新軟系統
Internet Security Fighter

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 伺服器帳號做爲記錄資料的依據，來自同一登入帳號之記錄將會被判定爲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 位址爲記錄基準。
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 位址爲記錄基準。
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）*

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）*

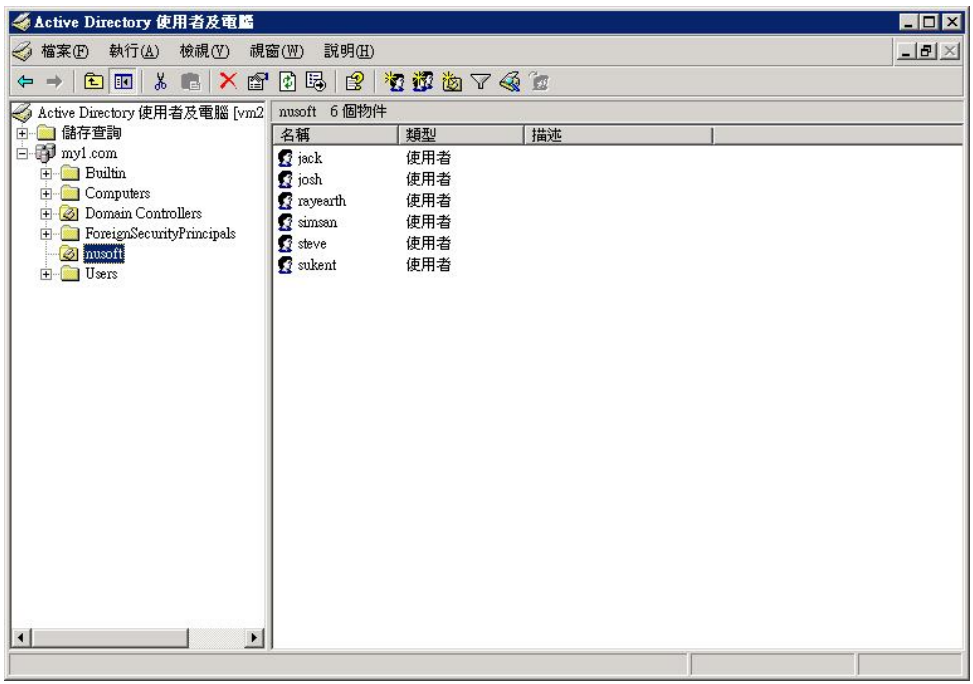

