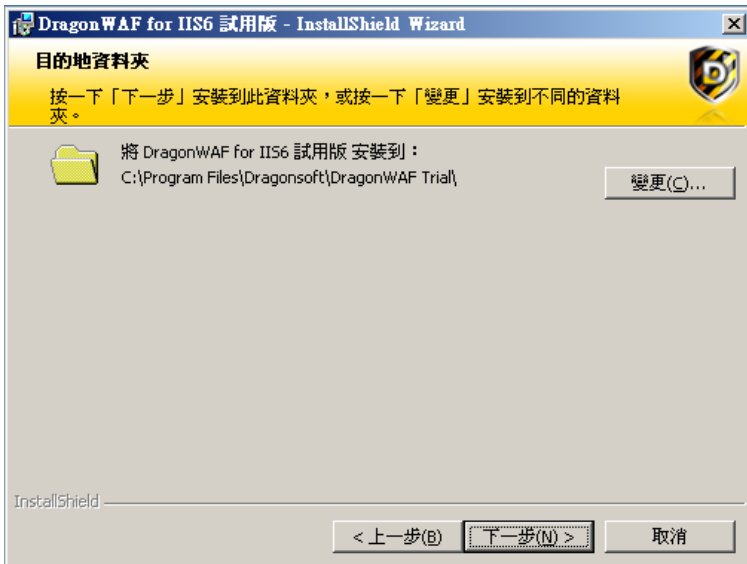


# DragonWAF (IIS6) Install Guide

## 網站應用程式防火牆 安裝手冊



### 選擇軟體安裝路徑

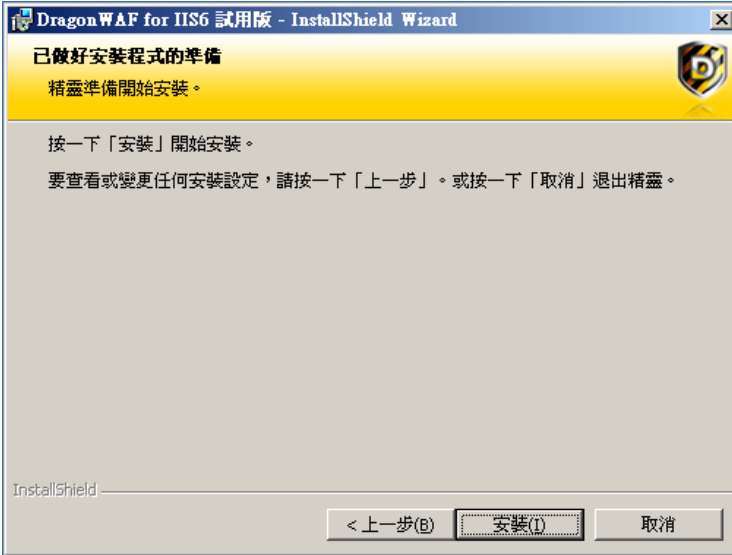




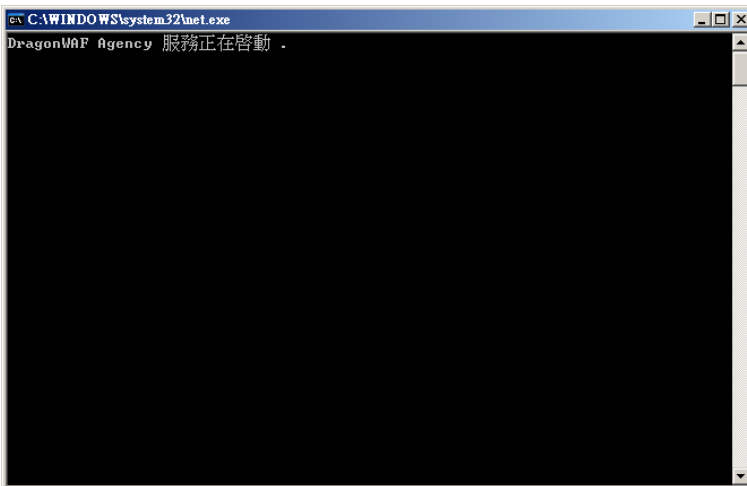
# DragonWAF (IIS6) Install Guide

## 網站應用程式防火牆 安裝手冊

請點選畫面中「安裝」，繼續安裝程序



系統將安裝 DragonWAF 相關服務





# DragonWAF (IIS6) Install Guide

## 網站應用程式防火牆 安裝手冊

服務啟動完畢，請點選「OK」進行下一步驟



請點選「完成」即完成安裝





# DragonWAF (IIS6) Install Guide

## 網站應用程式防火牆 安裝手冊

接下來您可以點選桌面，啟用 DragonWAF



或由「開始」→「程式集」→「DragonWAF」

→「DragonWAF 試用版」→「DragonWAF」啟用本軟體





## DragonWAF (IIS6) Install Guide

網站應用程式防火牆 安裝手冊

DragonWAF 軟體 進入畫面



DragonWAF 防護網站選擇 .

