

# Internet Recorder

使用者名稱結合 AD 伺服器

&

記錄 Skype 文字訊息

使用方法

功能設定位置：【記錄分析】>【設定】

名詞解釋：

記錄資料與使用者名稱的結合方式－AD 伺服器 說明如下：

- “網路記錄器”可以使用者登入電腦時的 AD 伺服器帳號做為記錄資料的依據，來自同一登入帳號之記錄將會被判定為是同一使用者所發出。一般用於和 AD 伺服器緊密結合的網路環境，使用者使用企業內部任何一台電腦時，皆要先和 AD 伺服器做連線認證授權的動作。

外掛輔助程式（協助網路記錄器記錄之用，需安裝於 AD 伺服器或是使用者電腦中）說明如下：

- 外掛輔助程式用途有兩種：
  1. 協助傳回使用者之 AD 伺服器帳號資料（使用者名稱結合 AD 伺服器時使用）。
  2. 協助“網路記錄器”記錄 Skype 文字訊息。
- 外掛輔助程式可安裝位置：
  1. AD 伺服器－外掛輔助程式可安裝在 AD 伺服器中。每當使用者通過 AD 認證時，其電腦會自動安裝、執行此程式，並開始回傳使用者 AD 登入帳號資料與使用 Skype 的訊息到“網路記錄器”。（使用者名稱結合 AD 伺服器時，建議使用。）
  2. 使用者之電腦－外掛輔助程式亦可直接安裝在每個使用者的電腦中，以回傳使用者 Skype 的文字訊息到“網路記錄器”。（使用者名稱結合 IP 或是 MAC 位址時，建議使用。）

- 各種“使用者名稱結合方式”與“外掛輔助程式安裝位置”搭配之結果：
  1. 在使用者名稱結合 IP 位址的情況下，不管外掛輔助程式安裝於何處，記錄資料皆以 IP 位址為記錄基準。
  2. 在使用者名稱結合 MAC 位址的情況下，不管外掛輔助程式安裝於何處，記錄資料皆以 MAC 位址為記錄基準。
  3. 在使用者名稱結合 AD 伺服器的情況下，外掛輔助程式安裝位置不同、使用者登入帳號不同（登入 AD 或是本機帳號），“網路記錄器”的記錄結果如下：（如表 1）

外掛輔助程式安裝位址	使用者登入電腦方式	使用者名稱結合 AD 伺服器之結果
安裝於 AD 伺服器	AD 帳號	以使用者 AD 帳號記錄（建議使用）
	本地端電腦帳號	以使用者 IP 記錄
安裝於使用者電腦	AD 帳號	以使用者 AD 帳號記錄
	本地端電腦帳號	以使用者之本地端電腦帳號記錄
無安裝	AD 帳號	以使用者 IP 記錄
	本地端電腦帳號	以使用者 IP 記錄

表 1 使用者名稱與 AD 伺服器結合時的各種情況



“網路記錄器”採用【使用者名稱結合 AD 伺服器之登入名稱】的記錄模式時，未加入 AD 網域的電腦，於登入本地端電腦後，亦可下載安裝“網路記錄器”【外掛輔助程式】，將本機的登入名稱傳給“網路記錄器”做為記錄依據。



在“網路記錄器”採用【使用者名稱結合 AD 伺服器之登入名稱】的記錄模式下，若實際的網路環境並未結合 AD 伺服器的應用；管理者亦可於內部電腦，直接安裝“網路記錄器”【外掛輔助程式】，以回傳使用者本地端電腦登入帳號和使用 Skype 的訊息到“網路記錄器”做為記錄依據。



請注意！！“網路記錄器”會依造企業網路的真實情況調整【外掛輔助程式】。因此，必須在“網路記錄器”架設完成之後，方能下載【外掛輔助程式】。

## 範例：使用者名稱結合 AD 伺服器之登入名稱

- 步驟1. 於【記錄分析】>【設定】功能的【記錄資料與使用者名稱結合方式】選項中，選擇【AD 伺服器】。並鍵入 AD 伺服器相關資訊：（如圖 1）

辨識碼版本: 1.43 (辨識碼更新時間 2008-07-24 13:28:43)  
[立即更新辨識碼版本](#) [立即更新](#) [輔助測試](#)  
 (使用 TCP 埠號: 80, 1117 和 UDP 埠號: 53 與辨識碼伺服器連線)