圖 2 AD 伺服器的指定識別名稱目錄

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 做爲使用者名稱。

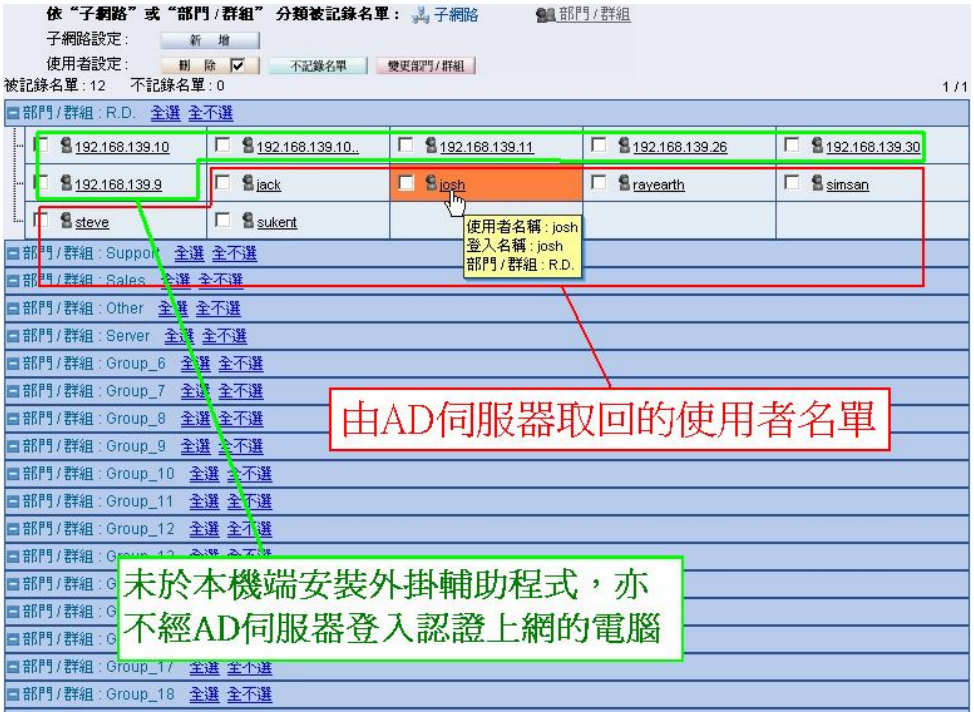

圖 3 結合 AD 伺服器登入名稱的使用者名單

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）*

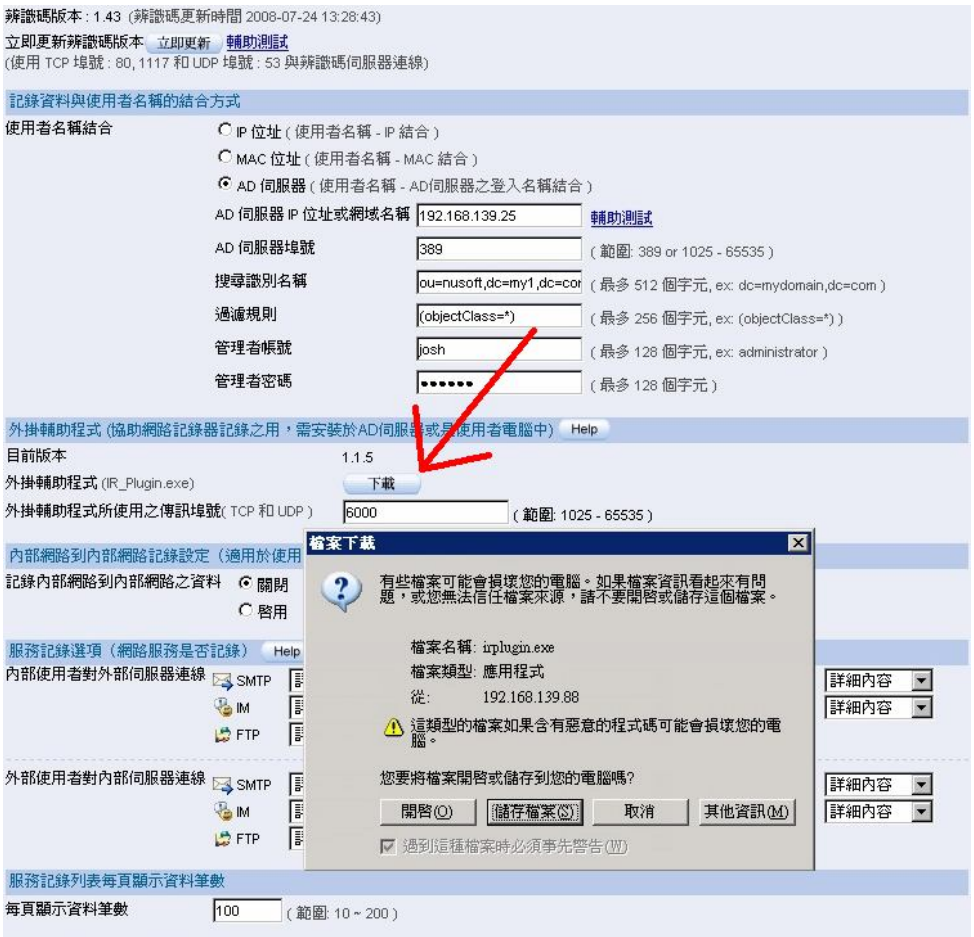

圖 4 於 AD 伺服器下載”網路記錄器”【外掛輔助程式】

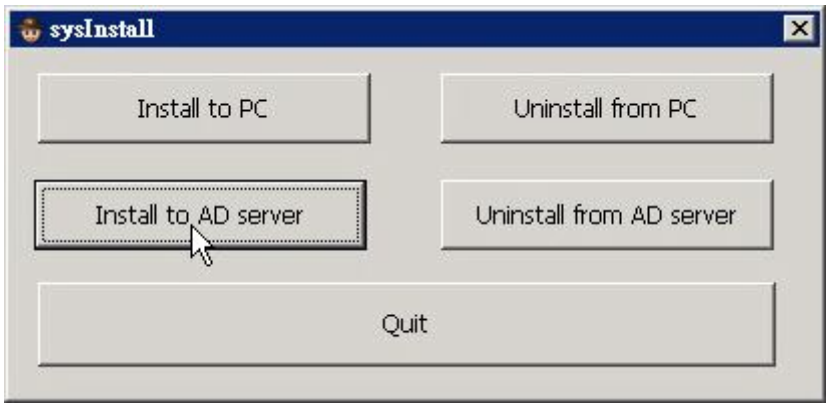

圖 5 於 AD 伺服器安裝”網路記錄器”【外掛輔助程式】

