*i*STAR™ UU200 使用手冊

Release 2.5

UUDynamics, Inc.

2005 年 1 月

本書約定

描述：

文檔中對軟體中不同類型的元素，使用不同的符號和樣式進行描述（請參見下表）。請讀者使用本手冊之前務必認真閱讀，以便區分。

元素	符號&樣式	字型大小	舉例	備註
按鈕	< >	五號	<確定>	
功能表、快顯功能表	“”	五號	“文件”	
超鏈結	帶下劃線字體	五號	下一步	
參數	[]	小五號	https://[*uuswitch 的 IP 地址*](或[*uuswitch 的 DNS 名稱*])	
螢幕回顯	斜體	小五號	*ErrorCode[11001]:認證失敗*	[]符號外部的內容，爲出錯提示，供使用者參考。[]內部的內容，爲系統內部資訊，供開放人員跟蹤。使用者可以不予理會，如有需要，亦可將其告知我公司技術支援人員。
重要、說明	加粗	五號	i 重要、**&** 說明	

解析度：

運行本產品，建議使用 800×600 或 1024×768 解析度，以獲得最佳視覺效果。

目 錄

第1章 *i*STAR™產品概述

感謝您使用 UUDynamics 公司 ***i*STAR™**系列產品。***i*STAR™** UU200 是 UUDynamics 公司的一種伺服器版本發布單元（Publisher）。

本使用手冊將對 ***i*STAR™**產品的功能特性及系統架構進行簡要描述，幷在後面章節詳細介紹 UU200 的安裝、設定與操作步驟。

1.1 *i*STAR™產品功能特性

***i*STAR™**（**I**nstant **S**ecure **T**unnel **Ar**chitecture）是 UUDynamics 公司首創的新一代安全 Instant Extranet 技術。

i*STAR™**用於構建由“發佈單元(Publisher)”向“使用者端(Subscriber)”發佈應用程式的 Extranet，這種方式能快速且安全地解決特定應用程式跨越企業網路和組織邊界的問題。i*STAR™**技術提供了基於“使用者端（Subscriber）”、 “發佈單元（Publisher）”和“交換單元(UUSwitch/UUExchange) ”的安全資訊網路模型，爲現代企業使用者和應用服務提供商（ASP）提供了應用程式或文件存取的發布、控制和管理平臺。同時，它涵蓋了傳統 VPN 的所有功能，爲現代企業網的 Intranet、Extranet、Remote Access、Application Export 等提供了安全、高效的整體解決方案；***i*STAR™**還能快速實現企業與其分支機搆和商業夥伴之間的 B2B、供應鏈、分散式 OA 等電子業務的需求。

1.2 *i*STAR™產品系統架構

***i*STAR™**的系統結構如下圖所示：

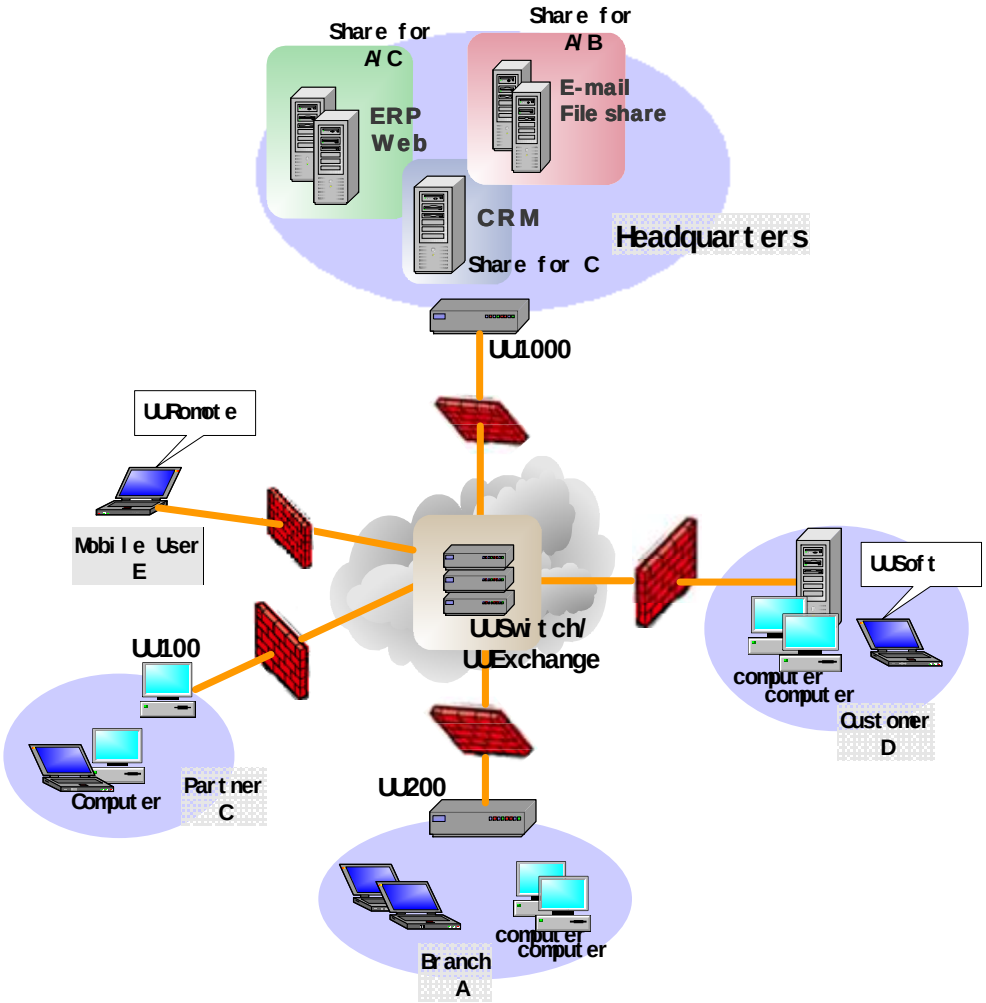


圖 1

如上圖所示，公司總部（headquarter）、合作夥伴(Partner)、分支機構(Branch)和移動使用者(Customer)間建立 ***i*STAR™**系統結構，分別以 UU200、UU100、UU1000 和中間的 UUSwitch/UUExchange 連接建立安全隧道；公司總部發布共用的應用給特定使用者，合作夥伴、分支機構等使用該些應用，從而實現了 Instant Extranet。UU1000/UU200/UU100 均具備發布單元的功能；個人使用者單元通過 IE/HTTPS 與伺服器相連接。***i*STAR™**技術中主要構成元件簡要介紹如下。

交換單元(UUSwitch/UUExchange)

UUSwitch/UUExchange 是 ***i*STAR™**系統結構的中心，它類似於電話系統中的交換中心，是高效的、均衡負載的伺服器群集或群集組，它負責維護著合法使用者資料庫，具有 Public Static IP 位址，在兩方進行應用資料交換之前提供“信令交換”的功能；UUSwitch/UUExchange 能物理上分佈在多個地點上，透明地轉發應用資料。

發佈單元（Publisher）

發佈單元（Publisher）UU100/UU200/UU1000 位於 ***i*STAR™**中發布應用的伺服器端，它可以將伺服器提供的服務安全的發布。

使用者端（Subscriber）

使用者端通過 IE/HTTPS 與伺服器相連接。

Registration (Logical naming)

每個發佈單元 Publisher 都必須配置成能夠到達 UUExchange，并且都有一個唯一的邏輯名字 UUID，在啓動時就用這個邏輯名字註冊到 UUSwitch/UUExchange,從而成爲整個 ***i*STAR™**的一部分。所以發布單元本身不一定需要 Public Static IP 位元元址。

End to End Security Connectivity

資訊安全的含義主要包含以下幾個方面：使用者端和伺服器端的認證、資訊的私密性、資訊的完整性和授權。***i*STAR™**結構中的發佈單元和使用者單元之間的隧道是基於 SSL 的安全連接，同時滿足以上幾個方面，實現端到端的安全。

第2章 系統安裝

2.1 安裝硬體

1. 設備外觀

UU200 產品包含硬體、軟體兩部分。您可以依照以下步驟進行安裝：

設備的外觀如下圖 2 所示：

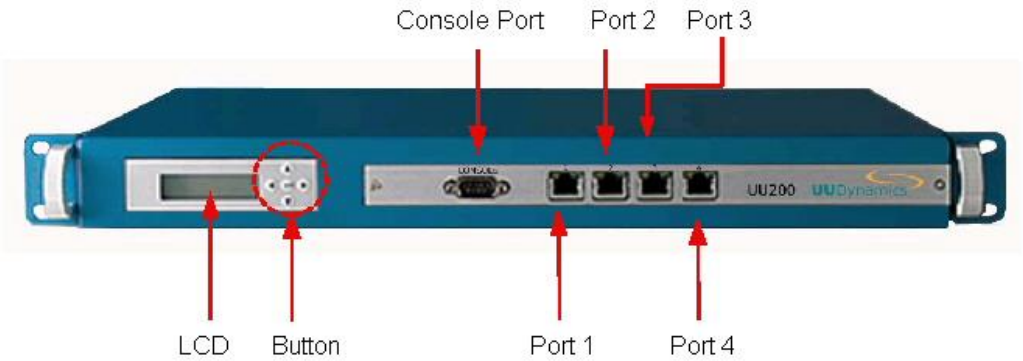


圖 2

正面從左到右爲：

Ÿ LCD 顯示螢幕：分兩行顯示 *i*STAR 底層重要的資訊。例如連接狀態、CPU 狀態、告警等。

顯示位置	回顯內容	說明
Line1	CPU 及 Memory 使用情況。	總是顯示。

Line2	正常情況下顯示連接狀態。 異常情況下顯示告警資訊。 **連接狀態**包括： Ready/ Not ready; Register/ Unregister; **告警資訊**包括： MemoryShortage CPUOverload InvalidLicense WrongSoftware IPConllision	**Ready（/ Not ready）**：連接方式爲 Direct Access 時，顯示 UU200 是否聯機。UU200 連接方式的說明請參考“術語表”。 **Registered（/Unregistered）**：連接方式爲 Private Access 時，顯示 UU200 是否成功註冊上指定的 UUSwitch（/UUExchage）。 **MemoryShortage**：當記憶體極值（threshold）達到 98%時顯示。 **CPUOverload**：當 CPU 極值（threshold）達到 80%時顯示。 **InvalidLicense**：當 license 不夠、不一致或過期時。 **WrongSoftware**：當安裝了錯誤的軟體（例如 UUSwitch 軟體）時顯示。 **IPConllision**：IP 位址和內網位址或外網位址發生衝突時顯示。

- 按鈕：共五個。（目前暫不使用）
- Console 埠：在初始化時使用。 通過 NULL Modem 線與配置電腦相連接 (串列傳輸速率：38400，校驗：N，資料位置：8，停止位置：1，資料流程控制：N)
- 乙太埠：共 4 個。

  埠“1”：爲預設的本地配置埠，首次安裝或恢復原廠設置時，應使用交叉綫連接該埠。進行配置。

  透明模式和路由模式下，該埠可用於連接 UU200 對內的網路，也可於連接叢集（Cluster）中的各台 UU200。（各模式的詳細說明，請參見“術語表”章節。）

  埠“2”：可在配置介面中啓用，用於進行本地配置（使用交叉綫連接）。一旦啓用該埠，埠“1”的本地配置功能即失效。

  埠“3”： 可在配置介面中啓用，用於連接叢集（Cluster）中的各台 UU200。一旦啓用該埠，則埠“4”的這一功能失效。

  埠“4”： 在單模式和透明模式下，可用於連接叢集（Cluster）中的各台 UU200。

  在透明模式和路由模式下，該埠用於連接 UU200 對外的網路；

背面爲：

- 電源線接頭
- 電源開關

2. 設備附件

- 電源線、NULL Modem 線、RJ-45 交叉線、CAT-5 UTP 網路線
- 用來配置 UU200 用的電腦一台（以下簡稱配置電腦）
  - i. 具備 10M/100M 乙太網卡
  - ii. 具備 Microsoft Internet Explorer 瀏覽器 5.0 版或以上
  - iii. 建議使用解析度爲 1024×768 的監視器

3. 硬體安裝。

您可以依照以下步驟進行安裝：

① 連接 *i*STAR 硬體產品的電源線，(可以使用 110V/220V 電源)；

② 用 RJ-45 交叉線將配置電腦的乙太網路埠，連接到 *i*STAR 標示“1”的乙太網路埠；

③ 啓動 *i*STAR 電源；

& 說明：

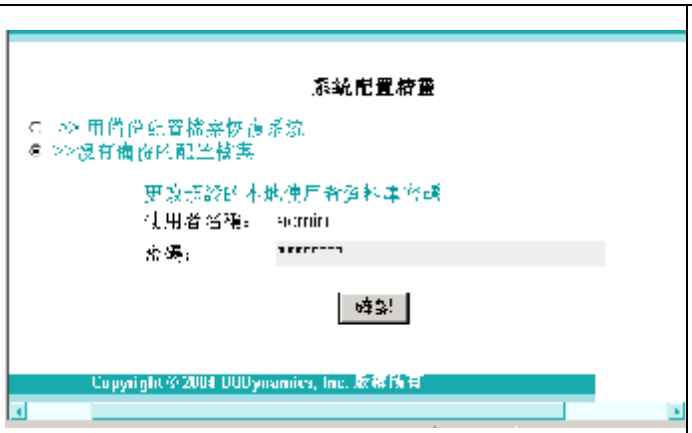
*i*STAR 的出廠預設 IP 位址是“1.1.1.1”，子網路遮罩是 255.255.255.0。

④ 啓動您設定電腦上的 Command Prompt，輸入“*ipconfig /renew*”，待獲得了 1.1.1.2 的位址之後，便可以繼續下面的步驟

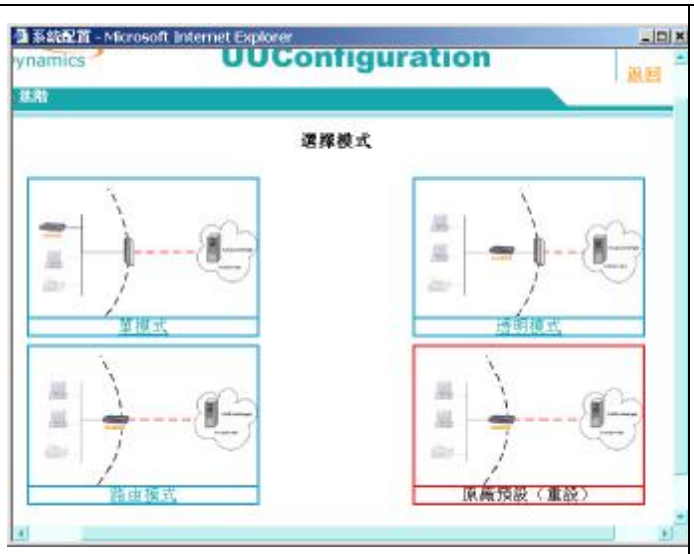
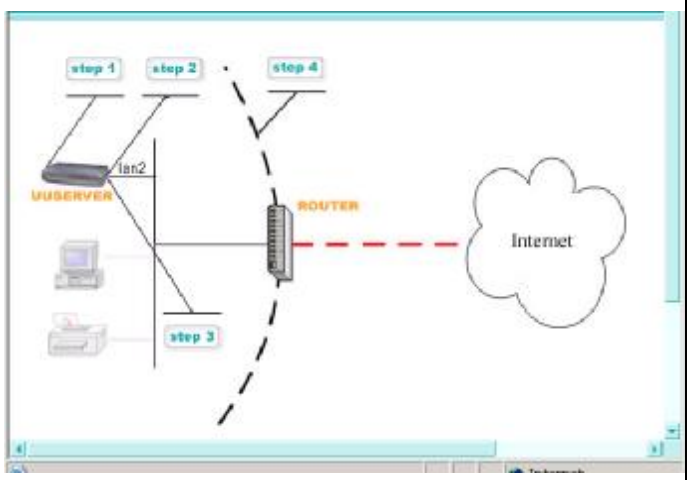
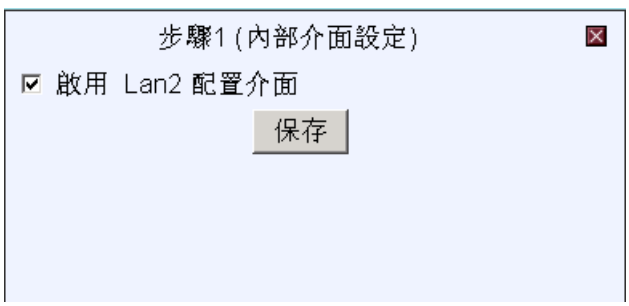
⑤ 啓動配置電腦的 IE 瀏覽器，開始安裝軟體。

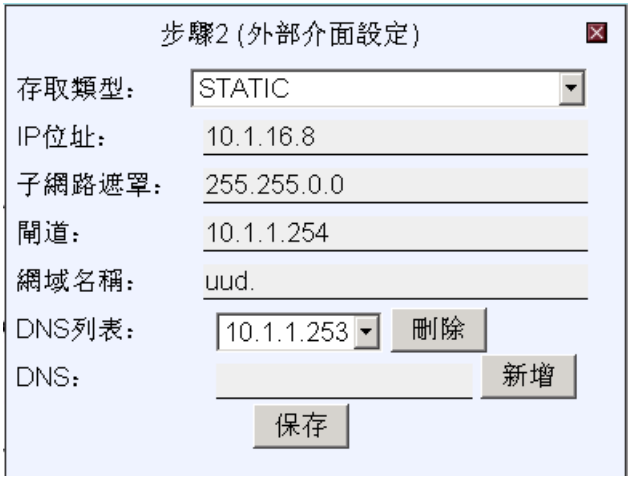
2.2 安裝軟體

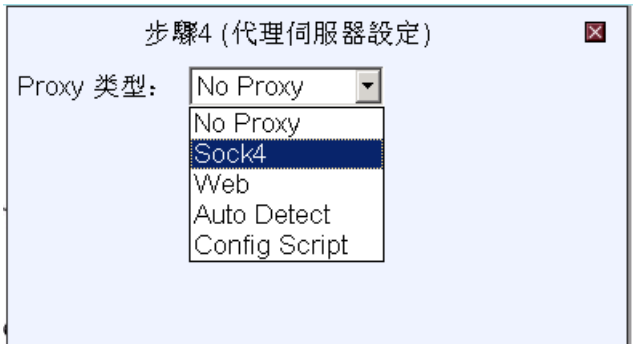
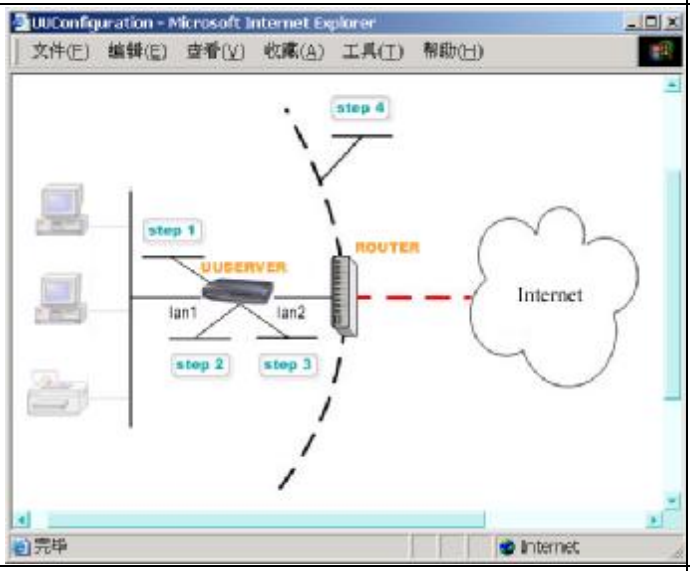
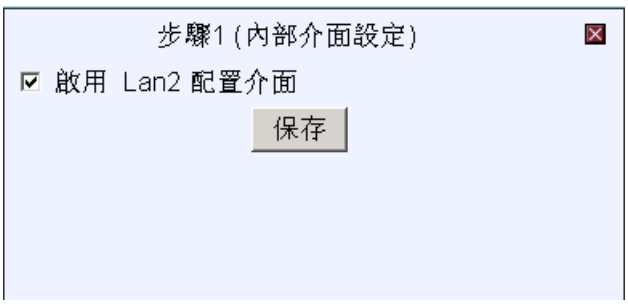
步驟序號	介面	步驟描述
A 開始配置		
A-1		請在 IE 瀏覽器位址欄輸入“http://1.1.1.1/admin”，在彈出的視窗介面中輸入使用者名稱和密碼（兩者都是“admin”），按鍵盤上的 **Enter** 鍵或點選介面中的<確認>按鈕，進入系統配置導引精靈。

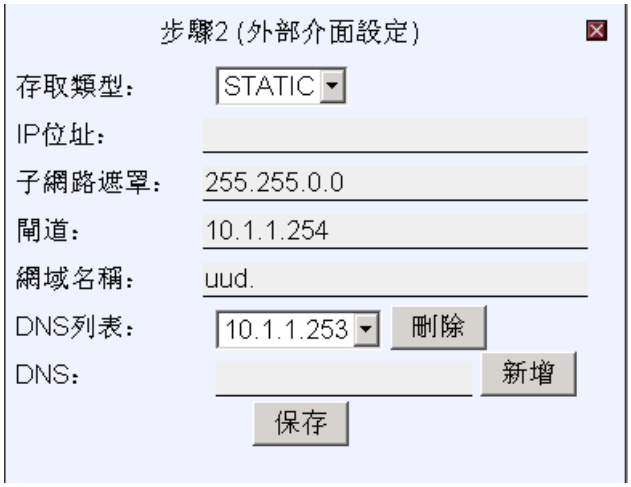
<table>
<tr><td>A-2</td><td>  </td><td>選擇是否重載以前的配置檔案。
Ÿ 如果是初次安裝或者沒有 UU200 的配置備份檔案，請選擇“沒有備份的配置檔案”選項；
Ÿ 如果您要恢復以前備份的 UU200 的配置，請選擇“用備份配置文件恢復系統”；
爲保護系統安全，請立即修改預設的管理員密碼。
點選下一步進入連接方式的配置。</td></tr>
<tr><td colspan="3">B 選擇使用者和 UU200 的連接方式</td></tr>
<tr><td>B-1</td><td>  </td><td>選擇 UU200 支援的連接方式，配置精靈會自動跳轉到該方式下的設定介面，如：
B-2： Direct Access 方式
使用者通過 UU200 的公共 IP 位址，直接存取 UU200 發布的資源。
B-3： Private Access 方式
使用者通過 UUSwitch（/UUExchange）的公共 IP 位址，結合 UU200 的 UUID，定位 UU200 幷存取 UU200 發布的資源。</td></tr>
<tr><td>B-2</td><td>  </td><td>“Direct Access”方式：
Ÿ 如果您需要匯入準備好的第三方的電子憑證。請點擊<輸入>鍵，在下一個介面中輸入另購的第三方電子數位憑證。
Ÿ 如果使用 UUDynamics 公司提供的預設的電子憑證，則請點擊<生效>繼續其他配置。</td></tr>
</table>

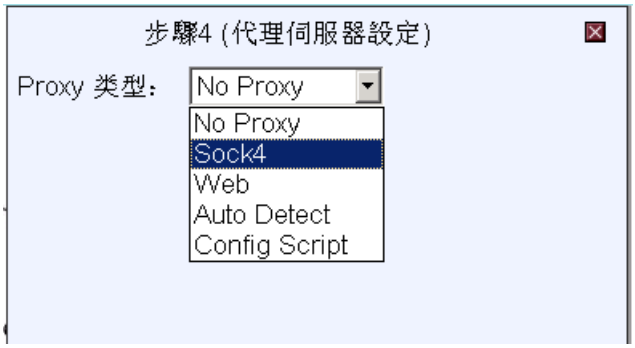
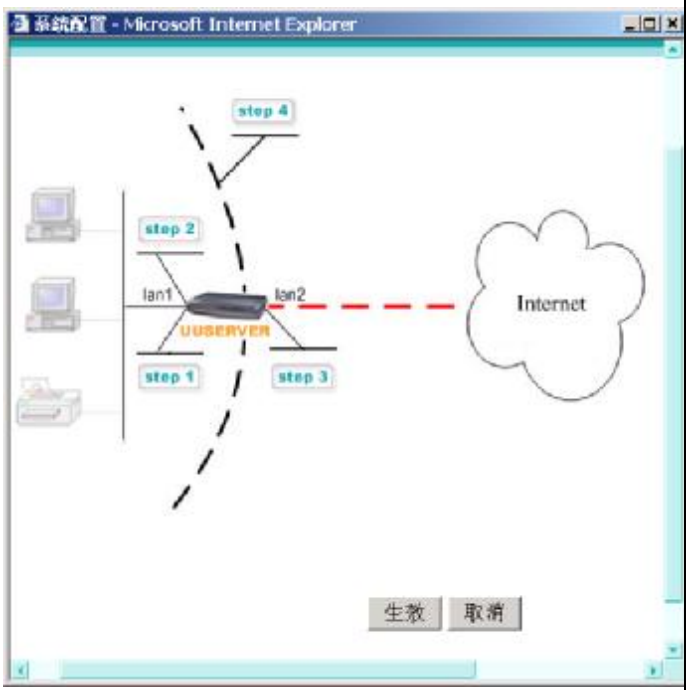
B-2-a		輸入該證書對應的 Key 檔案，證書檔案和 CA 的證書檔案，所有檔案要求是 Base64 編碼方式。 點擊<更新>，返回上層頁面。 **說明**： 第三方電子憑證的更多資訊請參見“術語表”。
B-3		**“Private Access”方式：** 點擊<輸入>,導入 UUID 檔案。(見 B-3-a) 輸入 UUSwitch/UUExchange 的 IP 位址或 DNS 名稱。 最後按<下一步>鍵，使當前的連接模式設定生效。
B-3-a		點擊<瀏覽>,導入 UUID 檔案，(這裏的 UUID 檔案由在這裏輸入的 UUSwitch/UUExchange 產生得到)。 如果該 UUID 文件有密碼保護，請先勾選“密碼”,並輸入密碼。 點擊<更新>,確認幷返回上一介面。
C 選擇 UU200 在網路中的放置地址		

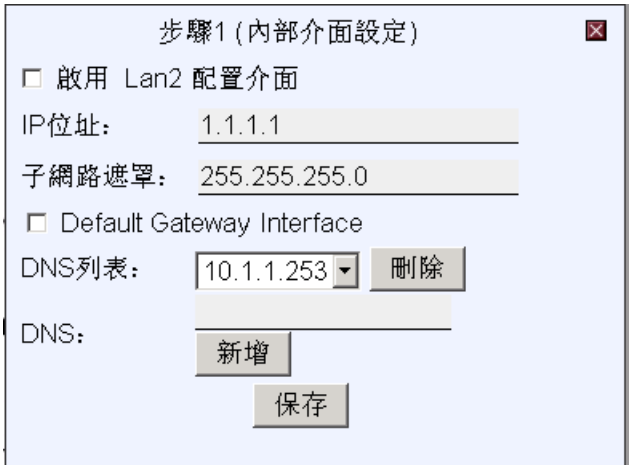
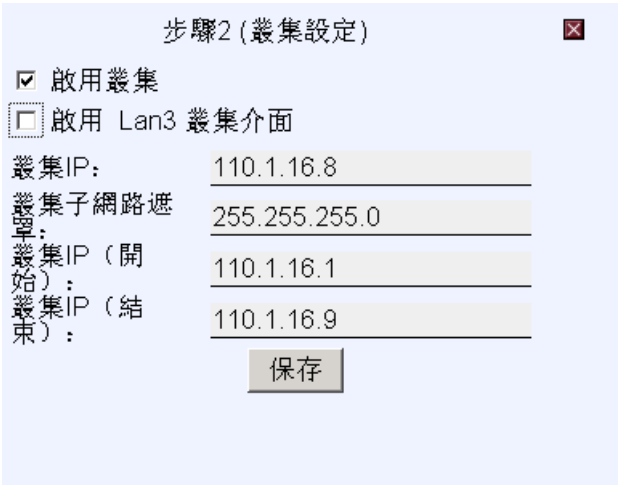
C-1		根據您在安裝準備階段預先確定的網路模式，在“單模式”、“路由模式” 和“透明模式”三種模式中選擇，配置精靈會自動跳轉到該模式下的網路設定介面，進行網路各種參數的設定。如： C-2：**錯誤! 找不到參照來源。** C-5：**錯誤! 找不到參照來源。** C-9：**錯誤! 找不到參照來源。** 點選預設出廠（重設），幷提供正確的管理員密碼後，可以恢復至出廠時的預設模式，重新設定各種參數。 **說明；** 三種模式詳細說明請參見“術語表”。
C-2		**單模式下的網路設定：** **說明：** 在網路基礎設定已完成幷生效後，當系統管理員重新進入此設定步驟，選上“啓用系統恢復”幷在“在 □ 分鐘之內”設定相應的時間（如 5 分鐘），表示如果在 5 分鐘內，無法連接到 UUSwitch/UUExchange，網路設定將自動恢復爲原來（改變前）的網路設定。
C-2-a		點選“步驟 1”。設定是否啓用 UU200 上標示爲“2”的埠作爲配置埠。 如果不啓用，則仍使用預設的埠“1”作爲配置埠。

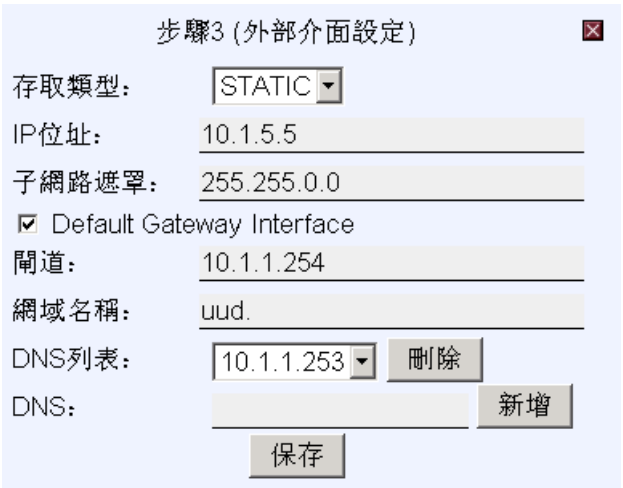
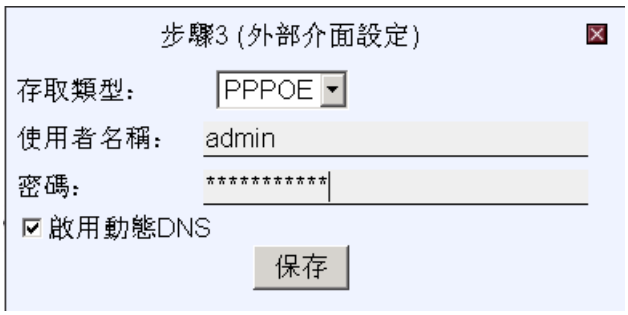
C-2-b		點選“步驟 2”， 配置本台 UU200 的訪問類型。“訪問類型”表示 UU200 接入網路的類型。 l 訪問類型設定爲“STATIC”時，開啓左圖所示介面：該台 UU200 的 IP 地址被指定。 選擇本台電腦的“適配器名稱”。UU200 的 IP 位址、對應的子網路遮罩、閘道及 DNS 等參數會自動從系統讀取。按<保存>儲存。
C-3		在 C-2 所示介面上，點選“步驟 3”進行叢集的設定。UU200 能夠以叢集的方式進行均衡負載。 n 勾選“啓用叢集”表示啓用叢集； 1. 輸入叢集 IP、及對應的叢集子網掩碼； 每一台被叢集的 UU200 需要一個專用的靜態 IP 位址，稱爲叢集 IP，一般爲 Private IP。 系統管理員可以自由設定這些叢集 IP，但同一個叢集的 UU200 必須位於同一個子網路。 2. 輸入叢集 IP（開始）、叢集 IP （結束）資訊； 這是用於描述同一個叢集 UU200 的 IP 位址範圍。 3. 輸入完畢後按<保存>進行儲存 n 勾選“啓用 Lan3 叢集介面”表示啓用標示爲“3”的埠作爲叢集的埠； **說明：** 詳細的叢集的說明請參考“術語表”。

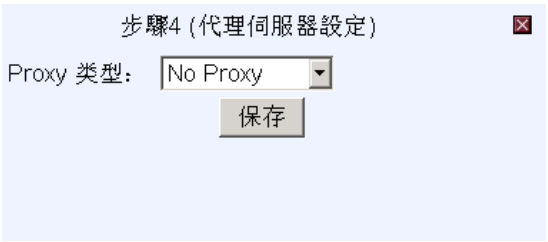
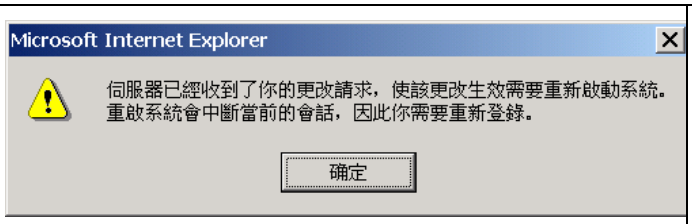
C-4		在 C-2 所示介面上，點選“步驟 4”進行代理伺服器的設定,預設爲“No Proxy”。 **說明：** 這裏的代理伺服器設定和 IE 的代理伺服器設定相似。 No Proxy：表示沒有代理伺服器,使用 NAT 或 Public IP 直接上網； Web：表示有 Web Proxy； SOCK4：表示有 SOCK4 Proxy； SOCK5：表示有 SOCK5 Proxy； AutoDetect：表示自動查找 Proxy 設定； Config Script：表示根據 config Script 來設定代理伺服器。
C-5		**透明模式下的網路設定：** **說明：** 在網路基礎設定已完成幷生效後，當系統管理員重新進入此設定步驟，選上“啓用系統恢復”幷在“在 □ 分鐘之內”設定相應的時間（如 5 分鐘），表示如果在 5 分鐘內，無法連接到 UUSwitch/UUExchange，網路設定將自動恢復爲原來（改變前）的網路設定。
C-6		點選“步驟 1”。設定是否啓用 UU200 上標示爲“2”的埠作爲配置埠。 如果不啓用，則仍使用預設的標示爲“1”的埠作爲配置埠。

