

# FottiOS 5.2 SSL VPN 配合 Windows AD 帳號 LDAP 認證設定說明

臺中市政府教育局資訊教育暨網路中心 沈俊達

## 壹、目的

解決在 FG-200D 上手動新增帳號及維護密碼的困境，採用與校內 AD 帳號或 LDAP 帳號結合方式來管理認證。

另一種採用 RADIUS 認證的方法，請參閱 2013 年這篇：[FG110C SSL VPN 配合 Windows AD 帳號認證設定說明.pdf](#)，因 LDAP 設定方式較簡單，如果可以建議再用 RADIUS 認證方式。

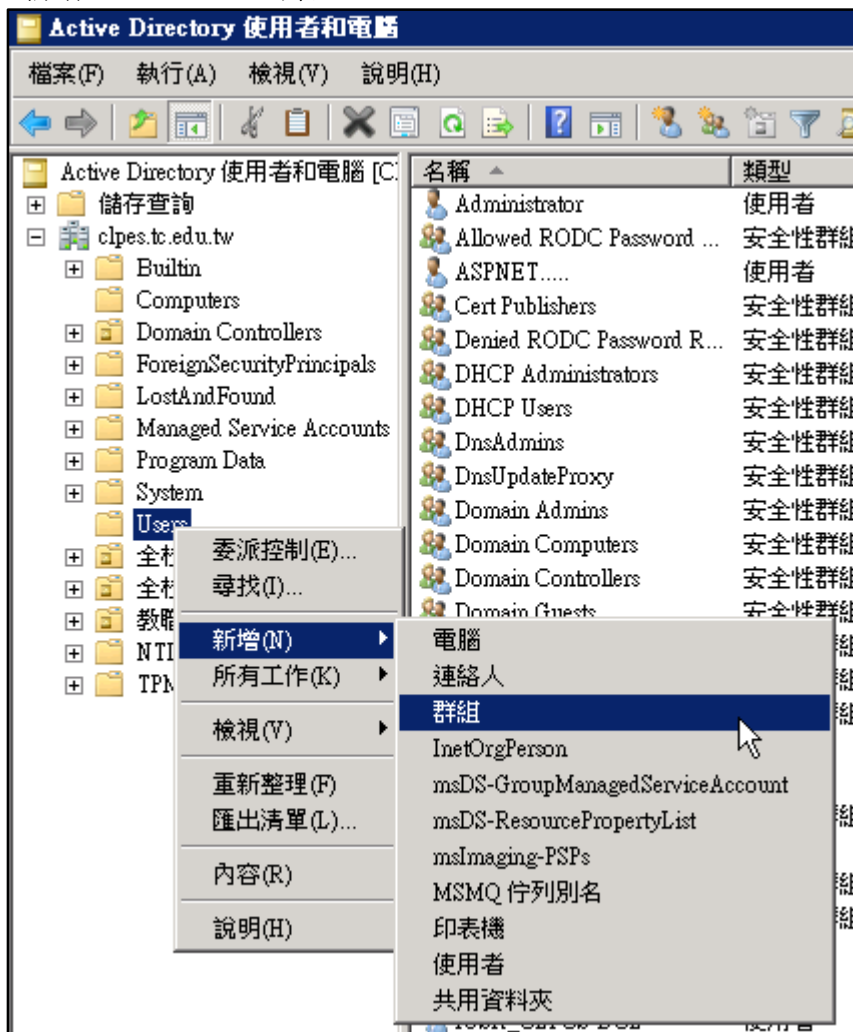
## 貳、本技術文件假定貴校已依據下面兩篇文件，完成相關設定，並已成功讓 vpndemo1 用戶可以正常登入 SSLVPN，並存取相關服務。

