

網路記錄器 / IR 系列報導

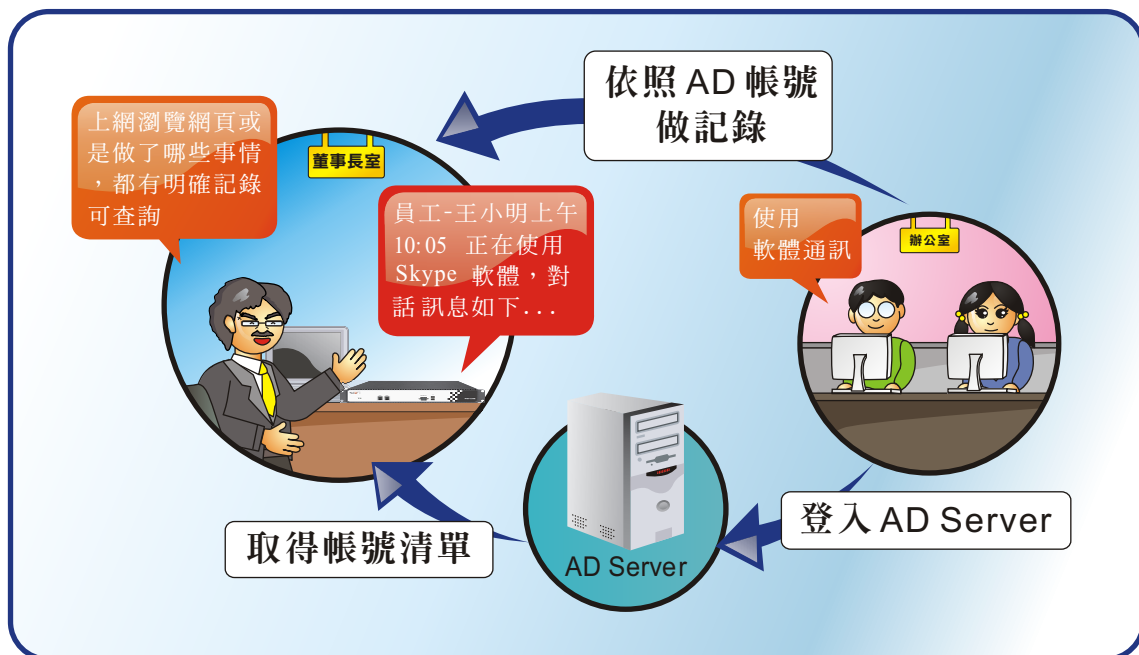
技術淺談與應用 - 產品新功能，記錄模式可結合 AD Server 登入帳號使用

甚麼是使用者名稱結合 AD 伺服器登入名稱

為了因應部份公司內部已架設 AD Server 的情況下，新軟系統近期於「網路記錄器 - IR」中，同時也新增了新的記錄模式功能，名稱為『AD 伺服器』，但此項新功能所指的並非是架設 AD Server，而是將公司原有的 AD Server 之登入名稱與系統作結合，換句話說就是可配合已架有 AD Server 的公司，利用 AD Server 登入的帳號(名稱)來進行記錄的功能，以方便公司內部資訊管理人員往後的記錄整合及歸檔。

能為公司帶來怎樣的好處

選取『AD 伺服器』功能後，『網路記錄器 - IR』的一切資料記錄則會根據員工電腦登入公司 AD Server 時，所使用的帳號(名稱)來做為記錄的依據，這樣的好處對於公司裡已架有 AD Server 的管理人員及上層主管而言，可以很清楚明確的從『網路記錄器 - IR』中查看到公司裡早已熟悉的帳號使用者做了哪些事，並且可以利用完整的記錄遏止員工摸魚、揪出濫用公司頻寬者，還給企業順暢無比的網路環境，以及迅速解決內部網路攻擊事件，快速找出中毒電腦，也可方便做更進一步的管理。



新功能示意圖：

日期時間	使用者名稱	網站
08/01 09:51	user	http://safebrowsing.clients.google.com/
08/01 09:22	user	http://www.paessler.com/

