# InstantScan
## 使用手冊

利基網路股份有限公司
**Secure Networks at Layer-7**

# 版權



InstantScan 使用手冊

版本 3.0

September 30, 2008

## 商標

# 技術支援

利基網路盡可能提供詳細的檔以供您安裝與設定您所購買的InstantScan產品。這些檔能說明您瞭解本產品的功能與設定步驟。您亦可從利基網路網頁http://www.L7-Networks.com下載相關產品的檔與資料。

如果您對InstantScan產品有任何技術上的問題或建議，請洽詢利基網路技術支持中心。當您洽詢技術支援的同時，請您務必準備好以下資訊，以節省您與技術人員溝通的時間：

- 產品型號與序號
- 保固期間
- 您收到本產品的日期
- 簡述產品的問題與您曾嘗試解決的步驟

| 聯絡方法 / 位置 | 電子郵件 | 電話<br>傳真 | 住址 |
|---|---|---|---|
| 臺灣臺北 | FAE@L7-Networks.com | +886-2-27936053 | 臺北市新湖三路289號3樓<br>3F, No. 289, Sinhu 3rd Rd., Neihu District, Taipei City 11494, Taiwan |
| 臺灣新竹 | FAE@L7-Networks.com | +886-3-5225946 | 新竹科學工業園區園區二路20號1樓<br>1F,No.20, Park Ave. II Rd.,<br>Science-based Park,<br>Hsinchu, Taiwan 300 |
| 中國上海 | FAE@L7-Networks.com | +86-21-52185699<br>+86-21-62386778 | 上海市北漁路28弄22號701室 |
| 中國廣州 | FAE@L7-Networks.com | +86-20-33820297*11<br>+86-20-3382-0297*18 | 廣州市天河區天陽路154號太陽廣場19D<br>19D, #154 TianYang Road,<br>TianHe Dist,Guangzhou,China. |
| 日本東京 | FAE@L7-Networks.com | +81-3-5434-9678<br>+81-3-5434-9686 | Alphasolutions Co., Ltd.<br>10F 8-8-5 Nishigotanda,<br>Shinagawa-ku,<br>Tokyo 141-0031, Japan |
| 美國<br>Santa Clara | FAE@L7-Networks.com | +1-408-844-8850<br>+1-408-844-8841 | Alpha Networks Inc.<br>3945 Freedom Circle, Suite 1150<br>Santa Clara, CA 95054, USA |

# 關於本手冊

本手冊利用 InstantScan內建的網頁介面（WBI）畫面說明，引導您設定並管理 InstantScan。爲了說明您瞭解如何使用本產品，您必須先瞭解 WBI 的使用方法。

## 對象

本手冊盡可能提供您設定 InstantScan 設備的詳細資訊。其主要指導物件爲設定 InstantScan、監控網路安全狀態、決定內容管理、與收發報表的網管人員。

## 相關檔

- InstantScan CD
  參考 CD 內附的檔資料。
- 快速安裝指南
  快速安裝指南協助您快速並且正確地安裝硬體與軟體。
- 線上協助
  線上協助提供個別的視窗說明與補充資料。
- 利基網路網頁
  請參考利基網路網頁 http://www.L7-Networks.com 的支援檔。

## 連絡訊息

本手冊內所提供的設定方法皆已經過測試與驗證，如果您發現某些功能已更改（或者發現任何錯誤），您可以將您發現的錯誤與您對將來版本的建議郵寄到以下的住址：


300 新竹科學工業園區園區二路 20 號 1樓
+886-3-6668896（電話）
+886-3-6668895（傳真）


您可利用電子郵件將訊息傳送給我們。如果您想讓本公司將您的電子郵件列入本公司郵寄清單中或索取產品目錄，請寄email到下列電子郵件信箱：


service@L7-Networks.com


尋求技術支援或對本手冊有任何評論，請寄到下列電子郵件信箱：


FAE@L7-Networks.com


尋求更近一步有關本手冊與本公司產品的資訊，請參觀本公司網站：

http://www.L7-Networks.com

# 目錄

# 第1部

## 產品簡介

# 版本快訊 3.0.04

本節敘述和之前的版本比較起來，本版新增或改善的產品功能。包含InstantScan的操作方式改變、因InstnatScan產品引擎效能與精確性的改善而造成的網頁設定介面變更。與上一版比較，2.2.05版提供下列加強功能：

## Release 3.0.04 (2008/09/24)

1. [BugFix] Incomplete MSN file recording.
2. [BugFix] Incorrect bandwidth accounting for bridge in CLI and UI (System Status).
3. [BugFix] Auto-reboot due to low memory during firmware upgrade?may cause corrupted flash.
4. [BugFix] Bypass card always goes into bypass since 3.0.
5. [BugFix] Web manager runs in sniffer mode by default.
6. [BugFix] URL keyword blocking now works in partial-matching mode.
7. [BugFix] Blocking policy in L7 must rely on enabling Traffic Manager.
8. [BugFix] No Game/Stock patterns shown in InstantScan series models.
9. [BugFix] UserConsole --> Group without Web Service
10. [BugFix] L4/L7 Manager will not reload configuration after modifing address objects in Object Manager
11. [NewFeature] Support new traffic discovery: App/Host/Policy views.
12. [NewFeature] Support default interface mapping for IX-5000V/IX-5000VB.
13. [Update] (Pattern) Built-in 2.1.05.326
14. [Update] (URLDB) Built-in 2.1.00.021

## Release 3.0.02 (2008/09/08)

1. [BugFix] Bridge learning timeout too long (15 seconds) when plugging the INT/EXT cables.
2. [BugFix] Web Manager may accidentally cause CPU 99%.
3. [BugFix] Logging system may be corrupted due to long pattern name.
4. [BugFix] Telnet/Ftp content recording may running out of free memory.
5. [BugFix] AD mapping causes heavy CPU loads at AD server.
6. [BugFix] AD mapping may not work well in Windows 2000 Active Desktop environments.
7. [BugFix] CLI "sys mgtserver" may cause "Invalid Checksum" problems.
8. [BugFix] Session count in AppView is not synchronized with that in HostView.
9. [NewFeature] Support multiple bridge with scheduled Traffic Manager policy rules.
10. [NewFeature] Support manual ordering/naming of network interface for all x86 hardware.
11. [Update] (Pattern) Built-in 2.1.05.320
12. [Update] (URLDB) Built-in 2.1.00.020

# 第1章
# 產品簡介

*本章介紹您如何快速安裝 InstantScan。*

員工上網不外乎用 Outlook 收信、用 Explorer 流覽網頁、用 MSN/Skype 等即時通訊（IM）跟朋友閒聊、用 KaZaA/Kuro/ezPeer 等點對點傳輸（P2P）下載非法資訊。其中，Email 與 IM 是洩密與病毒入侵的管道，而 P2P 更是頻寬的殺手與間諜軟體的溫床。L7 Networks 的 InstantScan 內容管理器，是無懼任何僞裝連線的第七層控管設備，以全球領先的 Inline 架構，依時間區段控管、側錄每個員工 IM/P2P 的細部使用行爲、聊天物件、傳檔檔案型別、聊天內容關鍵字、使用頻寬、傳檔掃毒、蠕蟲散佈等，並具備強大 IM/P2P 報表系統。除能追蹤員工洩密行爲/工作績效/側錄采證外，更對目前 Layer-4 埠號已無法反應實際流量頻寬的情況，提供了絕佳的頻寬管理與報表系統。

## 1.1 產品包裝檢查

請檢查您所購買的 InstantScan 產品包裝內容，如有遺失，請聯絡您當初購買本產品的經銷商。

| 編號 | 品名 | 備註 |
|---|---|---|
| 1. | 設備 | |
| 2. | L型固定鐵片 | |
| 3. | 螺絲組 | |
| 4. | 網路線 （RJ-45） | “串線” x 1 |
| 5. | AC 電源線 | |
| 6. | RS-232 console 線 | |
| 7. | CD | |

表格 1-1 產品包裝專案

## 1.2 硬體安裝

InstantScan 設備可以固定在標準 19 吋機架上，亦可以獨立放置於桌面上。請利用包裝盒內附的螺絲組將 L 型固定鐵片鎖於 InstantScan 上，然後將 InstantScan 安裝於機架上。

請依以下核對清單檢查您的網路連線是否已經備妥：

1. **InstantScan 設備**
2. **網路設備** – 如路由器、交換器、集線器（Hub）等。
   如果您將 InstantScan 連結到上述網路設備，請使用串線（through）相連。
3. **用戶端設備（CPE）** – 如桌上型 PC 或筆記型電腦等。
   如果您將 InstantScan 連結到上述用戶端設備，請使用跳線（cross-over）相連。
4. **將 InstantScan RJ-45 埠連結相對應之網路線**

InstantScan 系列產品的硬體規格根據您所購買的型號而有不同。當您將 InstantScan 安裝于路由器後方時，所有進出流量皆會受其控管。LAN 端的流量必須連接於 InstantScan Internal 端，而所有連外的流量必須藉由 InstantScan External 端與存取路由器（access router）相連。

## 1.3 將 InstantScan 連上網路

1. **電源**。首先將電源接上 InstantScan 背面的電源孔，然後將另一端接上電源插座。並將開關切換至 I。請稍候約兩分鐘，InstantScan 開機完畢後，再進行下一步連接動作。注意，IS-10 只需將變壓器的接頭接上其背後的電源孔即可啓動電源。
2. **Console 介面**。利用 RS-232 console 線，將 InstantScan console 埠與您用來設定 InstantScan 的 PC 對接。您即可透過 CLI 指令來設定 InstantScan 的系統參數。
3. **MGMT 介面**。此管理介面系用來傳送 InstantScan 的設定檔封包，所以必須透過網路線與 LAN 端的交換器或集線器相連，且要與管理伺服器在同一網段底下。
4. **Internal 介面**。此介面系透過網路線與您位於 LAN 端的交換器或集線器相連，用來管理所有內部可控管的網路流量。
5. **External 介面**。此介面系透過網路線將其與存取路由器相連，用來與網際網路連線。
6. **HA 介面**。用來連接備份設備，以確保網路不因硬體或意外而中斷。
7. **重設鍵**。用來重開機用，避免經常開關電源，而縮短軟硬體使用壽命。

## 1.4 InstantScan 的系統預設值 vs 範例設定

在下表中您可比較出廠預設值與本手冊範例中所使用的 IP 設定值。請記得，INT （Internal） 埠與 EXT （External） 埠並不需要設定任何 IP。因爲 Internal 埠是連接所有 LAN 端受 InstantScan 控管的用戶端，而 External 埠爲連接對外的網路。埠排列順序依您所購買的型號而有不同，當您首次使用 InstantScan 時，請進入 CLI 介面查看埠的排列順序。在許可權模式中輸入 “ip show”，您可以看出所有依照埠編號排列的埠，然後對照您設備上的編號，即可以此順序來連結您的網路線。

| 項目 | | 預設設定 | 範例設定 |
|---|---|---|---|
| Password | | admin | admin |
| Internal | Port No. | 1 | N/A |
| | IP Address | N/A | N/A |
| | Subnet mask | N/A | N/A |
| | Status | DOWN | UP |
| External | Port No. | 2 | N/A |
| | IP Address | N/A | N/A |
| | Netmask | N/A | N/A |
| | Status | DOWN | N/A |
| MGT | Port No. | 3 | 3 |
| | IP Address | 192.168.1.1 | 192.168.168.201 |
| | Netmask | 255.255.255.0 | 255.255.255.0 |
| | Gateway IP | 192.168.1.254 | 192.168.168.254 |
| | Primary DNS | 0.0.0.0 | 168.95.1.1 |
| | Secondary DNS | 0.0.0.0 | 0.0.0.0 |
| | Status | DOWN | UP |
| HA | Port No. | 4 | 4 |
| | IP Address | N/A | N/A |
| | Netmask | N/A | N/A |
| | Status | DOWN | DOWN |
| Management Server | IP Address | 尚未設定 | 10.1.1.10 |
| | Subnet mask | 尚未設定 | 255.255.255.0 |
| | Gateway IP | 尚未設定 | 10.1.1.254 |
| | Primary DNS | 尚未設定 | 168.95.1.1 |
| | Secondary DNS | 尚未設定 | N/A |

表格 1-2 InstantScan 相關系統預設值

# 第2部

# 基本設定

# 第2章
# 管理伺服器安裝

*本章節介紹管理伺服器的軟體安裝與網路設定*

## 2.1 管理伺服器軟體安裝

### 2.1.1 管理伺服器系統需求

- ✓ 作業系統 （OS） 至少應爲 Windows 2000/2003、Windows XP 或更高等級。如果您的作業系統爲英文板，請先安裝繁體中文字型套件，否則無法正常顯示中文字型。語言套件安裝視窗將於您開始安裝管理伺服器時顯示，請點選 Install 安裝。


圖表 2-1 語言套件安裝畫面

- ✓ 硬碟至少 80GB 以上可使用空間，建議最好有 120GB 可使用空間。
- ✓ CPU 最少是 Pentium 4 或同等級。
- ✓ 記憶體最少 256MB，建議最好 512MB 以上。
- ✓ 如果您的作業系統是 Windows XP service pack 2，且啓用其內建的防火牆，請記得依以下步驟開啓埠 514、1080 和 3306。如此一來，所有封包的進出，才不會因防火牆的攔阻而有所漏失，管理伺服器才會正常運作。
  1. 到開始 > 設定 > 網路連線。
  2. 點選區域連線，按滑鼠右鍵選擇內容。
  3. 到進階 > 設定值 > 例外。點擊新增埠...
  4. 輸入名稱與埠編號，點選此埠所使用的通訊協定（UDP 或 TCP）。點擊**確定**儲存設定值。

| 名稱 | 埠編碼 | 通訊協定 |
|---|---|---|
| Log Server | 514 | UDP |
| Socks | 1080 | TCP |
| Database Server | 3306 | TCP |

表格 2-1 管理伺服器埠設定

### 2.1.2 軟體安裝程式

1. 安裝 Management Server
2. 安裝 AD Log Server
3. Management Server 版本升級

4. 流覽光碟
5. 反安裝全部(只限移除 Management Server)
6. 反安裝 AD Log Server
7. 離開安裝介面

**注意：**

1. 當您重新安裝管理伺服器，或升級管理伺服器，請記得重新開機電腦，系統才會運作正常。詳細的安裝說明，請參考快速安裝指南。
2. 如果您曾經安裝過 MySQL 與 Apache 任何的版本，妳必須移除您所安裝的 MySQL 與 Apache 軟體，請參考附錄說明。

### 2.1.3 用戶端安裝

在您安裝好 InstantScan 管理伺服器並將 InstantScan 上的網路線連結完成後，您即可利用網頁流覽器，在網址列上鍵入 http://<管理伺服器 IP 地址>/ 來連上管理伺服器。當您第一次透過流覽器連上管理伺服器時，Java Plug-in 將從管理伺服器端安裝到您的用戶端電腦上。

**注意：**用戶端在第一次透過流覽器連上管理伺服器時，因流覽器的因素，必須花幾分鐘時間安裝 Java plug-in 程式，請耐心等候。

## 2.2 設定 InstantScan

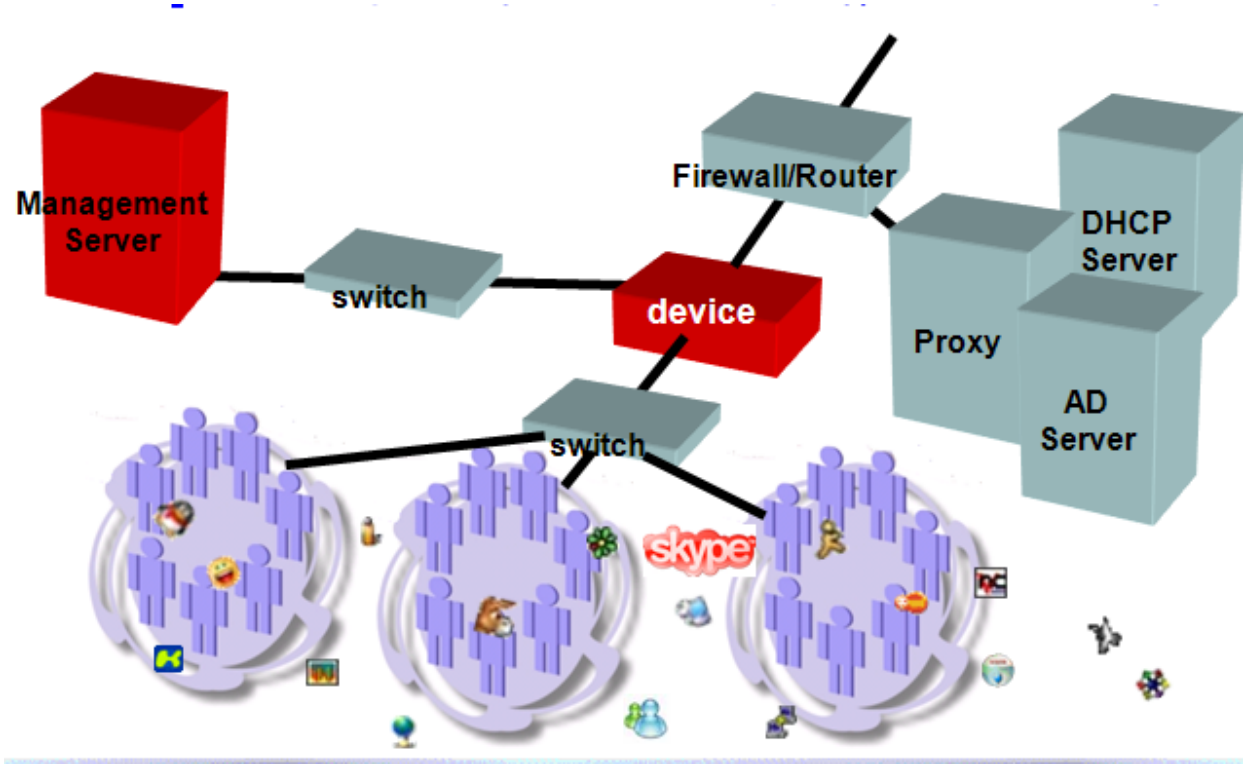
在您開始控管 InstantScan 設備前，請先利用 InstantScan 的 console 介面，直接用 RS-232 console 線與用來設定 InstantScan 用戶端的 PC 對接。然後，透過 CLI 指令來設定 InstantScan 的系統參數。之後，您可以利用 Telnet、SSH，或其他 terminal 等遠端連線方式來更改系統參數。

### 2.2.1 啓動系統

將鄰近 InstantScan 電源插槽的電源開關打開。在開機完成後，系統將要求您輸入 ID 與密碼。此時，預設的 ID 與密碼皆是 admin。在登入系統後，您可以利用 CLI 指令更改密碼。詳細 CLI 指令，請參閱附錄 A 說明。

### 2.2.2 系統架構

InstantScan以通透模式安裝於網路上，不需更改既有的網路架構。InstantScan管理伺服器配合InstantScan管理系統與報表系統，提供您簡而易用的使用者管理介面來設定管理政策。網管人員可根據網路架構與公司政策來訂定各式各樣的管理政策。一台管理伺服器可同時控管多台InstantScan，並且可接收與分析被控管的 InstantScan 之事件記錄。您可將管理伺服器安置於任何網路位置。本手冊提供一個基礎的 InstantScan 網路安裝架構。只要您瞭解基本的安裝原理，您即可根據貴公司的網路架構安裝您的 InstantScan。




圖表 2-2 InstantScan 系統的訊息遞送

如**錯誤! 找不到參照來源。** 所示，您必須指定 IP 位址給 **1） InstantScan 管理介面**（Management 埠）；**2） 管理伺服器**；與 **3）管理端 PC**。InstantScan 可安裝於企業網路內部或外部。當網管人員新增一條管理規則，並將設定文件上傳，管理伺服器立即將設定檔上傳至 InstantScan。當受到 InstantScan 控管的 PC 啓用任何即時通訊（IM）軟體或點對點（P2P）傳輸軟體時，InstantScan 會將這些事件記錄傳送給管理伺服器儲存。管理伺服器依您的時程規劃，定期產生報表寄送給網管人員分析。

### 2.2.3 系統參數設定

請用隨機內附的 RS-232 console 線，將InstantScan console介面與用來設定InstantScan的PC之序列埠相連，您可選擇COM1埠或COM2埠來設定InstantScan。請參考以下超級終端機的設定範例。

| **終端機類型** | 超級終端機 |
|---|---|
| 每秒傳輸位 | 115200 |
| 數據位元 | 8 |
| 同步檢查 | 無 |
| 停止位 | 1 |
| 流量控制 | 無 |

表格 2-2 終端機設定

| | |
|---|---|
| **步驟 1 登入系統**<br>系統預設的登入帳號密碼爲 **admin/admin**。之後您可以根據 CLI 指令來更改密碼。<br><br>**注意!!!** 密碼的長度必須藉於5~20字元間。小於5個字元或大於20個字元都會被系統拒絕。相關CLI指令請參考**錯誤! 找不到參照來源。**。 | InstantScan login: admin<br>Password:<br>Welcome to InstantScan...<br>InstantScan> |

**步驟 2 設定InstantScan IP 地址**

鍵入 **en** 進入許可權模式。鍵入 **ip set** 指令來設定 MGT 埠的相關 IP 位址。

**注意**，請先安裝好管理伺服器，否則系統將回復您”You must make sure the management server works well first.”的訊息。

```
Please enter the IP configuration for this device.
  IP Address [192.168.17.93]:
  Netmask [255.255.255.0]:
  Default Gateway [192.168.17.254]:
  Primary DNS [168.95.1.1]:
  Secondary DNS [0.0.0.0]:

  Your configuration is:
  ================================================================================
  Gateway: 192.168.17.254
  Primary DNS: 168.95.1.1
  Secondary DNS: 0.0.0.0
  Management Server: 192.168.17.205
  ================================================================================
  Port Interface IP Address       Netmask          Status
  ---- --------- ---------------- ---------------- ----------------------------
    1     INT3         N/A              N/A        UP   (Bridge 3)
    2     EXT3         N/A              N/A        UP   (Bridge 3)
    3     MGT    192.168.17.93    255.255.255.0    UP
    4     HA          N/A              N/A         DOWN (HA Disabled)
    5     INT1         N/A              N/A        UP   (Bridge 1)
    6     EXT1         N/A              N/A        UP   (Bridge 1)
    7     INT2         N/A              N/A        UP   (Bridge 2)
    8     EXT2         N/A              N/A        UP   (Bridge 2)
  ================================================================================
  Do you really want to apply and save [Y/N]? [N]? y
  Waiting for system setting.....
  Setting done.
```

**步驟 3 查看目前InstantScan設定狀況**

鍵入ip show，您可以看到目前InstantScan的IP設定狀況。

```
  ================================================================================
  Gateway: 192.168.17.254
  Primary DNS: 168.95.1.1
  Secondary DNS: 0.0.0.0
  Management Server: 192.168.17.205
  ================================================================================
  Port Interface IP Address       Netmask          Status
  ---- --------- ---------------- ---------------- ----------------------------
    1     INT3         N/A              N/A        UP   (Bridge 3)
    2     EXT3         N/A              N/A        UP   (Bridge 3)
    3     MGT    192.168.17.93    255.255.255.0    UP
    4     HA          N/A              N/A         DOWN (HA Disabled)
    5     INT1         N/A              N/A        UP   (Bridge 1)
    6     EXT1         N/A              N/A        UP   (Bridge 1)
    7     INT2         N/A              N/A        UP   (Bridge 2)
    8     EXT2         N/A              N/A        UP   (Bridge 2)
  ================================================================================
```

### 2.2.4 InstantScan 網頁介面設定

InstantScan 管理系統與報表系統使用 Java 平臺設計，需要支援 Java Plug-in 程式。所以用戶端必須從管理伺服器處安裝 Java Plug-in，才可流覽管理伺服器網頁。**當您第一次使用 IE 流覽器連結管理伺服器時，Java Plug-in 便會自動安裝進您的電腦。第一次登入時需要一些時間讓程式初始化，請耐心等候。**

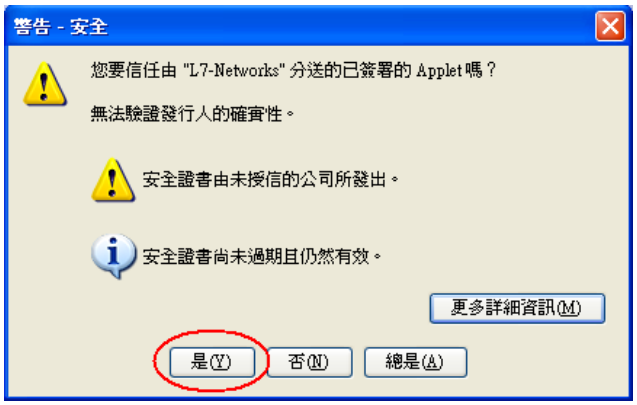
**步驟 1 連結管理伺服器**

指定一組 IP 地址給用來控管 InstantScan 的 PC （例如：192.168.168.1）。打開您的 IE 流覽器，在網址列上鍵入 http://<管理伺服器 IP 地址>。例如，輸入 http://10.1.1.10 來連結管理伺服器。

**注意：**如果您的管理端PC、管理伺服器、與InstantScan裝置不在相同網段內，請記得增加 NAT規則，允許不同網段的封包可以相互傳送接收。否則您無法透過管理伺服器連結到 InstantScan裝置。

**步驟 2 安全警告窗口**

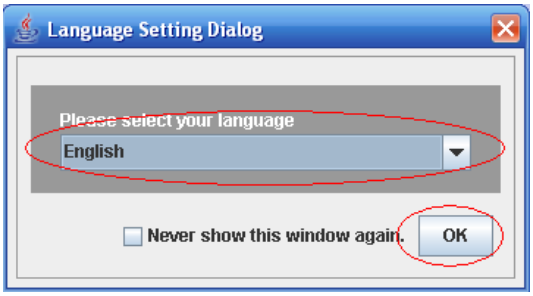
點擊**是**接受此驗證。如果您不想每次都出現此警告視窗，請點擊**總是**。當您點擊**是**或者**總是**後，您就可以進入登入畫面。




**步驟 3 選擇語言模組**

InstantScan目前提供英文、繁體中文、簡體中文等三種語言模組供您選擇，您可以選擇您喜愛的語言當成網頁介面的預設語言模組。點擊 OK 進入登入畫面。

注意，當進入網頁介面後，欲變更語言模組，您可以到 Tools > Language Setting 變更。




**步驟 4 登入**

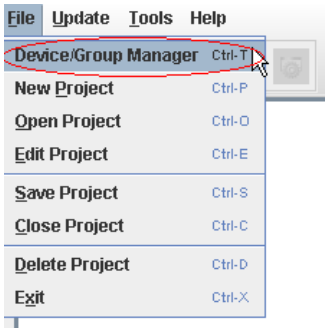
輸入ID/Password （預設都是 admin）。確認通過後，即可進入管理頁面。

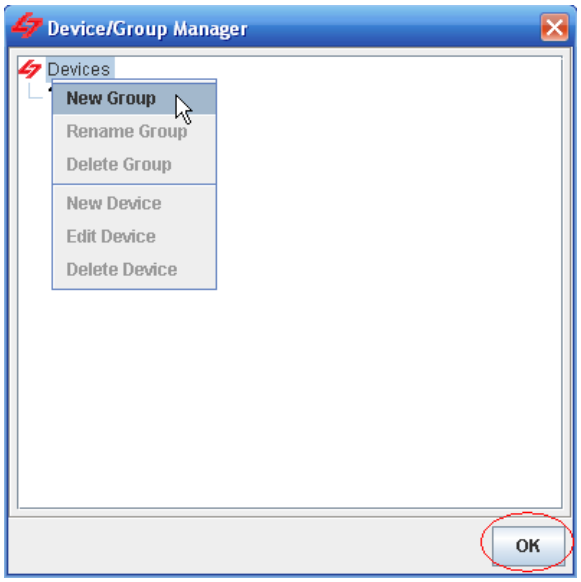
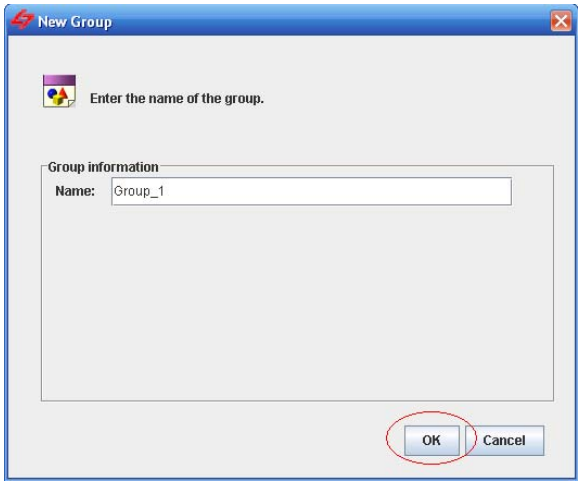
## 2.2.4.1 建立裝置/群組

**步驟 1 新增裝置/群組**

當您成功登入 InstantScan 後，請點選 Device/Group Manager 選項來新增 InstantScan 裝置與群組。

**File > Device/Group Manager**

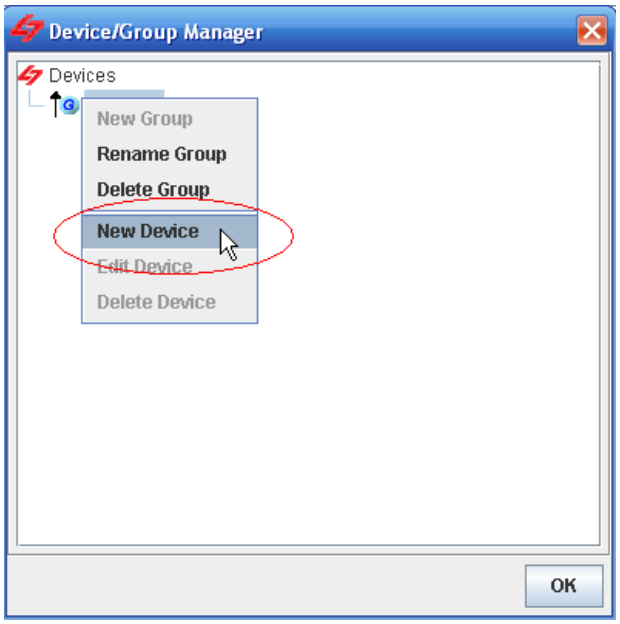


| | |
|---|---|
| **步驟 2 新增群組**<br>在Devices上按右鍵，然後點選**New Group**。 | **File > Device/Group Manager > New Group**<br>  |
| **步驟 3 輸入組名**<br>輸入此群組的名稱，然後點擊 **OK** 繼續。之後，組名將顯示在螢幕上。您可以按右鍵選擇Rename Group 或 Delete Group 來修改或刪除此群組。 | **File > Device/Group Manager > New Group**<br>  |

**步驟 4 新增裝置**

在群組 Group_1上按右鍵，然後點選New Device。

**File > Device/Group Manager > New Device**

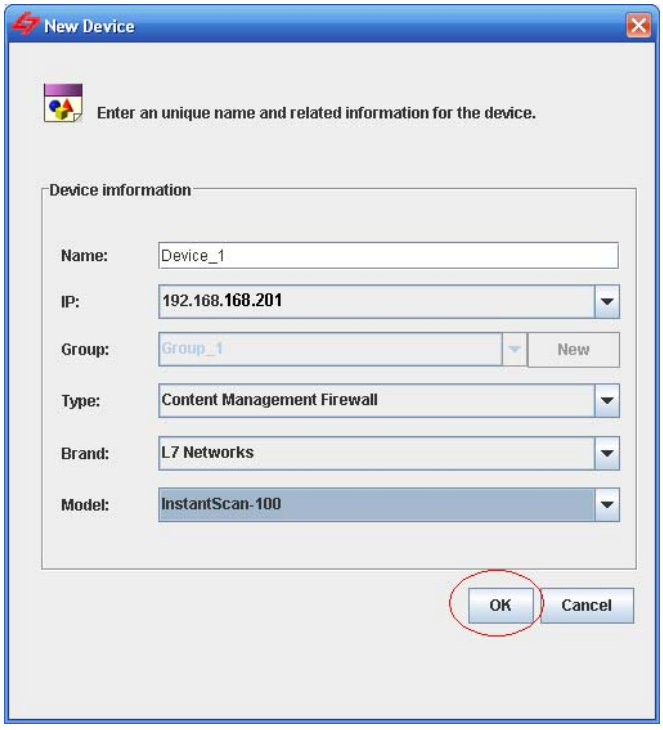



**步驟 5 編輯相關裝置的資訊**

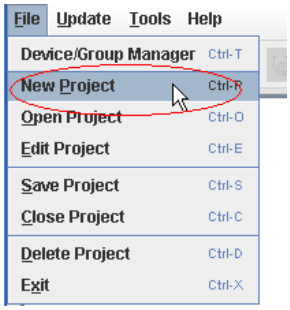
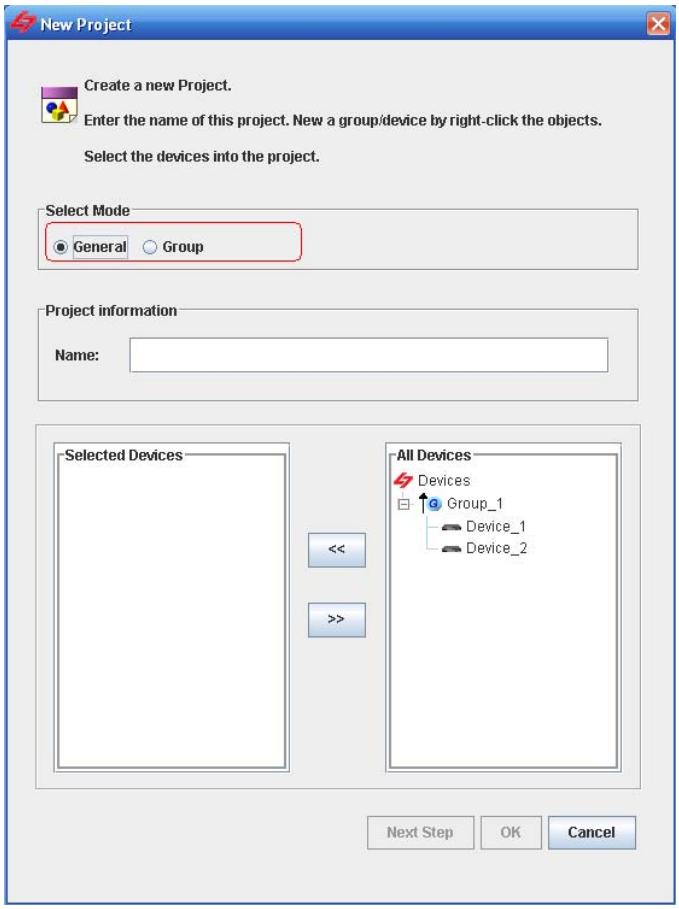
輸入裝置名稱，並選擇一組已指定其管理伺服器的 InstantScan 裝置之 IP 位址，然後輸入其餘相關資訊。點擊 **OK** 儲存設定。

注意：您必須先透過 CLI 介面，設定好裝置上的 IP，然後指定管理伺服器 IP 位址，否則您無法在 UI 上新增任何裝置。當您設定好裝置後，管理伺服器將自動擷取屬於其列管的 device 資訊。只要是已經設定過的裝置，就不可以再被設定。也就是說，當您已經設定好Device_1 192.168.168.201，如果您要再新增裝置時，IP 欄位內將不會再出現 192.168.168.201 這個 IP 位址。

**File > Device/Group Manager > New Device**



### 2.2.4.2 新增專案

| | |
|---|---|
| **步驟 1 新增專案**<br>選擇 **New Project**。 | **File > New Project**<br>  |
| **步驟 2 建立新專案**<br>首先，請點選項目的模式，輸入專案名稱，從 **All Devices** 欄位中選擇要加入此專案的裝置，然後點擊 **<<** （左向箭頭）將點選的裝置加到 Selected Devices 欄位。如果您要從此專案移除某個裝置，請點選該裝置，然後點擊 **>>** （右向箭頭）即可。 | **File > New Project > New Project**<br>  |

| 專案模式 | 說明 |
|---|---|
| General （一般）。 | 您希望每台 InstantScan 裝置可以擁有其個別的設定檔，每台裝置可擺放在不同的網路位置，且各自獨立運作，您可以選擇此模式。 |
| Group （群組） | 當您購買 2 台或 2 台以上 InstantScan 裝置，希望簡化設定的步驟，所有裝置的設定檔共用，其報表系統也共用。也就是說，不管您在哪一台 Device 上變更設定檔，此設定檔都會寫進基底裝置（Base Device）的設定檔中。其他裝置只要重載設定檔即可擷取最新的設定檔。 |

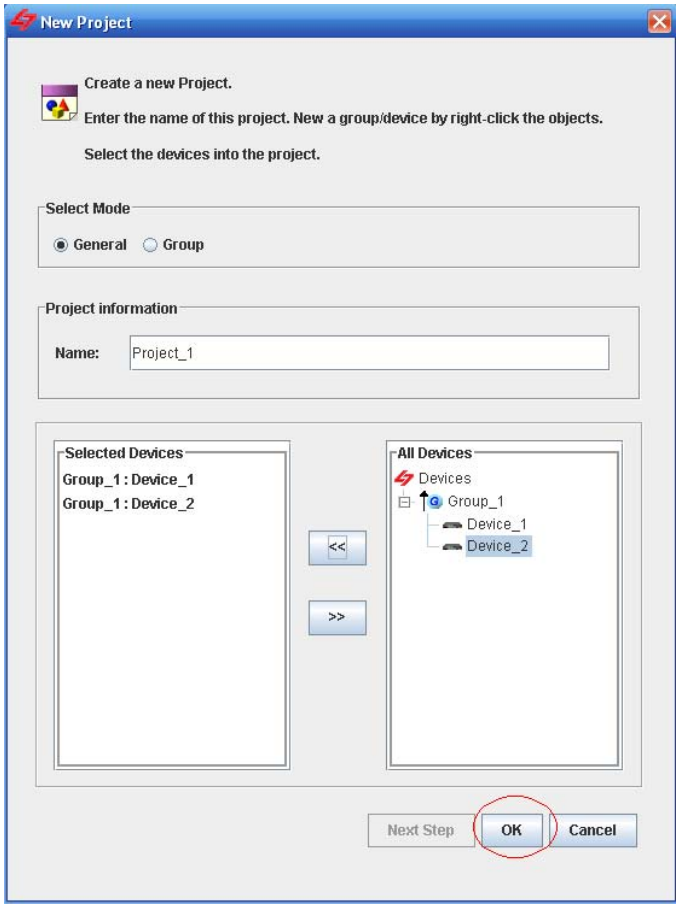
表格 2-3 專案模式

## 一般專案模式

**步驟 1 新增一般專案模式**

選擇 **General （一般）**爲專案的模式，這個模式適合大部分的案例。輸入項目名稱，從 **All Devices** 欄位中選擇要加入此專案的裝置，然後點擊 **<<（左向箭頭）**將點選的裝置加到 **Selected Devices** 欄位。如果您要從此專案移除某個裝置，請點選該裝置，然後點擊 **>>（右向箭頭）**即可。最後點擊 **OK** 結束設定。

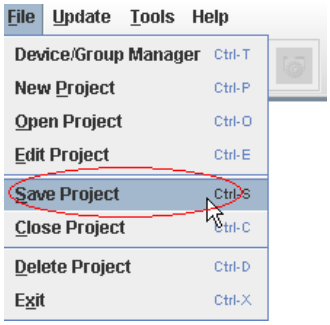
**File > New Project**




**步驟 2 儲存專案**

點選 **Save Project** 儲存已建立的專案。

**File > Save Project**

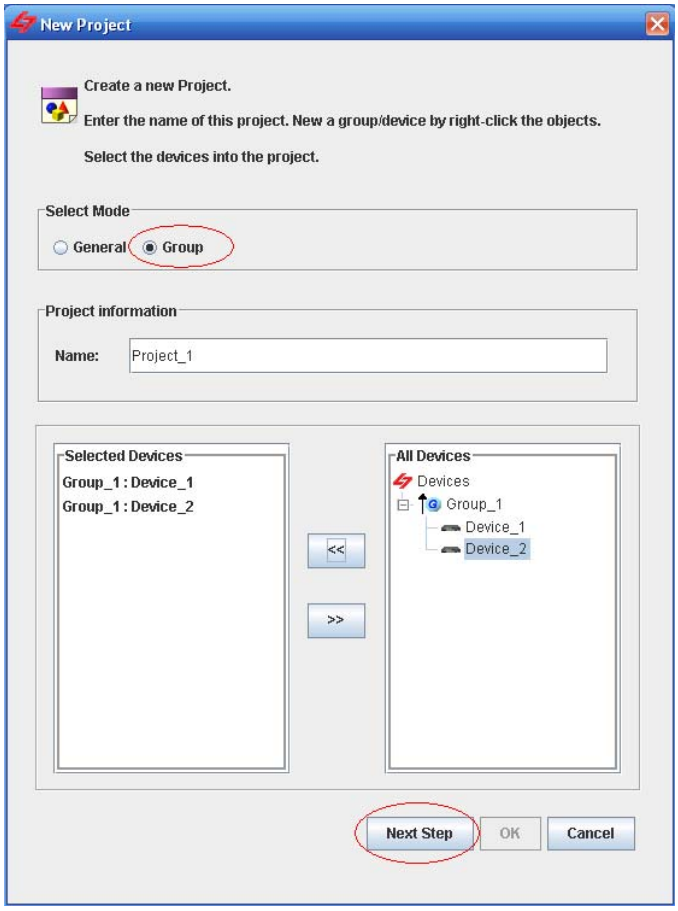


## 群組專案模式

**步驟 1 新增群組專案模式**

選擇 **Group （群組）**爲專案的模式，這個模式適合購買多台 InstantScan，希望簡化設定步驟，節省人力資源的公司。輸入項目名稱，從 **All Devices** 欄位中選擇要加入此專案的裝置，然後點擊 **<<**（**左向箭頭**）將點選的裝置加到 **Selected Devices** 欄位。如果您要從此專案移除某個裝置，請點選該裝置，然後點擊 **>>** （**右向箭頭**） 即可。最後點擊 **Next Step** 繼續下一步驟。

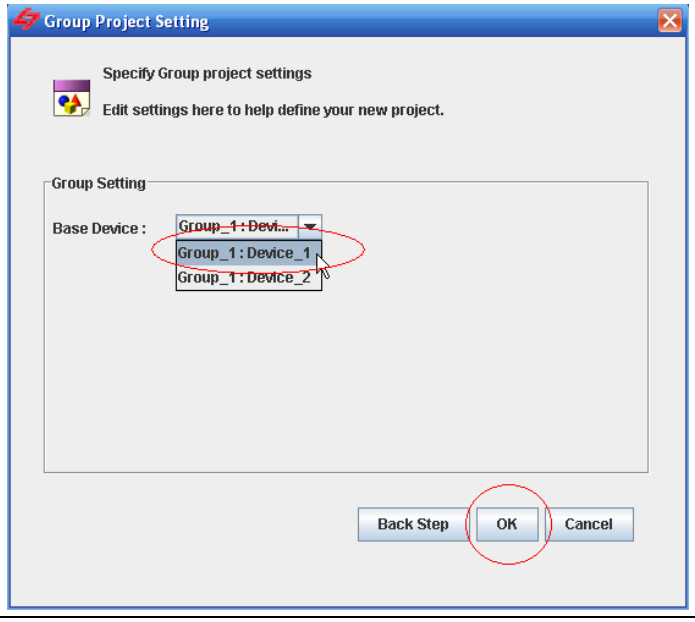
**File > New Project**

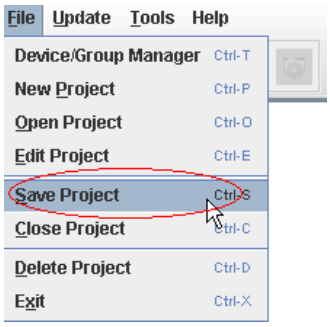



**步驟 2 選擇基底裝置**

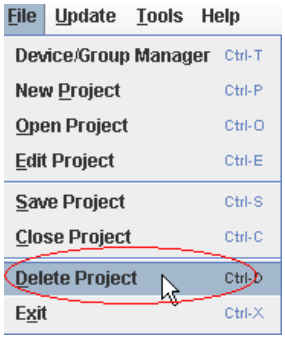
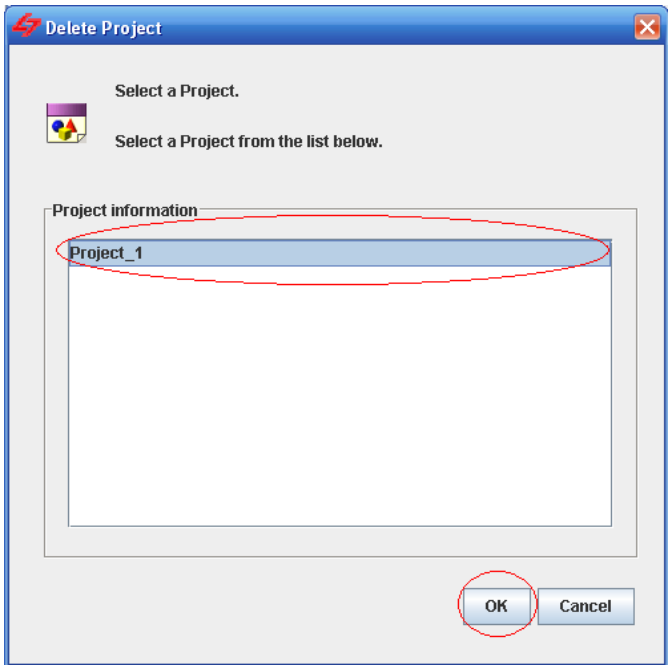
選擇 **Base Device**（基底裝置），當您選擇基底裝置後，所有此專案內的裝置都會讀取這個基底裝置的設定檔，且讀取的報表是所有裝置的總和。最後點擊 **OK** 結束設定。

**File > New Project > Next Step**

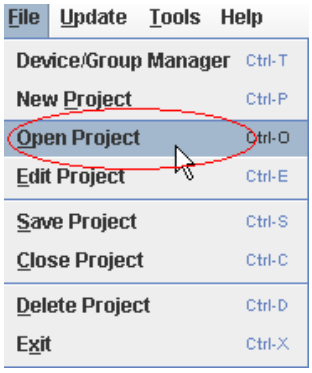
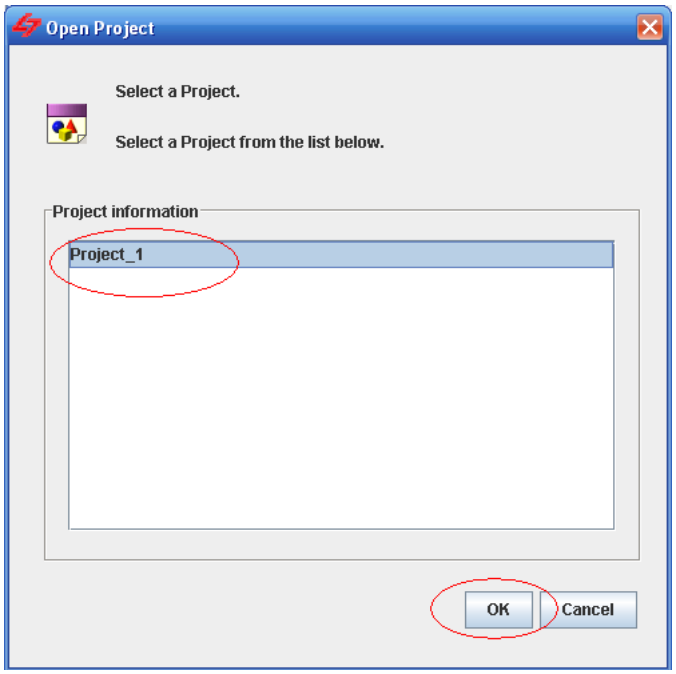


| | |
|---|---|
| **步驟 3 儲存專案**<br>點選 **Save Project** 儲存已建立的專案。 | **File > Save Project**<br>  |

### 2.2.4.3 刪除項目

| | |
|---|---|
| **步驟 1 點選刪除項目**<br>點選 **Delete Project** 選項。 | **File > Delete Project**<br>  |
| **步驟 2 刪除項目**<br>選擇您想刪除的項目，然後點擊 **OK** 關閉視窗。<br><br>**注意：**<br>1. 一旦您點擊 **OK** 按鈕後，此專案即刻會從系統中刪除。<br>2. 正在執行中的專案無法刪除，您必須先關閉項目，才可選擇刪除項目。 | **File > Delete Project**<br>  |

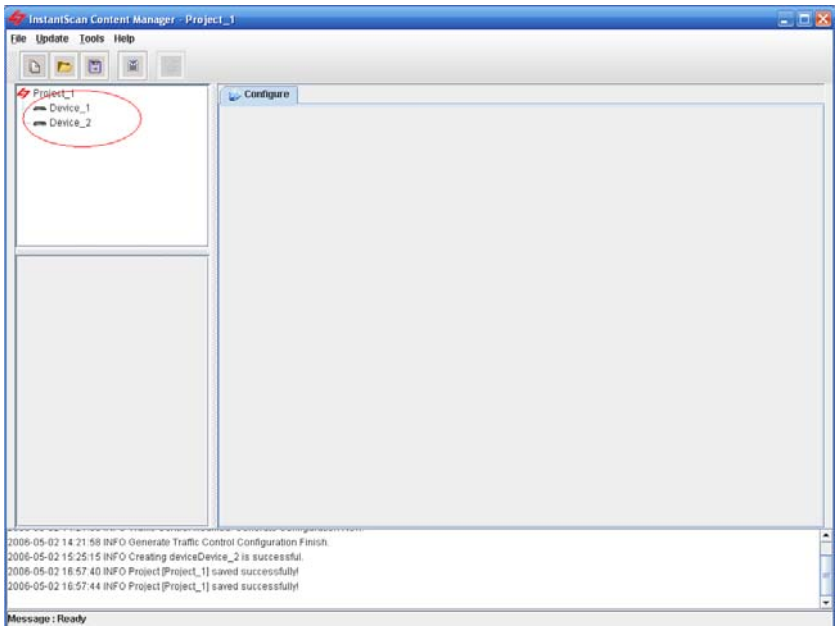
### 2.2.4.4 開啓已存在的項目

| | |
|---|---|
| **步驟 1 開啓專案**<br>點選 **Open Project** 選項。 | **File > Open Project**<br>  |
| **步驟 2 選擇要開啓的專案**<br>選擇您要開啓的專案。點擊 **OK** 關閉窗口。 | **File > Open Project**<br>  |

**步驟 3 管理 InstantScan**

現在，您可以開始管理您的 InstantScan。一個項目可以同時控管多台可能屬於不同群組的裝置。將滑鼠移到您要控管的裝置上點兩下，系統將連結到此裝置，並下載其設定檔。

**File > Open Project**



# 第3章 mailer

*本章介紹 mailer 的設定與其應用*

## 3.1 Mailer 概述

在管理伺服器安裝完成，且重開機後，有一小圖示 （mailer）將會顯示在伺服器的右下角。請將滑鼠移到圖示上，點兩下。mailer 的功用如下：

- **系統資訊：**查詢 CPU/Memory 使用狀態、資料庫/HTTP/管理伺服器的存取目錄、管理伺服器的 IP/MAC 等相關資訊。
- **郵件警告：**設定郵寄伺服器與自訂電子郵件警告內容。
- **FTP 備份：**設定 FTP 伺服器、資料備份時間與備份類型、並選擇備份狀態。
- **報表中心：**可選擇報表寄發的時間、格式、報表收件者與選擇報表的來源 (裝置)。在設定報表中心前，請在裝置上設定匯出報表的專案，相關設定請參考章節。
- **系統記錄：**設定系統操作記錄的收件者，與希望收到的系統記錄的嚴重等級。

詳細設定說明，參請考以下的說明。

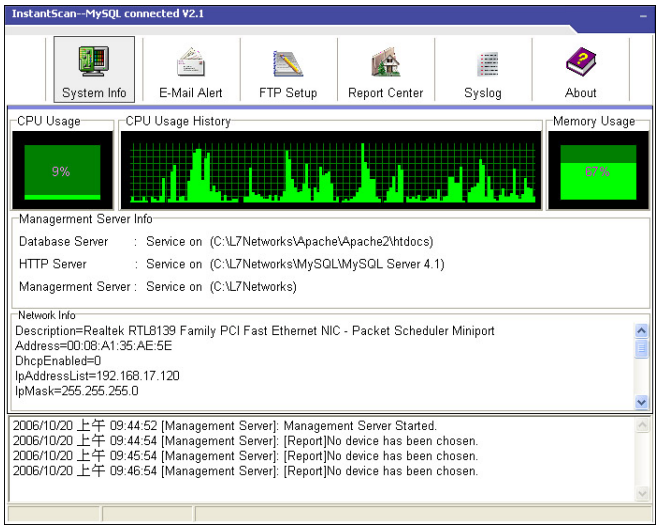
## 3.2 Mailer 設定

在管理伺服器安裝完成，且重開機後，有一小圖示將會顯示在伺服器的右下角。請將滑鼠移到圖示上，點兩下。

**步驟 1 系統資訊**

在這個頁面上，您可以看到 CPU 與記憶體的使用情況，還有一些管理伺服器的存放位置、網路訊息等。

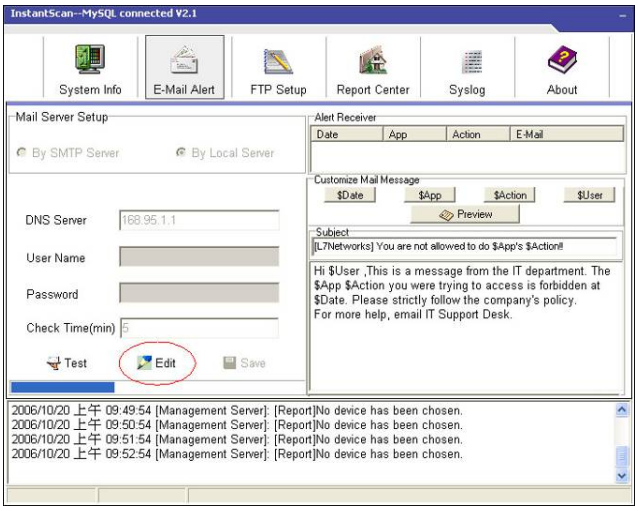
**mailer > System Info**



**步驟 2 設定郵件伺服器**

點擊 **Edit** 按鍵。選擇 **By Local Server** 選項。輸入 DNS 伺服器 IP 位址，並在 **Check Time（min）**欄位上鍵入系統檢查是否有警告信件的時間。如果您希望透過 SMTP 伺服器寄送警告信件，請點選 **By SMTP Server** 選項。您可以點擊 **Test**，然後在彈跳出來的視窗內輸入收件者的電子郵寄地址，最後點擊 **OK** ，測試連線狀態。

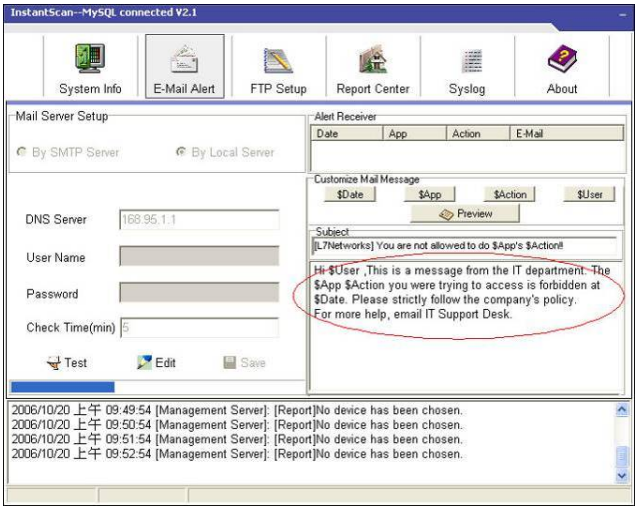
**Mailer > E-Mail Alert > Edit**




**步驟 3 客制化郵件訊息**

將游標移到文字方塊中要加入變數的位置，點擊變數（$Date、$App、$Action、$User）。

**Mailer > E-Mail Alert > Customize Mail Message**



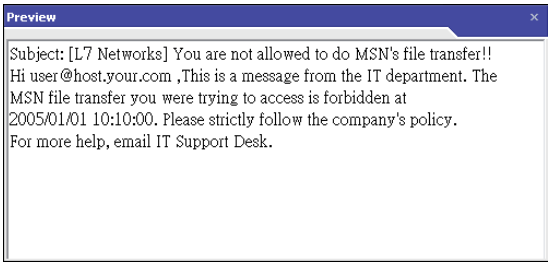

| 變數名稱 | 說明 | 範例 |
|---|---|---|
| $Date （日期） | 違反政策事件發生的日期。 | 2005/01/01 10:10:00 |
| $App （應用軟體） | IM使用者違反政策時所使用的IM軟體。 | MSN |
| $Action （使用行爲） | 不合法的IM使用行爲。 | file transfer |
| $User （使用者帳號） | 違反政策的IM使用者帳號。 | user@host.your.com |

表格 3-1 警告信件內的變數設定

**步驟 4 預覽警告郵件內容**

當您設定好警告信件內容，可點擊 **Preview** 預覽。關閉預覽視窗繼續下一步。

**Mailer > E-Mail Alert > Customize Mail > Preview**

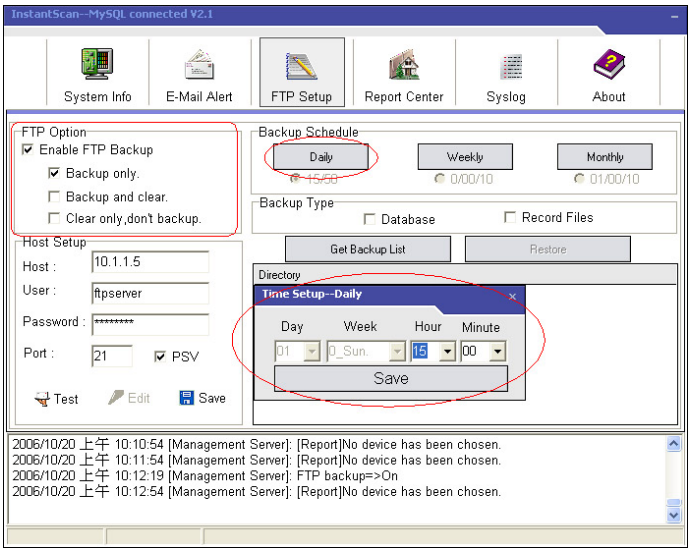



**步驟 5 FTP 設定**

在本頁，您可設定利用FTP備份記錄的方式。勾選 **Enable FTP Backup**，然後勾選 **Backup only**。

您可以選擇FTP自動備份的時間 1） 每日 2） 每週 3） 每月。點擊 **Daily**，然後選擇**15 : 00**。換句話說，每天下午 3 點，系統會開始透過 FTP 備份當天的事件記錄。

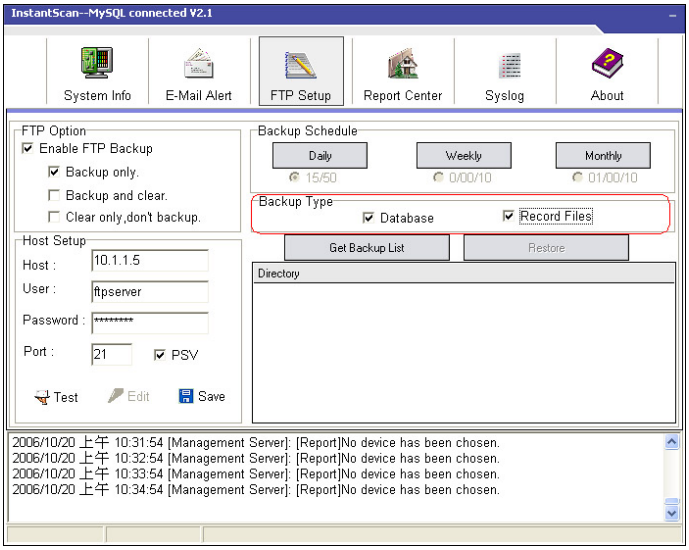
**Mailer > FTP Setup > FTP Schedule**




**步驟 6 設定備份類型**

請在 **Backup Type** 選擇資料備份類型。當您要還原您已被份的資料，請點擊 **Get Bakup List** 按鈕，然後選擇要從 FTP 伺服器上下載的路徑，點擊 **Restore** 開始資料庫或檔案還原。

**Mailer > FTP Backup > Backup Type**

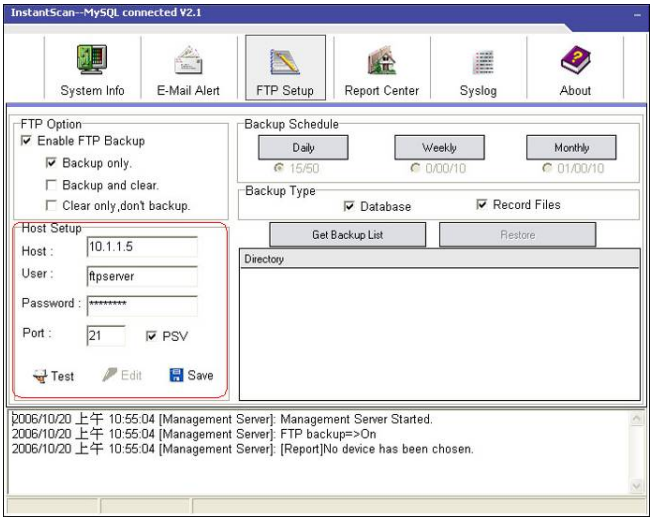


**步驟 7 FTP 伺服器設定**

點選 Edit 開始編輯相關設定，輸入 FTP 伺服器 IP 位址、使用者帳號與密碼。如果 FTP 伺服器使用 passive mode 的話，請勾選 PSV。點擊 Test 測試 FTP 連線狀況。再點選 Save 記錄您所設定的相關選項。

承上所述，您選擇每日下午 3 點 00 分備份 log，系統將於此時自動 FTP 備份 log。所備份的資料夾將會以該日的日期命名。

**Mailer > FTP Setup > Host Setup**

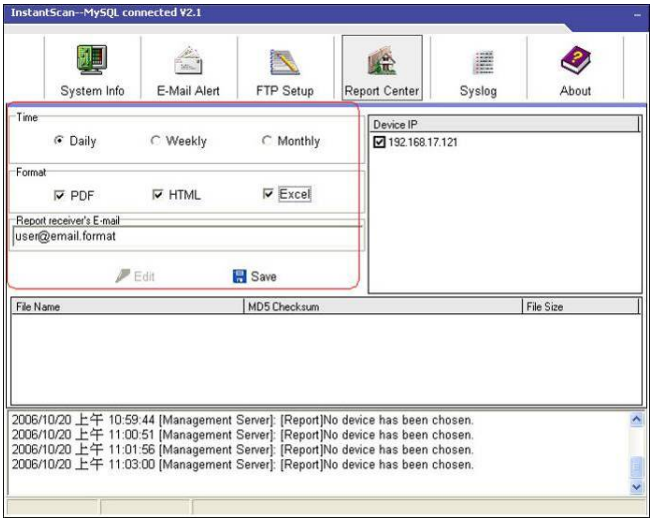



**步驟 8 報表中心**

點選 Edit 開始編輯相關設定，選擇寄送報表的時間（每日/每週/每月）。勾選您希望收到的報表格式（PDF/HTML/Excel），與勾選希望收到哪些 InstantScan 設備的 log。輸入收信者的電子郵件信箱。再點選 Save 記錄您所設定的相關選項。

**注意**：在您設定報表中心前，請先確定您已經在 InstantScan 使用者介面上上定好報表輸出的專案與格式，否則您收到的報表會是空的。

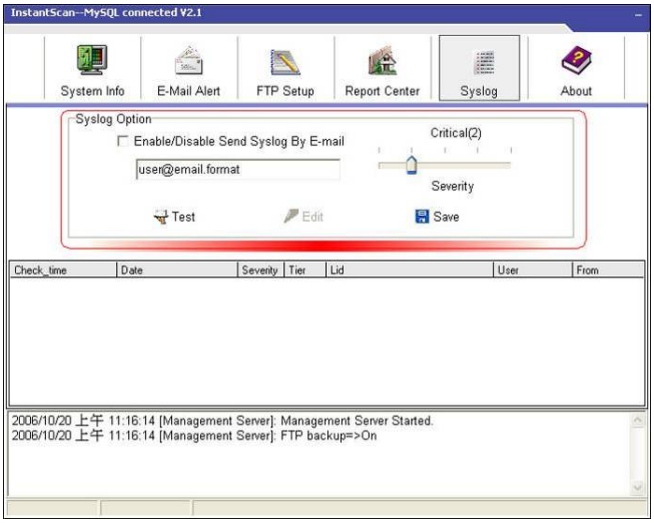
**Mailer > Report Center**




**步驟 9 系統記錄**

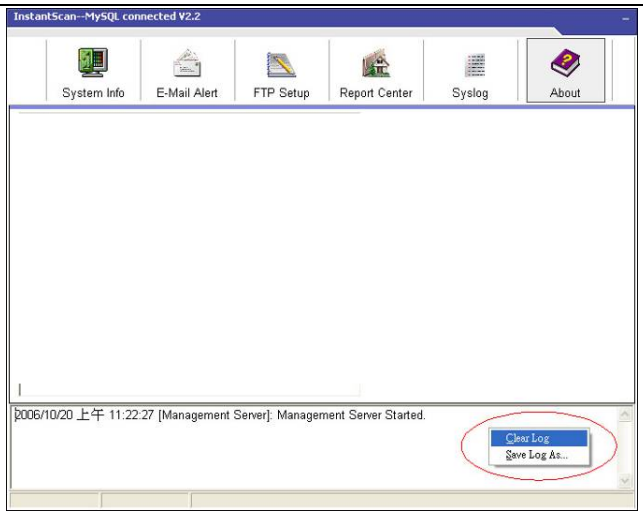
點選 Edit 開始編輯相關設定，勾選 Enable/Disable Send Syslog By E-mail，然後在空格處填寫您的 Email 位址。利用滑鼠移動到您想要收到的系統記錄的等級。共分爲 5 個等級 1) Alert （警告）2) Critical （嚴重） 3) Warning （警示） 4) Notification （注意）5) Information（資訊）。如果您只希望收到 Alert 等級的系統記錄，只要將指標拉到 Alert 的位置。但是，如果您希望收到所有的系統記錄，您必須把指標拉到 Information 的位置。點擊 Test 測試 E-Mail 信箱。再點選 Save 記錄您所設定的相關選項。

**Mailer > Syslog**



**步驟 10 清空/儲存系統記錄**

在狀態欄內按右鍵。您可選擇清空事件記錄或者將紀錄儲存到硬碟上。




⚠ 如果您不小心關閉 mailer，您可以在桌面或 C 磁槽根目錄，L7 Networks 資料夾內找到檔案 mailer.exe。移動您的滑鼠，在 mailer.exe 圖示上點兩下，即可開啓它。Mailer 預設儲存的路徑爲 C:/L7Network。

# 第4章
# IM 帳號驗證

*本章介紹如何設定 IM 帳號驗證，讓使用者透過 InstantScan 註冊即時通訊帳號。*

InstantScan 支持 POP3（s）、IMAP（s）、Radius、LDAP 等帳號驗證方式。使用者可以您可以結合現有的 POP3（s）、IMAP（s） 郵件系統資源，讓通過驗證的使用者註冊自己的即時通訊帳號。您亦可以利用 Radius 或 LDAP 伺服器讓使用者透過向伺服器驗證通過，取得註冊帳號的許可權。

## 4.1 驗證的種類

使用者必須透過流覽器完成帳號驗證。當您設定好驗證類型，使用者只要在網址列上鍵入 InstantScan 設備的 IP 位址，驗證的視窗就會顯示出來。

請參考下列五個步驟來設定帳號驗證：

1. 啓用驗證功能。
2. 設定驗證類別。
3. 設定驗證各項參數。
4. 透過 IE 流覽器，在網址列上鍵入 https:// InstantScan IP 地址/ （例如: https://192.168.168.201/） 連結驗證網頁.