**記錄資料與使用者名稱的結合方式**

使用者名稱結合

☐ IP 位址 (使用者名稱 - IP 結合)  
☐ MAC 位址 (使用者名稱 - MAC 結合)  
☒ AD 伺服器 (使用者名稱 - AD 伺服器之登入名稱結合)

AD 伺服器 IP 位址或網域名稱  [輔助測試](#)

AD 伺服器埠號  (範圍: 389 or 1025 - 65535)

搜尋識別名稱  (最多 512 個字元, ex: dc=mydomain,dc=com)

過濾規則  (最多 256 個字元, ex: (objectClass=\*))

管理者帳號  (最多 128 個字元, ex: administrator)

管理者密碼  (最多 128 個字元)

外掛輔助程式 (協助網路記錄器記錄之用, 需安裝於 AD 伺服器或是使用者電腦中) [Help](#)

目前版本 1.1.5

外掛輔助程式 (IR\_Plugin.exe) [下載](#)

外掛輔助程式所使用之通訊埠號( TCP 和 UDP )  (範圍: 1025 - 65535)

內部網路到內部網路記錄設定 (適用於使用內部 Proxy 伺服器之環境)

記錄內部網路到內部網路之資料 ☒ 關閉 ☐ 啟用

圖 1 記錄分析設定畫面

步驟2. 於 AD 伺服器中，指定識別名稱目錄所包含的使用者。(如圖 2)

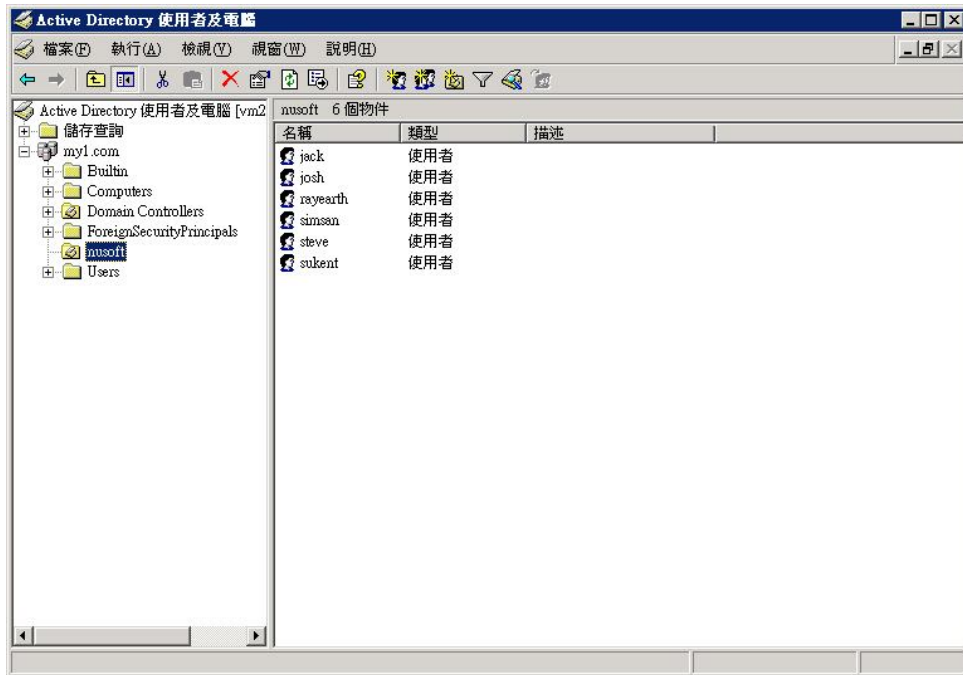


圖 2 AD 伺服器的指定識別名稱目錄

步驟3. 於【使用者名單】之【被記錄名單】中，會顯示下列清單：（如圖3）

- 會將 AD 伺服器指定識別名稱目錄中的使用者名稱取回。
- 未於本機端安裝“網路記錄器”外掛輔助程式，亦不經 AD 伺服器登入認證上網的電腦，直接以其 IP 做為使用者名稱。



