適用於FlexConnect的無線BYOD部署指南

目錄

簡介

流動裝置在計算方面越來越強大，在消費者中越來越受歡迎。數以百萬計的這些裝置通過高速Wi-Fi銷售給消費者，因此使用者可以進行通訊和合作。現在，消費者已經習慣了這些流動裝置為他們的生活帶來的生產力提升，並正在尋求將他們的個人體驗帶入工作空間。這就產生了在工作場所自帶裝置(BYOD)解決方案的功能需求。

本文檔提供自帶裝置解決方案的分支機構部署。員工使用新iPad連線到企業服務集識別符號(SSID)，並被重定向到自助註冊門戶。思科身份服務引擎(ISE)根據公司Active Directory(AD)對使用者進行身份驗證，並將具有嵌入式iPad MAC地址和使用者名稱的證書以及請求方配置檔案下載到iPad，該請求方配置檔案強制使用可擴展身份驗證協定 — 傳輸層安全(EAP-TLS)作為dot1x連線的方法。根據ISE中的授權策略，使用者可以使用dot1x連線並訪問適當的資源。

低於7.2.110.0的思科無線區域網控制器軟體版本中的ISE功能不支援通過FlexConnect接入點(AP)關聯的本地交換客戶端。7.2.110.0版支援用於本地交換和集中身份驗證客戶端的FlexConnect AP的這些ISE功能。此外，與ISE 1.1.1整合的版本7.2.110.0提供（但不限於）以下無線自帶裝置解決方案功能：

- 裝置分析和狀態
- 裝置註冊和請求方調配
- 個人裝置自註冊（調配iOS或Android裝置）

注意：雖然受支援，但本指南中不包括其他裝置，如PC或Mac無線筆記型電腦和工作站。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

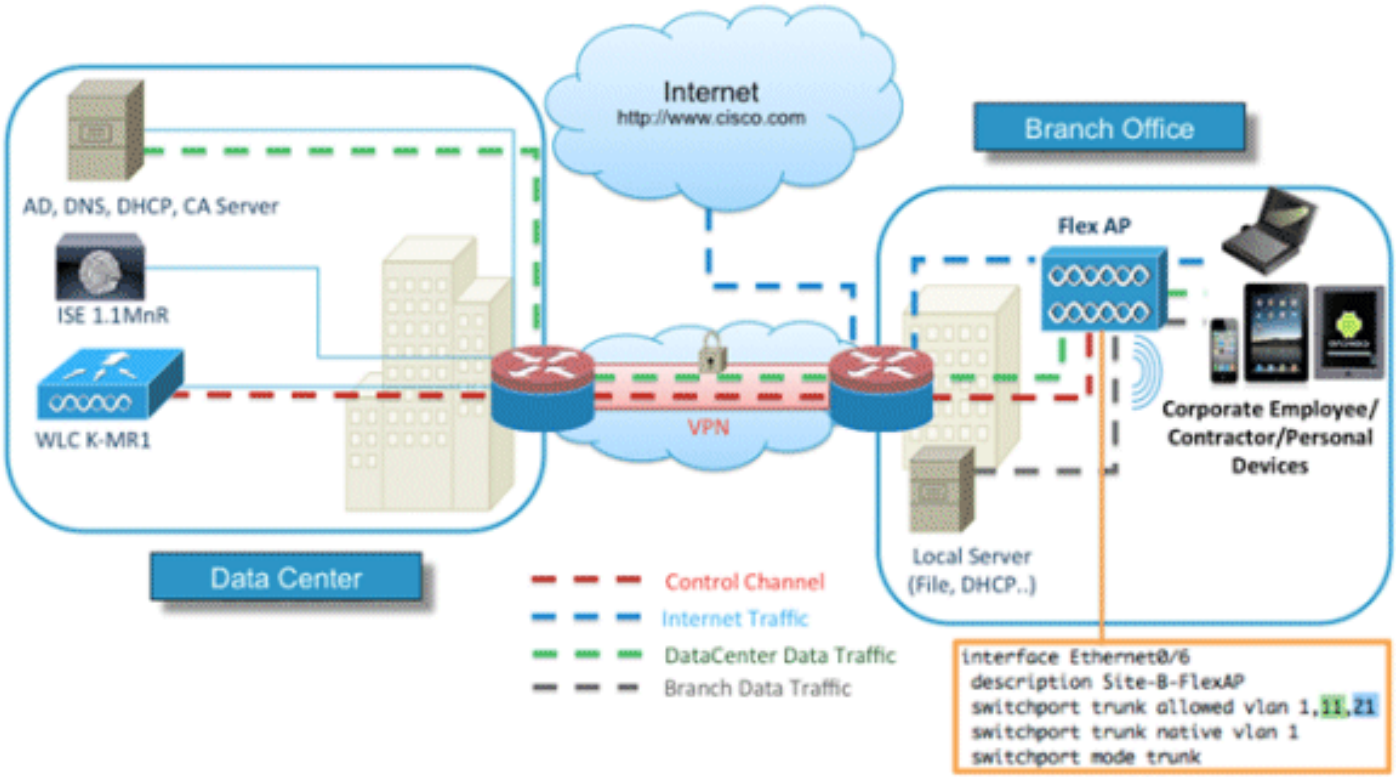
- Cisco Catalyst交換器
- Cisco無線LAN(WLAN)控制器
- Cisco WLAN Controller(WLC)軟體版本7.2.110.0及更新版本
- 在FlexConnect模式下的802.11n AP
- Cisco ISE軟體版本1.1.1及更高版本
- 含憑證授權單位(CA)的Windows 2008 AD
- DHCP伺服器
- 網域名稱系統(DNS)伺服器
- 網路時間協定(NTP)
- 無線客戶端筆記型電腦、智慧手機和平板電腦（Apple iOS、Android、Windows和Mac）

注意：有關此軟體版本的重要資訊，請參閱版本7.2.110.0的Cisco無線LAN控制器和輕量接入點版本說明。在載入和測試軟體之前，請登入到Cisco.com網站以獲取最新的版本說明。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

拓撲

若要正確實施和測試這些功能，需要最低限度的網路設定，如下圖所示：



對於此模擬，您需要一個具有FlexConnect AP的網路、一個具有本地DHCP、DNS、WLC和ISE的本地/遠端站點。FlexConnect AP連線到主幹以測試具有多個VLAN的本地交換。

裝置註冊和請求方調配

必須註冊裝置，以便其本機請求方可以提供dot1x身份驗證。根據正確的身份驗證策略，使用者被重定向到訪客頁面並通過員工憑據進行身份驗證。使用者會看到裝置註冊頁面，該頁面會詢問使用者的裝置資訊。然後開始裝置調配過程。如果調配不支援作業系統(OS)，則將使用者重定向到資產註冊門戶，以便將該裝置標籤為MAC身份驗證繞行(MAB)訪問。如果作業系統受支援，註冊過程將開始並配置裝置的本地請求方進行dot1x身份驗證。

資產註冊門戶

資產註冊門戶是ISE平台的元素，允許員工通過身份驗證和註冊流程啟動終端自註冊。

管理員可以從終端標識頁面刪除資產。每位員工都可以編輯、刪除和將其已註冊的資產列入黑名單。列入黑名單的終端被分配到黑名單身份組，並且建立授權策略以防止列入黑名單的終端訪問網路。

自助註冊門戶

在中央Web驗證(CWA)流程中，員工被重新導向至一個門戶，該門戶允許他們輸入其憑證、驗證以及輸入他們希望註冊的特定資產的具體資訊。此門戶稱為自助調配門戶，類似於裝置註冊門戶。它允許員工輸入MAC地址以及終端的有意義描述。

驗證與布建

一旦員工選擇自助註冊門戶，他們就會面臨提供一組有效員工憑據以進入調配階段的挑戰。身份驗證成功後，可將端點調配到端點資料庫中，並為端點生成證書。該頁面上的連結允許員工下載Supplicant Pilot Wizard(SPW)。

> **注意**：請參閱FlexConnect功能表思科文章，檢視BYOD的最新FlexConnect功能表。

iOS布建(iPhone/iPad/iPod)

對於EAP-TLS配置，ISE遵循Apple Over-the-Air(OTA)註冊流程：

- 身份驗證成功後，評估引擎將評估客戶端調配策略，從而生成請求方配置檔案。
- 如果請求方配置檔案用於EAP-TLS設定，則OTA進程確定ISE是使用自簽名還是由未知CA簽名。如果其中一個條件為true，則要求使用者下載ISE或CA的證書，然後才能開始註冊過程。
- 對於其他EAP方法，ISE在身份驗證成功後推送最終配置檔案。

Android調配

出於安全考慮，Android代理必須從Android市場網站下載，並且不能從ISE調配。思科通過思科Android市場發佈者帳戶將嚮導的候選版本上傳到Android市場。

這是Android調配過程：

1. 思科使用軟體開發工具包(SDK)建立副檔名為.apk的Android軟體包。
2. 思科將軟體包上傳到Android市場。
3. 使用者使用適當的引數在客戶端調配中配置策略。
4. 註冊裝置後，當dot1x身份驗證失敗時，終端使用者將被重定向到客戶端調配服務。
5. 調配門戶頁面提供將使用者重定向到Android市場門戶的按鈕，使用者可以在該門戶下載SPW。
6. Cisco SPW啟動並執行請求方的調配： SPW發現ISE並從ISE下載配置檔案。SPW為EAP-TLS建立證書/金鑰對。SPW向ISE發起簡單證書註冊協定(SCEP)代理請求呼叫並獲得證書。SPW應用無線配置檔案。如果配置檔案應用成功，SPW將觸發重新身份驗證。SPW退出。

雙SSID無線BYOD自註冊

以下是雙SSID無線BYOD自註冊的過程：

1. 使用者與訪客SSID關聯。
2. 使用者開啟瀏覽器並重定向到ISE CWA訪客門戶。
3. 使用者在訪客門戶中輸入員工使用者名稱和密碼。
4. ISE對使用者進行身份驗證，根據他們是員工而不是訪客的事實，將使用者重定向到Employee Device Registration訪客頁面。
5. 在DeviceID的Device Registration訪客頁面中預填充MAC地址。使用者輸入描述，如果需要，接受可接受的使用策略(AUP)。

6. 使用者選擇**Accept**並開始下載和安裝SPW。
7. 該使用者裝置的請求方會隨任何證書一起調配。
8. 發生CoA，裝置重新關聯到公司SSID(CORP)並使用EAP-TLS（或該請求方使用的其他授權方法）進行身份驗證。

單SSID無線BYOD自註冊

在此場景中，企業接入(CORP)有一個單一的SSID，它同時支援受保護的可擴展身份驗證協定(PEAP)和EAP-TLS。沒有訪客SSID。

這是單SSID無線BYOD自註冊的過程：

1. 使用者與CORP關聯。
2. 使用者向PEAP身份驗證請求方輸入員工使用者名稱和密碼。
3. ISE對使用者進行身份驗證，並根據PEAP方法提供接受授權策略，重定向至Employee Device Registration guest頁面。
4. 使用者開啟瀏覽器並重定向到「員工裝置註冊」訪客頁面。
5. 在DeviceID的Device Registration訪客頁面中預填充MAC地址。使用者輸入說明並接受AUP。
6. 使用者選擇**Accept**並開始下載和安裝SPW。
7. 該使用者裝置的請求方會隨任何證書一起調配。
8. 發生CoA，裝置重新關聯到CORP SSID並使用EAP-TLS進行身份驗證。

功能配置

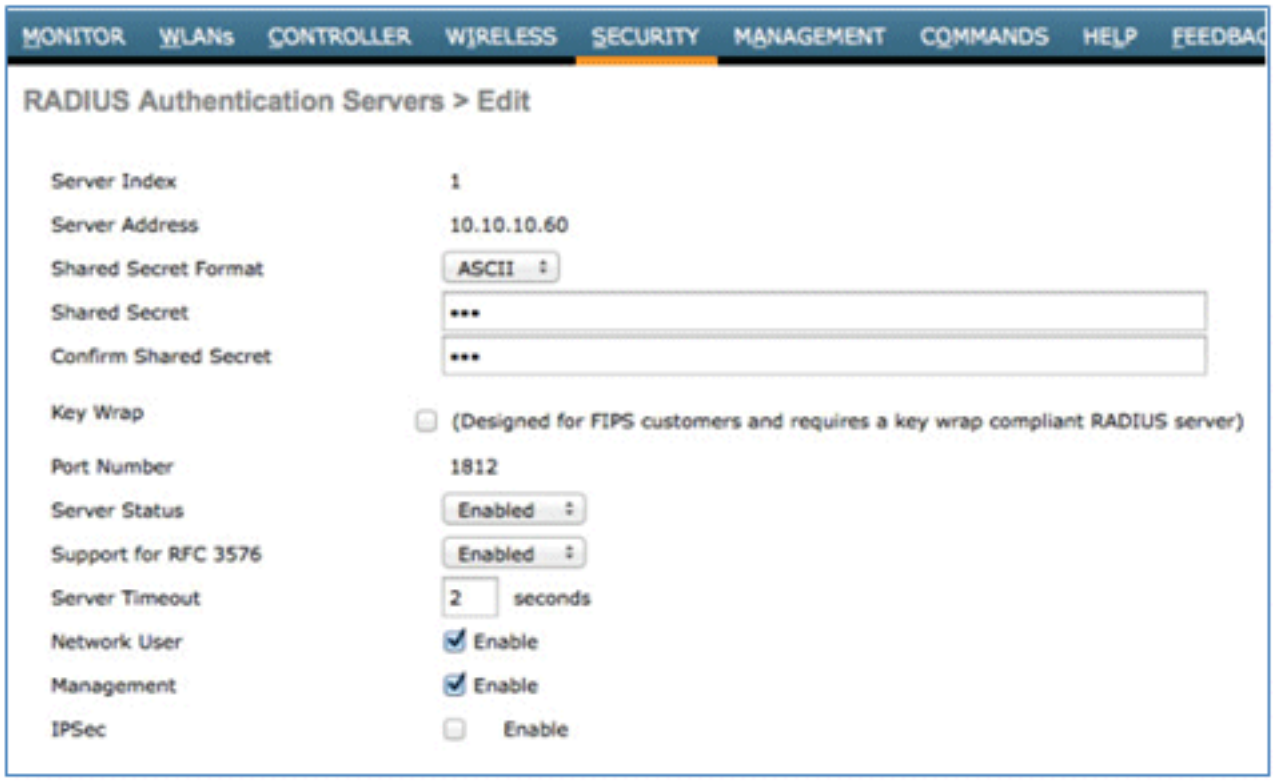
完成以下步驟即可開始設定：

1. 在本指南中，請確保WLC的版本是7.2.110.0或更高版本。

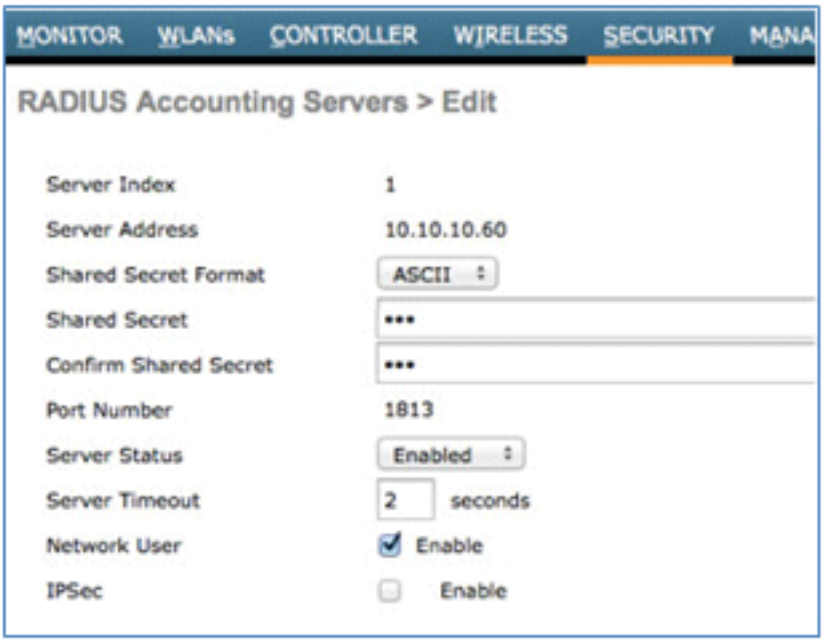
2. 導覽至**Security > RADIUS > Authentication**，然後將RADIUS伺服器新增到WLC。

3. 將ISE 1.1.1新增到WLC:

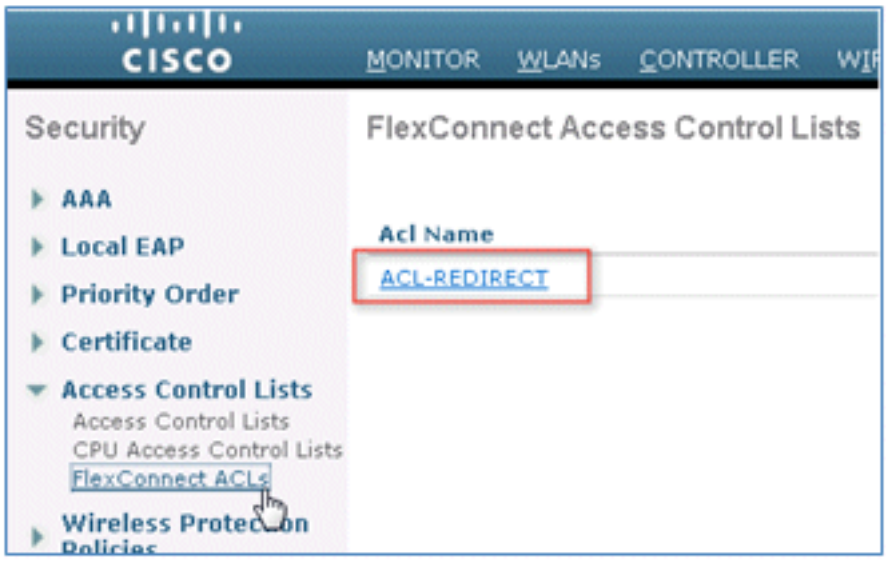
輸入共用金鑰。將RFC 3576的支援設定為**Enabled**。



4. 新增與RADIUS記帳伺服器相同的ISE伺服器。



5. 建立稍後用於ISE策略的WLC預身份驗證ACL。導覽至WLC > **Security > Access Control Lists > FlexConnect ACL**，然後建立一個名為**ACL-REDIRECT**的新FlexConnect ACL（在此範例中）。

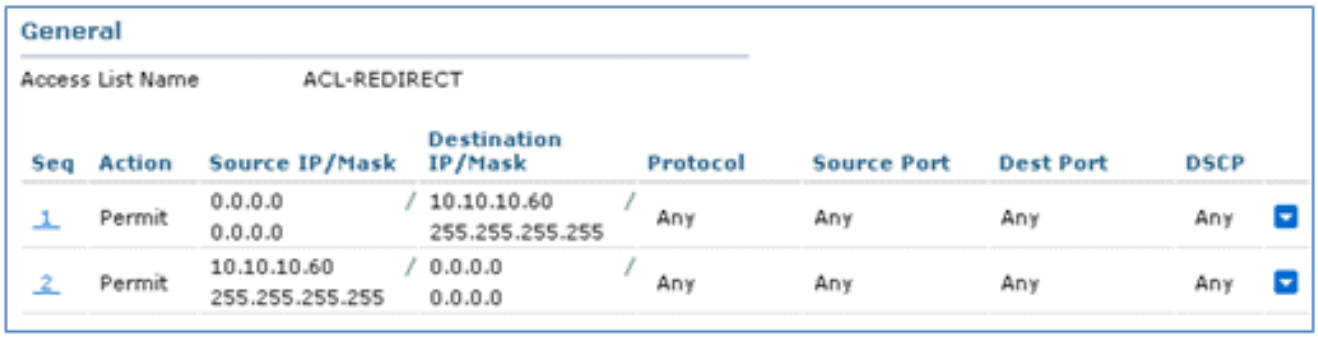


6. 在ACL規則中，允許所有流入/流出ISE的流量，並在請求方調配期間允許客戶端流量。

對於第一條規則（序列1）：

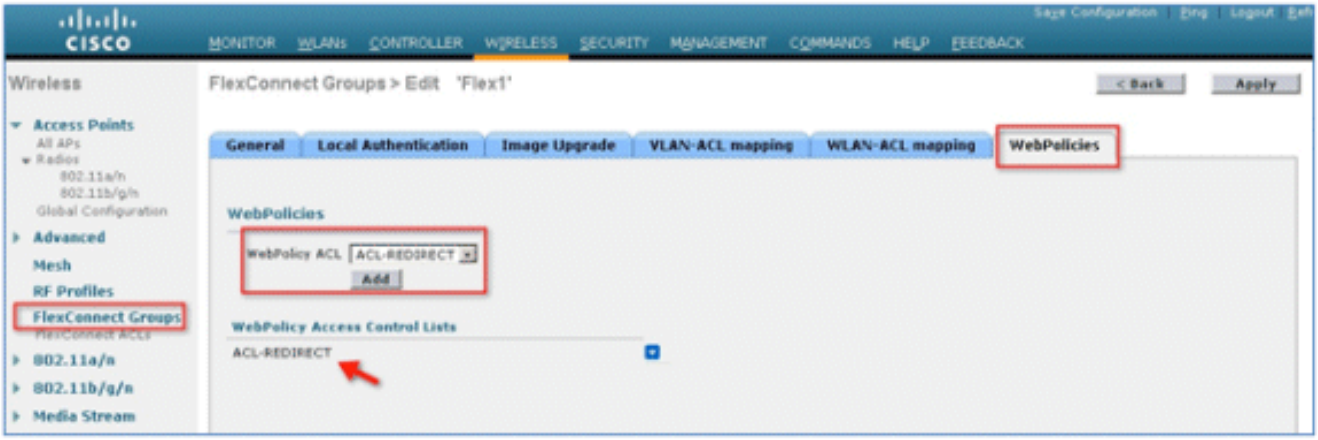
將Source設定為**Any**。設定IP（ISE地址）/網路**掩碼255.255.255.255**。將Action設定為**Permit**。

對於第二個規則（序列2），將源IP（ISE地址）/掩碼255.255.255.255設定為**Any**，將操作設定為**Permit**。



7. 建立一個名為Flex1的新FlexConnect組（在本例中）：

導航到**FlexConnect Group > WebPolicies**頁籤。在「WebPolicy ACL」欄位下，按一下**Add**，然後選擇**ACL-REDIRECT**或先前建立的FlexConnect ACL。確認它填充了**WebPolicy Access Control Lists**欄位。



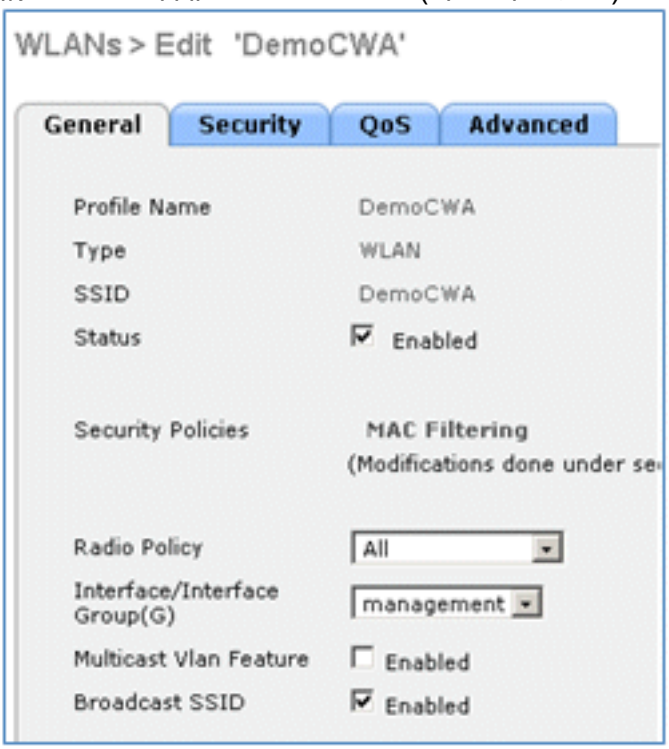
8. 按一下「**Apply**」和「**Save Configuration**」。

WLAN配置

完成以下步驟即可設定WLAN:

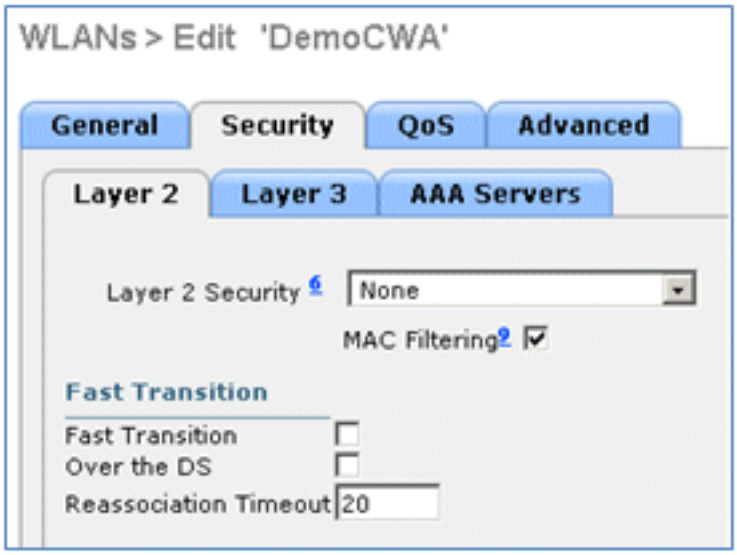
1. 建立雙SSID的開放式WLAN SSID示例：

   輸入WLAN名稱：**DemoCWA**（在此範例中）。選擇**Enabled**選項。



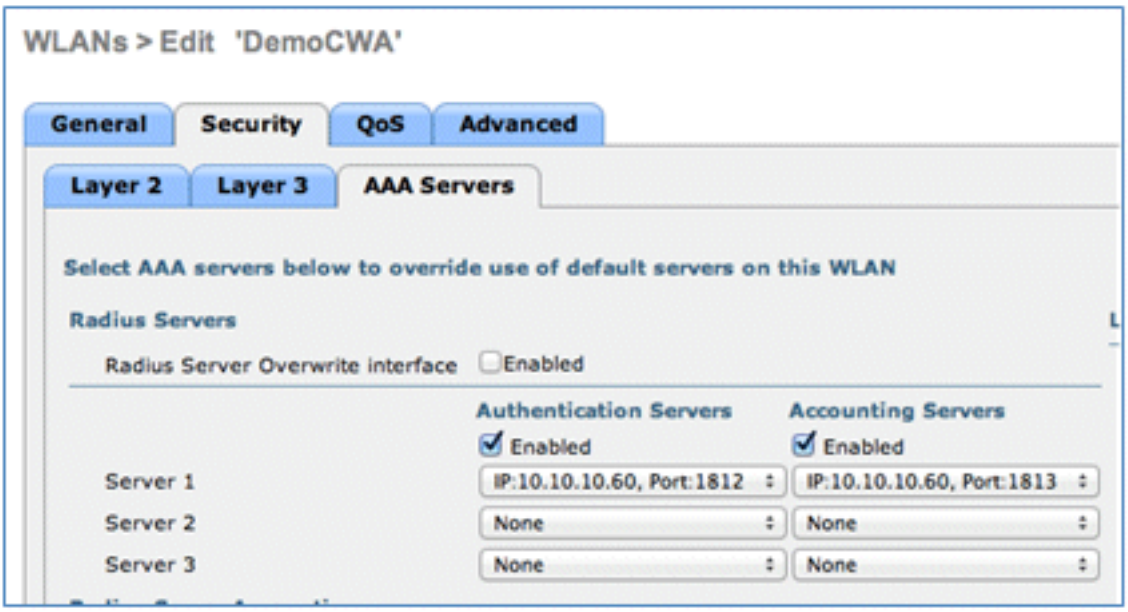
2. 導覽至**Security**索引標籤**> Layer 2**索引標籤，然後設定以下屬性：

