*i*STAR™ UU200 使用手冊

Release 2.2

UUDynamics, Inc.

2004 年 7 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、藍色字體	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	ⓘ 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 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，并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™**（Instant **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。

與其他 VPN 產品相比，***i*STAR™**具有更強大的功能和更具優勢的性價比：

1. 安全性高：

   ***i*STAR™**採用了 SSL(Secure Socket Layer)協定，從應用層面建立安全機制，是 Application Sharing 的概念。通訊雙方在應用層建立通訊，除了能確保雙方的安全之外，也大幅降低規劃 IP 網路的複雜工程。

   - 採用了 SSL(Secure Socket Layer)協定。從應用層面建立安全機制，是 Application Sharing 的概念。通訊雙方在應用層建立通訊，實現應用層使用者存取管理。徹底執行基於使用者的安全政策
   - 對應用程式透明。能夠保護企業網路免於遭受來自外部以及內部的威脅
   - 可以選擇對應用程式進行加密（Encryption & Hash）
   - 支援 Radius、Windows Domain 伺服器等使用者認證方式

2. 接入方式靈活：

   - 支援有公共靜態 IP 位址和沒有公共靜態 IP 位址的使用者
   - 能爲企業夥伴提供安全的，彈性的外聯網(Extranet) 接入方式

- 在任何時間，地點都能提供出外人員或遠端使用者即時，安全的接入
- *i*STAR™獨特的對應用程式透明(Application Transparent)的特性，無論是 Web、Client/Server 應用程式，或是 file sharing，iSTAR™能夠完全支援，不需要加裝軟體或對應用軟體作修改。支援 Web 、C/S 應用及 File Sharing
- 支援 LAN To LAN 功能（僅 UU200 支援）

3. 提供路由功能：

   UU200 和 UUSwitch/UUExchange 支援路由功能。

   - 交換單元網路可以提供最適化路由的選擇
   - 具備爲遠端使用者提供最適化路由的選擇

4. 經濟：

   ***i*STAR™**的另一項獨特設計就是能夠適應有 Public IP，及/或僅具備 Private IP 的使用環境，解決了部分企業因爲 Public IP 資源不足，或是擔心伴隨著使用 Public IP 而帶來的安全性問題。

   由於可以使用 Private IP，因此企業的應用軟體伺服器能夠被放置在內部網路的任何位置，而保護這些伺服器的也不需要做任何改變，真正的作到了不需要改變既有的網路與防火墻配置，適應不同網路架構的需求。

   - 可以共用數位電子憑證

     ***i*STAR™**還能夠將一張 SSL 數位電子憑證共用給多個使用 Private IP 的 Site 使用，節省了企業重複申請 SSL 數位電子憑證的費用。

   - 充分利用網際網路以降低龐大的通訊成本

     採用了 SSL(Secure Socket Layer)協定，從應用層面建立安全機制，是 Application Sharing 的概念。通訊雙方在應用層建立通訊，除了能確保雙方的安全之外，也大幅降低規劃 IP 網路的複雜工程。

   - 控制網路建設、擴充、管理、使用及維護的整體成本（TCO: Total Cost of Ownership）

5. 使用者介面友好：

   - 設備操作簡單，安裝容易。
   - 使用者端使用 IE 瀏覽器，各種應用都以圖示表示。

1.2 *i*STAR™產品系統架構

***i*STAR™**的系統結構如下圖所示：

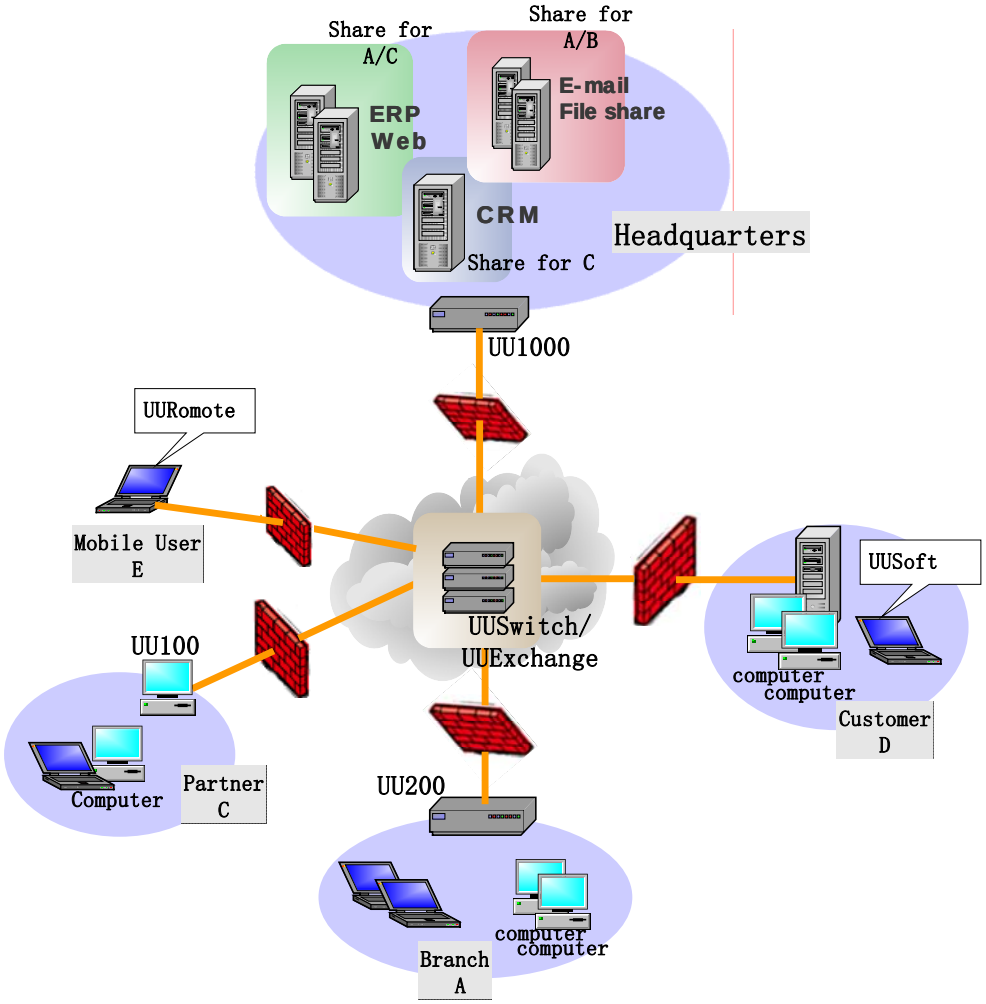


圖 1

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 系統的安裝、設定及復原

2.1 安裝 UU200 的準備

在開始安裝 UU200 之前，請先確認下列的準備：

1. UU200 設備：

- UU200 設備、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

> ⓘ 注意：
> 配置電腦的 Internet Protocol Properties 應該被設定成“自動獲得 IP 位址/自動獲得 DNS 伺服器”模式（DHCP），否則應設定 IP 爲除了 1.1.1.1 外的 1.1.1.0/24 子網內地址。

2. 確認連接方式：

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電子憑證。您可以申領一張第三方（如 Verisign 等）的證書，也可以直接使用系統預設的 UUDynamics 公司的證書。

- 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。

3. 確定 UU200 在網路中的位置：

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。

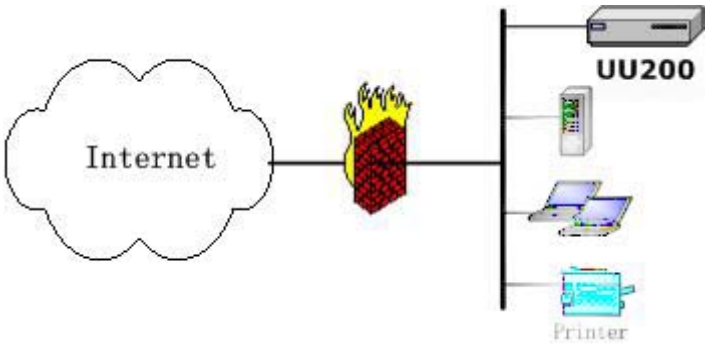


圖 2-1

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。(第 4 網口將在“2.2 安裝 UU200 硬體”中進行說明)

特點：不改變原網路中的任何設備狀態，配置簡單、方便、快捷，配置時隨意、隨時插到企業任何可上網際網路的網路上就可開始配置。可以使其所在的 LAN 得到安全的網路保護。

如果需要配置發佈整個子網（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。

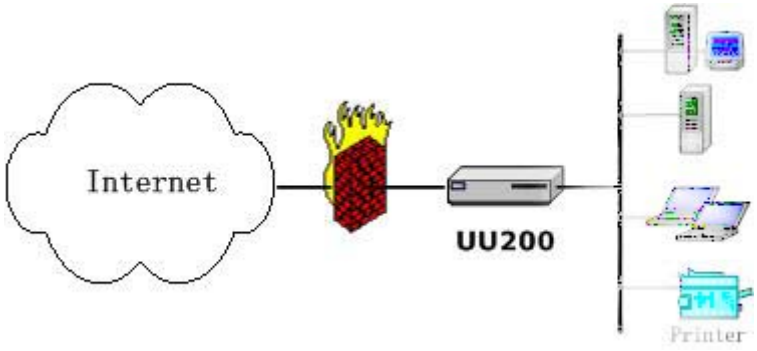


圖 2-2 透明模式示意圖

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。

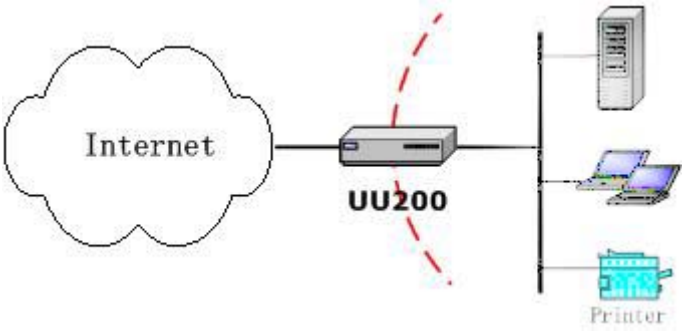


圖 2-3 路由模式示意圖

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。

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。

2.2 安裝 UU200 硬體

2.2.1 設備外觀

UU200 設備的外觀如下圖 3 所示：

圖 3

正面從左到右爲：

- LCD 顯示螢幕：分兩行顯示 UU200 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）**：UU200 連接方式爲 Direct Access 時，顯示 UU200 是否聯機。UU200 連接方式請參考“2.3 安裝 UU200 軟體”之步驟 3。 **Registered（/Unregistered）**：UU200 連接方式（詳見“2.3 安裝 UU200 軟體”之步驟 3）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。標示“1”的埠用於初始設定以及連接 LAN，標示“4”的埠用於連接 WAN。其他標示“2”、“3”的埠爲預設埠，目前暫不使用。

背面爲：

- 電源線接頭
- 電源開關

2.2.2 安裝步驟

您可以依照以下步驟進行安裝：

① 連接 UU200 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 UU200 標示“1”的乙太網路埠；

③ 啓動 UU200 電源；

> 🕮 說明：
> 您可以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）。

④ 啓動配置電腦的 IE 瀏覽器，開始安裝軟體。

2.3 安裝 UU200 軟體

初始設定是指安裝 UU200 成功後必須對系統進行初次設定，以便系統能正常工作。

步驟 1. 進入配置系統

UU200 的出廠預設 IP 位址是“1.1.1.1”，子網路遮罩是 255.255.255.0。因此 首次啓動設定時，請在 IE 瀏覽器位址欄輸入“http://1.1.1.1/admin”，如圖 4 所示，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，系統將進入如圖 5 的介面。

> ⓘ 重要：
> 爲了保障系統及內部資料安全，初次進入配置介面後，請務必修改 admin 的密碼。

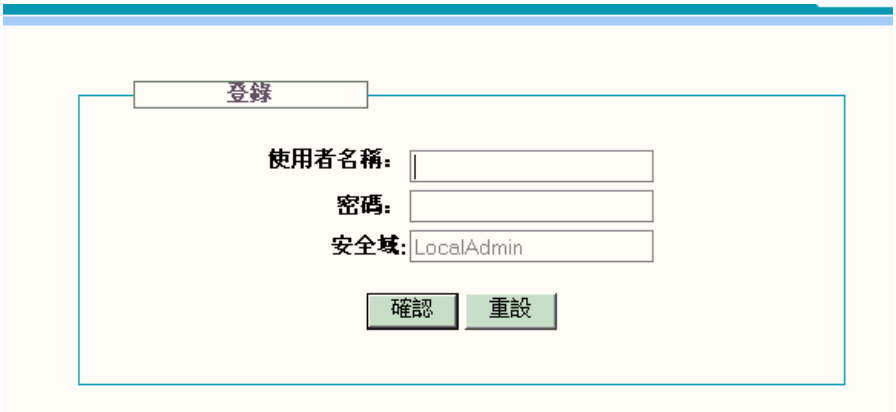


圖 4

步驟 2. 進入系統配置導引精靈

如圖 5，系統的預設爲“沒有備份的配置檔案”：

- “用備份配置檔恢復系統”表示恢復原來的設定。 一般用於完成系統復原後（有關“系統復原”請參考“2.4 系統復原”），恢復原有的設定。
- “沒有備份的配置檔案”表示不需要恢復原來的設定。 一般用於初始設定。

點選下一步進入下一個設定圖 9 的介面。

圖 5

步驟 3. 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。

使用者可以在圖 22 所示介面中點選“iSTAR 設置”，進入設定介面變更接入方式（如圖 6）。

- 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驗證接入安全。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 6 所示介面上，點選倒三角鍵下拉功能表，選擇“Direct Access”連接方式。
2. 如果您需要導入準備好的第三方的證書。請點選<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 7 所示。

> 🕮 **說明：**
> 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。導入的第三方證書必須能被 Apache Web 伺服器所識別,因此使用者在購買證書時，請注意確認所購買的證書類型。

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）。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驗證接入安全。具體內容請參見“UUSwitch 使用者手冊”。

1. 在圖 6 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，輸入 UUSwitch/UUExchange 的 IP 地址或 DNS 名稱。（這裏的 UUID 檔案由在這裏輸入的 UUSwitch/UUExchange 產生得到），如圖 8。
3. 最後按<生效>，使當前的連接模式設定生效。

圖 6

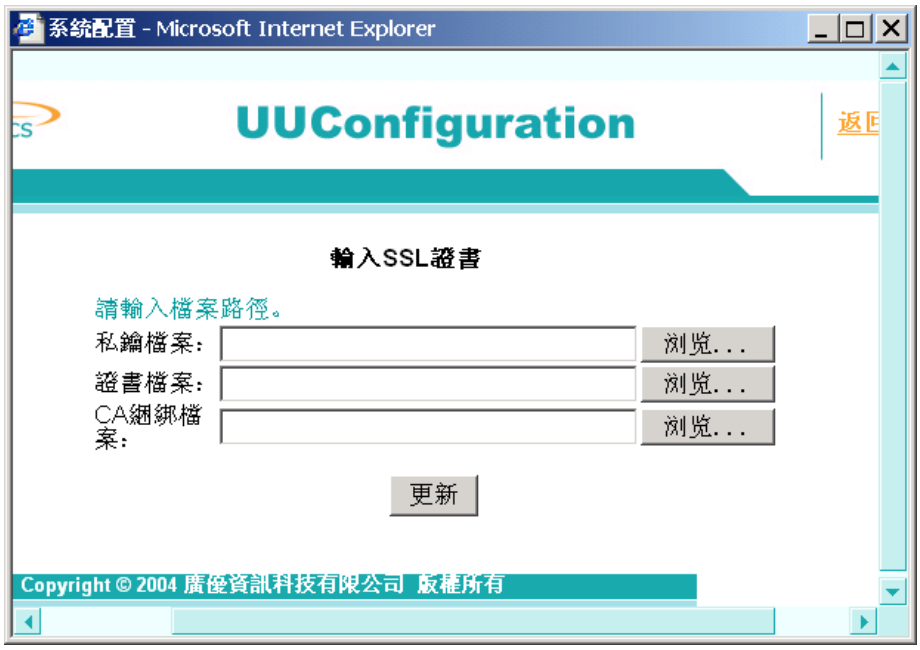


圖 7

圖 8

步驟 4. 選擇模式

如圖 9 所示，UU200 支援“單模式”、“路由模式” 和“透明模式”三種模式。

三種模式的區別請參考“2.1”章節中的 2.確認連接方式。

步驟 5. 進行網路基礎設定

- 單模式的網路設定

如圖 9，點選單模式，可以進入圖 10 所示的介面。

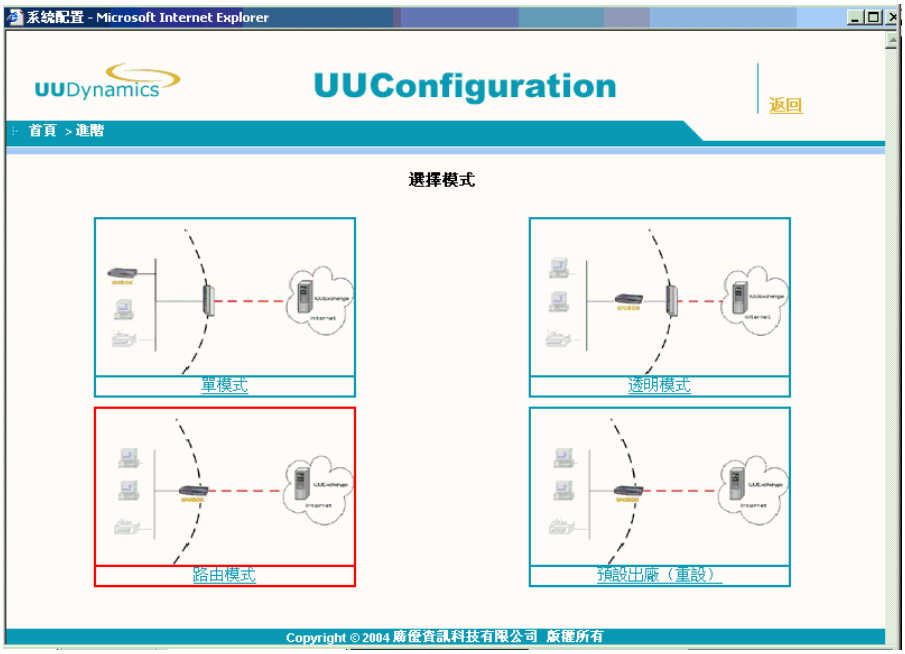


圖 9

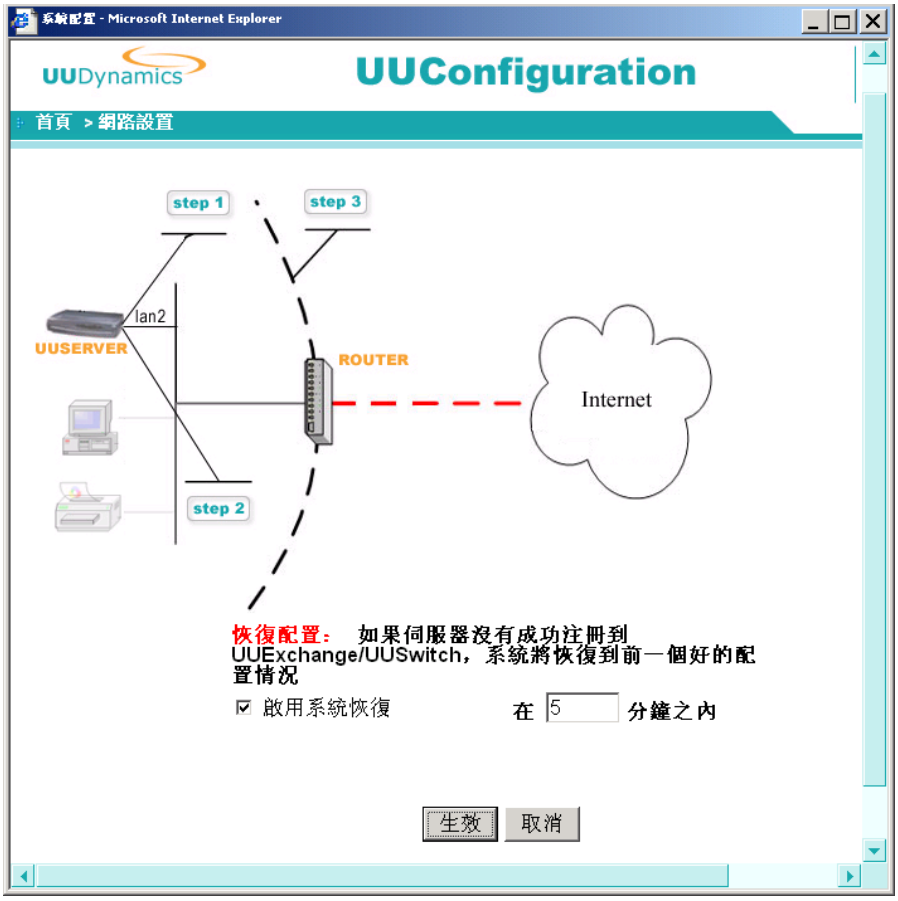


圖 10

🕮 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”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。

