InstantScan
快速安装指南

利基网络股份有限公司
Secure Networks at Layer-7

Version: 2.0

目　录

第1章
开始安装前的说明

InstantScan为一随插即用的内容管理设备，您不需更改既有的网络架构，即可使用此设备。InstantScan 管理系统与报表系统结合管理服务器，提供您简而易用的使用者网页接口。网管人员可根据公司内部的网络架构来设定管理政策规则，而管理服务器可同时控管多台 InstantScan 设备与分析来自所控管的 InstantScan 设备之事件记录。本手册仅介绍基础的 InstantScan 设定，包括管理服务器参数设定、软件安装，与 InstantScan 管理系统基本设定等。如您需要更详尽的政策规则设定，请参阅 InstantScan 使用手册。

1.1 产品包装检查

编号	项目	数量	备注
1.	InstantScan设备	1 台	
2.	L型固定铁片	2 片	
3.	螺丝组	6 个	IS-5000有10个
4.	网络线 (RJ-45)	1 条	
5.	电源线	1 条	IS-5000有2条
6.	RS-232 console线	1 条	
7.	CD	1 片	
8.	拉轴杆	2 条	只适用IS-5000

第2章
InstantScan 之硬件安装

2.1 硬件安装

InstantScan设备可以固定在标准19吋机架上，亦可以独立放置于桌面上。请利用包装盒内附的螺丝组将 L 型固定铁片锁于 InstantScan 上，然后将 InstantScan 安装于机架上。

请依以下核对清单检查您的网络联机是否已经备妥：

- ☐ **InstantScan设备**
- ☐ **网络设备** – 如路由器、交换器、集线器（Hub）等。
  如果您将 InstantScan 连结到上述网络设备，请使用串线（through）相连。
- ☐ **客户端设备 (CPE)** – 如路由器、桌上型PC、或笔记型计算机等。
  如果您将InstantScan连结到上述客户端设备，请使用跳线（cross-over）相连。
- ☐ **将InstantScan RJ-45端口连结相对应之网络线**

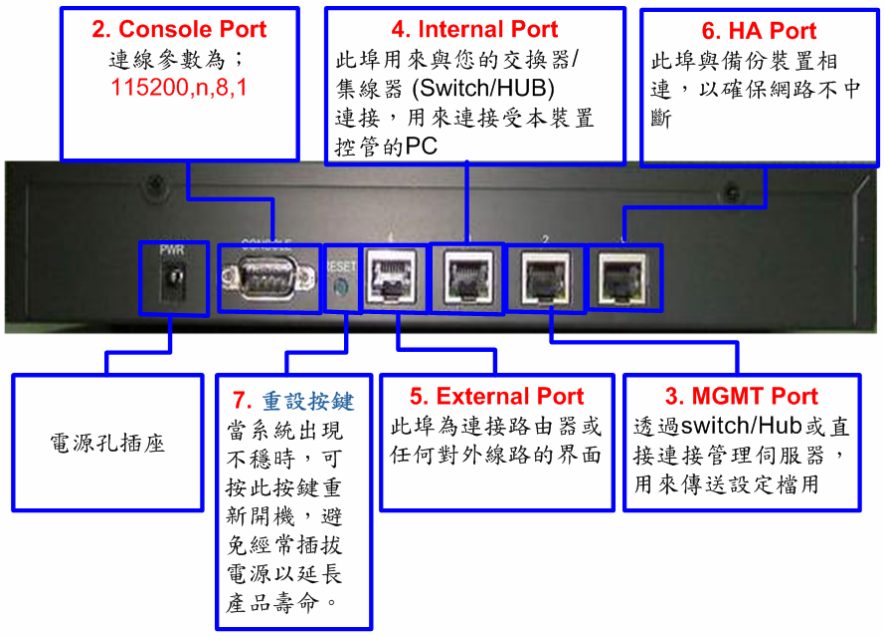
InstantScan 系列产品的硬件规格根据您所购买的型号而有不同。当您将 InstantScan 安装于路由器后方时，所有进出流量皆会受其控管。LAN 端的流量必须连接于 InstantScan Internal 端，而所有连外的流量必须藉由 InstantScan External 端与存取路由器（access router）相连。

2.2 将 InstantScan 连上网络

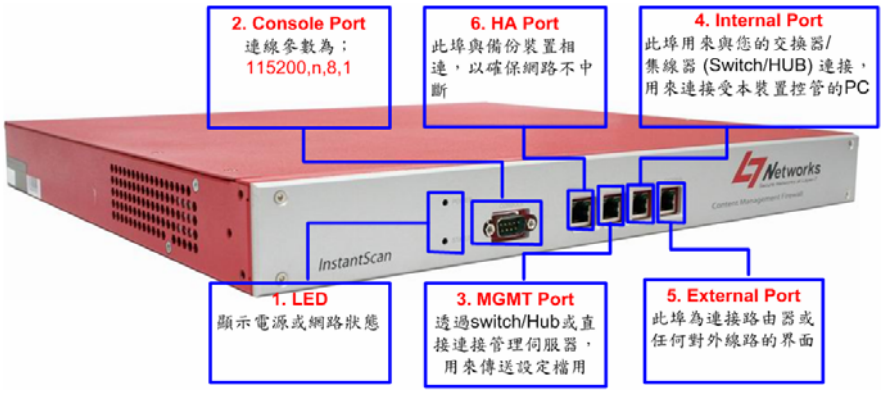
1. **电源**。首先将电源接上InstantScan背面的电源孔，然后将另一端接上电源插座。并将开关切换至 I。请稍候约两分钟，InstantScan开机完毕后，再进行下一步连接动作。注意，IS-10只需将变压器的接头接上其背后的电源孔即可启动电源。
2. **Console界面**。利用RS-232 console线，将InstantScan console埠与您用来设定InstantScan的PC对接。您即可透过CLI指令来设定InstantScan的系统参数。
3. **MGMT界面**。此管理接口系用来传送InstantScan的设定档封包，所以必须透过网络线与LAN端的交换器或集线器相连，且要与管理服务器在同一网段底下。

4. **Internal界面**。此界面系透过网络线与您位于LAN端的交换器或集线器相连，用来管理所有内部可控管的网络流量。
5. **External界面**。此界面系透过网络线将其与存取路由器相连，用来与因特网联机。
6. **HA界面**。用来连接备份设备，以确保网络不因硬件或意外而中断。
7. **重设键**。用来重开机用，避免经常开关电源，而缩短软硬件使用寿命。

连接端口的排列顺序依您的购买型号而有不同，以下的范例仅供参考。确实的连接端口排列顺序，请连结CLI界面，在权限模式下键入 “ip show”，即可以其排列顺序设定IP参数，并连结网络。详细CLI指令，请详见附錄 C。



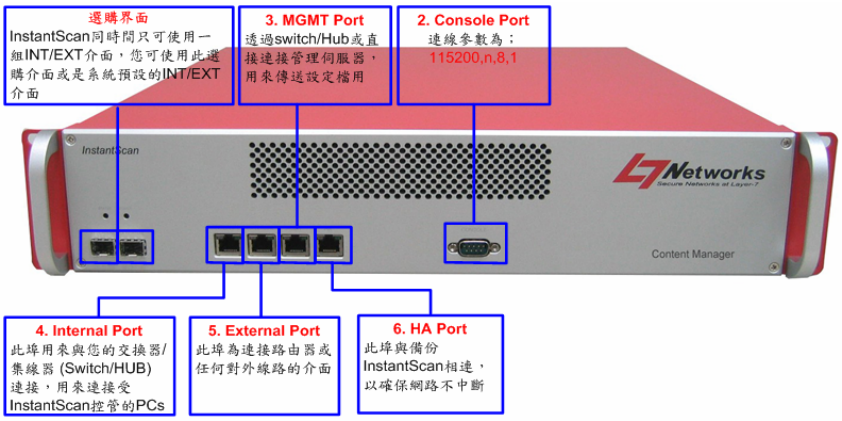
图表 2 1 InstantScan 10 网络联机



图表 2 2 InstantScan 100 网络联机

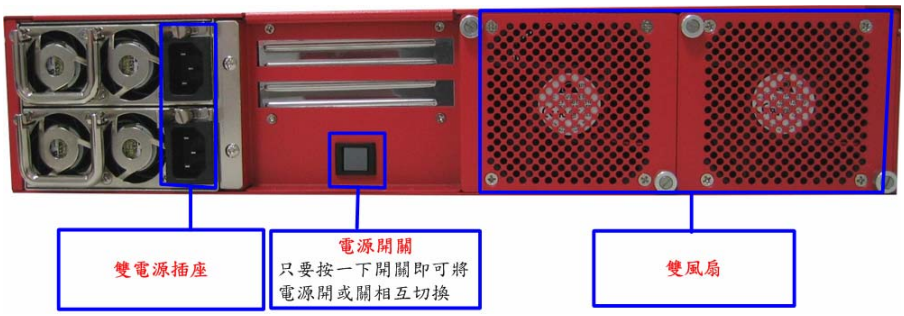
图表 2 3 InstantScan 1000 预设网络联机

图表 2 4 InstantScan 1000 背面面板



图表 2 5 InstantScan 5000 预设网络联机

InstantScan 5000 背面面板



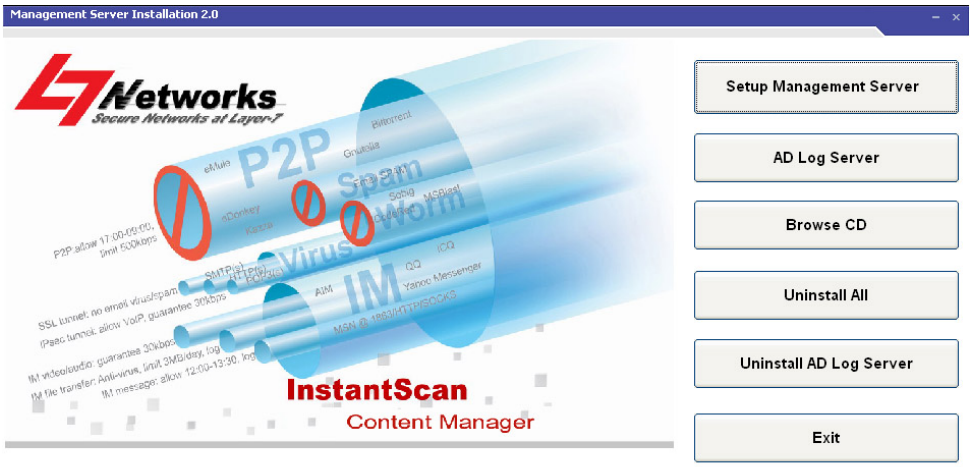
图表 2 6 InstantScan 5000 预设网络联机

IS-5000 提供以下不同的硬件规格：

1. IS-5000 提供使用者双 PCI 扩充插槽。使用者可以根据需求修改网络接口的设定。
2. 当您将电源打开后，双电源系统应正常运作，如其中有一电源故障，内建蜂音器便会响起，用以警告您电源有问题。

第3章
安装管理服务器

请拿出随机出货的管理服务器安装光盘片来安装您的管理服务器。如果安装软件在您将光盘片放入光驱后没有自动执行，请将鼠标移到光盘所在的位置点两下，找到执行档**setup.exe**，然后点两下，即会出现下列画面。



图表 3 1 主要设定窗口

请依下列步骤完成安装程序（视您需求，选择您喜爱的语系）：

步驟 1. 安装Management Server

3.1 管理服务器之硬件需求

✓ 操作系统 (OS) 至少应为 Windows 2000/2003、Windows XP 或更高等级。如果您的操作系统为英文板，请先安装繁体中文字型套件，否则无法正常显示中文字型。语言套件安装窗口将于您开始安装管理服务器时显示，请点选Install安装。

图表 3 2 Language pack installation page

- ✓ 硬盘至少**80GB**以上可使用空间，建议最好有**120GB**可使用空间。
- ✓ CPU最少是**Pentium 4**或**同等级**。
- ✓ 内存最少**256MB**，建议最好**512MB**以上。
- ✓ 如果您的操作系统是Windows XP service pack 2，且启用其内建的防火墙，请记得依以下步骤开启连接埠514、1080和3306。如此一来，所有封包的进出，才不会因防火墙的拦阻而有所漏失，管理服务器才会正常运作。
  1. 到**开始 > 设定 > 网络联机。**
  2. 点选**区域联机**，按鼠标右键选择**内容**。
  3. 到**进阶 > 设定值 > 例外**。点击**新增连接埠...**
  4. 输入**名称**与**连接埠编号**，点选此连接端口所使用的通讯协议(UDP或TCP)。点击**确定**储存设定值。