## 4.2 設定驗證類型

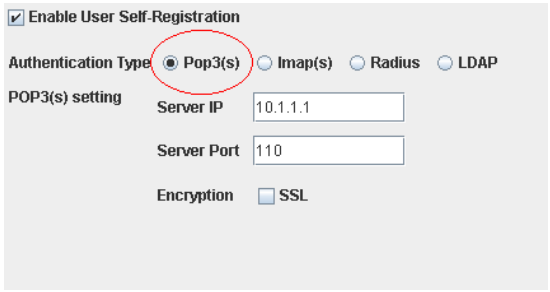
### 4.2.1 Pop3（s）設定

**步驟 1 設定 Pop3（s）驗證**

勾選 **Enable User Self-Registration（啓用驗證）**。選擇 **Pop3（s）**爲驗證類型。輸入伺服器 IP 和伺服器埠。如果您的伺服器需要透過加密（埠號 995）連線驗證，請勾選SSL。然後上傳設定檔。

**注意：**Pop3 服務透過埠 110 連線而 Pop3s 服務透過埠 995 連線。

**IM Manager > Auth > Pop3（s）**




| 欄位 | 說明 | 範例 |
|---|---|---|
| Server IP | Pop3（s）伺服器的 IP 地址。 | 10.1.1.1 |
| Server Port | Pop3（s）伺服器資料進出的通訊埠。例如，Pop3 服務透過埠 110 連線而 Pop3s 服務透過埠 995 連線。 | 110 |
| Encryption | 所謂的 SSL 是利用大數值編碼的技術將資料編碼後再傳至遠端，全球資訊網在建置之後，必須向一個有公信力的單位登入，並取得一個 Private Key，而將另一個 Public Key 放在網路上；資料在網際網路傳輸時都是經過編碼的資料，即使有人在中間要擷取這些經過編碼的資料，看到的都是一些毫不具 | 不啓用 |

| | | |
|---|---|---|
| | 意義的亂碼，這種編碼的另一種理論基礎是，凡是經過 Public Key 編碼過的資料，都必須利用 Private Key 才能解得開。 | |

表格 4-1 POP3（s）設定

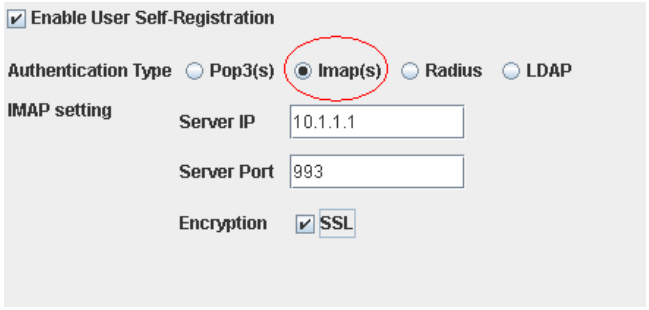
### 4.2.2 Imap（s）設定

**步驟 1 設定 Imap（s）驗證**

勾選 **Enable User Self-Registration（啓用驗證）**。選擇 Imap（s）爲驗證類型。輸入伺服器 IP 和伺服器埠。如果您的伺服器需要透過加密（埠號 995）連線驗證，請勾選SSL。然後上傳設定檔。

**注意：**Imap 服務透過埠 143 連線而 Imaps 服務透過埠 993 連線。

**IM Manager > Auth > Imaps（s）**




| 欄位 | 說明 | 範例 |
|---|---|---|
| Server IP | IMAP（s）伺服器的 IP 地址。 | 10.1.1.1 |
| Server Port | IMAP（s）伺服器資料進出的通訊埠。例如，IMAP 服務透過埠 143 連線而 IMAPs 服務透過埠 993 連線。 | 993 |
| Encryption | 所謂的 SSL 是利用大數值編碼的技術將資料編碼後再傳至遠端，全球資訊網在建置之後，必須向一個有公信力的單位登入，並取得一個 Private Key，而將另一個 Public Key 放在網路上；資料在網際網路傳輸時都是經過編碼的資料，即使有人在中間要擷取這些經過編碼的資料，看到的都是一些毫不具意義的亂碼，這種編碼的另一種理論基礎是，凡是經過 Public Key 編碼過的資料，都必須利用 Private Key 才能解的開。 | SSL |

表格 4-2 IMAP（s）設定

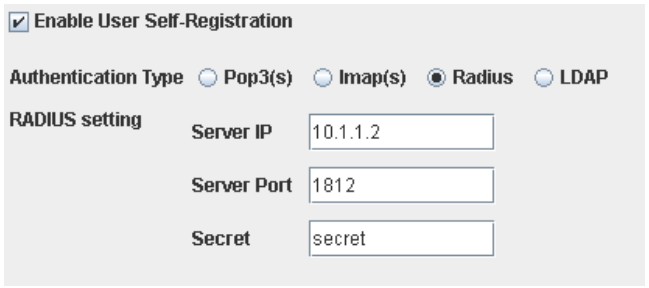
### 4.2.3 Radius 設定

**步驟 1 設定 Radius 驗證**

如果貴公司已經有安裝 Radius 伺服器，所有的員工資料都儲存在 Radius 伺服器中，您可以選擇 Radius 驗證類別。當使用者要自行註冊即時通訊帳號時，InstantScan 會連絡 Radius 伺服器提供通行驗證。

勾選 **Enable User Self-Registration（啓用驗證）**。選擇 Radius 爲驗證類型。輸入伺服器 IP 和伺服器埠。輸入與 Radius 伺服器溝通之Secret 碼。然後上傳設定檔。

**IM Manager > Auth > Radius**




| 欄位 | 說明 | 範例 |
|---|---|---|
| Server IP | Radius 伺服器 IP 地址。 | 10.1.1.2 |

| | | |
|---|---|---|
| Server Port | Radisu 伺服器資料進出的埠。 | 1812 |
| Secret | Secret 是 Radus 伺服器與用戶端驗證的加密金鑰。也就是通訊的各方彼此間共用一把加密金鑰，並且利用該金鑰的資訊來檢驗彼此的身份。 | secret |

表格 4-3 Radius 設定

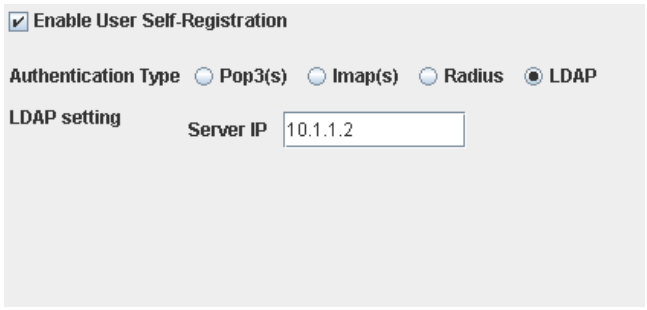
### 4.2.4 LDAP 設定

**步驟 1 設定 LDAP 驗證**

如果貴公司已經有安裝 LDAP 伺服器，所有的員工資料都儲存在 LDAP 伺服器中，您可以選擇 LDAP 使用者驗證類別。當使用者要自行註冊即時通訊帳號，InstantScan 會連絡 LDAP 伺服器提供使用者驗證，使用者只要輸入帳號與密碼，InstantScan 會將此組帳號密碼傳送給 LDAP 伺服器驗證，一旦通過驗證，即可註冊即時通訊帳號。

**勾選** Enable User Self-Registration（**啓用驗證**）。選擇 LDAP 爲驗證類型。輸入伺服器 IP，然後上傳設定檔。LDAP 相關設定，請參考以下章節。

**IM Manager > Auth > LDAP**




| 欄位 | 說明 | 範例 |
|---|---|---|
| 伺服器 IP | LDAP 伺服器 IP 地址 | 10.1.1.11 |

表格 4-4 LDAP 設定

# 第3部

# InstantScan 管理系統概述

# 第5章
# InstantScan 管理系統介紹

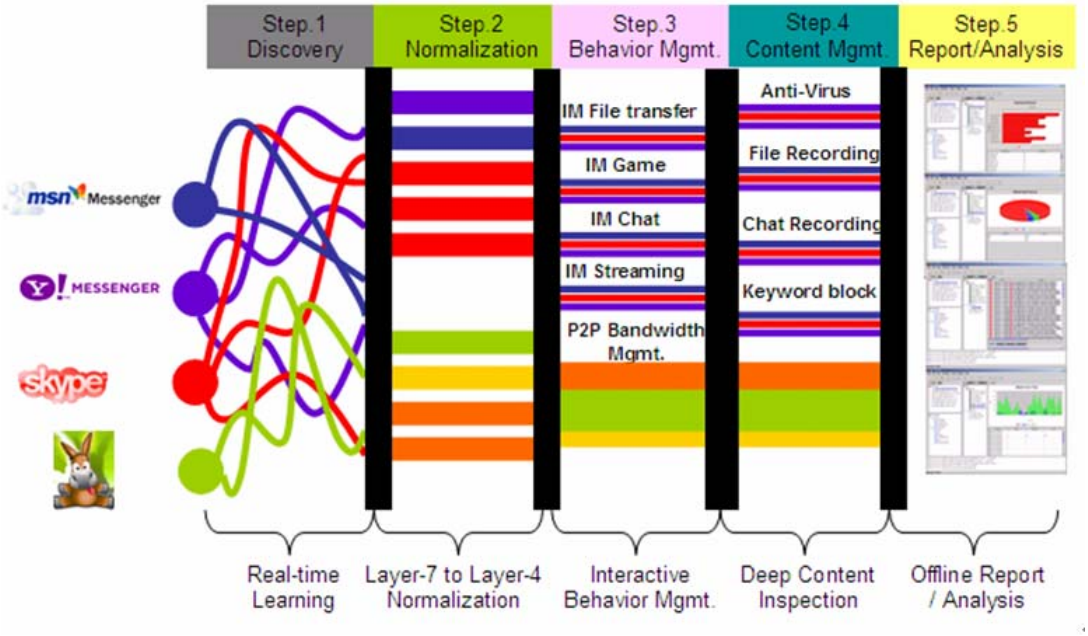
*本章節介紹如InstantScan 的設計原則與設定步驟。*

## 5.1 InstantScan 技術應用

InstantScan 管理系統爲一網頁應用介面，允許多個管理者同時管理一台或多台 InstantScan裝置。您可藉由任何電腦透過網頁流覽器來存取 InstantScan 管理伺服器。

**內容管理五步驟：**生產力/安全性最大化、威脅/總持有成本最小化

現今許多網際網路使用者已經安裝了即時通訊（IM）與點對點傳輸（P2P）應用軟體。這些軟體會自動隨機跳埠，或把自己僞裝在 HTTP 的地道裡，以規避管理者的檢查。爲了讓管理者克服這個問題，「內容管理五步驟」可用來最大化生產力/安全性，並最小化威脅性與總持有成本。

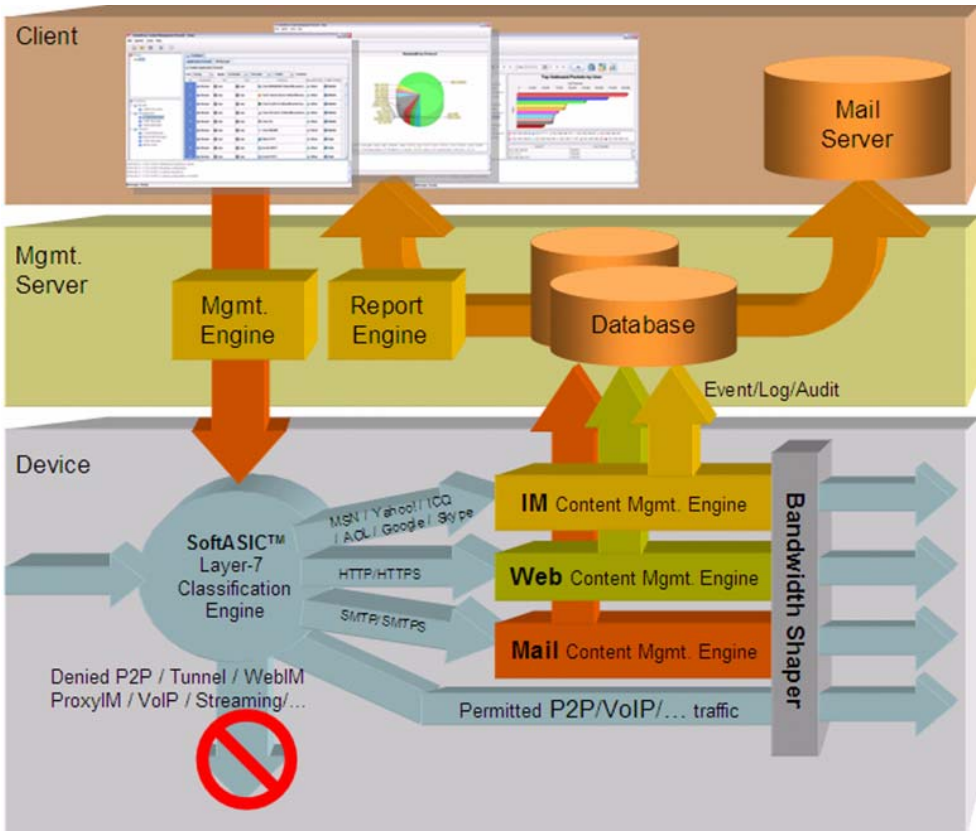



1. 隨插即用即時流量偵測/學習：爲了幫助管理者解決上述問題，InstantScan 提供了隨插即用流量偵測來當作第一步。只需要把網路線接起來，InstantScan 就回現場把網路流量展現在你面前。您可以看到有多少 MSN 是用 HTTP 地道來僞裝的，也可以看到有多少 IM 正在聊天。聊天的過程會被自動記錄，以方便管理者匯入到設定中。
2. 將第七層流量打回第四層：在流量偵測過後，若是列管的流量，您可以使用第七層防火牆來檔掉某些應用。在此圖中，InstantScan 會把在第七層亂竄的流量過濾，讓其乖乖地以第四層流量方式運行，說明您原有的第四層防火牆得以用埠號作最基本的控制。非但如此，InstantScan 可說明您阻擋非標準的 IM 連線。例如 MSN 會自動偵測防火牆設定，若 MSN 無法從標準的1860埠號連出去登入，則會開始用 HTTP 代理伺服器連線出去。更有甚者，任何人都可以手動設定他要連到哪一台 HTTP/SOCKS4/SOCKS5 代理伺服器（包括貴公司裡的 HTTP 代理伺服器）。最慘的是，員工還可以使用流覽器連到各種不同提供 MSN 服務的網頁，繼續跟外面的人聊天。這些 InstantScan 都可以幫助您解決。

3. 互動式行爲管理：設定個人化的政策。既然 InstantScan 可以認得應用程式的各種細部行爲，網管人員可以針對每個使用者給予不同的行爲許可權。使用者的資訊可以整合企業現有的使用者資料庫，例如 LDAP、Active Directory、POP3(S)、IMAP(S)、RADIUS。
4. 深度內容檢測：設定進階的內容過濾功能。在此圖中，InstantScan 可偵測/阻擋「壓縮檔裡的病毒」或「散佈在 MSN 窗口裡的 URL 或傳檔蠕蟲」。若要做到極端的安全性，所有的對話都可以被側錄，來預防內部資訊洩漏。若使用者違反了政策，說了些不該說的話，InstantScan 能夠直接在「IM視窗內」警告使用者公司的 IM 使用政策
5. 詳細報表分析：最後，報表分析可以幫網管人員找出問題。數十種的圖形報表，包括每天/每週/每月/每季/每年的頻寬報表、IM 使用行爲、以公司部門顯示聊天側錄、違反政策情況。報表可以客制化、搜尋，且得以用 PDF/HTML/Excel 的格式，在設定的時間週期內以附加檔寄出。

**三層式架構：**效能、可用性、功能最大化

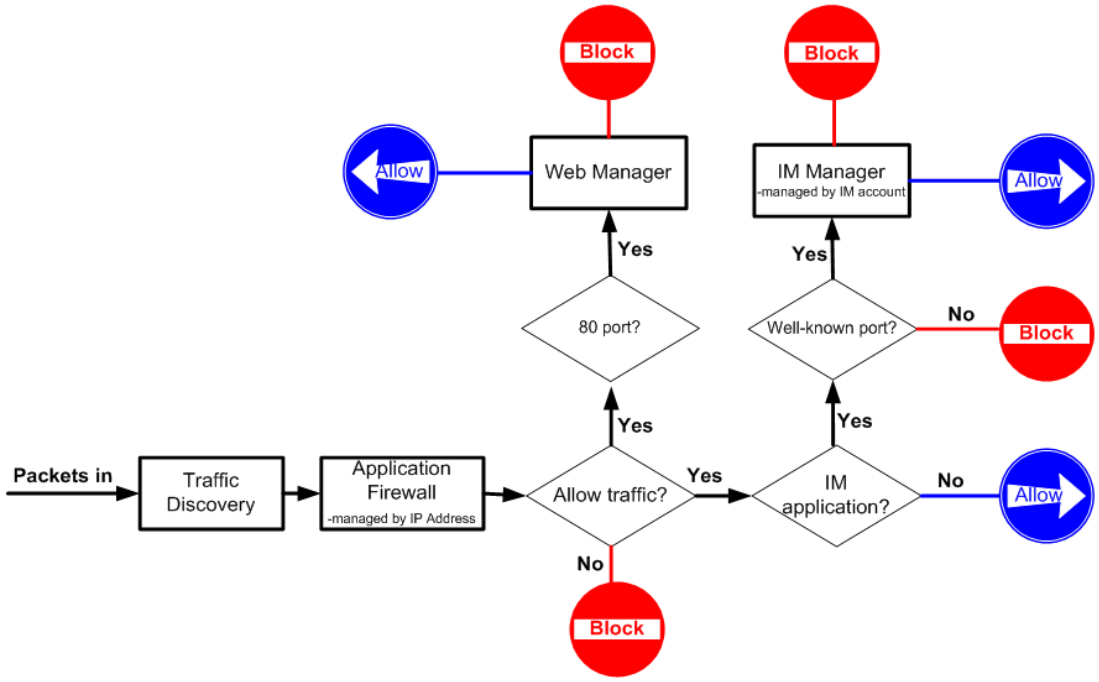
第七層網路設備通常要做「非常多的計算功夫」和「較好的分散架構」，以最大化效能、可用性，與功能性。InstantScan 採用了業界最先進的三層式架構來增加效能，讓各層各司其職，完成每一個目的。




1. **第七層設備：**第七層設備應該要專注的是「快速地」與「準確地」執行內容檢測。如此，第七層設備裝在網路進出口線上，才不會影響到網路的效能。
2. **管理伺服器：**管理伺服器要負責的是中央集中控管第七層設備，並接收來自於不同第七層設備的事件，整理於資料庫中更進一步製作報表分析。在管理伺服器上製作報表，不會影響第七層設備的效能。
3. **管理用戶端：**管理用戶端可用任何具備JAVA功能的流覽器連到管理伺服器。只要他連得到管理伺服器，他就可以連得到任何架設於管理伺服器之下的第七層設備。

## 5.2 內容管理流程

InstantScan 內容管理器可控管時下盛行的即時通訊軟體 （IM）、點對點 （P2P） 傳輸軟體、檔案傳輸軟體、與遠程式控制管軟體、VoIP 軟體與網頁內容管理等等。您可以藉由這些內容管理專案來做最適當的網路管理，保障公司的網路安全、杜絕一切藉由網際網路的便利而機密外泄的管道，更可加強員工的產能。不但可以不用全面封鎖即時通訊與點對點傳輸軟體的使用，更可控管這些軟體，借助即時通訊、點對點傳輸軟體的時效性與便利性而達到真正公司業務往來省時又省錢的目的。在接下來的章節中，我們將針對內容管理的細項逐一介紹。




圖表 5-1 內容管理器之管理流程

如圖表 5-1 所示，InstantScan 將進來的流量導給流量監控監看。而當您啓用應用層防火牆時，所有應用軟體不管是透過 TCP 通訊協定或是代理伺服器（例如 HTTP/SOCKS）連線，企圖欺騙管理人員，其流經 InstantScan 的封包在經過利基網路第七層辨識引擎辨認後，再依使用者對發送該封包的 IP（來源端）與其送往的物件（目的端 IP）所定義的政策規則決定是否讓其通行，只要進來的封包符合設定的條件，就套用該政策規則。

當您啓用即時通訊管理員時，MSN/Yahoo/AIM/ICQ 等即時通訊軟體將會被規範透過正規的埠連線出去。也就是說 MSN 必須透過埠 1863、Yahoo 5050、AIM/ICQ 5190。如果即時通訊軟體透過非正規埠連線，其連線就會被 InstantScan 攔阻。例如，在應用層防火牆允許 MSN 連線，且您亦開啓即時通訊管理員並允許 MSN 連線的條件下，MSN_A 透過埠 1863，可以正常連線；而 MSN_B 企圖透過埠 80 連線，就會被正規化的政策攔阻。

當網頁管理員也啓用時，所有透過埠 80 傳送的封包都會導給網頁管理員監看。管理人員可以依制定的政策做網頁內容過濾、URL 側錄、網頁掃毒等網頁內容管理。

## 5.3 InstantScan 網頁介面設計原則

InstantScan 管理系統包含下列五個視窗：

1. **工具列**：可設定 InstantScan 參數的工具，包含快速功能鍵。
2. **InstantScan 專案樹狀圖**：包含已選擇的項目與受此專案控管的所有裝置。
3. **功能樹狀圖**：所有 InstantScan 的功能樹狀圖。包含監看、管理與報表系統等大項。
4. **內容視窗**：各項功能參數的設定視窗。接下來的章節將依序引導您設定 InstantScan。

**5. 狀態列**：顯示所有系統操作資訊。您也可以點擊圖示 將此狀態列隱藏起來。

## 5.4 InstantScan 圖示說明

| 圖示 | | 功能 |
|---|---|---|
| 工具列 |  | 新增專案 |
| |  | 開啓專案 |
| |  | 顯示/隱藏 狀態列 |
| |  | 上傳設定檔 |
| 內容視窗 |  | 物件群組 |
| |  | 單一物件 |
| |  | 除了此選定物件群組外，全部套用該通訊協定的防火牆規則。 |
| |  | 除了此選定物件 （範圍/子網/主機） 外，全部套用該通訊協定的防火牆規則。 |
| |  | 日期選項，可依日期期間指定顯示選定的事件記錄或報表。 |
| |  | 進階搜尋功能。可依設定的條件搜尋事件記錄。 |
| |  | 重新整理事件的時間設定。 |
| |  | 報表匯出設定 |

表格 5-1 InstantScan 圖示說明

## 5.5 工具列說明

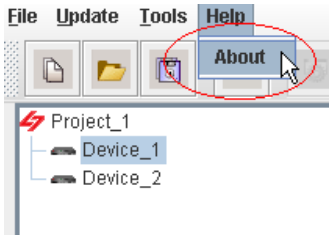
| 標籤 | 項目 | 說明 |
|---|---|---|
| File | Device/Group Manager | 建立新裝置或群組 |
| | New Project | 建立新專案 |
| | Open Project | 開啓已存在的項目 |
| | Close Project | 關閉使用中的專案 |
| | Delete Project | 刪除選取的項目 |
| | Exit | 離開使用者網頁設定介面 |
| Update | Upload Configuration | 上傳設定檔到裝置上 |
| | Register | 進入產品註冊網頁線上註冊您所購買的裝置。*您要更新特徵碼、應用程式列爲、病毒/url 資料庫或升級韌體前一定要先完成註冊手續。 |
| | Update IM engine | 從更新中心更新特 IM 引擎 |
| | Update pattern | 從更新中心更新應用程式列爲 |
| | Update AV database | 從更新中心更新病毒資料庫 |
| | Update URL database | 從更新中心更新 URL 資料庫 |
| | License | 如果您有購買 Web 模組，您必須在此填寫您的授權碼，並經過驗證後，才可使用。 |
| | Option | 更新中心設定 |
| | Support list | InstantScan 所支援的應用程式清單 |
| Tools | Account Manager | 依使用層級，設定使用者帳號與許可權 |
| | Change Password | 更改登入密碼 |
| | Language Setting | 設定語言模組，可選擇英文、繁體中文與簡體中文三種語言。 |
| | SNMP Control | 遠端監控設備的系統狀態以及網路 |
| | Config Backup | 備份現行的設定檔到本地端磁片 |
| | Config Restore | 還原已儲存的設定檔到裝置上 |
| Help | About | 顯示 InstantScan 版本訊息 |

## 5.6 管理伺服器版本

**步驟 1 查閱管理伺服器版本**

InstantScan 韌體必須搭配相符的管理伺服器版本。請點選 About 查看管理伺服器版本。

**Help > About**




**步驟 2 顯示管理伺服器的版本**

如右圖所示，您可以看到管理伺服器的版本與出版的日期。

# 第6章
# 階層式管理與稽核

*本章介紹 InstantScan 階層式管理與稽核的設計與應用。*

## 6.1 需求

面對層出不窮的資安事件，企業爲解決資安問題不能單由技術面著手，應藉由建立完整管理系統以有效解決資安問題。根據政府資通會報規定：政府部會中 A、B 級單位需在民國 97 年以前通過 BS7799 認證。由此可見，BS7799 內容的適用性與重要性。此外，由於 BS7799 巨細彌遺的說明企業控管資訊安全所應採取的步驟及應制訂哪些應變措施。由此可見，BS7799 是一套完整的計畫，能有效建構資訊安全防護機制。IT 專業人員可將這套資訊安全標準規則當作藍圖，依其導引制定企業的安全政策與程式。InstantScan 內容管理器，爲符合 BS7799 的規範，說明企業執行 BS7799 計畫，特地設計階層式管理與稽核系統。

## 6.2 目的

內容管理因牽涉到個人隱私與公司機密，在處理上需要特別小心謹慎。InstantScan 階層式管理與稽核，利用許可權控管資安內容，將風險降到最低與資安防護效果最大化，將管理與稽核人員分開，各司其職且相互合作。

## 6.3 方法

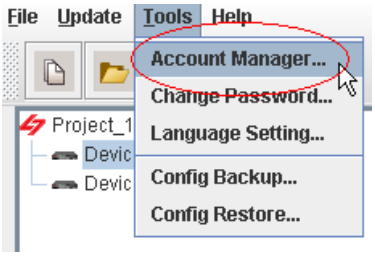
InstantScan目前規劃三種許可權群組，分別爲：

1. **Admin**：管理人員，擁有最高許可權，可制定管理政策與流覽側錄訊息。
2. **MIS**：網管人員，可制定管理政策但無法流覽側錄訊息。
3. **Audit**：稽核人員，可流覽側錄訊息，但無法制定管理政策。

## 6.4 步驟

在您第一次登入 InstantScan 內容管理器時，您可以在帳號管理員編輯可存取管理伺服器的帳號與密碼。借由設定的許可權階層式控管 InstantScan，讓貴公司確保員工個人隱私與公司機密，更能符合公司稽核的需求。

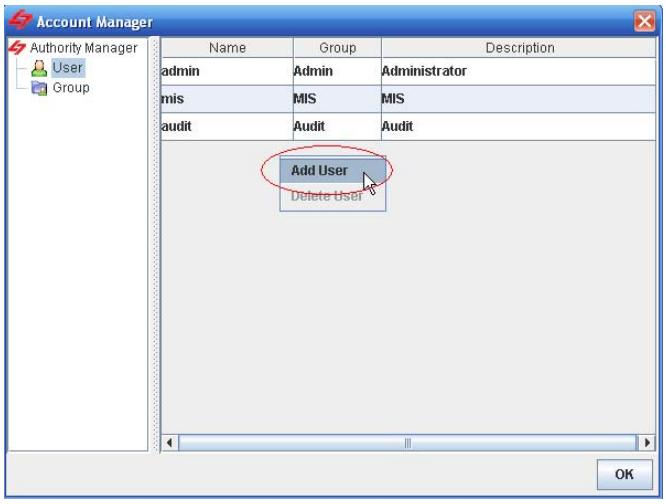
### 6.4.1 新增使用者帳號

| | |
|---|---|
| **步驟 1 管理帳號設定**<br>選擇 **Account Manager（帳號管理員）**選項。 | **Tool > Account Manager**<br>  |

**步驟 2 新增使用者帳號**

InstantScan 可同時多人連線控管，您可在 Account Manager（帳號管理員）建立可存取管理伺服器的帳號，包含使用者與其所歸屬的群組。

**Tool > Account Manager > User > Add User**



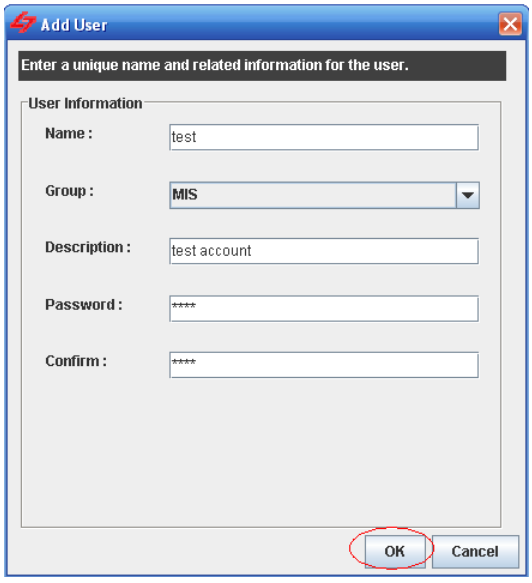

| 欄位 | 說明 | 範例 |
|---|---|---|
| Name（名稱） | 可存取管理伺服器的使用者帳號名稱。 | test |
| Group（群組） | 可存取管理伺服器的使用者群組，可分成三種授權群組：<br>1. admin（管理人員）：可設定 InstantScan、流覽報表與查看側錄記錄等所有權限。<br>2. mis（網管人員）：只可設定 InstantScan，但無法流覽報表與查看側錄記錄。<br>3. audit（稽核人員）：只可查看側錄記錄，但無法設定 InstantScan。<br>**注意：群組不可增刪修改。** | mis |
| Description（描述） | 針對帳號的詳細說明。 | test account |

表格 6-1 帳號管理員

**步驟 3 編輯帳號**

請輸入您要新增的帳號名稱、對此帳號的描述、與其密碼，並選擇所屬群組。點擊 **OK** 完成設定。

**Tool > Account Manager > User > Add User**



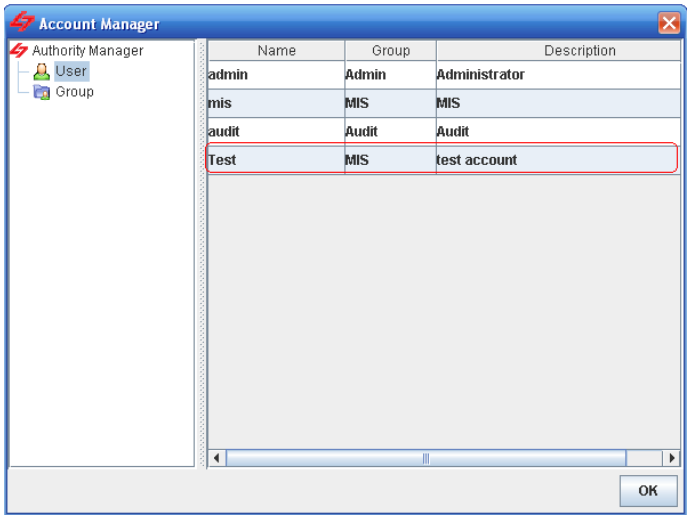
**步驟 4 帳號建立成功訊息**

當您建立帳號成功，將有如右圖的視窗通知您新增成功。


**步驟 5 顯示已增加的帳號**

當您成功建立帳號，您可以在 **Account Manager**（帳號管理員）的視窗上看到這筆資料。

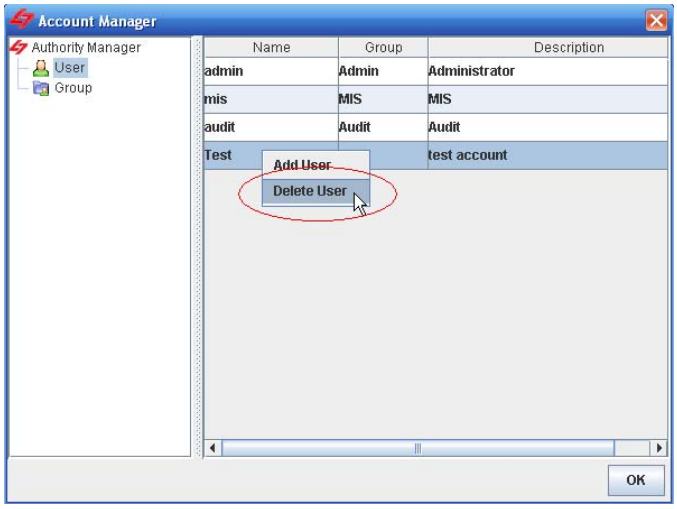
**Tool > Account Manager > User**



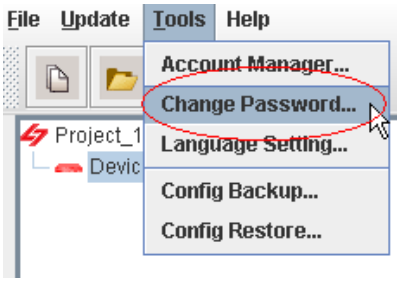
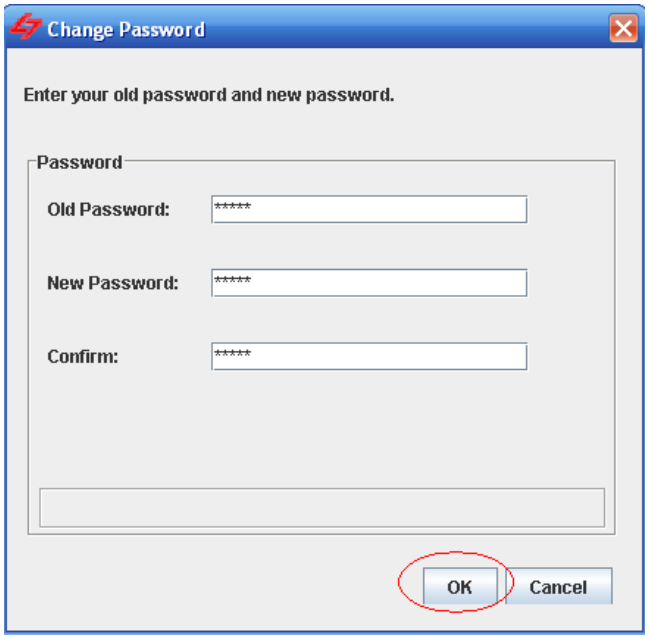

**步驟 6 刪除帳號**

欲刪除某筆帳號，只要點選此筆資料，然後按右鍵，選擇 **Delete User**（刪除使用者）即可。

**Tool > Account Manager > User > Delete User**



### 6.4.2 修改使用者登入網頁介面的密碼

| | |
|---|---|
| **步驟 1 點選更改密碼**<br>選擇 **Change Password**（**更改密碼**）選項。 | **Tool > Change Password**<br>  |
| **步驟 2 輸入新的密碼**<br>輸入 **Old Password**（**舊的密碼**）與 **New Password**（**新的密碼**），然後在 **Confirm**（**確認**）欄位內再次輸入新的密碼。點擊 **OK** 完成設定。 | **Tool > Change Password**<br>  |

# 第4部

# 網路監看

# 第7章
# 網路監看

*本章節介紹網路監看的應用。*

## 7.1 監看公司網路

InstantScan Traffic Discovery （流量監控）功能，讓所有流經 InstantScan 裝置的流量一覽無遺地呈現在管理者的眼前。管理者可以藉由檢視網路流量來決定針對特定流量管理的方式，用以避免頻寬遭到員工濫用。MSN/Yahoo/ICQ/AIM 等即時通訊軟體，當其企圖透過非正規的埠連線，系統將會以紅字標示，將此連線顯示在 Traffic Discovery 上。透過 Traffic Discovery，網管人員可即時看到整過網路的使用狀況，進而做最適當的頻寬控管。

**步驟 1 監看網路狀態**

在Traffic Discovery上點兩下，您可一目了然目前網路的連線狀況。以紅字標示的連線爲經由非正規埠之連線。請注意，Traffic Discovery 爲一樹狀結構，第一層爲通訊協定、第二層爲正在使用此通訊協定的 IP 位址，第三層爲該 IP 位址使用此通訊協定的連線狀況。

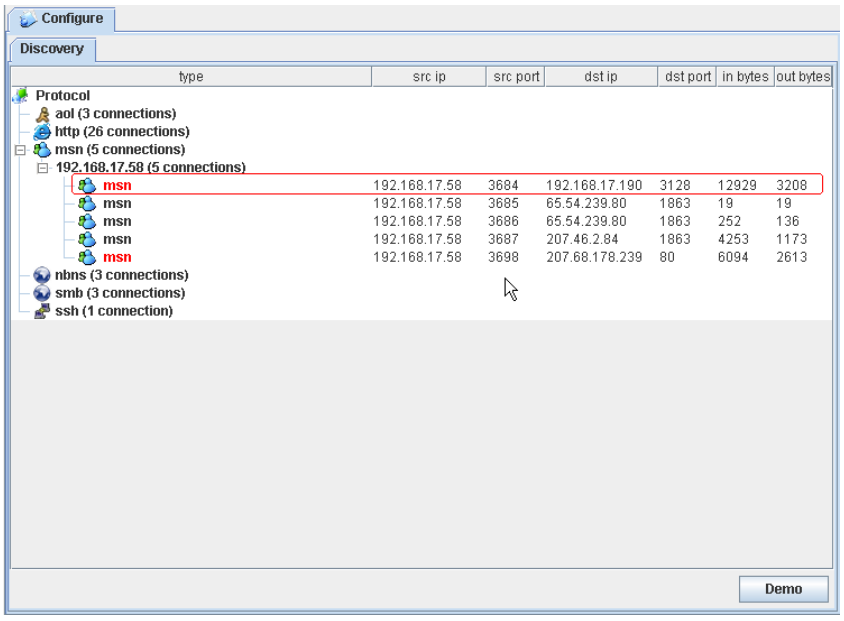
**注意**，所謂正規埠爲：

MSN：1863

Yahoo：5050

AIM/ICQ：5190

**Function > Monitor > Traffic Discovery > Dicovery**




| 欄位 | 說明 | 範例 |
|---|---|---|
| Type | 通訊協定的類別。當某通訊協定以紅字標記時，代表此連線透過非正規埠連線。 | msn |
| Src IP | 流經InstantScan的封包之來源端 IP 地址。 | 192.168.17.58 |
| Src port | 流經InstantScan的封包之來源端埠。 | 3684 |
| Dest IP | 流經InstantScan的封包之目的端 IP 位址。 | 192.168.17.190 |
| Dest port | 流經InstantScan的封包之目的端埠。 | 3128 |
| In bites | 選定連線的對內流量大小。 | 12929 |
| out bites | 選定連線的對外流量大小。 | 3028 |

表格 7-1 流量監控欄位解釋

# 第5部

# 物件管理員

# 第8章
# 物件管理員 – IP 與 Schedule

*本章介紹 IP 與排程的設定與使用方式。*

## 8.1 需求

1. ABC 公司希望管理公司內部的所有 IP 的網路使用權限。但是，CEO 與 CTO 有完整的許可權存取網際網路的資源。
2. ABC 公司的上班時間是星期一早上 8:30 – 12:00，下午 13:00 – 17:30。中午 12:00 – 13:00 爲午休時間。依公司政策，某些即時通訊或點對點傳輸軟體在上班時間不准使用。
3. 性質相同的物件最好能夠將其群組一起以方便政策規則的設定。

## 8.2 方法

1. 點選 InstantScan 物件管理員之位址，設定 CEO 的 IP 位址爲 192.168.168.2，CTO 的 IP 位址爲 192.168.168.10，並將此兩個都是管理階層的位址物件群組在一起。
2. 在物件管理員之排程設定上班時間，並將不連續的上班時間群組成一個排程。

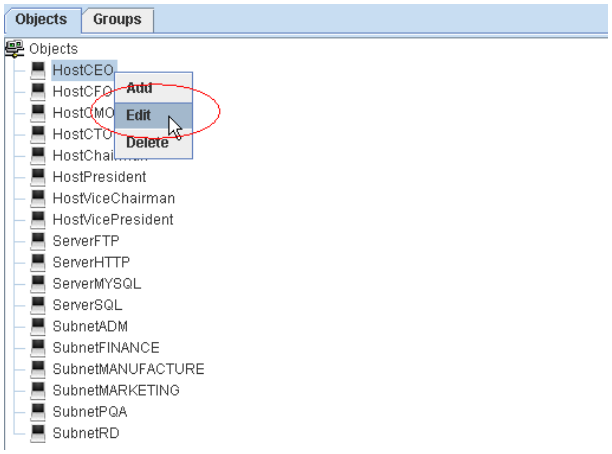
## 8.3 步驟

### 8.3.1 地址設定

**步驟 1 新增物件位址**

在 **HostCEO** 上按右鍵，然後選擇 **Edit**。爲了您制定規則的便利性，InstantScan已預設一些常用的位址物件供您選擇使用，您可以直接修改默認的 IP 位址，或將預設物件刪除，然後自行新增物件。

**Function > Management > Object Manager > Address > Objects**



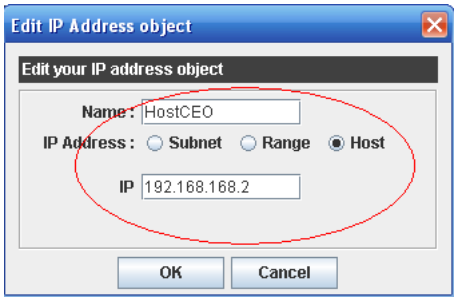

**步驟 2 編輯 HostCEO**

將 HostCEO 默認的 IP 地址改成 192.168.168.2。您亦可根據貴公司的網路架構，變更此物件的名稱與 IP 位址。

IP 位址可以是 **1）Subnet（子網）**; **2）Range（範圍）**; 或 **3）Host （主機）**。

對象HostCEO設定亦同。

**Function > Management > Object Manager > Address > Objects**



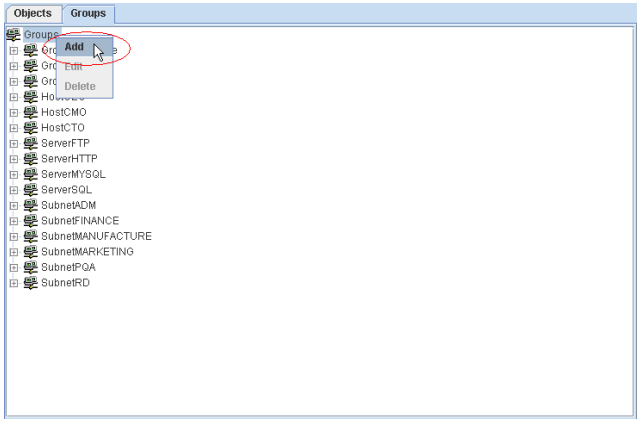

| IP Address | | 說明 | 範圍 / 格式 | 範例 |
|---|---|---|---|---|
| Subnet | IP | 子網 IP 地址 | IPv4 格式 | 192.168.168.0 |
| | Mask（0-32） | 子網路遮罩 | 子網路遮罩格式 | 24 |
| Range | Start IP | 此物件範圍的起始 IP 位址。 | IPv4 格式 | 192.168.168.1 |
| | End IP | 此物件範圍的結束 IP 位址。 | IPv4 格式 | 192.168.168.10 |
| Host | IP | 單一主機 IP 位址。 | IPv4 格式 | 192.168.168.2 |

表格 8-1 定義位址物件

**步驟 3 新增物件群組**

在螢幕上按右鍵，然後點選 **Add**。

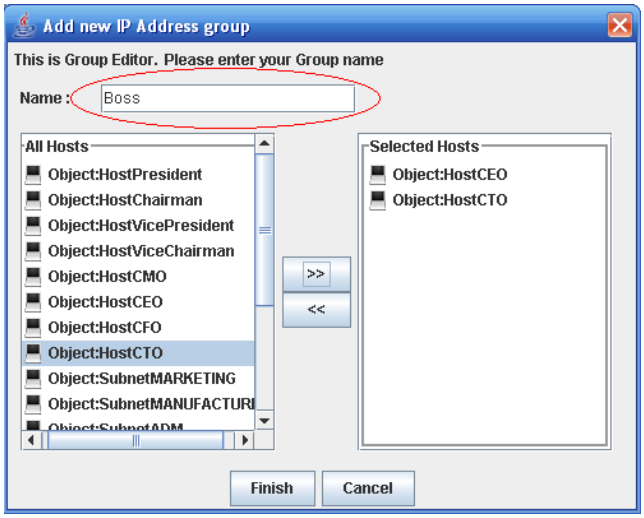
**Function > Management > Object Manager > Address > Groups**




**步驟 4 編輯群組**

在名稱欄位內輸入 **Boss**，在 All Hosts 欄位內選擇 **Object:HostCEO** 與 **Object:HostCTO**，然後點擊 **>>** （右向箭頭），將此兩個位址物件加到 **Selected Hosts** 欄位內。欲移除群組中某個位址物件，請在 Selected Hosts 欄位內選擇要移除的物件，然後點擊 **<<**（左向箭頭）即可。

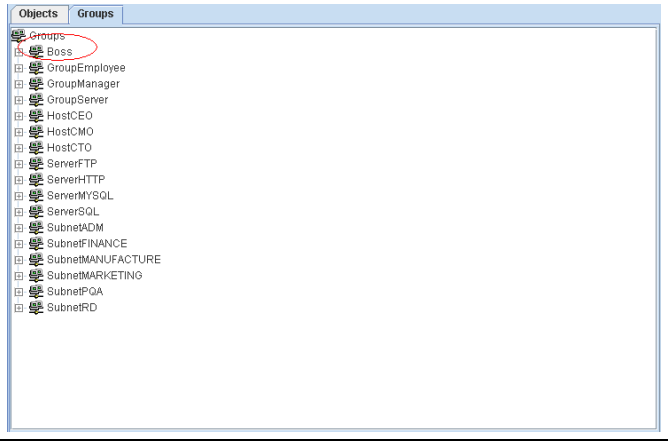
**Function > Management > Object Manager > Address > Groups**




**步驟 5 顯示已建立的群組**

當您點擊 **Finish** 按鈕後，已建立的群組將顯示在螢幕上。如右圖所示。

**Function > Management > Object Manager > Address > Groups**



**步驟 6 上傳設定檔到裝置中**

點選 **Upload Configuration** 選項，或者點擊  圖示，將現行的設定檔上傳到裝置上。

⚠ 如果某個物件已經被某個群組或某條政策規則所使用，在刪除此物件前，您必須先刪除包含此物件的位址群組或是政策規則，否則您無法刪除此物件。

## 8.3.2 排程設定

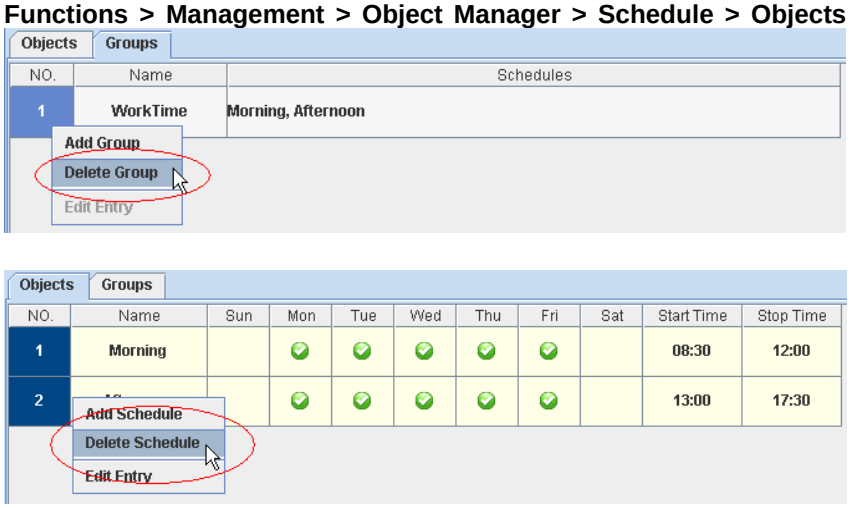
**步驟 1 刪除預設排程**

InstantScan已提供您兩條預設的排程，如果預設的排程不符您的需求，您可以修改此排程，或者將其直接刪除。

在接下來的範例中，我們將刪除預設的排程規則，然後透過新增排程介紹您排程的設定。
請注意，在刪除排程前請先確認排程群組或其他政策規則是否已經含有此排程了。

右邊的例子爲排程物件已經被排程群組所使用了，所以您必須先刪除排程群組，然後才可刪除排程物件。

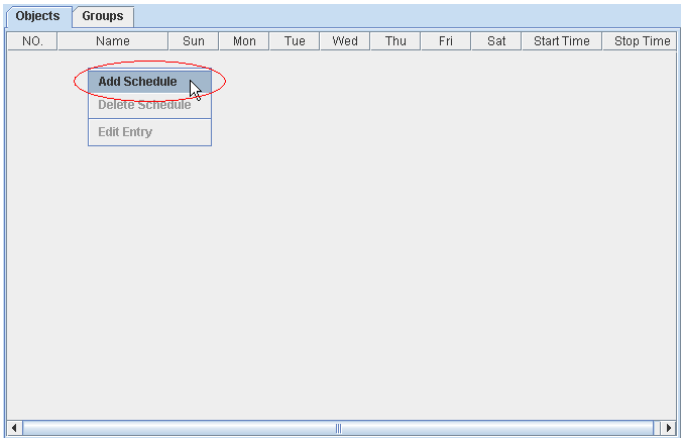
**Functions > Management > Object Manager > Schedule > Objects**




**步驟 2 在排程物件螢幕上按右鍵**

在螢幕上按右鍵，然後點擊 **Add Schedule** 選項。

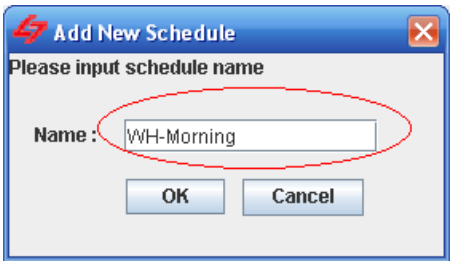
**Functions > Management > Object Manager > Schedule > Objects**



**步驟 3 新增排程**

輸入排程名稱。點擊 **OK** 關閉窗口。

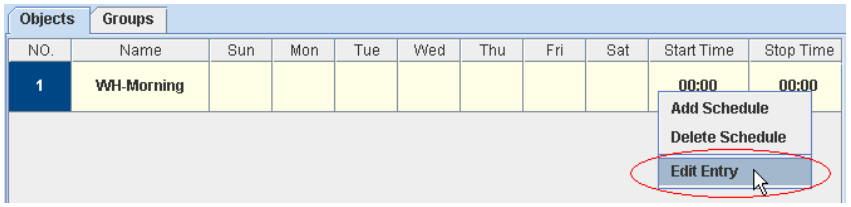
**Functions > Management > Object Manager > Schedule > Objects**




**步驟 4 編輯時間**

在 WH-Morning 規則的 **Start Time** 欄位上按右鍵，然後點選 **Edit Entry** 選項。

**Functions > Management > Object Manager > Schedule > Objects**

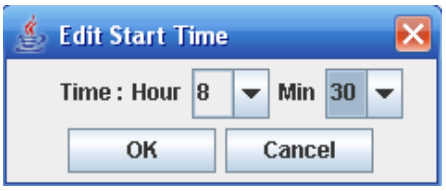



**步驟 5 拉選起始時間**

拉選 **Start Time** 的時與分，然後點擊 **OK** 關閉視窗。

Stop Time 的設定相同，請參照起始時間的設定。

**Functions > Management > Object Manager > Schedule > Objects**

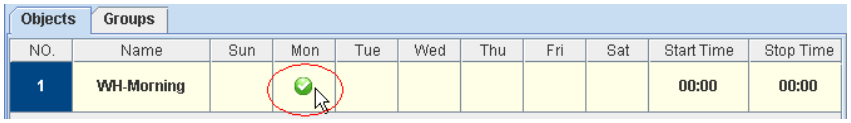



**步驟 6 日期管理**

ABC公司的上班時間爲星期一到星期五，所以您必須將滑鼠移動到 **Mon** 欄位上點一下，即有一圖示 顯示在表格內。接下來設定 Tue ~ Fri。

其他排程的設定皆相同。

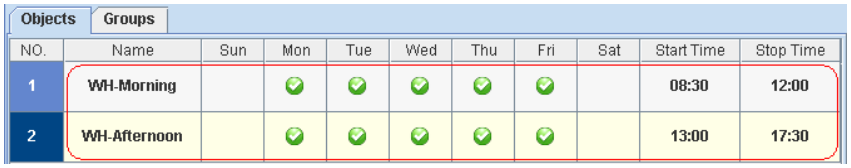
**Functions > Management > Object Manager > Schedule > Objects**

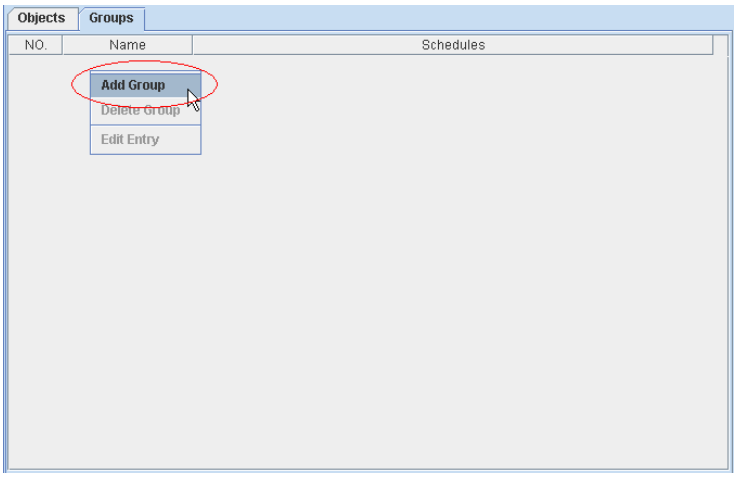
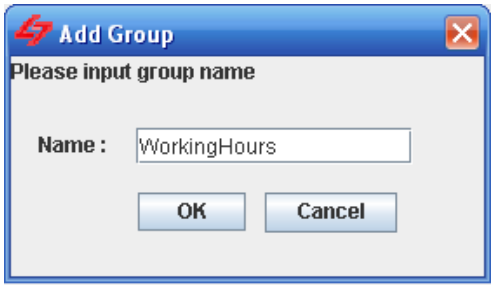
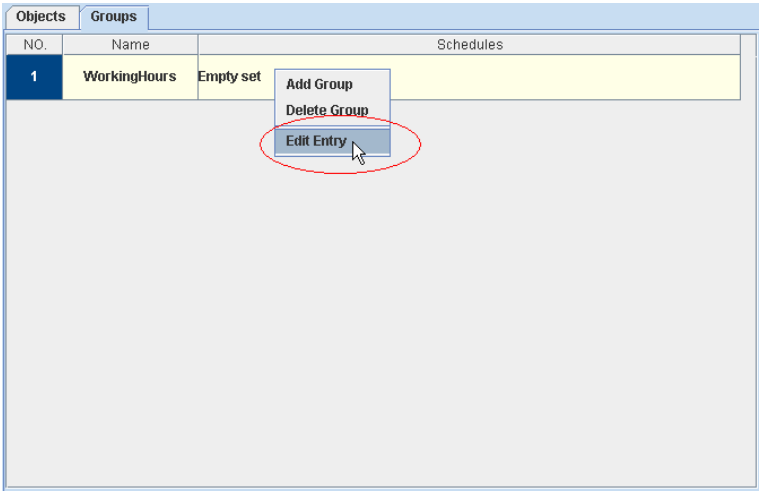



**步驟 7 流覽排程設定結果**

現在，我們已經設定好了兩條排程。您可以開始將這兩條排程群組一起了。

**Functions > Management > Object Manager > Schedule > Objects**

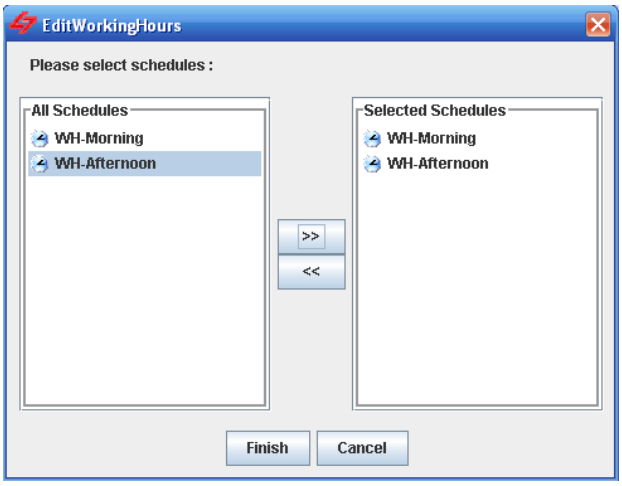


| | |
|---|---|
| **步驟 8 新增群組**<br>因爲 ABC 公司的上班時間爲 8:30~12:00 與 13:00~17:30，所以您必須將此兩個不連續的時間群組在一起，以方便管理規則的建立。在螢幕上按右鍵，然後選擇 **Add Group** 選項。 | **Functions > Management > Object Manager > Schedule > Groups**<br>  |
| **步驟 9 輸入組名**<br>輸入組名，然後點擊 **OK** 關閉視窗。 | **Functions > Management > Object Manager > Schedule > Groups**<br>  |
| **步驟 10 編輯群組**<br>在 WorkingHours 規則的 Schedule 欄位上按右鍵，然後選擇 **Edit Entry** 選項。 | **Functions > Management > Object Manager > Schedule > Groups**<br>  |

**步驟 11 編輯群組**

在 All Schedules 欄位內選擇您要加入此群組的排程，然後點擊 **>>** （右向箭頭），將選定的排程加入 Selected Schedules 欄位內。如果您要移除某個在此群組中的排程，請在 Selected Schedules 欄位中點選該排程，然後點擊 **<<** （左向箭頭）即可移除。點擊 **Finish** 結束設定。

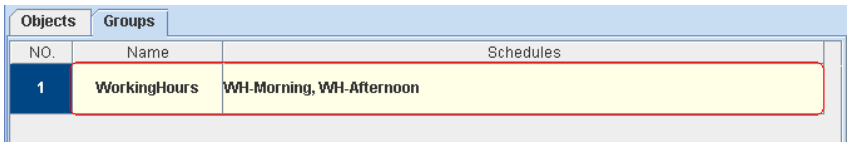
**Functions > Management > Object Manager > Schedule > Groups**




**步驟 12 檢視已設定的排程群組**

在您完成上列設定後，畫面將回到排程群組的首頁，您可以在此檢視您的設定。

**Functions > Management > Object Manager > Schedule > Groups**




**步驟 13 上傳設定檔到裝置上**

點選 **Upload Configuration** 選項，或者點擊圖示  上傳設定檔到裝置中。

⚠ 如果某個物件群組已經被某條政策規則所使用，在刪除此群組前，您必須先刪除包含此群組的政策規則，否則您無法刪除此群組。

# 第6部

# 流量管理員、應用層防火牆

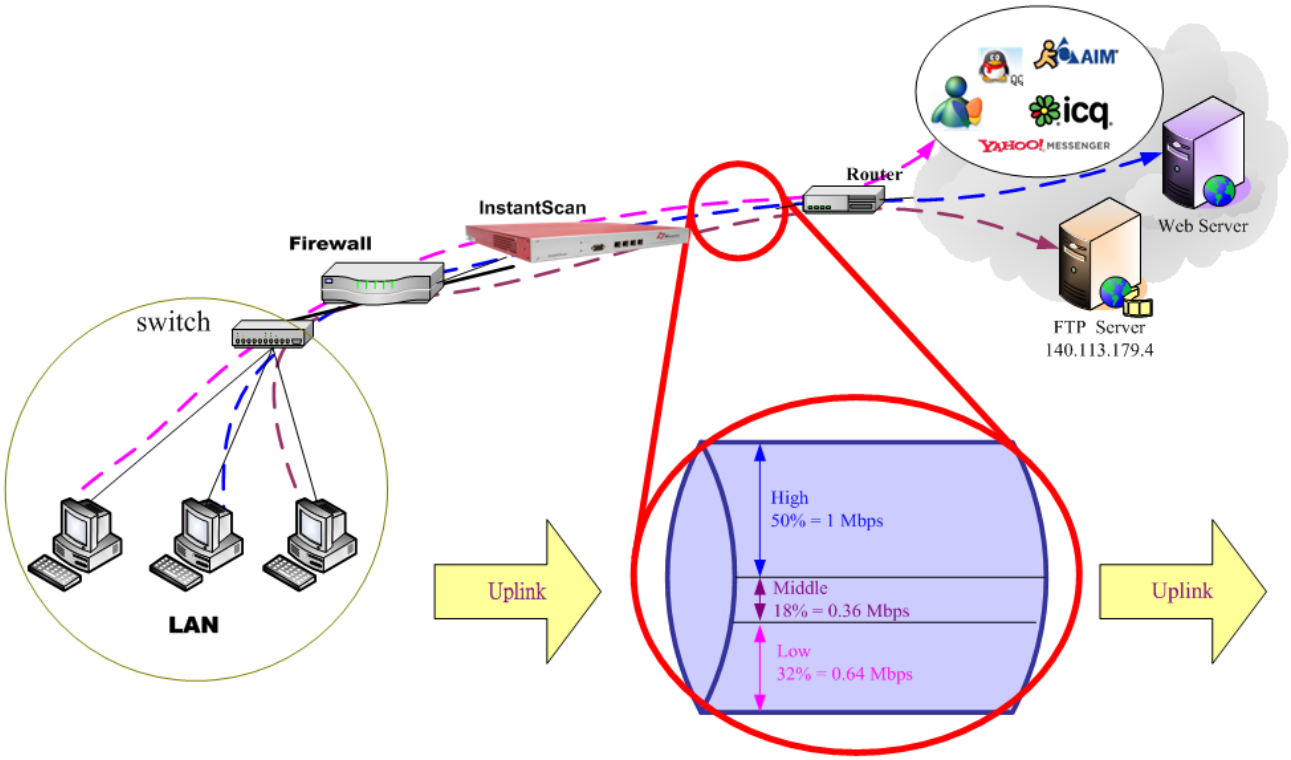
# 第9章
# 流量管理員

*本章介紹 Traffic Manager 與其使用方式。*

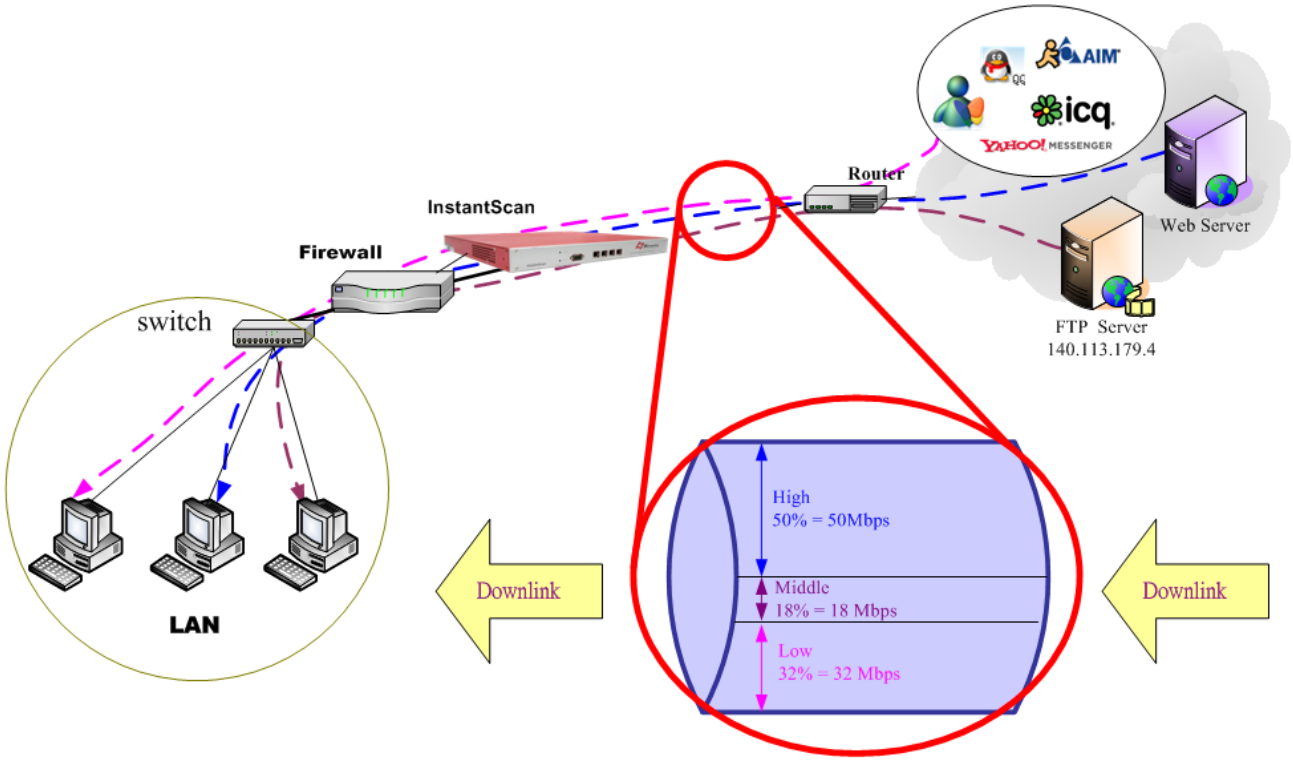
由於網際網路的盛行，員工上網隨時隨地都可以上傳或下載資料/檔案，濫用頻寬的結果常導致重要訊息/檔案無法即時傳送/接收，造成公司莫大的損失。有鑒於濫用頻寬的事件頻仍，InstantScan 流量管理員設計用來管理時下盛行的應用軟體之頻寬。借由滑鼠拖拉的動作即可有效的控管頻寬，省時省力又大大提升網路頻寬的應用效率。

## 9.1 需求

爲了讓網路頻寬能夠做最適當的安排，管理者希望將 FTP 服務分類成**中 （Middle）** 類別，並且限制**中**類別只可占對外或對內之總頻寬的 18%。詳見下列圖表。




圖表 9-1 對外頻寬管理




圖表 9-2 對內頻寬管理

## 9.2 方法

InstantScan 分別將對外與對內流量區分成三個類別，如下表所示。對外流量的總頻寬爲 2Mbps，而對內流量的總頻寬爲 100 Mbps。

| 頻寬流向 | 總頻寬 | 類別 | 頻寬分配 |
|---|---|---|---|
| 對外流量 | 2 Mbps | 高 （High） | 50% = 1 Mbps |
| | | 中 （Middle） | 18% = 0.36 Mbps |
| | | 低 （Low） | 32% = 0.64 Mbps |
| 對內流量 | 100 Mbps | 高 （High） | 50% = 50 Mbps |
| | | 中 （Middle） | 18% = 18 Mbps |
| | | 低 （Low） | 32% = 32 Mbps |

依上表所示，如果某個應用軟體被歸類爲低類別，其最大對外頻寬限制爲 0.64 Mbps，其對內頻寬限制爲 32 Mbps。例如，MSN/Yahoo/ICQ/AOL/GoogleTalk 等即時通訊軟體皆被歸類爲低類別，那麼 MSN + Yahoo + ICQ + AOL + GoogleTlak + Webim = 32 % 總對外或對內頻寬，也就是說其對外頻寬爲 2 * 32% = 0.64 Mbps，而對內頻寬爲 100 * 32% = 32 Mbps。