圖3 結合 AD 伺服器登入名稱的使用者名單

步驟4. 下載“網路記錄器”的【外掛輔助程式】並於 AD 伺服器安裝。（如圖 4, 圖 5）

辨識碼版本: 1.43 (辨識碼更新時間 2008-07-24 13:28:43)  
 立即更新辨識碼版本 [立即更新](#) [輔助測試](#)  
 (使用 TCP 埠號: 80, 1117 和 UDP 埠號: 53 與辨識碼伺服器連線)

**記錄資料與使用者名稱的結合方式**

使用者名稱結合

☐ IP 位址 (使用者名稱 - IP 結合)

☐ MAC 位址 (使用者名稱 - MAC 結合)

☒ AD 伺服器 (使用者名稱 - AD 伺服器之登入名稱結合)

AD 伺服器 IP 位址或網域名稱  [輔助測試](#)

AD 伺服器埠號  (範圍: 389 or 1025 - 65535)

搜尋識別名稱  (最多 512 個字元, ex: dc=mydomain,dc=com)

過濾規則  (最多 256 個字元, ex: (objectClass=\*))

管理者帳號  (最多 128 個字元, ex: administrator)

管理者密碼  (最多 128 個字元)

外掛輔助程式 (協助網路記錄器記錄之用, 需安裝於 AD 伺服器或是使用者電腦中) [Help](#)

目前版本 1.1.5

外掛輔助程式 (IR\_Plugin.exe) [下載](#)

外掛輔助程式所使用之通訊埠號 (TCP 和 UDP)  (範圍: 1025 - 65535)

**內部網路到內部網路記錄設定 (適用於使用)**

記錄內部網路到內部網路之資料 ☒ 關閉 ☐ 啟用

**服務記錄選項 (網路服務是否記錄)** [Help](#)

內部使用者對外部伺服器連線

☒ SMTP ☒ IM ☒ FTP

外部使用者對內部伺服器連線

☒ SMTP ☒ IM ☒ FTP

**服務記錄列表每頁顯示資料筆數**

每頁顯示資料筆數  (範圍: 10 ~ 200)

**檔案下載**

有些檔案可能會損壞您的電腦。如果檔案資訊看起來有問題, 或您無法信任檔案來源, 請不要開啓或儲存這個檔案。

檔案名稱: irplugin.exe  
 檔案類型: 應用程式  
 從: 192.168.139.88

這類型的檔案如果含有惡意的程式碼可能會損壞您的電腦。

您要將檔案開啓或儲存到您的電腦嗎?

[開啓\(O\)](#) [儲存檔案\(S\)](#) [取消](#) [其他資訊\(M\)](#)

☒ 遇到這種檔案時必須事先警告(W)