   第2層安全：**無**MAC Filtering: **Enabled**（覈取方塊為選中狀態）快速轉換： **Disabled**（未選中框）



3. 轉到**AAA Servers**頁籤，並設定以下屬性：

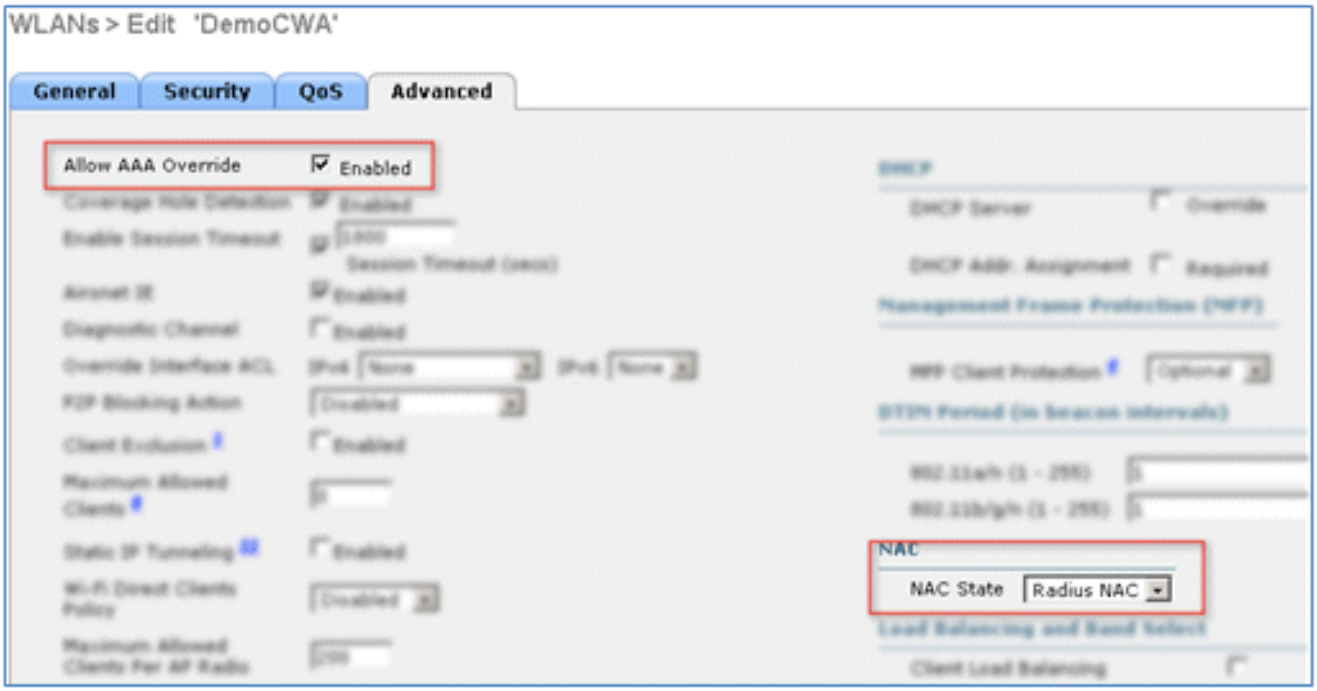
   身份驗證和帳戶伺服器：已**啟用**伺服器1:*<ISE IP地址>*



4. 從**AAA Servers**頁籤向下滾動。在Web-auth使用者的「Authentication priority order（驗證優先順序）」下，請確認**RADIUS**已用於驗證，但其他未使用。

5. 轉到**Advanced**索引標籤，並設定以下屬性：

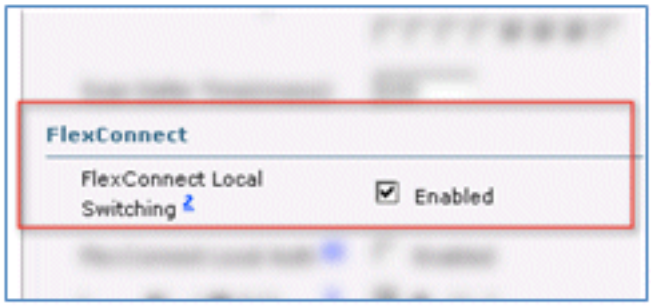
允許AAA覆蓋：**啟用**NAC狀態：**Radius NAC**



註：當FlexConnect AP處於斷開連線模式時，不支援RADIUS網路准入控制(NAC)。因此，如

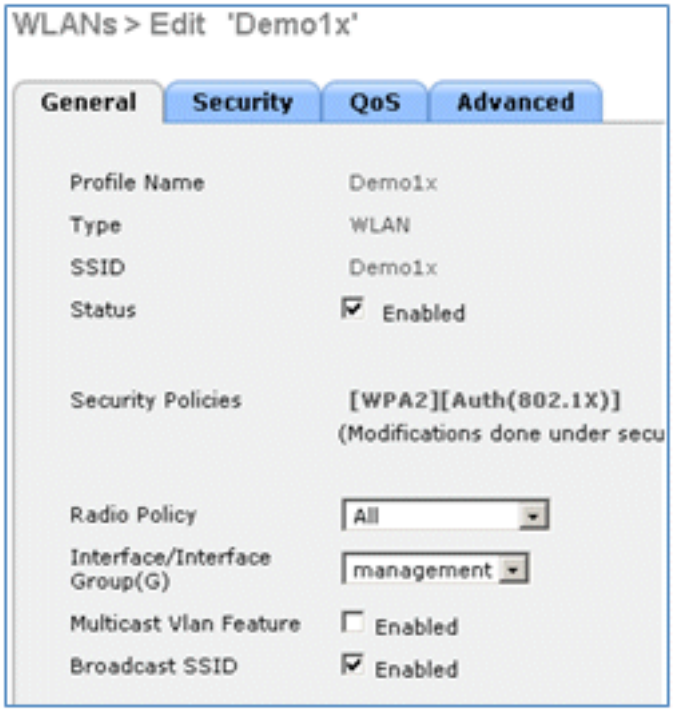
果FlexConnect AP處於獨立模式且失去與WLC的連線，則所有客戶端都會斷開連線，並且SSID不再被通告。

6. 在「高級」頁籤中向下滾動，並將「FlexConnect本地交換」設定為**啟用**。



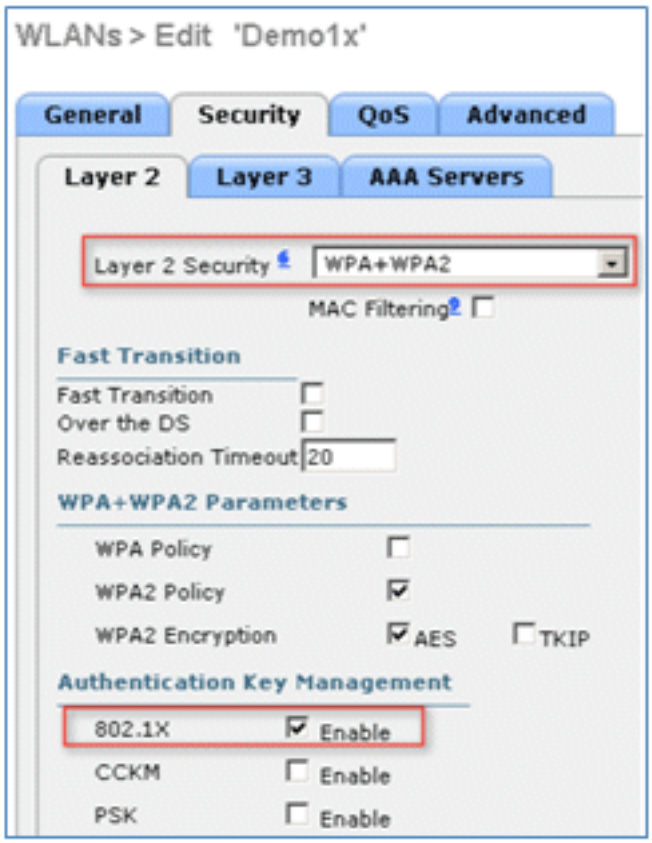
7. 按一下「**Apply**」和「**Save Configuration**」。

8. 為單SSID和雙SSID方案建立名為**Demo1x**（在本示例中）的802.1X WLAN SSID。



9. 導覽至**Security**索引標籤**> Layer 2**索引標籤，然後設定以下屬性：

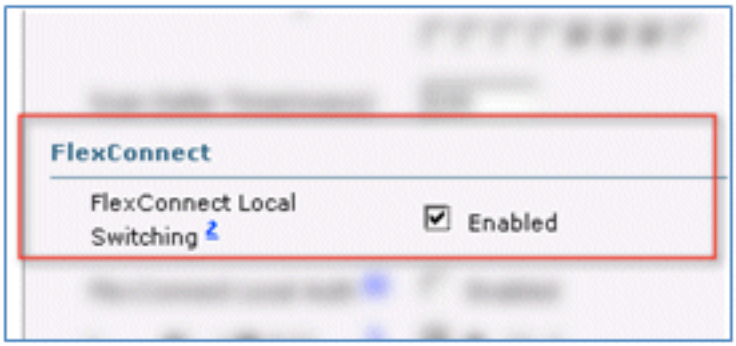
第2層安全:**WPA+WPA2**快速轉換： **Disabled**（未選中框）身份驗證金鑰管理：802.IX：**啟用**



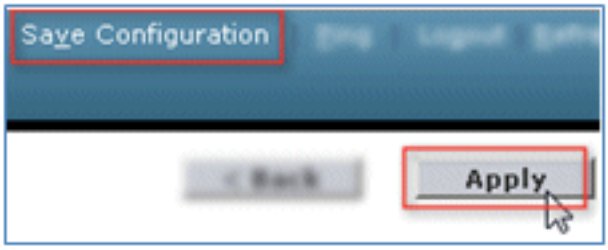
10. 轉到**Advanced**索引標籤，並設定以下屬性：

    允許AAA覆蓋：啟用NAC狀態：**Radius NAC**

11. 在**Advanced**索引標籤中向下滾動，並將FlexConnect Local Switching設定為**Enabled**。



12. 按一下「Apply」和「Save Configuration」。



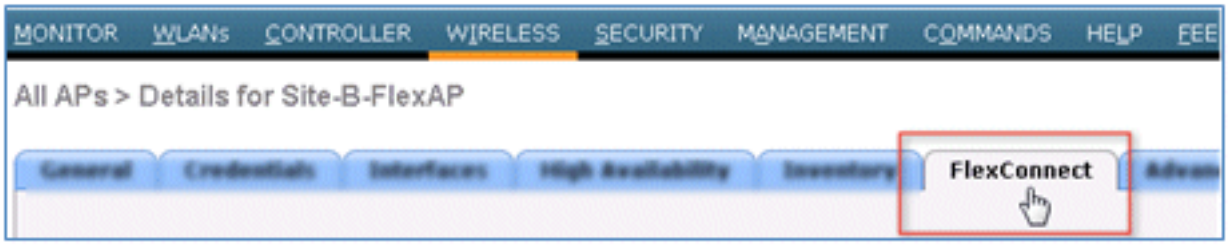
13. 確認兩個新的WLAN都已建立。

FlexConnect AP配置

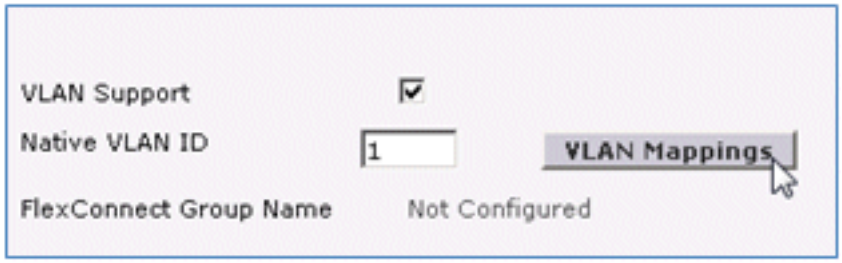
完成以下步驟以設定FlexConnect AP:

1. 導覽至**WLC > Wireless**，然後按一下目標FlexConnect AP。

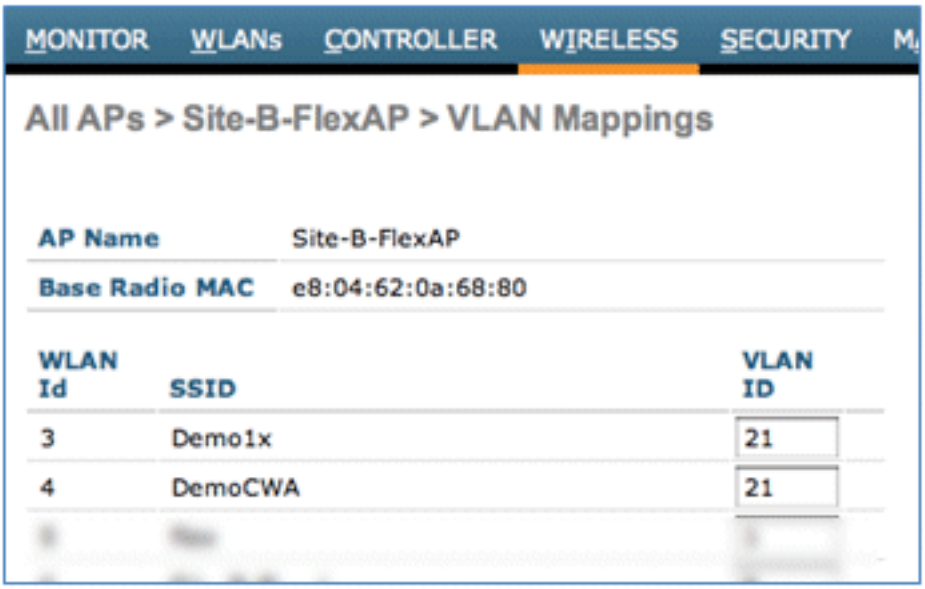
2. 按一下**FlexConnect選**項卡。



3. 啟用VLAN支援（覈取方塊為選中狀態），設定本徵VLAN ID，然後點選**VLAN對映**。



4. 將SSID的VLAN ID設定為**21**（在本例中），以便進行本地交換。



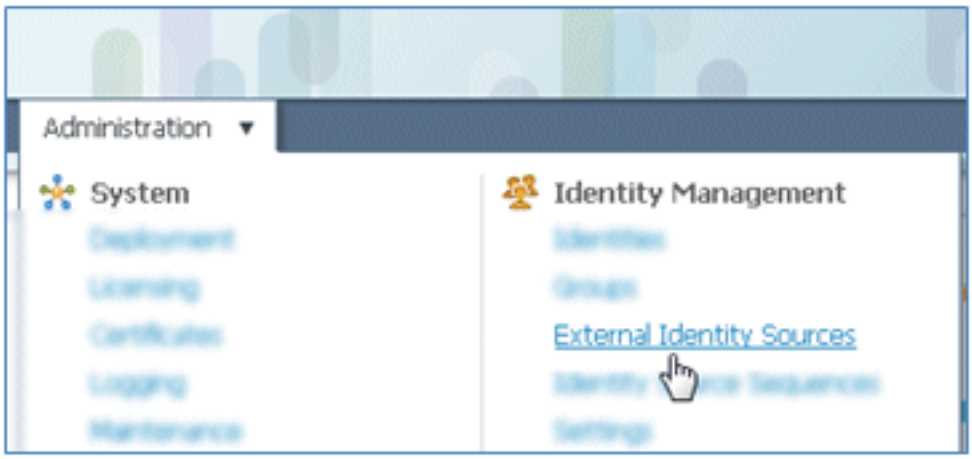
5. 按一下「Apply」和「Save Configuration」。

ISE 組態

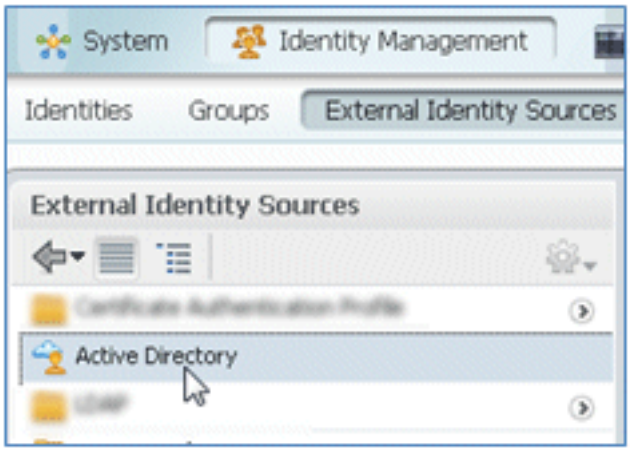
完成以下步驟以配置ISE:

1. 登入ISE伺服器：<*https://ise*>。

2. 導航到Administration > Identity Management > External Identity Sources。

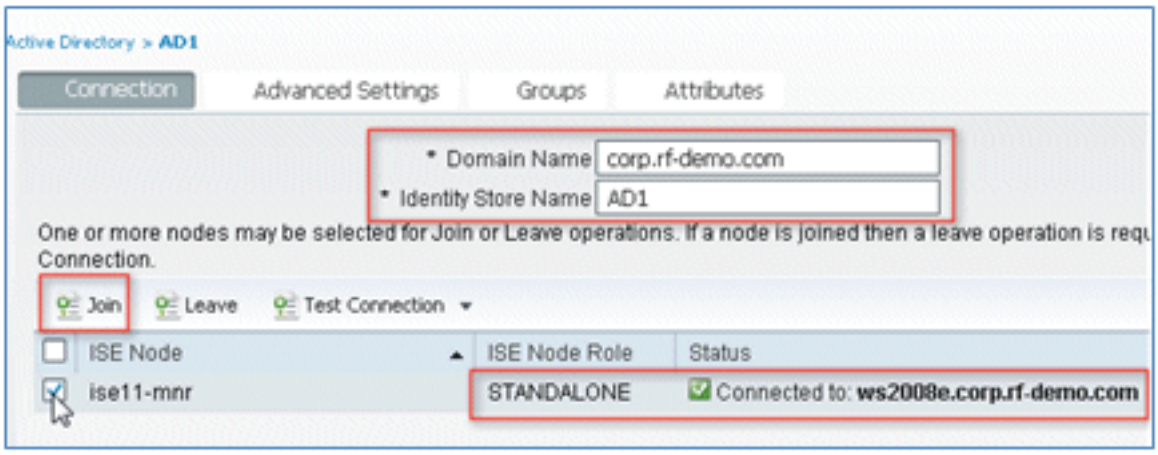


3. 按一下**Active Directory**。

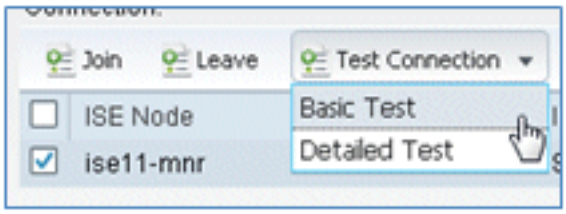


4. 在Connection頁籤中：

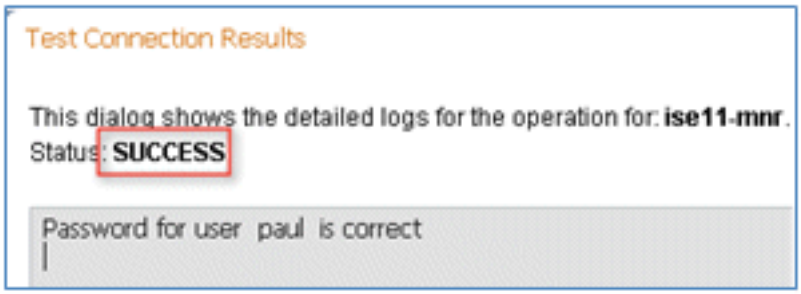
新增**corp.rf-demo.com**的域名（在本例中），並將身份庫名稱預設值更改為**AD1**。按一下「**Save Configuration**」。按一下**Join**，並提供加入所需的AD管理員帳戶使用者名稱和密碼。「狀態」必須為綠色。啟用**Connected to:**（覈取方塊已選中）。



5. 使用當前域使用者執行與AD的基本連線測試。

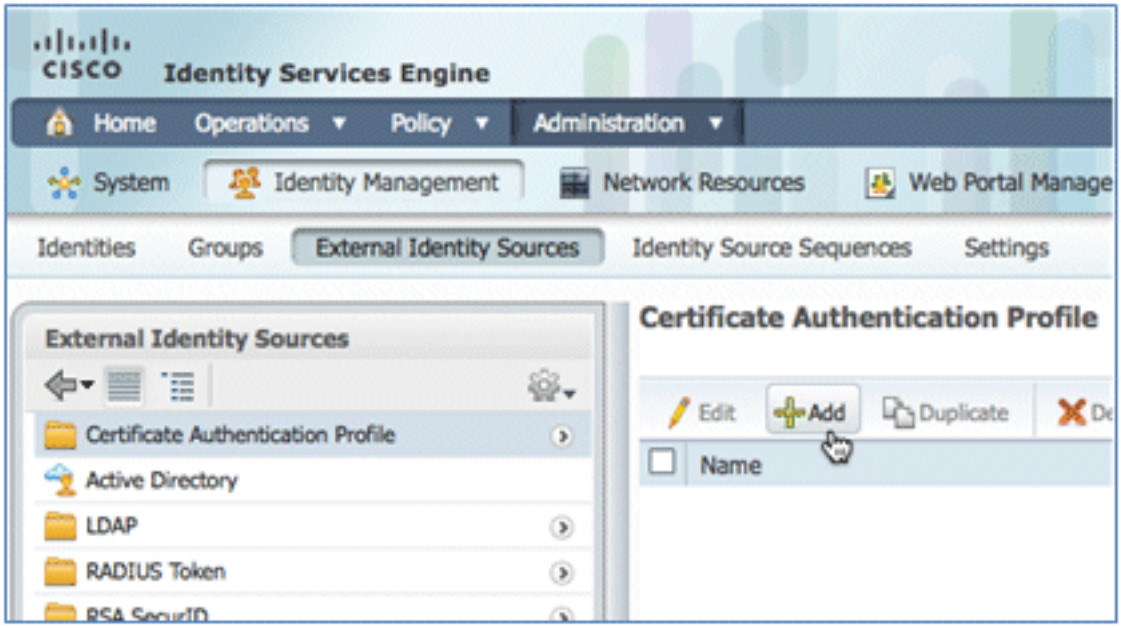


6. 如果與AD的連線成功，則會出現一個對話方塊，確認密碼正確。

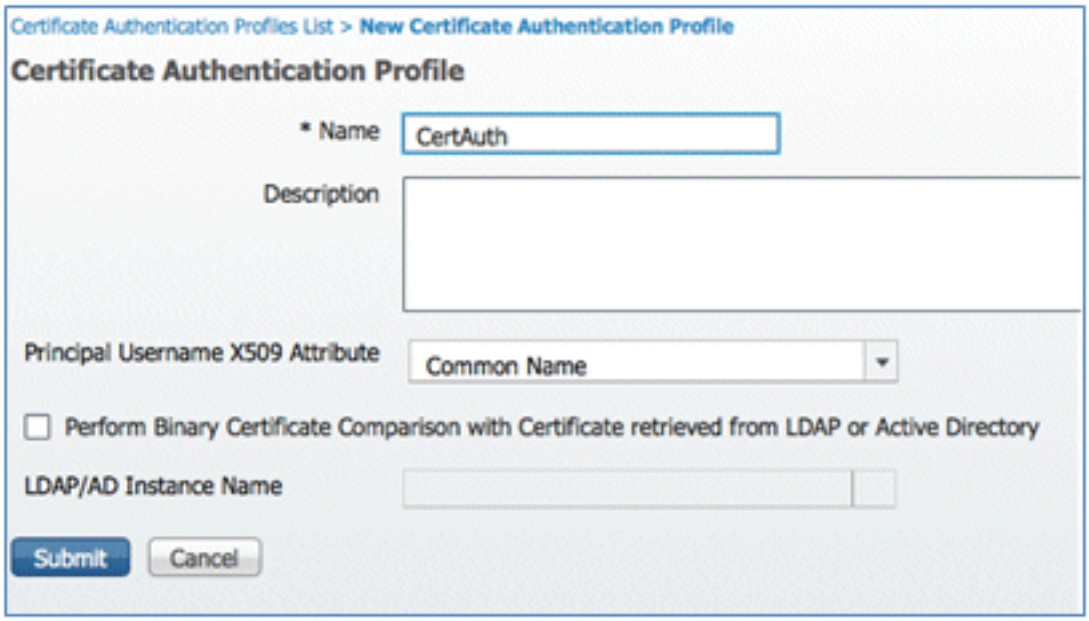


7. 導航到**Administration > Identity Management > External Identity Sources**:

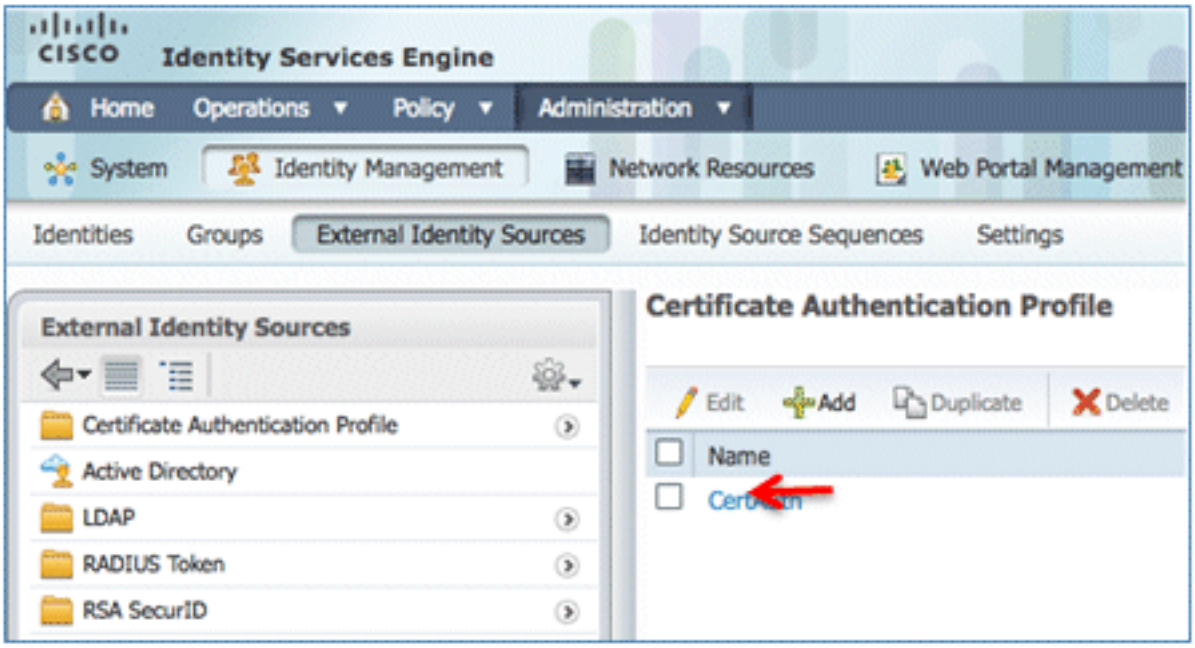
   按一下「**Certificate Authentication Profile**」。按一下「**Add**」以新增憑證驗證設定檔(CAP)。



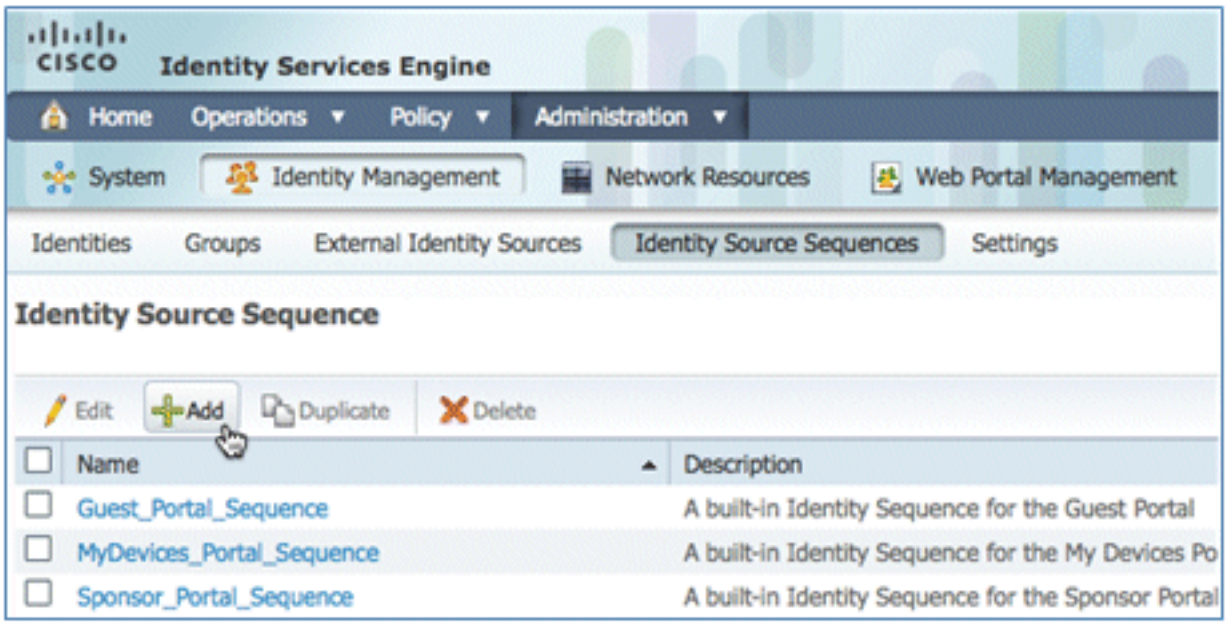
8. 為CAP輸入名稱**CertAuth**（在本例中）；對於主體使用者名稱X509屬性，選擇**Common Name**；然後按一下**Submit**。



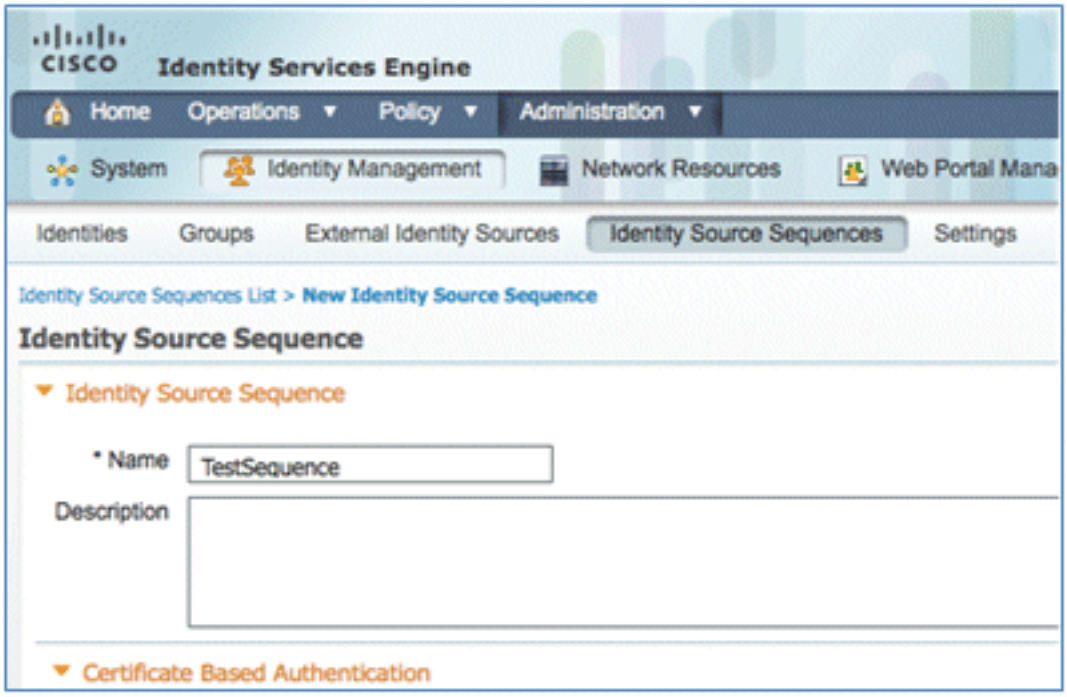
9. 確認已新增新的CAP。



10. 導航到**Administration > Identity Management > Identity Source Sequences**，然後點選**Add**。

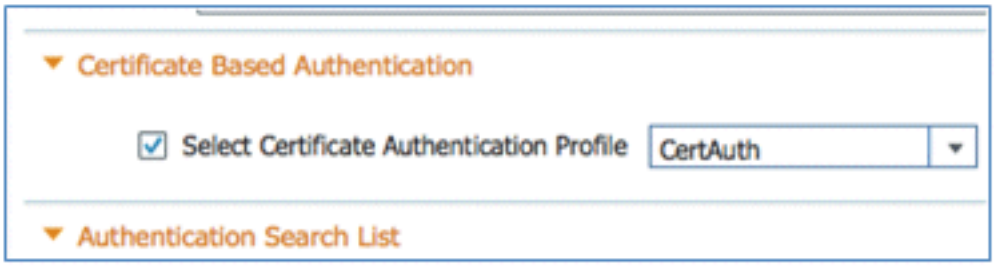


11. 為序列指定名稱**TestSequence**（在本例中）。



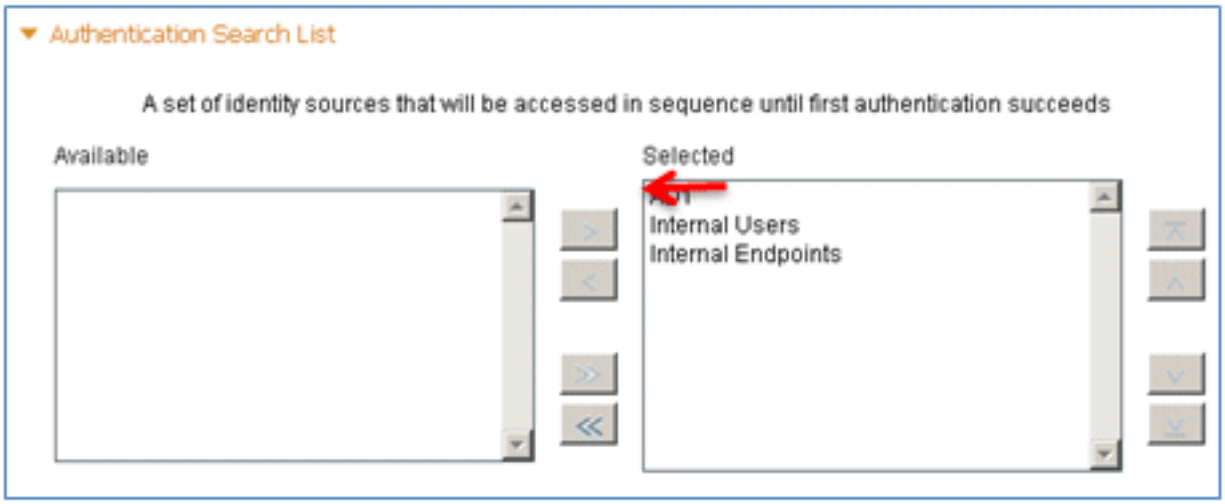
12. 向下滾動至**Certificate Based Authentication**:

啟用**Select Certificate Authentication Profile**（覈取方塊處於選中狀態）。選擇**CertAuth**（或之前建立的其他CAP配置檔案）。

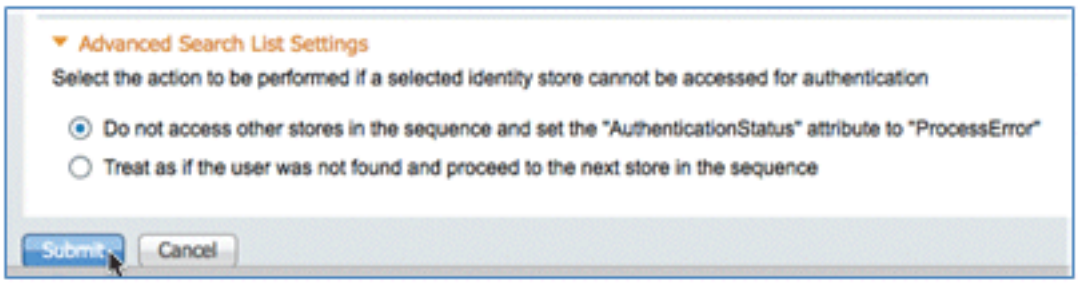


13. 向下滾動至**Authentication Search List**:

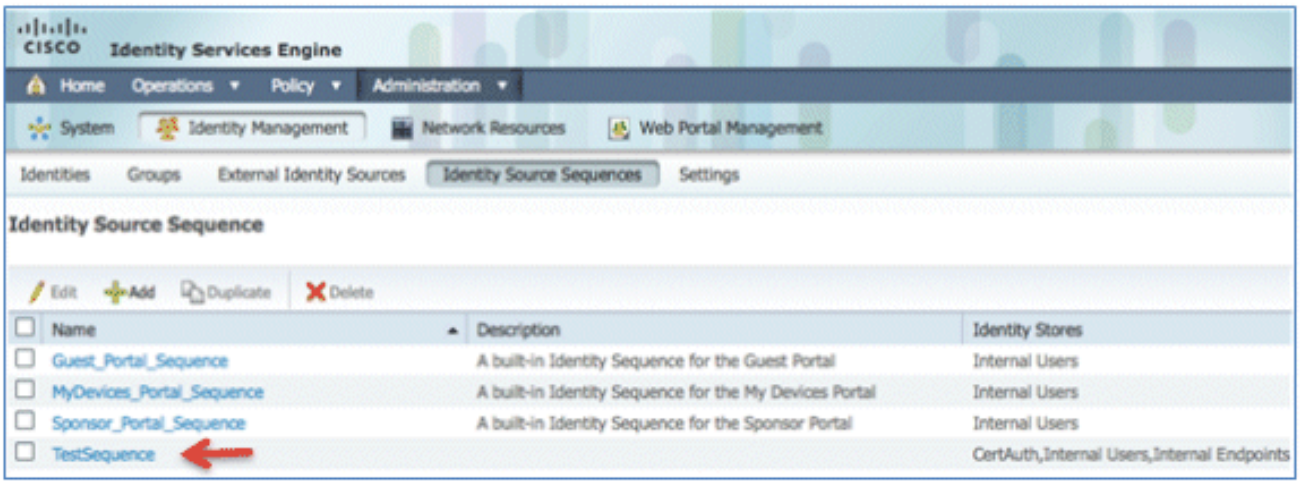
將AD1從「可用」移動到「選定」。按一下up按鈕將AD1移至最高優先順序。



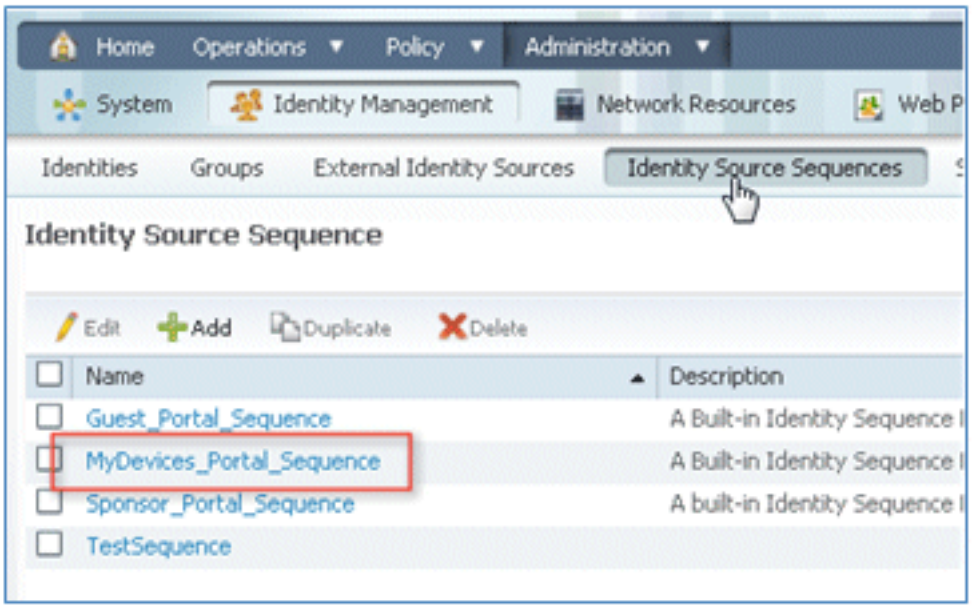
14. 按一下「**Submit**」以儲存。



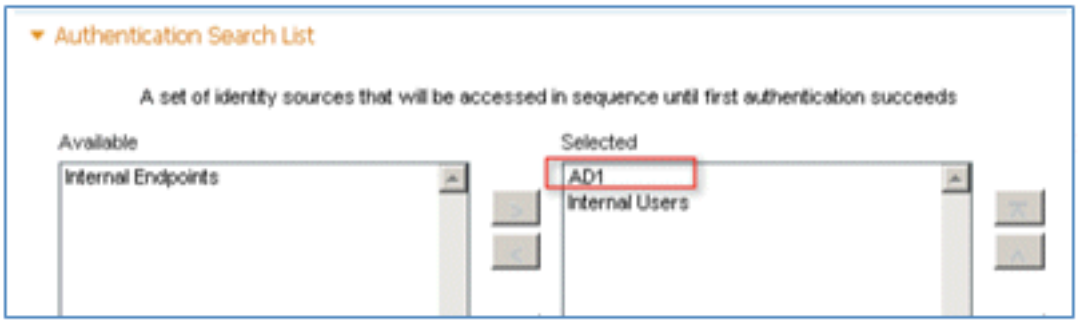
15. 確認已新增新的身份源序列。



16. 使用AD驗證「My Devices Portal（我的裝置門戶）」。導航到ISE > **Administration** > **Identity Management** > **Identity Source Sequence**，然後編輯MyDevices_Portal_Sequence。



17. 將**AD1**新增到Selected清單，然後按一下up按鈕將AD1移動到最高優先順序。

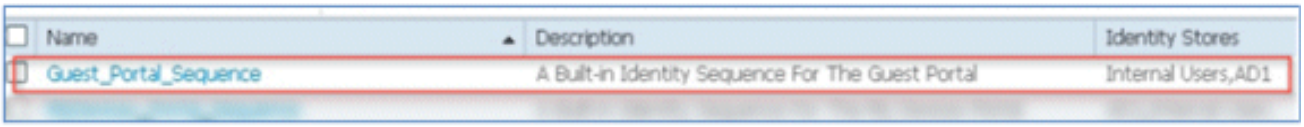


18. 按一下「**Save**」。

19. 確認MyDevices_Portal_Sequence的身份儲存序列包含**AD1**。

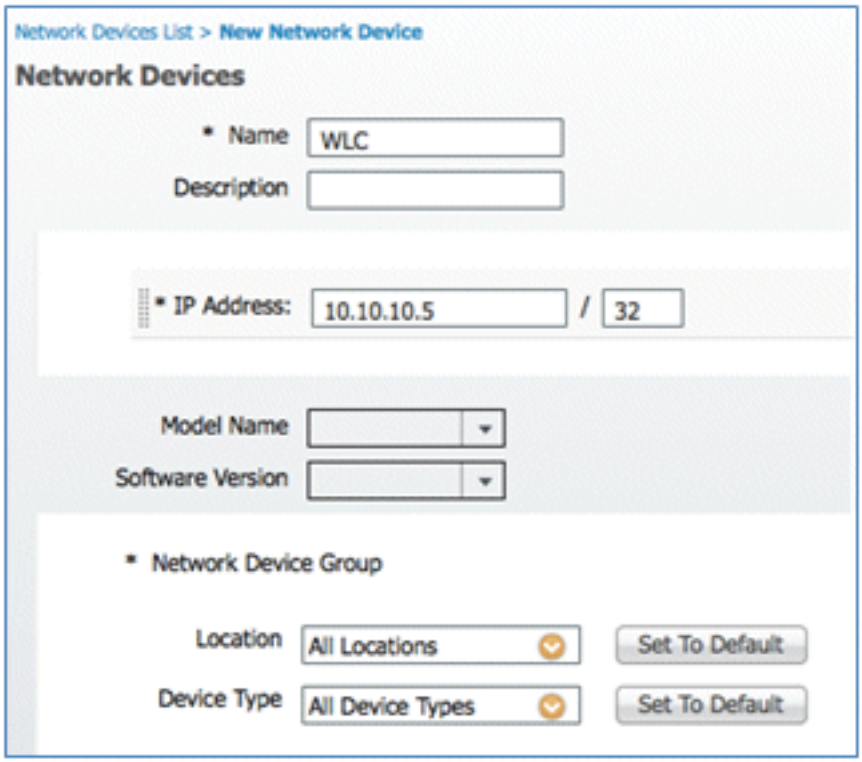
20. 重複步驟16-19以便為Guest_Portal_Sequence新增AD1，然後按一下**Save**。