## 9.3 步驟

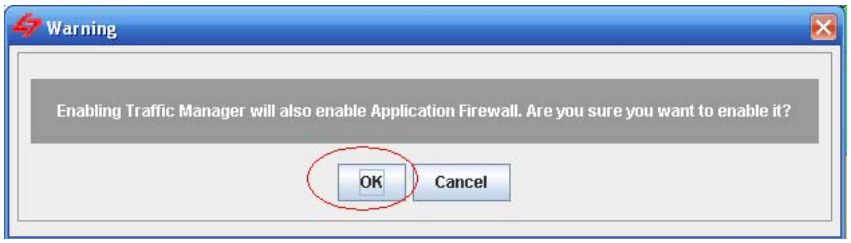
**步驟 14 啓用流量管理**

勾選 **Enable Traffic Management**。

**Functions > Management > Traffic Manager > Traffic Manager**


**步驟 15 警告訊息**

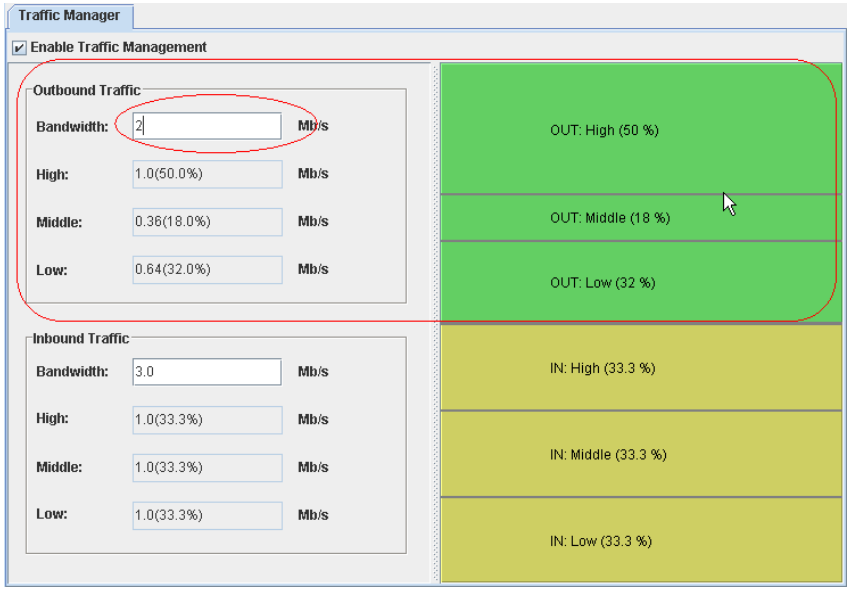
當您啓用流量管理員時，系統同時間亦會將應用層防火牆啓用。




**步驟 16 訂定對外流量**

在 **Outbound Traffic** 欄位內輸入 **2** 。利用滑鼠拖拉右邊的頻寬控制線，讓 High 類別占 50% 總頻寬，Middle 類別占 18% 總頻寬，而 Low 類別占 32% 總頻寬。當您設定好頻寬大小後，頻寬的分配狀況即會顯示在左邊頻寬類別欄位上。

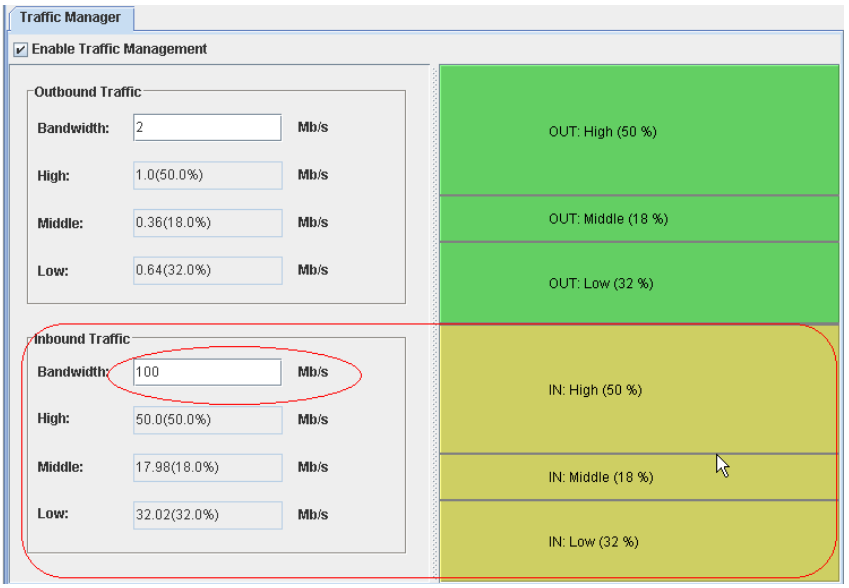
**Functions > Management > Traffic Manager > Traffic Manager**



**步驟 17 訂定對內流量**

同 Outbound Traffic 設定。在 Inbound Traffic 欄位內輸入**100**。利用滑鼠拖拉右邊的頻寬控制線，讓 High 類別占 50% 總頻寬，Middle 類別占 18% 總頻寬，而 Low 類別占 32% 總頻寬。當您設定好頻寬大小後，頻寬的分配狀況即會顯示在左邊頻寬類別欄位上。

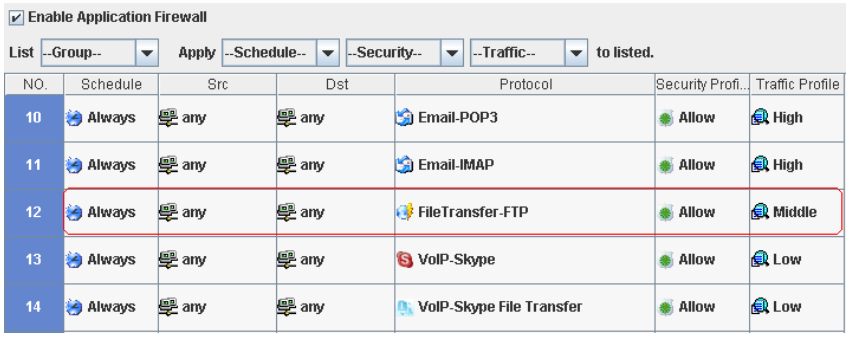
**Functions > Management > Traffic Manager > Traffic Manager**




**步驟 18 啓用應用層防火牆**

請檢查啓用應用層防火牆是否已經勾選。如圖表 9-1 與圖表 9-2 所示，將 FTP 服務的頻寬類別設定爲 Middle，並允許其流量通行。

**Functions > Management > Application Firewall**




**步驟 19 上傳設定檔**

**點選** Upload Configuration **選項，或點擊圖示** **將現行的設定檔上傳到 InstantScan 裝置上。**

# 第10章
# 應用層防火牆

*本章節介紹應用層防火牆與其設定。*

## 10.1 應用防火牆介紹

根據 2005 年 5 月 Gartner 提出的「Application Delivery and Web Application Firewall Are Ready to Converge」報告中指出，現今所有的網路攻擊事件中，約有 75%的攻擊事件是瞄準應用層，我們可以發現網路攻擊已經不僅是單純的掃瞄網段或主機，而是以企業必須開啓的埠爲發動攻擊開端，爲了確保網路安全，「應用層防火牆（Application Firewall）」是最佳的防禦方式。

應用層防火牆只是一個防禦環節，最重要的還是相對應的防禦政策。所以應用層防火牆必須根據其所需保護的應用程式定義不同的防禦政策。以目前應用程式網頁化的趨勢而言，小至網頁郵件、大至整個企業的 ERP 系統，都可以透過流覽器使用，我們可以想見網頁伺服器攻擊的比例將會越來越高，而防護難度也相對提升。InstantScan 的應用層防火牆系將所有通過該裝置的應用軟體加以辨識控管，讓企業阻絕一些不必要的應用，且透過頻寬控管，讓企業內部的網路可發揮其最大的功效。

## 10.2 需求

1. CEO 與 CTO 擁有完整的許可權可以使用網際網路資源。
2. 除了 MSN 以外，上班時間不允許使用其他即時通訊軟體。
3. 除了 Skype 以外，上班時間不允許使用其他點對點傳輸軟體。
4. 上班時間，R&D 部門不允許使用 Skype 傳檔。

## 10.3 方法

1. 允許所有來自 CEO 與 CTO 的網路流量。
2. 除了 CEO 與 CTO 外，員工在上班時間內只允許使用 MSN，其餘即時通訊軟體一律攔阻。
3. 除了 CEO 與 CTO 外，員工在上班時間內只允許使用 Skype 傳送簡訊與檔案，其餘點對點傳輸軟體與 VoIP 一律攔阻。
4. 上班時間不允許 R&D 部門的員工透過 Skype 傳檔。

## 10.4 步驟

1. 啓用應用層防火牆、設定上班時間排程、允許所有來自 Boss 群組的網路流量、允許 MSN 並攔阻其餘即時通訊軟體的使用。
2. 允許 Skype 並攔阻其餘點對點傳輸軟體的使用。
3. 上班時間，攔阻 R&D 部門的 Skype 檔案傳輸。

**注意：**

1. 如果您選擇讓某個應用軟體通過 InstantScan，不管其來源端/目的端的 IP 位址爲何，所有屬於該應用軟體的流量皆可通過 InstantScan。

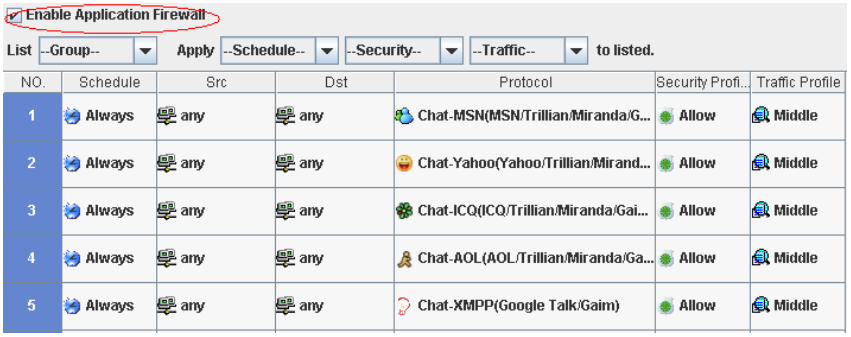
2. 如果 InstantScan 擺放在貴公司防火牆外，且透過防火牆轉址，因 InstantScan 本身設計上的考慮，您無法透過特定的 IP 控管任何應用軟體。且 Traffic Discovery 上所看到的來源端 IP 都是防火牆的 WAN 端 IP，無法顯示其真實的 IP。

### 10.4.1 設定即時通訊軟體規則

**步驟 1 啓用應用層防火牆**

勾選 **Enable Application Firewall**。

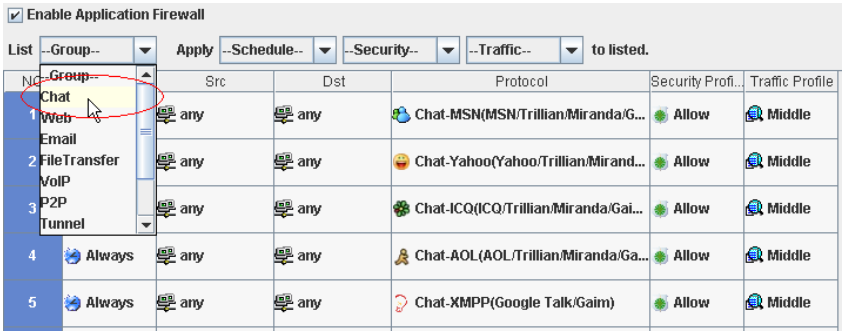
**Function > Management > Application Firewall**




**步驟 2 列舉 Chat 群組**

在搜尋工具列上選擇 **List Chat**，列舉所有屬於 Chat 群組的規則。

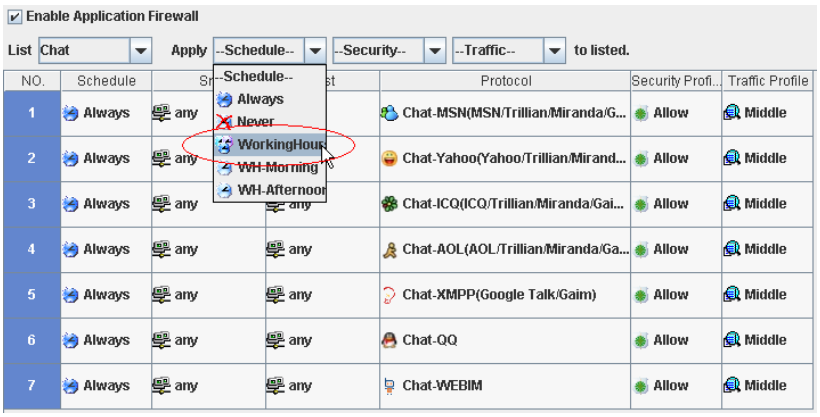
**Function > Management > Application Firewall**




**步驟 3 選擇排程**

在工具列上選擇Apply **WorkingHours** 排程，將此排程套用在所有 **Chat** 群組中。您亦可以手動選擇每條應用程式列爲的排程。

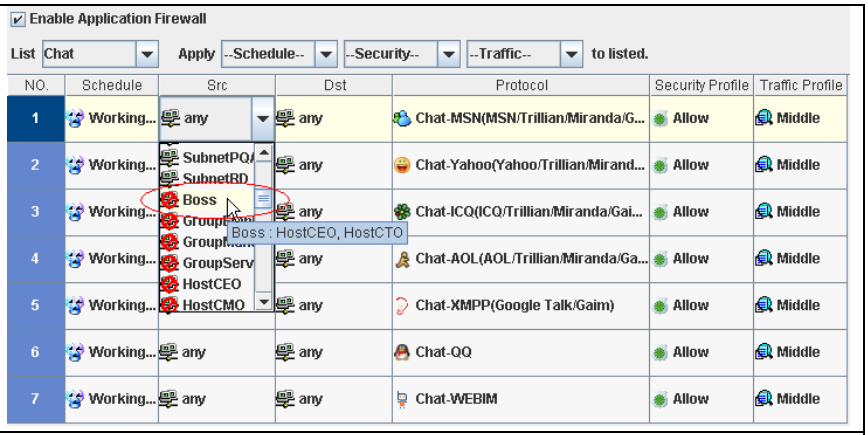
**Function > Management > Application Firewall**




**步驟 4 選擇來源端 IP**

因爲CEO與CTO有完整的許可權存取網際網路資源，且在上一章節中我們已建立一群組 **Boss（HostCEO, HostCTO）**。選擇圖示 Boss，意味著除了 **Boss** 這個群組外，所有來源端 IP 使用即時通訊軟體都套用選定的應用層防火牆規則。

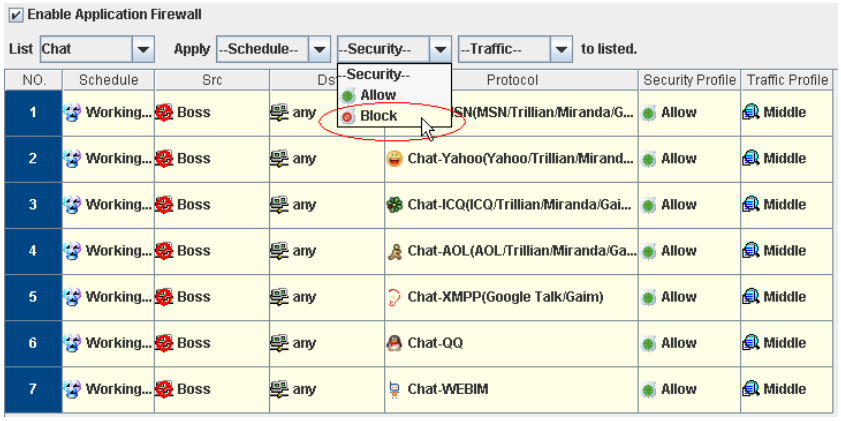
**Function > Management > Application Firewall**




**步驟 5 選擇安全行爲（Security Profile）**

在工具列的 **Security** 選項上選擇套用 **Block** 在所有即時通訊應用軟體上，但是請記得之後要將 MSN 的 Security 選擇**Allow**。因爲依公司規定，上班時間允許使用 MSN。

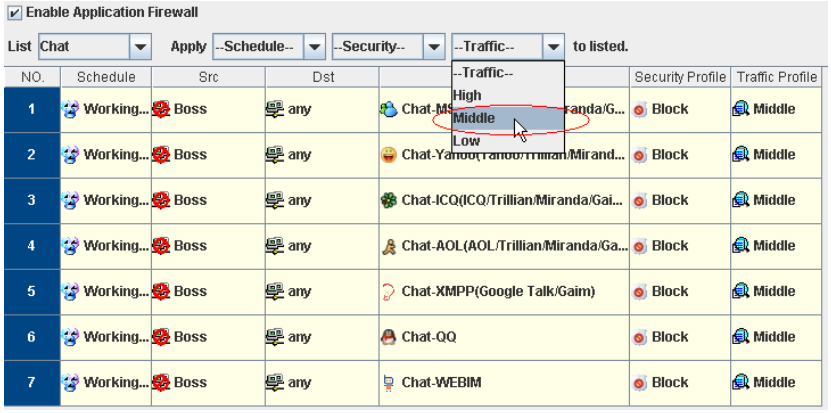
**Function > Management > Application Firewall**




**步驟 6 選擇頻寬類別（Traffic Profile）**

在工具列的 Traffic 選項上選擇套用 Middle 在所有即時通訊應用軟體上。使所有即時通訊軟體的頻寬限制爲 Middle 類別。

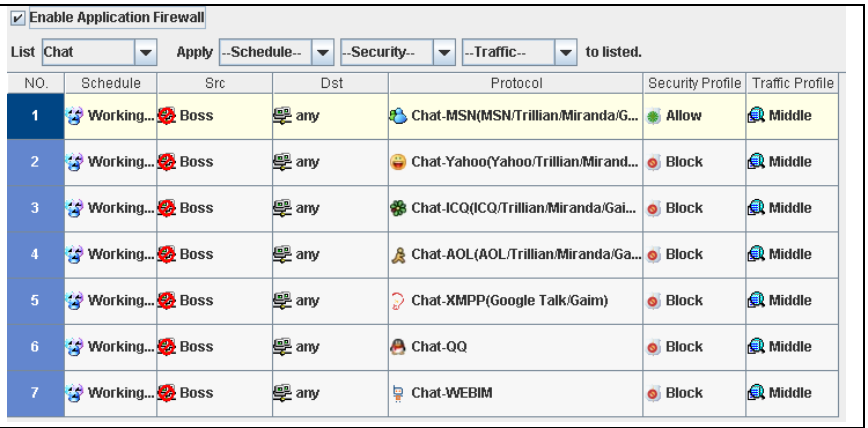
**Function > Management > Application Firewall**




**步驟 7 流覽已設定好的即時通訊政策**

流覽已設定好的即時通訊政策規則。

**Function > Management > Application Firewall**




| 欄位 | | 說明 | 範圍 / 格式 | 範例 |
|---|---|---|---|---|
| List | Group | 依群組搜尋所有應用層防火牆規則，並列舉搜尋結果。 | 所有 InstantScan 定義的群組 | Chat |
| Apply _____ to listed. | Schedule | 將選取的排程規則套用在所列舉的清單中。 | 使用者定義 | WorkingHours |
| | Security Profile | 將選取的安全行爲規則套用在所列舉的清單中。 | Allow / Block | Block |
| | Traffic Profile | 將選取的頻寬類別規則套用在所列舉的清單中。 | High / Middle / Low | Middle |

表格 10-1 應用層防火牆功能列

| 欄位 | 說明 | 範圍 / 格式 | 範例 |
|---|---|---|---|
| Src | 進入 InstantScan 之封包的來源端 IP 地址。請注意，圖示 Boss 指的是除了 Boss 這個位址群組外的其餘 IP 位址。 | Subnet / Range / Host | Boss |
| Dst | 進入 InstantScan 之封包的目的端 IP 位址。請注意，圖示 Boss 指的是除了 Boss 這個位址群組外的其餘 IP 位址。 | Subnet / Range / Host | any |
| Protocol | 通訊協定類別，或是可受 InstantScan 控管的應用程式類別。 | 所有可控管的通訊協定 | Chat-MSN |
| Security Profile | 控管應用程式的使用行爲。 | Allow / Block | Allow |
| Traffic Profile | 在流量管理員中所定義的頻寬類別。 | High / Middle / Low | Middle |

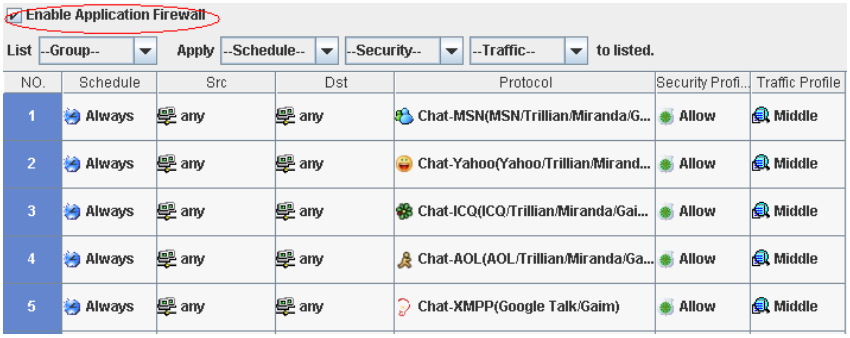
表格 10-2 應用層防火牆欄位說明

## 10.4.2 設定點對點傳輸軟體規則

**步驟 1 啓用應用層防火牆**

勾選 **Enable Application Firewall**。

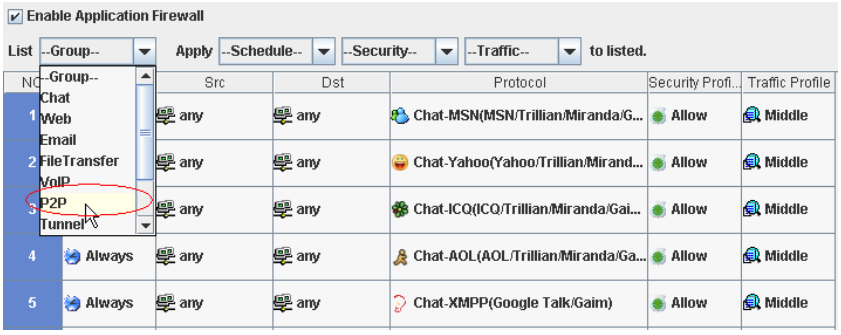
**Functions > Management > Application Firewall**




**步驟 2 列舉 P2P 群組**

在工具列之 **Group** 上選擇 **List P2P** 。所有P2P的清單就會顯示在螢幕上。

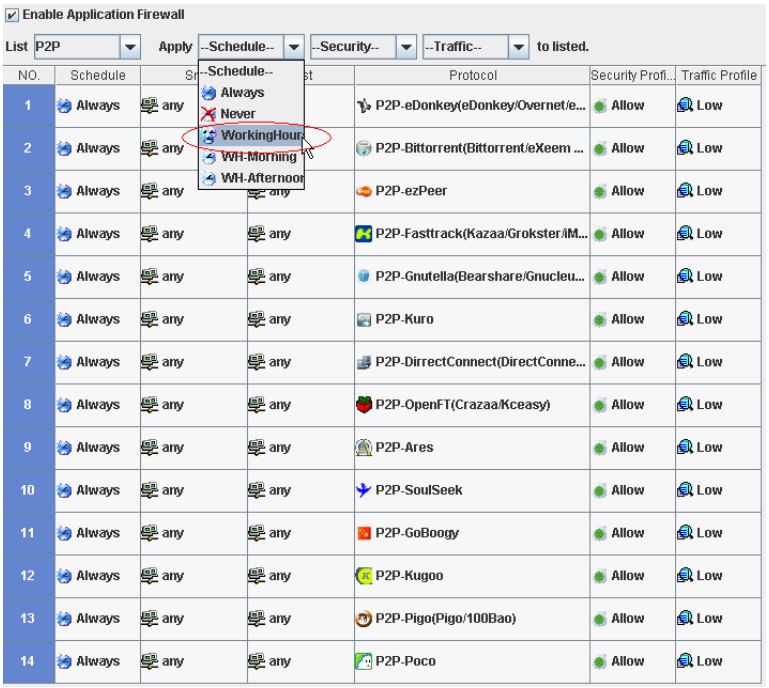
**Functions > Management > Application Firewall**




**步驟 3 選擇排程**

在工具列上選擇 **WorkingHours** 排程，將此排程套用在所有 **P2P 群組**中。您亦可以手動逐一選擇適合選定政策的排程。

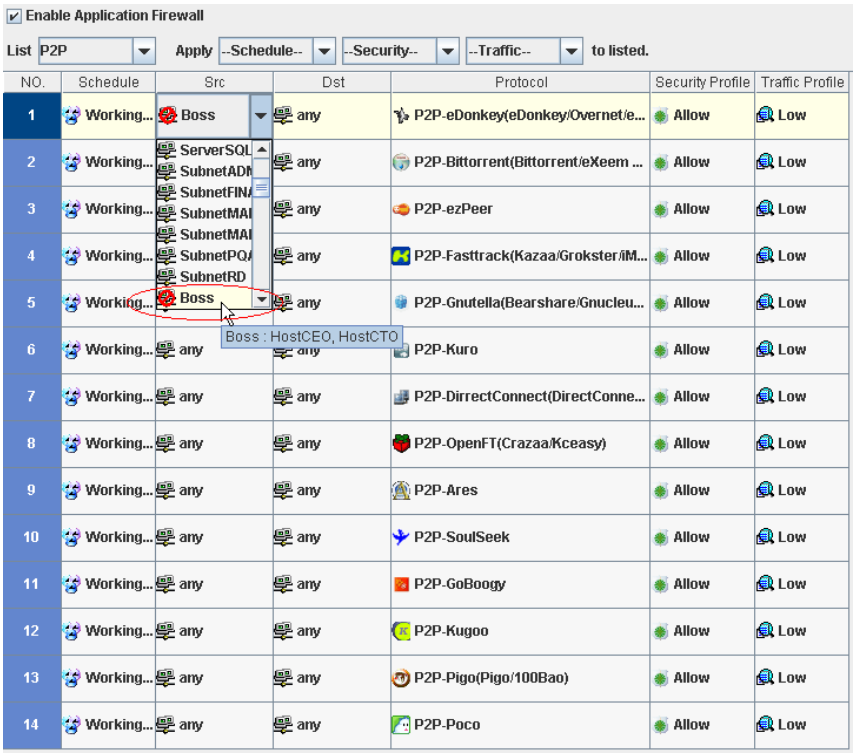
**Functions > Management > Application Firewall**



**步驟 4 選擇來源端 IP**

因爲CEO與CTO有完整的許可權存取網際網路資源，且在上一章節中我們已建立一群組 **Boss（HostCEO, HostCTO）**。選擇圖示 Boss，意味著除了 **Boss** 這個群組外，所有來源端 IP 使用點對點傳輸軟體都套用選定的應用層防火牆規則。

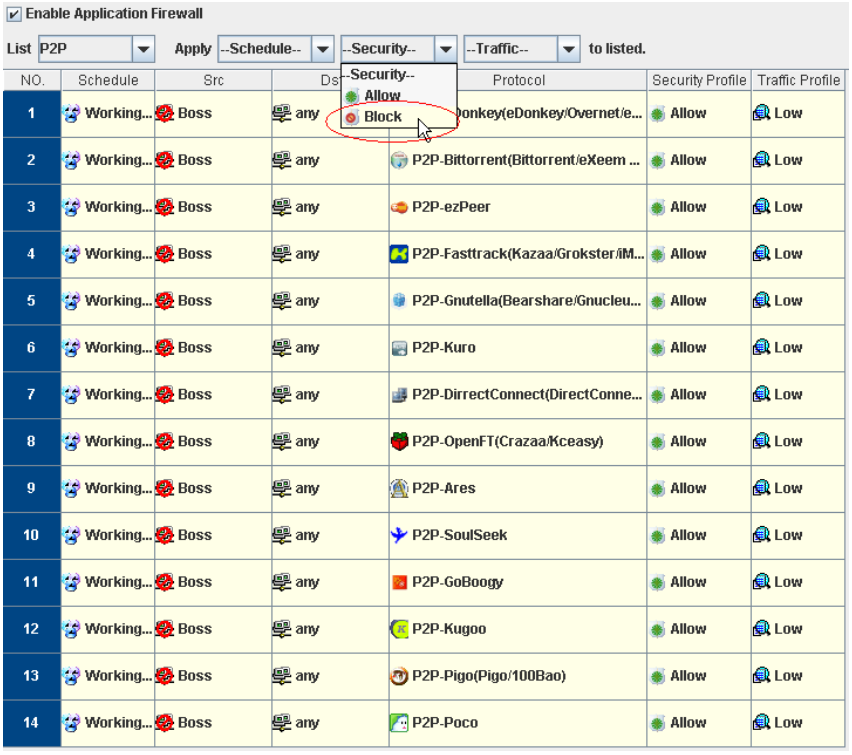
**Functions > Management > Application Firewall**




**步驟 5 選擇安全行爲**

在工具列的 **Secuirty Profile** 選項上選擇套用 **Block** 在所有點對點傳輸軟體。

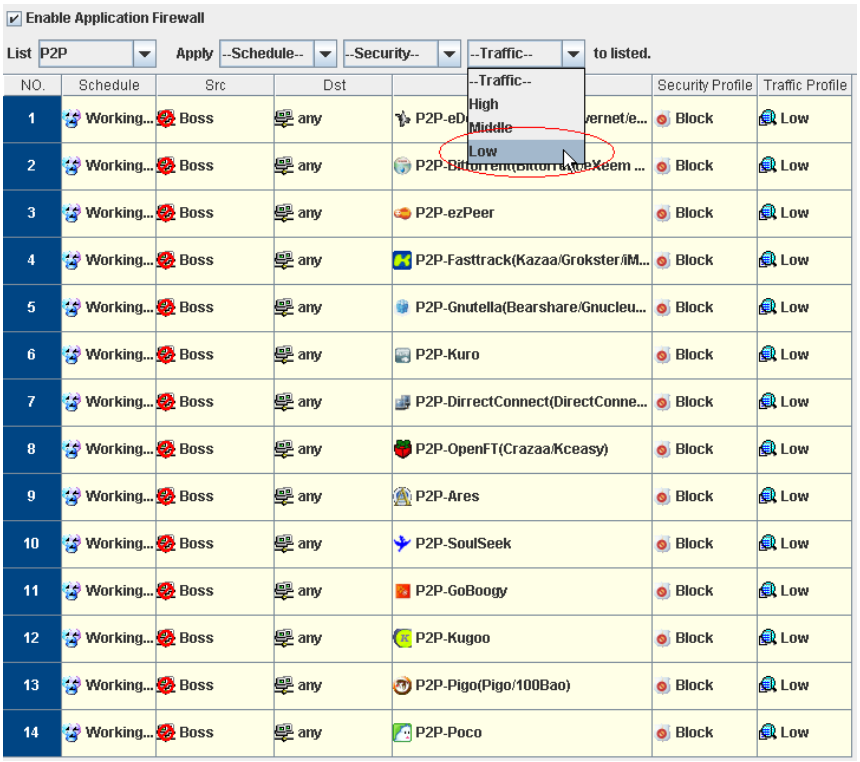
**Functions > Management > Application Firewall**



**步驟 6 選擇頻寬類別**

在工具列的 Traffic Profile 選項上選擇套用 **Low** 類別在所有點對點傳輸軟體上。使所有即時通訊軟體的頻寬限制爲 **Low** 類別。

**Functions > Management > Application Firewall**

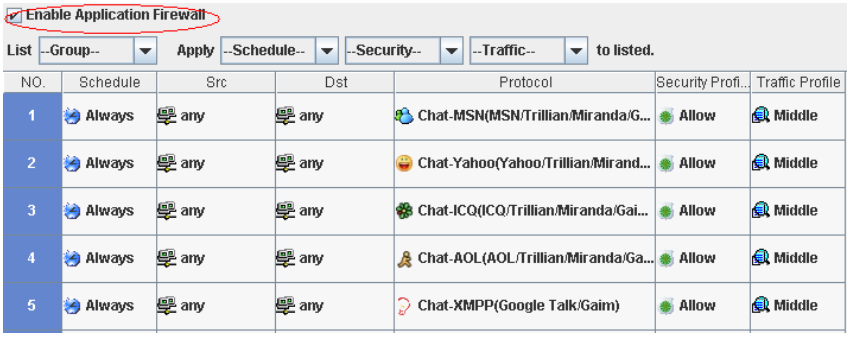



## 10.4.3 設定 VoIP 規則

**步驟 1 啓用應用層防火牆**

勾選 **Enable Application Firewall**。

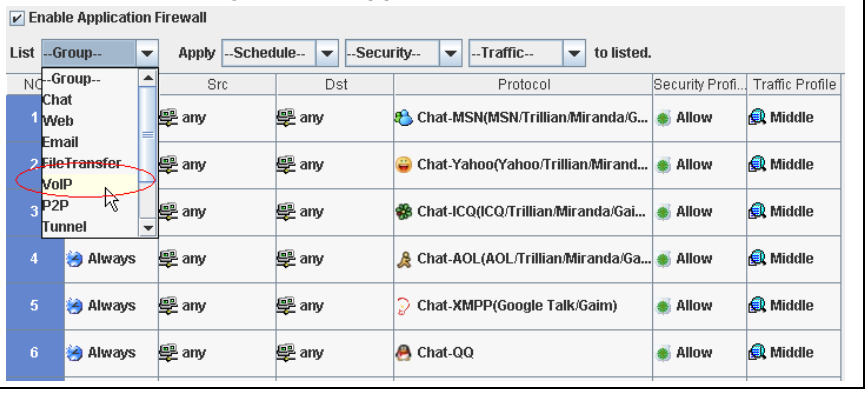
**Functions > Management > Application Firewall**




**步驟 2 列舉 VoIP 群組**

在工具列之 **Group** 上選擇 **List VoIP**。所有VoIP的清單就會顯示在螢幕上。

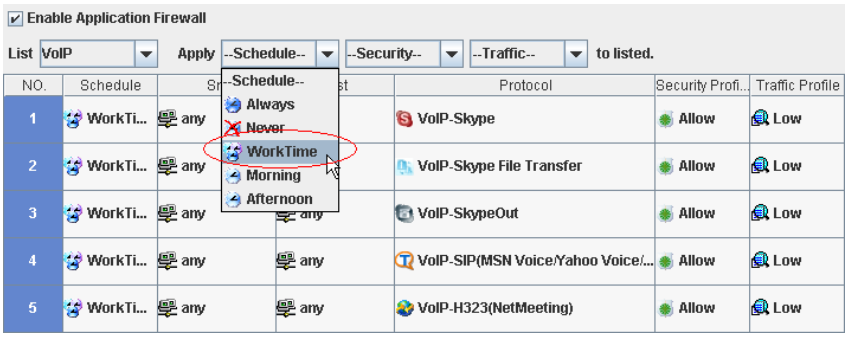
**Functions > Management > Application Firewall**



**步驟 3 選擇排程**

在工具列上選擇 **WorkingHours** 排程，將此排程套用在所有 **VoIP 群組**中。您亦可以手動選擇每條應用程式列爲政策的排程。

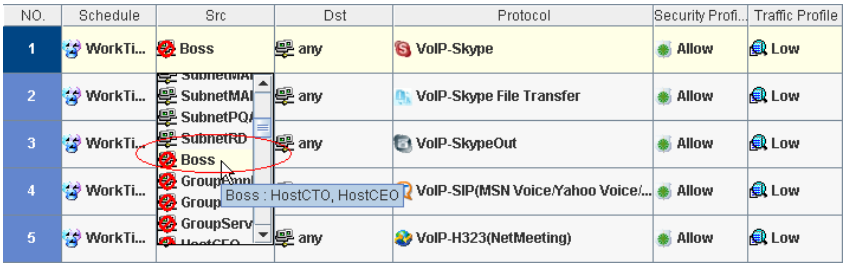
**Functions > Management > Application Firewall**




**步驟 4 選擇來源端 IP**

因爲CEO與CTO有完整的許可權存取網際網路資源，且在上一章節中我們已建立一群組 **Boss（HostCEO, HostCTO）**。選擇圖示 Boss，意味著除了 **Boss** 這個群組外，所有來源端IP使用點對點傳輸軟體都套用選定的應用層防火牆規則。

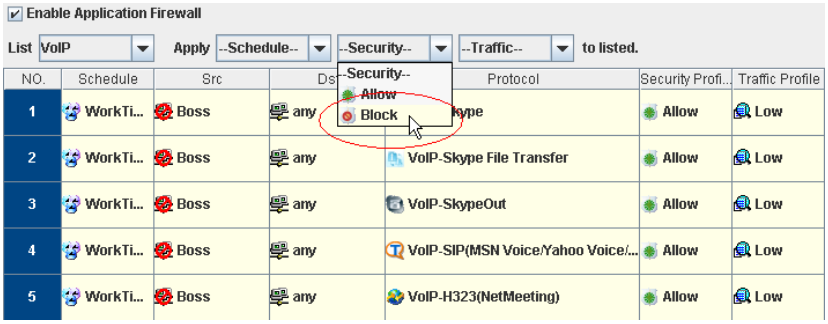
**Functions > Management > Application Firewall**




**步驟 5 選擇安全行爲**

在工具列的 **Security Profile** 選項上選擇套用 **Block** 在所有點對點傳輸軟體上。

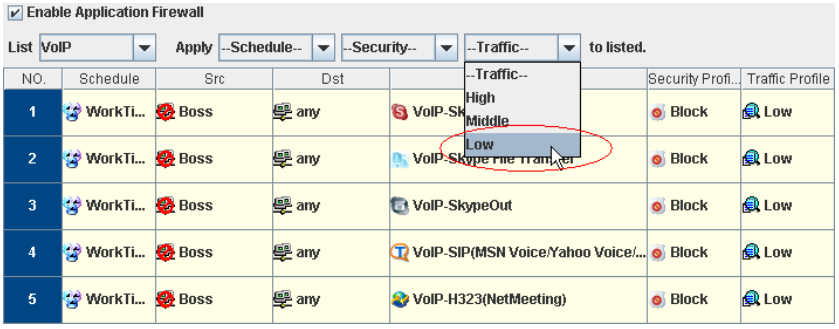
**Functions > Management > Application Firewall**




**步驟 6 選擇頻寬類別**

在工具列的 **Traffic Profile** 選項上選擇套用 **Low** 在所有點對點傳輸軟體上。使所有即時通訊軟體的頻寬限制爲 **Low** 類別。

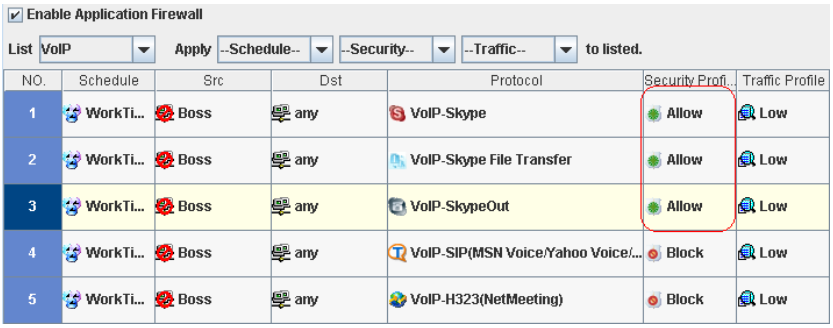
**Functions > Management > Application Firewall**



**步驟 7 調整 Skype 的安全行爲**

依公司政策允許員工上班使用 Skype，所以您必須手動調整 Skype 的安全行爲到 **Allow** 的狀態。這樣 Skype 的流量才可以通過InstantScan。

**Functions > Management > Application Firewall**



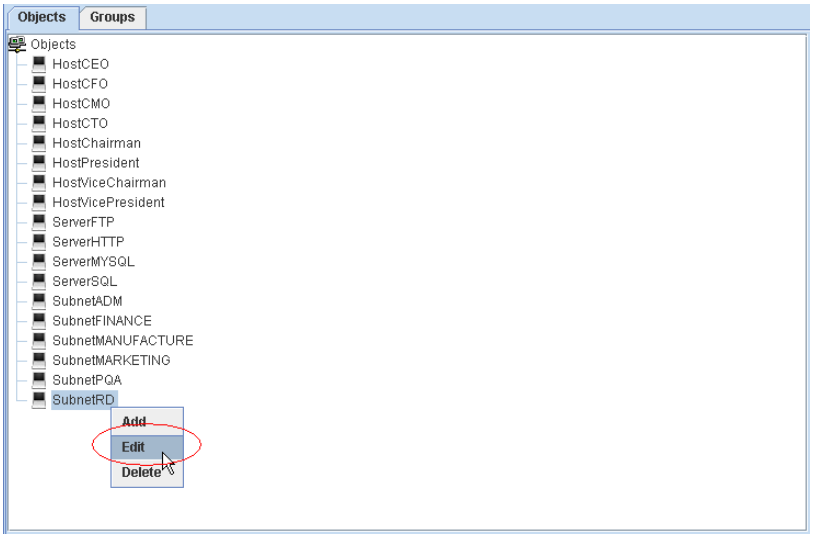

## 10.4.4 攔阻 VoIP - Skype File Transfer

**步驟 1 檢查物件管理員**

因爲R&D部門不可使用 Skype 的檔案傳輸功能，所以包含在R&D部門的IP地址範圍，從 192.168.17.1 ~ 192.168.17.254，屬於 192.168.17.0 之網段。請先編輯好物件 SubnetRD，然後才可編輯 Skype的規則。

在 SubnetRD 上按右鍵，然後點擊 **Edit**。

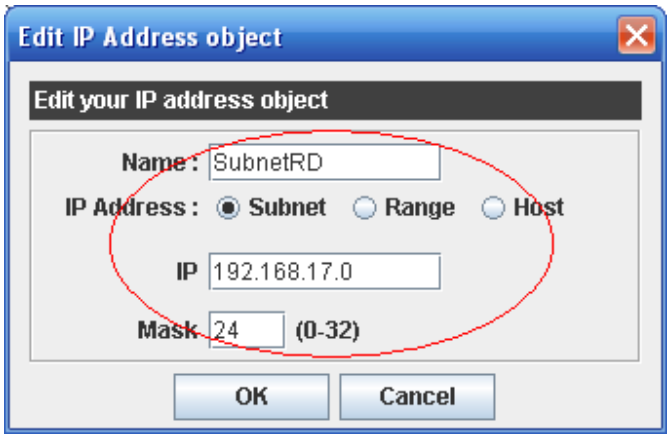
**Functions > Management > Object Manager > Address > Objects**




**步驟 2 設定R&D部門的IP地址**

位址物件可以是子網、範圍、單一主機。SubnetRD 的位址性質屬於子網，所以請編輯 SubnetRD 爲 192.168.17.0/24。 點擊 **OK** 關閉窗口。

**Functions > Management > Object Manager > Address > Objects**



**步驟 3 上班時間攔阻 R&D 部門員工使用 Skype檔案傳輸**

根據 ABC 公司的政策，所有VoIP應用軟體只開放使用 Skype，但是 R&D 部門的員工因爲機密性因素，在上班時間不准使用 Skype 檔案傳輸。

上一節我們已設定好 VoIP 的使用規則了，現在要將其加以調整。點選 VoIP-Skype File Transfer，在 Src 欄位上選擇 SubnetRD 選項，然後在 Security Profile 上選擇 **Block**。

當 RD 想透過 Skype 傳檔時，這個動作就會被 InstantScan 攔阻下來。

**Functions > Management > Application Firewall**

| NO. | Schedule | Src | Dst | Protocol | Security Profi... | Traffic Profile |
|---|---|---|---|---|---|---|
| 1 | WorkTi... | Boss | any | VoIP-Skype | Allow | Low |
| 2 | WorkTi... | SubnetRD | any | VoIP-Skype File Transfer | Block | Low |
| 3 | WorkTi... | Boss | any | VoIP-SkypeOut | Allow | Low |
| 4 | WorkTi... | Boss | any | VoIP-SIP(MSN Voice/Yahoo Voice/... | Block | Low |
| 5 | WorkTi... | Boss | any | VoIP-H323(NetMeeting) | Block | Low |

**步驟 4 上傳設定檔**

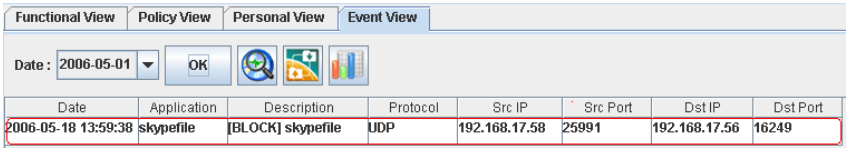
當設定好以上的政策規則後，請記得上傳設定檔到InstantScan裝置上，否則當您重新連上裝置後，現行的設定檔就會被系統清除。

選擇 **Upload Configuration** 選項，或者點擊圖示  上傳現行的設定檔。

**步驟 5 Skype傳檔的事件記錄**

由右圖我們可以看出，RD 部門 IP 192.168.17.58 企圖透過 Skype 傳檔，但被 InstantScan 攔阻下來的事件記錄。

**Functions > Reports > Application Firewall > Event View**




| Date | Application | Description | Protocol | Src IP | Src Port | Dst IP | Dst Port |
|---|---|---|---|---|---|---|---|
| 2006-05-18 13:59:38 | skypefile | [BLOCK] skypefile | UDP | 192.168.17.58 | 25991 | 192.168.17.56 | 16249 |

**設定小技巧：**

1. 如果您要選取/取消選取某條規則時，只要利用 ＜Ctrl＞ + ＜滑鼠左鍵＞ 在該規則的編號上點一下即可轉換選取的動作。
2. 如果在編輯應用層防火牆時，某條規則呈現淡黃色背景時，代表您已選取該條規則。如果您希望透過篩選工具列套用選定的政策在所有的通訊協定上時，請將滑鼠移到第一條規則上，按滑鼠左鍵往下拉，當所有規則的背景都呈現淡黃色時，代表所有規則已被選取。
3. 如果您要選取排列不連續的規則，您可以按住 ＜Ctrl＞，然後透過滑鼠在選取的規則上點一下即可。

# 第7部

# 即時通訊管理員

# 第11章
# 自訂警告訊息

## 11.1 需求

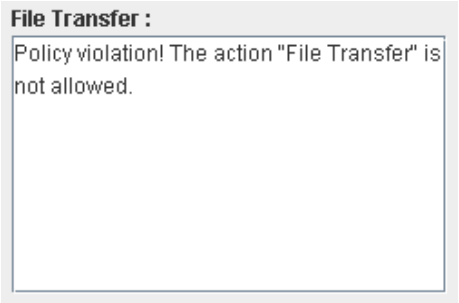
管理人員希望自訂符合即時通訊行爲的警告訊息，當使用者違反即時通訊政策，並即時在即時通訊視窗內收到警告訊息時才可從警告訊息的內容中得知自己的行爲違反了哪條政策規則。

## 11.2 方法

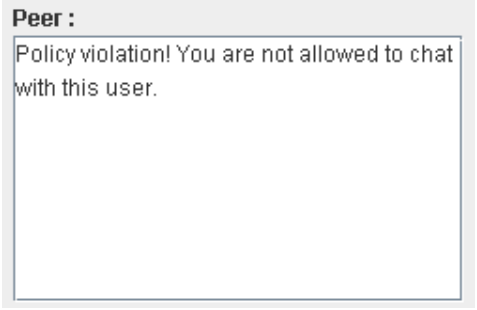
到 **Functions > Management > IM Manager > Message** 中編輯警告訊息。

## 11.3 步驟

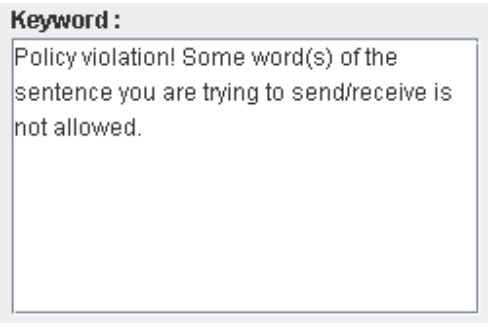
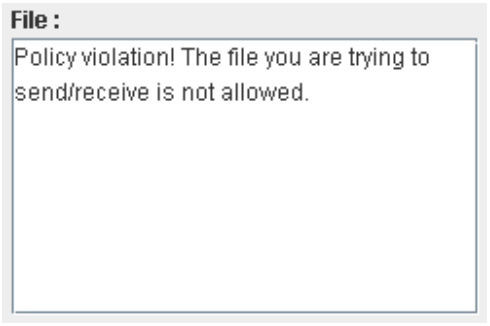
### 11.3.1 即時通訊服務

| **步驟 1 違反檔案傳送規則之警告訊息**<br>編輯使用者違反檔案傳輸規則時，系統會在即時通訊視窗內發送給使用者的警告訊息。<br><br>其餘違反即時通訊服務的警告訊息編輯原則一樣。 | **Functions > Management > IM Manager > Message > IM Service**<br>  |
|---|---|

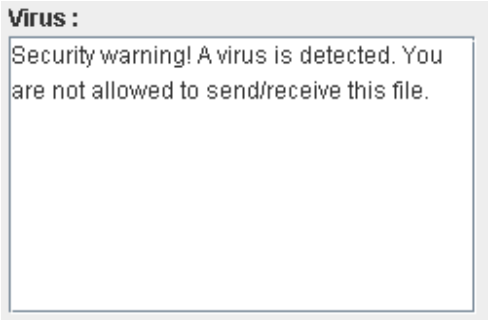
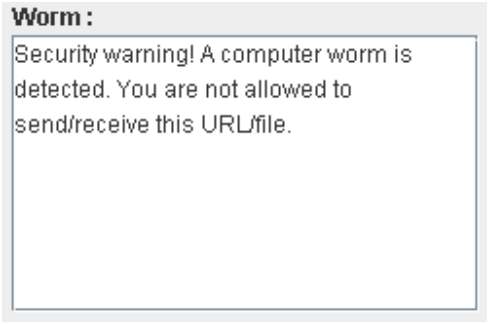
### 11.3.2 即時通訊聊天物件

| **步驟 1 違反聊天物件規則之警告訊息**<br>編輯使用者違反即時通訊聊天物件規則時，系統會在即時通訊視窗內發送給使用者的警告訊息。 | **Functions > Management > IM Manager > Message > IM Peer**<br>  |
|---|---|

### 11.3.3 即時通訊內容

| | |
|---|---|
| **步驟 1 關鍵字攔阻**<br>編輯傳送不合法的關鍵字時，系統會在即時通訊視窗內發送給使用者的警告訊息。 | **Functions > Management > IM Manager > Message > IM Content**<br>  |
| **步驟 2 檔案攔阻**<br>編輯傳送不合法的檔案時，系統會在即時通訊視窗內發送給使用者的警告訊息。 | **Functions > Management > IM Manager > Message > IM Content**<br>  |

### 11.3.4 即時通訊病毒防護

| | |
|---|---|
| **步驟 1 病毒攔阻**<br>編輯傳送/接收的檔案內如果藏匿有病毒，系統會在即時通訊視窗內發送給使用者的警告訊息。 | **Functions > Management > IM Manager > Message > IM Security**<br>  |
| **步驟 2 電腦蠕蟲攔阻**<br>編輯傳送/接收的URL/檔案內如果藏匿有電腦蠕蟲，系統會在即時通訊視窗內發送給使用者的警告訊息。 | **Functions > Management > IM Manager > Message > IM Security**<br>  |

### 11.3.5 其餘加密軟體

| | |
|---|---|
| **步驟 1 攔阻加密軟體**<br>編輯當使用者透過協力廠商加密軟體聊天，被攔阻時，系統在即時通訊視窗顯示給使用者的訊息。 | **Functions > Management > IM Manager > Message > Others**<br>**Encryption software :**<br>Policy violation! A third-party encryption software is detected. You are not allowed to send/receive this message. |
| **步驟 2 上傳設定檔**<br>選擇 Upload Configuration 或者點擊圖示  ，將現行的設定檔上傳到裝置上。 | |

**注意：**

所謂協力廠商加密軟體就是非由正規即時通訊軟體如 MSN/Yahoo/ICQ/AOL 官方網站所提供，但可與其相容的軟體。當您啓用 IM Manager 時，這些協力廠商加密軟體就會被限制不可使用。

# 第12章
# 即時通訊服務/群組

## 12.1 需求

1. 網管人員希望依照工具性質來定義每位元員工的即時通訊行爲之許可權。
2. 所有員工將依工作性質分成許多不同的群組，以方便網管人員控管其網路之使用。

## 12.2 方法

1. 定義即時通訊服務，讓管理者可以視使用者需求爲其選擇適當的服務。
2. 將每個員工分配到其適合的群組中。

## 12.3 步驟

### 12.3.1 即時通訊服務

**步驟 1 預設即時通訊服務**

預設即時通訊服務如右圖所示。你可依照您的需求修改或刪除預設服務規則。

注意，如果某條即時通訊服務規則已被其他規則使用了，您不可以直接刪除此規則，如欲刪除，請先刪除所有已包含此服務規則的其他規則。

**Functions > Management > IM Manager > IM Services**


**步驟 2 新增即時通訊服務**

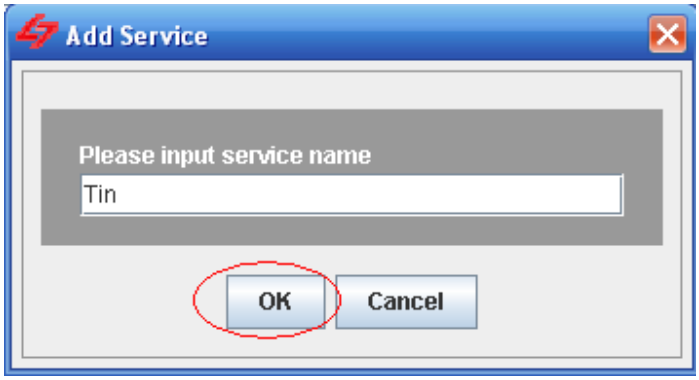
將滑鼠移到即時通訊服務上按右鍵，然後點選 New Service。

**Functions > Management > IM Manager > IM Services**


**步驟 3 輸入新服務名稱**

輸入新增服務的名稱，然後點擊 **OK** 關閉視窗。

**Functions > Management > IM Manager > IM Services**



**步驟 4 開啓適用此規則的即時通訊行爲**

新增的即時通訊服務規則預設爲禁止所有即時通訊行爲，所以當您新增一條規則即要調整其預設設定。

將滑鼠移到您要開啓的項目上點一下，待圖示 出現即可。

**Functions > Management > IM Manager > IM Services**


**步驟 5 啓用即時通訊使用行爲**

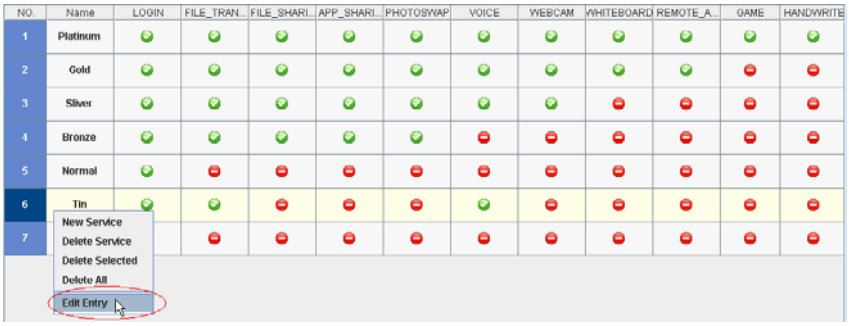
啓用 Login、FileTransfer、與 Voice。

**Functions > Management > IM Manager > IM Services**


**步驟 6 變更即時通訊服務規則名稱**

在選取的規則上按右鍵，然後點選 **Edit Entry**。

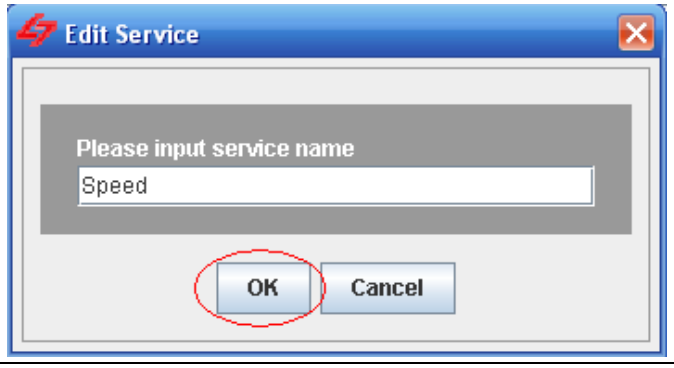
**Functions > Management > IM Manager > IM Services**




**步驟 7 編輯服務名稱**

輸入您要修改的服務名稱，點擊 **OK** 關閉視窗。

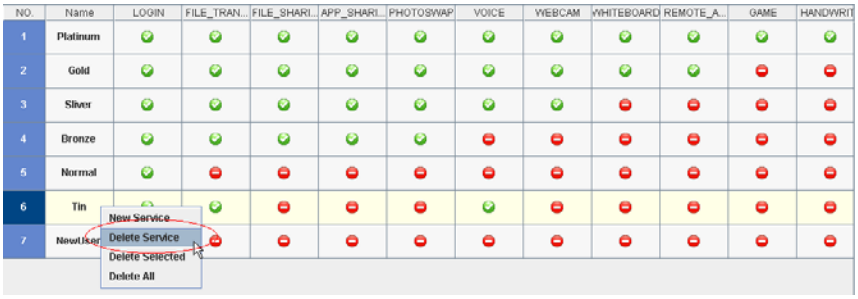
**Functions > Management > IM Manager > IM Services**




**步驟 8 刪除服務**

將滑鼠移到要刪除的服務規則上按右鍵，點選 Delete Service 或 Delete Selected 即可刪除此服務。

**Functions > Management > IM Manager > IM Services**



**步驟 9 上傳設定檔到裝置上**

選擇 **Upload Configuration** 或者點擊圖示  ，將現行的設定檔上傳到裝置上。

| 即時通訊使用行爲 | 說明 |
|---|---|
| 登入 | 允許使用者登入即時通訊軟體與其他即時通訊使用者線上傳送訊息。 |
| 檔案傳送 | 允許即時通訊使用者與其他使用者傳送或接收檔案。 |
| 檔案分享 | 允許即時通訊使用者與其他使用者分享檔案。 |
| 應用程式分享 | 允許即時通訊使用者與其他使用者分享應用程式。 |
| 相片分享 | 允許即時通訊使用者與其他使用者分享相片。 |
| 語音 | 允許即時通訊使用者與其他使用者使用語音交談。 |
| 影像 | 允許即時通訊使用者與其他使用者透過視訊交談。 |
| 白板 | 允許即時通訊使用者與其他使用者透過白板書寫筆記、畫圖或傳送簡訊。 |
| 遠程協助 | 允許即時通訊使用者與其他使用者使用遠端協助功能。 |
| 遊戲 | 允許即時通訊使用者與其他使用者互相玩線上遊戲。 |
| 手寫 | 允許即時通訊使用者透過手寫功能傳遞訊息。 |

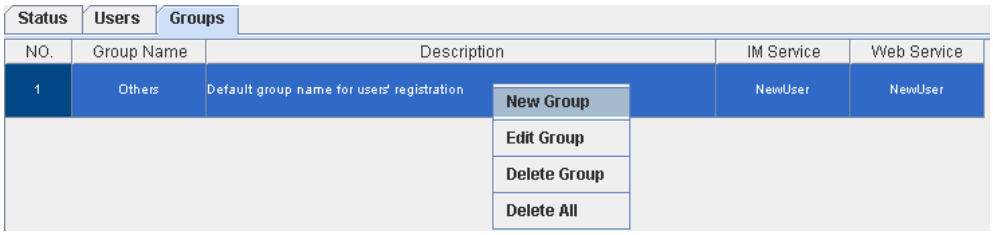
表格 12-1 可管理的即時通訊使用行爲

### 12.3.2 即時通訊群組

**步驟 1 自訂即時通訊群組**

將滑鼠移到即時通訊群組螢幕上按右鍵，然後選擇 New Group。命名此Group爲Boss。

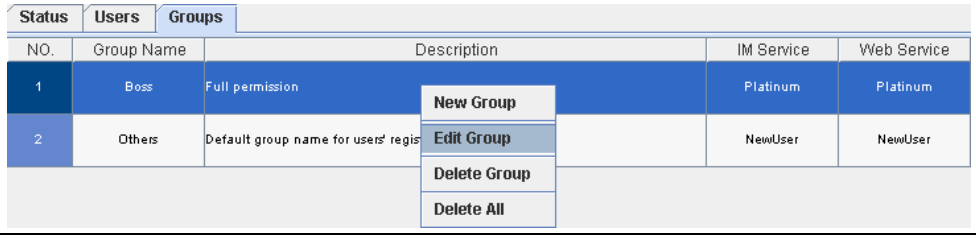
**Functions > Console > User Console**




**步驟 2 編輯群組說明**

將滑鼠移到 Boss 規則的說明欄位上按右鍵，然後選擇 **Edit Entry**。

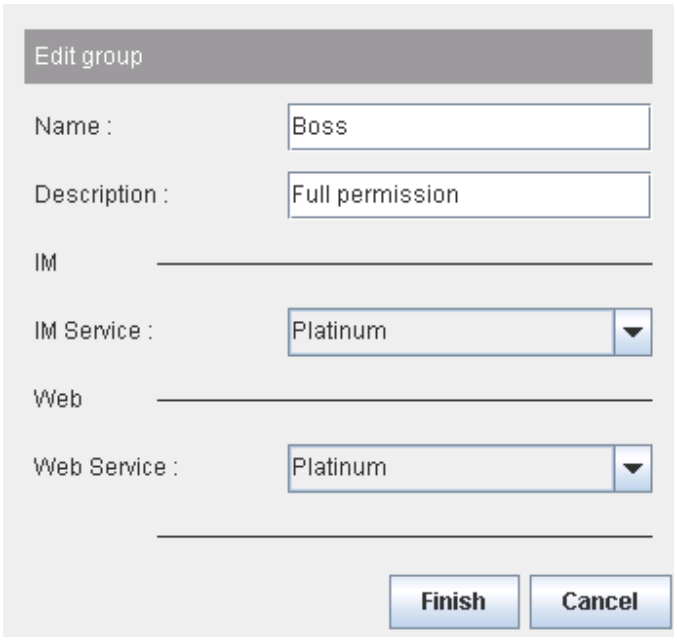
**Functions > Console > User Console**



**步驟 3 輸入群組說明**

在 **Content** 欄位內輸入您要爲此群組做的說明，然後點擊 **OK** 繼續。

**Functions > Console > User Console**




**步驟 4 設定此群組的預設服務**

選擇此群組的預設服務。當即時通訊使用規則排程已過，系統將會套用預設規則於屬於該群組的即時通訊使用者上。

**Functions > Console > User Console**


**步驟 5 上傳設定檔**

選擇 **Upload Configuration** 或點擊圖示  將設定檔上傳到裝置上。

**注意：**

除了手動建立即時通訊群組外，您也可以透過 AD Import 或者 File Import 的方式，從既有的資料庫中匯入群組資料。請參閱以下章節。

# 第13章
# 即時通訊使用者設定

## 13.1 需求

1. 即時通訊使用者必須與現有的 AD 資料庫整合。
2. 在上班時間，員工只可以使用 MSN，且需要被側錄存證，其餘即時通訊軟體一率禁止。員工可以選擇使否要收到違反規則之警告信件。
3. 管理者想將已設定好的即時通訊使用者備份存檔。

## 13.2 方法

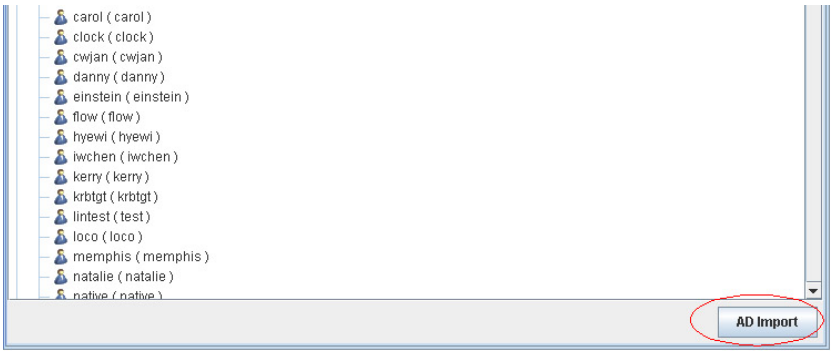
1. 從已存在的資料庫中匯入即時通訊使用者。
2. 將即時通訊使用規則預設爲”Block”，上班時間只可以使用 MSN。每筆聊天記錄都需要被側錄，且當使用者違反規則時將收到警告信件。
3. 選擇”File Export”將編輯好的即時通訊使用者匯出儲存成檔案。

## 13.3 步驟

當您啓用即時通訊管理員，並上傳設定檔到 InstantScan 裝置上時，即時通訊使用者立即受 InstantScan 控管。當您設定寄送警告信件給違反規則的使用者時，使用者將隨時被知會其是否違反了公司的政策規則。InstantScan 提供您三個方法來編輯即時通訊使用者的清單：1） 從現存的 AD 伺服器匯入使用者資料；2） 將現有資料庫匯出的文字檔匯入使用者資料；3） 手動自行編輯使用者清單。

管理者可以自行定義預設使用者的行爲模式爲攔阻或是允許通行。以下的範例，將介紹您如何設定即時通訊使用者。

### 13.3.1 AD Import – Open LDAP

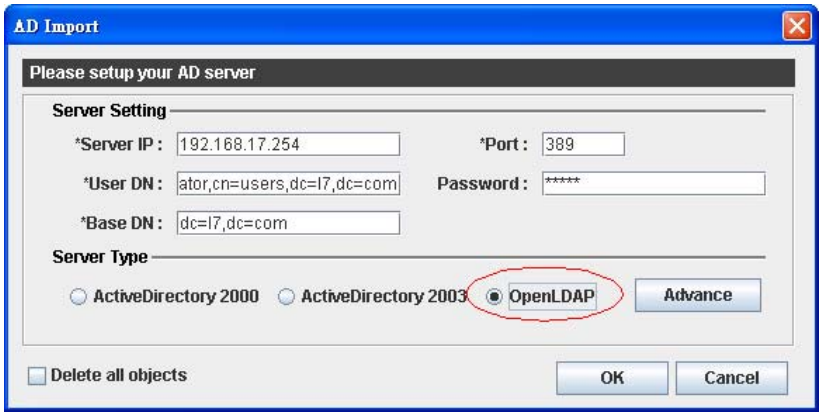
| | |
|---|---|
| **步驟 1 選擇透過 AD 匯入使用者資料**<br>點擊 **AD Import** 繼續。 | **Functions > Management > Object Manager > AD > AD Import**<br>  |

**步驟 2 從 OpenLDAP 匯入**

在伺服器設定區域內，輸入伺服器 IP、埠（預設 = 389）、與您用來連結 OpenLDAP 伺服器的 User DN 與密碼。然後輸入使用者資料所在的 Base DN。圈選 OpenLDAP 爲伺服器類型。相關 OpenLDAP 的設定，請參考章節 **錯誤! 找不到參照來源。** 與 **錯誤! 找不到參照來源。**。

請注意，打星號的欄位爲必填欄位。

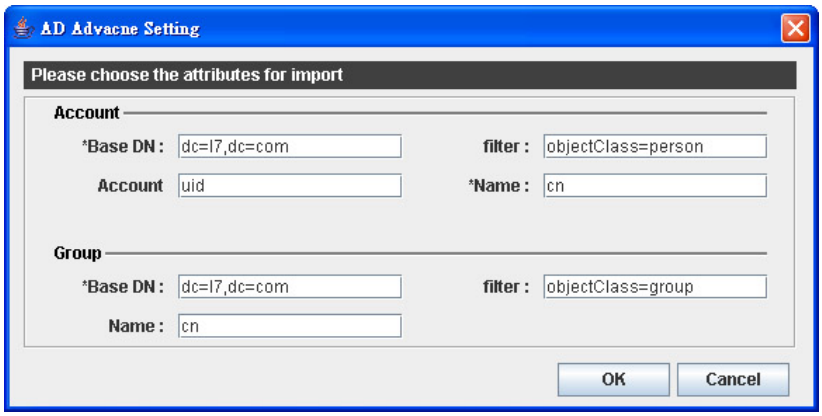
**Functions > Management > Object Manager > AD > AD Import**




**步驟 3 OpenLDAP 進階設定**

進階設定的篩選功能可讓您更精確的匯入您需要的資料。有關 LDAP 進階設定，請參考章節 **錯誤! 找不到參照來源。**。

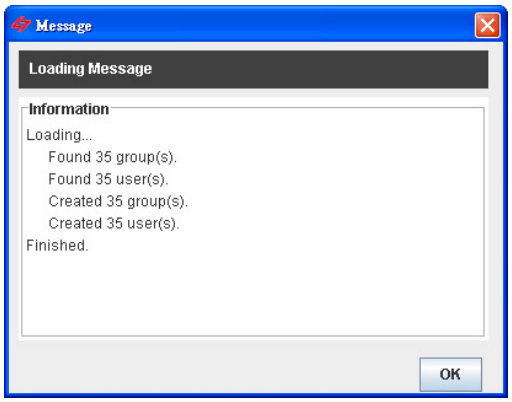
**Functions > Management > Object Manager > AD > AD Import**