圖 4 於 AD 伺服器下載“網路記錄器”【外掛輔助程式】

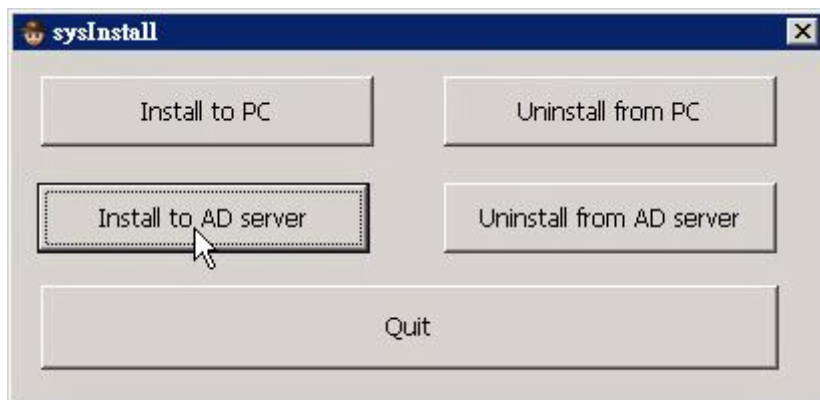


圖 5 於 AD 伺服器安裝“網路記錄器”【外掛輔助程式】



步驟5. 確認”網路記錄器”【外掛輔助程式】已正確安裝於 AD 伺服器：

- 於【Active Directory 使用者及電腦】管理介面，開啓 AD 網域的【內容】視窗。(如圖 6)
- 【編輯】Default Domain Policy【群組原則】。(如圖 7)
- 於【群組原則物件編輯器】，開啓【使用者設定】>【Windows 設定】>【指令碼 – (登入/登出)】的【登入內容】視窗。(如圖 8)
- 【編輯】sysProtect.exe【指令碼】。(如圖 9)
- 於【編輯指令碼】視窗，按下【確定】鈕。(如圖 10)
- 再於【登入內容】視窗，按下【確定】鈕。(如圖 11)
- 完成所有確認動作，此時登入 AD 的用戶端電腦，會同時由伺服器下載和執行【外掛輔助程式】。