21. 確認Guest_Portal_Sequence包含**AD1**。

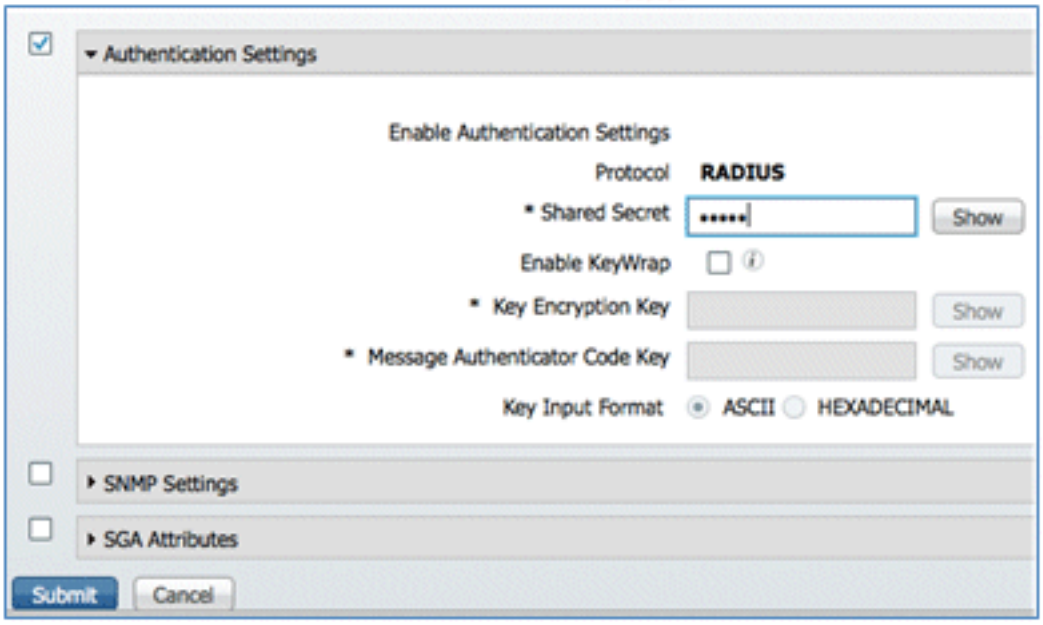


22. 若要將WLC新增到網路存取裝置(WLC)，請導覽至**管理 > 網路資源 > 網路裝置**，然後按一下**Add**。

23. 新增WLC名稱、IP地址、子網掩碼等。

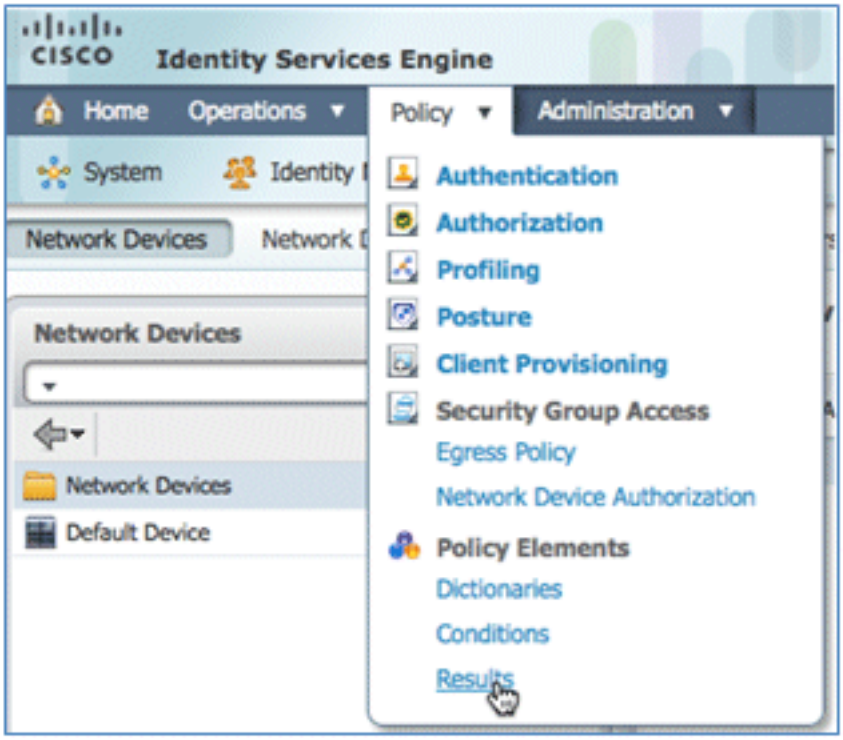


24. 向下滾動到Authentication Settings，然後輸入Shared Secret。此專案必須與WLC RADIUS的共用金鑰相符。

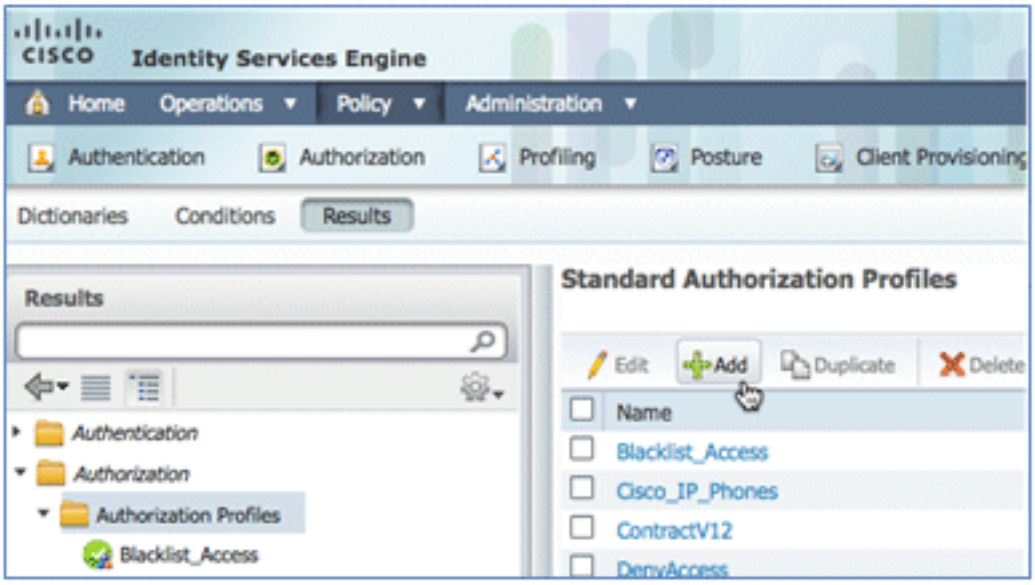


25. 按一下「**Submit**」。

26. 導覽至**ISE > Policy > Policy Elements > Results**。

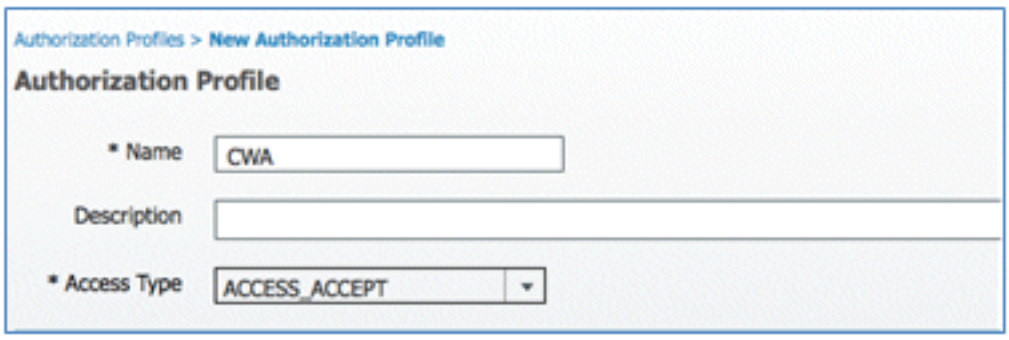


27. 展開Results和Authorization，按一下Authorization Profiles，然後為新配置檔案按一下Add。



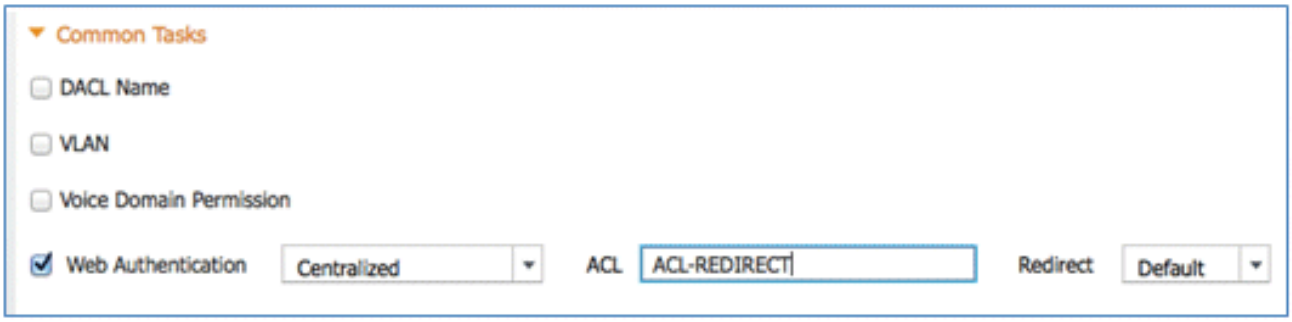
28. 為此配置檔案指定以下值：

名稱：CWA

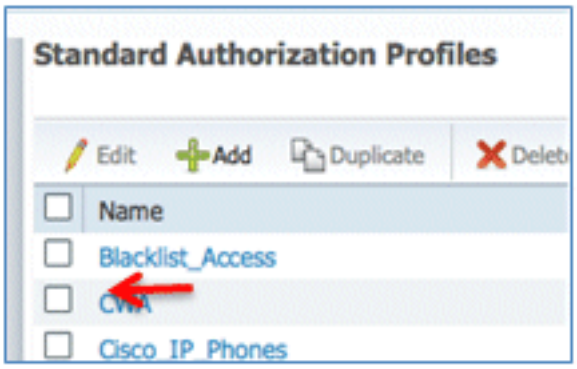


啟用Web驗證（覈取方塊為選中狀態）：

Web驗證：集中ACL: **ACL-REDIRECT**（必須與WLC預先驗證ACL名稱相符。）重定向：默認



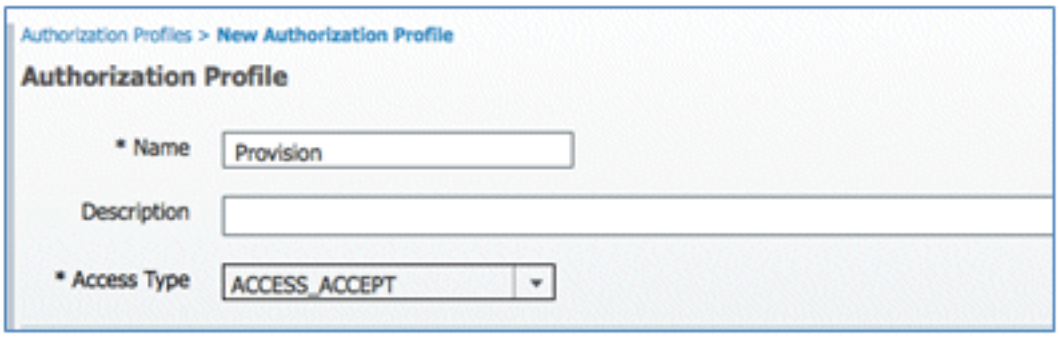
29. 按一下**Submit**，並確認已新增CWA授權配置檔案。



30. 按一下**Add**以建立新的授權設定檔。

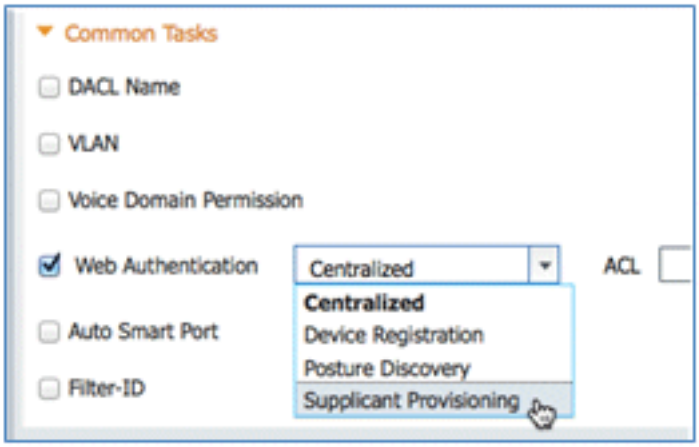
31. 為此配置檔案指定以下值：

名稱：**配置**

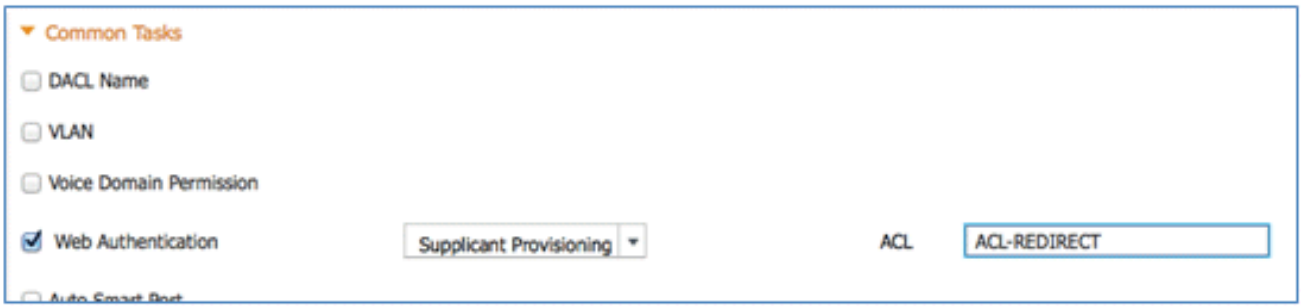


啟用Web驗證（覈取方塊為選中狀態）：

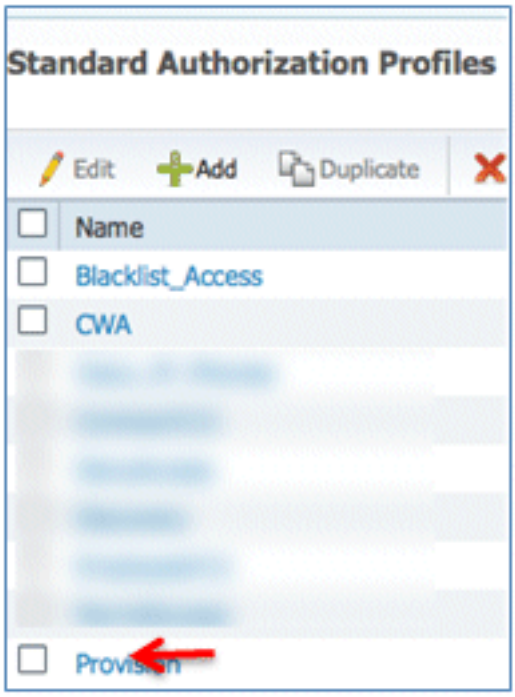
Web驗證值：請求**方調配**



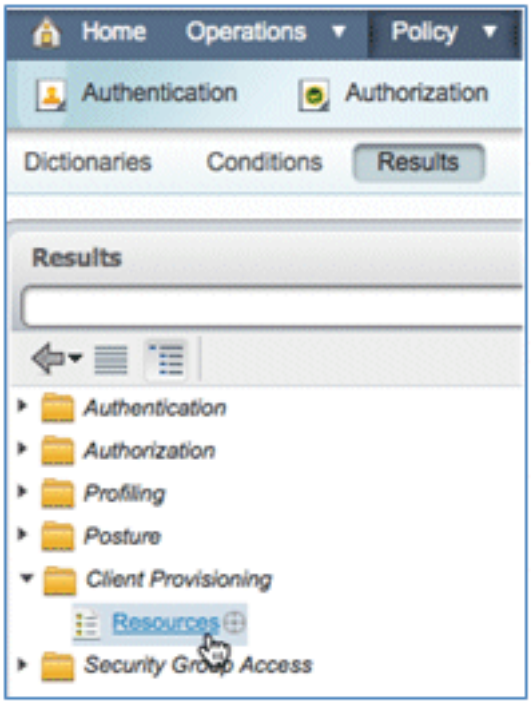
ACL: **ACL-REDIRECT**（必須與WLC預先驗證ACL名稱相符。）



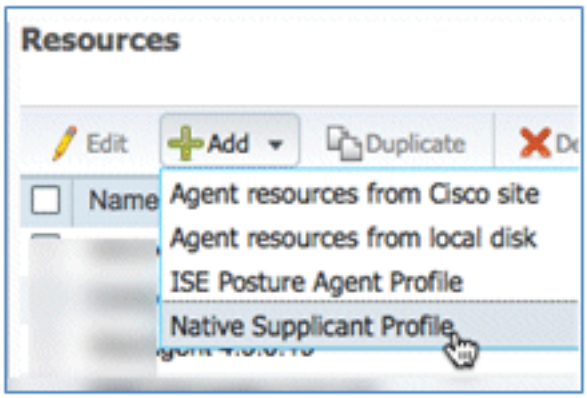
32. 按一下**Submit**，並確認已新增Provision授權配置檔案。



33. 在「結果」中向下滾動，展開**Client Provisioning**，然後按一下**Resources**。



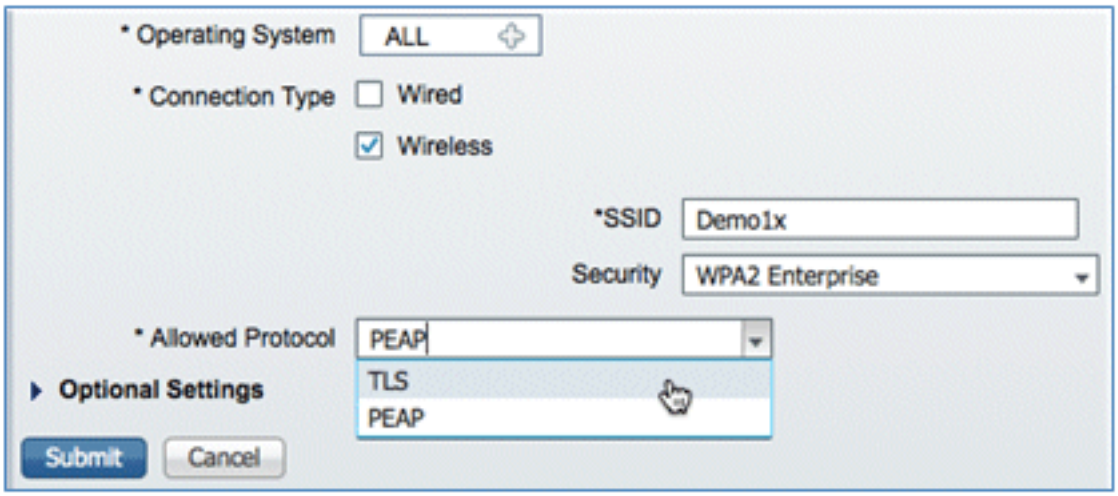
34. 選擇**Native Supplicant Profile**。



35. 為配置檔案指定名稱**WirelessSP**（在本例中）。

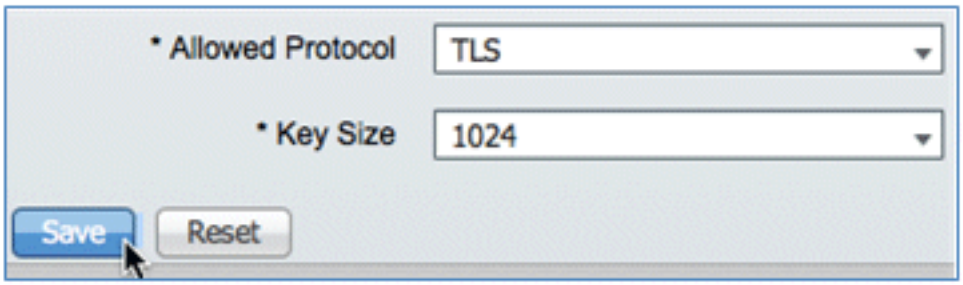
36. 輸入以下值：

連線型別：**無線**SSID: **Demo1x**（此值來自WLC 802.1x WLAN配置）允許的協定：**TLS**金鑰大小：**1024**

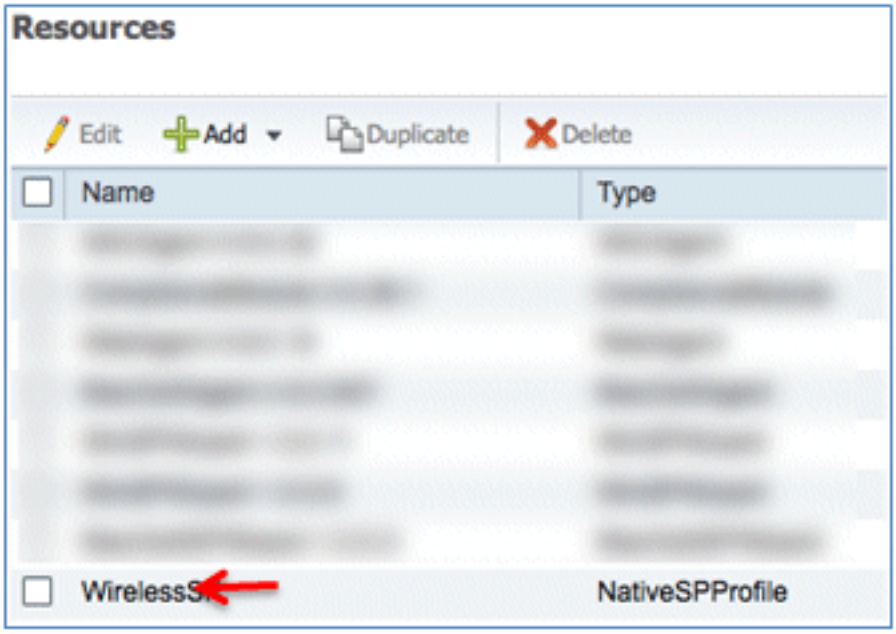


37. 按一下「**Submit**」。

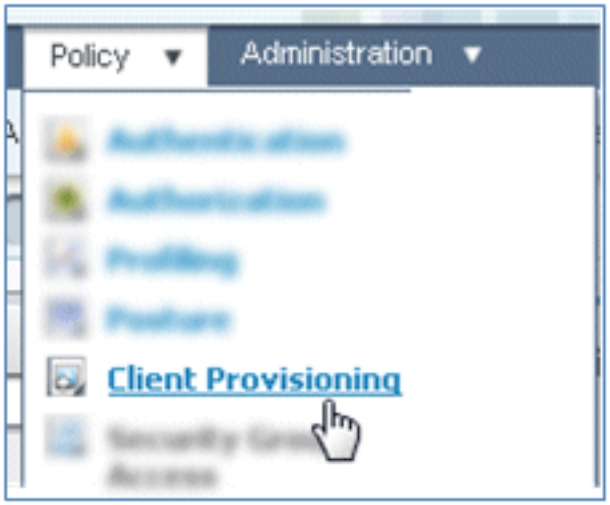
38. 按一下「**Save**」。



39. 確認已新增新配置檔案。

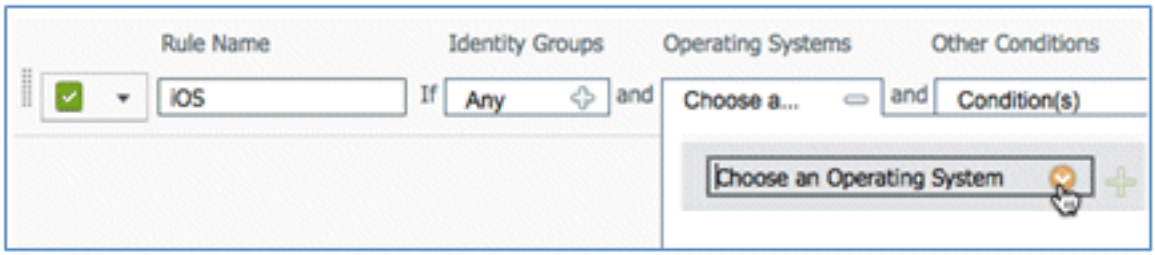


40. 導覽至**Policy > Client Provisioning**。

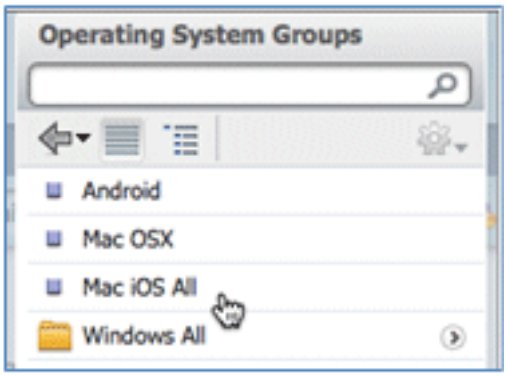


41. 為iOS裝置的調配規則輸入以下值：

規則名稱：**iOS**身份組：任**意**

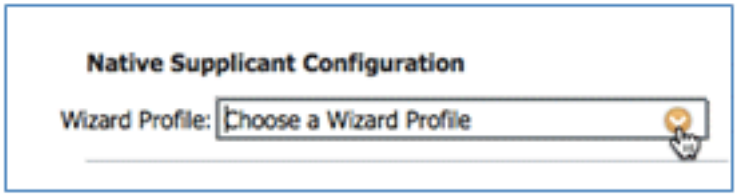


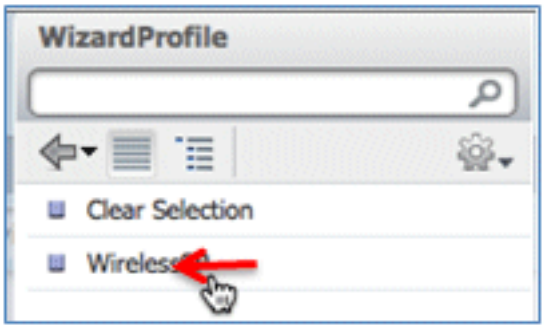
作業系統：**Mac iOS All**



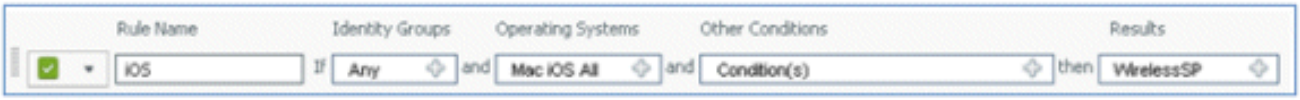
結果：**WirelessSP**（這是之前建立的本地請求方配置檔案）

導覽至**Results > Wizard Profile**（下拉選單）**> WirelessSP**。

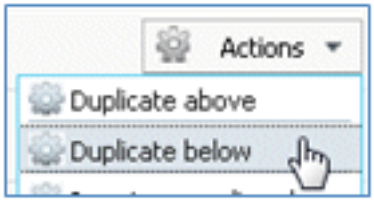




42. 確認已新增iOS設定配置檔案。

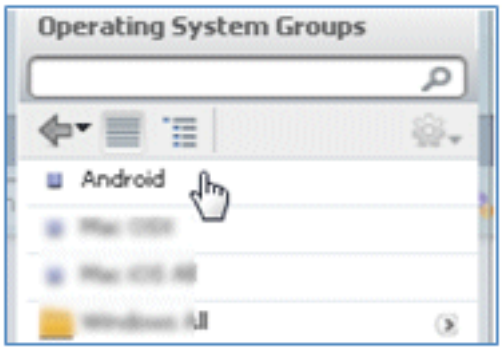


43. 在第一個規則的右側，找到「操作」(Actions)下拉選單，然後選擇**Duplicate below**（或以上）。



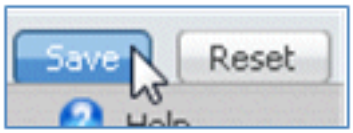
44. 將新規則的Name更改為**Android**。

45. 將作業系統更改為**Android**。

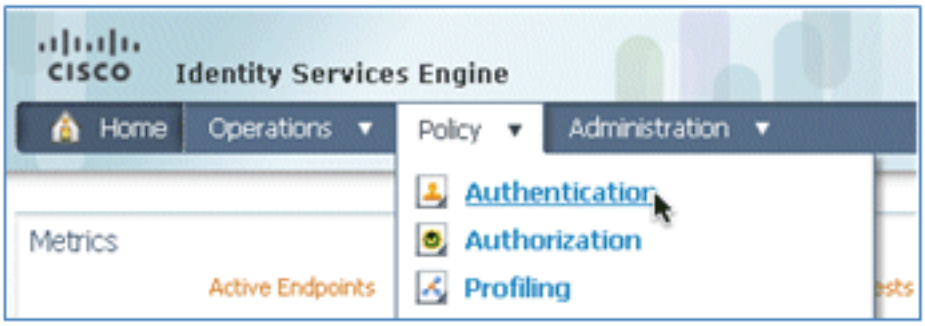


46. 保留其他值不變。

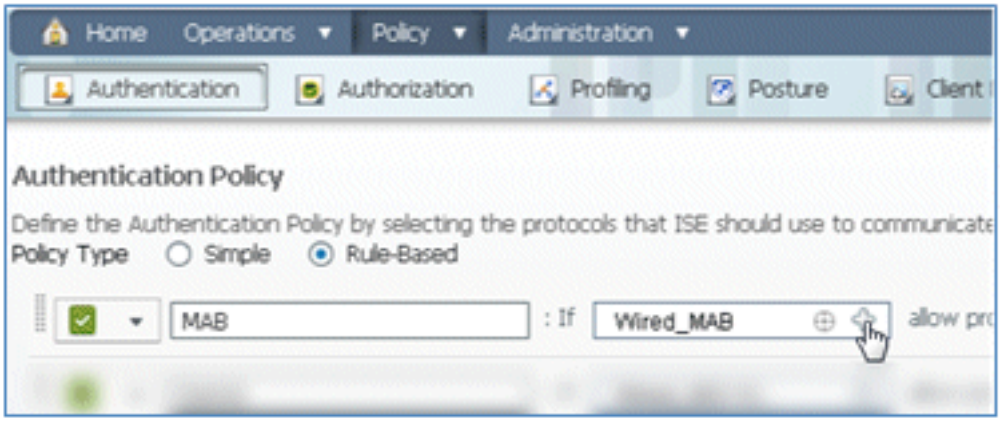
47. 按一下**Save**（左下螢幕）。



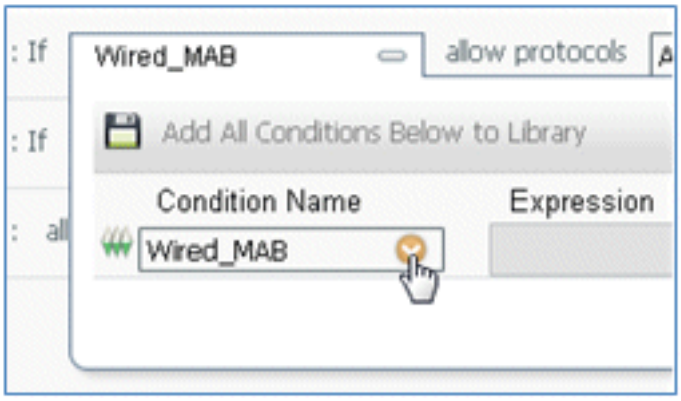
48. 導覽至**ISE > Policy > Authentication**。



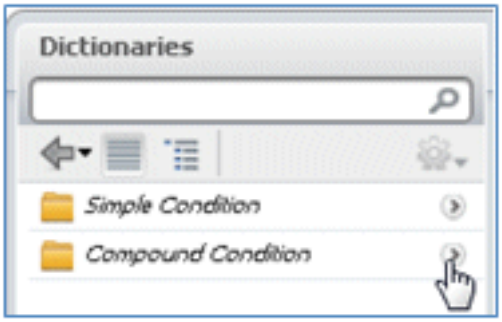
49. 修改條件以包括Wireless_MAB，然後展開**Wired_MAB**。