圖 11

1. 點選“步驟 1” （進入圖 11 所示介面），輸入本台 UU200 的 IP 位址、及對應的子網路遮罩、閘道、DNS 等參數；輸入完畢後按<保存>進行儲存。

🕮 說明：

– 選“STATIC”時， UU200 的 IP 位址、對應的子網掩碼、閘道及 DNS 等參數會自動從系統讀取。按<保存>儲存。

– 選“DHCP”時（當需要對本台機器動態分配 IP 時適用），點選<保存>保存。

此類型只在“Private Access”方式下出現。

– 選“STATIC/PORT FORWARDING”時（當從防火牆上 port forwarding 到該台 UU200 時使用），選擇本台電腦的“轉接器名稱”，系統讀取本台 UU200 的私有 IP 地址、對應的子網掩碼、閘道及 DNS 等參數，此外還要輸入 DNAT IP，即配置 NAT 的源位元元址。請參考下例。

此類型只有在“Direct Access”方式下出現。

例如：

UU200 放置在局域網路內。該局域網路的防火牆的 PUBLIC IP：61.***.**.1。防火牆裏的埠映射設定爲：61.***.**.2（另一可用 PUBLIC IP）⇔192.168.1.1（UU200 內網地址）。則 DNAT IP 應設定爲 61.***.**.2。

2. 點選“步驟 2” （進入圖 12 所示介面）進行叢集的設定；
   - 勾選“啓用叢集”表示啓用叢集；
   - 輸入叢集 IP、及對應的叢集子網掩碼；

     UU200 能夠以叢集的方式進行均衡負載。 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。
   - 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
   - 輸入完畢後按<保存>進行儲存
3. 點選“步驟 3” （進入圖 13 所示介面）進行代理服务器的設定，系統預設無代理服务器；
4. 完成以上操作後按<生效>，使當前的網路設定生效。

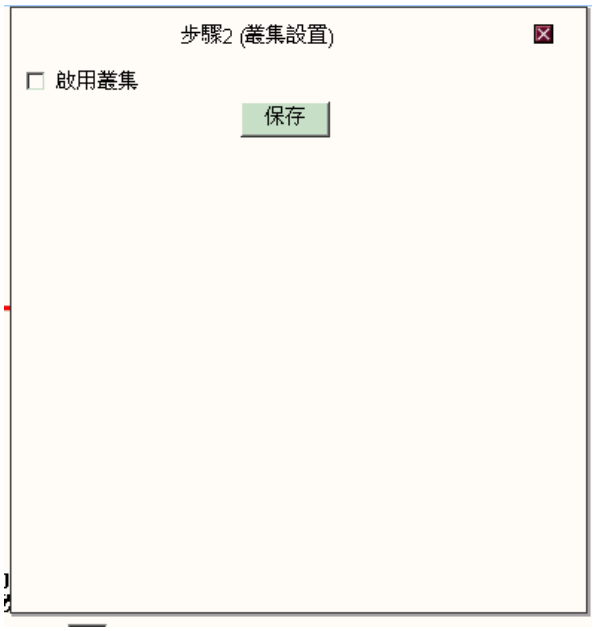


圖 12

圖 13

- 透明模式的網路設定

如圖 9，點選“透明模式”，進入圖 14 所示介面。

1. 點選“步驟 1” （進入圖 15 所示介面），設定本台 UU200 的 IP 位址、及對應的子網掩碼、閘道、DNS 等參數。具體操作步驟請見單模式下“步驟”的設定。輸入完畢後按<保存>進行儲存。

> 🕮 說明：
> - 當預定 UU200 的連接方式爲 Direct Access 時，IP 位址處應輸入公共靜態 IP 位址。
> - 當預定 UU200 的連接方式爲 Private Access 時，IP 位址處可以輸入私有靜態 IP 位址。

2. 點選“步驟 2” （進入圖 12 所示介面）進行叢集的設定，具體同單模式中的叢集的設定相同；
3. 點選“步驟 3” （進入圖 16 所示介面）進行代理服务器的設定，系統預設無代理服务器；
4. 完成以上操作後按<生效>，使當前的網路設定生效。

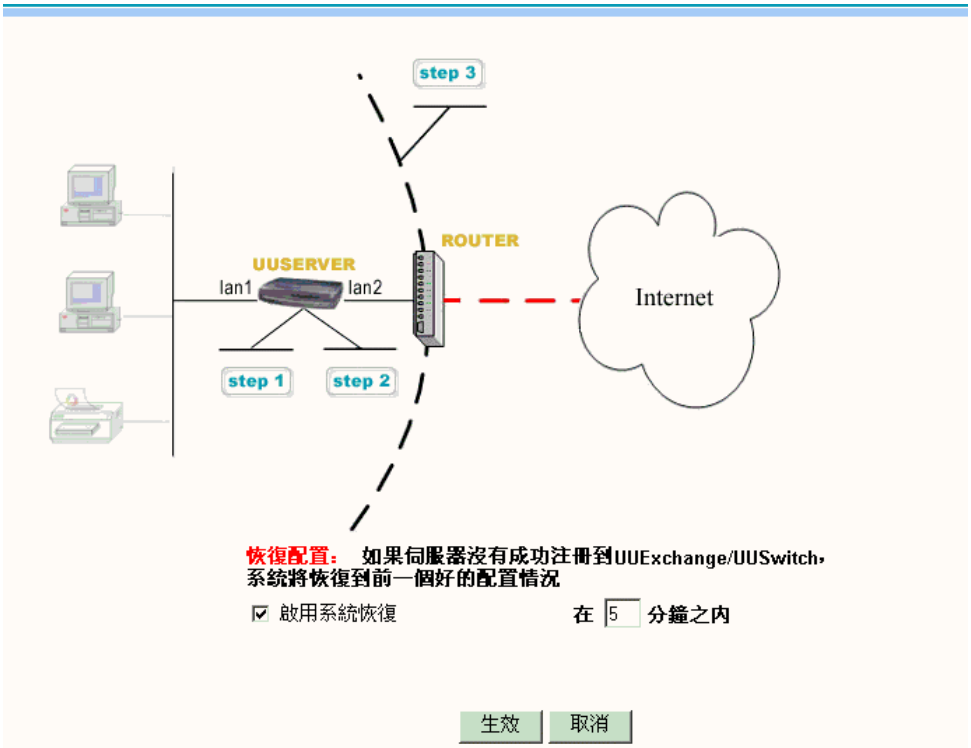


圖 14

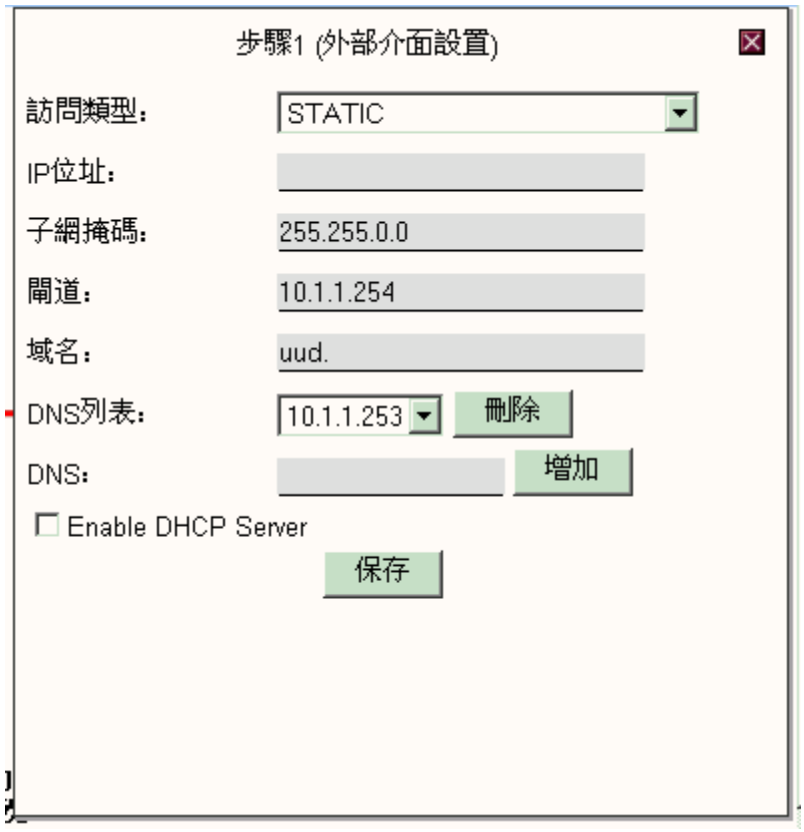


圖 15

圖 16

- 路由模式的網路設定

如圖 5，點選“路由模式”，進入圖 17 所示介面。

1. 點選“步驟 1”（ 如圖 18），輸入 UU200 所在網路中的 IP 地址（這個 IP 地址由網路管理人員根據本地網路的實際情況分配得到），子網掩碼將由 DHCP 自動獲得。路由模式 UU200 可作爲 DHCP 伺服器，在步驟 1 中可以設定可用的 IP 位址範圍。
2. 點選“步驟 2”進行叢集的設定（如圖 8），具體同單模式中的叢集的設定相同；
3. 點選“步驟 3” （如圖 19），分別選用下列不同的上網方式進行相關的設定。

- Static IP 連接網際網路（同單模式中“步驟 1”預定 UU200 的連接方式爲 Direct Access 時的設定）

- DHCP 連接網際網路（同單模式中“步驟 1”的設定，推薦選用連接方式爲 UUSwitch 或 UUExchange 時起用這種方式）

- PPPoE 連接網際網路（同單模式中“步驟 1”的設定，推薦選用連接方式爲 UUSwitch 或 UUExchange 時起用這種方式，需要設定使用者名及密碼）

- Static/Port forwarding（當從防火牆上 port forwarding 到該台 UU200 時使用），需要輸入本台 UU200 的私有 IP 位址、對應的子網掩碼、閘道及 DNS 等參數。此外還要輸入 DNAT IP，即配置 NAT 的源位元元址。請參考下例。

此類型只有在“Direct Access”方式下出現。

輸入完畢後按<保存>鍵進行儲存。

例如：

UU200 在局域網路內。防火牆的 PUBLIC IP：61.***.**.1。防火牆裏的埠映射設定爲：61.***.**.2（另一可用 PUBLIC IP）⇔192.168.1.1（UU200 內網地址）。則 DNAT IP 應設定爲 61.***.**.2。

4. 點選“步驟 4”進行代理服务器的設定（如圖 20），系統預設無代理服务器；
5. 完成以上操作後按<生效>，使當前的網路設定生效。

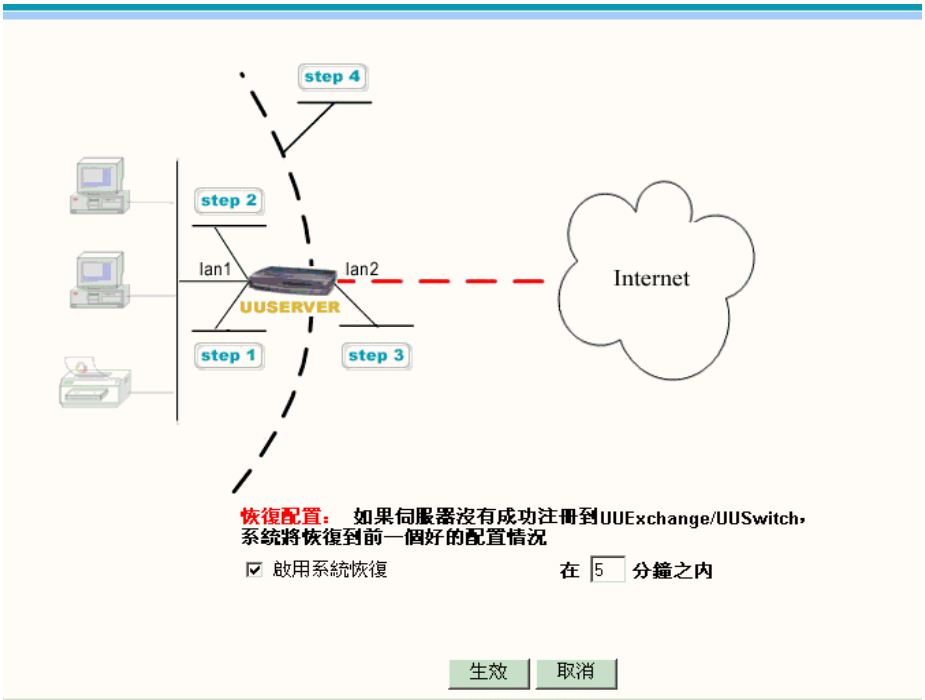


圖 17

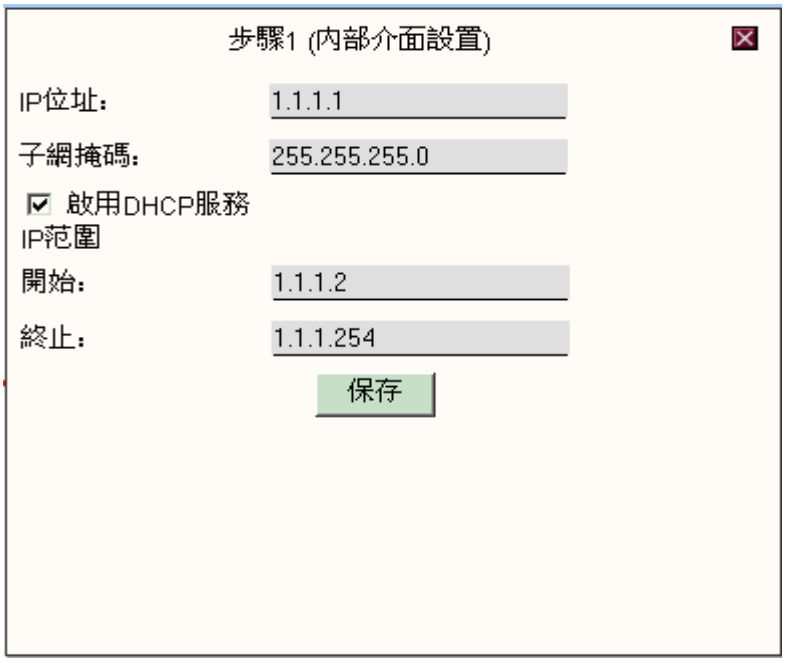


圖 18

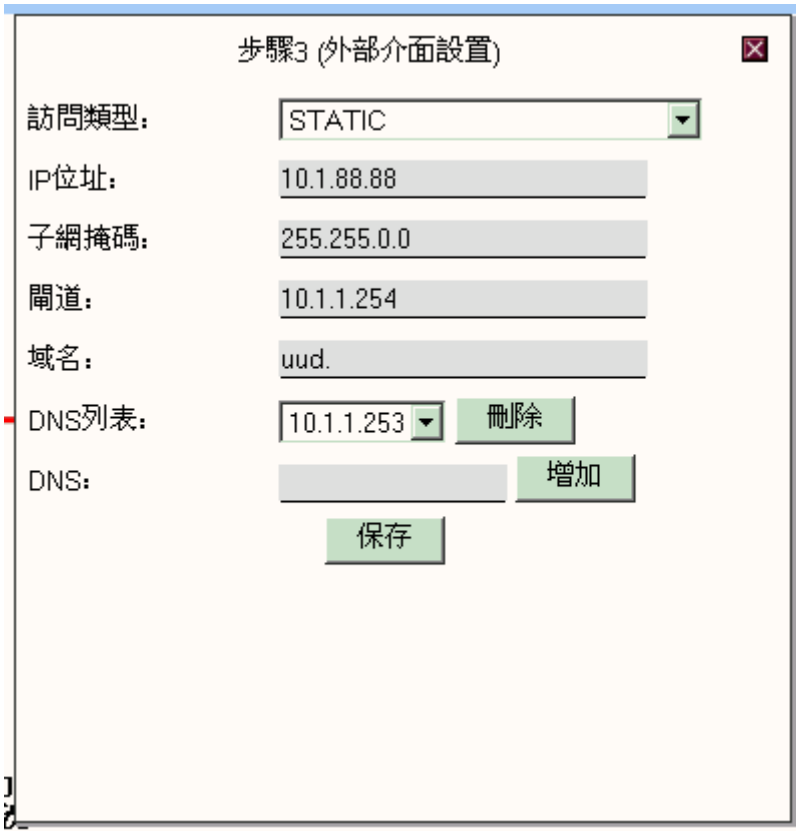


圖 19

圖 20

網路基礎設定完成後，系統會如圖 21 顯示一個提示您重新登錄的介面，按<確定>鍵返回如圖 4 的介面，重新登錄後就會進入如圖 22 所示的系統主介面。

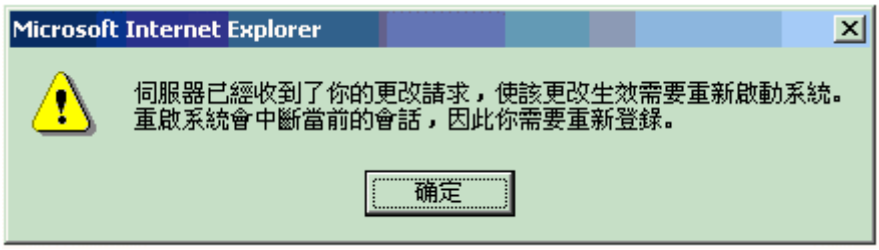


圖 21

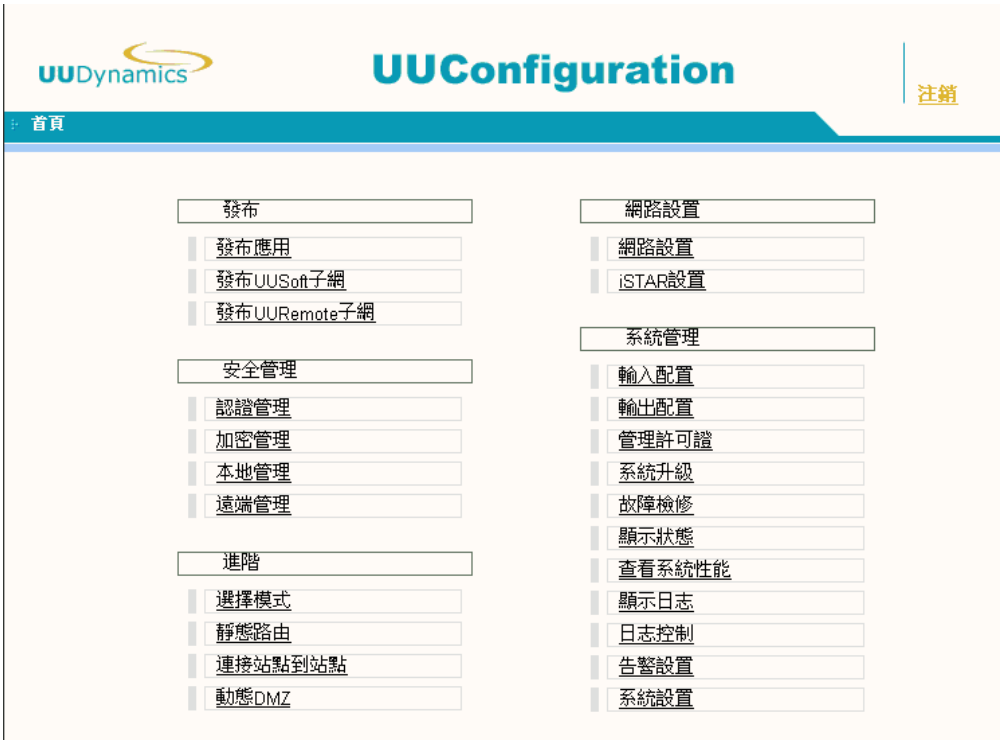


圖 22

步驟 6. 設定認證類型

如圖 22，點選“安全管理”下的認證控制，設定認證類型。

UU200 提供了多種認證方式，根據制定的認證策略不同，設置也會有很大的不同，請在設定前詳細參閱“3.3.1 認證控制”章節。

步驟 7. 設定系統時間

在圖 22 的系統主介面中，點選“安全管理”下的系統設置，進入圖 23 所示的設定系統時間介面，將系統時間設定爲當前時間。

注意：

不正確的系統時間會導致數位憑證不能使用、日誌時間錯誤等等的後果。

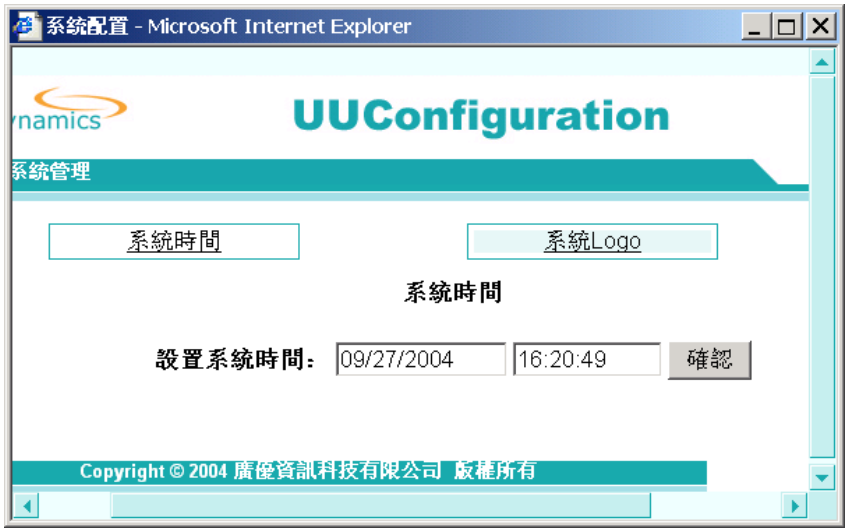


圖 23

步驟 8. 設定本地管理（/遠端）系統管理員

您可以通過本地或遠端方式，對 UU200 進行管理。

在“本地管理”視窗中被加入的使用者能且僅能從本機登錄 UU200 系統管理介面。反之，在“遠端管理”視窗中被加入的使用者能且僅能從遠端登錄 UU200 系統管理介面。

