新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2010/3/15- 2010/3/28 第113期

## 網路記錄器 / IR 系列報導

# 技術淺談與應用 - 即時通訊『QQ』預設規則的兩種設定方式

網路即時通訊軟體的方便為公司帶來了更多的商機與利益，同時卻也是員工利用來處理私人事情、打混摸魚的主要管道之一，不但嚴重影響到上班風氣，也因利用即時通訊軟體來互傳檔案而佔據公司頻寬，甚至不少公司也因員工濫用即時通訊軟體而導致內部機密外流的情況發生。因此公司對於內部即時通訊的管制也漸漸重視，而導入相關的資訊安全設備也成為了一項不可或缺的重要步驟之一。

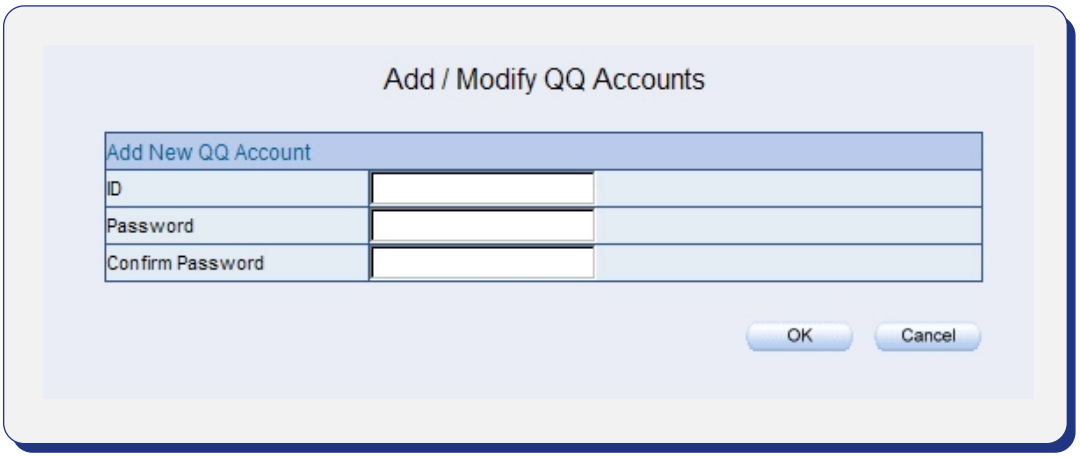
對於目前大家最耳熟能詳的即時通訊軟體，除了 MSN、YAHOO、SKYPE 之外，QQ 也同樣是使用者最常使用的一項即時通訊軟體之一。新軟系統『網路記錄器 - IR』不僅能有效管制多數即時通訊軟體，對於即時通訊的管制項目也細分的很清楚。管理人員於設定管制時則必需瞭解到每一項規則的使用方式，由於 MSN、YAHOO、SKYPE…等通訊軟體的預設規則較為容易上手，所需執行的步驟比較簡單，所以對於管理人員而言也容易上手不成問題，而即時通訊軟體 QQ 於預設規則的設定上，所需設定的步驟較其他即時通訊軟體多，於這方面管理人員則需要格外注意。

至於為何 QQ 是需要多一項設定步驟呢？因為 QQ 採用加密方式傳送訊息，所以『網路記錄器 - IR』必須先透過驗證機制並取得正確的 QQ 帳號與密碼，才可將訊息解密並加以記錄。所以，當管理人員將『網路記錄器 - IR』的 QQ 預設規則 ( Behavior Management > IM Management > Default Rules) 勾選為【Accept：Everyone / Drop：None 】或【 Accept：Authenticated user / Drop：Unauthenticated user】，並在『網路記錄器 - IR』使用未知的 QQ 帳號和密碼時，於網路記錄器中只會有其使用報表，但無法記錄相互傳遞的訊息內容。

而針對需先通過驗證才可正常連入 QQ 的預設規則可分為『允許有效密碼』、『允許認證且有效密碼』兩種，以下將分別說明兩種預設規則的詳細設定方式。

情況一：因應公司內部政策，只讓員工使用有經公司核准允許的 QQ 帳號密碼來登入。管理人員於『網路記錄器 - IR』操作介面 "Behavior Management > IM Management > Default Rules" 下，若管理人員將 QQ 這部份的預設規則設定為『Accept：Valid password / Drop：Invalid password』時，如欲使用即時通訊軟體 QQ，則管理人員或使用者必須先於【新增 QQ 帳號】介面（"http:// IR 介面位址 /qq"，例如：http://192.168.1.1/qq）輸入正確的 QQ 帳號與密碼，才可正常使用即時通訊軟體 QQ，並進行記錄。


