採用PEAP/GTC WPA的Cisco安全服務客戶端配置示例

目錄

簡介

本檔案介紹如何在思科安全服務使用者端上設定受保護的可擴充驗證通訊協定(PEAP)/通用權杖卡(GTC)Wi-Fi保護存取(WPA)。

必要條件

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科安全服務使用者端版本4.0可從Cisco.com Software Center（僅限註冊客戶）下載Cisco Secure Services Client。
- Windows XP SP2或2000 SP 4（最少）

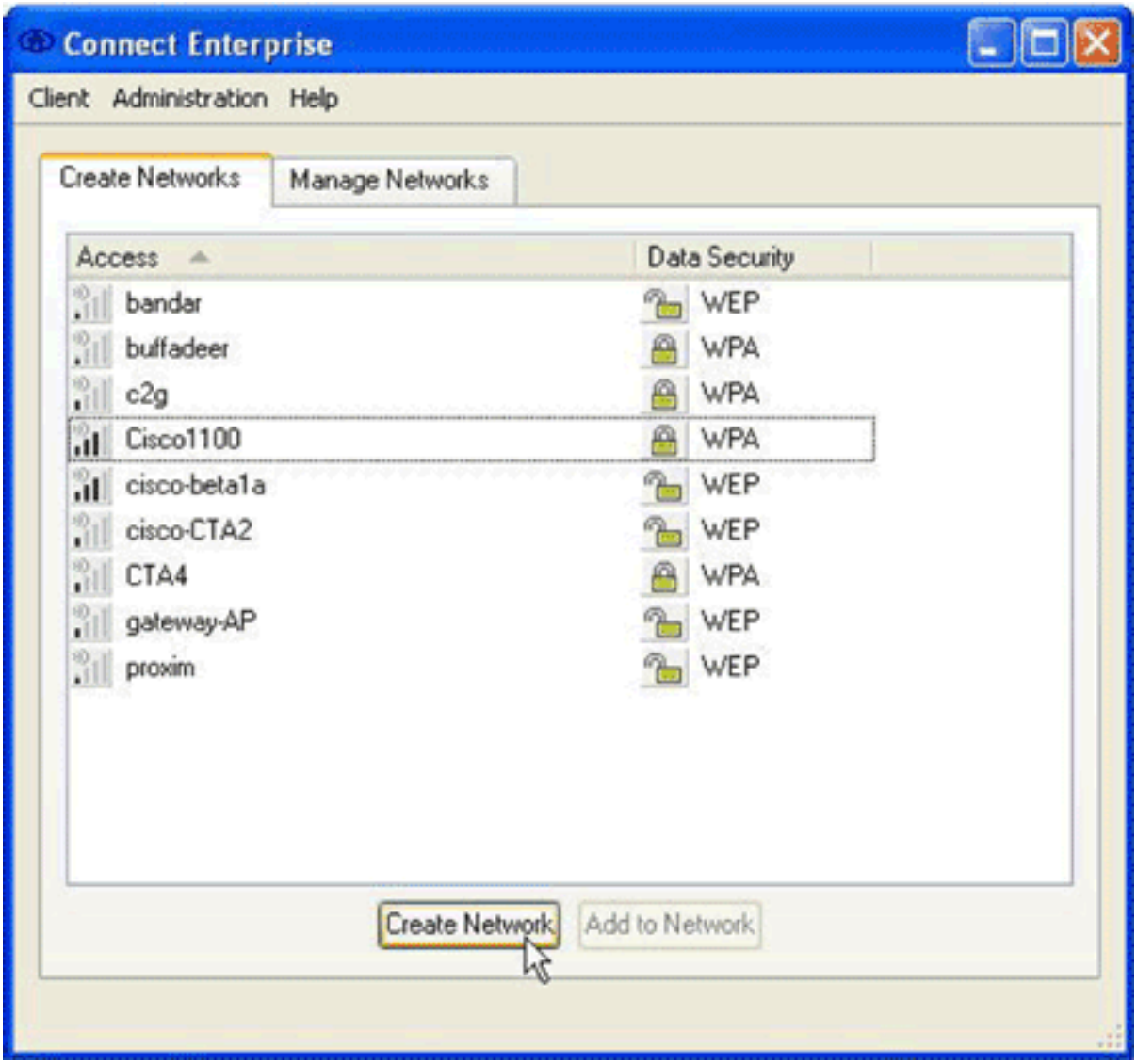
慣例

如需檔案慣例的詳細資訊，請參閱思科技術提示慣例。

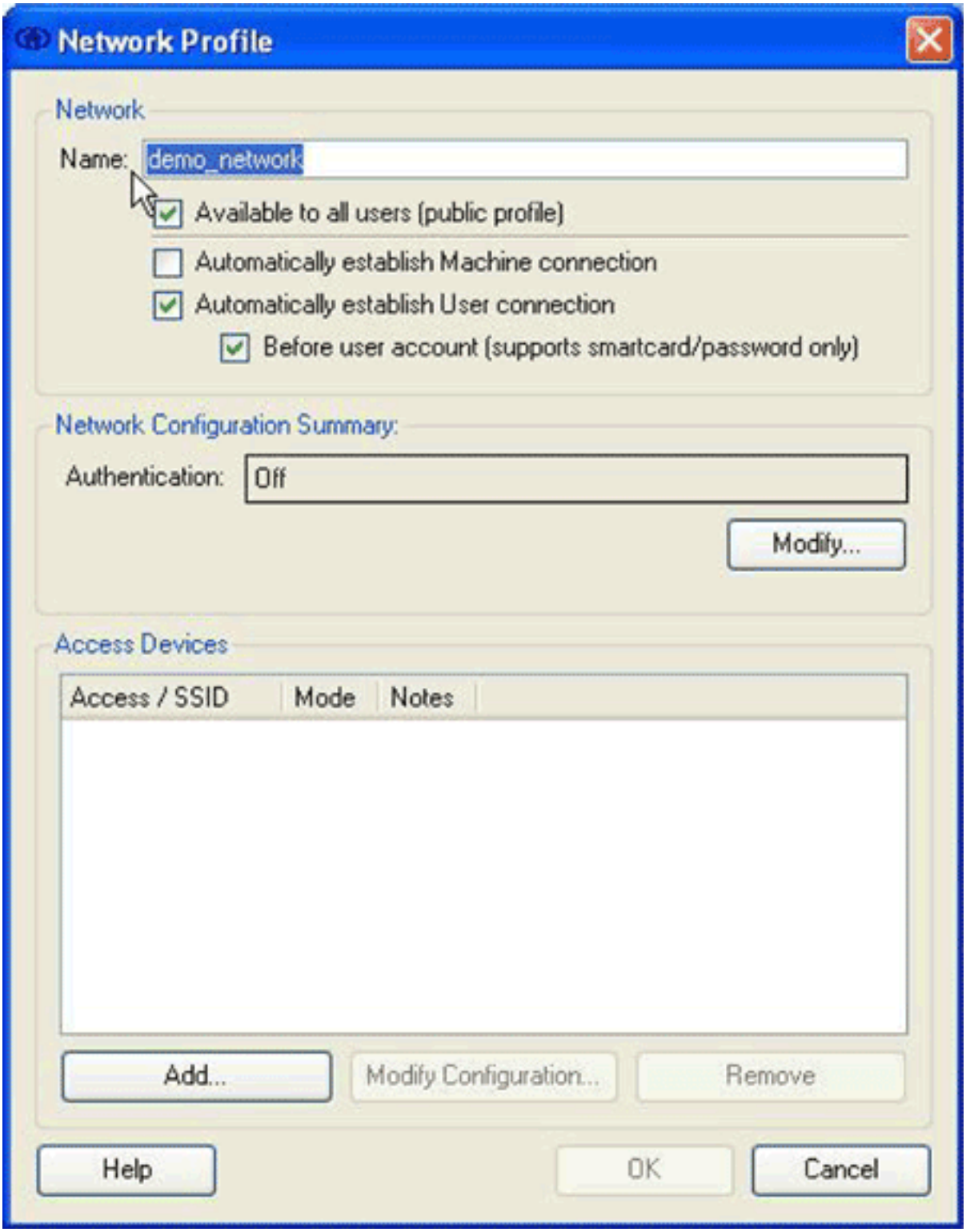