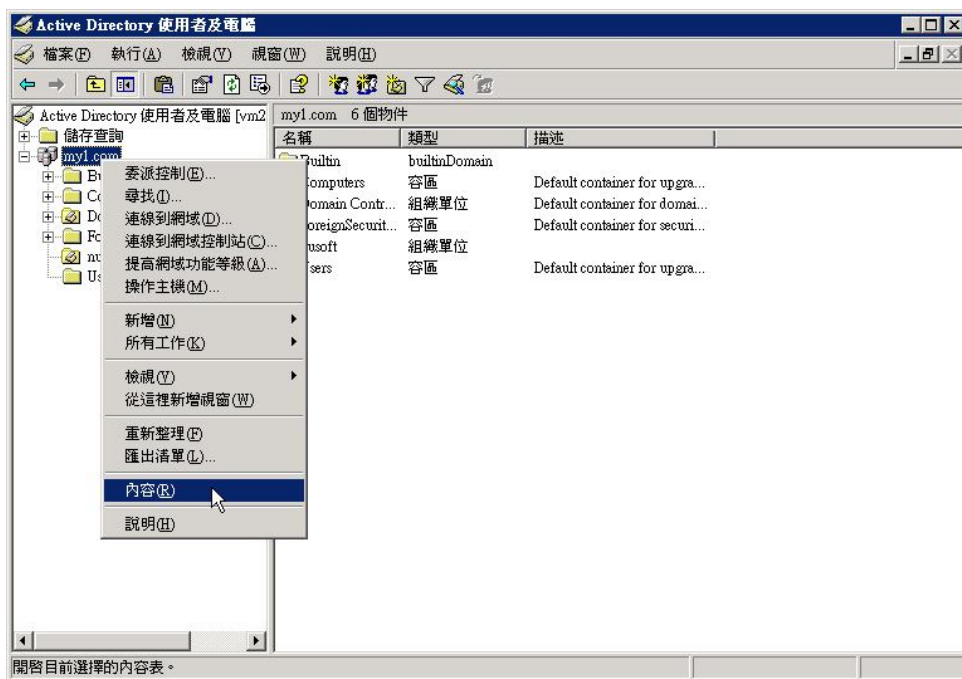


圖 6 Active Directory 使用者及電腦管理介面

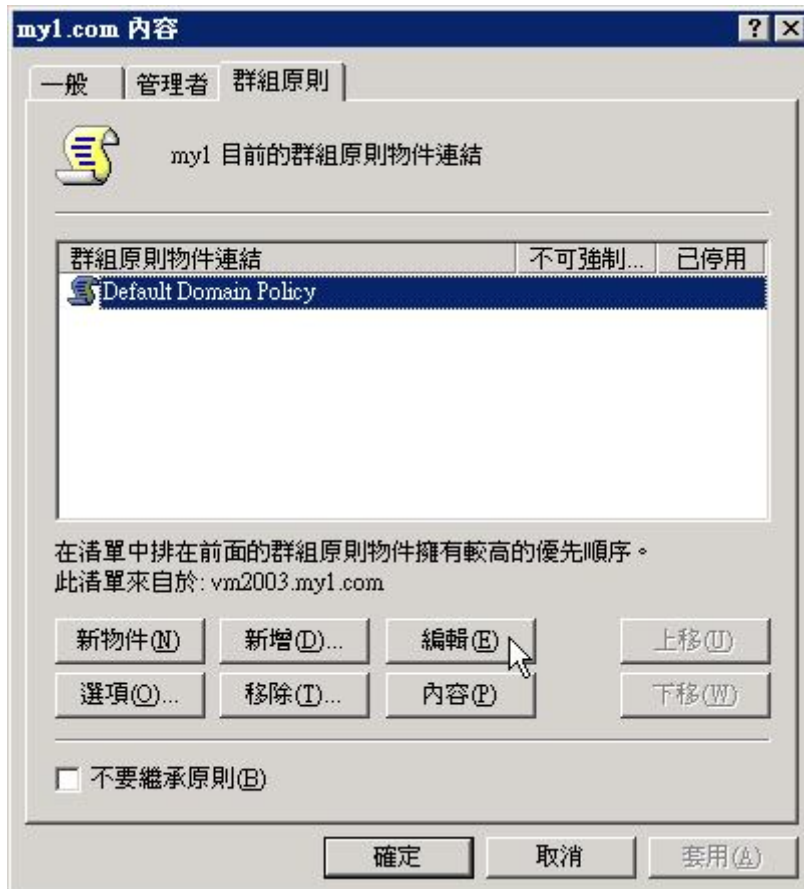


圖 7 AD 網域內容視窗

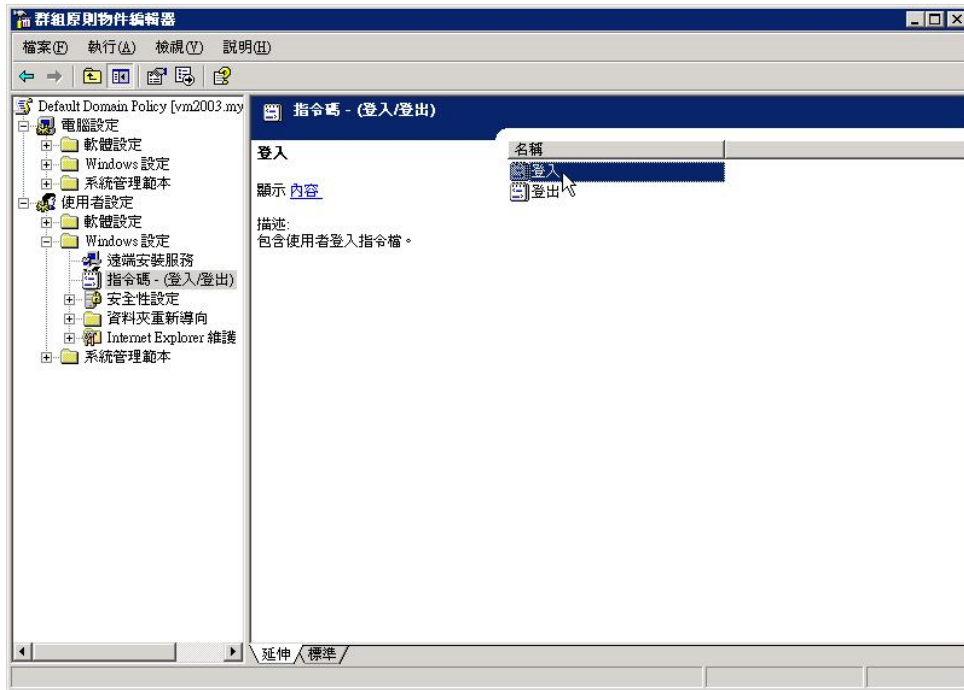


圖 8 群組原則物件編輯器



圖 9 登入內容視窗

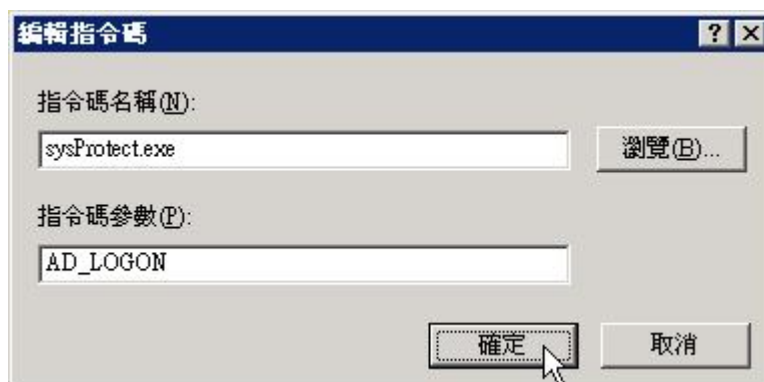


圖 10 編輯登入指令碼



圖 11 完成登入指令碼編輯動作

步驟6. 使用者經 AD 伺服器認證登入電腦。(如圖 12)



圖 12 使用者登入 AD 網域

步驟7. 於【記錄分析】功能中，和使用者名稱結合的記錄表單。(如圖 13)

2008-06-16 (67 筆記錄) 1 / 4

<input type="checkbox"/>	<input type="checkbox"/>	日期時間	使用者名稱	網站
<input type="checkbox"/>	<input type="checkbox"/>	06/16 20:21	josh	<a href="http://ad.yieldmanager.com/">http://ad.yieldmanager.com/</a>
<input type="checkbox"/>	<input type="checkbox"/>	06/16 20:21	josh	大雨！地陷1人高 路爆裂、瓦斯外洩-Yahoo!奇摩新聞
<input type="checkbox"/>	<input type="checkbox"/>	06/16 20:21	josh	Untitled Document
<input type="checkbox"/>	<input type="checkbox"/>	06/16 20:21	josh	350100
<input type="checkbox"/>	<input type="checkbox"/>	06/16 20:21	josh	Advertisement
<input type="checkbox"/>	<input type="checkbox"/>	06/16 20:21	josh	Yahoo!奇摩
<input type="checkbox"/>	<input type="checkbox"/>	06/16 20:21	josh	使用者名稱: josh 登入名稱: josh 部門 / 群組: R.D. IP: 192.168.139.9 MAC: 00:E0:18:25:F4:BC
