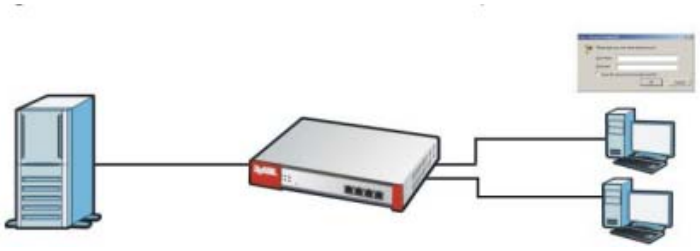
USG 韌體版本 2.20， SSL 結合 LDAP server 驗證設定範例



範例: LDAP server 資訊

LDAP Server:10.100.100.50 建立的群組 Group(有 CSO、sales 群組)

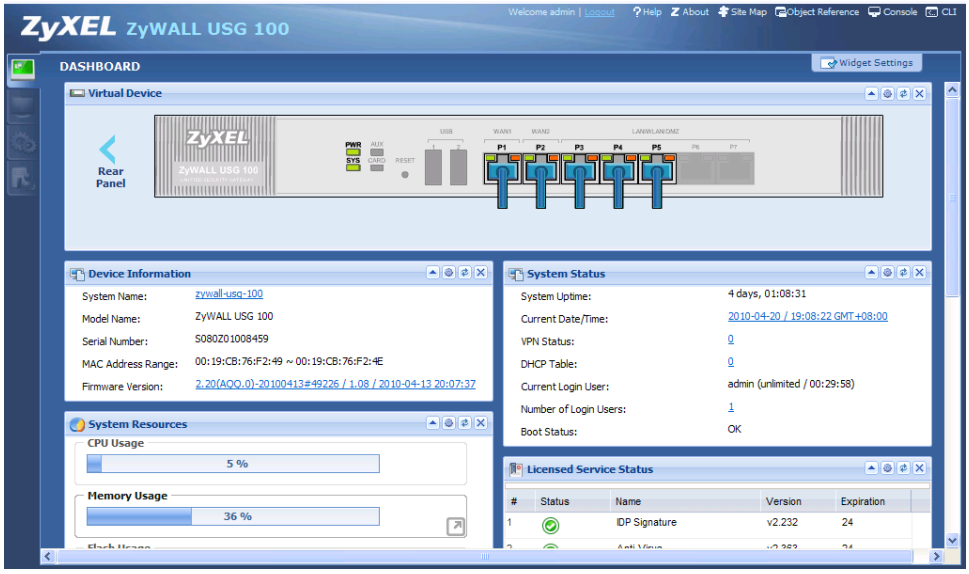
Sales 群組成員(anney) CSO 群組成員 (jones,thomas) 該網域的管理者 manager

名稱解釋：		
Base DN	指的是 LDAP/Windows AD 的搜尋的物件的儲存路徑的啓始位置. 如需跟 nwa.idv.tw 網域中的使用者驗証或特定群組 Base DN 爲(ou=users,dc=nwa,dc=idv,dc=tw)	
Bind DN	需要輸入儲存”足夠管理網域的使用者權限”物件的儲存路徑,用於與 AD or LDAP 連線授權用． (cn= leopard , dc=nwa,dc=idv,dc=tw) 注意的是如果此處的使用者帳號沒有足夠的權限的話 ，那此 LDAP Client 是無法認證 User 的	
LDAP 中 Attribute	UID	的指使用者名稱
	OU (OrganizationalUnitDN)	OU 是一種 Active Directory 容器，您可以在其中放置使用者、群組、電腦及其他 OU。OU 無法包含其他網域中的物件。
	UPN (userPrincipalName)	指的登入網域 mail，如 manage@nwa.idv.tw
	CN(Display Name)	使用者名稱_*UserDN* 的一般名稱 (CN) 值中的最多前 20 個字元, 指定安全性帳戶管理員 (SAM) 名稱做爲此使用者的唯一帳戶名