- 設定本地系統管理員：

1. 在圖 22 的系統主介面中，點選“安全管理”下的本地管理，進入如圖 24 所示的本地系統管理員介面。
2. 勾選“顯示使用者”，可以顯示所有的使用者（組群）資訊。
3. 在“使用者列表”視窗中選擇某個使用者（組群），然後按<增加>鍵將其加入“使用者”視窗中的本地系統管理員列表中。

   同樣也可以選擇“使用者”視窗中的使用者（組群），然後按<移除>，將其從本地系統管理員列表中移除。
4. 按<生效>使配置生效。

圖 24

- 設定遠端系統管理員

1. 在圖 22 的系統主介面中，點選“安全管理”下的遠端管理，進入如圖 25 所示的遠端系統管理員介面。
2. 勾選“顯示使用者”，可以顯示所有的使用者（組群）資訊。

   如果在設定認證類型時，選擇的認證類型爲“Windows AD/LDAP”，同時“使用者名稱”中輸入的使用者名屬於該域的“Domain Admins”組，則圖 25 中的“使用者列表” 列表將顯示該域中所有的使用者，如果“使用者名稱”中輸入的使用者名不屬於該域的“Domain Admins”組，則圖 25 中的“使用者列表” 列表只能顯示該域中的部分使用者。
3. 在“使用者列表”的視窗中選擇某個使用者（組群），然後按<增加>鍵將其加入“使用者”視窗中的遠端系統管理員列表中。

   同樣也可以選擇“使用者”視窗中的使用者（組群），然後按<移除>，將其從遠端系統管理員列表中移除。
4. 按<生效>使配置生效。

🕮 說明：

“唯讀”表示該本地/遠端使用者登入系統後只能看系統裏的資訊，不能更改系統裏的任何設定。

“更改”表示該本地/遠端使用者登入系統後可以更改系統裏的任何設定。

“拒絕”表示拒絕該本地/遠端使用者登入系統。

圖 25

2.4 系統復原

2.4.1 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并備份系統配置資訊，在系統無法工作，并且按 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！

2.4.2 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，重新打開 UU200 設備的電源，在系統啓動過程中會看顯示提示資訊：“*Start System Recover? Yes(Y), No(N) or Continue(C)*”。選擇“Y”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. 在配置電腦上打開瀏覽器，輸入 URL: *http://1.1.1.1/admin*, 得到如圖 22 所示的介面。

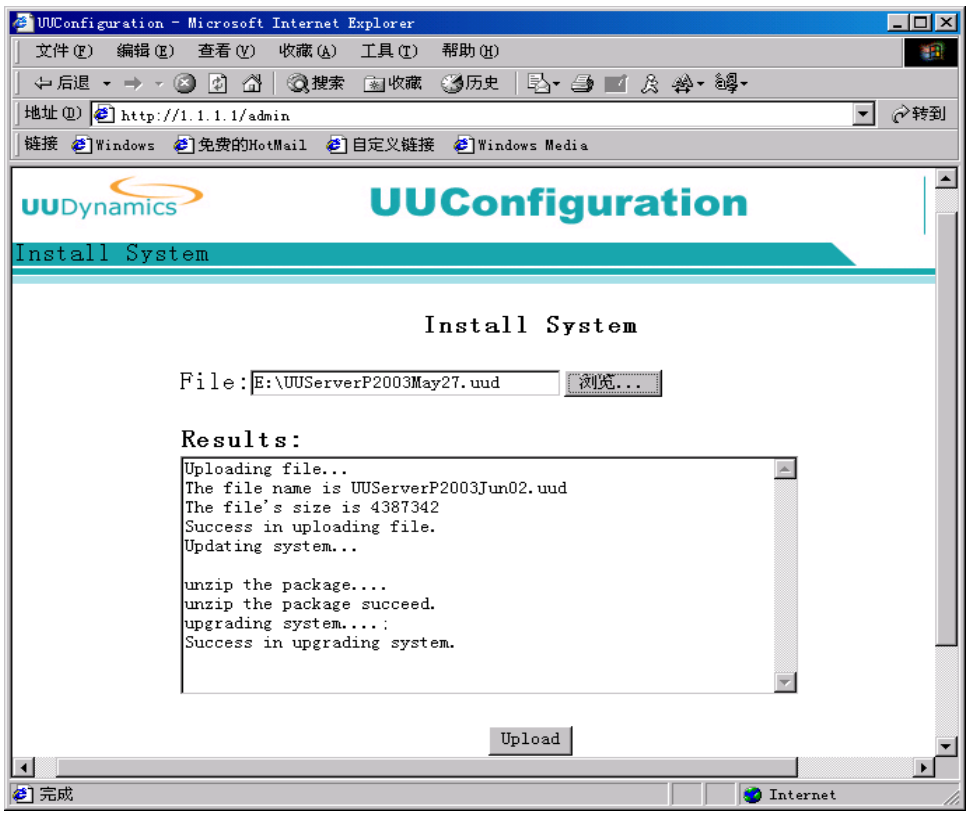


圖 26

5. 按<瀏覽……>，選擇 UUDynamics 套裝軟體，然後按<Upload>，系統會進行安裝。
6. 安裝完成後，請關閉 UU200 電源，數秒後重新開啓。
7. 當面板上的 LCD 显示“Unregester”後，在瀏覽器中重新輸入：http://1.1.1.1/admin。出現如圖 4 所示的介面，接下去的操作同本手冊第“2.3 安裝 UU200 軟體”部分。

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

配置介面採用 WEB 方式，進入配置介面前需要登錄。設定成不同網絡模式的 UU200，其登錄方式各不相同：

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（即 Lan 1，請參考圖 17）中的 IP 地址*]/admin”。

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通過 rm 方式打開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”（Switch 模式）或“https://[*uu200 的 IP 位址*]/rm”(Direct 模式)

輸入正確的使用者名和密碼(admin/admin)後，將會出現如圖 22 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 27 提示資訊，要求使用者重新登錄。

圖 27

重要：

爲了保障系統及內部資料安全，首次進入設定介面後，請務必修改 Admin 的密碼。

- 在系統主介面中，點選“安全管理”下的認證控制。選中某一使用者，點選<編輯>，即可在打開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 方式打開遠端使用者應用列表介面，在打開的介面中雙擊“更改密碼”圖示，即可在打開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“2.3 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“4.1 發佈應用程式”。

發布 UUSoft 子網：設定相應的使用者或使用者組可以通過 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：模式選擇，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“4.4 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 地址、子網掩碼、閘道、代理服务器、Internet 的接入方式等）。

iSTAR 設置 ：改變當前的連接方式。

【安全管理】

輸入設置：將原來保存好的配置檔導入到系統中。

輸出設置：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。

告警控制：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，請點選<返回>或<取消>。
- 保存配置的修改，請點選<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 22 所示設定介面，點選註銷退出。否則，再次（或用同樣的使用者名稱從其他機器）登錄時，系統將提示以下資訊 ：

“使用者 [username] *目前已登錄本系統”*

此時，相同使用者或者管理權限更高的使用者可以勾選“*停止使用者 [username]*” ，重新登錄系統。

🕮 說明：

如果勾選“*停止使用者 [username]*”時出錯（如圖 28），有可能是因爲您沒有許可權使該使用者失效。如果仍要登錄，請聯繫系統管理員。

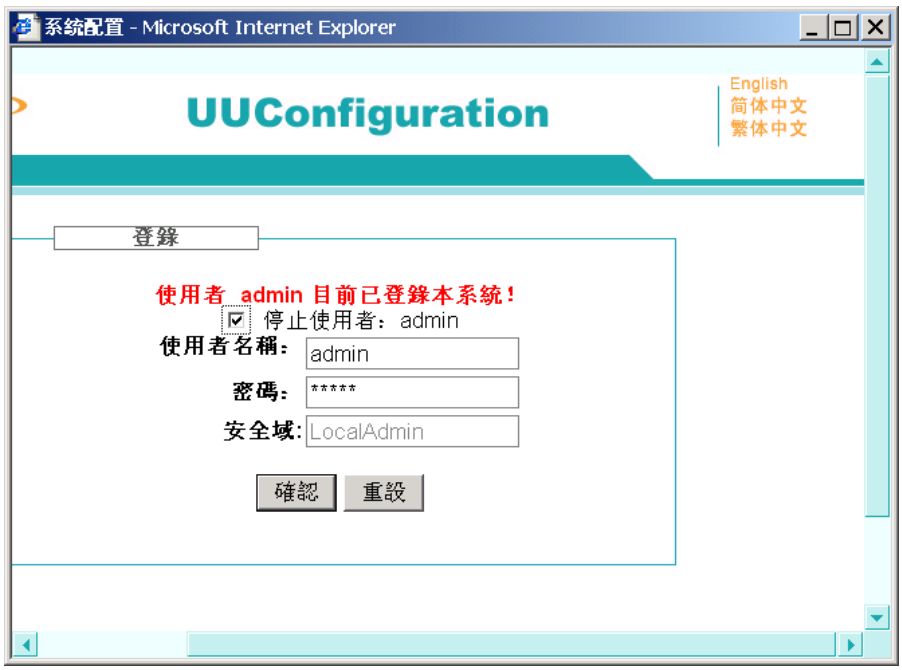


圖 28

3.1.4 使設定生效

“生效”表示使你的設定生效。

修改設定後，點選<確認>或<保存>鍵後進行保存。保存成功後，還必須點選<生效>，設定方可生效（如圖 29）。

重要：

- 以下七項設定完成後，點選<生效>會中斷 Session，同時系統會提示使用者重新登錄。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；

  選擇模式；管理許可證；升版系統；日誌控制；

- 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。

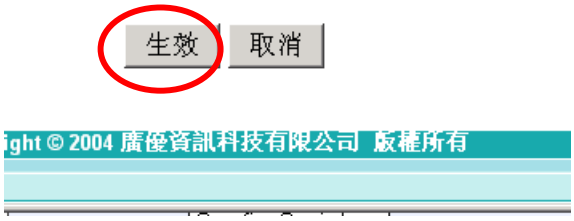


圖 29

3.2 網路設定

3.2.1 改變網路環境

如圖 22，點選“網路設置”下的 網路設置，可以進入圖 10 的介面更改網路設定，其設定方法詳見手冊“2.3 安裝 UU200 軟體”章節中的步驟 5：進行網路基礎設定。

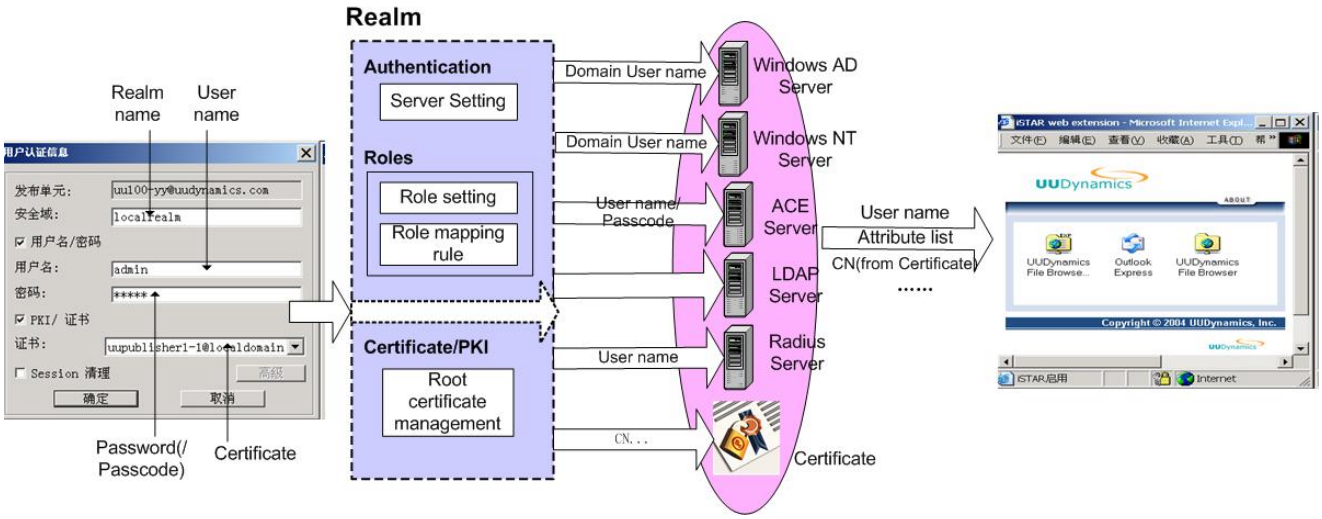
3.2.2 改變連接模式

在圖 22 所示介面中，點選“網路設置”下的 iSTAR 設置，進入圖 6 所示介面，其設定方法詳見手冊“2.3 安裝 UU200 軟體”章節中的步驟 3：設定連接方式。

3.3 安全管理

3.3.1 認證控制

相關概念：



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。認證伺服器用於驗證使用者端傳來的使用者名稱、證書等代表身份的資訊。身份驗證有以下幾種途徑：
  1. Client 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. Client 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映射而來）。
- 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。
- 安全域：每一個使用者隸屬於一個或多個安全域。安全域涵蓋了上文提及的一個或多個方面，包括認證、授權、規定、Certificate/PKI、角色。
  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。

例一：

- 背景

某企業爲大型銀行。使用者類型包括：局域網路路使用者、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，並點選<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		點選<增加/編輯映射規則…>，可以增加/編輯角色的映射規則。

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 LocalAdmin。使用使用者名稱/密碼在 Local 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：局域網路路使用者、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。

   LocalUsers：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，並點選<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 LocalAdmin。使用使用者名稱/密碼在 Local 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。

步驟：

1. 在系統主介面中（如圖 22）的“安全管理” 下，點選認證控制。

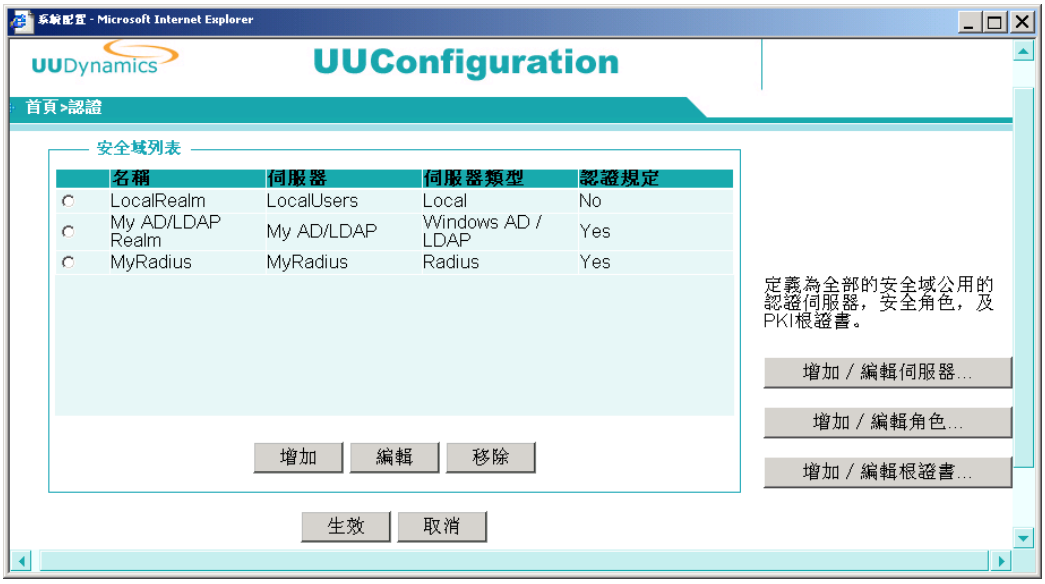


圖 30

2. 在圖 30 所示介面上點選<增加>，可以增加新的安全域。

   選中列表中某個安全域，點選<編輯>，可以修改該安全域的屬性。

3. 如圖 31，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。

圖 31

4. 在“伺服器”欄指明需要在哪個伺服器上進行使用者身份驗證。

   如果需要增加列表中沒有的伺服器，請點選圖 30 中的<增加/編輯伺服器>，進入下圖 32 所示介面。

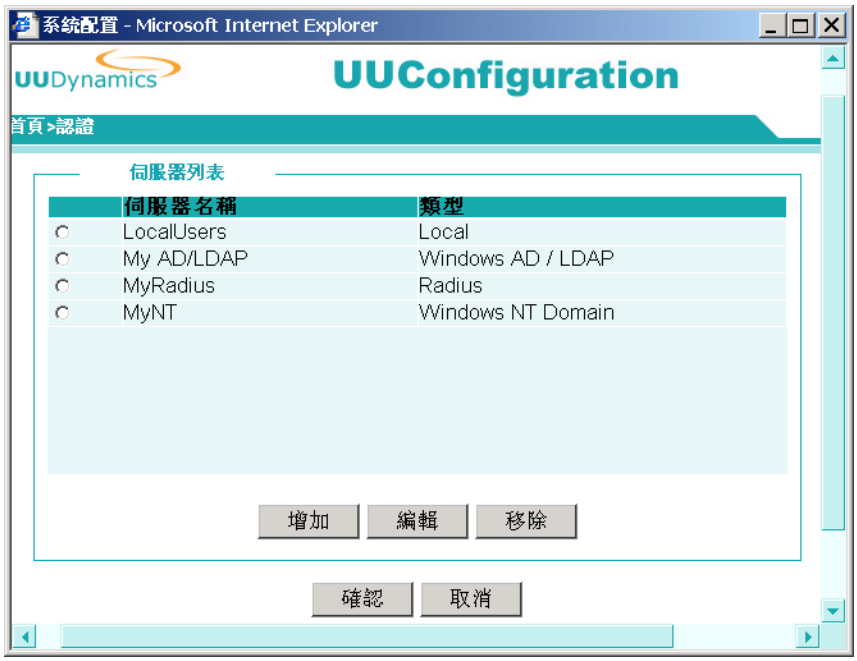


圖 32

5. 點選<增加>，進入圖 33 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。

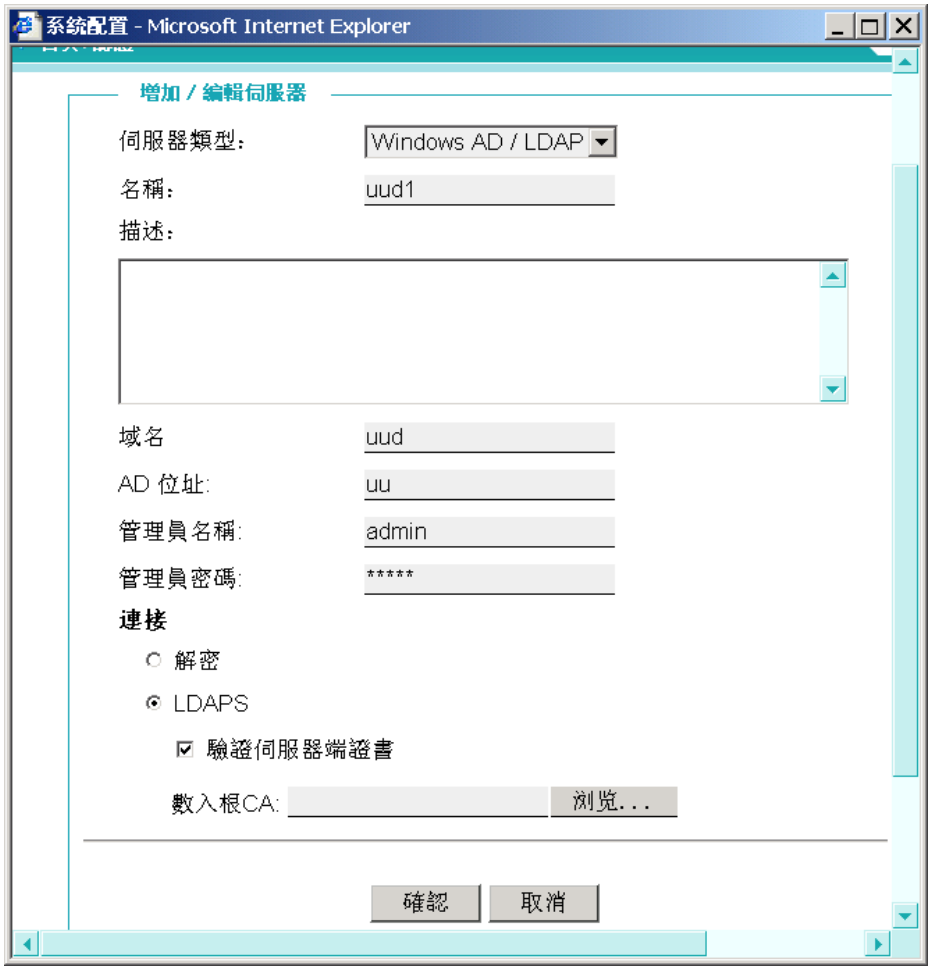


圖 33

伺服器 Type	輸入項		說明
Window AD/LDAP（Window AD/NTLM）	名稱		輸入伺服器名稱
	描述		輸入對該伺服器的描述（可選）
	功能變數名稱		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（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）
	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	解密	連接過程不加密