**步驟 4 匯入成功**

當從LDAP伺服器匯入資料成功，系統將會顯示如右圖的訊息告訴您。點擊 **OK** 完成設定。

**Functions > Management > Object Manager > AD > AD Import**




**步驟 5 上傳設定檔**

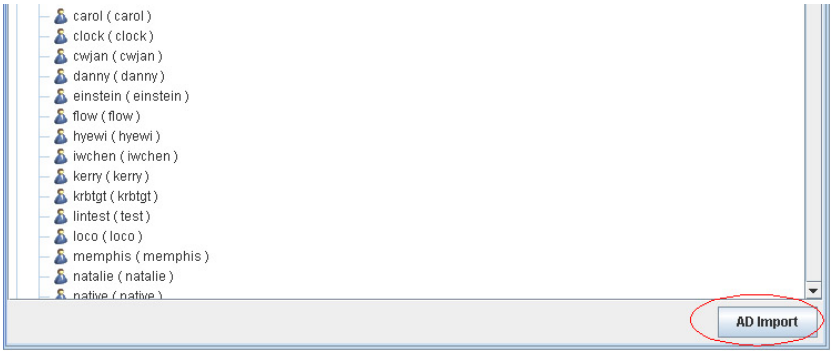
選擇 **Upload Configuration** 或點擊圖示  將設定檔上傳到裝置上。

### 13.3.2 AD Import – ActiveDirectory

**步驟 1 選擇透過 AD 匯入使用者資料**

點擊 **AD Import** 繼續。

**Functions > Management > Object Manager > AD > AD Import**

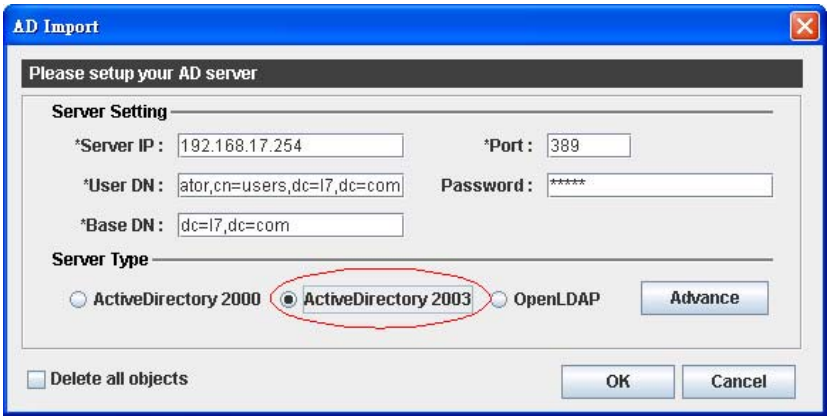



**步驟 2 從 ActiveDirectory 匯入**

在伺服器設定區域內，輸入伺服器 IP、埠（預設 = 389）、與您用來連結 ActiveDirectory 伺服器的 User DN 與密碼。然後輸入使用者資料所在的 Base DN。圈選 ActiveDirectory 2003 爲伺服器類型。相關 ActiveDirectory 的設定，請參考章節 **錯誤! 找不到參照來源。** 與 **錯誤! 找不到參照來源。**。

請注意，打星號的欄位爲必填欄位。

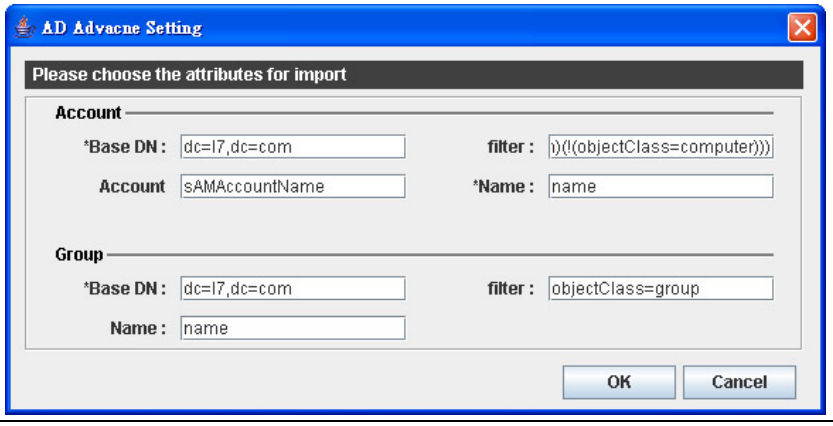
**Functions > Management > Object Manager > AD > AD Import**




**步驟 3 ActiveDirectory 進階設定**

進階設定的篩選功能可讓您更精確的匯入您需要的資料。有關 LDAP 進階設定，請參考章節 **錯誤! 找不到參照來源。**。

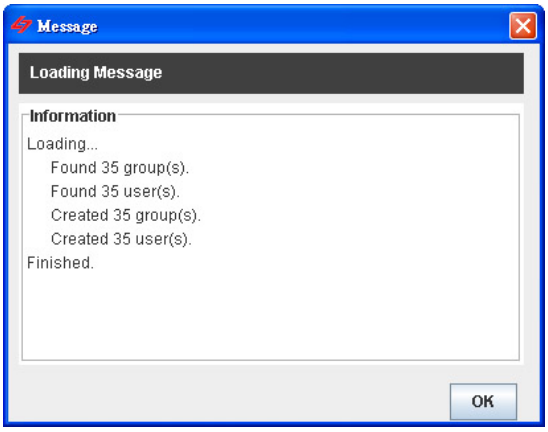
**Functions > Management > Object Manager > AD > AD Import**



**步驟 4 匯入成功**

當從 AD 伺服器匯入資料成功，系統將會顯示如右圖的訊息告訴您。點擊確定完成設定。

**Functions > Management > IM Manager > IM User > LDAP Import**




**步驟 5 上傳設定檔**

選擇 **Upload Configuration** 或點擊圖示  將設定檔上傳到裝置上。

| 欄位 | 說明 | ActiveDirectory 範例 | Open LDAP 範例 |
|---|---|---|---|
| **Server Setting** | | | |
| Server IP | LDAP 伺服器的 IP 地址 | 10.17.17.3 | 10.17.17.3 |
| Port | LDAP 伺服器資料進出的埠。 | 389 （預設） | 389 （預設） |
| User DN | User DN 爲授權用來存取 LDAP 伺服器的資源。相當於使用者的帳號。 | Administrator | cn=manager,dc=yourCompany,dc=com |
| Password | 使用者存取 LDAP 伺服器所需的密碼。 | ADLdapABC | OpenLDAP |
| Base DN | Base DN 爲 LDAP 伺服器上查詢使用者所需的路徑目錄。 | cn=users,dc=ABC,dc=com | ou=people,dc=ABC,dc=com |
| **Server Type** | | | |
| ActiveDirectory 2002 | | | |
| ActiveDirectory 2003 | | | |
| OpenLDAP | | | |
| **Advance** | | | |
| **Account** | | | |
| Base DN | Base DN 是你在 AD 所建立組織的名字，如 ou=group,dc=ABC,dc=com。而這些都是你在安裝的過程中，在設定 AD 時所做的設定。 | cn=users,dc=yourCompany,dc=com | ou=people,dc=yourCompany,dc=com |
| filter | 如果您想要匯入某個使用者的資料，您可以透過這個篩檢程式來搜尋您要的資料。（ObjectClass=person） | (&(objectClass=person)(!(objectClass=computer))) | objectClass=person |
| Account | 在此的名稱是 LDAP 伺服器上用來辨識使用者的帳號欄位。 | sAMAccountName | uid |
| Name | 在此的名稱是 LDAP 伺服器上用來辨識使用者的名稱欄位。 | name | cn |
| **Group** | | | |
| Base DN | Base DN 是你在 LDAP 所建立組織的名字，如 ou=group,dc=ABC,dc=com。而這些都是你在安裝的過程中，在設定 LDAP 時所做的設定。 | cn=manager,dc=ABC,dc=com,dc=tw | ou=group,dc=ABC,dc=com |
| filter | 如果您想要匯入某個使用者的資料，您可 | objectClass=group | objectClass=group |

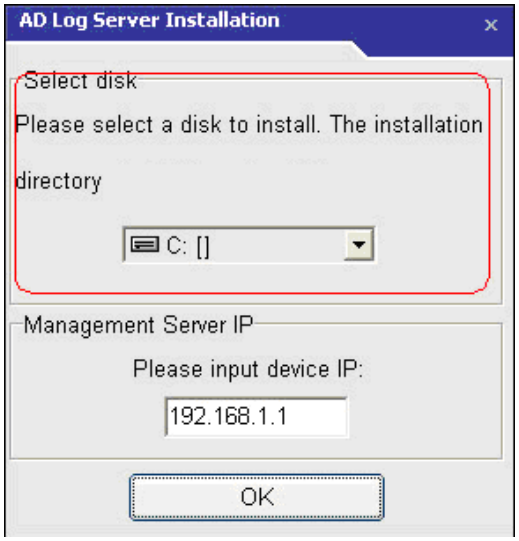
| | | | |
|---|---|---|---|
| | 以透過這個篩檢程式來搜尋您要的資料。（ObjectClass=person） | | |
| Name | 在此的名稱是 LDAP 伺服器上用來辨識使用者群組的名稱欄位。 | name | cn |

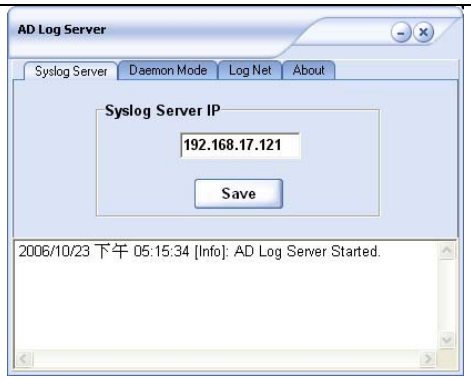
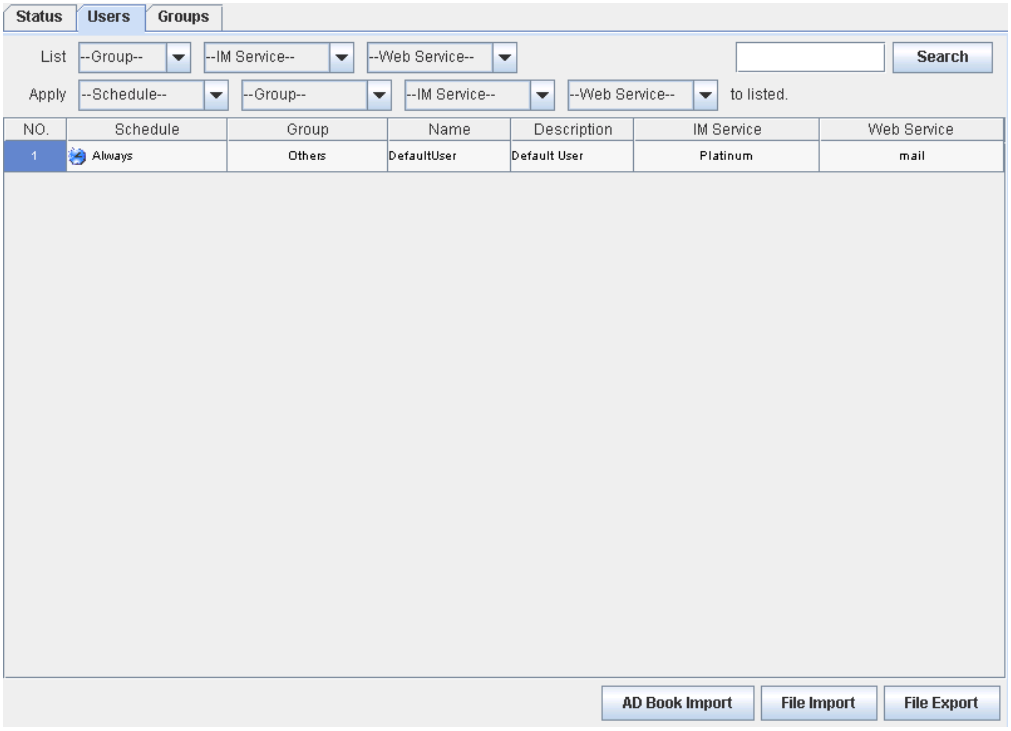
### 13.3.3 使用 AD Book Import

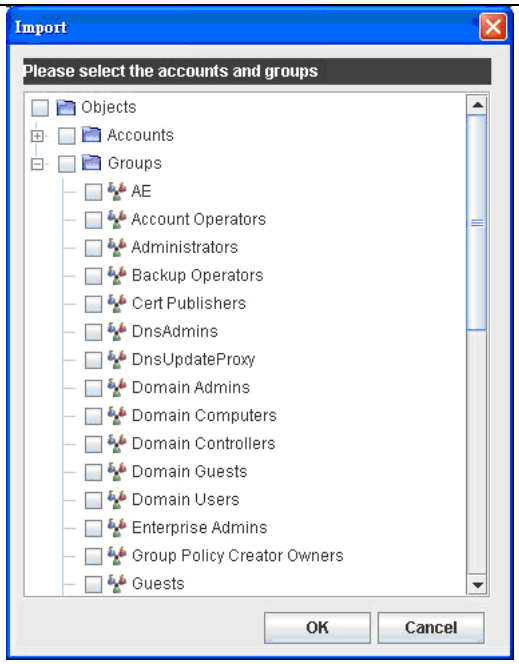
**IM Manager 可以搭配 AD Server 自動從 AD Server 匯入使用者的帳號與群組作管理。**

**安裝程式概述：**

- 安裝 AD Log Server
- 啓動 AD Manager(選購)
- AD Book Import…

| | |
|---|---|
| **步驟 1 安裝 AD Log Server**<br>啓動本軟體得安裝程式 Setup.exe，點選 AD Log Server。 | **安裝介面 > AD Log Server** |
| **步驟 2 設定安裝路徑與設定 device IP**<br>選擇 AD Log Server 要安裝到那裡。選將 IP 設定爲跟設備的 IP 相同。<br><br>請注意：此 IP 設定的意思爲 AD Log Server 是將 Log 送到那台 device 的意思。 | **安裝介面 > AD Log Server > AD Log Server Installation**<br>  |
| **步驟 3 安裝完成**<br>安裝完成後會出現完成的訊息，點選確定即可。 | **安裝介面 > AD Log Server > AD Log Server Installation > Install completed**<br>  |
| **步驟 4 AD Log Server 設定**<br>點選確定後會出現 AD Log Server 的設定介面。<br>第 1 頁爲 Syslog Server，可以改變步驟 3 所設定的值，按 Save 儲存設定。<br><br>請注意：此 IP 設定的意思爲 AD Log Server 是將 Log 送到那台 device。如果此視窗已被關閉，使 | **Install completed > AD Log Server Setting** |

| | |
|---|---|
| 用者想再開啓時，可到安裝路徑(本範例)下的 C:\L7Networks_AD 下啓動 AD.exe 檔即可。 |  |
| **步驟 5 開啓 AD Manager 設定介面**<br>此功能爲選購功能，必須到本關網註冊選購，再到 Managerment 操作介面開啓即可使用(Update > License 輸入所得到的 License Key)。完成開啓後 Management 會出現 AD Manager 與 Encapsulation Manager 兩種選項。 |  |
| **步驟 6 AD Book Import**<br>點選 AD Book Import 則會跳出 Import 的窗口。 | **Functions > Management > IM Manager > IM User > AD Book Import**<br>  |
| **步驟 7 將 AD 帳號匯入**<br>點選想匯入的帳號與群組，點選 OK 後即可。 | **Functions > Management > IM Manager > IM User > AD Book Import** |

| | |
|---|---|
| 請注意:請先完成 13.3.1 的相關操作後,此視窗內才會出現 AD 帳號與群組。 |  |

**步驟 8 上傳檔案**

選擇 **Upload Configuration** 或點擊圖示  將設定檔上傳到裝置上。

⚠ **問題：**當 RD_1 爲 RD Group 的一員，但是此兩個帳號同時出現在 IM User 時，設定檔該以誰爲主?
**解答：**設定檔的比對規則 IM account > AD User > AD Group > Default User

### 13.3.4 從本地端檔案載入即時通訊使用者與其群組

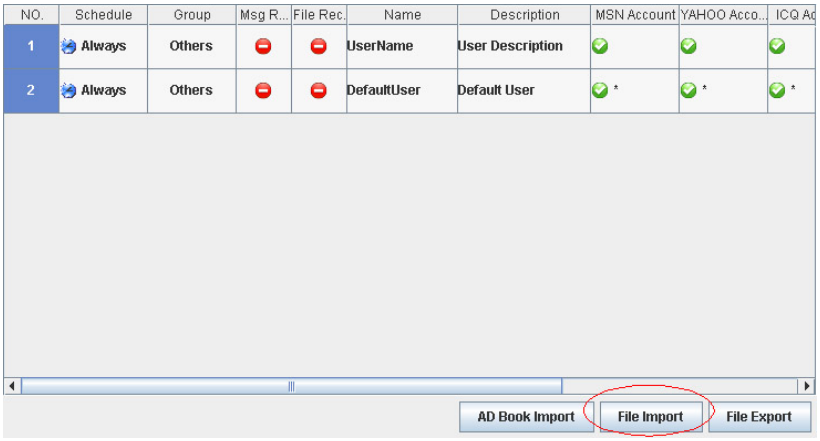
如果貴公司不支援 LDAP 匯入的方式,您可以將既有的資料庫按照即時通訊使用者的欄位排列方式將資料匯出並存成純文字檔，然後藉由檔案匯入的方式將即時通訊使用者的資料匯入。

| | |
|---|---|
| **步驟 1 可匯入的純文字檔**<br>您從既有的資料庫匯出的文字檔必需依據右圖的格式，欄位與欄位間要用逗號分開。請注意，名稱是主鍵，不可重複，所以在您透過檔案匯入使用者資料前，請檢查資料是否有重複、欄位是否符合要匯入的目標欄位。 | **Functions > Management > IM Manager > IM User > File Import**<br>`ceo, boss, ceo@yourCompany.com, ceo@hotmail.com, ceo1111`<br>`cto, boss, cto@yourCompany.com, cto@hotmail.com, cto1010` |

**步驟 2 匯入檔案資料**

點擊 File Import 繼續。

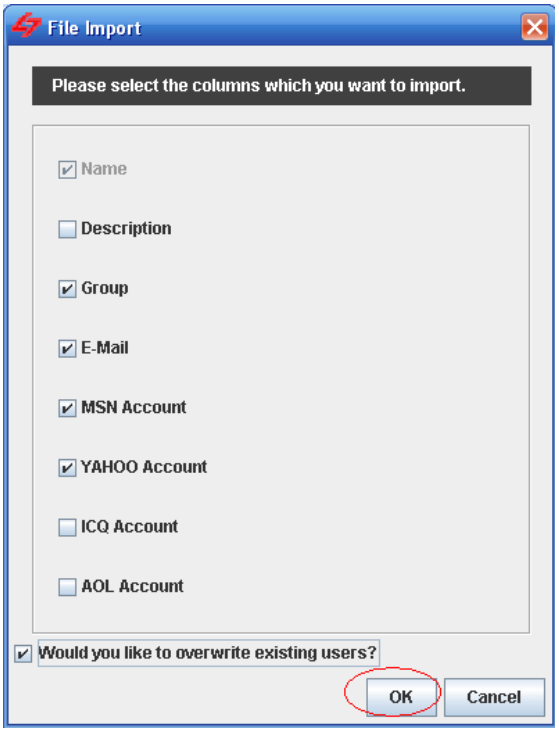
**Functions > Management > IM Manager > IM User > File Import**




**步驟 3 選擇要匯入的欄位**

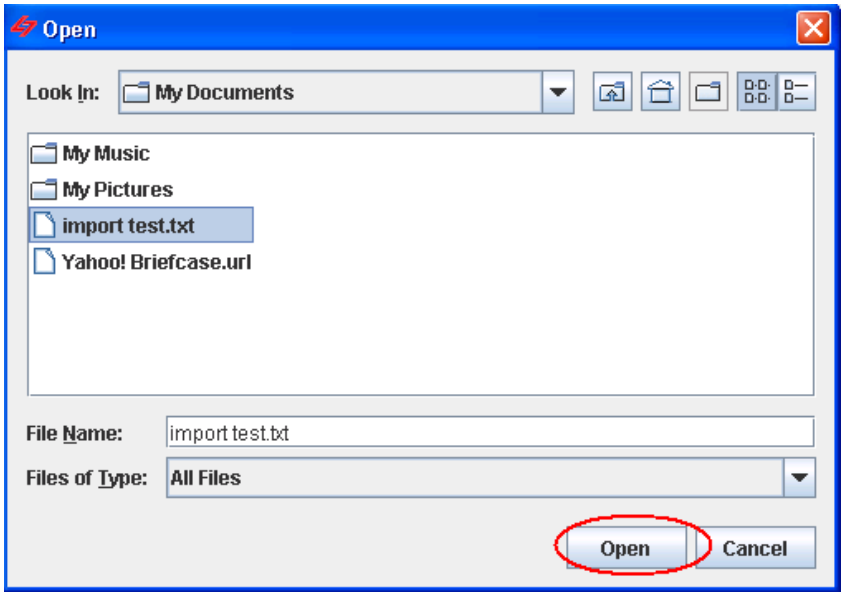
勾選 Group、E-Mail、MSN Account、Yahoo Account，然後勾選 **Would you like to overwrite existing users?** 覆寫已存在的使用者，點擊 **OK** 進入下一個視窗。

**Functions > Management > IM Manager > IM User > File Import**



**步驟 4 選擇要匯入的檔案**

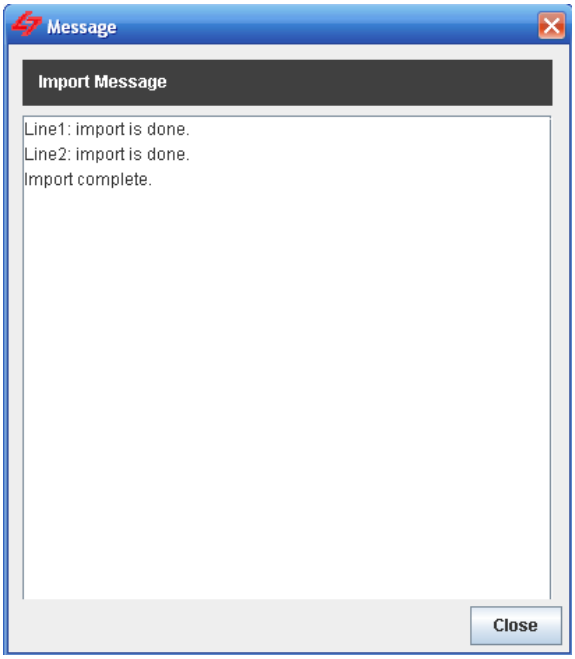
選擇您要匯入的文字檔，然後點擊 **Open** 開始匯入動作。




**步驟 5 匯入成功**

當檔案匯入資料成功後，系統將會顯示如右圖的訊息告訴您匯入成功。點擊 **Close** 完成設定。

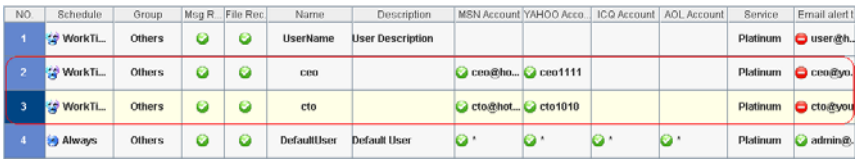
**Functions > Management > IM Manager > IM User > File Import**




**步驟 6 顯示檔案匯入的結果**

當匯入資料後，您可以在本頁檢視匯入結果。請注意，匯入的資料其設定都是預設值，網管人員必須視情況調整每位元即時通訊使用者的規則。

**Functions > Management > IM Manager > IM User**




**步驟 7 上傳設定檔**

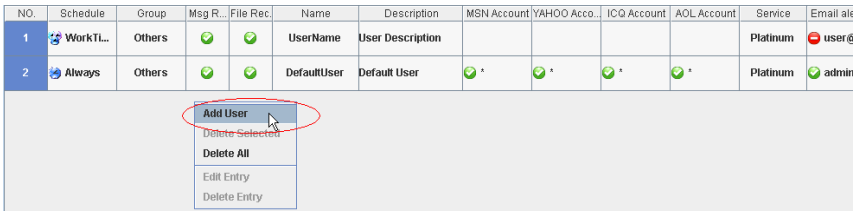
選擇 **Upload Configuration** 或點擊圖示  將設定檔上傳到裝置上。

## 13.3.5 手動編輯即時通訊使用者

**步驟 1 新增即時通訊使用者**

在 IM User 視窗上按右鍵，然後選擇 Add User。

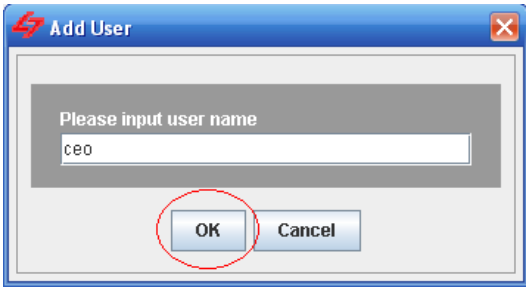
**Functions > Management > IM Manager > IM User**




**步驟 2 輸入使用者名稱**

輸入即時通訊使用者的規則名稱。點擊 **OK** 關閉窗口。

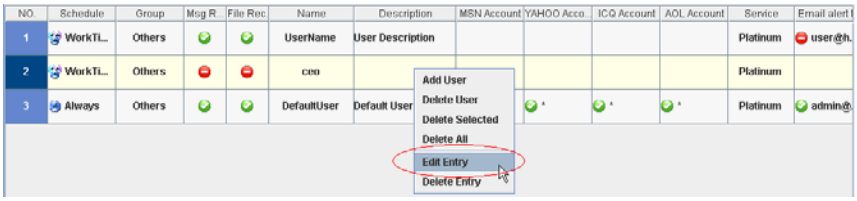
**Functions > Management > IM Manager > IM User**




**步驟 3 編輯使用者描述**

在 Description 欄位上按右鍵，然後選擇 **Edit Entry**。

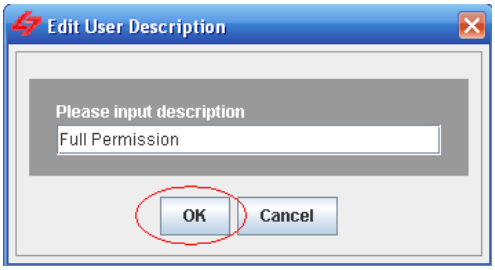
**Functions > Management > IM Manager > IM User**




**步驟 4 輸入描述欄位內容**

輸入針對此使用者的描述內容。點擊 **OK** 結束窗口。

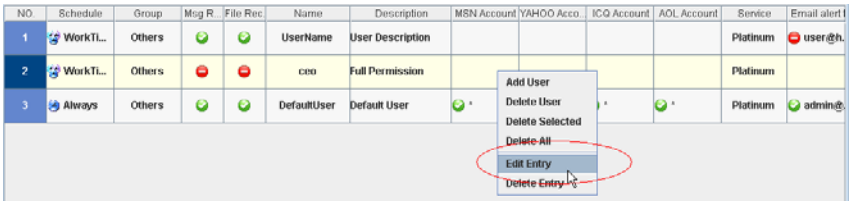
**Functions > Management > IM Manager > IM User**




**步驟 5 編輯使用者的即時通訊帳號**

在 MSN Account 欄位上按右鍵，然後選擇 **Edit Entry**。

**Functions > Management > IM Manager > IM User**

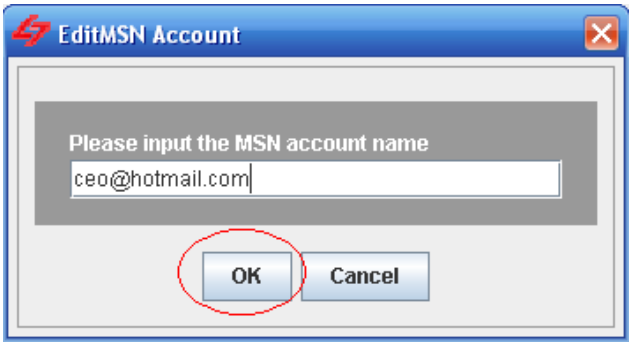


**步驟 6 輸入使用者的即時通訊帳號**

在 Account 欄位內輸入此使用者的 MSN 帳號。

其餘即時通訊帳號設定步驟同 MSN 帳號。

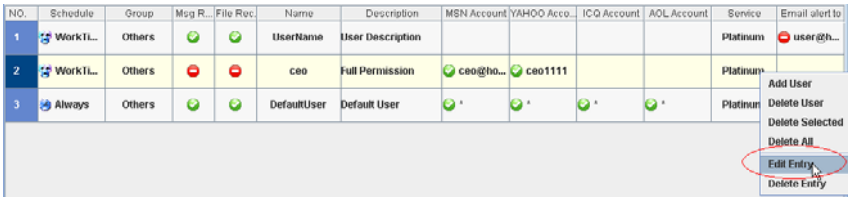
**Functions > Management > IM Manager > IM User**




**步驟 7 編輯警告信件信箱**

在 Eamil alert to 欄位上按右鍵，然後選擇 Edit Entry。

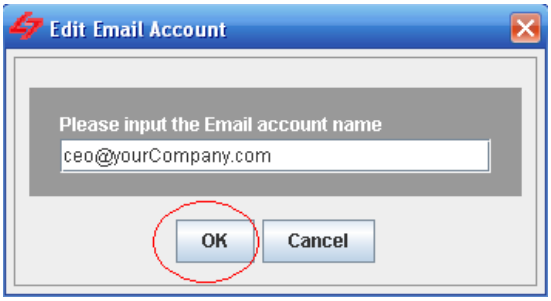
**Functions > Management > IM Manager > IM User**




**步驟 8 輸入電子郵件信箱**

輸入要接收警告信件的電子郵件信箱。當您設定好此郵件信箱，並啓用設定後，當此使用者違反政策規則時，系統將會寄送警告信件給此使用者。

**Functions > Management > IM Manager > IM User**




**步驟 9 檢視已編輯好的即時通訊使用者**

新增加的即時通訊使用者的設定都是預設值，網管人員必須視情況調整每位元即時通訊使用者的規則。

**Functions > Management > IM Manager > IM User**


**步驟 10 上傳設定檔**

選擇 **Upload Configuration** 或點擊圖示 將設定檔上傳到裝置上。

Email alert to 的欄位是讓管理者可以設定是否要讓使用者在其違反政策規則時收到警告信件，瞭解自己是觸犯哪條政策規則。如果管理者允許使用者使用即時通訊，也就是說即時通訊帳號是啓用的狀態 ，請詳見下表的規則：

| 圖示 | 欄位 | 說明 |
|---|---|---|
| | Email alert to | 當使用者違反即時通訊政策時，將收到警告信件。 |
| | Email alert to | 當使用者違反即時通訊政策時，將不會收到警告信件。 |

表格 13-1 即時通訊政策允許使用即時通訊軟體

如果管理者不允許使用者使用即時通訊，也就是說即時通訊帳號是未啓用的狀態 ，請詳見下表的規則：

| 圖示 | 欄位 | 說明 |
|---|---|---|
| | Email alert to | 當即時通訊使用者企圖使用即時通訊行爲，將會收到警告信件。 |
| | Email alert to | 即時通訊使用者將不會收到任何即時通訊警告信件。 |

表格 13-2 即時通訊政策不允許使即時通訊軟體

| 欄位 | 說明 | 範圍/格式 | 範例 |
|---|---|---|---|
| No | 即時通訊使用者的編號。數字越小代表優先權越高。因其爲由上到下的比對法。 | 數字 | 2 |
| Schedule | 啓用或取消即時通訊使用者政策規則的時間。 | Always / Never / 使用者定義 | Always |
| Group | 使用者定義的即時通訊使用者群組。 | 使用者定義 | boss |
| Msg Rec. | 即時通訊訊息側錄器。當您開啓時，所有即時通訊訊息都會被側錄。 | （啓用）/ （取消） | |
| File Rec. | 即時通訊檔案側錄器。當您開啓時，所有即時通訊檔案都會被側錄。 | （啓用）/ （取消） | |
| Name | 即時通訊使用者規則名稱。 | 使用者定義 | ceo |
| Description | 即時通訊使用者的描述。 | 使用者定義 | Full permission |
| MSN account | MSN 帳號。 | MSN 帳號格式 | ceo@hotmail.com |
| YAHOO account | Yahoo 帳號。 | Yahoo 帳號格式 | ceo1111 |
| ICQ account | ICQ 帳號。 | ICQ 帳號格式 | -- |
| AOL account | AOL 帳號。 | AOL 帳號格式 | -- |
| Service | 即時通訊使用行爲許可權。 | 使用者定義 | Platinum |
| Email alert to | 當即時通訊違反政策規則時，可接收警告信件的帳號。 | 電子郵件帳號格式 | ceo@abc.com |

表格 13-3 即時通訊使用者欄位說明

### 13.3.6 自動學習即時通訊用戶名單

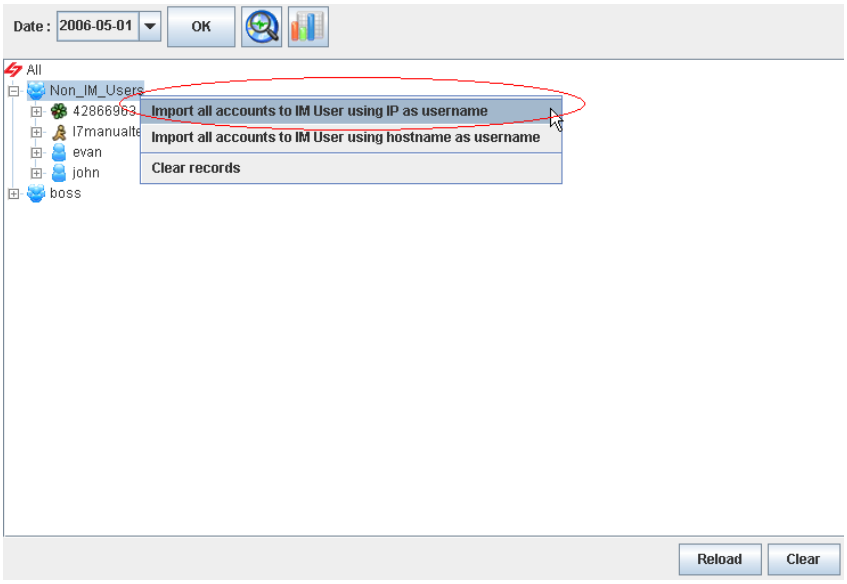
爲了讓管理者能夠快速設定使用者的即時通訊帳號，設定了即時通訊帳號自動學習的功能。管理者只要利用即時通訊記錄器上側錄到的帳號，即可按右鍵選擇帳號匯入的方式即可。詳細設定，請參照下表說明。

**步驟 1 匯入所有使用者**

在 Non_IM_Users （非 IM Users 清單上的帳號）上按右鍵，選擇您要將即時通訊帳號匯入的方式。

**注意**，已經加入的群組或即時通訊使用者就不可以再次匯入帳號了。也就是說，當您將 Non_IM_Users 的帳號匯入 IM Users 清單內，則系統將會自動將該帳號顯示為 IM Users 上所設定的名稱。記錄器上所顯示的樹狀圖，第一層為群組、第二層為 IS 內部的即時通訊帳號、第三層為該帳號與其他帳號之間的通訊記錄。

**Functions > Auditor > IM Recorder**




| 欄位 | 說明 |
|---|---|
| Import all accounts to IM User using IP as username | 將所有已記錄的帳號匯入即時通訊使用者中，並以其傳送/接收訊息者的 IP 為用戶名稱。 |
| Import all accounts to IM User using hostname as username | 將所有已記錄的帳號匯入即時通訊使用者中，並以其傳送/接收訊息者的主機名稱為用戶名稱。 |
| Clear records | 清除所有通訊記錄。 |

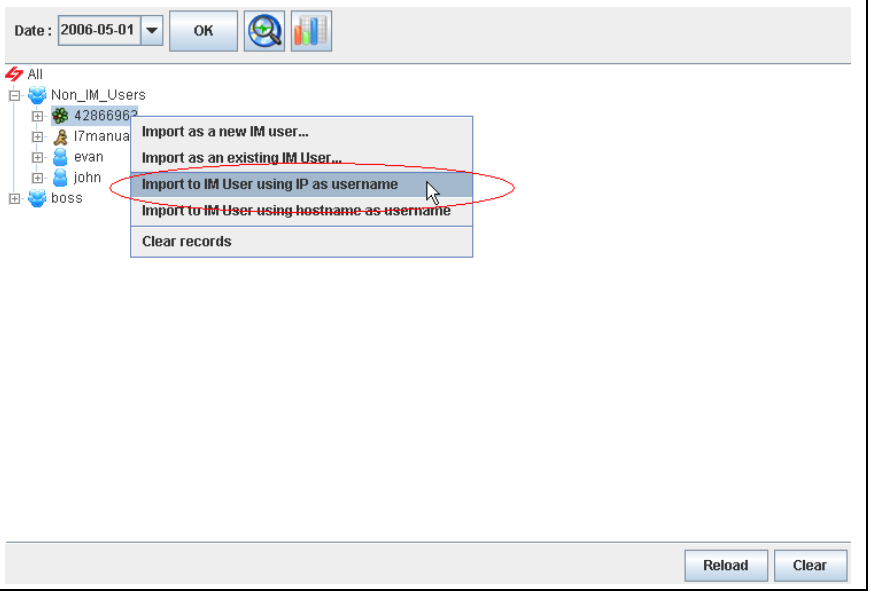
表格 13-1 自動帳號學習 - 匯入所有非即時通訊使用者清單上的帳號

**步驟 2 匯入選定的使用者**

除了將所有帳號匯入外，您也可以選定帳號匯入。

在 Non_IM_Users 群組下，選擇您要匯入的帳號，然後在此帳號上按右鍵，選擇您要將帳號匯入的方式。相關說明請參考表格介紹。

**Functions > Auditor > IM Recorder**




| Field | Description | Example |
|---|---|---|
| Import as a new IM user | 將選定的即時通訊帳號，以新增一筆新規則的 | 4286963 |

| | | |
|---|---|---|
| | 方式匯入即時通訊使用者清單內。 | |
| Import as an existing IM User | 將選定的即時通訊帳號，匯入已存在的即時通訊使用者清單內。 | Evan |
| Import to IM User using IP as username | 將選定的即時通訊帳號，依其 IP 位址命名匯入即時通訊使用者清單內。 | 192.168.168.10 |
| Import to IM User using hostname as username | 將選定的即時訊帳號，依其主機名稱匯入即時通訊使用者清單內。 | ABC-Evan |
| Clear records | 清除選定帳號的所有記錄。 | -- |

表格 13-2 自動帳號學習 - 匯入選定的非即時通訊使用者清單上的帳號

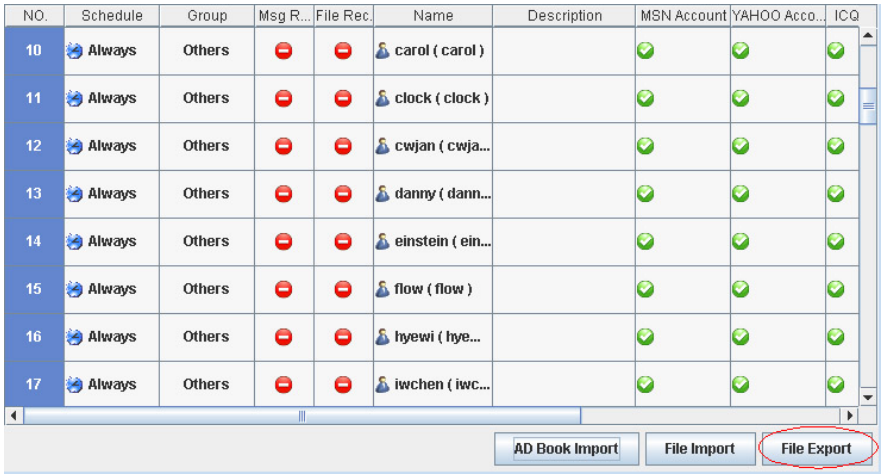
### 13.3.7 從本地端檔案匯出即時通訊使用者與其群組

爲了避免不可預期的因素，造成已設定好的即時通訊使用者設定檔損毀，您可隨時將即時通訊使用者匯出成檔案儲存，以備不時之需。

**步驟 1 檔案匯出**

點擊 File Export 匯出即時通訊使用者資料。

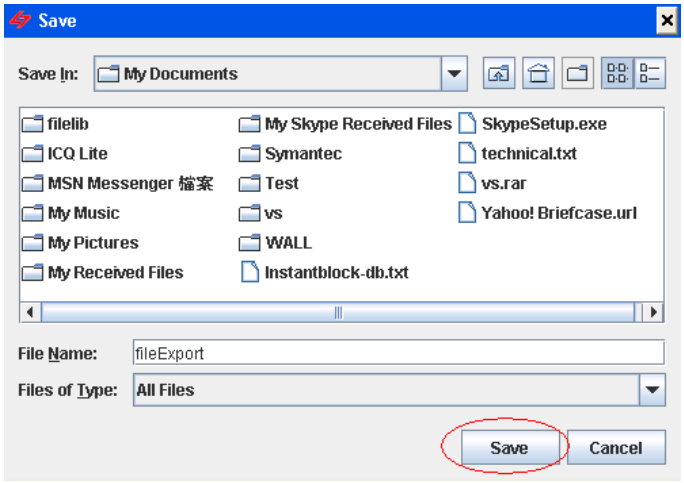
**Functions > Management > IM Manager > IM User > File Export**

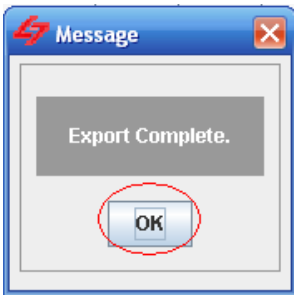



**步驟 2 輸入要儲存的檔案**

在 File Name 欄位內輸入要儲存的檔案，然後點擊 Save 儲存。

**Functions > Management > IM Manager > IM User > File Export**



| | |
|---|---|
| **步驟 3 匯出完成**<br>當檔案匯出成功後，將有如右圖的訊息告知您。請點擊 **OK** 結束設定。 | **Functions > Management > IM Manager > IM User > File Export**<br>  |

### 13.3.8 即時通訊使用者設定輔助工具列

爲了加速即時通訊使用者的設定，InstantScan 提供下列設定輔助工具列： **1） 列舉（List）**選定的專案。所有選定的群組/服務將被列舉在螢幕上。**2） 套用（Apply）**選定的專案到列舉的即時通訊使用者清單中。


| 欄位 | | 說明 | 範圍 / 格式 | 範例 |
|---|---|---|---|---|
| List ① | Group | 列舉選定的群組在即時通訊使用者清單上。 | 使用者定義的群組 | Boss |
| | Service | 列舉選定的服務在即時通訊使用者清單上。 | 使用者定義的服務 | -- |
| Apply ____ to listed. ② | Schedule | 套用選定的排程到列舉的即時通訊使用者清單上。 | 使用者定義的排程 | Always |
| | Msg Rec. | 套用選定的訊息側錄規則到列舉的即時通訊使用者清單上。 | （啓用） / （取消） | |
| | File Rec. | 套用選定的檔案側錄規則到列舉的即時通訊使用者清單上。 | （啓用） / （取消） | |
| | MSN | 套用選定的 MSN 規則到列舉的即時通訊使用者清單上。 | Block/Allow | Allow |
| | YAHOO | 套用選定的 Yahoo 規則到列舉的即時通訊使用者清單上。 | Block/Allow | Allow |
| | AOL | 套用選定的 AOL 規則到列舉的即時通訊使用者清單上。 | Block/Allow | Allow |
| | ICQ | 套用選定的 ICQ 規則到列舉的即時通訊使用者清單上。 | Block/Allow | Allow |
| | Service | 套用選定的服務規則到列舉的即時通訊使用 | 使用者定義的服務 | Platinum |
| Search | | 此搜尋功能讓您利用關鍵字快速尋找特定的規則。 | | |

表格 13-4 即時通訊使用者輔助設定工具列

# 第14章
# 管理即時通訊使用者

## 14.1 需求

1. 爲了設定的方便，需要調整新增即時通訊使用者的預設值。
2. 在上班時間，員工只可以使用 MSN，且需要被側錄存證，其餘即時通訊軟體一率禁止。當員工使用某些即時通訊軟體被阻檔時，需要知道其違反了哪項政策規則。
3. 因工作性質關係，研發部 RD 在上班時間不准與公司外的人員聊天。
4. 所有傳送的即時通訊訊息與檔案都需要作內容過濾，避免員工利用即時通訊的便利在上班時間聊工作之外的事情與傳送不必要的檔案，浪費公司網路頻寬。
5. 所有傳送接收的檔案都需要掃毒，以保護公司內部的電腦。
6. 因爲管理部門的 CEO 與 CTO 有特殊的需求，所以不列入即時通訊管理員控管的範圍。

## 14.2 方法

1. 在 Functions > Management > IM Manager > Status > New IM User Setting 頁面上設定新增加的即時通訊使用者預設值。
2. 在 Functions > Management > IM Manager > IM Users 頁面設定即時通訊使用者的政策。
3. 在 Functions > Management > IM Manager > IM Peers 頁面設定 RD 群組不可以與 Non_IM_User 聊天。
4. 在 Functions > Management > IM Manager > IM Contents 頁面設定要過濾的訊息與檔案，並啓用設定。
5. 在 Functions > Management > IM Manager > IM Security 頁面啓用防毒與防蠕蟲功能。
6. 在 Functions > Management > IM Manager > Exempt Sources 頁面設定，Boss（CEO/CTO）的連線都避開即時通訊管理員的控管。

## 14.3 步驟

### 14.3.1 新增的即時通訊使用者預設值

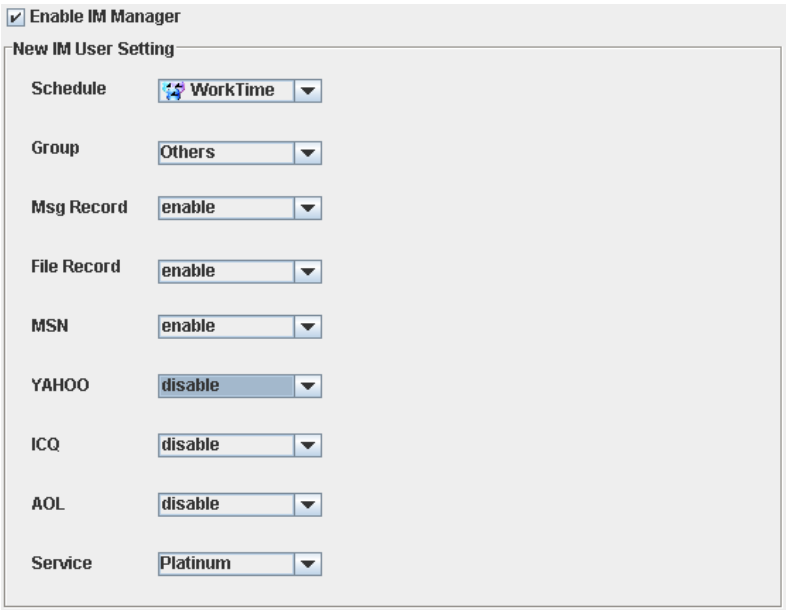
**步驟 1 調整即時通訊使用者預設值**

爲了配合即時通訊使用者的政策，所以調整 New IM User 的設定值爲：

Schedule: WorkTime
Group: Others
Msg Record: enable
File Record: enable
MSN: enable
YAHOO: disable
ICQ: disable
AOL: disable
Service: Platinum

當您設定好此預設值後，往後增加的即時通訊使用者都會套用此設定。

**Functions > Management > IM Manager > Status**

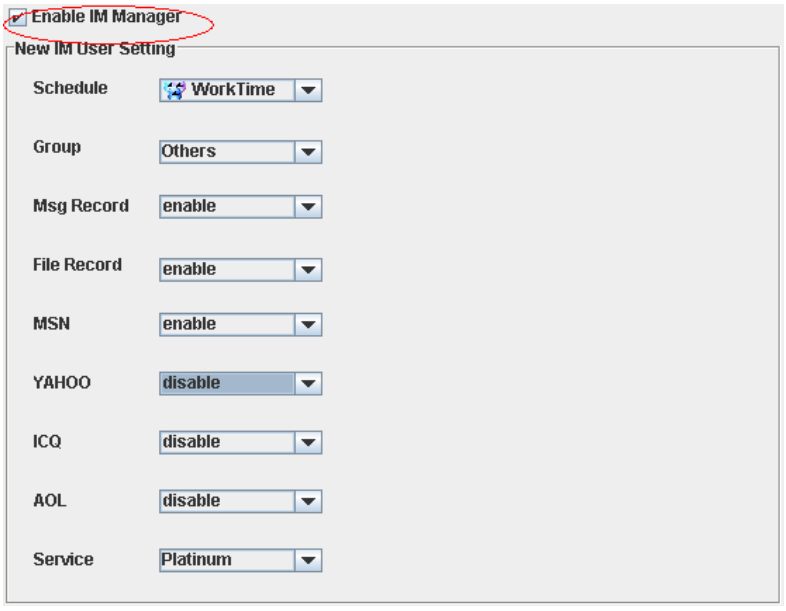



## 14.3.2 即時通訊使用者管理

**步驟 1 啓用即時通訊管理員**

勾選 **Enable IM Manager**。

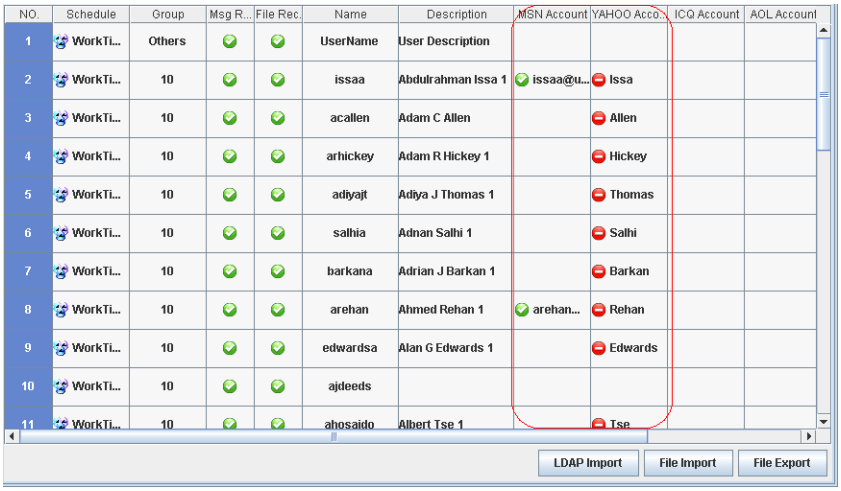
**Functions > Management > IM Manager > Status**



**步驟 2 允許使用 MSN，攔阻其他即時通訊**

移動滑鼠在 MSN Account 上點一下，讓圖示呈現 （允許），然後讓其他即時通訊軟體的圖示呈現 （攔阻）。您亦可藉由 IM Users 視窗上的工具列，快速設定即時通訊使用者的政策。

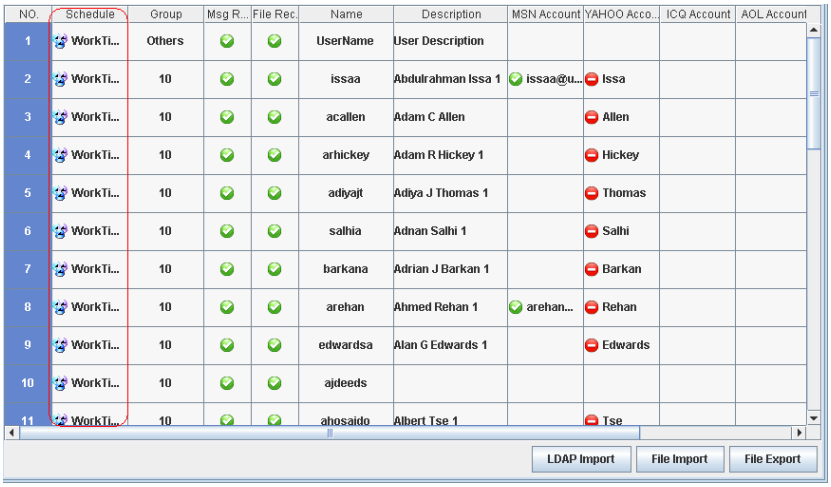
**Functions > Management > IM Manager > IM Users**




**步驟 3 設定排程爲 WorkTime**

在前面的章節，我們已經介紹您如何設定 Schedule 了。請在 Schedule 欄位上拉選 WorkTime。您亦可以利用 <ctrl> + 滑鼠選擇/取消您要套用的即時通訊使用者，然後在工具列上選擇 Apply “WorkTime” to listed。

**Functions > Management > IM Manager > IM Users**

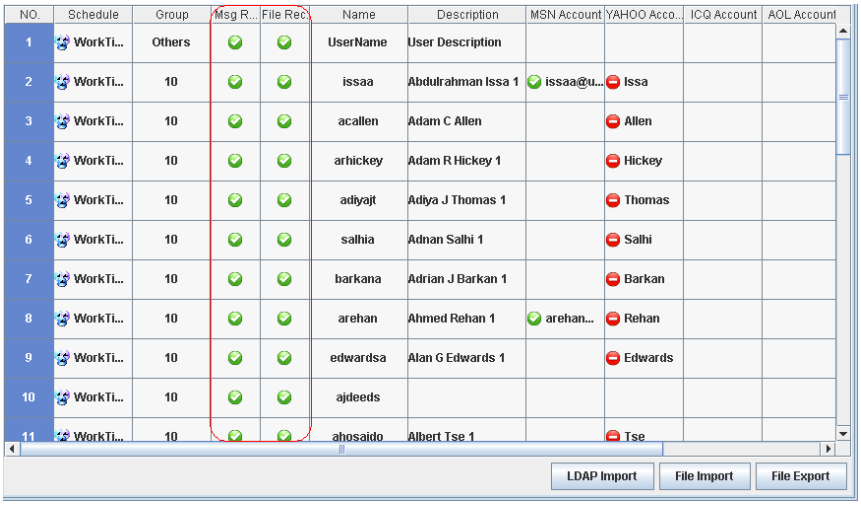



**步驟 4 開啓訊息/檔案側錄功能**

移動滑鼠在 Msg Rec. 欄位上點一下 開啓訊息側錄與在 File Rec. 欄位上點一下 開啓檔案側錄。然後在 Email alert to 欄位上點一下 開啓郵寄警告信件的服務。

**注意**：您也可以藉由 IM Users 視窗上的工具列，快速設定即時通訊使用者政策。

**Functions > Management > IM Manager > IM Users**




**步驟 5 上傳設定檔**

選擇 **Upload Configuration** 或點擊圖示 將設定檔上傳到裝置上。

### 14.3.3 即時通訊聊天物件管理

**步驟 1 新增即時通訊聊天物件規則**

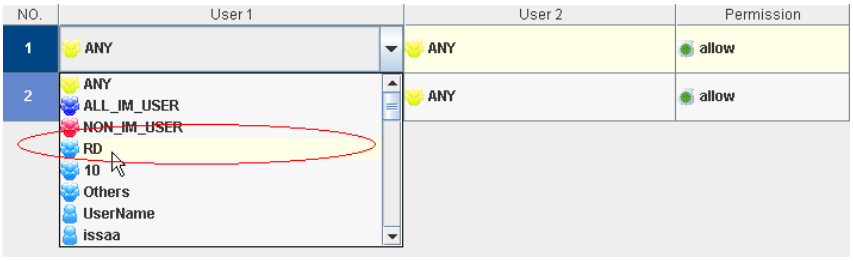
將滑鼠移到 IM Peer 的螢幕上按右鍵，點選 Add Peer。

**Functions > Management > IM Manager > IM Peer**


**步驟 2 選擇 User1**

在 User 1 欄位上選擇 RD。

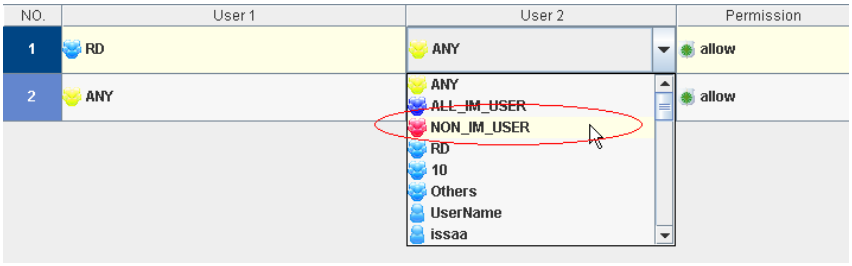
**Functions > Management > IM Manager > IM Peer**




**步驟 3 選擇 User2**

在 User2 欄位上選擇 NON_IM_USER。

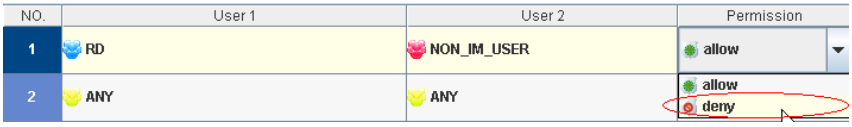
**Functions > Management > IM Manager > IM Peer**




**步驟 4 攔阻 RD 與 NON_IM_User間的對話**

在 Permission 欄位上選擇 deny。

**Functions > Management > IM Manager > IM Peer**



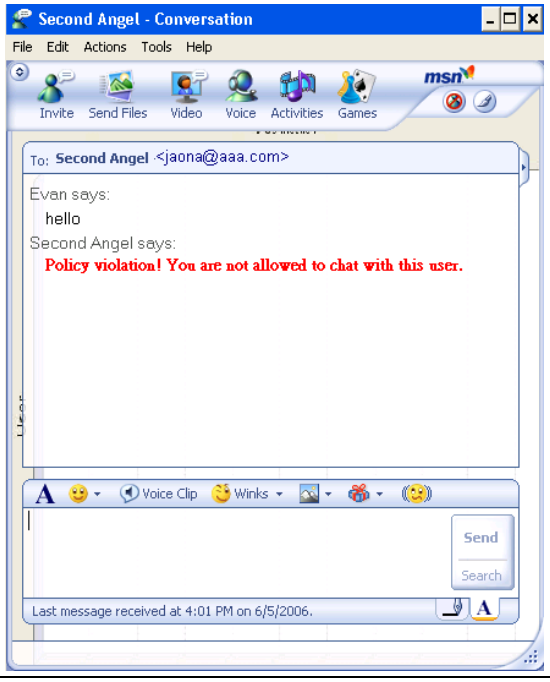

**步驟 5 檢視新增的即時通訊聊天物件規則**

檢視已新增的聊天物件規則。

**Functions > Management > IM Manager > IM Peer**

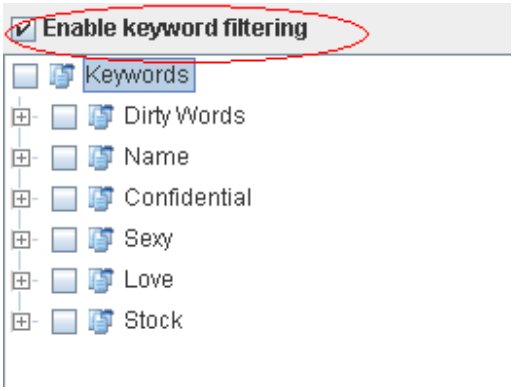

**步驟 6 上傳設定檔**

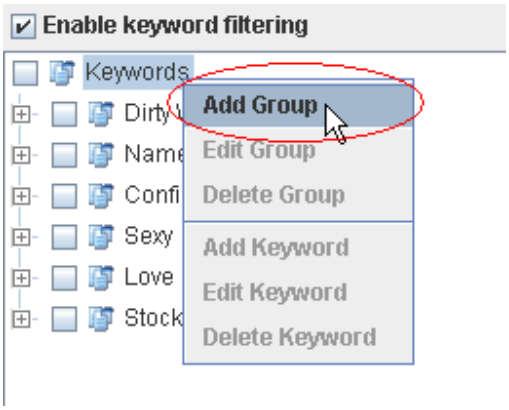
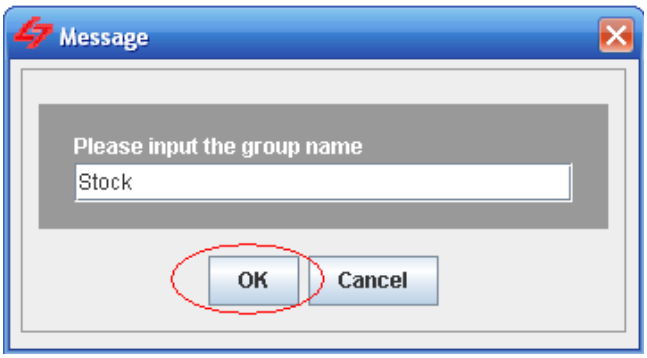
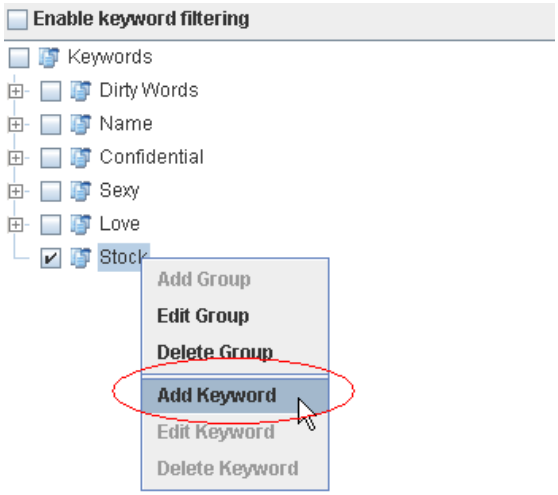
選擇 **Upload Configuration** 或點擊圖示 將設定檔上傳到裝置上。

| | |
|---|---|
| **步驟 7 違反聊天物件警告訊息**<br>當屬於 RD 部門的 Evan 企圖與非公司內部員工且已列舉在 IM Users 清單上的使用者聊天時，InstantScan 將攔阻他們之間的對話，且在即時通訊視窗顯示如右圖的警告。 |  |

## 14.3.4 即時通訊內容過濾

### 14.3.4.1 關鍵字過濾

| | |
|---|---|
| **步驟 1 啓用關鍵字過濾**<br>勾選 **Enable keyword filtering**。 | **Functions > Management > IM Manager > IM Contents > Chat**<br>  |

| | |
|---|---|
| **步驟 2 新增關鍵字**<br>將滑鼠移到 IM Contents > Chat 的螢幕上按右鍵，點選 **Add Group**。 | **Functions > Management > IM Manager > IM Contents > Chat**<br>  |
| **步驟 3 輸入關鍵字組名**<br>輸入關鍵字組名，然後點擊**確定**繼續。 | **Functions > Management > IM Manager > IM Contents > Chat**<br>  |
| **步驟 4 新增關鍵字**<br>在剛剛新增的群組上按右鍵，然後點選 Add Keyword。 | **Functions > Management > IM Manager > IM Contents > Chat**<br>  |

**步驟 5 輸入關鍵字**

輸入需要內容過濾的關鍵字。

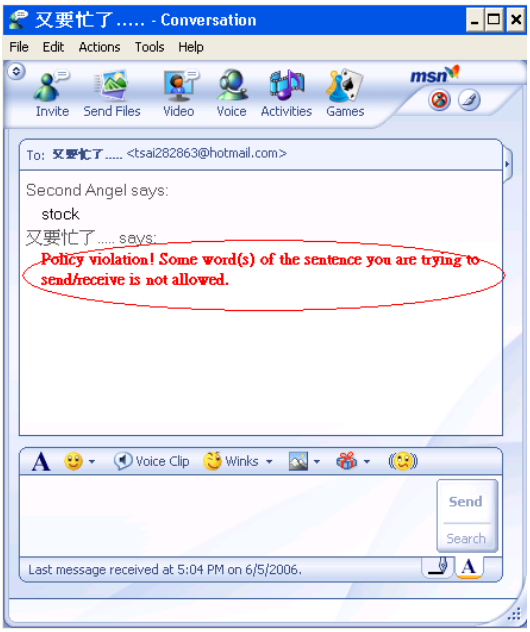
**Functions > Management > IM Manager > IM Contents > Chat**


**步驟 6 上傳設定檔**

選擇 **Upload Configuration** 或點擊圖示 將設定檔上傳到裝置上。

**步驟 7 違反聊天關鍵字過濾警告訊息**

當使用者違反聊天關鍵字時，將如右圖在即時通訊視窗內出現警告訊息。

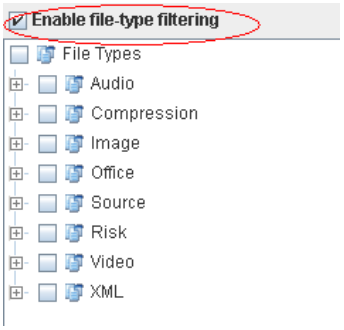


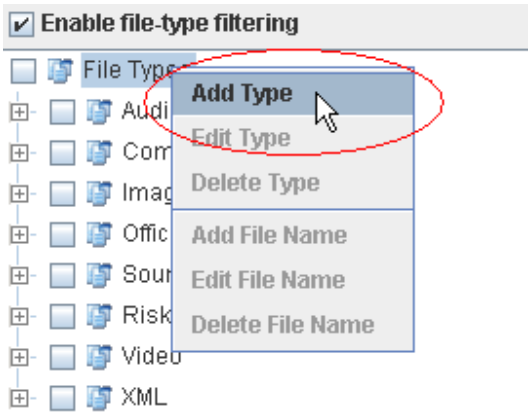
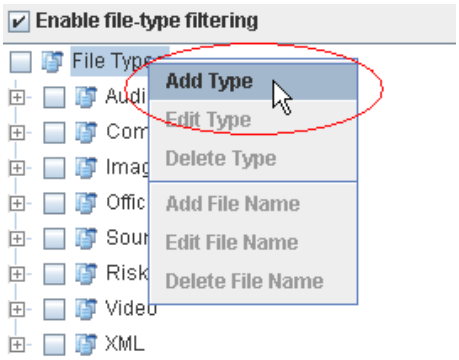
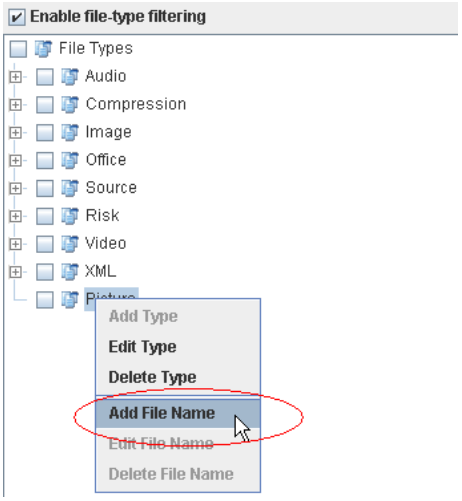

### 14.3.4.2 檔案類型過濾

**步驟 1 啓用檔案類型過濾**

勾選 **Enable file-type filtering**。

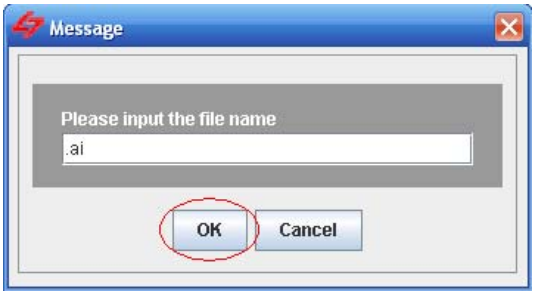
**Functions > Management > IM Manager > IM Contents > File**



| | |
|---|---|
| **步驟 2 新增檔案類型**<br>將滑鼠移到 IM Contents > File 的螢幕上按右鍵，點選 **Add Type**。 | **Functions > Management > IM Manager > IM Contents > File**<br>  |
| **步驟 3 輸入檔案類型**<br>輸入檔案類型，然後點擊**確定**繼續。 | **Functions > Management > IM Manager > IM Contents > File**<br>  |
| **步驟 4 新增檔案名**<br>在剛剛新增的檔案類型上按右鍵，然後點選 Add File Name。 | **Functions > Management > IM Manager > IM Contents > File**<br>  |