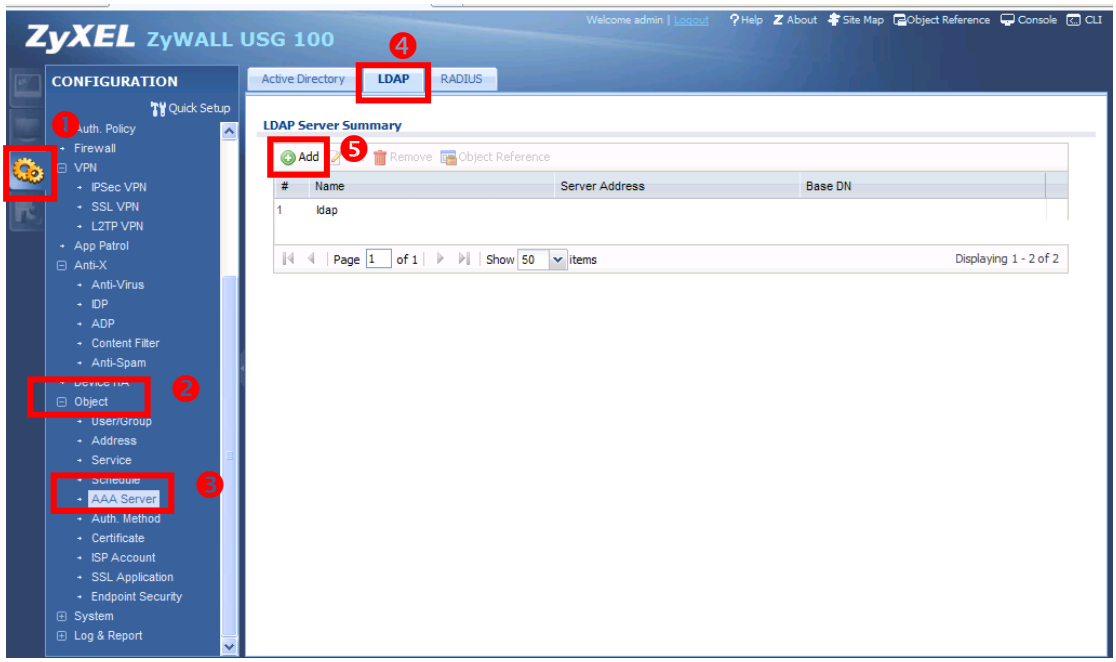
設定五大要點：

1. 檢查韌體版本
2. 設定 LDAP Server 資訊
3. 設定帳唬登入時，所查詢的帳號資料庫。
4. SSL VPN→設定存取規則
   (可存取的使用者/群組、配置登入的使用者 IP 位址、可存取的資源)
5. Zone 的設定 SSL_VPN 的應用規則