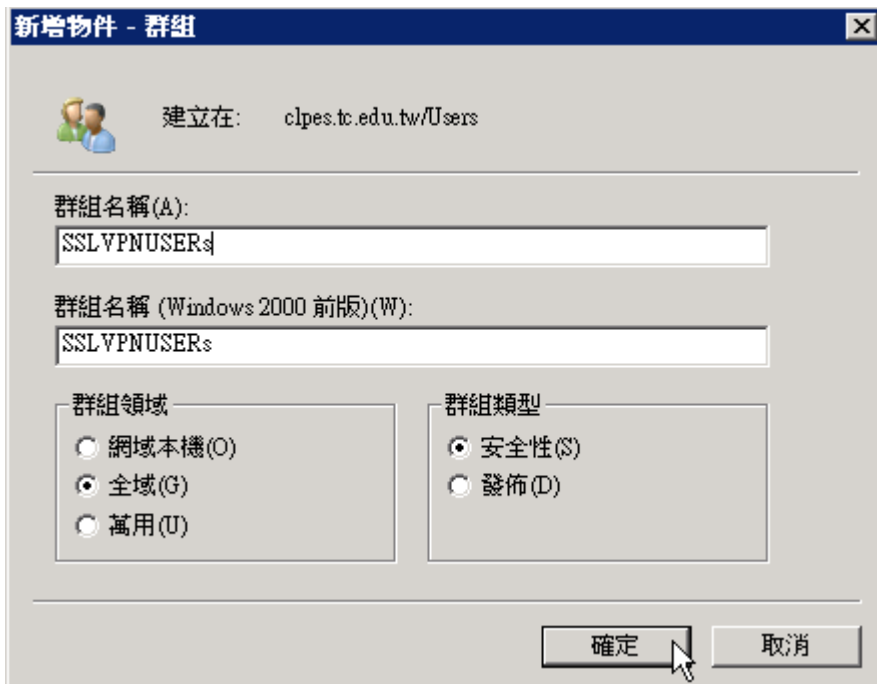
本文件重點再直接將 AD 帳號或 LDAP 帳號，加入一個新的群組，並讓此群組可以登入 SSLVPN，並存取相關服務。

## 參、DC 或 LDAP Server 上的預備動作：

建立一個新的群組，例如：SSLVPNUSERS，將要允許 SSLVPN 登入的帳號，一一加入此群組，注意是帳號，不能用群組加入群組方式。

### 一、新增 SSLVPNUSERS 群組

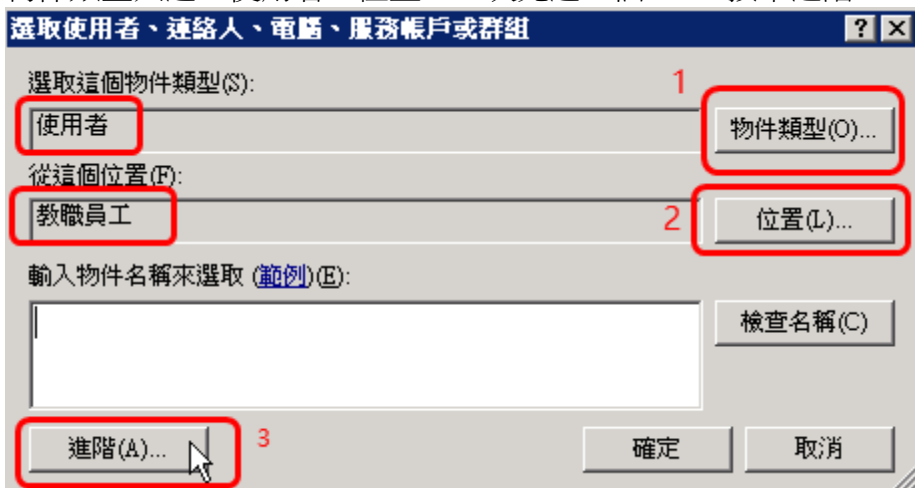




二、將允許 SSLVPN 登入的帳號，一一加入此群組



物件類型只選：使用者，位置：一次先選一個 OU，按下進階



按下立即尋找

選取使用者、連絡人、電腦、服務帳戶或群組

選取這個物件類型(S): 使用者 物件類型(O)...

