



## UU250 Quick Start Guide

### 群浩科技股份有限公司

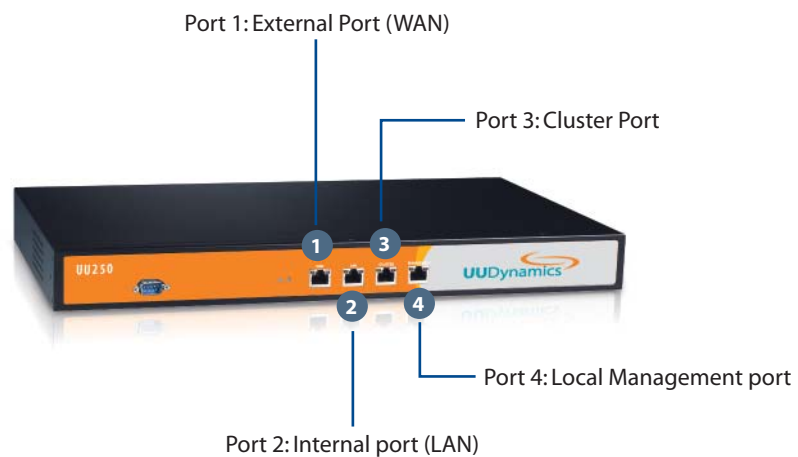
110台北市信義區忠孝東路五段508號7樓之1 TEL: 02-27278080 FAX: 02-27275544  
7F-1, No.508, Sec. 5, Zhongxiao E. Rd., Xinyi Dist., Taipei City 110, Taiwan (R.O.C.) TEL: +886-2-27278080 TEL: +886-2-27275544

# 目錄

|                            |    |
|----------------------------|----|
| 一、硬體介面 .....               | 2  |
| 二、系統設定 .....               |    |
| Step1. Admin Local登入 ..... | 5  |
| Step2. 建立使用帳號 .....        |    |
| 建立Local User帳號/群組 .....    | 8  |
| 建立Windows AD認證 .....       | 10 |
| Step3. 發佈應用 .....          | 14 |
| Web Server .....           | 15 |
| Terminal Server .....      | 18 |
| File Server .....          | 21 |
| Custom Roaming .....       | 23 |
| iSTAR Remote Access .....  | 28 |
| 網路磁碟 .....                 | 30 |
| Step4. 使用者遠端登入 .....       | 33 |
| 三、附錄 .....                 |    |
| 直接連線模式 .....               | 38 |
| UUCentral模式 .....          | 44 |