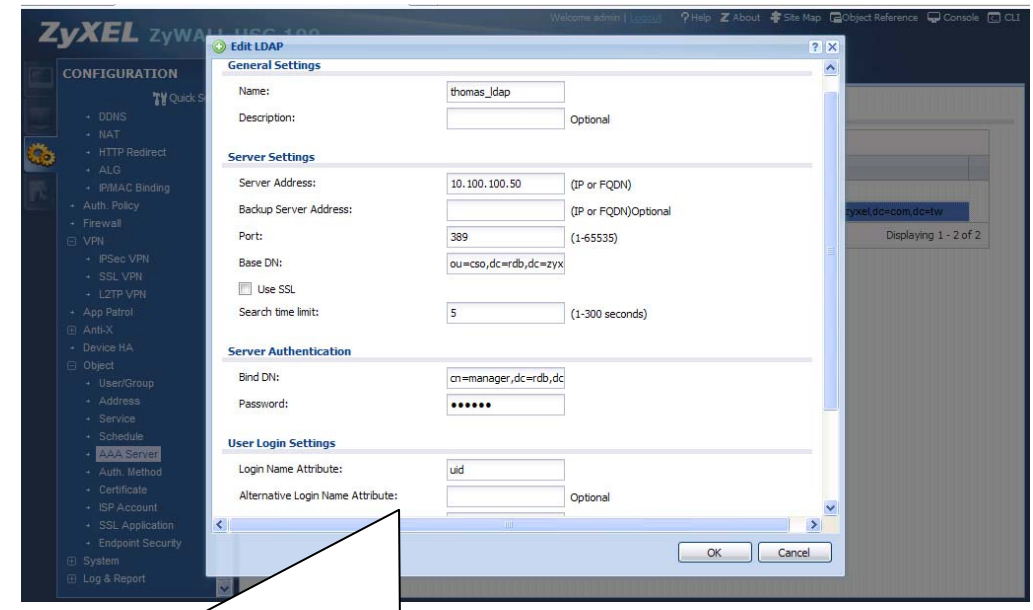
步驟一：確認韌體版本爲：2.20 版本

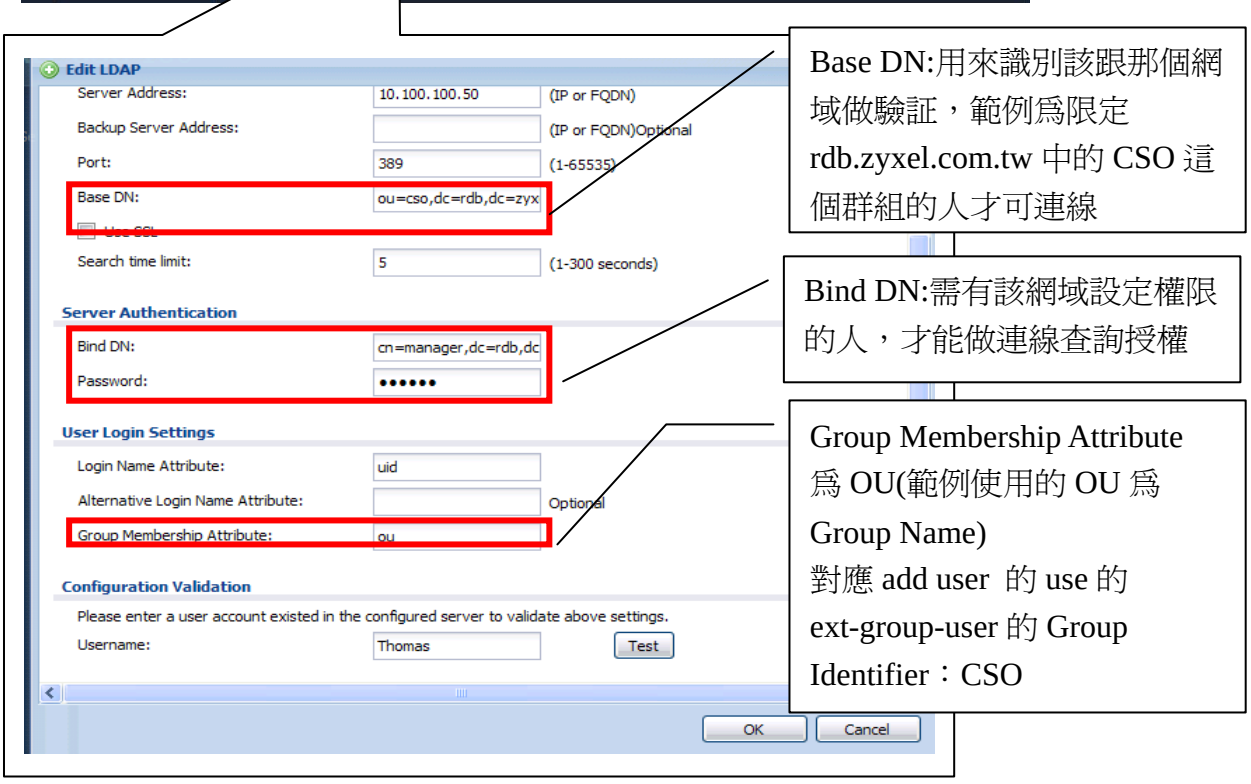


步驟二：以 LDAP 爲範例，❶先點選 Configuration→❷點選 Object(物件)→ ❸點選 AAA Server→點選❹ LDAP →❺點選 Add，手動建立新的驗證規則，名稱爲 thomas_LDAP。