使用PEAP/GTC WPA配置思科安全服務客戶端

要使用PEAP/GTC WPA配置思科安全服務客戶端，請完成以下步驟：

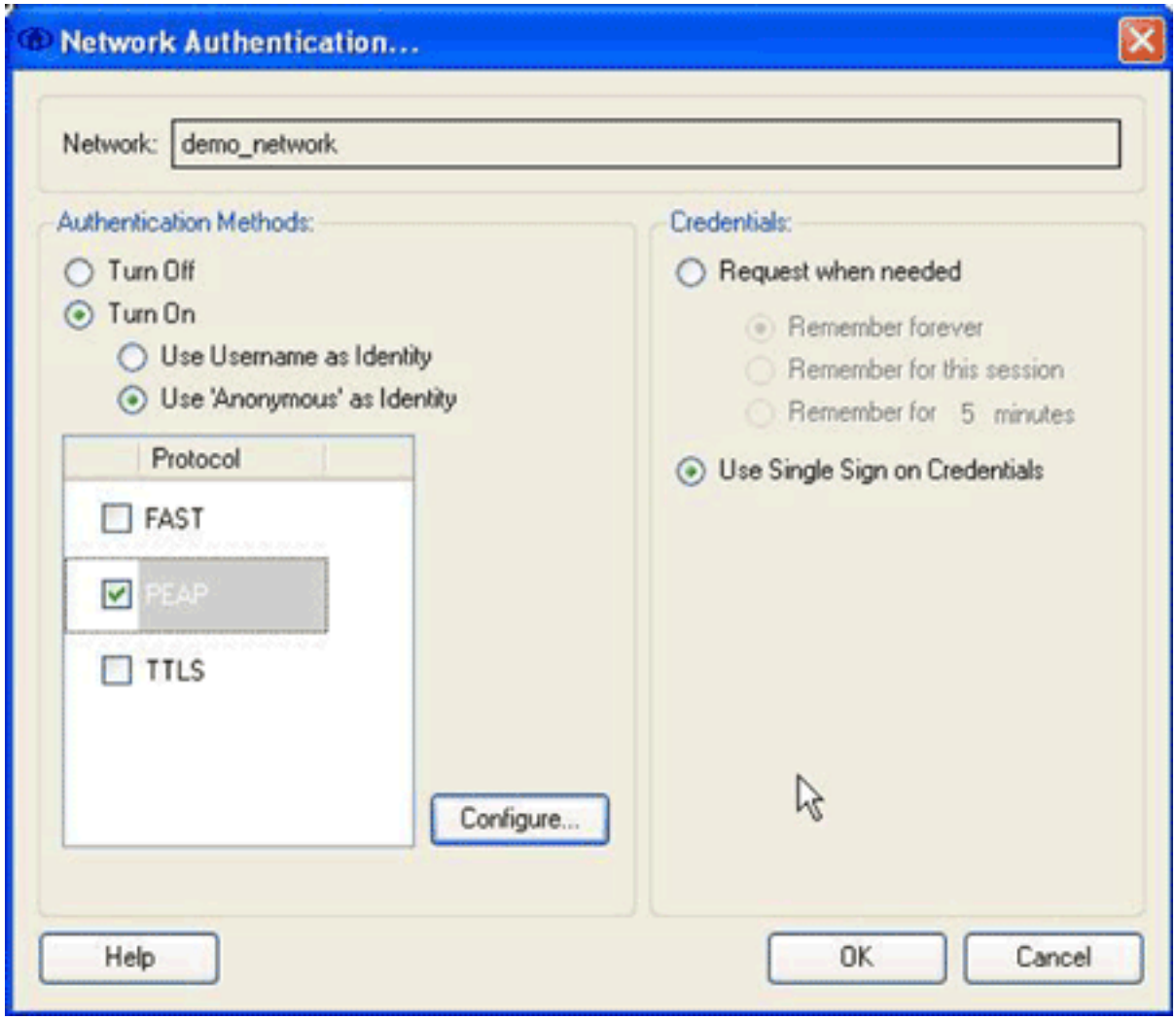
1. 按一下右鍵思科安全服務客戶端系統托盤圖示，然後選擇**開啟**。**注意：**如果未連線到網路，則系統托盤圖示將變暗。系統將顯示Connect Enterprise對話方塊。