**步驟 5 輸入檔案名**

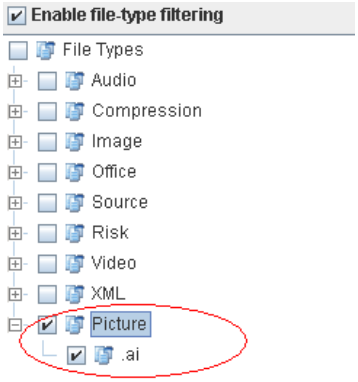
在此您可以輸入副檔名如 .ai，系統將會過濾所有 .ai 類型的檔案。




**步驟 6 啓用檔案類型過濾**

勾選 **Enable file-type filtering**，並勾選剛剛新增的檔案類型。

**Functions > Management > IM Manager > IM Contents > File**

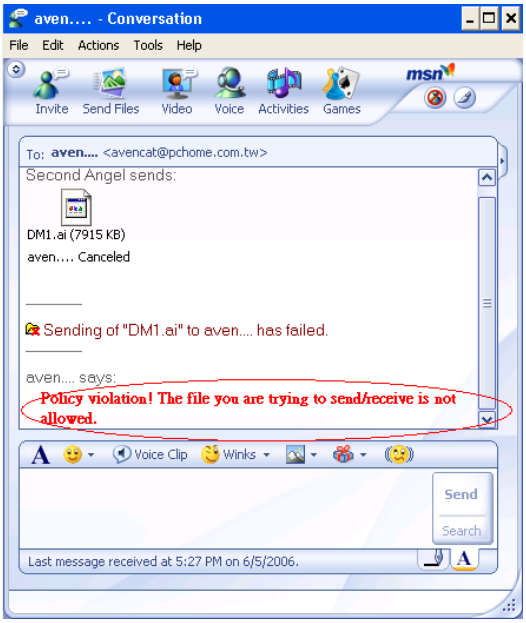



**步驟 7 上傳設定檔**

選擇 **Upload Configuration** 或點擊圖示  將設定檔上傳到裝置上。

**步驟 8 違反檔案類型過濾警告訊息**

當使用者違反檔案類型過濾時，將如右圖在即時通訊視窗內出現警告訊息。



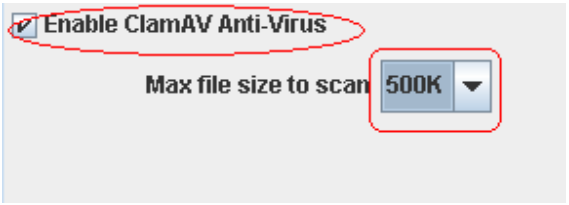
## 14.3.5 即時通訊安全防護

### 14.3.5.1 防毒（Anti-Virus）

**步驟 1 啓用 ClamAV 防毒**

勾選 **Enable ClamAV Anti-Virus**，然後選擇您希望 InstantScan 掃描的最大檔案大小。例如 500K，當傳送的檔案大小是 500K 以下才掃毒，超過 500K的檔案一律放行。

**Functions > Management > IM Manager > IM Security > Anti-Virus**

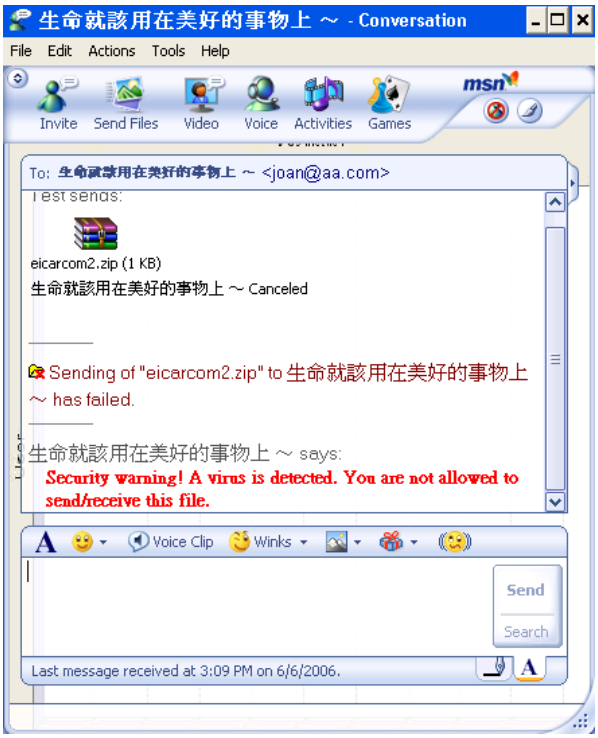



**步驟 2 上傳設定檔**

選擇 **Upload Configuration** 或點擊圖示 將設定檔上傳到裝置上。

**步驟 3 傳送/接收的檔案含有病毒的警告訊息**

當使用者傳送/接收的檔案含有病毒時，在您或聊天物件接收檔案後，系統將會在即時通訊視窗內傳送警告訊息告知 InstantScan 內部的使用者。

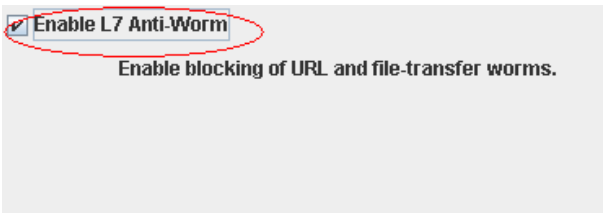



### 14.3.5.2 防蠕蟲（Anti-Worm）

**步驟 1 啓用第七層防蠕蟲**

勾選 **Enable L7 Anti-Worm**。

**Functions > Management > IM Manager > IM Security > Anti-Worm**

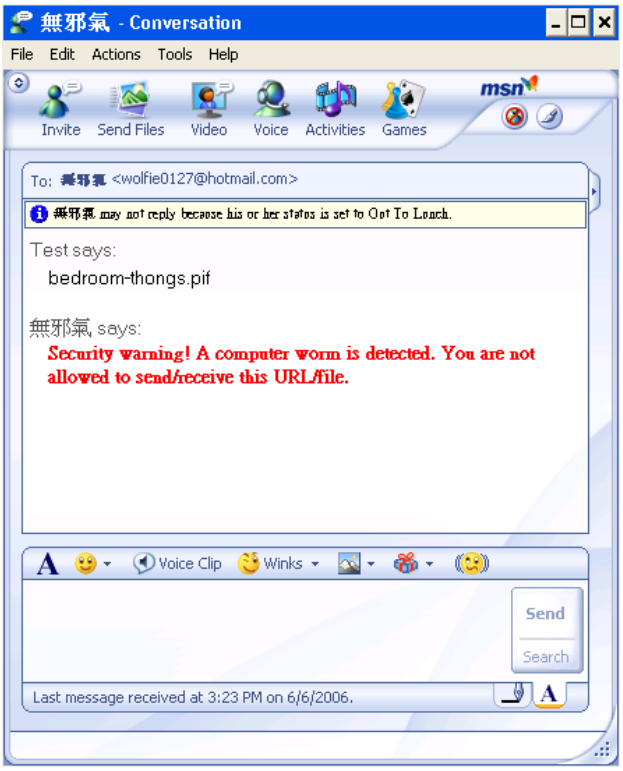



**步驟 2 上傳設定檔**

選擇 **Upload Configuration** 或點擊圖示 將設定檔上傳到裝置上。

**步驟 3 傳送/接收的URL/檔案含有病毒的警告訊息**

當使用者傳送/接收的URL/檔案含有電腦蠕蟲時，系統將會在即時通訊視窗內傳送警告訊息告知 InstantScan 內部的使用者。

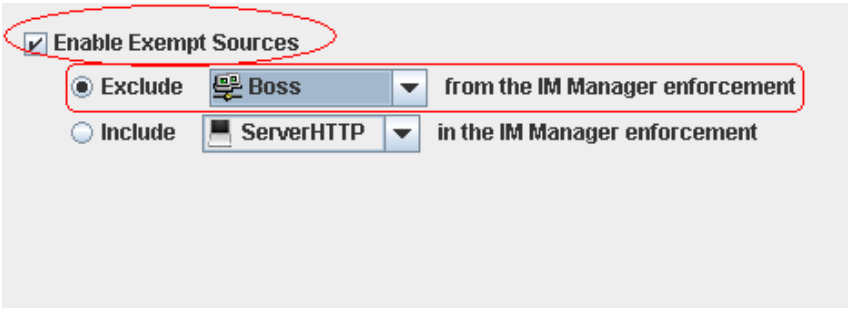



## 14.3.6 除外來源端設定

**步驟 1 啓用除外來源端**

勾選 **Enable Exempt Sources**，然後選擇 **Exclude Boss from the IM Manager enforcement**。在上面的章節我們已提過 Boss（包含 CEO 與 CTO）有完整的許可權存取網際網路，所以將其列入除外來源，避開即時通訊管理員的控管。

**Functions > Management > IM Manager > Exempt Source**




**步驟 2 上傳設定檔**

選擇 **Upload Configuration** 或點擊圖示  將設定檔上傳到裝置上。

| 欄位 | 說明 | 範圍 / 格式 | 範例 |
|---|---|---|---|
| Enable Exempt Sources | 啓用除外來源功能。 | 啓用 / 不啓用 | 啓用 |
| Exclude ____ from IM Manager enforcement | 所列舉的 IP 位址除外，其餘的電腦皆強制執行即時通訊管理政策。 | 所有 Object 地址/群組列表 | Boss |
| Include ___ in IM Manager enforcement | 即時通訊管理政策只適用於所列舉的電腦。 | 所有 Object 地址/群組列表 | -- |

表格 14-1 除外來源端欄位解釋

# 第15章
# LDAP (ActiveDirctory) Import 設定範例

LDAP 代表 Lightweight Directory Access Protocol（輕量目錄存取協定）。在 LDAP 的協定之中，很像硬碟目錄結構或倒過來的樹狀結構。LDAP 的根就是全世界，第一級是屬於國別（countries）性質的層級，之後可能會有公司（organization）的層級，接著是部門（organizationalUnit），再來爲個人。而就像個人檔案，每個人都會有所謂的顯名（distinguished name，簡稱 dn），dn 可能類似 cn=John Smith,ou=Accounts,dc=myCompany,dc=tw。

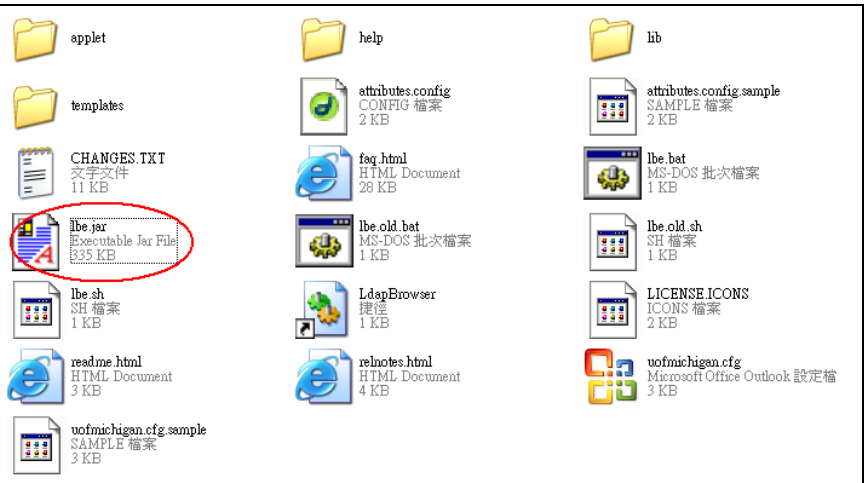
針對 LDAP Import 這個功能，因其本身的複雜性，所以有許多使用者可能不甚瞭解如何設定。在此，我們提供詳盡的設定範例，希望提供使用者設定時的參考。

在使用 LDAP Import 這個功能之前，要先確認您現在用來操作使用者介面的電腦是否可以透過 LDAP 這個 Protocol，連線到貴公司的 LDAP 伺服器（例如：ActiveDirectory、OpenLDAP 等）。建議您先用一套 LDAP Browser 的軟體來測試是否可以連線到 LDAP 伺服器上，您可以在 http://www-unix.mcs.anl.gov/~gawor/ldap/ 這裡找到這套軟體以及更多 LDAP 相關資訊。以下的範例爲我們在上列網站上下載 Browser282b2.zip，解壓縮後執行。

## 15.1 設定 LDAP Browser 軟體

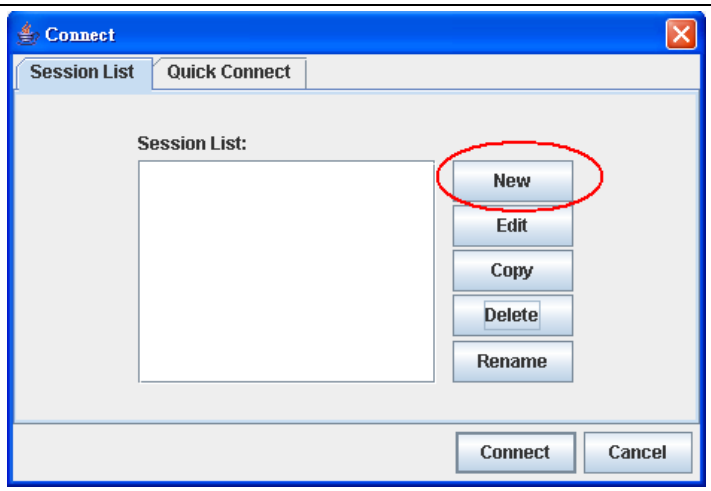
**步驟 1 開啓 LDAP Browser 軟體**

將滑鼠移到 lbe.jar 檔案上點兩下。



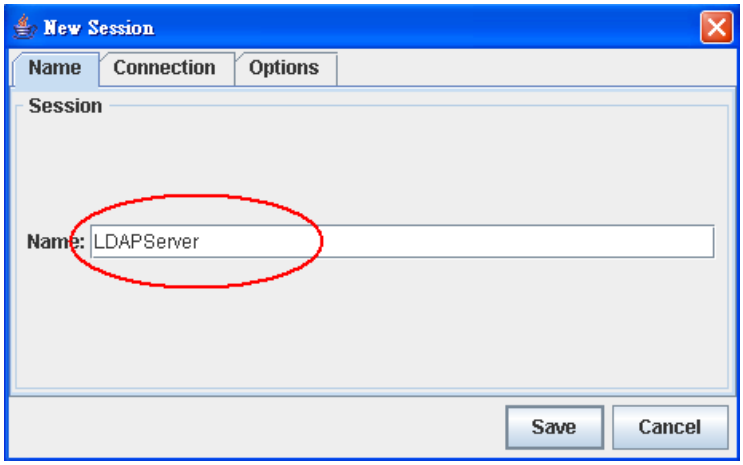

**步驟 2 啓用 LDAP Browser 軟體**

啓動 LDAP Browser 的軟體後，您可以看到如右圖的畫面，點擊 New 建立新的連線（Session）。



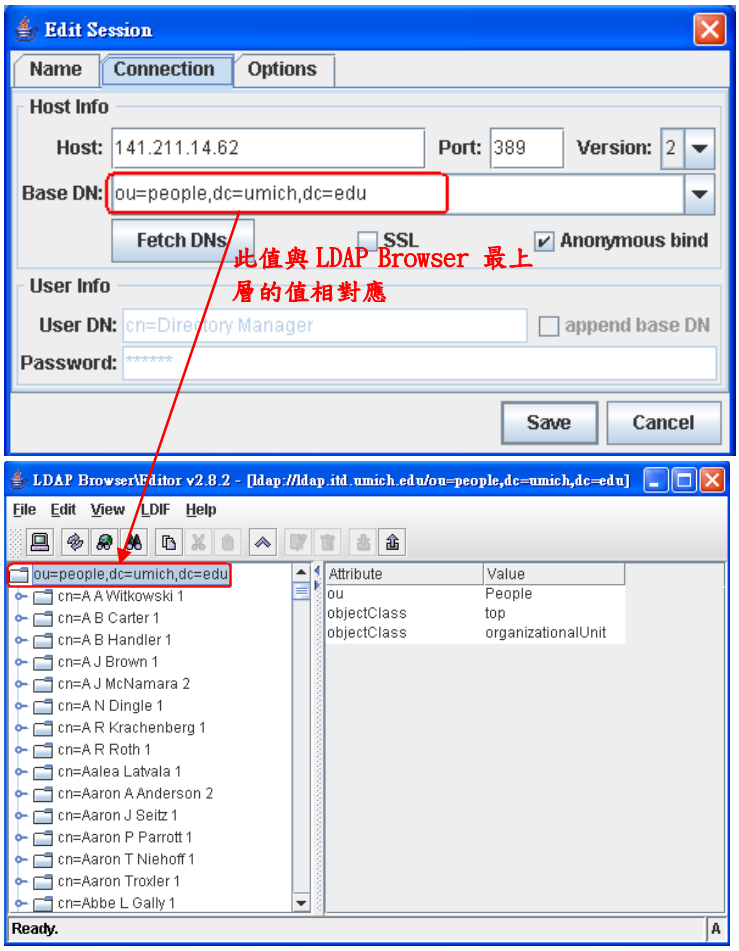
**步驟 3 輸入連線的名稱**

輸入此連線的名稱。



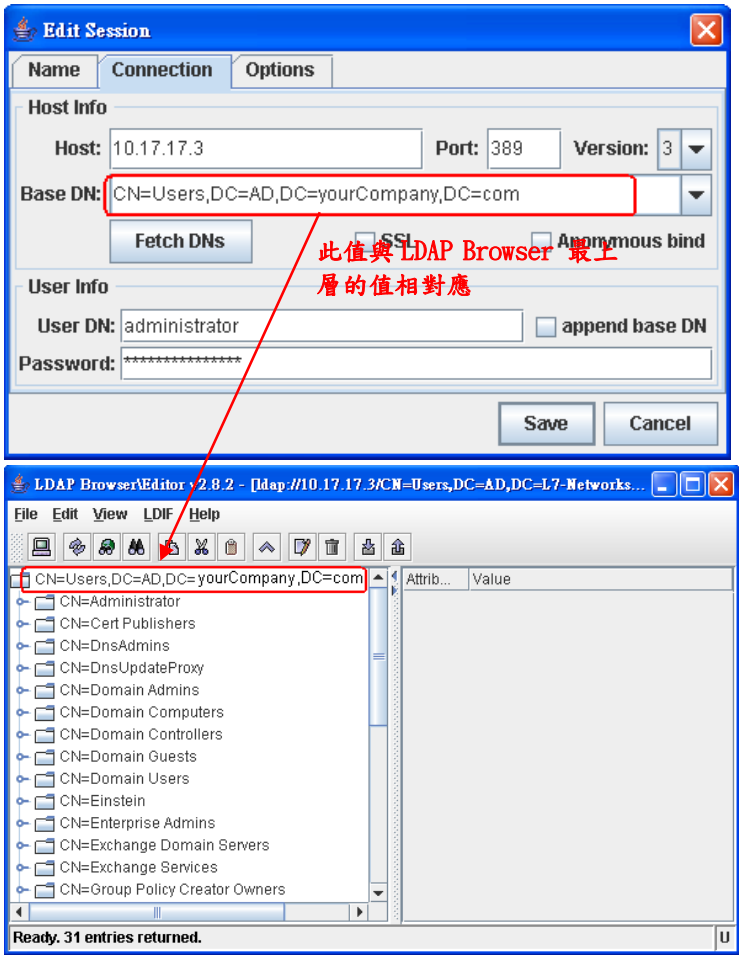

**步驟 4 a 設定 LDAP 伺服器連線參數 – OpenLDAP**

輸入 LDAP 伺服器的 IP 位址或網址、埠與您在伺服器上所設定的 Base DN。如果不確定 Base DN 爲何，可以嘗試用 Fetch DNs 來自動取得 Base DN。請注意，當您使用 Fetch DNs 時，所擷取到的 Base DN 爲最上層的 Base DN。爲了確保 LDAP Import 時資料的正確性，請務必確認使用者資料所存放的 Base DN 爲何。一般而言，OpenLDAP 使用者資料會儲存在ou=People 的路徑目錄下。



**步驟 4b 設定 LDAP 伺服器連線參數 – ActiveDirectory**

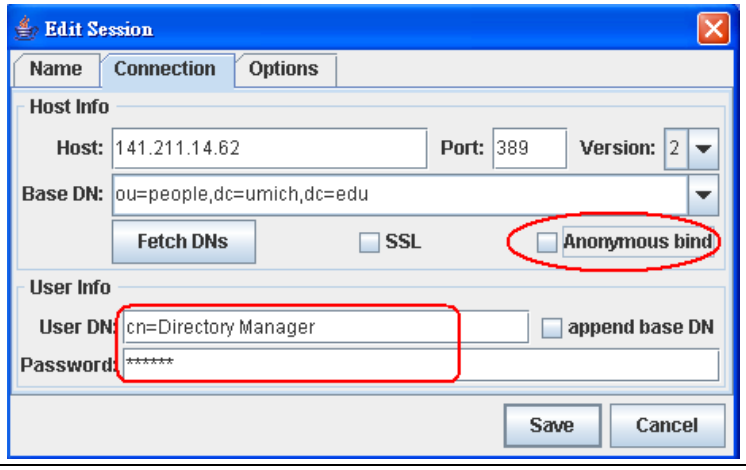
輸入 LDAP 伺服器的 IP 位址或網址、埠與您在伺服器上所設定的 Base DN。如果不確定 Base DN 爲何，可以嘗試用 Fetch DNs 來自動取得 Base DN。請注意，當您使用 Fetch DNs 時，所擷取到的 Base DN 爲最上層的 Base DN。爲了確保 LDAP Import 時資料的正確性，請務必確認使用者資料所存放的 Base DN 爲何。一般而言，ActiveDirectory 使用者資料會儲存在cn=Users（ActiveDirectory） 的路徑目錄下。




**步驟 5 a 取消匿名綁定設定 - OpenLDAP**

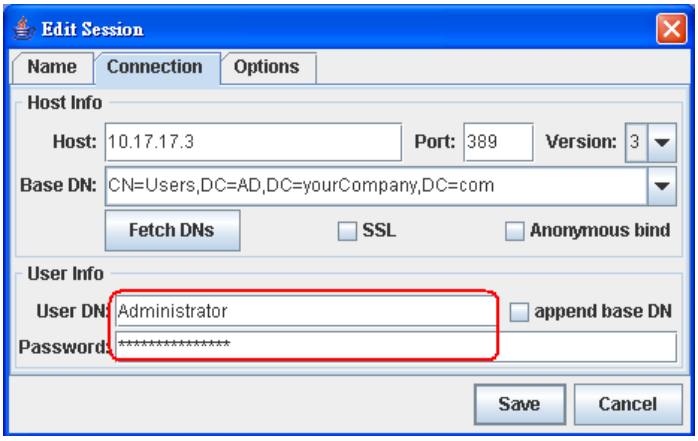
取消勾選匿名綁定（anonymous bind），然後在 User DN 那邊輸入管理者的帳號與密碼。

注意: 在Open LDAP中您所輸入的 User DN必須爲 cn=[yourAccount]，例如 cn=Directory Manager。



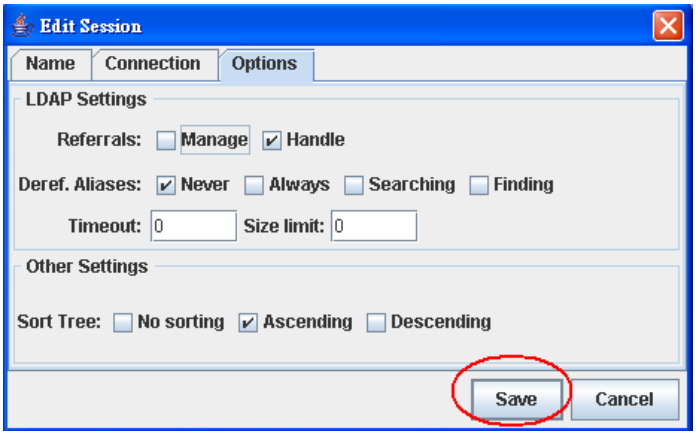
**步驟 5b 取消匿名綁定設定 - ActiveDirectory**

取消勾選匿名綁定（anonymous bind），然後在 User DN 那邊輸入管理者的帳號與密碼。



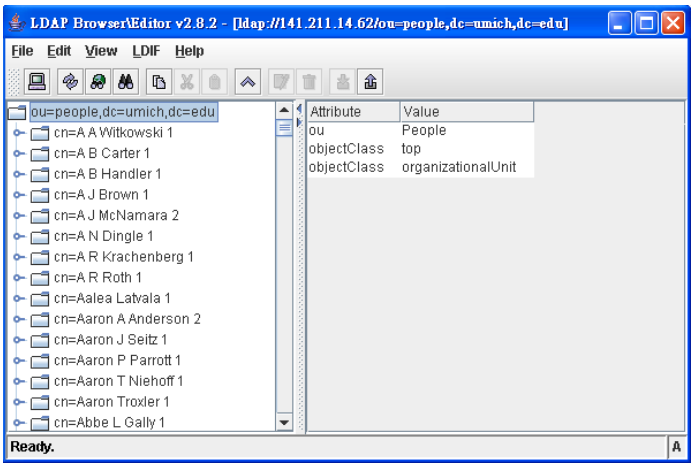

**步驟 6 進階設定**

在 Options 這邊有些其他相關的設定，可以視你的需求去調整。一般而言不需要更動。



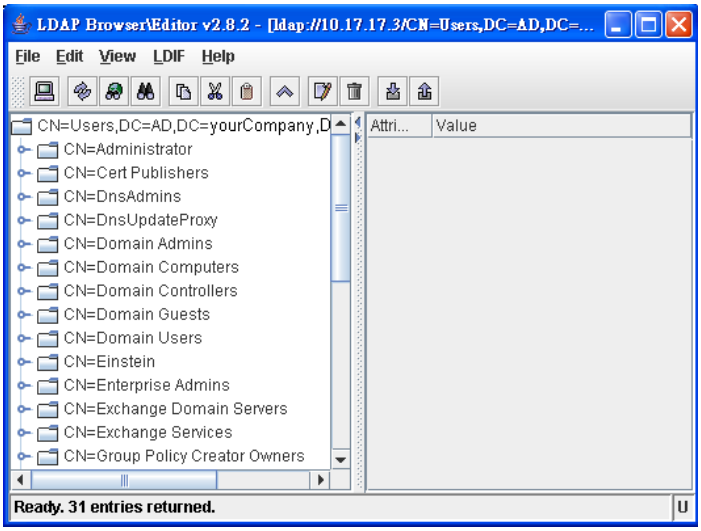

**步驟 7 a 測試連線狀況 - OpenLDAP**

最後使用這個已經設定好的連線，如果可以成功看到伺服器上所儲存的資料，則表示連線正常，如果連線不正常的話，請參考**錯誤! 找不到參照來源。**試著排解問題。



**步驟 7b 測試連線狀況 - ActiveDirectory**

最後使用這個已經設定好的連線，如果可以成功看到伺服器上所儲存的資料，則表示連線正常，如果連線不正常的話，請參考**錯誤! 找不到參照來源。錯誤! 找不到參照來源。**試著解決問題。




## 15.2 設定 LDAP Import – 基本設定

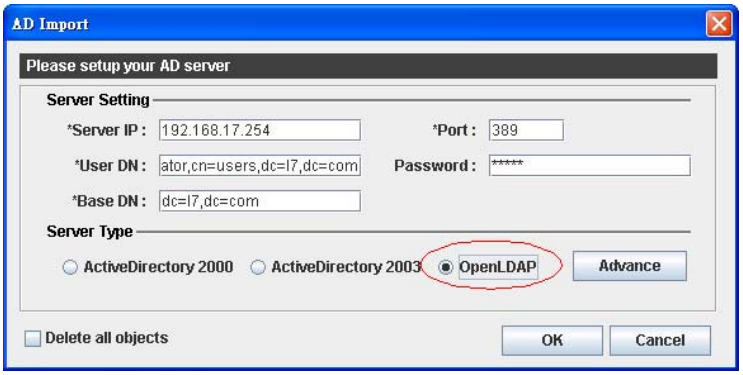
**步驟 1 設定 LDAP Import 參數**

設定伺服器的 IP、埠，以及管理者的帳號密碼。並且設定伺服器上的 Base DN。

**步驟 2 選擇 LDAP 伺服器類型**

選擇您的LDAP Server類型，選擇正確的Server類型，會幫您做好預設篩選使用者與群組資訊的方式。如果您需要自行調整LDAP內容參數，請參考進階設定中的說明。

**A: OpenLDAP**




**B: ActiveDirectory**

## 15.3 設定 LDAP Import – 進階設定

**步驟 1 設定篩檢程式**

設定使用者的篩檢程式（filter），指定的篩檢程式會把滿足條件的資料視爲有效的使用者資料，否則該筆資料將會被略過，關於過濾的設定方式請參照搜尋過濾條件的字串標記法，定義於 RFC 2254（http://www.ietf.org/rfc/rfc2254.txt）中。

**步驟 2 名稱與描述的進階設定**

設定匯入時每筆使用者資料中，指定要當做使用者名稱（name）、描述（description）以及群組（Group）的欄位。

**步驟 3 選擇匯入方式**

設定群組所在的Base DN，指定的目錄與其子目錄，即爲匯入群組資訊的範圍。

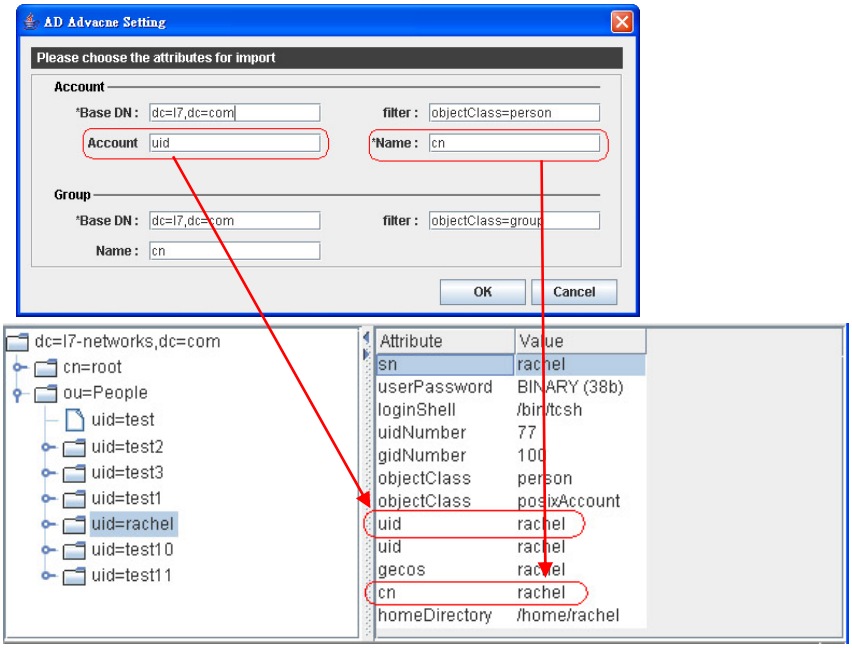
**步驟 4 匯入欄位設定**

設定群組參照的欄位，一般在使用者的資訊中，群組欄位的內容不是簡單的組名，而是參照用的數位或者字串，所以在群組資訊中，通常也會有一個欄位做爲參照用，只要比對使用者資訊中的群組欄位與群組資訊中的參照域值是否相同，就可以判斷此一使用者是否屬於此一群組。

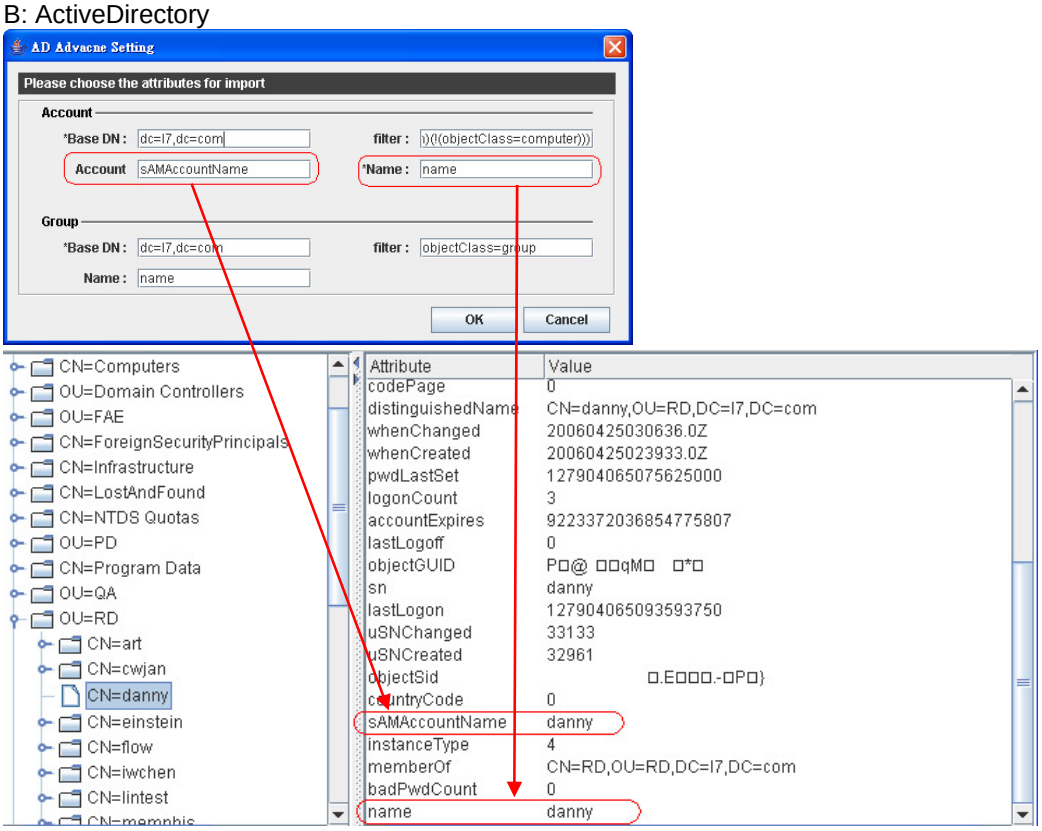
**步驟 5 數據匯入**

設定匯入每筆群組資料中，指定要當組名（name）、描述（description）的欄位。

A: OpenLDAP




B: ActiveDirectory



## 15.4 LDAP 匯入疑難排解

**問題一：爲何我無法連到我的 LDAP 伺服器？**

**答：**首先要先確認伺服器的 IP 與埠是否正確。如果沒有錯誤的話，可以用 telnet <ip> <port>的方式，看看是否能正常連接。在操作 UI 的電腦與 LDAP 伺服器之間是否有防火牆阻擋？LDAP 伺服器設定是否有開放許可權，讓外部的電腦存取（access）資料？（關於 LDAP 伺服器要怎麼設定存取許可權，請洽詢你的 LDAP 伺服器軟體供應商。

**問題二：爲何匯入成功，卻沒有新增任何使用者資料？**

**答：**這可能是因爲你所指定要匯入資訊的位置錯誤，或者篩檢程式的條件設定有誤，以致於沒有任何資訊符合條件。

**問題三：爲何我所匯入的使用者數量比我存在 LDAP 伺服器上的還要少？**

**答：**因爲多數 LDAP 伺服器會設定一次查詢（query）中，能回應結果（result）的數量上限，如果希望能正常匯入所有使用者的資料，必須要修改你所使用的 LDAP 伺服器的參數。請參照 http://www.ldapbrowser.com/forum/viewtopic.php?t=14 的討論，或者請洽詢你的 LDAP 伺服器軟體供應商。

# 第16章
# 封裝管理員

*本章節介紹 InstantScan 的封裝管理功能與其設定。*

## 16.1 需求

1. 當管理 MSN 與 Yahoo 即時軟體入下聯機時，不須要更改任何的防火牆與使用者端的設定

## 16.2 方法

1. 在 Functions > Management > Enapsulation Manager 頁面上開始封裝管理員即可。

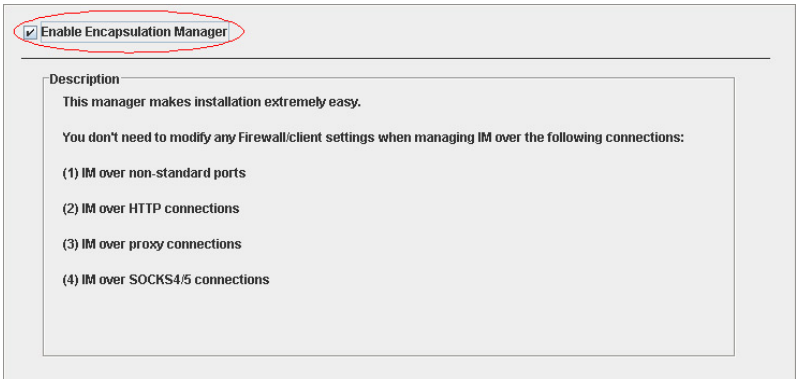
## 16.3 步驟

### 16.3.1 啓動封裝管理員

**步驟 1 開啓封裝管理員**

勾選 Enable Encapsulation Manager。

**Functions > Managements > Enapsulation**




**步驟 2 上傳設定檔**

選擇 **Upload Configuration** 或點擊圖示  將設定檔上傳到裝置上。

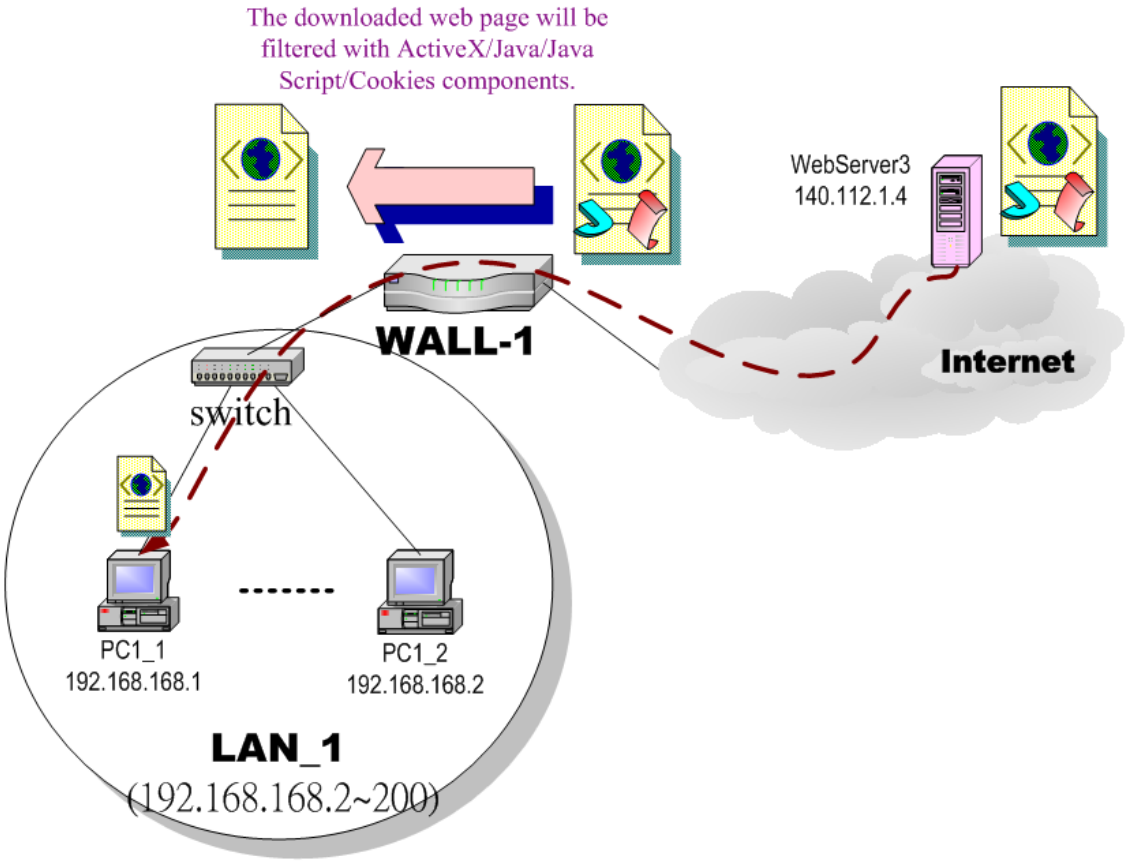
# 第8部

# 網頁管理員

# 第17章 網頁管理員

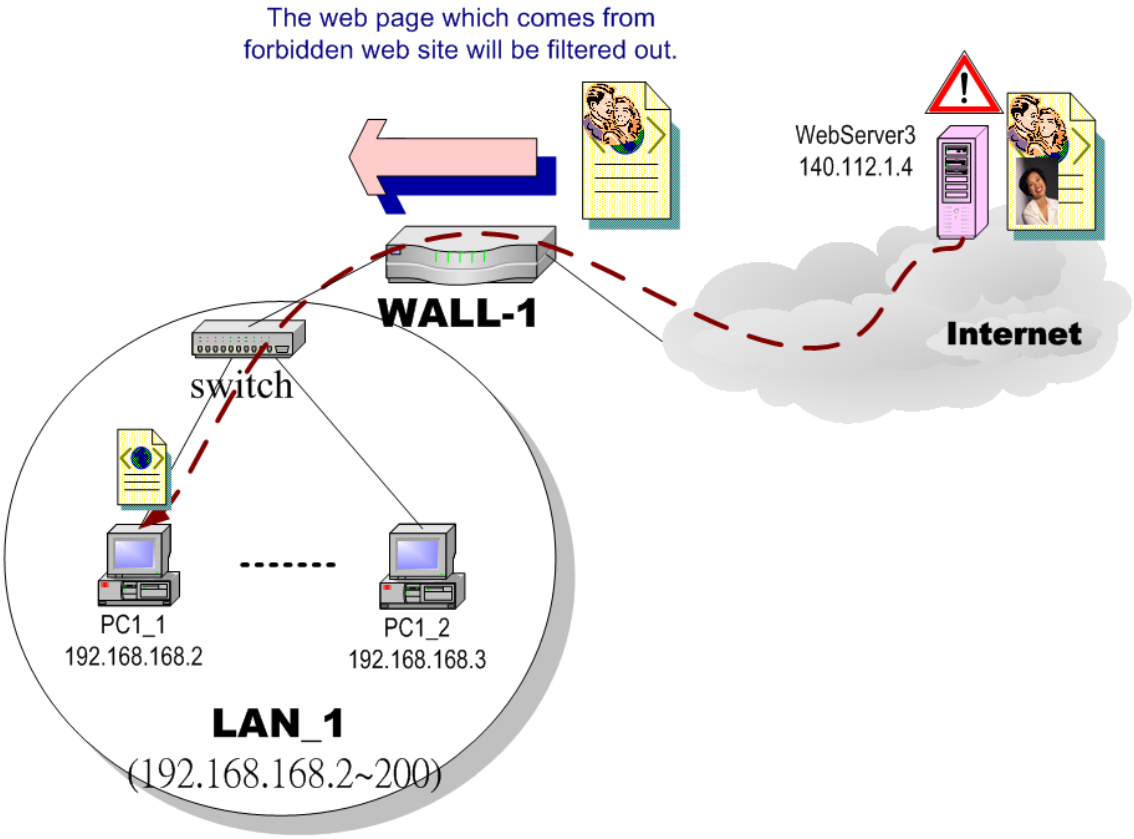
*本章節介紹 IntantScan 的網頁管理功能與其設定。*

## 17.1 需求




圖表 17-1 透過網頁過濾防止員工流覽被禁止的網站

1. 如圖表 17-1 所示，PC1_1 正在流覽 WebServer3 的網頁。網頁的內容包含 cookies、Java applets、Java scripts 或者 ActiveX 物件等，這些內容也許包含惡意軟體伺機竊取使用者資料。所以，您希望能夠禁止 PC1_1 下載這些禁止流覽的組件。




圖表 17-2 透過網頁過濾禁止員工流覽 WebServer3 的網頁

2. 如圖表 17-2 所示，PC1_1 在上班時間流覽禁止流覽 WebServer3 的網頁。這些網頁內容也許包含股票市場資訊、暴力或色情，且會浪費公司網際網路的頻寬，降低員工生產力。所以，您希望透過設定 InstantScan 就可以攔阻 PC1_1 流覽這些類型的網站。

## 17.2 目的

1. 移除網頁內含的 cookies、Java applet、ActiveX 對象等。
2. 防止員工連上禁止流覽的網站。

## 17.3 方法

1. 設定要過濾的網頁元件，例如 cookies 或 Java applets。
2. 設定網頁過濾。當流覽網頁時，InstantScan 會根據設定的規則檢查網域、網址或關鍵字來判斷是否放行網頁流量。

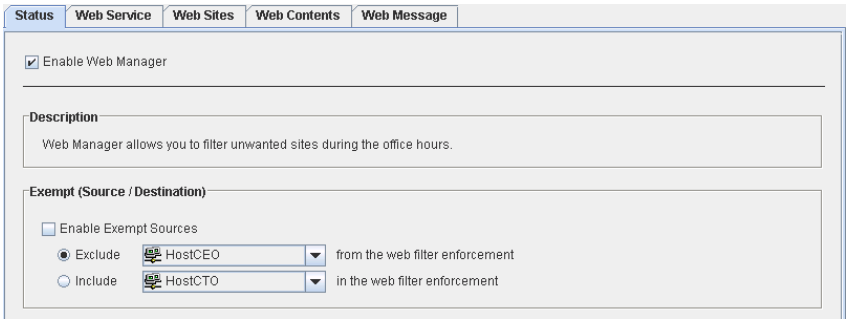
## 17.4 步驟

**步驟 1 啓用網頁過濾**

勾選 **Enable Web Filter**。

請注意，當您套用網頁過濾時，系統將自動勾選過濾所有流經標準 HTTP（80埠號）的網頁流量。若想要將某些人除外，可勾選**Enable Exempt Sources**，其中Exclude是除外，Inlcude是只對選定的人進行Web過濾。

**Content Manager > Web Manager > Status**

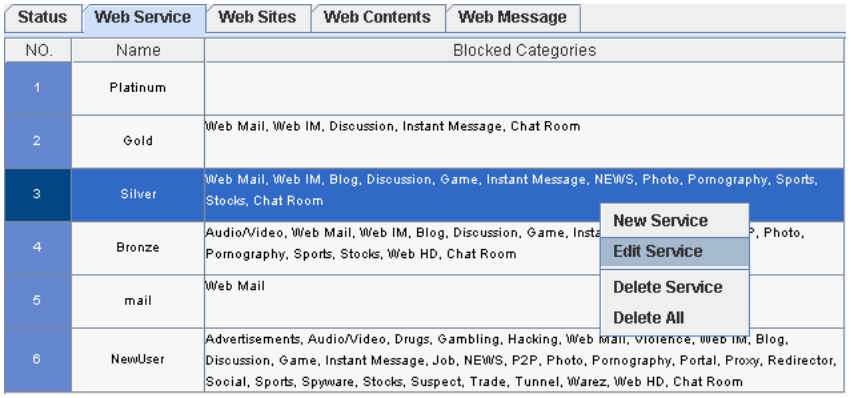



**步驟 2 編輯Web Service**

決定Web Service的各個許可權等級。

你可以新增Web Service，或者編輯現有Web Serivce。

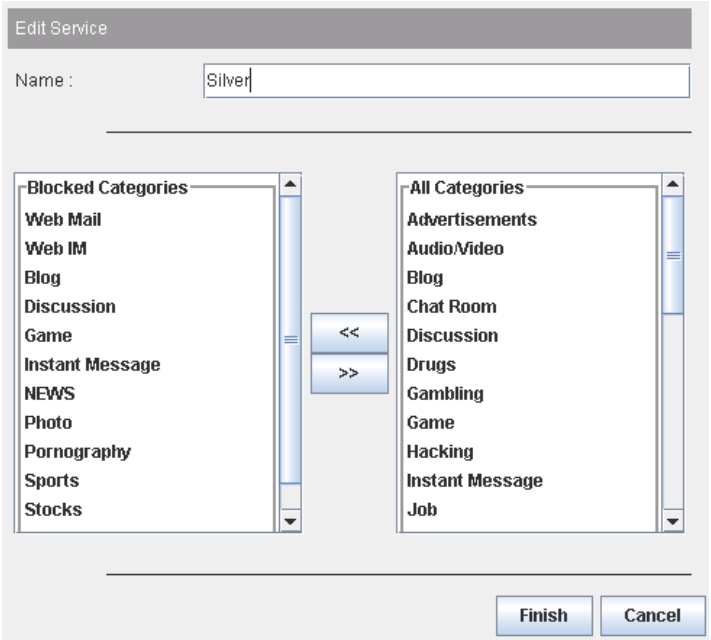
**Content Manager > Web Manager > Web Service**




**步驟 3 編輯Silver Web Service**

將您想要阻擋的Web database網站種類，加到Silver等級的Web Service。若用戶被指定爲此Service者，連到這幾種網頁時，就會被阻擋。

**Content Manager > Web Manager > Web Service > Edit Service**

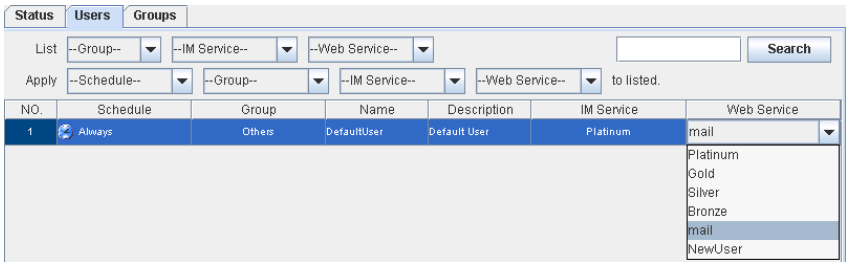


**步驟 4 於用戶控制台加入用戶**

你可以從AD Import進來使用者資料，然後讓使用者登入時自動讓系統得知AD登入，並對其後的Web Service作相對應的過濾。

系統內建DefaultUser，任何沒有比對身份到的Web流量，都會給予設定的Web Service。

**Functions > Console > User Console**

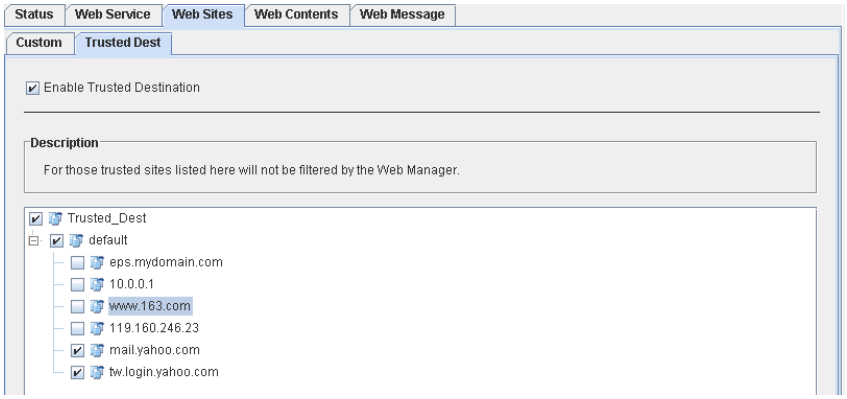



**步驟 5 訂定信任的網域**

勾選 Enable Trusted Domain。然後新增信任的網域群組與網功能變數名稱稱。

請輸入信任的網功能變數名稱稱。注意，如果您所輸入的網功能變數名稱稱無法被 DNS 伺服器辨識，這筆網功能變數名稱稱將會被忽略。再則是，如果您啓用太多的網功能變數名稱稱，在開始網頁過濾時將需要較長的時間來作名稱辨識。

**Management > Web Manager > Exclude > Trusted Dest**



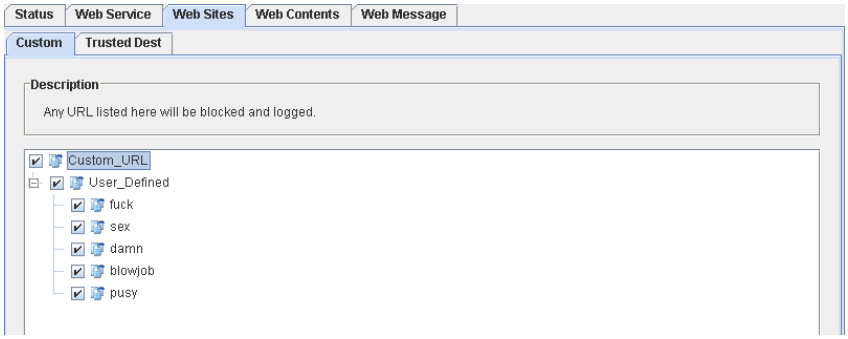

| 欄位 | 說明 | 範圍 / 格式 | 範例 |
|---|---|---|---|
| Enable Exempt Sources | 啓用用除外來源端。 | 啓用 / 不啓用 | 啓用 |
| Exclude ____ from the web filter enforcement | 所列舉的 IP 位址除外，其餘的電腦皆強制執行網頁過濾。也就是說當您選擇 Boss 時，除了 CEO 與 CTO 外的 IP 都需要執行網頁過濾。 | 啓用 / 不啓用 | 啓用 / Boss |
| Include ___ in the web filter enforcement | 網頁過濾只適用於所列舉的電腦。 | 啓用 / 不啓用 | 不啓用 |

表格 17-1 除外來源端欄位說明

**步驟 6 客制化 URL 關鍵字攔阻**

勾選 **Custom_URL**，攔阻任何包含關鍵字清單之 URL 位址。InstantScan 已預設一些常用的關鍵字，如不敷需求您可以在螢幕上按右鍵新增/修改/刪除關鍵字群組/關鍵字。

**Functions > Management > Web Manager > Web Sites > Custom**



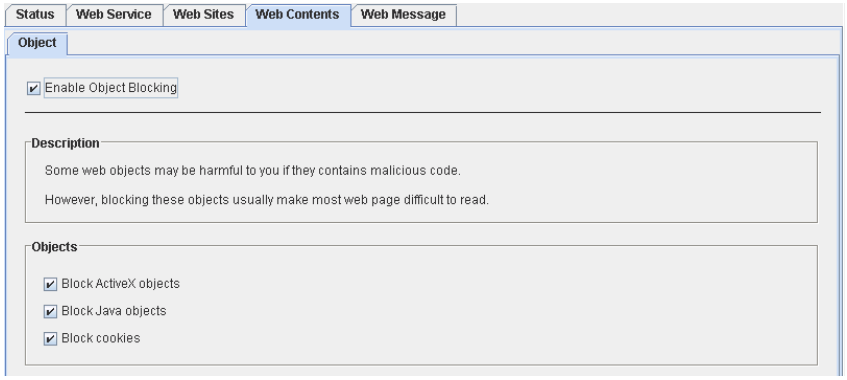
| 欄位 | 說明 | 範圍 / 格式 | 範例 |
|---|---|---|---|
| URL Keywords | 如果您要流覽的 URL 網址出現所輸入的關鍵字，當您利用網際網路連上此網址後，此 URL 的內容將會被 InstantScan 攔阻。 | 文字字串 | Adv/advertise/adsrv/ banner/splash |

表格 17-2 URL 關鍵字過濾

**步驟 7 網頁物件特徵過濾**

勾選 Enable Object Blocking。然後勾選要利用特徵過濾的網頁物件。當您啓用此功能後，透過 PC1_1 流覽網頁可能還可以看到這些物件。這可能是因爲網頁暫存（cache）所致。請清除所有網頁流覽器內的網頁暫存記憶，關閉流覽器。重新開啓流覽器，然後重連網頁即可。

**Functions > Management > Web Manager > Web Contents > Object**




| 欄位 | 說明 | 範例 |
|---|---|---|
| 啓用物件特徵攔阻 | 選擇以下的網頁元件以作爲網頁之特徵過濾。 | 啓用 |
| ActiveX | 過濾包含 ActiveX 的網頁。 | 啓用 |
| Java | 過濾包含 Java 的網頁。 | 啓用 |
| Cookies | 過濾包含 Cookies 的網頁。 | 啓用 |

表格 17-3 網頁特徵過濾

| 欄位 | 說明 | 範圍 / 格式 | 範例 |
|---|---|---|---|
| Enable Keyword Blocking | 啓用網頁內容關鍵字攔阻。 | 啓用 / 不啓用 | 啓用 |
| Stop transferring the web page when the same keyword appears for __ times. | 當勾選關鍵字攔阻，如果您要開啓的網頁中含有本頁所列舉的關鍵字，此網頁將會被攔阻而無法正常顯示。"限關鍵字每出現 __ 次" 意味著只要關鍵字出現等於或大於所輸入的數字時，攔阻要開啓的網頁。例如，只要關鍵字出現 5 次，攔阻該網頁。 | 啓用 / 不啓用<br>數字 | 啓用<br>5 次 |
| Keywords | 輸入您想攔阻的關鍵字。 | 文字字串 | adv<br>advertise<br>adsrv<br>banner<br>splash |

表格 17-4 網頁關鍵字過濾

# 第9部

# 報表系統

# 第18章
# 報表系統簡介

*本章介紹 InstantScan 報表系統。*

## 18.1 InstantScan 報表系統

InstantScan 提供客戶隨選即用人性化的使用者介面，除了易於設定的管理系統外，更提供使用者簡潔易懂的報表系統。讓使用者可以依據需求定義報表搜尋方式、查詢各式各樣的排行榜資料、更可依功能面、政策面與個人面作特殊的搜尋與排行。除此之外，更有事件記錄的資料可供使用者查詢。

## 18.2 報表設計原則

### 18.2.1 報表類別

目前 InstantScan 依功能列分成五種報表：

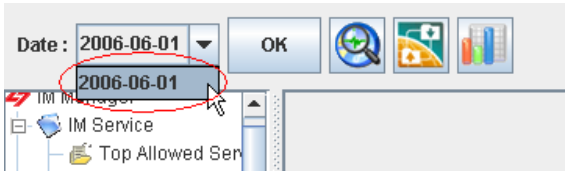
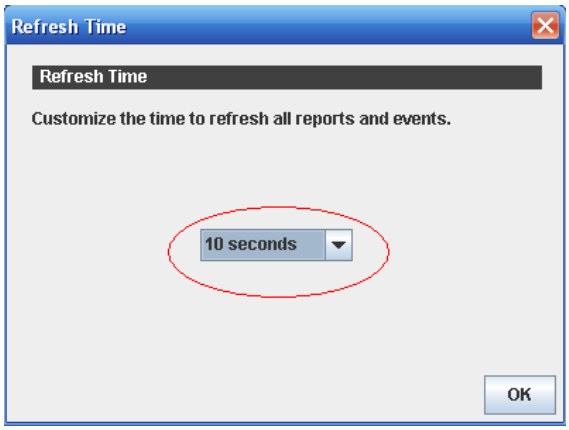
1. 應用層防火牆報表：可檢視與查詢所有應用層防火牆通訊協定的排行榜與事件記錄。
2. 即時通訊管理員報表：可檢視與查詢所有即時通訊行爲的排行榜與事件記錄。
3. 網頁管理員報表：可檢視與查詢所有網頁流量的圖形報表與事件記錄。
4. 流量管理員報表：可檢視與查詢每日、每週、每月、每季與每年的流量排行榜與事件記錄。
5. 系統管理員報表：可檢視與查詢所有系統的操作資訊。詳見**錯誤! 找不到參照來源。**系統紀錄的說明。

所有報表，除了系統管理員報表外，皆依其性質分成四個類別：

1. 功能面（Funcational View）：依功能作用排行。
2. 政策面（Policy View）：依使用者所制定的政策排行，也可以說是管理面的報表。
3. 個人面（Personal View）：依個別使用的狀況排行，也可以說是個人化的報表。
4. 事件面（Event View）：所有行爲動作的事件記錄。

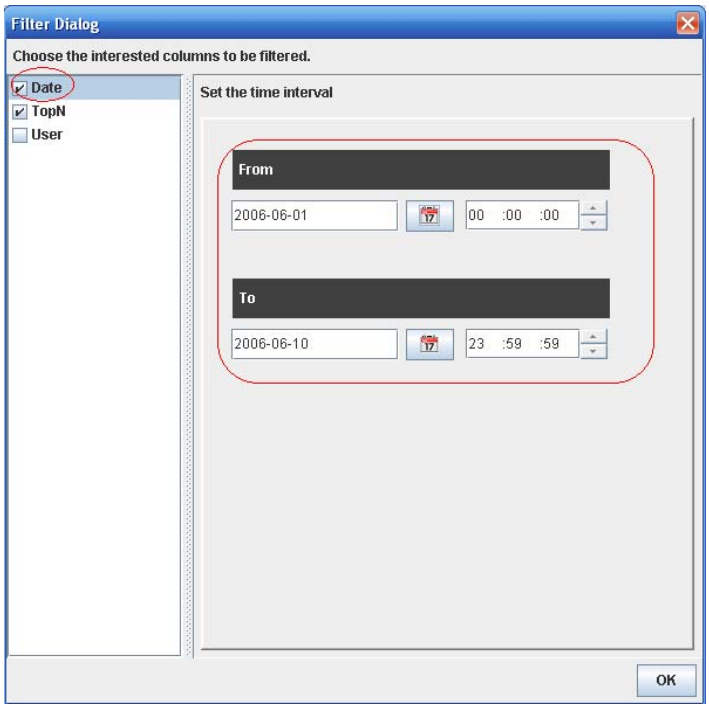
### 18.2.2 搜尋工具

爲了加速使用者在尋找特定事件記錄或報表的速度，InstantScan 搜尋工具列可以讓您依日期或特定的關鍵字搜尋你要的資訊。

| | |
|---|---|
| **步驟 1 搜尋期間設定**<br>報表系統上所顯示的日期期間爲您在安裝管理伺服器時所選擇的資料分割期間。可分成 1) 每週 2) 每月 3) 每季，三種期間。如右圖所示，分割期間爲每個月。所以日期顯示會以每個月的第一天爲主，例如 2006-06-01。同理類推。<br>**注意，爲了確保資料搜尋的速度與保留資料的完整性，在資料分割後，當您選擇每週/每月/每季後，您無法跨周/月/季搜尋。** |  |
| **步驟 2 重新整理報表與事件記錄時間設定**<br>點擊圖示  設定重新整理報表與事件記錄的時間。 |  |
| **步驟 3 選擇重新整理時間**<br>選擇 10 seconds，然後點擊 **OK** 完成設定。一旦您套用這個設定，往後每 10 秒鐘系統會根據您所選擇的時間重新整理報表與事件紀錄的資料。 |  |
| **步驟 4 進階搜尋**<br>點擊圖示  （進階）。 |  |

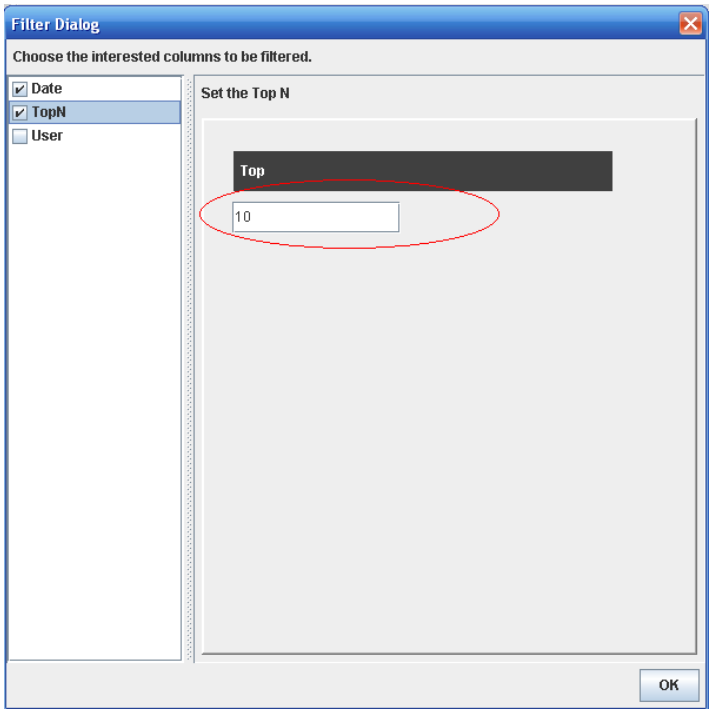
**步驟 5 選擇搜尋日期**

勾選 Date。在此您可以縮小搜尋的範圍。也就是說當您資料分割是以每月爲主，您可以在當月內選擇一個時間區段作數據搜尋的期間。請在時間間隔內選擇搜尋的起始時間與結束時間。



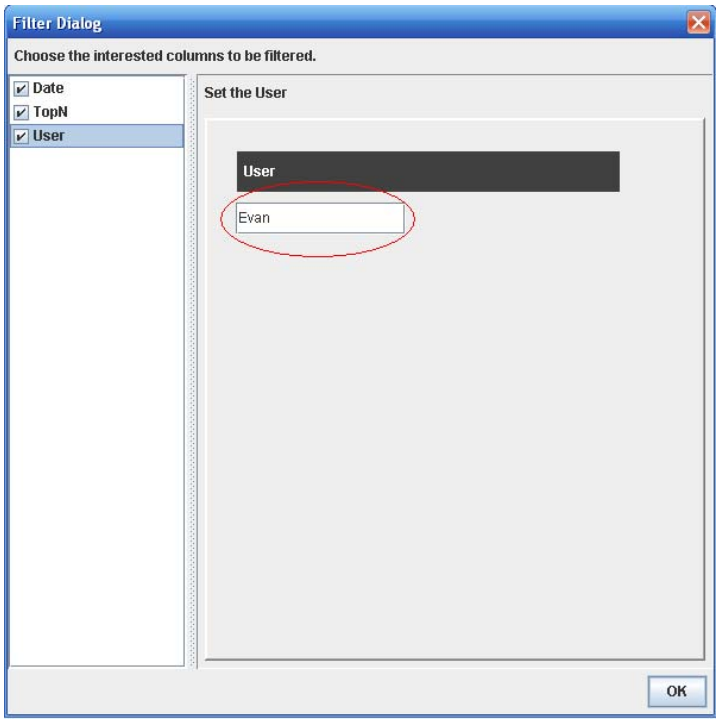

**步驟 6 輸入要流覽的排名數**

勾選 TopN 預設上，系統顯示的所有事件的排名列表，如果您只需要前 N 名排名列表，您可以在空格內輸入您想要流覽的數目。



**步驟 7 細部搜尋**

如果您希望做更細部的搜尋，您可以特定的細部搜尋項目。例如：user、receiver、sender、application、action 等等，視您所選擇的報表專案而定。



# 第19章
# 應用層防火牆報表

*本章介紹應用層防火牆報表的應用。*

## 19.1 需求

1. 有鑒於網路頻寬的濫用頻繁，管理人員希望獲得哪些通訊協定被企圖非法使用的統計資料。
2. 管理人員希望知道前 10 名使用 skype 被 InstantScan 攔阻的排行榜。
3. 管理人員希望知道使用者（IP：192.168.17.58）前 10 名被攔阻的通訊協定排名。
4. 管理人員希望將事件記錄儲存成 Excel 檔，可以依據自己的需求產生其他的報表格式。

## 19.2 方法

1. 到 Reports > Application Firewall > Funcational View > Top Blocked Protocol 檢視圖形報表。
2. 到 Reports > Application Firewall > Policy View > Top Blocked Users of Application，並于 Advanced 上勾選 Application 選擇 skpye。
3. 到 Reports > Application Firewall > Personal View > Top Blocked Applications of User，並點擊 Advanced 設定搜尋 source IP 192.168.17.58。
4. 到 Reports > Application Firewall > Event View，點擊 Export，選擇資料匯出類型爲 Excel。