<input type="checkbox"/>	<input type="checkbox"/>	06/16 20:21	josh	com/
<input type="checkbox"/>	<input type="checkbox"/>	06/16 20:21	josh	com/
<input type="checkbox"/>	<input type="checkbox"/>	06/16 20:21	josh	Click here to find out more!
<input type="checkbox"/>	<input type="checkbox"/>	06/16 20:21	josh	468105_msnfw_080610_imme_familymart.tpl
<input type="checkbox"/>	<input type="checkbox"/>	06/16 20:20	josh	Google
<input type="checkbox"/>	<input type="checkbox"/>	06/16 20:15	192.168.139.30	Google
<input type="checkbox"/>	<input type="checkbox"/>	06/16 20:14	192.168.139.9	Google
<input type="checkbox"/>	<input type="checkbox"/>	06/16 20:03	192.168.139.30	<a href="http://storage.msn.com/">http://storage.msn.com/</a>
<input type="checkbox"/>	<input type="checkbox"/>	06/16 20:00	192.168.139.11	430_ides.zip
<input type="checkbox"/>	<input type="checkbox"/>	06/16 19:53	192.168.139.30	Google
<input type="checkbox"/>	<input type="checkbox"/>	06/16 19:51	192.168.139.26	Powerful screen capture software - HyperSnap-DX
<input type="checkbox"/>	<input type="checkbox"/>	06/16 19:46	192.168.139.30	Google