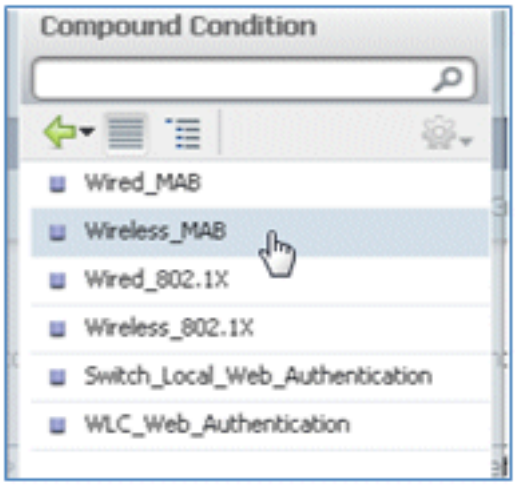
50. 按一下**Condition Name**下拉選單。



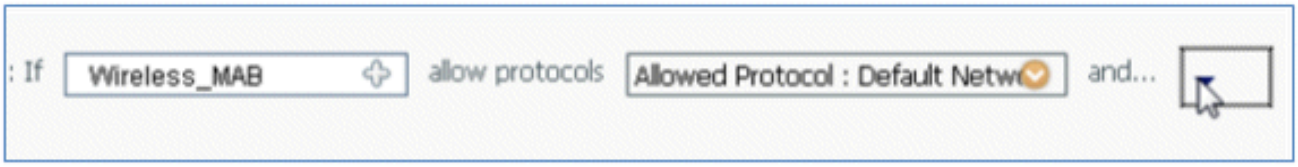
51. 選擇**Dictionaries > Compound Condition**。



52. 選擇**Wireless_MAB**。

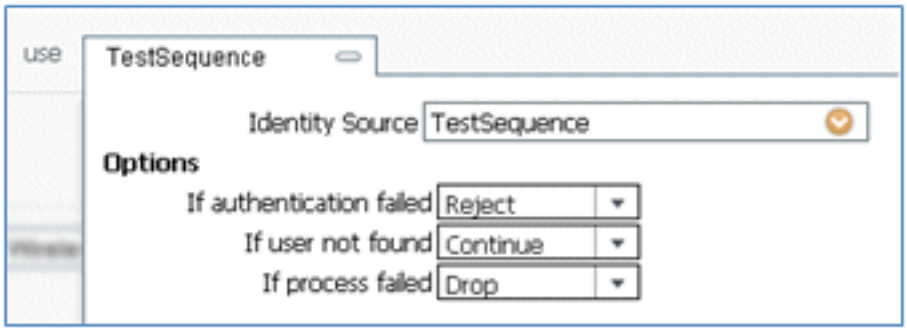


53. 在規則的右側，選擇要展開的箭頭。

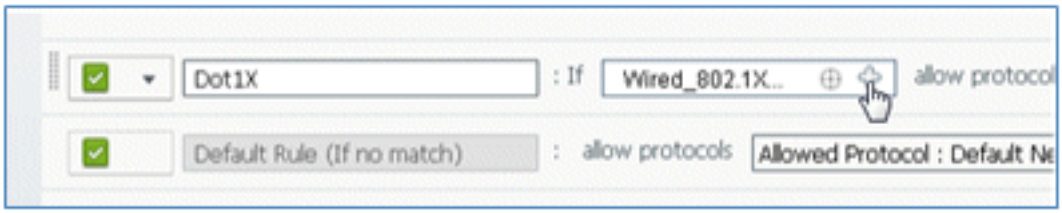


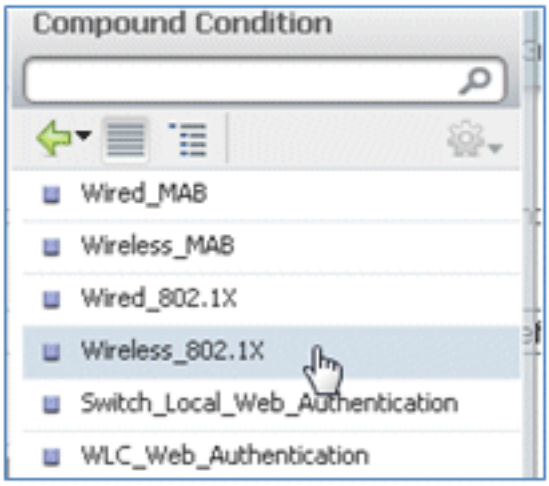
54. 從下拉選單中選擇以下值：

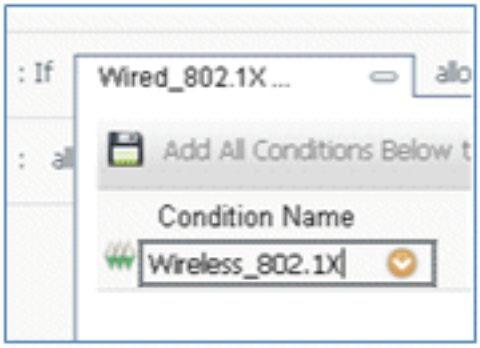
身份源：**TestSequence**（這是之前建立的值）如果身份驗證失敗：拒絕如果找不到使用者：繼續如果進程失敗：**Drop**



55. 轉到**Dot1X**規則，然後更改以下值：

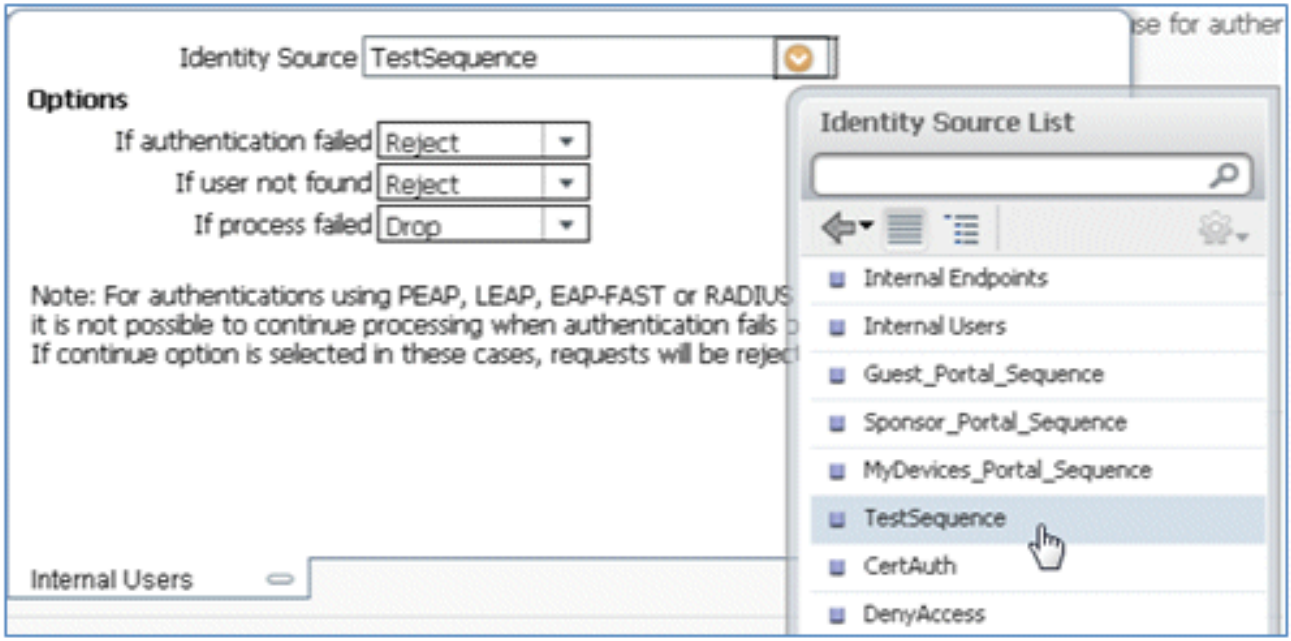






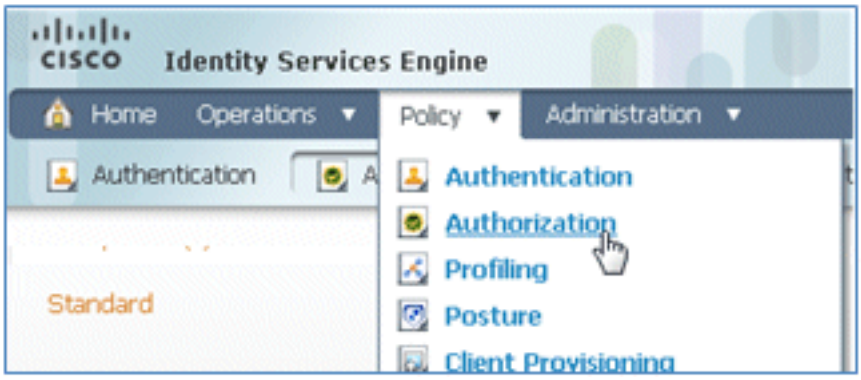
條件:**Wireless_802.1X**

身份源：測**試**

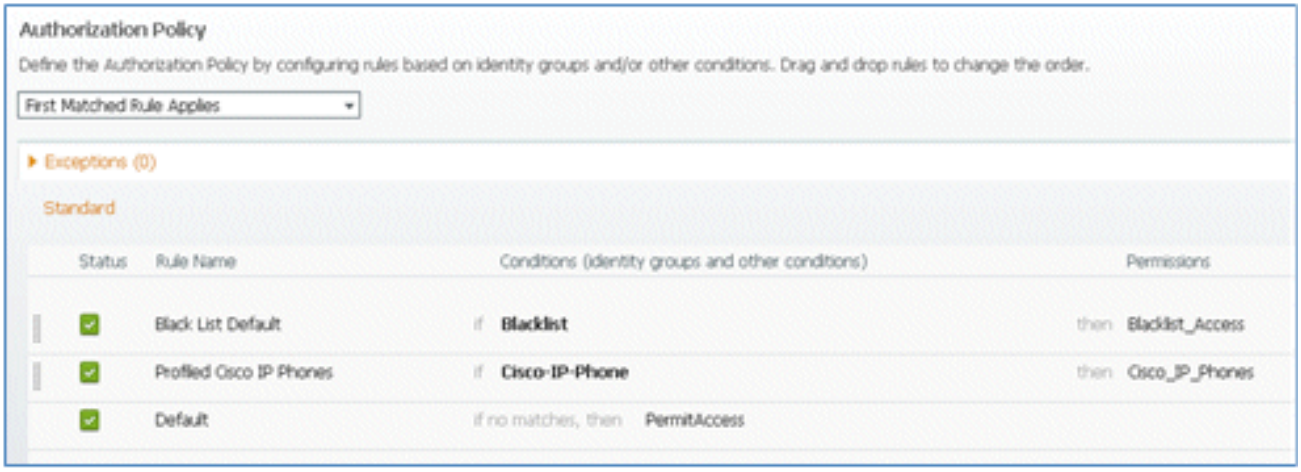


56. 按一下「**Save**」。

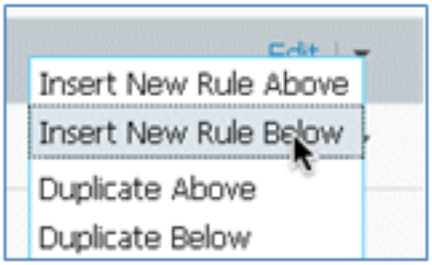
57. 導覽至**ISE > Policy > Authorization**。



58. 預設規則（如Black List Default、Profiled和Default）已在安裝中配置；前兩個規則可以忽略；預設規則將在以後編輯。

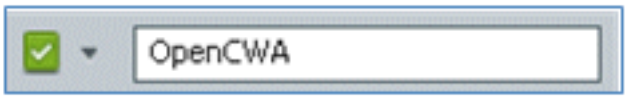


59. 在第二個規則（已分析的Cisco IP電話）的右側，點選Edit旁邊的向下箭頭，然後選擇**Insert New Rule Below**。

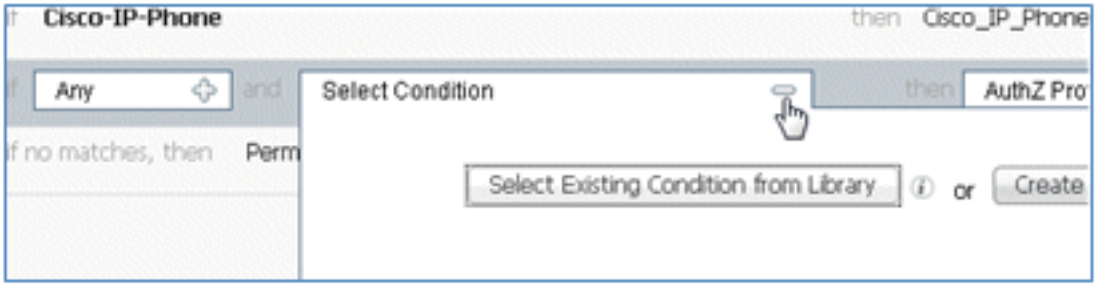


新增新的標準規則編號。

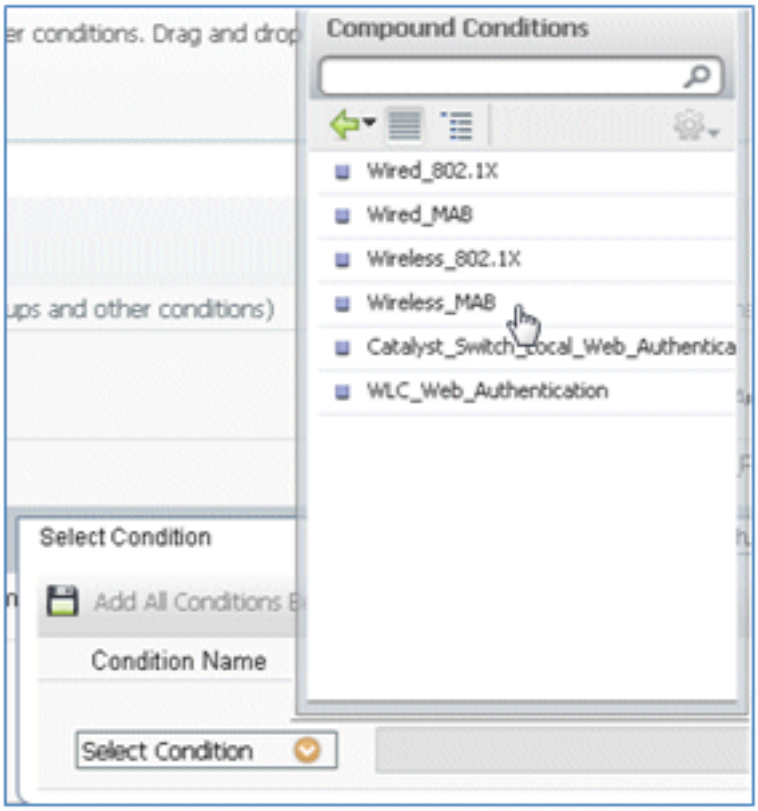
60. 將Rule Name從Standard Rule #更改為**OpenCWA**。此規則在開放式WLAN（雙SSID）上為進入訪客網路以便調配裝置的使用者啟動註冊過程。



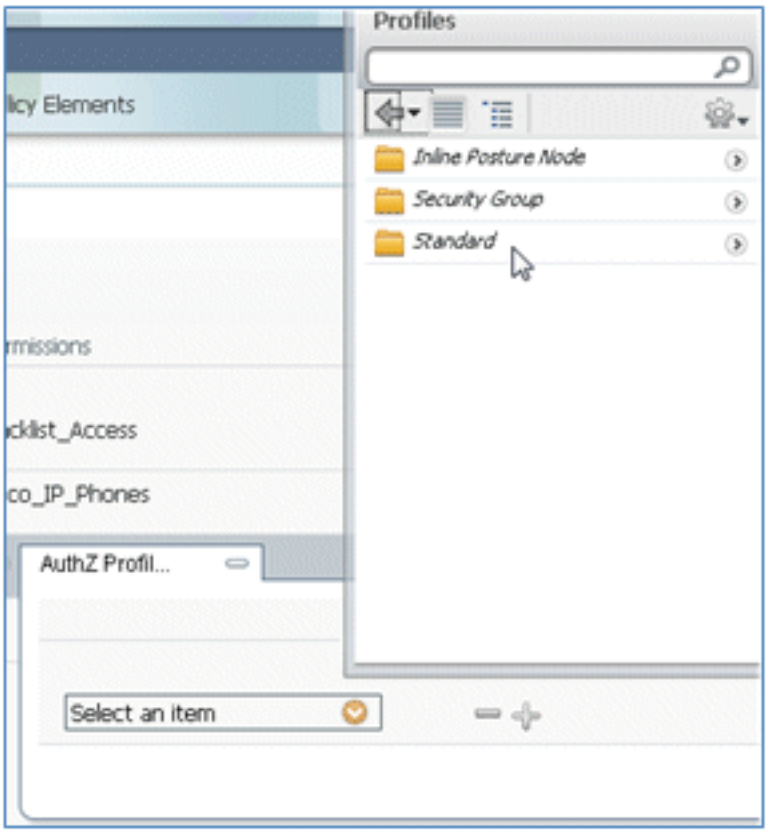
61. 按一下「條件」的**加號(+)**，然後按一下「**從庫中選擇現有條件**」。



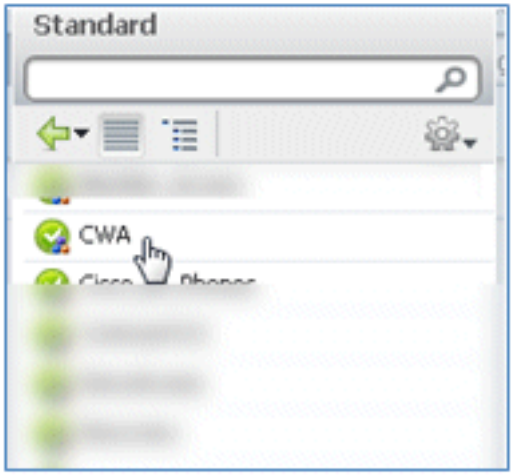
62. 選擇**Compound Conditions > Wireless_MAB**。



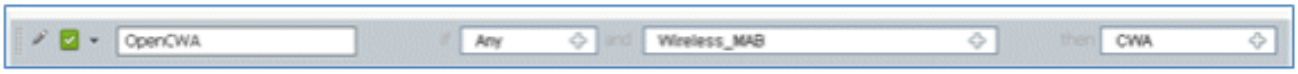
63. 在AuthZ配置檔案中，按一下加號**(+)**，然後選擇**Standard**。



64. 選擇標準**CWA**（這是之前建立的授權配置檔案）。



65. 確認新增規則時使用了正確的條件和授權。



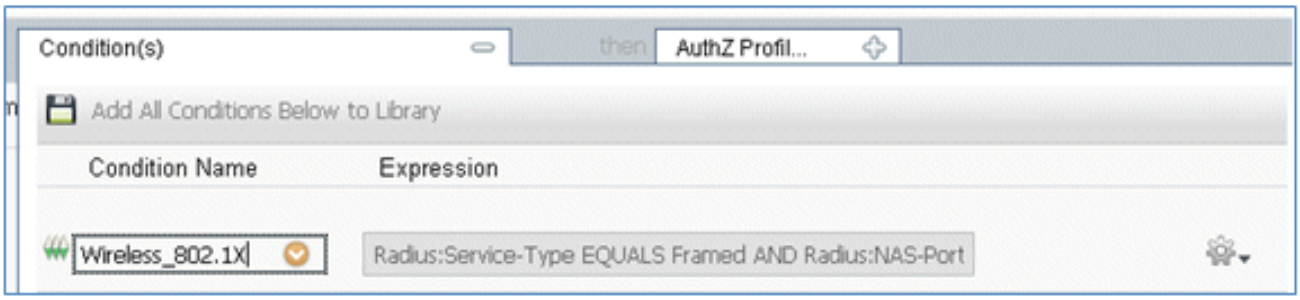
66. 按一下**Done**（在規則的右側）。

67. 在同一規則的右側，按一下「Edit（編輯）」旁邊的向下箭頭，然後選擇「**Insert New Rule**

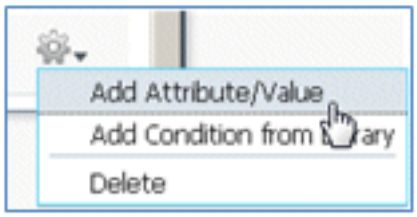
Below（在下面插入新規則）」。

68. 將Rule Name從Standard Rule #更改為**PEAPrule**（在本例中）。此規則用於PEAP（也用於單SSID方案）以檢查沒有傳輸層安全(TLS)的802.1X身份驗證，以及網路請求方調配是使用之前建立的調配授權配置檔案啟動的。

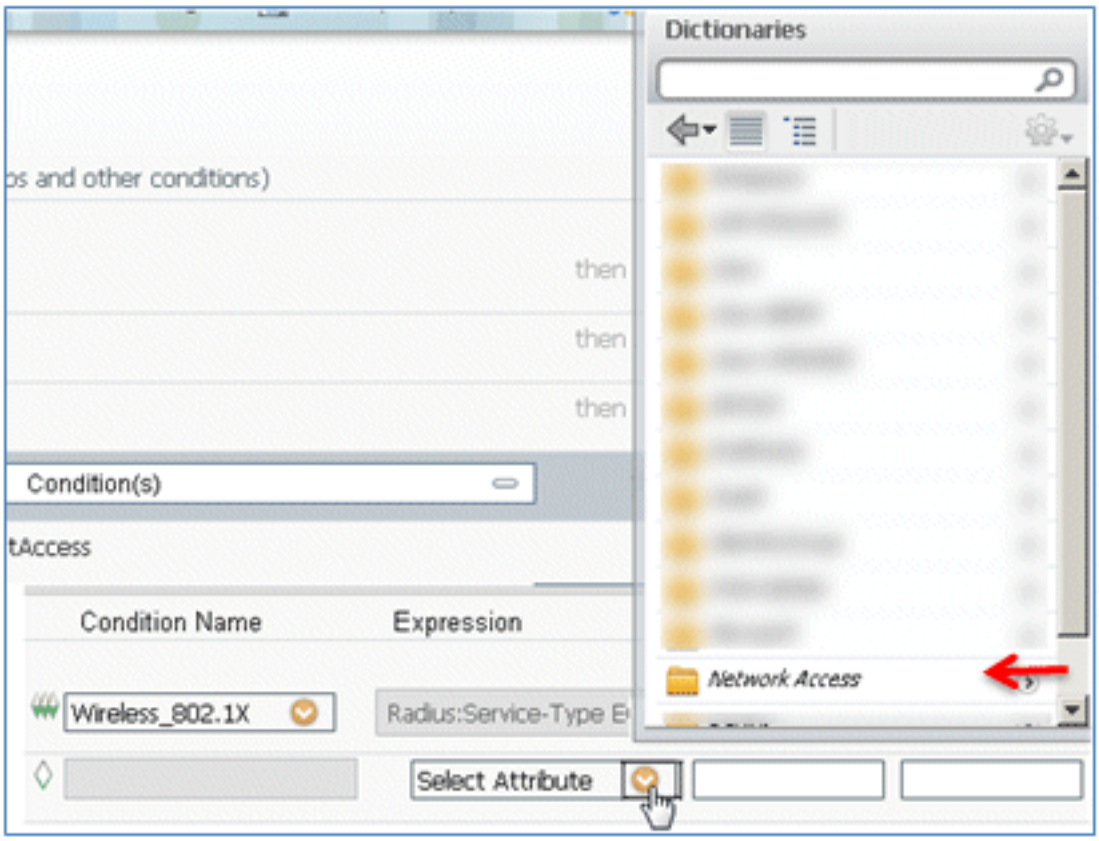
69. 將「Condition（條件）」更改為**Wireless_802.1X**。



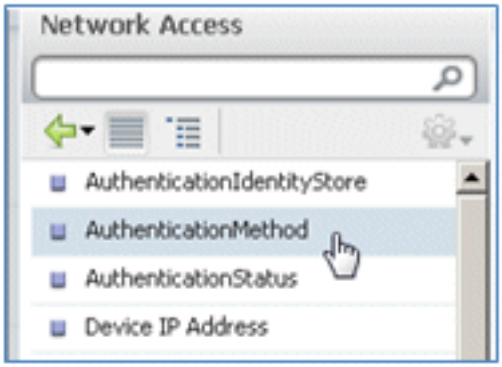
70. 按一下條件右側的齒輪圖示，然後選擇**Add Attribute/Value**。這是一個「and」條件，而不是「or」條件。