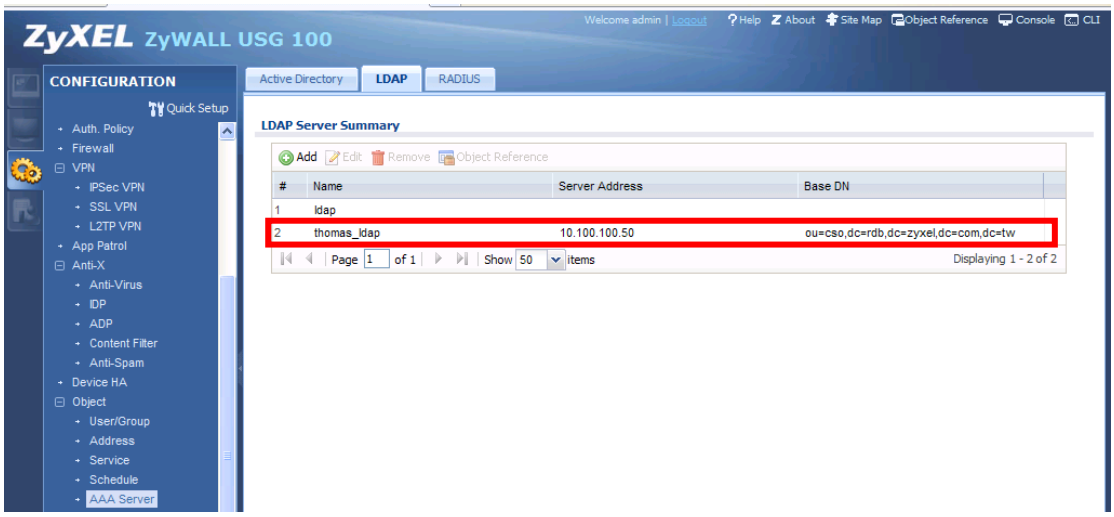


步驟三：手動建立新的驗證規則，輸入 LDAP 相關資訊，名稱爲 thomas_LDAP





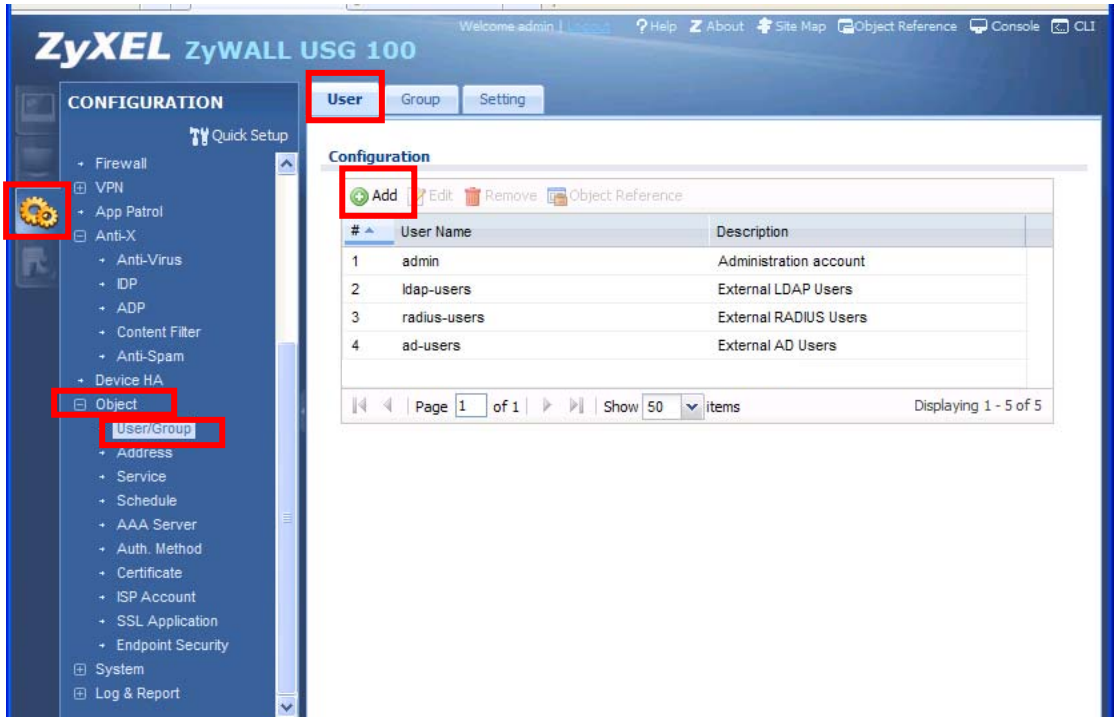
步驟四：確認建立 LDAP 驗證規則爲成功。



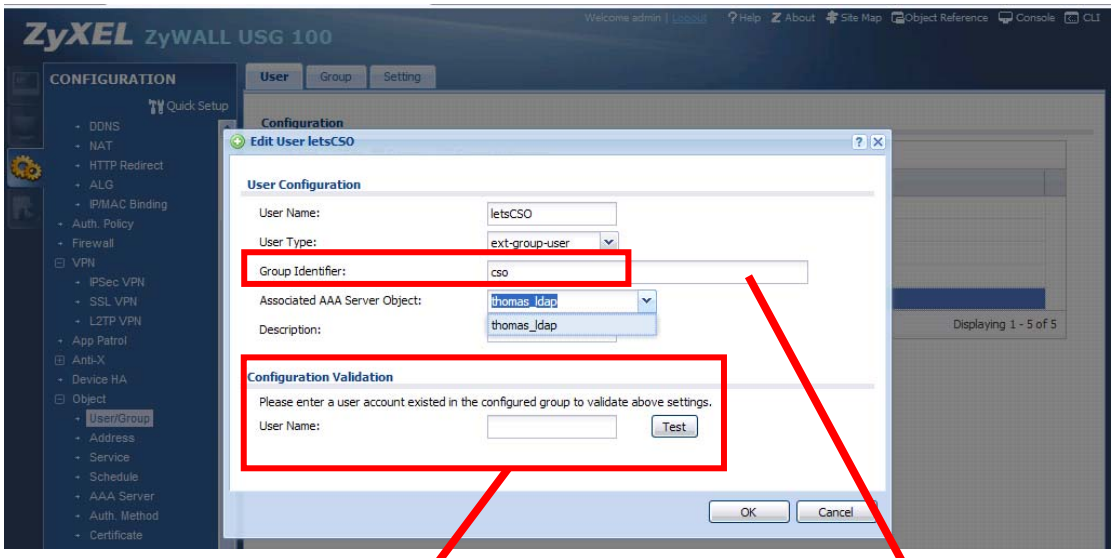
設定登入帳號的驗証方式，在 USG 提供使用者登入的驗證方式有四種：

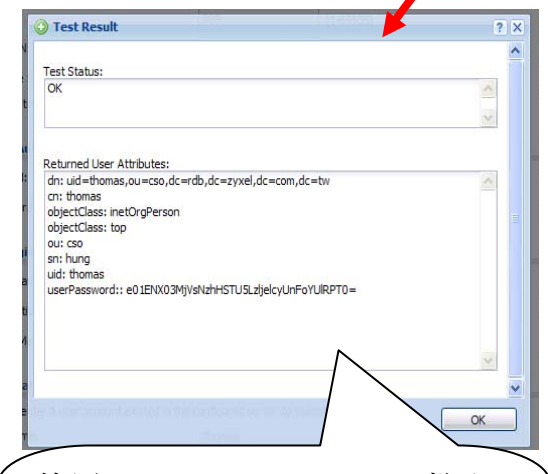
1. USG 設備中的建立的使用者帳號
2. 與網路中的 AD 伺服器進行驗證
3. 與網路中的 LDAP 伺服器進行驗證
4. 與網路中的 RADIUS 伺服器進行驗證