C-6-a		點選“步驟 2”，配置本台 UU200 的訪問類型、IP 位址、及對應的子網掩碼、閘道、DNS 等參數。 l “訪問類型”表示 UU200 接入網路的類型。訪問類型爲“STATIC”,開啓左圖所示介面。指定該台 UU200 的外網 IP 位址以便外部網用戶訪問。選擇本台電腦的“適配器名稱”。UU200 的 IP 位址、對應的子網路遮罩、閘道及 DNS 等參數會自動從系統讀取。按<保存>儲存。
C-7		在 C-5 所示介面上，點選“步驟 3”進行叢集的設定。UU200 能夠以叢集的方式進行均衡負載。 n 勾選“啓用叢集”表示啓用叢集； 1. 輸入叢集 IP、及對應的叢集子網掩碼； 每一台被叢集的 UU200 需要一個專用的靜態 IP 位址，稱爲叢集 IP，一般爲 Private IP。 系統管理員可以自由設定這些叢集 IP，但同一個叢集的 UU200 必須位於同一個子網路。 2. 輸入叢集 IP(開始)、叢集 IP（結束）資訊； 這是用於描述同一個叢集 UU200 的 IP 位址範圍。 4. 輸入完畢後按<保存>進行儲存 n 勾選“啓用 Lan3 叢集介面”表示啓用標示爲“3”的埠作爲叢集的埠； **說明：** 詳細的叢集的說明請參考“術語表”。

C-8		在 C-5 所示介面上，點選“步驟 4”進行代理伺服器的設定，預設爲“No Proxy”。 **說明：** 這裏的代理伺服器設定和 IE 的代理伺服器設定相似。 No Proxy：表示沒有代理伺服器,使用 NAT 或 Public IP 直接上網； Web：表示有 Web Proxy； SOCK4：表示有 SOCK4 Proxy； SOCK5：表示有 SOCK5 Proxy； AutoDetect：表示自動查找 Proxy 設定； Config Script：表示根據 config Script 來設定代理伺服器。
C-9		**路由模式下的網路設定：** **說明：** 在網路基礎設定已完成并生效後，當系統管理員重新進入此設定步驟，選上“啓用系統恢復”并在“在 □ 分鐘之內”設定相應的時間（如 5 分鐘），表示如果在 5 分鐘內，無法連接到 UUSwitch/UUExchange，網路設定將自動恢復爲原來（改變前）的網路設定。

C-9-a		點選“步驟 1”。 Ÿ 設定是否啓用 UU200 上標示爲“2”的埠作爲配置埠。 如果不啓用，則仍使用預設的標示爲“1”的埠作爲配置埠。 Ÿ 設定是否以該配置埠的 IP 作爲預設的閘道地址。 **說明：** 配置埠（埠“1”或“2”）和埠“4”，只能有一個被用作預設的閘道。
C-10		在 C-9 所示介面上，點選“步驟 2”進行叢集的設定。UU200 能夠以叢集的方式進行均衡負載。 **n** 勾選“啓用叢集”表示啓用叢集； 1. 輸入叢集 IP、及對應的叢集子網掩碼； 每一台被叢集的 UU200 需要一個專用的靜態 IP 位址，稱爲叢集 IP，一般爲 Private IP。 系統管理員可以自由設定這些叢集 IP，但同一個叢集的 UU200 必須位於同一個子網路。 2. 輸入叢集 IP（開始）、叢集 IP （結束）資訊； 這是用於描述同一個叢集 UU200 的 IP 位址範圍。 3. 輸入完畢後按<保存>進行儲存 **n** 勾選“啓用 Lan3 叢集介面”表示啓用標示爲“3”的埠作爲叢集的埠； **說明：** 詳細的叢集的說明請參考“**錯誤! 找不到參照來源。**設定叢集分攤負載”。

C-10-a		在 C-9 所示介面上，點選“步驟 3”。 1. 配置本台 UU200 的訪問類型： “訪問類型”表示 UU200 接入網路的類型。訪問類型爲“STATIC”,開啓左圖所示介面。 指定該台 UU200 的 IP 地址。幷選擇本台電腦的“適配器名稱”。UU200 的 IP 位址、對應的子網路遮罩、閘道及 DNS 等參數會自動從系統讀取。按<保存>儲存。 2. 設定是否以埠“4”的 IP 作爲預設的閘道地址： **說明：** 配置埠（埠“1”或“2”）和埠“4”，只能有一個被用作預設的閘道。
C-11		選用連接方式爲“Private Access”時，可以啓用這種方式，需要設定使用者名及密碼。

C-12		在 C-9 所示介面上，點選“步驟 4”進行代理伺服器的設定,預設爲“No Proxy”。 **說明：** 這裏的代理伺服器設定和 IE 的代理伺服器設定相似。 No Proxy：表示沒有代理伺服器,使用 NAT 或 Public IP 直接上網； Web：表示有 Web Proxy； SOCK4：表示有 SOCK4 Proxy； SOCK5：表示有 SOCK5 Proxy； AutoDetect：表示自動查找 Proxy 設定； Config Script：表示根據 config Script 來設定代理伺服器。
D 完成		
D-1		在 C-2 介面上，點擊<生效>,使網路設定生效。點擊<確定>結束配置步驟。
D-2		在 IE 瀏覽器位址欄輸入“http://1.1.1.1/admin”,輸入使用者名稱和密碼（兩者都是“admin”），重新登入，即可開啓左圖所示介面，進行修改設定、發佈應用、管理系統等操作。

第3章 系統設定

完成上述 UU200 的系統安裝和初次配置之後，您可以隨時進行 UU200 的系統設定。

3.1 熟悉介面操作

3.1.1 進入設定介面

圖 3

配置介面採用 WEB 方式（見圖 3），進入配置介面前需要登入。設定成不同網絡模式的 UU200，其登入方式各不相同：

內部網使用者(通過交叉線與 UU200 連接)：

- 單模式：

  在 IE 瀏覽器位址欄輸入“http://1.1.1.1/admin”。

- 透明模式：

  在 IE 瀏覽器位址欄輸入“http://[*UU200 的 IP 地址*]/admin”

- 路由模式：

在 IE 瀏覽器位址欄輸入“http://[*UU200 在內部網絡中的 IP 地址*]/admin”。

內部網絡即 Lan 1，請參考圖 34。

外部網（遠端）使用者：

遠端系統管理員可以在任何一台聯機到網際網路的電腦上，使用 HTTP 協定通過 rm 方式開啓遠端使用者應用列表介面，即：在瀏覽器地址欄輸入“https://[*uuswitch 或 uuexchange 的 DNS 名稱/IP 地址*]/[*uu200 名稱*]/rm”（Private Access 方式）或“https://[*uu200 的 IP 位址*]/rm”(Direct Access 方式)

輸入正確的使用者名和密碼(admin/admin)後，將會出現如圖 3 所示的系統主介面。原因是系統處于安全考慮，設定了“Session Timeout”（會話超時）。Timeout 的時間爲 10 分鐘。

& 說明：

如果使用者超過 10 分鐘後需要對系統繼續進行操作，系統會彈出圖 4 提示資訊，要求使用者重新登入。

圖 4

i 重要：

爲了保障系統及內部資料安全，成功安裝 UU200 後，請務必修改 Admin 的密碼。

- 在系統主介面中，點選“安全管理”下的認證管理。選中某一使用者，點擊<編輯>，即可在開啓的介面中修改該使用者的密碼。
- 通過 IE 瀏覽器，遠端使用者可以在任何一台聯機到網際網路的電腦上通過 rm 方式開啓遠端使用者應用列表介面，在開啓的介面中雙擊“更改密碼”圖示，即可在開啓的介面中修改該使用者的密碼。

介面中各設定項功能簡要介紹如下。其中部分功能在安裝手冊“安裝 UU200 軟體”章節已作具體說明，使用者可參考上文。

【發布】

發布應用：設定 Publisher 要發佈的應用，包括增加、刪除和編輯相關應用的功能，對於每個應用可以設定授權使用者和指定限制該應用存取的位址和埠。

具體配置步驟請參見“**錯誤! 找不到參照來源。**發佈應用程式”。

發布 UUSoft 子網：設定相應的使用者或使用者群組可以通過 UUSoft 存取已共用的子網；同時，設定在已共用的 subnet 裏可以被存取的電腦。

發布 UURemote 子網： 設定相應的使用者或使用者群組可以通過 UURemote 存取已共用的子網；同時，設定在已共用的子網裏可以被存取的電腦。

【安全管理】

認證控制： 設定系統的認證類型（主要包括 Local File 和 Windows AD），并根據系統的認證類型，進行相關配置。

加密管理：可以用於選擇資料安全傳輸的加密演算法和 Hash 演算法。

本地管理：對本地管理進行授權，授權使用者可以對系統進行本地管理。

遠端管理：對遠端管理進行授權，授權使用者可以對系統進行遠端管理。

【進階】

選擇模式：選擇模式，包括單模式、透明模式和路由模式。根據系統在實際網路中的位置選擇具體的模式。

靜態路由：UU200 作爲路由器時用來設定靜態路由表。（僅路由模式支援）

連接站點到站點：設定安全的連接本地站點與遠端站點的服務。

動態 DMZ:設定和管理 DMZ 的服務 Dynamic DMZ。DMZ 的功能及用法請詳見 "**錯誤! 找不到參照來源。**配置動態非軍事區"。

【網路設置】

網路設置：該模組用以設定系統所在的內部網路和 UUExchange/UUSwitch 的相關資訊（包括 IP 位址、子網掩碼、閘道、代理伺服器、Internet 的接入方式等）。

iSTAR 設置 ：改變當前的連接方式。

【系統管理】

設定匯入：將原來保存好的配置檔導入到系統中。

設定匯出：將系統中已配置的配置檔導出到指定的檔夾保存。

管理許可證：輸入新的 License 檔案，更新當前 License。

升版系統：導入升級檔，升級當前的版本。

故障檢修：選擇 Ping、TraceRoute、Netstat 命令檢測系統的網路運行狀況。

顯示狀態：查看系統的狀況，包括 UUServer 的類型、系統的模式、系統的當前運行狀態等，以及當前系統的模式等。

查看系統性能：查看系統的各種的統計資訊。

查看日誌：包括查看系統每天指定時間段中，由重點到詳細的日誌情況，并可隨時保存日誌，以便隨時審閱。

日誌控制：系統日誌的設定。

警告通知設定：系統報警級別的設定

系統管理：系統伺服器的時間設定

3.1.2 介面間的跳轉

IE 瀏覽器上自帶的“Forward（前進）”、“Back(後退)”等按鈕及“檔”、“編輯”等功能表均不再出現在介面上。

- 返回上一級介面，請點擊<返回>或<取消>。
- 保存配置的修改，請點擊<確認>或<保存>鍵。

3.1.3 退出設定介面

退出配置介面前，請退回到圖 3 所示設定介面，點選 登出 退出。否則，再次（或用同樣的安全功能變數名稱稱稱和使用者名稱、密碼從其他機器）登入時，系統將提示以下資訊 ：

“使用者 [*username*] 目前已登入到本系統”

此時，如果使用者或者管理權限更高的使用者了勾選 “停止使用者[*username*]”重新登錄系統，則將強行中斷之前以該使用者名稱登入的其他會話。

例如：使用者在上一次非正常退出後，可以勾選該選項，強制停止自己的帳號，重新登入系統。或者，管理員可以停止其他只有“唯讀”許可權的使用者帳號，但不能停止其他管理員帳號(詳細內容請參考“設定本地/遠端管理員”章節)。

& 說明：

如果勾選“停止使用者 [*username*]”時出錯（如圖 5），有可能是因爲您沒有許可權使該使用者失效。如果仍要登入，請聯繫系統管理員。

圖 5

3.1.4 使設定生效

“生效”表示使你的設定生效。

修改設定後，點擊<確認>或<保存>鍵後進行保存。保存成功後，還必須單擊點擊<生效>，設定方可生效（如圖 6）。

重要：

- 以下七項設定完成後，點擊<生效>會中斷 Session，同時系統會提示使用者重新登入。因此，建議您：避免在系統繁忙時改變這幾項設定。

  網路設置；iSTAR 設置；認證控制；設定匯入；

  選擇模式；管理許可證；升版系統；

- 按<生效>後有時會重新啓動系統的服務，這時介面上可能會出現“非法 IP”等資訊，這時需要稍等片刻，輸入 http://1.1.1.1/admin，重新進入設定介面。

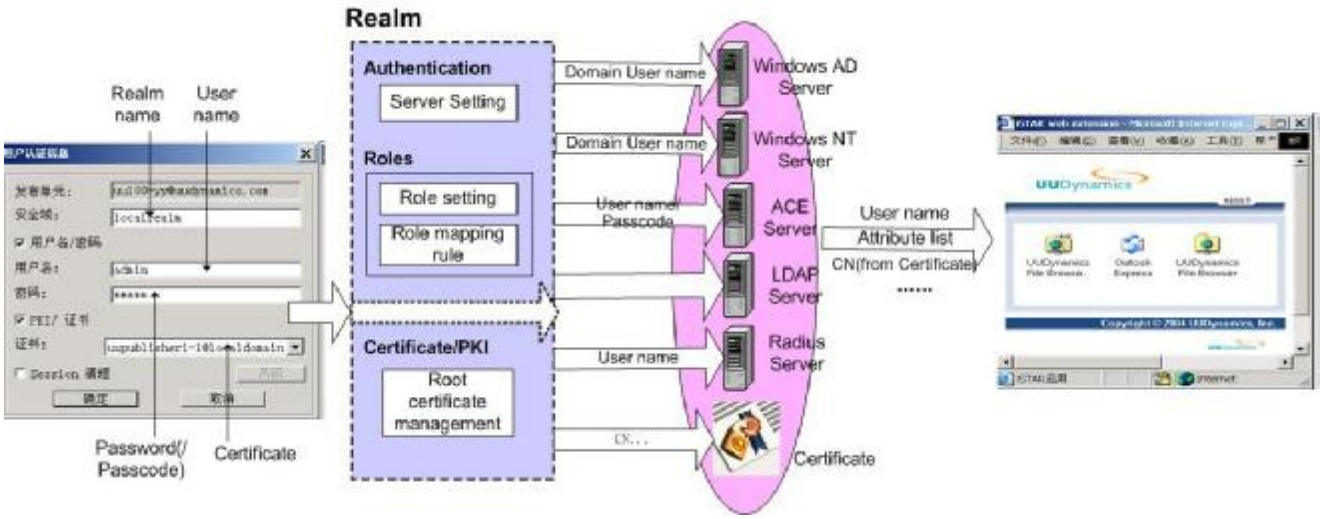
圖 6

3.2 用戶管理

UU200 的用戶包括使用者、本地管理員和遠端管理員。管理者可以在本地或遠端對 UU200 進行設定和維護，包括管理使用者帳號，升版系統、發布應用等。

相關概念：

UU200 用戶包括 UU200 管理員和遠端使用者。管理者可以在本地或遠端對 UU200 進行設定和維護，包括管理使用者帳號，升版系統、發布應用等。



UU200 允許管理員使用嚴密的安全控制方式，層層驗證接入安全。包括登入身份驗證、授權和應用級驗證策略等，杜絕了各種未經認證和授權的非法連接。

爲了實現這種安全控制思想，伺服器端（UU200）需要完成相關的設定。以下對涉及到的各種概念進行說明和舉例。

- 認證:身份驗證。系統使用認證伺服器或證書驗證使用者端傳來代表使用者身份的資訊。身份驗證有以下幾種途徑：
  1. 使用者端輸入的使用者名稱/密碼。如果使用者名稱和密碼不符，則驗證失敗。
  2. 使用者端導入的證書的 CN 等屬性驗證。證書的可信任性由簽發的根證書負責。
  3. 認證伺服器上該使用者相應的屬性。使用者屬性需要根據使用者名稱在指定的認證伺服器檢索和匹配。
  4. 一次性有效的密碼。例如 RSA 的 token code。這種一次性有效的密碼通常用於雙因數身份認證。這種方式的認證要求使用者輸入使用者名稱、passcode（PIN＋Token code）。
- 授權：應用授權。發布應用時通常將應用授權給已通過身份驗證的使用者。授權依據通常是以下一種或多種資訊：
  1. 代表使用者身份的使用者名稱
  2. 使用者隸屬的群組列表
  3. 使用者對應的角色（從證書中的屬性以及使用者在認證伺服器上對應的屬性對應而來）。
- 規定：安全管理綜合策略。管理員可以根據安全級別組合各種包括身份驗證、授權在內的所有的安全管理方法。

  例如，當安全需求極高時，可以設定一種較嚴密的規定：使用雙因數身份認證（使用者名稱 + 證書）和通過另一張證書授權，即：Client 端必須同時提供使用者名稱和證書，并通過驗證另一張證書是否給該使用者授權或授權該使用者使用何種應用。
- Certificate/PKI（根證書）：證書。由 CA 簽發，包含使用者 CN 或其他屬性等安全資訊。

通常用於驗證使用者的身份或對通過身份驗證的使用者進行應用授權。

- 角色:角色定義。

  PKI 和 Radius 類型的伺服器中，通常將一組相同屬性定義爲一個角色。使用者屬於某一角色意味著他（/她）具有相應的所有屬性。UU200 在 PKI 和 Radius 兩種類型的安全域中引入了角色這一概念，目的是方便將某一應用授權給某一角色（即具有某些相同屬性的使用者）。

  角色通常在驗證 AD/Radius 伺服器上的使用者身份和應用授權時作爲主要依據。

- 主機檢查器：

  管理員可以制定規則用以檢查用戶端機器的運行環境。包括：作業系統的版本、作業系統 patch 的版本，應用程式的版本。例如：檢查用戶端機器是否運行在 Windows 2000 系列的作業系統上，檢查的時機依 iSTAR 的 Server 端設定而定，通常設定爲：在使用者登入安全域，進行身份驗證的同時檢查用戶端的運行環境；或者在使用者已獲取應用列表，幷啓動某項應用時進行檢查。

- 安全域：每一個使用者隸屬於一個或多個安全域。安全域代表了使用 iSTAR 產品時使用者的安全特徵。iSTAR 產品將依據域中的各項特徵逐一驗證使用者身份。

  在安全域中設定的內容包括：驗證使用者身份的伺服器、證書以及驗證策略等資訊。

  使用者隸屬于某個安全域，意味著該使用者將使用該域中指定的綜合安全管理策略，包括：在指定的認證伺服器或（/和）證書進行身份驗證，驗證通過後，UU200 將根據指定的授權策略或（/和）證書對使用者進行應用授權。安全域的使用可以參考以下例子。

  & 說明：

  本系統中有一個預設的安全域：LocalAdmin。LocalAdmin 中設定了一個預設的伺服器 — LocalUsers，該伺服器中有預設的 User/密碼：admin/admin。預設的使用者 admin、伺服器和安全域不能被刪除。這樣可以保證至少有一位具有“唯讀/更改”許可權的使用者存在。

  LocalAdmin 中不允許設定 Certificate/PKI。

實例：

例一：

- 背景

某企業爲大型銀行。使用者類型包括：區域網路路使用者、Radius、遠端存取使用者……

其中：

User1：本地使用者，安全需求一般。在 LocalSever 中驗證使用者名稱身份。企業的合作夥伴或代理商適合使用這種使用者身份連入企業的內部網。

User2：本地使用者，沒有使用者名稱/密碼，但持有某 CA 簽發的證書。

User3：Radius 使用者。安全需求高，在 Radius 伺服器上有使用者名稱/密碼，屬於某一角色。

User4：遠端使用者，安全需求極高，需要使用使用者名稱/Passcode(PIN+ Token code).在 ACE 伺服器上驗證身份進行雙重身份認證。

Group1：成員包括 User1。

- 身份驗證設定

1. 預置以下幾個伺服器。

   RadiusUsers：類型爲 Radius；

   ACEUsers：類型爲 ACE/Server；

2. 預置以下幾個安全域。

   LocalAdmin：預設。不需增刪也不能更改。

   PKIRealm: 新增。僅需要驗證證書。

設定項	值	說明
使用以下伺服器進行認證/制定策略	None	類型：無
通過 Certificate/PKI 認證	True	選中該選項，並點擊<管理證書>選擇信任的根證書。

RadiusRealm：新增。用於驗證 Radius 域的使用者。選擇 MyRadius 作爲認證伺服器。

設定項	值	說明
使用以下伺服器進行認證/制定策略	RadiusUsers	類型：Radius
通過 Certificate/PKI 認證	False	不選中該選項。
角色		點擊<增加/編輯映射規定…>，可以增加/編輯角色 的對應規定。

ACERealm：新增。用於驗證遠端使用者。

設定項	值	說明
使用以下伺服器進行認證/制定策略	ACEUsers	類型：ACE
通過 Certificate/PKI 認證	False	不選中該選項。

3. 將使用者/群組按安全需求加入到相應的安全域中。

   User1/Group1：加入伺服器 LocalUsers。使用使用者名稱/密碼在 LocalUsers 伺服器上認證身份。

   User2：加入 PKIRealm，沒有使用者名稱/密碼，但持有某 CA 簽發的證書。通過證書中 CN 或其他屬性驗證使用者身份。驗證通過後，從證書中獲取該使用者的屬性，進行應用授權。

   User3：加入 RadiusRealm，在 Radius 伺服器上驗證使用者名稱/密碼，驗證通過後，從 Radius 伺服器上獲取該使用者的屬性，進行應用授權。

   User4：加入 ACERealm，使用使用者名稱/passcode（PIN+Token code）在 ACE 伺服器上驗證身份。

例二：

- 背景

某企業爲中小型企業。使用者類型包括：區域網路路使用者、遠端存取使用者……

其中：

User1：遠端存取使用者，安全需求一般。在 LocalSever 中有使用者名稱/密碼。企業的合作夥伴或代理商可使用這種使用者身份連入企業的內部網。

User2：Windows NT 域使用者。安全需求較高，在 Windows NT 伺服器上有使用者名稱/密碼。需要 Windows NT 域使用者名稱進行身份認證。

Group1：成員包括 User1。群組的設定可參考使用者的設定。

- 身份驗證設定

1. 預置以下幾個伺服器。

   LocalAdmin：預設。不需增刪也不能更改。類型爲 Local；

   NTUsers：類型爲 Windows NT。

2. 預置以下幾個安全域。

   LocalAdmin：預設。不需增刪也不能更改。

   NTRealm: 新增。需要驗證 NT domain 的使用者名稱/密碼。

設定項	值	說明
使用以下伺服器進行認證/制定策略	NTUsers	類型：Windows NT
通過 Certificate/PKI 認證	True	選中該選項，並點擊<管理證書>選擇信任的根證書。

3. 將使用者/群組按安全需求加入到相應的安全域中。

   User1/Group1：加入伺服器 LocalUsers。使用使用者名稱/密碼在 LocalUsers 伺服器上認證身份。驗證通過後，進行應用授權。

   User2：加入 NTRealm，通過企業的 Windows NT 伺服器驗證使用者身份。驗證通過後，進行應用授權。

3.2.1 管理認證伺服器和使用者

添加伺服器：

1. 在系統主介面中（如圖 3）的“安全管理” 下，點選 認證管理。
2. 點選圖 14 中的<增加/編輯伺服器>，進入圖 7 所示介面。

圖 7

3. 點擊<增加>，進入圖 8 所示介面。從“伺服器類型”列表中選擇類型，選擇不同的類型後，會出現不同的介面，填入相應的資料。各輸入項的填寫說明請參見下表。

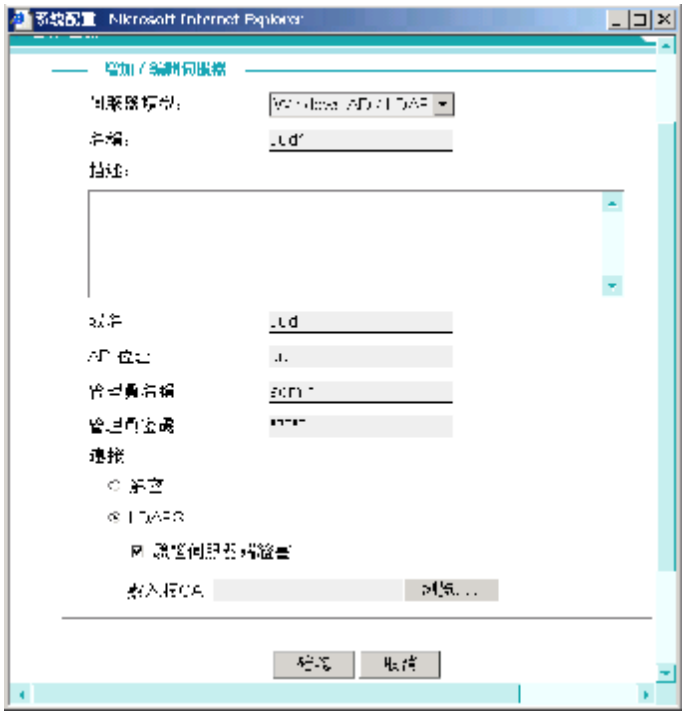


圖 8

4. 設定完畢後，重復點擊<確認>，直到返回圖 14 所示介面。
5. 點擊<生效>，保存設定。

表：各輸入項的填寫說明

伺服器類型	輸入項	說明
Window	名稱	輸入伺服器名稱

AD/LDAP（Window AD/NTLM）	描述		輸入對該伺服器的描述（可選）
	功能變數名稱稱		輸入對應的 DNS 名稱
	AD 位址		輸入該域服務器的 IP 位址或功能變數名稱稱（Window AD/LDAP 類型中如果下面的“連接” 選項爲 LDAPS 時，必須輸入功能變數名稱稱）
	管理員名稱/管理員密碼		輸入登錄該域的管理員使用者名稱、密碼
	連接（僅 Window AD/LDAP 類型）	解密	連接過程不加密
		LDAPS	驗證伺服器端證書：選中該選項後，連接不但被加密，還需要驗證伺服器提供的證書
			導入根 CA：導入簽發 Certificate 的根 CA
LocalUsers	名稱		輸入伺服器名稱
	描述		輸入對該伺服器的描述（可選）
	使用者		在該伺服器中增加使用者
	群組		在該伺服器中增加群組
Windows NT Domain	名稱		輸入 NT 伺服器名稱
	描述		輸入對該伺服器的描述（可選）
	網功能變數名稱稱		輸入該 NT 域的名稱
	網網域控制器		輸入該 NT 域中的網網域控制器的 IP 位址或 DNS 名稱
	管理員名稱		輸入對 NT 伺服器管理員的登入帳號
	管理員密碼		輸入對 NT 伺服器管理員的登入密碼
LDAP(可參考表格下的實例）	名稱		輸入伺服器名稱
	描述		輸入對該伺服器的描述（可選）
	類型		ŸActive Directory; ŸOpenLDAP; ŸGeneric LDAP with Static Groups：除了以上兩種類型之外的其他類型
	伺服器		LDAP 伺服器的 IP 位元址或名稱

	使用預設埠		可選項。預設埠號爲： Ÿ 不加密：389 Ÿ 使用 SSL 協定加密：636 如果沒有選中該項，則需要另行設定埠號
	授權需要經過 LDAP 搜尋	Admin DN	指定在 LDAP 伺服器上搜尋管理員的目錄路徑
		密碼	輸入該管理員的密碼。
	指定如何找出使用者輸入	Base DN	指定在 LDAP 伺服器上搜尋使用者的目錄路徑
		屬性	指定以哪個屬性類型（可以是 LDAP 伺服器管理員定制的屬性類型）作爲使用者名稱
		過濾器	設定過濾條件
	決定群組成員	Base DN	指定在 LDAP 伺服器上搜尋組的目錄路徑
		屬性	指定以哪個屬性類型（可以是 LDAP 伺服器管理員定制的屬性類型）作爲組名稱
		過濾器	設定過濾條件
		成員屬性	指定 LDAP 伺服器上的屬性類型（可以是 LDAP 伺服器管理員定制的屬性類型），用於驗證靜態組的成員。
	連接	解密	連接過程不加密
		LDAPS	驗證伺服器端證書：選中該選項後，連接不但被加密，還需要驗證伺服器提供的證書 導入根 CA：導入簽發 Certificate 的根 CA
Radius	名稱		輸入伺服器名稱
	描述		輸入對該伺服器的描述（可選）
	Radius 伺服器		輸入 Radius 伺服器的 IP 位址
	Radius 埠		輸入 Radius 伺服器的埠
	Shared Key		輸入 Shared Key
ACE / Server	名稱		輸入伺服器名稱
	描述		輸入對該伺服器的描述（可選）
	導入至		導入.REC 文件後，系統自動記錄幷回顯導入的時間
	導入新的配置檔		將相應的 .REC 文件導入。該文件由 ACE 伺服器分配。

	刪除節點 Secret	用於和 ACE/Server 端的同步。如果在某一端刪除了節點 Secret，必須在另一端也相應刪除。

舉例：LDAP 類型伺服器的目錄如下

dc= qa,dc=com	說明：	
Ou=people	管理員	DN：cn=root,dc=qa,dc=com
Uid=tester1	使用者	屬性：cn；
Uid=tester2		過濾: objectclass=person
Ou=group	組成員	屬性：cn；
Cn=test		過濾: objectclass=posixgroup,
Cn=test1		成員屬性：MemberUid

（test、 test1 爲群組。tester1、 tester2 爲使用者，配置見圖 9）

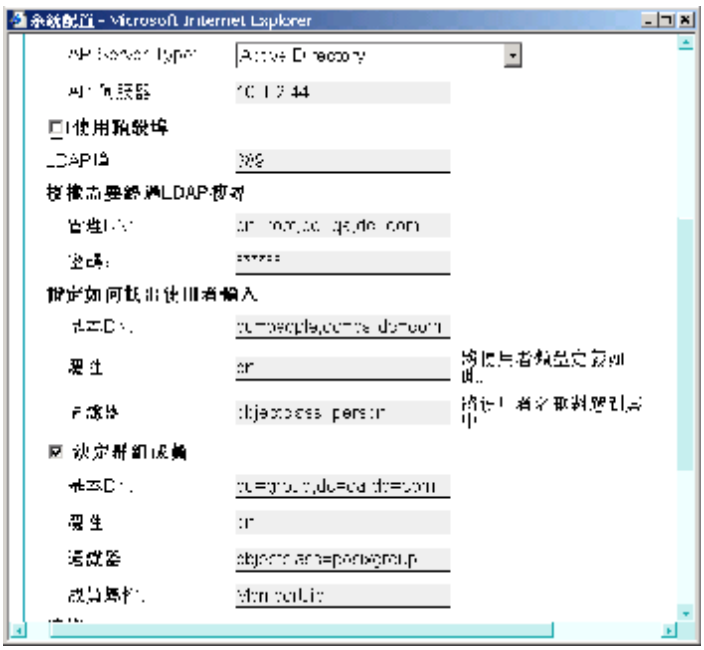


圖 9

& 說明：

Ÿ **Windows AD/LDAP** 伺服器與 **Windows AD/NTLM** 伺服器比較

前者有三條限制：

1. Windows AD/LDAP 方式下，“名稱”欄內填入的名稱必須與下一欄所指定 IP 的伺服器中存在的 AD 名稱一致。
2. Windows AD/LDAP 方式下，僅能搜索出 1000 條以下的“遠端管理員”記錄（有關搜索遠端管理員記錄的內容請參考“**錯誤! 找不到參照來源。**設定本地（/遠端）管理員”）。

3. Windows AD/LDAP 方式下，在對應的 Windows AD 域中增加的組可能需要 20 分鐘後才能生效。增加的組包括“新增的新組”和“刪除後增加的同名稱組”。
   該組中的使用者如果無法登錄 UU200，請稍候再試。

Ÿ **LocalUsers** 伺服器

LocalUsers 是預設的伺服器類型。如果選擇 **LocalUsers** 類型的伺服器，則表示選擇在 UU200 中單獨建立一個使用者認證檔案。這個檔案是經過加密保護的。換言之，使用者應使用本系統定義的帳戶和密碼連入。該伺服器中有預設的使用者/密碼：admin/admin。預設的使用者 admin、伺服器和安全域不能被刪除。這樣可以保證至少有一位具有“唯讀/更改”許可權的使用者存在。

管理用戶：

Ÿ 如果僅使用證書/PKI 進行認證（不指定認證伺服器的認證方式），則不需要添加使用者。使用者存取 UU200 時，僅需提供證書即可。

Ÿ 在添加 LocalUsers 伺服器時，可以通過點擊<使用者>添加使用者，并設定密碼。也可以修改原有使用者的密碼。

Ÿ 在添加其他類型伺服器時，只要按照表格中的說明填寫各輸入項，UU200 會自動到指定的認證伺服器獲取該伺服器中的符合條件的使用者列表。這種結合現有的認證伺服器進行用戶認證的方式，使得企業可以使用統一的安全認證策略，無需另外添加用戶。
此方式下，如果要修改使用者密碼，請聯繫認證伺服器的管理員，修改該伺服器中該帳戶的密碼。

3.2.2 管理證書

1. 在系統主介面中（如圖 3）的“安全管理” 下，點選 認證控制。
2. 點選圖 14 中的<增加/編輯根證書>。在介面中點擊<增加>，在下圖所示介面中輸入相應的證書資訊。
   “證書約束條件”欄用於輸入證書的限制規則。其語法結構爲：
   [*系統變數名稱*].[*屬性名稱*] [*操作符*] [*屬性值*]（或另一 [*系統變數名稱*].[*屬性名稱*]）。
   舉例：
   ①Certattr.CN =’Zhang san’含義爲：證書中 CN 必須爲 Zhang san。
   ②Certattr.CN =User.name 含義爲：證書中 CN 必須和登錄時所用的使用者名稱一致。

& 說明：

***i*STAR™**定義了三類系統變數：User 類、Userattr 類、Certattr 類。其中，

User 類包括 name、groupname 屬性。User.name 表示登錄時所用的使用者名稱，User.groupname 表示該使用者名稱所屬的群組。

Userattr 類 包括：Service-Type、Framed-IP-Address、Framed-IP-子網掩碼等用戶屬性。

Certattr 類 包括：C,CN,L,O,OU,Email 等證書的屬性。

操作符 是 sql 的操作符，如 =,!=,>,<,like,in 等。

3. 設定完畢後，重復點擊<確認>，直到返回圖 14 所示介面。
4. 點擊<生效>，保存設定。

3.2.3 管理角色

如果認證伺服器指定的是“None” （僅使用 PKI）或“Radius”類型的伺服器，則還需要預先定義角色。以便設定規定將相應的角色與 Radius 伺服器或證書中的用戶對應起來（見圖 15）。

1. 在系統主介面中（如圖 3）的“安全管理” 下，點選 認證控制。
2. 在圖 14 所示介面，點擊<增加/編輯角色>。開啓圖 10 所示介面。
3. 點擊<新建>，進入圖 11 所示介面。輸入角色名稱。