將預設規則設定為『Accept：Valid password / Drop：Invalid password』

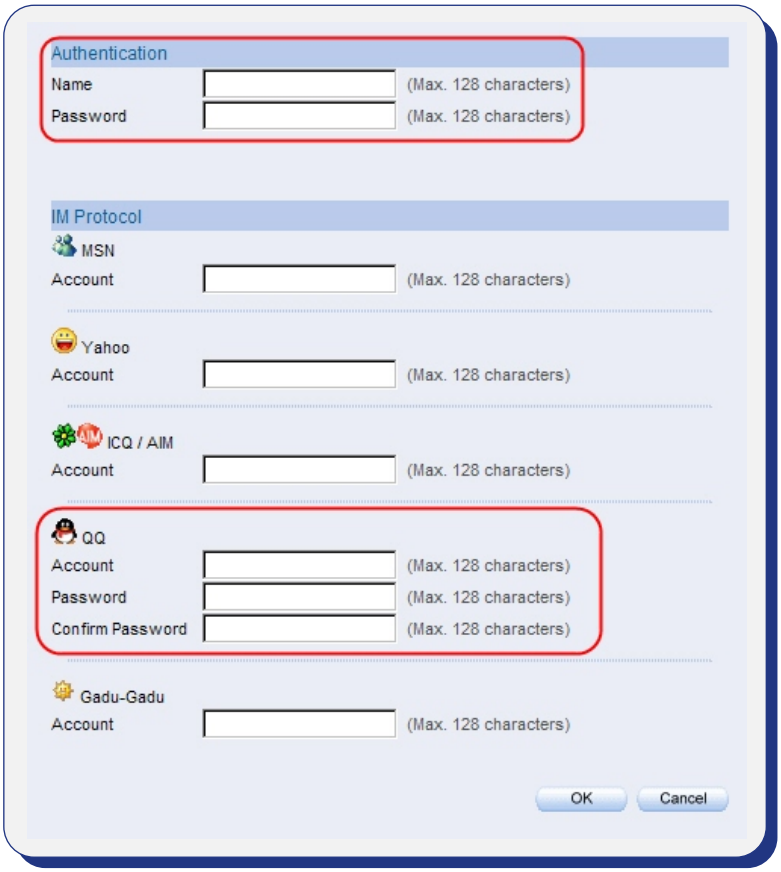



於『http://IR 介面位址 /qq』下輸入欲進行驗証的帳號密碼

情況二：因應公司內部政策，只提供有經過認證的使用者來使用公司所核准的 QQ 帳號密碼。

管理人員於『網路記錄器- IR』操作介面 "Behavior Management > IM Management > Default Rules" 下，若管理人員將 QQ 這部份的預設規則設定為『Accept：Authenticated user with valid password / Drop：Unauthenticated user or invalid password』時，如欲使用即時通訊軟體 QQ，則管理人員或使用者必須先於【認證、新增 QQ 帳號】介面（ "http:// IR 介面位址/auth"，例如：http://192.168.1.1/auth）輸入正確的認證資訊與 QQ 帳號、密碼，才可正常使用即時通訊軟體 QQ，並進行記錄。


將預設規則設定為『Accept：Authenticated user with valid password / Drop：Unauthenticated user or invalid password』




於『http://IR 介面位址 /auth』下輸入認證的使用帳號密碼及欲進行驗証的 QQ 帳號密碼

文 陳殿鴻 kim@nusoft.com.tw

# 市場行銷報導 - 新軟網路記錄器提供企業「事前管制」及「事後記錄」雙保護方案

自 ADSL 網路服務平民化以後，網路發展迅速進步，上網行為逐漸普遍蔚為風行，其後勢也帶動社會、經濟全方面的 e 化整合。然而網路普及化後所帶來的龐大商業利益等等，雖屬正面效益；可是過於快速發展普及之網路科技所帶來的後遺症，卻常常令使用者愉快地使用網路之餘，卻遺忘其背後隱藏的可怕之處。

現在使用者在上網時經常忽略了最基本的“網路危機意識問題”—「太輕忽網路上所有可能存在的網路陷阱」。許多使用者經常在自己認為“沒問題！很安全！”的情況下，肆無忌憚任意使用網路應用軟體；殊不知，這些看起來似乎無危險性且使用方便的網路應用軟體，其實才是真正資安漏洞來源，如此毫無危機意識的使用方式已經為他自己帶來無法想像的資安危機。日前，據報導指出有政府公家機關單位員工無視單位政令宣導，私自於其公務電腦上使用知名 P2P 分享軟體「Foxy」下載影音檔案，卻導致該單位許多機密資料讓有心人士經由 Foxy 軟體上搜尋取得，因而導致該單位發生機密外洩事件，造成無法想像的龐大損失。