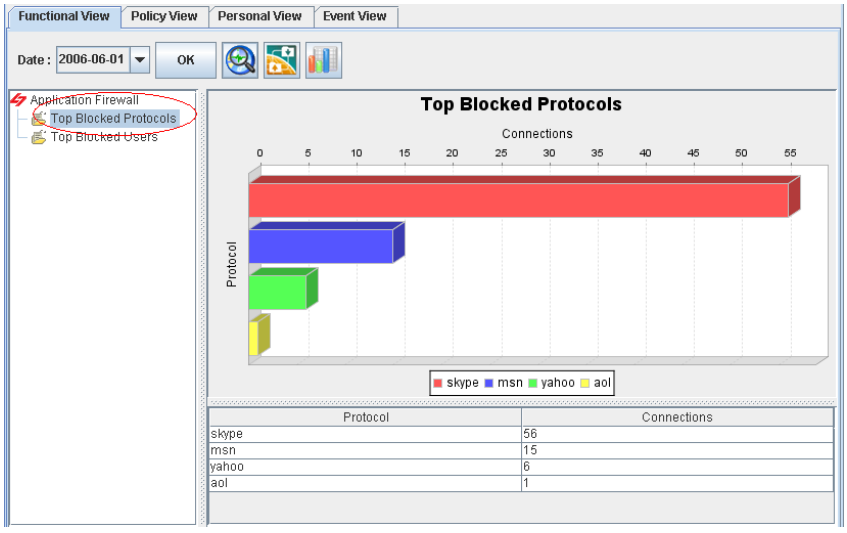
## 19.3 步驟

### 19.3.1 功能面報表流覽

**步驟 1 點擊被攔阻的通訊協定排行**

點擊 **Top Blocked Protocols**。

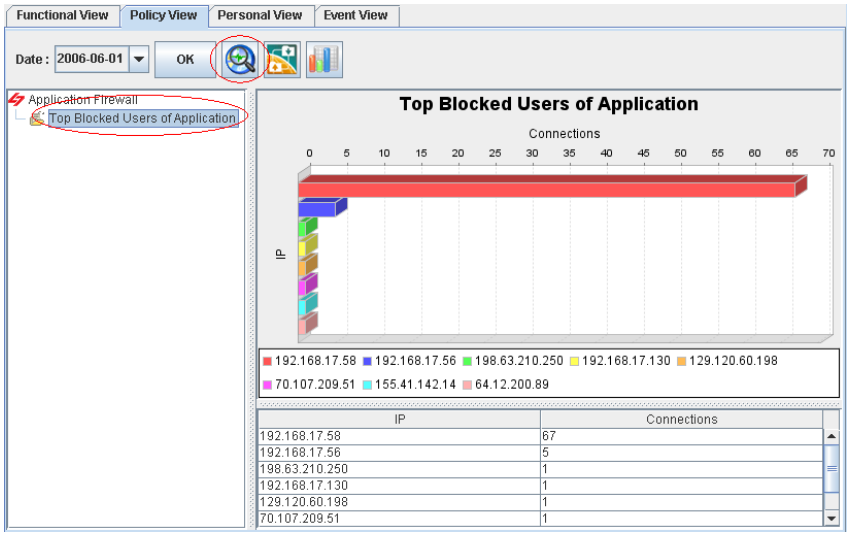
**Reports > Application Firewall > Functional View > Top Blocked Protocols**




| 報表專案 | 說明 |
|---|---|
| Top Blocked Protocols | 經常被攔阻的通訊協定排行。也就是企圖非法闖關的通訊協定排行。 |
| Top Blocked Users | 經常被攔阻的使用者排行。也就是企圖非法使用某些通訊協定的使用者排行。 |

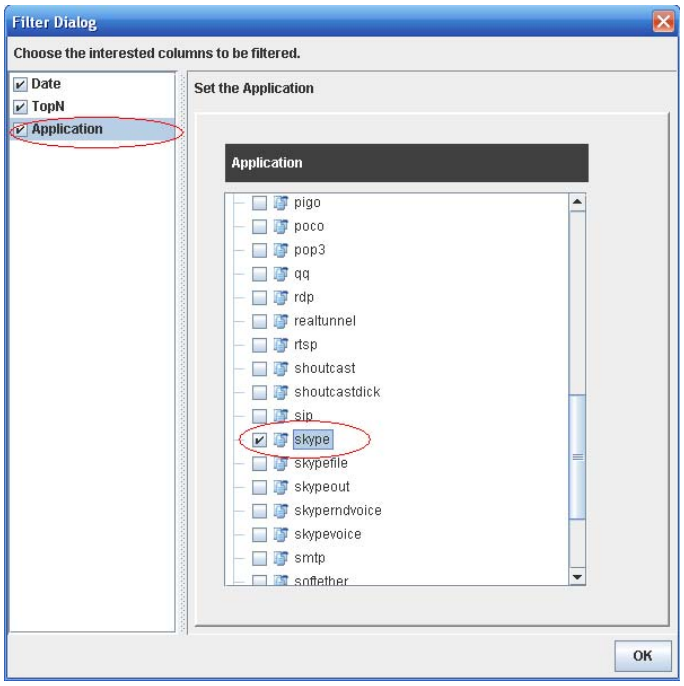
表格 19-1 應用層防火牆 - 功能面報表說明

### 19.3.2 政策面報表流覽

| **步驟 1 流覽因違法使用通訊協定而被攔阻的使用者排名**<br>點擊 **Top Blocked Users of Application**。然後點擊圖示 進階設定。 | **Reports > Application Firewall > Policy View > Top Bloced Users of Application**<br>  |
|---|---|

| 報表專案 | 說明 |
|---|---|
| Top Blocked Users of Application | 經常因違法使用通訊協定的使用者排行。 |

表格 19-2 政策面報表說明

| **步驟 2 進階搜尋報表**<br>勾選 Application，然後在 Application 列表上勾選 **Skype**。點擊 **OK** 流覽結果。 | **Reports > Application Firewall > Policy View > Top Blocked Users of Application > Advanced**<br>  |
|---|---|

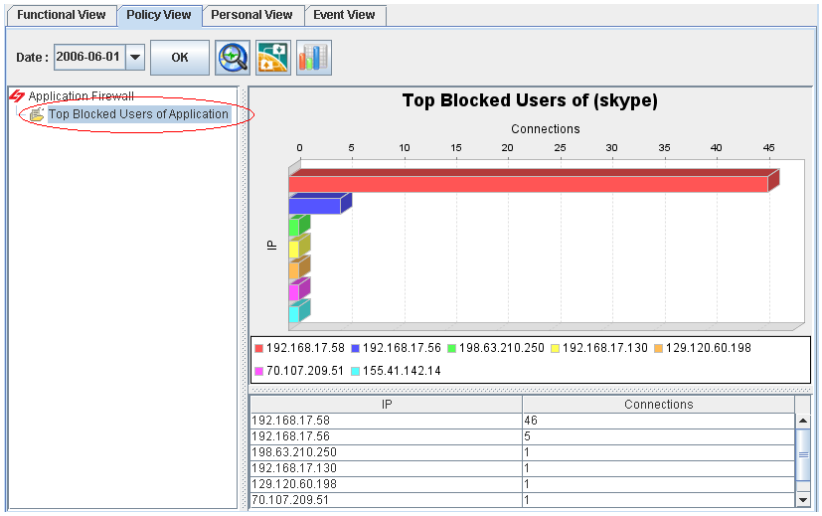
| 報表專案 | 說明 | 範例 |
|---|---|---|
| Date | 可設定要搜尋的資料之期間。注意，這個期間的有效範圍爲當您在管理伺服器所設定的資料分割週期，超過資料分割週期的期間設定是無效的。也就是當您所設定的資料分割週期爲每個月分割一個表格，您所選擇的搜尋期間就不可以超過該月的範圍。預設上，這個日期期間會依當周的日期爲主，如果您在報表畫面上看不到過去的圖表，請在此選擇適當的日期。 | 2006/06/01 ~ 2006/06/30 |
| TopN | 您在報表畫面上希望看到的排行數。如果您希望只看前 10 筆，請填入 10。 | 10 |
| Application | 您希望流覽哪些使用者經常違法使用某些通訊協定的排行。可複選。 | skype |

表格 19-3 應用層防火牆 - 政策面報表進階搜尋說明

**步驟 3 流覽設定的結果**

右圖爲因爲企圖非法使用 Skype 的使用者排名。

**Reports > Application Firewall > Policy View > Top Blocked Users of Application**

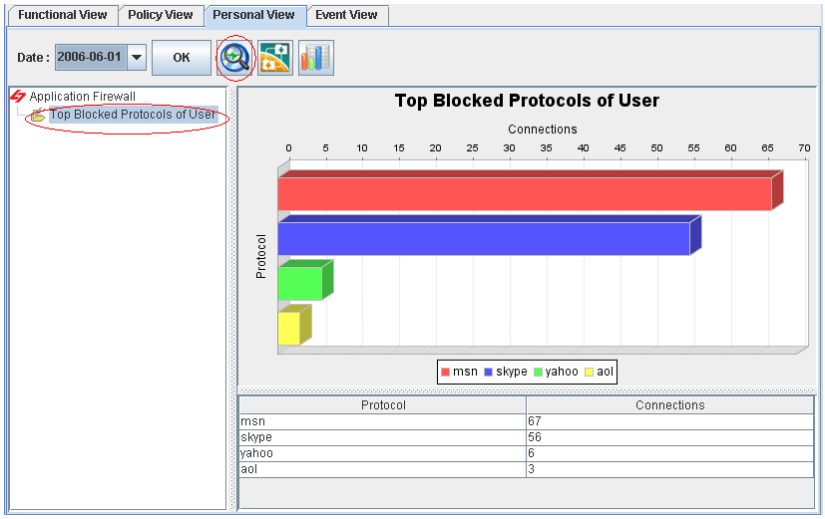



## 19.3.3 個人面報表流覽

**步驟 1 流覽使用者所違法使用的通訊協定排行**

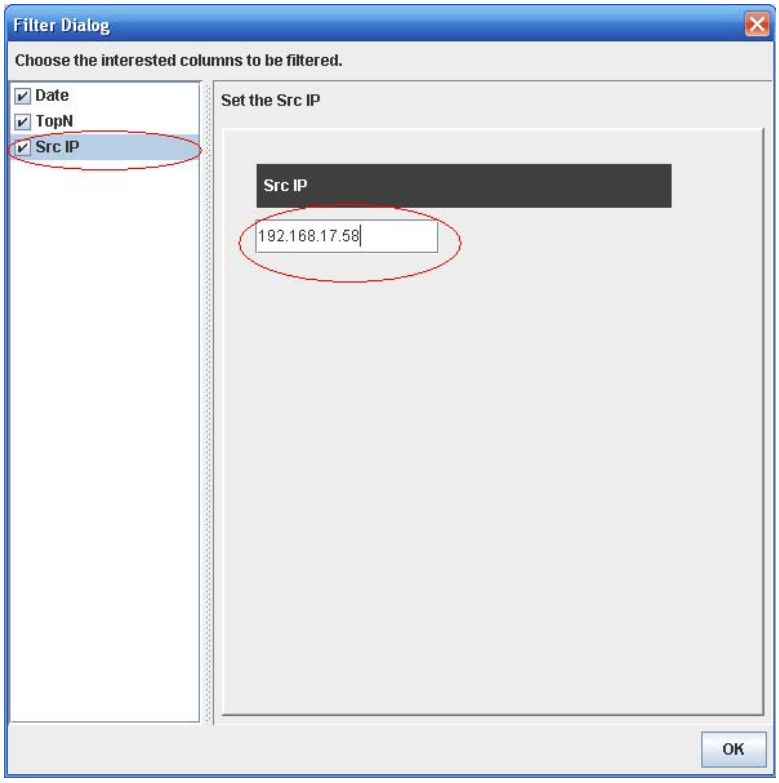
點擊 **Top Blocked Protocols of Users**。然後點擊圖示 進階設定。

**Reports > Application Firewall > Personal View > Top Bloced Protocols**



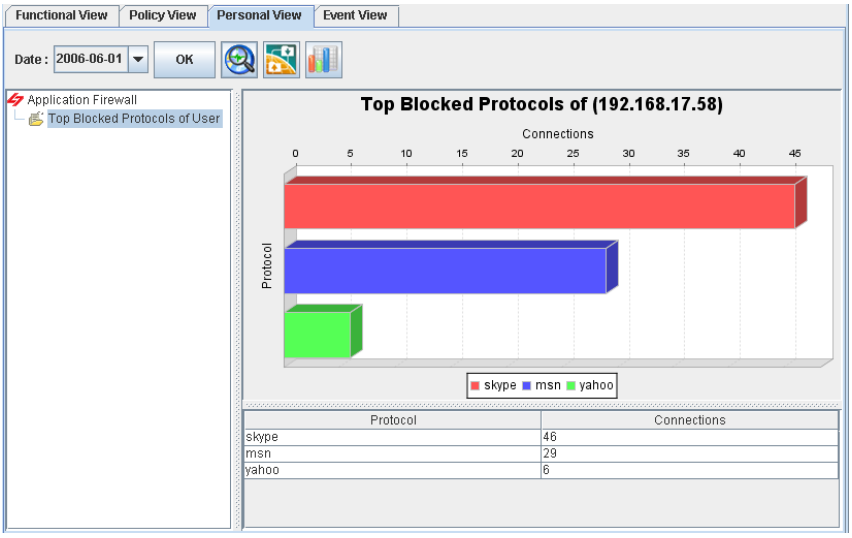
| 報表專案 | 說明 |
|---|---|
| Top Blocked Protocols of User | 特定的使用者所違法使用的通訊協定排行。 |

表格 19-4 應用層防火牆 - 個人面報表說明

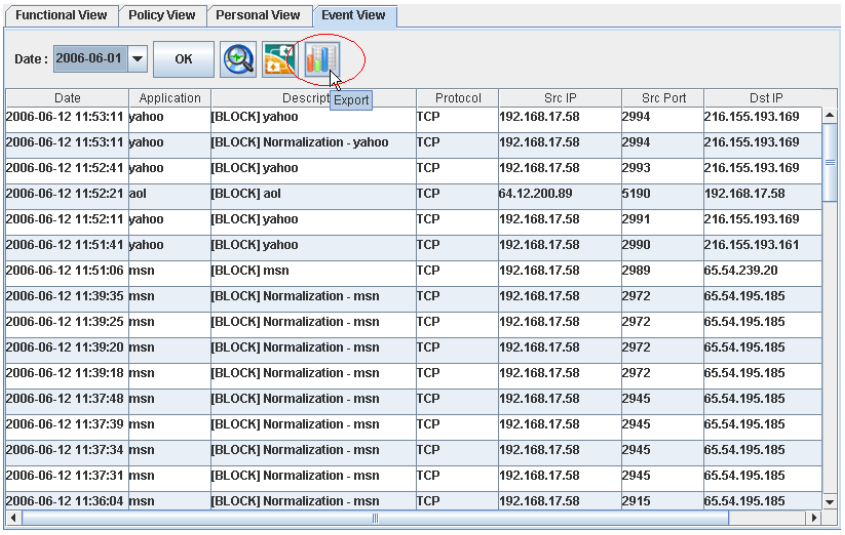
| | |
|---|---|
| **步驟 2 進階搜尋報表**<br>勾選 Src IP，然後在 Src IP 欄位上輸入 **192.168.17.58**。點擊 **OK** 流覽結果。 | **Reports > Application Firewall > Personal View > Top Blocked Protocols of User > Advanced**<br>  |

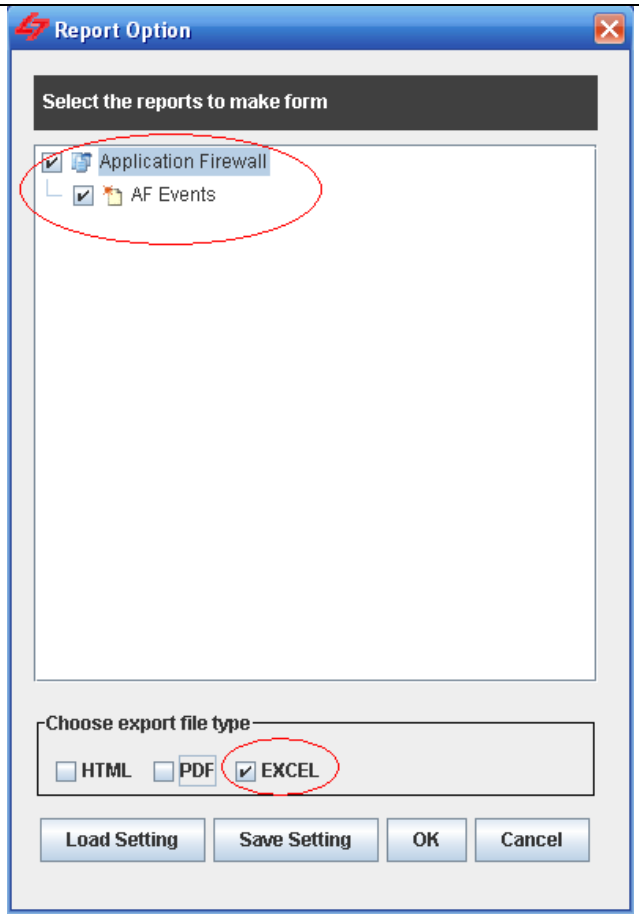
| 報表專案 | 說明 | 範例 |
|---|---|---|
| Date | 可設定要搜尋的資料之期間。注意，這個期間的有效範圍爲您在管理伺服器所設定的資料分割週期，超過資料分割週期的期間設定是無效的。也就是當您所設定的資料分割週期爲每個月分割一個表格，您所選擇的搜尋期間就不可以超過該月的範圍。預設上，這個日期期間會依當周的日期爲主，如果您在報表畫面上看不到過去的圖表，請在此選擇適當的日期。 | 2006/06/01 ~ 2006/06/30 |
| TopN | 您在報表畫面上希望看到的排行數。如果您希望只看前 10 筆，請填入 10。 | 10 |
| Src IP | 您希望查詢的使用者，其經常違法使用而被攔阻的通訊協定排行。 | 192.168.17.58 |

表格 19-5 應用層防火牆 - 個人面報表進階搜尋說明

| | |
|---|---|
| **步驟 3 流覽搜尋結果**<br>右圖使用者 192.168.17.58 企圖非法使用的通訊協定排行表。 | **Reports > Application Firewall > Personal View > Top Blocked Protocols of User**<br>  |

## 19.3.4 匯出事件報表

| | |
|---|---|
| **步驟 1 匯出事件報表**<br>點擊圖示 進階設定。 | **Reports > Application Firewall > Event View**<br>  |
| **步驟 2 選擇匯出報表的專案**<br>勾選您要匯出的報表專案，然後勾選會出報表的類型爲 Excel，點擊 OK 繼續。 | **Reports > Application Firewall > Event View > Export** |



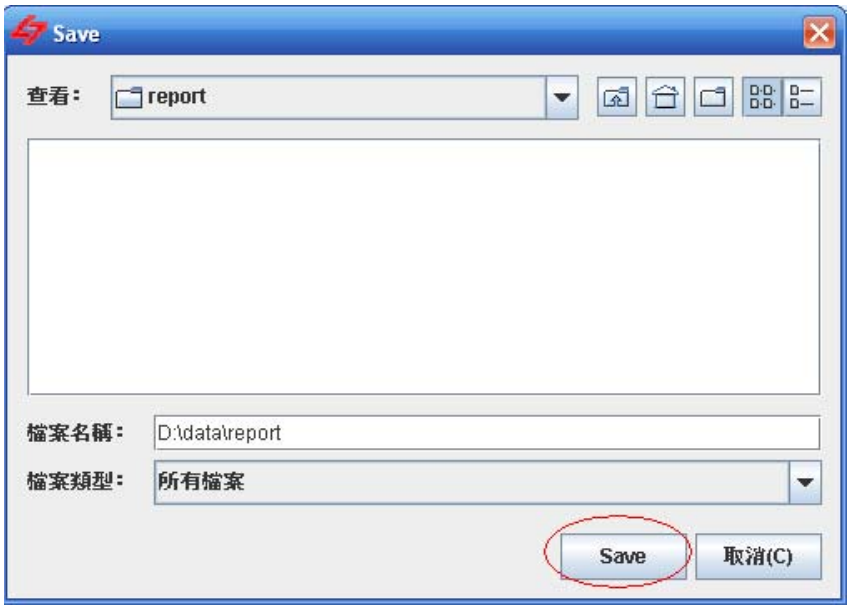

| 欄位 / 按鈕 | 說明 | 範例 |
|---|---|---|
| Application Firewall | 應用層防火牆可以匯出的事件記錄。 | AF Events |
| Choose export file type | 選擇要匯出報表的格式。有三種檔案類型可供選擇：1) HTML 2) PDF 3) EXCEL （提供原始事件資料，可供使用者自行制定報表。） | EXCEL |
| **Button** | | |
| Load Setting | 將之前已儲存的報表設定檔載入。 | |
| Save Setting | 儲存報表設定檔。 | |
| OK | 套用設定。 | |
| Cancel | 取消設定並關閉窗口。 | |

表格 19-6 應用層防火牆 - 報表匯出欄位說明

**步驟 3 儲存報表**

選擇您要儲存報表的資料夾，然後點擊 **Save** 完成設定。

**Reports > Application Firewall > Event View > Export**



# 第20章
# 即時通訊管理員報表

*本章介紹即時通訊管理員報表的應用。*

## 20.1 需求

1. 管理人員希望知道前 10 名合法的即時通訊使用者排行。
2. 管理人員希望知道合法傳送檔案的即時通訊使用者排行。
3. 管理人員希望知道 RD “Evan” 合法使用的即時通訊行爲。
4. 管理人員希望將事件記錄儲存成 Excel 檔，可以依據自己的需求產生其他的報表格式。

## 20.2 方法

1. 到 Reports > IM Manager > Funcational View > Top Allowed Users 檢視圖形報表。
2. 到 Reports > IM Manager > Policy View > Top Allowed Users of Service，並於進階搜尋上勾選 Action 選擇 file。
3. 到 Reports > IM Manager > Personal View > Top Allowed Services of User，並於進階搜尋的 User 欄位填入 Evan。
4. 到 Reports > IM Manager > Event View，點擊 Export，選擇資料匯出類型爲 Excel。

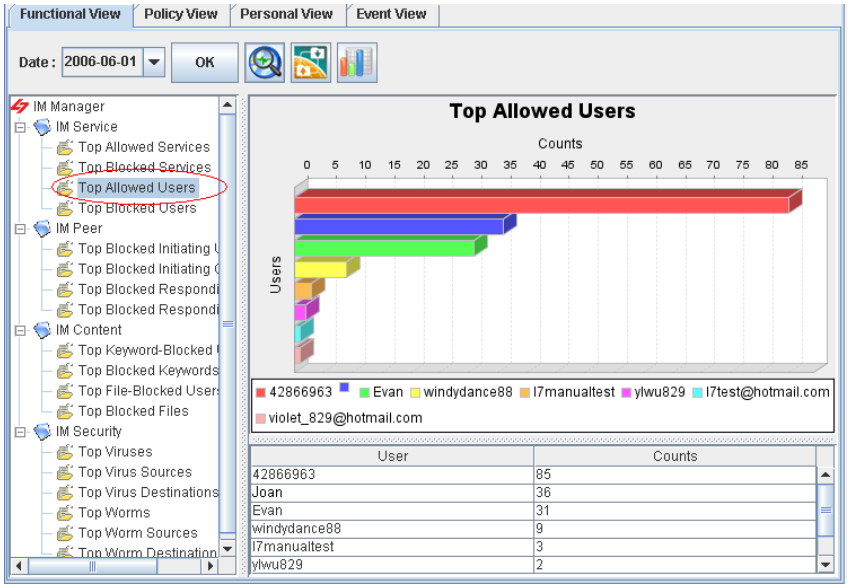
## 20.3 步驟

### 20.3.1 功能面報表流覽

**步驟 1 點擊被許可的使用者排行**

點擊 **Top Allowed Users**。

**Reports > IM Manager > Functional View > Top Allowed Users**




| 欄位 | 說明 |
|---|---|
| IM Service | 依管理者所設定的即時通訊服務規則，定義其服務與使用者之間的關係。即時通訊服務報表可分成：1) 被許可的服務排行), 2) 被攔阻的服務排行), 3) 被許可的使用者排行, 4) 被攔阻的使用者排行。 |
| IM Peer | 依管理者所設定的即時通訊聊天物件規則，定義聊天物件彼此之間的關係。聊天物件報表可分成兩 |

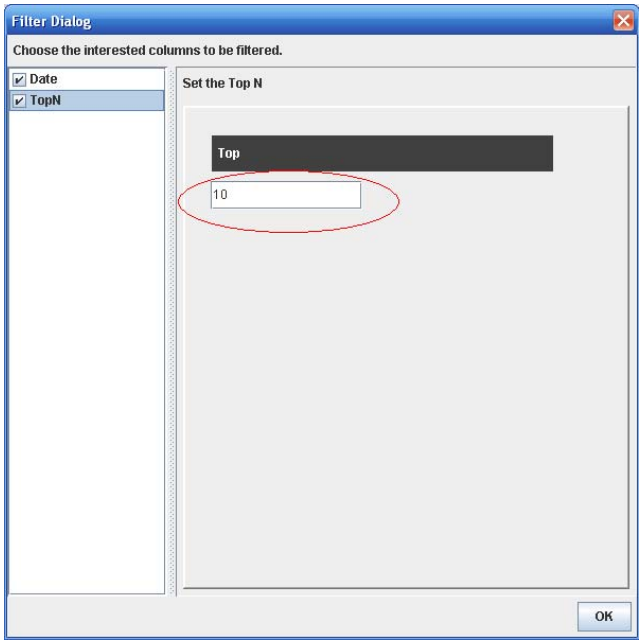
| | |
|---|---|
| | 大類：1) 因發起聊天被攔阻之使用者/群組排行）; 2) 因回應聊天被攔阻之使用者/群組排行。 |
| IM Content | 依管理者所設定的即時通訊內容過濾（關鍵字過濾、檔案過濾），可檢視非法關鍵字與檔案的使用情形。可分成：1) 被攔阻關鍵字的使用者排行; 2) 被攔阻的關鍵字排行; 3) 傳送檔案被攔阻的使用者排行; 4) 被攔阻的檔案名排行。 |
| IM Security | 依管理者所設定的即時通訊安全防護所產生的報表，可檢視病毒/蠕蟲排行、遭受攻擊的目的端排行，與發送病毒攻擊的來源端排行。 |

表格 20-1 即時通訊管理員 - 報表專案說明

**步驟 2 進階搜尋報表**

勾選 TopN，然後在 Top 欄位上輸入 10。點擊 **OK** 流覽結果。

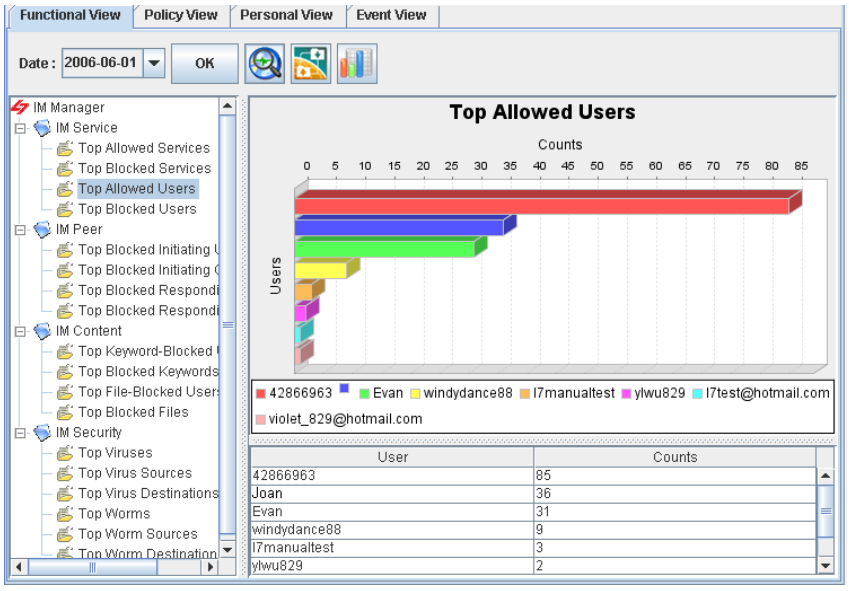
**Reports > IM Manager > Functional View > Top Allowed Users**



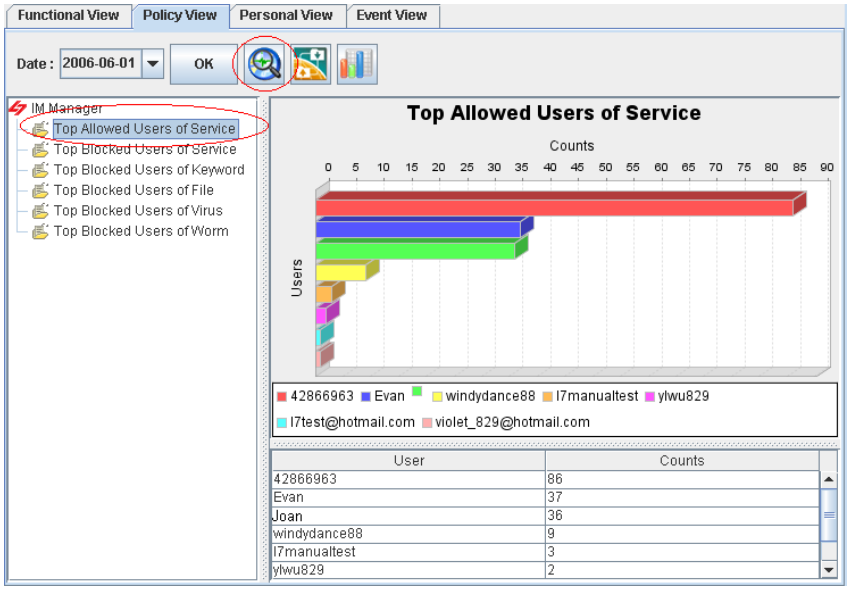

**步驟 3 流覽搜尋的結果**

右圖爲前 10 名被允許的使用者排名圖表。

**Reports > IM Manager > Functional View > Top Allowed Users**



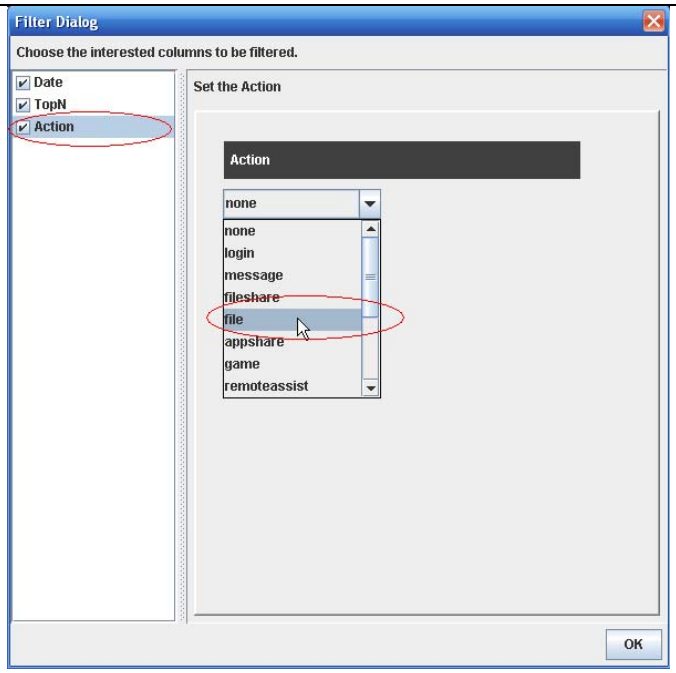
### 20.3.2 政策面報表流覽

| **步驟 1 流覽被允許使用即時通訊的使用者排名**<br>點擊 **Top Allowed Users of Service**。然後點擊圖示 進階設定。 | **Reports > IM Manager > Policy View > Top Allowed Users of Service**<br>  |
|---|---|

| 報表專案 | 說明 |
|---|---|
| Top Allowed Users of Service | 可依搜尋的服務，查詢被允許使用此服務的使用者排行。 |
| Top Blocked Users of Service | 可依搜尋的服務，查詢因使用此服務而被攔阻的使用者排行。 |
| Top Blocked Users of Keyword | 可依搜尋的關鍵字，查詢因傳送訊息內容含有此關鍵字而被攔阻的使用者排行。 |
| Top Blocked Users of File | 可依搜尋的檔名，查詢因傳送此檔名而被攔阻的使用者排行。 |
| Top Blocked Users of Virus | 可依搜尋的病毒，查詢因傳送/接收此病毒而被攔阻的使用者排行。 |
| Top Blocked Users of Worm | 可依搜尋的蠕蟲，查詢因傳送/接收此蠕蟲而被攔阻的使用者排行。 |

表格 20-2 即時通訊管理員 - 政策面報表說明

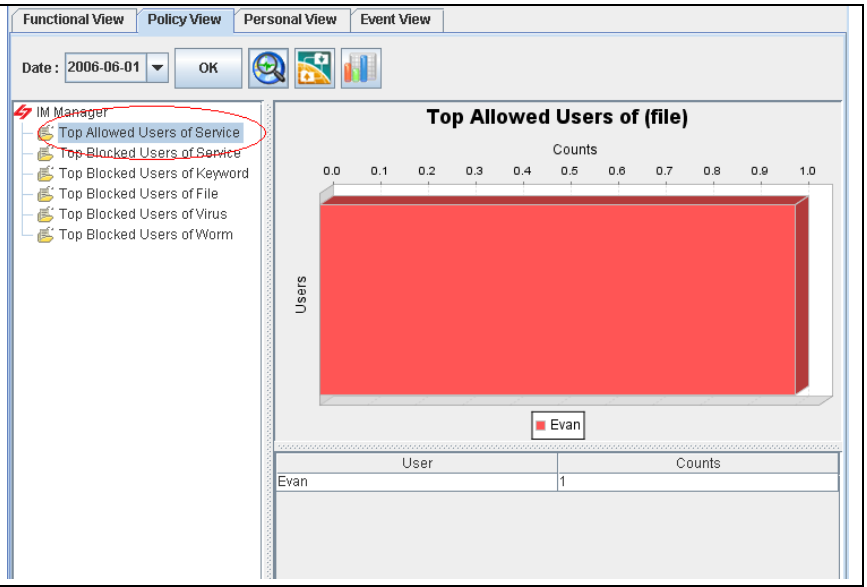
| **步驟 2 進階搜尋報表**<br>勾選 Action，然後在 Action 列表上點選 **File**。點擊 **OK** 流覽結果。 | **Reports > IM Manager > Policy View > Top Allowed Users of Service > Advanced** |
|---|---|




| 報表專案 | 說明 | 範例 |
|---|---|---|
| Date | 可設定要搜尋的資料之期間。注意，這個期間的有效範圍爲當您在管理伺服器所設定的資料分割週期，超過資料分割週期的期間設定是無效的。也就是當您所設定的資料分割週期爲每個月分割一個表格，您所選擇的搜尋期間就不可以超過該月的範圍。預設上，這個日期期間會依當周的日期爲主，如果您在報表畫面上看不到過去的圖表，請在此選擇適當的日期。 | 2006/06/01 ~ 2006/06/30 |
| TopN | 您在報表畫面上希望看到的排行數。如果您希望只看前 10 筆，請填入 10。 | 10 |
| Action | 即時通訊服務的搜尋條件。可依搜尋的即時通訊服務，查詢使用此即時通訊服務而被允許/被攔阻的使用者排行。 | File |

表格 20-3 即時通訊管理員 - 政策面報表進階搜尋說明

| **步驟 3 流覽設定的結果**<br>右圖爲被允許傳送檔案的使用者排行。 | **Reports > IM Manager > Policy View > Top Allowed Users of Service of (File)** |
|---|---|

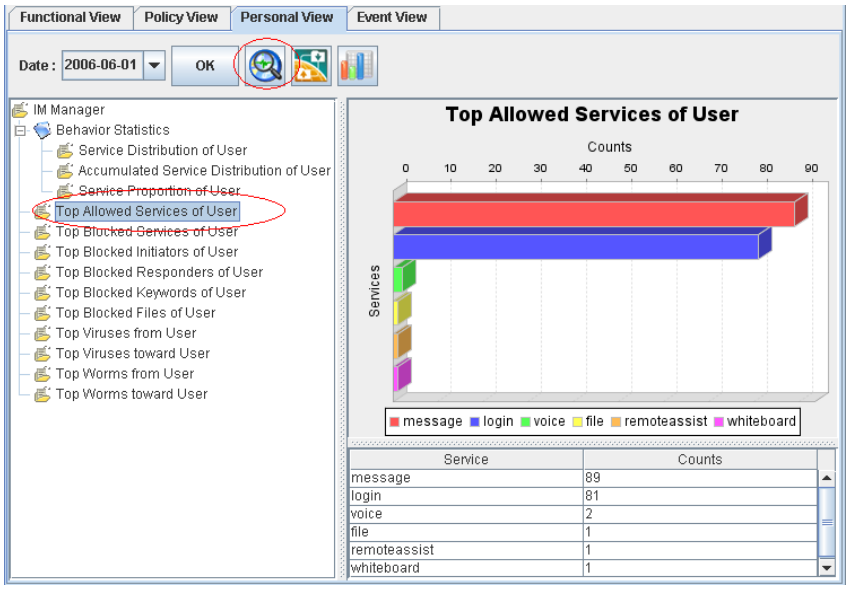



## 20.3.3 個人面報表流覽

**步驟 1 流覽合法的即時通訊服務排行**

點擊 **Top Allowed Services of Users**。然後點擊圖示 進階設定。

**Reports > IM Manager > Personal View > Top Allowed Services of User**




| 報表專案 | 說明 |
|---|---|
| Behavior Statistics | 可流覽所搜尋的使用者，其使用即時通訊細部行爲的分佈狀況、累積服務分佈與該使用者的使用的服務比例。 |
| Top Allowed Services of User | 依搜尋的使用者，查詢其合法使用的服務排行。 |
| Top Blocked Services of User | 依搜尋的使用者，查詢其違法使用的服務排行。 |
| Top Blocked Initiators of User | 依搜尋的使用者，查詢其因發起聊天而被攔阻的使用者排行。 |
| Top Blocked Responders of User | 依搜尋的使用者，列出因回應聊天要求而被攔阻的使用者排行。 |

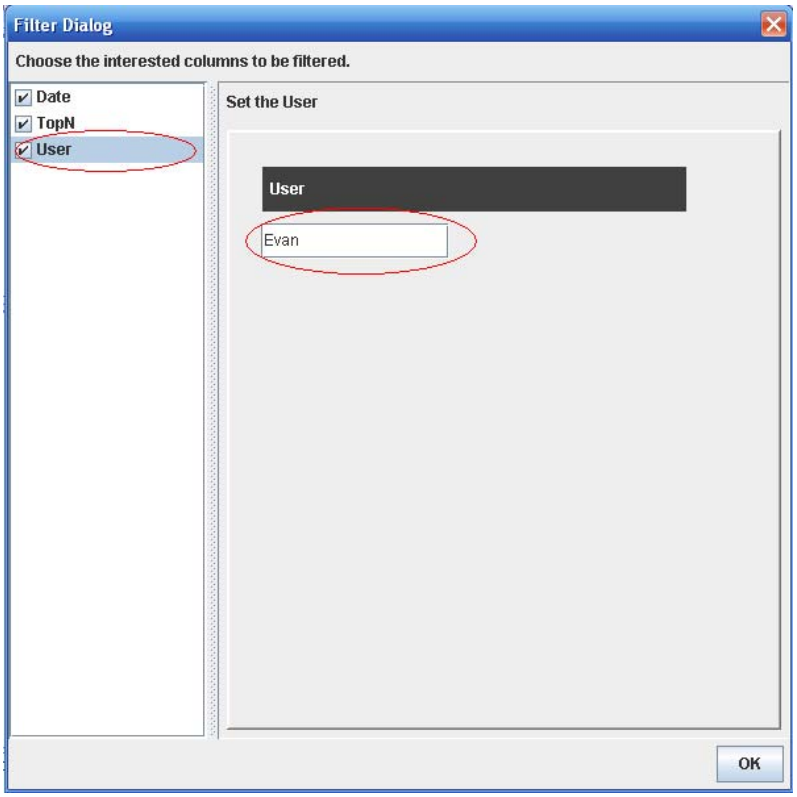
| | |
|---|---|
| Top Blocked Keywords of User | 依搜尋的使用者，查詢其被攔阻的關鍵字排行。 |
| Top Blocked Files of User | 依搜尋的使用者，查詢其被攔阻的檔案排行。 |
| Top Viruses from User | 依搜尋的使用者，查詢其發送的病毒種類排行。 |
| Top Viruses toward User | 依搜尋的使用者，查詢其遭受的病毒種類排行。 |
| Top Worms from User | 依搜尋的使用者，查詢其發送的蠕蟲種類排行。 |
| Top Worms toward User | 依搜尋的使用者，查詢其遭受的蠕蟲種類排行。 |

表格 20-4 即時通訊管理員 - 個人面報表說明

**步驟 2 進階搜尋報表**

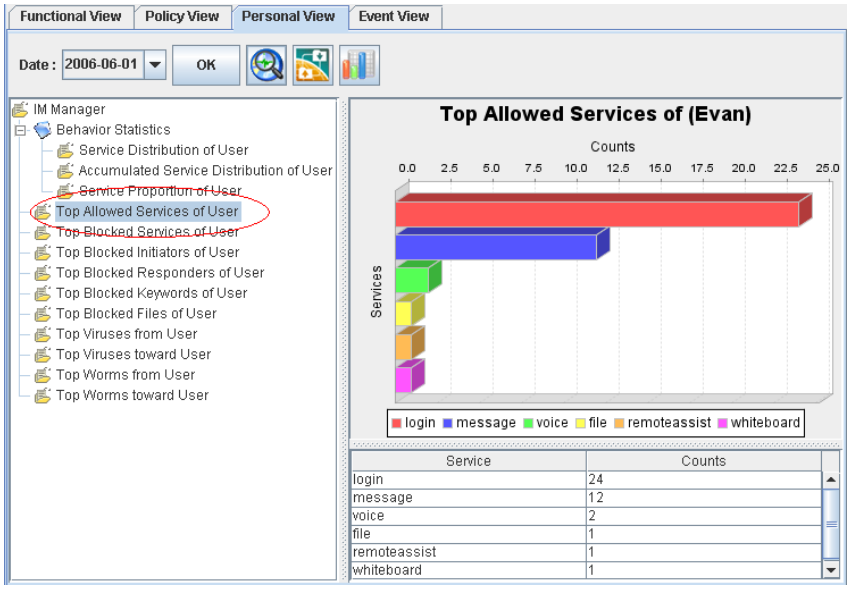
勾選 Src IP，然後在 User 欄位上輸入 **Evan**。點擊 **OK** 流覽結果。

**Reports > IM Manager > Personal View > Top Allowed Services of User > Advanced**

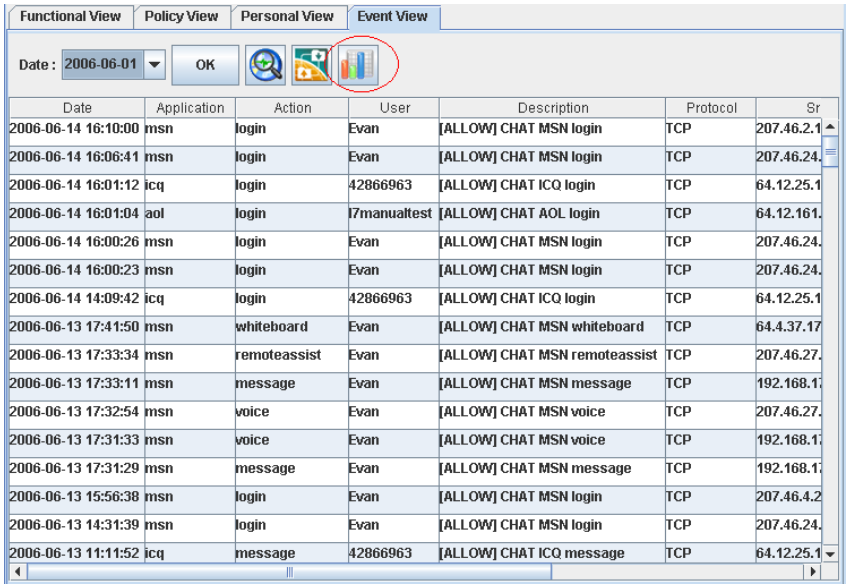


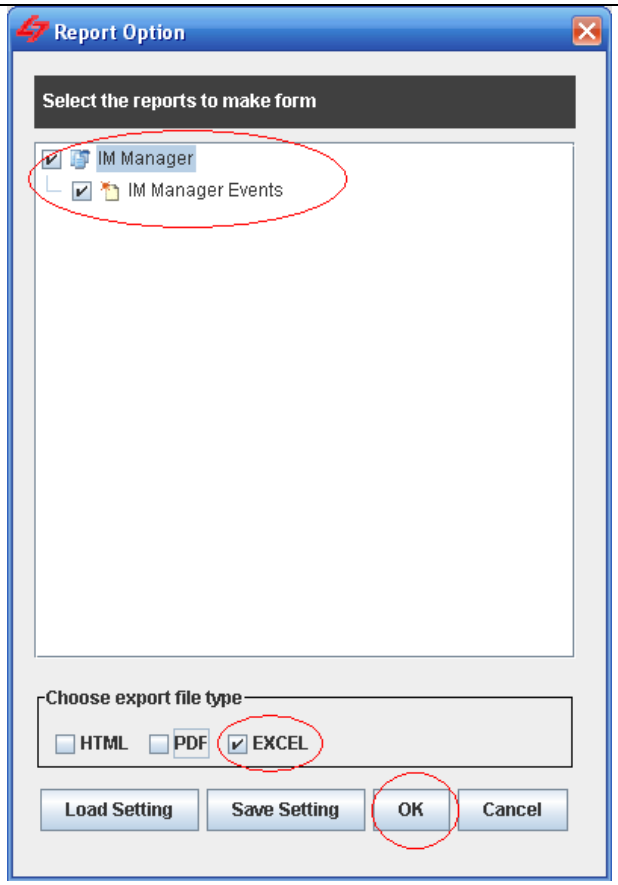

| 報表專案 | 說明 | 範例 |
|---|---|---|
| Date | 可設定要搜尋的資料之期間。注意，這個期間的有效範圍爲您在管理伺服器時所設定的資料分割週期，超過資料分割週期的期間設定是無效的。也就是當您所設定的資料分割週期爲每個月分割一個表格，您所選擇的搜尋期間就不可以超過該月的範圍。預設上，這個日期期間會依當周的日期爲主，如果您在報表畫面上看不到過去的圖表，請在此選擇適當的日期。 | 2006/06/01 ~ 2006/06/30 |
| TopN | 您在報表畫面上希望看到的排行數。如果您希望只看前 10 筆，請填入 10。 | 10 |
| User | 查詢使用者（在此指的是 IM User），列舉此使用者所使用的合法服務排名。 | 192.168.17.58 |

表格 20-5 即時通訊管理員 - 個人面報表進階搜尋說明

| | |
|---|---|
| **步驟 3 流覽搜尋結果**<br>右圖使用者 Evan 所使用的合法即時通訊服務排名。 | **Reports > IM Manager > Personal View > Top Allowed Services of (Evan)**<br>  |

## 20.3.4 匯出事件報表

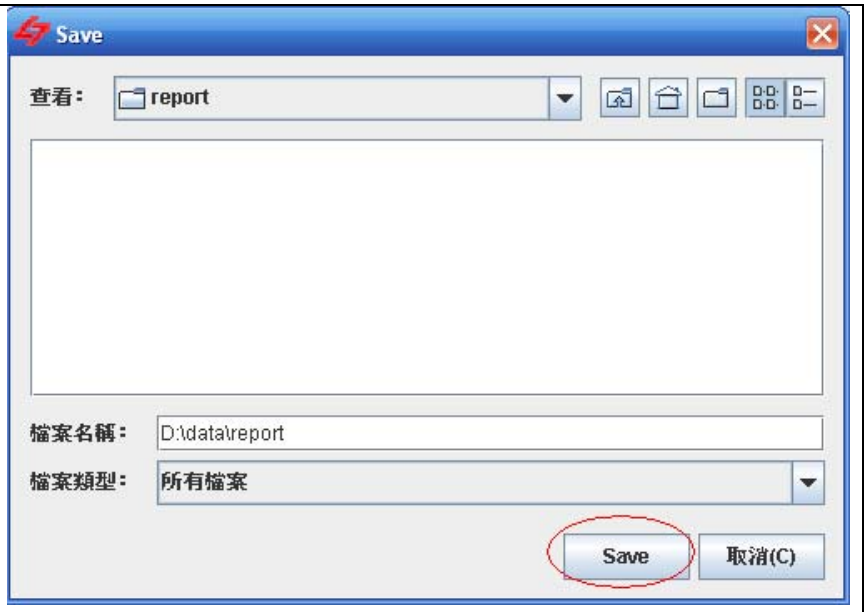
| | |
|---|---|
| **步驟 1 匯出事件報表**<br>點擊圖示 進階設定。 | **Reports > IM Manager > Event View**<br>  |
| **步驟 2 選擇匯出報表的專案**<br>勾選您要匯出的報表專案，然後勾選會出報表的類型爲 Excel，點擊 OK 繼續。 | **Reports > IM Manager > Event View > Export** |




| 欄位 / 按鈕 | 說明 | 範例 |
|---|---|---|
| IM Manager | 即時通訊管理員可以匯出的事件記錄。 | AF Events |
| Choose export file type | 選擇要匯出報表的格式。有三種檔案類型可供選擇：1) HTML 2) PDF 3) EXCEL （提供原始事件資料，可供使用者自行制定報表。） | EXCEL |
| **Button** | | |
| Load Setting | 將之前已儲存的報表設定檔載入。 | |
| Save Setting | 儲存報表設定檔。 | |
| OK | 套用設定。 | |
| Cancel | 取消設定並關閉窗口。 | |

表格 20-6 即時通訊管理員 - 報表匯出欄位說明

| **步驟 3 儲存報表**<br>選擇您要儲存報表的資料夾，然後點擊 **Save** 完成設定。 | **Reports > IM Manager > Event View > Export** |
|---|---|


Save
查看:
report
檔案名稱:
D:\data\report
檔案類型:
所有檔案
Save
取消(C)

# 第21章
# 網頁管理員報表

*本章節介紹網頁管理員報表的應用。*

## 21.1 需求

1. 管理人員希望知道前 10 名存取網站排名。
2. 管理人員希望知道因違反網頁管理員政策的控管類別（content_object）而被攔阻的網站排名。
3. 管理人員希望知道 192.168.17.58 這台電腦到目前爲止的前 10 名存取網頁排名。
4. 管理人員希望將事件記錄儲存成 Excel 檔，可以依據自己的需求產生其他的報表格式。

## 21.2 方法

1. 到 Reports > Web Manager > Funcational View > Top Access Sites 檢視圖形報表。
2. 到 Reports > Web Manager > Policy View > Top Blocked Sites of Reason，並於進階搜尋上勾選 Function Type 選擇 content_object。
3. 到 Reports > Web Manager > Personal View > Top Access Sites of User，並於進階搜尋的 Src IP 欄位填入 192.168.17.58。
4. 到 Reports > Web Manager > Event View，點擊 Export，選擇資料匯出類型爲 Excel。

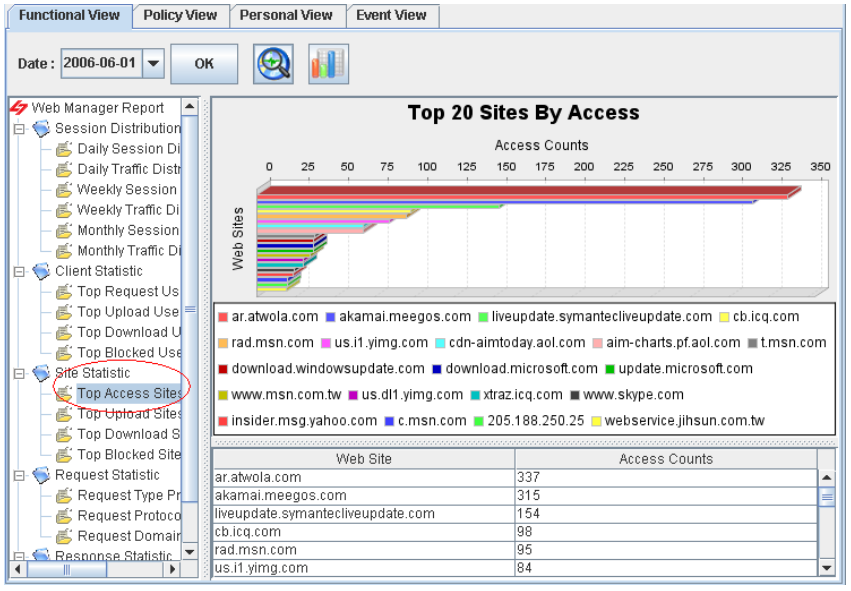
## 21.3 步驟

### 21.3.1 功能面報表流覽

**步驟 1 點擊存取網站排名項目**

點擊 **Top Access Sites**。

**Reports > Web Manager > Functional View > Top Access Sites**




| 項目 | 說明 |
|---|---|
| Session Distribution | 可查詢每日、每週、每月的流覽/回應網頁的連線次數與流量分佈狀況。每日以 24 小時爲單位， |

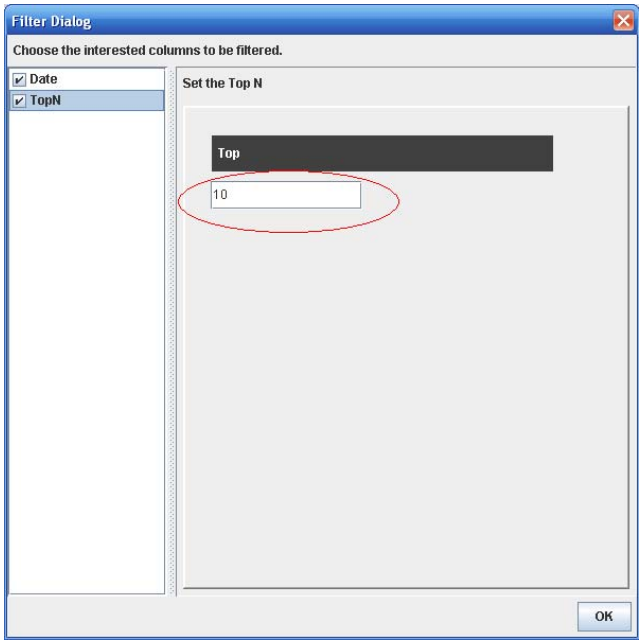
| | |
|---|---|
| | 每週與每月皆以日期爲單位。 |
| Client Statistic | 可查詢網頁流覽網頁/上傳/下載與因流覽網頁而被攔阻的使用者排行。 |
| Site Statistic | 可查詢熱門存取網站/上傳網站/下載網站/被攔阻的網站排行。 |
| Request Statistic | 可查詢網頁流覽的存取方法/通訊協定/網域等的比例。 |
| Response Statistic | 可查詢網頁回應內容型別/流量等的比例。 |

表格 21-1 網頁管理員 - 功能面報表專案說明

**步驟 2 進階搜尋報表**

勾選 TopN，然後在 Top 欄位上輸入 10。點擊 **OK** 流覽結果。

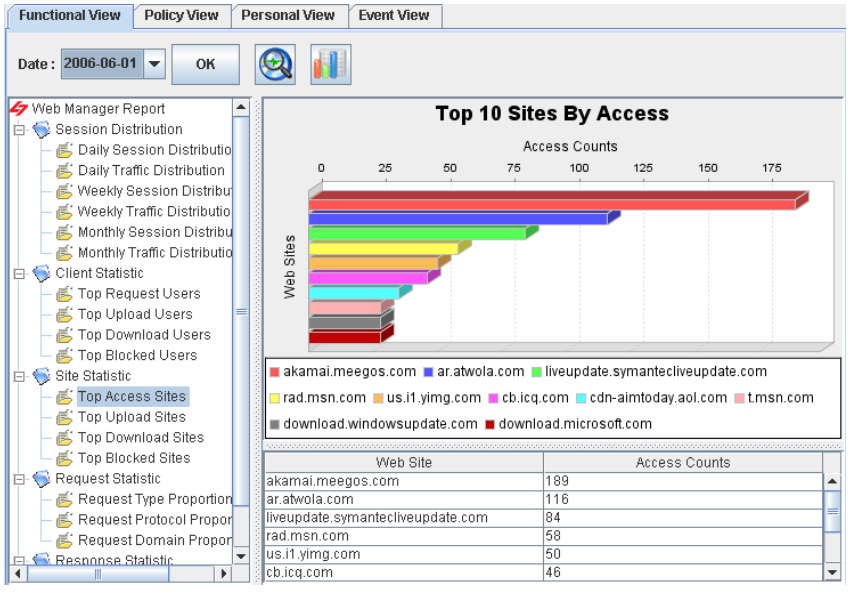
**Reports > Web Manager > Functional View > Top Access Sites**




**步驟 3 流覽搜尋的結果**

右圖爲前 **10** 名被允許的使用者排名圖表。

**Reports > Web Manager > Functional View > Top Access Sites**

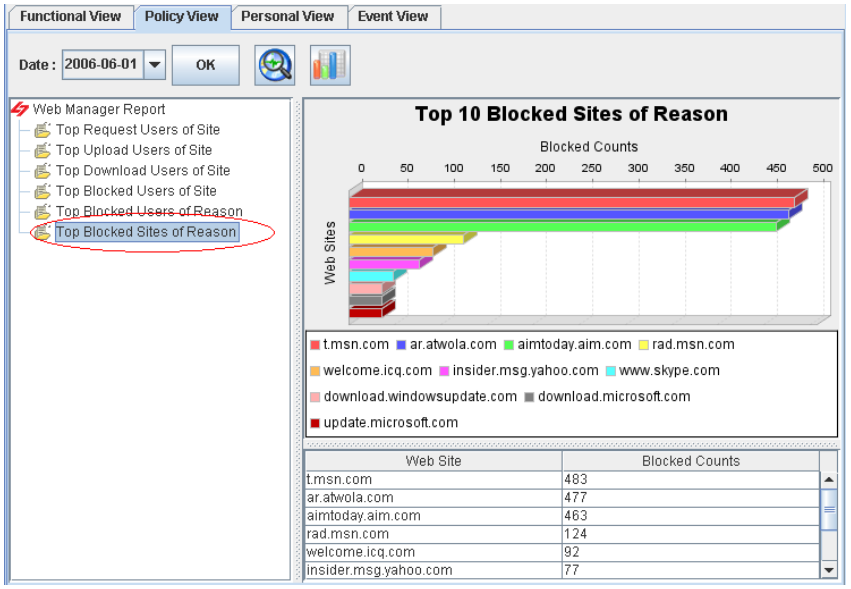


### 21.3.2 政策面報表流覽

**步驟 1 流覽被攔阻的網站排名**

點擊 **Top Blocked Sites of Reason**。然後點擊圖示 進階設定。

**Reports > Web Manager > Policy View > Top Blocked Sites of Reason**



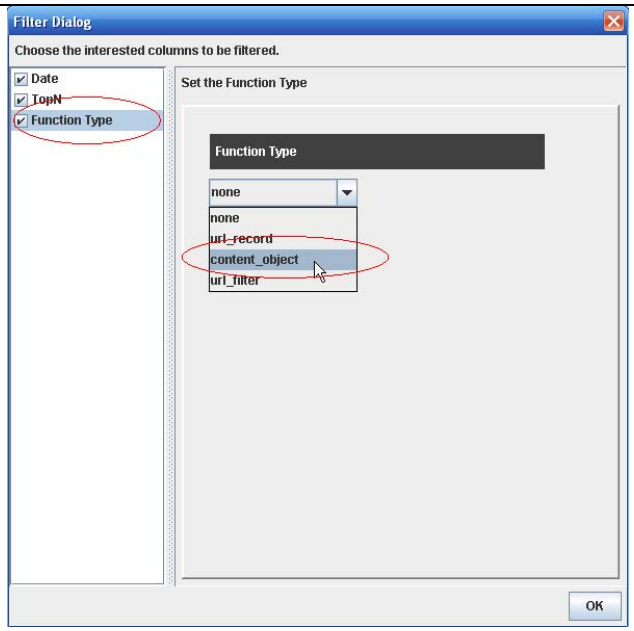

| 報表專案 | 說明 |
|---|---|
| Top Request Users of Site | 可依搜尋的網站，查詢經常流覽此網站的使用者排行。 |
| Top Upload Users of Site | 可依搜尋的網站，查詢經常上傳此網站的使用者排行。 |
| Top Download Users of Site | 可依搜尋的網站，查詢經常下載此網站的使用者排行。 |
| Top Blocked Users of Site | 可依搜尋的網站，查詢因流覽此網站而被攔阻的使用者排行。 |
| Top Blocked Users of Reason | 可依搜尋的控管類別，查詢因違反此控管類別政策而被攔阻的使用者排行。 |
| Top Blocked Sites of Reason | 可依搜尋的控管類別，查詢因違反此控管類別政策的網站排行。 |

表格 21-2 網頁管理員 - 政策面報表說明

**步驟 2 進階搜尋報表**

勾選 Function Type，然後在 Function Type 列表上點選 **content_object**。點擊 **OK** 流覽結果。

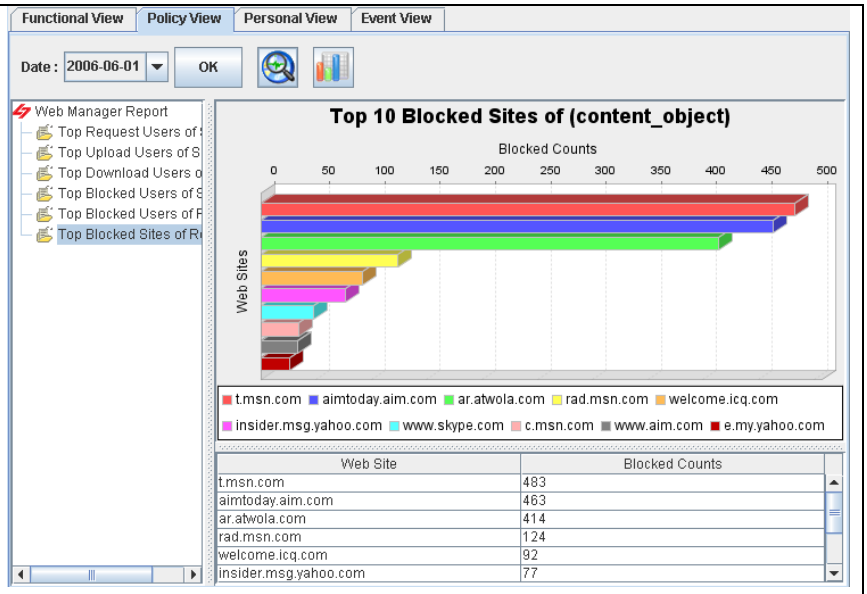
**Reports > Web Manager > Policy View > Top Blocked Sites of Reason > Advanced**




| 報表專案 | 說明 | 範例 |
|---|---|---|
| Date | 可設定要搜尋的資料之期間。注意，這個期間的有效範圍爲當您在管理伺服器所設定的資料分割週期，超過資料分割週期的期間設定是無效的。也就是當您所設定的資料分割週期爲每個月分割一個表格，您所選擇的搜尋期間就不可以超過該月的範圍。預設上，這個日期期間會依當周的日期爲主，如果您在報表畫面上看不到過去的圖表，請在此選擇適當的日期。 | 2006/06/01 ~ 2006/06/30 |
| TopN | 您在報表畫面上希望看到的排行數。如果您希望只看前 10 筆，請填入 10。 | 10 |
| Function Type | 網頁管理員報表的細部搜尋條件。可依搜尋的控管類別（Function Type），查詢所有違反控管類別政策的網站排名。 | content_object |

表格 21-3 網頁管理員政策 - 面報表進階搜尋說明

| **步驟 3 流覽設定的結果**<br>右圖爲因違反控管類別政策而被攔阻的網站排名。 | **Reports > Web Manager > Policy View > Top Blocked Sites of Reason** |
|---|---|

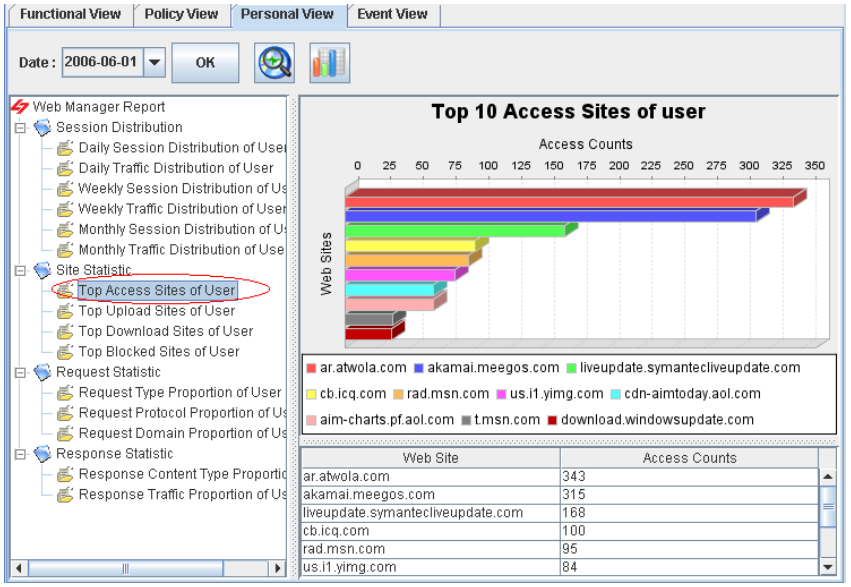



### 21.3.3 個人面報表流覽

**步驟 1 流覽使用者經常存取的網站排行**

點擊 **Top Allowed Services of Users**。然後點擊圖示 進階設定。

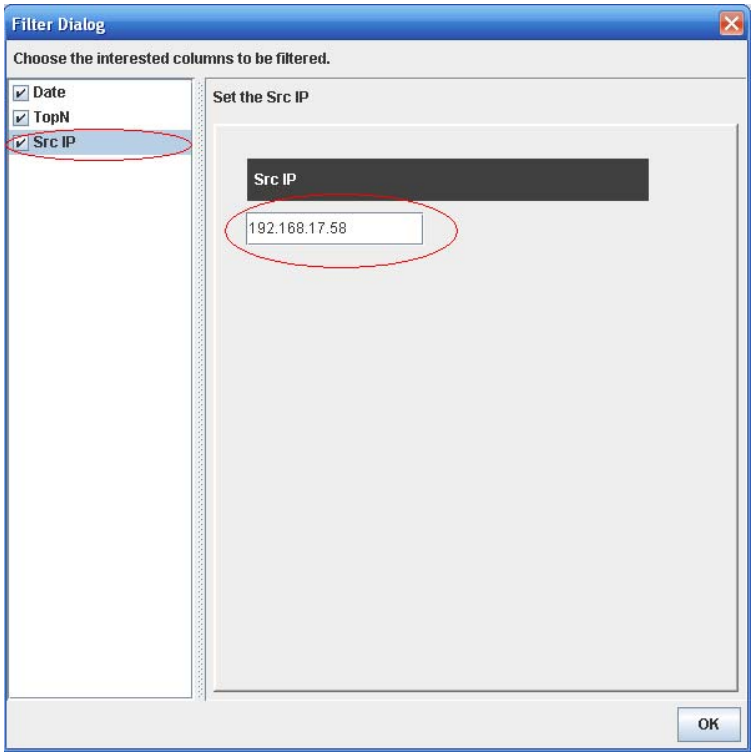
**Reports > Web Manager > Personal View > Top Access Sites of User**




| 報表專案 | 說明 |
|---|---|
| Session Distribution of User | 可依搜尋的使用者（IP），查詢此使用者每日、每週、每月的流覽/回應網頁的連線次數與流量分佈狀況。每日以 24 小時爲單位，每週與每月皆以日期爲單位。 |
| Site Statistic | 可依搜尋的使用者（IP），查詢此使用者存取網站/上傳/下載與流覽違法的網站排行。 |
| Request Statistic | 可依搜尋的使用者（IP），查詢此使用者經常存取網站/上傳網站/下載網站/被攔阻的網站排行。 |
| Response Statistic | 可依搜尋的使用者（IP），查詢此使用者網頁流覽的存取方法/通訊協定/網域等的 |

| | |
|---|---|
| | 比例。 |

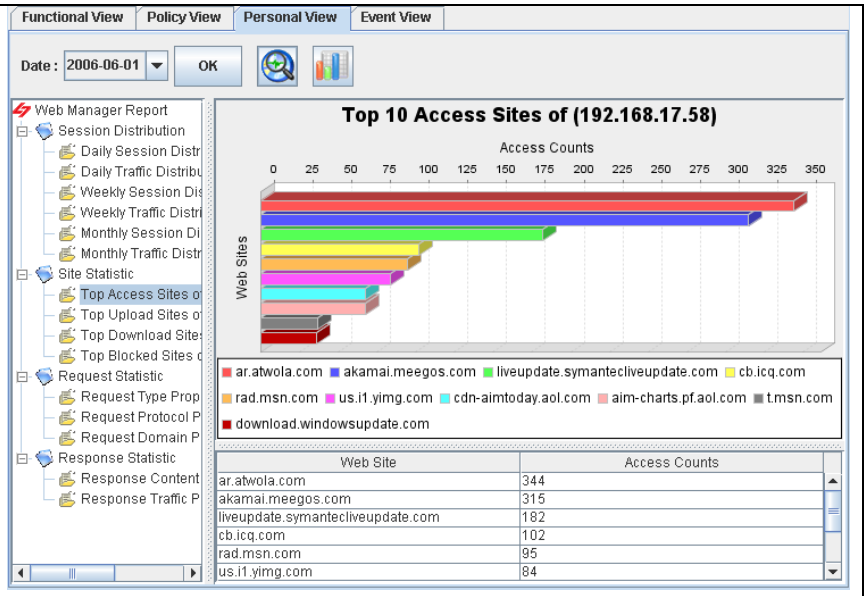
表格 21-4 網頁管理員 - 個人面報表說明

| | |
|---|---|
| **步驟 2 進階搜尋報表**<br>勾選 Src IP，然後在 Src IP 欄位上輸入 **192.168.17.58**。點擊 **OK** 流覽結果。 | **Reports > Web Manager > Personal View > Top Access Sites of User > Advanced**<br>  |

| 報表專案 | 說明 | 範例 |
|---|---|---|
| Date | 可設定要搜尋的資料之期間。注意，這個期間的有效範圍爲您在管理伺服器所設定的資料分割週期，超過資料分割週期的期間設定是無效的。也就是當您所設定的資料分割週期爲每個月分割一個表格，您所選擇的搜尋期間就不可以超過該月的範圍。預設上，這個日期期間會依當周的日期爲主，如果您在報表畫面上看不到過去的圖表，請在此選擇適當的日期。 | 2006/06/01 ~ 2006/06/30 |
| TopN | 您在報表畫面上希望看到的排行數。如果您希望只看前 10 筆，請填入 10。 | 10 |
| Src | 查詢使用者（在此指的是使用者的 IP），查詢此使用者的存取網站排行。 | 192.168.17.58 |

