新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2010/3/15- 2010/3/28 第113期

## 网络记录器 / IR系列报导

# 技术浅谈与应用 - 实时通讯『QQ』预设规则的两种设定方式

网络实时通讯软件的方便为公司带来了更多的商机与利益，同时却也是员工利用来处理私人事情、打混摸鱼的主要管道之一，不但严重影响到上班风气，也因利用实时通讯软件来互传文件而占据公司带宽，甚至不少公司也因员工滥用实时通讯软件而导致内部机密外流的情况发生。因此公司对于内部实时通讯的管制也渐渐重视，而导入相关的信息安全设备也成为了一项不可或缺的重要步骤之一。

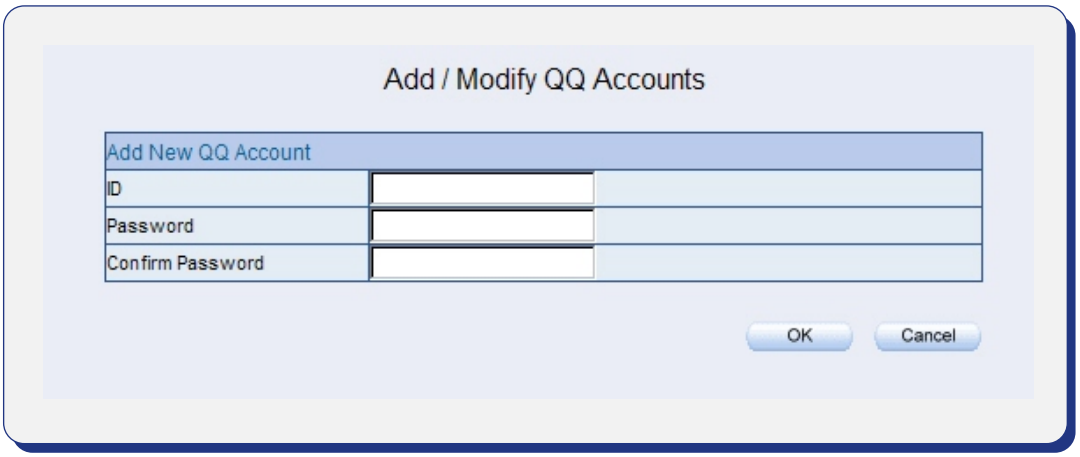
对于目前大家最耳熟能详的实时通讯软件，除了 MSN、YAHOO、SKYPE 之外，QQ 也同样是使用者最常使用的一项实时通讯软件之一。新软系统『网络记录器-IR』不仅能有效管制多数实时通讯软件，对于实时通讯的管制项目也细分的很清楚。管理人员于设定管制时则必需了解到每一项规则的使用方式，由于 MSN、YAHOO、SKYPE…等通讯软件的预设规则较为容易上手，所需执行的步骤比较简单，所以对于管理人员而言也容易上手不成问题，而实时通讯软件 QQ 于预设规则的设定上，所需设定的步骤较其它实时通讯软件多，于这方面管理人员则需要格外注意。

至于为何 QQ 是需要多一项设定步骤呢？因为 QQ 采用加密方式传送讯息所以『网络记录器 - IR』必须先透过验证机制并取得正确的 QQ 账号与密码，才可将讯息解密并加以记錄。所以，当管理人员将『网络记录器 - IR』的 QQ 预设规则( Behavior Management > IM Management > Default Rules) 勾选为【Accept : Everyone / Drop : None 】或【 Accept : Authenticated user / Drop : Unauthenticated user】，并在『网络记录器 - IR』使用未知的 QQ 账号和密码时，于网络记录器中只会有其使用报表，但无法记錄相互传递的讯息内容。

而针对需先通过验证才可正常连入 QQ 的预设规则可分为『允许有效密码』、『允许认证且有效密码』两种，以下将分别说明两种预设规则的详细设定方式。

情况一：因应公司内部政策，只让员工使用有经公司核准允许的 QQ 账号密码来登入。管理人员于『网络记录器 - IR』操作接口 "Behavior Management > IM Management > Default Rules" 下，若管理人员将 QQ 这部份的预设规则设定为『Accept : Valid password / Drop : Invalid password』时，如欲使用实时通讯软件 QQ，则管理人员或使用者必须先于【新增 QQ 账号】接口（"http:// IR 接口地址 /qq"，例如：http://192.168.1.1/qq）输入正确的 QQ 账号与密码，才可正常使用实时通讯软件 QQ，并进行记录。