步驟五：若在 AAA server 是自己手動建的規則，非修改原本預設 ldap 規格名稱，則需手動建立一個新使用者，點選❶Configuration→❷點選 Object(物件)→ ❸點選 User/Group→❹點選 User→ ❺點選 Add



步驟六：手動建立一個新使用者（User Name 僅用於識別該群組作用），此使用者用於與 AAA Server 中 LDAP 驗證查詢的資料庫使用，User type 需選 ext-group-user，Associated AAA Server Object 需套用在 AAA Server-LDAP 手動建立規則的名稱(此範例 thomas_ldap)，Group Identifer 的值需對應 AAA server 的 Base DN 的值 及 Group Membership Attribute 使用的識別(object Attribute)再按下 ok 鈕



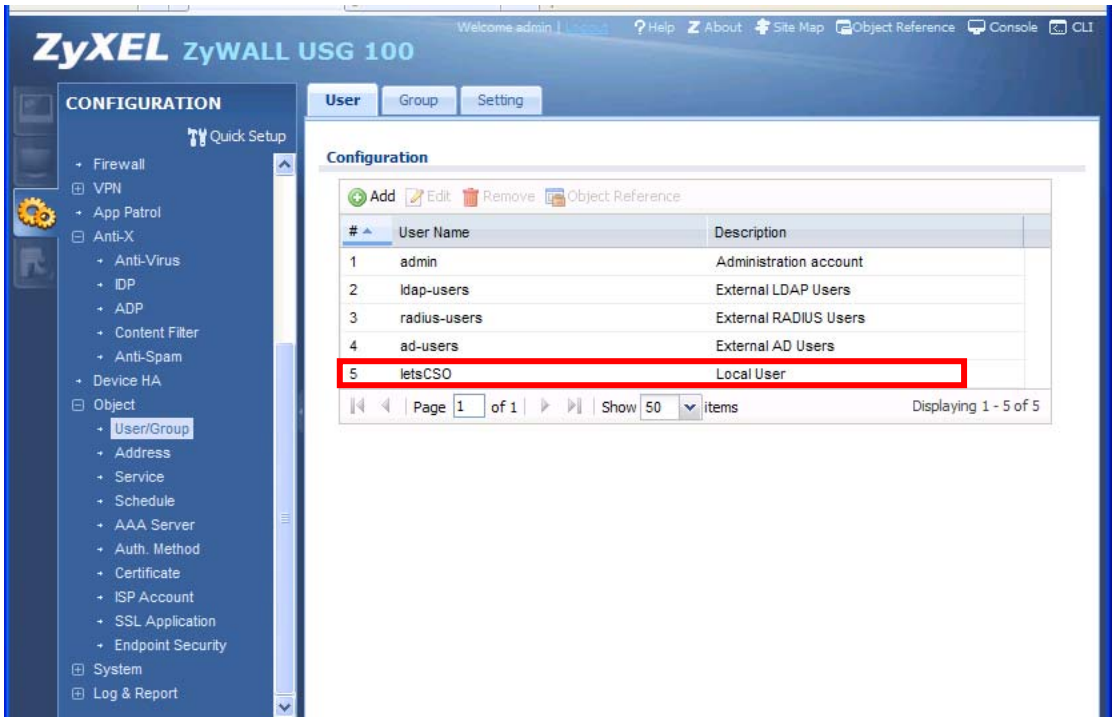


使用 configuration validation 輸入一個 LDAP server 上 CSO 群組的成員，此範例我們輸入 thomas 來驗證測試。

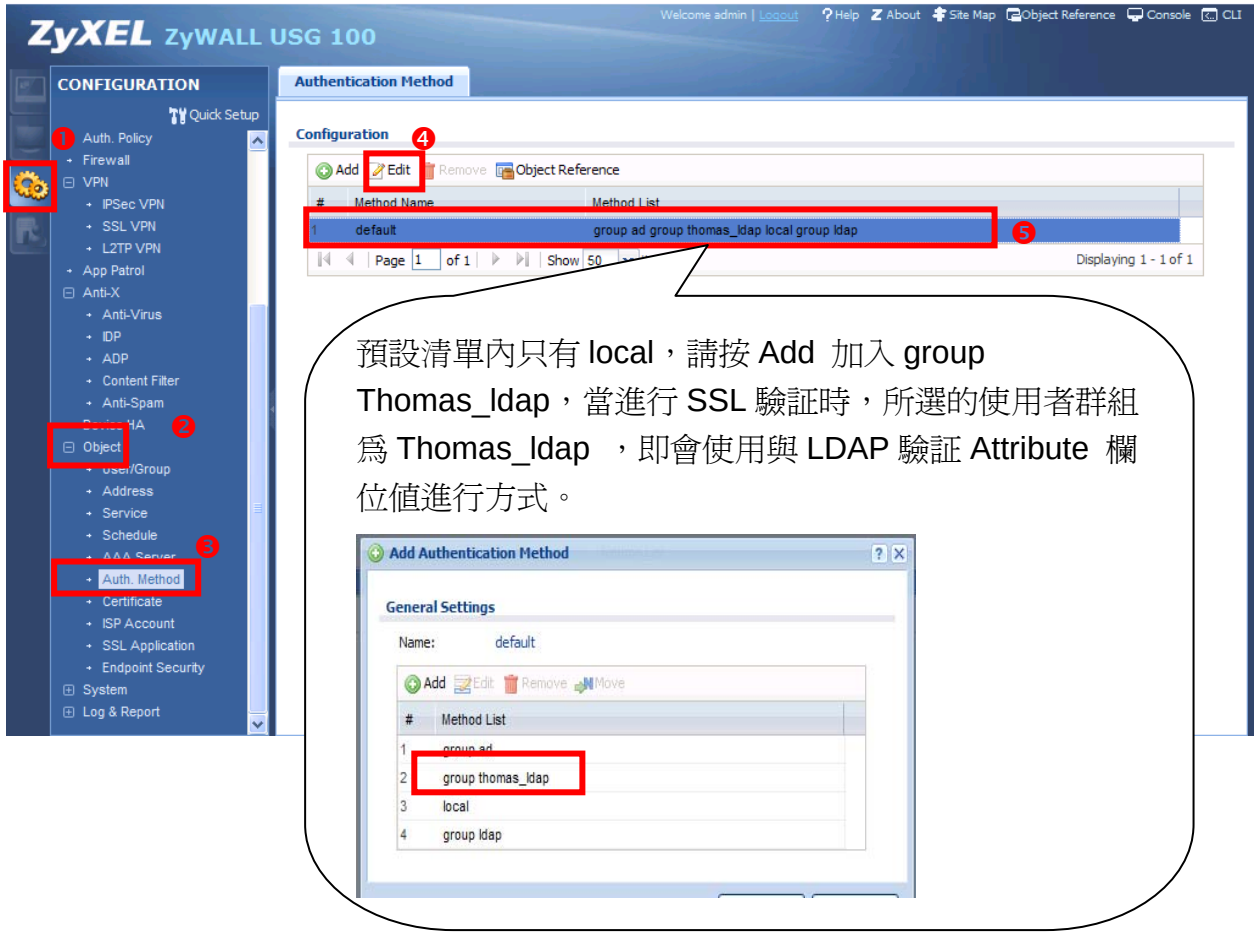
Group identifier 需對應 AAA server 的 Base DN 的值 及 Group Membership Attribute 使用的識別(object)。

此範例我們在 LDAP server 上 group 有 sales and cso，但在 USG 系列 AAA server 的 LDAP 的 Base DN 是 ou=cso， Group Membership Attribute 所輸入爲 OU，故此 Group Identifier 需輸入的 CSO。