圖 10

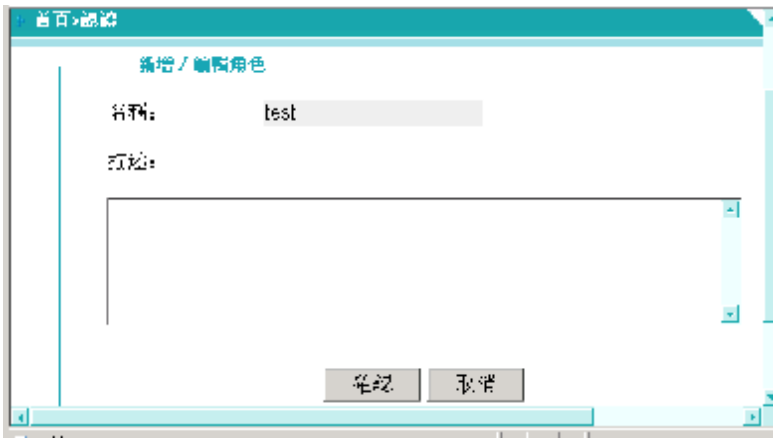


圖 11

4. 設定完畢後，重復點擊<確認>，直到返回圖 14 所示介面。

5. 點擊<生效>，保存設定。

3.2.4 檢查用戶端主機的運行環境

在 UU200 的 Server 端增加主機檢查器規則，用於檢查用戶端主機的運行環境是否符合要求：

1. 在圖 14 所示介面，點擊<增加/編輯主機檢查器>。開啓設定介面。
2. 點擊<新增>，在開啓的頁面中輸入新規則的名稱。

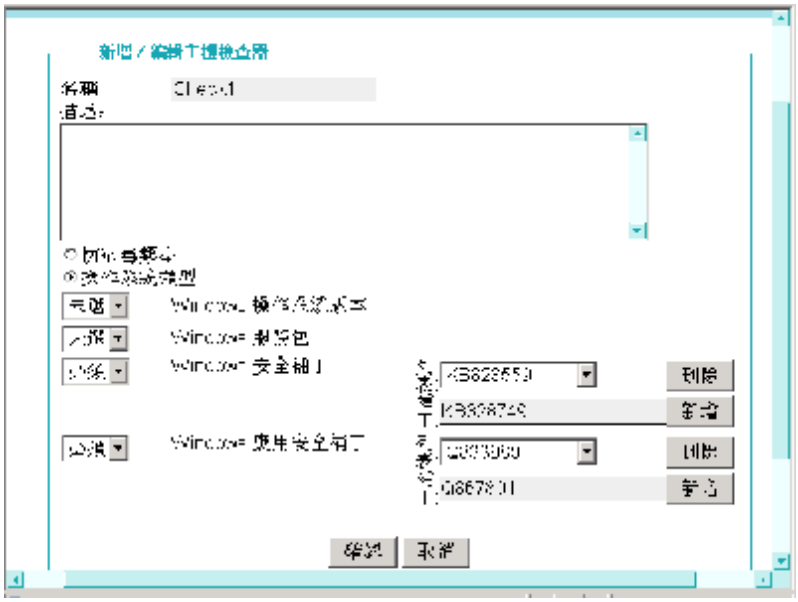


圖 12

3. 選擇對何種類型的運行環境進行檢查：
   - Ÿ 點選“防病毒類型”，可以檢測用戶端是否使用指定的防毒軟體的類型；
   - Ÿ 點選“作業系統類型”，可以檢測用戶端是否使用指定的作業系統、服務包、安全補丁以及應用安全補丁；可以將新的安全補丁和應用安全補丁 ID 加入列表，以便選擇。
     例如： KB828749（Windows 2000 補丁）、Q867801（IE 補丁）。
   - Ÿ 如果選擇了“必須”選項，則要求用戶端運行環境必須與其後的所有設定相吻合；
   - Ÿ 如果選擇了“拒絕”選項，則如果用戶端運行環境與其後的任一項設定相吻合，該 UU200 將會拒絕用戶端的相應操作。

例如：

添加了五項 Windows 安全補丁，并且在“Windows 安全補丁”前，

- Ÿ 如果選中“必須”選項，則用戶端必須已經安裝此五種安全補丁，方可通過此項檢測；
- Ÿ 如果選中“拒絕”選項，則用戶端只要已經安裝此五種安全補丁中的任一種，都不能通過此項檢測。

4. 設定完畢後，重復點擊<確認>，直到返回圖 14 所示介面。

5. 點擊<生效>，保存設定。

3.2.5 管理安全域

添加安全域之前，應預先準備必須的伺服器、角色或證書等。準備的流程可參考下圖：

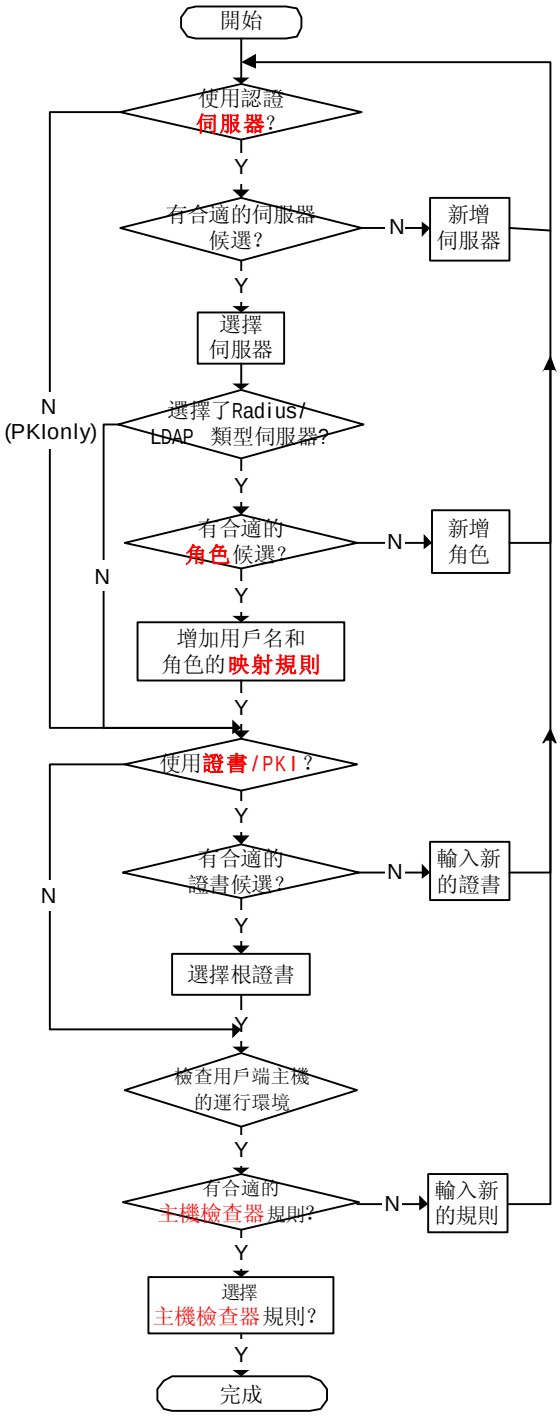


圖 13 設定流程圖

1. 在系統主介面中（如圖 3）的“安全管理” 下，點選 認證控制。

圖 14

2. 在圖 14 所示介面上點擊<增加>，可以增加新的安全域。

   選中列表中某個安全域，點擊<編輯>，可以修改該安全域的屬性。

3. 輸入或修改安全域的名稱。如果需要對該安全域進行描述，請在“描述”欄內輸入說明性文字。

   例如圖 15 中，安全功能變數名稱稱：RadiusUsers。

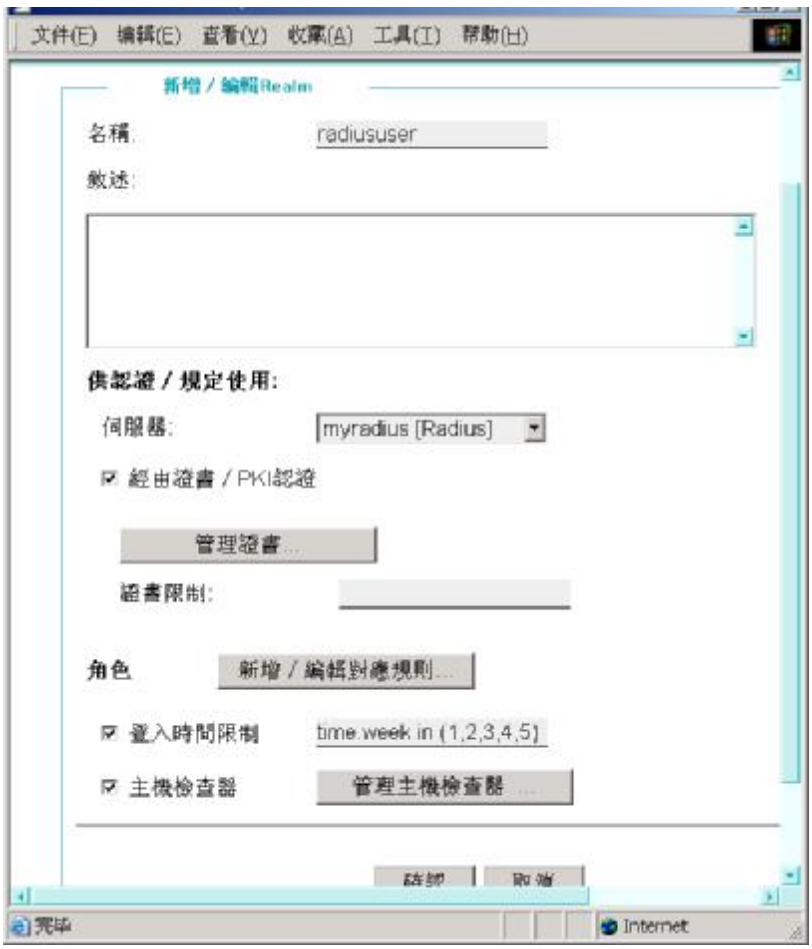


圖 15

4. 在“伺服器”欄選擇需要在哪個伺服器上進行使用者身份驗證。例如圖 15 中，選擇伺服器 MyRadius。在列表中選擇伺服器後，則直接轉至下一步繼續其他操作。但是如果列表中沒有您所需要的伺服器，請先添加伺服器。
5. 如果需要驗證 Client 端使用者提供的證書，請勾選“通過 Certificate/PKI 認證”。否則，直接跳轉至下一步（步驟 7）。

   點擊<管理證書>，可以選擇已有的證書。如果沒有需要的證書，請先添加合適的證書。
6. 如果認證伺服器指定了除 “None”（僅使用 PKI）或“Radius”兩種類型之外的其他類型伺服器，跳轉至步驟 9。

   如果認證伺服器指定的是“None” （僅使用 PKI）或“Radius”類型的伺服器，則還需要爲角色設定相應的規則（見圖 15）。
7. 在圖 15 所示介面中點擊<增加/編輯映射規則…>，進入所示圖 16 介面。

圖 16

以 Radius 伺服器爲例：

點選圖 16 介面上的<增加>，進入圖 17 所示介面增加新的規則。

增加規則的內容包括：根據 Radius 伺服器中的使用者屬性，設定過濾條件，篩選出所有的符合條件的使用者，然後將這些使用者歸入某一角色中。這樣，當對某個角色進行授權或其他操作時，實際上是對所有符合規則中過濾條件的使用者同時進行操作。其語法結構爲：

[*系統變數名稱*].[*屬性名稱*] [*操作符*] [*屬性值*]（或另一 [*系統變數名稱*].[*屬性名稱*]）。

舉例：

①圖 17 中的規則含義爲：Radius 伺服器中所有屬性 service-type 取值爲 framed-user 的使用者都屬於角色“admin”。

②Certattr.CN =User.name 含義爲：證書中 CN 必須和登錄時所用的使用者名稱一致。

③當“規則”列爲空的含義爲：Radius 伺服器中所有使用者都屬於指定的角色。

& 說明：

***i*STAR™**定義了三類系統變數：User 類、Userattr 類、Certattr 類。其中，

User 類包括 name、groupname 屬性。User.name 表示登錄時所用的使用者名稱，User.groupname 表示該使用者名稱所屬的群組。

Userattr 類 包括：Service-Type、Framed-IP-Address、Framed-IP-子網掩碼等用戶屬性。

Certattr 類 包括：C,CN,L,O,OU,Email 等證書的屬性。

操作符 是 sql 的操作符，如 =,!=,>,<,like,in 等。

圖 17

8. 設定完畢後，重復點擊<確認>，直到返回圖 15 所示介面。
9. 如果要限制使用者的登入時間，可以選中“登入時間限制”核取方塊，并輸入約束條件。

   約束條件所遵循的語法結構與設定 Radius 伺服器的規則類似，其語法結構爲：

   time.[*屬性名稱*] [*操作符*] [*屬性值*]（或另一 [*系統變數名稱*].[*屬性名稱*]）。

   & 說明：

   此處的 time 爲表示時間的系統變數名稱。

   屬性名稱包括 year, month, day, hour, minute, second, week。其中，

   year 表示 4 位數年份；**month** 表示月份；**day** 表示日期；

   hour 表示小時（按 24 小時制）；**month** 表示分鐘；**second** 表示秒；

   操作符 是 sql 的操作符，如 =,!=,>,<,like,in 等。

   舉例：

   下面的約束條件限制了使用者只能在 2005 年，8:00～18:00 之間驗證身份，并在驗證成功後登入系統：

   (time.year =2005) and (time.hour between 8 and 18)

10. 設定完畢後，點擊<確認>返回圖 15 所示介面。
11. 如果要檢測用戶端的運行環境是否符合要求，請勾選“主機檢查器”選項，并點擊<管理主機檢查器>按鈕。在開啓的視窗中選擇檢測規則。

    在“符合時便停止”列中：

    - 點選“不是”：則檢測到符合該規則後，繼續檢測下一規則；如果不符合該規則，則拒絕該使用者登入。
    - 點選“是”：則一旦檢測到符合該規則後，即停止繼續檢測，允許該使用者以遠端管理員身

份登入管理介面。如果不符合該規則，則拒絕該使用者登入。

說明：

Ÿ 在“符合時便停止”列中選擇“是”的規則應被放置在所有選擇“不是”的規則之後，否則當用戶端的運行環境符合該條設定爲“是”的規則後，將不會繼續檢測，這樣，其後的規則將不會再有機會被檢測。

Ÿ 如果“防病毒類型”和“作業系統類型”兩種類型都有規則被選中，則要求同時檢測用戶端主機安裝的防病毒軟體和系統設定（系統設定包括：作業系統版本、系統安全補丁、應用的安全補丁等）。只要不符合這兩種類型中的任何一條規則，該用戶端都無法登入該安全域。

圖 18

12. 設定完畢後，重復點擊<確認>，直到返回圖 14 所示介面。
13. 點擊<生效>，保存設定。

3.2.6 設定本地（/遠端）管理員

在系統主介面中（如圖 3）的“安全管理”之下，按下本地管理。會出現如圖 19 的視窗；用以增加或移除本地系統管理員。按下遠端管理會出現如圖 20 的視窗；用以增加或移除遠端系統管理員。

i **注意：**

1. 在本地管理 中添加的使用者爲本地管理員，能且僅能從本機登入 UU200 系統管理介面。
2. 在遠端管理 中添加的使用者，遠端系統管理員必須首先是本地管理員，即必須先在 本地管理 中加

入該使用者名稱。

Ÿ 本地管理：

1. 如圖 19，在“使用者列表”選項組中選擇使用者類型爲“使用者”或是“群組”，列出所有的使用者或群組。
2. 本地管理員存取策略爲“拒絕”，意即預設情形下使用者列表中所有的使用者都不能訪問。
   只有在“使用者列表”選項組下的“使用者列表”列表中勾選使用者，並按<增加>將其加入下方的“除了下列的”列表中，這些使用者才能通過本地方式對 UU200 進行存取操作。
   重復在“使用者列表”中勾選，幷按<增加>，可以繼續加入多個使用者（/群組/角色）。
3. 在“訪問類型”中設定該管理員的權限。各種許可權的含義分別爲：
   唯讀:表示該使用者對系統管理介面有“唯讀”許可權。
   更改:表示該使用者對系統管理介面有“唯讀”、“修改”和“使更改生效”的許可權。
4. 以上步驟完成後，點擊<生效>保存設定結果，幷返回到圖 3 系統主介面。

Ÿ 遠端管理：

1. 如圖 20 所示，爲保證管理員遠端管理時建立的 SSL 連接的安全，您可以設定允許會話持續的最長時長和允許會話空閑的最長時長。超過設定的時長，系統會自動斷開這次連接。
2. 如果勾選“允許同一使用者多次訪問”， 則同一管理員再次（或使用同樣的使用者名稱從其他機器）獲取管理專案列表（見圖 27）時，不影響之前以該使用者名稱管理專案列表的其他會話。
   反之，如果不勾選該選項，則會強行中止之前的所有以該使用者名稱獲取管理專案列表的會話。
3. 選擇需要進行遠端管理的應用服務，點擊<編輯>，進入圖 21 所示介面。
4. 設定是否對該服務使用加密、哈希以及壓縮演算法。
5. 點擊<規定>設定，進入圖 22 所示的視窗。輸入您爲這個規定所取的名稱；目前 UU200 能提供的策略包括：
   - Ÿ 驗證證書：
     可以指定證書，在使用者登入、獲取應用時驗證用戶端是否提供了正確的證書。此外，還可以對該證書設定限制條件。。
   - Ÿ 限制存取時間：
     如果要限制使用者的存取時間，可以選中“存取時間限制”核取方塊，幷輸入約束條件。
     約束條件所遵循的語法結構與設定 Radius 伺服器的規則類似，其語法結構爲：
     time.[*屬性名稱*] [*操作符*] [*屬性值*]（或另一 [*系統變數名稱*].[*屬性名稱*]）。

& 說明：

此處的 time 爲表示時間的系統變數名稱。

屬性名稱包括 year, month, day, hour, minute, second, week。其中，

year 表示 4 位數年份；**month** 表示 2 位數月份；**day** 表示 2 位數的日期；

hour 表示小時（按 24 小時制）；**month** 表示分鐘；**second** 表示秒；

操作符 是 sql 的操作符，如 =,!=,>,<,like,in 等。

舉例：下面的約束條件限制了使用者只能在 2005 年，8:00～18:00 驗證身份，并在驗證成功後存取應用列表：

(time.year =2005) and (time.hour between 8 and 18)

Ÿ 檢測用戶端運行環境：

如果要檢測用戶端的運行環境是否符合要求，可以點擊<管理主機檢查器>。選擇在安全域設定時預先加入的檢測規則。

在“符合時便停止”列中點選“不是”：則檢測到符合該規則後，繼續檢測下一規則；如果不符合該規則，則拒絕該使用者以遠端管理員身份登入管理介面。

在“符合時便停止”列中點選“是”：則一旦檢測到符合該規則後，即停止繼續檢測，允許該使用者以遠端管理員身份登入管理介面。如果不符合該規則，則拒絕該使用者以遠端管理員身份登入管理介面。

說明：

Ÿ 在“符合時便停止”列中選擇“是”的規則應被放置在所有選擇“不是”的規則之後，否則當用戶端的運行環境符合該條設定爲“是”的規則後，將不會繼續檢測，這樣，其後的規則將不會再有機會被檢測。

Ÿ 如果“防病毒類型”和“作業系統類型”兩種類型都有規則被選中，則要求同時檢測用戶端主機安裝的防病毒軟體和系統設定（系統設定包括：作業系統版本、系統安全補丁、應用的安全補丁等）。只要不符合這兩種類型中的任何一條規則，該用戶端都無法以遠端管理員身份登入管理介面。

Ÿ 驗證校驗碼

該功能用於防止非法或有潛在威脅的用戶端應用程式攻擊應用伺服器。例如被病毒或木馬篡改的應用程式的校驗碼必定與合法應用程式的校驗碼不同，這樣，當使用者嘗試連入時，iSTAR 只要驗證用戶端運行的程式的校驗碼和伺服器端爲該程式設定的校驗碼是否一致，便可以判定用戶端的應用程式是否合法。如果合法，則該項驗證通過，否則使用者將不能啓動該應用。

校驗碼採用 SHA 1 演算法。

6. 點擊<使用者>設定該服務的遠端管理者。
7. 如圖 23 所示，將遠端管理員所屬的安全域從“可選擇”列表框中移至“已選定”列表框。如果選擇的是包含有角色資訊的 Radius 或 PKI 類型的安全域，會顯示圖 24 所示的操作介面。
8. 設定該管理員對 UU200 的訪問策略，系統預設的是“拒絕”，意即所有的管理員都不能訪問。

9. 在“使用者列表”選項組中指定以何種方式（“使用者”或“群組”）設定遠端管理員。
10. 在選項組下的“使用者列表”列表中勾選使用者(/群組/角色)，並按<增加>將其加入下方的“除了下列的”列表中；

    重復該步驟，可以繼續加入多個使用者（/群組/角色）。

    通過這一步驟結合設定訪問策略步驟相結合，管理員可以靈活的設定訪問許可權，即：僅允許某一些管理員訪問，或者允許除某一些管理員外的所有管理員訪問。

    如果安全域指定的伺服器類型爲“Windows AD/LDAP”，同時該伺服器中的“管理員名稱”中輸入的管理員屬於該域的“Domain Admins”群組，則圖 23 中的“使用者列表” 列表將顯示該域中所有的使用者，否則，圖 23 中的“使用者列表” 列表只能顯示該域中的部分使用者。
11. 如果在圖 23 的視窗中的空白欄輸入要搜索的字串幷點擊<搜索/開始>，介面上將返回模糊查詢後的結果。圖中顯示了對“test”搜索的結果。(是否有搜索功能與伺服器的類型有關。)
12. 在“訪問類型”中設定該管理員的權限。各種許可權的含義分別爲：

    唯讀:表示該使用者對系統管理介面有“唯讀”許可權。

    更改:表示該使用者對系統管理介面有“唯讀”、“修改”和“使更改生效”的許可權。
13. 以上步驟完成後，保存設定結果，幷返回到圖 3 系統主介面中。

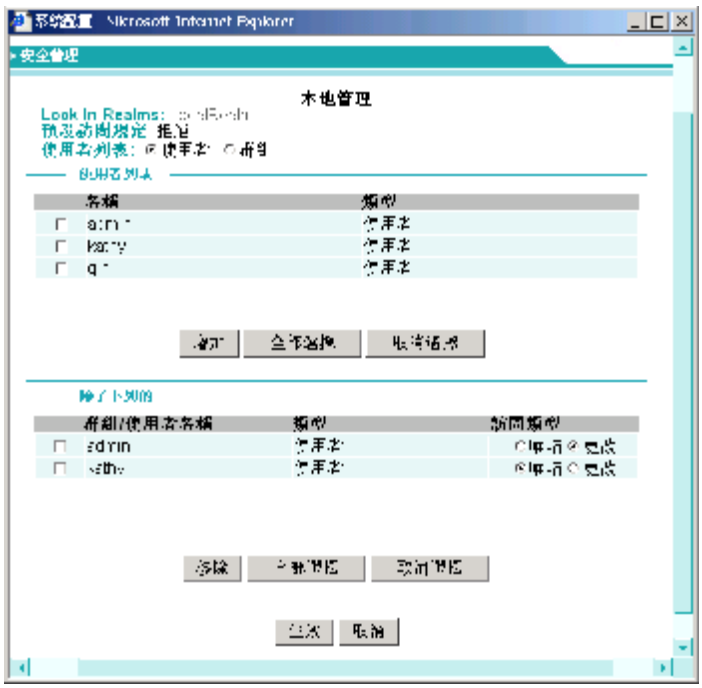


圖 19

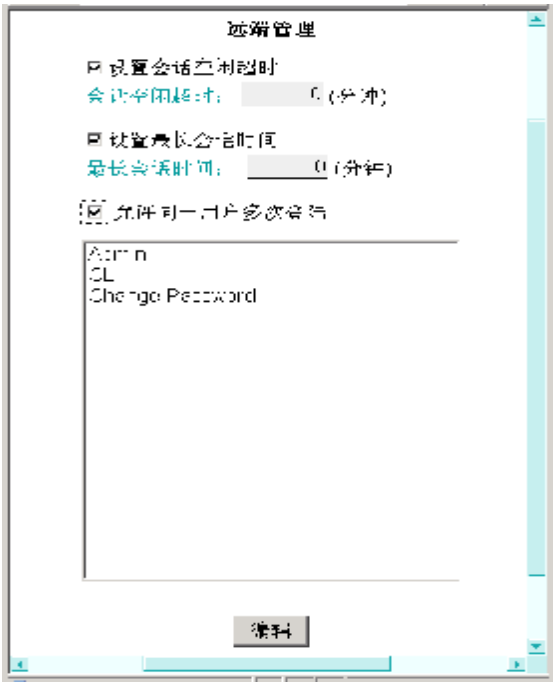


圖 20

圖 21

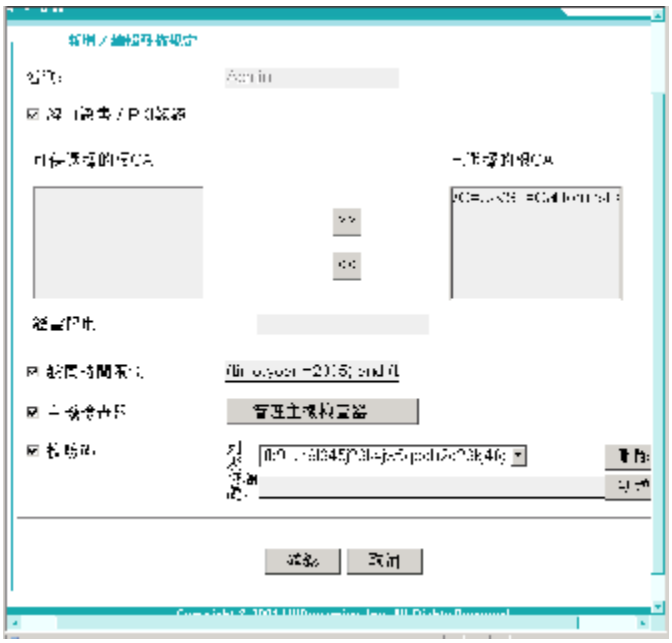


圖 22

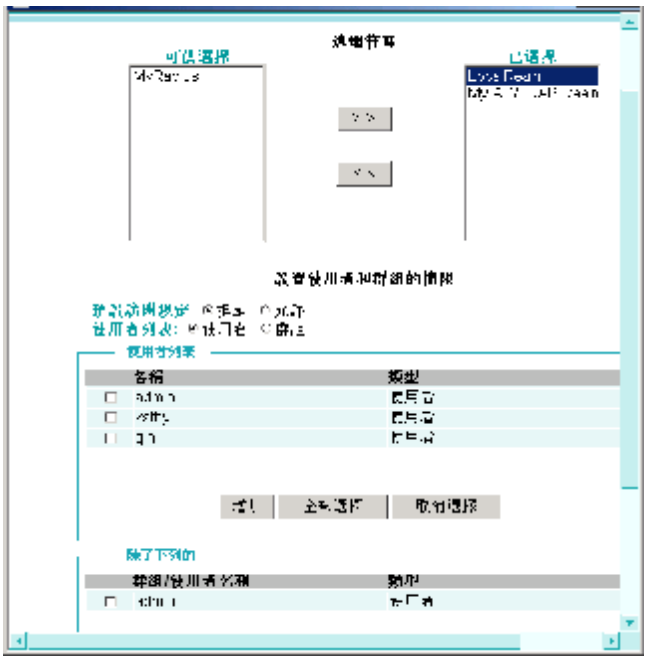


圖 23

圖 24

3.2.7 不同用戶存取 UU200 的方法

Ÿ 使用者

使用者通常從遠端存取 UU200，并訂閱 UU200 所發布的的各類應用。僅具有使用者號的用戶是不能管理 UU200 的。

多個不同的使用者可以同時獲取應用列表。同一使用者可以多次獲取應用列表，前提是 發布應用中勾選了“允許同一使用者多次訪問”。

例如：

- Ø 不同使用者名稱的使用者可以同時獲取應用列表。
- Ø 不同安全域中同名的使用者可以同時獲取應用列表。
- Ø 管理員在發布應用時勾選了“允許同一使用者多次訪問”，則相同安全域中同名的使用者可以同時獲取應用列表。
- Ø 管理員在發布應用時沒有勾選“允許同一使用者多次訪問”，則相同安全域中同名的使用者獲取應用列表時。會將原已連入的會話斷開。

獲取應用列表的方式：通過 IE 瀏覽器，使用者可以在任何一台聯機到網際網路的電腦上輸入：

https:/ /[*uu200 的 IP 位址*] (Direct Access 方式) ，或者，

https:/ /[*uuswitch（ /uuexchange 的 DNS 名稱或 IP 位址*）/[*uu200UUID*] （Private Access 方式）

點選列表中的圖示，點擊滑鼠右鍵，彈出快顯功能表。

點選“配置”一項可以修改該應用程式在該用戶端存放的路徑，還可以設定相應參數；點選“啓動”

一項可以啓動該應用；點選“調試選項”，可以設定調試和收集調試資訊的方式。

調試選項說明如下：

Ÿ 追蹤應用用戶端和伺服器端的資料：

目的：記錄日誌以便跟蹤和調試。

選中該選項後，所有應用用戶端和伺服器端之間的資料都會被記錄在\windows\system32\（或者WINNT\system32\）下的 uuspd.log 文件中。將該文件另存，便可打開進行查看。

“Custom-Network driver based C/S”、Outlook（MS exchange server 模式下）兩種應用不支援該功能。

Ÿ 切換用戶端工作方式：

目前，iSTAR 用戶端允許以兩種方式工作。當用戶端啓動應用出現問題時，可以選擇該選項，切換到另一方式工作。以便排查問題原因。

另外，選中該選項後，請檢查 iSTAR 用戶端各應用配置的參數不能爲功能變數名稱，應該設置成 IP 地址。

Ÿ 直接用戶端資料收發：

目的：測試不通過 iSTAR 的 tunnel，是否可以直接連接遠端伺服器。

iSTAR 用戶端應用列表中的某個應用不能成功啓動時，可以選擇該選項排查問題原因。如果不通過 iSTAR 的 tunnel，可以直接連接遠端伺服器，說明問題是 iSTAR 引起。如果不可達，則說明是可能存在其他因素導致連接失敗。

遠端伺服器：輸入要連接的遠端伺服器的 IP 位址。

遠端埠：輸入要啓動的應用在遠端伺服器上的埠。例如，要啓動 Web 應用，則設置遠端埠爲 80；要啓動 Telnet，則設置遠端埠爲 23。

本地埠：輸入一個本地未被使用的埠，如 1234。

另外，選中該選項後，請檢查 iSTAR 用戶端各應用配置的參數設置。

例如：

Telnet 應用：127.0.0.1 1234

Web 應用：http：//127.0.0.1：1234

使用 UURemote 虛擬連入被發布的子網：用戶可以使用 UURemote 虛擬連入 UU200 所發布出來的子網。通過 IE 瀏覽器，使用者可以在任何一台聯機到網際網路的電腦上輸入：

https://[*uu200 的 IP 位址*]/ra (Direct Access 方式) ，或者，

Ÿ https://[*uuswitch（/uuexchange 的 DNS 名稱或 IP 位址*）/[*uu200UUID*]/ra 本地管理員

本地管理員僅能從本機存取 UU200，通過身份驗證後，登入 UU200 進行管理。本地管理員不能訂閱 UU200 發布的應用。任何時候，只能有一位管理員登入。如果之前未正常登出或已有其他管理員登入，需要先將原登入者停掉。詳細說明請參考“**錯誤! 找不到參照來源。**退出設定介面”。

獲取管理專案列表的方式：通過 IE 瀏覽器，在本機上輸入：

http://1.1.1.2/admin

顯示以下的視窗。輸入正確管理員名稱、密碼。即可登入。

圖 25

Ÿ 遠端管理員

遠端管理員僅能從遠端存取 UU200，通過身份驗證後，登入 UU200 進行管理。遠端管理員如果需要訂閱 UU200 向他發布的應用，請按照使用者方式操作。任何時候，只能有一位管理員登入。如果之前未正常登出或已有其他管理員登入，需要先將原登入者停掉。詳細說明請參考“**錯誤! 找不到參照來源。**退出設定介面”。 但是多個不同的使用者可以同時獲取應用列表。同一使用者也可以多次獲取應用列表，前提是遠端管理 中勾選了“允許同一使用者多次訪問”。

例如：

- Ø 不同使用者名稱的管理員可以同時獲取管理專案列表。
- Ø 不同安全域中同名的管理員可以同時獲取管理專案列表。
- Ø 管理員在發布應用時勾選了“允許同一使用者多次訪問”，則相同安全域中同名的管理員可以同時獲取管理專案列表。
- Ø 管理員在發布應用時沒有勾選“允許同一使用者多次訪問”，則相同安全域中同名的管理員獲取應用列表時。會將原已連入的會話斷開。

獲取管理專案列表的方式：通過 IE 瀏覽器，遠端系統管理員可以在任何一台聯機到網際網路的電腦上輸入：

https://[*uu200 的 IP 位址*]/rm (Direct Access 方式) ，或者，

https://[*uuswitch（/uuexchange 的 DNS 名稱或 IP 位址）/[uu200UUID*]/rm （Private Access 方式）

顯示以下的視窗：

圖 26

在圖 26 所示介面中輸入身份認證所需要素，點擊<確定>之後，可獲取管理專案列表（如圖 27 視窗），遠端系統管理員啓動“Admin”圖示，輸入對應的管理員帳號和密碼，便可以對 UU200 進行遠端管理。（如果 Admin 等服務需要證書驗證身份，則還需在圖 28 所示介面中選取正確的證書）

點選列表中的圖示，點擊滑鼠右鍵，彈出快顯功能表。

點選“配置”一項可以修改該應用程式在該用戶端存放的路徑，還可以設定相應參數；點選“啓動”一項可以啓動該應用；點選“調試選項”，可以設定調試和收集調試資訊的方式。

調試選項說明參見本章節關於“使用者”存取 UU200 的內容：

任何時候，只能有一位管理員登入管理介面。如果之前未正常登出或已有其他管理員登入，需要先將原登入者停掉。詳細說明請參考“**錯誤! 找不到參照來源。**退出設定介面”。 但是多個不同的使用者可以同時獲取應用列表。同一使用者也可以多次獲取應用列表，前提是 遠端管理 中勾選了“允許同一使用者多次訪問”。

例如：

- 不同使用者名稱的管理員可以同時獲取管理專案列表。
- 不同安全域中同名的管理員可以同時獲取管理專案列表。
- 管理員在發布應用時勾選了“允許同一使用者多次訪問”，則相同安全域中同名的管理員可以同時獲取管理專案列表。

管理員在發布應用時沒有勾選“允許同一使用者多次訪問”，則相同安全域中同名的管理員獲取應用列表時。會將原已連入的會話斷開。

& 說明：

- 如果身份認證在 LocalRealm 上進行，則僅需要輸入 LocalRealm 中的使用者名稱及密碼。
- 如果認證在 ACE 伺服器上進行，則請輸入 ACE 伺服器上的使用者名稱及密碼，並在密碼後接著輸入 Token code。（當 Token 的顯示幕顯示的六格短橫杠僅剩一格時，說明該 token code 即將失效，此時請等待 ACE 伺服器分配下一個 code，並輸入這個新的 code。
- 如果認證在其他類型的安全域中進行，則需要輸入相應認證伺服器中的使用者名稱及密碼。