	（僅 Window AD/LDAP 類型）	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
Local	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
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。

🕮 **說明：**

- **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， “Windows AD Name”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“3.3.3 設定本地（/遠端）”）。

a) Windows AD/LDAP 方式下，在對應的 Windows AD Domain 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。

- **Local 伺服器**

Local 是缺省的伺服器類型。如果選擇 Local 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。該伺服器中有缺省的使用者名稱/密碼：admin/admin。缺省的使用者 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。

當選擇該認證類型時，每台 UU200 可管理 1000 個使用者帳號或組。

6. 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）。

   點選<管理證書>，可以選擇已有的證書。如果要增加新的證書，請在圖 30 所示介面中點選<增加/編輯根證書>。在介面中點選<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”欄用于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-子網掩碼等使用者屬性。

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。

7. 如果認證伺服器指定的是 Radius 類型的伺服器或 PKI 方式，則還需要爲角色設定相應的規則。否則，點選<確認>保存設定。

   在圖 31 所示介面中點選<增加/編輯映射規則…>，進入所示圖 34 介面。

   如果要增加/編輯角色，請在圖 30 中點選< 增加/編輯角色>。

圖 34

8. 點選圖 34 介面上的<增加>，進入圖 35 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 35 中的規則含義爲：Radius 伺服器中所有属性 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。

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-子網掩碼等使用者屬性。

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。

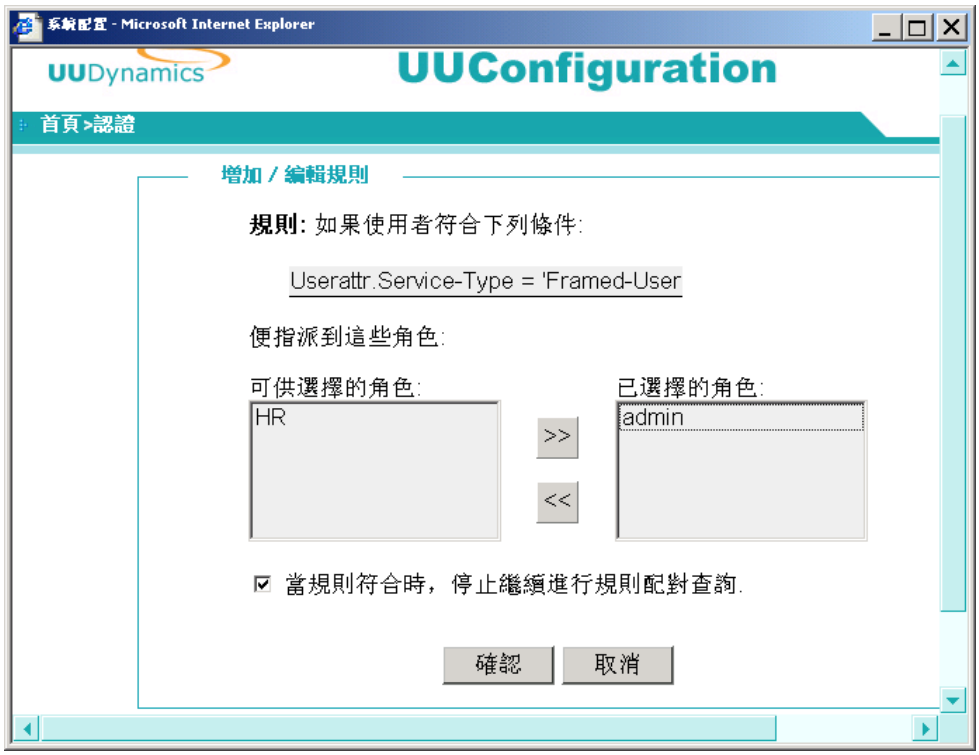


圖 35

3.3.2 設定加密演算法

在系統主介面中（圖 22）的“安全管理”下，按下加密管理， 會出現如圖 36 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。

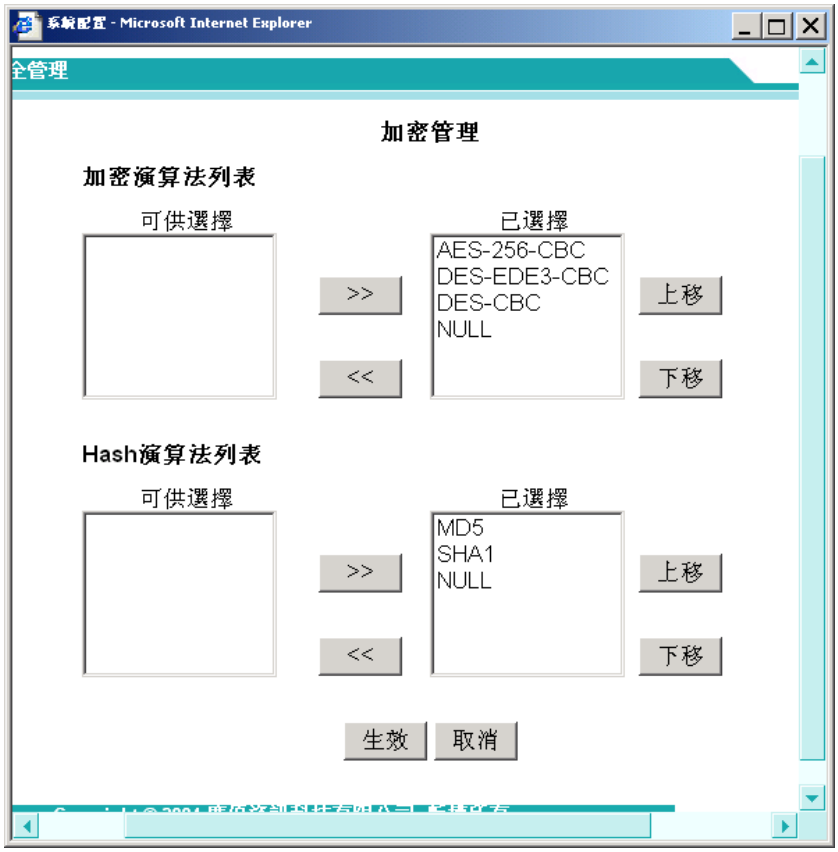


圖 36

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。

3.3.3 設定本地（/遠端）管理員

在系統主介面中（如圖 22）的“安全管理”之下，按下本地管理員會出現如圖 37 的視窗；用以增加或移除本地系統管理員。按下遠端管理員會出現如圖 38 的視窗；用以增加或移除遠端系統管理員。

以“遠端管理員”爲例：

> ⓘ 注意：
> 在“本地管理”視窗中被加入的使用者能且僅能從本機登錄 UU200 系統管理介面。

1. 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（設定本地管理員時，該步驟不需要）。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 39

所示的操作介面。

2. 設定該管理員對 UU200 的存取策略，系統預設的是“拒絕”，意即所有的管理員都不能存取。
3. 在“使用者列表”中指定排除在存取策略之外的方式。在其下的“使用者列表”列表中勾選使用者（/組/角色）方式，並按<增加>將其加入下方的“除了以下列出的”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（/組/角色）。

   通過這一步驟結合設定存取策略步驟相結合，管理員可以靈活的設定存取許可權，即：僅允許某一些管理員存取，或者允許除某一些管理員外的所有管理員存取。
4. 如果在圖 38 的視窗中的空白欄輸入要搜索的字串幷點選<搜索/開始>，介面上將返回模糊查詢後的結果。圖 38 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。）
5. “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。
6. 以上步驟完成後，保存設定結果，幷返回到圖 22 系統主介面中，點選本地管理，增加與遠端管理員相同的本地管理員帳號（設定本地管理員時，該步驟不需要）。

圖 37

圖 38

圖 39

🕮 說明：

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://<*uuswitch* 或 *uuexchange* 的 *DNS* 名稱/*IP* 位址>/<*UU200* 名稱>/rm”（Private Access 方式）或“https://<*UU200* 的 *IP* 位址>/rm”(Direct Access 方式)，該台電腦會顯示以下的視窗（圖 40）

圖 40

在圖 40 所示介面中輸入身份認證所需要素，點選<確定>之後，出現如圖 41 視窗，遠端系統管理員啓動 “Admin”圖示，便可以對 UU200 進行遠端管理。

🕮 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。
- 如果認證需要核實 Certificate/PKI，則需要勾選 “PKI/證書” ，並在 “證書” 欄選擇證書。
- 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，并輸入這個新的 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。

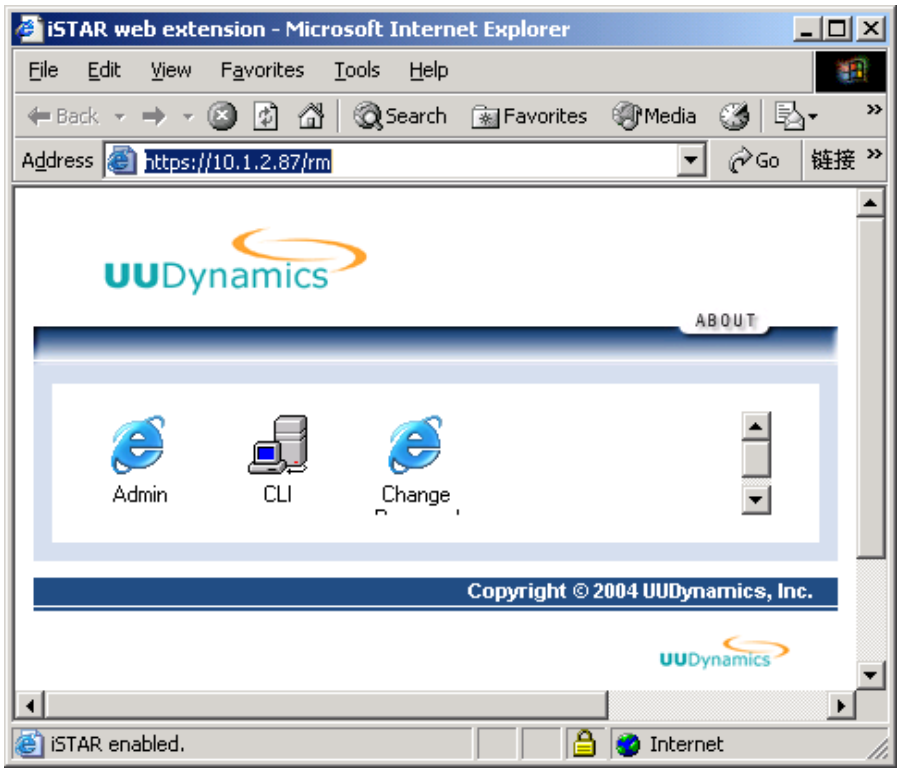


圖 41

在圖 40 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。點選<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” 功能表中的最近打開文檔的記錄列表	[*系統盤符*]:\Documents and Settings\[*username*]\Recent
最後登錄使用者	清除上一次登錄的使用者名稱	
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

3.4 系統安全管理

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。

3.4.1 輸入（/輸出）系統設定

在圖 22 的視窗中，選擇在“安全管理”之下的輸入配置，會顯示如圖 42 所示的視窗，將原來保存好的設定檔案輸入到系統中。

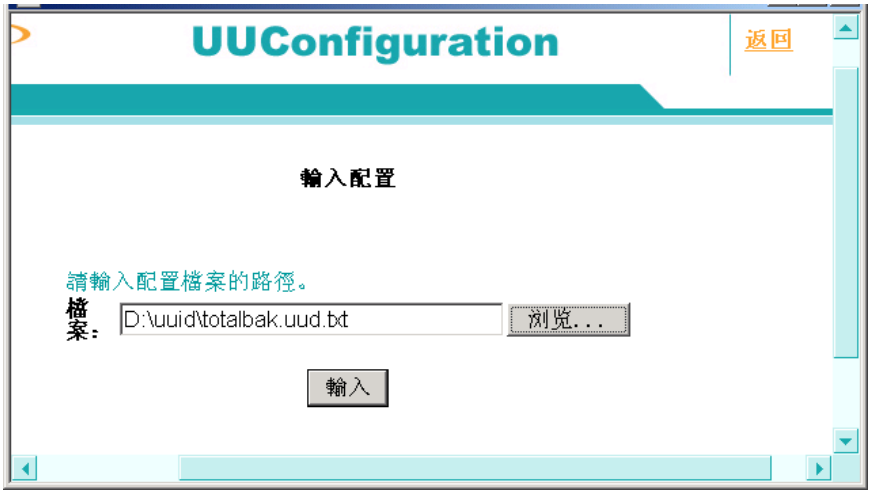


圖 42

按<瀏覽…>，選擇你原先輸出的系統設定檔案（參見本節“輸出配置”的內容），然後按下麵的<輸入>，系統會提示下列資訊（圖 43），

圖 43

按 <確認>鍵，配置輸入完成。

在圖 22 的視窗中，選擇在“安全管理”下的輸出配置，會顯示如圖 44 所示的視窗，可以將設定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。 您可以選擇輸出基本配置，輸出有關服務器資訊的設定，或是輸出整個系統設定。

圖 44

初次進入這個介面，會顯示如圖 45 所示的安裝 ActiveX 的提示介面。 您必須按<是>，才能繼續完成輸出設定檔案。 (這是一個資料下載的控制項，不會對你的系統造成影響)

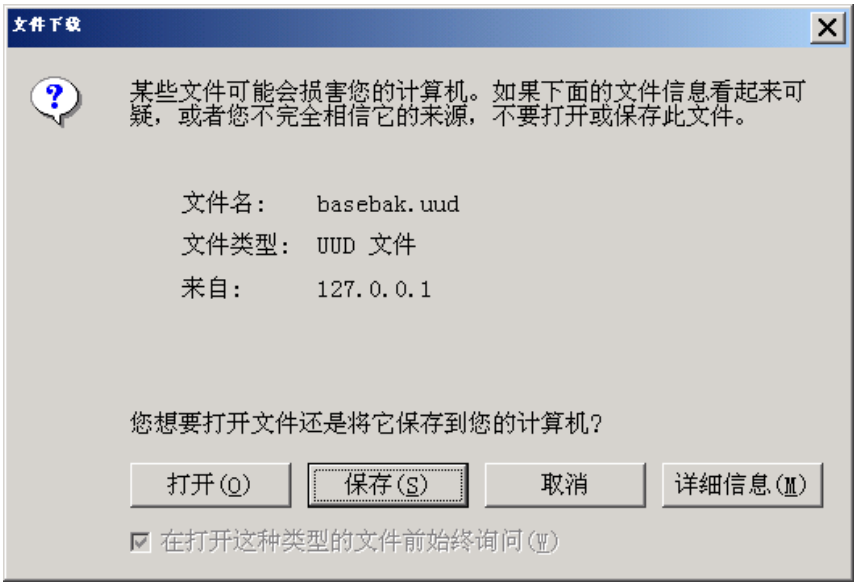


圖 45

3.4.2 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“安全管理”下的管理許可證，進入下圖所示介面（圖 46）

圖 46

2. 點選<上傳>，在圖 47 所示介面中點選<瀏覽>，選擇要替換的證書的完整路徑和檔案名，點選<確認>。

圖 47

3. 最後按<生效>，使設定生效。

3.4.3 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“安全管理”下的升版系統，進入圖 48 所示介面。

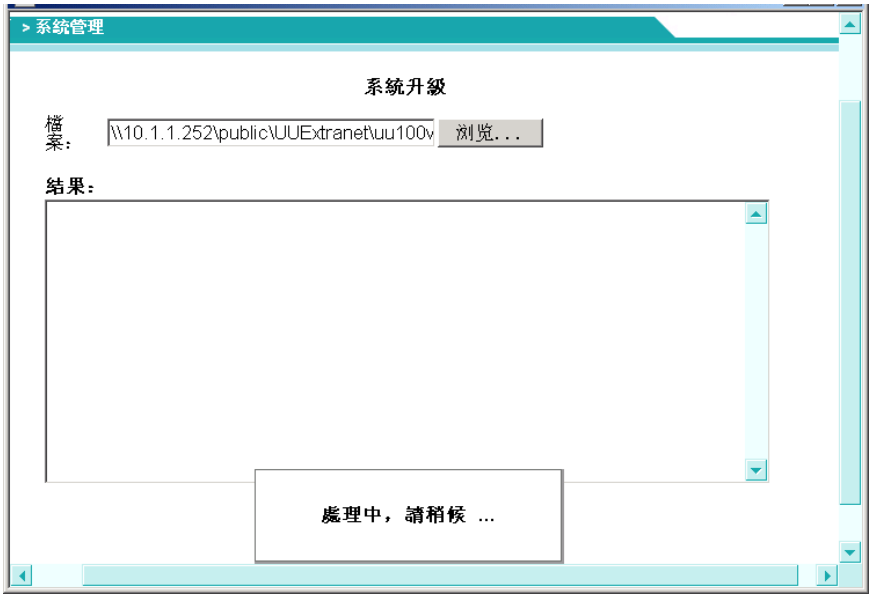


圖 48

2. 點選<瀏覽……>，選擇新版本的安裝程式的完整路徑和檔案名，點選<更新>，系統將自動進行版本升級，并在升級完成後，彈出提示框見圖 49 要求使用者重新登錄。

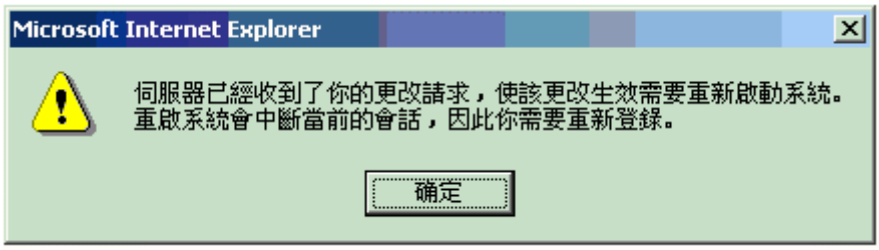


圖 49

重要：

在點選<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。

3.4.4 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 50)

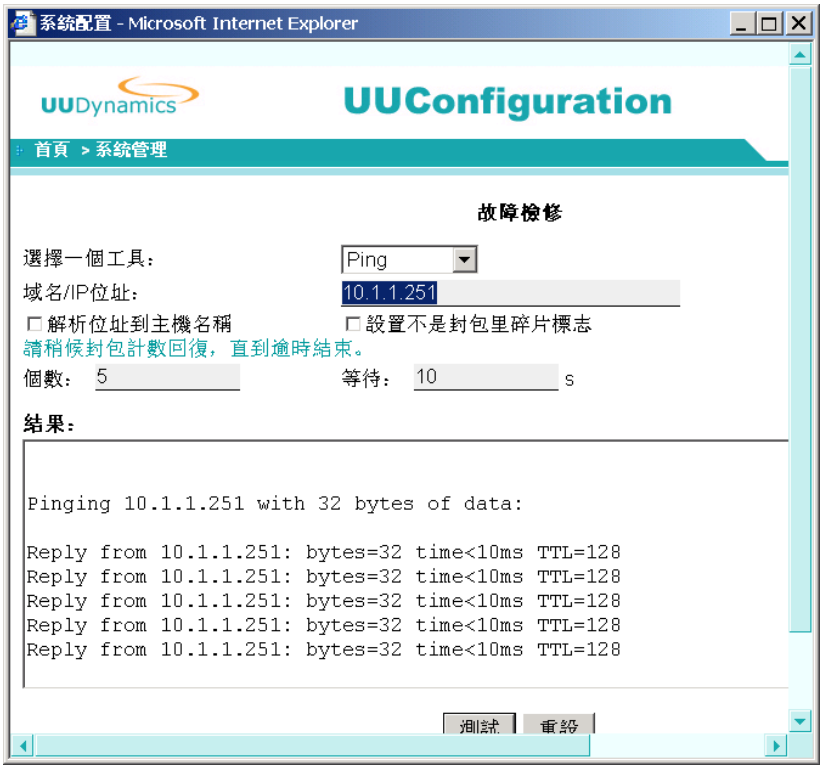


圖 50

3.4.5 顯示狀態

點選“安全管理”下的顯示狀態，可進入圖 51 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 51

3.4.6 查看系統性能

在圖 22 的視窗中，選擇在“安全管理”之下的查看系統性能，可以選擇不同的專案進行查看：

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

如圖 52 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 Licence 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。