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】。

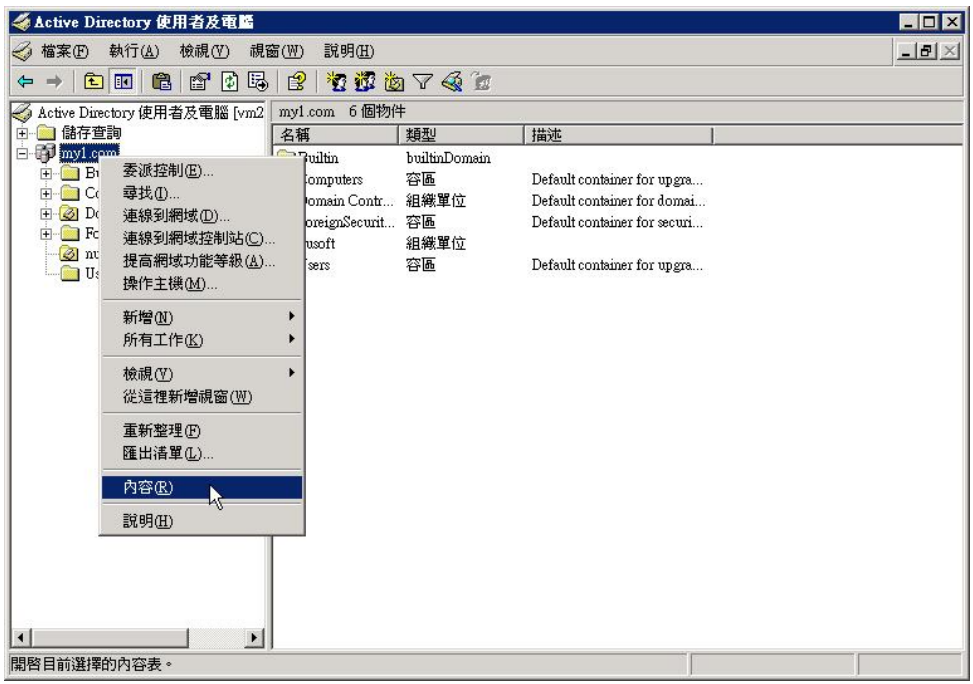

圖 6 Active Directory 使用者及電腦管理介面

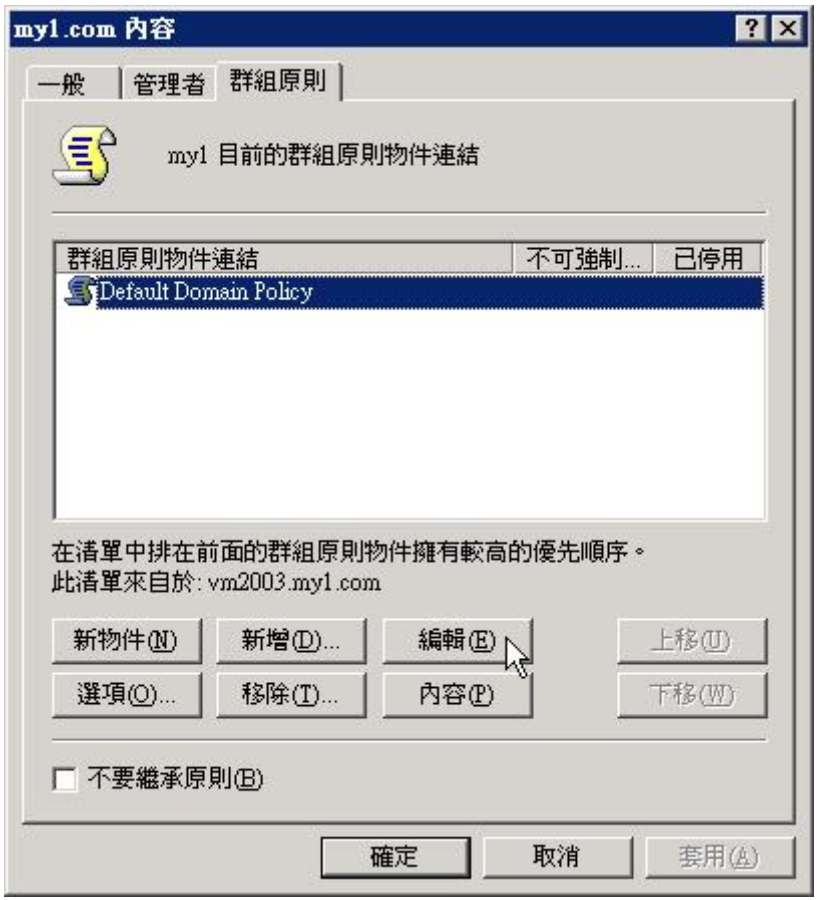
my1.com 內容
一般
管理者
群組原則
my1 目前的群組原則物件連結
群組原則物件連結
不可強制...
已停用
Default Domain Policy
在清單中排在前面的群組原則物件擁有較高的優先順序。
此清單來自於: vm2003.my1.com
新物件(N)
新增(D)...
編輯(E)
上移(U)
選項(O)...
移除(T)...
內容(P)
下移(W)
不要繼承原則(B)
確定
取消
套用(A)