Ÿ 如果在安全域進行認證需要核實 Certificate/PKI，則需要勾選“高級”，並在“證書”欄選擇證書。在安全域中使用的證書與上面提及的 Admin、CLI、Change Password 等服務中使用的證書可以不一樣。

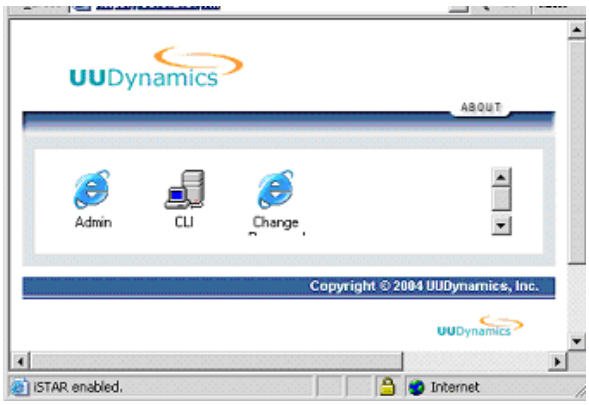


圖 27

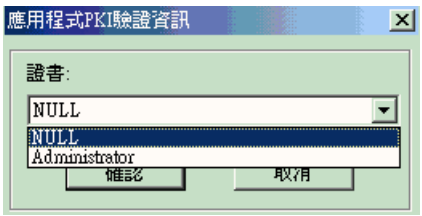


圖 28

在圖 26 所示介面中，勾選“Session 清理”。將會將電腦中的各種與該使用者相關的暫存檔案、cookies 等資訊刪除。點擊<高級>可以指定要清理的專案。系統將在 Session 結束後立即清空，並且不能撤銷，請謹慎操作。

& 說明

使用者使用共用電腦（如網吧電腦）連入 UU200 時，可以考慮此功能，以保護個人資訊安全。

設定項	說明	位置
Internet 瀏覽暫存	清除 Cache 中該使用者的所有臨時的 Internet 檔	[*系統盤符*]:\Documents and Settings\[*username*]\Temporary Internet Files
Internet 瀏覽歷史記錄	清除 IE 中所有的瀏覽頁面的歷史記錄	
Internet Cookies	清除 IE 中的所有 Cookies	[*系統盤符*]:\Documents and Settings\[*username*]\Cookies
鍵入的 URL	清除 IE 位址欄裏的所有的 URL 記錄	

自動填充表格	清除 IE 上所有表單中自動填充部分的內容	
自動填充密碼	清除所有自動填充的密碼	
Internet 收藏	清除該使用者在 IE 收藏夾裏的所有內容	[*系統盤符*]:\Documents and Settings\[*username*]\Favorites
暫存檔案	清除所有的暫存檔案	
Telnet 歷史記錄	清除該使用者在本機上所有的 Telnet 記錄	
垃圾箱	清空系統盤符下的垃圾箱	
運行歷史記錄	清除 Windows“開始->程式”功能表中的最近運行程式的記錄列表	[*系統盤符*]:\Documents and Settings\[*username*]\Start Menu\Programs
最近的文檔	“開始->文檔”功能表中的最近開啓文檔的記錄列表	[*系統盤符*]:\Documents and Settings\[*username*]\Recent
最後登入使用者	清除上一次登入的使用者名稱	
查找文件歷史記錄	清除上一次查找檔的搜索結果	
查找電腦歷史記錄	清除上一次查找電腦的搜索結果	
網路歷史記錄	清除“網路芳鄰”中所有的映射目錄	[*系統盤符*]:\Documents and Settings\[*username*]\NetHood

3.3 安全管理

3.3.1 設定加密 / Hash 演算法

在系統主介面中（圖 3）的“安全管理”下，按下加密管理， 會出現如圖 29 的視窗； 用來選擇對資料的加密演算法和 Hash 演算法，以確保資料傳輸的安全。

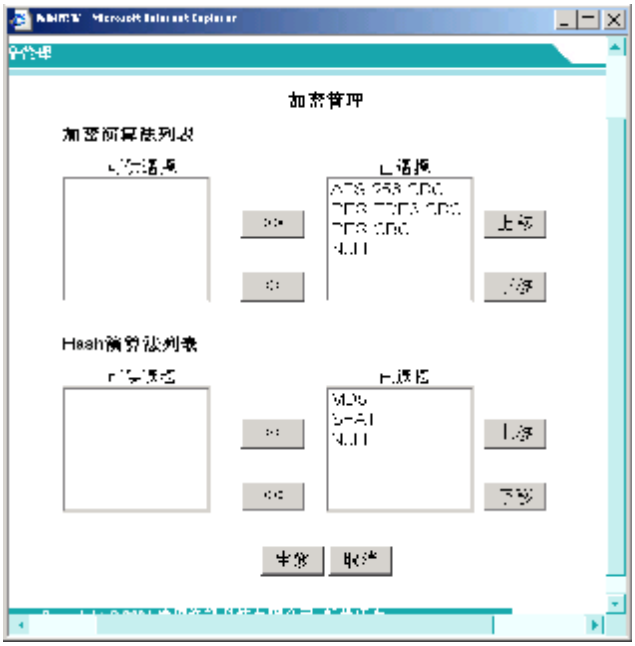


圖 29

右邊“已選定”列表內的是當前被啓動且使用中的加密和 Hash 演算法； 如果使用者想要停止其中任何一種或多種的加密和 Hash 演算法， 可以使用 << ，將其移至左邊的“可選擇”列表內； 反之可以使用 >> ，將其再加回到右邊的“已選定”列表內。

在“已選定”列表右側的<上移>以及<下移>，用於調整各種加密和 Hash 演算法的協商優先等級； 在上端的優先等級較高，在下端的優先等級較低，使用者可以根據實際狀況自行調整。

3.3.2 會話管理

會話管理功能用於查看或強制結束當前連入的會話。一旦使用者遠端登入系統，并成功獲得應用列表（即：能看到 UU2100 發布出來的應用的圖示），會話即已建立起來了（該類會話也被稱爲 command tunnel）。

在系統主介面中的“安全管理”之下，按下 會話管理 出現如圖 30 的視窗；視窗上會顯示當前所有的活動的 command tunnel(s)資訊，即所有連入 UU200 并獲得應用列表的使用者的相關資訊。

可以在“現役的使用者列表”中選中會話記錄，將其強制斷開。

圖 30

3.4 網路設定

3.4.1 設定連接方式

UU200 支援兩種接入方式：Direct Access 和 Private Access。系統預設爲 Direct Access 連接方式。

使用者可以在主介面（圖 3）中點選“網路設置”下的 iSTAR 設置，進入設定介面變更接入方式（如圖 31）。（如果此時正在安裝軟體，則系統會自動跳轉到設定介面圖 31，繼續以下設定步驟。）

- Direct Access 方式

該方式下，遠端使用者可以通過 UU200 的公共 IP 位址直接存取該台 UU200 所發布的應用或對它進行遠端管理。存取應用時，在使用者端的 IE 5.0（或以上）的地址欄輸入“https://[*UU200 的公共 IP 位址*]”。如果要進行遠端管理，則輸入“https://[*UU200 的公共 IP 位址*]/rm”。

這種連接方式通過在 UU200 上使用數位電子憑證向使用者證明自己的身份。您可以使用默認的數位電子憑證，也可以另行購買第三方證書。

1. 在圖 31 所示介面上，點選倒三角鍵下拉功能表，選擇“Direct”連接方式。
2. 如果您需要導入準備好的第三方的證書。請點擊<輸入>，輸入該證書對應的 Key 文件，證書檔和 CA 的證書檔，所有檔要求是 Base64 編碼方式，如圖 32 所示。
3. 最後按<生效>，使當前的連接模式設定生效。

- Private Access 方式

該方式下，UU200 與一台或多台 UUSwitch/UUExchange 相連。遠端使用者必須經由其中一台 UUSwitch/UUExchange 連接到該台 UU200。一台 UUSwitch/UUExchange 可接入多台 UU200，每台 UU200 由該 UUSwitch/UUExchange 分配一個唯一的有效標識（即 UUID 檔案。在安裝前，請

先聯繫 UUSwitch/UUExchange 管理員獲取壓縮的 UUID 檔案）。

因此，Private Access 方式優於 Direct Access 方式之處在於：該模式下，只需通過 UUSwitch/UUExchange 的公共 IP 位址即可存取多台 UU200。

存取應用時，在使用者端的 IE 5.0（或以上）的地址欄輸入“https://[*uuswitch 或 uuexchangeDNS 名稱/IP 地址]*/[*UU200 的 UUID*]”。如果要進行遠端管理，則輸入“https://[*uuswitch* 或 *uuexchangeDNS 名稱/IP 地址]*/[*UU200 的 UUID*]/rm”。

這種連接方式通過在 UUSwitch/UUExchange 上使用數位電子憑證向使用者證明該 UU200 的身份。具體內容請參見“UUSwitch 使用者手冊”。

1. 在圖 31 所示介面上，點選倒三角鍵下拉功能表，選擇“UUSwitch/UUExchange”。
2. 導入 UUID 檔案，並輸入產生該檔案的 UUSwitch/UUExchange 的 IP 地址或 DNS 名稱。如圖 33。
3. 最後按<生效>，使當前的連接模式設定生效。

圖 31

圖 32

圖 33

3.4.2 設定網路參數

在系統主介面中（如圖 3）的“網路設置”之下，按下網路設置。系統會根據當前的網路模式自動跳轉到相應的頁面繼續以下設定步驟。）

- 單模式的網路設定

點選單模式，可以進入圖 34 所示的介面。詳細設定步驟請參見“**錯誤! 找不到參照來源。**安裝軟體”章節中的 C-2～C-4。

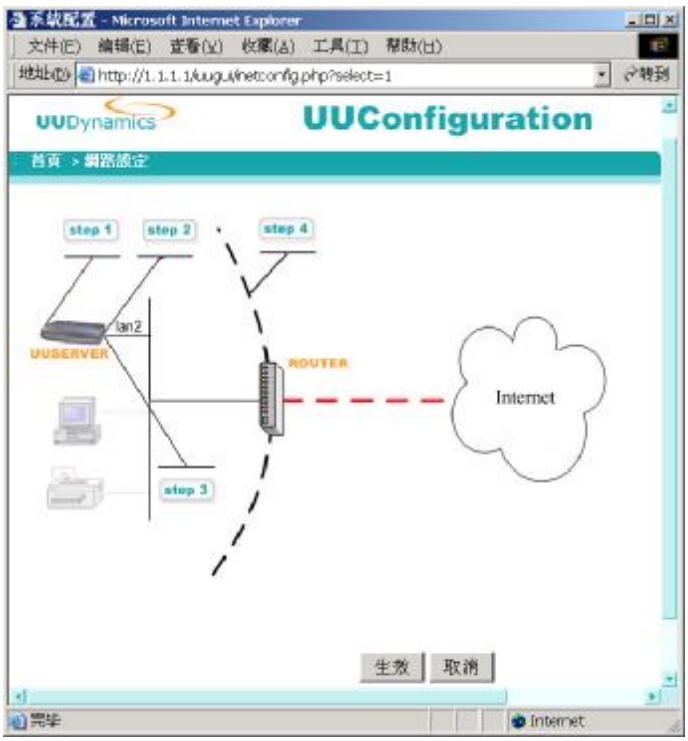


圖 34

& 說明：

在網路基礎設定已完成幷生效後，當系統管理員重新進入此設定步驟中改變“步驟 1、2、3、4”上的某些設定幷使之生效後，選上“啓用系統恢復”並在“在 □ 分鐘之內”設定相應的時間（如 5 分鐘），表示如果在 5 分鐘內，無法連接到 UUSwitch/UUExchange，網路設定將自動恢復爲原來（改變前）的網路設定。其他模式也相同。

- 透明模式的網路設定

點選“透明模式”，進入圖 35 所示介面。詳細設定步驟請參見“**錯誤! 找不到參照來源。**安裝軟體”章節中的 C-5～C-8。

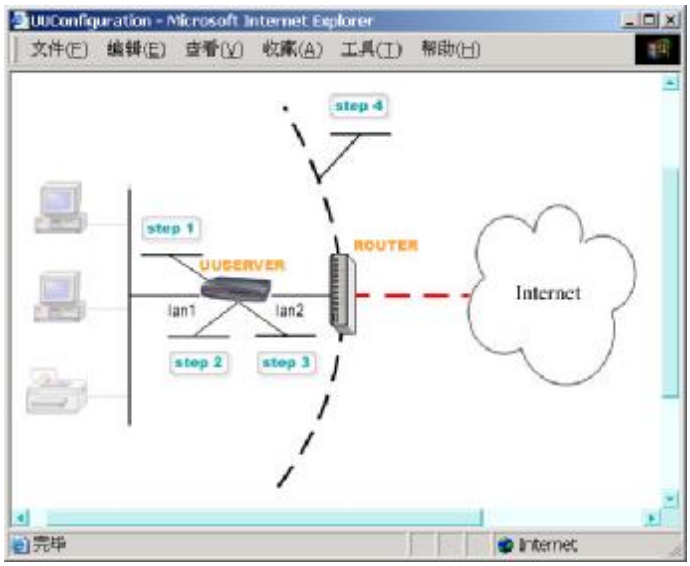


圖 35

- 路由模式的網路設定

點選“路由模式”，進入圖 36 所示介面。詳細設定步驟請參見“**錯誤! 找不到參照來源。**安裝軟體”章節中的 C-9～C-12。

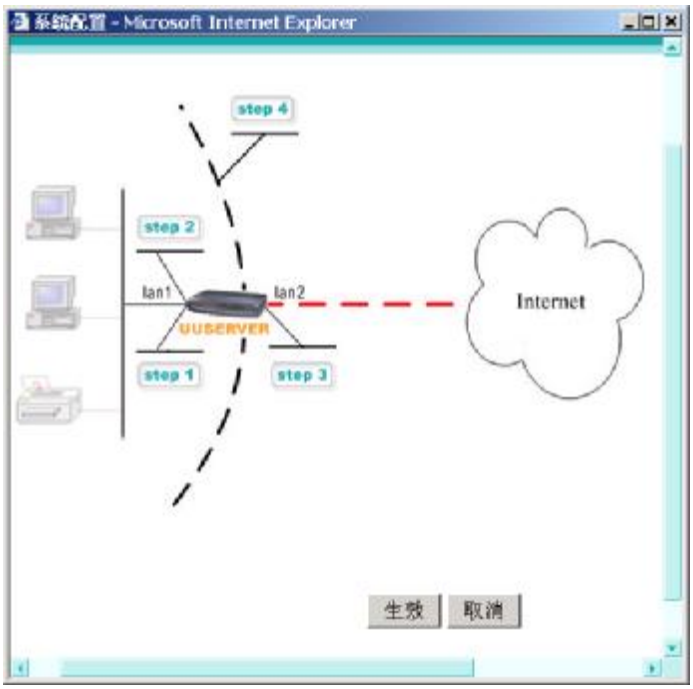


圖 36

3.5 系統維護

UU200 爲系統管理員提供以下系統管理功能：輸入和輸出系統設定，察看日誌以及日誌和報警等級的設定等。

3.5.1 匯入（/匯出）系統的設定資訊

在圖 3 的視窗中，會顯示如圖 37 所示的視窗，將原來保存好的配置檔案匯入到系統中。

圖 37

按<瀏覽…>，選擇你原先匯出的系統配置檔案（參見本節“設定匯出”的內容），然後按下面的<輸入

>，系統會提示下列資訊（圖 38），

圖 38

按 <確認>鍵，配置匯入完成。

在圖 3 的視窗中，選擇在“系統管理”下的設定匯出，會顯示如圖 39 所示的視窗，可以將配置檔案輸出到一個指定的檔案路徑，以複製檔案的形式保存起來。 您可以選擇匯出基本配置，匯出有關服務器資訊的配置，或是匯出整個系統配置。

圖 39

3.5.2 管理許可證

許可證用來控制可以連接到 UU200 的最大併發使用者數。UU200 出廠時預設一個允許 100 個併發使用者的許可證。我們額外提供 UURomote 和 UUSoft 的許可證，如果需要可以向我們購買這兩種額外的許可證。

& 說明：

UURomote 允許使用者從遠端通過 UU200 虛擬連入企業內部網路。

UUSoft 允許使用者使用命令行對 UU200 進行管理。具體使用方法請參考《UUSoft 使用手冊》。

如果您已購買額外的許可證，可以通過以下步驟升級許可證：

1. 點選“系統管理”下的管理許可證，進入下圖所示介面（圖 40）

圖 40

2. 點擊<上傳>，在圖 41 所示介面中點擊<瀏覽>，選擇要替換的證書的完整路徑和檔案名，點擊<確認>。

圖 41

3. 最後按<生效>，使設定生效。

3.5.3 更新、升版系統

您可以在本機或者通過遠端按照以下操作步驟升級系統版本：

1. 點選“系統管理”下的升版系統，進入圖 42 所示介面。

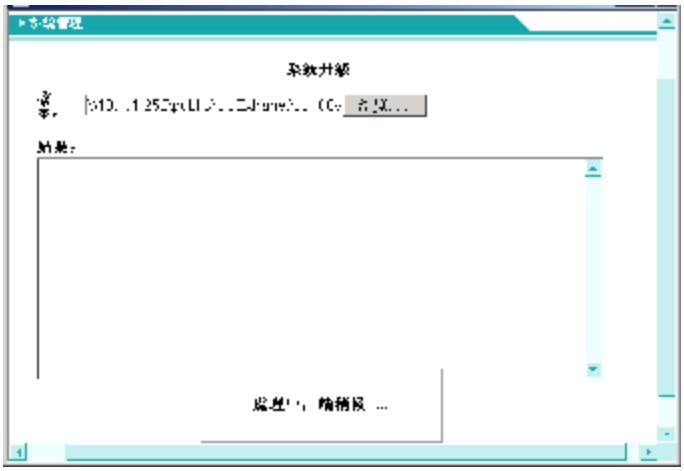


圖 42

2. 點擊<瀏覽…>，選擇新版本的安裝程式的完整路徑和檔案名，點擊<更新>，系統將自動進行版本升級，并在升級完成後，彈出提示框要求使用者重新登入（見圖 43）。

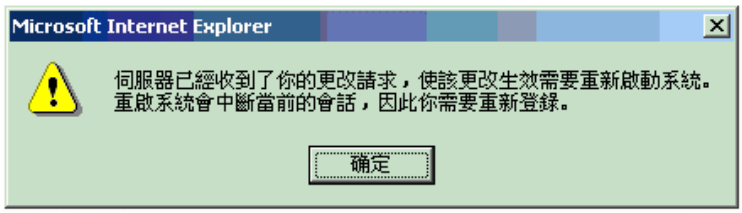


圖 43

重要：

在點擊<更新>升級系統後，而提示框未出現之前，請不要人爲中止升級過程，否則，會導致 UU200 系統發生嚴重後果。

3.5.4 故障檢修

我們爲您提供了三種常用的網路檢測工具：

ping：檢測遠端主機或本地主機的連通性

traceroute：檢測從本地主機到遠端主機的路由

netstat：顯示網路連接、路由表和網路介面資訊

您可以方便得在 UU200 的管理介面下使用這三種標準的檢測工具，監視和分析現有網路狀態，檢測網路連接性。(圖 44)

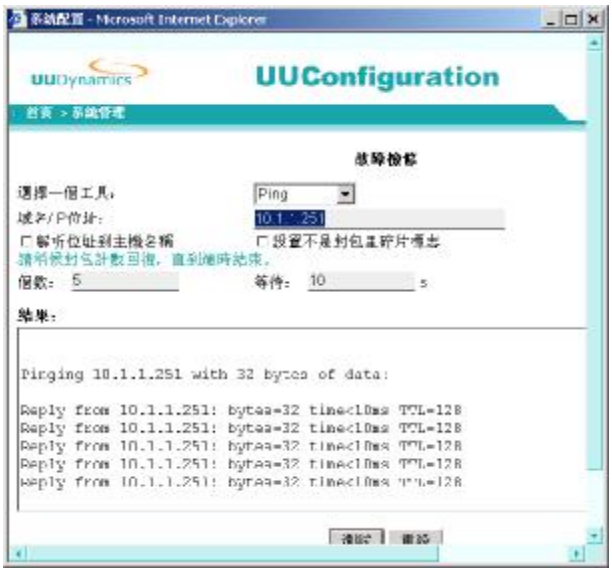


圖 44

3.5.5 顯示狀態

點選“系統管理”下的顯示狀態，可進入圖 45 所示介面查看系統當前的狀態，包括：UUID、運行狀態、路由表、當前版本等資訊。

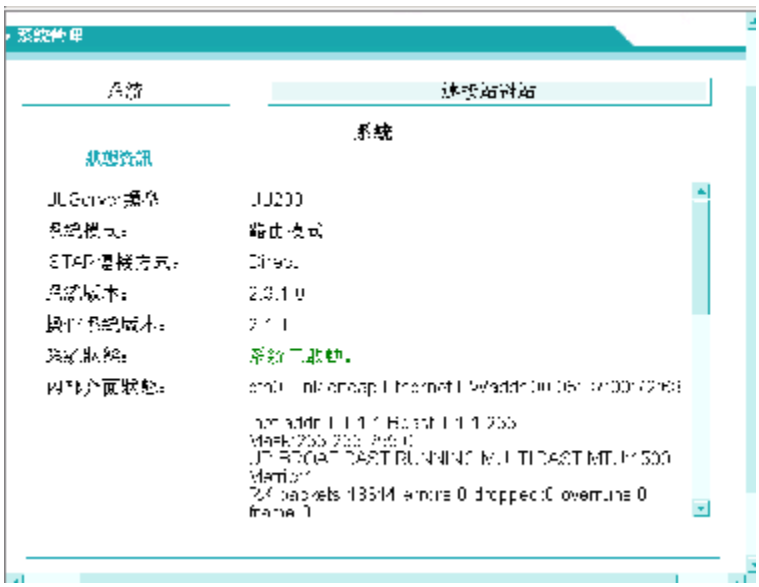


圖 45

3.5.6 查看系統性能

在圖 3 的視窗中，選擇在“系統管理”之下的查看系統性能，可以選擇不同的專案進行查看：

- “Remote desktops”：查看連入 UU200 的連接數或者使用者訂閱應用時 UU200 所使用的 data tunnels。
- “Remote Subnet”：查看連入 UU200 所發佈的 Subnet 的連接數目。
- “UUSoft”：查看連入 UU200 的 UUSoft 數目。
- “System Utilization View”：查看 UU200 硬體的 CPU 和 Memory 的使用情況。

如圖 46 中所示，座標圖中的橫軸爲時間點，縱軸爲數量。不同顏色曲綫代表不同的跟蹤項的數量變化軌跡。如果近期 Remote desktops 的數量持續逼近許可證數值，則說明該 UU200 的使用者數量已趨近最大值，此時應該考慮購買更多許可證以滿足日漸增長的需求。

點擊<顯示>，靜態顯示選定時間段的統計資訊；

點擊<現今>，動態顯示即時的統計資訊；

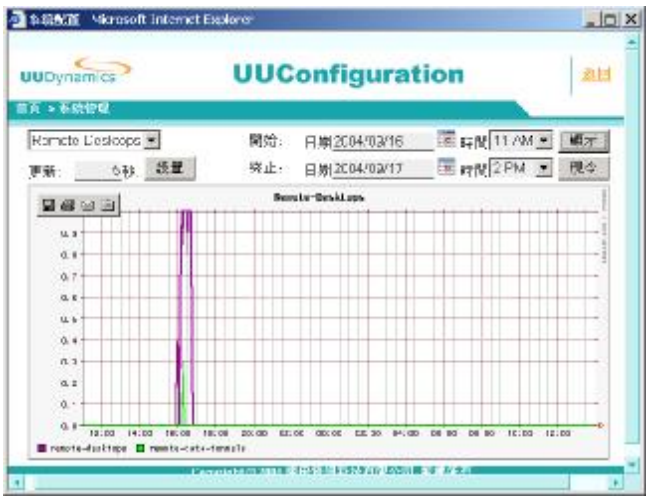


圖 46

3.5.7 日誌等級的設定

在圖 3 的視窗中，選擇在“系統管理”之下的日誌控制，會顯示如圖 47 所示的視窗，系統管理員可以進行系統日誌的設定。

圖 47

其中，“日誌類型”是指定日誌保存的地方。有“本地”和“遠端”兩種： Local 是指將 UU200 的日誌保存在本機上，而 Remote 可以將 UU200 的日誌保存在遠端的 syslog 日誌伺服器上。

“日誌等級”是指顯示和保存的日誌詳細程度，總共有 0～6 級，等級越高，日誌越詳細， 系統管理員可以根據實際需要來設定。以下是每一級別所代表的含義：

級別	含義
0	No log（不記錄日誌）
1	any condition that demand immediate attention（應該立即被糾正的情況）
2	critical conditions like hardware problems（嚴重情況）
3	any errors（一般性錯誤）
4	any warnings（警告）
5	conditions that may require attention（要注意的消息）
6	informational messages（資訊消息）

勾選選中收集調試資訊核取方塊後，系統會將 debug 資訊寫入 Log 文件。

3.5.8 查看日誌

在圖 3 的視窗中，選擇在“系統管理”之下的查看日誌，會顯示如圖 49 所示的視窗。

系統管理員可以自行選擇查看特定時間段間的系統日誌；系統管理員還可以自行選擇查看由 Level 0 到 Level 6 不同等級的日誌情況，越高的 Level 表示日誌的記錄越爲詳細。等級 0～6 的含義請參見“**錯誤! 找不到參照來源。**日誌等級的設定”

系統管理員可以選擇保存日誌，以便日後使用。 在設定了要查看的日誌時間範圍以及等級之後，按下<顯示>，可以顯示在設定條件下的全部日誌；

按<保存顯示日誌>，則可以將螢幕上顯示的日誌保存到指定檔案路徑。初次進入這個介面，會彈出安裝 ActiveX 的提示介面。 您必須按<是>，才能繼續完成輸出配置檔案。 (這是一個資料下載的控制項，不會對您的系統造成影響)

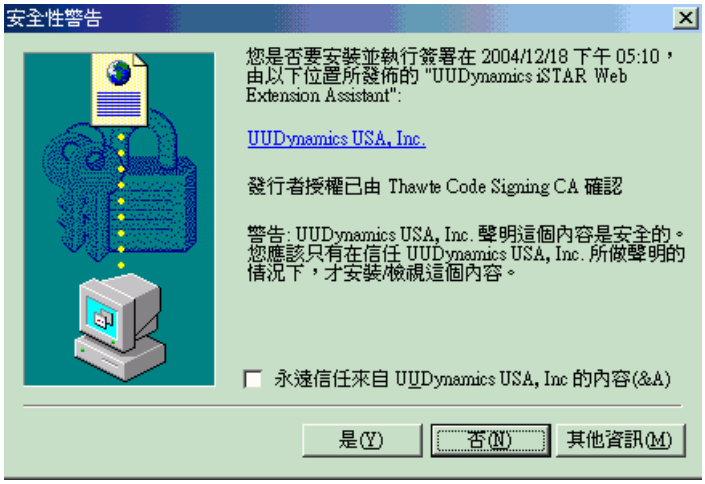


圖 48

如果在設定日誌等級時已勾選了“收集調試資訊”核取方塊，按下<全部保存>,則保存的 Log 檔中不僅包括螢幕上顯示的日誌而且包含系統的 debug 資訊。

注意：

1. UU200 日誌中所紀錄的日期及時間，是根據 UU200 伺服器作業系統的設定日期及時間進行紀錄；您必需確定 Windows 伺服器的日期及時間設定正確，才能獲得正確的日誌紀錄。
2. 日誌資訊[ ]符號外部的內容，爲出錯提示，供使用者參考。[]內部的內容，爲系統內部資訊，供開放人員跟蹤。使用者可以不予理會，如有需要，亦可將其告知我公司技術支援人員。

圖 49

3.5.9 告警等級的設定

在圖 3 的視窗中，選擇在“系統管理”之下的警告通知設定，會顯示如圖 50 所示的視窗。

“告警級別”是指發出警告資訊的日誌級別，例如，設定告警級別爲 5，則表示如果有 5 級及以下的日誌產生的話，就以警告的形式通知系統管理員。

系統管理員可以設定報警等級，并發往指定的電子郵件地址。

圖 50

3.5.10 系統時間設定

在圖 3 的視窗中，選擇在“系統管理”之下的系統設定,您可以修改 UU200 的系統時間（圖 51）。

圖 51

3.5.11 系統 LOGO 設定

在圖 3 的視窗中，選擇在“系統管理”之下的系統設定,您可以修改顯示在左上角的 LOGO 檔（圖 52），您可以使用您公司的 LOGO 替換它，但必須是 gif 檔格式，Size 小於 5KB。

圖 52

3.5.12 SNMP 設定

UU200 支援 SNMP 協定，所有 SNMP 工具或應用可以方便的對 UU200 硬體這個受管節點進行管理。

在圖 3 的視窗中，選擇在“系統管理”之下的 系統設定,您可以設定與 SNMP 相關的資訊。例如：當在 SNMP 工具中顯示的 UU200 的聯繫方式和位置，以便管理員參考（如圖 53）。

圖 53

點擊<新增>，設定哪些機器可以使用 SNMP 工具存取 UU200（如圖 54）

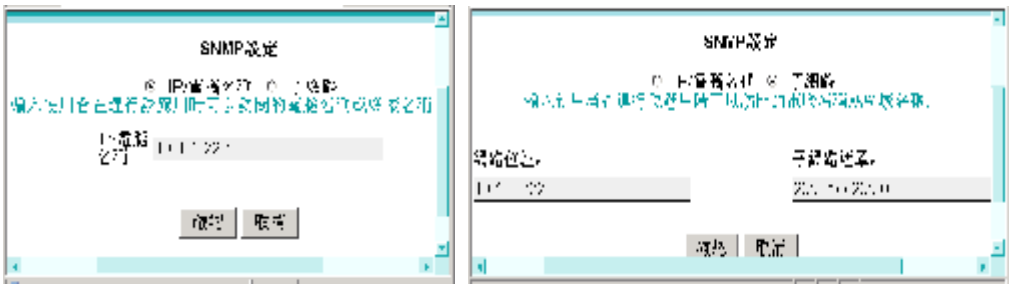
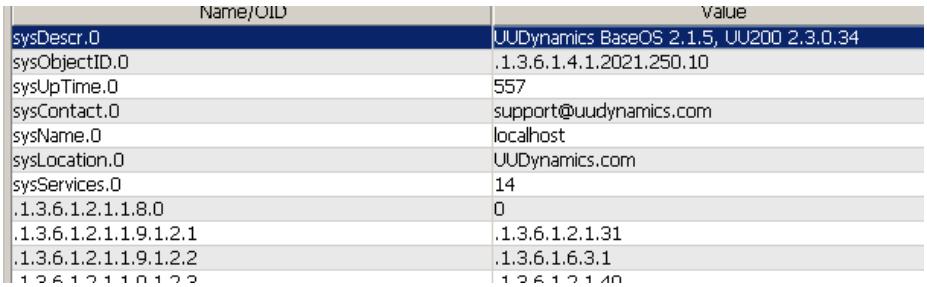


圖 54

例如：添加了一個 IP 位址爲 10.1.1.222 的機器。則在這台機器上運行某個 SNMP 工具，指定 UU200 的

IP 位址後，下列物件 ID（OID） 反映配置檔中的指引值：



Name/OID	Value
sysDescr.0	UUDynamics BaseOS 2.1.5, UU200 2.3.0.34
sysObjectID.0	.1.3.6.1.4.1.2021.250.10
sysUpTime.0	557
sysContact.0	support@uudynamics.com
sysName.0	localhost
sysLocation.0	UUDynamics.com
sysServices.0	14
.1.3.6.1.2.1.1.8.0	0
.1.3.6.1.2.1.1.9.1.2.1	.1.3.6.1.2.1.31
.1.3.6.1.2.1.1.9.1.2.2	.1.3.6.1.6.3.1

圖 55

sysdescr：受管節點的文字說明。圖中該欄的值表示：該受管節點爲 UUDynamics 公司出品的 UU200，硬體的作業系統版本號爲 2.1.5。

sysname：圖中的“localhost”表示 UU200 是 Direct Access 方式。如果 UU200 以 Private Access 方式連接時，該欄顯示該 UU200 的 UUID。

sysservices：指出這個受管節點可能提供的一組服務的值。預設爲 14

syscontact：聯絡的文字識別方式。如果未在圖 53 中設定該欄的值，則該值的字串長度爲 0。

syslocation：這個受管節點的管理指派名稱。依慣例，這是節點的完整網功能變數名稱稱。如果未在圖 53 中設定該欄的值，則該值的字串長度爲 0。

3.5.13 連接埠轉遞

在圖 3 的視窗中，選擇在“系統管理”之下的系統設定，啓用“連接埠轉遞”可以將一個或多個防火墻外部的 IP 位址對應到某個防火墻後面的內網 IP 位址上（圖 56）。

在“外部 IP 位址”輸入列填入外網 IP，點擊<新增>，可以指定新的外網 IP 位址。

選中列表中的外網 IP 位址，點擊<刪除>，可以移除該外網 IP 的對應。

說明：

當多個 UU200 作叢集時，指定的內網 IP 位址不能與叢集中的其他 UU200 的 IP 位址相同，否則會引起衝突。此處指定的內網 IP 位址爲整個叢集的代用 IP。當其他機器存取這個內網 IP 位址時，訪問的實際上是叢集中的任一台 UU200。這樣，當叢集中的某一台 UU200 未能聯機時，負載可以無隙的轉移到叢集中的其他 UU200 上。

圖 56

3.5.14 啓用 DHCP 服務

在單模式和路由模式下，UU200 可以作爲 DHCP 伺服器使用。爲內網的機器動態分配 IP 位址。啓用該服務後，UU200 會強行改變內網的機器原來的 IP 位址，因此請慎用。

選中“僅爲 UURemote，UUSoft 提供服務”核取方塊，則 UU200 只對使用了 UURemote 或 UUSoft 服務的機器動態分配 IP 位址，而不會影響本地網路內的其他機器。