步驟七：確認所建立的使用者。



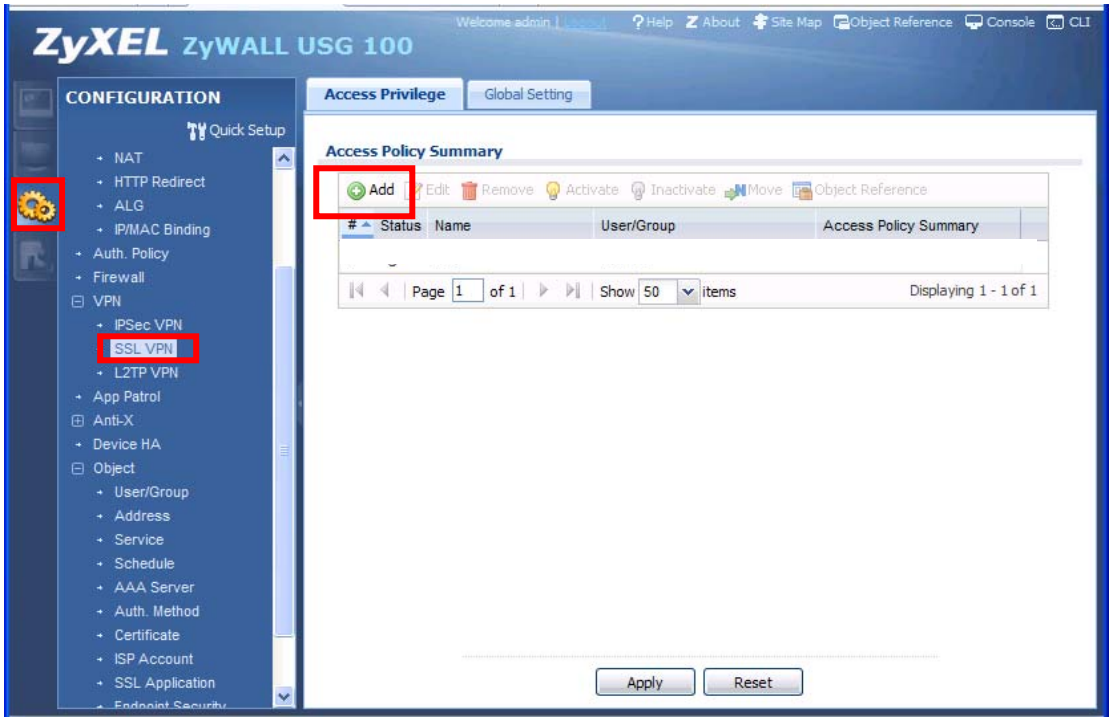
步驟八：點選❶Configuration→❷點選 Object(物件)→ ❸點選 Auth. Methood→❹點選 default 此筆 →❺點選 edit 此筆進行編輯。



SSL VPN 設定

SSL VPN 爲讓出差在外的使用者從遠端，透過網際網路使用安全的加密方式來存取內部資源，在無需安裝額外特定程式，使用瀏覽器即可連入 USG 並進行帳號驗證。

步驟九：USG VPN 的 SSL 的 VPN 規則設定，新增一筆 SSL 的規則，請點選 ❶Configuration→❷點選 VPN→ ❸點選 SSL VPN→❹點選 Add