名称	连接端口编码	通讯协议
Log Server	514	UDP
Socks	1080	TCP
Database Server	3306	TCP

表格 3 1 连接埠设定

3.2 安装管理服务器

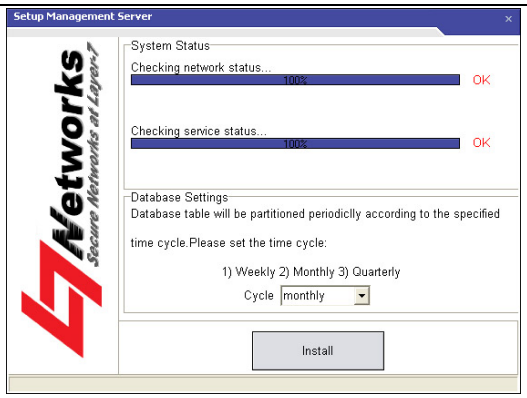
InstantScan 管理服务器方便您管理多台 InstantScan 设备，且可产生报表供您做网络分析。因此，您要执行此程序需搭配 JRE、利用数据库储存事件记录，还有其它辅助程序来显示报表。

步驟 1. 安装管理服务器

点击 **Setup Management Server**。系统将逐步引导您安装管理服务器。

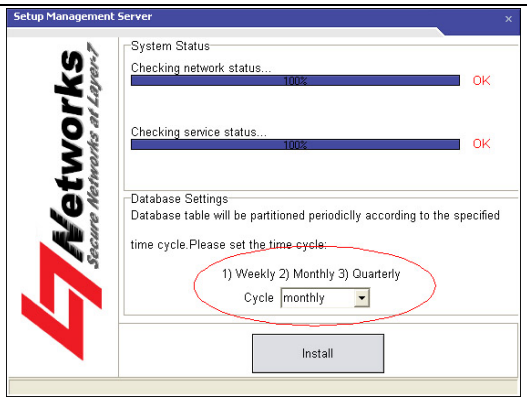
步驟 2. 新安装管理服务器

如果第一次安装管理服务器，请点击 **Install**。安装程序会检查是否有旧系统存在。如果已安装过请先行移除就程序再安装。



步驟 3. 选择报表产生周期

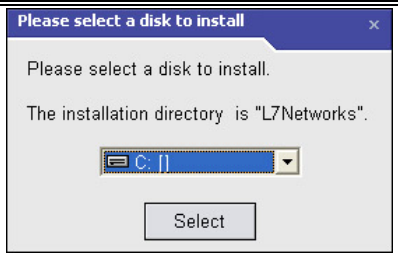
为了加强数据库处理的效能，InstantScan 将根据您所选择的分割周期来做数据库的分割。请选择适合的数据库分割周期：1) 每周； 2) 每月； 3) 每季。例如，当您选择每月，数据库将根据数据的种类，每种数据每月产生一个表格（Table）。当然这样的设计有其限制，您无法做跨月的搜寻。



步驟 4. 选择安装目录

当您点击 **Install** 后，系统将会跳出一个请您选择安装目录的窗口。

点击 Select 之后便开使进行安装。



步驟 5. 重新启动系统

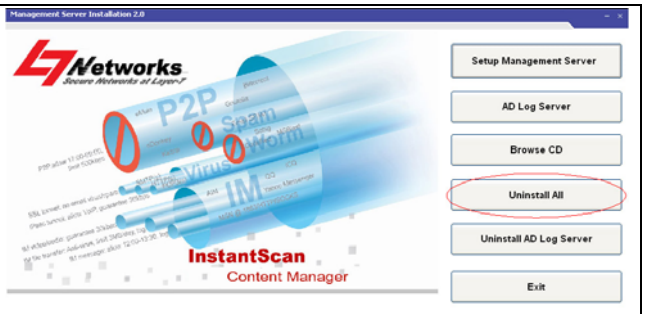
点击 Reboot Now 系统将会自动重开机。这可让您所安装的软件正确地执行。

3.3 反安装程序

步驟 1. 点击反安装程序

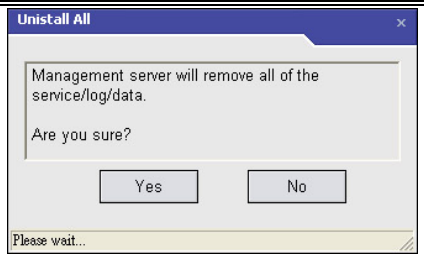
当您要升级 InstantScan 管理服务器，或要重新安装它时，建议最好先将要升级的程序反安装，之后再安装要升级的版本。

点击 **Uninstall All**，将会弹跳出反安装程序窗口。



步驟 2. 反安装管理服务器

点击 Yes，系统将会被移除。



第4章
设定系统参数

4.1 设定 InstantScan

在您开始控管InstantScan设备前，请先利用InstantScan的console接口，直接用RS-232 console线与用来设定 InstantScan 客户端的 PC 对接。然后，透过 CLI 指令来设定 InstantScan 的系统参数。之后，您可以利用Telnet、SSH，或其它terminal等远程联机方式来更改系统参数。

4.1.1 启动系统

将邻近InstantScan电源插槽的电源开关打开。在开机完成后，系统将要求您输入 ID 与密码。此时，预设的 ID 与密码皆是 admin 。在您登入系统后，您可以利用CLI 指令更改密码。详细 CLI 指令，请参阅附錄 C 说明。

4.1.2 出厂默认值 vs. 范例设定

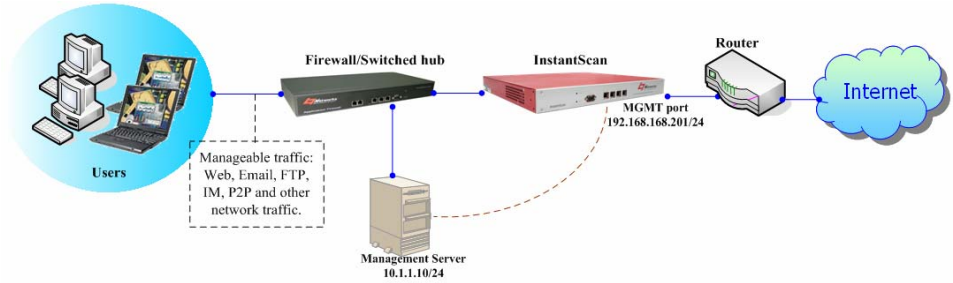
在下表中您可比较出厂默认值与本手册范例中所使用的 IP 设定值。请记得，INT（Internal）连接埠与 EXT（External）连接埠并不需要设定任何 IP。因为 Internal 连接埠是连接所有 LAN 端受 InstantScan 控管的客户端，而 External 连接埠为连接对外的网络。连接端口排列顺序依您所购买的型号而有不同，当您首次使用 InstantScan 时，请进入 CLI 接口查看连接端口的排列顺序。在权限模式中输入 “ip show”，您可以看出所有依照连接埠编号排列的连接埠，然后对照您设备上的编号，即可以此顺序来连结您的网络线。

项目		预设设定	范例设定
Password		admin	admin
Internal	Port No.	1	N/A
	IP Address	N/A	N/A
	Subnet mask	N/A	N/A
	Status	DOWN	UP
External	Port No.	2	N/A
	IP Address	N/A	N/A

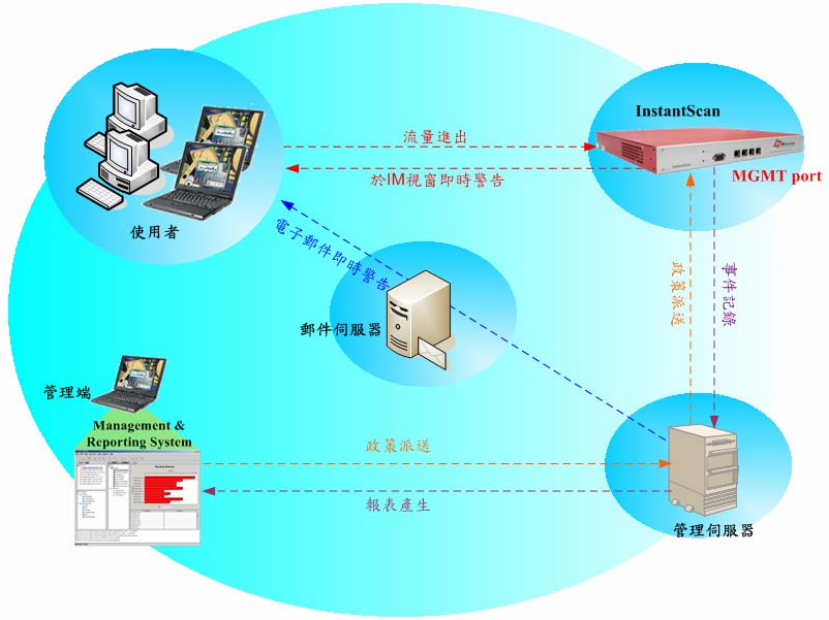
	Netmask	N/A	N/A
	Status	DOWN	N/A
MGT	Port No.	3	3
	IP Address	192.168.1.1	192.168.168.201
	Netmask	255.255.255.0	255.255.255.0
	Gateway IP	192.168.1.254	192.168.168.254
	Primary DNS	0.0.0.0	168.95.1.1
	Secondary DNS	0.0.0.0	0.0.0.0
	Status	DOWN	UP
HA	Port No.	4	4
	IP Address	N/A	N/A
	Netmask	N/A	N/A
	Status	DOWN	DOWN
Management Server	IP Address	尚未设定	10.1.1.10
	Subnet mask	尚未设定	255.255.255.0
	Gateway IP	尚未设定	10.1.1.254
	Primary DNS	尚未设定	168.95.1.1
	Secondary DNS	尚未设定	N/A

表格 4 1 InstantScan 相关系统默认值

InstantScan以通透模式安装于网络上，不需更改既有的网络架构。InstantScan管理服务器配合InstantScan管理系统与报表系统，提供您简而易用的使用者管理接口来设定管理政策。网管人员可根据网络架构与公司政策来订定各式各样的管理政策。一台管理服务器可同时控管多台InstantScan，并且可接收与分析被控管的InstantScan 之事件记录。您可将管理服务器安置于任何网络位置。本手册提供一个基础的 InstantScan 网络安装架构。只要您了解基本的安装原理，您即可根据贵公司的网络架构安装您的 InstantScan。



图表 4 1 InstantScan 联机范例



图表 4 2 InstantScan 系统的讯息递送

如图表 4-2 所示，您必须指定 IP 地址给 **1） InstantScan 管理接口**（Management 连接端口）；**2） 管理服务器**；与 **3）管理端 PC**。InstantScan 可安装于企业网络内部或外部。当网管人员新增一条管理规则，并将设定文件上传，管理服务器立即将设定档上传至 InstantScan。当受到 InstantScan 控管的 PC 启用任何实时通讯（IM）软件或点对点（P2P）传输软件时，InstantScan 会将这些事件记录传送给管理服务器储存。管理服务器依您的时程规划，定期产生报表寄送给网管人员分析。

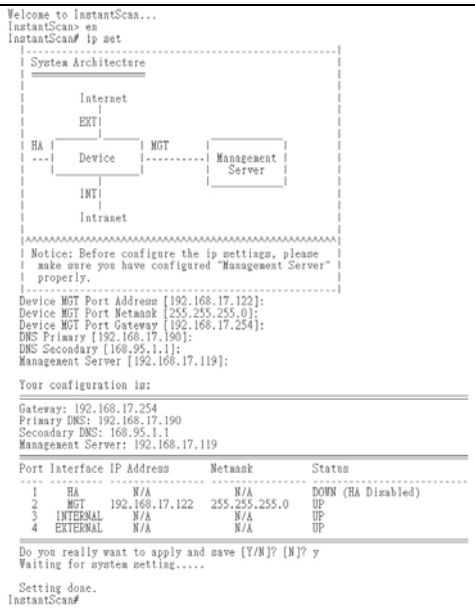
4.1.3 透过 CLI 界面设定系统参数

请用随机内附的 RS-232 console 线，将 InstantScan console 接口与用来设定 InstantScan 的 PC 之串行端口相连，您可选择 COM1 埠或 COM2 埠来设定 InstantScan。请参考以下超级终端机的设定范例。