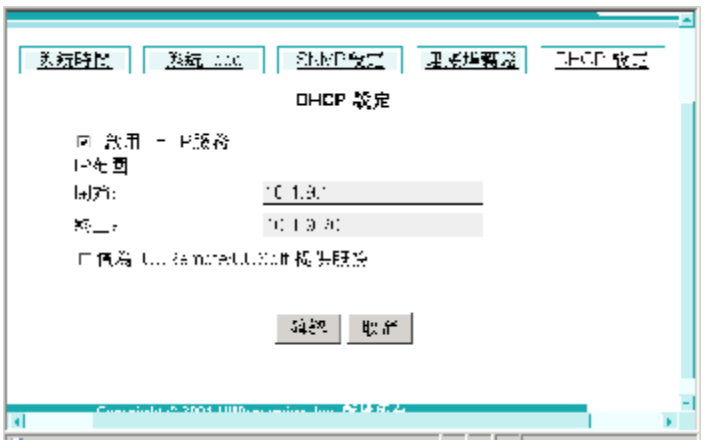


圖 57

3.6 進階

3.6.1 選擇網路模式

如圖 58 所示，UU200 支援“單模式”、“路由模式” 和“透明模式”。三種模式的區別請參考安裝手

冊“術語表”章節。

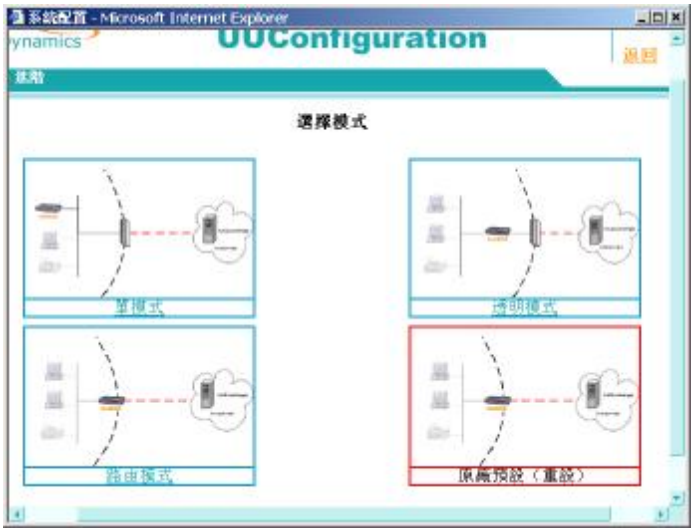


圖 58

按照 UU200 在網路中的位置，點選相應模式。系統會自動保存設定，并彈出提示框提示您稍後重新登入系統。

3.6.2 設定靜態路由

UU200 作爲路由器時可以設定靜態路由表。（僅路由模式支援該功能）

在圖 3 的視窗中，選擇在“進階”之下的靜態路由,進入圖 59 所示介面。

圖 59

選中一條靜態路由記錄,點擊<編輯>,可以修改該條記錄；點擊<移除>,則可以刪除該條記錄；

如果點擊<增加>，則可以進入圖 60 所示介面增加靜態路由。

& 說明：

有兩種路由類型可供選擇：

Net：當下一跳指向的是不同子網中的機器時，需選擇該類型，同時需設定 Netmark 的 IP 地址。

Host：當下一跳指向的是同一子網中的機器時，需選擇該類型，此時不需設定 Netmark 的 IP 地址。

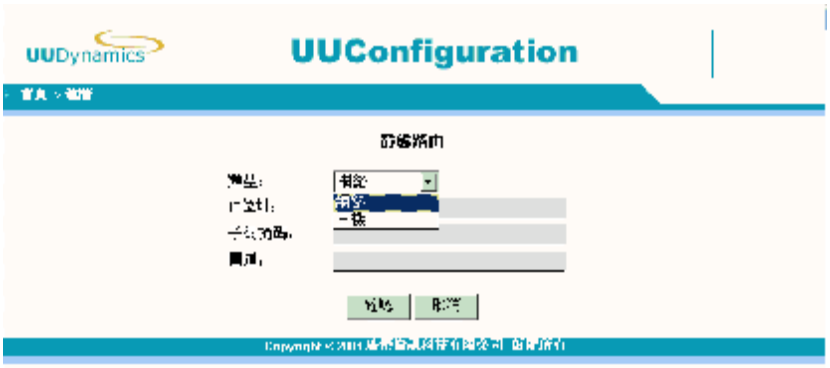


圖 60

3.6.3 連接兩個子網

詳見“**錯誤! 找不到參照來源。**連接兩個子網”。

3.6.4 設定動態非軍事動態區

DMZ（非軍事區）是放置公共資訊的最佳位置，您可以將一些必須公開的伺服器設施，如企業 Web 伺服器、FTP 伺服器和郵件伺服器等這樣的服務放置在這個區域中，而將公司中的機密的和私人的資訊可以安全地存放在內網中，即 DMZ 的後面。這樣使用者、潛在使用者和外部存取者都可以直接獲得他們所需的關於公司的一些資訊，而不用通過內網。

UU200 爲您提供了一種設定和管理 DMZ 的服務——動態 DMZ。所謂動態（Dynamics）的 DMZ，是指您可以根據您現在的網路狀況，靈活的選擇 UU200 所處的位置，您可以將 UU200 配置爲網路中的第一台防火墻，或是將它放在已有防火墻之後，以得到增強的安全性。

UU200 的 DDMZ 通過這一系列安全策略的組合，幫助您將一些在已在 DMZ 中配置好的服務，例如檔伺服器，WEB 伺服器，FTP 伺服器等，發佈給外部存取者和需要這些公共服務的使用者，而不用擔心對公司內部網路的未授權的存取。

設定 DDMZ 服務:

您可以按以下步驟設定 DDMZ 服務：

1. 在圖 3 中點選進階中動態 DMZ，進入圖 61 介面。

到 DDMZ：設定存取 DMZ 的安全策略

系統默認到 DDMZ 資料包的存取策略是“拒絕”，既指拒絕所有到 DDMZ 的資料包。修改這個策略可以設定爲默認到 DDMZ 的存取策略是“接受”。

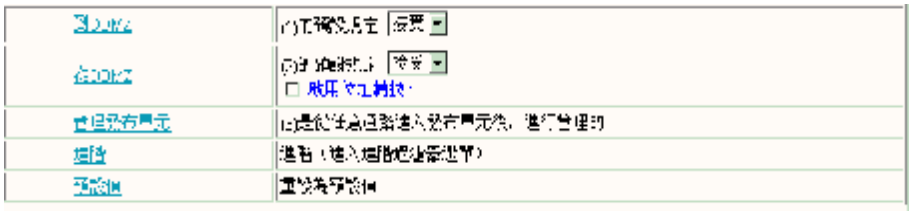


圖 61

2. 點選左面的連接，進入圖 62 頁面。在這一頁面增加與上一部不同的存取策略。例如，上一步中設定拒絕（拒絕）所有到 DDMZ 的資料包，則該頁增加的是允許哪些資料包是可以存取 DDMZ 的；同樣的，如果上一步中設定接受所有到 DDMZ 的資料包，則該頁增加的是拒絕哪些資料包存取 DDMZ。

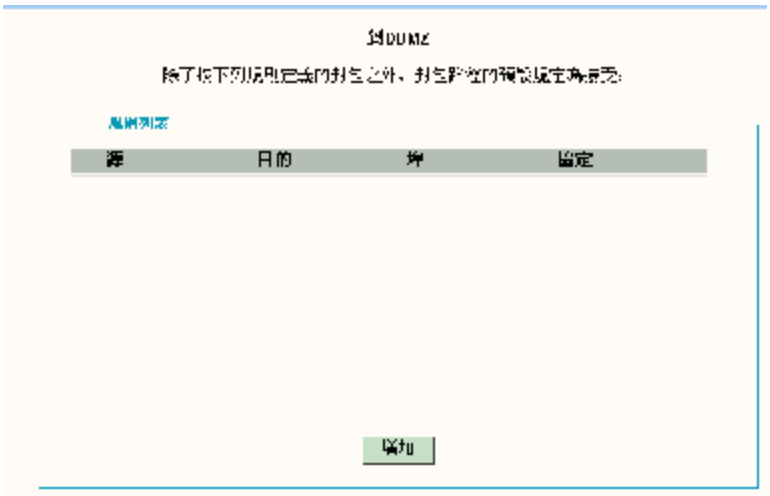


圖 62

點擊<增加>，進入圖 63 介面，增加到 DDMZ 規定。

Dynamic DMZ 服務允許設定總數不超過 100 條的規定，包括到 DDMZ 規定和從 DDMZ 規定。

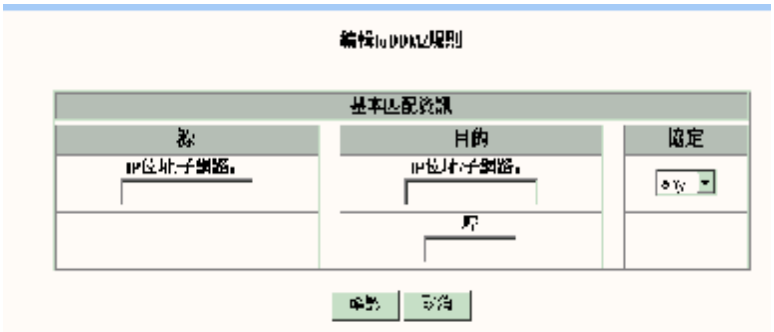


圖 63

源：資料包源，可以是主機，也可是子網。空則表示可以是任何位址的資料包。

目的：資料包目的地，可以是主機，也可是子網。空則表示目的地可以爲 DDMZ 中所有位址。源和目的不能同時爲空。

埠：目的主機埠。

協定：使用的協定。可以設定爲 icmp，tcp，udp，any（所有協定）。

3. 返回圖 62 介面，按<生效>生效。

從 DDMZ：設定從 DMZ 存取外網的安全策略。

系統默認從 DDMZ 資料包的存取策略是“接受”，既指允許所有從 DDMZ 的資料包。修改這個策略可以設定爲默認從 DDMZ 的存取策略是“拒絕”。如果 DDMZ 內的資料包需要存取公共位元元址，而 DDMZ 本身是私有位元元址，則需要選擇“啓用位址轉換”。這個功能使用 NAT 協定翻譯私有位址爲公共位址。

4. 點選左面的連接，進入圖 64 頁面。在這一頁面增加與上一部不同的存取策略。例如，上一步中設定拒絕（拒絕）所有從 DDMZ 的資料包，則該頁增加的是允許哪些資料包是可以從 DDMZ 的；同樣的，如果上一步中設定接受所有從 DDMZ 的資料包，則該頁增加的是拒絕哪些資料包從 DDMZ。

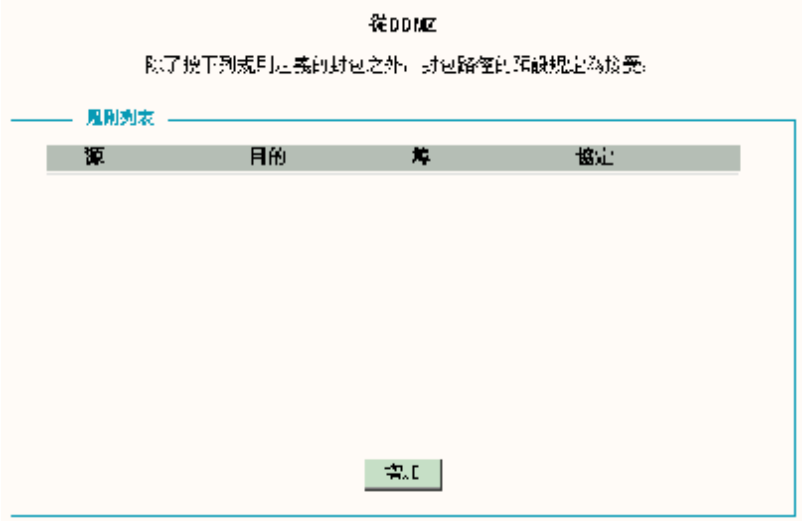


圖 64

5. 點擊<增加>，進入圖 65 介面，增加從 DDMZ 規定。

Dynamic DMZ 服務允許設定總數不超過 100 條的規定，包括到 DDMZ 規定和從 DDMZ 規定。

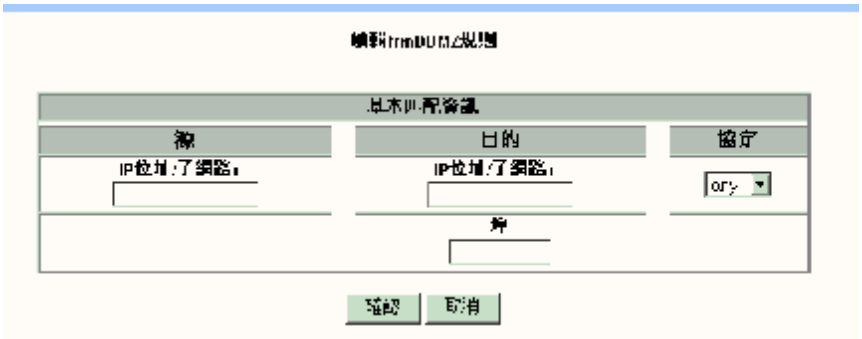


圖 65

源：資料包源，可以是主機，也可是子網。空則表示可以是 DDMZ 中任何位址的資料包。

目的：資料包目的地，可以是主機，也可是子網。空則表示目的地可以爲任何位址。源和目的不能同時爲空。

埠：目的主機埠。

協定：使用的傳輸協定。可以設定爲 ICMP，TCP，UDP，any（所有協定）。

6. 返回圖介面，按<生效>生效。

管理發佈單元：

您可以按以下步驟管理發布，設定存取 uu200 的安全策略

1. 在圖 61 介面中點選管理發佈單元，進入圖 66 介面。

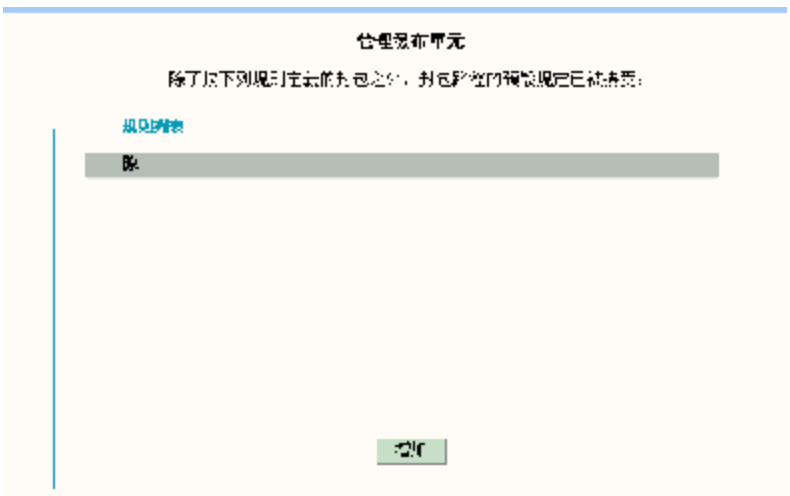


圖 66

系統默認所有機器到 Publisher 的存取都是允許的。在這個頁面中增加規定，設定哪些機器不能存取此台 UU200。

2. 點擊<增加>，進入圖 67 介面，增加存取規定。這邊只需要簡單的增加主機或是子網的 IP 位址就可以了。

圖 67

進階：

你可以在此處進行高級設定。如：更詳細的設定各種資料包的安全策略。其中“送到本機”，“本機送出”，“本機轉送”分別對應於 iptable 中 filter 表的 input，output，forward；pre routing 和 post routing 對應於 NAT 表，實現地址轉換。

以下我們將以設定“送到本機”爲例，簡單介紹如何定制安全策略。其他功能的設定方法也類似，關於 iptable 的具體使用方法請參閱 linux 的幫助文檔和相關資料。

注意：

錯誤的設定這些安全策略可能會破壞您的網路連接性，使某些主機或子網不可達。請謹慎定制這些安全策略，最好是對 iptable 的設定和功能有一定瞭解的網路安全管理員來制定這些安全策略，并在設定後檢測設定是否正確。

1. 點擊<進階>，進入圖 68 介面。
2. 點擊<送到本機>，進入圖 69 介面。
3. 點擊<增加>，進入圖 70 介面，增加規定。Dynamic DMZ 服務允許設定不超過 100 條的規定。

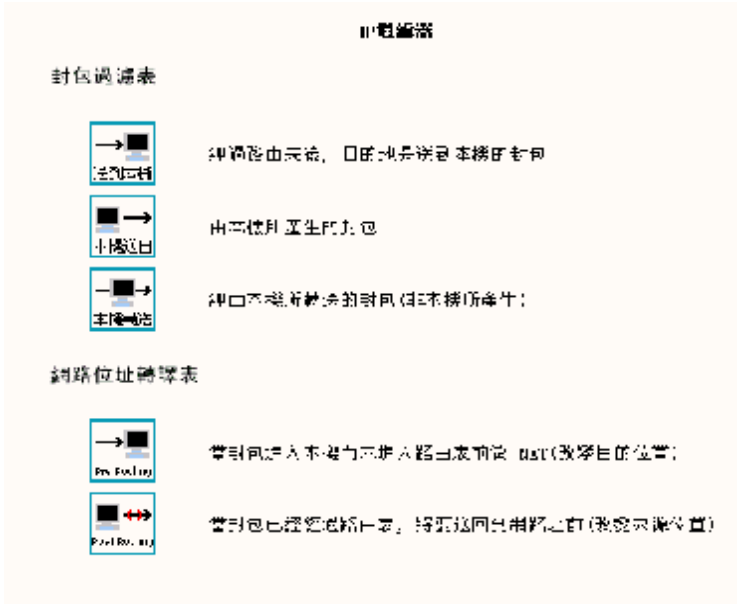


圖 68

圖 69

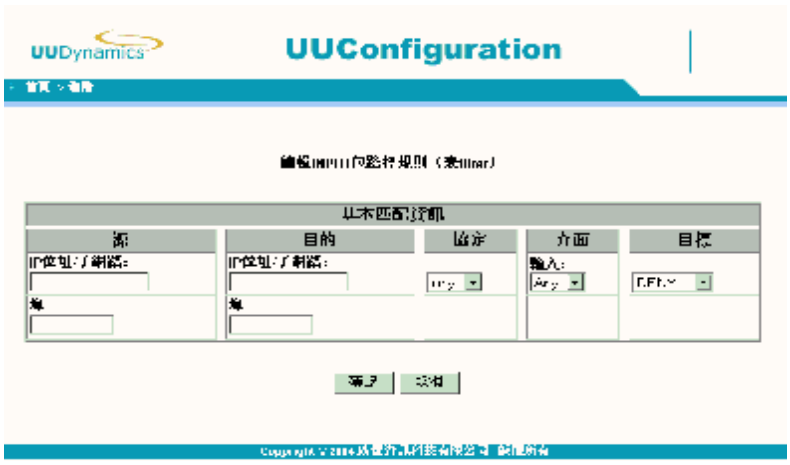


圖 70

源：資料包源的 IP 地址和埠。

目的：資料包目的地 IP 地址和埠。此處，源和目的可以爲空。

協定：使用的傳輸協定，可以爲 ICMP，TCP，UDP，any（所有協定）。

介面：傳輸的方式。Lan1 指到 DDMZ ；Lan2 指從 DDMZ；Lo 指 Local；Any 包含以上三種。

目標：策略目標，拒絕或是接受。

配置後，您還可以修改原有的安全策略。在圖 71 中的 action 有修改，刪除，插入新規定，上移下移規定等功能。

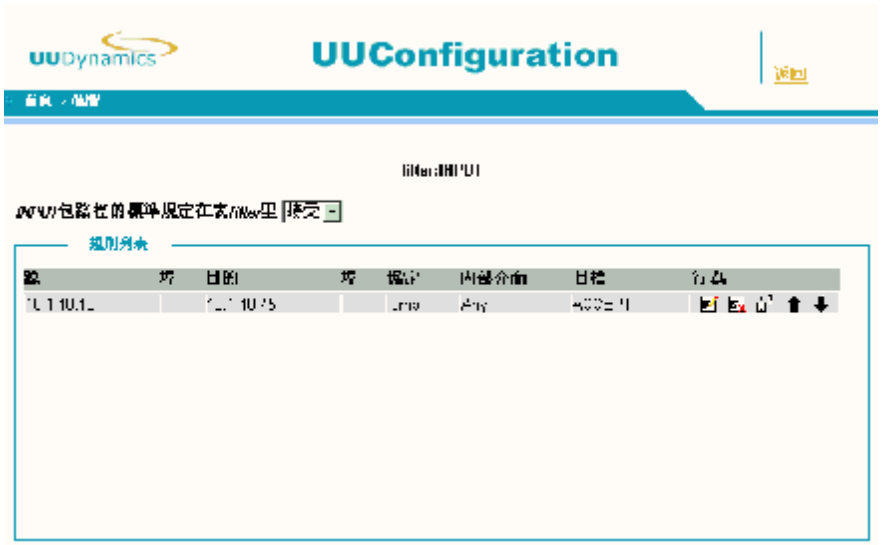


圖 71

預設值：

還原到初始配置狀態。

第4章 應用設定

4.1 發佈應用程式

每個 UU200 能發佈多達 1000 個應用。幷且每個應用允許設定總數不超過 1000 個的接入規定，其中包括：需要接入的機器、需要接入的使用者或者需要接入的埠。

在發布應用程式設定視窗介面中，按下<增加>；您會看到一些預設的應用程式選擇專案,它們計有：Internet Explorer，CVS, Outlook, Telnet, Ftp, Netmeeting, pcAnywhere 等等常用的應用程式； 此外還有一個“Custom”選擇專案，當您要發佈的應用程式不存在於預設的應用程式選擇專案之中，您便可以使用“Custom”來設定該應用程式的發佈。 另外，由 UUDynamics 所提供的遠端檔案瀏覽程式“UUDynamics File Browser”和“UUDynamics File Browser Express”也在選擇專案中。有關“UUDynamics File Browser”和“UUDynamics File Browser Express”的相關配置及使用方法，詳見本使用手冊的附錄部分“**錯誤! 找不到參照來源。**UUDynamics File Browser Express/ File Browser 使用説明”。

有關 ***i*STAR™**支援的客戶/伺服器應用及其所受限制，請參考本使用手冊的附錄部分“**錯誤! 找不到參照來源。** *i*STAR™支援的客戶/伺服器應用”。

如圖 3 主功能表介面，點選“發布”下的 發布應用，進入發布應用程式設定介面（如圖 72）。

4.1.1 增加應用程式

在系統應用程式列表框內，您可以看到預置的應用程式，如：Internet Explorer，CVS, Outlook, Telnet, Ftp, Netmeeting, pcAnywhere 等常用的第三方應用程式；此外還有由 UUDynamics 提供的遠端檔存取軟體 UUDynamics File Browser 和 UUDynamics File Browser Express（其使用方法見本手冊附錄）。如果列表框內沒有需要的應用，您可以自行定制應用。

① 在圖 72 所示介面 ，爲保證遠端使用者存取應用時建立的 SSL 連接的安全，您可以設定允許會話持續的最長時長和允許會話空閑的最長時長。超過設定的時長，系統會自動斷開這次連接。

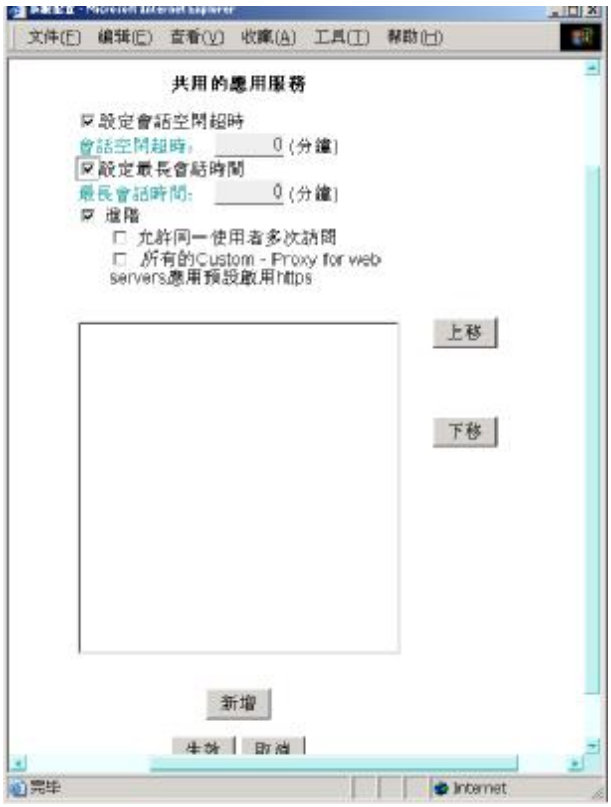


圖 72

② 如果勾選“進階”下的“允許同一使用者多次訪問”，則同一使用者再次(或使用同樣的使用者名稱從其他機器)獲取應用列表時，不影響之前以該使用者名稱獲取應用列表的其他會話。
反之，如果不勾選該選項，則登入時會強行中止之前的所有以該使用者名稱獲取應用列表的會話。

③ 如果勾選“進階”下的“ “所有的 Custom - Proxy for web servers 應用預設啓用 https” ”，則所有 Proxy for web servers 類型的應用(請參見“**錯誤! 找不到參照來源。**定制新的應用程式章節”）使用 https 協定工作。

④ 點擊<增加>，進入圖 73 所示介面。

圖 73

⑤ 選擇列表框內的應用程式 ，點擊<確認> ，進入圖 74 所示介面。

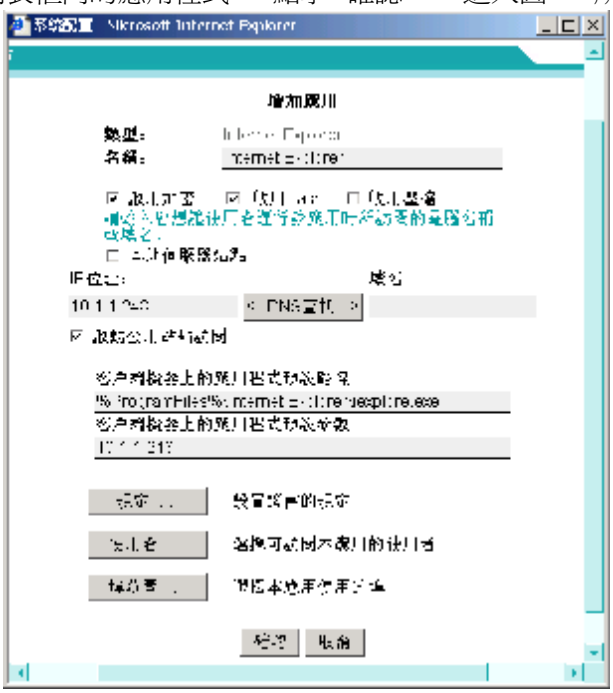


圖 74

⑥ 點擊<規定…>，進入圖 75 所示的視窗。輸入您爲這個策略所取的名稱；目前 UU200 能提供的策略包括：

Ÿ 驗證證書：
可以指定證書，在使用者登入、獲取應用時驗證用戶端是否提供了正確的證書。此外，還可以對該證書設定限制條件。。

Ÿ 限制存取時間：
如果要限制使用者的存取時間，可以選中“存取時間限制”核取方塊，幷輸入約束條件。

約束條件所遵循的語法結構與設定 Radius 伺服器的規則類似，其語法結構爲：
time.[屬性名稱] [操作符] [屬性值]（或另一 [系統變數名稱].[屬性名稱]）。

& 說明：
此處的 time 爲表示時間的系統變數名稱。
屬性名稱包括 year, month, day, hour, minute, second, week。其中，
year 表示 4 位數年份；**month** 表示 2 位數月份；**day** 表示 2 位數的日期；
hour 表示小時（按 24 小時制）；**month** 表示分鐘；**second** 表示秒；
操作符 是 sql 的操作符，如 =,!=,>,<,like,in 等。

舉例：下面的約束條件限制了使用者只能在 2005 年，8:00～18:00 驗證身份，并在驗證成功後存取應用列表：
(time.year =2005) and (time.hour between 8 and 18)

Ÿ 檢測用戶端運行環境：
如果要檢測用戶端的運行環境是否符合要求，可以點擊<管理主機檢查器>。選擇在安全域設定時預先加入的檢測規則。
在”符合時便停止”列中，點選“不是”：則檢測到符合該規則後，繼續檢測下一規則；如果不符合該規則，則拒絕該使用者登入。
在”符合時便停止”列中，點選“是”：則一旦檢測到符合該規則後，即停止繼續檢測，允許該使用者以遠端管理員身份登入管理介面。。如果不符合該規則，則拒絕該使用者登入。

說明：
Ÿ 在“符合時便停止”列中選擇“是”的規則應被放置在所有選擇“不是”的規則之後，否則當用戶端的運行環境符合該條設定爲“是”的規則後，將不會繼續檢測，這樣，其後的規則將不會再有機會被檢測。
Ÿ 如果“防病毒類型”和“作業系統類型”兩種類型都有規則被選中，則要求同時檢測用戶端主機安裝的防病毒軟體和系統設定（系統設定包括：作業系統版本、系統安全補丁、應用的安全補丁等）。只要不符合這兩種類型中的任何一條規則，該用戶端都無法登入。

Ÿ 檢測校驗碼
該功能用於防止非法或有潛在威脅的用戶端應用程式攻擊應用伺服器。例如被病毒或木馬篡改的應用程式的校驗碼必定與合法應用程式的校驗碼不同，這樣，當使用者嘗試連入時，iSTAR 只要驗證用戶端運行的程式的校驗碼和伺服器端爲該程式設定的校驗碼是否一致，便可以判定用戶端的應用程式是否合法。如果合法，則該項驗證通過，否則使用者將不能啓動該應用。
校驗碼採用 SHA 1 演算法。

⑦ 如果要限制使用者的存取時間，可以選中“存取時間限制”核取方塊，并輸入約束條件。
約束條件所遵循的語法結構與設定 Radius 伺服器的規則類似，其語法結構爲：
time.[*屬性名稱*] [*操作符*] [*屬性值*]（或另一 [*系統變數名稱*].[*屬性名稱*]）。

& 說明：
此處的 time 爲表示時間的系統變數名稱。
屬性名稱包括 year, month, day, hour, minute, second, week。其中，
year 表示 4 位數年份；**month** 表示月份；**day** 表示日期；
hour 表示小時（按 24 小時制）；**month** 表示分鐘；**second** 表示秒；
操作符 是 sql 的操作符，如 =,!=,>,<,like,in 等。

舉例：下面的約束條件限制了使用者只能在 2005 年，8:00～18:00 之間驗

證身份，并在驗證成功後存取應用列表：

(time.year =2005) and (time.hour between 8 and 18)

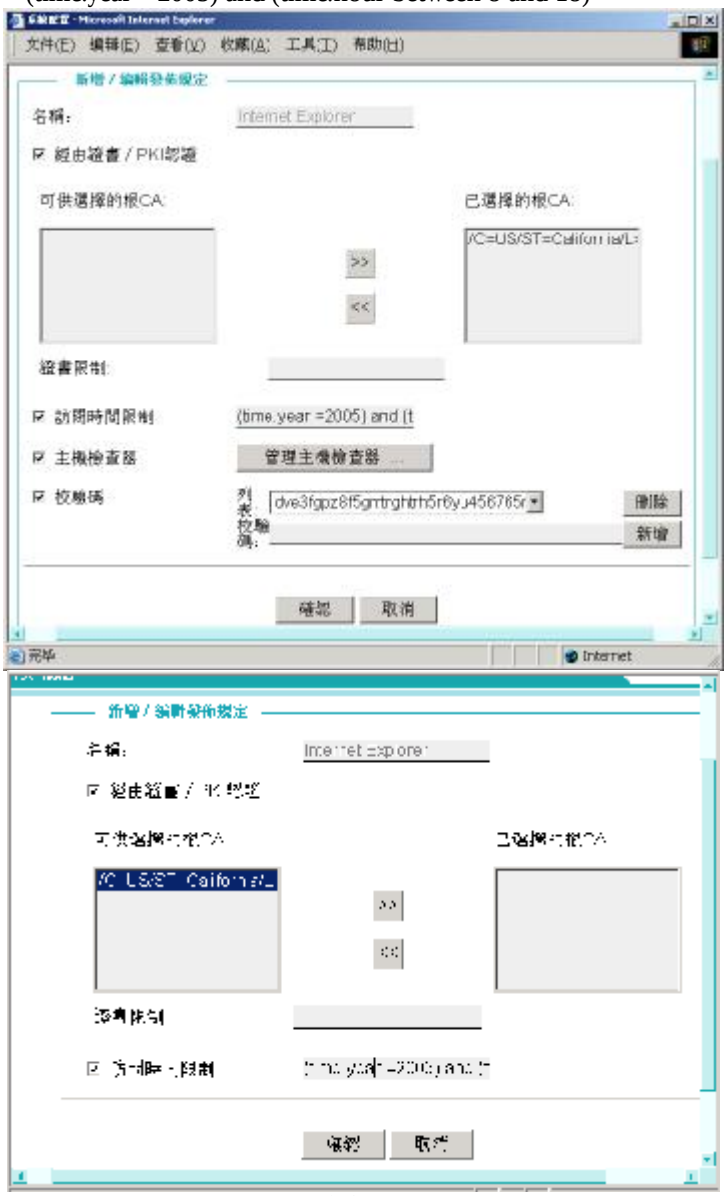


圖 75

⑧ 輸入共用應用程式所在伺服器的 IP 位址等相關資訊，點擊<使用者…>，根據需要增加使用者（/群組/角色）。進入圖 76 所示的視窗；選擇使用者（/群組/角色）所在的安全域。如果選擇的是包含有角色角色資訊的 Radius 或 PKI 類型的安全域，會顯示圖 77 所示的操作介面。

圖 76

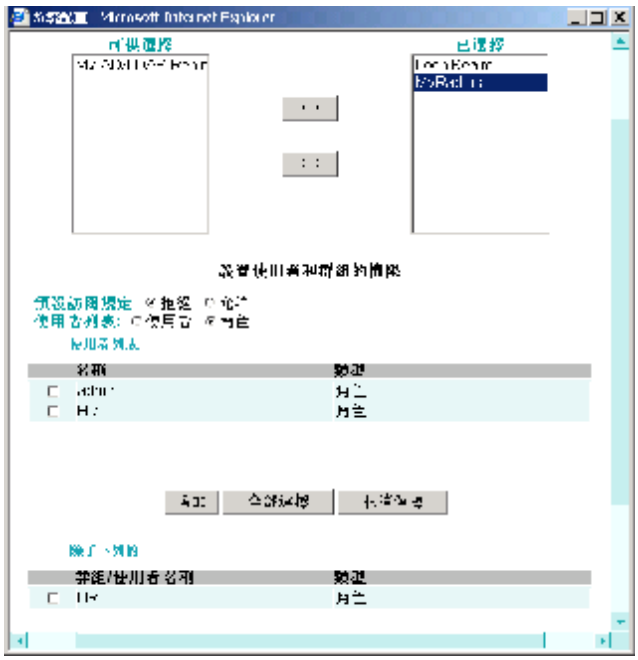


圖 77

⑨ 設定該應用的訂閱策略，系統預設的是“拒絕”，意即所有的使用者都不能訂閱該應用。

⑩ 在“使用者列表”中指定排除在訂閱策略之外方式。在其下的“使用者列表”列表中勾選使用者（/群組/角色），並按<增加>將其加入下方的“已選定的使用者”目錄中；重復在“使用者列表”中勾選，並按<增加>，可以繼續加入多個使用者（/群組/角色）。