## 硬體介面

### 1. 硬體介面說明



### 2. 硬體連接設定



## 系統設定

### 1. 簡易系統設定步驟

#### Step 1

Admin Local  
登入

#### Step 2

建立使用者帳號

建立Local User  
帳號/群組

建立Windows AD  
認證

#### Step 3

發佈應用

Web Server

Terminal Server

File Server

#### Step 4

使用者遠端登入

Custom Roaming

iSTAR Remote  
Access

網路磁碟

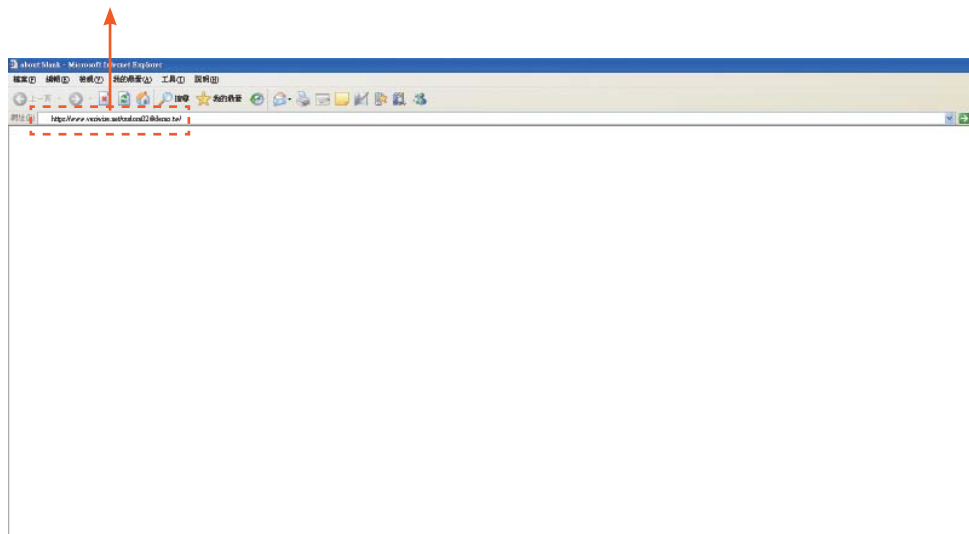
## Step 1. Admin Local登入

### 硬體連接設定



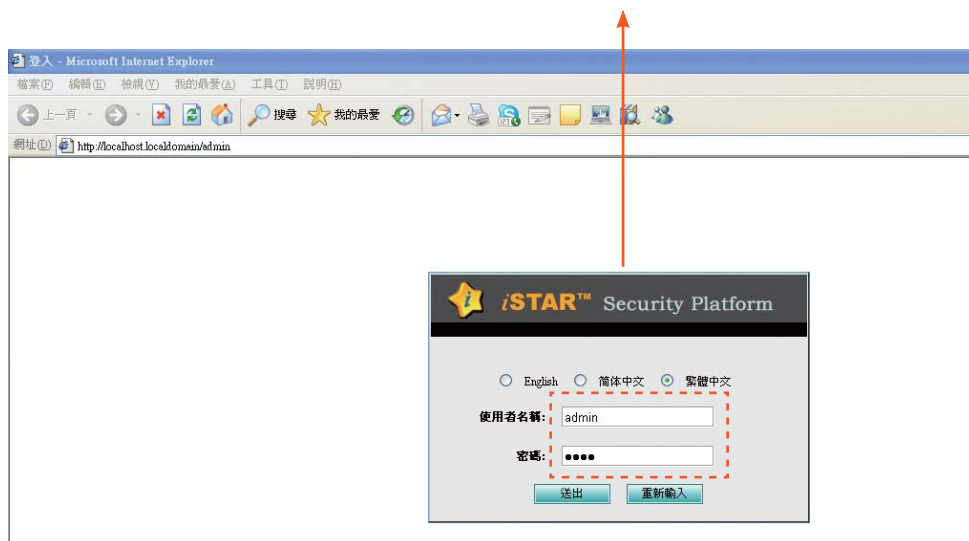
## 輸入遠端登入網址

打開IE瀏覽器，於網址列輸入「http://1.1.1.1/admin」



## 輸入Admin帳號/密碼

在彈出的IE視窗上再次輸入admin及密碼後點選「送出」



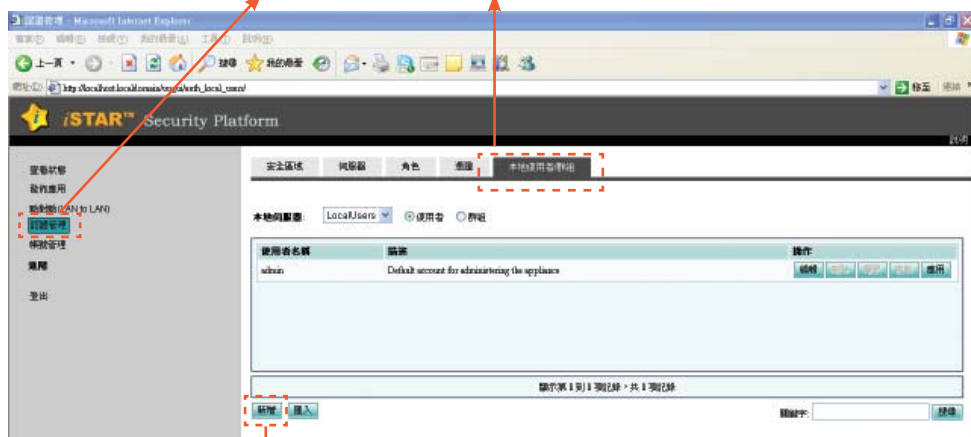
## 完成admin Local登入作業



## Step 2. 建立使用者帳號

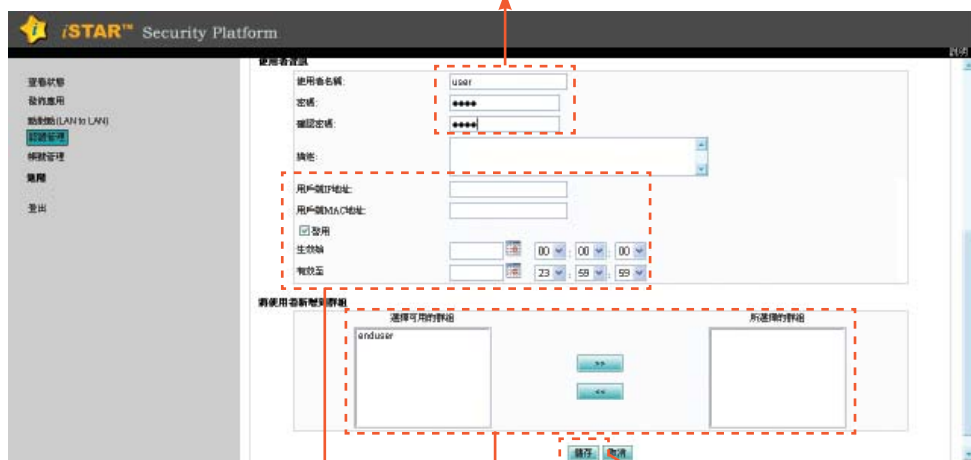
### 建立Local User 帳號/群組

- 1 於管理畫面中點選「認證管理」「本地使用者/群組」



- 2 點選「新增」

- 1 必填項目：輸入「使用者名稱」及「密碼」及「確認密碼」欄位



- 2 選填項目：輸入相關欄位對應的資訊
- 3 選填項目：選擇是否加入群組
- 4 確認輸入相關資訊後，點選儲存

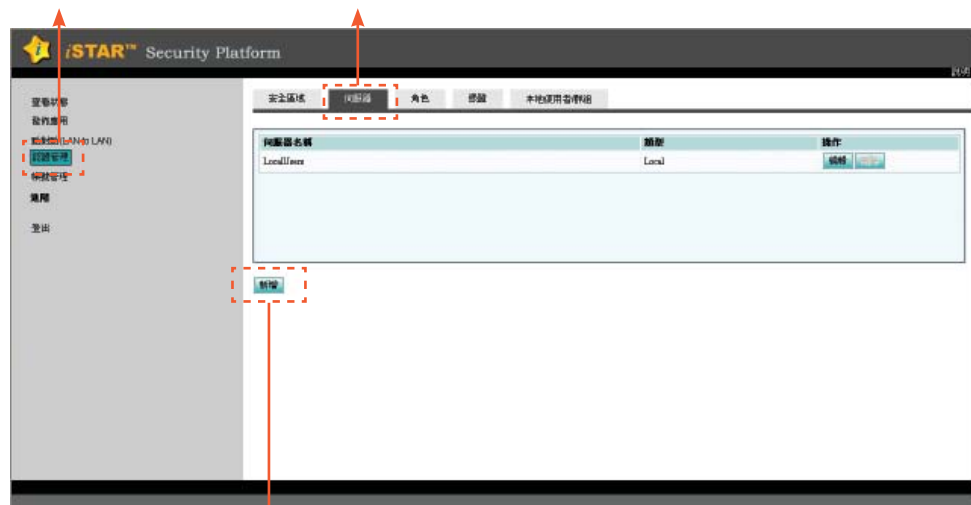


完成新增使用者帳號

## 建立Windows AD認證

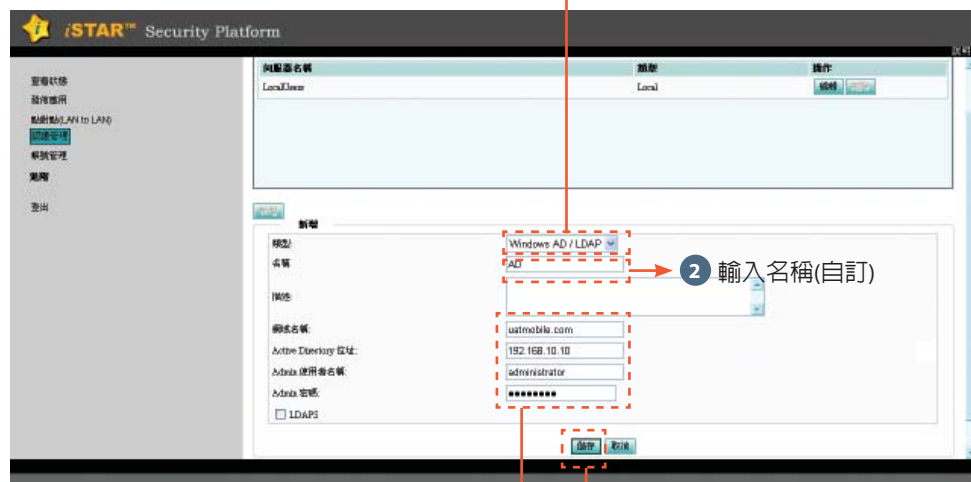
### 新增Windows AD伺服器

1 於管理畫面中點選「認證管理」「伺服器」

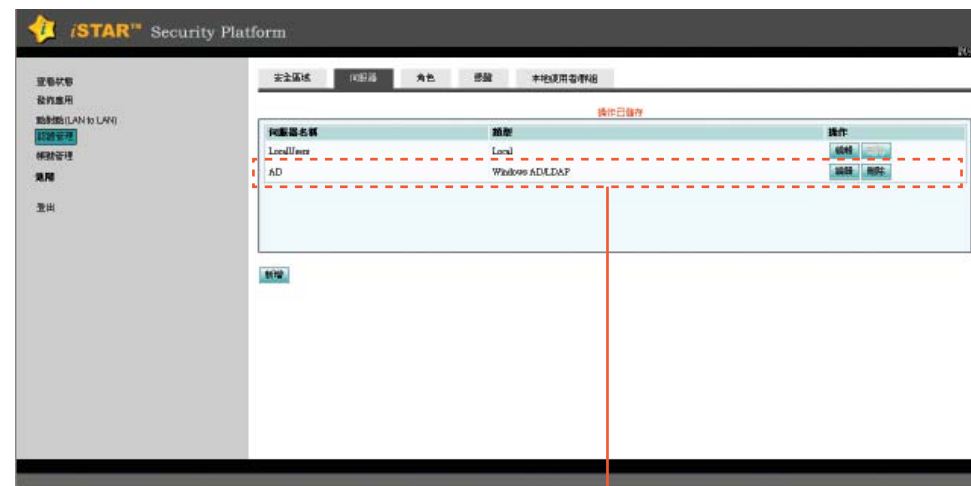


2 點選「新增」

1 選擇認證類型：Windows AD認證可選擇「Windows AD/LDAP」或是「Windows AD/NTM」



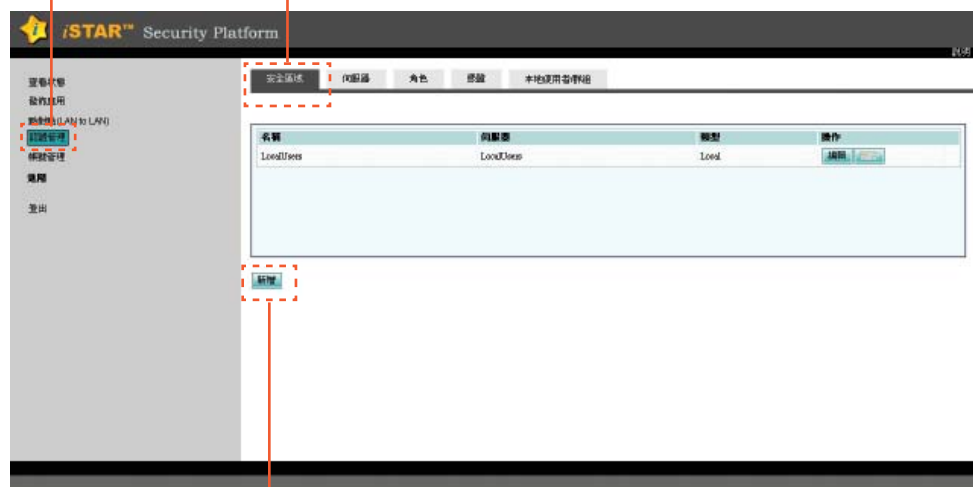
3 輸入相關欄位對應的資訊 4 確認輸入相關資訊後，點選儲存



完成新增Windows AD伺服器

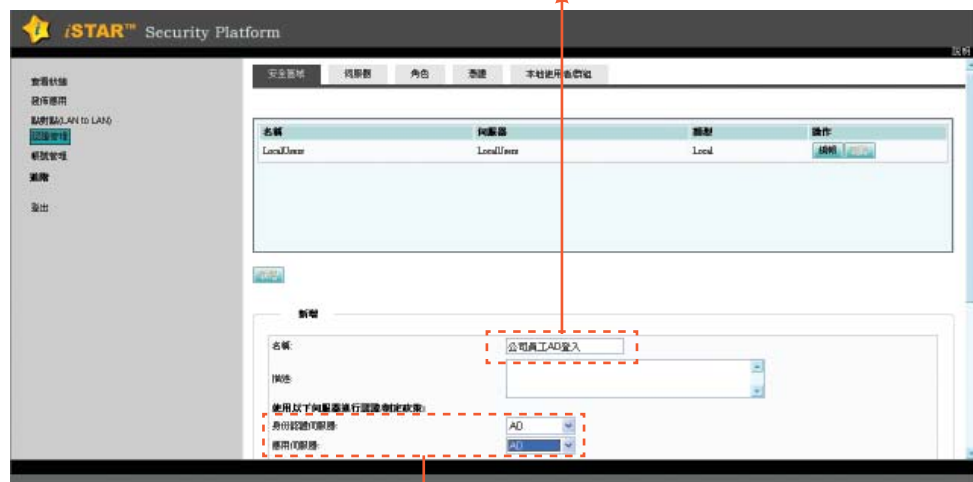
## 新增Windows AD安全區域

- 1 於管理畫面中點選「認證管理」「安全區域」



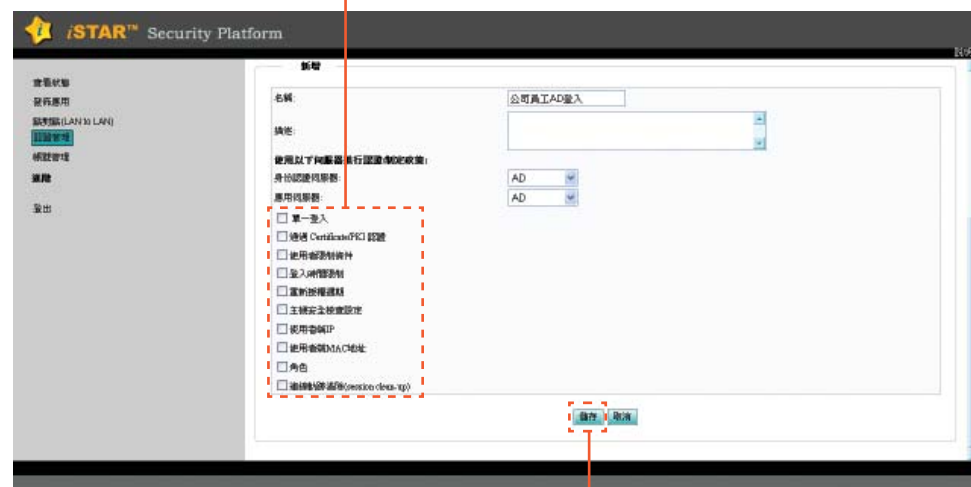
- 2 點選「新增」

- 1 必填項目：輸入安全域名稱，這個名稱將會是使用者登入時所看到的認證方式名稱

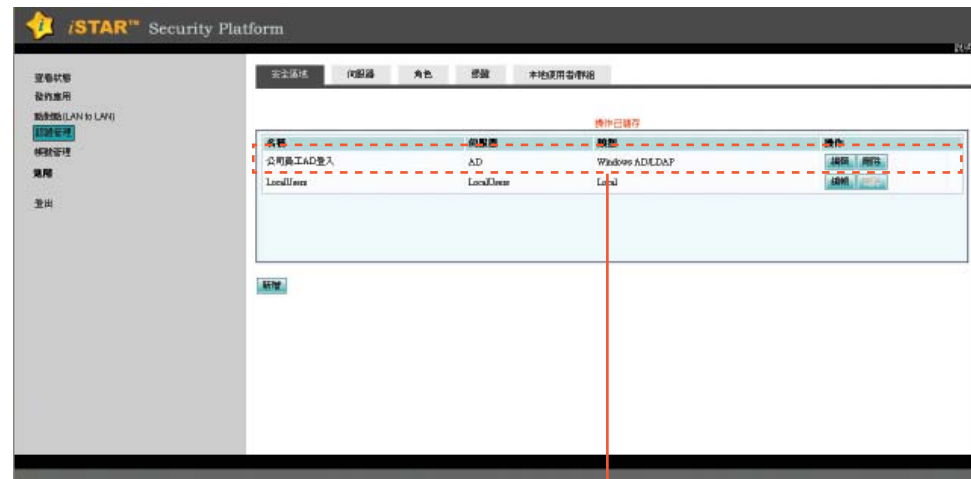


- 2 必填項目：於「身份認證伺服器」及「應用伺服器」欄位選擇先前所建立的Windows AD伺服器名稱

- 1 選填項目：勾選相關項目進行細部設定，各項設定功能說明及設定方式請點選設定頁面右上角的「說明」



- 2 確認輸入相關資訊後，點選「儲存」



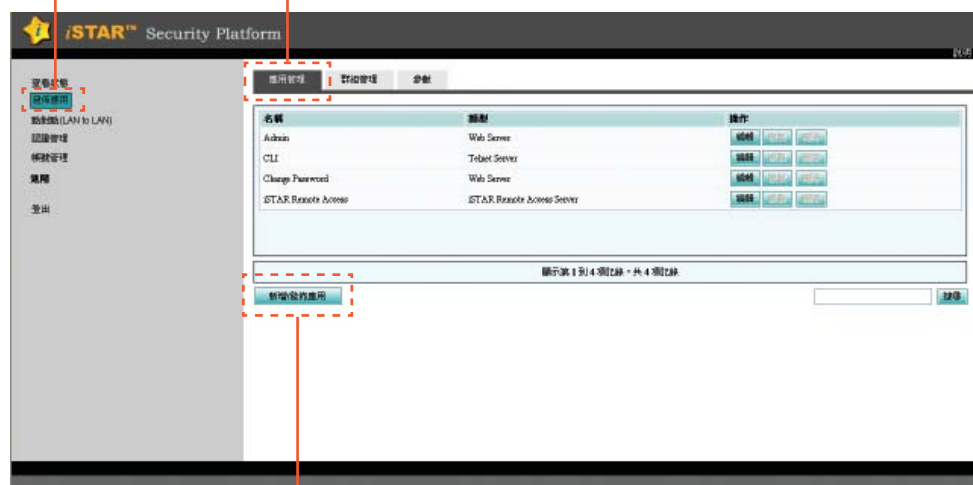
完成建立Windows AD認證(安全區域)