如此問題更顯現出「現在使用者的硬體使用環境雖然獲得相當大的品質提升，但對於資安危機意識之認知上的確尚待不足」。因此許多企業為了避免自家公司也發生類似的機密外洩事件，所以紛紛採購相關可做“事前管理的網路管理設備”或可做“事後舉證的網路行為側錄設備”，想藉此妥善保護企業資訊安全。然而，一間資安防護機制健全之企業所必備的，並非單只擁有「事前管制」或者「事後記錄」其中之一，而是須同時並存，但是現在許多企業的資安防護重點僅著墨於“由外而來的網路攻擊”，所以一般企業所使用防火牆之類的資安防護產品，但是若要做到「事後記錄」的機制，一般企業所使用的防火牆設備是完全無法滿足的。有鑑於此，新軟系統網路記錄器的產品設計概念皆立於「補足企業防火牆不足之處」上，提供規劃給用戶加強企業防火牆不足之處的「事前管制」以及「事後記錄」等兩項重點使用方向：

- 事前管制

  預防資訊安全危機發生的最佳方法就是妥善做好「事前預防」之機制，為了避免企業公司內發生不必要的資安危機事件，可管制員工使用業務上不必要的網路軟體，因此新軟網路記錄器提供多款網路上常用 "應用程式" 及 "IM 即時通訊軟體" 之相對應管制機制予用戶，讓管理人員可依公司政策自行訂定相關使用規則，可使員工無法於公司內使用其他非公務使用的程式，藉此提高企業資安防護的安全性。

  **目前提供的《應用程式管制機制》有：**

  P2P 分享軟體、影音串流軟體、線上遊戲、VPN 通道軟體、遠端電腦控制軟體

  **目前提供的《IM 即時通訊程式機制》有：**

  MSN、Yahoo 即時通、Skype、QQ、GoogleTalk、ICQ、AIM、Gadu-Gadu

- 事後記錄

  企業除了做好最基本的「事前預防」機制以外，最基本的就是「事後記錄」功能了。若因應業務需求，必須開放公司員工自由使用其他網路服務的話，新軟系統網路記錄器也提供其他常用的網路服務記錄機制予用戶自行設定使用，可讓員工在不影響業務運作的情況下使用其他網路服務，但是所有的使用情況，將會在新軟系統網路記錄器底下一五一十的完整呈現。倘若有發生內部不肖員工使用其他服務洩漏公司商業機密的話，就可以依據平時所記錄的完整資料做為事後法律告訴時的舉證依據。

  **目前提供的其他常用的網路服務記錄機制：**

  SMTP、POP3/IMAP、HTTP/HTTPS、WebMail、FTP、Telnet、IM 即時通訊、WebSMTP、WebPOP3

新軟網路記錄器所提供給用戶的「事前管制」及「事後記錄」的重點使用方向，皆可有效提高企業資安防護的安全性，藉此更有效的協助企業運作順暢、提升公司營運績效。

| | 事前管制 | 事後記錄 |
|---|---|---|
| 方案目標 | 為了避免企業內發生資安危機事件，新軟網路記錄器提供多款網路上常用 "應用程式" 及 "IM 即時通訊軟體" 相對應之管制機制予用戶，讓管理人員可依公司政策自行訂定相關管制規則，藉此提高企業資安防護的安全性。 | 若因應業務需求，必須開放公司員工使用其他網路服務的話，新軟網路記錄器提供其他網路服務記錄機制予用戶，可讓員工使用其他網路服務，但是所有的使用情況將會完整記錄。倘若日後有發生洩密事件的話，可依據完整的資料記錄做為事後法律的舉證。 |
| 方案機制 | 提供《應用程式管制機制》：<br>P2P 分享軟體、影音串流軟體、<br>線上遊戲、VPN 通道軟體、<br>遠端電腦控制軟體<br>提供《IM 即時通訊程式機制》：<br>MSN、Skype、QQ、<br>Yahoo 即時通、Google Talk、<br>ICQ/AIM、Gadu - Gadu | 提供《其他常用的網路服務》記錄機制：<br>SMTP、POP3/IMAP、<br>HTTP/HTTPS、WebMail、<br>FTP、Telnet、WebPOP3、<br>WebSMTP、IM 即時通訊 |

文 黃政銘 ming@nusoft.com.tw