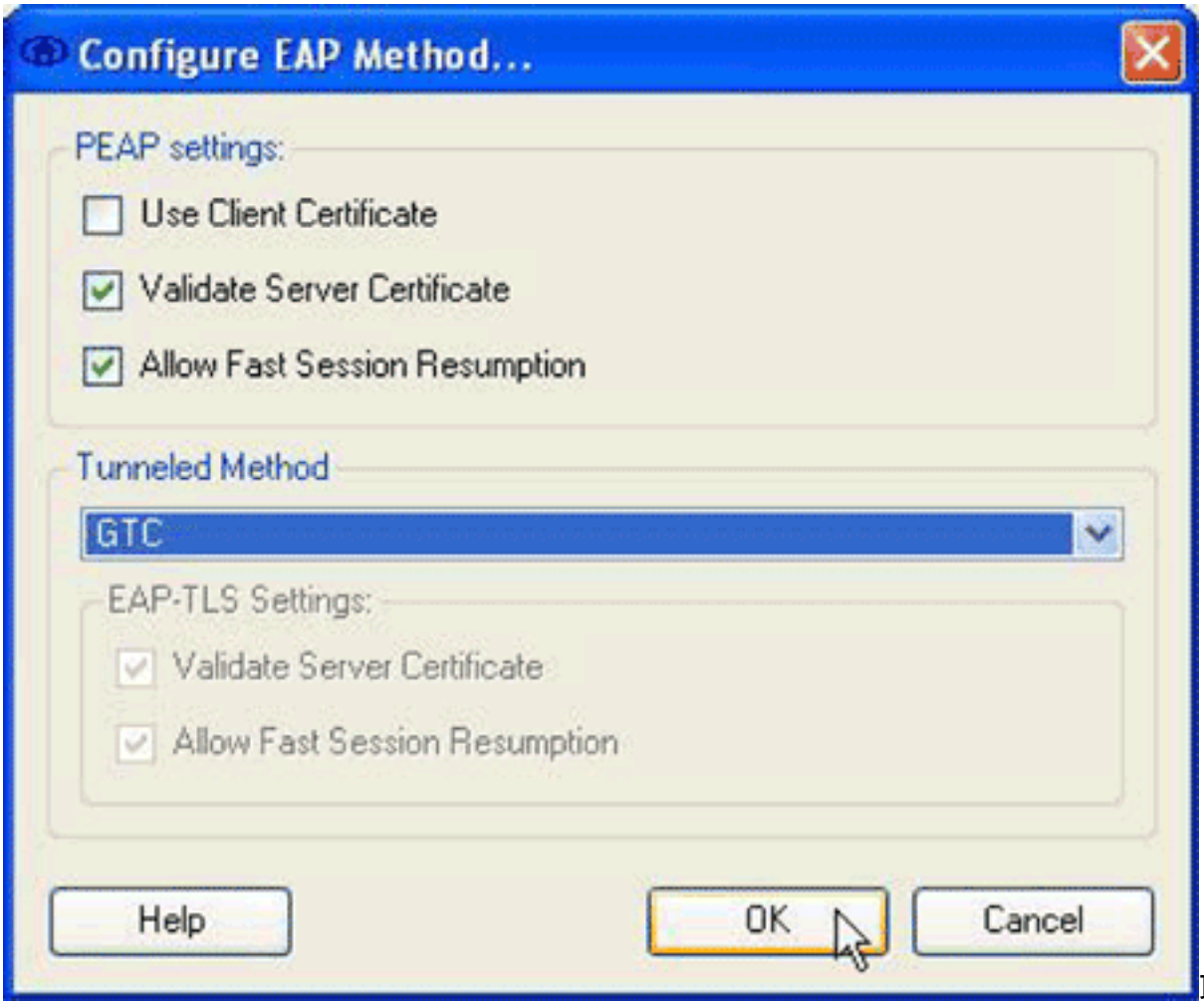
2. 按一下**Create Networks**頁籤。Create Networks區域顯示廣播其服務集識別符號(SSID)的網路。
3. 按一下**Create Network**按鈕。系統將顯示Network Profile對話方塊。