终端机类型	超级终端机
每秒传输位	115200
数据位	8
同步检查	无

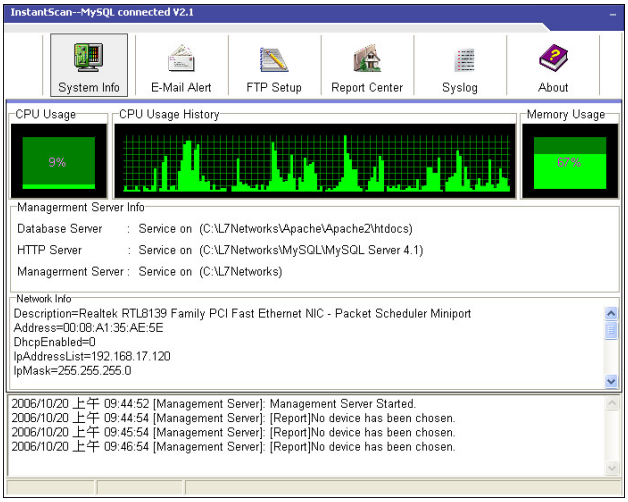
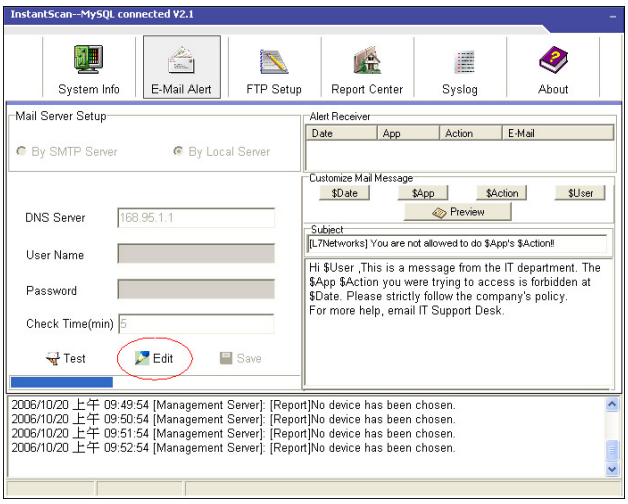
停止位	1
流量控制	无

表格 4 2 超级终端机参数设定

步驟 1. 登入系统 系统预设的登入账号密码为 **admin/admin**。之后您可以根据 CLI 指令来更改密码。 **注意!!!** 密码的长度必须藉于 5~20 字符间。小于 5 个字符或大于 20 个字符都会被系统拒绝。	InstantScan login: admin Password: Welcome to InstantScan... InstantScan>
步驟 2. 设定 InstantScan IP 地址 键入 **en** 进入权限模式。键入 **ip set** 指令来设定 MGT 端口的相关 IP 地址。	
步驟 3. 查看目前 InstantScan 设定状况 键入 **ip show**，您可以看到目前 InstantScan 的 IP 设定状况。	InstantScan# ip show Gateway: 192.168.168.254 Primary DNS: 168.95.1.1 Secondary DNS: 0.0.0.0 Management Server: 10.1.1.10 Port Interface IP Address Netmask Status 1 INTERNAL N/A N/A UP 2 EXTERNAL N/A N/A UP 3 MGT 192.168.168.201 255.255.255.0 UP 4 HA N/A N/A DOWN (HA Disabled) InstantScan#

4.1.4 设定 InstantScan Mailer

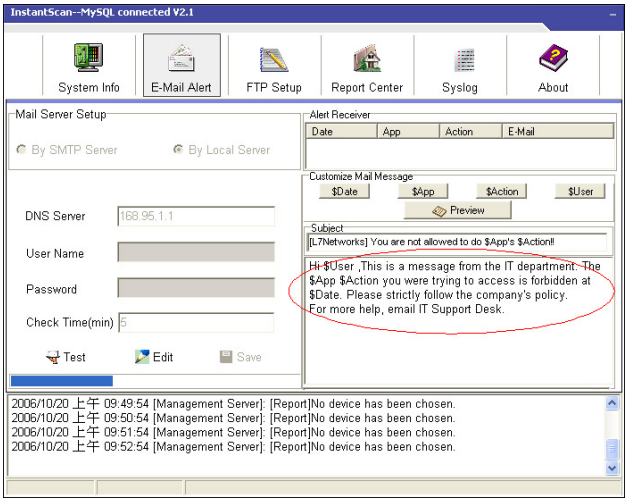
在管理服务器安装完成，且重开机后，有一小图示将会显示在服务器的右下角。请将鼠标移到图标上，点两下。

步骤 1. 系统信息 在这个页面上，您可以看到 CPU 与内存的使用情况，还有一些管理服务器的存放位置、网络讯息等。	**mailer > System Info** 
步骤 2. 设定邮件服务器 点击 **Edit** 按键。选择 **By Local Server** 选项。输入 **DNS** 服务器 IP 地址，并在 **Check Time(min)**字段上键入系统检查是否有警告信件的时间。如果您希望透过 SMPT 服务器寄送警告信件，请点选 **By SMTP Server** 选项。您可以点击 **Test** 测试您是否可顺利收到警告邮件。	**Mailer > E-Mail Alert > Edit** 

步驟 3. 客制化邮件讯息

将光标移到文字方块中要加入变量的位置，点击变量($Date 、 $App 、 $Action 、 $User)。

Mailer > E-Mail Alert > Customize Mail Message



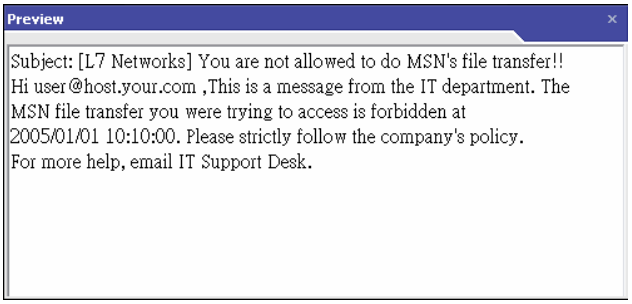
变量名称	说明	范例
$Date (日期)	违反政策事件发生的日期。	2005/01/01 10:10:00
$App (应用软件)	IM使用者违反政策时所使用的IM软件。	MSN
$Action (使用行为)	不合法的IM使用行为。	file transfer
$User (使用者账号)	违反政策的IM使用者账号。	sales@msn.com

表格 4 3 警告信件内的变量设定

步驟 4. 预览警告信件内容

当您设定好警告信件内容，可点击 **Preview** 预览。关闭预览窗口继续下一步。

Mailer > E-Mail Alert > Customize Mail > Preview

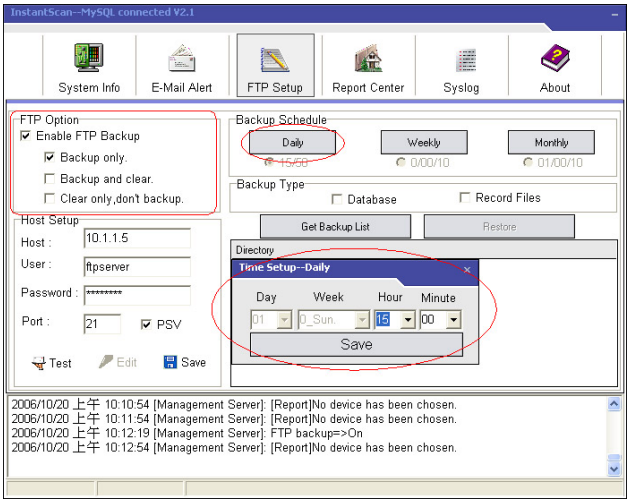


步驟 5. FTP 设定

在本页，您可设定利用FTP备份记录的方式。勾选 **Enable FTP Backup**，然后勾选 **Backup only**。

您可以选择FTP自动备份的时间 1) 每日 2) 每周 3) 每月。点击 **Daily**，然后选择**15 : 00**。换句话说，每天下午 3 点，系统会开始透过 FTP 备份当天的事件记录。

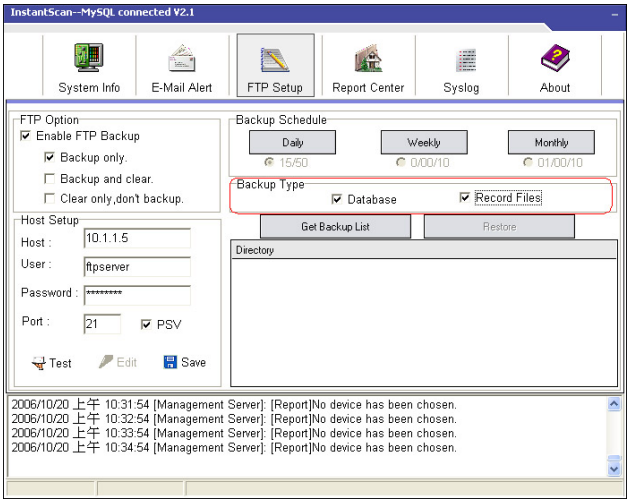
Mailer > FTP Setup > Backup Schedule



步驟 6. 设定备份类型

请在 Backup Type 选择数据备份类型。当您要还原您已被份的数据，请点击 Restore/Connect 按钮，然后选择要从 FTP 服务器上下载的路径，点击 Download 开始数据库或档案还原。

Mailer > FTP Setup > Backup Type

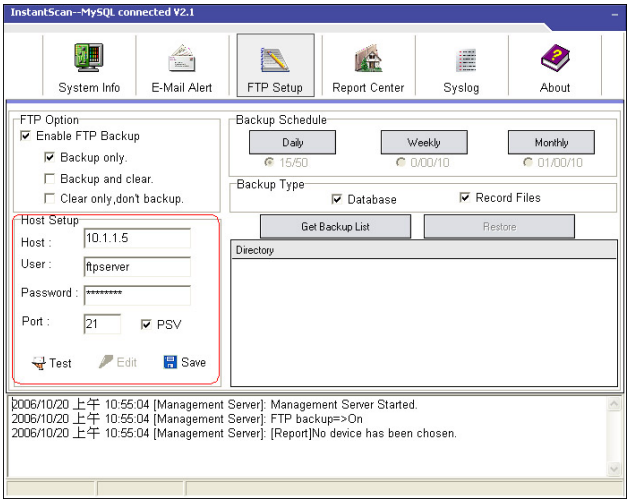


步驟 7. 设定 FTP 服务器

点选 Edit 开始编辑相关设定，输点入 FTP 服务器 IP 地址、使用者账号与密码。如果 FTP 服务器使用 passive mode 的话，请勾选 PSV。点击 **Test Connect** 测试 FTP 联机状况。再点选 Save 记录您所设定的相关选项。

承上所述，您选择每日下午 3 点 55 分备份 log，系统将于此时自动 FTP 备份 log。所备份的数据夹将会以该日的日期命名。

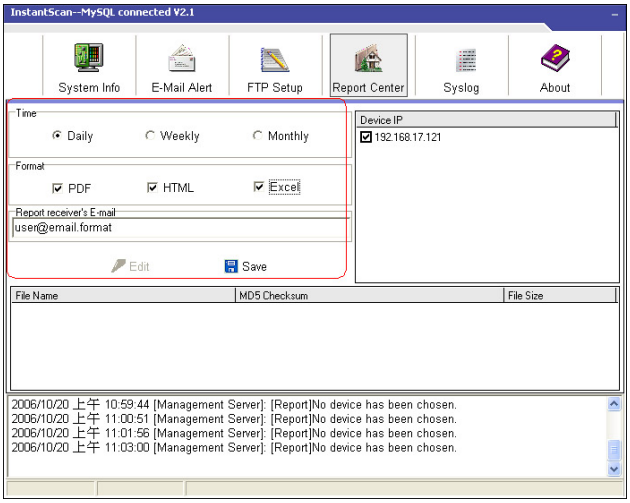
Mailer > FTP Setup > Host Setup



步驟 8. 报表中心

点选 Edit 开始编辑相关设定，选择寄送报表的时间(每日/每周/每月)。勾选您希望收到的报表格式(PDF/HTML/Excel)，与勾选希望收到哪些 InstantScan 设备的 log。输入收信者的电子邮件信箱。再点选 Save 记录您所设定的相关选项。

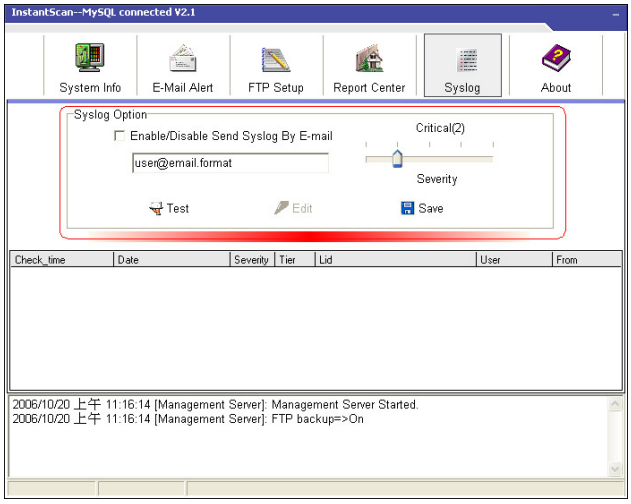
Mailer > Report Center



步驟 9. 系统记录

点选 Edit 开始编辑相关设定，勾选 Enable/Disable Send Syslog By E-mail，然后在空格处填写您的 Email 地址。利用鼠标移动到您想要收到的系统记录的等级。共分为 5 个等级 1) Alert（警告）2) Critical（严重） 3) Warning （警示） 4) Notification （注意） 5) Information （信息）。如果您只希望收到 Alert 等级的系统记录，只要将指针拉到 Alert 的位置。但是，如果您希望收到所有的系统记录，您必须把指针拉到 Information 的位置。再点选 Save 记录您所设定的相关选项。