表格 21-5 網頁管理員 - 個人面報表進階搜尋說明

| | |
|---|---|
| **步驟 3 流覽搜尋結果**<br>右圖爲使用者 192.168.17.58 的存取網站排行。 | **Reports > Web Manager > Personal View > Top Access Sites of User** |

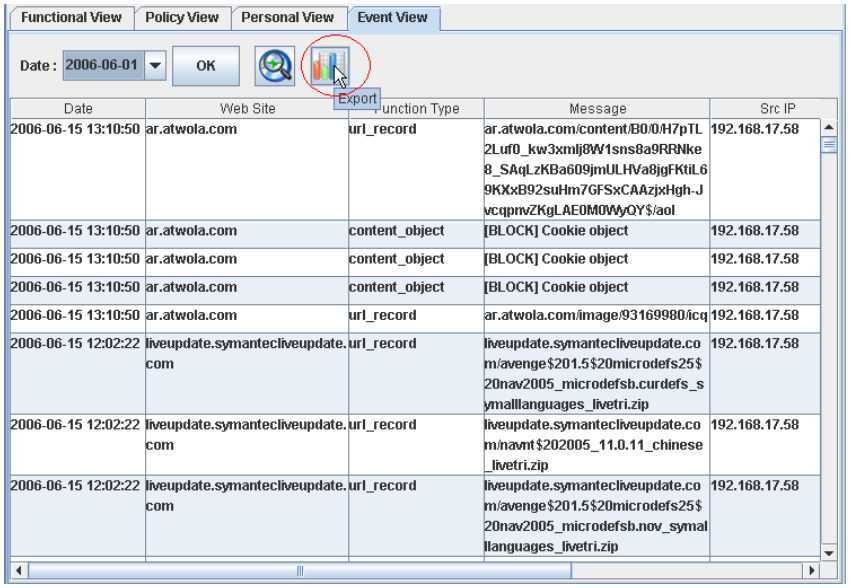



## 21.3.4 匯出事件報表

**步驟 1 匯出事件報表**

點擊圖示 進階設定。

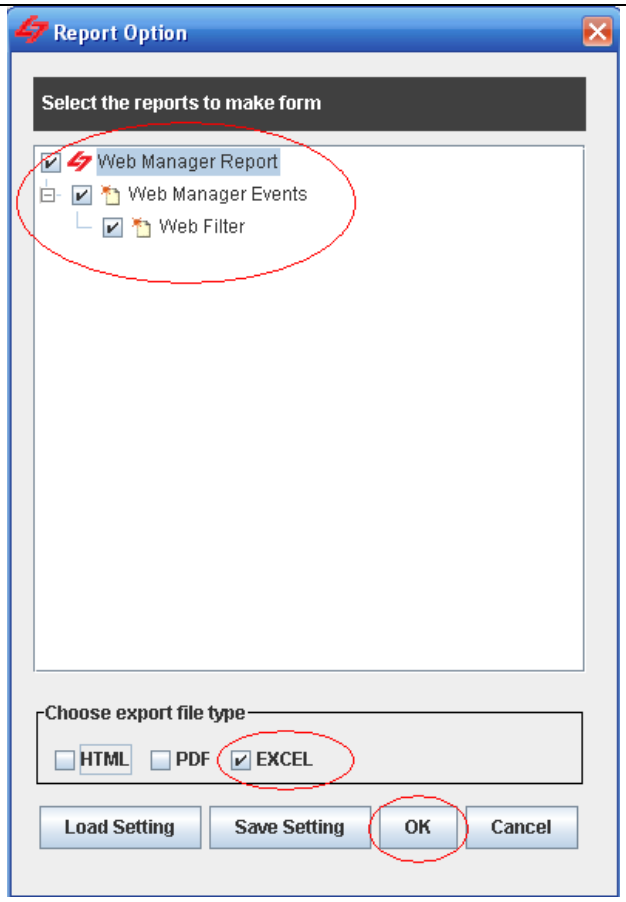
**Reports > Web Manager > Event View**




**步驟 2 選擇匯出報表的專案**

勾選您要匯出的報表專案，然後勾選會出報表的類型爲 Excel，點擊 OK 繼續。

**Reports > Web Manager > Event View > Export**



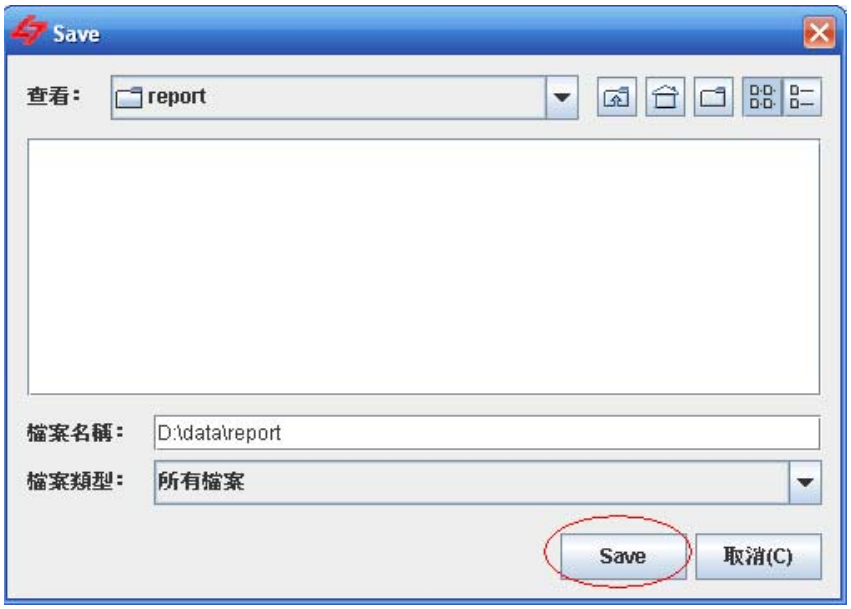

| 欄位 / 按鈕 | 說明 | 範例 |
|---|---|---|
| Web Manager | 網頁管理員可以匯出的事件記錄。 | Web Manager Events<br>Web Filter |
| Choose export file type | 選擇要匯出報表的格式。有三種檔案類型可供選擇：1) HTML 2) PDF 3) EXCEL （提供原始事件資料，可供使用者自行制定報表。） | EXCEL |
| **Button** | | |
| Load Setting | 將之前已儲存的報表設定檔載入。 | |
| Save Setting | 儲存報表設定檔。 | |
| OK | 套用設定。 | |
| Cancel | 取消設定並關閉窗口。 | |

表格 21-6 網頁管理員 - 報表匯出欄位說明

**步驟 3 儲存報表**

選擇您要儲存報表的資料夾，然後點擊 **Save** 完成設定。

**Reports > Web Manager > Event View > Export**



# 第22章
# 流量管理員報表

*本章節介紹流量管理員報表的應用。*

## 22.1 需求

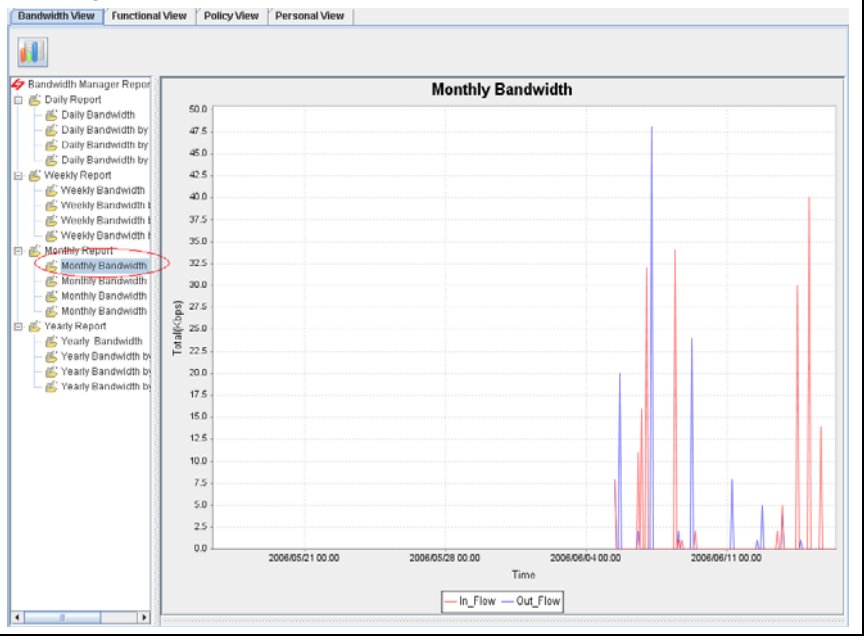
1. 管理人員希望知道 2006 年 6 月份的頻寬使用狀況。
2. 管理人員希望知道 2006 年 6 月 15 日網路進出總流量最大的前 5 名使用者排行。
3. 管理人員希望知道 2006 年 6 月 15 日使用 FTP 與 HTTP 等應用軟體的最大總流量之使用者排行。
4. 管理人員希望知道 2006 年 6 月 15 日使用者（192.168.17.58）使用的應用軟體之最大總流量排行。

## 22.2 方法

1. 到 Reports > Traffic Manager > Bandwidth View > Monthly Report > Monthly Bandwidth 檢視圖形報表。
2. 到 Reports > Traffic Manager > Functional View > Daily Totoal Traffic > Daily Top Total Traffic by User，並於進階搜尋上的 TopN 欄位上填入 5。
3. 到 Reports > Traffic Manager > Policy View > Daily Top Total Traffic by User of Application，並於進階搜尋的 Application 欄位選擇 ftp 與 http。
4. 到 Reports > Traffic Manager > Personal View > Daily Top Total Traffic by Application of User，並於進階搜尋上勾選 Sip，然後填入 IP 位址 192.168.17.58。

## 22.3 步驟

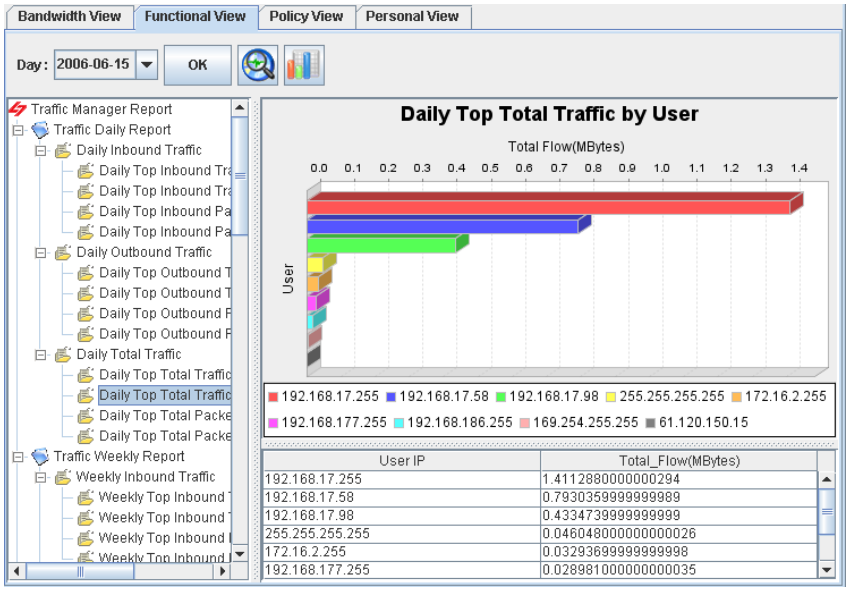
### 22.3.1 頻寬面報表流覽

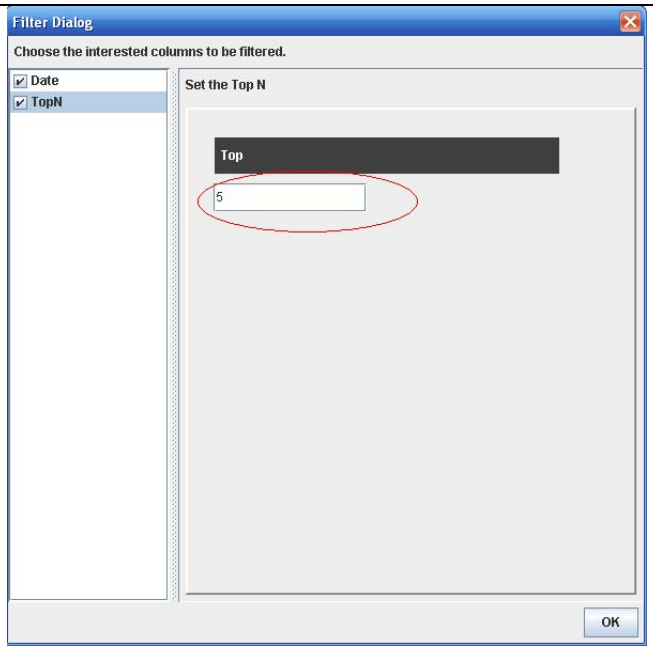
| | |
|---|---|
| **步驟 1 點擊每月頻寬折線圖**<br>點擊 Monthly Bandwidth。 | **Reports > Traffic Manager > Bandwidth View > Monthly Report > Monthly Bandwidth**<br>  |

| 欄位 | 說明 |
|---|---|
| Daily Report | 查詢每日頻寬狀況，依應用程式/頻寬類別/應用程式類別等分類方式，方便查詢對內頻寬/對外頻寬/總頻寬的流量。 |
| Weekly Report | 查詢每週頻寬狀況，依應用程式/頻寬類別/應用程式類別等分類方式，方便查詢對內頻寬/對外頻寬/總頻寬的流量。 |
| Monthly Report | 查詢每月頻寬狀況，依應用程式/頻寬類別/應用程式類別等分類方式，方便查詢對內頻寬/對外頻寬/總頻寬的流量。 |
| Yearly Report | 查詢每年頻寬狀況，依應用程式/頻寬類別/應用程式類別等分類方式，方便查詢對內頻寬/對外頻寬/總頻寬的流量。 |

表格 22-1 流量管理員 - 頻寬面報表專案說明

### 22.3.2 功能面報表流覽

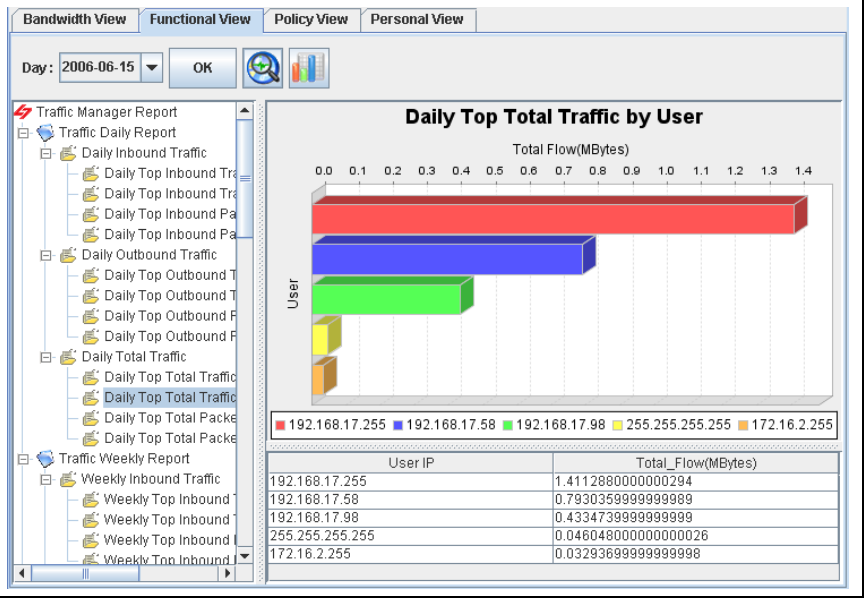
| | |
|---|---|
| **步驟 1 點擊每日最大流量之使用者排行**<br>在工具列上的 Day 欄位選擇 2006-06-15，點擊 **OK** 繼續。點擊 **Daily Top Total Traffic by User**，然後點擊圖示 進階設定。 | **Reports > Traffic Manager > Functional View > Daily Traffic Report > Daily Totoal Traffic > Daily Top Total Traffic by User**<br>  |
| **步驟 2 進階搜尋報表**<br>勾選 TopN，然後在 Top 欄位上輸入 5。點擊 **OK** 流覽結果。 | **Reports > Traffic Manager > Functional View > Daily Traffic Report > Daily Totoal Traffic > Daily Top Total Traffic by User** |




**步驟 3 流覽搜尋的結果**

右圖爲前 5 總流量最大的使用者排名。

**Reports > Traffic Manager > Functional View > Daily Traffic Report > Daily Totoal Traffic > Daily Top Total Traffic by User**

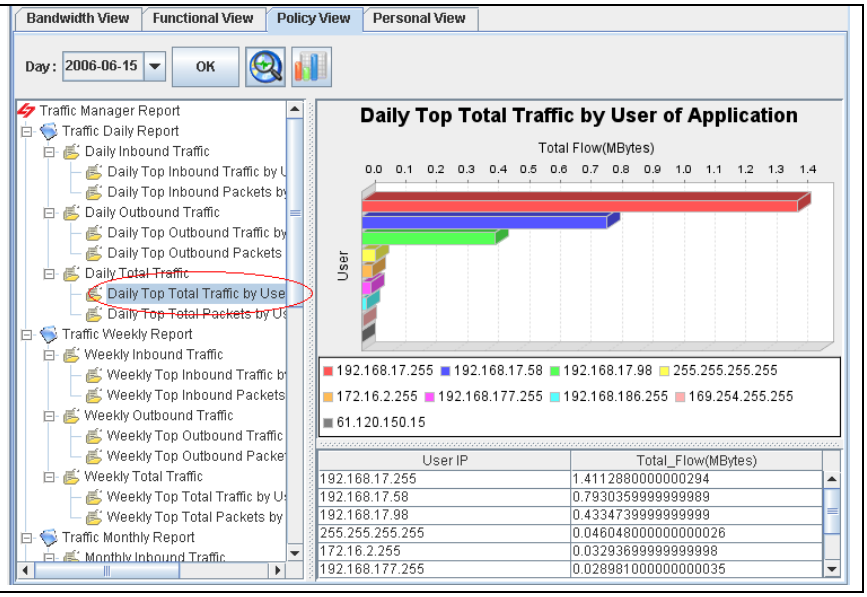



## 22.3.3 政策面報表流覽

**步驟 1 流覽每日應用程式流量最大的使用者排行**

點擊 **Daily Top Total Traffic by User of Application**。然後點擊圖示 進階設定。

**Reports > Traffic Manager > Policy View > Traffic Daily Report > Daily Total Traffic > Daily Top Totoal Traffic by User of Application**



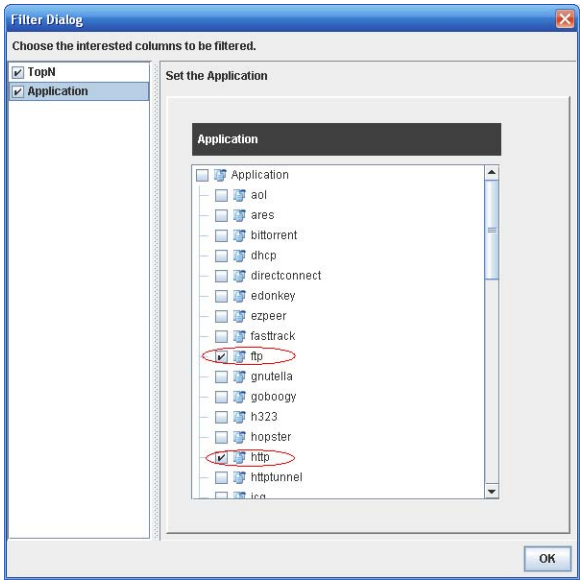

| 報表專案 | 說明 |
|---|---|
| Traffic Daily Report | 可查詢每日流量與封包數的對內/對外/總流量/總封包數的使用者排行與應用軟體排行。 |
| Traffic Weekly Report | 可查詢每週流量與封包數的對內/對外/總流量/總封包數的使用者排行與應用軟體排行。 |
| Traffic Monthly Report | 可查詢每月流量與封包數的對內/對外/總流量/總封包數的使用者排行與應用軟體排行。 |
| Traffic Quarterly Report | 可查詢每季流量與封包數的對內/對外/總流量/總封包數的使用者排行與應用軟體排行。 |
| Traffic Yearly Report | 可查詢每年流量與封包數的對內/對外/總流量/總封包數的使用者排行與應用軟體排行。 |

表格 22-2 流量管理員 - 政策面報表說明

**步驟 2 進階搜尋報表**

勾選 Application，然後在 Application 列表上勾選 **ftp 與 http**。點擊 **OK** 流覽結果。

**Reports > Traffic Manager > Policy View > Traffic Daily Report > Daily Total Traffic > Daily Top Totoal Traffic by User of Application**



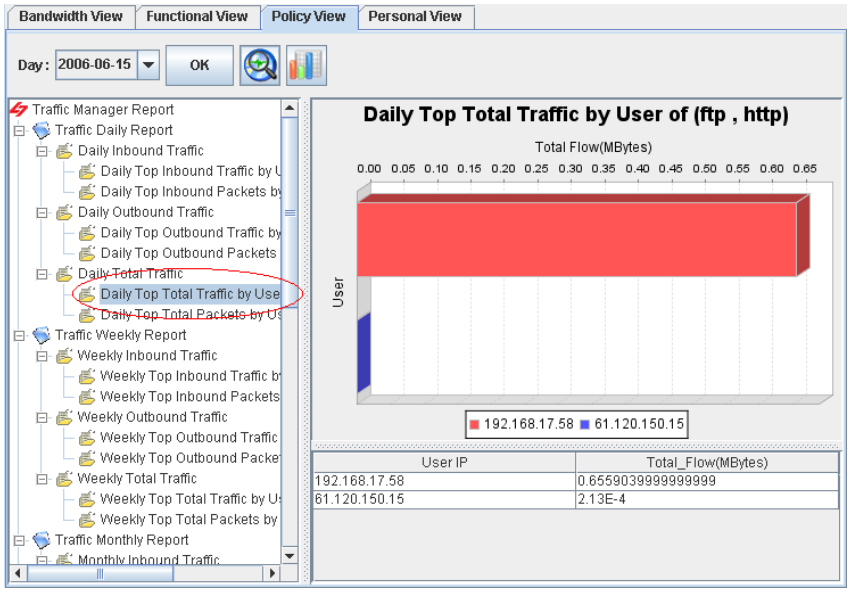
| 報表專案 | 說明 | 範例 |
|---|---|---|
| TopN | 您在報表畫面上希望看到的排行數。如果您希望只看前 10 筆，請填入 10。 | 10 |
| Application | 應用軟體的搜尋條件。可依搜尋的應用軟體，查詢使用此即時應用軟體的使用者排行。（可複選） | File |

表格 22-3 流量管理員 - 政策面報表進階搜尋說明

**步驟 3 流覽設定的結果**

右圖爲最常使用 ftp 與 http 應用軟體的使用者排行。

**Reports > Traffic Manager > Policy View > Traffic Daily Report > Daily Total Traffic > Daily Top Totoal Traffic by User of Application**

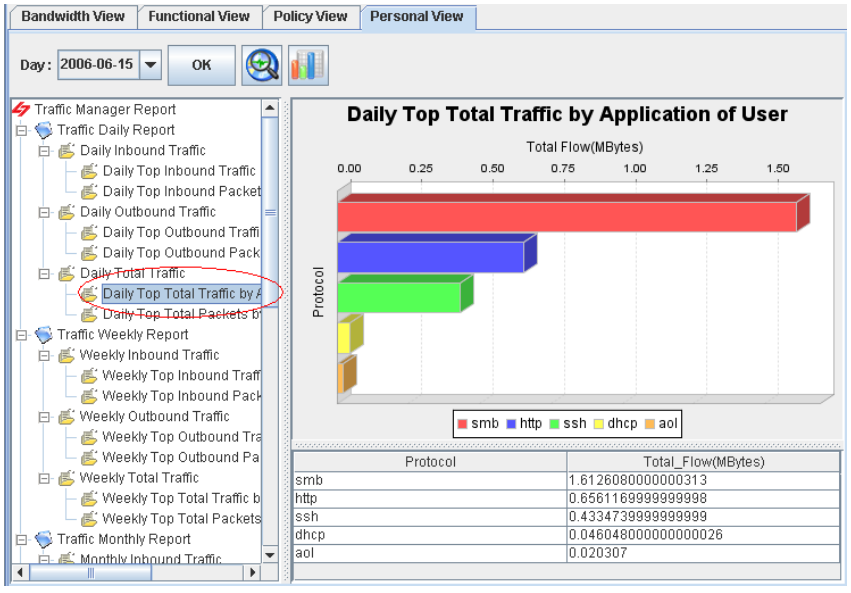



## 22.3.4 個人面報表流覽

**步驟 1 流覽使用者應用軟體的流量排行**

點擊 **Daily Top Total Traffic by Application of User**。然後點擊圖示 進階設定。

**Reports > Traffic Manager > Personal View > Traffic Daily Report > Daily Total Traffic > Daily Top Total Traffic by Application of User**



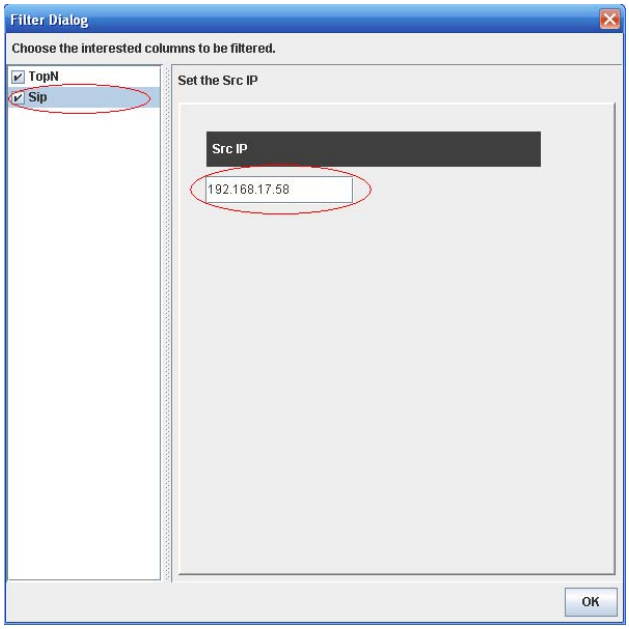
| 報表專案 | 說明 |
|---|---|
| Traffic Daily Report | 可依選擇的使用者，查詢其每日流量與封包數的對內/對外/總流量/總封包數排行與應用軟體排行。 |
| Traffic Weekly Report | 可依選擇的使用者，查詢其每週流量與封包數的對內/對外/總流量/總封包數的使用者排行與應用軟體排行。 |
| Traffic Monthly Report | 可依選擇的使用者，查詢其每月流量與封包數的對內/對外/總流量/總封包數的使用者排行與應用軟體排行。 |
| Traffic Quarterly Report | 可依選擇的使用者，查詢其每季流量與封包數的對內/對外/總流量/總封包數的使用者排行與應用軟體排行。 |
| Traffic Yearly Report | 可依選擇的使用者，查詢其每年流量與封包數的對內/對外/總流量/總封包數的使用者排行與應用軟體排行。 |

表格 22-4 流量管理員 - 個人面報表說明

**步驟 2 進階搜尋報表**

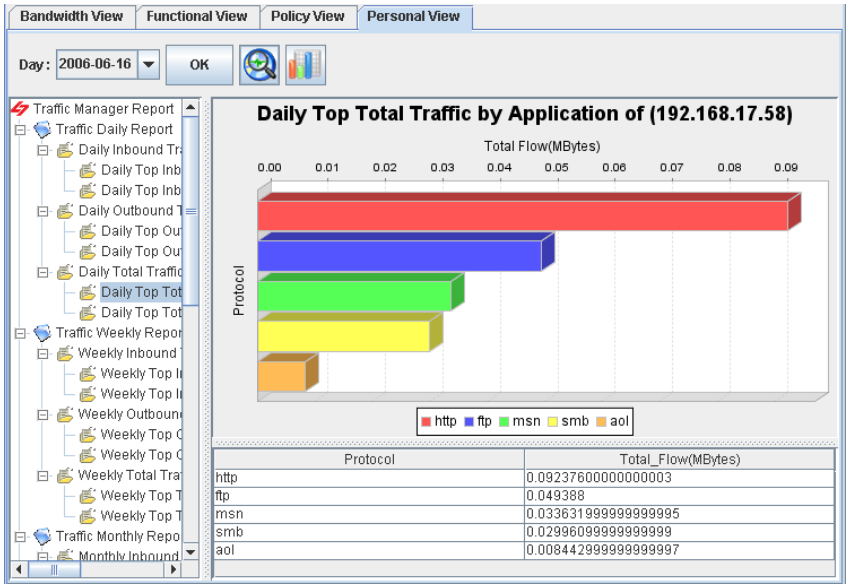
勾選 Src IP （Source IP），然後在 User 欄位上輸入 **Evan**。點擊 **OK** 流覽結果。

**Reports > IM Manager > Personal View > Top Allowed Services of User > Advanced**




| 報表專案 | 說明 | 範例 |
|---|---|---|
| Date | 可設定要搜尋的資料之期間。注意，這個期間的有效範圍爲您在管理伺服器時所設定的資料分割週期，超過資料分割週期的期間設定是無效的。也就是當您所設定的資料分割週期爲每個月分割一個表格，您所選擇的搜尋期間就不可以超過該月的範圍。預設上，這個日期期間會依當周的日期爲主，如果您在報表畫面上看不到過去的圖表，請在此選擇適當的日期。 | 2006/06/01 ~ 2006/06/30 |
| TopN | 您在報表畫面上希望看到的排行數。如果您希望只看前 10 筆，請填入 10。 | 10 |
| Sip | 查詢使用者（在此指的是來源端的 IP 位址），查詢此使用者所使用的應用軟體流量排行。 | 192.168.17.58 |

表格 22-5 流量管理員 - 個人面報表進階搜尋說明

| | |
|---|---|
| **步驟 3 流覽搜尋結果**<br>右圖使用者 Evan 所使用的合法即時通訊服務排名。 | **Reports > Application Firewall > Personal View > Top Blocked Protocols of User**<br>  |

# 第10部

# 側錄稽核

# 第23章 側錄稽核

*本章節介紹即時通訊與網頁的側錄。*

## 23.1 需求

爲符合 BS7799 的規範，說明企業執行 BS7799 計畫，InstantScan 階層式管理與稽核系統能夠保護使用者的隱私，免於一般人隨便流覽其聊天資訊。然而，當有洩密情況發生時，這些測錄資料亦可供稽核人員隨時采證，防範員工不法的舉動而危及公司。所以只有管理人員與稽核人員可以看到側錄的內容，網管人員只可以設定 InstantScan，無法進入側錄系統。目前側錄共有兩大類：

1) 即時通訊內容側錄：使用者使用的即時通訊軟體 MSN/Yahoo/ICQ/AOL 皆可即時側錄傳送的訊息與檔案，並以紅字標示違法的關鍵字與傳檔檔案名。
2) 網頁網址側錄：使用者流覽的網頁即時側錄。可以查詢使用者流覽網頁的狀況與其合法性。

## 23.2 方法

1. 到 Auditor > IM Recorder 檢視側錄內容。
2. 到 Auditor > Web Recorder 檢視側錄內容。

## 23.3 步驟

### 23.3.1 即時通訊內容側錄

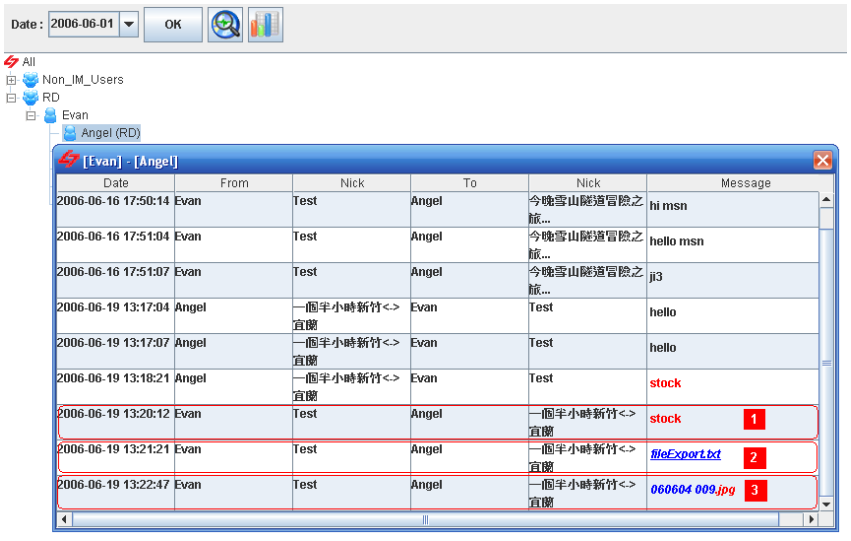
**步驟 4 即時通訊內容側錄**

只有管理人員與稽核人員可以看到側錄內容。當您打開即時通訊側錄器後，將有類似右圖的訊息顯示。即時通訊側錄器以樹狀結構顯示。第一層爲群組，第二層爲在此群組內的使用者，第三者爲與此使用者聊天的對象，第四層爲側錄到的訊息。如果您已經設定使用者規則，經由同一使用者規則內的所有帳號所傳送/ 接收的訊息內容都會顯示在同一個視窗內。當使用者不在即時通訊使用者群組內時，將會以 Non_IM_Users 顯示，所有側錄到的訊息會依使用者的即時通訊帳號逐條顯示。

側錄如右圖所示：

1. 關鍵字過濾：關鍵字以紅字顯示。
2. 檔案傳送：可將滑鼠移到檔案名上，點一下檔案，將其儲存在本地端電腦上，並開啓流覽。
3. 檔案過濾：違反檔案傳送規則的檔案名會以紅字顯示，並禁止使用者傳檔。

**Auditor > IM Recorder**




| 欄位 | 說明 | 範例 |
|---|---|---|
| Date | 傳送訊息的日期與時間。 | 2006-06-19 13:20:12 |
| From | 傳送訊息的使用者。當您在 IM User 上已有設定此使用者，則在此欄位會顯示您所設定的用戶名稱，否則將顯示即時通訊帳號。 | Evan |
| Nick | 傳送訊息的使用者的昵稱。此昵稱爲您在 MSN 即時通訊帳號所設定 | Test |

| | | |
|---|---|---|
| （只適用 MSN） | 的顯示名稱。 | |
| To | 接收訊息的使用者。當您在 IM User 上已有設定此使用者，則在此欄位會顯示您所設定的用戶名稱，否則將顯示即時通訊帳號。 | Angel |
| Nick<br>（只適用 MSN） | 接收訊息的使用者的昵稱。此昵稱爲您在 MSN 即時通訊帳號所設定的顯示名稱。 | 一個半小時新竹<->宜蘭 |
| Message | 即時通訊訊息內容。 | stock |

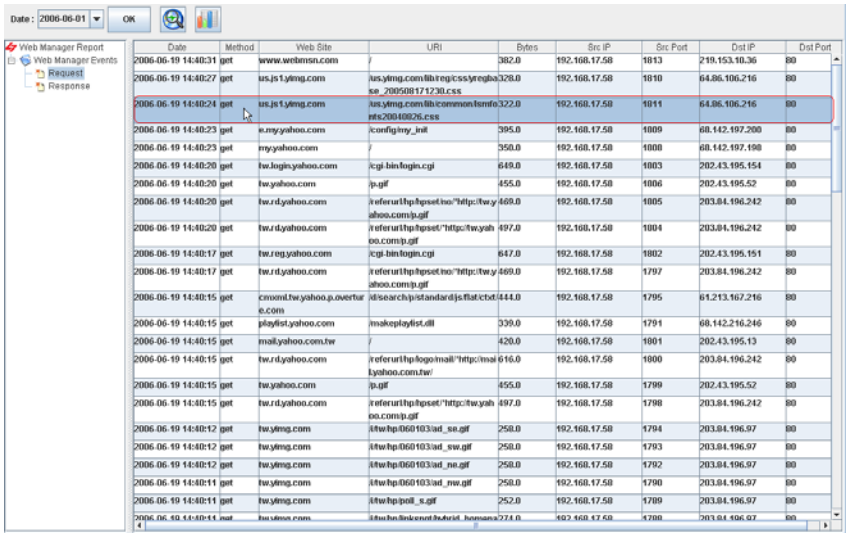
表格 23-1 即時通訊側錄內容欄位說明

### 23.3.2 網頁內容側錄

**步驟 1 流覽的網頁側錄**

當您在 Web Manager > Status 頁面上開啓 URL Recorder，所有您要流覽的網頁將會被記錄在這個側錄頁面上。

**Auditor > Web Recorder > Request**




| 欄位 | 說明 | 範例 |
|---|---|---|
| Date | 發送流覽網頁要求的時間。 | 2006-6-19 14:40:24 |
| Method | method 用以規範表單被送出時，所採用的 HTTP method，預設值是 GET。POST 方法是將資料包裝在 HTTP 標頭內傳送給 Web server；而 GET 方法則是將資料直接加在 URI 之後。使用 GET method 所能傳遞的資料有限（連同 URI 共 255 字元），在需要上傳大量資料或檔案時，必須使用 POST method。 | get |
| Web Site | 要流覽的網站。 | us.js1.yimg.com |
| URI | Uniform Resource Identifiers 的縮寫，資源識別字串，是用於在網路環境中識別檔、可供下載的檔案、各式服務及電子郵箱等等的各式資源。 | /us.yimg.com/lib/common/lsmfonts_20040826.css |
| Bytes | 發送流覽要求的網頁流量。 | 322 |
| Src IP | 發送流覽要求的來源端 IP 地址。 | 192.168.17.58 |
| Src Port | 發送流覽要求的來源端埠。 | 1811 |

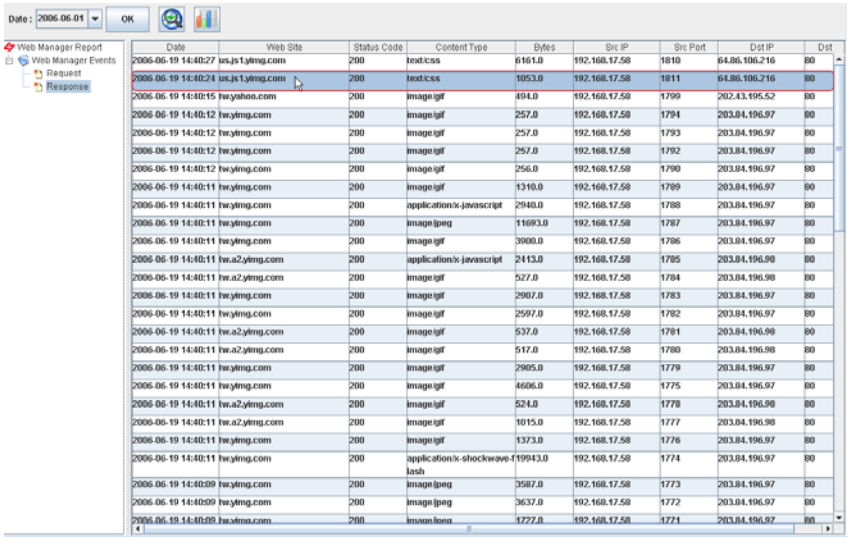
| | | |
|---|---|---|
| Dst IP | 欲流覽的網站之 IP 地址。 | 64.86.106.216 |
| Dst Port | 欲流覽的網站之埠。 | 80 |

表格 23-2 網頁側錄 - 流覽欄位說明

**步驟 2 回應的網頁側錄**

用來儲存 request （要求） 生成的 response（回應）。回應的網頁系依以上網頁流覽要求發生時，對應的回應網頁也會被側錄在這個頁面上。

**Auditor > Web Recorder > Response**




| 欄位 | 說明 | 範例 |
|---|---|---|
| Date | 回應流覽網頁要求的時間。 | 2006-06-19 14:40:24 |
| Web Site | 要流覽的網站。 | Us_js1.yimg.com |
| Status Code | 狀態碼值，表示網頁流覽的成功或失敗。 | 200 |
| Content Type | 網頁內容型別標示。 | Text/css |
| Bytes | 回應流覽需求的網頁流量。 | 1053.0 |
| Src IP | 流覽網頁要求的來源端 IP 地址。 | 192.168.17.58 |
| Src Port | 流覽網頁要求的來源端埠。 | 1811 |
| Dst IP | 欲流覽的網站之 IP 地址。 | 64.86.106.216 |
| Dst Port | 欲流覽的網站之埠。 | 80 |

表格 23-3 網頁側錄 – 回應欄位說明

# 第11部

## 系統維護

# 第24章
# 系統記錄

## 24.1 需求

1. 網管人員希望知道過去所有系統執行狀態，不希望有非法設定。
2. 網管人員每天必須核對系統操作記錄，但是希望簡化並縮減核對的程式。
3. 網管人員希望即時收到 alert （警告）與 critical（嚴重） 等級的事件記錄，希望當系統有問題時，能即時提供解決之道。

## 24.2 目的

1. 網管人員希望知道過去所有系統的管理動作。
2. 網管人員希望每天收到 InstantScan 的記錄報表。
3. 網管人員希望即時收到嚴重等級以上的系統記錄。

## 24.3 方法

1. 透過系統記錄的追蹤，您可以檢視管理動作的合法與否。
2. 透過 mailer 接收電子郵件。設定每天定時自動寄送記錄檔給網管人員。
3. 在 mailer 上啓用透過 e-mail 即時寄送系統記錄。

## 24.4 步驟

### 24.4.1 系統記錄

**步驟 3 檢視系統記錄**

您可以在 Functions > Reports > System Manager 頁面上流覽所有的系統記錄。系統記錄依嚴重性分成 5 個等級。

Alert （警告）

Critical （嚴重）

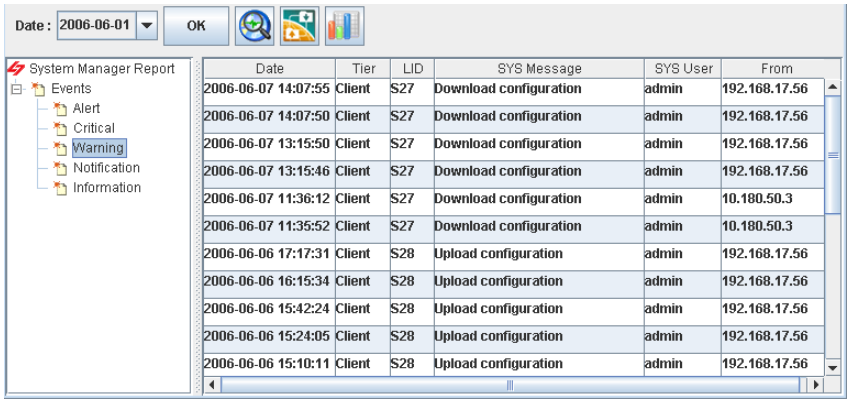
Warning （警示）

Notification （注意）

Information （信息）

系統記錄詳細資訊請參考**錯誤! 找不到參照來源。**。

**Functions > Reports > System Manager**




| 欄位 | 說明 |
|---|---|
| Date | 系統事件記錄產生的日期與時間。 |
| Tier | 產生系統記錄的層級。因爲 InstantScan 屬於三層式架構，所以有 Device 層、Management Server 層，與 Client 層。 |
| LID | 系統記錄的編號。 |
| SYS Message | 系統記錄的操作說明，. |

| | |
|---|---|
| SYS User | 登入並操作此 InstantScan 的使用者帳號。 |
| From | 造成此系統事件的來源端。 |

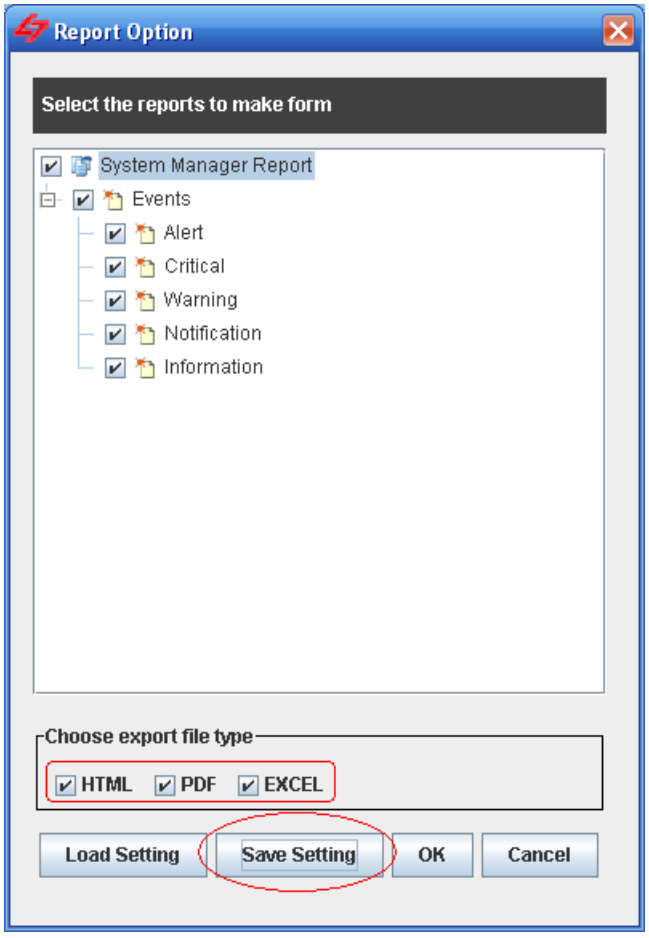
表格 24-1 系統記錄說明

### 24.4.2 設定接收系統記錄的時間

**步驟 1 設定系統記錄的輸出格式**

在 Reports > System Manager 的頁面上按圖示  。選擇您有接收的報表類型，然後勾選輸出報表的檔案類型，最後點擊 Save Settings。以後如果您升級韌體，只要點擊 Load Settings，就可將之前的設定載入了。

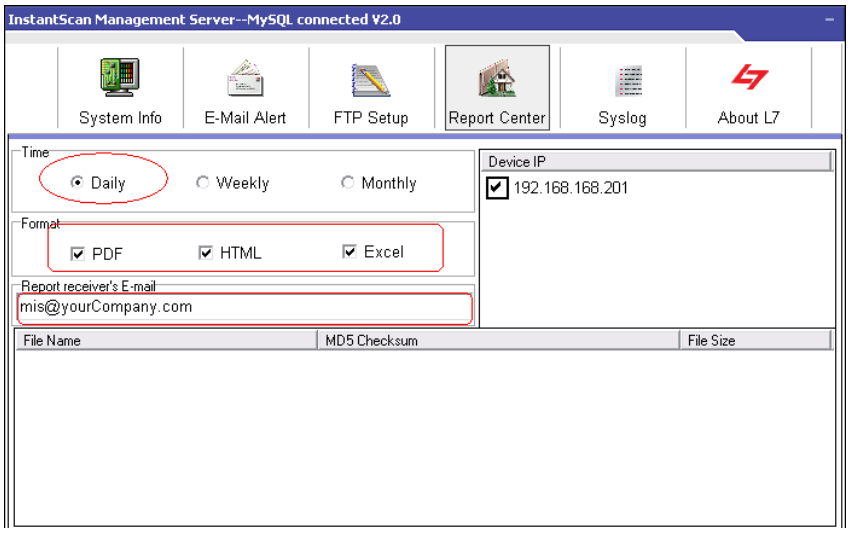
**Functions > Reports > System Manager > Export**



**步驟 2 設定接收系統記錄的時間**

在 mailer > Report Center 上選擇希望接收系統記錄報表的時間、報表格式及勾選要接收哪個裝置上的系統記錄。最後輸入報表接收者的電子郵件信箱。

**Mailer > Report Center**



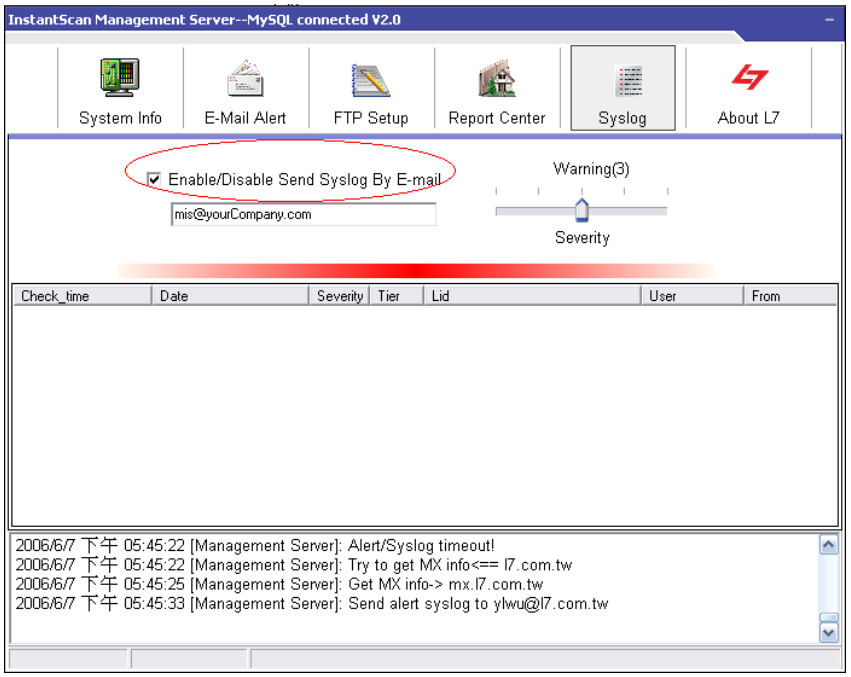

## 24.4.3 啓用即時接收系統記錄

**步驟 1 啓用透過電子郵件傳送系統記錄**

勾選 Enable/Disable Send Syslog By Email，拉選您要即時接收系統記錄的嚴重性，然後輸入報表接收者的電子郵件帳號。

設定完成後，每當有符合設定的事件記錄產生，您便可即時接收電子郵件寄送的系統記錄警告信件。

**mailer > Syslog**



# 第25章 系統維護

*本章介紹系統維護。*

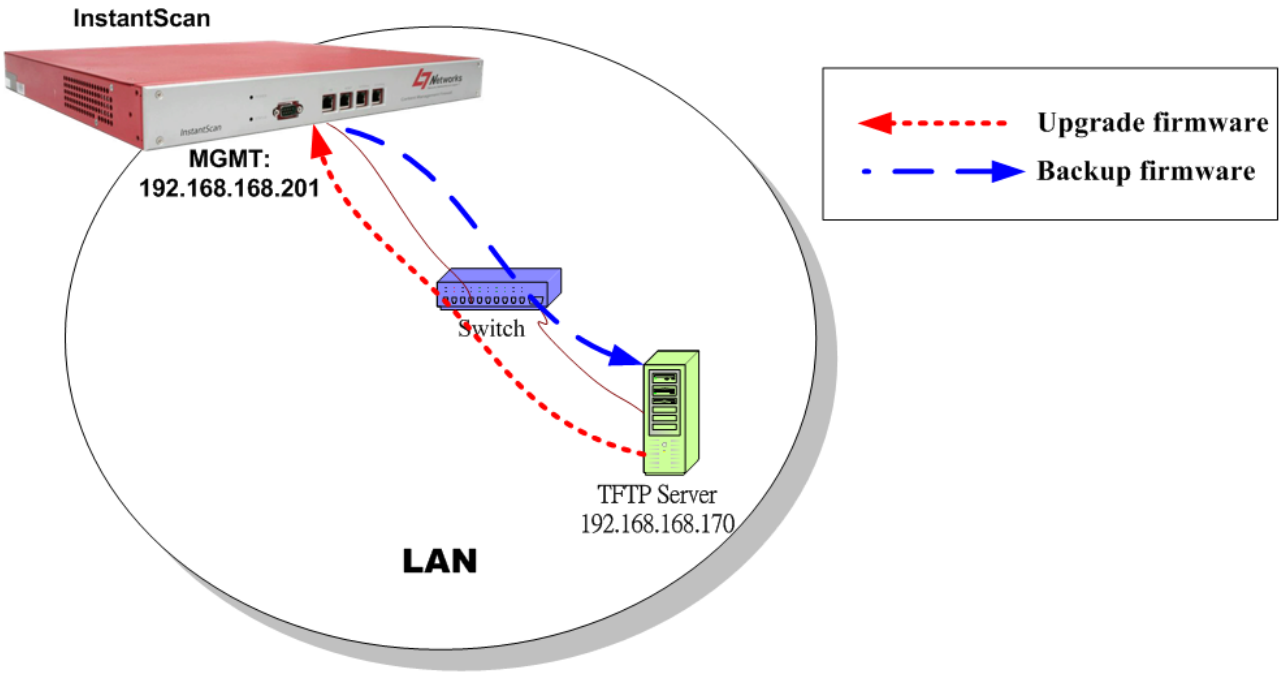
## 25.1 需求

1. InstantScan 讓您可以隨時更新韌體與資料庫以符合當前的網路狀態。新的功能、新的攻擊、新的 URL 資料庫，與新的病毒定義都需要不定時更新，所以本章介紹如果透過 TFTP 伺服器與網頁介面更新 InstantScan。

2. 當您忘記密碼、韌體或設定檔損毀，您可以透過網頁介面或是 console 介面將韌體恢復到出廠預設值。但當您忘記密碼時，您只可以透過 console 介面，利用救援模式恢復出廠預設值。

3. 當您設定好 InstantScan 後，爲避免因不明原因而造成設定檔損毀，所以您可以將現行的設定檔備份，以備不時之需。

## 25.2 透過 TFTP 伺服器升級韌體




圖表 25-1 從 TFTP 伺服器處升級 / 備份韌體

| | |
|---|---|
| **步驟 1 設定 TFTP 伺服器**<br>將 TFTP 伺服器置於 C:\ 槽底下。將所有韌體副檔名爲 bin 的檔案也放在一起。將這台有安裝 tftp 伺服器的 PC 之 IP 地址設定與 InstantScan LAN1 端的 IP 在同一個網段。登入 InstantScan console 介面。輸入 "en" 進入許可權模式。 | **N/A** |

**步驟 2 升級韌體**

輸入 ip tftp upgrade image <FILENAME> 192.168.168.170。完成後，InstantScan 將會重開機。相關 CLI 指令，請參考附錄 A 說明。

**步驟 3 檢查更新後的韌體設定**

待重開機完成，請用sys ver檢查所有相關設定是否正確。

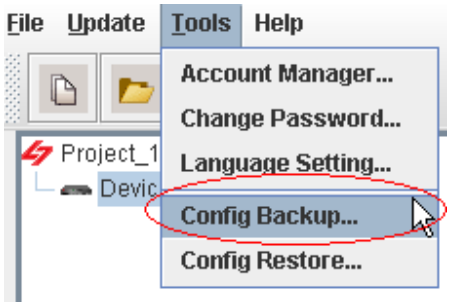
```
============ Firmware Information ===============
Device Model:          5000U
Firmware Version:      Version 3.0.04
Building Time:         20080926-20:07:05
Hardware ID:           EFEE4BE373F6940CDE0977DA
                       01591D876FC797ADF7192D16
Serial Number:         00D0C99CAA66
=========== Engines/Modules Version =============
pattern engine:        2.1.05
virus db engine:       1.1.02
im-engine:             2.0.54
pattern:               2.1.05.326
virus database:        1.1.02.006
url database:          2.1.00.021
================================================
```

## 25.3 備份設定檔

**步驟 1 備份設定檔**

在工具列上點擊 **Tools**，然後點選 **Config Backup**。

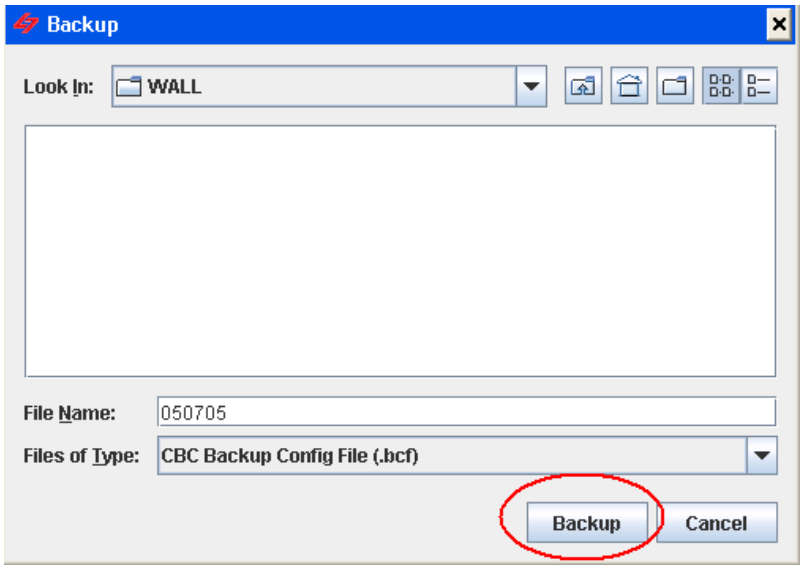
**Tools > Config Backup**



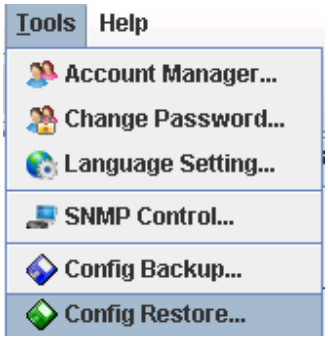
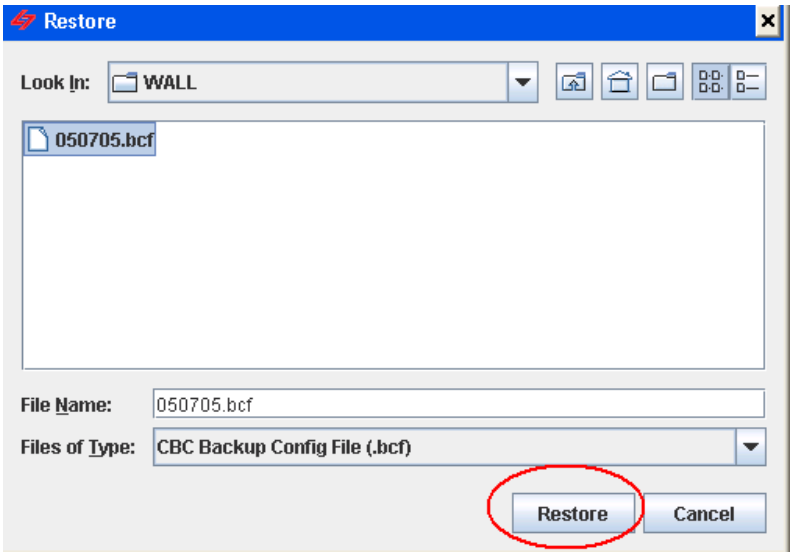

**步驟 2 儲存設定檔**

請選擇要將設定檔儲存的資料夾，然後輸入檔案名。點擊 **Backup** 完成設定。

**Tools > Config Backup**

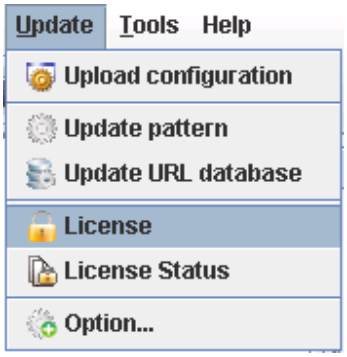


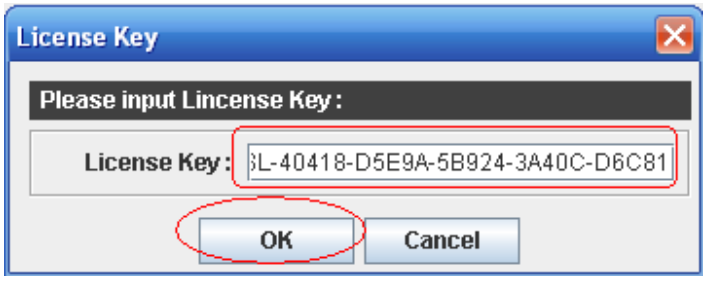
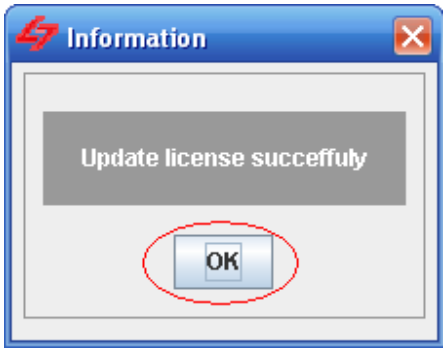
## 25.4 還原設定檔

| | |
|---|---|
| **步驟 1 還原設定檔**<br>在工具列上點擊 **Tools**，然後點選 **Config Restore**。 | **Tools > Config Restore**<br>  |
| **步驟 2 選擇要還原的設定檔**<br>請選擇要還原的設定檔，然後點擊 Restore 完成設定。 | **Tools > Config Restore**<br>  |

## 25.5 啓用選購的模組

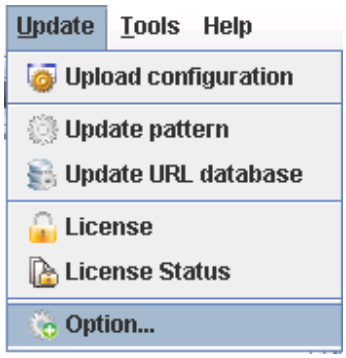
當您購買 InstantScan 時，只有標準的 Application Firewall 模組、Traffic Manager 模組、IM Manager 模組與 Object Manager 模組。如果您有選購 Web Manager，您必須透過使用者介面上傳 Web Manager 模組的 License Key 來啓用它，否則您無法使用 Web Manager，且也無法在 UI 上面看到這個模組。

| | |
|---|---|
| **步驟 1 連上註冊網頁**<br>在工具列上的 update，點選 License。 | **Update > License**<br>  |

| | |
|---|---|
| **步驟 2 輸入 License Key**<br>輸入您所選購模組的授權碼，然後點擊 **OK** 繼續。 | **Update > License**<br>  |
| **步驟 3 上傳授權碼成功**<br>當您上傳授權碼成功，將有如右圖的視窗顯示。 |  |

## 25.6 升級 IM 引擎 / 應用程式列爲 / 病毒資料庫 / URL 資料庫

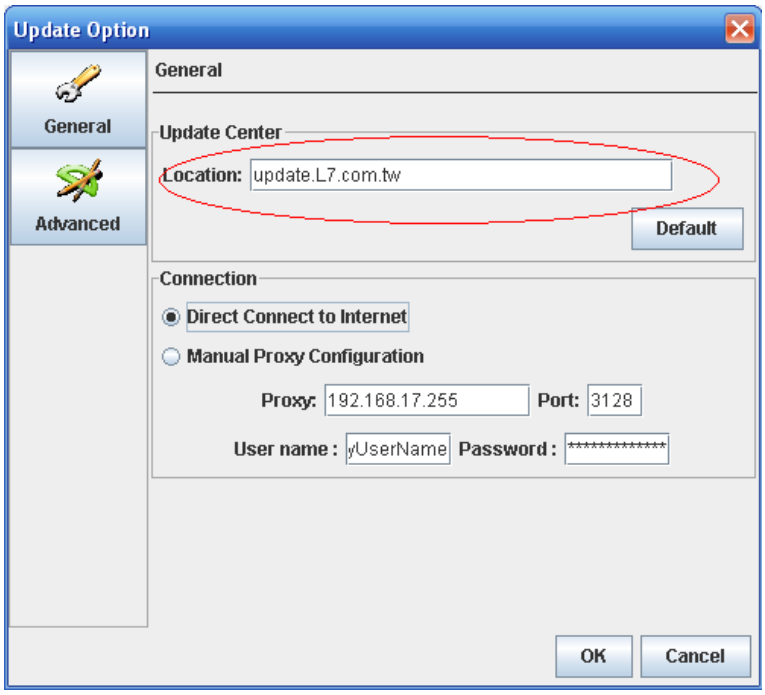
### 25.6.1 自動升級 IM 引擎 / 應用程式列爲 / 病毒資料庫 / URL 資料庫

| | |
|---|---|
| **步驟 1 自動更新設定**<br>點擊 **Option...** 。 | **Update > Option…**<br>  |

**步驟 2 輸入更新中心資料**

輸入更新中心的位址，您亦可以點擊 Default 按鈕來獲得預設的更新中心網址。然後選擇連線方式，如果貴公司透過 proxy 伺服器連上網路，請點選 Manual Proxy Configuration。然後輸入 proxy 伺服器的 IP 位址、伺服器埠與您的用戶名稱 和密碼。點擊 Advanced 設定更新項目與排程。