## Step 3. 發佈應用

### 新增發佈應用

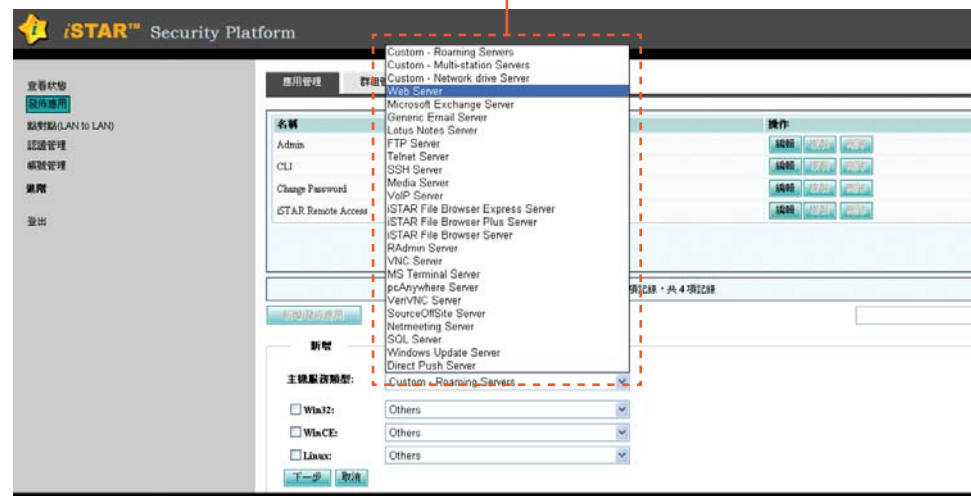
1 於管理畫面中點選「發佈應用」「應用管理」



2 點選「新增發佈應用」

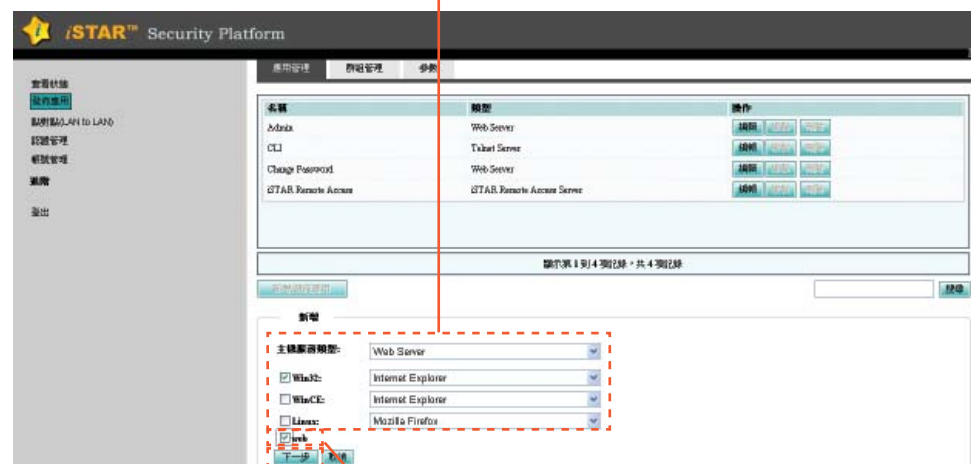
## Web Server

下拉「主機服務類型」，選擇「Web server」



1 選擇Client端所使用的作業系統，其中：

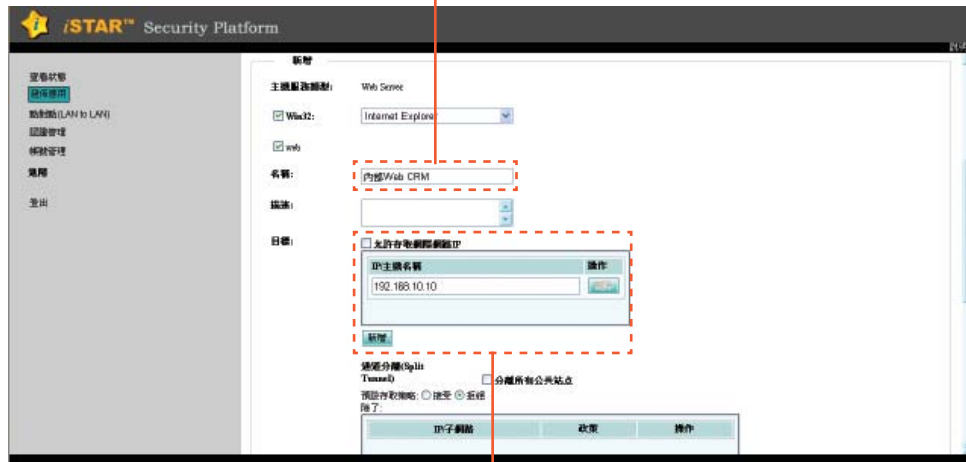
- Win32(64)選項為一般PC或Notebook安裝Microsoft windows 2000以上作業系統
- WinCE選項為SmartPhone或PDA安裝Microsoft Windows Mobile(5.0以上)作業系統
- Linux選項為裝Linux作業系統