NO.	使用者名稱	KBytes	
1	user	105.69	99.44%
2	192.168.139.15	0.31	0.29%
3	192.168.139.16	0.29	0.27%

IR 記錄畫面截圖

如何使用

此項新功能選項位於產品系統中『記錄分析 > 設定 > 設定』裡的“使用者名稱結合模式設定”底下，如下圖：

使用者名稱的結合模式設定

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 - 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)

設定畫面截圖

關於安裝設定方面，資訊管理人員要如何才有辦法使用『網路記錄器 - IR』來與公司的 AD Server 作結合運用呢？為避免管理人員手忙腳亂，新軟系統為此而貼心的設計，當『網路記錄器 - IR』以使用者的“AD 伺服器之登入名稱”做為記錄資料的依據時，管理人員只需在公司所架的 AD Server 上或是於使用者電腦中使用『網路記錄器 - IR』所內附的『外掛輔助程式』來進行安裝即可輕鬆完成，而輔助程式的用處則在於協助網路記錄器記錄之用，以便網路記錄器取得使用者所登錄之名稱。



系統畫面截圖

文  陳殿鴻 kim@nusoft.com.tw

市場行銷報導 - 網路側錄的重要性

網際網路的使用越來越普遍，網路不但已成為企業內部的溝通橋梁，也是企業和外部進行各項業務往來的重要管道。相對的檔案資料的管理已不再僅限於各類紙張文檔，也必需包括各類來往的電子訊息及電子郵件。

電子郵件的傳輸速度快、有效率，在許多企業，已漸漸具備正式公文的性質，而對於網際網路的其他應用，如最基本的網頁瀏覽功能，msn、QQ等IM即時通訊工具，Google、百度…等搜索引擎，以及企業網站等等，也越來越成為企業必不可少的業務通道，但在如此方便的環境下，也可能被員工當作有意或無意洩漏機密的主要管道。

據調查，美國大約四分之三的大型企業，利用特殊軟體，檢查員工的電子郵件及即時通訊內容，防止洩漏公司機密。這些側錄的資料包括了使用的訊息類型，以及在網路上找到的訊息等，也都已變成調查犯罪的重要證據。

同樣的位於台灣近幾年也因為商業間諜而影響了不少企業，如幾年前，前股王威盛與網通大廠友訊的官司震驚社會，而最新知名個案就是鴻海旗下的富士康，指控對岸手機製造廠比亞迪竊取商業機密，2003年網路產品大廠友訊指控威盛涉及商業間諜行為…等多不勝數的個案，基於此原因，對企業電子郵件及零零種種的即時通訊工具進行側錄、備份已經是有相當必要。

新軟網路記錄器 - IR 是一個功能強大的網路側錄、管理工具，它能記錄企業內部員工的上網紀錄 - 所瀏覽的網頁、Web Mail所收發之信件、一般電子郵件、即時通訊、FTP及TELNET，不但可有效預防企業內部資料外洩，並可用來制止員工於上班時間利用企業之網路資源從事私人活動，及網路資源遭濫用，能夠有效的提昇工作效率。

網路記錄器 - IR 在安裝環境上，可採旁接（Sniffer）模式或橋接（Bridge）模式架設並支援Bypass功能，此兩種模式可讓管理者依現有的網路環境來規劃，網路記錄器 - IR 並且擁有強大的搜尋系統，不論是要搜尋某一位員工的上網記錄，或是某一項服務的使用者，再配合關鍵字搜尋系統，可迅速、輕易的找到所要的記錄，還提供中毒者警示功能，一發現異常流量，立即通知管理者及使用者，讓管理者即時瞭解網路異狀，馬上做出應變之道，對於大公司而言，系統也可各別建立群組管理員，配合企業化階層式群組管理，權限劃分，分層負責管理。並且還擁有其他多項功能，與目前其他市售的網路側錄設備相較之下，新軟網路記錄器 - IR 絕對是目前網路安全系統中不可或缺的管理利器，同時也是最佳的選擇。

如需瞭解更詳細的產品資訊，歡迎至 <http://www.nusoft.com.tw>

文  陳殿鴻 kim@nusoft.com.tw