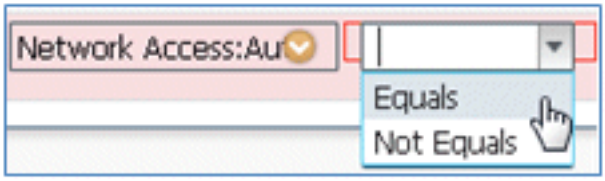
71. 找到並選擇**Network Access**。



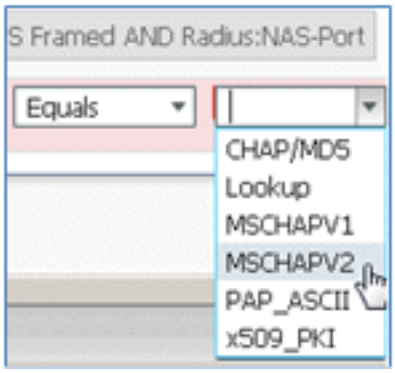
72. 選擇**AuthenticationMethod**，然後輸入以下值：



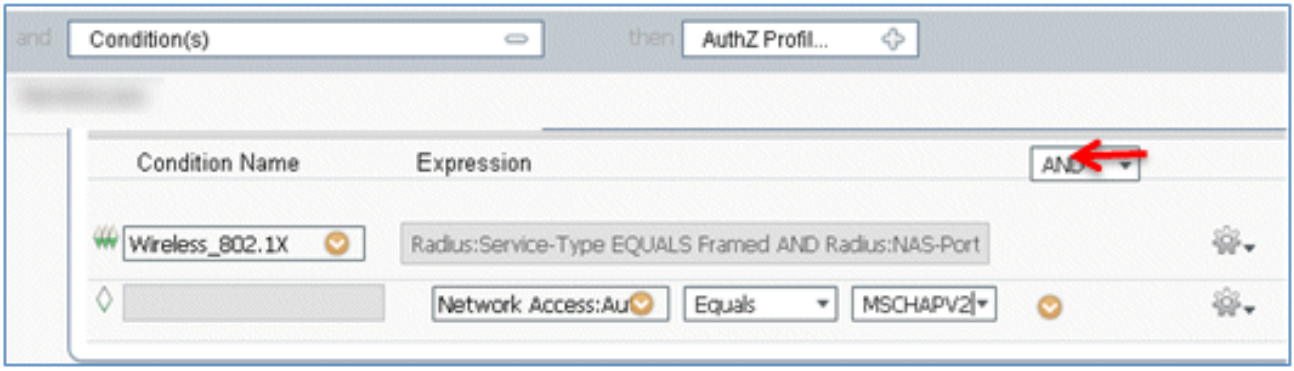
AuthenticationMethod：**等於**



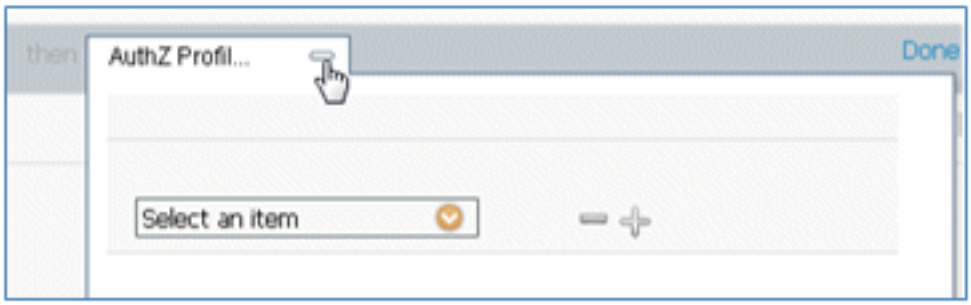
選擇MSCHAPV2。

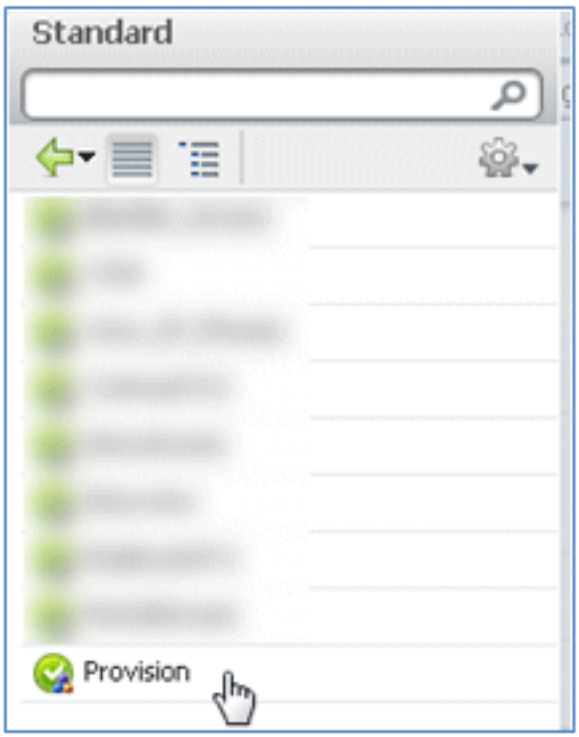


這是規則的示例；請務必確認條件是AND。



73. 在AuthZ設定檔中，選擇**Standard > Provision**（這是先前建立的授權設定檔）。

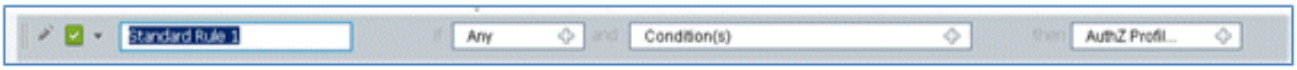




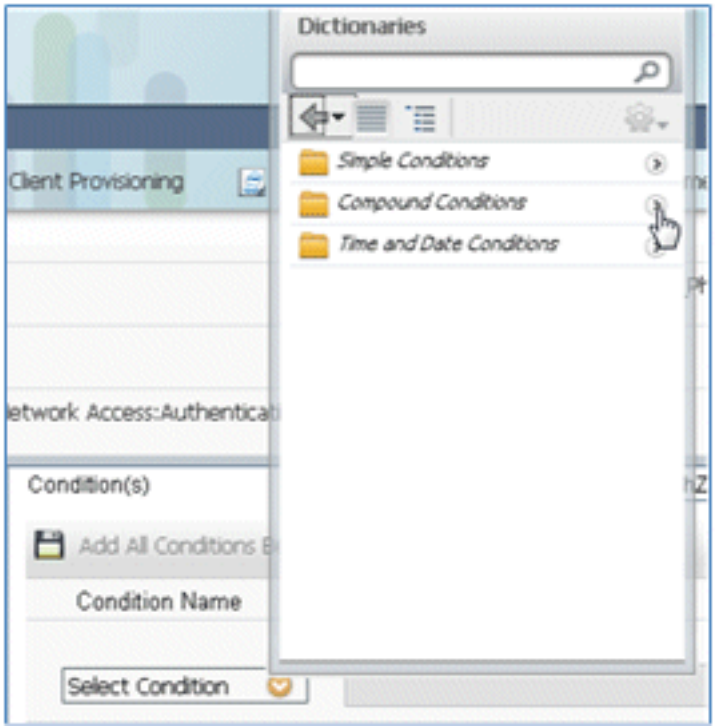
74. 按一下「**完成**」。

75. 在PEAPrule的右側，點選Edit旁邊的向下箭頭，然後選擇**Insert New Rule Below**。

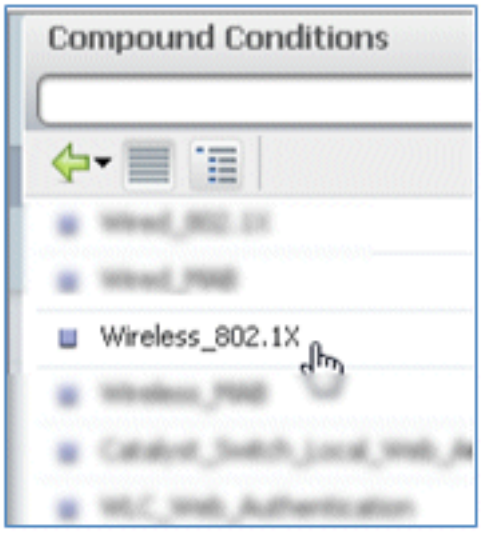
76. 將Rule Name從Standard Rule #更改為**AllowRule**（在本例中）。將使用此規則來允許訪問安裝了證書的註冊裝置。



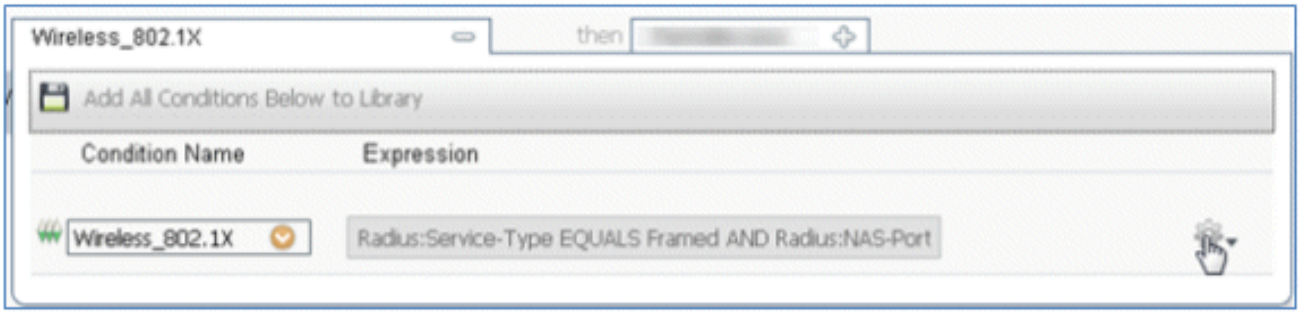
77. 在「條件」下，選擇**複合條件**。



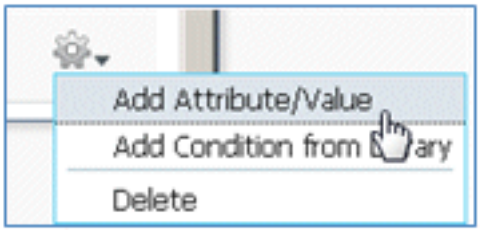
78. 選擇**Wireless_802.1X**。



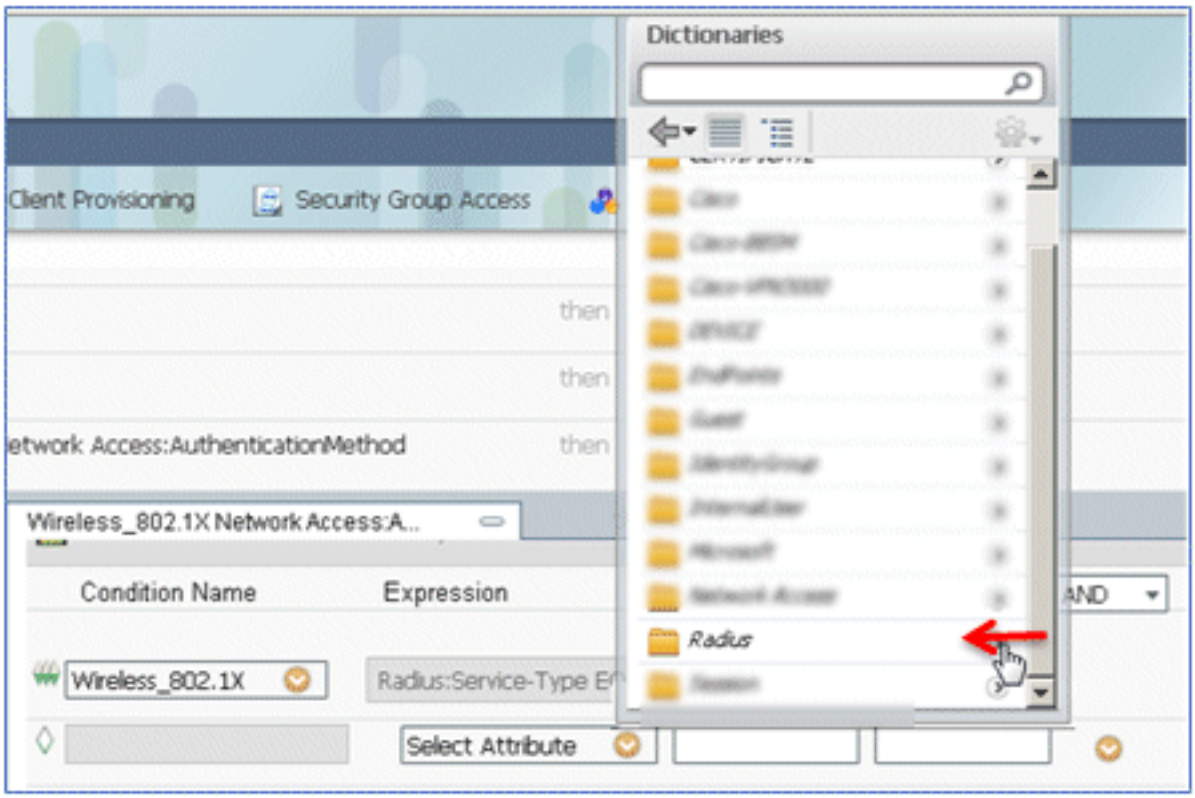
79. 新增AND屬性。



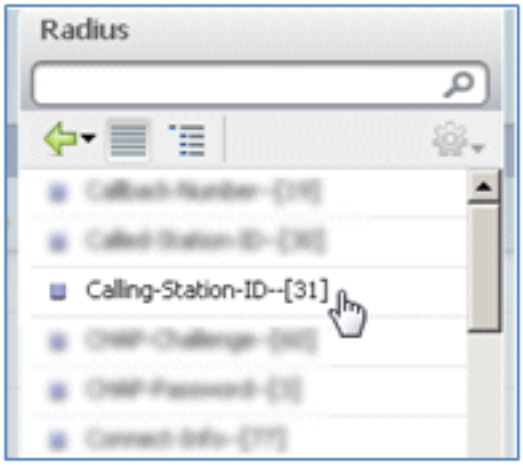
80. 按一下條件右側的齒輪圖示，然後選擇**Add Attribute/Value**。



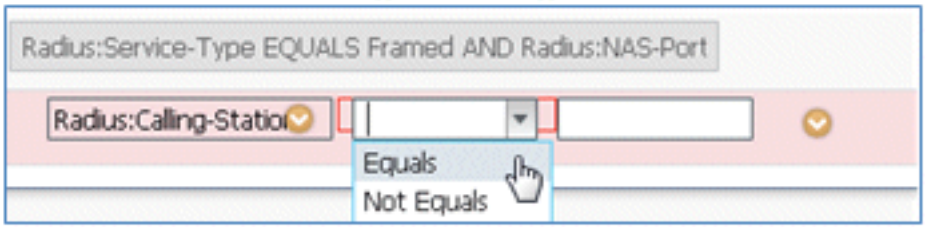
81. 找到並選擇**Radius**。



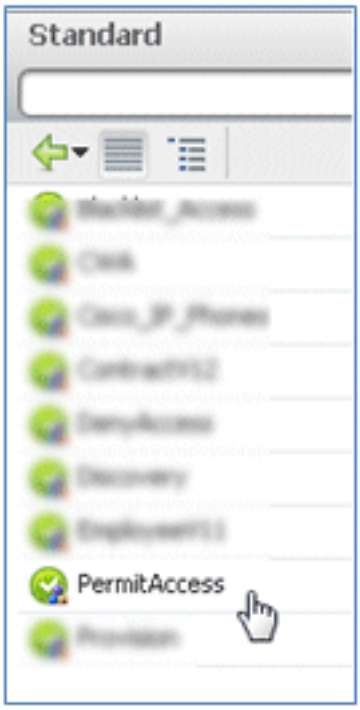
82. 選擇Calling-Station-ID—[31]。



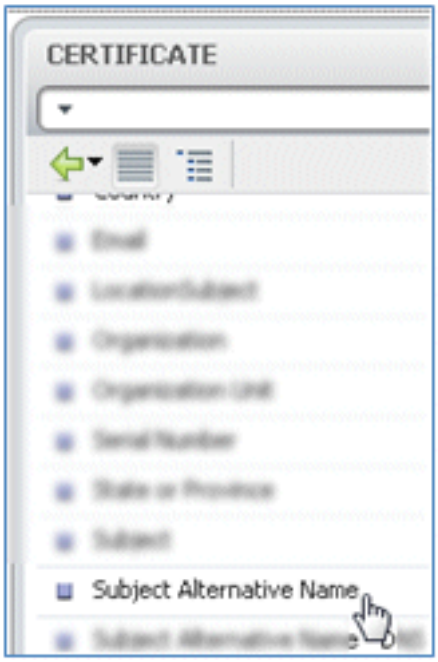
83. 選擇Equals。



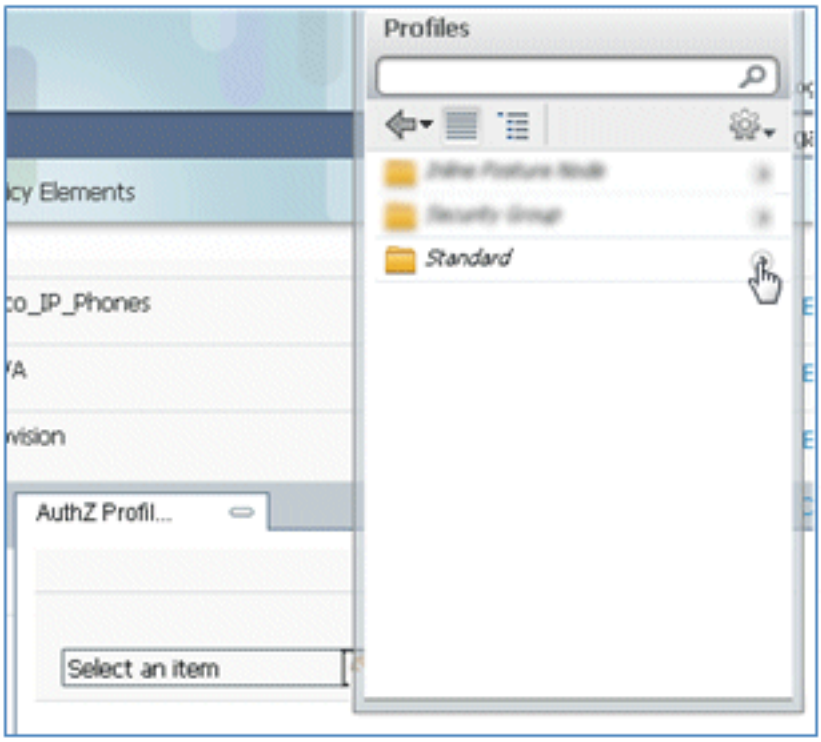
84. 轉到CERTIFICATE，然後按一下右箭頭。



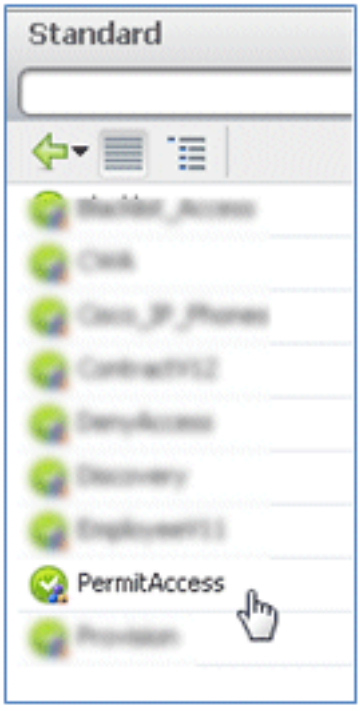
85. 選擇**Subject Alternative Name**。



86. 對於AuthZ配置檔案，請選擇**Standard**。



87. 選擇**Permit Access**。

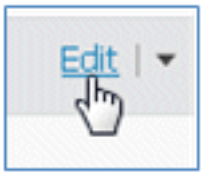


88. 按一下「**完成**」。

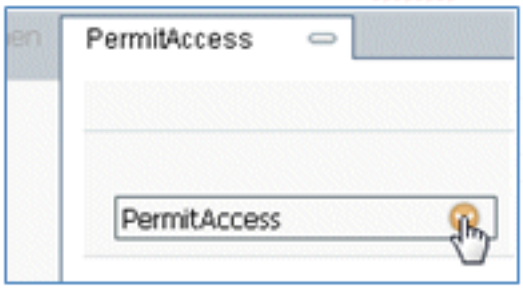
以下是規則的範例：

89. 找到Default規則，將PermitAccess更改為DenyAccess。

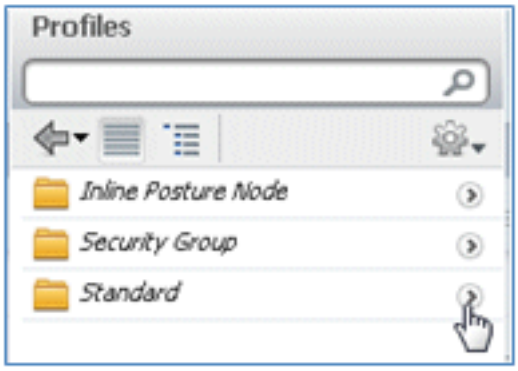
90. 按一下「**Edit**」以編輯「Default」規則。



91. 轉到PermitAccess的現有AuthZ配置檔案。



92. 選擇**Standard**。

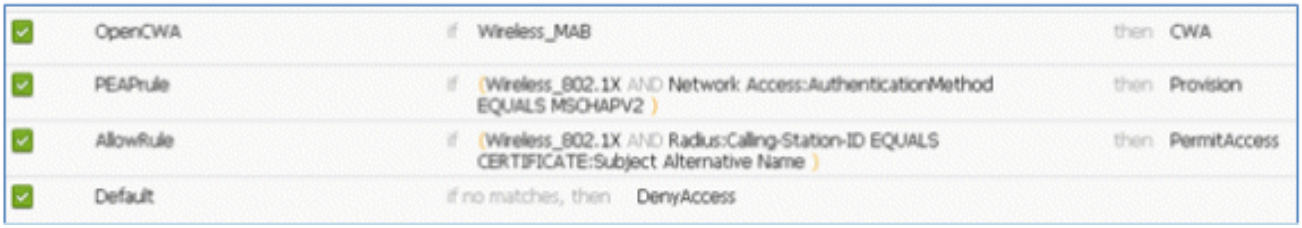


93. 選擇**DenyAccess**。

94. 如果找不到匹配項，請確認預設規則具有DenyAccess。

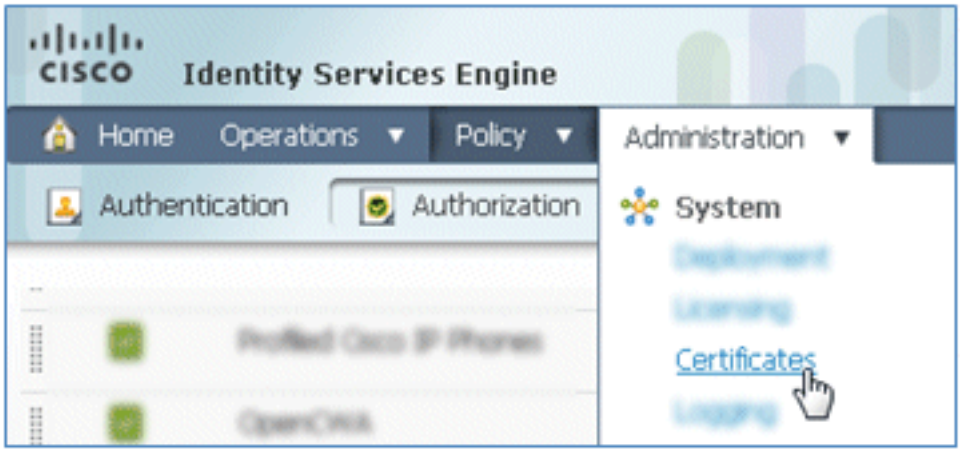
95. 按一下「**完成**」。

這是此測試所需的主要規則的示例；它們適用於單SSID或雙SSID方案。

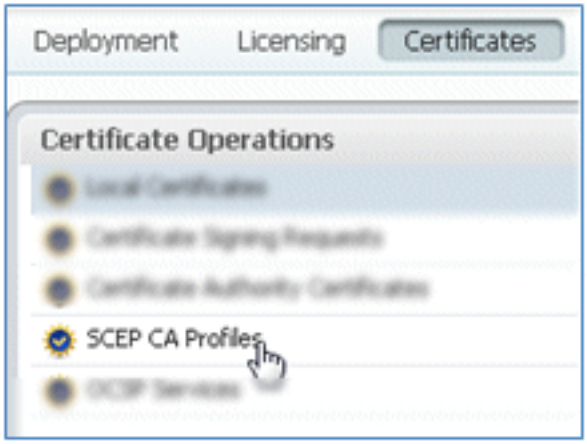


96. 按一下「**Save**」。

97. 導覽至**ISE > Administration > System > Certificates**，以便使用SCEP配置檔案配置ISE伺服器。



98. 在Certificate Operations中，按一下**SCEP CA Profiles**。



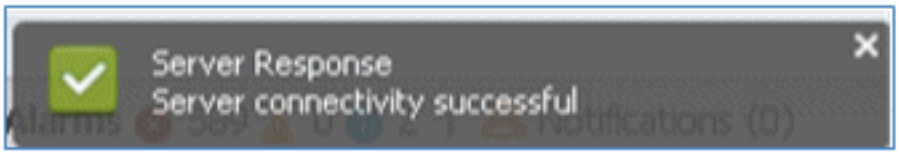
99. 按一下「**Add**」。

100. 為此配置檔案輸入以下值：

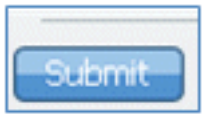
名稱：**mySCEP**（在本例中）URL: **https://<*ca-server*>/CertSrv/mscep/**（請檢查CA伺服器配置中的正確地址。）

101. 按一下**測試連線**以測試SCEP連線的連線。

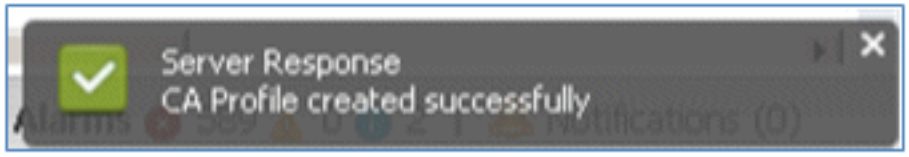
102. 此響應顯示伺服器連線成功。



103. 按一下「**Submit**」。



104. 伺服器響應已成功建立CA配置檔案。



105. 確認已新增SCEP CA配置檔案。

使用者體驗 — 調配iOS

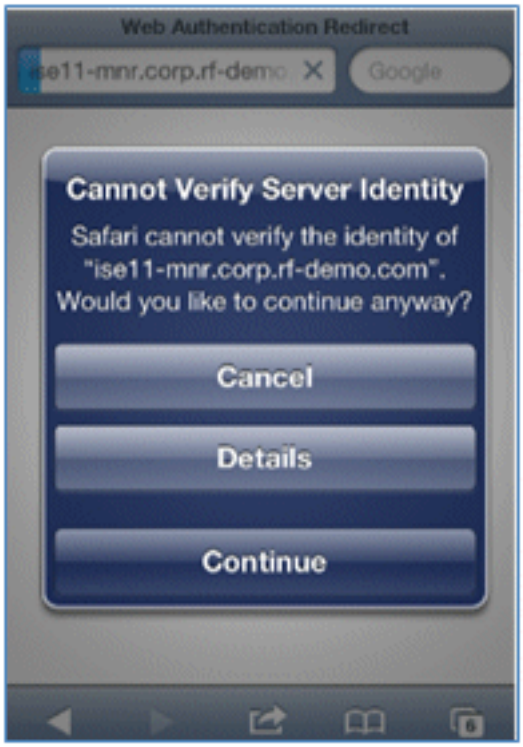
雙SSID

本節介紹雙SSID，並說明如何連線到要布建的訪客，以及如何連線到802.1x WLAN。

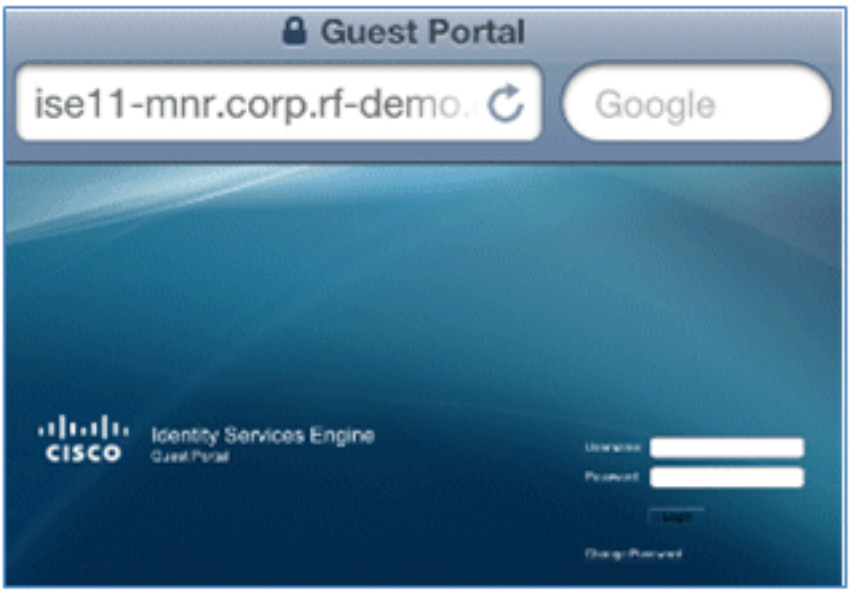
完成以下步驟，以便在雙SSID場景中調配iOS:

1. 在iOS裝置上，轉至**Wi-Fi Networks**，然後選擇**DemoCWA**（在WLC上配置開放式WLAN）。

2. 在iOS裝置上開啟Safari瀏覽器，然後訪問可訪問的URL（例如，內部/外部Web伺服器）。ISE會將您重定向到門戶。按一下「**Continue**」（繼續）。



3. 系統會將您重新導向至訪客輸入網站以登入。



4. 使用AD使用者帳戶和密碼登入。出現提示時，安裝CA配置檔案。

5. 按一下**Install** CA伺服器的受信任證書。

6. 配置式安裝完成後，按一下**Done**。

7. 返回瀏覽器，然後按一下**Register**。記下包含裝置MAC地址的裝置ID。

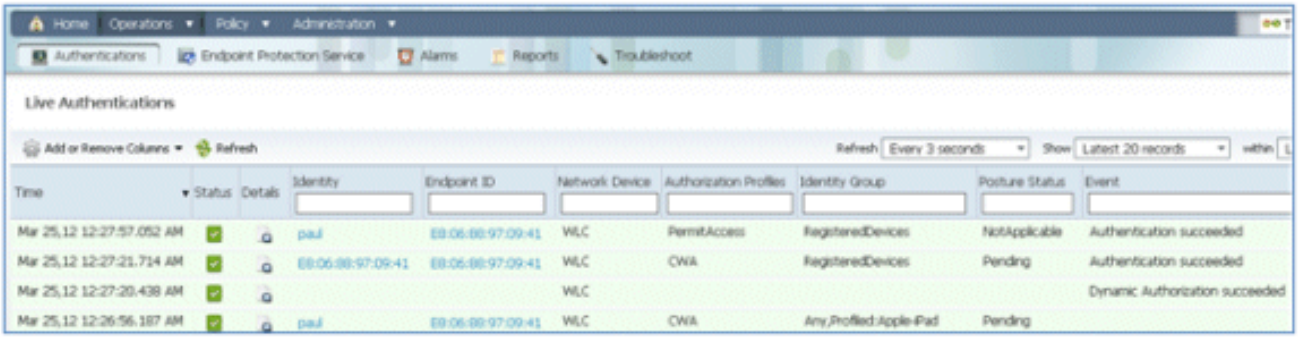
8. 按一下「**Install**」以安裝已驗證的設定檔。

9. 按一下「**Install Now**」。

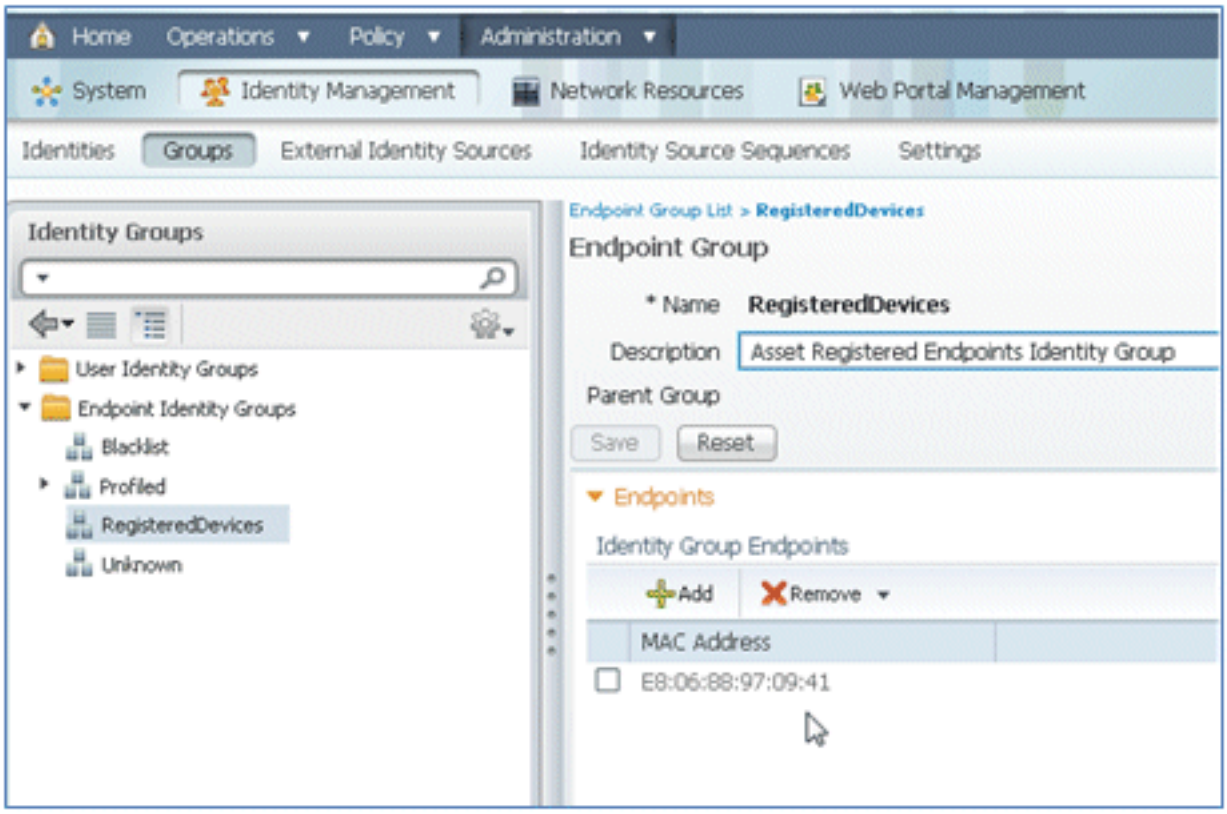
10. 完成該過程後，WirelessSP配置檔案確認已安裝該配置檔案。按一下「**完成**」。

11. 轉到**Wi-Fi網路**，將網路更改為**Demo1x**。您的裝置現已連線並使用TLS。

12. 在ISE上，導航到**操作 > 身份驗證**。事件顯示裝置連線到開放訪客網路的過程，使用請求方調配完成註冊過程，並在註冊後允許訪問。



13. 導航到ISE > Administration > Identity Management > **Groups > Endpoint Identity Groups > RegisteredDevices**。MAC地址已新增到資料庫。

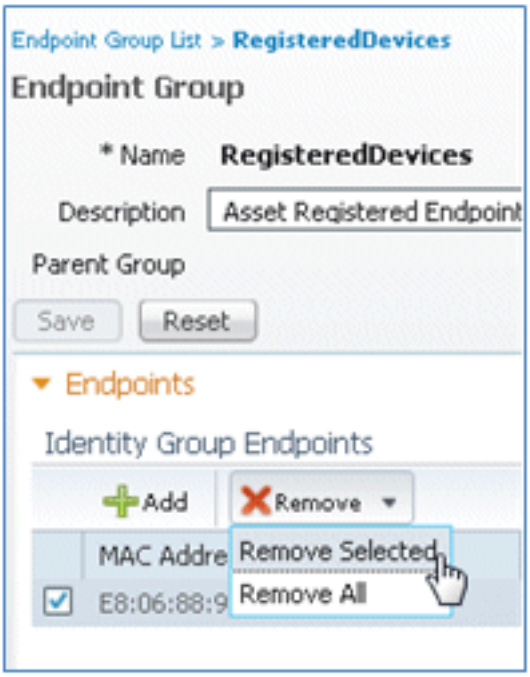


單SSID

本節介紹單SSID，並說明如何直接連線到802.1x WLAN、提供PEAP身份驗證的AD使用者名稱/密碼、通過訪客帳戶調配以及重新連線TLS。

完成以下步驟，以便在單SSID場景中調配iOS:

1. 如果您使用的是同一個iOS裝置，請從已註冊裝置中刪除終端。



2. 在iOS裝置上，導航到**設定 > General > Profiles**。刪除本示例中安裝的配置檔案。

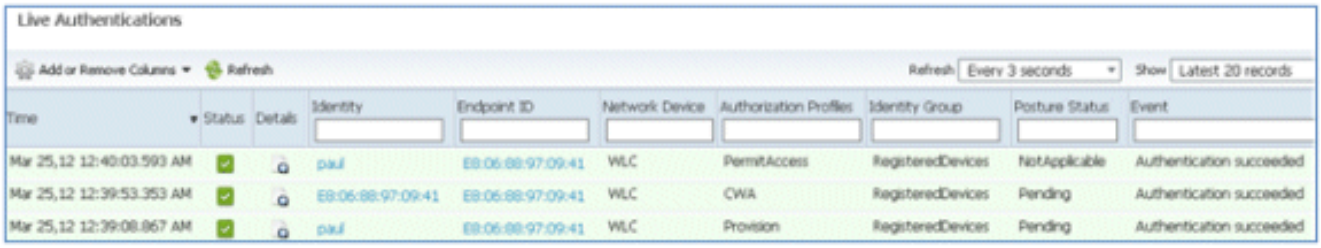
3. 按一下「**Remove**」以移除先前的設定檔。

4. 使用現有的（已清除）裝置或新的iOS裝置直接連線到802.1x。

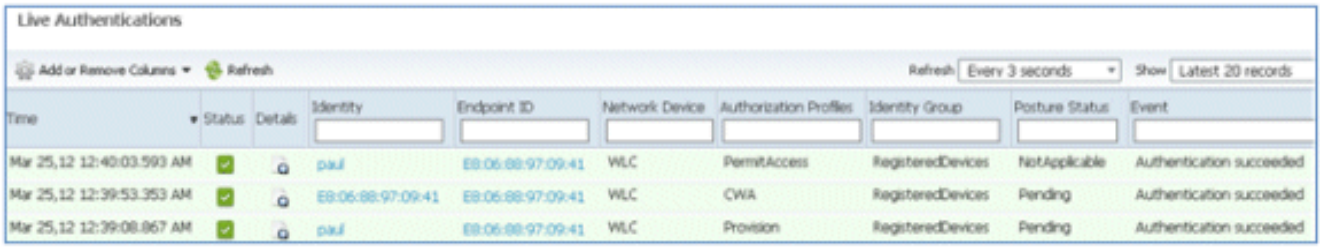
5. 連線到**Dot1x**，輸入使用者名稱和密碼，然後按一下**Join**。

6. 從ISE配置部分重複步驟90和on，直到完全安裝相應的配置檔案。

7. 導覽至ISE > Operations > Authentications以監控流程。此範例顯示使用TLS來布建、斷開並重新連線到同一WLAN時，直接連線到802.1X WLAN的客戶端。



8. 導覽至WLC > Monitor > [Client MAC]。在客戶端詳細資訊中，請注意客戶端處於RUN狀態，其資料交換設定為local，身份驗證設定為Central。對於連線到FlexConnect AP的客戶端而言，情況也是如此。



使用者體驗 — 調配Android

雙SSID

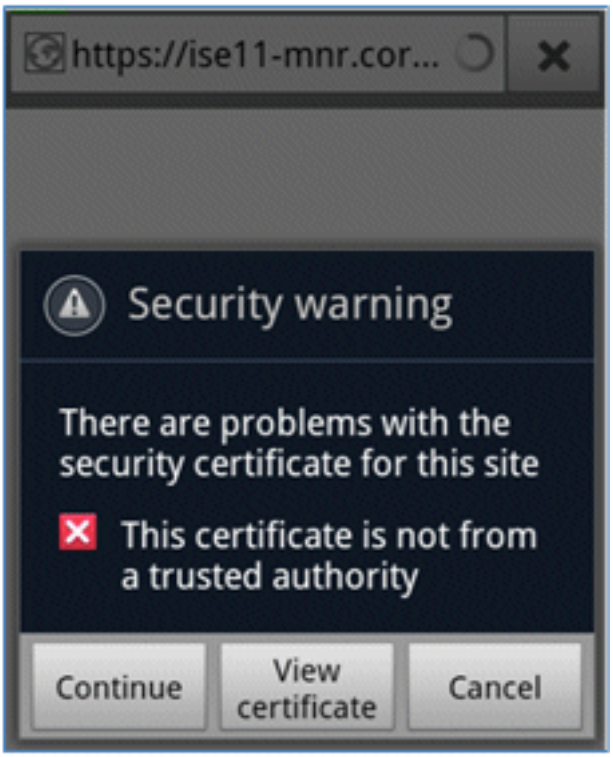
本節介紹雙SSID，並說明如何連線到要布建的訪客，以及如何連線到802.1x WLAN。

Android裝置的連線過程與iOS裝置（單或雙SSID）的連線過程非常相似。然而，一個重要的區別是，Android裝置需要訪問Internet才能訪問Google Marketplace（現在是Google Play）和下載請求者代理。

完成以下步驟，以便在雙SSID場景中調配Android裝置（如本示例中的Samsung Galaxy）：

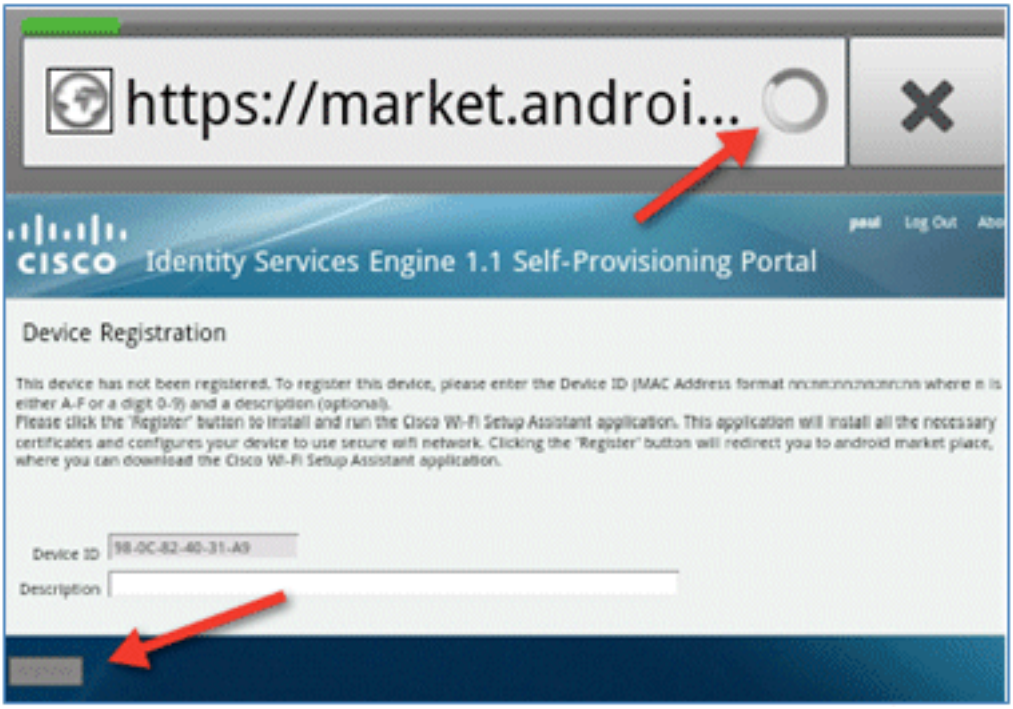
1. 在Android裝置中，使用Wi-Fi連線到**DemoCWA**，然後開啟訪客WLAN。

2. 接受任何證書以連線到ISE。

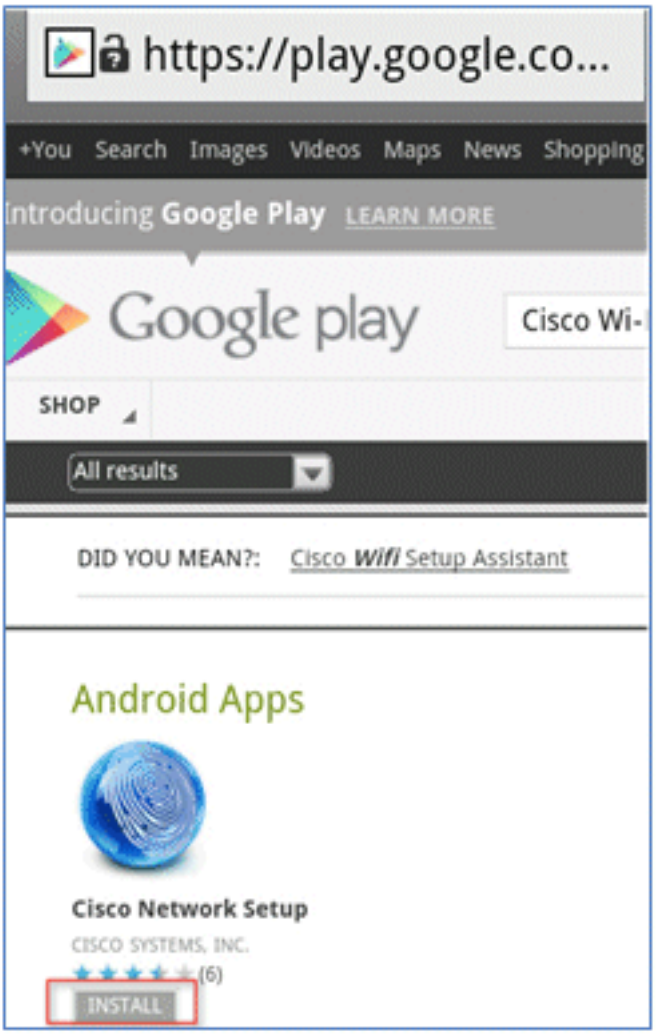


3. 在訪客門戶輸入使用者名稱和密碼以登入。

4. 按一下「**Register**」。裝置嘗試訪問Internet以訪問Google市場。將任何其他規則新增到控制器中的預先驗證ACL（例如ACL-REDIRECT），以便允許存取網際網路。

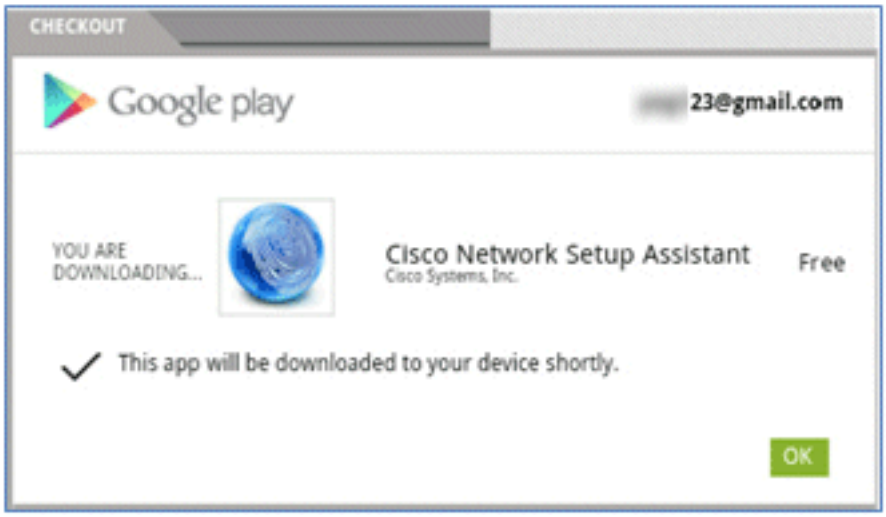


5. Google將思科網路設定列為Android應用。按一下「**INSTALL**」。

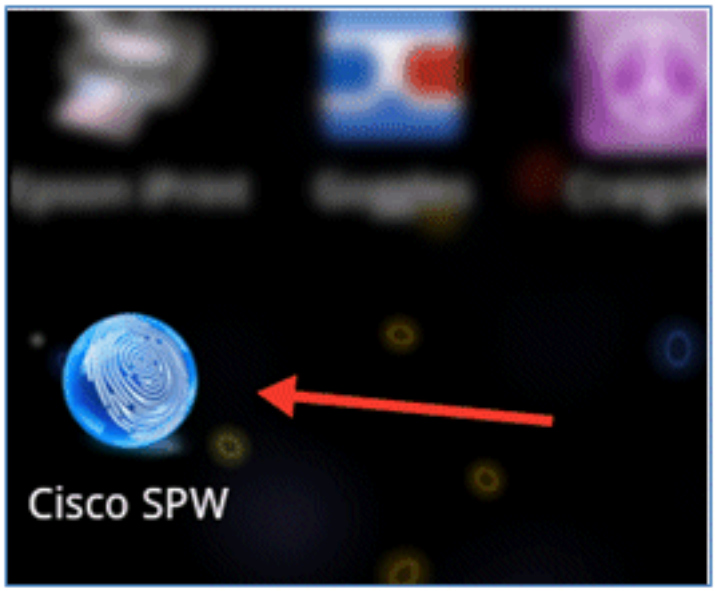


6. 登入Google，然後點選**安裝**。

7. 按一下「OK」（確定）。



8. 在Android裝置上，找到已安裝的Cisco SPW應用，然後將其開啟。



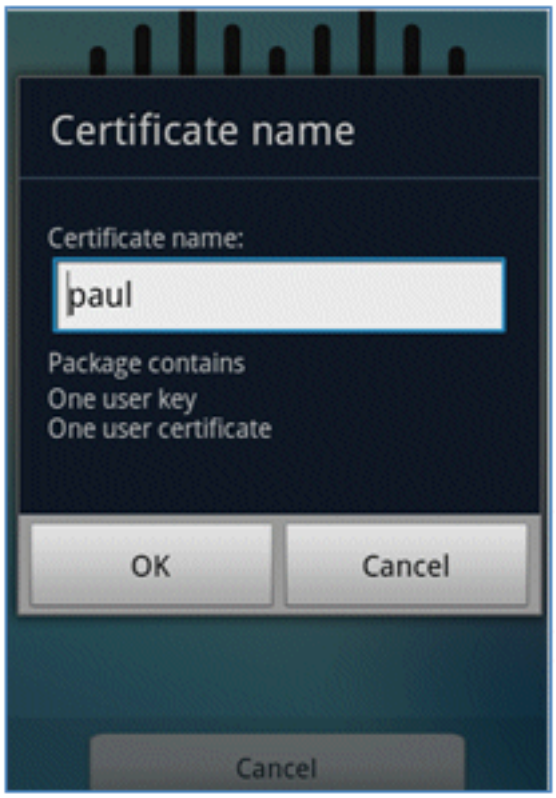
9. 確保您仍然從您的Android裝置登入到訪客門戶。

10. 按一下**開始**以啟動Wi-Fi設定助手。

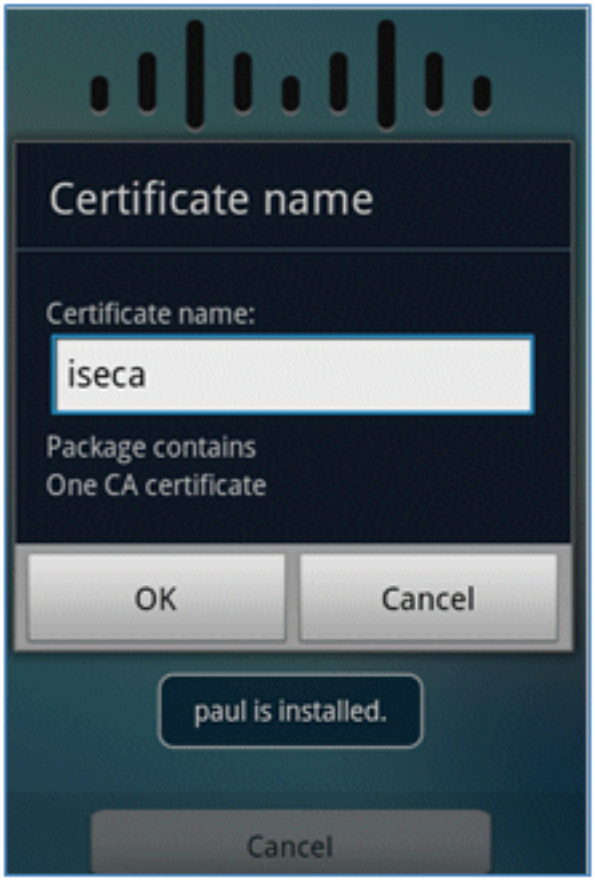
11. Cisco SPW開始安裝證書。

12. 出現提示時，設定憑據儲存的密碼。

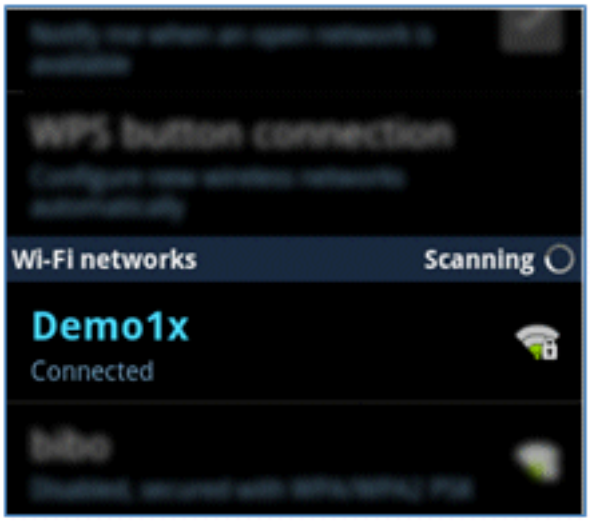
13. Cisco SPW返回證書名稱，其中包含使用者金鑰和使用者證書。按一下「OK」以確認。