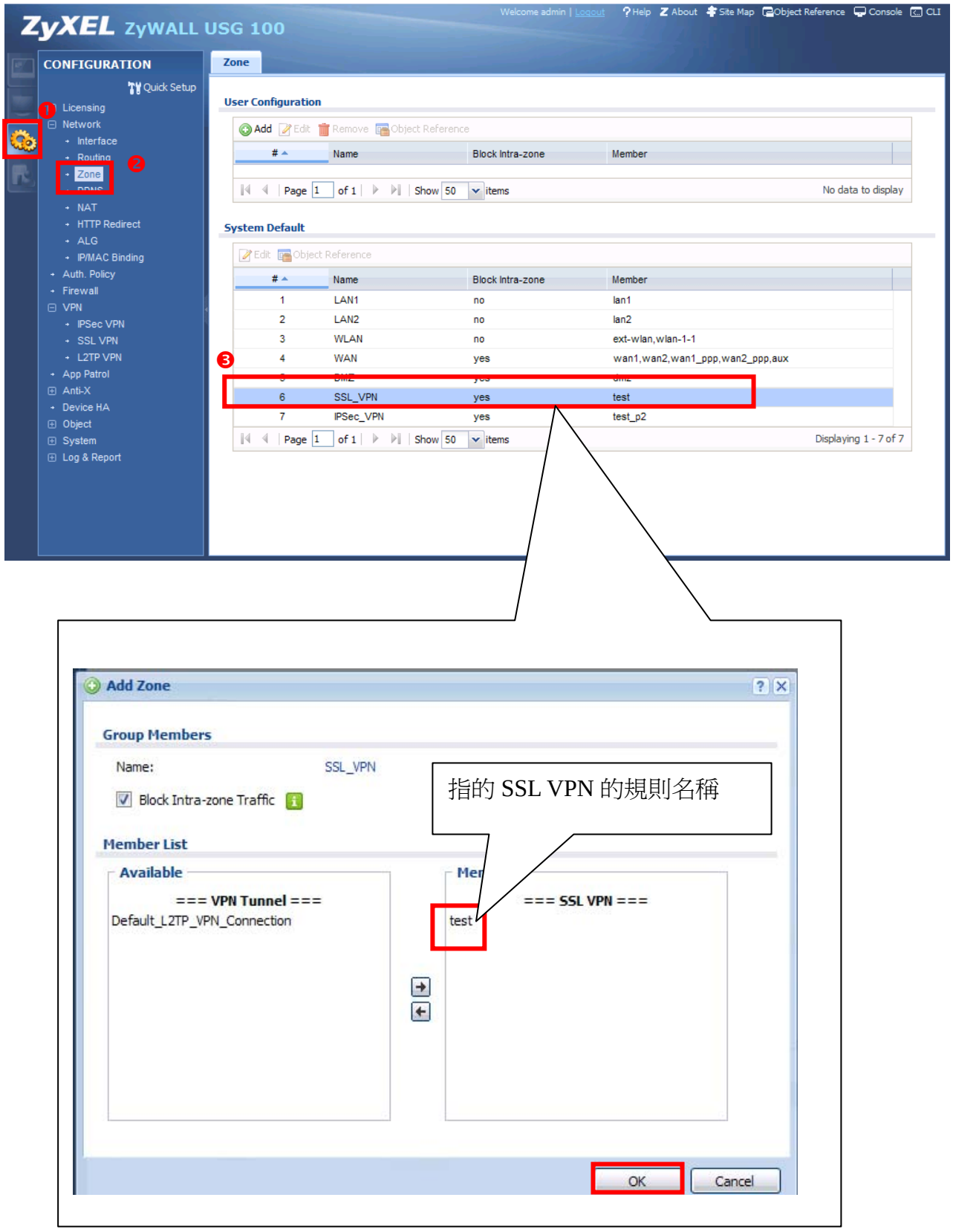


步驟十：建立 SSL 存取的規則名稱，建議易於識別如:AAA_user_access (此範例：暫將規則名稱爲 test)

若用的是 AAA Server default 規則設定的，請將 ldap-users 群組加入到右列清單，此範例爲自己建立 AAA Server 中的 LDAP 驗証規則，故需選取已套用自己建立與 LDAP 規則驗証的使用者名稱(此範例：lets-CSO)

請將 lets-CSO 加入到右列清單，並於 Network extension 配置 SSL 登入的使用者網段 IP 及 SSL 登入可存取的網路資源。

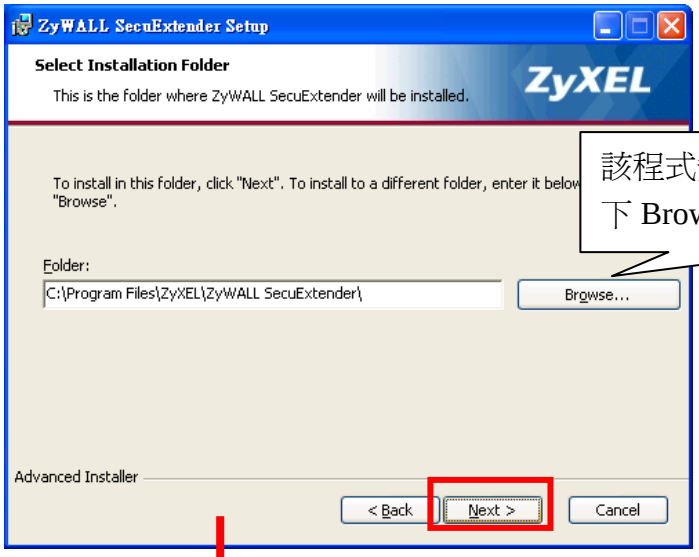
步驟十一：點選❶Configuration→❷點選 Network→ ❸點選 Zone→點選 SSL_VPN 中確認是否有加入的 VPN→SSL VPN 新增一筆 SSL 的規則名稱(此範例爲 test)



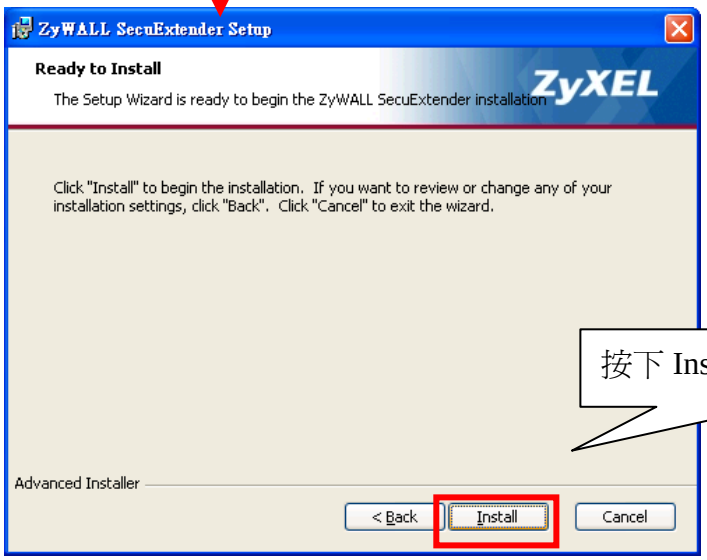
步驟十二：驗証設定是否正確，使用登入帳號爲 AD Server 上的帳號，輸入使用者帳號及密碼並點選 SSL 登入。

步驟十三：在登入後 **SSL**，需安裝 Active x 並請允許執行 **JRE(jave runtime 環境)**。

步驟十四：請安裝附加元件。



該程式安裝在電腦上的位置，可按下 Browse 來變更路徑。



按下 Install 開始進行安裝。

按下 Finish 完成安裝並關閉此視窗。

在電腦工作列上即可看到您取得的 IP 位置