從這個位置(F): 教職員工 位置(L)...

公用查詢

名稱(A): 開頭含有 [ ] 欄位(C)...

描述(D): 開頭含有 [ ] 立即尋找(N)

停用帳戶(B)

密碼不會到期(X)

上次登入至今的天數(I): [ ] 停止(T)

搜尋結果(U): [ ] 確定 [ ] 取消

將要加入的帳號複選起來，按確定

選取使用者、連絡人、電腦、服務帳戶或群組

選取這個物件類型(S): 使用者 物件類型(O)...

從這個位置(F): 教職員工 位置(L)...

公用查詢

名稱(A): 開頭含有 [ ] 欄位(C)...

描述(D): 開頭含有 [ ] 立即尋找(N)

停用帳戶(B)

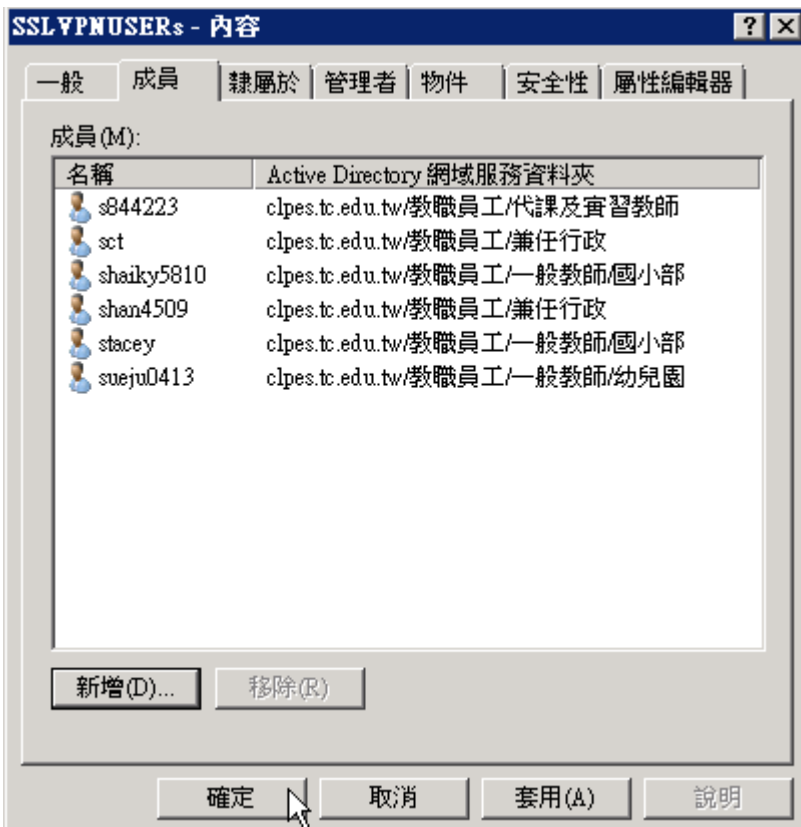
密碼不會到期(X)

上次登入至今的天數(I): [ ] 停止(T)