将预设规则设定为『Accept：Valid password / Drop：Invalid password』

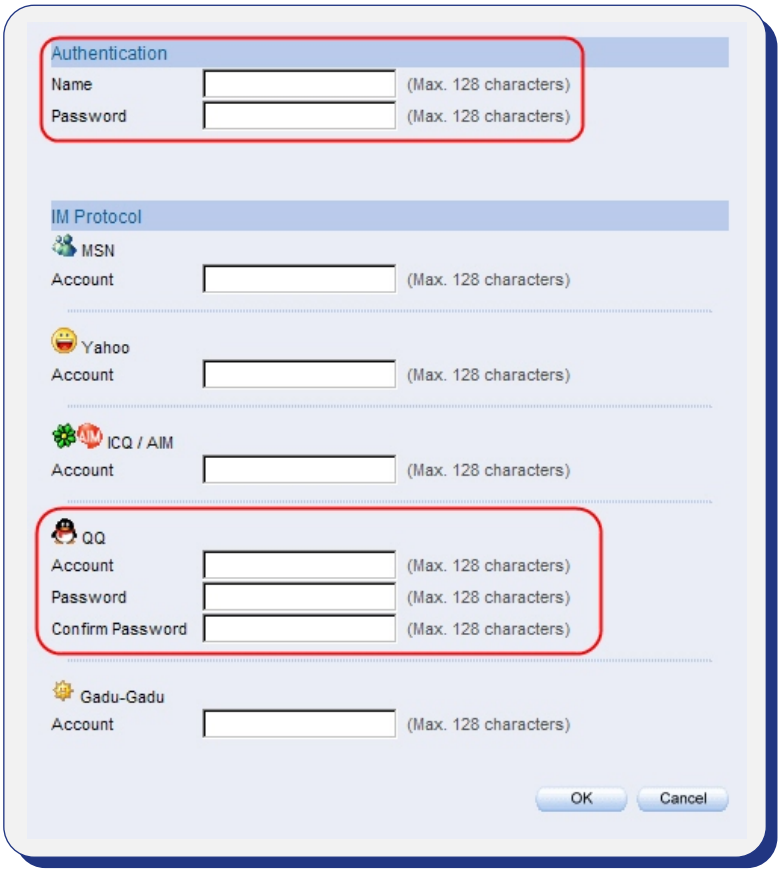



于『http://IR 接口地址 /qq』下输入欲进行验证的帐号密码

情况二：因应公司内部政策，只提供有经过认证的使用者来使用公司所核准的 QQ 账号密码。

管理人员于『网络记录器 - IR』操作接口 "Behavior Management > IM Management > Default Rules" 下，若管理人员将 QQ 这部份的预设规则设定为『Accept：Authenticated user with valid password / Drop：Unauthenticated user or invalid password』时，如欲使用实时通讯软件 QQ，则管理人员或使用者必须先于【认证、新增 QQ 账号】界面（"http:// IR 接口地址/auth"，例如：http://192.168.1.1/auth）输入正确的认证信息与 QQ 账号、密码，才可正常使用实时通讯软件 QQ，并进行记录。


将预设规则设定为『Accept：Authenticated user with valid password / Drop：Unauthenticated user or invalid password』




于『http://IR 接口地址 /auth』下输入认证的使用帐号密码及欲进行验证的 QQ 帐号密码

文 陈殿鸿 kim@nusoft.com.tw

## 市场营销报导 - 新软网络记录器提供企业「事前管制」及「事後记录」双保护方案

自 ADSL 网络服务平民化以后，网络发展迅速进步，上网行为逐渐普遍蔚为风行，其后势也带动社会、经济全方面的 e 化整合。然而网络普及化后所带来的庞大商业利益等等，虽属正面效益；可是过于快速发展普及之网络科技所带来的后遗症，却常常令使用者愉快地使用网络之余，却遗忘其背后隐藏的可怕之处。

现在使用者在上网时经常忽略了最基本的"网络危机意识问题"—『太轻忽网络上所有可能存在的网络陷阱』。许多使用者经常在自己认为"没问题！很安全！"的情况下，肆无忌惮任意使用网络应用软件；殊不知，这些看起来似乎无危险性且使用方便的网络应用软件，其实才是真正资安漏洞来源，如此毫无危机意识的使用方式已经为他自己带来无法想象的资安危机。日前，据报导指出有政府公家机关单位员工无视单位政令倡导，私自于其公务计算机上使用知名 P2P 分享软件『Foxy』下载影音文件，却导致该单位许多机密数据让有心人士经由 Foxy 软件上搜寻取得，因而导致该单位发生机密外泄事件，造成无法想象的庞大损失。