點選<顯示>，靜態顯示選定時間段的統計資訊；

點選<現今>，動態顯示即時的統計資訊；

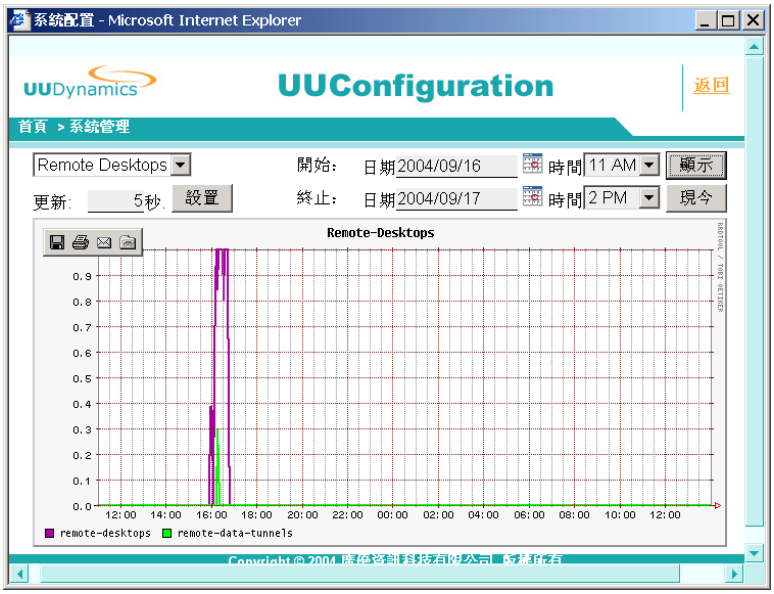


圖 52

3.4.7 日誌等級的設定

在圖 22 的視窗中，選擇在“安全管理”之下的日誌控制，會顯示如圖 53 所示的視窗，系統管理員可以進行系統日誌的設定。

圖 53

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（不作日志）
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。

3.4.8 查看日誌

在圖 22 的視窗中，選擇在“安全管理”之下的查看日誌，會顯示如圖 54 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“3.4.7 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。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。

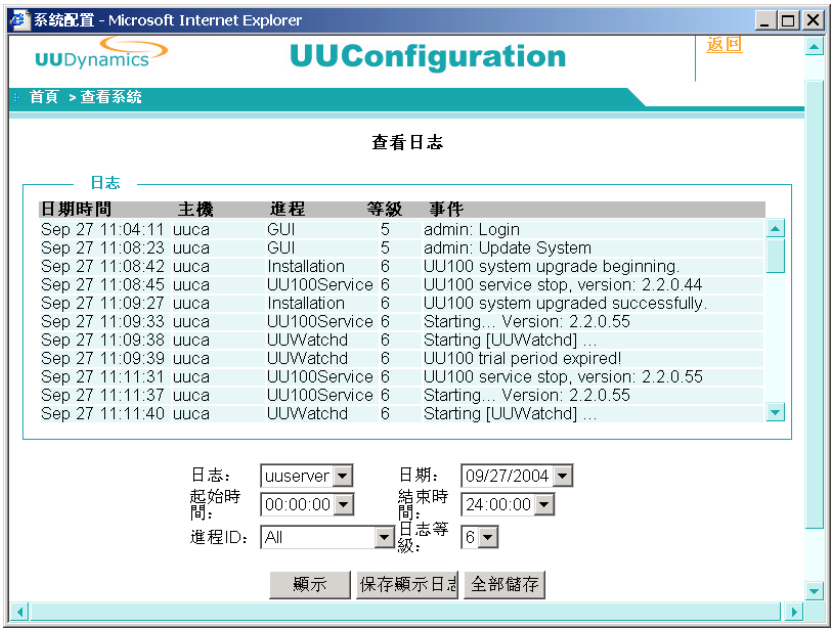


圖 54

3.4.9 告警等級的設定

在圖 22 的視窗中，選擇在“安全管理”之下的告警控制，會顯示如圖 55 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。

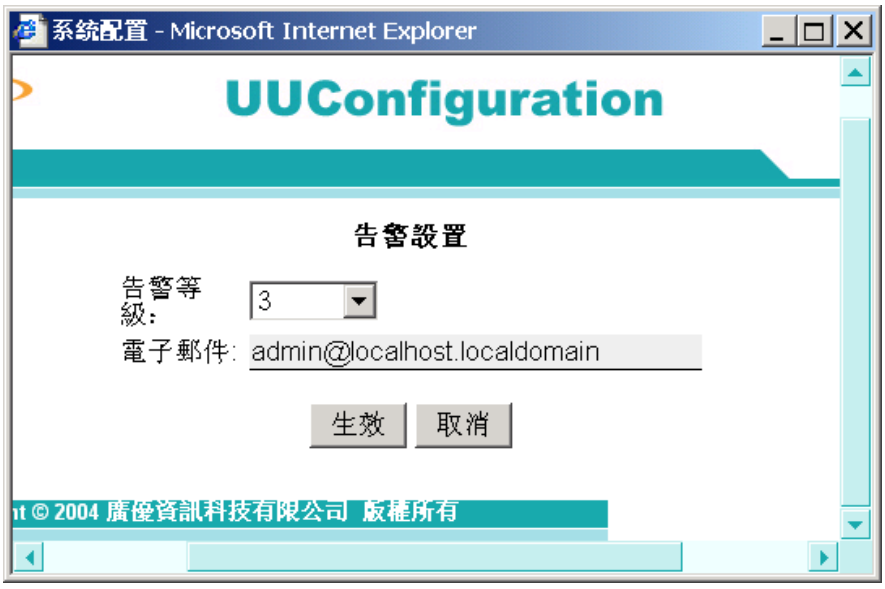


圖 55

3.4.10 系統時間及 LOGO 設定

在圖 22 的視窗中，選擇在“安全管理”之下的系統管理,您可以修改 UU200 的系統時間（圖 56），或是修改顯示在左上角的 LOGO 檔（圖 57），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。

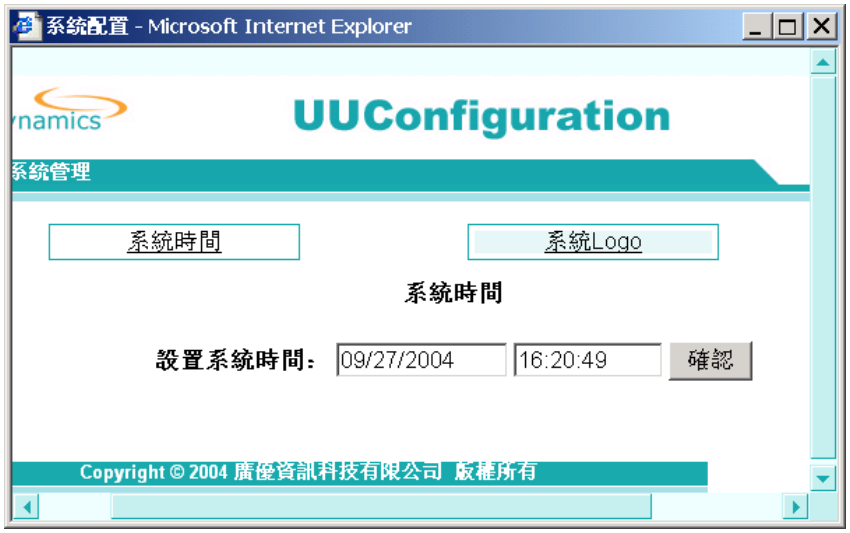


圖 56

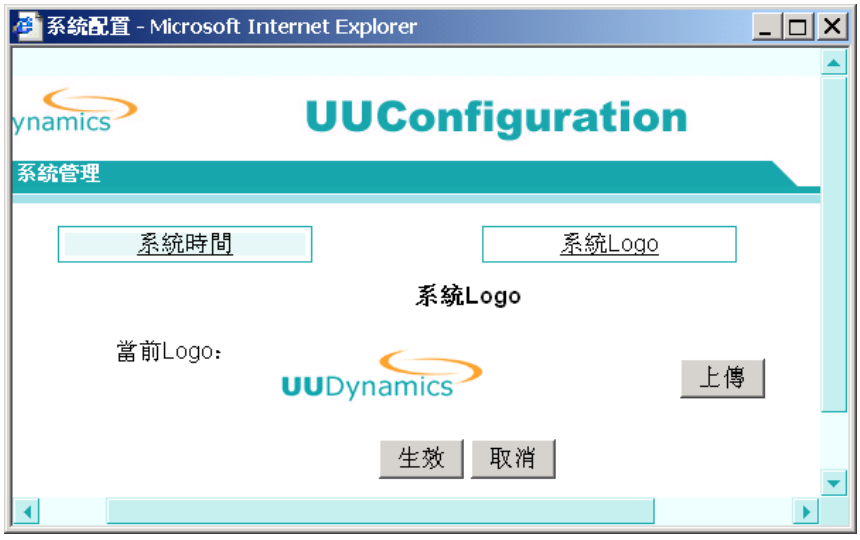


圖 57

3.5 進階

3.5.1 選擇網路模式

如圖 9 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“2.1 安裝 UU200 的準備”章節。

具體配置步驟請參考“2.3 安裝 UU200 軟體”章節中的步驟 3：設定連接方式。

3.5.2 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 22 的視窗中，選擇在“進階”之下的靜態路由,進入圖 58 所示介面。

圖 58

選中一條靜態路由記錄,點選<編輯>,可以修改該條記錄；點選<移除>,則可以刪除該條記錄；如果點選<增加>，則可以進入圖 59 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。

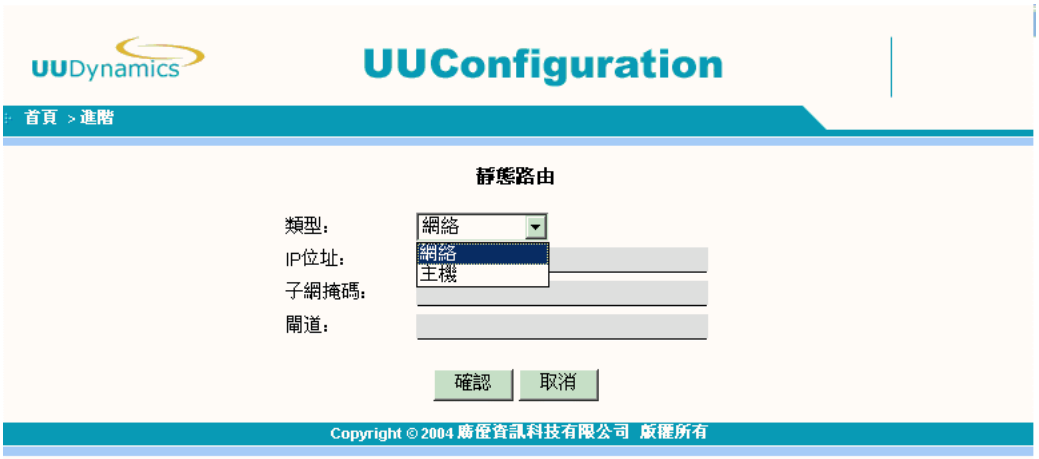


圖 59

3.5.3 連接兩個子網

詳見“4.3 連接兩個子網”。

3.5.4 設定動態非軍事動態區

詳見“4.4 配置動態非軍事區”。

第4章 應用設定

4.1 發佈應用程式

每個 UU200 能發佈不超過 100 個應用。每個應用允許設定總數不超過 100 個的接入規則，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 “6.1UUDynamics 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 “6.2 *i*STAR™ 支援的客戶/伺服器應用” 。

如圖 22 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 60）。

- **增加系統應用程式列表框內已有的應用程式：**

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 1）。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 60 所示介面 ，點選<增加>，進入圖 61 所示介面。

② 選擇列表框內的應用程式 ，點選<確認> ，進入圖 62 所示介面。

③ 點選<規定…>，進入圖 64 所示的視窗。輸入您爲這個策略所取的名稱；
目前 UU200 僅能提供驗證證書這一發佈策略，更多策略方案將陸續提供。

④ 輸入共用應用程式所在伺服器的 IP 位址等相關資訊，點選<使用者…>，根據需要增加使用者（/組/角色）。進入圖 65 所示的視窗；在 Look In Realms 下拉清單中選擇使用者（/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 66 所示的操作介面。

⑤ 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。

⑥ 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（/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（/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。

⑦ 點選<埠範圍>，進入圖 67 所示介面。設定開放的埠。

您也可以點選<增加>，進入圖 68 所示介面，增加新的埠。

埠設定完成後，點選<返回>返回圖 62 介面。

⑧ 點選<確認>，完成所有設定。

- **增加系統應用程式列表框內沒有的應用程式**：

您可以增加“Custom”類應用以定制自己的服務。目前 UU200 中提供兩種“Custom”應用：

Custom – Multi-station application：遠端使用者可以通過 UUSwitch/UUExchange 存取多台機器，這時，這些機器的埠號是統一的。

Custom – Roaming application：遠端使用者可以通過 UUSwitch/UUExchange 存取多台機器中的任一台。這時，必須指定這台被存取的機器埠號。

Custom – Network drive based C/S：該應用支援遠端 Client 端使用者存取 UU100 所在內部網的共用資源（Client 端運行的應用程式已將此共用資源映射爲指定的網路映射盤）。例如：現有一個 MIS 系統，已將 Database 的完整路徑映射到網路映射盤“N：”，幷且管理員在 UU100 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。

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

① 在圖 60 所示介面 ，點選<增加>，進入圖 61 所示介面。

② 選擇列表框內的 Custom– Multi-station application，點選<確認>，進入圖 63 所示介面。

③ 點選<規定…>，進入圖 64 所示的視窗。輸入您爲這個策略所取的名稱；

目前 UU200 僅能提供驗證證書這一發佈策略，更多策略方案將陸續提供。

④ 輸入共用應用程式所在伺服器的 IP 位址等相關資訊，點選<使用者…>，根據需要增加使用者（/組/角色）。進入圖 65 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 66 所示的操作介面。

⑤ 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。

⑥ 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（/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（/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。

⑦ 點選<電腦> ，進入如圖 68 所示介面。可以通過點選<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，點選<返回>返回圖 63 介面 。

⑧ 點選<埠範圍>，進入圖 67 所示介面。設定開放的埠。

您也可以點選<增加>，進入圖 69 所示介面，增加新的埠。

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

⑨ 輸入“起始埠”和“終止埠”後，點選<確認>完成埠設定。設定完成後，點選返回返回圖 63 介面。

⑩ 點選<確認>，返回上一介面，點選<生效>，完成所有設定。

圖 60

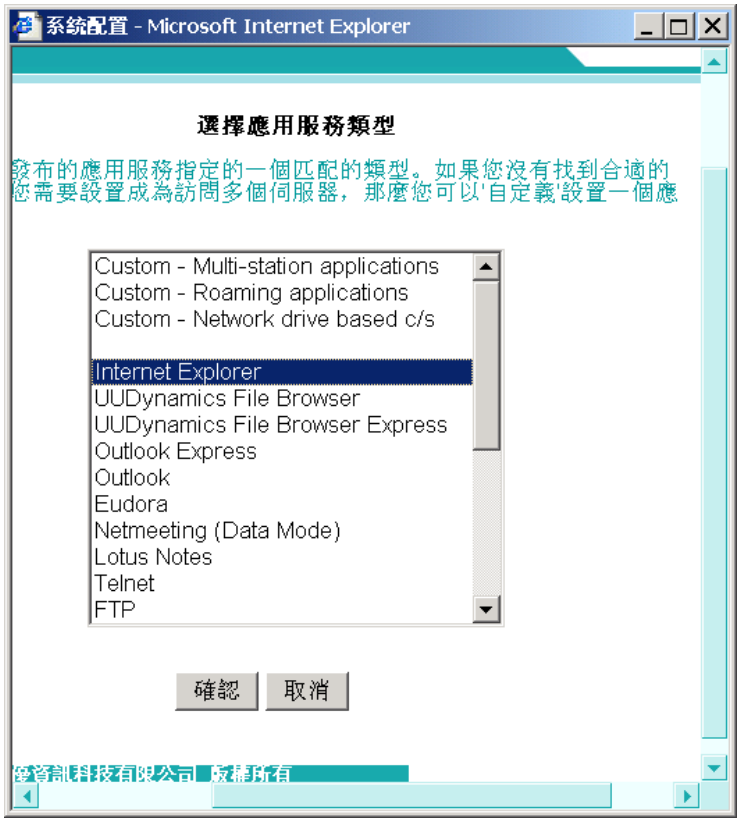


圖 61

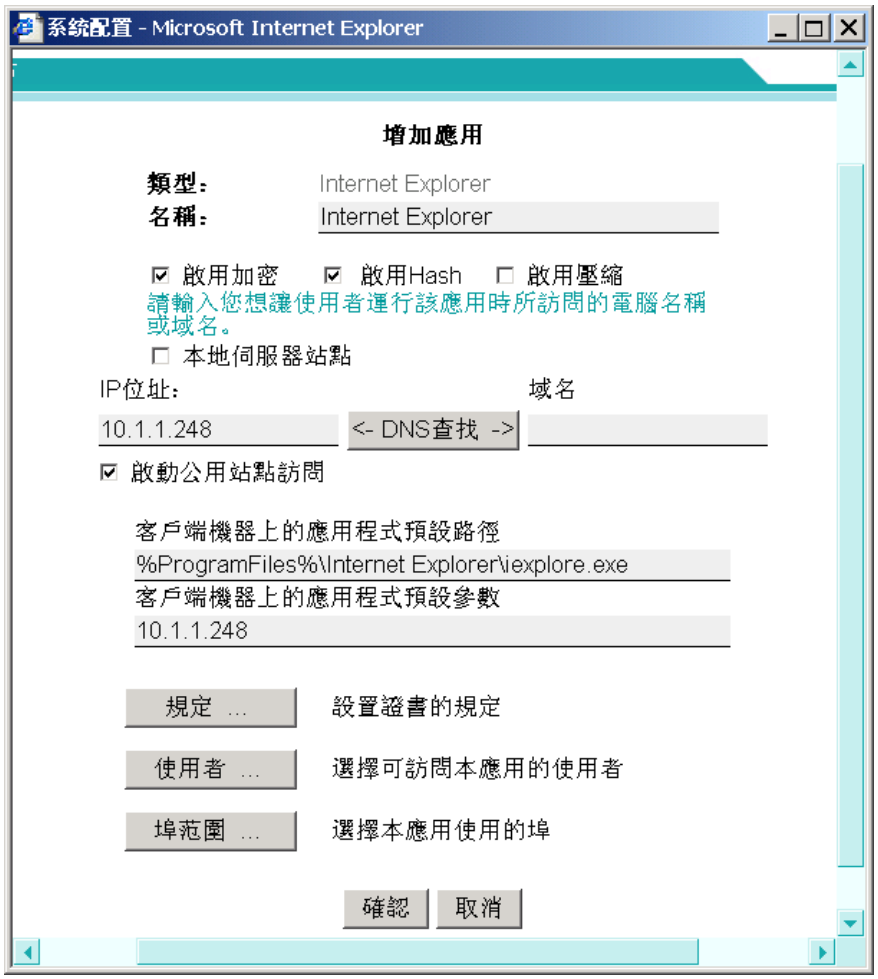


圖 62

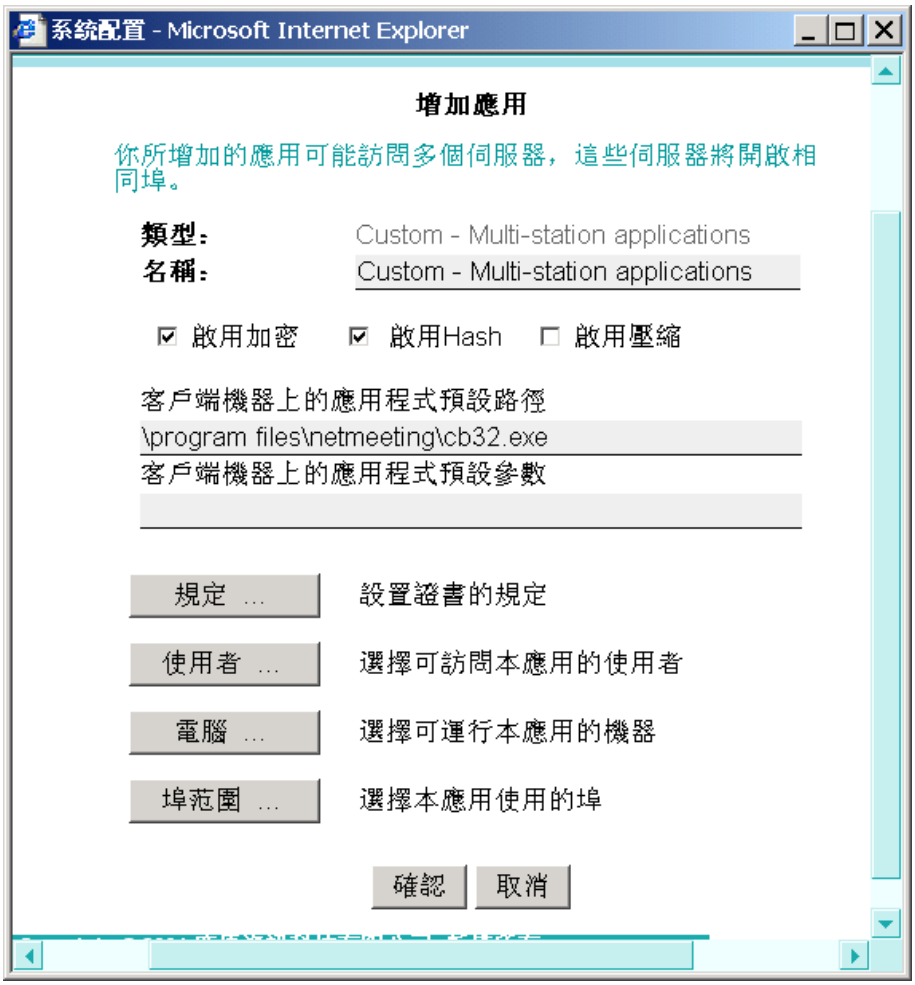


圖 63

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 64

圖 65

圖 66

參數/控鍵	含義
顯示使用者	表示將在“使用者列表”列表框內顯示所有的使用者
使用者列表內的使用者/組	點選<增加>鍵，所選的使用者/組將顯示在“已選定的使用者”內的列表框內，表示該使用者將有權存取共用的應用程式
全選	表示選上列表框內的所有使用者/組
撤銷選中	表示取消已選的使用者/組