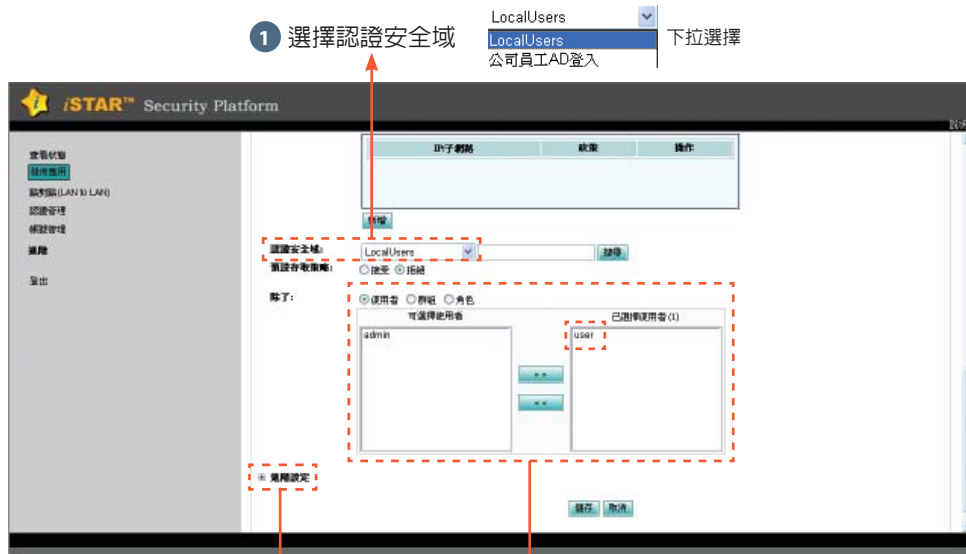
3 相關資訊確認後點選「下一步」

2 選擇啟動這個web應用的reverse web功能(不需下載安裝Active X控制項即可連結使用，此功能僅支援web應用

1 輸入這個應用所顯示的名稱



2 輸入web伺服器IP位址，若允許client端透過這個應用可同時存取多台web server，可點選「新增」加入其他web server IP

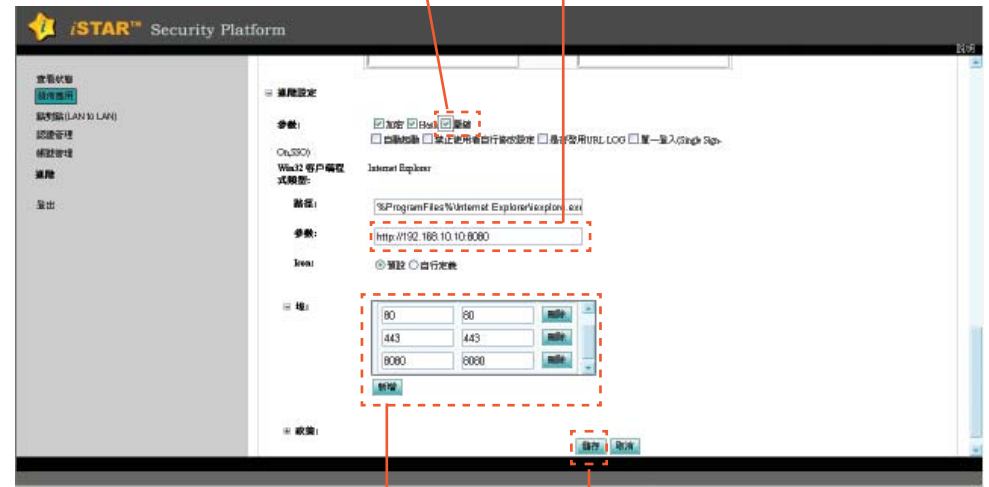


3 點選「進階設定」前面的「+」欄位

2 在左邊「可選擇使用者」欄中選取欲授權的使用者後，點選「>>」將使用者移到右邊的已選擇使用者欄位

1 點選「壓縮」功能可啟動資料傳輸壓縮

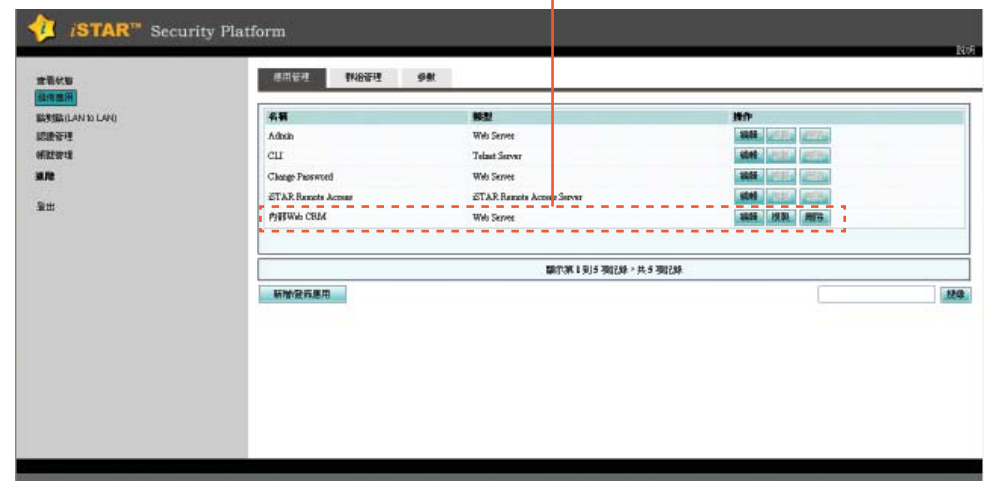
2 輸入web server連結的完整URL



3 新增或删除service port

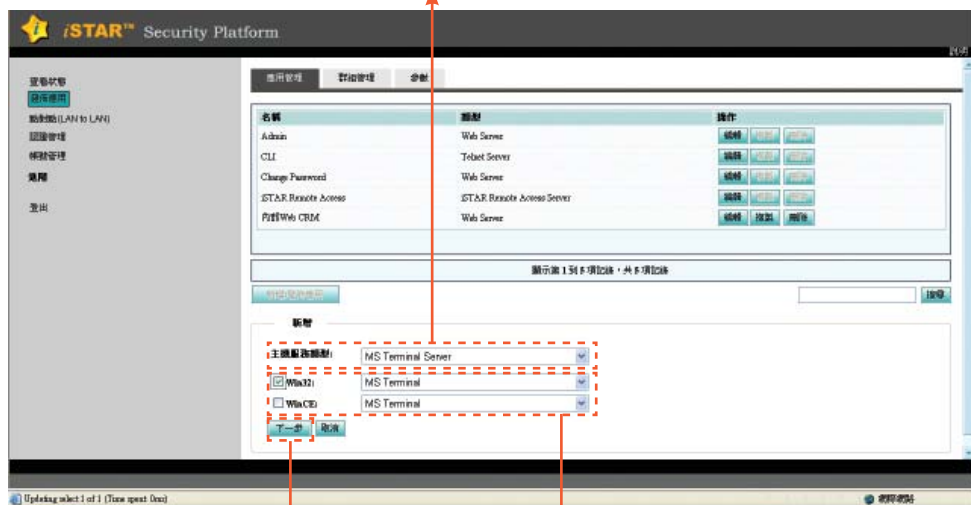
4 確認相關資訊無誤後，點選「儲存」

完成發佈web server



## Terminal Service

1 選擇主機服務類型為「MS Terminal Server」

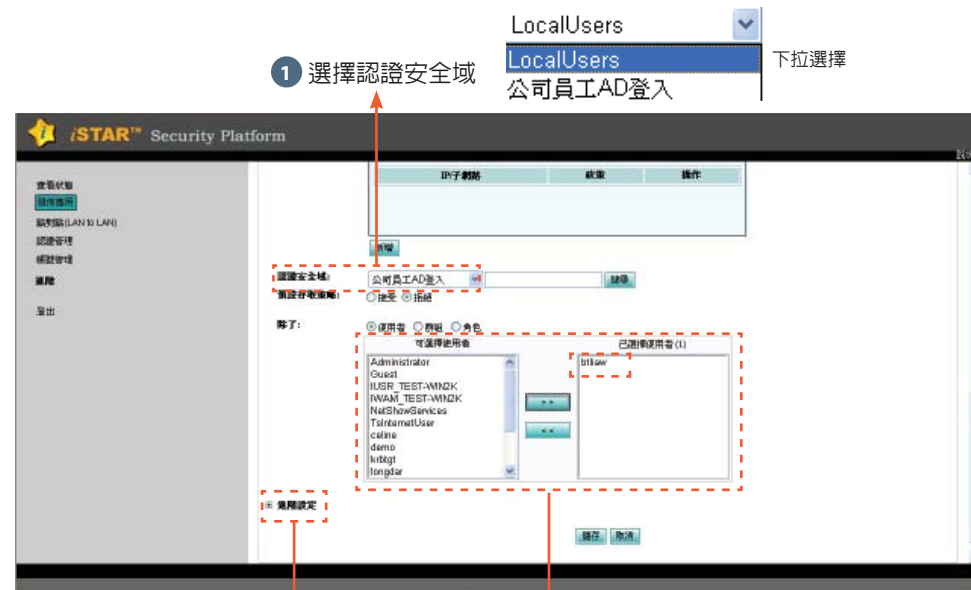


3 點選「下一步」 2 勾選client端作業系統平台



2 輸入Terminal Server IP位址，若允許client端透過這個應用可同時存取多台Terminal server，可點選「新增」加入其他Terminal server IP

1 選擇認證安全域

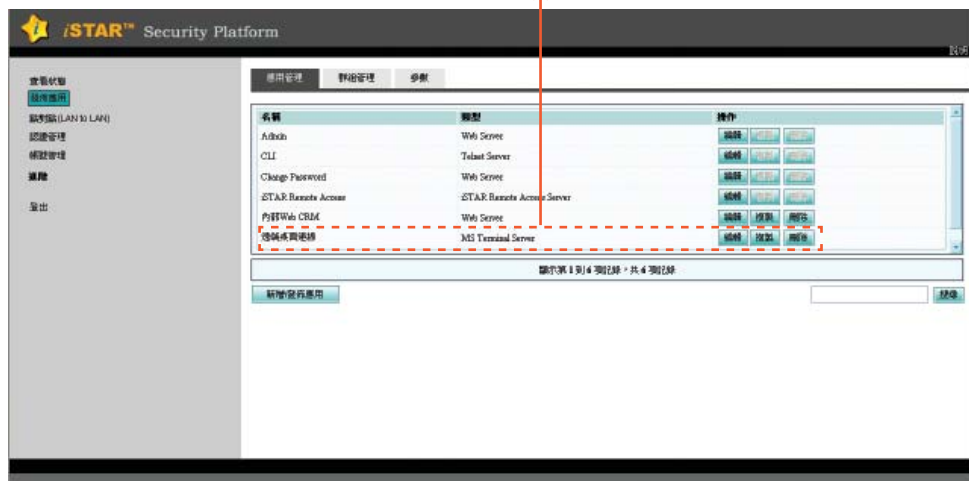


3 點選「進階設定」前面的「+」 2 在左邊「可選擇使用者」欄中選取欲授權的使用者後，點選「>>」將使用者移到右邊的已選擇使用者欄位



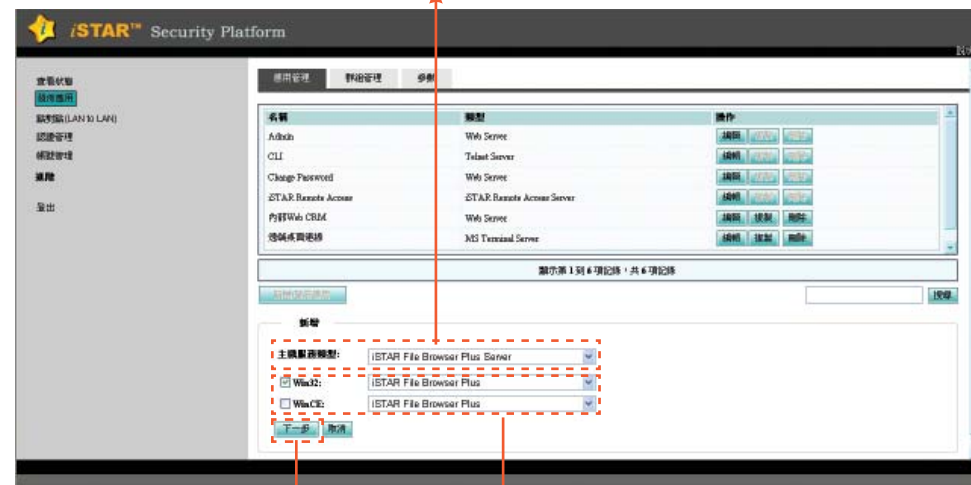
2 確認相關資訊無誤後，點選「儲存」

完成發佈Terminal service



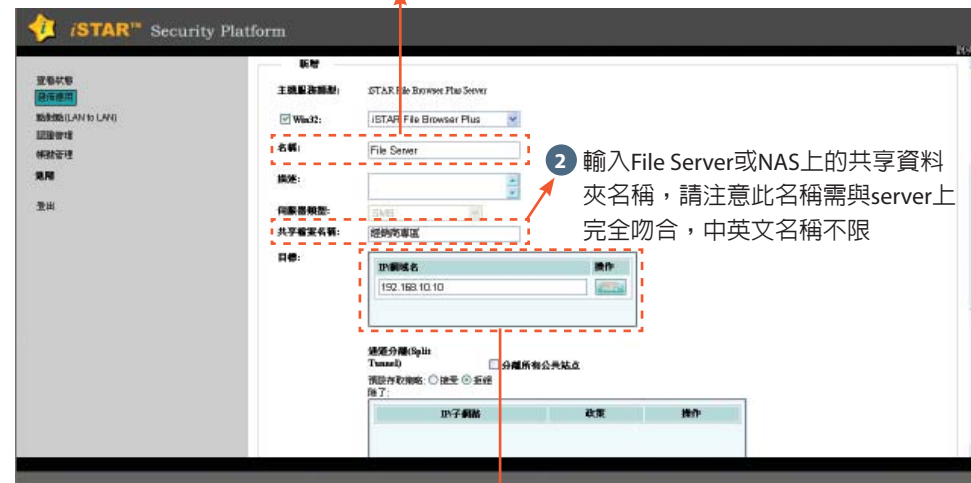
## File Server

1 選擇主機服務類型為「iSTAR File Browser Plus Server」



3 點選「下一步」 2 勾選client端作業系統平台

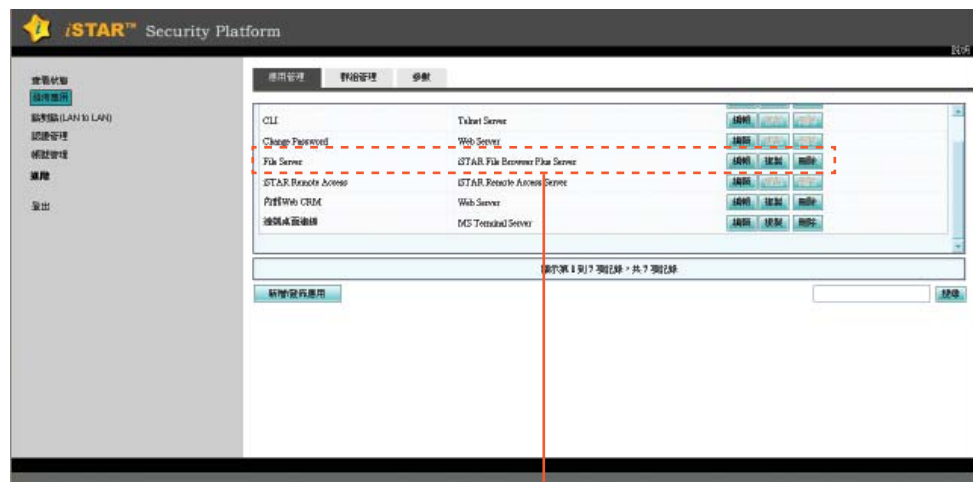
1 輸入這個應用所顯示的名稱



3 輸入檔案伺服器IP位址



2 在左邊「可選擇使用者」欄中選取欲授權的使用者後，點選 將使用者移到右邊的已選擇使用者欄位



## Custom-Roaming Servers

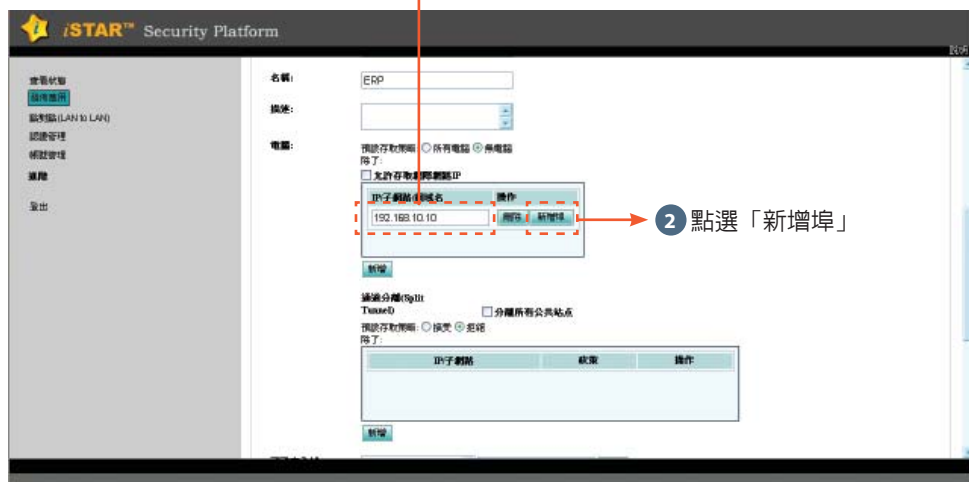


說明：

Custom為自定應用的選項，而Custom-Roaming Servers則是用來發布如2 Tier架構，前後端server需連結不同的service port，如某些應用前端是AP server；後端是DB Server，而Client端連結時會連結前端AP server，但同一個應用session還會連結到後端的DB Server

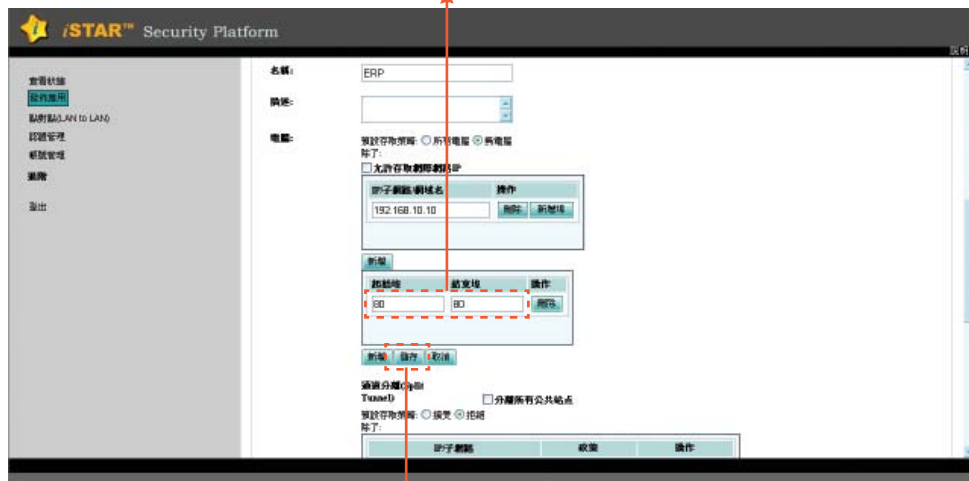


1 輸入第一台主機的 IP，假設第一台是設定Web Server



2 點選「新增埠」

1 輸入這台Server所需的port，因為假設是Web Server，所以輸入port 80，若還有其他port，如Port 443；則再點選下方「新增」來加入