通過這一步驟結合設定訂閱策略步驟相結合，管理員可以靈活的設定應用的使用範圍，即：僅允許某一些使用者訂閱所發佈應用，或者允許除某一些使用者外的所有使用者訂閱。

⑪ 點擊<埠範圍>，進入圖 78 所示介面。設定開放的埠。

您也可以點擊<增加>，進入圖 79 所示介面，增加新的埠。

埠設定完成後，點擊<返回>返回圖 74 介面。

圖 78

圖 79

注意：

① “名稱”、 “啓用加密/Hash/壓縮”、 “該應用在使用者端機器上的默認路徑”、 “使用者端機器運行該應用時所需的參數”、 <使用者…>注釋同圖 74 下的表格説明。

② 點選 <電腦…>，進入設定允許或拒絕存取該共用應用程式的電腦的相關資訊介面（如圖 82）。

– <所有電腦>：點擊<增加>鍵，設定不被允許存取的電腦，表示允許已共用的 subnet 裏的所有電腦都允許被存取，除了在列表裏設定的電腦不被允許存取外。
例如，當使用者要將其已共用的子網上的 100 台電腦中的 98 台允許被存取，而其中的 2 台不被允許存取時，可用此功能。

– <無電腦>：點擊<增加>，設定被允許存取的電腦，表示允許已共用的子網裏的所有電腦都不被允許存取，除了在列表裏設定的電腦被允許存取外。
例如，當使用者要將其已共用的子網上的 100 台電腦中的 98 台不被允許存取，而其中的 2 台被允許存取時，可用此功能。

⑫ 點擊<確認>，完成所有設定。

4.1.2 定制新的應用程式

您可以增加“Custom”類應用以定制自己的服務。目前 UU200 中提供三種“Custom”應用：

Custom – Multi-station application：遠端使用者通過 UU200 存取多台機器中任一台的指定埠。如此，使用者便可存取任一台機器的相同服務。例如，存取多個 Web 伺服器的 Internet Explorer，就是這樣的應用。

Custom – Roaming application：遠端使用者通過 UU200 存取多台機器中的任一台的某一個埠。這時，管理員需要單獨指定每一台被存取的機器埠號。通常情況下，使用者通過該 UU200 可以存取任一台機器的任一服務。例如，需要存取多個伺服器的 ERP 軟體，需要同時訪問資料庫伺服器、應用伺服器等，這時便可使用這一應用。

Custom – Network drive based C/S：該應用支援遠端 Client 端用戶象使用網路驅動器一樣訪問由 UU200 發布的共用資源（Client 端運行的應用程式已將此共用資源對應爲指定的網路映射盤）。例如：現有一個 MIS 系統，已將 Database 的完整路徑對應到網路映射盤“N：”，并且管理員在UU200中將該Database 發佈。這樣，多個Client端使用者便可同時對該Database進行操作。

Custom – Proxy for web servers：該類型應用區別於其他類型應用之處在於它同時支援 Modal dialog box、Modalless dialog box 兩種實現方式的 Web 伺服器。

例一：增加“Custom– Multi-station application”應用：

① 在圖 72 所示介面 ，爲保證遠端使用者存取應用時建立的 SSL 連接的安全，您可以設定允許會話持續的最長時長和允許會話空閑的最長時長。超過設定的時長，系統會自動斷開這次連接。

② 點擊<增加>，進入圖 73 所示介面。

③ 點擊<選擇列表框內的 Custom– Multi-station application，點擊<確認>，進入圖 80 所示介面。

④ 點擊<規定…>，進入圖 75 所示的視窗。輸入您爲這個策略所取的名稱；目前 UU200 能提供的策略包括：

- 驗證證書：
  可以指定證書，在使用者登入、獲取應用時驗證用戶端是否提供了正確的證書。此外，還可以對該證書設定限制條件。。
- 限制存取時間：
  如果要限制使用者的存取時間，可以選中“存取時間限制”核取方塊，并輸入約束條件。
  約束條件所遵循的語法結構與設定 Radius 伺服器的規則類似，其語法結構爲：
  time.[屬性名稱] [操作符] [屬性值]（或另一 [系統變數名稱].[屬性名稱]）。

  & 說明：
  此處的 time 爲表示時間的系統變數名稱。
  屬性名稱包括 year, month, day, hour, minute, second, week。其中，
  year 表示 4 位數年份；**month** 表示 2 位數月份；**day** 表示 2 位數的日期；
  hour 表示小時（按 24 小時制）；**month** 表示分鐘；**second** 表示秒；
  操作符 是 sql 的操作符，如 =,!=,>,<,like,in 等。

  舉例：下面的約束條件限制了使用者只能在 2005 年，8:00～18:00 驗證身份，并在驗證成功後存取應用列表：
  (time.year =2005) and (time.hour between 8 and 18)
- 檢測用戶端運行環境：

如果要檢測用戶端的運行環境是否符合要求，可以點擊<管理主機檢查器>。選擇在安全域設定時預先加入的檢測規則。

在”符合時便停止”列中，點選“不是”：則檢測到符合該規則後，繼續檢測下一規則；如果不符合該規則，則拒絕該使用者登入。

在”符合時便停止”列中，點選“是”：則一旦檢測到符合該規則後，即停止繼續檢測，允許該使用者以遠端管理員身份登入管理介面。。如果不符合該規則，則拒絕該使用者登入。

說明：

Ÿ 在“符合時便停止”列中選擇“是”的規則應被放置在所有選擇“不是”的規則之後，否則當用戶端的運行環境符合該條設定爲“是”的規則後，將不會繼續檢測，這樣，其後的規則將不會再有機會被檢測。

Ÿ 如果“防病毒類型”和“作業系統類型”兩種類型都有規則被選中，則要求同時檢測用戶端主機安裝的防病毒軟體和系統設定（系統設定包括：作業系統版本、系統安全補丁、應用的安全補丁等）。只要不符合這兩種類型中的任何一條規則，該用戶端都無法登入。

Ÿ 檢測校驗碼

該功能用於防止非法或有潛在威脅的用戶端應用程式攻擊應用伺服器。例如被病毒或木馬篡改的應用程式的校驗碼必定與合法應用程式的校驗碼不同，這樣，當使用者嘗試連入時，iSTAR 只要驗證用戶端運行的程式的校驗碼和伺服器端爲該程式設定的校驗碼是否一致，便可以判定用戶端的應用程式是否合法。如果合法，則該項驗證通過，否則使用者將不能啓動該應用。

校驗碼採用 SHA 1 演算法。

⑤ 輸入共用應用程式所在伺服器的 IP 位址等相關資訊，點擊<使用者…>，根據需要增加使用者（/群組/角色）。進入圖 76 所示的視窗；將使用者所屬的安全域從“可選擇”列表框中移至 Selected 列表框。如果選擇的是包含有角色角色資訊的 Radius 或 PKI 類型的安全域，會顯示圖 77 所示的操作介面。

⑥ 設定該應用的訂閱策略，系統預設的是“拒絕”，意即所有的使用者都不能訂閱該應用。

⑦ 在“使用者列表”中指定排除在訂閱策略之外方式。在其下的“使用者列表”列表中勾選使用者（/群組/角色），並按<增加>將其加入下方的“已選定的使用者”目錄中；重復在“使用者列表”中勾選，並按<增加>，可以繼續加入多個使用者（/群組/角色）。

通過這一步驟結合設定訂閱策略步驟相結合，管理員可以靈活的設定應用的使用範圍，即：僅允許某一些使用者訂閱所發佈應用，或者允許除某一些使用者外的所有使用者訂閱。

⑧ 點擊<電腦> ，進入如圖 79 所示介面。可以通過點擊<增加>增加允許或拒絕存取該共用應用程式的電腦的相關資訊。設定完成後，點擊<返回>返回圖 80 介面 。

⑨ 點擊<埠範圍>，進入圖 78 所示介面。設定開放的埠。

您也可以點擊<增加>，進入圖 81 所示介面，增加新的埠。

系統預設開放 80 埠，點擊<增加>或<編輯>鍵可以增加/編輯新的埠或現有的埠資訊。

⑩ 輸入“起始埠”和“終止埠”後，點擊<確認>完成埠設定。設定完成後，點選返回返回圖 80 介面。

⑪ 點擊<確認>，返回上一介面，點擊<生效>，完成所有設定。

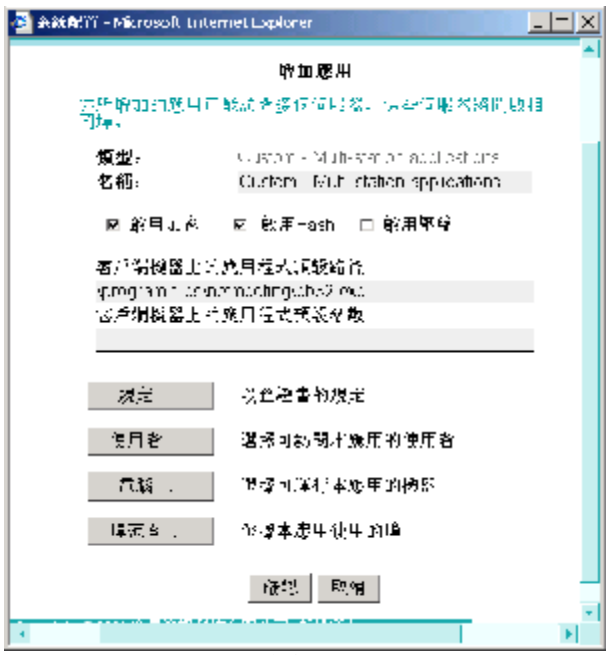


圖 80

參數/控鍵	含義	備註
名稱	指共用應用程式的名稱	
啓用加密	表示該共用的應用程式通過加密演算法	Encrypt 演算法:是指對傳輸資料進行加密的策略，通常標準的演算法有：AES、3DES、DES 等。***i*STAR™**系列產品採用的就是以上這三種演算法，并可以任意選擇。NULL 表示不加密，用明文傳輸
啓用 Hash	表示該共用的應用程式通過 Hash 演算法	Hash 演算法:表示該共用的應用程式通過演算法。Hash 演算法是指把資訊進行混雜，使得它不可能恢復原狀的策略。這種形式的加密將產生一個 HASH 值，這個值帶有某種資訊，并且具有一個長度固定的表示形式。***i*STAR™**系列產品採用的是 MD5、SHA1 這兩種 hash 演算法，可以任意選擇。
啓用壓縮	系統將對資料包進行壓縮	
IP 地址	指該應用所在的伺服器的 IP 地址	
DNS 查找	表示可將 IP 位址轉換成 DNS 名稱	
該應用在使用者端機器上的默認路徑	指共用的應用程式指在使用者端電腦上的預設路徑。	雖然系統裏發佈的是指定伺服器上的相關應用，但是在使用者端電腦上一定要安裝有該應用。
使用者端機器運行該應用時所需的參數	指共用的應用程式在使用者端上運行的參數。	
規定…	進入設定允許存取該共用應用程式的策略介面	

使用者…	進入設定允許（/禁止）存取該共用應用程式的使用者介面	
埠範圍…	進入設定開放的埠介面	如果增加的是 “Custom – Roaming application”應用，則不需要指定埠範圍。

圖 81

圖 82

參數/控鍵	含義
單個電腦	表示設定一台電腦不允許被存取
電腦組	表示設定一組電腦不允許被存取
功能變數名稱稱	表示設定域範圍的電腦不允許被存取

例二：增加“Custom– Network drive based C/S”應用：

1. 如圖 72，爲保證遠端使用者存取應用時建立的 SSL 連接的安全，您可以設定允許會話持續的最長時長和允許會話空閑的最長時長。超過設定的時長，系統會自動斷開這次連接。
2. 按下<增加>，進入圖 73 的視窗；
3. 選擇“Custom – Network drive based C/S”，按<確認>，進入圖 83 的視窗；

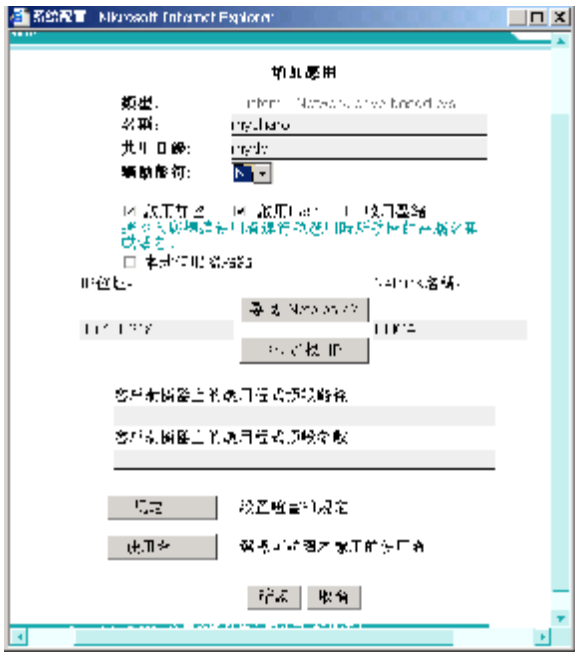


圖 83

4. 在“名稱”欄中，輸入您爲這個應用所取的名稱；
5. 在“共用目錄:”欄中，輸入您要作對應的 Folder 名稱，並請確保輸入正確；
6. 勾選“啓用加密 ”會啓動系統設定的加密演算法；(請參考“例一：增加“Custom– Multi-station application”應用“的表格中內容)。
7. 勾選“啓用 Hash”會啓動系統設定的 Hash 演算法
8. 勾選“啓用壓縮”會啓動系統設定的壓縮演算法；
9. 如果該應用要對應的盤符在本機，則可以勾選“本地伺服器站點”，此時不需要爲 Internet Explorer 應用特別填寫 IP Address；
   如果該應用要對應的盤符不在本機，就不能勾選“本地伺服器站點”，而必需在“IP Address:”欄中輸入該盤符所在的伺服器 IP 位址;或在“Netbios Name:”欄中輸入該盤符所在的伺服器的 Netbios 名稱。
   按 Lookup Netbios >> 鍵可以將伺服器的 IP 位址自動轉換爲 Netbios 名稱;
   按 << Lookup IP 可以將伺服器的 Netbios 名稱自動轉換爲 IP 位址。
10. 如果僅將某一個目錄下的內容對應成爲用戶端的虛擬碟符而不需要發布相應程式，則可以選擇“僅連接驅動盤符”。否則不要選中該項。
11. 在“該應用在使用者端機器上的默認路徑”欄中所顯示的，是指遠端使用者在使用這個應用時，遠端使用者電腦中的使用者端應用軟體路徑的預設位置；
12. 在“使用者端機器運行該應用時所需的參數”欄中所顯示的，是指遠端使用者在使用這個應用時，遠端使用者電腦中的使用者端應用軟體預設的運行參數。
13. 點擊<規定…>，進入圖 75 所示的視窗。輸入您爲這個策略所取的名稱；目前 UU200 能提供的策略包括：
    - Ÿ 驗證證書：
      可以指定證書，在使用者登入、獲取應用時驗證用戶端是否提供了正確的證書。此外，還可以對該證書設定限制條件。。
    - Ÿ 限制存取時間：
      如果要限制使用者的存取時間，可以選中“存取時間限制”核取方塊，并輸入約束條件。
      約束條件所遵循的語法結構與設定 Radius 伺服器的規則類似，其語法結構爲：
      time.[屬性名稱] [操作符] [屬性值]（或另一 [系統變數名稱].[屬性名稱]）。

& 說明：
此處的 time 爲表示時間的系統變數名稱。
屬性名稱包括 year, month, day, hour, minute, second, week。其中，
year 表示 4 位數年份；**month** 表示 2 位數月份；**day** 表示 2 位數的日期；
hour 表示小時（按 24 小時制）；**month** 表示分鐘；**second** 表示秒；
操作符 是 sql 的操作符，如 =,!=,>,<,like,in 等。

舉例：下面的約束條件限制了使用者只能在 2005 年，8:00～18:00 驗證身份，并在驗證成功後存取應用列表：
(time.year =2005) and (time.hour between 8 and 18)

Ÿ 檢測用戶端運行環境：
如果要檢測用戶端的運行環境是否符合要求，可以點擊<管理主機檢查器>。選擇在安全域設定時預先加入的檢測規則。
在”符合時便停止”列中，點選“不是”：則檢測到符合該規則後，繼續檢測下一規則；如果不符合該規則，則拒絕該使用者登入。
在”符合時便停止”列中，點選“是”：則一旦檢測到符合該規則後，即停止繼續檢測，允許該使用者以遠端管理員身份登入管理介面。。如果不符合該規則，則拒絕該使用者登入。

說明：
Ÿ 在“符合時便停止”列中選擇“是”的規則應被放置在所有選擇“不是”的規則之後，否則當用戶端的運行環境符合該條設定爲“是”的規則後，將不會繼續檢測，這樣，其後的規則將不會再有機會被檢測。
Ÿ 如果“防病毒類型”和“作業系統類型”兩種類型都有規則被選中，則要求同時檢測用戶端主機安裝的防病毒軟體和系統設定（系統設定包括：作業系統版本、系統安全補丁、應用的安全補丁等）。只要不符合這兩種類型中的任何一條規則，該用戶端都無法登入。

Ÿ 檢測校驗碼
該功能用於防止非法或有潛在威脅的用戶端應用程式攻擊應用伺服器。例如被病毒或木馬篡改的應用程式的校驗碼必定與合法應用程式的校驗碼不同，這樣，當使用者嘗試連入時，iSTAR 只要驗證用戶端運行的程式的校驗碼和伺服器端爲該程式設定的校驗碼是否一致，便可以判定用戶端的應用程式是否合法。如果合法，則該項驗證通過，否則使用者將不能啓動該應用。
校驗碼採用 SHA 1 演算法。

14. 點擊<使用者…>，根據需要增加使用者（/群組/角色）。進入圖 76 所示的視窗；在 Look In Realms 下拉清單中選擇使用者（/群組/角色）所在的安全域。如果選擇的是包含有角色角色資訊的 Radius 或 PKI 類型的安全域，會顯示圖 77 所示的操作介面。
15. 設定該應用的訂閱策略，系統預設的是“拒絕”，意即所有的使用者都不能訂閱該應用。
16. 在“使用者列表”中指定排除在訂閱策略之外方式。在其下的“使用者列表”列表中勾選使用者（/群組/角色），並按<增加>將其加入下方的“已選定的使用者”目錄中；重復在“使用者列表”中勾選，並按<增加>，可以繼續加入多個使用者（/群組/角色）。
通過這一步驟結合設定訂閱策略步驟相結合，管理員可以靈活的設定應用的使用範圍，即：僅允許某一些使用者訂閱所發佈應用，或者允許除某一些使用者外的所有使用者訂閱。
17. 按下<返回>返回圖 83 的視窗；
18. 按下<確認>完成對發佈 Network drive based C/S 的設定，並點擊<生效>使設定

生效。

對於其他預設應用程式選擇專案內已有的應用程式發布方法，都和以上發布的兩種應用的方法類似，您可以參照以上方法發布其他各種應用程式。

4.1.3 編輯（更改）已發布的應用程式的配置

在圖 3 的視窗中，選擇在“發布”之下的發布應用，會顯示如圖 72 所示的視窗。

“共用的應用服務”列表中，列出了已發布的應用，選擇其中的某一項，點擊<編輯>，可以更改該項應用的配置。（請參考圖 74、圖 80）完成編輯後，請務必記得點擊<生效>，使所做的更改生效。

更改已發布應用的任一配置，僅會對此後連入 UU200 的 Session 生效，即不會影響更改之前已經連入 UU200 的 Session。

例如，某一 User 現正通過 UU200，使用 IE 服務。此時如果將該 User 從已發布的 IE 應用中移除，并不會影響該 User 的任何操作。但是，一旦該 User 登出，本次 Session 結束，則將無法重新建立另一個新的 Session，再次登入該台 UU200。

4.2 發佈子網

UU200 提供兩種發佈子網功能：向 UUSoft 發佈子網和向 UURemote 發佈子網，只有安裝了相關許可證的 UU200 才提供發佈子網的功能。

4.2.1 準備工作

爲了發布子網，首先必須確定：

- 哪個子網需要發佈
- 哪些遠端使用者可以存取該子網
- 該子網中的哪些電腦可以被存取
- 使用者可以允許執行哪些應用

另外，網路管理員需要在發布區域網路內配置一個 DHCP 伺服器（UU200 在單模式下）。或由 UU200 充當 DHCP 伺服器（UU200 在透明模式或路由模式下）。如果所發佈子網的 IP 地址是內部地址，則網路管理員還必須採取措施，讓遠端使用者瞭解子網位址，遠端使用者必須確保原有的 IP 位址與動態得到的 IP 位址不衝突，即不在同一個網段，否則會引起位址混亂，導致網路不通。

4.2.2 UU200 對 DHCP 的支援

單模式下，UU200 不提供 DHCP 服務，必須利用發佈區域網路路內的 DHCP 伺服器或在該區域網路內安裝一個 DHCP 伺服器，遠端使用者端電腦在獲取一個有該 DHCP 伺服器動態分配的 IP 位址後虛擬接入該子網，如圖 84 所示：

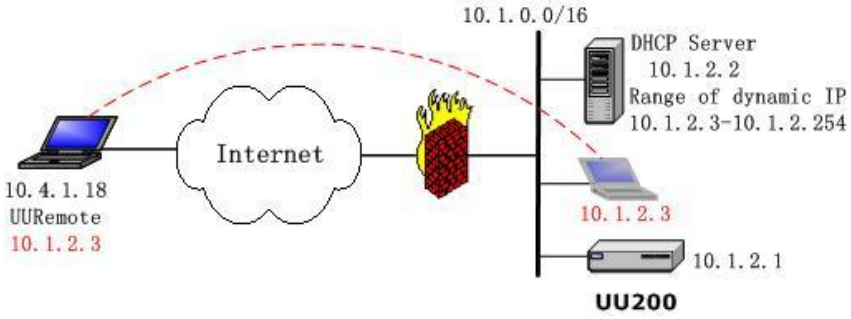


圖 84

如果 UU200 的接入網路的方式爲透明模式或路由模式，則你可以直接啓用 UU200 中的 DHCP 服務，亦可利用選擇利用區域網路內原有 DHCP 伺服器。

透明模式下，若直接啓用 UU200 中的 DHCP 服務，則在配置 UU200 的網路設定時，在步驟 1 需要選中“啓用 DHCP 伺服器”，填入動態分配的 IP 地址範圍，如圖 85：

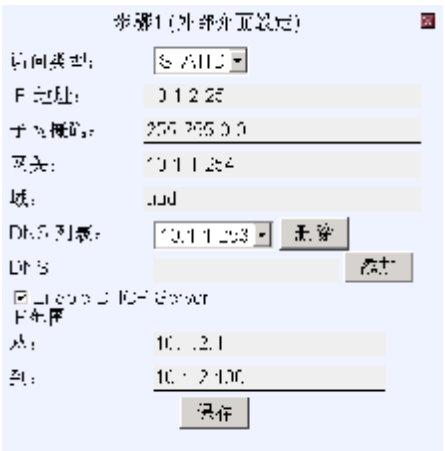


圖 85

該模式下，遠端使用者的電腦可以被動態分配一個範圍內的 IP 位址，虛擬接入 UU200 所在子網，其結構如圖 86 所示。（這裏的連接方式與圖 84 所示不同，只要將 UU200 直接接入區域網路，通過該 UU200，遠端電腦可以虛擬接入該 UU200 所在區域網路）

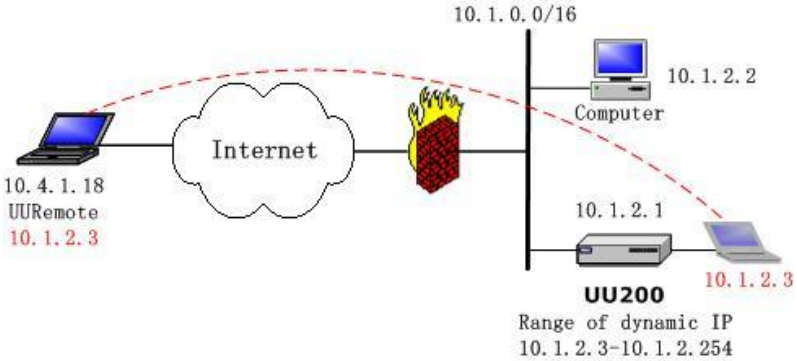


圖 86

路由模式下，也可直接啓用 UU200 中的 DHCP 服務。配置 UU200 的網路設定時，在步驟 1 需要選中“啓用 DHCP 伺服器”，填入動態分配的 IP 地址範圍，如圖 87。

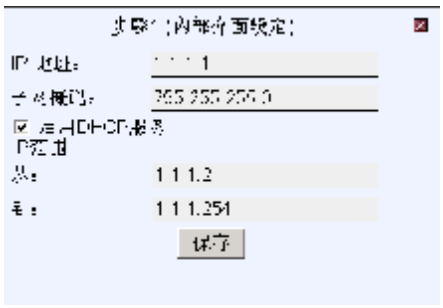


圖 87

該模式下，UU200 可以置於一個 Site 中的任何一個子網前面，充當路由器角色，通過 UU200 提供的 DHCP 服務，遠端使用者的電腦可以被動態分配一個 UU200 後面的子網的 IP 位址，虛擬接入 UU200 所保護的子網。其結構如圖 88。

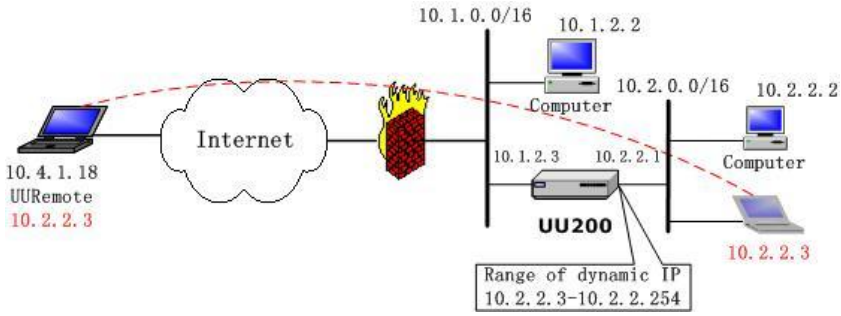


圖 88

4.2.3 啓用子網發佈功能

發布子網分爲兩部分：UURemote，UUSoft

UURemote 針對遠端接入使用者，動態分配位址。

UUSoft 針對遠端伺服器，可以進行 User ß à IP 的對應。

- 發布 UUSoft 子網

點選圖 3 主介面功能表上“發布”下的發佈 UUSoft 子網進入圖 89 介面。

— 設定可存取該 Subnets 的使用者：

— 設定可存取該 Subnets 的電腦組：

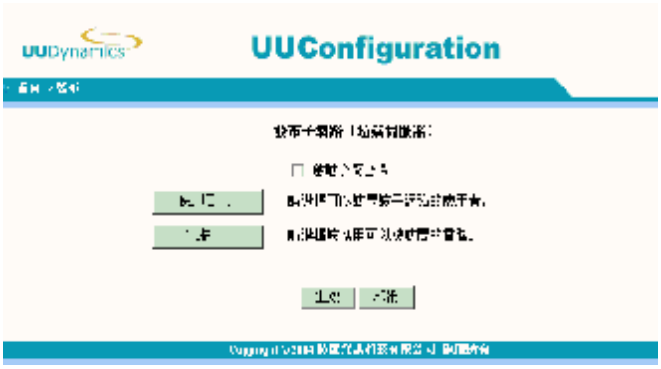


圖 89

上圖中，“啓動交叉訪問”是指通過 UURemote 或 UUSoft 連接到 UU200 的遠端客戶或伺服器之間是否可以互相存取，如果勾選擇表示可以，否則表示會不可以。

點擊<使用者…>，根據需要增加使用者（/群組/角色）。根據使用者所屬的安全域類型不同,會出現對應的不同畫面。

選擇安全域。幷設定該應用的訂閱策略，系統預設的是“拒絕”，意即所有的使用者都不能訂閱該應用。

選擇“使用者列表”欄的“使用者”或者“群組”，在“使用者列表”列表中會列出該安全域中的所有 User 或者群組。

在“使用者列表”中指定排除在訂閱策略之外方式。在其下的“使用者列表”列表中勾選使用者（/群組/角色），並按<增加>將其加入下方的“已選定的使用者”目錄中；重復在“使用者列表”中勾選，並按<增加>，可以繼續加入多個使用者（/群組/角色）。

通過這一步驟結合設定訂閱策略步驟，管理員可以靈活的設定應用的使用範圍，即：僅允許某一些使用者訂閱所發佈應用，或者允許除某一些使用者外的所有使用者訂閱。

& 說明：

- 如果在視窗中的空白欄輸入要搜索的字串幷點擊<搜索/開始>，介面上將返回模糊查詢後的結果（是否有搜索功能與伺服器的類型有關。）
- 由於 Radius 類型的伺服器可以基於角色進行身份認證。因此，對應安全域的“遠端管理”介面上可以按照“角色” （而非“群組”）顯示。

在“訪問類型”中設定該管理員的權限。各種許可權的含義分別爲：

唯讀:表示該使用者對系統管理介面有“唯讀”許可權。

更改:表示該使用者對系統管理介面有“唯讀”、“修改”和“使更改生效”的許可權。

拒絕: 表示該使用者不能登入系統管理介面。

視窗上面顯示的是可以指定的 IP 位址範圍，勾選“顯示使用者”會顯示所有使用者。選中上面框口中的使用者或群組，按中間的<增加>，就可以把選中的使用者或群組增加到下面的視窗中，表示這些使用者和群組可以使用該子網。

& 說明：

單模式沒有此功能。

按<電腦…>，選擇可以存取的電腦。詳細步驟與發佈應用的配置頁面一致，這裏就不再敍述。

圖 90

- 發佈 UURemote 子網

  點選圖 3 主介面功能表上“發布”下的發佈 UURemote 子網進入圖 91 介面。

  — 設定可存取該 Subnets 的使用者：

  — 設定可存取該 Subnets 的電腦組：

圖 91

注：使用者，電腦與發佈自定義應用的配置頁面一致，這裏就不再敍述。

使用者虛擬連入被發布的子網：用戶可以使用 UURemote 虛擬連入 UU200 所發布出來的子網。通過 IE 瀏覽器，使用者可以在任何一台聯機到網際網路的電腦上輸入：

https://[*uu200 的 IP 位址*]/ra (Direct Access 方式) ，或者，

https://[*uuswitch（/uuexchange 的 DNS 名稱或 IP 位址*）/[*uu200UUID*]/ra （Private Access 方式）

4.3 連接兩個子網

UU200 爲您提供了一種安全的連接本地站點與遠端站點的服務，連接站點到站點。使用這種服務，您也可以方便的將本地子網連接存取遠端子網，實現 LAN to LAN 功能，又最大程度的保證了安全性。配置“連接站點到站點”服務需要兩台 UU200，分別處於要連接的兩個站點/子網兩邊，每一邊的 UU200 的配置是相同的。

每台 UU200 允許連接不超過 100 個其他站點/子網。

4.3.1 建立“站點到站點”隧道的條件

和傳統 VPN 一樣，要求建立 Site to Site 隧道的兩個子網的 IP 地址不衝突。子網的位址用 CIDR 格式表示，如：10.1.1.0/24, 建立 Site to Site 隧道的條件是兩個子網的位址不能交叉。

4.3.2 設定“站點到站點”隧道的方法

點選“進階”中的連接站點到站點，進入圖 92 的介面。

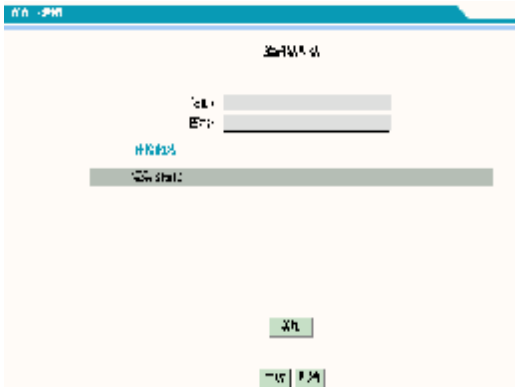


圖 92

站 ID：如果您的 UU200 是選擇 Direct Access 連接方式，則需要爲這個 UU200 命名一個 Site ID，並且保證這個 Site ID 的唯一性；如果您的 UU200 是選擇 Private Access 連接方式，則這個 Site ID 則爲自己的 UUID，無需輸入。本圖爲 Direct Access 連接方式。

密鑰：互相連接的兩個 UU200 需要一個共同的密鑰，這個密鑰由兩邊協商確定，並且是必須的。實際可以使用任何由字母數位元元組成的字串，但必須以字母開頭。

您可以按以下步驟增加一個遠端站點：

1. 在圖 92 所示介面中，“密鑰”欄填入與遠端 UU200 共用的密鑰，如果是 Direct Access 連接方式則在站 ID 欄填入本地 UU200 的名字。
2. 選擇<增加>按鈕，進入圖 93 介面，增加遠端站點或子網。
3. 在遠端站 ID 中填入你所要連接的遠端 UU200 的站 ID，若在 Private Access 連接方式下，則輸入對方的 UUID，按<確認>鍵返回圖 92 介面，按生效生效。增加的遠端 UU200 會出現在介面中。

圖 93

遠端 UU200 配置步驟同上。如果兩邊的 UU200 都配置正確，則“連接站點到站點”功能就能正常工作了。

4.3.3 查看“站點到站點”隧道的狀態

站點到站點隧道是否正常工作可以通過主配置功能表中的顯示狀態選項看到。選擇顯示狀態選項後進入查看系統狀態的介面，點選介面上的連接站點到站點，就可以看到站點到站點隧道的工作狀態，Connected 表示站點到站點隧道已經連接。

第5章 設定叢集分攤負載

5.1 叢集概述

UUDynamics 在其所有的安全設備上均使用了叢集技術以保證系統的高可用性和負載分流。此項技術被應用在 UUDynamics 的所有安全設備中，包括主模式下的 UUSwitch (/UUExchange)，和 UU200 發布單元。

當網路中有多台 UU200，并且負載非常不均衡，可以考慮使用叢集的方式平衡它們之間的工作量負載。叢集的最大值可達 10 台。

- 容量規劃: N+1
  叢集功能使參與叢集的伺服器得到了綫性的增長。在特定的應用環境下，參與叢集的伺服器數目依賴於必須使用的伺服器數目 N（N 的值由計劃的容量計算所決定）。并增加一台用於冗余和容錯。
- 負載分流
  在綫工作期間，負載被平均地分流到所有的 N+1 個伺服器。
- 單系統鏡像
  不論加入了多少個伺服器，一個叢集意味著單個系統，即被叢集的所有伺服器可被視爲一個整體。除了 LAN Settings，叢集中的所有伺服器的配置資料庫都可以作爲一個整體被維護。對於 LAN Settings，可以通過在叢集中選擇特定的伺服器進行在綫修改。
  要支援 UUSwitch (/UUExchange)的單系統鏡像，需要先支援 DNS 服務，以便該叢集中的伺服器可以共用同一個 DNS 功能變數名稱稱。
- 高可用性
  一旦檢測到任何錯誤，負載都將在剩餘的正常工作的伺服器上重新分配。當某台伺服器出錯時，其他 N 台伺服器將會自動接管網路中的所有工作量負載，
- 重構
  可以毫不費力地加入新的伺服器以增加網路的額外容量。此時，網路中原有的叢集僅需要重新配置一下“Lan settings”。當前正在運行的伺服器將會自動地更新現行的應用服務的相應配置。新加入的伺服器所運行的軟體版本也會和叢集中的其他伺服器保持一致。