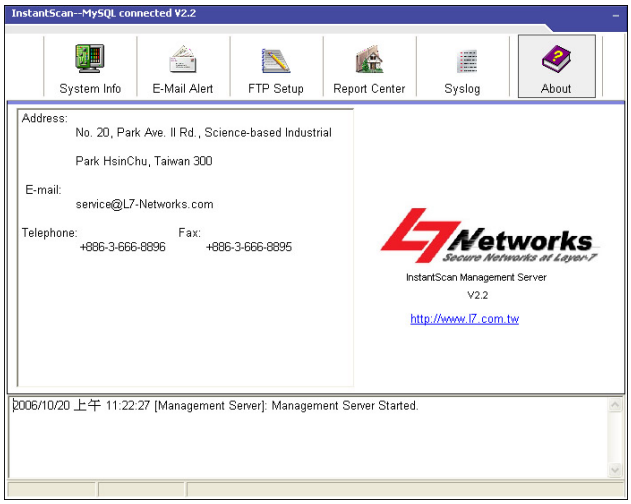
Mailer > Syslog



步驟 10. 版本宣告

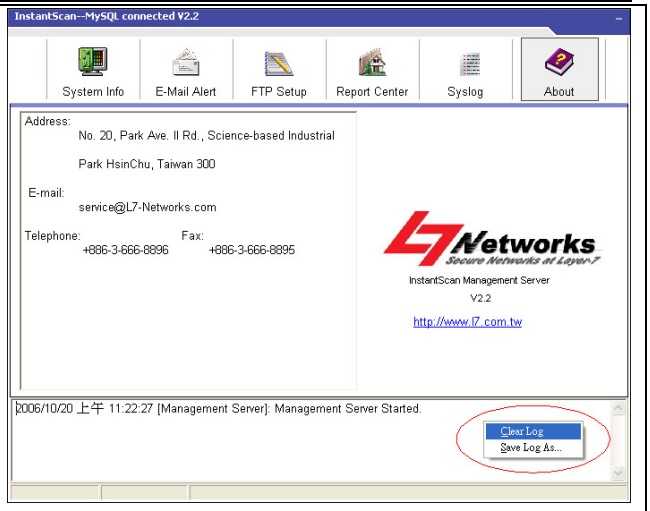
请参阅此版本宣告与重要讯息。

Mailer > About L7



步驟 11. 清空或储存系统纪录

在状态区内按右键。您可选择清空事件记录或者将纪录储存到硬盘上。



如果您不小心关闭邮件收发机，您可以在 C 磁槽根目录，L7 Networks数据夹内找到档案mailer.exe。移动您的鼠标，在mailer.exe图示上点两下，即可开启它。mailer预设储存的路径为C:/L7Network。

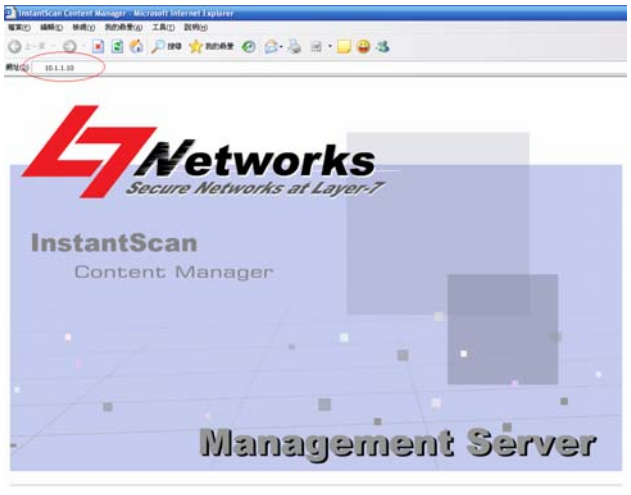
第5章
管理 InstantScan

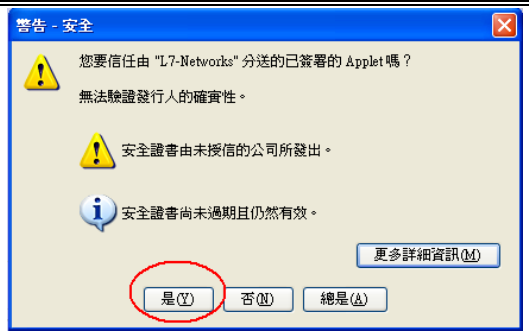
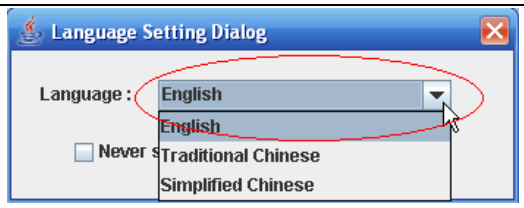
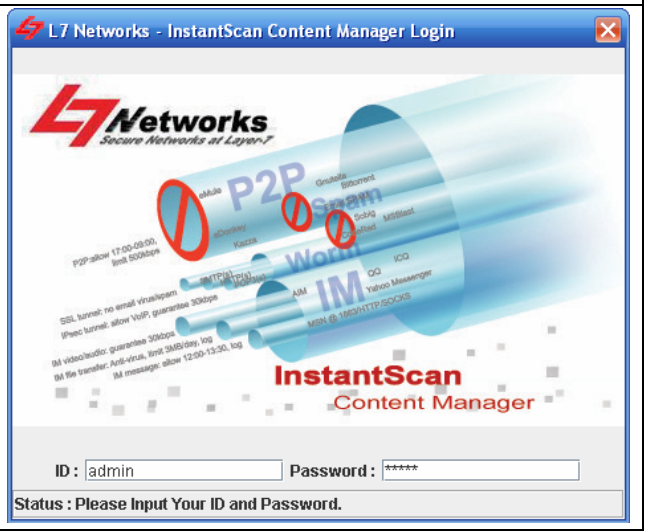
5.1 InstantScan 基本设定

一旦您完成上个章节的系统参数设定，现在就可以透过IE浏览器连结管理服务器，利用使用者网页界面来管理InstantScan。如果您需要更详尽的设定范例，请参考InstantScan使用手册。

5.1.1 连结管理服务器

InstantScan管理系统与报表系统使用Java平台设计，需要支持Java Plug-in程序。所以客户端必须从管理服务器处安装Java Plug-in，才可浏览管理服务器网页。当您第一次使用IE浏览器连结管理服务器时，Java Plug-in便会自动安装进您的计算机。**第一次登入时需要一些时间让程序初始化，请耐心等候。**

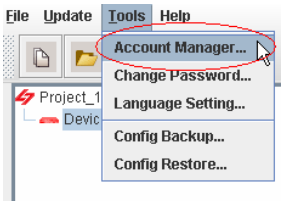
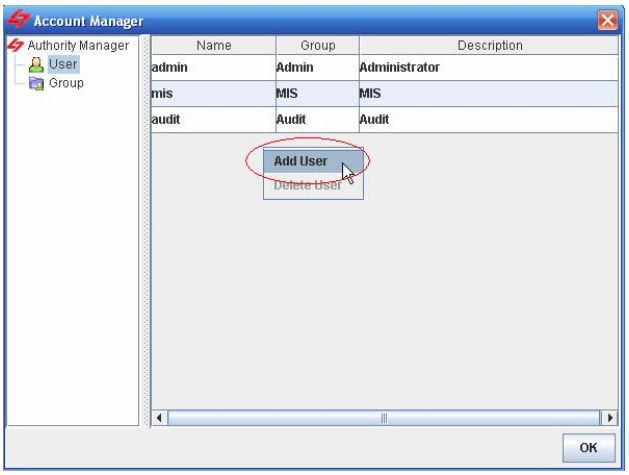
步驟 1. 连结网页服务器 打开您的 IE 浏览器，在网址列上键入 http://<管理服务器 IP 地址>。例如，输入 http://10.1.1.10 来连结管理服务器。	**连结 http://10.1.1.10** 

步骤 2. 安全警告窗口 点击**是**接受此验证。如果您不想每次都出现此警告窗口，请点击**总是**。当您点击**是**或者**总是**后，您就可以进入登入画面。	
步骤 3. 选择语言模块 InstantScan 目前提供英文、繁体中文、简体中文等三种语言模块供您选择，您可以选择您喜爱的语言当成网页接口的预设语言模块。点击 OK 进入登入画面。	
步骤 4. 登入 输入 ID/Password (预设都是 **admin**)。通过确认后，即可进入管理页面。	

◆ 账号管理

在您第一次登入 InstantScan 内容管理器时，您可以在账号管理员编辑可存取管理服务器的账号与密码。借由权限阶层式控管 InstantScan，让贵公司确保员工个人隐私与公司机密，更能符合公司稽核的需求。

5.1.1.1 新增使用者账号

步驟 1 管理账号设定 选择 **Account Manager（账号管理员）**选项。	**Tool > Account Manager** 
步驟 2 新增使用者账号 InstantScan 可同时多人联机控管，您可在 Account Manager（账号管理员）建立可存取管理服务器的账号，包含使用者与其所归属的群组。	**Tool > Account Manager > User > Add User** 

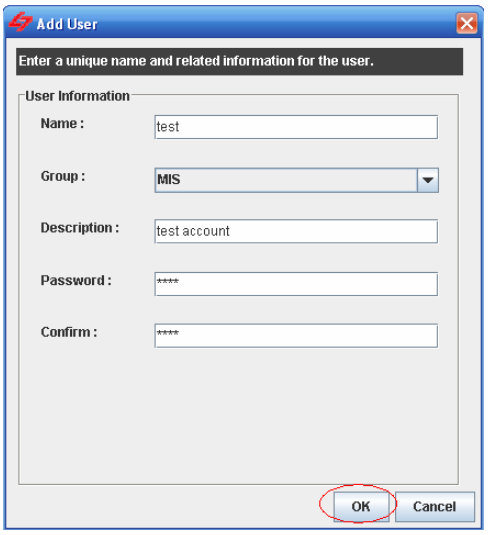
字段	说明	范例
Name（名称）	可存取管理服务器的使用者账号名称。	test
Group（群组）	可存取管理服务器的使用者群组，可分成三种授权群组： 1. admin（管理人员）：可设定 InstantScan、浏览报表与查看侧录记录等所有权限。 2. mis（网管人员）：只可设定 InstantScan，但无法浏览报表与查看侧录记录。 3. audit（稽核人员）：只可查看侧录记录，但无法设定 InstantScan。 **注意：群组不可增删修改。**	mis
Description（描述）	针对账号的详细说明。	test account

表格 5 1 账号管理员

步驟 3 编辑账号

请输入您要新增的账号名称、对此账号的描述、与其密码，并选择所属群组。

Tool > Account Manager > User > Add User



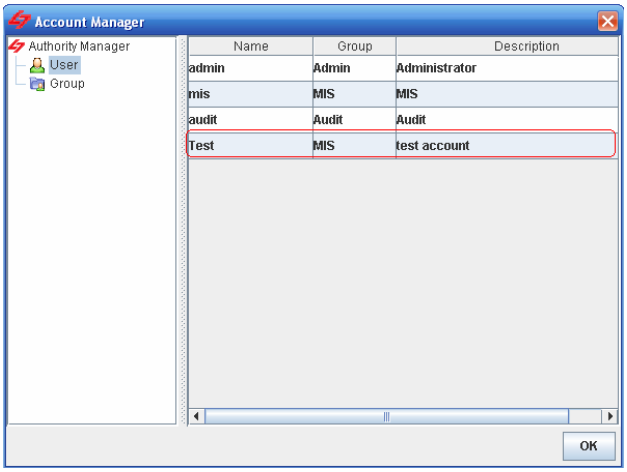
步驟 4 账号建立成功讯息

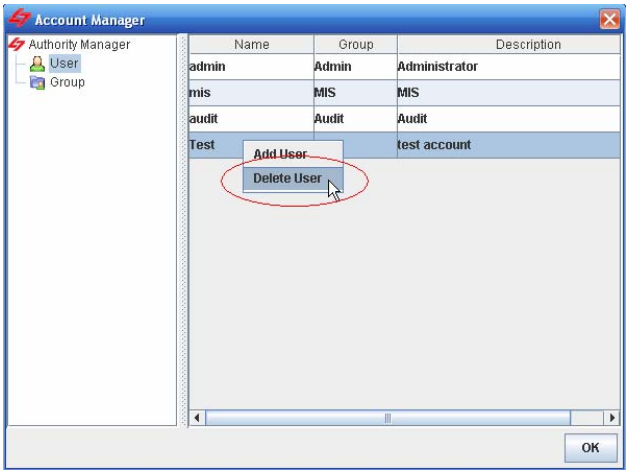
当您建立账号成功，将有如右图的窗口通知您新增成功。

步驟 5 显示已增加的账号

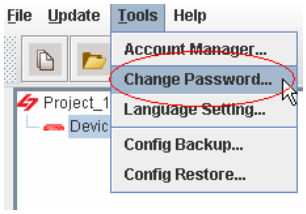
当您成功建立账号，您可以在 **Account Manager**（账号管理员）的窗口上看到这笔数据。