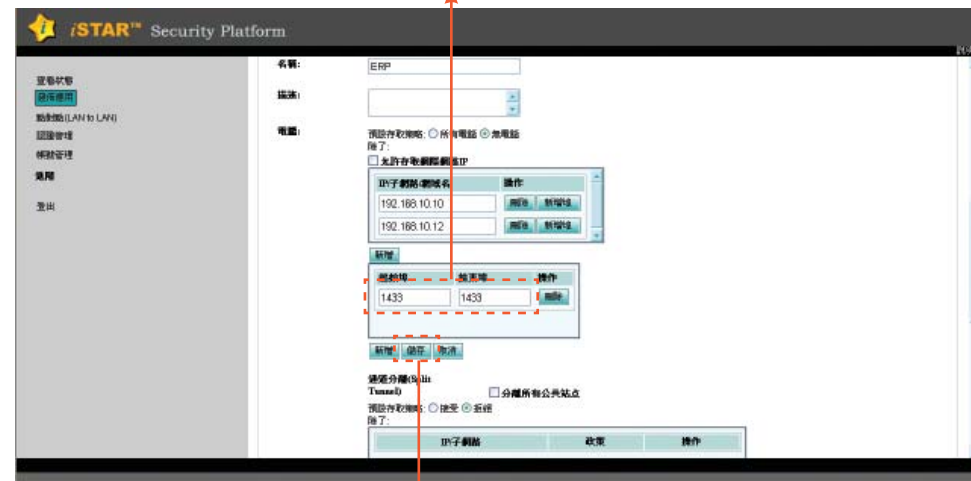
2 確認所有port完全輸入後，點選「儲存」

1 輸入第二台主機的 IP，假設第一台是設定SQL Server



2 點選「新增埠」

1 輸入這台Server所需的port，因為假設是SQL Server，所以輸入port 1433，若還有其他port需加入，則再點選下方「新增」來加入



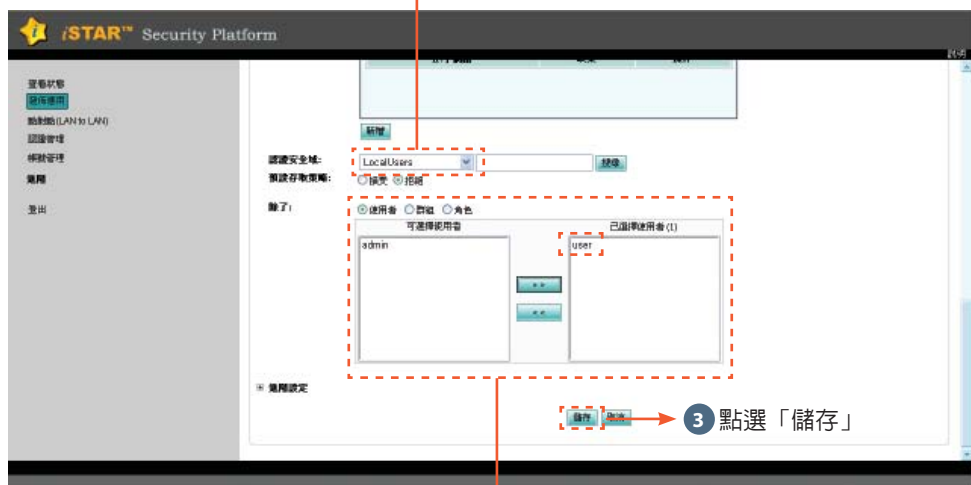
2 確認所有port完全輸入後，點選「儲存」



若還有其他server需加入，請點選「新增」依上述步驟加入即可



1 選擇認證安全域 LocalUsers  
公司員工AD登入

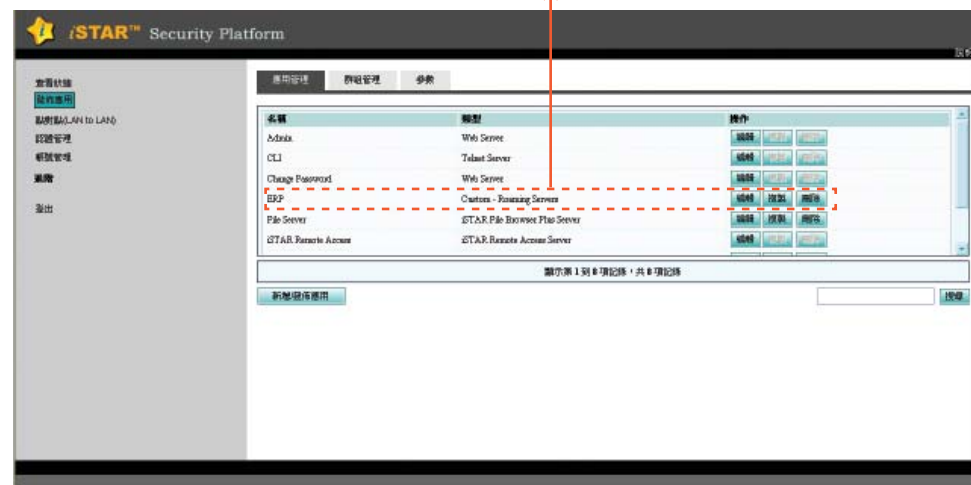


2 在左邊「可選擇使用者」欄中選取欲授權的使用者後，點選「>>」將使用者移到右邊的已選擇使用者欄位

1 輸入client端應用程式的執行檔存放路徑，如這個範例中client端會以IE瀏覽器去執行ERP，所以此處需輸入IE瀏覽器的執行檔存放路徑為：C:\Program Files\Internet Explorer\IEXPLORE.EXE

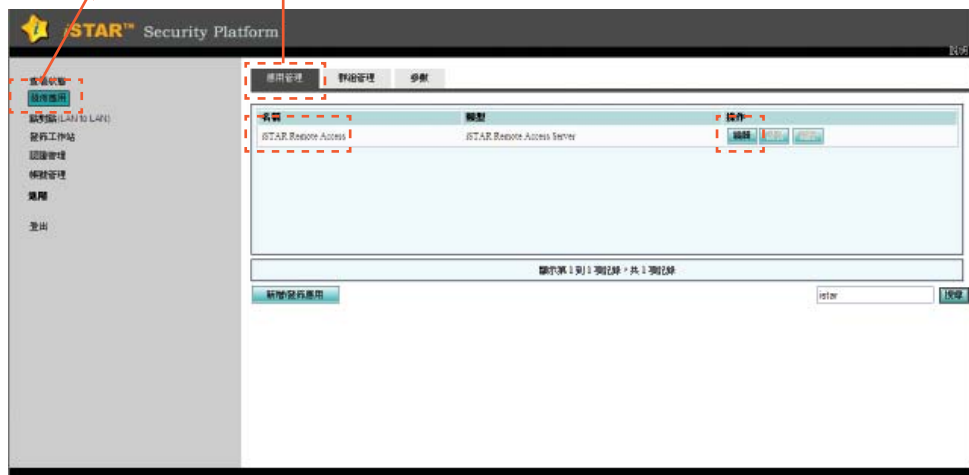


完成發佈Custom-Roaming Servers



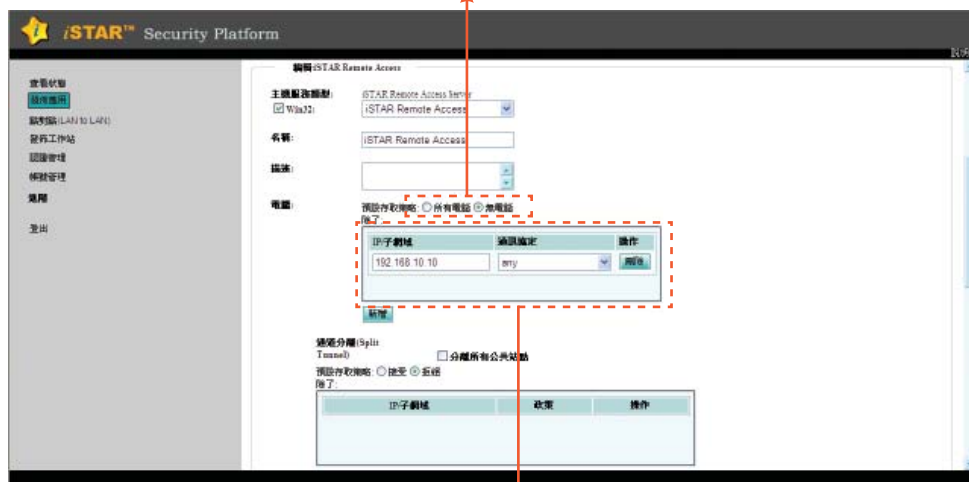
## iSTAR Remote Access

- 1 於管理畫面中點選「發佈應用」「應用管理」->「iSTAR Remote Access」的編輯



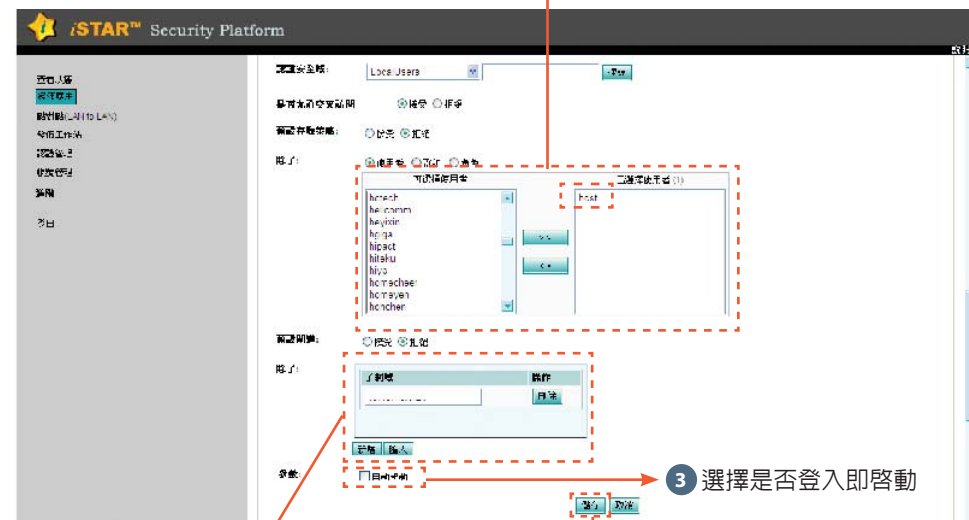
- 1 選擇使用者取得IP後的「預設存取策略」，即可連線存取的目的IP，若選擇

1. 「所有電腦」即為不限制取得IP後可到達的目的IP
2. 「無電腦」則需進行下方欄位可到達的IP(服務)設定



- 2 若於「預設存取策略」中選擇「無電腦」則須於此處指定可存取的目的IP或服務，可直接輸入IP或以xx.xx.xx.xx/24表至一個Class C網段，若需輸入多筆，請點選「新增」後輸入