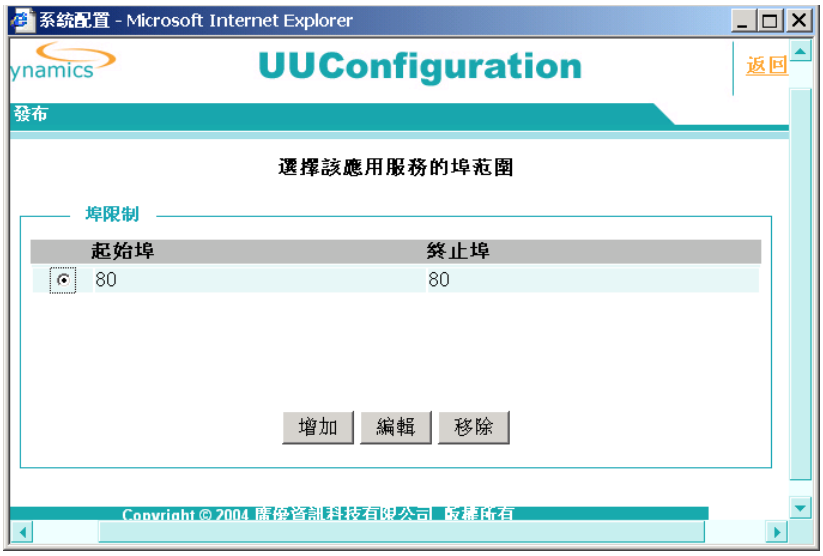


圖 67

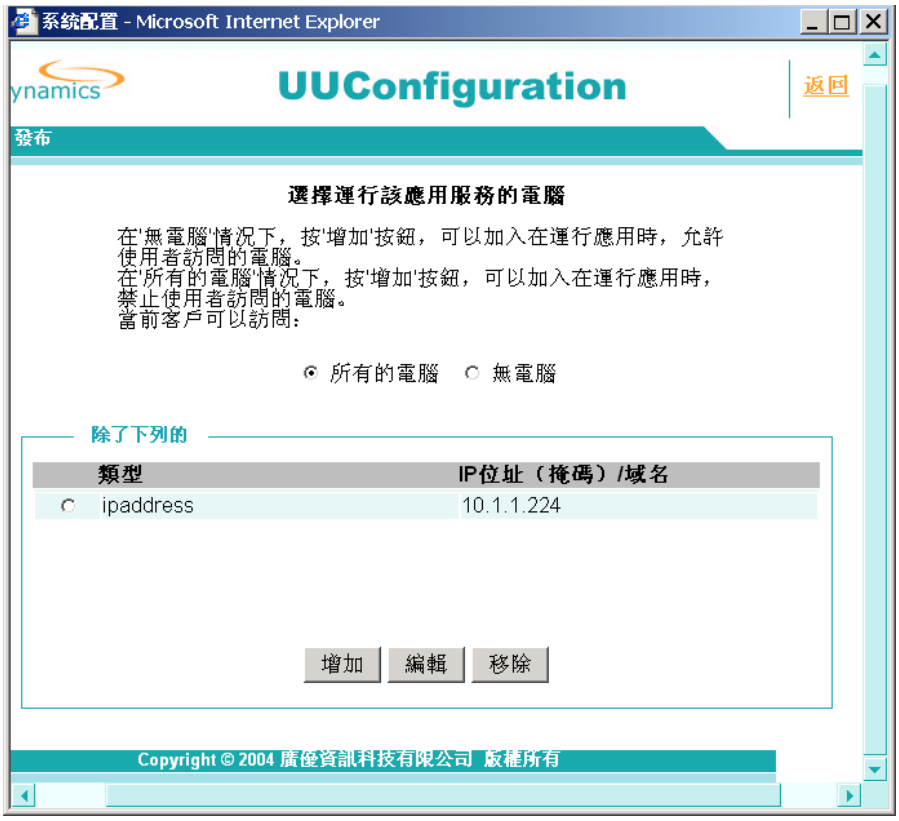


圖 68

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 62 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 70）。

– <所有電腦>：點選<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>：點選<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。

圖 69

圖 70

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	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 60，按下<增加>，進入圖 61 的視窗；
2. 選擇“Custom – Network drive based C/S”，按<確認>，進入圖 71 的視窗；

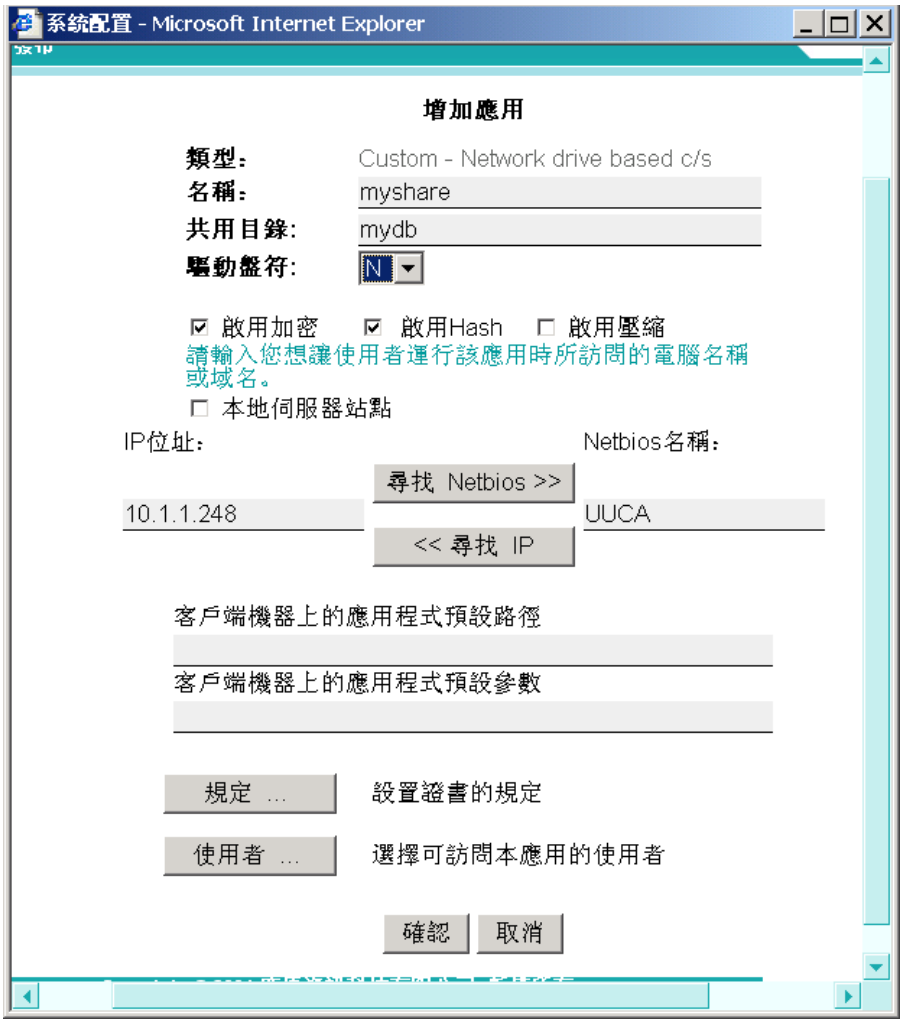


圖 71

3. 在“名稱”欄中，輸入您爲這個應用所取的名稱；
4. 在“共用目錄:”欄中，輸入您要作映射的 Folder 名稱，並請確保輸入正確；
5. 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)。
6. 勾選“啓用 Hash”會啓動系統設定的 Hash 演算法
7. 勾選“啓用壓縮”會啓動系統設定的壓縮演算法；
8. 如果該應用要映射的盤符在本機，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；如果該應用要映射的盤符不在本機，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。
9. 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；

10. 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。
11. 點選<規定…>，進入圖 64 所示的視窗。輸入您爲這個策略所取的名稱；

    目前 UU200 僅能提供驗證證書這一發佈策略，更多策略方案將陸續提供。

    1. 點選<使用者…>，根據需要增加使用者(/組/角色)。進入圖 65 所示的視窗；在 Look In Realms 下拉清單中選擇使用者（/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 66 所示的操作介面。
    2. 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。
    3. 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（/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（/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。
12. 按下<返回>返回圖 71 的視窗；
13. 按下<確認>完成對發佈 Network drive based C/S 的設定，並點選<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。

4.2 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，網路管理員還需要在發佈局域網路路內配置一個 DHCP 伺服器（UU200 採用單模式時），或由 UU200 充當 DHCP 伺服器（UU200 採用 Transparent 模式或 Route 模式時）。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

如果 UU200 的接入網路的方式爲**單模式**，則 UU200 不提供 DHCP 服務，必須利用發佈局域網路路內的 DHCP 伺服器或在該局域網路內安裝一個 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 72 所示：

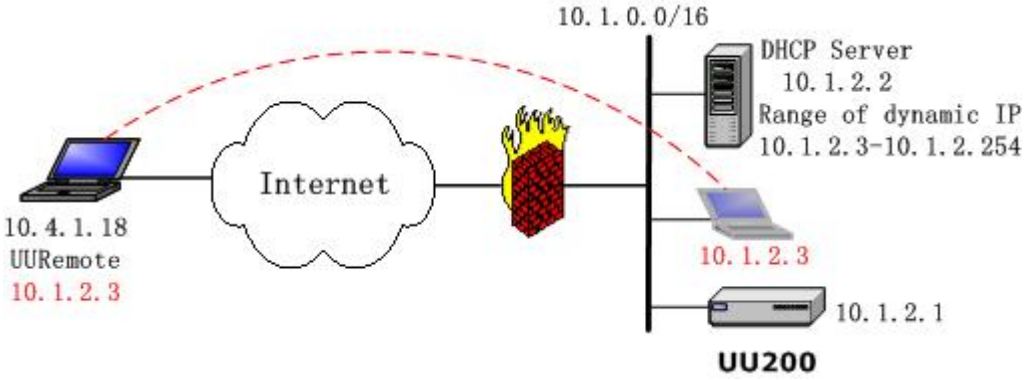


圖 72

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，亦可利用選擇利用局域網路內原有 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 73：

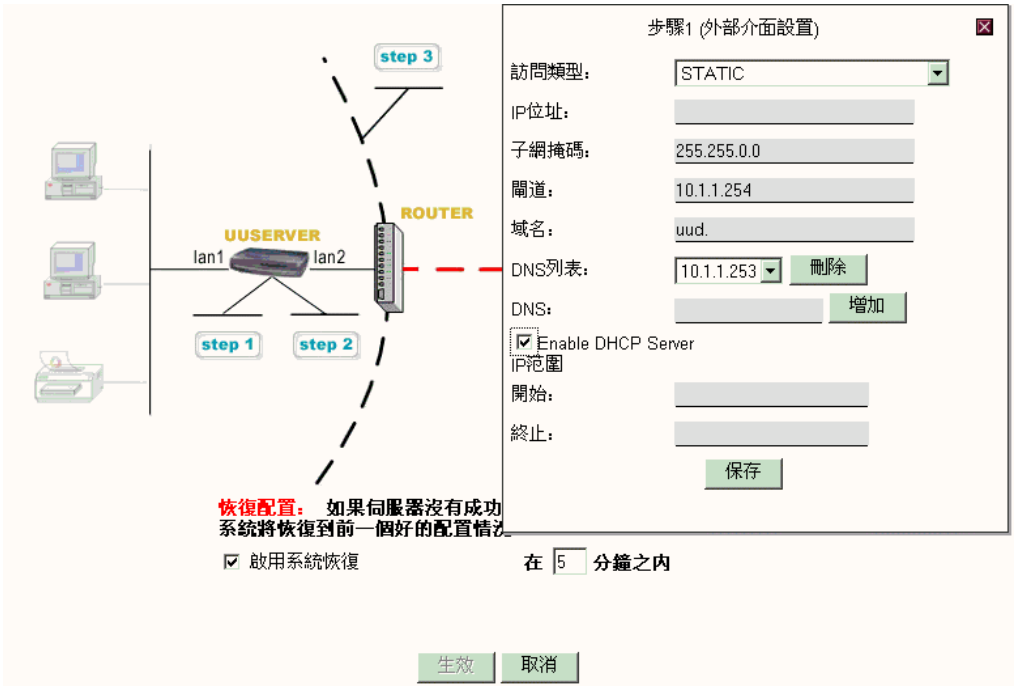


圖 73

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 74 所示。（這裏的連接方式與圖 72 所示不同，只要將 UU200 直接接入局域網路，通過該 UU200，遠端電腦可以虛擬接入該 UU200 所在局域網路）

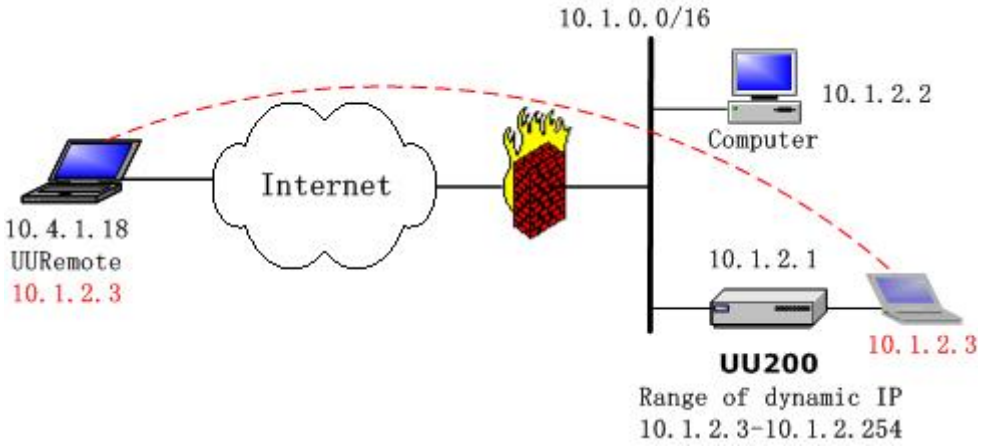


圖 74

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 75。

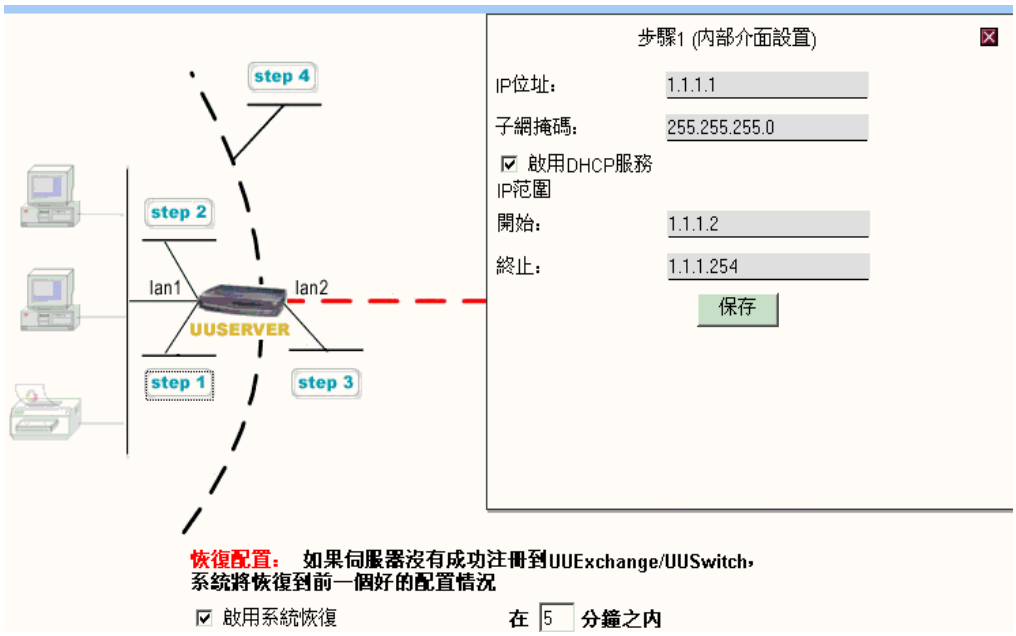


圖 75

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 76。

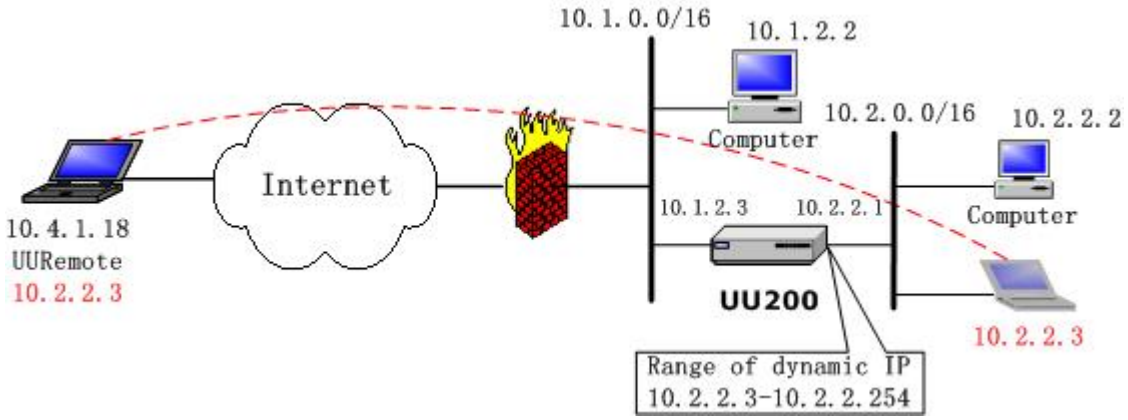


圖 76

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←→IP 的映射。

- 發布 UUSoft 子網

點選圖 22 主介面功能表上“發布”下的發佈 UUSoft 子網進入圖 77 介面。

— 設定可存取該 Subnets 的使用者：

— 設定可存取該 Subnets 的電腦組：

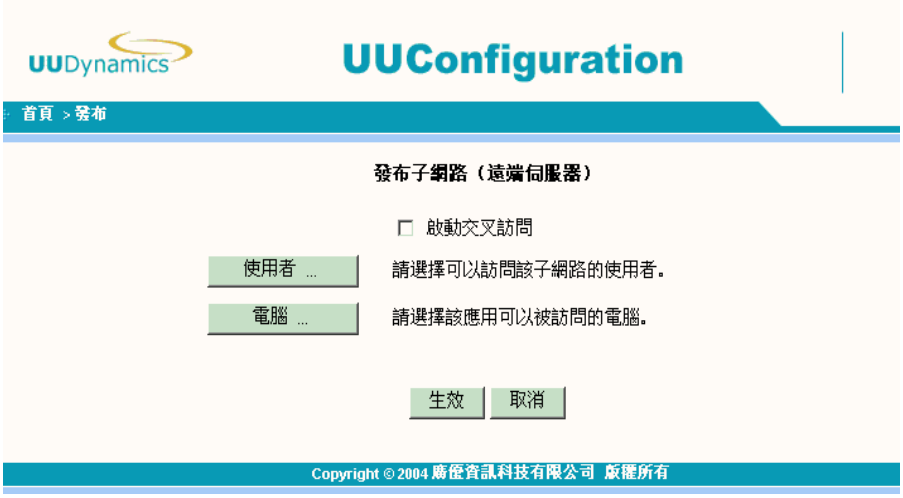


圖 77

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。

點選<使用者...>，根據需要增加使用者（/組/角色）。根據使用者所屬的安全域類型不同,會出現如圖

78~圖 81 所示的畫面。

在“Look in Realms”欄內選擇安全域。

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（/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（/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：

- 如果在圖 79 的視窗中的空白欄輸入要搜索的字串幷點選<搜索/開始>，介面上將返回模糊查詢後的結果。圖 79 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。）
- 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”介面如圖 39。

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錄系統管理介面。

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組，按中間的<增加>，就可以把選中的使用者或組增加到下面的視窗中，表示這些使用者和組可以使用該子網。