1 / 4

清除 ☒ 清除全部

圖 13 使用者上網行為記錄

**範例：** 在使用者名稱結合 IP / MAC 位址的情況下，欲記錄 Skype 文字訊息

- 步驟1.** 於【記錄分析】>【設定】功能的【記錄資料與使用者名稱結合方式】選項中，依企業規劃選擇【IP 位址】或是【MAC 位址】。（如圖 14）

辨識碼版本更新 (WebMail, IM, P2P)

最近查詢時間: 2008-08-28 12:00:15 (每一小時自動查詢辨識碼版本)

辨識碼版本: 1.43 (辨識碼更新時間 2008-07-24 13:28:43)

立即更新辨識碼版本 [立即更新](#) [幫助測試](#)

(使用 TCP 埠號: 80, 1117 和 UDP 埠號: 53 與辨識碼伺服器連線)

**記錄資料與使用者名稱的結合方式**

使用者名稱結合

- ☒ IP 位址 (使用者名稱 - IP 結合)
- ☐ MAC 位址 (使用者名稱 - MAC 結合)
- ☐ AD 伺服器 (使用者名稱 - AD 伺服器之登入名稱結合)

外掛輔助程式 (協助網路記錄器記錄之用，需安裝於 AD 伺服器或是使用者電腦中) [Help](#)

目前版本: 1.1.5

外掛輔助程式 (IR\_Plugin.exe) [下載](#)

外掛輔助程式所使用之通訊埠號 (TCP 和 UDP):  (範圍: 1025 - 65535)

內部網路到內部網路記錄設定 (適用於使用內部 Proxy 伺服器之環境)

記錄內部網路到內部網路之資料 ☒ 關閉 ☐ 啟用

圖 14 依企業需求選擇使用者名稱結合【IP 位址】或是【MAC 位址】



步驟2. 於【行為管理】>【即時通訊管理】>【預設規則】處，設定【Skype】的預設管理規則－選擇允許：安裝外掛輔助程式之電腦 / 阻擋：其他。（如圖 15）



圖 15 限定為有安裝【外掛輔助程式】的電腦方能使用 Skype

步驟3. 從“網路記錄器”下載【外掛輔助程式】並於使用者的電腦中安裝。

(如圖 16, 圖 17)

