

## 网络记录器 / IR 系列报导

### 技术浅谈与应用 - 产品新功能，记录模式可结合 AD Server 登入帐号使用

甚么是使用者名称结合 AD 服务器登入名称

为了因应部份公司内部已架设 AD Server 的情况下，新软系统近期于「网络记录器 - IR」中，同时也新增了新的记录模式功能，名称为『AD 服务器』，但此项新功能所指的并非是架设 AD Server，而是将公司原有的 AD Server 之登入名称与系统作结合，换句话说就是可配合已架有 AD Server 的公司，利用 AD Server 登入的账号(名称)来进行记录的功能，以方便公司内部信息管理人员往后的记录整合及归档。

能为公司带来怎样的好处

选取『AD 服务器』功能后，『网络记录器 - IR』的一切数据记录则会根据员工计算机登入公司 AD Server 时，所使用的账号(名称)来做为记录的依据，这样的好处对于公司里已架有 AD Server 的管理人员及上层主管而言，以很清楚明确的从『网络记录器 - IR』中查看到公司里早已熟悉的账号使用者做了哪些事，并且可以利用完整的记录遏止员工摸鱼、揪出滥用公司带宽者，还给企业顺畅无比的网络环境，以及迅速解决内部网络攻击事件，快速找出中毒计算机，也可方便做更进一步的管理。



新功能示意图：

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/

使用者 8-Recorded Service 其他

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 记录画面截图

## 如何使用

此项新功能选项位于产品系统中『记录分析 > 设定 > 设定』里的“使用者名称结合模式设定”底下，如下图：

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)

设定画面截图

关于安装设定方面，信息管理人员要如何才有办法使用『网络记录器 - IR』来与公司的 AD Server 作结合运用呢？为避免管理人员手忙脚乱，新软系统为此而贴心的设计，当『网络记录器 - IR』以使用者的“AD 服务器之登入名称”做为记录数据的依据时，管理人员只需在公司所架的 AD Server 上或是于使用者计算机中使用『网络记录器 - IR』所内附的『外挂辅助程序』来进行安装即可轻松完成，而辅助程序的用处则在于协助网络记录器记录之用，以便网络记录器取得使用者所登录之名称。



系统画面截图

文  陈殿鸿 kim@nusoft.com.tw

## 市场营销报导 - 网络侧录的重要性

因特网的使用越来越普遍，网络不但已成为企业内部的沟通桥梁，也是企业和外部进行各项业务往来的重要管道。相对的文件数据的管理已不再仅限于各类纸张文档，也必需包括各类来往的电子讯息及电子邮件。

电子邮件的传输速度快、有效率，在许多企业，已渐渐具备正式公文的性质，而对于因特网的其它应用，如最基本的网页浏览功能，msn、QQ等IM实时通讯工具，Google、百度…等搜索引擎，以及企业网站等等，也越来越成为企业必不可少的业务通道，但在如此方便的环境下，也可能被员工当作有意或无意泄漏机密的主要管道。

据调查，美国大约四分之三的大型企业，利用特殊软件，检查员工的电子邮件及实时通讯内容，防止泄漏公司机密。这些侧录的数据包括了使用的讯息类型，以及在网络上找到的讯息等，也都已变成调查犯罪的重要证据。

同样的位于台湾近几年也因为商业间谍而影响了不少企业，如几年前，前股王威盛与网通大厂友讯的官司震惊社会，而最新知名个案就是鸿海旗下的富士康，指控对岸手机制造厂比亚迪窃取商业机密，2003年网络产品大厂友讯指控威盛涉及商业间谍行为…等多不胜数的个案，基于此原因，对企业电子邮件及零零种种的实时通讯工具进行侧录、备份已经是有相当必要。

新软网络记录器 - IR 是一个功能强大的网络侧录、管理工具，它能记录企业内部员工的上网纪录 - 所浏览的网页、Web Mail所收发之信件、一般电子邮件、实时通讯、FTP及TELNET，不但可有效预防企业内部数据外泄，并可用来制止员工于上班时间利用企业之网络资源从事私人活动，及网络资源遭滥用，能够有效的提升工作效率。

网络记录器 - IR 在安装环境上，可采旁接 ( Sniffer ) 模式或桥接 ( Bridge ) 模式架设并支持 Bypass 功能，此两种模式可让管理者依现有的网络环境来规划，网络记录器 - IR 并且拥有强大的搜寻系统，不论是要搜寻某一位员工的上网记录，或是某一项服务的使用者，再配合关键词搜寻系统，可迅速、轻易的找到所要的记录，还提供中毒者警示功能，一发现异常流量，立即通知管理者及使用者，让管理者实时了解网络异状，马上做出应变之道，对于大公司而言，系统也可各别建立群组管理员，配合企业化阶层式群组管理，权限划分，分层负责管理。并且还拥有其它多项功能，与目前其它市售的网络侧录设备相较之下，新软网络记录器 - IR 绝对是目前网络安全系统中不可或缺的管理利器，同时也是最佳的选择。

如需了解更详细的产品信息，欢迎至 <http://www.nusoft.com.tw>

文  陈殿鸿 kim@nusoft.com.tw