Tool > Account Manager > User



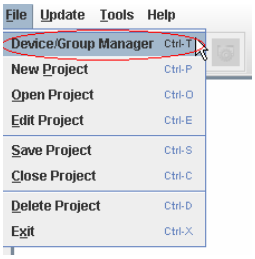
步驟 6 删除账号 欲删除某笔账号，只要点选此笔数据，然后按右键，选择 **Delete User** （删除使用者）。	**Tool > Account Manager > User > Delete User** 

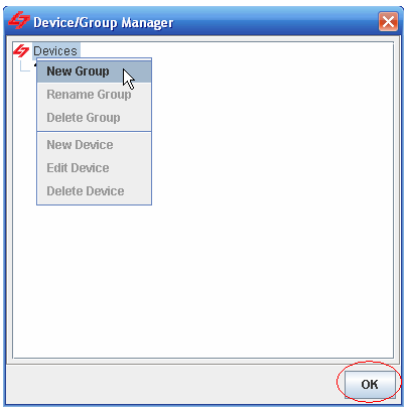
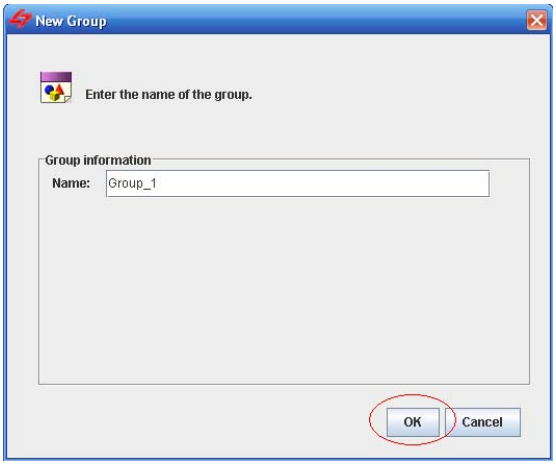
5.1.2 修改管理服务器密码

步驟 1 点选更改密码 选择 **Change Password**（**更改密码**）选项。	**Tool > Change Password** 

步驟 2 输入新的密码 输入 **Old Password**（旧的密码）与 **New Password**（新的密码），然后在 Confirm（**确认**）字段内再次输入新的密码。点击 **OK** 完成设定。	**Tool > Change Password** 

◆ 新增 InstantScan 装置/群组

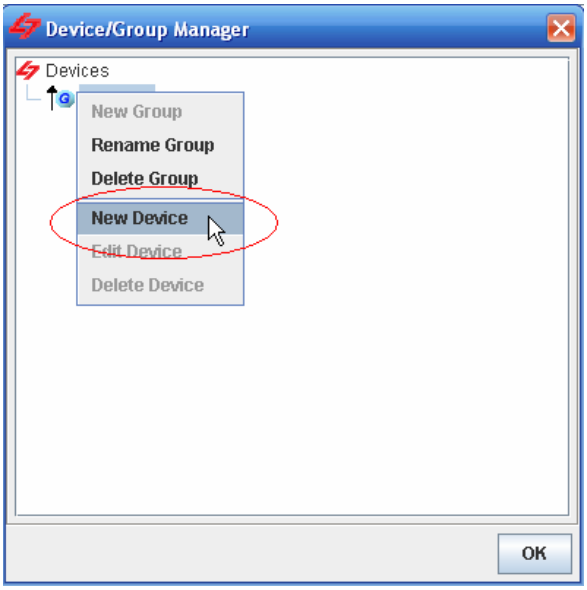
步驟 1 选择群组管理员 点 选 **Device/Group Manager** 选项。	**File > Device/Group Manager** 

步驟 2 新增群组 在 **Devices** 上按右键，然后点选 **New Group**。	**File > Device/Group Manager > New Group** 
步驟 3 新增群组名称 输入此群组的名称，然后点击 **OK** 继续。之后，群组名称将显示在屏幕上。您可以按右键选择 **Rename Group** 或 **Delete Gorup** 来修改或删除此群组。	**File > Device/Group Manager > New Group** 

步驟 4 新增装置

在群组 **Group_1** 上按右键，然后点选 **New Device**。

File > Device/Group Manager > New Device

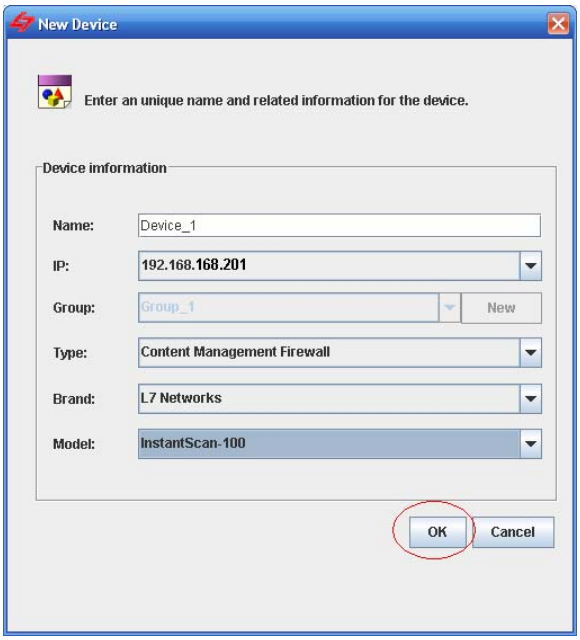


步驟 5 编辑新装置相关信息

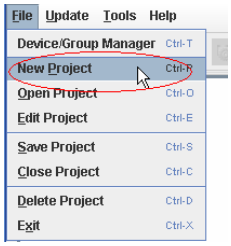
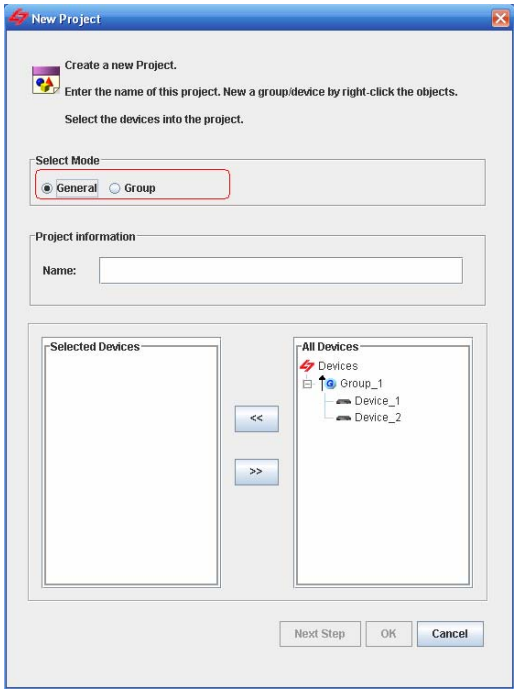
输入装置名称，并选择一组已指定其管理服务器的 InstantScan 装置之 IP 地址，然后输入其余相关信息。点击 **OK** 储存设定。

注意：您必须先透过 CLI 接口，设定好装置上的 IP，然后指定管理服务器 IP 地址，否则您无法在 UI 上新增任何装置。当您设定好装置后，管理服务器将自动撷取属于其列管的 device 信息。只要是已经设定过的装置，就不可以再被设定。也就是说，当我已经设定好 Device_1 192.168.168.201，当您要再新增装置时，192.168.168.201 将不再出现在 IP 字段内了。

File > Device/Group Manager > New Device



◆ 新增专案

步驟 1 新增专案 选择 **New Project**。	**File > New Project** 
步驟 2 建立新项目 首先，请点选项目的模式，输入项目名称，从 **All Devices** 字段中选择要加入此项目的装置，然后点击 **<<**（**左向箭头**）将点选的装置加到 **Selected Devices** 字段。如果您要从此项目移除某个装置，请点选该装置，然后点击 **>>** （**右向箭头**）即可。	**File > New Project > New Project** 

项目模式	说明
General（一般）。	您希望每台 InstantScan 装置可以拥有其个别的设定文件，每台装置可摆放在不同的部门，且各自独立运作，您可以选择此模式。
Group（群组）	当您购买 2 台或 2 台以上 InstantScan 装置，希望简化设定的步骤，所有装置的设定文件共享，其报表系统也共享。也就是说，不管您在哪一台 Device 上变更设定档，此设定档都会写进基底装置（Base Device）

	的设定档中。其它装置只要重新加载设定文件即可撷取已更新过的设定档。

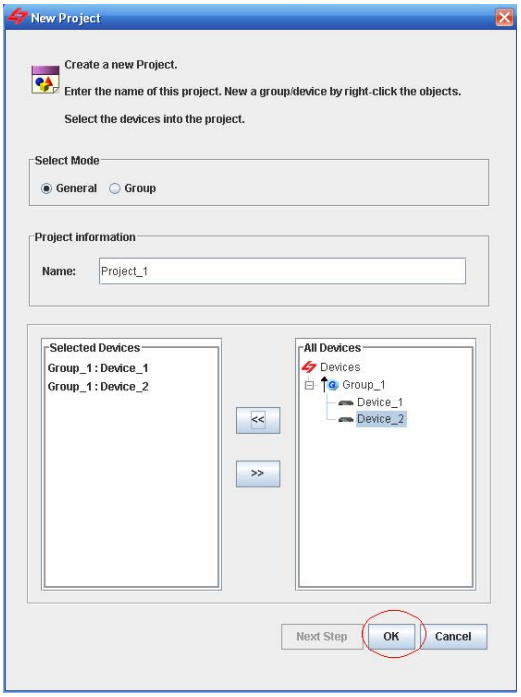
表格 5 2 项目模式

5.1.2.1 一般项目模式

步驟 1 新增一般项目模式

选择 **General （一般）**为项目的模式，这个模式适合大部分的案例。输入项目名称，从 **All Devices** 字段中选择要加入此项目的装置，然后点击 **<<（左向箭头）**将点选的装置加到 **Selected Devices** 字段。如果您要从此项目移除某个装置，请点选该装置，然后点击 **>>（右向箭头）**即可。最后点击 OK 结束设定。

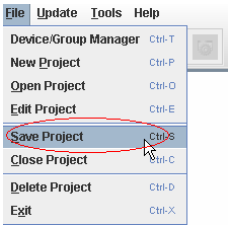
File > New Project



步驟 2 储存项目

点选 **Save Project** 储存已建立的项目。

File > Save Project

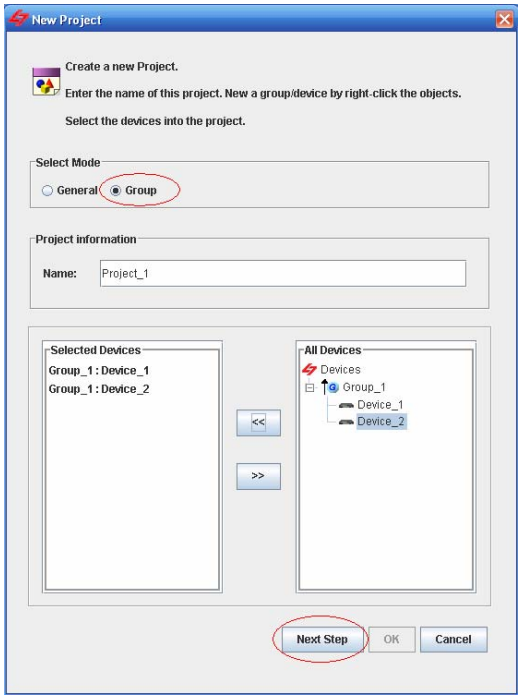


5.1.2.2 群组项目模式

步骤 1 新增群组项目模式

选择 **Group （群组）**为项目的模式，这个模式适合购买多台 InstantScan，希望简化设定步骤，节省人力资源的公司。输入项目名称，从 **All Devices** 字段中选择要加入此项目的装置，然后点击 **<<（左向箭头）**将点选的装置加到 **Selected Devices** 字段。如果您要从此项目移除某个装置，请点选该装置，然后点击 **>> （右向箭头）**即可。最后点击 **Next Step** 继续下一步骤。