- 1 在左邊「可選擇使用者」欄中選取欲授權的使用者後，點選 將使用者移到右邊的已選擇使用者欄位

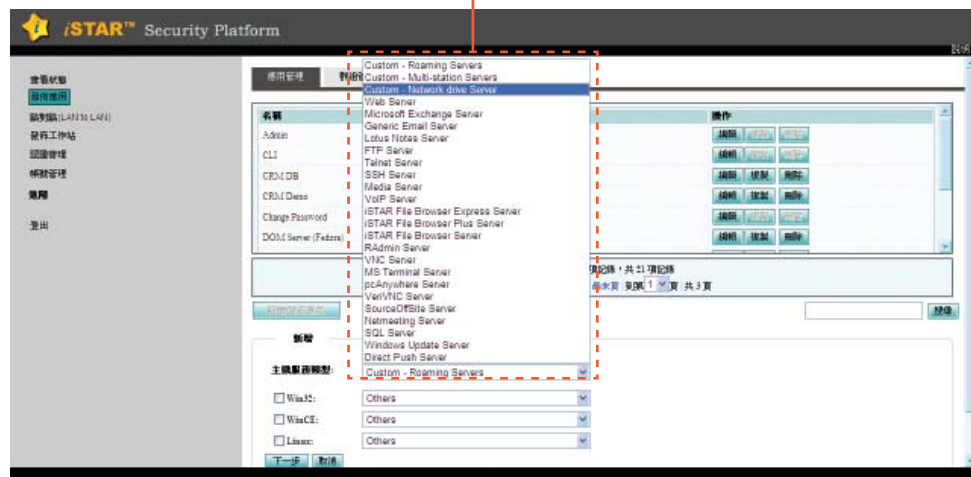


- 2 選擇是否提供使用者「預設閘道」，若選擇：
  - 「接受」則遠端使用者啟用取得IP後其default gateway將同時被設定為VPN通道
  - 「拒絕」將不修改使用者端default gateway，但使用者只能連結所取得IP的同網段IP，若需存取其他網段可搭配下方設定其他網段
- 3 選擇是否登入即啟動
- 4 點選「儲存」

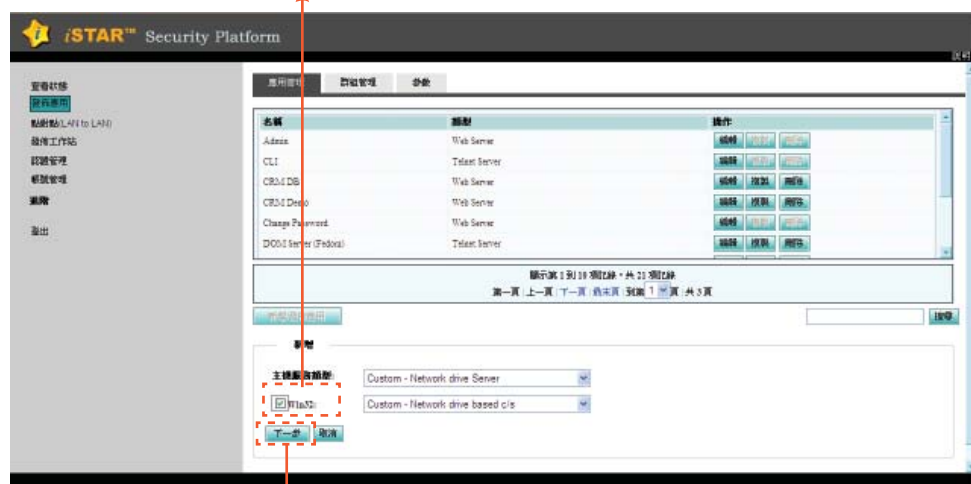


## Network Drive Server 網路磁碟

- 選擇「主機服務類型」為「Custom-Network drive Server」



- 勾選「Win32」



- 點選「下一步」

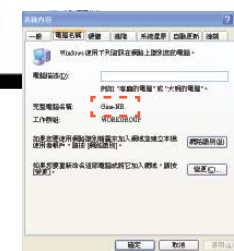
- 輸入這個應用所顯示的名稱



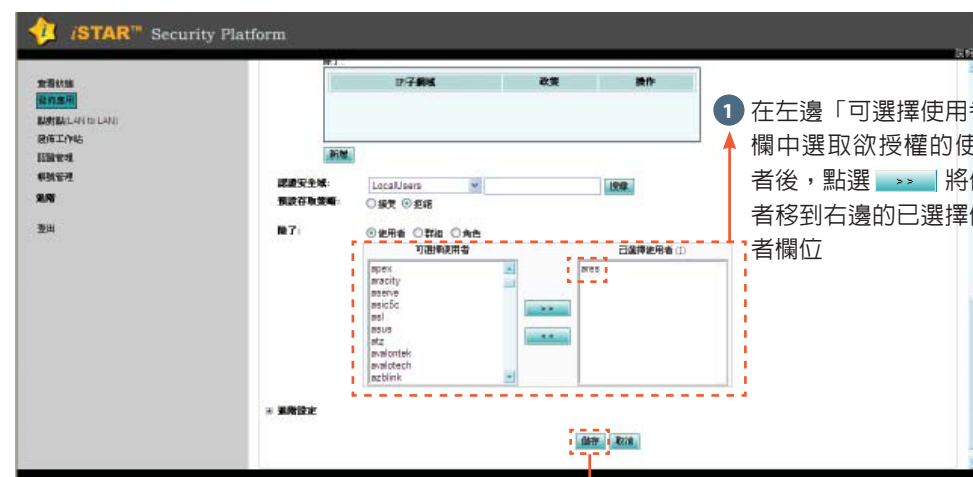
- 輸入File Server或NAS上的共享資料夾名稱，請注意此名稱為網路分享名稱，非實際資料夾名稱，而且需與server上設定完全吻合，中英文名稱不限

- 選擇使用者端掛載網路磁碟機的磁碟代號

- 輸入檔案伺服器的相關資訊：  
第一行：輸入伺服器IP位址  
第二行：輸入伺服器電腦名稱，若電腦名稱包含網域資訊，則輸入時請去除網域的部份



EX：Windows內的電腦名稱



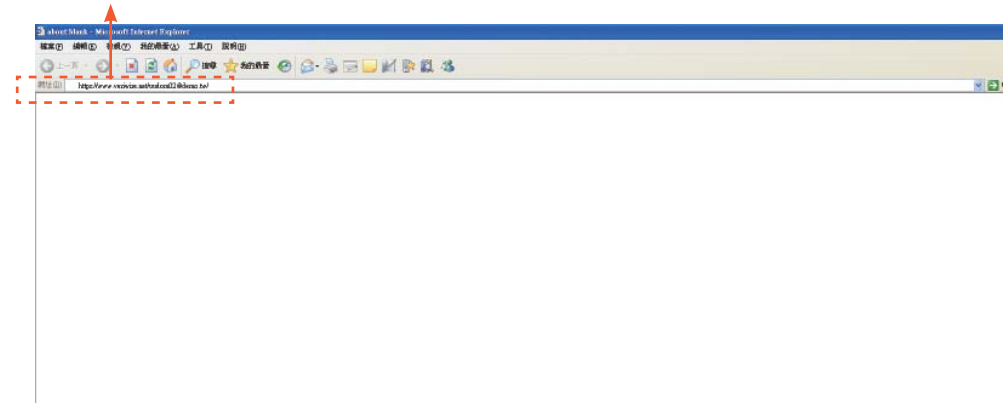
- 在左邊「可選擇使用者」欄中選取欲授權的使用者後，點選「>>」將使用者移到右邊的「已選擇使用者」欄位

- 點選「儲存」

## Step 4. 使用者遠端登入

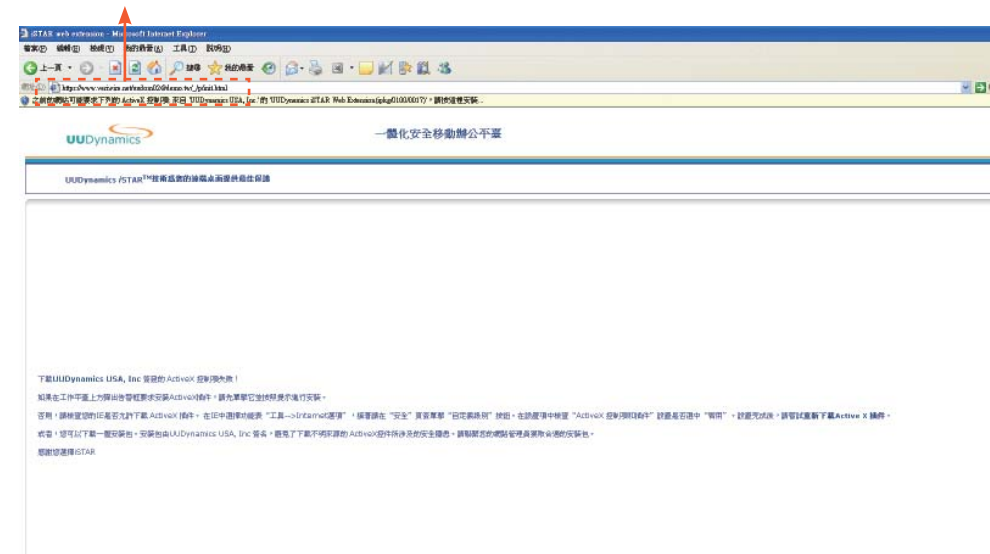
## 輸入遠端登入網址

打開IE瀏覽器，於網址列輸入「https://www.veriwire.net/UUID名稱」，請注意此處的UUID名稱，為先前於設定出廠值時匯入的UUID檔案名稱(不含副檔名)，例如UUID名稱為「uudom02@demo.tw」則於IE網址列所輸入的遠端連線網址為「https://www.veriwire.net/uudom02@demo.tw」