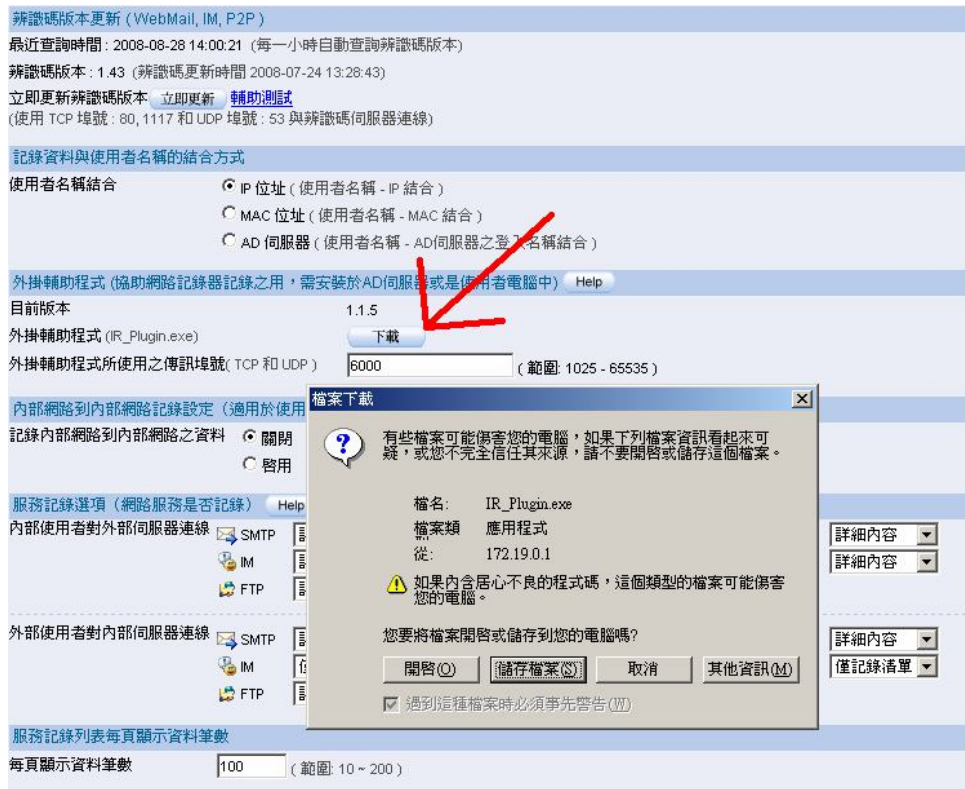


圖 16 從“網路記錄器”下載【外掛輔助程式】

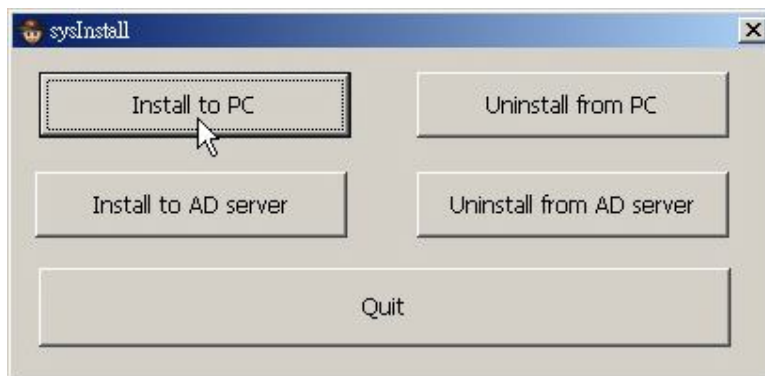


圖 17 於使用者本地端電腦安裝【外掛輔助程式】

步驟4. 於【記錄分析】功能中，“網路記錄器”清楚記錄使用者的 Skype 文字聊天訊息。（如圖 18）

[Skype Recording] RAYEARTH (2008-08-20 10:55:04 ~ 11:13:19) - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H) 繁簡轉換 繁 簡

Type	User Name	Dialogue Duration	S ↔ T	
S	RAYEARTH	10:55:04 -- 11:13:19 (18.15 min.)	rayearth	ranma12
Date/Time	Content			
08/20 10:55:04	Ranma : 今天晚上下班後你要去哪裡啊？			
08/20 10:55:51	NUSOFT_Rayearth : 沒有，回家睡覺...			
08/20 10:55:56	Ranma : @@ 拜託！！今天禮拜五耶～你竟然浪費這麼美好的週末～～Orz			
08/20 10:56:50	NUSOFT_Rayearth : 不然要怎樣~~~~			
08/20 11:11:45	NUSOFT_Rayearth : 我這禮拜快累死了，3個廠商大搞烏龍，我快要氣炸了...>_<			
08/20 11:11:54	Ranma : 別氣～別氣～陪我出來看電影吧～消消氣～這禮拜上映的電影好像還不錯喔～			
08/20 11:12:06	NUSOFT_Rayearth : 哪部電影？？			
08/20 11:12:11	Ranma : 媽媽咪呀～			
08/20 11:12:20	NUSOFT_Rayearth : 這是啥？			
08/20 11:13:14	Ranma : 歌舞劇類型的電影			
08/20 11:13:19	Ranma : 聽說蠻好看，也蠻好笑的。笑笑剛好可以紓解壓力～^_~a			

圖 18 “網路記錄器”清楚記錄使用者的 Skype 文字聊天訊息