4. 在Network區域中，配置以下選項：在Name欄位中，輸入網路的名稱。此名稱顯示為此網路的SSID。在本示例中，名稱為*demo_network*。選中**Available to all users(public profile)**覈取方塊。選中**Automatically established User connection**覈取方塊，並驗證Automatically established Machine connection覈取方塊未選中。選中**Before user account(supports smartcard/password only)**覈取方塊。**注意：**選中**Before user account（僅支援智慧卡/密碼）複選框時，身份驗證將在輸入憑據後立即進行，但將在域登入之前進行。**如果您使用使用者證書，請不要選中**Before user account（僅支援智慧卡/密碼）**覈取方塊。因為它們在Windows登入之前不可用，所以不能將使用者證書與域登入一起使用。
5. 在Network Configuration Summary區域中，按一下**Modify**按鈕。系統將顯示Network Authentication對話方塊。

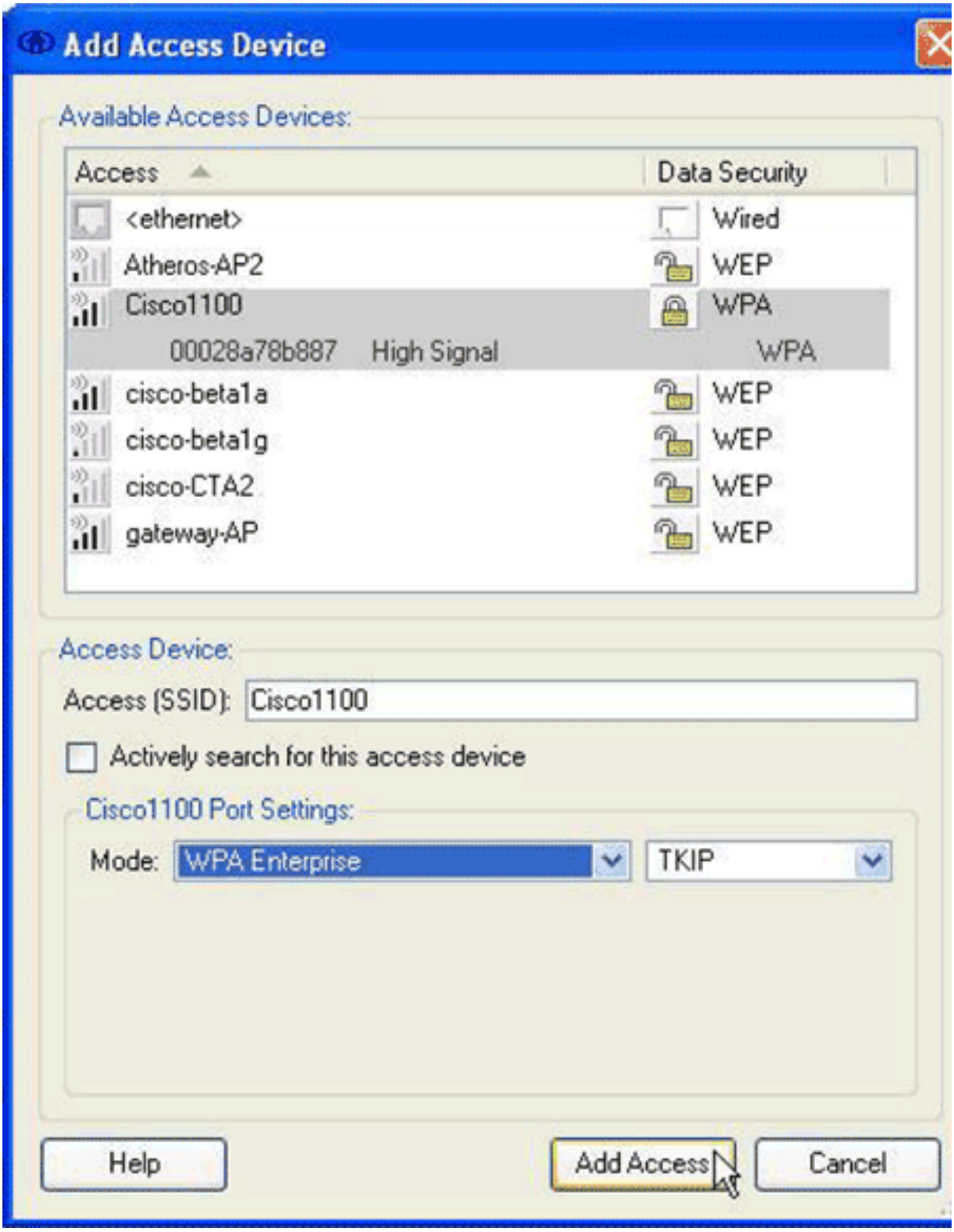


6. 在網路身份驗證對話方塊中，配置以下選項：在「憑據」區域中，按一下**使用單一登入憑據**單選按鈕。在Authentication Methods區域中，按一下**Turn On**單選按鈕，然後按一下**Use 'Anonymous'as Identity**。Turn On單選按鈕填充Authentication Methods區域顯示的協定清單。Use 'Anonymous'as Identity單選按鈕將清單限製為僅隧道化身份驗證協定。選中**PEAP**覈取方塊，然後按一下**Configure**。系統將顯示Configure EAP Method對話方塊。



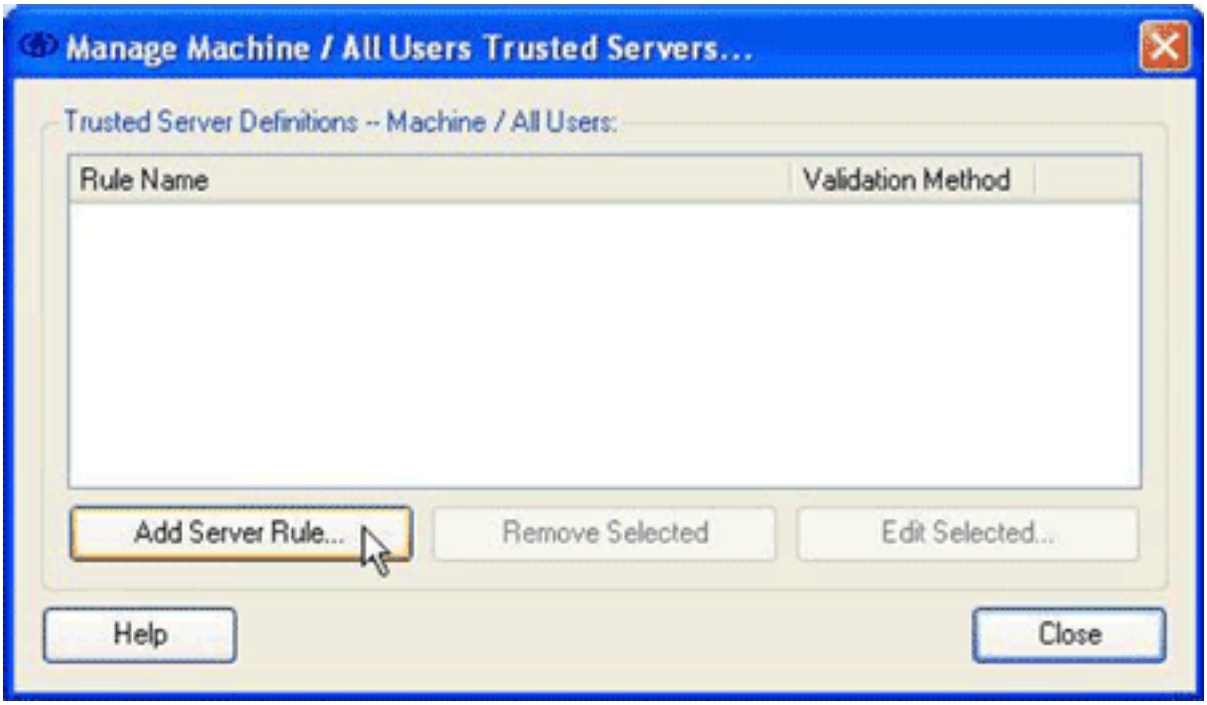
取消選中**Use Client Certificate**覈取方塊。選中**Validate Server Certificate**和**Allow Fast Session Resumption**覈取方塊。從Tunneled Method下拉選單中選擇**GTC**。按一下**OK**返回到Network Authentication對話方塊，然後按一下**OK**返回到Network Profile對話方塊。