如此问题更显现出『现在使用者的硬件使用环境虽然获得相当大的质量提升，但对于资安危机意识之认知上的确尚待不足』。因此许多企业为了避免自家公司也发生类似的机密外泄事件，所以纷纷采购相关可做"事前管理的网络管理设备"或可做"事后举证的网络行为侧录设备"，想藉此妥善保护企业信息安全。然而，一间资安防护机制健全之企业所必备的，并非单只拥有『事前管制』或者『事后记录』其中之一，而是须同时并存，但是现在许多企业的资安防护重点仅着墨于"由外而来的网络攻击"，所以一般企业所使用防火墙之类的资安防护产品，但是若要做到『事后记录』的机制，一般企业所使用的防火墙设备是完全无法满足的。有鉴于此，新软系统网络记录器的产品设计概念皆立于『补足企业防火墙不足之处』上，提供规划给用户加强企业防火墙不足之处的『事前管制』以及『事后记录』等两项重点使用方向：

- 事前管制

  预防信息安全危机发生的最佳方法就是妥善做好『事前预防』之机制，为了避免企业公司内发生不必要的资安危机事件，可管制员工使用业务上不必要的网络软件，因此新软网络记录器提供多款网络上常用"应用程序"及"IM 实时通讯软件"之相对应管制机制予用户，让管理人员可依公司政策自行订定相关使用规则，可使员工无法于公司内使用其它非公务使用的程序，藉此提高企业资安防护的安全性。

  **目前提供的《应用程序管制机制》有：**

  P2P 分享软件、影音串流软件、在线游戏、VPN 信道软件、远程计算机控制软件

  **目前提供的《IM 实时通讯程式机制》有：**

  MSN、Yahoo 實时通、Skype、QQ、GoogleTalk、ICQ、AIM、Gadu-Gadu

- 事后记录

企业除了做好最基本的『事前预防』机制以外，最基本的就是『事后记录』功能了。若因应业务需求，必须开放公司员工自由使用其它网络服务的话，新软系统网络记录器也提供其它常用的网络服务记录机制予用户自行设定使用，可让员工在不影响业务运作的情况下使用其它网络服务，但是所有的使用情况，将会在新软系统网络记录器底下一五一十的完整呈现。倘若有发生内部不肖员工使用其它服务泄漏公司商业机密的话，就可以依据平时所记录的完整数据做为事后法律告诉时的举证依据。

**目前提供的其他常用的网络服务记录机制：**

SMTP、POP3/IMAP、HTTP/HTTPS、WebMail、FTP、Telnet、IM 实时通讯、WebSMTP、WebPOP3

新软网络记录器所提供给用户的『事前管制』及『事后记录』的重点使用方向，皆可有效提高企业资安防护的安全性，藉此更有效的协助企业运作顺畅、提升公司营运绩效。

| | 事前管制 | 事後记录 |
|---|---|---|
| 方案目标 | 为了避免企业内发生资安危机事件，新软网络记录器提供多款网络上常用 "应用程序" 及 "IM 实时通讯软件" 相对应之管制机制予用户，让管理人员可依公司政策自行订定相关管制规则，藉此提高企业资安防护的安全性。 | 若因应业务需求，必须开放公司员工使用其他网络服务的话，新软网络记录器提供其他网络服务记录机制予用户，可让员工使用其他网络服务，但是所有的使用情况将会完整记录。倘若日後有发生泄密事件的话，可依据完整的数据记录做为事後法律的举证。 |
| 方案机制 | 提供《应用程式管制机制》：<br>P2P 分享软件、影音串流软件、<br>在线游戏、VPN 信道软件、<br>远程计算机控制软件<br>提供《IM 即时通讯程式机制》：<br>MSN、Skype、QQ、<br>Yahoo 实时通、Google Talk、<br>ICQ/AIM、Gadu - Gadu | 提供《其他常用的网络服务》记录机制：<br>SMTP、POP3/IMAP、<br>HTTP/HTTPS、WebMail、<br>FTP、Telnet、WebPOP3、<br>WebSMTP、IM 实时通讯 |

文 黄政铭 ming@nusoft.com.tw