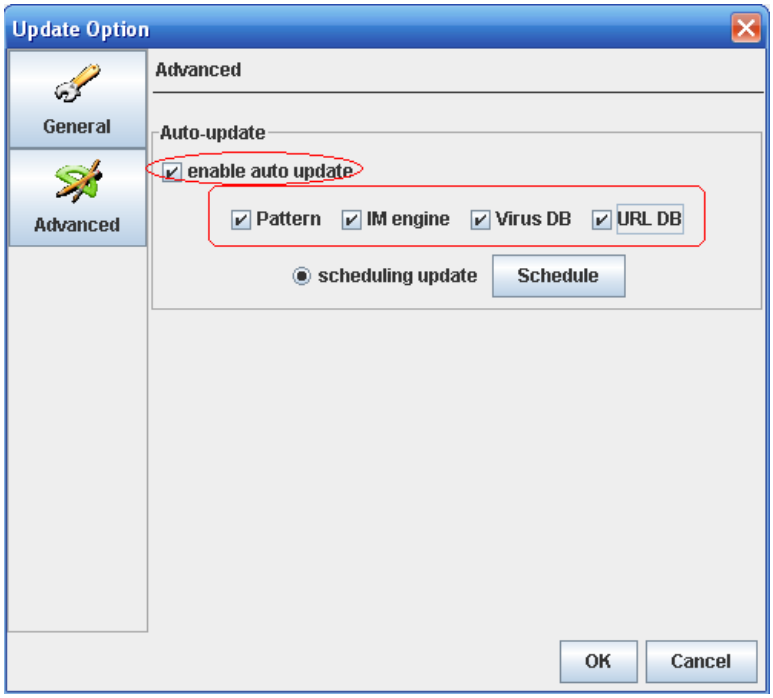
**Update > Option… > General**

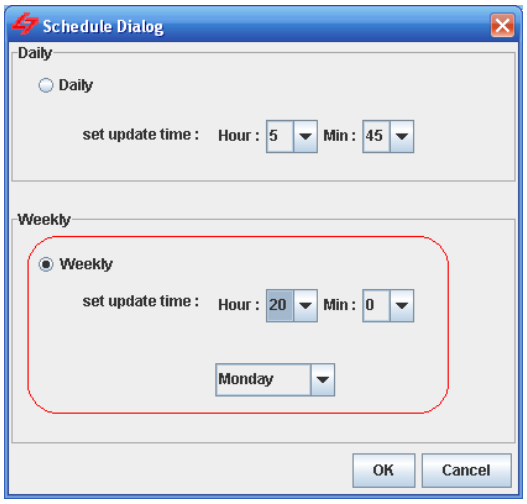



**步驟 3 啓用自動更新**

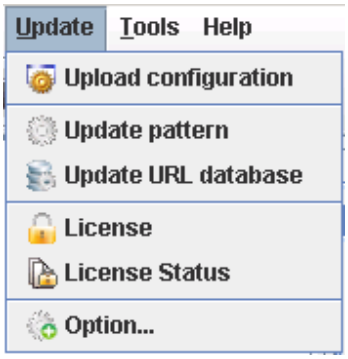
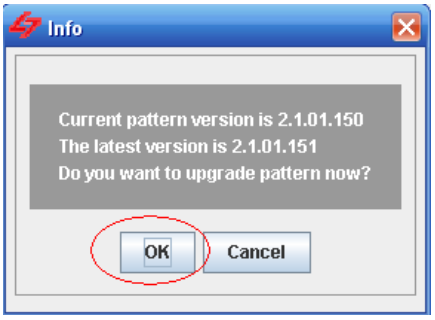
勾選 enable auto update，並勾選要自動更新的項目。點擊 Schedule 設定更新排程。

**Update > Option… > Advanced**

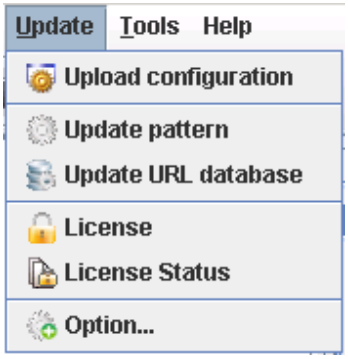
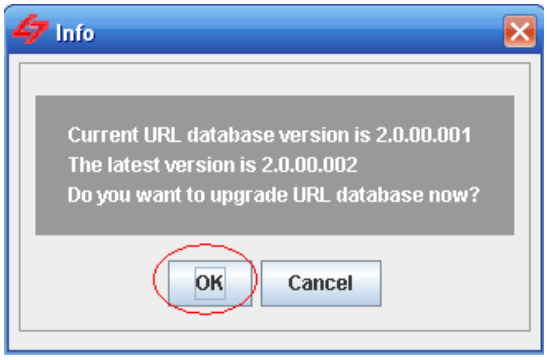


| | |
|---|---|
| **步驟 4 設定更新排程**<br>選擇 Weekly，然後選擇每週自動更新的時間與日期。點擊 OK 完成設定。 | **Update > Option… > Advanced > Schedule**<br>  |

### 25.6.2 手動升級應用程式列爲

| | |
|---|---|
| **步驟 1 從 UI 上手動升級應用程式列爲**<br>點擊 **Update pattern**。 | **Update > Update pattern**<br>  |
| **步驟 2 更新應用程式列爲**<br>點擊 OK 開始更新應用程式列爲。 | **Update > Update pattern**<br>  |

### 25.6.3 手動升級 URL 資料庫

| | |
|---|---|
| **步驟 1 從 UI 上手動升級 URL 資料庫**<br>點擊 **Update URL database**。 | **Update > Update URL database**<br>  |
| **步驟 2 更新 URL 資料庫**<br>如果您裝置上的 url 資料庫爲最新版本，將出現右圖的訊息。請點擊 **OK** 結束更新的動作。 | **Update > Update URL database**<br>  |

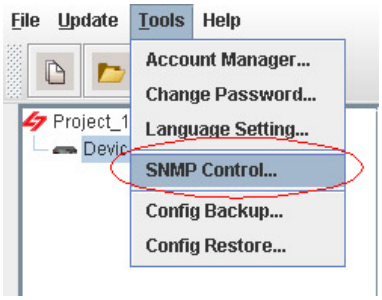
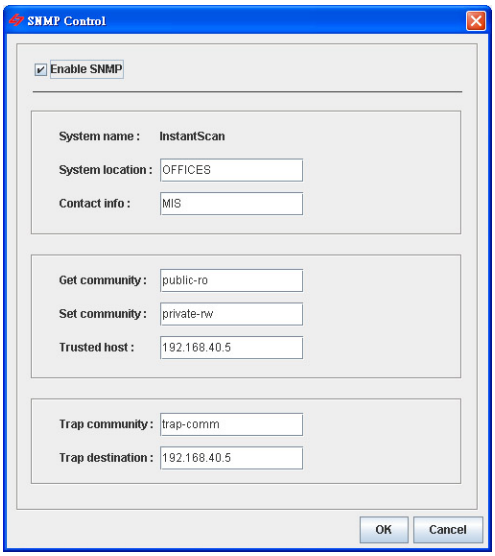
### 25.6.4 在 CLI 標準模式下，恢復出廠預設值

| |
|---|
| **步驟 3 恢復出廠預設值**<br>在 CLI 模式下鍵入 **sys resetconf now**，按 Enter 後，系統將重新開機，所有設定將回復到出廠預設值。 |

### 25.6.5 在 CLI 救援模式下，回復出廠預設值

| | |
|---|---|
| **步驟 4 進入安全模式**<br>在 5 秒的倒數計時內，按 ctrl+e，進入救援模式。在這個核心模式中，您可以利用 tftp 指令來安裝韌體或者將設定檔回復到出廠預設值，甚至您忘記密碼也可以在這個模式下操作。<br>輸入 sys resetconf now，系統將重新開機將設定檔回復到出廠預設值。 | `Press ctrl+e in 5 secs to start with emergency kernel.`<br>`Enter emergency mode.`<br><br>`(Emergency Mode) login as "admin", no password`<br>`[EMERGENCY] login: admin`<br>`[EMERGENCY]> en`<br>`[EMERGENCY]#`<br>`  disable  Turn off privileged mode command`<br>`  exit     Exit command shell`<br>`  ip       Configure/Display IP related settings`<br>`  sys      Configure system parameters`<br>`[EMERGENCY]# sys resetconf now`<br>`Config reset to default.`<br>`System will reboot now` |

### 25.6.6 SNMP 控制設定

| | |
|---|---|
| **步驟 1** 開啓 SNMP 控制視窗<br>點選 Tool Bar 上面的 Tools 選項，就會跳出選單，點選 SNMP Control 選項之後，就會跳出 SNMP 的控制介面。 | **Tools > SNMP Control**<br>  |
| **步驟 2 設定 SNMP 控管**<br>只要在介面上設定好 SNMP 各項參數，您就可以透過 SNMP 管理員遠端監控 InstantScan 的系統狀態、網路狀態等。 | **Tools > SNMP Control**<br>  |

| 欄位 | 說明 | 範例 |
|---|---|---|
| 啓用 SNMP | 啓用 SNMP 遠程監控。 | 啓用 |
| 系統名稱 | InstantScan 裝置名稱。 | WALL-1.yourCompany.com |
| 系統位置 | InstantScan 安裝的位置。 | Office |
| 連絡人信息 | 控管 InstantScan 的網管人員。 | mis |
| Get community | 透過社群可以獲得 SNMP 的資訊。這裡的 get community 類似密碼，用來做身份驗證用。 | public-ro |
| Set Community | 透過社群可以獲得 SNMP 的資訊。這裡的 set community 類似密碼，用來做身分驗證。 | private-rw |
| 信賴的主機 | 可以透過 InstantScan 獲得或設定社群的 IP 地址。 | 192.168.1.5 |
| Trap community | 傳送 SNMP trap 的社群。 | trap-comm |
| Trap destination | 透過 InstantScan 傳送 SNMP trap 的 IP 位址。 | 192.168.1.5 |

# 附錄

# 附錄 A
# 指令行介面（CLI）

您可以利用 web 介面（http/https）來設定 InstantScan，除此之外，當遇到緊急時刻，您亦可利用 console/ssh/telnet 遠端連線方式來更改或查詢設定。CLI 指令是非常有用的工具，它可以讓您設定或更改所有介面的 IP 位址、將設定檔重設成出廠預設值或者是重開機。我們將所有 CLI 指令整理成以下表格，以供您參考。

## A.1 CLI 指令清單 - 標準模式

當您透過 console/telnet/SSH 連上 InstantScan，必須使用 CLI 指令來設定 InstantScan。您可依據以下表格所描述的指令來完成 InstantScan 的設定。

**非許可權模式 Non-privileged mode**

| 主要指令 | 次要指令 | 範例 | 指令說明 |
|---|---|---|---|
| **?** | | ? | 顯示所有指令主選單 |
| **enable (en)** | | enable | 開啓許可權模式指令 |
| **exit (ex)** | | exit | 離開 CLI 介面 |
| **ip** | | | 設定相關 IP 參數 |
| | ping | ip ping 202.11.22.33 | 發送 ICMP 回應需求訊息 |
| | traceroute | ip traceroute 202.11.22.33 | 追查路由到目的地址所經過的路徑 |
| **sys** | | | 設定系統參數 |
| | status (st) | sys status | 顯示系統與網路狀態 |
| | version (ver) | sys version | 顯示 InstantScan 韌體版本資訊 |

表格 A-1 標準模式下的非許可權模式

⚠ **注意：**如果您不曉得某個指令的參數，您可以在指令後空一格打問號” ?” 例如: “ip ?” 。所有ip底下可能的參數就會顯示出來。。

**許可權模式 Privileged mode**

| 主要指令 | 次要指令 | 範例 | 指令說明 |
|---|---|---|---|
| **?** | | ? | 顯示所有指令的主選單 |
| **disable (dis)** | | disable | 關閉許可權模式 |
| **exit (ex)** | | exit | 離開 CLI 介面 |
| **ip** | | | 設定相關 IP 參數 |
| | ifset | ip ifset INTF1 | 顯示或變更網路介面設定 |
| | ping | ip ping 202.11.22.33 | 發送 ICMP 回應需求訊息 |
| | set | ip set | 設定 InstantScan 相關 IP 地址 |
| | show | ip show | 顯示所有網路設定 |
| | tftp (upgrade) | ip tftp upgrade image <FILENAME> 192.168.168.170. | 從 tftp 伺服器處升級韌體 |
| | traceroute | ip traceroute 202.11.22.33 | 追查路由到目的地址所經過的路徑 |
| **sys** | | | 設定系統參數 |
| | date | sys date | 顯示/設定目前系統時間 |
| | halt | sys halt now | 關機 |
| | highavail | sys highavail set | High-Availability 相關參數設定 |
| | module | sys module | 更新/還原系統模組設定 |
| | password | sys password | 變更管理員密碼 |
| | reboot | sys reboot now | 重開機 |
| | resetconf | sys resetconf now | 重設系統設定檔成出廠預設值 |
| | sessionlog | sys ressionlog on | Session 記錄的設定 |
| | showmac | sys showmac | 顯示網路卡的 MAC 位址 |
| | status (st) | sys status | 顯示系統狀態 |
| | tcpdump | sys tcpdump management | 傾印 (dump) 流經的封包 |
| | uptime | sys uptime | 顯示 InstantScan 正常運作的時間 |
| | version (ver) | sys version | 顯示 InstantScan 韌體版本 |

表格 A-2 標準模式下的許可權模式

完整的 sys module 與 ip tftp upgrade 指令，請參閱下表。

| 首碼指令 | 第二指令 | 第三指令 | 字尾指令 | 範例 | 指令說明 |
|---|---|---|---|---|---|
| **sys** | module | flushstate | -- | sys module flushstate | 手動清除系統內閒置不用的連線 |
| | | query | -- | sys module query | 詢問模組版本 |
| | | restore | all | sys module restore all | 復原系統應用程式列 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | 爲/特徵碼/病毒資料庫 |
| | | | av | sys module restore av | 復原系統病毒和蠕蟲資料庫 |
| | | | pattern | sys module restore pattern | 復原系統應用程式列爲 |
| | | | signature | sys module restore signature | 復原系統特徵碼 |
| | | setting | set | sys module setting set | 更改更新伺服器設定 |
| | | | show | sys module setting show | 顯示更新伺服器設定 |
| | | update | all | sys module update all | 更新系統應用程式列爲/特徵碼/病毒資料庫 |
| | | | av | sys module update av | 更新系統病毒和蠕蟲資料庫 |
| | | | pattern | sys module update pattern | 更新系統應用程式列爲 |
| | | | signature | sys module update signature | 更新系統特徵碼 |
| **ip tftp** | upgrade | firmware | FILENAME tftp server IP address | ip tftp upgrade firmware <FILENAME> 192.168.168.170 | 從 tftp 伺服器處升級韌體 |
| | | image | FILENAME tftp server IP address | ip tftp upgrade image <FILENAME> 192.168.168.170 | 從 tftp 伺服器處升級 image 檔 |
| | | module | FILENAME tftp server IP address | ip tftp upgrade module <FILENAME> 192.168.168.170 | 從 tftp 伺服器處升級系統模組 |

表格 A-3 Sys module 與 IP tftp 指令說明

⚠ **注意，IP TFTP upgrade字尾指令意義如下：**

**WORD：** tftp 伺服器IP地址。

**FILENAME：** 升級設定檔或韌體的image檔案名。

完整 sys sessionlog 指令，請參閱下表。

| 首碼指令 | 第二指令 | 第三指令 | 字尾指令 | 範例 | 指令說明 |
|---|---|---|---|---|---|
| sys | Sessionlog | Off | -- | sys sessionlog off | 關閉系統記錄 |
| | | On | -- | sys sessionlog on | 啓用系統記錄 |
| | | Status | -- | sys sessionlog status | 系統記錄狀態 |

表格 A-5 sys tcpdump 指令說明

完整 sys tcpdump 指令，請參閱下表。

| 首碼指令 | 第二指令 | 第三指令 | 字尾指令 | 範例 | 指令說明 |
|---|---|---|---|---|---|
| **sys** | tcpdump | External | dump | sys tcpdump external dump | 傾印流經 external 端的封包 |
| | | | interactive | sys tcpdump external interactive | 依交談模式列舉流經 external 端的封包 |
| | | Internal | dump | sys tcpdump internal dump | 傾印流經 internal 端的封包 |
| | | | interactive | sys tcpdump internal interactive | 依交談模式列舉流經 internal 端的封包 |
| | | Management | dump | sys tcpdump management dump | 傾印流經 management 端的封包 |
| | | | interactive | sys tcpdump management interactive | 依交談模式列舉流經 management 端的封包 |

表格 A-6 sys tcpdump 指令說明

## A.2 CLI 指令清單 - 救援模式

如果原始韌體因某些意外而損毀，您需要利用救援模式將韌體回復到出廠預設值。將 InstantScan 重新開機後，在 5 秒鐘的倒數程式內按 <ctrl> + e 鍵，請輸入 admin 後進入救援模式。

**非許可權模式 Non-privileged mode**

| 主要指令 | 次要指令 | 範例 | 指令說明 |
|---|---|---|---|
| **?** | | ? | 顯示所有指令主選單 |
| **enable (en)** | | Enable | 開啓許可權模式指令 |
| **exit (ex)** | | Exit | 離開 CLI 介面 |
| **ip** | | | 設定相關 IP 參數 |
| | ping | ip ping 202.11.22.33 | 發送 ICMP 回應需求訊息 |
| | traceroute | ip traceroute 202.11.22.33 | 追查路由到目的地址所經過的路徑 |
| **sys** | | | 設定系統參數 |
| | date | sys date | 顯示目前系統時間 |

表格 A-7 救援模式之非許可權模式

**許可權模式 Privileged mode**

| 主要指令 | 次要指令 | 範例 | 指令說明 |
|---|---|---|---|
| **?** | | ? | 顯示所有指令主選單 |
| **disable (dis)** | | Disable | 關閉許可權模式 |
| **exit (ex)** | | Exit | 離開 CLI 介面 |
| **ip** | | | 設定相關 IP 參數 |
| | ping | ip ping 202.11.22.33 | 發送 ICMP 回應需求訊息 |

| | | | |
|---|---|---|---|
| | set | ip set | 設定 device 的 IP 地址 |
| | show | ip show | 顯示所有網路設定 |
| | tftp (upgrade) | ip tftp upgrade image <FILENAME> 192.168.168.170. | 從 tftp 伺服器處升級韌體 (相關設定與標準模式同) |
| | traceroute | ip traceroute 202.11.22.33 | 追查路由到目的地址所經過的路徑 |
| **sys** | | | 設定系統參數 |
| | date | sys date | 顯示目前系統時間 |
| | halt | sys halt now | 關機 |
| | reboot | sys reboot now | 重開機 |
| | resetconf | sys resetconf now | 重設系統設定檔成出廠預設值 |
| | resetpasswd | sys resetpasswd | 變更管理員密碼 |
| | showmac | sys showmac | 顯示網路卡的 MAC 位址 |

表格 A-8 救援模式之許可權模式

# 附錄 B
# 疑難排解

1. 安裝 InstantScan 後爲什麼 MSN 或 Yahoo 都無法登入？

答：您可能碰到以下幾種情況：

1-1 啓動 IM Manager 功能後 User 無法登入 MSN

A. 先到 Report 中的 Application Firewall 查看 log 狀況，是否被 IS 所阻擋？爲何被擋？

B. 如果用戶端的 MSN 無法登入是因爲走 port 80，而我們只允許用戶端走正常連線的 1863。請在用戶端的 PC 上，把 MSN 中的進階選項 TCP 打勾，取消勾選其他如 SOCKS、SOCKS 5、HTTP Proxy 選項。

C. 到防火牆端開 1 條規則 ※＝＞ LAN TO WAN Service：1863 Allow

1-2 啓動 IM Manager 功能後 User 無法登入 Yahoo

A. 先到 Report 中的 Application Firewall 查看 log 狀況，是否被 IS 所阻擋？爲何被擋？

B. 如果用戶端的 Yahoo 無法登入是因爲走埠 80，而我們只允許用戶端走正常連線的 5050。請在用戶端的 PC 上，把 Yahoo 中的網路連線設定選擇第一項 不需使用代理伺服器，這時請勿選擇其他選項。

C. 到防火牆端開 1 條規則 ＝＞LAN TO WAN Service：5050 Allow。

2. 如何知道目前設備的網路處理效能？

答：進入 Console 模式下，輸入指令 sys status，可瞭解本裝置的 CPU Loading、Concurrent Sessions 等等。

3. 如果我設定 Auto update pattern，那我如何得知目前最新 pattern 有哪些變動？

答：您有兩個方法可以查詢 pattern 變動情況：

3-1 在管理介面點選 Update ＞ Support list ，系統會自動開啓 IE 流覽器告知您目前使用的 pattern 版本與其所支援的通訊協定。

3-2 請上利基網路網頁 www.L7-Networks.com 點選 **網路安全 > 發行須知** 尋找最新版本的 pattern 內容，並點選內容最後附加的 Support List 連結，即可看到支援清單頁面。

4. 最新版本的 Pattern 或 URL database 要怎樣更新呢？

答：

4-1 在管理介面的工具列上點選您要更新的項目，例如 Update > Update Pattern/Database。

4-2 在 console 模式中輸入 sys module update all 或逐項更新 (例如 sys module update pattern)。在此之前，請先確認您的對外網路是暢通的。

5. 如何更新韌體呢？

答：首先請先接洽您購買本裝置的經銷商，向其取得最新韌體，然後在 Console 模式下輸入指令 ip tftp upgrade image <檔案名> （例如：ip tftp upgrade image filename.bin 192.168.1.10）。至於怎麼設定 tftp 伺服器與如何從 tftp 伺服器升級韌體，請參考本手冊章節**錯誤! 找不到參照來源。**。

6. 管理伺服器爲什麼都收不到記錄？

答：請依下列步驟檢查您的設定：

6-1 請確認在 console 模式中已經設定好本裝置對應的管理伺服器 IP 位址了。

6-2 請確認管理伺服器是否有安裝個人防火牆。

6-3 如有啓動防火牆，請於防火牆設定中開啓三個讓管理伺服器與本裝置間溝通用的埠（514、1080 與 3306）。

6-4 如果上述 3 個步驟都排除後，最後請確認在服務選項中的 LogServer 之服務是否已經啓動了。

7. 爲什麼我在 Console 下都看不到畫面？

答：

7-1 請確認終端機選項中，每秒傳輸位是否選擇 115200。超級終端機上的設定值爲（8 資料位元、1 停止位元、無同位檢查、115200 每秒傳輸位）。

7-2 假如步驟 7-1 的設定皆已完整，還是無法進入 console 畫面。那麼請準備一台 PC 或筆記型電腦與管理埠對接，然後 Ping 管理埠的 IP （出廠預設值爲 192.168.1.1）查看 Request 是否有回應。

7-3 如果步驟 7-2 也 ping 不到管理埠之 IP，那麼請直接將本裝置連接到網路上，測試網路是否斷線來測試硬體開機問題，再進一步確認硬體是否有損壞。

7-4 依上述步驟 3，將本裝置連接到網路上，請依以下結果處理後續事宜：

A. 網路正常：請更換 Console 線。

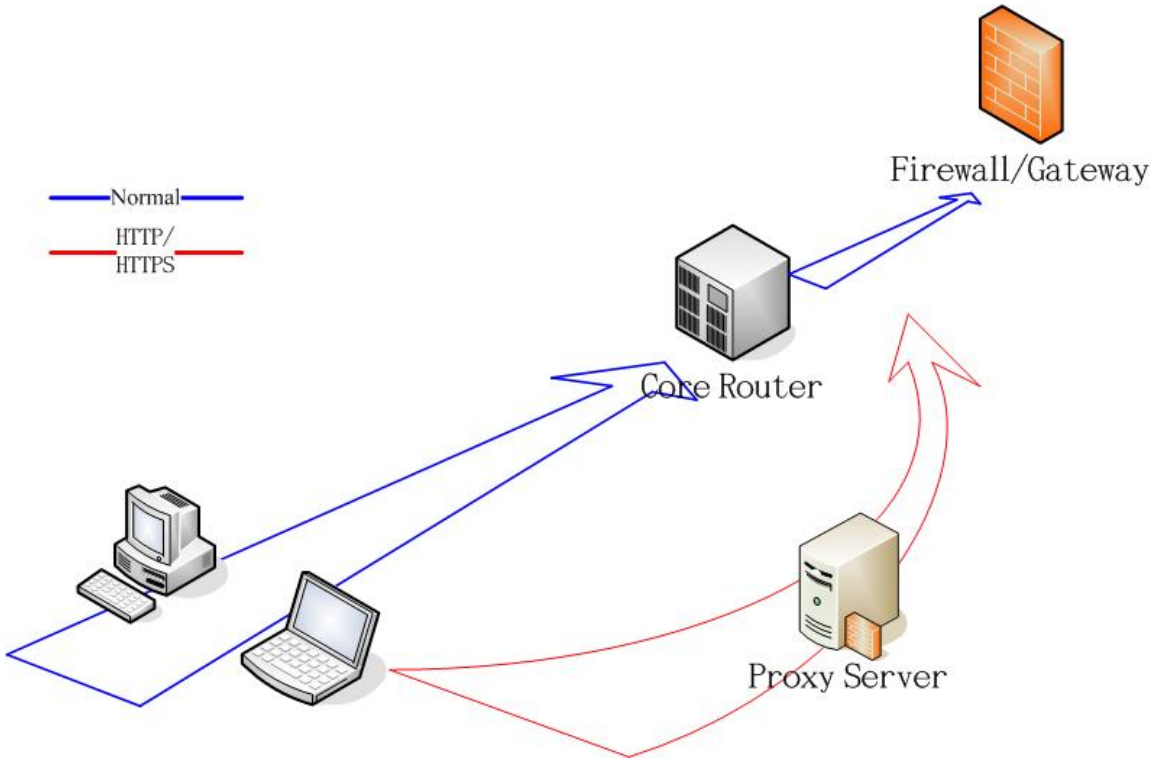
B. 網路斷線：請用 RMA 方式聯絡原廠。

# 附錄 C
# InstantScan 配置圖暨相關設定調整建議



## 一、Cache Proxy

### 1. 圖例




圖表 B-1 普遍且沒有限制的網路架構

### 2. 說明

除限制 HTTP/HTTPS 流量需透過 Proxy 代理，防火牆並無其他設定限定用戶端上 IM/P2P 軟體的使用。此爲最常見的網路概況。此網路下，IM/P2P 不需額外調整設定即可自由地使用。

### 3. 配置暨設定

InstantScan 應配置在路由器與 Firewall/Gateway 之間。無需再另行調整其他設備上的設定。

### 4. 注意事項

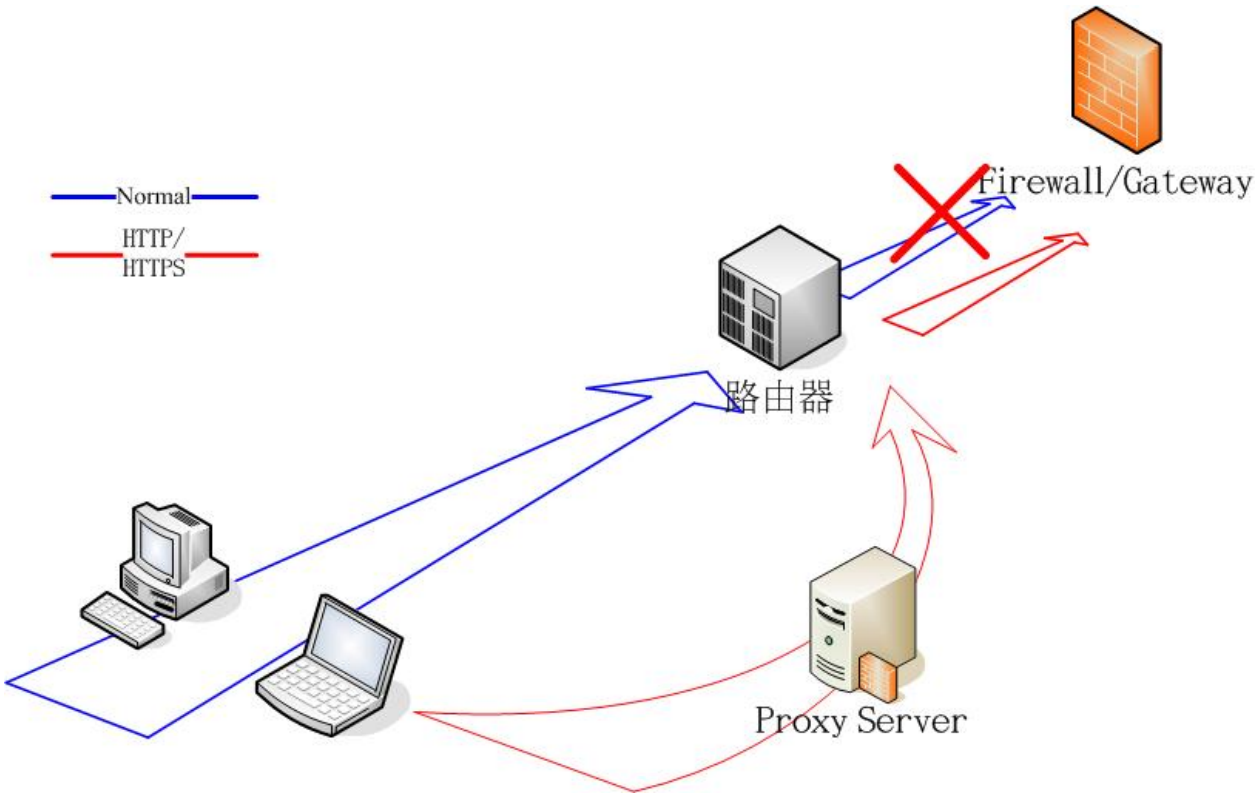
A. 如發現 Client 端在使用 MSN 時有無法登入的問題，可在 Proxy 設定 Deny URL http://gateway.messenger.hotmail.com/gateway/gateway.dll。此問題的發生在於 MSN 會嘗試使用 IE 上的 HTTP

Proxy 設定，透過 port 80 與 MSN Server 連線，然而 InstantScan 在啓動 IM 管理時，並不允許該種（非正規）連線方式，故產生 User 在不知情的狀況下，因使用 port 80 之 MSN 連線被 InstantScan 阻擋而無法登入。

B. InstantScan 可於主幹道上過濾所有流量，控管 IM 使用、阻擋 P2P 軟體的連線及管制 P2P 頻寬。

# 二、Cache Proxy + Limitations of Firewall

## 1. 圖例




圖表 B-2 有限度使用的網路架構圖

## 2. 圖例說明

Firewall/Gateway 限定只有 Server （HTTP/HTTPS Proxy、Mail） 的 IP 可自由通行，通常在這種環境下，主要目的爲只讓 User 使用 HTTP/HTTPS 連線，並透過 Proxy Server 管理/監控使用行爲。

此種網路下，稍爲進階的 IM/P2P 軟體使用者，仍能透過設定軟體中 HTTP（S）/SOCKS Proxy Server 的參數，經伺服器代理而進行連線。一般第四層防火牆對此種方式完全無法管控。

## 3. 配置暨設定

InstantScan 應配置在路由器與 Firewall/Gateway 之間。設定方式如下：

A. 調整 Firewall 的政策，開放用戶端可使用各項 IM 的標準埠（MSN：1863、Yahoo：5050、ICQ：5190、AOL：5190），例：LAN （來源端） to WAN （目的端） 的埠 1863 方向之連線設定爲允許通行。

B. 建議使用者取消各項 IM 上 Proxy 的設定，可減少無法連線的情形。

C. 建議在 Proxy 設定拒絕存取 URL http://gateway.messenger.hotmail.com/gateway/gateway.dll 以防止用戶端在 MSN 嘗試使用代理連線方式時，會等待較久時間才重新使用標準連線方式。

## 4. 注意事項

A. 原本可透過代理伺服器進行連線的 IM/P2P 軟體，因 InstantScan 能辨視出隱藏在 HTTP/SOCKS 的 IM/P2P 流量，故此類連線方式即被阻擋。

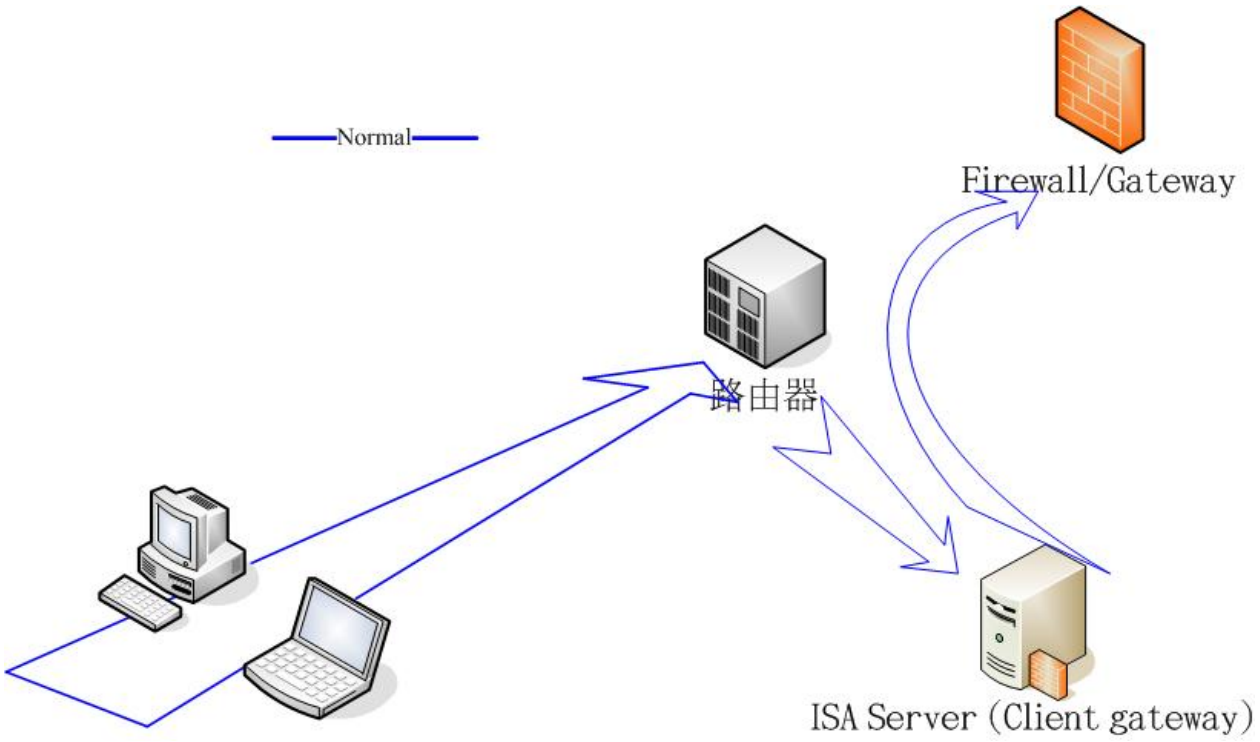
B. Firewall 開放用戶端對外通訊，因設定是內部（LAN、trust） 可存取外部 （WAN、un-trust）伺服器的服務 （埠 1863、5050...等），由外部網路對內部網路 （WAN to LAN） 所發起的連線，仍處於被 Firewall 阻擋的保護下。

C. 開放各項 IM 的標準埠，InstantScan 可在這些通道內控管 IM。

D. 雖然 Firewall 內對外的適度開放，造成 P2P 軟體可能會利用這些 IM 的埠進行連線，然而 InstantScan 的應用防火牆仍可以辨識出來並進行阻擋或管理頻寬的工作。

# 三、ISA Proxy Server

## 1. 圖例




圖表 B-3 使用 ISA Server 做爲 default gateway

## 2. 圖例說明

在此種網路配置上，使用 Microsoft ISA Server 架設 HTTP 等代理伺服器，並指定用戶端的網路設定，將預設閘道器（default gateway） 指向 ISA Server。ISA 除了會將 HTTP Proxy 等服務重新導向自己本身執行代理工作外，具備有 Firewall 與路由器能力的 ISA 會將其他的連線路由到出口的 Firewall/Gateway。

無論藉由 ISA Server 上的政策做爲連線管制，亦或是由上一層的 Firewall 設定規則管制，就如同圖例二的狀況一樣，無法防制進階的 IM/P2P 軟體使用者透過 HTTP Proxy 的服務連線。

## 3. 配置暨設定

InstantScan 應配置在路由器與 Firewall/Gateway 之間。設定如下：

A. 調整 Firewall 或是 ISA Server 的政策，開放用戶端可使用各項 IM 的標準埠（MSN：1863、Yahoo：5050、ICQ：5190、AOL：5190），例：LAN （來源端） to WAN （目的端） 的埠 1863 方向之連線設定爲允許通行。

B. 設定 ISA Server 需讓各項 IM 的標準埠的連線可路由往出口閘道。

C. 建議使用者取消各項 IM 上 Proxy 的設定，可減少無法連線的情形。

D. 建議在 Proxy 設定拒絕存取 URL http://gateway.messenger.hotmail.com/gateway/gateway.dll 以防止用戶端在 MSN 嘗試使用代理連線方式時，會等待較長久的時間才重新使用標準連線方式。

### 4. 注意事項

A. 原本可透過代理伺服器進行連線的 IM/P2P 軟體，因 InstantScan 能辨識出隱藏在 HTTP/SOCKS 的 IM/P2P 流量，故此類連線方式即被阻擋。

B. Firewall 開放用戶端對外通訊，因設定是內部 （LAN、trust） 可存取外部 （WAN、un-trust）伺服器的服務 （埠 1863、5050...等），由外部網路對內部網路 （WAN to LAN） 所發起的連線，仍處於被 Firewall 阻擋的保護下。

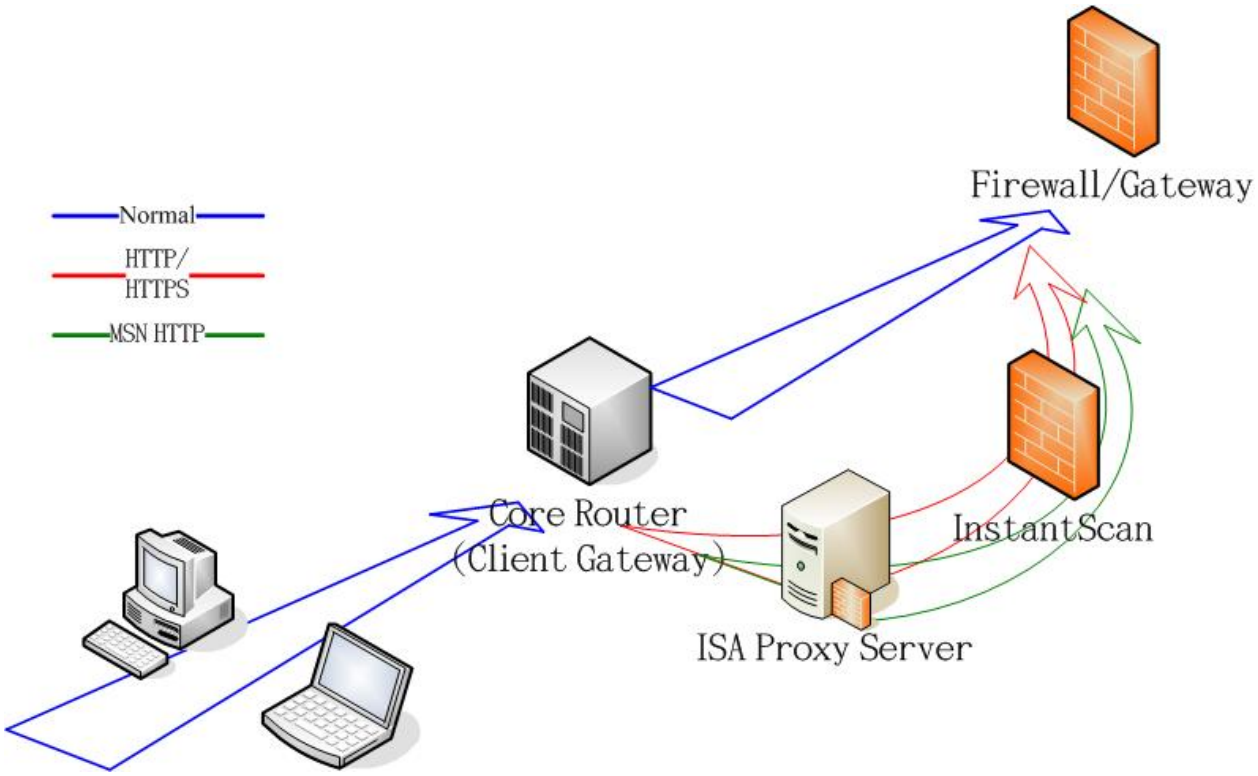
C. 因用戶端的閘道設定爲 ISA Server，所以在 ISA Server 上必需確定經過 1863、5050、5190 及 5222 等埠的連線，會被重新路由往出口閘道，連線才有辦法建立。

D. 開放各項 IM 的標準埠，InstantScan 可在這些通道內控管 IM。

E. 雖然 Firewall 內對外的適度開放，造成 P2P 軟體可能會利用這些 IM 的埠進行連線，然而仍可被 InstantScan 的應用防火牆辨識出來並進行阻擋或管理頻寬的工作。

## 四、ISA Proxy Server（NAT）

### 1. 圖例




圖表 B-4 ISA Proxy Server 架構

### 2. 圖例說明

使用 Microsoft ISA Server 架設 HTTP 等代理伺服器，但並非將 gateway 指向 ISA Server，相對地僅教育使用者，將 IE 流覽器及 MSN 連線 HTTP Proxy 設定指到 ISA Server。

## 3. 配置暨設定

InstantScan 應配置在 ISA Server 往 Firewall/Gateway 的線路上。設定如下：

A. 在 Core Router 上設定政策，將各項 IM 的標準埠（MSN：1863、Yahoo：5050、ICQ：5190、AOL：5190、） 導入 ISA Server。

B. 設定 ISA Server 爲 NAT 模式，讓一般流量或是各項 IM 的標準埠的連線可 NAT 往出口閘道。

C. Firewall 設定允許來源位址爲 ISA Server，且目的端埠爲 1863、5050、5190、5222 通過。例：ISA 的 IP （來源端） to WAN （目的端） 的埠 1863 方向之連線設定爲允許通過。

D. 建議使用者取消各項 IM 上 Proxy 的設定，可減少無法連線的情形。

E. 建議在 Proxy 設定拒絕存取 URL http://gateway.messenger.hotmail.com/gateway/gateway.dll 以防止用戶端在 MSN 嘗試使用代理連線方式時，會等待較長久的時間才重新使用標準連線方式。

## 4. 注意事項

A. InstantScan 所在的位置，只能管控 HTTP Proxy （IM-HTTP Proxy） 流量，故需做上述調整，讓 IM 的正常連線，可通過 InstantScan 以進行 IM 管控。

B. 原本可透過代理伺服器進行連線的 IM/P2P 軟體，因 InstantScan 能辨視出隱藏在 HTTP/SOCKS 的 IM/P2P 流量，故此類連線方式即被阻擋。

C. Firewall 開放用戶端對外通訊，因設定是內部（LAN、trust）可 access 外部（WAN、un-trust）伺服器的服務（埠 1863、5050...etc），由外部網路對內部網路 （WAN to LAN） 所發起的連線，仍處於被 Firewall 阻擋的保護下。

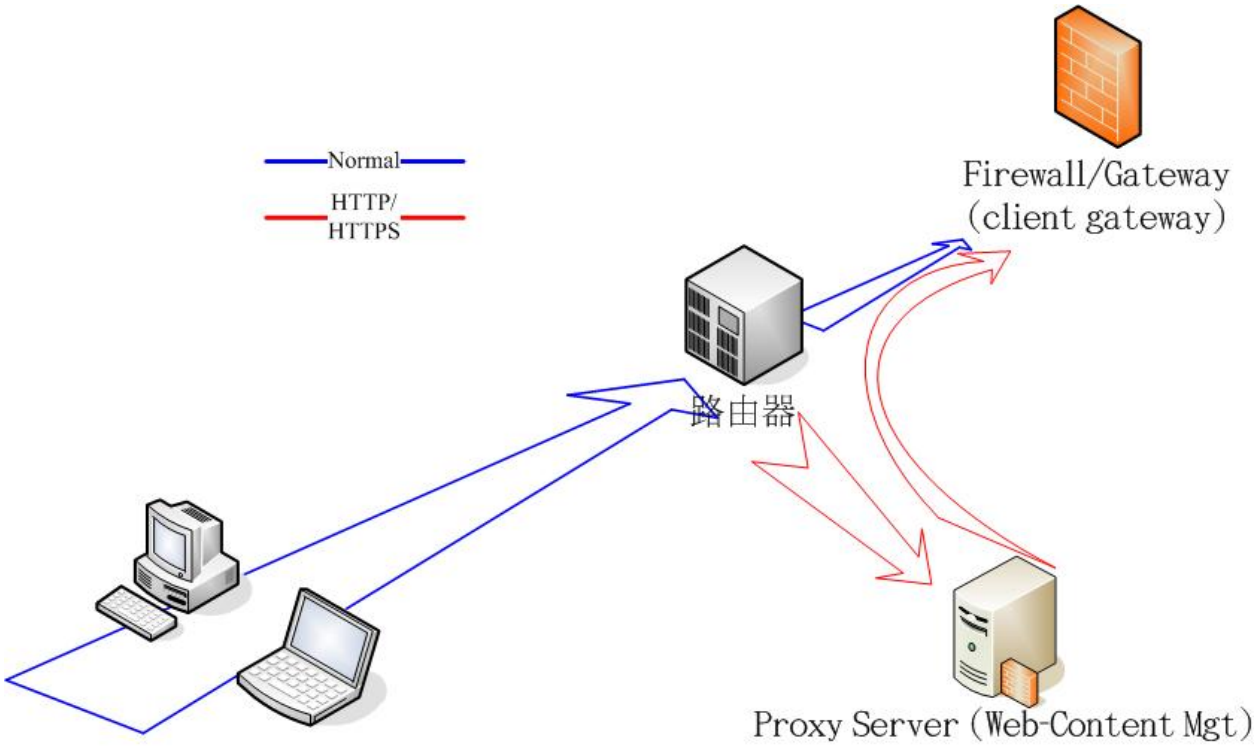
D. 由於原本的 IM 標準的連線方式，不會經過 InstantScan，故需借助 Core Router 將流量導入。

E. ISA Server 需使用 NAT 模式，目的是協助 MSN 可以建立標準連線。

F. Firewall 僅開放 ISA 可以使用開放的 80、443、1863 埠，故沒有 P2P 軟體可能會直接從主要線路 （不經過 InstantScan） 穿過的疑慮。

# 五、Redirect to Web-Proxy

## 1. 圖例




圖表 B-5 使用路由重導 HTTP 流量架構

## 2. 圖例說明

連線藉由路由設備，過濾出通往 80、3128 等埠之連線；亦或借助有能力辨識 HTTP/HTTPS 連線之設備，將連線重新導向 Proxy Server、Web 管理伺服器。此種方式的特點在於不需教導用戶端調整任何設定即可達到 Web 行爲的監控。

由於一般 Web 管理工具無法辨別 HTTP 連線中的內容，IM/P2P 透過 HTTP 模式連線時，便可藉助 Proxy 之便穿出防火牆；使用 HTTP 協定而發展出的 Tunnel 軟體，也可建立連線，將內部網路曝露在不安全的環境下。

## 3. 配置暨設定

InstantScan 應配置在路由器與 Firewall/Gateway 之間。設定如下：

A. 調整 Firewall 的政策，開放 Client 可使用各項 IM 的標準埠（MSN：1863，Yahoo：5050，ICQ：5190，AOL：5190），例：LAN （來源端） to WAN （目的端） 的埠 1863 方向之連線設定爲允許通過。

B. 建議在 Proxy 設定 Deny URL http://gateway.messenger.hotmail.com/gateway/gateway.dll 以防止 Client 在 MSN 嘗試使用代理連線方式時，會等待較久時間才重新使用標準連線方式。

## 4. 注意事項

A. 原本可透過代理伺服器進行連線的 IM/P2P 軟體，因 InstantScan 能辨視出隱藏在 HTTP/SOCKS 的 IM/P2P 流量，故此類連線方式即被阻擋。

B. Firewall 開放用戶端對外通訊，因設定是內部 （LAN、trust） 可存取外部 （WAN、un-trust）伺服器的服務 （埠 1863、5050...等），由外部網路對內部網路 （WAN to LAN） 所發起的連線，仍處於被 Firewall 阻擋的保護下。

C. 開放各項 IM 的標準埠，InstantScan 可在這些通道內控管 IM。

D. 雖然 Firewall 內對外的適度開放，造成 P2P 軟體可能會利用這些 IM 的埠進行連線，然而 InstantScan 的應用防火牆仍可以辨識出來並進行阻擋或管理頻寬的工作。

# 附錄 D
# 系統記錄語法

## 系統記錄語法

InstantScan: time=2005-01-10 12:57:27; mod=SYS; sev=<1|2|3|4|5>; tier=<TIER>; lid=<LID>; msg=<Message>; by=<user|system>; from=<IP|console|system>;

| *嚴重等級* | ***Level name*** |
|---|---|
| 1 | Alert （警告） |
| 2 | Critical （嚴重） |
| 3 | Warning （警示） |
| 4 | Notification （注意） |
| 5 | Information （信息） |

| ***TIER*** | ***LID*** | ***Message*** | ***Severity*** |
|---|---|---|---|
| Client tier=1 | A01 | Login success | Information |
| | A01 | Login fail, miss password | Information |
| | A02 | Change password | Information |
| | A04 | A new user <user> has been added | Notification |
| | A05 | User <user> has been deleted. | Notification |
| | A07 | Login user <user> login failed due to invalid user name | Information |
| | S25 | Backup configuration file by admin | Warning |
| | S26 | Restore configuration file by admin | Warning |
| | S27 | Download configuration | Warning |
| | S28 | Upload configuration | Warning |
| Mgtsvr tier=2 | L01 | Database is full | Critical |
| | L02 | Database is cleanup | Critical |
| | L03 | Backup database to 192.168.17.130 | Warning |
| | L04 | Send report to user@yourCompany.com | Information |
| | L05 | Restore database from 192.168.1.1 | Warning |
| | L06 | Send alert to user@yourCompany.com | Information |
| | M01 | Change E-Mail Alert setting | Notification |
| | M02 | Change FTP Backup setting | Notification |
| | M03 | Change Report Center setting | Notification |
| | M04 | Change Syslog setting | Notification |
| Device | A03 | Login success | Information |

| | | | |
|---|---|---|---|
| tier=3z | A03 | Login fail, miss password | Information |
| | A06 | Change password | Information |
| | S01 | Device Startup | Warning |
| | S02 | Device Reboot | Critical |
| | S03 | MGT set to192.168.17.114 | Notification |
| | S04 | Gateway IP set to 192.168.17.254 | Notification |
| | S05 | Primary DNS set to 10.1.1.1 | Notification |
| | S06 | Secondary DNS set to 168.95.1.1 | Notification |
| | S07 | Management server set to 192.168.17.112 | Notification |
| | S08 | System time updated to 2005-09-04 12:00:00 | Notification |
| | S09 | Factory reset to default settings | Warning |
| | S10 | Firmware upgraded to version X.X.XX | Warning |
| | S10 | Firmware upgrade has failed | Critical |
| | S11 | Application Firewall pattern updated to version X.X.XX.XXX | Warning |
| | S11 | Application Firewall pattern update has failed | Critical |
| | S12 | IM signature updated to version X.X.XX.XXX | Warning |
| | S12 | IM signature update has failed | Critical |
| | S13 | AVDB updated to version X.X.XX.XXX | Warning |
| | S13 | AVDB update has failed | Critical |
| | S14 | Enable application firewall | Notification |
| | S14 | Disable application firewall | Notification |
| | S15 | Enable IM Manager | Notification |
| | S15 | Disable IM Manager | Notification |
| | S16 | Enable Traffic Manager | Notification |
| | S16 | Disable Traffic Manager | Notification |
| | S17 | Enable HA | Critical |
| | S17 | Disable HA | Critical |
| | S18 | HA mode changed to AA | Critical |
| | S18 | HA mode changed to AS | Critical |
| | S19 | HA type changed to master | Critical |
| | S19 | HA type changed to slave | Critical |
| | S20 | HA monitored node <node_name> failed | Warning |
| | S21 | HA control changed to master | Alert |
| | S21 | HA control changed to slave | Alert |
| | S22 | HA Virtual IP Address: 192.168.17.100 | Notification |
| | S23 | HA In-Ping-Nodes: 192.168.17.111 | Notification |
| | S24 | HA Ex-Ping-Nodes: 192.168.17.254 | Notificaiton |

| | | | |
|---|---|---|---|
| | S29 | URLDB | |
| | S31 | Application Firewall pattern updated to version X.X.XX.XXX | Warning |
| | S31 | Application Firewall pattern update has failed(error code:XX) | Critical |
| | S32 | reserved for future using | |
| | S33 | AVDB updated to version X.X.XX.XXX | Warning |
| | S33 | AVDB update has failed(error code:XX) | Critical |
| | S34 | URLDB updated to version X.X.XX.XXX | Warning |
| | S34 | URLDB update has failed(error code:XX) | Critical |
| | S35 | IM engine updated to version X.X.XX | Warning |
| | S35 | IM engine has failed(error code:XX) | Critical |
| | S36 | Application Firewall engine updated to version X.X.XX | Warning |
| | S36 | Application Firewall engine update has failed(error code:XX) | Critical |
| | S37 | reserved for future using | |
| | S38 | Antivirus database engine updated to version X.X.XX | Warning |
| | S38 | Antivirus database engine update has failed(error code:XX) | Critical |
| | S39 | URL database engine updated to version X.X.XX.XXX | Warning |
| | S39 | URL database engine update has failed(error code:XX) | Critical |
| | S40 | reserved for future using | |
| | S41 | Application Firewall pattern restored to version X.X.XX.XXX | Warning |
| | S41 | Application Firewall pattern restore has failed(error code:XX) | Critical |
| | S42 | reserved for future using | |
| | S43 | AVDB restored to version X.X.XX.XXX | Warning |
| | S43 | AVDB restore has failed(error code:XX) | Critical |
| | S44 | URLDB restored to version X.X.XX.XXX | Warning |
| | S44 | URLDB restore has failed(error code:XX) | Critical |
| | S45 | IM engine restored to version X.X.XX.XXX | Warning |
| | S45 | IM engine restore has failed(error code:XX) | Critical |
| | S46 | Application Firewall engine restored to version X.X.XX | Warning |
| | S46 | Application Firewall engine restore has failed(error code:XX) | Critical |
| | S47 | reserved for future using | |
| | S48 | Antivirus database engine restored to version X.X.XX | Warning |
| | S48 | Antivirus database engine restore has failed(error code:XX) | Critical |
| | S49 | URL database engine restored to version X.X.XX | Warning |
| | S49 | URL database engine restore has failed(error code:XX) | Critical |
| | S50 | reserved for future using | |
| | S51 | $SWID<br>(Update Successfully. Update database and then respond a new SWID.) | |

| | | | |
|---|---|---|---|
| | S52 | $SWID<br>(Keep old license. Don't need to update database and then respond the old SWID.) | |
| | S53 | Request is rejected | |
| | S54 | Invalid HWID | |
| | S55 | This device is not registered | |
| | S56 | This license is invalid | |
| | S57 | This license has been registered | |
| | S58 | This license cannot be used on this device | |
| | S59 | Can not connect to database | |
| | S60 | No such device | |
| | S61 | Can not connect to device | |
| | S62 | Unable to clear database table | |
| | S63 | Filter List error | |
| | S64 | Post parameters error | |
| | S65 | Post value is invalid | |
| | S66 | Invalid software ID | |
| | S67 | Execute SQL command fail | |
| | S68 | No version obtained | |
| | S69 | No such database | |
| | S70 | Backup database fail | |
| | S71 | Restore database fail | |
| | S72 | Unmatched pattern version | |
| | S73 | Software ID was reset to trial version | |
| | S74 | Invalid checksum | |
| | S75 | Can not find backup SQL scheme | |
| | S76 | Enable Web Manager | Notification |
| | S76 | Disable Web Manager | Notification |

表格 D-1 系統記錄格式說明

# 附錄 E
# 詞彙集

**DDoS （分段式阻斷服務，Distributed Denial-of-Service ）**

DDoS 是 DoS 的一種變形，因爲它是透過網路分散來源的技巧，所以將之稱作分散 式 DoS（Distributed DoS，簡稱 DDoS）攻擊。

**DoS （Denial of Service ）**

DoS 是一種入侵程式，可以讓電腦無法直執行某些動作，或者無故當機。與一般駭客入侵不同的是，DoS 攻擊並不會讓電腦內部資料遭到竊取或竄改，而是以癱瘓主機爲目的。

**FTP （檔案傳輸協定 File Transfer Protocol）**

FTP 是在傳輸控制協定 （TCP/IP ） 網路使用的一種檔案通訊協定，定義如何將一個電腦系統，連接現有的網路（Network） ，以便存取網路上的系統資源。其主要工作是提供檔案非錄清單，負責檔案傳輸與轉換工作。

**H.323**

H.323 規範是在 1996 年經國際電信聯盟認定，可以解決多媒體傳輸所要求的即時性與連續性問題。其主要內容是在定義分封切換式網路上終端機之間的壓縮和解壓縮標準、通話程式及媒體傳輸等協定，同時也定義了在分封切換式網路上的終端如何與傳統的電話網絡互相通話的機制。H.323 界定語音及視訊的壓縮／解壓縮設備，雙方溝通的設定與控制。在語音方面，它支援多種標準，其中以 G.711 爲主；至於視訊方面，H.323 則支援 H.261 與 H.263 兩種主要的視訊壓縮／解壓縮標準。

**IM （即時通訊，Instant Messaging）**

即時通訊是一種聊天應用，透過網際網路即時地與他方使用者傳送文字簡訊，現在更可以傳送檔案、語音、視訊或玩網路遊戲等。

**IPS （異常偵測，Anomaly-Based IPS）**

異常偵測則是對使用者或網路流量先建立一個「正常」的行爲，再對通過的封包去做比對，假如超過正常行爲的門檻值就是視爲異常。此種做法的優點是可以偵測未知型態的入侵，但是誤判率會表較高。

**IP Spoofing （IP 地址欺僞）**

這是一種攻擊者得知主機位址之後，利用外部封包攻擊主機的方法，由於封包 （Packet） 的來源位址和內部封包一樣，因此主機 （Host） 會認爲這是來自內部的封包，因而允許進行鏈結 （Link） ，這種攻擊方法也會被內部破壞者使用。

**LDAP （Lightweight Directory Access Protocol）**

LDAP 是 Lightweight Directory Access Protocol 的簡稱，是目前最流行的目錄服務 （Directory Service, DS） 存取協定。

**License Key （授權碼）**

InstantScan 由多個模組組成，某些模組必須購買授權碼並于開機時輸入此授權碼才可以啓用該服務。

**P2P （點對點，Peer-To-Peer）**

這是一種傳輸模式，以點對點的方式傳輸訊息，例如曾經瘋狂流行過的 Napster （Napster），就是以點對點的方式傳輸，使用者在對方提供的檔案伺服器上直接上傳或下載 （Download） 樂曲；P2P 架構要比主從架構 （Client/Server） 簡單便宜，因爲無須太多高深的技術就可以執行，不過當網路負擔太重的啥喉，傳輸的狀況就不會比主從架構理想。

**Port**

資料 （Data） 進入或出去的一個接連點。

**Protocol （通訊協定）**

一個議定主要的就是幾個通信處理之間，要被交換的一些訊息格式和訊息內涵的一組協約或規則。讓實施和使用更加方便，在一些複雜的網路 （Network） 中，高階議定可以用一種分層的方式來使用一些低階議定。

**RADIUS （遠端認證撥接使用者服務，Remote Authentication Dial-In User Service）**

RADIUS 是被許多網際網路服務供應商 （ISP ） 所使用的認證與記帳系統。當你撥入 ISP 時，你必須輸入你的用戶名稱和密碼。這個資訊被傳送到 RADIUS 伺服器 （Server） ，查看資訊是否正確，並授權 ISP 系統的存取。雖然 RADIUS 不是一個公認的標準，但是它的規格是由網際網路工程工作團隊所維持。

**RDP （遠端桌面協議，Remote Desktop Protocol）**

RDP 是 Windows 終端機伺服器和用戶端用來彼此通訊的通訊協定。 用戶端會利用它將擊鍵及滑鼠點按資訊傳送到伺服器，而伺服器則會利用此協定將顯示 資訊傳送給用戶端。

Router （路由器）

路由器又稱爲路徑器，使用者在網路層上連接不同網路所用的硬體與軟體，路由器與橋接器 （Bridge） 的功能類似，借著將許多較小的網路連結在一起，以便有效擴充網路。路由器可以連接使用不同網際網路通訊協定 （IP ） 和傳輸方法的區域網路 （LAN ） 。

RS-232

RS-232 爲 EIA 標準，是裝置間連結資料最普遍的方式。

**Scan**

Scan 可以是埠、IP 或弱點掃描。駭客掃埠來尋找入侵的目標。他們可能使用 TCP connect( ) call、SYN 掃描（half-open scanning）、Nmap 等等。

**Severity**

入侵攻擊的嚴重性被定義成最低到最嚴重 5 個等級，其對預設對應的動作視其嚴重性而定。

**Signature**

特徵碼是辨識惡意軟體之獨特的行爲模式。

**Smurf Attack**

Smurf 攻擊者將僞造來源的 ICMP echo request 封包送到 IP broadcast addresses，而來源地址設成被害者的位址，造成 broadcast 位址回傳大量的 ICMP echo reply 封包給被害者，使被害者的網路擁塞甚至中斷。

**Spam （垃圾信件）**

Spam 原是一種美國肉罐頭的商標，隨著網際網路 （Internet） 的出現，而被用來指稱垃圾電子郵件 （E-mail ） ，這類垃圾郵件內含許多使用者可能不想看的商業廣告，並傳送給大量的收件人。用於動詞時，則是指將許多使用者不想要的訊息 （message（MESG）（MSG）） ，貼在相關的郵件或網頁上。

**Spoofing （欺僞）**

指的是以未經過授權的身份，在網路 （Network） 上從事傳輸動作，通常是惡意的行爲。

**SSL （Secured Socket Layer）**

SSL 是將公開金鑰的加密技術加入合併到網景領航員 （Netscape Navigator） 的網路流覽器 （Browser ） 裡面，還有網景公司商業用的伺服器 （Server） 裡，且目前大多數的網路 （Network） 伺服器與流覽器也已經採用 SSL。SSL 的加密與解密過程當中，必須透過密碼簿中的金鑰才能將亂碼完全解開，爲了確保使用者拿到的金鑰安全性與公正性，金鑰必須透過具有公信力的伺服器認證中心認證。

**SYN Attack**

此種攻擊方式主要是利用 TCP 連結的 three way handshaking 的缺陷。在 TCP/IP 通訊協定中，傳輸雙方 （A、B） 的連結方式是，A 會從特定埠送出一個 SYN 封包給 B 的特定埠，而此時 B 會響應一個 SYN-ACK 的封包給 A，如果順利到達，A 會再回送一個 ACK 的封包給 B 作確認。在完成這些程式之後，A 與 B 便能確認彼此的連結，此時連線建立，雙方能夠溝通，並傳送與收發資料。SYN 這類攻擊讓 TCP 協議無法完成三次握手協議;

**TCP （傳輸控制協議 Transmission Control Protocol）**

TCP/IP 是一組用來連接網際網路 （Internet） 上主機 （Host） 的協定標準。TCP 相當於開放系統互相連線參考模型的第四層 （運輸層） 協議，而 IP 則相當於 OSI/RM 的第三層（網路層）協定。但 TCP/IP 通常是指一組完整的網路通訊協定。

**Teardrop**

Teardrop attack 的目的不是要去偷取你電腦中的資料，而是要讓使用者的電腦當機無法繼續使用。利用封包重組時的弱點，當資料經由網路傳送，IP 封包經常會被切割成許多小片段。每個小片段和原來封包的結構大致都相同，除了一些記載位移的資訊。而 Teardrop 則創造出一些 IP 片段，這些片段包含重迭的位移值。當這些片段到達目的地而被重組時，可能就會造成一些系統當機。當它檢查到後面片段的資料長度大於重迭的資料片段時，重迭部份將會被略過，但是後面的片段的資料長度小於重迭的資料片段時，使得資料片段長度太小，當接收到傳來的封包時，只會去檢查是否太長，是否應該捨棄重迭多餘的部分，但卻不會去檢查是否太短而造成了錯誤.

**Telnet**

終端機 （terminal（T）（TERM）（TML）） 模擬程式是遠端登入的網際網路通訊協定 （IP ），使電腦使用者可與伺服器 （Server） 做互動式的連結，並存取 （Access） 遠端網站。

**Terminal Emulator （終端機模擬器）**

容許在個人電腦和主機電腦或裝置間做同步資料傳送，而資料則以主機可接受的格式來交換。。

**TFTP （簡單檔案傳輸通訊協定 Trivial File Transfer Protocol）**

TFTP 是 TCP/IP Protocol 中的一員，和 FTP 一樣是傳輸檔案用，但是 FTP 是使用 TCP，但是 TFTP 是使用 UDP 來傳輸，使用 UDP 是不作傳輸資料正確性的驗證，所以實際的檔案傳輸是不會使用到 TFTP，然而若您是經常使用網路設備如 Terminal Server、Router 或是 SNMP Hub 的話，那您便可能需要使用 TFTP 來 Upgrade 網路設備的 Firmware 或 Software。

**Transparent Mode （透通模式）**

產品的複雜作業情形已被隱藏起來，使用者使用產品時一點都不會覺得有何困難，而且操作容易。一般的透通模式裝置，容易安裝於任何網路架構底下，且不需要改變既有的網路設定。

**Transport （傳輸模式）**

IPsec 封裝機制的一種，傳輸模式即是所謂的 Host-to-Host 的封裝機制，亦即由連線兩端主機對其交換的 IP 封包以前段所述的 AH 或（及）ESP 做安全保護，兩通訊主機皆須實作有 IPsec。

**Trojan （特洛伊木馬，Trojan Horse）**

顧名思義，特洛伊木馬是一種看似無害其實會隱藏起來在電腦內部作怪的程式。它以合法功能的面貌僞裝，將病毒碼放在一個外表看起來十分正常的程式當中，等到適當的時機才開始破壞的動作。特洛伊木馬一種惡性程式碼 （Malicious code） ，但和病毒 （Virus） 最大的不同是，特洛伊通常不會自我複製，大多用來竊取電腦密碼。

**UDP （使用者資料流程通協議，User Datagram Protocol）**

UDP 是傳輸層通訊方法或通信協定，用於傳送短暫需求的少量資料。這個通信協定可提供資料傳輸量有限的服務，因此不需要驗證目的端是否已接收動作的應用程式資料通訊機制。

**UID （使用者識別字，User IDentification）**

一種碼，具有惟一性，可以用來識別一個系統的使用者。

**URL （統一資源定位器，Uniform Resource Locator）**

指明某個體所在位置的標準方式，所謂某個體，通常是指網際網路 （Internet） 上的網頁，至於其他的個體我們在下面說明。全球資訊網 （WWW ） 以 URL 作爲網址的格式。在超檔標示語言 （HTML ） 的檔中，利用 URL 來指定超鏈結（Hyperlink ） 的目標位置，通常這個目標位置就是另一個 HTML 檔 （而且還可能儲存在另一台電腦上）。

**Virus （病毒）**

病毒是一種程式，一種會將自己附加在其他程式裡面的軟體，當附加程式被執行的時候，病毒程式也跟著啓動。病毒具有傳播和感染的特性，可能會造成系統損害、刪除程式或者資料。病毒通常會附著在可執行檔或開機磁片、磁片，甚至硬碟分割磁區，不過必須附加在其他程式中才能感染另一台電腦，某些病毒也會借著電子郵件 （E-mail ） 感染其他電腦。

**VPN （私有虛擬網路，Virtual Private Network）**

VPN 是通道 （Tunneling）、加密 （Encryption ）、身分辨認 （Authentication ）、存取控制 （Access Control） 等技術，及經由 Internet、管理式 IP 網路、或網路供應商骨幹來傳遞資料等服務之眾多專案的綜合體。VPN 能利用公用網絡來建立與遠端使用者、分支辦公室及夥伴建立專屬連結。如果企業想要有一個安全有保障的廣域網路環境， VPN 可以透過目前的公眾網路，在網路上劃分出一條類似私有專線所提供的通道，即所謂的 VPN 的主要元件 — Tunneling，企業包括 Internet、企業內網際網路、 企業外部網路的使用者都可以在通過安全認證後，在這個通道內不受時間與地點限制，享有其所需的網路服務。

**Vulnerability （弱點）**

系統或應用程式容易被攻擊的點。

**WAN （Wide Area Networks）**

廣域網路是能在廣大地理區域傳輸資料的電腦網路，它是由一些透過電信服務連接的區域網路組成。與區域網路不同點在於，它們使用的規約不相同，傳輸速率比區域網路低。

**Worm （電腦蠕蟲）**

電腦蠕蟲也可說是電腦病毒的一種，與病毒不同的是，蠕蟲不會感染寄生在其他檔案。蠕蟲的主要特性是會自我複製並主動散播到網路系統上的其他電腦裡面。就像蟲一樣在網路系統裡面到處爬竄，所以稱爲「蠕蟲」。

**WWW （World Wide Web ）**

網際網路的通稱。

# 附錄 F
# 索引