圖 7 AD 網域內容視窗

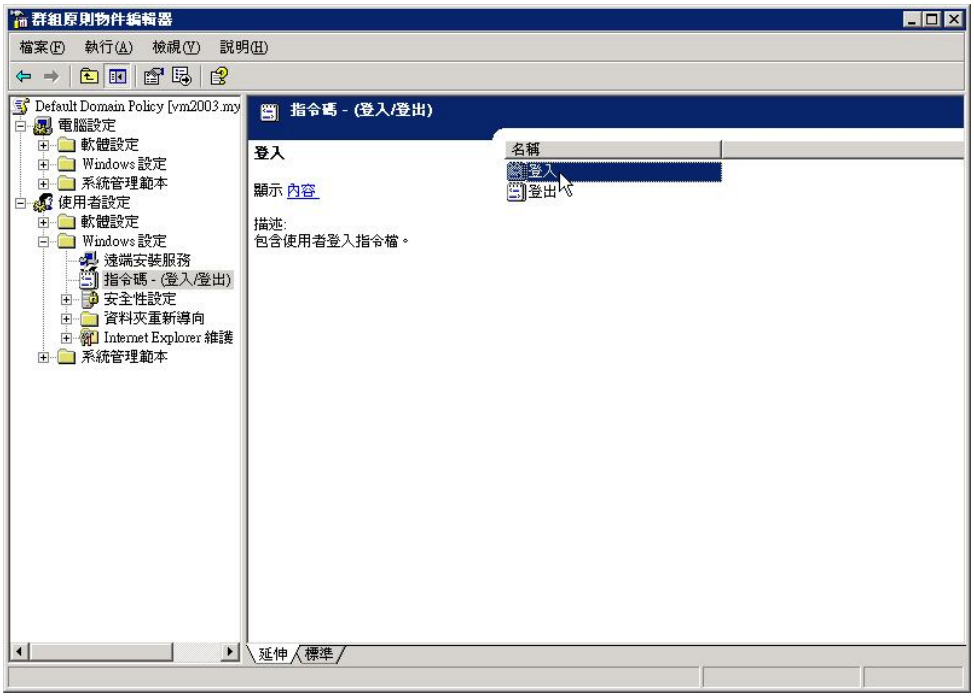

圖 8 群組原則物件編輯器

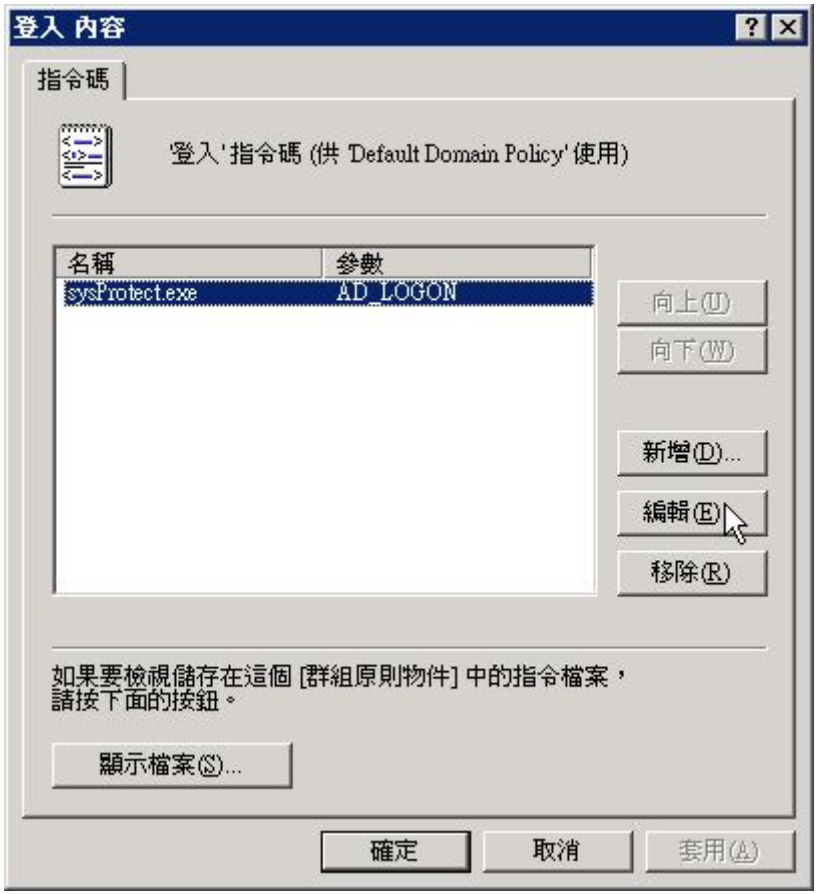

圖 9 登入內容視窗

圖 10 編輯登入指令碼

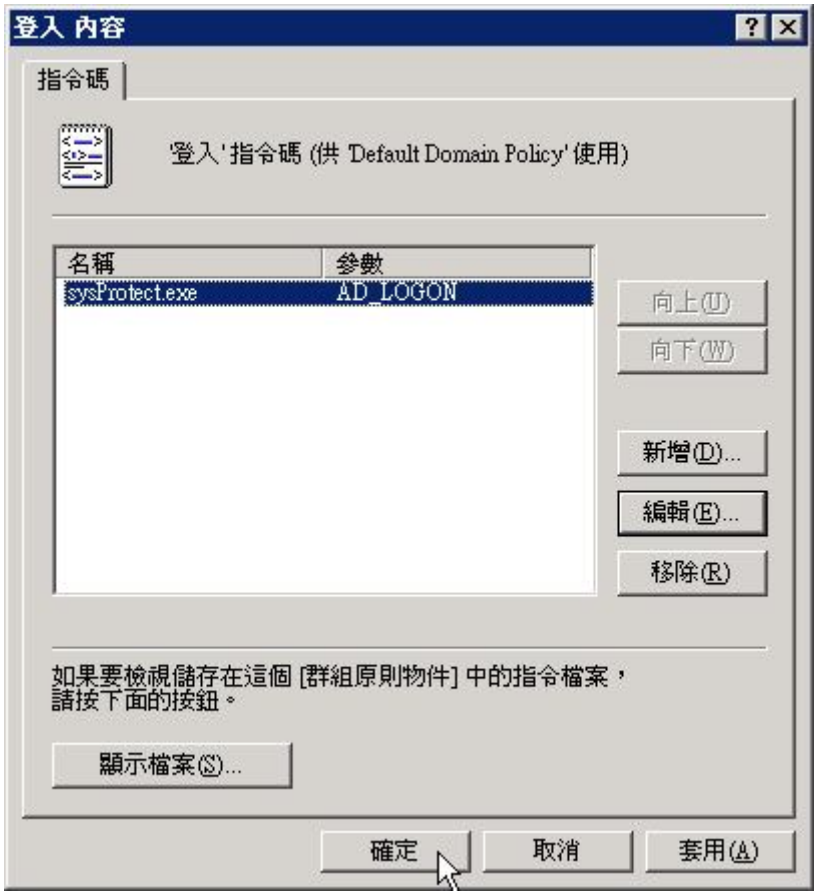

圖 11 完成登入指令碼編輯動作

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）*

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）*

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【行爲管理】>【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）