## 提示安裝Active X控制項

初次連結使用時系統會在網址列下方提示必須下載安裝Active X控制項

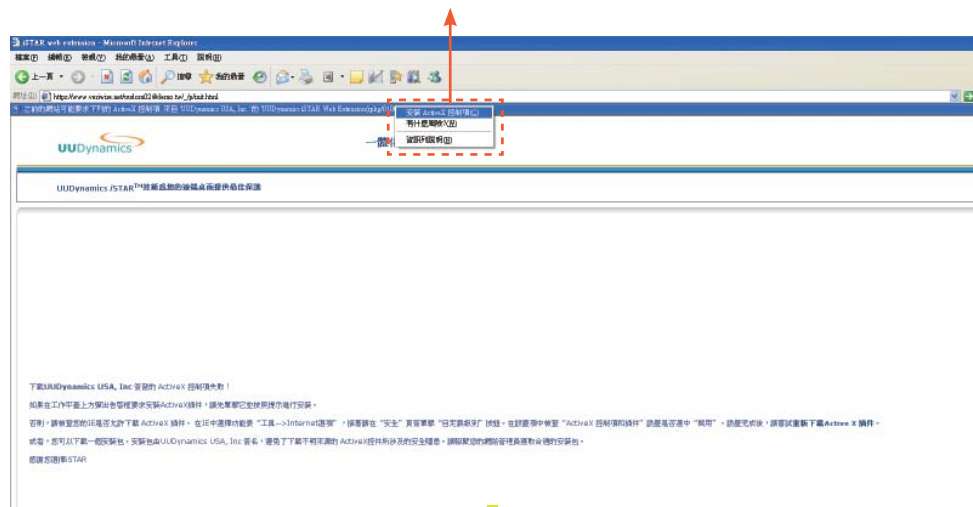


完成發佈網路磁碟



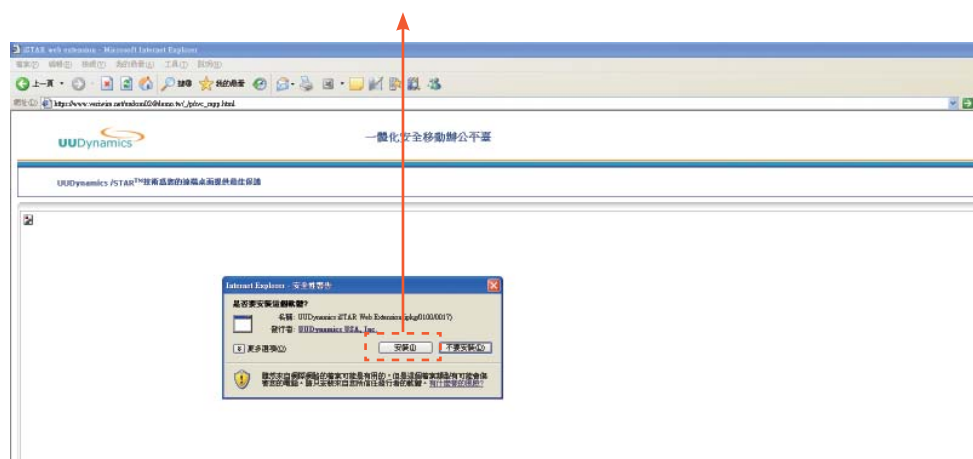
## 選擇安裝Active X控制項

於網址列下方提示訊息上按滑鼠右鍵，並點選「安裝Active X控制項(C)」



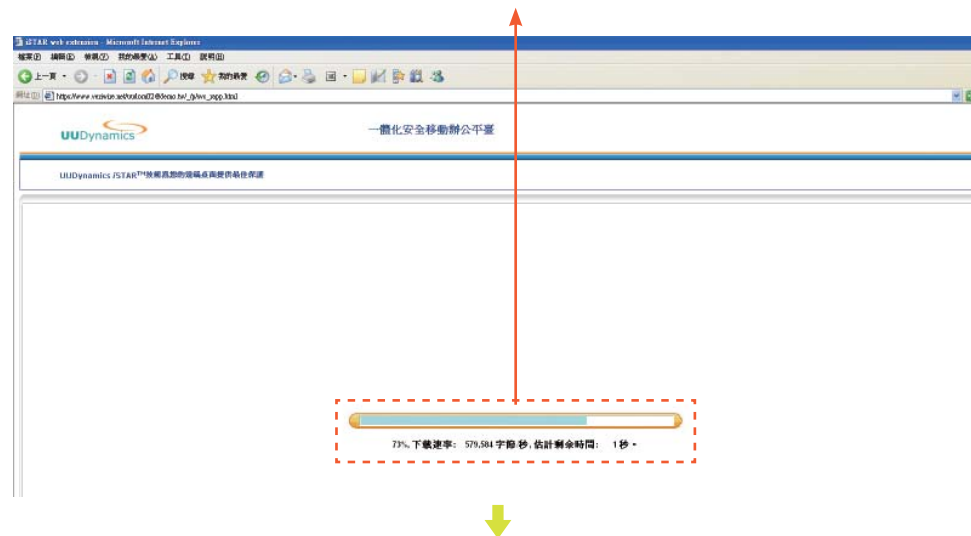
## 確認安裝Active X控制項

於所彈出的確認視窗上點選「安裝(I)」



## 安裝作業進行中

下載及安裝作業進行中，請稍待片刻

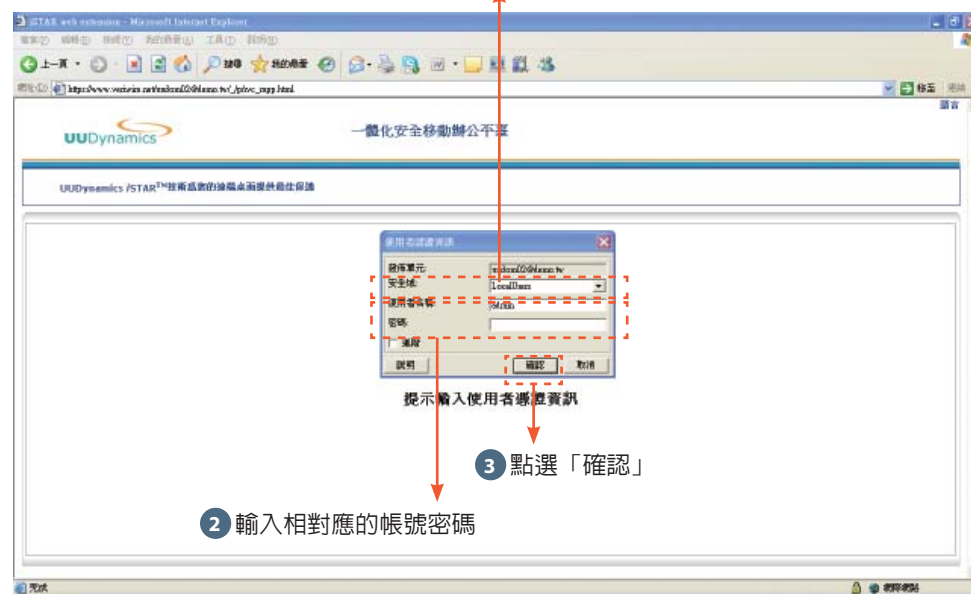


## 使用者登入

1 選擇登入的安全域



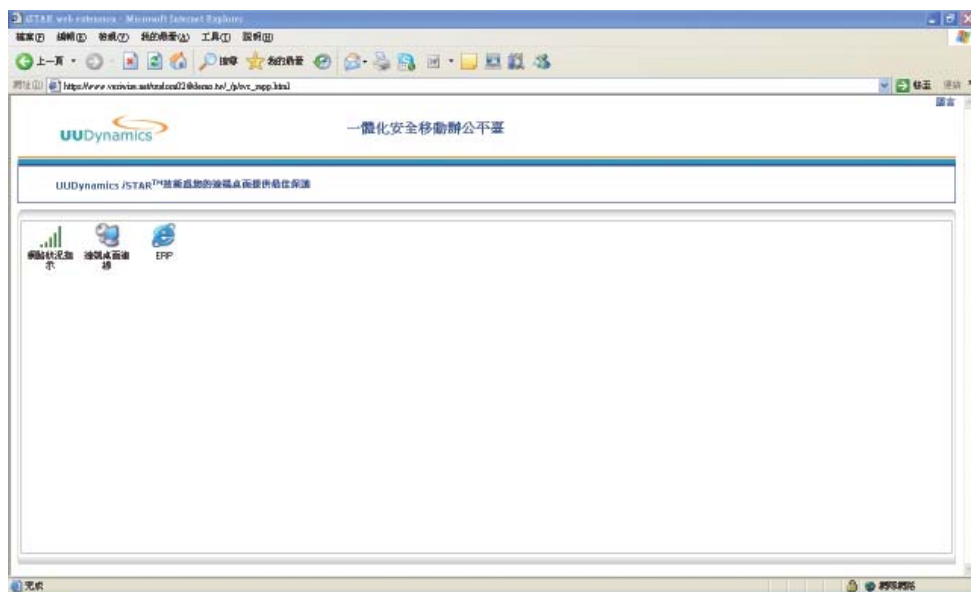
下拉選擇



2 輸入相對應的帳號密碼

3 點選「確認」

登入完成



## 附錄

## 直接連線模式

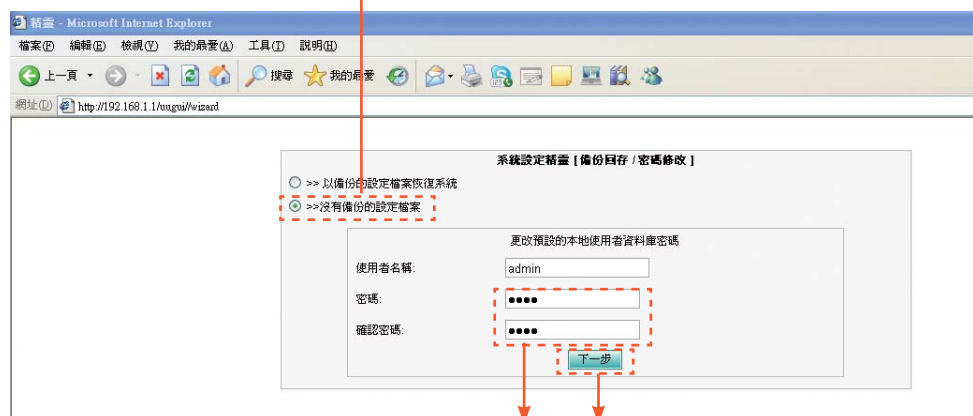
### 進入管理設定頁面

開啓用來設定的Notebook上的IE瀏覽器，於網址列輸入「1.1.1.1/admin」



### 設定admin登入密碼

1 初次設定，請選擇「>>沒有備份設定」

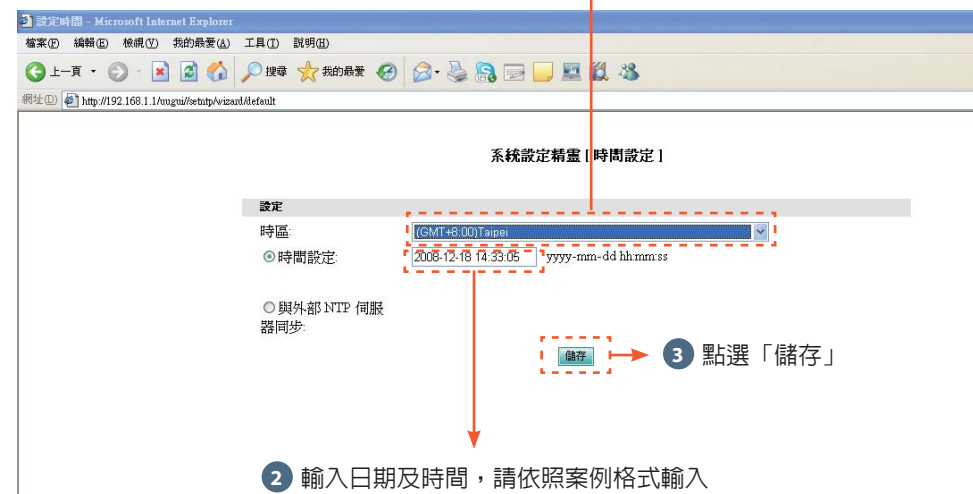


2 設定管理者(admin)的密碼

3 設定完成後點選「下一步」

### 設定系統時區及時間

1 選擇所在時區

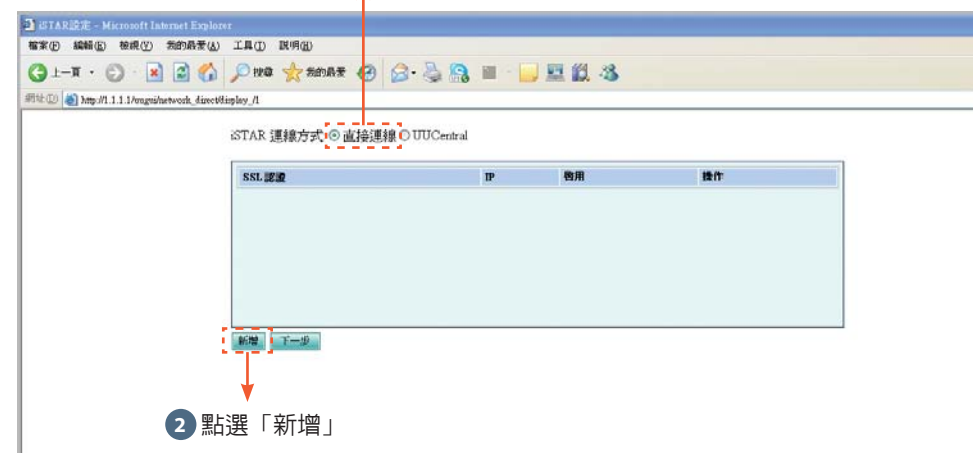


2 輸入日期及時間，請依照案例格式輸入

3 點選「儲存」

### 選擇直接連線模式

1 選擇iSTAR連線方式為「直接連線」模式



2 點選「新增」

## 建立公開憑證資訊

① 若未購買公開憑證服務(如Verisign)，請點選「新建」

③ 填入相關欄位資料

④ 點選「新建」

## 完成新建公開憑證

點選「下一步」

## 設定系統憑證(內建的CA)資訊

① 如圖輸入相關憑證資訊(一般是自訂)