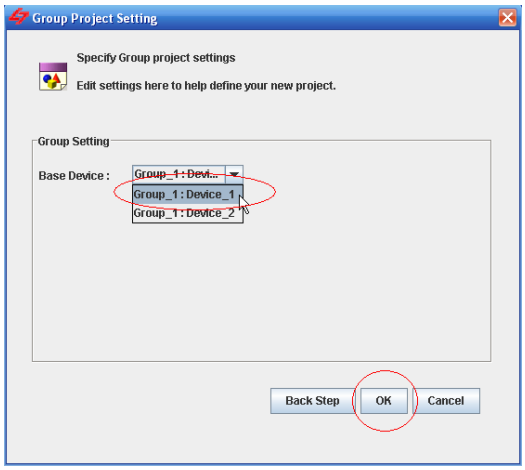
File > New Project

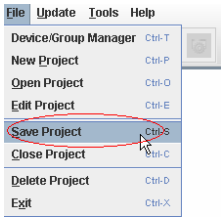


步骤 2 选择基底装置

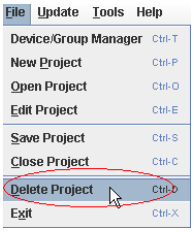
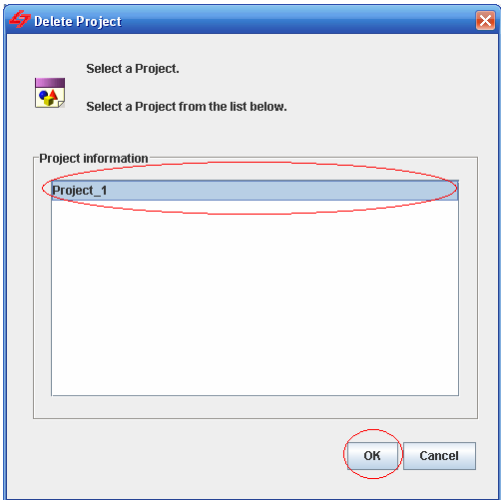
选择 Base Device（基底装置），当您选择基底装置后，所有此项目内的装置都会读取这个基底装置的设定文件，且读取的报表是所有装置的总和。最后点击 **OK** 结束设定。

File > New Project > Next Step

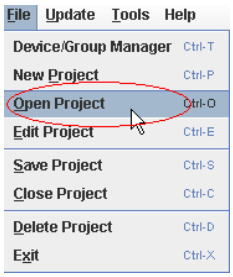
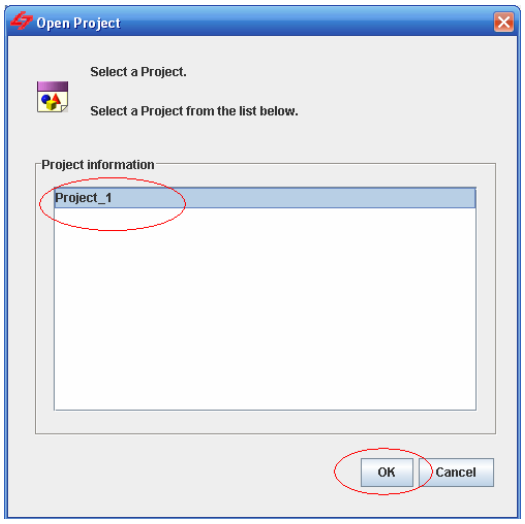


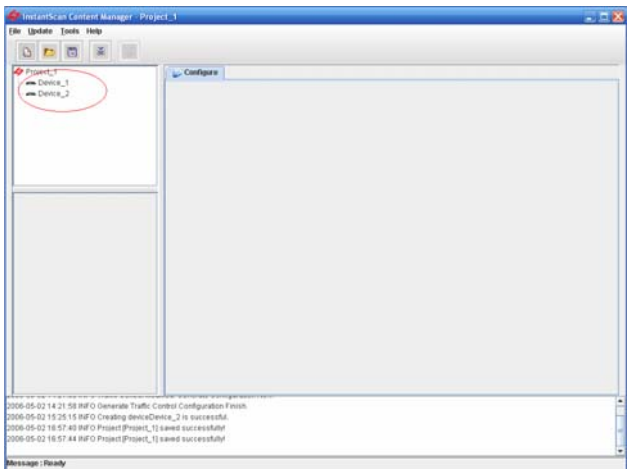
步驟 3 储存项目 点选 **Save Project** 储存已建立的项目。	**File > Save Project** 

◆ 删除项目

步驟 1 点选删除项目 点选 **Delete Project** 选项。	**File > Delete Project** 
步驟 2 删除项目 选择您想删除的项目，然后点击 **OK** 关闭窗口。 **注意：** 1. 一旦您点击 **OK** 按钮后，此项目即刻会从系统中删除。 2. 正在执行中的项目无法删除，您必须先关闭项目，才可选择删除项目。	**File > Delete Project** 

◆ 开启已存在的项目

步驟 1 开启专案 点选 **Open Project** 选项。	**File > Open Project** 
步驟 2 选择要开启的专案 选择您要开启的专案。点击 **OK** 关闭窗口。	**File > Open Project** 

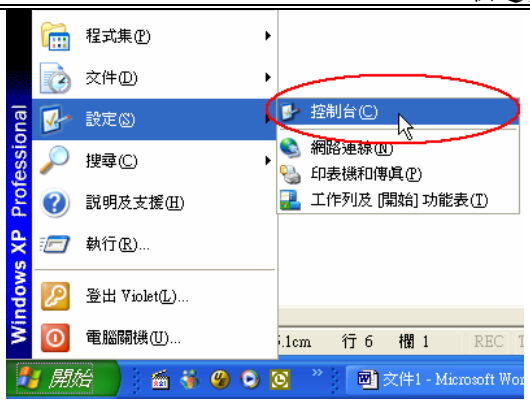
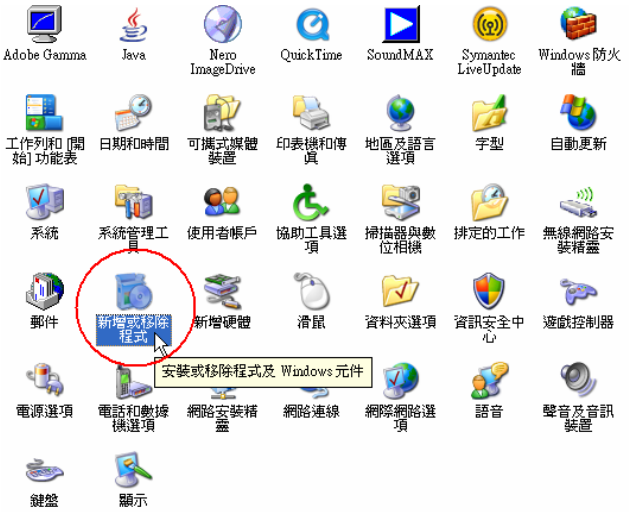
步驟 3 管理 InstantScan 现在，您可以开始管理您的 InstantScan。一个项目可以同时控管多台可能属于不同群组的装置。将鼠标移到您要控管的装置上点两下，系统将连结到此装置，并下载其设定档。	**File > Open Project** 

附錄 A
移除 MySQL 4.1 之前的版本

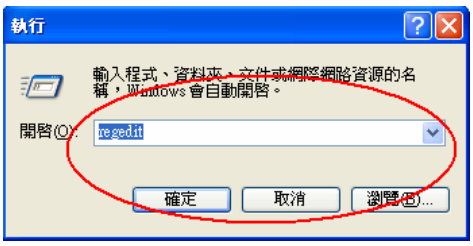
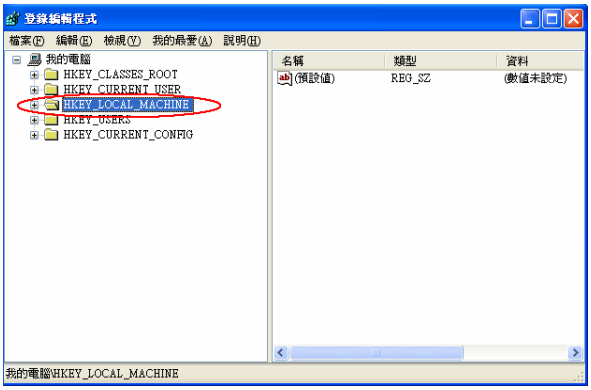
为了增强数据库的处理效能，我们建议您将数据库升级为 MySQL 4.1 版本。如果您已经安装 MySQL 4.1 之前的版本，请先移除旧有的版本再进行 MySQL 4.1 的安装。

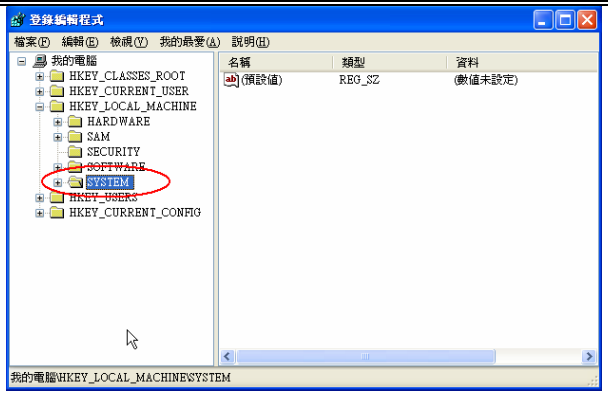
移除旧有版本

步驟 1. 控制台 点选**控制台**。	**到 开始 > 设定 > 控制台**

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>步驟 2. 新增或移除程序
点选新增或移除程序。</td><td>开始 > 设定 > 控制台 > 新增或移除程序
 
</td></tr>
<tr><td>步驟 3. 移除 MySQL 旧版本
点选 MySQL Server and Clients 3.23，然后点击变更/移除。</td><td>开始 > 设定 > 控制台 > 新增或移除程序 > MySQL Server Clients 3.23 > 变更/移除</td></tr>
</table>

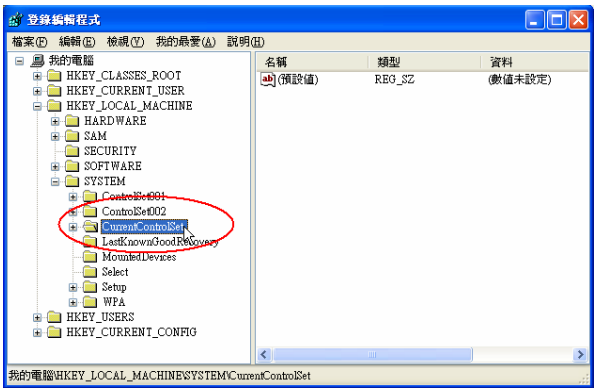
<table>
<tr><td></td><td> 
</td></tr>
<tr><td>步驟 4. 删除 MySQL 3.23 服务
上个步骤并无法完全移除 MySQL 3.23，所以您必须到登录编辑程序内移除其服务，才可完全将程序移除。

在执行的窗口内输入 regedit，然后点击确定。</td><td>开始 > 执行
 
</td></tr>
<tr><td>步驟 5. 点选 HKEY_LOCAL_MACHINE</td><td>开始 > 执行 > HKEY_LOCAL_MACHINE
 
</td></tr>
<tr><td>步驟 6. 点选 SYSTEM</td><td>开始 > 执行 > HKEY_LOCAL_MACHINE > System</td></tr>
</table>



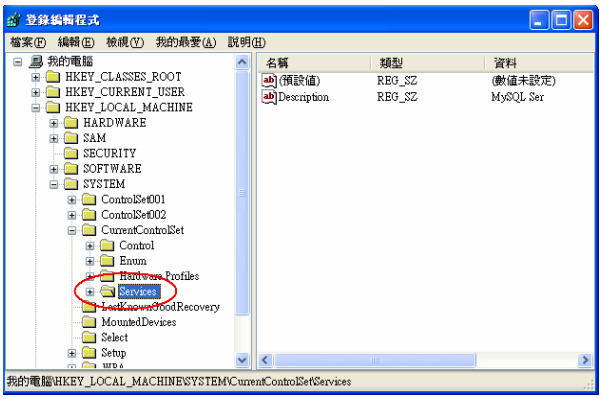
步驟 7. 点选 CurrentControlSet

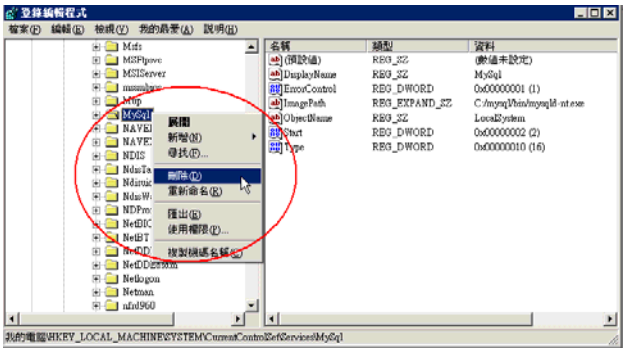
开始 > 执行 > **HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet**