5.2 工作量均攤原理

- UU200 的工作量均攤
  當檢測到錯誤時，工作量負載會被重新分配給正在運行的發布單元。這些負載包括所有的命令通道和資料通道。受到影響的通道會有暫時的連接斷開的現象，直到新的叢集被成功地重建。
- 工作量負載重分配對用戶端的影響
  在負載重分配過程中，用戶端已搭建好的通道可能會面臨連接斷開的情況。但是，連接斷開卻并不一定說明發布單元存在問題。下面列出了通道斷開的幾種可能情況：
  - 發布單元的工作量重分配，可能是由於伺服器出現問題或新加入了新的發布單元。
  - 用戶端和發布單元之間的路由器受到的網路幹擾。
  - 發布單元因爲會話超時而斷開連接。
  - 用戶端因爲會話超時而主動斷開連接。

出於安全考慮，那些爲 Remote Desktop (UUApp) 和 UURemote 而建立的通道不會自動重新連接。用戶必須手動地重新登入。而爲 UUSoft 建立的通道，則會自動重新進行連接。

5.3 叢集的設定

1. 如圖 3 主功能表介面，點選“網路設定”下的 網路設定，進入網路參數設定介面。點選“Step2” 設定叢集。
2. 勾選“啓用叢集”表示啓用叢集；
3. 輸入叢集 IP、及對應的叢集子網掩碼；
   每一台被叢集的 UU200 需要一個專用的靜態 IP 位址，稱爲叢集 IP，一般爲私有 IP。系統管理員可以自由設定這些叢集 IP，但同一個叢集的 UU200 必須位於同一個子網路。同時，叢集 IP 不能與任何私有地址相同。在路由模式下，叢集 IP 不但不能與任何私有 IP 位址相同，而且不能與任何公共 IP 位址相同。否則會導致衝突。
4. 輸入叢集 IP（開始）、叢集 IP （結束）資訊； 這是用於描述同一個叢集內 UU200 的 IP 位址範圍。
   叢集中所有的叢集 IP 位址必須在叢集 IP 位址範圍內。
5. 輸入完畢後按<保存>進行儲存幷返回網路參數設定介面。
6. 點擊<生效>，結束叢集設定。

第6章 子網虛擬接入服務

6.1 UURemote 服務

UURemote 是基於 UU200 的可選的附加服務。可以讓遠端用戶在需要的時候接入虛擬子網，如同在本地局域網裏一樣。

UURemote 在 Internet 中建立點到點安全通道，爲伺服器提供一種使用簡便、安全的遠端存取方式。使用 UURemote 的機器不需要改變任何防火牆、路由器等邊緣設備，就可以安全地、有選擇性地加入 UU200 端的子網。

UURemote 服務不需要另行安裝。需要使用 UURemote 服務時，只需在瀏覽器的 URL 欄中輸入：

- https://[*uu200 的 IP 位址*]/ra (Direct Access 方式)
- https://[*uuswitch（/uuexchange 的 DNS 名稱或 IP 位址*）/[*uu200UUID*]/ra （Private Access 方式）

6.2 UUSoft 服務

UUSoft 是基於 UU200 的可選的附加服務。使用 UUSoft，使用者可以在伺服器上增加虛擬網卡，動態（或人工指定）獲得遠端 UU200 發佈的子網中的 IP 位址，該伺服器就“虛擬接入”遠端子網。UUSoft 爲遠端維護伺服器或 IT 服務運營商提供的是不間斷的遠端接入模式。

UUSoft 在 Internet 中建立點到點安全通道，爲伺服器提供一種使用簡便、安全的遠端存取方式。使用 UUSoft 的機器不需要改變任何防火牆、路由器等邊緣設備，就可以安全地、有選擇性地加入 UU200 端的子網。

UUSoft 的獨特構建，能夠使網路服務供應商（ISP）和應用服務提供商（ASP）等，集中式地爲客戶提供安全連接和遠端服務。

UUSoft 服務與通過“/rm”方式接入遠端子網的區別在於 UUSoft 爲命令行介面，需要另行購買。

6.2.1 安裝/升級/卸載

UUSoft 的系統需求

操作環境	Microsoft® Windows® XP、Microsoft® Windows® 2000
硬碟空間	10MB
瀏覽器	Microsoft Internet Explorer 5.0 或更新版本。

Ÿ 安裝 UUSoft

關閉所有正在運行的應用程式，輕按兩下 UUSoft 安裝程式，系統會自動執行安裝過程。

注意：
如果你的電腦上安裝的 Personal Firewall 等程式有可能會導致 UUSoft 不能正常工作。

Ÿ 升級 UUSoft

直接運行 UUSoft 升級程式，系統會重新啓動電腦。

Ÿ 卸載

選擇 Start -> Settings -> Control Panel -> Add/Remove Programs -> Uninstall UUSoft，系統會提示重新啓動電腦。

6.2.2 設定並測試您的網路連接

UUSoft 支援 Command Line 命令的操作方式來設定和管理，管理人員可以在安裝 UUSoft 的電腦上執行這些命令，也可以遠端執行 Telnet 連接到安裝 UUSoft 的電腦上，UUSoft 軟體中捆綁了 Telnet Server 和 FTP Server，以便遠端使用 Line Command 對 UUSoft 進行管理以及下載或上載文件時使用。

(1) 設定 System 參數

使用 uusoft set 命令可以選擇需要設定的參數進行設定。這個命令執行所修改的設定不會立即生效，所以執行完所有設定命令後需要重啓 UUSoft 服務，重啓時會導致系統中斷原有連接，重新建立連接，因此，重啓前要確認修改的設定。RecoverTime 設定的是確定是否恢復上次設定的時間，即如果設定的參數導致系統在所設定的時間內不能建立 Tunnel，系統會自動恢復到最近可以正常工作的設定。

uusoft set –p UUAdmin

– UUExchange 211.96.216.78 //Direct Access方式爲publisher IP or DNS

- Cipher AES,3DES //設置加密演算法爲“AES”、“3DES”
- Hash MD5,SHA1 //設置Hash演算法爲“MD5”、“SHA1”
- LogL 6 //查看Level爲6以下（包括6）的日誌
- LogMS 20 //設置日誌文件的最大位元組數（單位：
- ProxyT 3 //Proxy
- ProxyS 192.168.0.1
- ProxyP 8080
- ProxyUser user1
- ProxyPwd asd123
- AdminPWD asd123 //修改管理員密碼爲asd123
- RecoverTime 5 //在5秒內連接發布單元不成功，自動重置。時間單位：秒。
- UploadUrl ftp://ftp.domain1.com/uusoft //上傳Log文件至Ftp Server。
- UploadBackupUrl ftp://ftp.domain2.com //上傳Log文件至備用的Ftp Server
- UploadUser test //上傳Log文件時指定User名稱。
- UploadPwd 123456 //上傳Log文件時指定User的Passward。

有關 Proxy 的設定預設讀取系統的 Internet Setting 的設定。Set 命令的參數含義請參閱本手冊附錄。

(2) 設定 Publisher 資訊

uusoft add/remove 用於增加/刪除 Publisher 資訊。

a) Direct Access 連接方式下：

UUsoft –p UUAdmin set –uuexchange [publisher IP]

UUsoft –p UUAdmin add localhost –uid [*user name*] –pwd [*password*] –Realm [*realm name*]
如果無法連上該 Publisher，應考慮 UUSoft 是否已連入其他 Pubilsher。如果是，請先將其刪除。刪除時只需要指定 Localhost
如： uusoft remove localhost

b) Private 連接方式下，

增加時參數爲[*Publisher UUID*]，如：

Uusoft –p UUAdmin set –uuexchange [*exchange ip*]

Uusoft –p UUAdmin remove [uuid]
Uusoft –p UUAdmin add [*uuid*] –uid [*user name*] –pwd [*passwd*] –realm [*realm name*]
如果無法連上該Publisher，應考慮UUSoft是否已連入其他Pubilsher。如果是，請先將其刪除。刪除時只需要指定[*Publisher UUID*]即可。
如： uusoft remove[*publisher uuid*]。

6.2.3 UUSoft 的啓動、停止和重新啓動

uusoft start/stop/restart 用於啓動、停止和重新啓動 UUSoft;

6.2.4 匯入/匯出設定

Importcfg/Exportcfg 用於匯入/匯出設定資訊至指定路徑下，幷以.uif 文件的形式保存在執行 uusoft 命令的電腦上；

例如：

匯出設定資訊： uusoft exportcfg –f "c:\documents and settings\my documents\uucfg.uif" –p UUAdmin

匯入設定資訊： uusoft importcfg –f uucfg.uif –p UUAdmin

& 說明：
Ÿ 如果沒有指定路徑，則文件位於當前路徑下。
Ÿ 如果指定的路徑中包含有空白字元號，請務必使用引號將完整的路徑和檔案名包含起來，見上例。

6.2.5 匯出 UUSoft 日誌

如果你用 uusoft set 命令設定了自動 Dump 和發送 Log 的相關參數，UUSoft 會自動發送

Configuration, Log 等資訊到指定的郵箱內。(每天凌晨 1：00 發送前一天 0：00 到當天 0：00 的日誌)

Exprotlog 指令用於匯出指定時間段的 log 至指定路徑下。

例如：

匯出 8 月 1 日 到 8 月 12 日之間的日誌: uusoft exportlog –f cust1.log –BT 0801 –ET 0812 –p UUAdmin

& 說明：

Ÿ 如果沒有指定路徑，則文件位於當前路徑下。

Ÿ 如果指定的路徑中包含有空白字元號，請務必使用引號將完整的路徑和檔案名包含起來，見上例。

6.2.6 查看 UUExchange 的運行狀態

執行 uusoft status

顯示結果：

Connected to UUExchange: uuswitch.uudynamics.com
Registered to UUExchange: uuswitch.uudynamics.com
Connected to Publisher: uu200-test4@qa.uud
Up time: 0 days 0 hours 5 minutes.

6.2.7 查看 UUSoft 參數設定

uusoft show 命令用於查看 UUSoft 的參數設定。

例如：

執行 uusoft show

顯示結果：

System setting is :
-UUExchange 211.96.216.78
-Encript AES,3DES
-Hash MD5,SHA1
-LogL 6
-LogS 10.1.2.216
-FWS 3
-ProxyS 192.168.0.1
-ProxyP 8080
-ProxyUser user1
-ProxyPwd asd123
-RecoverTime 5
Publisher: uucare@uudynamics.com, User: test, Realm: slk,

6.2.8 遠端使用 Line Command

UUSoft 中捆綁了 Telnet 和 FTP 伺服器,所以管理人員可以遠端使用上述 Line Command。

1. 遠端設定管理

在任何可以存取安裝 UUSoft 的電腦的工作站上運行標準 Telnet 用戶端。UUSoft 軟體中的 Telnet 伺服器預設埠爲 21023，用戶名爲 uusoft，密碼就是管理員密碼，預設是 UUAdmin.

例如：

Telnet 1.1.1.15 21023
Login: uusoft
Password: *******
uusoft>

這時就可以執行上述 Line Command,只要直接輸入命令即可，如顯示 UUSoft 執行狀態：

uusoft> status

顯示結果：

Register to UUExchang 211.96.216.78
Publisher1 has Connected for 0days 2 hours 15 minutes

2. 遠端文件上載和下載

在任何可以存取安裝 UUSoft 的電腦的工作站上運行標準 Ftp 用戶端。UUSoft 軟體中的 Ftp 伺服器預設埠爲 21021，用戶名爲 uusoft，密碼就是管理員密碼，預設是 UUAdmin.

例如：

ftp
ftp>open 1.1.1.15 21021
user: uusoft
Password: *******
ftp>

這時就可以執行標準的 FTP 命令，上載和下載文件。

6.2.9 用戶端 Proxy 設定的修改

用戶端 Proxy 設定的修改是在 Proxy 設定錯誤或 Proxy 設定改變時使用，有兩種實現方案：

1 在安裝 UUSoft 的電腦上,通過上面介紹的 Command Line 命令“uusoft set”進行查看或手工修改設定的功能，供技術服務人員使用；

2 由客戶自己設定 Internet Explorer，在確保 IE 可以進行 HTTPS 連接，然後運行”uusoft reset”，修改 Proxy 的設定重新啓動 UUSoft。

第7章 系統復原

7.1 何時需要系統復原

系統復原是指將系統恢復到出廠狀態，復原的過程會導致：

- UUDynamics 套裝軟體丟失
- UU200 中的設定資訊丟失

復原後必須重新安裝 UUDynamics 套裝軟體，重新配置系統，丟失的配置資訊將永久性不可恢復。因此，我們強烈建議您經常輸出幷備份系統配置資訊，在系統無法工作，幷且按 UUDynamics 技術支援無法解決時才使用系統復原功能。

重要：
不當的系統復原會產生嚴重的後果，不到萬不得已，不要執行系統復原操作！

7.2 系統復原方法

在 UU200 系統在設定處理時出現停電等情況可能會導致系統備破壞，這時需要進行系統復原工作。

1. 準備工作
   （1） 準備一台配置 PC 電腦，設定成動態獲取 IP 位址；
   （2） 將備份的系統配置資訊複製到該配置電腦上；
   （3） 與 UUDynamics 技術支援聯繫，獲取 UUDynamics 套裝軟體；
2. 用 Null Modem 線與 UU200 的 Console 介面連接，重新開啓 UU200 設備的電源，系統啓動過程中在超級終端的螢幕上會看顯示提示資訊：

   UUDynamics iStar Server:
   We will pause for 5 seconds to give you a chance to execute recovery if desired.

   Press "Tab" first to enter into recovery process.
   Please enter "R" behind the "boot: " prompt for recovery, or "N" for No-recovery boot:

   選擇“R”即開始系統復原；
3. 選擇 UU200 上標“1”字樣的網口，用交叉線將配置電腦與 UU200 連接起來；
4. 在配置電腦上開啓瀏覽器，輸入 URL: http://1.1.1.1/admin, 得到如圖 94 所示的介面。

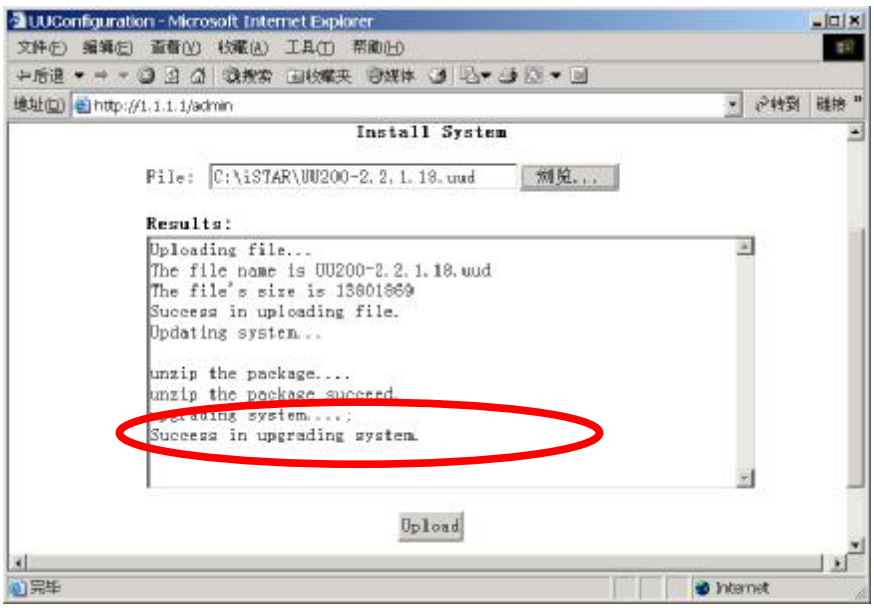


圖 94

5. 按<瀏覽……>，選擇 UUDynamics 套裝軟體，然後按<Upload>，系統會進行安裝。
6. 當“Results”框裏顯示“Success in upgrading system.”資訊，表明安裝完成，請關閉 UU200 電源，數秒後重新開啓。
7. 當面板上的 LCD 顯示“Unregester”後，在瀏覽器中重新輸入：http://1.1.1.1/admin。
   出現使用者登入介面，接下去的操作同本手冊“安裝 UU200 軟體”部分。

第8章 故障檢測和排除

（1） 啓動配置環境時，用交叉線方式將用於配置 UU200 的電腦與 UU200 連接起來，進行相關 IP 位址的修改後，重啓 UU200，但是配置電腦與 UU200 不能建立連接？

a) 檢查網路是否連通；

b) 檢查網線是否完好無損；

c) 檢查網口是否已插好網線；

（2） 完成基礎設定後，結果連接或註冊 UUSwitch(/UUExchange)失敗，爲什麼？

a) 網路設定不正確，請檢查路由，使用 ping 工具檢查是否能夠 ping 通 UUSwitch(/UUExchange)；

b) 運行 Telnet uuswitch 443 檢查是否能夠連接到 UUSwitch(/UUExchange)。檢查網路設定是否正確，UUSwitch(/UUExchange)是否已經啓動。

c) 如果連接成功，註冊不成功，檢查 UUID 檔案是否正確；

d) 如果 UUID 檔案正確，應確保 UUSwitch(/UUExchange)上確有此 UUID，沒有被停止或刪除, 也沒有被更新, UUID 也沒有過期。

（3） 發布應用程式、發布子網或遠端管理時，遠端使用者無法訂閱相關內容，爲什麼？

***i*STAR™**處理的連接和加密針對的是通信雙方的應用通道，而非雙方主機間的整個通道。因此，首先應確保所有應用在區域網路裏能夠正常使用，以排除 Internet 連接等外部因素引起的故障。有些應用的配置複雜，部署時牽涉多項事件，稍有差錯便無法運行，如 MS Outlook 等便是較典型的例子。

此外還需檢查這些應用是否屬於 ***i*STAR™**支援的客戶/伺服器應用（請參閱附錄）。

如以上要求均已滿足，而在遠端的使用者仍無法訂閱，則請逐一排除以下可能原因：

a) 未選擇正確的認證方式：

如果使用伺服器進行認證，請先確保此伺服器存在，且可存取。

如果切換了認證方式，所有應用中的使用者設定將刪除。此時，應該爲每個應用程式重新配置使用者。如果安全域 LocalAdmin 或其他認證伺服器中使用者有改變，也應檢查應用中的使用者設定是否正確。

b) DNS 服務未能正確解析該 DNS 名稱：

如果在電腦設定中，使用 DNS 名稱配置，請應確保 Publisher 的 DNS 能解析該 DNS 名稱。如果配置的是域，應確保能夠反向解析。否則，如果設定爲“除了配置的機器，其他的機器都不能存取”時，將會發生錯誤。

（4） 登入管理介面時，系統將提示資訊：“使用者 *[username]* 目前已在本系統登入”。同時，勾選“停止使用

者 [*username*]”時出錯。

管理介面不允許一個以上使用者同事登入。如果您沒有許可權使該使用者失效，則不能登入。如果仍要登入，請聯繫系統管理員。

（5） 訂閱不到已發佈的應用程式，問題在哪？

a) 訂閱者和發佈者是否都已連接上同一個 UUSwitch(/UUExchange)，並且均註冊成功。

b) 使用者名，密碼，域 是否填寫正確。

（6） 選擇網路模式時應注意哪些問題？

a) 根據 UUSwitch(/UUExchange)所在網路中的實際情況，選擇正確的模式；

b) 檢查網口是否插正確。

c) 對於靜態 IP，要設定正確，否則網路將不通。

d) 對於 DHCP，應確保 DHCP 伺服器工作

（7） 高級設定裏應該注意哪些事項？

a) Static route 應遵守路由設定的規定。如，閘道須與 uuserver 的 IP 在同一網段。

b) Select Mode 中，Manufacturing 將恢復出廠設定。所有配置丟失。包括 IP 設定。配置口 IP 恢復爲:1.1.1.1。重新配置。

（8） 配置 UU200 時，哪些情況下需要修改路由表，怎麼修改？

UU200 可以配置爲單模式、透明模式和路由模式。

單模式下，如果需要配置兩個子網連接（Connect Site to Sites, 也稱 LAN-LAN）時需要在原有路由器上增加一條從路由器到 UU200 的靜態路由；或在每個需要存取遠端子網的使用者端增加目標子網爲遠端子網，則閘道爲 UU200 的靜態路由。

透明模式不需要變更原有路由器或使用者端的任何配置。

路由模式下，UU200 同時具有路由器功能，使用者端電腦的閘道自然設爲 UU200 的 IP 位址，也不用另外修改路由表。

在 Windows 環境下修改路由表的命令是 Route, 如增加一條路由命令：

Route ADD 10.4.0.0 mask 255.255.0.0 10.1.99.95

表示目標子網是 10.4.0.0 的網路包的閘道是 10.1.99.95

在 Linux 環境下修改路由表的命令是 Route, route help 可以查閱該命令的使用說明。如增加一條路由命令：

route add -net 10.4.0.0/16 gw 10.1.99.95

表示目標子網是 10.4.0.0 的網路包的閘道是 10.1.99.95

（9） 配置好叢集後，在 View Status 中沒有見到所有伺服器的叢集 IP。

a) 過一會再看，因爲叢集需要一段時間，才能夠完全叢集成功。

b) 仍然沒有看到，應檢查叢集的配置。各台伺服器上的子網掩碼, 叢集 ip （開始）, 叢集 ip （結

束）是否完全一致。叢集 IP 有沒有衝突。

c) 檢查網綫是否插好，各伺服器是否在同一個 Lan 裏面。

d) 以上一切都正確，但是叢集仍然無法成功，重啓所有的伺服器。

（10） 不能存取 UU100/UU200。

如果您通過“Direct Access”或“Private Access”連接模式不能存取 UU100/UU200，原因之一可能是 UU100/UU200 或 UUSwitch/UUExchange DNS 名稱解析失敗。請先確認 DNS 名稱解析服務能正確執行。

以下幾種方式會影響 DNS 名稱解析服務。

1. DNS 伺服器指向非預期的地方。
2. DNS 名稱被固化在“hosts”文件中。在 Windows XP/2000 中，該檔被保存在“\windows\system32\drivers\etc”目錄下。
3. IE 代理伺服器設定指向一個已有的 WEB 代理伺服器（無論通過自動檢測還是通過直接分配），該 WEB 代理伺服器可能會將名稱直接指向其他非預期的地方。
4. 啓用了 DNS 使用者端服務，幷且可能包含了一個舊的暫存的值。

解決辦法：

請檢測每種可能的情況並確保這些設定均正確。

1. 確認 DNS 伺服器確實爲需要使用的伺服器。
2. 確認您的“hosts”檔沒有被修改，而且設定正確。
3. 確認您的代理伺服器已被正確指定。有時，IE “區域網路設定”代理伺服器一項中的一些核取方塊會無意地被選中。
4. 如果啓用了使用者端服務，電腦中會在暫存中保存以前解析過的主機名。該項服務在本系統中作用不大，反而可能會因爲暫存了舊的解析名稱而導致無法正確存取 UU100/UU200。您可以臨時停用該服務以查看這些問題是否已被解決。

（11） 無法通過 IE 下載使用者端軟體，原因何在，如何解決？

當使用者無法遠端下載使用者端軟體時，請考慮以下兩種可能的原因：

a) 使用者許可權不足；

該使用者可能不具備下載或安裝 ActiveX 元件的許可權，請聯繫管理員確認。

b) 系統是否不支援 ActiveX 元件的下載；

和其他大多數 SSL VPN 產品一樣，UU200 使用者端機器對 IE 的安全設定有以下要求：

“ActiveX 元件和插件”設定項	**設定值**
對已標誌爲可安全執行腳本的 ActiveX 元件執行腳本	啓用/提示
下載已簽名的 ActiveX 元件	啓用/提示
運行 ActiveX 元件和插件	啓用/提示

否則 IE 將拒絕下載 UU200 的使用者端軟體，使用者介面也不會顯示在螢幕上。您可以存取網頁“http://autos.msn.com/gallery/”（該網頁有一些 ActiveX 元件）。通過查看是否所有的圖片都能在該網頁正確顯示，由此可驗證是否能排除這種可能。如果這些圖片確實不能在該網頁正確顯示，請修改您機器上的安全設定。

（12） 初始安裝 UUSOFT 軟體時，無法順利安裝，爲什麽？

檢查安裝 UUSOFT 的 PC 上是否安裝了其他 VPN 用戶端軟體、個人防火墻軟體，或帶有 virtual adapter 的軟體等，因爲這些軟體可能會與 UUSOFT 不相容，請先卸載這些軟體後，再安裝 UUSOFT。

（13） 升級 UUSOFT 新的版本時，無法正常升級，怎麽辦？

請檢查升級時，是否退出當前正在運行的 UUSOFT，如果還是不行，請先卸載原來舊的版本，重新啓動電腦後，再安裝新的版本。

第9章 附 錄

9.1 UUDynamics File Browser Express/ File Browser 使用説明

“UUDynamics File Browser Express”和“UUDynamics File Browser”是 UUDynamics 公司爲客戶提供的兩種遠端檔案存取服務機制。通過配置 ***i*STAR™**系統架構中 UU100/UU200/UU1000，可以將檔伺服器上的共用檔案安全簡便的發布給遠端的使用者使用。

只需簡單的配置，“UUDynamics File Browser Express”就可以將伺服器端的 Windows Share 顯示在使用者端，通過命令按鈕的使用者介面提供上傳、下載、刪除、更名等操作功能；而“UUDynamics File Browser”則在伺服器端和 IIS/FTP 集成，在使用者端和 Windows Explorer 集成，能提供 Windows 平臺上標準的檔 drag/drop, copy/paste 等完整的檔管理功能，爲了使用此功能，使用者必須瞭解 IIS/FTP 的配置方法。

使用者可以根據不同的情況，選用“UUDynamics File Browser Express”或“UUDynamics File Browser”。

I UUDynamics File Browser Express

NetBIOS 目錄共用是基於 NetBIOS 協定，存取某台伺服器上所有的共用檔案夾；但由於它是基於區域網路的設計，所以在進行跨地域的遠端檔案存取時，如果從使用者端到遠端伺服器端的網路延遲超過 300-500ms 時，那 NetBIOS 目錄共用就無法工作。UUDynamics File Browser Express 目錄共用在網路的一邊使用 NetBIOS，因此檔伺服器端無需任何修改就能在 UU100/UU200/UU1000 上發佈共用檔案；而在網路的另一邊使用了 HTTP 傳輸機制，使得跨地域傳輸檔案時，既提供易用性又能夠避免 NetBIOS 在遠端服務時網路延遲的問題，在網際網路上提供非常好的存取性能。

UUDynamics File Browser Express 用 Internet Explorer，檔伺服器端無需任何修改就能在 UU100/UU200/UU1000 上發佈共用檔夾。同時，UUDynamics File Browser Express 整合了許可權存取機制，保護檔案不被未經授權的使用者存取。目前 UUDynamics File Browser Express 只支援單個的檔案上傳，簡單的檔案管理。

設定 UUDynamics File Browser Express 服務：

1． 設定檔伺服器端：

發佈 UUDynamics File Browser Express 服務，實際上在檔伺服器端無需額外安裝設定，只需要按照常規共用一個或多個檔夾，爲共用的檔案夾設定合適的存取許可權。如果需要允許匿名存取，則需要開啓 Guest 使用者。

對於 Linux 的 File Server，需要將 Linux 機器設定成 SMB Server 或者 NFS Server（只在 UU200 上支援）。

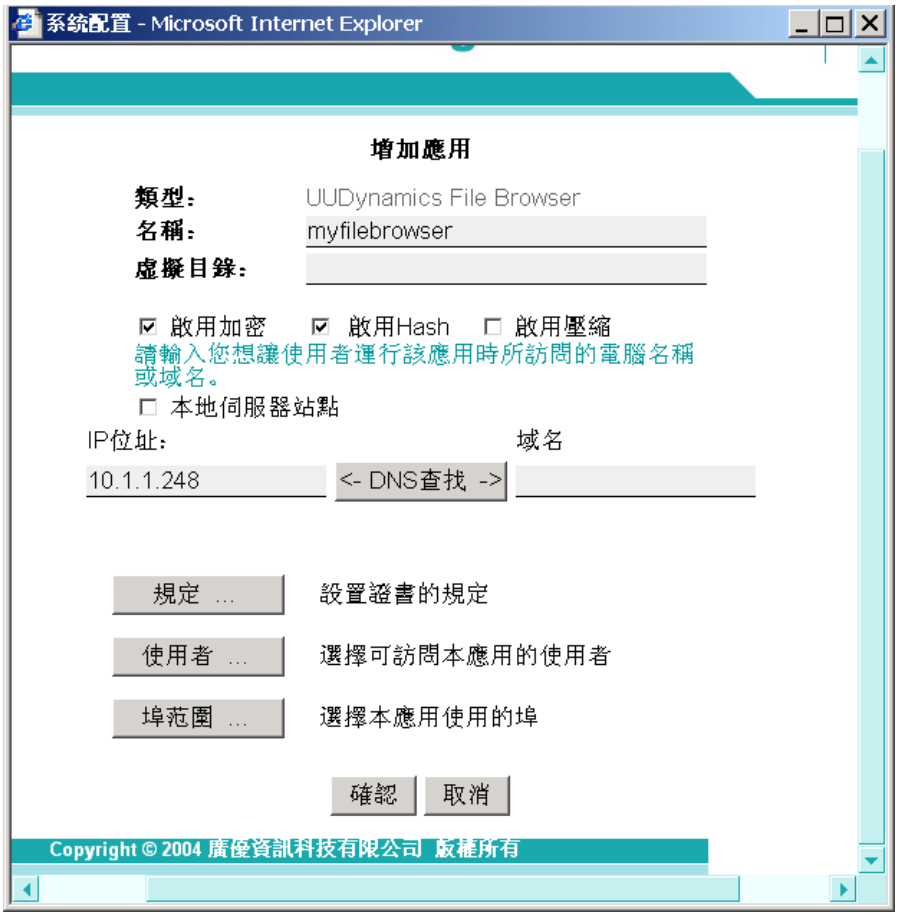
ⅰ 注意：

在發佈 UUDynamics File Browser Express 服務之前，請先驗證共用的檔案夾的設定。您可以通過區域網路存取某台已共用檔夾的伺服器，驗證是否能夠正確存取這個共用檔夾，存取許可權設定的是否正確。Windows 2000/XP/2003 的檔伺服器，請檢查域或本地安全策略的設定，以保證授權使用者可以存取共用檔夾。如果存取能夠正確執行，就可以正確發佈 UUDynamics File Browser Express 服務。

2． 配置 UU100/UU200/UU1000：

在 UU100/UU200/UU1000 上發佈 UUDynamics File Browser Express 服務與發佈其他應用程式類似。發佈應用的詳細方法請參閱“UU100/UU200/UU1000 使用者手冊”中的發佈應用程式（Shared Application Service）部分。

發佈 UUDynamics File Browser Express 服務的介面如下圖所示：



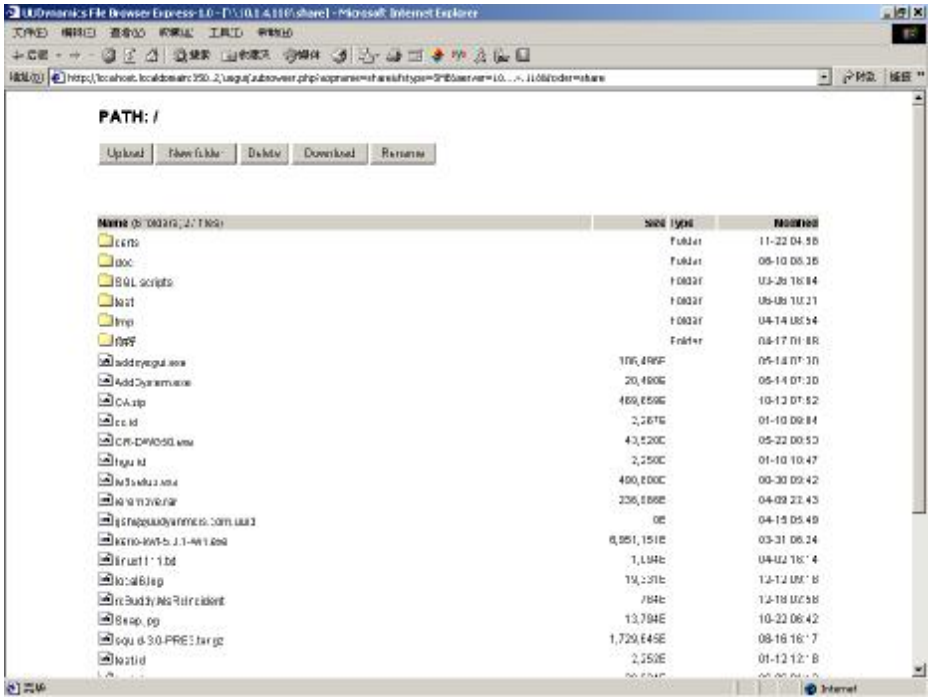
參數名	說明
名稱	爲這個應用服務取一個名字，這個名字將顯示在使用者端的視窗中。如果有多個

	UUDynamics File Browser Express 服務，則必須爲每一個服務取不同的名字。
伺服器類型	選擇檔伺服器的類型。默認爲 SMB，我們在將來會提供更多的可用類型。
虛擬目錄	共用檔夾名。設定成伺服器上共用名稱，以存取特定的共用檔夾。[目前不支援中文或其他含特殊字元的共用名稱]
啓用加密/Hash/壓縮	選擇加密/Hash 演算法/壓縮方法。
IP 位址、功能變數名稱	檔伺服器的位址或 DNS 名稱。DNS 查找的結果依賴於本地 DNS 的配置。
使用者	選擇可以使用這個服務的使用者。

例如，一台地址爲 192.168.0.1（DNS 名：file.test.uud），共用了名爲 share 的檔夾，則虛擬目錄輸入“share”，IP Address 輸入“192.168.0.1”，或者 DNS 輸入“file.test.uud”。

3． 設定使用者端：

UUDynamics File Browser Expres 的使用方法與其他被發佈的應用程式的使用方法完全相同。雙擊視窗中的 UUDynamics File Browser Expres 的圖表，在新視窗中輸入認證資訊，通過認證就可以進入共用檔夾，使用者可以按照所擁有的許可權，執行標準的檔案操作。File Browser Express 的介面如下圖所示：