② 確認所有欄位(除「描述」欄)均已正確填入後，點選「儲存」



## 設定網路資訊

- 1 選擇網路存取類型 (共有「DHCP」、「Static」以及「PPPoE」三種類型可選擇)

系統設定精靈 [區域網路設定]

系統模式: Stencilone

外部連接埠

|       |               |
|-------|---------------|
| 存取類型  | Static        |
| 工位址   | 192.168.1.120 |
| 子網路遮罩 | 255.255.255.0 |
| 網盾    | 192.168.1.254 |

DNS:

|        |            |
|--------|------------|
| 設定方式   | 手動設定       |
| DNS伺服器 | 138.95.1.1 |
| 次要DNS  |            |

3 確認「儲存成功」後點選「確定」即完成出廠值設定作業,此時系統將自動重新啟動

儲存

2 輸入相對應網路存取類型的資訊後點選「儲存」

## 登入Local管理介面

- 1 於完成出廠設定值後約10秒鐘, 開啟IE瀏覽器, 並於網址列輸入「1.1.1.1/admin」

2 輸入於出廠設定過程中所輸入的「admin」及其「密碼」, 然後點選「送出」

## 設定連接埠轉遞

3 勾選「啟用連接埠轉遞」選項

2 點選「連接埠轉遞(Port Forward)」

4 填入設備所對應的Public IP地址

5 點選「儲存」並確認顯示「儲存成功」即完成初步設定

1 於管理畫面中點選「進階」「系統」「網路設定」



## UUCentral模式

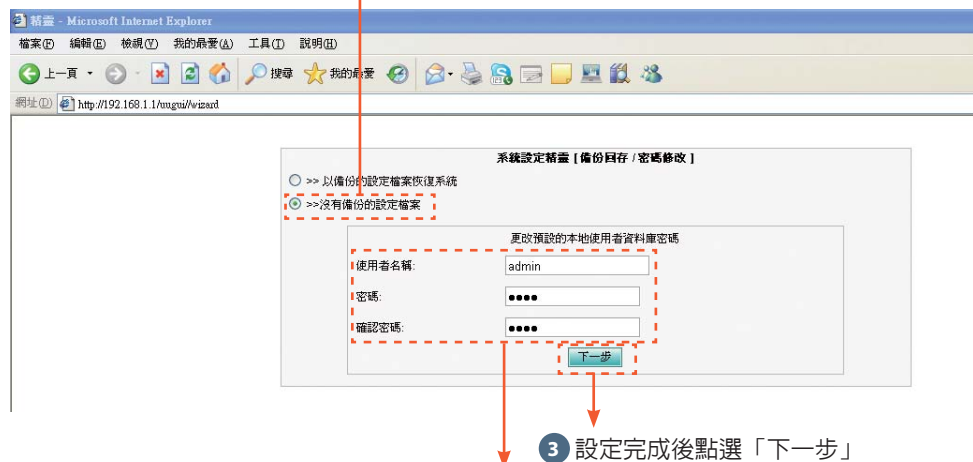
### 進入管理設定頁面

開啓用來設定的Notebook上的IE瀏覽器，於網址列輸入「1.1.1.1/admin」



### 設定admin登入密碼

1 初次設定，請選擇「>>沒有備份設定檔案」

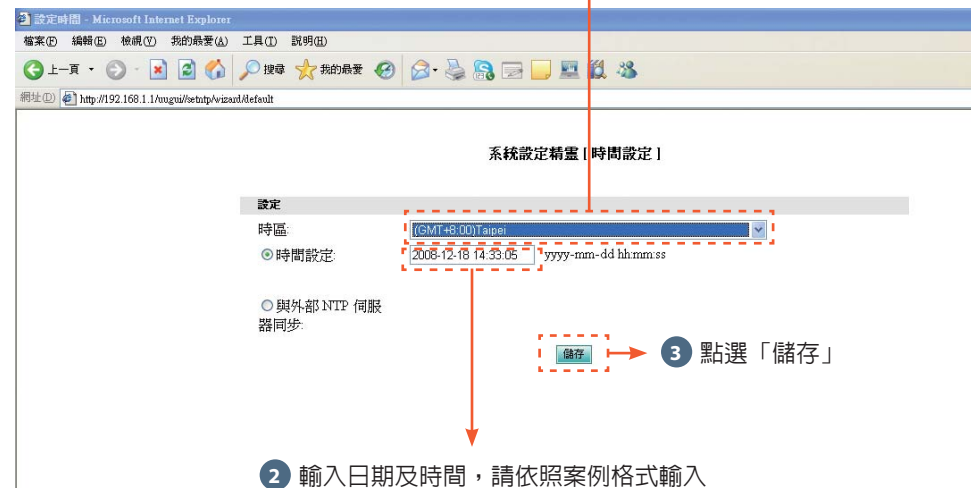


2 設定管理者(admin)的密碼

3 設定完成後點選「下一步」

### 設定系統時區及時間

1 選擇所在時區

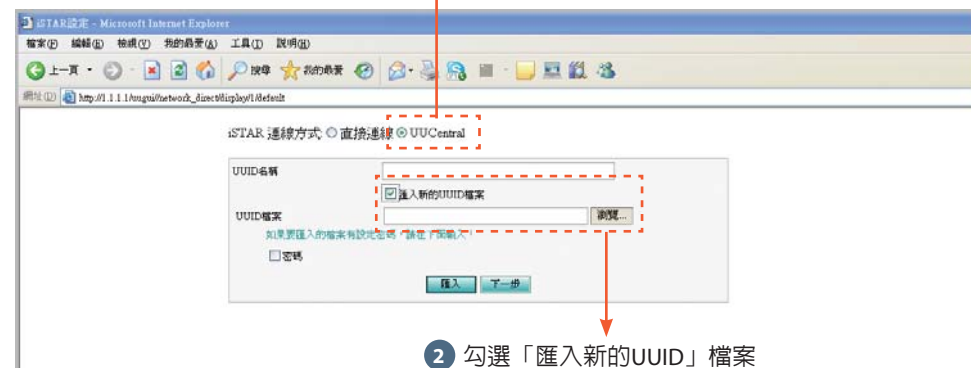


2 輸入日期及時間，請依照案例格式輸入

3 點選「儲存」

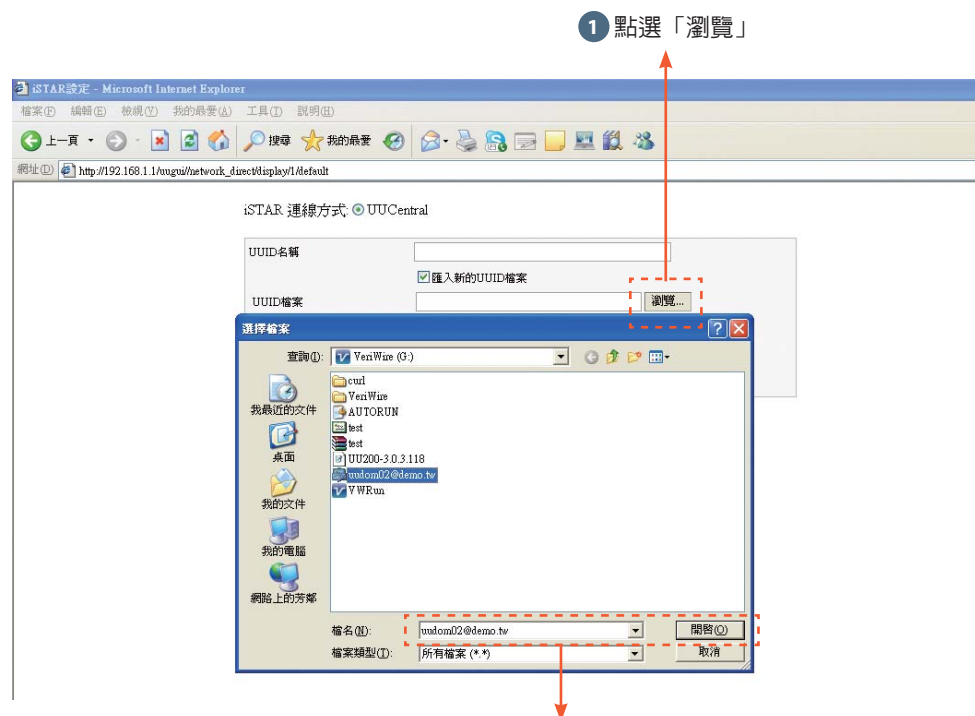
### 導入UUID檔案

1 選擇iSTAR連線方式為「UUCentral」模式

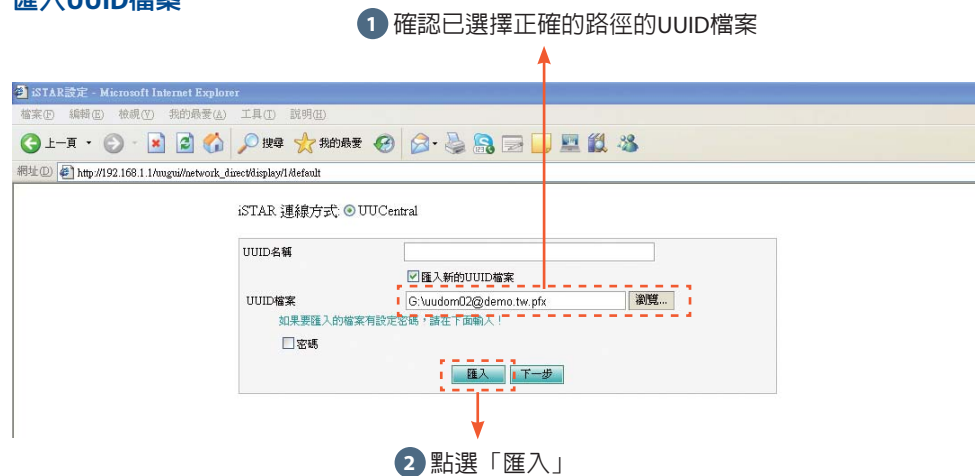


2 勾選「匯入新的UUID」檔案

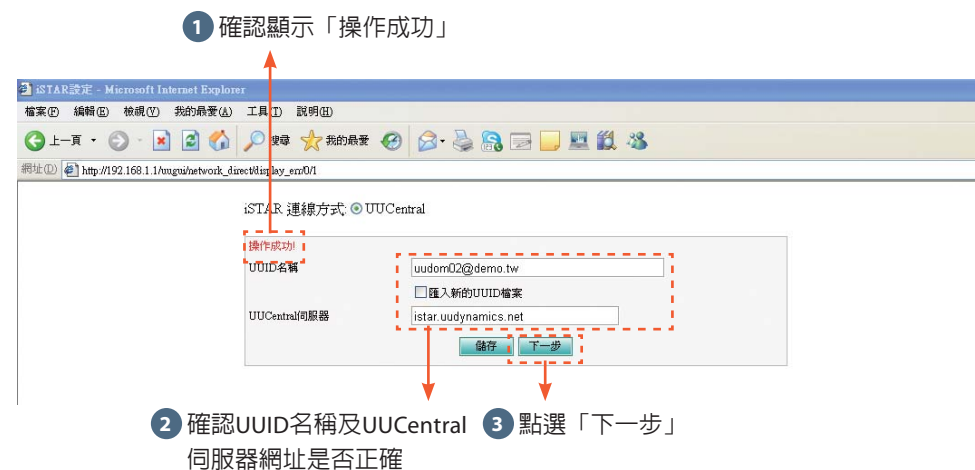
## 選擇UUID檔案



## 匯入UUID檔案



## 完成導入UUID



## 設定系統憑證(內建的CA)資訊

1 如圖輸入相關憑證資訊(一般是自訂)

2 確認所有欄位(除「描述」欄)均已正確填入後,點選「儲存」

## 選擇UUID檔案

3 確認「儲存成功」後點選「確定」即完成出廠值設定作業

1 選擇網路存取類型(共有「DHCP」、「Static」以及「PPPoE」三種類型可選擇)

2 輸入相對應網路存取類型的資訊後點選「儲存」