7. 在Network Profile對話方塊的Access Devices區域中，按一下**Add**。系統將顯示Add Access Device對話方塊。

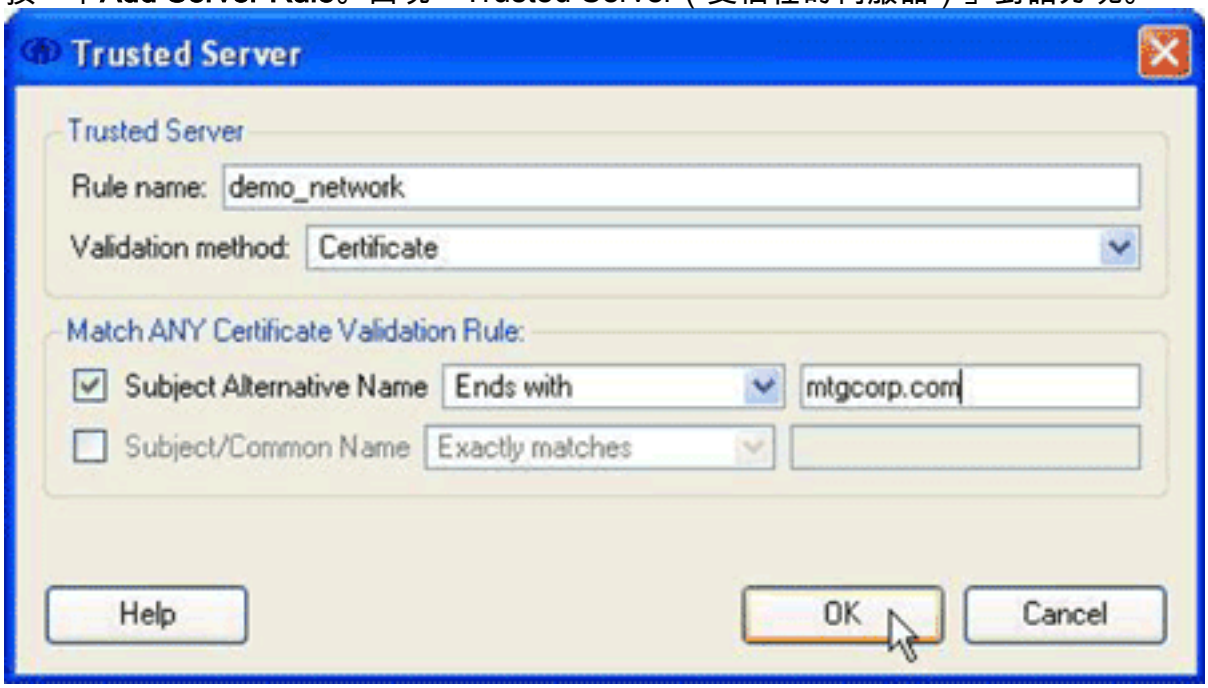


8. 在Add Access Devices對話方塊中，選擇要配置的裝置，然後按一下**Add Access**。**註**：如果要配置的裝置在範圍內，則該裝置的SSID應顯示在Available Access Devices清單中。如果未顯示裝置，請在Access(SSID)欄位中輸入裝置的SSID，在Cisco 1100 Port Settings區域輸入埠設定，然後按一下**Add Access**。
9. 在「網路配置檔案」對話方塊中，按一下**確定**以返回到「連線企業」對話方塊。
10. 在Connect Enterprise對話方塊中，從Client選單中選擇**Trusted Servers > Manage Machine / All Users** trusted servers。系統將顯示Manage Machine / All Users Trusted Servers對話方