🕮 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 78

圖 79

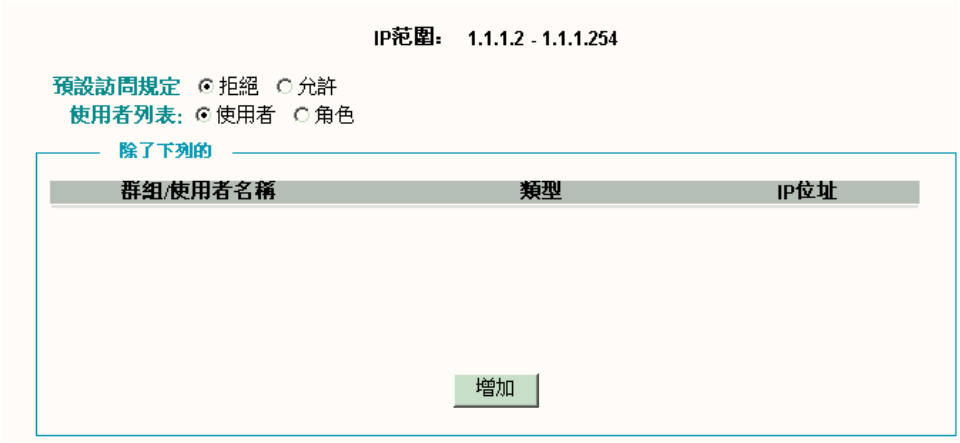


圖 80

圖 81

- 發佈 UURemote 子網

  點選圖 22 主介面功能表上“發布”下的發佈 UURemote 子網進入圖 82 介面。

  — 設定可存取該 Subnets 的使用者：

  — 設定可存取該 Subnets 的電腦組：

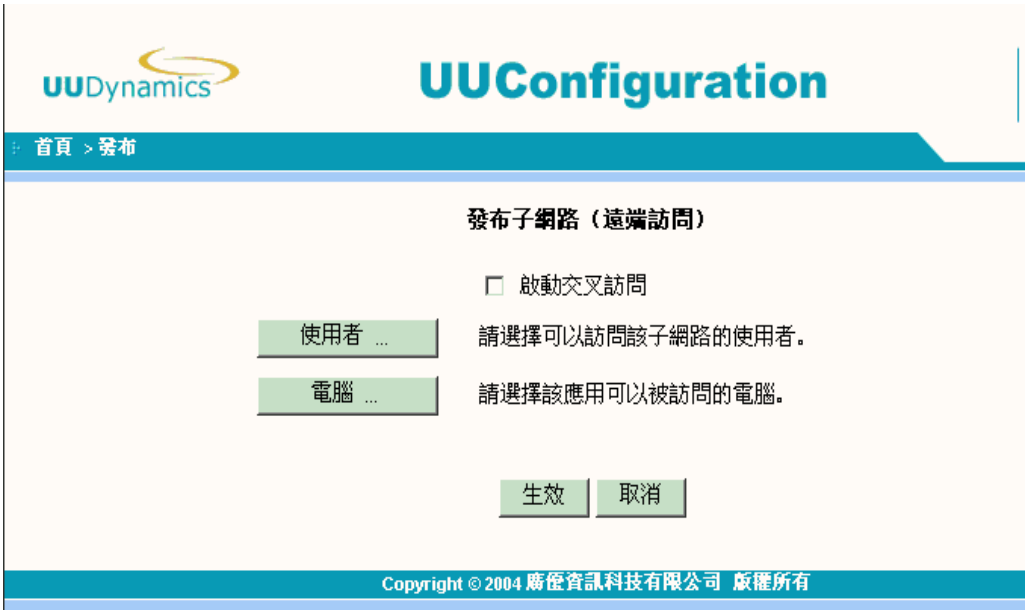


圖 82

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。

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，也要求建立 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 83 的介面。

圖 83

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 switch 或 exchange 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 83 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 84 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 83 介面，按生效生效。增加的遠端 uu200 會出現在介面中。

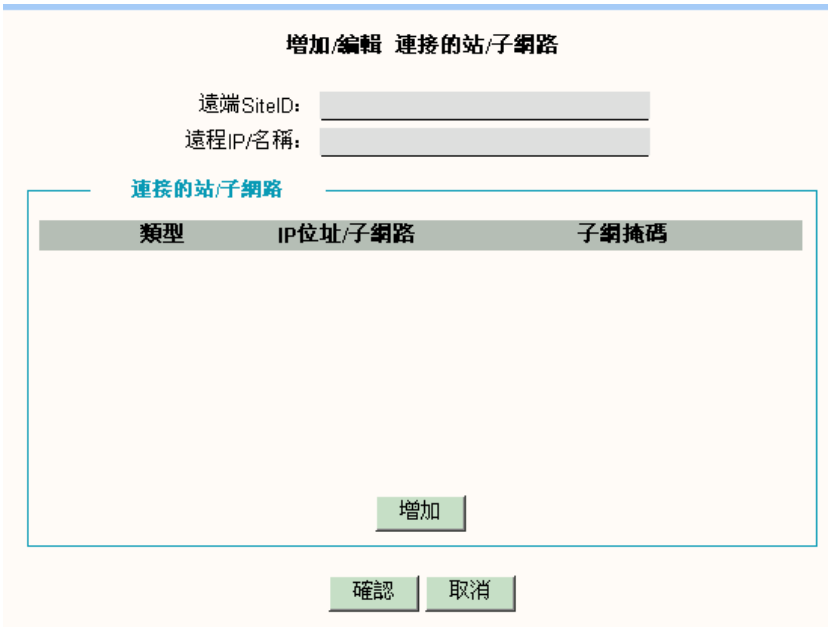


圖 84

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。

4.4 設定動態非軍事區

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 22 中點選進階中動態 DMZ，進入圖 85 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”。

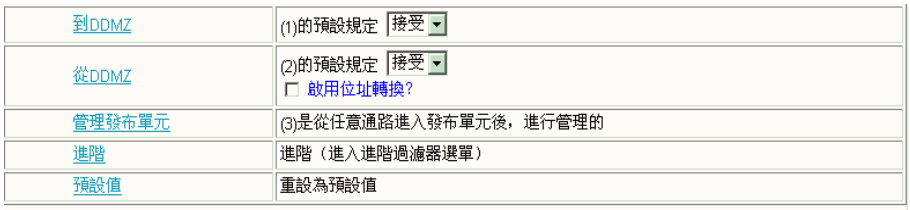


圖 85

2. 點選左面的連接，進入圖 86 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 86

點選<增加>，進入圖 87 介面，增加到 DDMZ 規則。

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

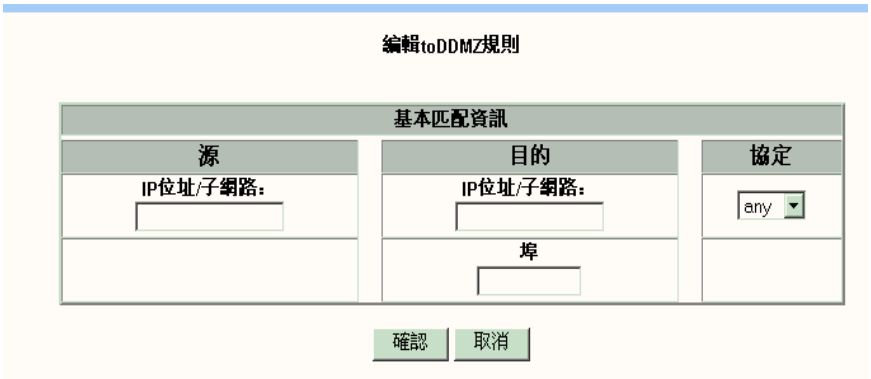


圖 87

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 86 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 88 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。

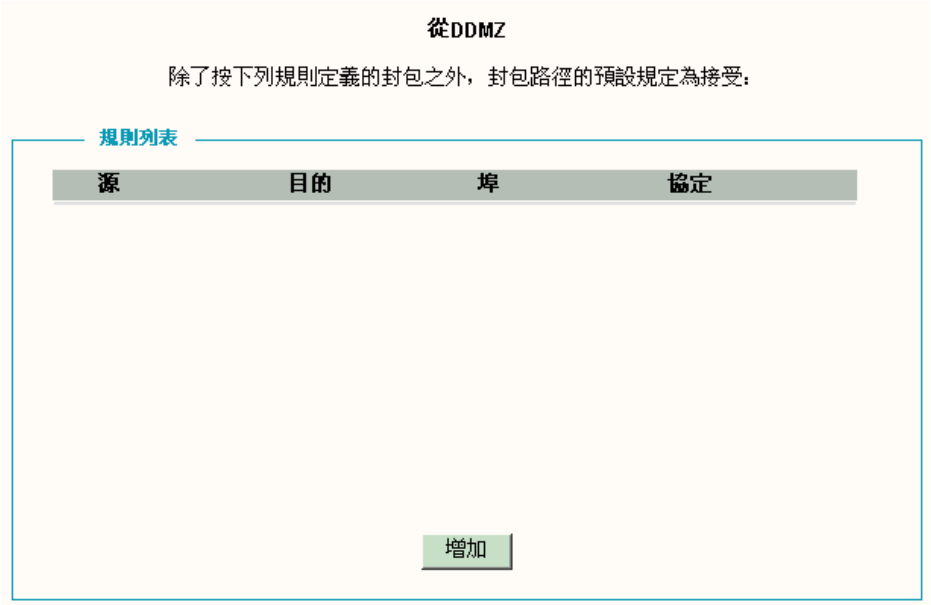


圖 88

5. 點選<增加>，進入圖 89 介面，增加從 DDMZ 規則。

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

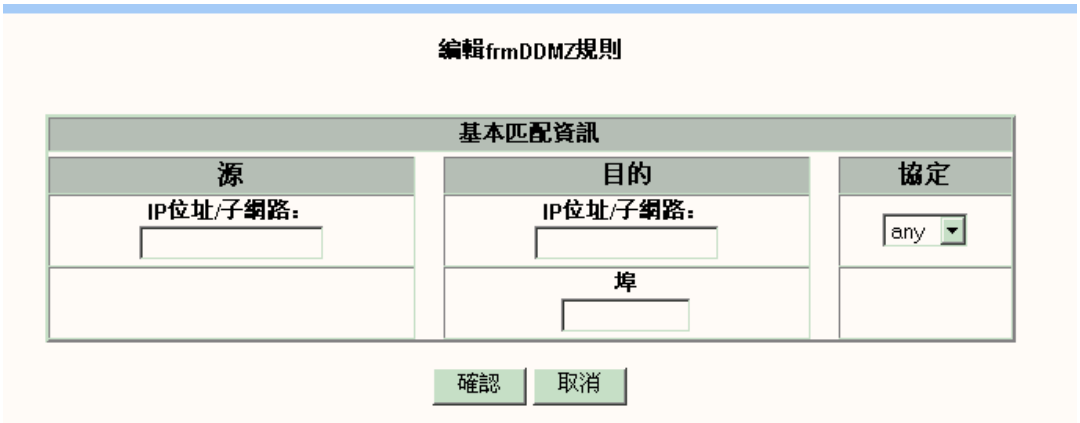


圖 89

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 85 介面中點選管理發佈單元，進入圖 90 介面。

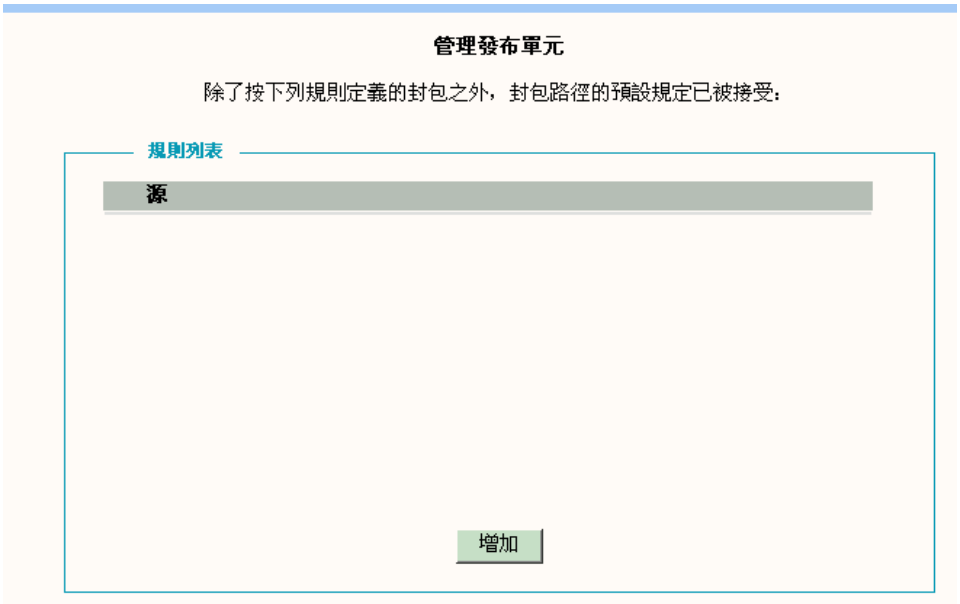


圖 90

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則，設定哪些機器不能存取此台 UU200。

2. 點選<增加>，進入圖 91 介面，增加存取規則。這邊只需要簡單的增加主機或是子網的 IP 位址就可以了。

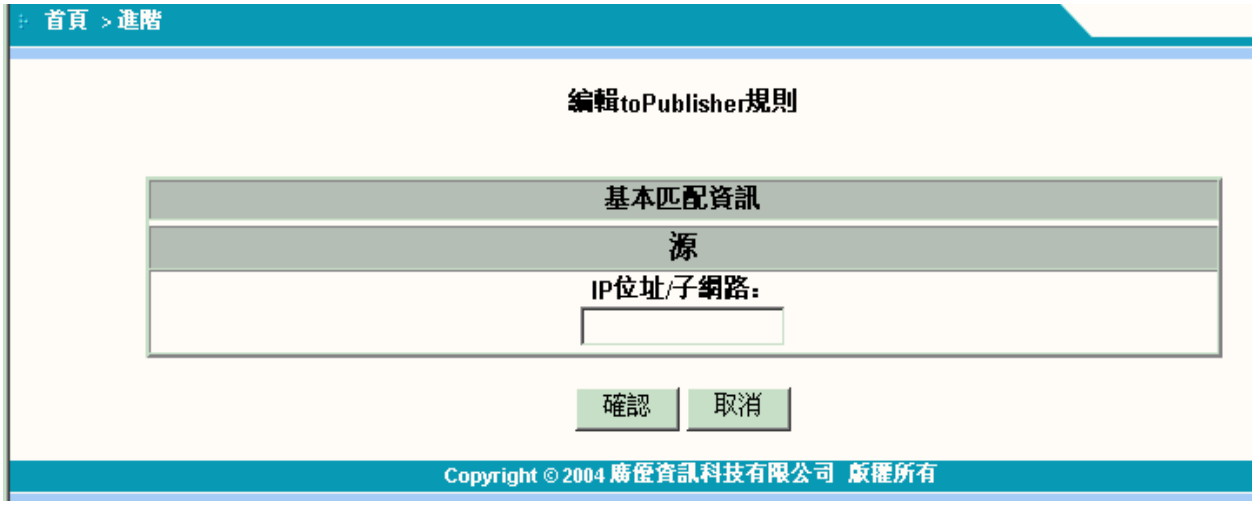


圖 91

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. 點選<進階>，進入圖 92 介面。
2. 點選<送到本機>，進入圖 93 介面。
3. 點選<增加>，進入圖 94 介面，增加規則。Dynamic DMZ 服務允許設定不超過 100 條的規則。

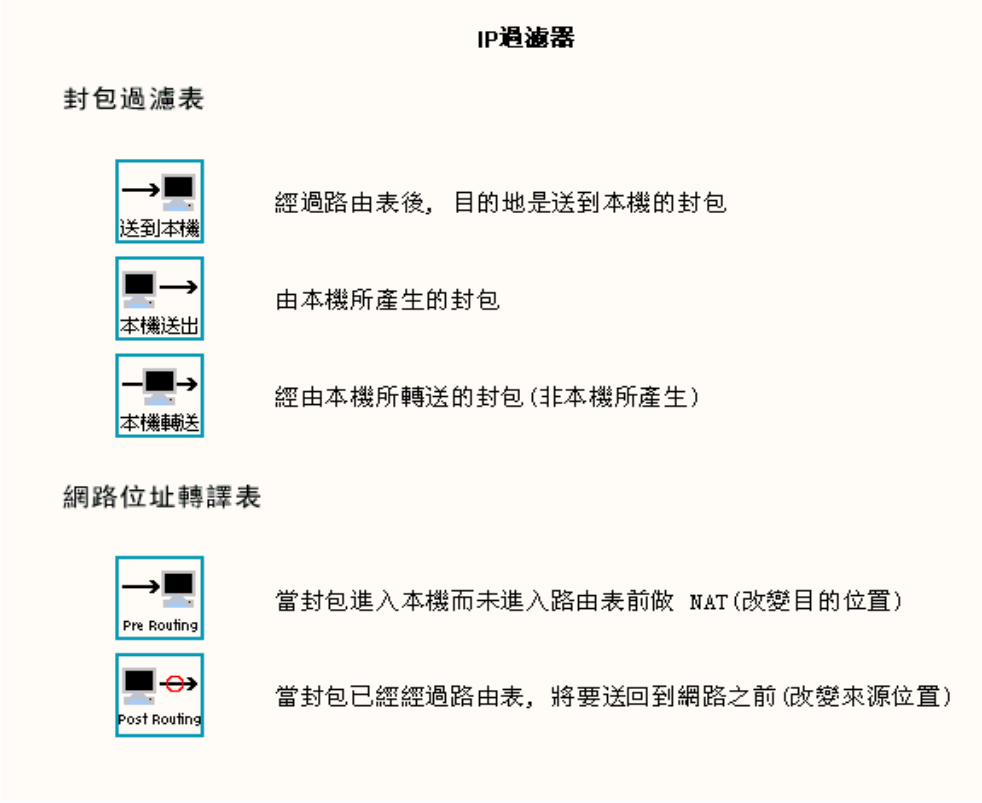


圖 92

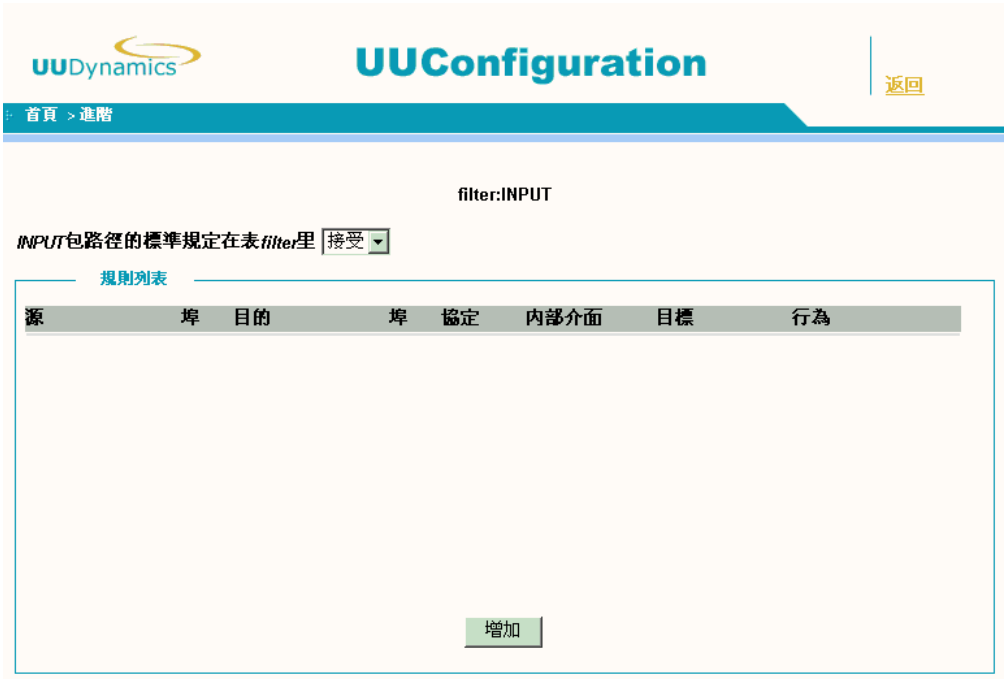


圖 93

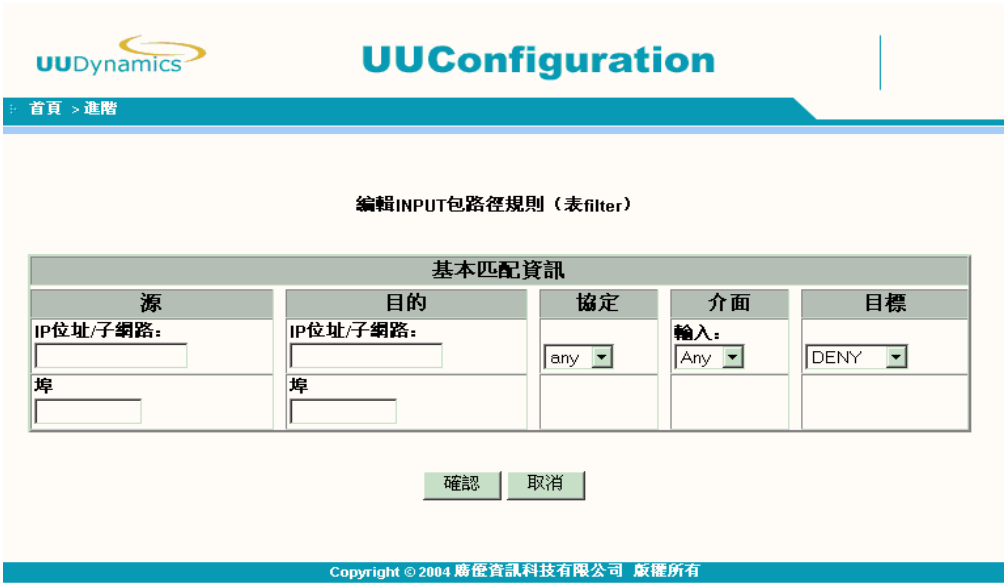


圖 94

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 95 中的 action 有修改，刪除，插入新規則，上移