步驟 8. 点选 Services

开始 > 执行 > HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services

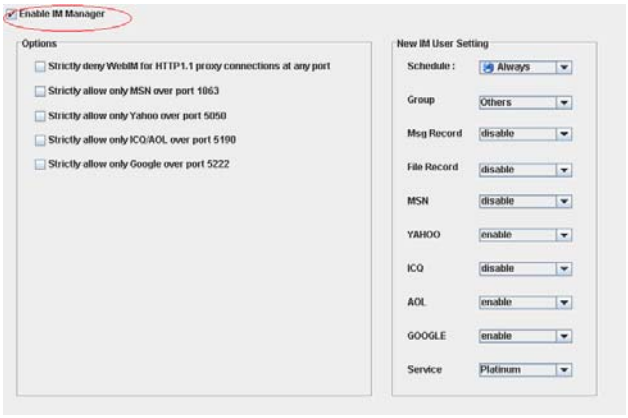
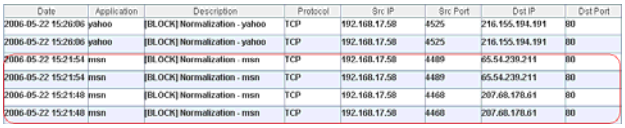


步驟 9. 删除 MySQL 点选 **MySQL**。在 **MySQL** 上按右键，然后点选**删除**。重新开机后，之前的 MySQL 服务就会直接从系统中被删除。	**开始 > 执行 > HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > MySQL > 删除** 

附錄 B
客户端实时通软件之联机设定

当您启用 IM Users 后，政策设定允许员工使用 IM 软件。也许有员工向您抱怨无法登入实时通讯软件，此时您可依以下的步骤，解决无法登入的问题。因为 IM 软件往往会自动尝试各种不同的联机方式出去，不会乖乖走您规范的联机方式。当他走非正规联机出去，即会被 InstantScan 阻挡下来，所以您必须引导他们走 InstantScan 规范好的联机方式。

B.1 客户端 MSN 联机设定步骤

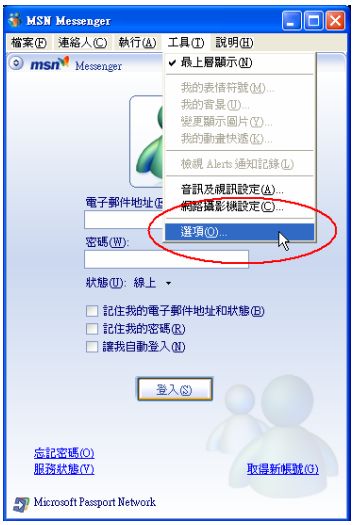
步驟 1. 检查IM Users的设定 检查您是否已经将IM Users启动。然后检查客户端是否被允许使用MSN。是，请进行下一步骤。	**Functions > Management > IM Manager > Status** 
步驟 2. 检阅 Application Firewall 的事件记录 检阅所有Application Firewall的事件记录，确认为何客户端的MSN会被InstantScan阻挡。右图的事件记录告诉您，MSN企图走80埠联机出去，不是MSN正规的1863埠联机方式，所以被挡下来了。	**Functions > Reports > Application Firewall > Event View** 

步骤 3. 教导MSN游戏规则

因为大部分的实时通讯软件会尝试各种联机方式以避开您的控管，所以您可利用InstantScan制定游戏规则，规范每种实时通讯软件。因此，您必须先教导MSN正确的游戏规则。

在客户端计算机的右下角找到MSN 图示，点两下。在MSN工具列上，点选**工具**，选择**选项**。

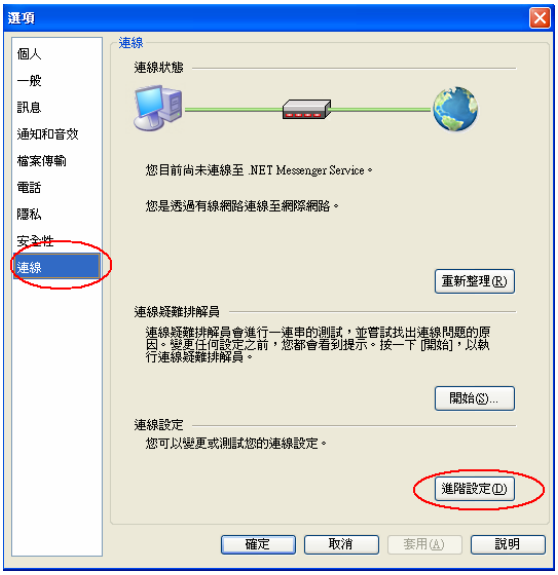
工具 > 选项



步骤 4. 检查MSN联机设定

选择**联机**，然后点击**进阶测试**。

工具 > 选项 > 联机 > 进阶设定

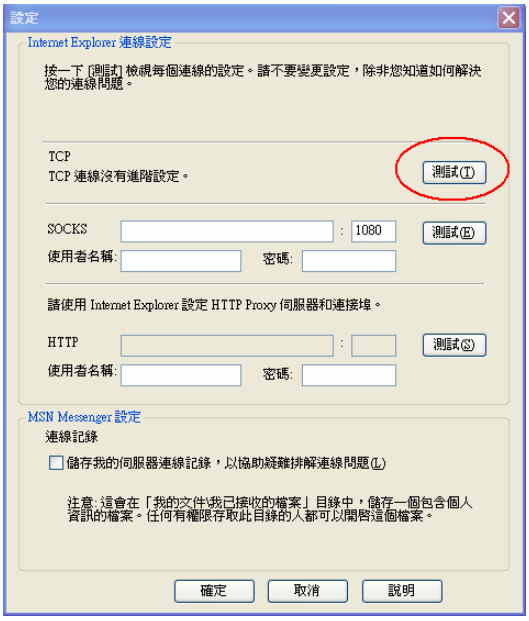


步骤 5. 检查 TCP联机

请注意，只要选择TCP测试。其余SOCKS/HTTP等皆不填写。

点击**测试**来测试联机。

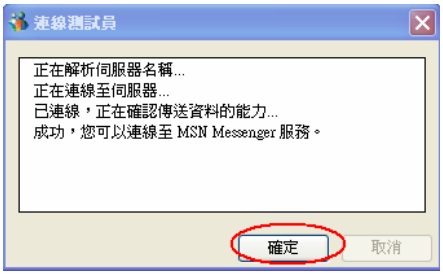
工具 > 选项 > 联机 > 进阶设定 > 测试



步骤 6. 联机测试

当联机测试成功，将出现如右图的画面。

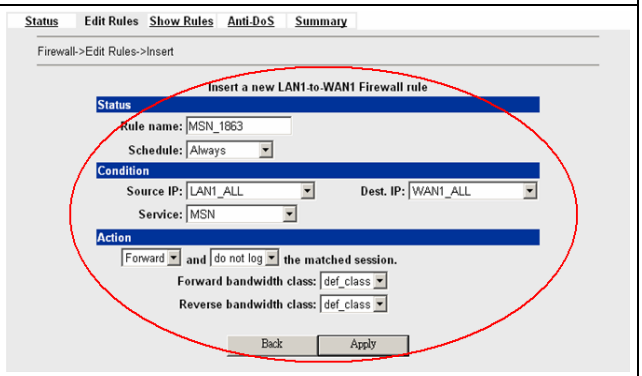
当您再次登入MSN时，它将开始透过1863埠联机出去。



步骤 7. LAN-to-WAN 防火墙规则

检视您的防火墙设定。确认来自LAN-to-WAN方向、服务为MSN (1863埠)的封包是否可顺利通过防火墙。所以，请确认此防火墙的规则是forward的。

右图是以InstantBlock 100为防火墙设定范例。

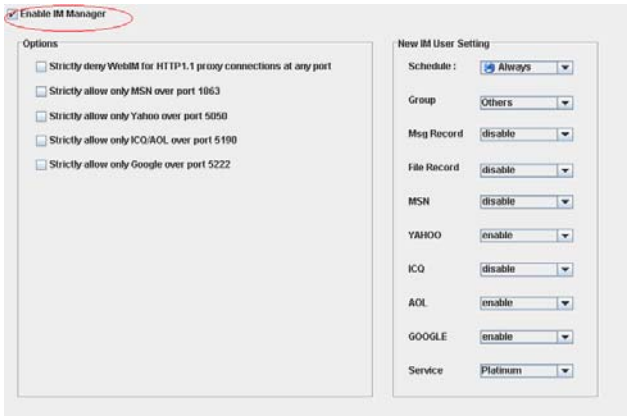


B.2 客户端 Yahoo 联机设定步骤

步骤 1 查IM Manager的设定

检查您是否已经启动IM Users了。是，请继续下一步骤。

Functions > Management > IM Manager > Status



步骤 2 查Application Firewall的事件记录

检查Application Firewall的事件记录，您可以了解为什么某位客户端的Yahoo实时通被InstantScan挡住。由右图的事件记录可知，此客户端的Yahoo企图走80埠联机出去，而非正规的5050埠。

Functions > Reports > Application Firewall > Event View

Date	Application	Description	Protocol	Src IP	Src Port	Dst IP	Dst Port
2006-05-22 15:26:06	yahoo	[BLOCK] Normalization - yahoo	TCP	192.168.17.58	4525	216.155.194.191	80
2006-05-22 15:26:06	yahoo	[BLOCK] Normalization - yahoo	TCP	192.168.17.58	4525	216.155.194.191	80
2006-05-22 15:21:54	msn	[BLOCK] Normalization - msn	TCP	192.168.17.58	4489	65.54.239.211	80
2006-05-22 15:21:54	msn	[BLOCK] Normalization - msn	TCP	192.168.17.58	4489	65.54.239.211	80
2006-05-22 15:21:48	msn	[BLOCK] Normalization - msn	TCP	192.168.17.58	4468	207.68.178.61	80
2006-05-22 15:21:48	msn	[BLOCK] Normalization - msn	TCP	192.168.17.58	4468	207.68.178.61	80

步骤 3 查Yahoo实时通联机

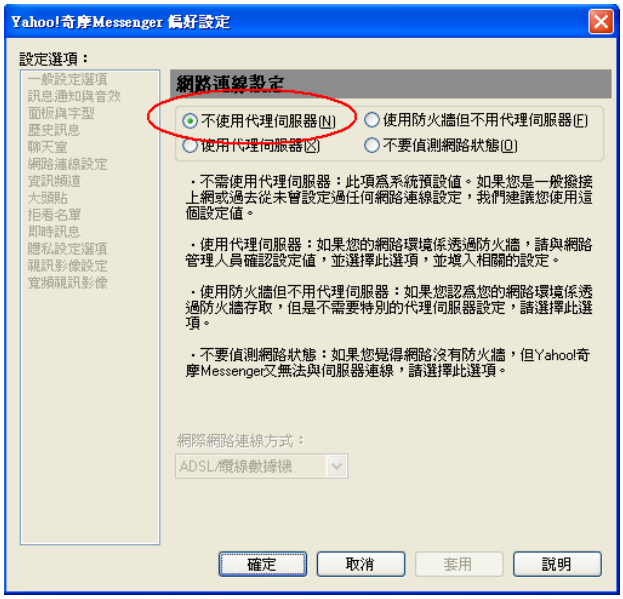
在客户端计算机右下角找到Yahoo实时通的图示，将鼠标移到图标上点两下。在Yahoo实时通工具列上选择**实时通**，然后点选**网络联机设定**。

实时通 > 网络联机设定

步骤 4 选择联机方式

点选**不使用代理服务器**为Yahoo的联机方式。点击**确定**。

实时通 > 网络联机设定 >

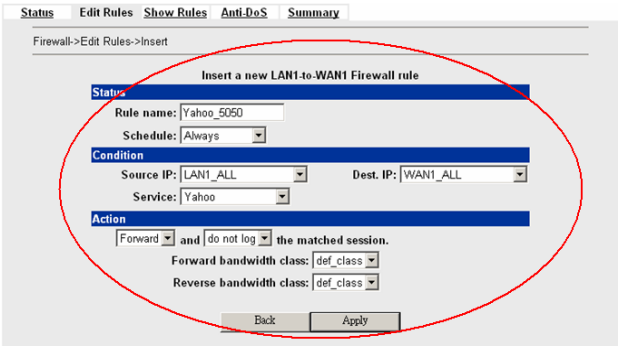


步驟 5 查LAN-to-WAN方向之防火墙规则

检视您的防火墙设定。确认来自LAN-to-WAN方向、服务为Yahoo (5050)的封包是否可顺利通过防火墙。所以，请确认此防火墙的规则是forward的。

右图是以InstantBlock 100为防火墙设定范例。

然后再次尝试登入Yahoo实时通。



附錄 C
Common Line Interface

C.1 CLI 指令清单 - 标准模式

当您透过 console/telnet/SSH 连上 InstantScan，必须使用 CLI 指令来设定 InstantScan。您可依据以下表格所描述的指令来完成 InstantScan 的设定。