搜尋結果(U): [ ] 確定 [ ] 取消

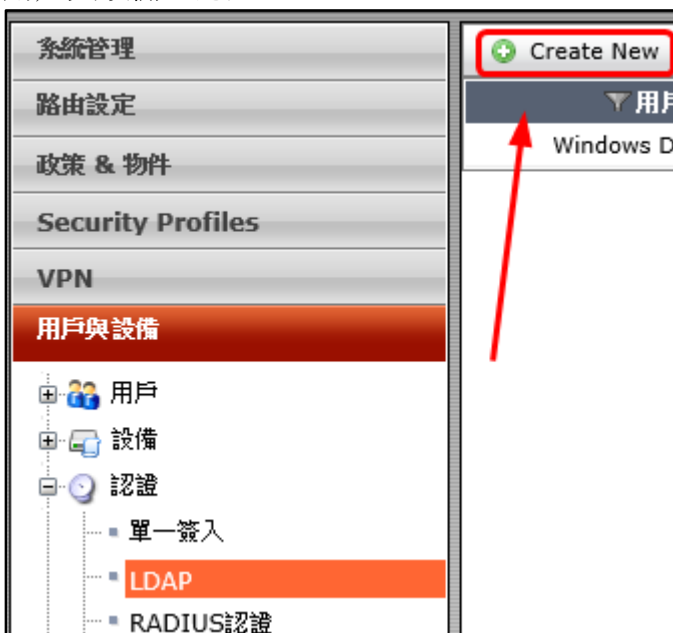
名稱 (RDN)	電子郵件地址	在資料夾
S5276ABD		clpes.tc.edu.tw/...
s844223		clpes.tc.edu.tw/...
sammi80820		clpes.tc.edu.tw/...
sandy		clpes.tc.edu.tw/...
school		clpes.tc.edu.tw/...
sct	sct@tc.edu.tw	clpes.tc.edu.tw/...
shaiky5810		clpes.tc.edu.tw/...
shan4509		clpes.tc.edu.tw/...
stacey		clpes.tc.edu.tw/...
sueju0413		clpes.tc.edu.tw/...

繼續新增帳號，或按確定離開



肆、FG-200D 的設定

用戶與設備→認證→LDAP→Create New



設定一個用戶名稱，例如 Windows DC LDAP，並輸入 DC 的 ip 位址  
可識別名稱填入 AD 網域的 LDAP 路徑

Bind Type 選擇：正規模式

使用者 DN 及密碼：請填一個擁有讀取 AD 帳號內容權限的帳號及密碼，如果要用 Administrator 的話，標準路徑是：CN=Administrator,CN=Users,DC=clpes,DC=tc,DC=edu,DC=tw

完成後請按「讀取 DN」及「測試」都會出現成功訊息。  
最後請按確定，完成。

用戶名	Windows DC LDAP
主機名稱/IP	163.17.89.129
伺服器埠口	389
通用名稱標識	cn
可辨識名稱	dc=clpes,dc=tc,dc=edu,dc=tw
	<input type="button" value="讀取 DN"/>
Bind Type	<input type="radio"/> 簡單模式 <input type="radio"/> 匿名 <input checked="" type="radio"/> 正規模式
使用者 DN	CN=sct,OU=兼任行政,OU=教職員工,DC=clpes,DC=
密碼	●●●●●●
<input type="checkbox"/> 安全連線	
<input type="button" value="測試"/>	
	<input type="button" value="確定"/>