您可以於 IIS 所存在之網域列表中，選擇您想防護之網域，按下「註冊」



台灣資安軟體之先驅與領導廠商

Copyright© DragonSoft Security Associates, Inc. All rights reserved

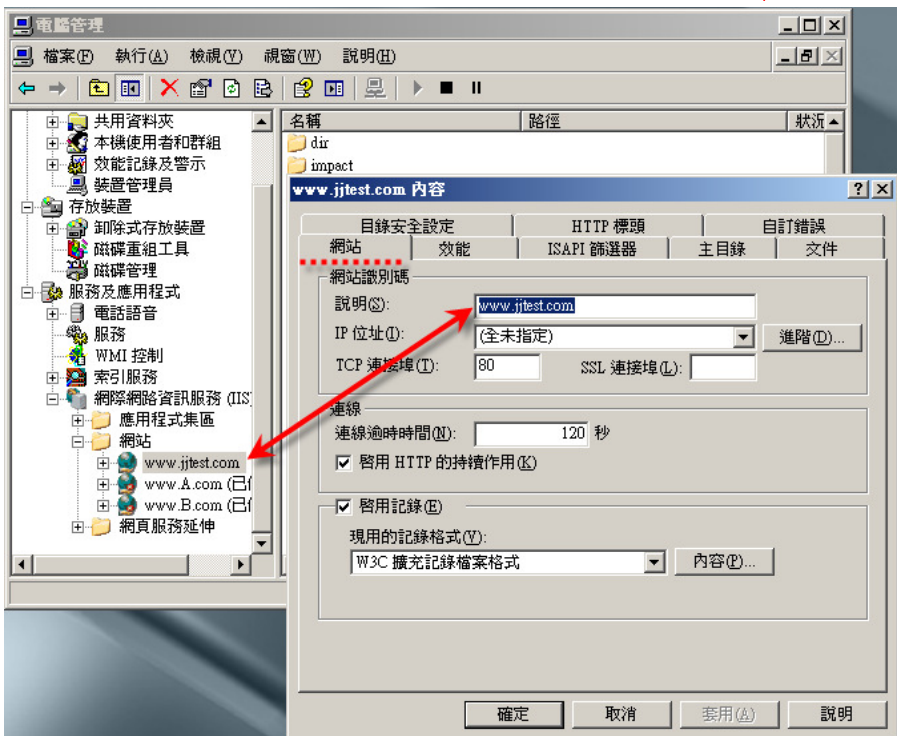


# DragonWAF (IIS6) Install Guide

## 網站應用程式防火牆 安裝手冊

若您所想要防護之網域不在「IIS 管理員網站」清單中，請確認，防護的網站上按右鍵裡的 [內容] -> [網站]，說明裡填入)

(網域名稱需為 DNS (Domain Name System) 可解析之網域名稱，或暫時替代 DNS 之解析設定方式，如本機 hosts 文件設定網址指向本機)





# DragonWAF (IIS6) Install Guide

## 網站應用程式防火牆 安裝手冊

如安裝版本為測試版，將顯示試用期限說明（如下圖），請按下「OK」繼續



您可以快速方便的防護網域列表以「>>增列」或「<<移除」，進行防護網站的調整，並可點選「啟用圖示」DragonWAF 將立即啟動網站防禦保護，捍衛您的網站安全，現在就來快速體會 DragonWAF 強大的網站防護能力吧。