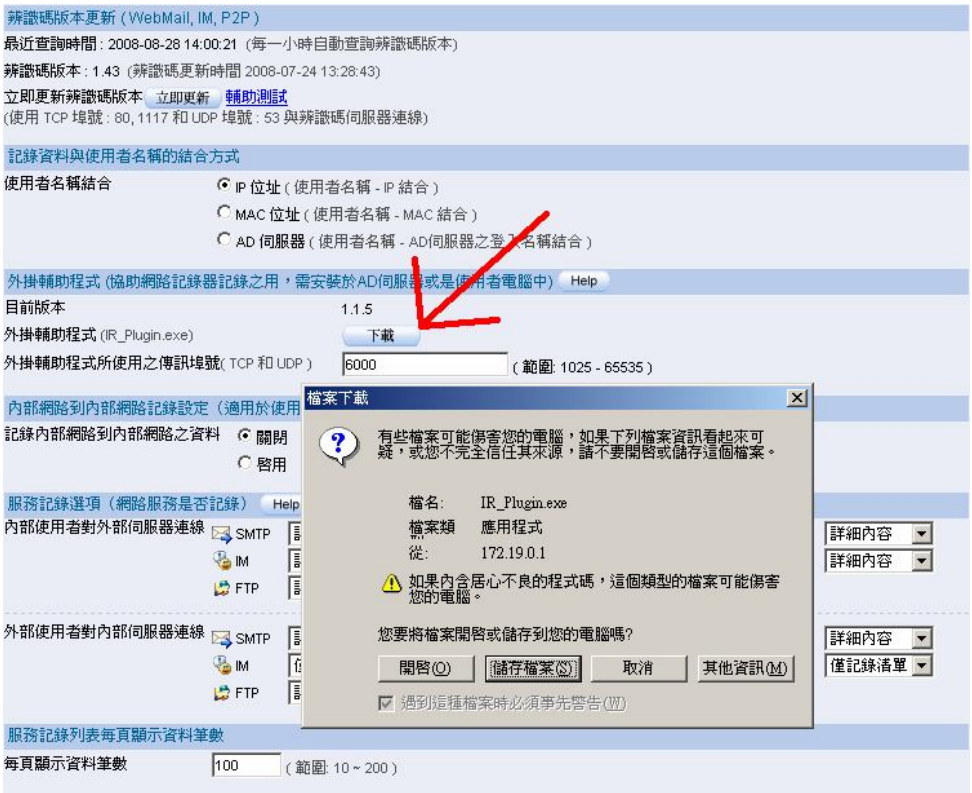

圖 16 從“網路記錄器”下載【外掛輔助程式】

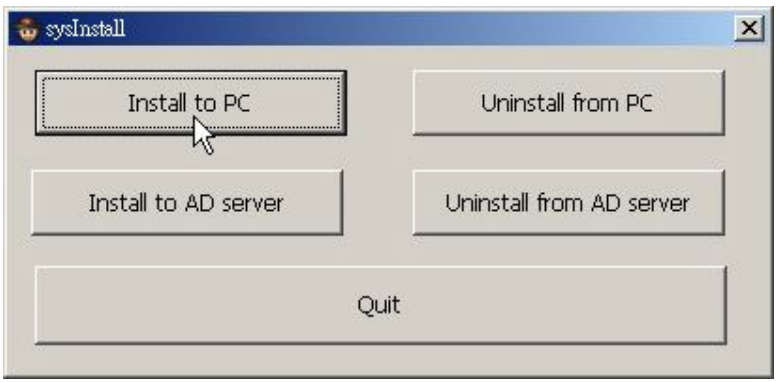

圖 17 於使用者本地端電腦安裝【外掛輔助程式】