伍、把 AD 帳號加入 vpndemo\_users 群組

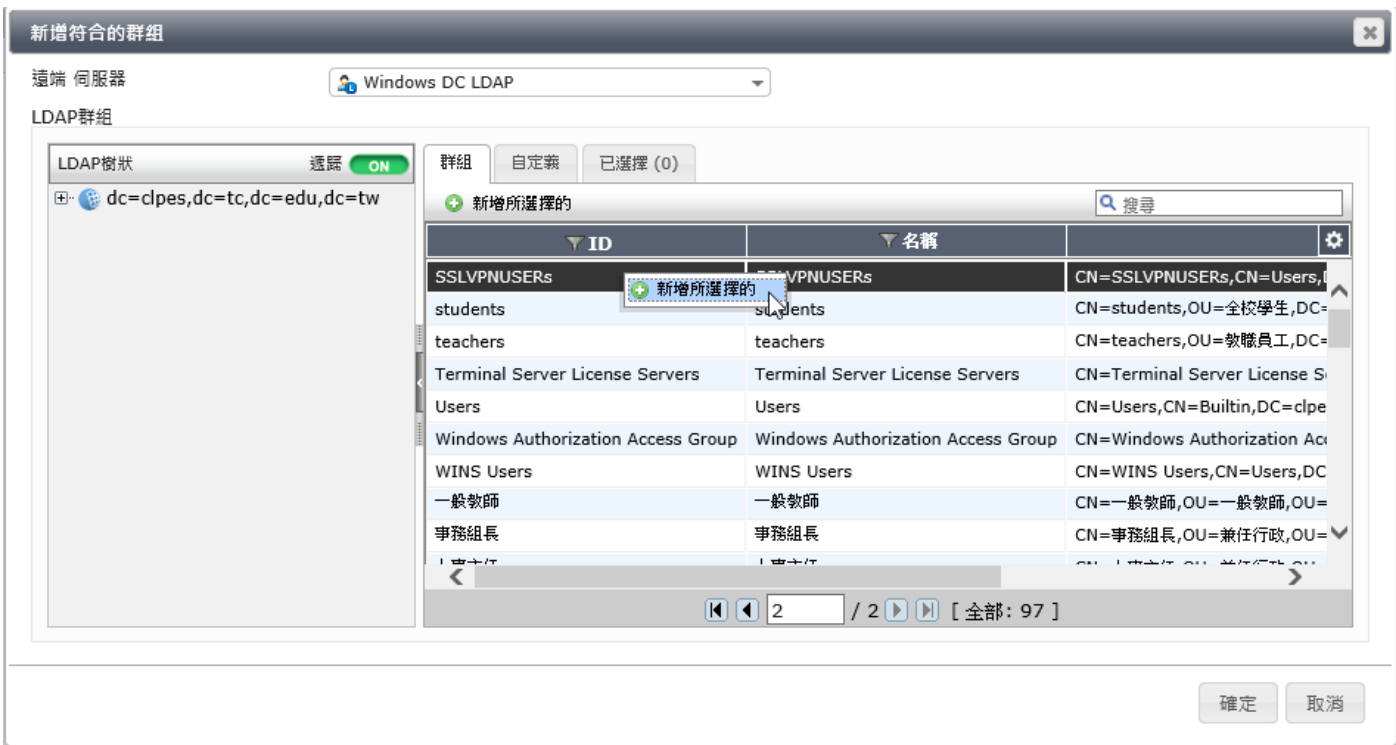
操作步驟：編輯之前建立的 vpndemo\_users 群組，按 Create New

用戶名	vpndemo_users
類型	<input checked="" type="radio"/> 防火牆 <input type="radio"/> Fortinet單一簽入(FSSO) <input type="radio"/> 訪客 <input type="radio"/> RADIUS單一簽入(RSSO)
成員	<input type="button" value="vpndemo1"/>
遠端群組	<input checked="" type="button" value="Create New"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
遠端伺服器	
沒有找到符合的項目	
<input type="button" value="確定"/> <input type="button" value="取消"/>	

遠端伺服器下拉選單點選剛剛建立的 Windows DC LDAP

新增符合的群組	
遠端 伺服器	<input type="text"/>
群組	<input type="text" value="請選擇..."/> <ul style="list-style-type: none"> <li>LDAP</li> <li><input checked="" type="radio"/> Windows DC LDAP</li> <li>RADIUS</li> <li><input type="radio"/> DC</li> </ul>

分頁尋找到剛剛在 DC 上建立的 SSLVPNUSERS 群組，按滑鼠左鍵一下選「新增所選擇的」，然後按下確定



完成遠端群組加入 FG-200D 的 vpndemo\_users 群組，按確定離開



陸、現在只要是 AD 帳號隸屬於 SSLVPNUSERS 群組的，都可以使用 SSLVPN 連線了！您可以開放所有老師，國中為了十二年國教也可以開放學生使用。

但建議學生部分建一個獨立的 Web-only 門戶網站，只提供一個書籤連到學務系統即可。

教師部分另建一個或多個門戶網站，是各校需求設定 Web-only 或 Tunnel Mode。

此部分細節，爾後辦理研習時，再實作給大家練習。