## DragonWAF (IIS6) Install Guide

### 網站應用程式防火牆 安裝手冊

DragonWAF 安裝需求，於安裝前強制設定 DEP 資料執行防止設定項目  
本章節將協助您回復本設定項目：

若您「DEP 資料執行防止」原設定為

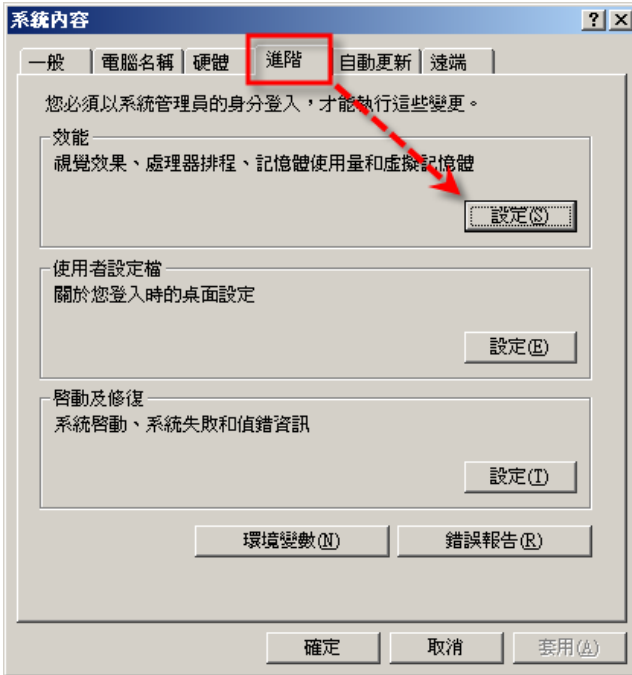
- A. 「只為基本的 Windows 程式和服務開啟 DEP(T)」，請忽略以下設定步驟。
- B. 「為所有的 Windows 程式和服務開啟 DEP，除了我選擇的這些(U)」，請點選，我的電腦點選「右鍵」→「系統內容」→「進階」(設定)點選→開啟資料執行防止





# DragonWAF (IIS6) Install Guide

## 網站應用程式防火牆 安裝手冊



請設定回「為所有的 Windows 程式和服務開啟 DEP，除了我選擇的這些(U)」  
並「新增」→ 以 C:\Program Files\Dragonsoft\DragonWAF\

試用版用戶，請於安裝路徑下增加、確定即可：

- DWPCC.EXE
- DragonWAFService.exe

正式版用戶，請於安裝路徑下增加、確定即可：

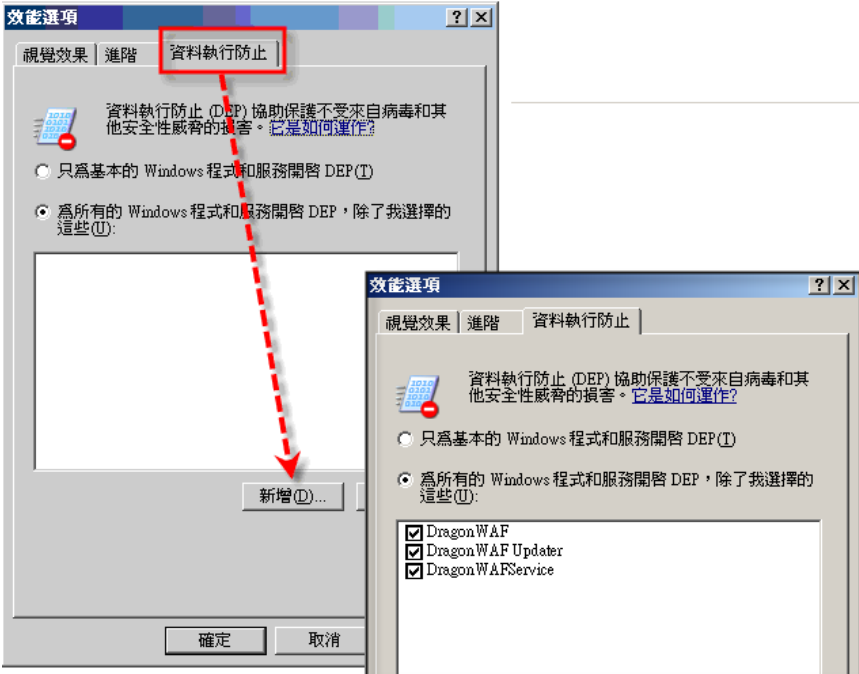




# DragonWAF (IIS6) Install Guide

## 網站應用程式防火牆 安裝手冊

- DragonWAFService.exe
- WAFUpdater



### 1. IIS 進階設定 適用設定規範

DragonSoft 建議您 基於提供網站更佳安全性，建議您進行以下設定避免惡意人士採用 IP 輸入方式進行非法攻擊字串輸入。

「請注意：因本設定為提供安全性規範設定，將禁止用戶以 IP 行為方式瀏覽網站，若網站是需要 IP 方式與他方串接驗證，如 銀行金流驗證..等等，則可忽略本項設定建議。」