其中：

按鈕名	說明
Upload	表示文檔上傳到遠端檔伺服器上的 Windows share 中
New Folder	表示在遠端伺服器上的 Windows share 中新建一個子目錄
Delete	用於刪除一個檔或子目錄
Download	用於將遠端文件伺服器上的 Windows share 中的文件下載到使用者端
Rename	用於對文件或子目錄的改名

I UUDynamics File Browser

Ftp 是常用的一個 C/S（客戶/伺服器）架構的檔案傳輸工具，它在網際網路上有很好的性能。Microsoft IIS 中的 FTP 服務整合 Windows 的認證和存取控制機制。“UUDynamics File Browser”就是利用 Microsoft IIS 中的 FTP 服務，可以與 Windows 平臺完全整合，在網際網路上提供很好的性能的文檔存取服務；同時，“UUDynamics File Browser”也可以通過一般的 FTP 伺服器來提供 Linux/UNIX 伺服器上的遠端檔案存取。由於 UUDynamics File Browser 結合了 IIS 服務，與 UUDynamics File Browser Express 相比提供了完整的檔案操作，使用者可以執行標準的檔案建立、複製、移動和移除等操作；而 UUDynamics File Browser Express 只能做基於按鈕的操作。

設定 UUDynamics File Browser 服務：

1. 設定檔伺服器端：

在 Linux/UNIX 上的設定很簡單，就是一個一般的 FTP 伺服器的設定，這裏不再敍述。以下介紹在 Windows 平臺上設定和使用 UUDynamics File Browser 的方法。

Windows 平臺上的 IIS/FTP 組合不僅提供對本地電腦上的虛擬目錄的存取，還提供通過 FTP 伺服器實現對區域網路上共用資源的存取。有關 IIS/FTP 的設定，本手冊中只做簡單介紹，詳細操作指南請使用者參考 Windows 的相關幫助資訊。

要使用 UUDynamics File Browser 存取遠端檔案，除了部署 ***i*STAR™**產品之外，還要完成以下步驟：(1) 首先要安裝和設定 IIS；(2) 然後在 UU100/UU200/UU1000 上發佈 UUDynamics File Browser 給遠端使用者。

1.1 **IIS 的安裝**：

根據您使用的作業系統不同，你可能需要安裝 IIS。

（1）Microsoft Windows 2000 伺服器/ Microsoft Windows 2000 Advance 伺服器

Microsoft Windows 2000 伺服器/ Microsoft Windows 2000 Advance 伺服器上已經預設安裝幷啓動了 Microsoft IIS（如果您的 IIS 沒有啓動，請參考 Microsoft Windows 2000 伺服器/ Microsoft Windows 2000 Advance 伺服器幫助系統，啓動 IIS）

（2）Microsoft Windows 2000 Professional/ Microsoft Windows XP Professional/ Microsoft Windows 伺服器 2003

Microsoft Windows 2000 Professional/ Microsoft Windows XP Professional/ Windows 伺服器 2003 的預設安裝不包括 Microsoft IIS 的安裝，但系統盤包括該軟體，使用者必須手動安裝。 安裝 IIS 的方法如下：

開啓控制面板中的“增加或移除程式”，在“增加或移除程式”視窗中選擇“增加/移除 Windows 組件”後，在彈出的如附圖 1 所示視窗中，選擇“Internet 資訊服務（IIS）”後,按“下一步”就可以安裝 IIS，您只要根據提示進行操作即可。

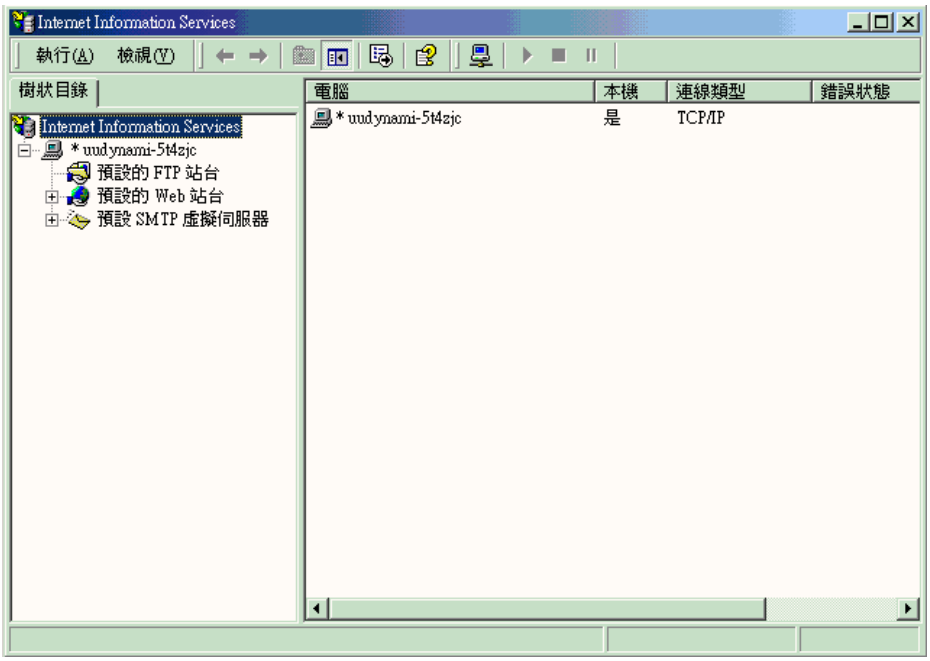
1.2 **IIS 的配置：**

安裝好 IIS 後，您還需設定 IIS 中的 FTP 來指定被遠端存取的 folder 和存取許可權。

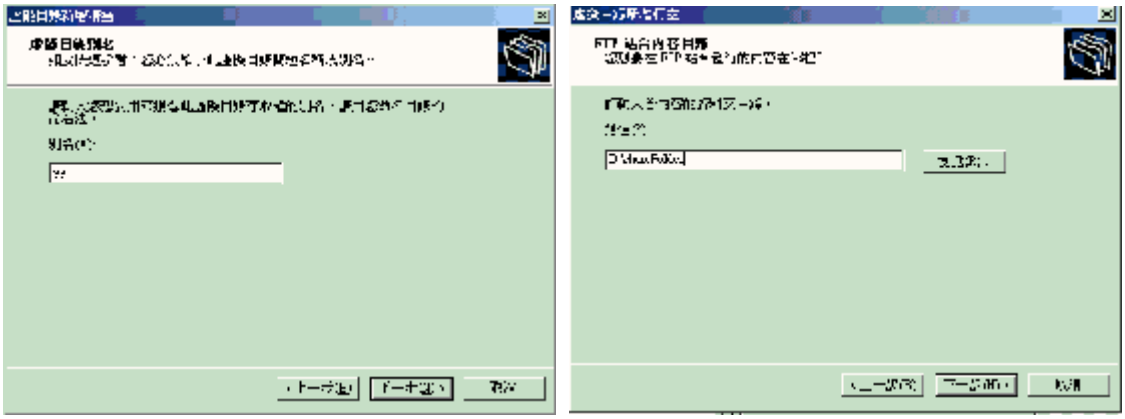
（1）創建 Virtual Directory

首先確定需要被遠端存取的本地目錄，在 FTP 伺服器上創建虛擬目錄，與該實際目錄連接。具體操作方法如下：

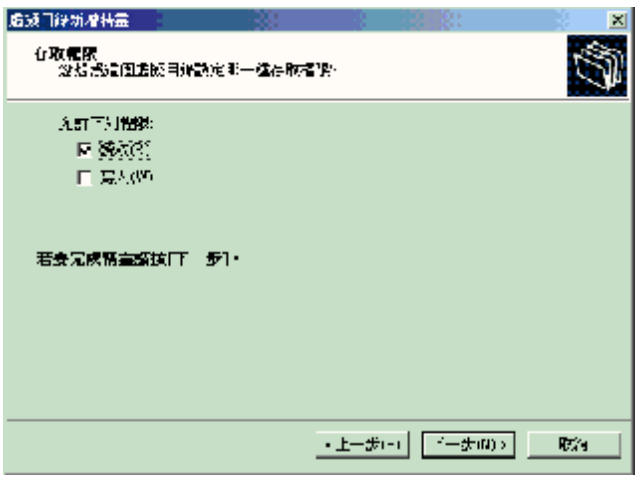
開啓控制面板中的“管理工具”，運行“Internet 服務”管理器（如附圖 2 所示）；配製“默認 FTP 站點”的屬性，選中“默認 FTP 站點”，點選滑鼠右鍵，選擇“新建”->“虛擬目錄”，出現如附圖 3 所示的介面，輸入別名“虛擬目錄名”；然後 Browse 或輸入物理錄；如附圖 4，設定該目錄的存取許可權；最後按“完成”就創建好了虛擬目錄。



附圖 2



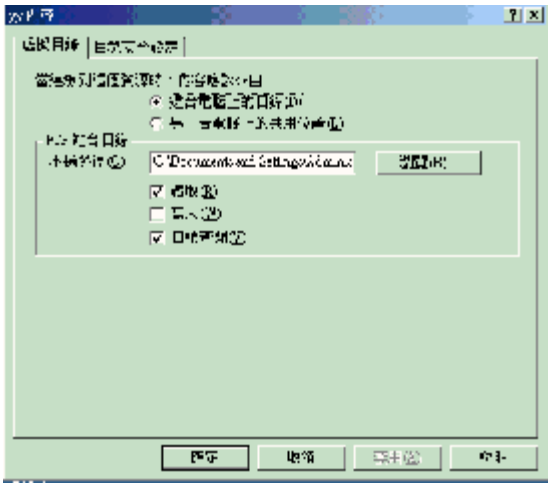
附圖 3



附圖 4

（2）建立連接網路中電腦的共用位置的虛擬目錄

選中某個建好的虛擬目錄，點選滑鼠右鍵，選擇“屬性”，可以看到如附圖 5 所示的視窗：



附圖 5

連接此資源時，內容應該來自於：選擇“另一台電腦上的共用位置”，然後再下面的網路共用中按照\\伺服器\共用的格式填入區域網路中的共用位置，再按“連接爲”輸入對此資源存取的使用者名和密碼；最後選擇遠端客戶的存取許可權。

（3）設定存取許可權

可以從以下四個方面來設定存取許可權：FTP 站點許可權設定、NTFS 許可權設定、允許以匿名存取、啓用 FTP 基本驗證方式。

FTP 站點許可權設定：

IIS 的 FTP 服務器具有靈活的目錄存取控制，它可限制使用者對站點或目錄的讀、寫許可權，此外它還可根據使用者端 IP 位元址進行存取控制。具體方法如下：開啓 IIS 管理控制臺：開始->程式->管理工具->Internet 服務管理器；右鍵選擇 FTP 站點或虛擬目錄屬性，在主目錄或虛擬目錄屬性頁中，選擇讀取及寫入選項。

NTFS 許可權設定：

FTP 伺服器可以利用 Windows 作業系統中的檔或檔夾的 NTFS 許可權屬性來控制使用者存取，因此一個使用者若需存取某個 FTP 站點或目錄，則其必須對該實際目錄有至少讀的許可權。

檔或檔夾的 NTFS 許可權屬性具體的設定方法爲：

開啓 Windows 資源管理器 ，找到 FTP 站點或虛擬目錄所對應的實際目錄，右鍵點選屬性，選擇安全性 ，賦給該 FTP 使用者相應的 NTFS 許可權(讀取，寫入)。

允許以匿名或指定使用者身份存取：

開啓 IIS 管理控制臺：開始->設定->控制臺，開啓控制臺中的“系統管理工具”，運行“Internet 服務管理員”；點選“默認 FTP 站臺”，右鍵選擇“內容”，在彈出的視窗中（見附圖 6），選擇“安全設定帳戶”，勾選“允許匿名連接”。這樣，遠端客戶訪問時就有系統預設使用者 IUSR_…的許可

權，您也可以指定一個使用者。

附圖 6

啓用 FTP 驗證：

如果您想讓每一個來存取的使用者輸入自己的使用者名和密碼，擁有自己的許可權，則不要勾選“允許匿名連接”，這樣就起用了 FTP 基本驗證方式。

對於利用 FTP 基本驗證方式存取的使用者，其存取權利除了前面敍述的 FTP 站點許可權和 NTFS 許可權外，還需要使用者許可權設定。

因 FTP 採用基本驗證方式，所以基本驗證的使用者權利要求也適用於 FTP 驗證。基本驗證方式要求存取的使用者對目標主機具有從網路存取此電腦和在本地登入兩種許可權。這兩種許可權需要在安全策略中設定。在 Windows2000 中，存在三種安全策略：域安全策略，本地安全策略，網網域控制器安全策略，它們的優先順序爲：網網域控制器安全策略、域安全策略、本地安全策略。在設定安全策略時需注意有效的策略中允許使用者從網路存取此電腦和在本地登入兩種許可權。

配置方法爲：

如果 FTP 伺服器安裝在網網域控制器上，則由於網網域控制器安全策略的策略設定優先順序最高，因此我們在網網域控制器安全策略中進行策略更改（爲減少安全風險，強烈建議使用者不要在網網域控制器上建立 FTP 站點）：

開始->程式->管理工具->網網域控制器安全策略

如果 FTP 伺服器不是網網域控制器(DC)，則由於一般域安全策略中不會對使用者許可權進行設定，因此本地安全策略中的設定也可生效：

開始->程式->管理工具->本地安全策略

雙擊展開本地策略，雙擊展開使用者權利指派，在從網路存取此電腦和在本地登入中檢查該 FTP 使用者是否已具有該許可權，否則，增加該 FTP 使用者。

如果安全策略配置有改動，可用以下命令手動刷新策略配置，使其立即失效：

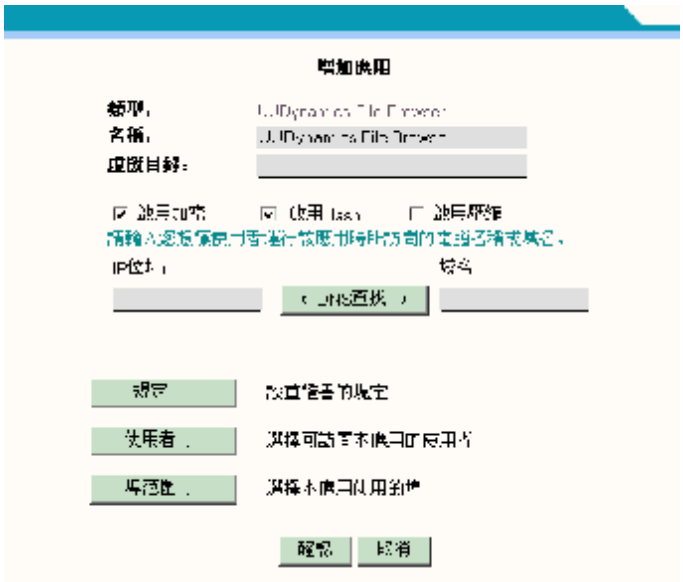
secedit /refreshpolicy machine_policy /enforce

ⅰ 注意：

IIS/FTP 的配置正確與否，可以先在區域網路中進行測試，即在區域網路中選擇一台電腦，啓動 IE,通過 FTP 連接到 FTP 伺服器，執行所需的操作。我們建議只有在區域網路測試成功後，才將它配置到 *i*STAR™上實現遠端操作。

2．UU100/UU200/UU1000 端配置

在 UU100/UU200/UU1000 上發佈 UUDynamics File Browser 的方法請參見“UU100/UU200/UU1000 使用者手冊”中的發佈應用程式（Shared Application Service）部分。 發佈“UUDynamics File Browser”的介面如附圖 7 所示，除了和其他應用一樣需要填寫共用應用名及所在伺服器位址或名字外，還需填寫 Virtual Directory 名，即 IIS 伺服器端設定的別名。



附圖 7

其他有關設定請參見本手冊第 4 章。

3．配置使用者端：

UUDynamics File Browser 在使用者端的使用和其他被發布的應用程式沒有任何區別，輕按兩下視窗中 UUDynamics File Browser 的圖示（即 IE 的圖示），我們的軟體會自動將 FTP 設定成 Passive 模式，使用者可以執行標準的檔案建立、複製、移動和移除等操作。

9.2 *i*STAR™支援的客戶/伺服器應用

市場上不同的 SSL VPN 產品所支援的應用屬於以下幾種情況：

1． 基於 Web 的應用的逆向代理：

這種方法僅僅支援那些被 Web 化的應用，就是用 Web 工具開發且使用者端是 Internet 瀏覽器的應用。

2． 傳統應用的客戶/伺服器工具：

由於大量應用是在 Web 時代前開發的，這種類型已經變成任何 SSL VPN 的必備功能。大多數廠商用 ALG(應用層閘道)來支援這類應用，即爲一些流行的應用，如 Outlook, Lotus Notes, Telnet 等，提供專門的或特定的支援。

3． 遠端虛擬接入：

這一種全能的方法，它可以解決前面兩種方法解決不了的問題。所有的廠商都採用傳統的 VA(虛擬網卡)機制來講一個本地電腦虛擬接入遠端網路。由於這種機制建立在第三層網路結構上的，使用者端和伺服器端必須解決好可能的 IP 位址不相容的問題。

在不同 Microsoft 平臺上的 ***i*STAR™**客戶軟體是 ***i*STAR™**體系結構中最重要的元件之一，***i*STAR™**支援所有三類應用，但和我們的競爭者不同的是，***i*STAR™**用一個通用的工具來支援客戶/伺服器軟體，包括幾乎所有的傳統客戶/伺服器應用軟體。儘管爲了確認對客戶應用的支援，***i*STAR™**還是需要“應用認證”，但提交到我們驗證中心的應用軟體中還沒有不被 ***i*STAR™**支援的。借助於這個強大的使用者端軟體工具，***i*STAR™**在一個統一、通用的框架下支援上述的 1，2 項，基於這個統一的框架，伺服器的管理也被大大簡化了。

本文檔試圖要定義由 ***i*STAR™**的通用客戶工具支援的這類客戶/伺服器應用。下列的條件只適用於第 1 和 2 類。

9.2.1 使用者端到伺服器端

***i*STAR™**是通過“虛擬化”使用者端應用來實現對客戶/伺服器應用的支援的。所有的網路環境和操作被 ***i*STAR™**的客戶軟體截獲並隨即被 ***i*STAR™**發布單元代理傳輸到伺服器端。這種虛擬化的運行對於特定啓動的應用是透明的。

注意，只有使用者端的網路操作被代理了，TCP/IP 的操作必須從使用者端發起；伺服器邏輯獨立於 ***i*STAR™** 而運行，所以不允許發起對使用者端的網路操作。

9.2.2 對網路資料包中的使用者端位址的敏感性

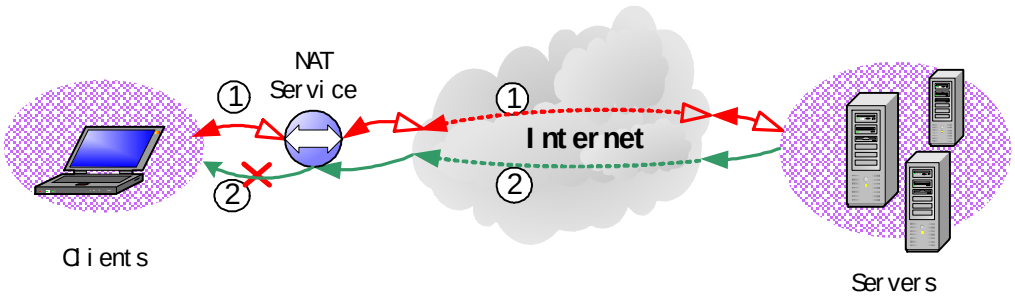
由於 ***i*STAR™**虛擬化使用者端應用，所以那些發出包含使用者端的網路環境裏的 IP 位址的網路包的應用不能被支援。

9.2.3 支援 IP 應用及特定的 NetBIOS 應用

***i*STAR™**客戶軟體僅支援 TCP/IP 應用。原始的 NetBIOS 不能支援，但有一類 NetBIOS 除外，即由 UUDynamics 提供了的“**Custom – Network drive based C/S**”應用(詳細內容請參考“**錯誤! 找不到參照來源。**發佈應用程式” 中的例二)。

9.2.4 NAT(網路位址轉換)的友好性

伺服器不能發起對使用者端網路操作，而且網路資料包不能包含使用者端的 IP 位址資訊，有一個簡單的測試可以來判斷應用是否滿足這個規定。應用必須能從 NAT 後面運行，去存取 NAT 外的伺服器。換句話說，滿足條件的應用必須是 NAT 友好的。



附圖 10

Passive 應用：

如果是這種應用，由 Client 端發起的 TCP 連接請求經過 NAT 伺服器到達伺服器端（如連接①→所示），伺服器端僅利用原有連接將資料包返回 Client 端（如連接①←所示）。這種應用由於使用的是已有的連接通道，因而可以真正送達 Client 端。

這種應用的典型例子有 Data 模式的 Netmeeting 應用及 FTP 服務等。

***i*STAR™**支援這類應用。

Active 應用：

如果是這種應用，由 Client 端發起的 TCP 連接請求經由連接穿越 NAT 伺服器到達伺服器端（如連接①→所示），伺服器端會將許多其他控制資訊（如 IP 位址、埠等）連同資料包一起打包，沿著新建的連接（連接②）返回 Client 端。由於這種資料包無法穿透 NAT 伺服器，因而不能真正送達 Client 端。這種應用的典型例子有語音模式的 Netmeeting 應用。

對於這類應用，***i*STAR™**暫不支援。

9.2.5 WinSock 應用

支援的應用必須基於 Windows Winsock。

9.3 *i*STAR™安全機制的實現

確保系統的安全性是 ***i*STAR™**系統結構的最基本特點。衡量一個系統的安全與否主要從安全認證、授權和資料加密三個方面考慮。這裏介紹 ***i*STAR™**在這幾個方面的實現要點。

- **安全認證**

i*STAR™**系統結構中兩級安全認證。第一級是建立通信隧道前註冊到 UUExchange/UUSwitch 時的認證，每個 UU200 都有一個唯一的 UUID 檔來標識，通過提供自己的證書、認證對方證書在使用 ***i*STAR™**技術服務前都經過身份驗證；第二級認證是應用服務認證，i*STAR™**中提供了兩種認證方式：集成 Windows AD 使用者認證和本地加密檔認證；此外，具體應用（如 FTP, IBM Notes, MS Terminal 等）也提供的各自身份驗證。

- **授權**

授權是指系統控制只有有權使用某一應用服務的使用者才能使用該服務。***i*STAR™**系統結構中對所發布應用、子網及遠端管理都有授權控制，沒有被授權的使用者不能使用這些資源。在發布一個應用服務時，可以設定哪些使用者被授權存取該應用，使用者可以使用哪台伺服器上的該應用服務，該應用只能使用哪些埠；發佈一個子網時，需要設定哪些使用者可以使用這個子網中的哪些電腦。

- **保密性**

經過 ***i*STAR™**結構傳輸的資料實現端到端的加密，即加密和解密都在使用者端執行，傳輸的全程都是加密資料；同時，***i*STAR™**中採用標準的加密和 HASH 演算法，并提供演算法協商功能，確保使用者資料的保密性。對於注重性能的應用，也可以選擇不要加密，即演算法爲 NULL。

9.4 UUSoft 命令集

UUSoft 支援 Command Line 命令的操作方式來設定和管理，管理人員可以在安裝 UUSoft 的電腦上執行這些命令，也可以遠端執行 Telnet 連接到安裝 UUSoft 的電腦上，遠端執行 Command Line 命令的電腦必須安裝 FTP Server，以便使用下載或上載文件時使用。

命令格式：

uusoft [*command*] [*parameter1*] … –p [*admin-pwd*]

命令名：uusoft

command：子命令。包括：

set, status, importcfg, exportcfg, exportlog, add, change, remove, start, restart

parameter：表示執行此命令時所需的參數；

admin-pwd：是管理員密碼，只有知道此密碼的人才能管理 UUSoft，每條命令都需要輸入管理員的密碼，初始密碼是 Uuadmin，可以通過 uusoft set 命令修改管理員密碼;

Command	**Parameter**	**Default Value**	**Mandatory / Optional**	**Comment**	**Remark**
set	UUExchange		M	1) Direct Access 方式: Publisher 的 IP 地址或 DNS 名稱 2) Private Access 方式：UUExchange 的 IP 地址或 DNS 名稱	
	Cipher	AES-256-CBC DES-EDE3-CBC DES-CBC	O	加密演算法設定	
	Hash	MD5,SHA1	O	Hash 演算法設定	
	LogL	6	Optional	Log Level (0-7)	
	LogMS	1M	Optional	Max Size of Local Log File (MB)	
	LogS		Optional	Log Server IP 或 DNS 名稱	
	-UploadUrl			上傳 Log 文件至 Ftp Server。	

	-UploadBackupUrl			上傳 Log 文件至備用的 Ftp Server。	
	-UploadUser			上傳 Log 文件時所使用的 User 名稱。	
	-UploadPwd			上傳 Log 文件時指定 User 的 Password。	
	ProxyT	0	Optional	Proxy Type (0: directly connect, 1: Sock4, 2: reserved for Socks5, 3: Web Proxy)	
	ProxyS		Optional	Proxy Server IP 或 DNS 名稱	
	ProxyP		Optional	Port of Proxy Server	
	ProxyUser		Optional	Username for Proxy authentication	
	ProxyPwd		Optional	Password for Proxy authentication	Case Sensitive
	AdminPWD	UUAdmin	Optional	系統管理員密碼	Case Sensitive
	RecoverTime	5	Optional	確定是否需要恢復上次設定的時間(Minutes)	
	p		Mandatory	當前管理員密碼	Case Sensitive
	view			查看當前設定參數	
add			Mandatory	1) Direct 模式: 增加連接的 Local host 2) UUExchange 模式： 增加連接的 Publisher UUID	目前最多支援 1 個

Remove			Mandatory	1) Direct 模式: 刪除連接的 Local host 2) UUExchange 模式： 刪除連接的 Publisher UUID	
Start/ Restart	p		Mandatory	當前管理員密碼 (啓動/重啓 UUSoft)	Case Sensitive
Importcfg/ Exportcfg	f		Mandatory	導入導出設定資訊的文件	
	p		Mandatory	當前管理員密碼	Case Sensitive
Exportlog	f		Mandatory	導出日誌的文件	
	BT			導出日誌的起始時間	
	ET			導出日誌的終止時間	
	p		Mandatory	當前管理員密碼	Case Sensitive
Reset				根據當前 Internet Setting 來重新設定	
Show				查看當前設定參數	

術語表

10~15 劃

第三方證書（數位元電子憑證）

第三方證書是用於該 UU200 和使用者端之間建立 https 安全連接時所需的標識該伺服器的數位證書。

從第三方發證機構處獲得數位元憑證的申請的方式及費用可以參考以下兩個網站。

http://www.hitrust.com.tw/hitrustexe/frontend/verisign_price.asp

http://www.globaltrust.com.tw/apply/index.html

某些發證機構所簽發的數位憑證，其根憑證沒有被 Microsoft 公司預先包括在其 IE 的受信任根憑證資料庫之中，在這種情況下，除非使用者將該根憑證輸入到使用者的 IE 瀏覽器根憑證資料庫中，不然會在使用者端跳出一個警告資訊，此時使用者可以用<查看證書>功能鍵檢視數位憑證的詳細內容，待確定之後，按<是>鍵繼續進行操作。

無論第三方發證機構的根憑證有沒有被 Microsoft 公司預先包括在其 IE 的受信任根憑證資料庫之中，都不會影響 iSTAR™的功能。

以下這個網站有詳述 User 如何製作自身的 CSR 檔案，然後再至認證中心申請憑證檔。

http://www.globaltrust.com.tw/support/index.html

http://www.openssl.org/related/binaries.html

注意事項：

- 申請的憑證必須符合 Apache Server 的格式。客戶或經銷商可以利用 OpenSSL 產生 CSR 檔案。
- 由於涉及資訊安全，建議客戶自行辦理較好。
- 建議經銷商或客戶在申請電子憑證時，最好是選擇 DNS Name 而不是 IP。
- 通常辦理電子憑證需，在資料齊全的情況下，應該一個工作天可以完成。

連接方式

UU200 有兩種接入方式供使用者選擇：Direct Access 和 Private Access。

- Direct Access

  如果希望遠端使用者通過 Public IP 訂閱由 UU200 發佈的應用，可選擇該連接方式。

  該方式下, UU200 需要預先準備公共靜態 IP 位址以及閘道、子網掩碼和 DNS。

  此外，爲了使用者端能與它建立 SSL 連接，UU200 上還需要一張數位元元電子憑證。您可以申領一張第三方（如 VeriSign 或 Globaltrust 等）的證書，也可以直接使用系統預設的 UUDynamics 公司的證書。

  & 說明：

  有關第三方證書的獲取和注意事項，請參閱“術語表”之“第三方證書”。

- Private Access

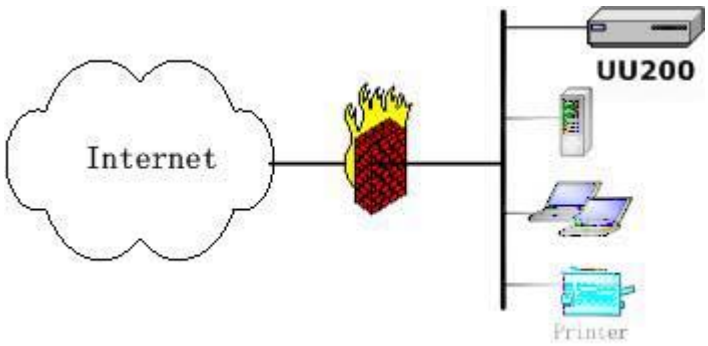
  如果希望遠端使用者通過 Private IP 訂閱由 UU200 發佈的應用，可選擇該連接方式。

  當 UU200 通過 UUSwitch 或 UUExchange 連接時，需要爲 UU200 準備 UUID、私有 IP 位址以及閘道、子網

掩碼和 DNS。

網路模式

UU200 在網路中有三種模式可供選擇：單模式、透明模式和路由模式。您可以根據您的網路結構參考下面的說明來選擇一種模式。



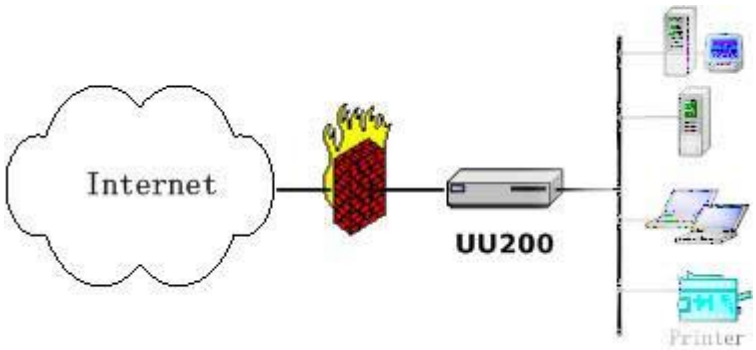
單模式示意圖

單模式：是 UU200 被放置於內部網路中的任意位置的一種模式（見上圖）。

連接方式：UU200 的第 4 網口與您的內部網路相連接。

特點：不改變原網路中的任何設備狀態，配置簡便、快捷。需要時，插到連接網際網路的內部網路上就可使用。可以使其所在的 LAN 得到安全的網路保護。

如果需要發佈整個子網（即 LAN to LAN，參見本手冊“4.2 發布子網”部分）時需要在原有路由器或使用者端增加路由。網路安全保護只限在其所在的 LAN 上。

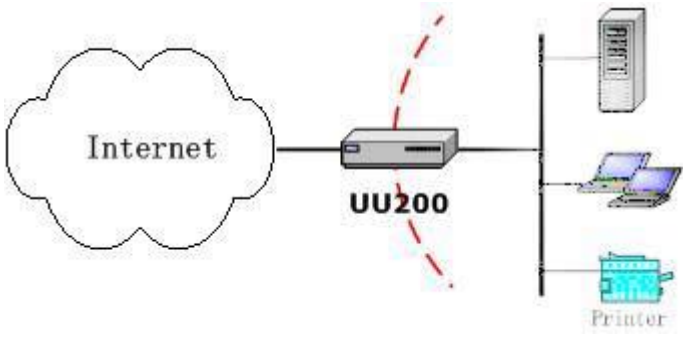


透明模式示意圖

透明模式：是 UU200 被放置於內部網路和防火墻或路由器之間的位置的一種模式。

連接方式：UU200 的第 **1** 網口與內部網路相連，UU200 的第 **4** 網口與防火牆或路由器相連。

特點：配置時不需要變更原有路由器或使用者端的任何配置。可以使在其後面的整個網路得到安全的保護。



路由模式示意圖

路由模式：是 UU200 被放置於防火墻或路由器的位置的一種模式，即 UU200 取代了防火墻或路由器。
連接方式：UU200 的第 **1** 網口與內部網路相連，UU200 的第 **4** 網口與外部網路相連。
特點：在提供 Publisher 功能的同時，也提供了防火墻或路由器功能。

& 說明：
配置時爲了減少影響網路的日常運行，建議先連接到某個 LAN 上進行配置，然後再移到指定的模式位置上。

D

DMZ/DDMZ

（非軍事區）是放置公共資訊的最佳位置，您可以將一些必須公開的伺服器設施，如企業 Web 伺服器、FTP 伺服器和郵件伺服器等這樣的服務放置在這個區域中，而將公司中的機密的和私人的資訊可以安全地存放在內網中，即 DMZ 的後面。這樣使用者、潛在使用者和外部存取者都可以直接獲得他們所需的關於公司的一些資訊，而不用通過內網。

UU200 爲您提供了一種設定和管理 DMZ 的服務——動態 DMZ（即 DDMZ：Dynamics DMZ）。所謂 DDMZ，是指您可以根據您現在的網路狀況，靈活的選擇 UU200 所處的位置，您可以將 UU200 配置爲網路中的第一台防火墻，或是將它放在已有防火墻之後，以得到增強的安全性。

UU200 的 DDMZ 通過這一系列安全策略的組合，幫助您將一些在已在 DMZ 中配置好的服務，例如檔伺服器，WEB 伺服器，FTP 伺服器等，發佈給外部存取者和需要這些公共服務的使用者，而不用擔心對公司內部網路的未授權的存取。

U

UUID

UUID 由主模式 UUSwitch（/UUExchange）分配。UUID 必須是唯一的。用於有效標識發布單元 Publisher（例如：UU100,UU200），以及子模式 UUSwitch(/UUExchange)。
如果 Publisher 的連接方式爲 Private Access 方式，則該 Publisher 必須擁有一個唯一的 UUID。在啓動時 Publisher 用 UUID 註冊到 UUSwitch（/UUExchange）,從而成爲整個 ***i*STAR™**的一部分。
UUID 的格式如 Email 一樣：AAA@bbb.ccc，其中 bbb.ccc 是 Domain 名，例如：aaa@uudynamics.com。
在安裝 Publisher 前，請先聯繫 UUSwitch（/UUExchange）管理員獲取壓縮的 UUID 檔案。