塊。



11. 按一下**Add Server Rule**。出現「Trusted Server（受信任的伺服器）」對話方塊。



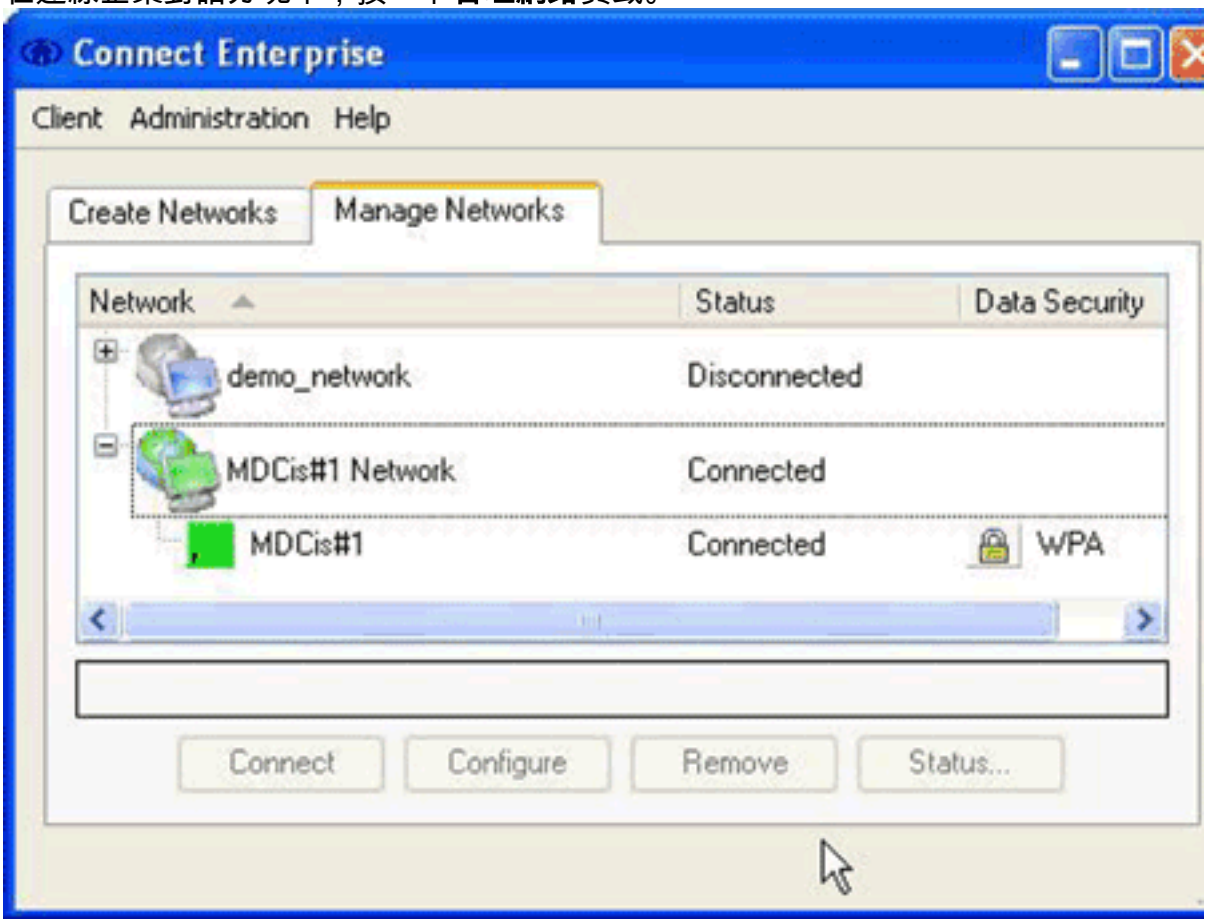
12. 在「受信任的伺服器」對話方塊中，配置以下選項：在Rule name欄位中，輸入規則的名稱。在「驗證方法」下拉選單中，選擇「**證書**」。在Match ANY Certificate Validation Rule區域中，配置規則的選項。要構建規則，您必須知道伺服器證書的內容，並在Match ANY Certificate Validation Rule區域中輸入這些值。例如，如果主題替代名稱包含伺服器的域名*mtgcorpserver.mtgcorp.com*，請從Subject Alternative Name下拉選單中選擇**Ends with**，然後在文本欄位中輸入**mtgcorp.com**。按一下**OK**以返回到Manage Machine / All Users Trusted Servers對話方塊。
13. 在管理電腦/所有使用者受信任的伺服器對話方塊中，按一下**關閉**以返回連線企業對話方塊。

配置完成，您可以連線到網路。

連線到網路

要連線到新網路，請完成以下步驟：

1. 在連線企業對話方塊中，按一下**管理網路**頁籤。



2. 斷開連線到新網路使用的介面卡的任何網路。
3. 在Network清單中，選擇新的網路配置檔案，然後按一下**Connect**。

成功進行配置和連線後，思科安全服務客戶端系統托盤圖示顯示為綠色。

注意：如果電腦中安裝了病毒防護軟體，且該軟體配置為解析Cisco Secure Services Client日誌目錄，則使用Cisco Secure Services Client身份驗證時可能會遇到高CPU週期。為了提高效能，請將您的病毒防護軟體配置為排除思科安全服務客戶端日誌目錄。

相關資訊

- 技術支援與文件 - Cisco Systems