設定步驟如下：

請設定「開始」→「程式集」→「工具管理員」，在要設定的網址列上，

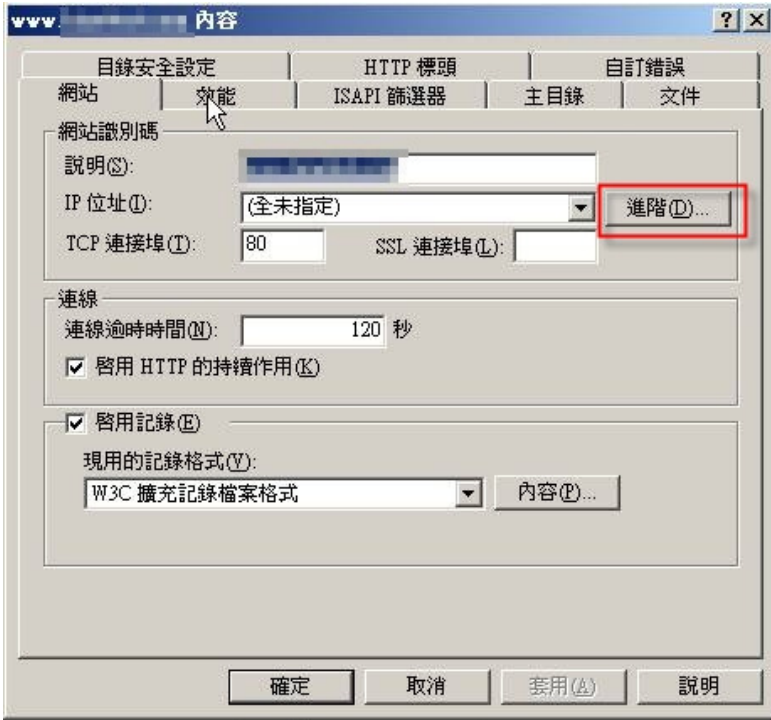




# DragonWAF (IIS6) Install Guide

## 網站應用程式防火牆 安裝手冊

點選右鍵→「內容」，進入「網站」設定分頁→請點選「進階」



畫面將出現「進階網站識別」設定畫面，請點選妳要設定的網址後，





## DragonWAF (IIS6) Install Guide

### 網站應用程式防火牆 安裝手冊

點選「編輯」(若無網址請自行點選「新增」,依序設定網址資料)



請輸入「網址」於畫面中「主機標頭值」,即完成以禁止以 IP 檢視網頁



## DragonWAF (IIS6) Install Guide

### 網站應用程式防火牆 安裝手冊

## 2. 多語系檔案/網頁名稱安全性建議 (測試版不提供本項修改)

網站包含多語系名稱，如：中文網頁與中文檔名，屬於惡意人士常採用之編碼漏洞攻擊方法，於 DragonWAF 安裝時，已預設阻絕網站提供「中文網頁/檔案」瀏覽/下載等功能。

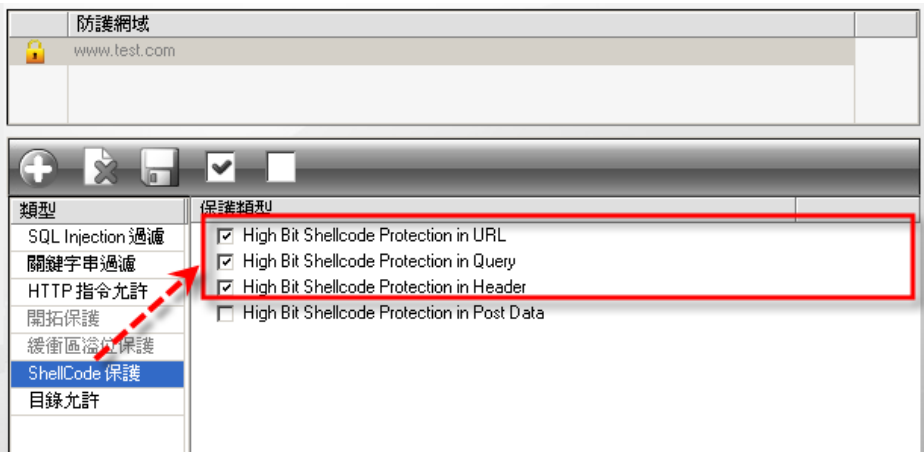
如單位暫時無考慮變更相關 多語系檔名、網頁名稱，您可以調整防護設定，以下畫面框架中 預設保護為採用「勾選」項目