下移規則等功能。

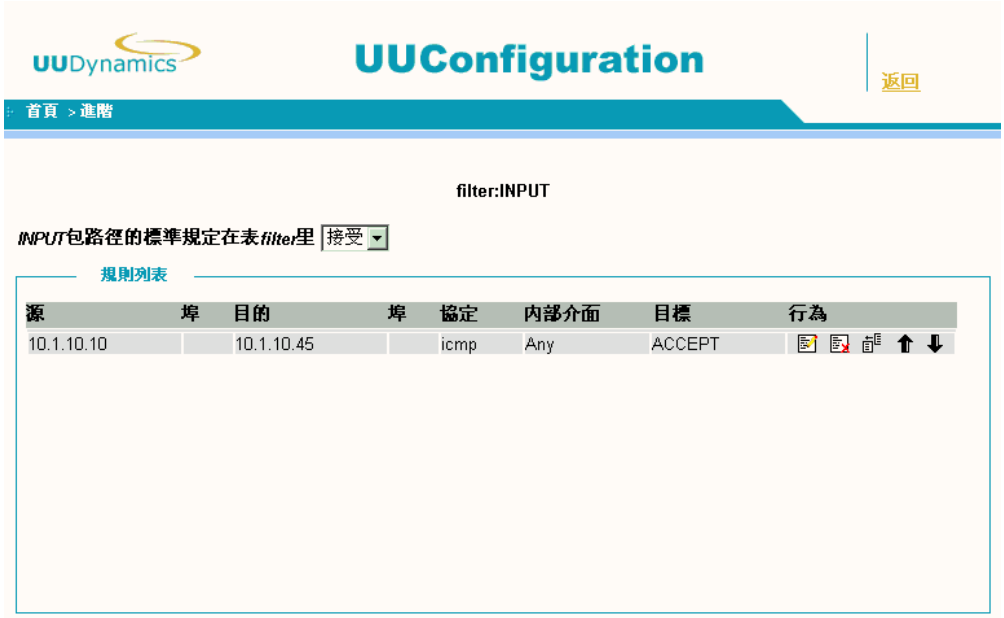


圖 95

預設值：

還原到初始配置狀態。

第5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 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 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，UUExchange/UUSwitch 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) 如果證書正確，應確保 UUExchange/UUSwitch 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局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） 登錄時，系統將提示資訊：*“使用者 [username] 目前已在本系統登錄”*。同時，勾選*“停止使用者 [username]*”時出錯。

因爲您沒有許可權使該使用者失效。如果仍要登錄，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 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 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則。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 “局域網路設定”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：

b) 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。

c) 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	啓用/提示

元件執行腳本	
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。

第6章 附 錄

6.1 UUDynamics File Browser Express/ File Browser 使用說明

“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”。

● 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；但由於它是基於局域網路的設計，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）。

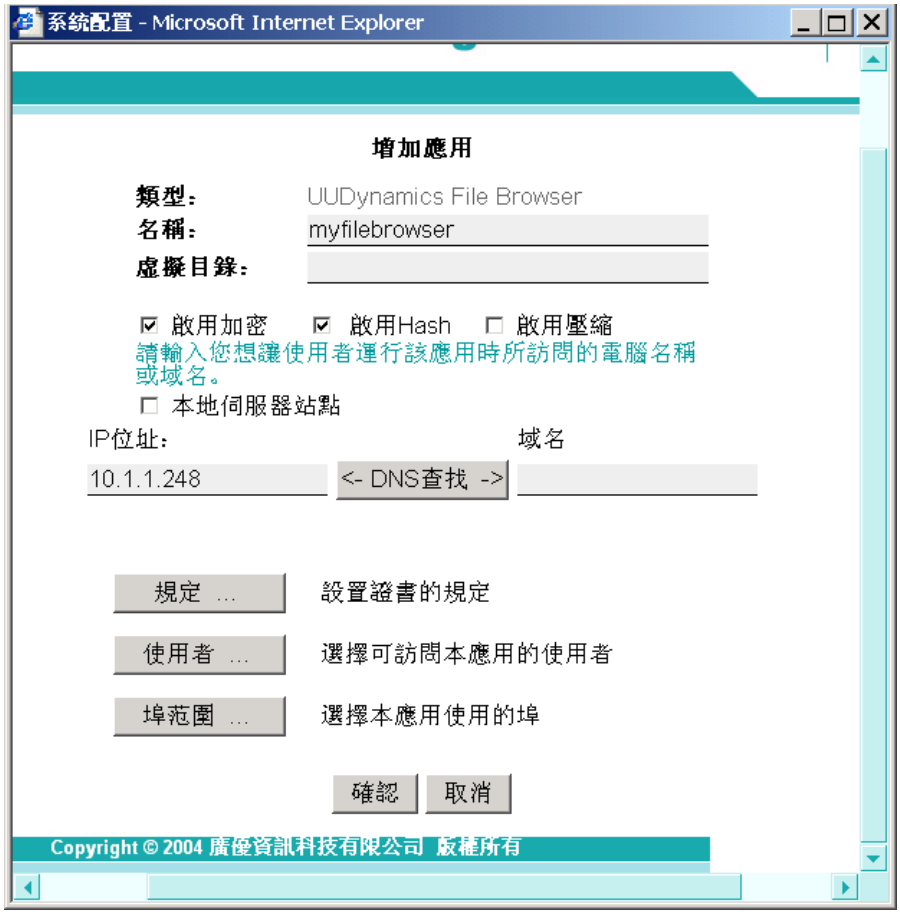
注意：

在發佈 UUDynamics File Browser Express 服務之前，請先驗證共用的檔案夾的設定。您可以通過局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：



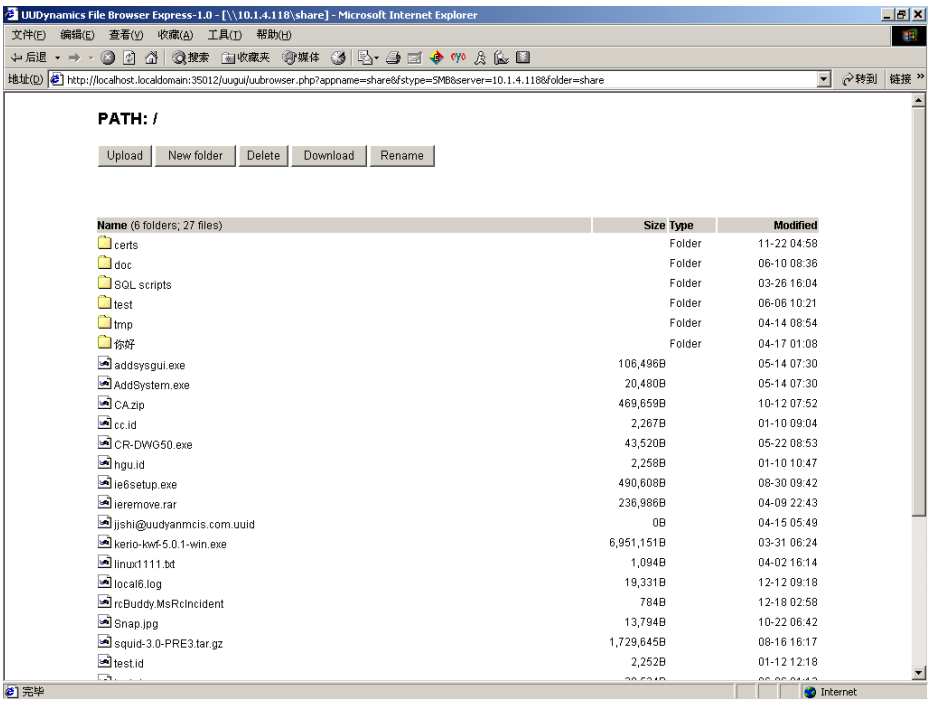
參數名	說明

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、域名	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

● 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 伺服器實現對局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。

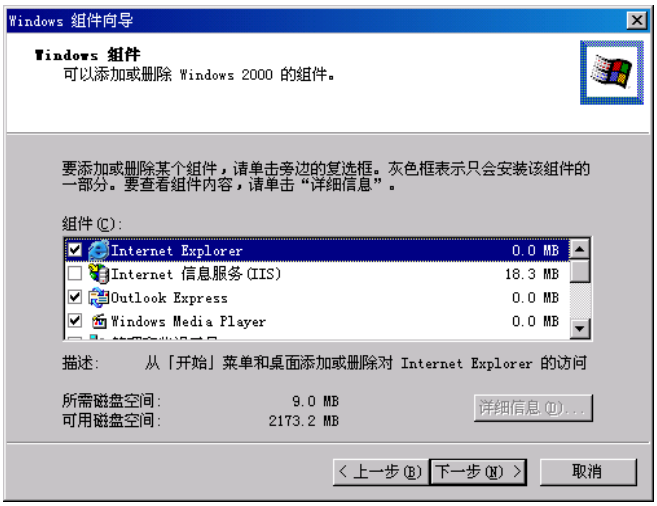
（1）Microsoft Windows 2000 伺服器/ Microsoft Windows 2000 Advance 伺服器

Microsoft Windows 2000 伺服器/ Microsoft Windows 2000 Advance 伺服器上已經預設安裝并啓動了 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：

打開控制面板中的“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，彈出如附圖 1 所示視窗：



附圖 1

如圖所示，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。

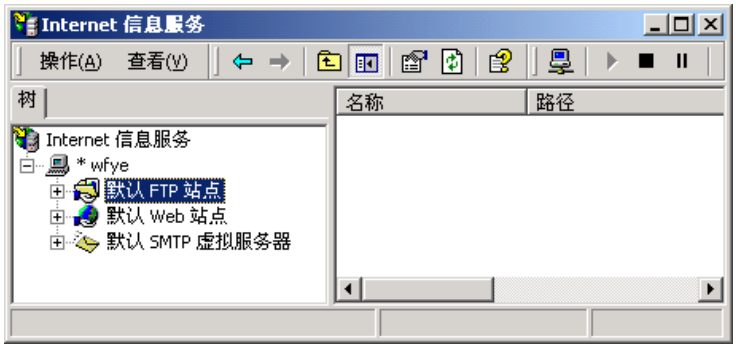
1.2 IIS 的配置：

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。

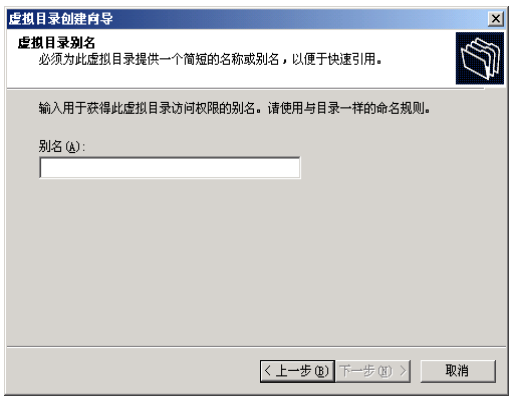
（1）創建 Virtual Directory

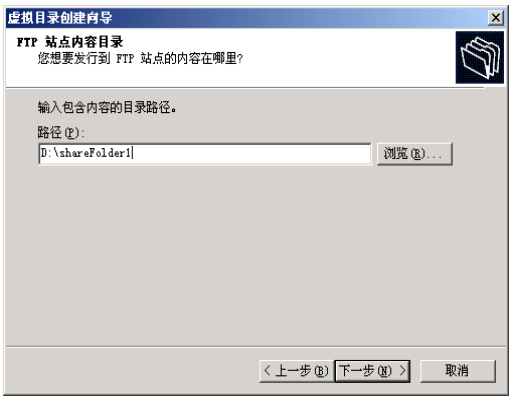
首先確定需要被遠端存取的本地目錄，在 FTP 伺服器上創建虛擬目錄，與該實際目錄連接。具體操作方法如下：

打開控制面板中的“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。

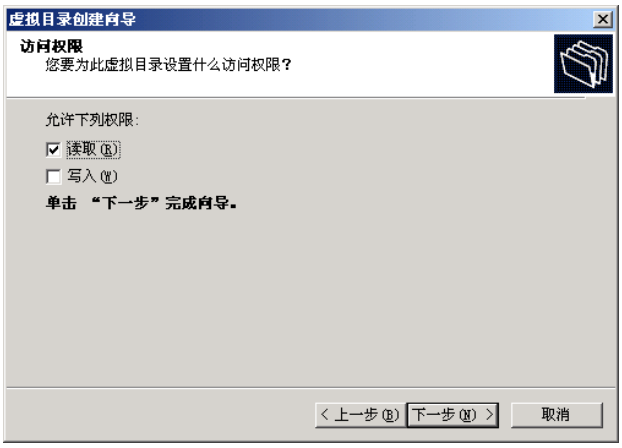


附圖 2





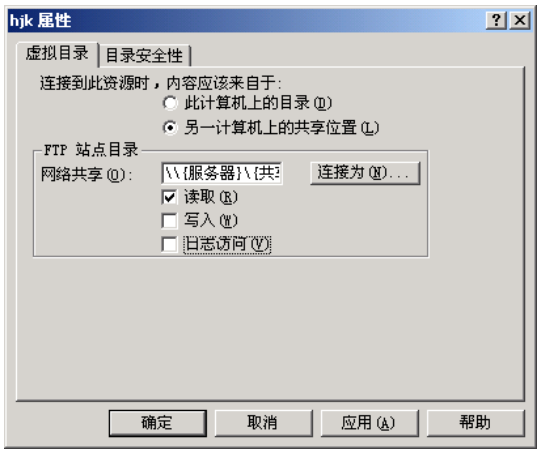
附圖 3



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\共用的格式填入局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 位址進行存取控制。具體方法如下：打開 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：

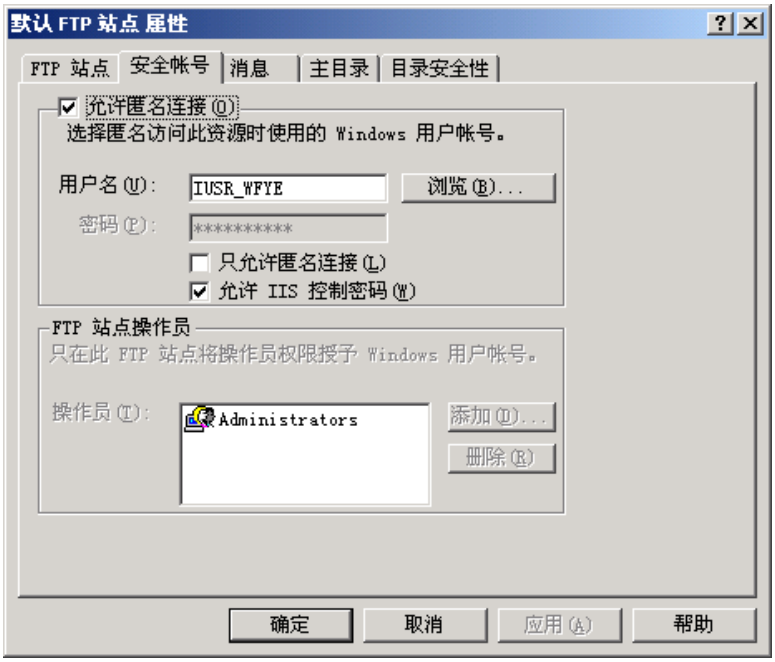
FTP 伺服器可以利用 Windows 作業系統中的檔或檔夾的 NTFS 許可權屬性來控制使用者存取，因此一個使用者若需存取某個 FTP 站點或目錄，則其必須對該實際目錄有至少讀的許可權。

檔或檔夾的 NTFS 許可權屬性具體的設定方法爲：

打開 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：

打開 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 站點屬性，如附圖 6，選擇安全帳號，勾選“允許匿名連接” 。這樣，遠端客戶存取時就有系統默認使用者 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錄兩種許可權。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，網網網網域控制器安全策略，它們的優先順序爲：網網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錄兩種許可權。

配置方法爲：

如果 FTP 伺服器安裝在網網網網域控制器上，則由於網網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錄中檢查該 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：

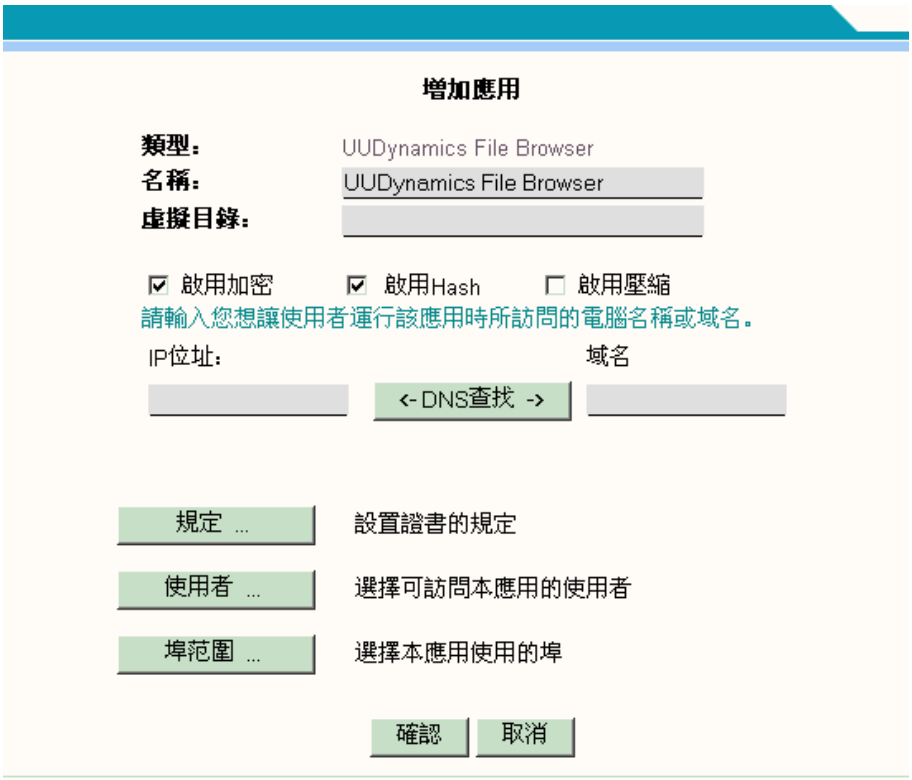
secedit /refreshpolicy machine_policy /enforce

ⓘ 注意：

IIS/FTP 的配置正確與否，可以先在局域網路中進行測試，即在局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。我們建議只有在局域網路測試成功後，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，雙點擊視窗中 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。

6.2 *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。

6.2.1 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。

6.2.2 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。

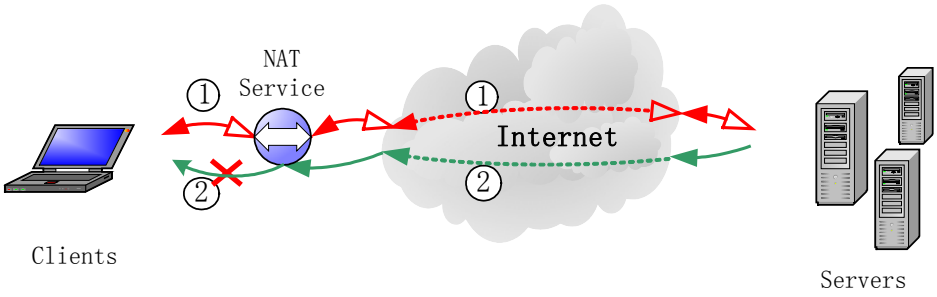
6.2.3 支援 IP 應用及特定的 NetBIOS 應用

***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“4.1 發佈應用程式” 中的例二）。

6.2.4 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則。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。

6.2.5 WinSock 應用

支援的應用必須基於 Windows Winsock。

6.3 *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。

6.4 其他

（1） 如想得到其他相關文檔請存取網站www.uudynamics.com；

（2） 在使用UUDynamics公司的產品時，如果有什麼疑問或產品發生了故障，請參考以上文檔，或發送問題報告到tech_support@uudynamics.com；

（3） UUDynamics 公司對文檔中內容擁有最終解釋權。