非权限模式 Non-privileged mode

主要指令	次要指令	范例	指令说明
?		?	显示所有指令主选单
enable (en)		enable	开启权限模式指令
exit (ex)		exit	离开 CLI 界面
ip			设定相关 IP 参数
	ping	ip ping 202.11.22.33	发送 ICMP 响应需求讯息
	traceroute	ip traceroute 202.11.22.33	追查路由到目的地址所经过的路径
sys			设定系统参数
	status (st)	sys status	显示系统与网络状态
	version (ver)	sys version	显示 InstantScan 韧体版本信息

表格 C□1 标准模式下的非权限模式

注意：如果您不晓得某个指令的参数，您可以在指令后空一格打问号” ?” 例如: “ip ?”。所有ip底下可能的参数就会显示出来。。

权限模式 **Privileged mode**

主要指令	次要指令	范例	指令说明
?		?	显示所有指令的主选单
disable (dis)		disable	关闭权限模式
exit (ex)		exit	离开 CLI 界面
ip			设定相关 IP 参数
	ifset	ip ifset INTF1	显示或变更网络界面设定
	ping	ip ping 202.11.22.33	发送 ICMP 响应需求讯息
	set	ip set	设定 InstantScan 相关 IP 地址
	show	ip show	显示所有网络设定
	tftp (upgrade)	ip tftp upgrade image <FILENAME> 192.168.168.170.	从 tftp 服务器处升级韧体
	traceroute	ip traceroute 202.11.22.33	追查路由到目的地址所经过的路径
sys			设定系统参数
	date	sys date	显示/设定目前系统时间
	halt	sys halt now	关机
	highavail	sys highavail set	High-Availability 相关参数设定
	module	sys module	更新/还原系统模块设定
	password	sys password	变更管理员密码
	reboot	sys reboot now	重开机
	resetconf	sys resetconf now	重设系统设定文件成出厂默认值
	sessionlog	sys ressionlog on	Session 记录的设定
	showmac	sys showmac	显示网络卡的 MAC 地址
	status (st)	sys status	显示系统状态
	tcpdump	sys tcpdump management	倾印 (dump) 流经的封包
	uptime	sys uptime	显示 InstantScan 正常运作的时间
	version (ver)	sys version	显示 InstantScan 韧体版本

表格 C 2 标准模式下的权限模式

完整的 sys module 与 ip tftp upgrade 指令，请参阅下表。

前缀指令	第二指令	第三指令	字尾指令	范例	指令说明
sys	module	flushstate	--	sys module flushstate	手动清除系统内闲置不用的联机
		query	--	sys module query	询问模块版本
		restore	all	sys module restore all	复原系统应用程序行为/特征码/病毒数据库
			av	sys module restore av	复原系统病毒和蠕虫数据库
			pattern	sys module restore pattern	复原系统应用程序行为
			signature	sys module restore signature	复原系统特征码
		setting	set	sys module setting set	更改更新服务器设定
			show	sys module setting show	显示更新服务器设定
		update	all	sys module update all	更新系统应用程序行为/特征码/病毒数据库
			av	sys module update av	更新系统病毒和蠕虫数据库
			pattern	sys module update pattern	更新系统应用程序行为
			signature	sys module update signature	更新系统特征码
ip tftp	upgrade	firmware	FILENAME tftp server IP address	ip tftp upgrade firmware <FILENAME> 192.168.168.170	从 tftp 服务器处升级韧体
		image	FILENAME tftp server IP address	ip tftp upgrade image <FILENAME> 192.168.168.170	从 tftp 服务器处升级 image 檔
		module	FILENAME tftp server IP address	ip tftp upgrade module <FILENAME> 192.168.168.170	从 tftp 服务器处升级系统模块

表格 C 3 Sys module 与 IP tftp 指令说明

完整 sys highavail 指令，请参阅下表。

前缀	第二指令	第三指令	第四指令	字尾指令	范例	指令说明
Sys	Highavail	set	(mode)	1 Active-Active 2 Active-Standby	2	设定 High-Availability 的模式
			(node)	Internal-Ping-Nodes External-Ping-Nodes	192.168.168.100 140.113.1.1	设定系统外 ping 或内 ping 的节点(public 或 private IP)
			(type)	1. master 2. slave	1	设定 High-Availability 类型
			(vip)	N/A	192.168.168.100	显示/设定 High-Availability 的虚拟 IP 地址
		status	N/A	N/A	sys highavail status	显示 High-Availability 的状态

表格 C 4 Sys highavail 指令说明

IP TFTP upgrade **字尾指令意义如下：**

WORD： tftp 服务器 IP 地址

FILENAME： 升级设定档或韧体的 image 文件名称

完整 sys sessionlog 指令，请参阅下表。

前缀指令	**第二指令**	**第三指令**	**字尾指令**	**范例**	**指令说明**
sys	Sessionlog	off	--	sys sessionlog off	关闭系统记录
		on	--	sys sessionlog on	启用系统记录
		status	--	sys sessionlog status	系统记录状态

表格 C 5 sys tcpdump 指令说明

完整 sys tcpdump 指令，请参阅下表。

前缀指令	第二指令	第三指令	字尾指令	范例	指令说明

sys	tcpdump	external	dump	sys tcpdump external dump	倾印流经 external 端的封包
			interactive	sys tcpdump external interactive	依交谈模式列举流经 external 端的封包
		internal	dump	sys tcpdump internal dump	倾印流经 internal 端的封包
			interactive	sys tcpdump internal interactive	依交谈模式列举流经 internal 端的封包
		management	dump	sys tcpdump management dump	倾印流经 management 端的封包
			interactive	sys tcpdump management interactive	依交谈模式列举流经 management 端的封包

表格 C 6 sys tcpdump 指令说明

C.2 CLI 指令清单 - 救援模式

如果原始韧体因某些意外而损毁，您需要利用救援模式将韧体回复到出厂默认值。将 InstantScan 重新开机后，在 5 秒钟的倒数程序内按 <ctrl> + e 键，请输入 admin 后进入救援模式。

非权限模式 Non-privileged mode

主要指令	次要指令	范例	指令说明
?		?	显示所有指令主选单
enable (en)		enable	开启权限模式指令
exit (ex)		exit	离开 CLI 界面
ip			设定相关 IP 参数
	ping	ip ping 202.11.22.33	发送 ICMP 响应需求讯息
	traceroute	ip traceroute 202.11.22.33	追查路由到目的地址所经过的路径
sys			设定系统参数
	date	sys date	显示目前系统时间

表格 C 7 救援模式之非权限模式

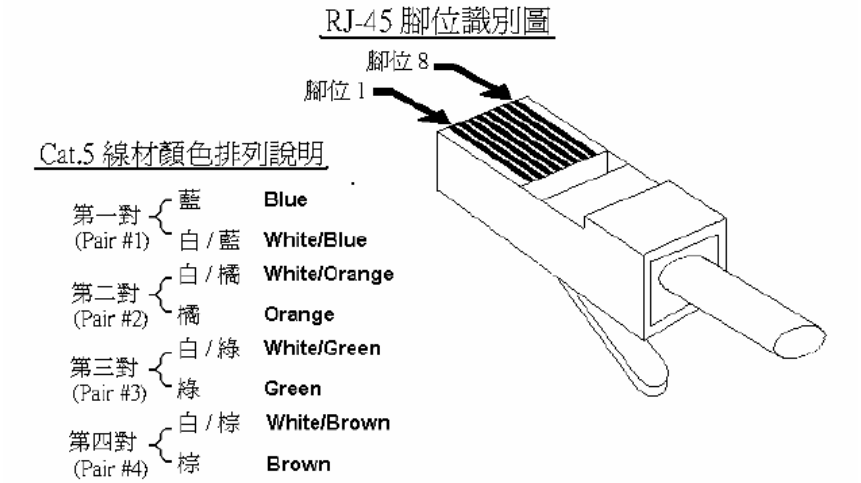
权限模式 Privileged mode

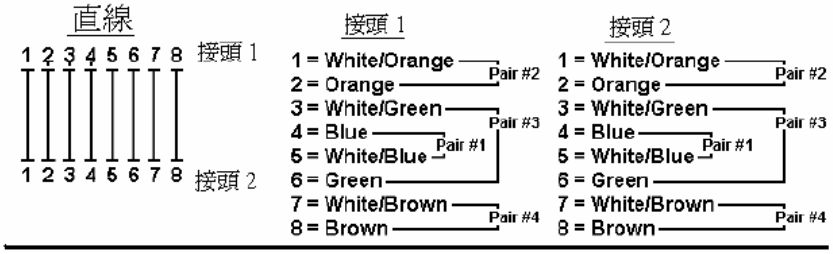
主要指令	次要指令	范例	指令说明
?		?	显示所有指令主选单
disable (dis)		disable	关闭权限模式
exit (ex)		exit	离开 CLI 界面
ip			设定相关 IP 参数
	ping	ip ping 202.11.22.33	发送 ICMP 响应需求讯息
	set	ip set	设定 InstantScan 的 IP 地址
	show	ip show	显示所有网络设定
	tftp (upgrade)	ip tftp upgrade image <FILENAME> 192.168.168.170.	从 tftp 服务器处升级韧体 (相关设定与标准模式同)
	traceroute	ip traceroute 202.11.22.33	追查路由到目的地址所经过的路径
sys			设定系统参数
	date	sys date	显示目前系统时间
	halt	sys halt now	关机
	reboot	sys reboot now	重开机
	resetconf	sys resetconf now	重设系统设定文件成出厂默认值
	resetpasswd	sys resetpasswd	变更管理员密码
	showmac	sys showmac	显示网络卡的 MAC 地址
	uptime	sys uptime	显示 InstantScan 正常运作的时间

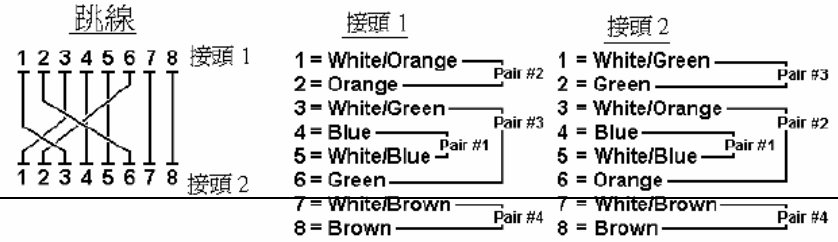
表格 C 8 救援模式之权限模式

附錄 D
RJ-45 连接头标准排列方式

本附录将为您说明以太网络RJ-45 连接头标准排列方式 (EIA 568A/B)







附錄 E
技术支持

利基网络尽可能提供详细的文件以供您安装与设定您所购买的InstantScan产品。这些文件能帮助您瞭解本产品的功能与设定步骤。您亦可从利基网络网页 http://www.L7-Networks.com 下载相关产品的文件与数据。

如果您对InstantScan产品有任何技术上的问题或建议，请洽询利基网络技术支持中心。当您洽询技术支持的同时，请您务必准备好以下信息，以节省您与技术人员沟通的时间：

1. 产品机种与序号
2. 保固期间
3. 您收到本产品的日期
4. 简述产品的问题与您曾尝试解决的步骤

聯絡方法 / 位置	电子邮件	电话 传真	住址
台湾新竹	FAE@L7-Networks.com	+886-3-666-8896 +886-3-666-8895	利基网络股份有限公司 新竹科学工业园区园区二路20号1楼 L7 Networks Inc. (Headquarters) 1F,No.20, Park Ave. II Rd., Science-based Park, Hsinchu, Taiwan 300
日本东京	FAE@L7-Networks.com	+81-3-5434-9678 +81-3-5434-9686	Alphasolutions Co., Ltd. 10F 8-8-5 Nishigotanda, Shinagawa-ku, Tokyo 141-0031, Japan
美国 Santa Clara	FAE@L7-Networks.com	+1-408-844-8850 +1-408-844-8841	Alpha Networks Inc. 3945 Freedom Circle, Suite 1150 Santa Clara, CA 95054, USA