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）*

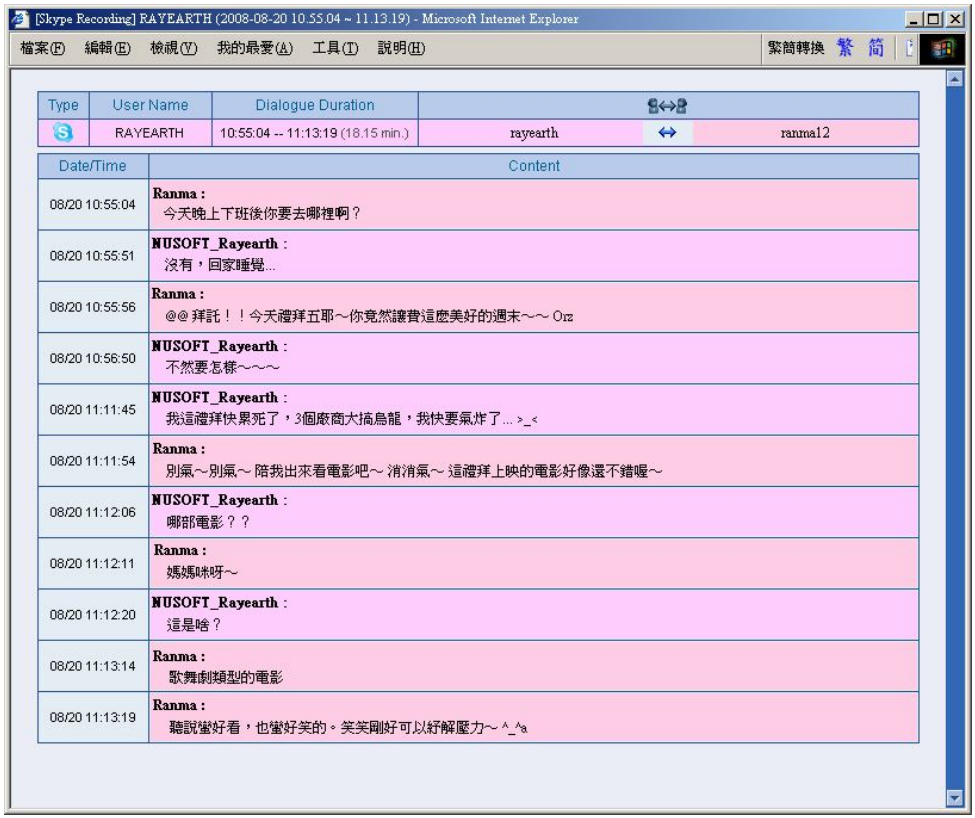

圖 18“網路記錄器”清楚記錄使用者的 Skype 文字聊天訊息