### 「Shell Code Command 過濾防護」

不勾選：High Bit Shellcode Protection in URL

不勾選：High Bit Shellcode Protection in Query

不勾選：High Bit Shellcode Protection in Header





# DragonWAF (IIS6) Install Guide

## 網站應用程式防火牆 安裝手冊

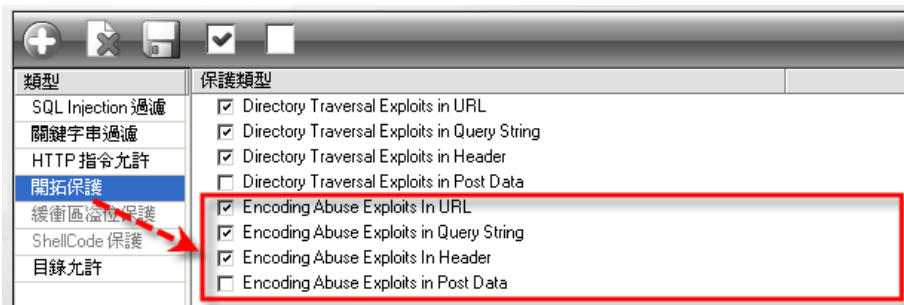
### 「Encoding Attack 編碼過濾防護」

不勾選：Encoding Abuse Exploit in URL

不勾選：Encoding Abuse Exploit in Query

不勾選：Encoding Abuse Exploit in Header

不勾選：Encoding Abuse Exploit in Post Data



### 注意：

當貴單位決定 不勾選以上防護選項時，即代表您已接受此風險存在於網站

DragonSoft 強烈建議您採用「英文與數字」為網頁（網站）檔案命名依循，若需更改以上細部設定請先行評估該停止之防護項目，可能影響遭受攻擊之風險性，為確保網站安全性、可用性仍建議您採取非中文編碼字元建置。





# DragonWAF (IIS6) Install Guide

## 網站應用程式防火牆 安裝手冊

中華龍網股份有限公司 DragonSoft Security Associates, Inc. 於民國九十二年元月成立，網路系統安全為本公司最主要的核心技術，並致力於網路安全產品開發，不斷以深耕台灣自有品牌出發提供國際水準之產品與服務，以網路安全軟體最佳提供者 (Security Solutions Provider) 為經營目標。

由新竹科學園區所延攬的資深研發人才、以及經營管理人，加上具豐富業界經驗之市場行銷專業人才加入，組成精實的團隊。其中技術團隊具專業的規劃及研發能力，能以企業管理的觀念提供最實際的網路安全產品。

目前資安產品領域包括：

- 弱點掃描風險挖掘.....DVM 網路安全弱點管理系統
  - 網站防掛馬防竄改.....DragonWAF 網站應用程式防火牆
  - DDoS 阻斷攻擊防禦.....RioRey DDoS 防禦系統
- .....

### Vulnerability Management (弱點管理)



作業環境： Vista, Windows XP,  
Windows 2000, Server 2003, Server  
2008

### DragonSoft Vulnerability Management

遠端安全弱點管理系統是專門為中大型企業的網路安全弱點實施網路安全漏洞管理的最佳解決方案，包含了安全漏洞掃描 (Security Scanner) 以及弱點風管理 (Vulnerability Risk Management) 兩大功能.....





## DragonWAF (IIS6) Install Guide

網站應用程式防火牆 安裝手冊

### DragonWAF (網站應用程式防火牆)



免費下載

作業環境：Windows  
XP, Windows 2000, Server  
2003, IIS 4.0、5.0、5.1、  
6.0

### Application Web Protector (伺服器防護軟體)

DragonWAF 採取過濾保護技術，當 IIS Web Server 面臨惡意攻擊行為時，DragonWAF 立即啟動防護功能，即時防止主機掛馬、網頁竄改等危機....

---

### DDoS Attack Prevention (阻斷攻擊防禦)



作業環境：(For rVIEW管理介面)  
Windows XP, Vista, Windows 2000,  
Server 2003, Server 2008, Linux and  
Mac OSX, requires Java ver. 1.5 or  
later

### DDoS Attack Prevention

台灣區獨家代理 RioRey DDoS防禦系統專為企業網站、電子商務、網路金流、網際網路服務提供者提供最佳DDoS阻斷式服務攻擊過濾防護解決方案，能有效保護網路服務主機.....