14. Cisco SPW繼續並提示輸入另一個證書名稱，該名稱包含CA證書。輸入名稱**iseca**（在本例中），然後按一下**OK**以繼續。



15. Android裝置現已連線。

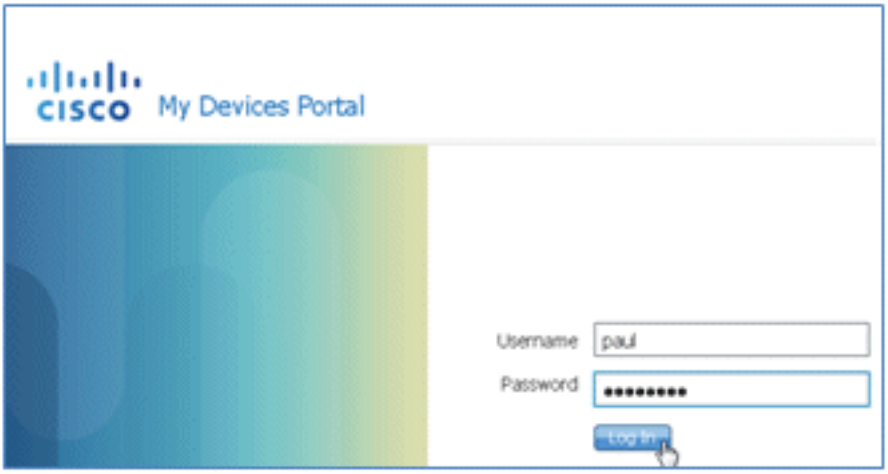


我的裝置入口網站

My Devices Portal允許使用者在裝置丟失或被盜的情況下將先前已註冊的裝置列入黑名單。此外，還允許使用者在需要時重新登記。

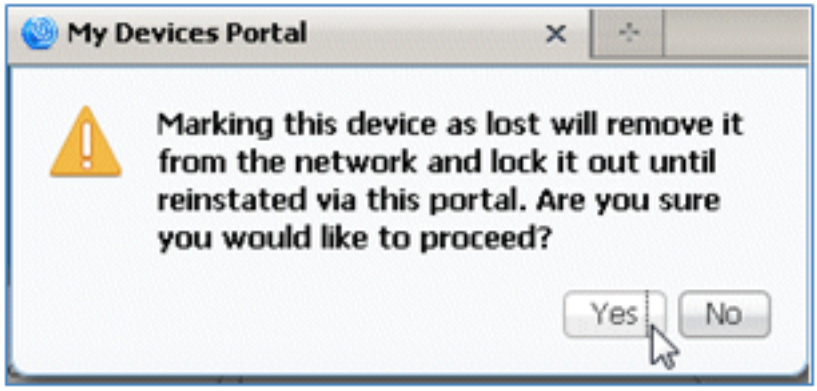
完成以下步驟以將裝置列入黑名單：

1. 若要登入My Devices Portal，請開啟瀏覽器，連線到https://ise-server:8443/mydevices（注意連線埠號碼8443），然後使用AD帳戶登入。



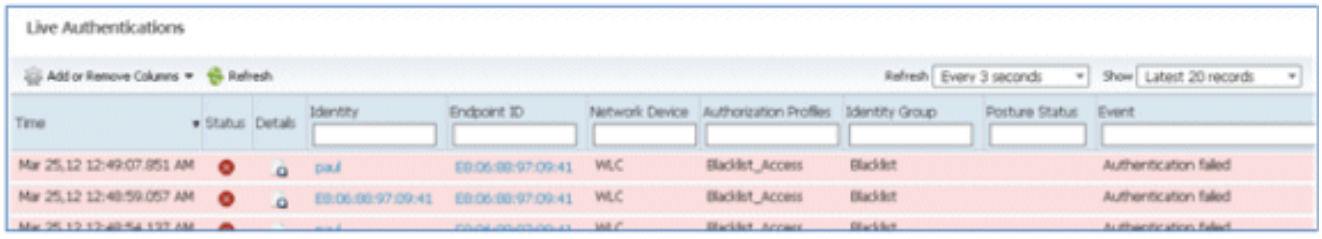
2. 在「Device ID（裝置ID）」下找到裝置，然後按一下**Lost?**以啟動裝置的黑名單。

3. 當ISE提示警告時，按一下**Yes**繼續。

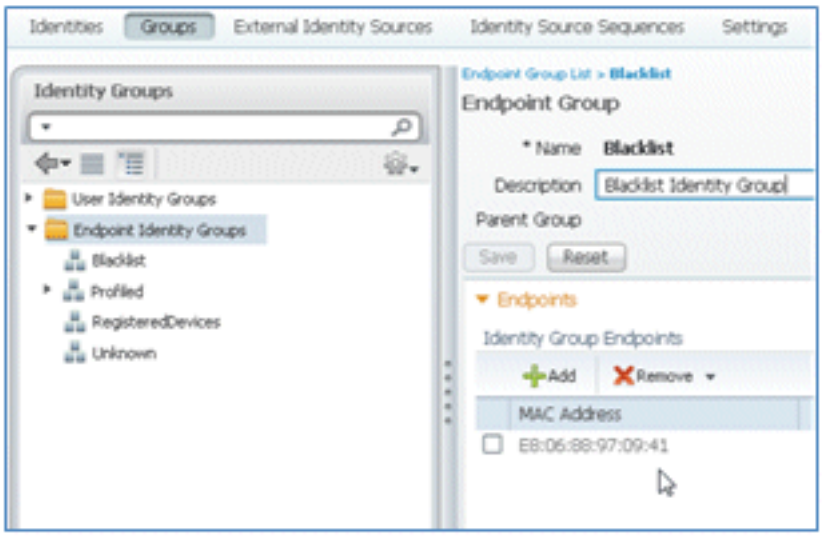


4. ISE確認裝置已標籤為**lost**。

5. 現在，即使安裝了有效的證書，任何使用先前註冊的裝置連線到網路的嘗試都會被阻止。以下是身份驗證失敗的黑名單裝置示例：



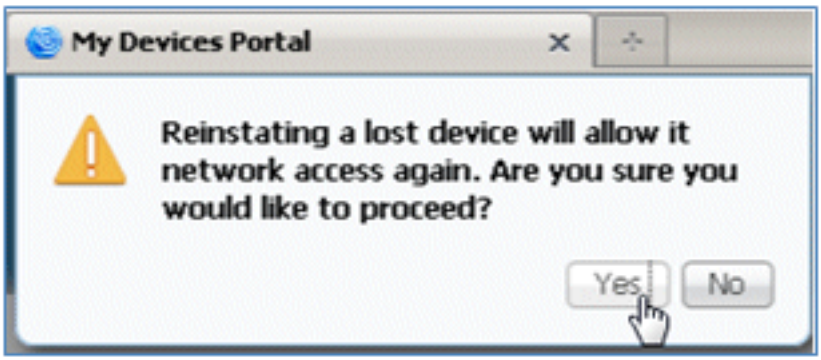
6. 管理員可以導航到ISE > Administration > Identity Management > **Groups**，按一下**Endpoint Identity Groups** > **Blacklist**，然後檢視裝置已列入黑名單。



完成以下步驟以恢復列入黑名單的裝置：

1. 在My Devices Portal（我的裝置門戶）中，為該裝置按一下**Reinstate**。

2. 當ISE提示警告時，按一下**Yes**繼續。



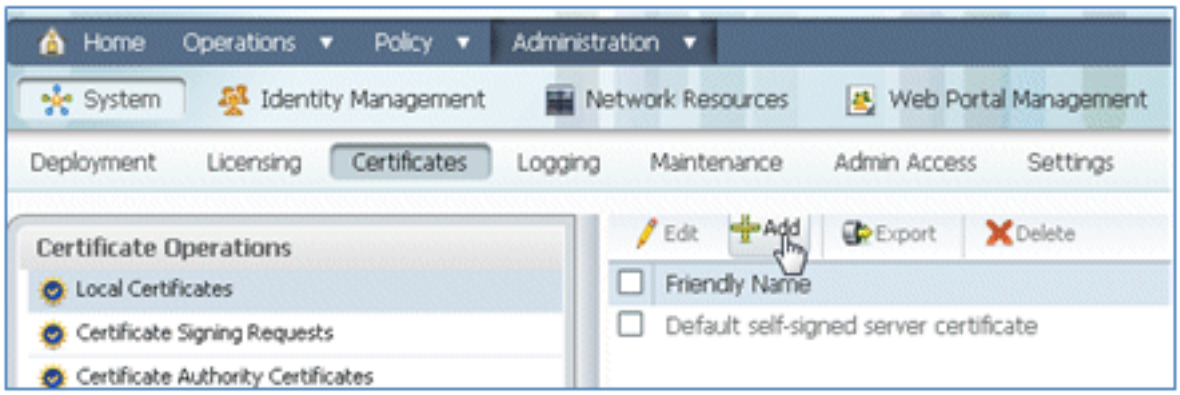
3. ISE確認裝置已成功恢復。將恢復後的裝置連線到網路，以測試該裝置現在是否被允許。

引用 — 證書

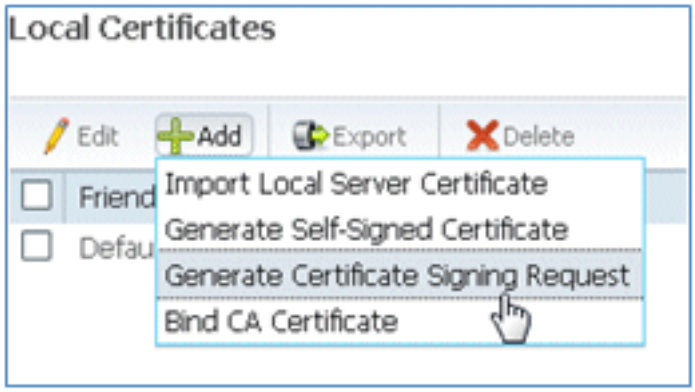
ISE不僅需要有效的CA根證書，還需要由CA簽署的有效證書。

完成以下步驟，以便新增、繫結和匯入新的受信任CA證書：

1. 導航到ISE > Administration > System > **Certificates**，點選**Local Certificates**，然後點選**Add**。

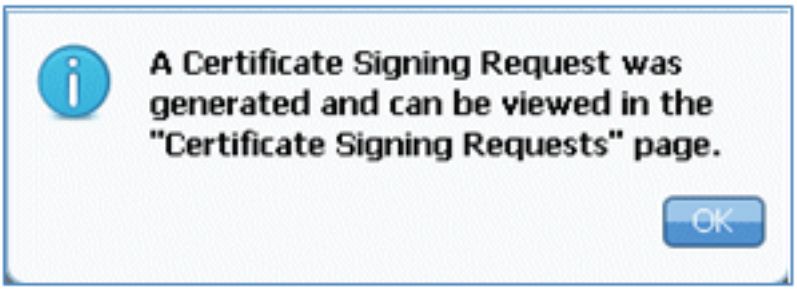


2. 選擇**Generate Certificate Signing Request**(CSR)。

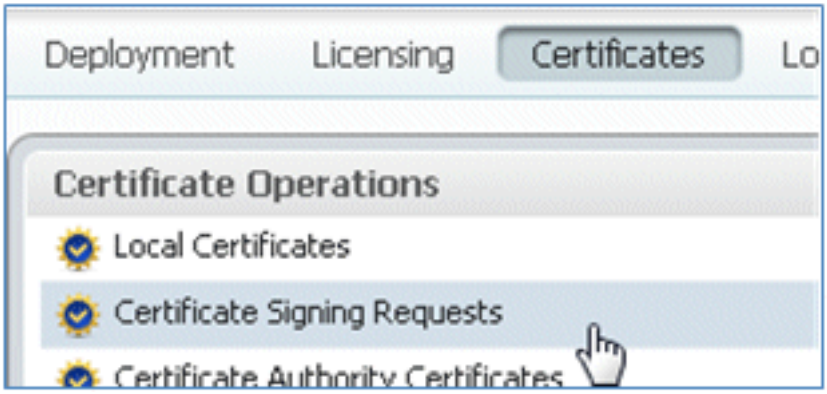


3. 輸入證書主體**CN=<***ISE-SERVER hostname.FQDN***>**。對於其他欄位，您可以使用CA設定所需的預設值或值。按一下「**Submit**」。

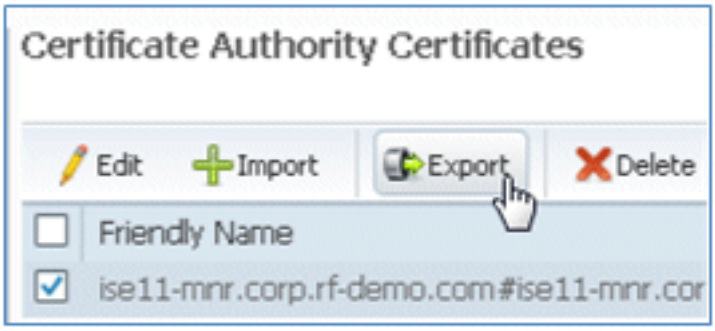
4. ISE驗證是否已生成CSR。



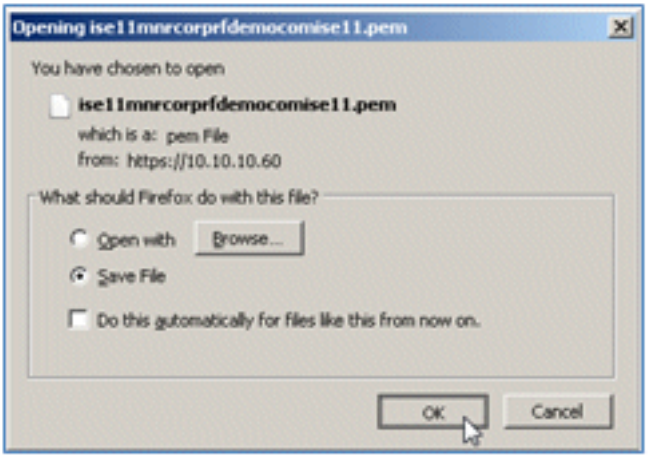
5. 若要存取CSR，請按一下「**Certificate Signing Requests**」操作。



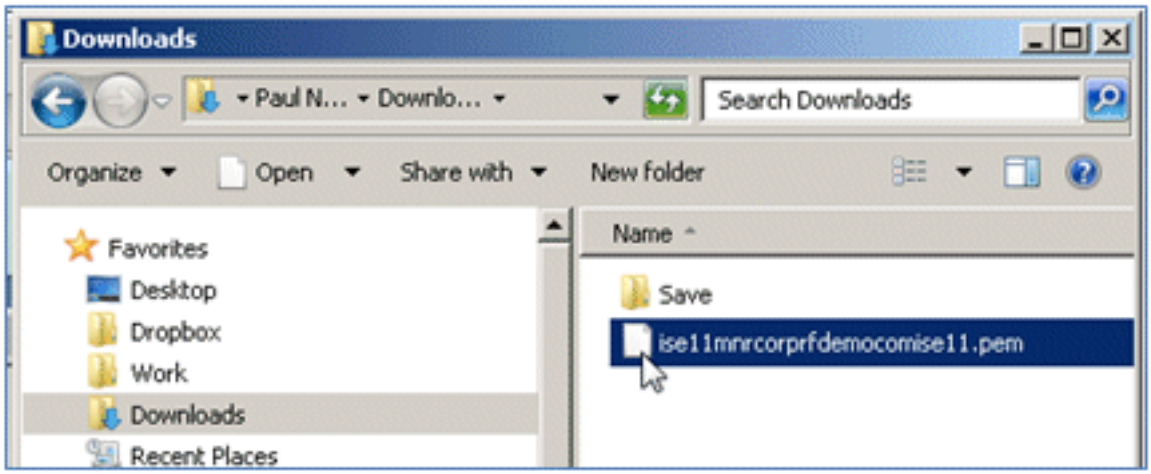
6. 選擇最近建立的CSR，然後按一下**匯出**。



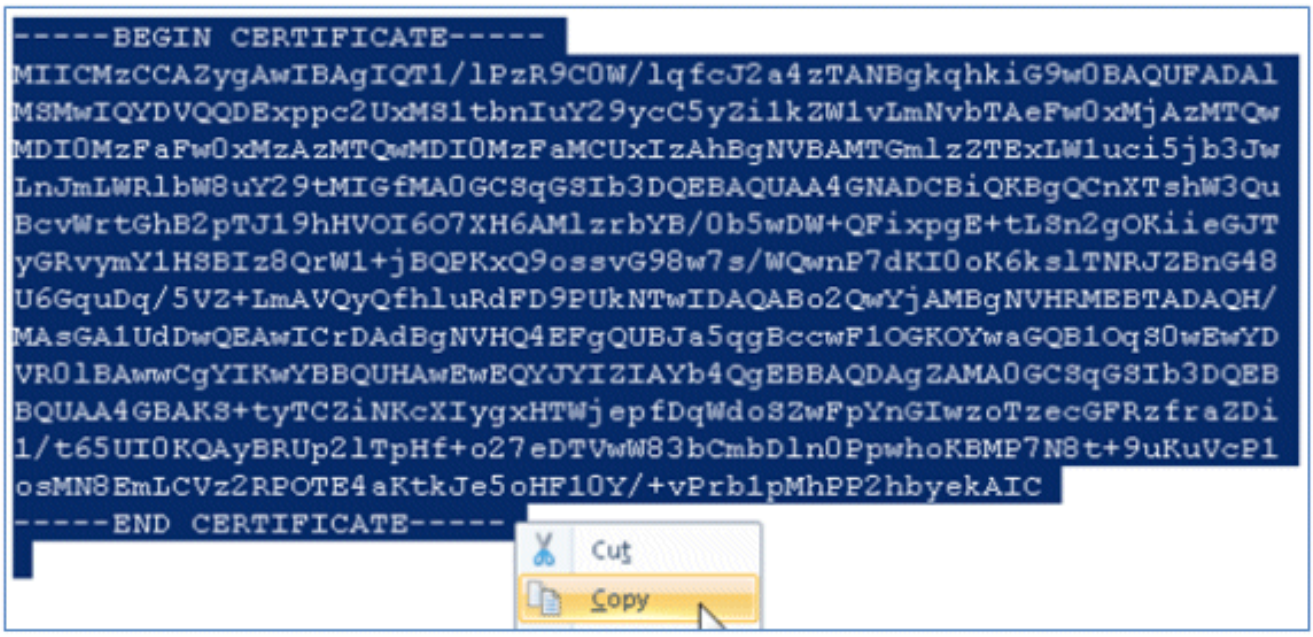
7. ISE將CSR匯出到.pem檔案。按一下**Save File**，然後按一下**OK**將檔案儲存到本地電腦。



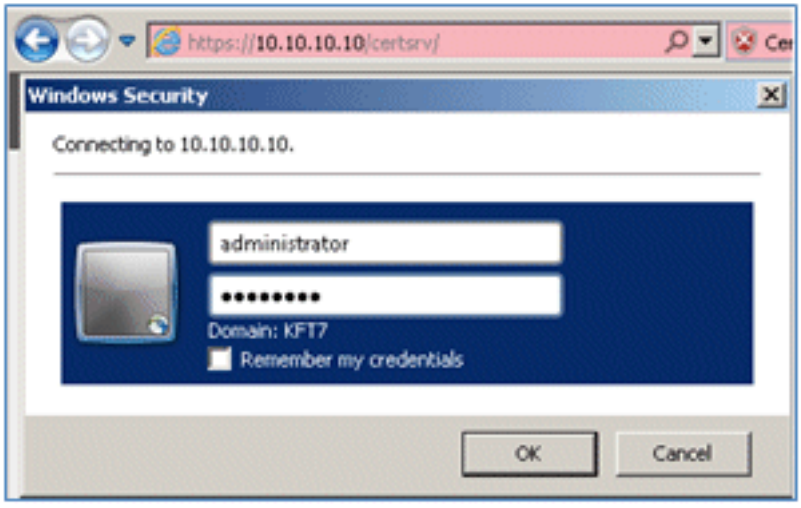
8. 使用文本編輯器查詢並開啟ISE證書檔案。



9. 複製證書的整個內容。

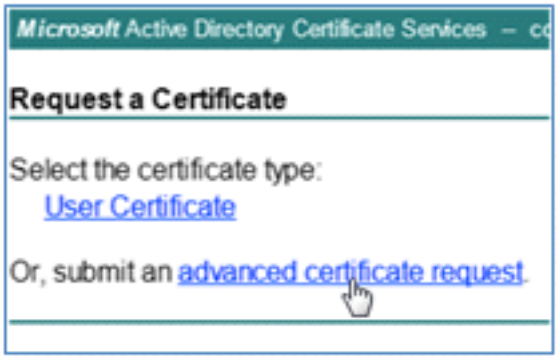


10. 連線到CA伺服器，然後使用管理員帳戶登入。伺服器是一個Microsoft 2008 CA，位於 https://10.10.10.10/certsrv（在本例中）。

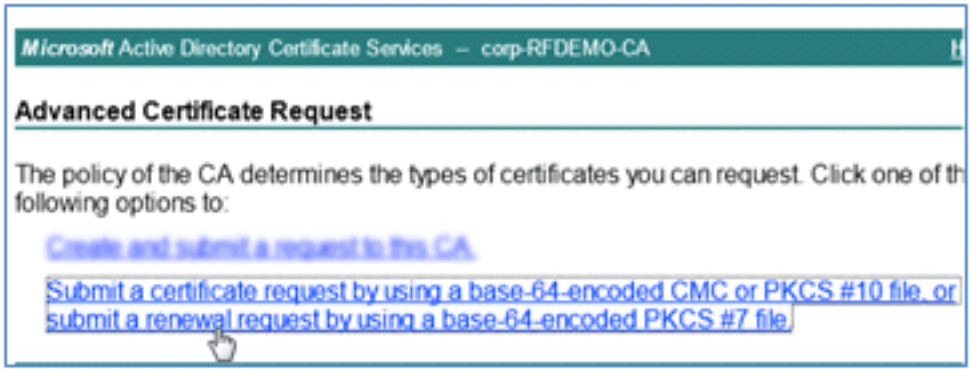


11. 按一下「**Request a certificate**」。

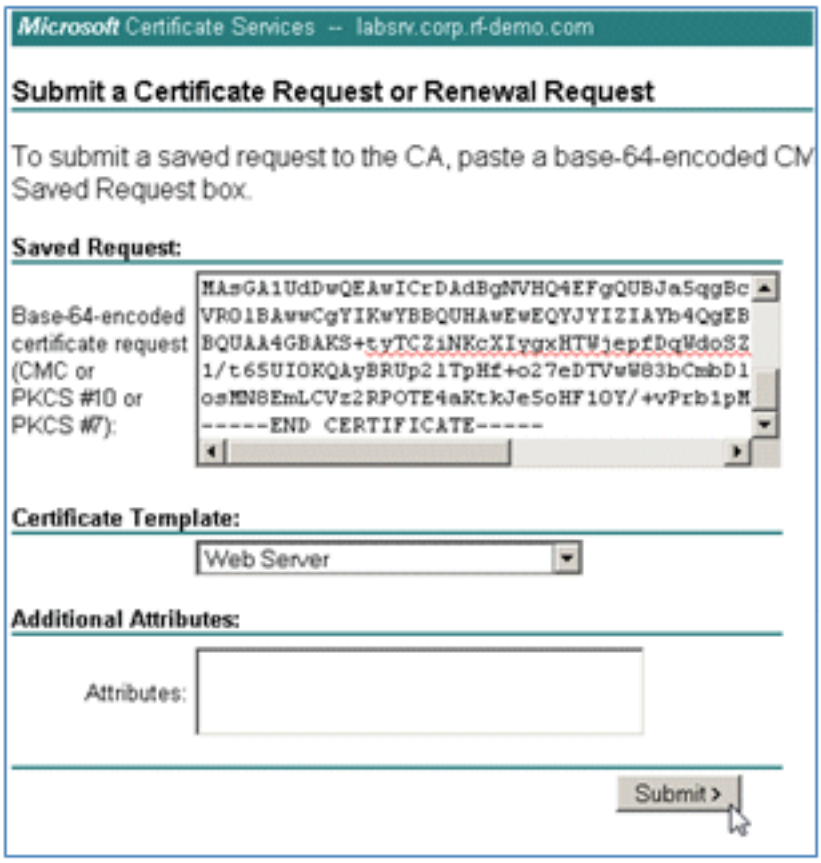
12. 按一下「**advanced certificate request**」。



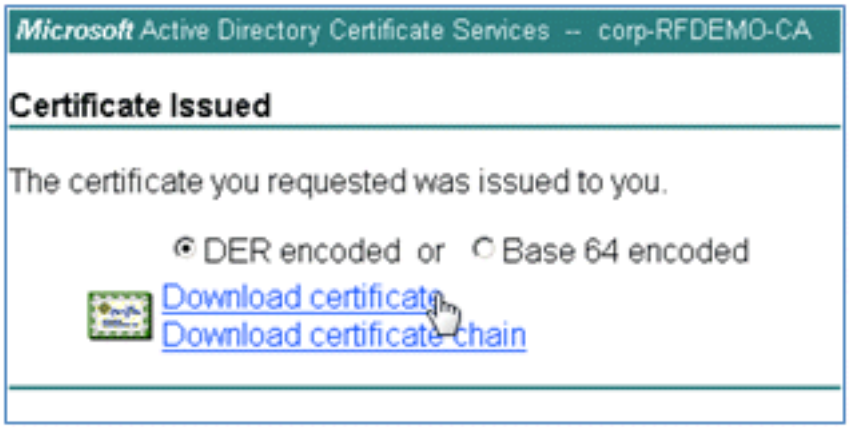
13. 按一下第二個選項可**以使用base-64編碼的CMC或……提交證書請求**.



14. 將ISE證書檔案(.pem)中的內容貼上到Saved Request欄位，確保Certificate Template is **Web Server**，然後按一下**Submit**。

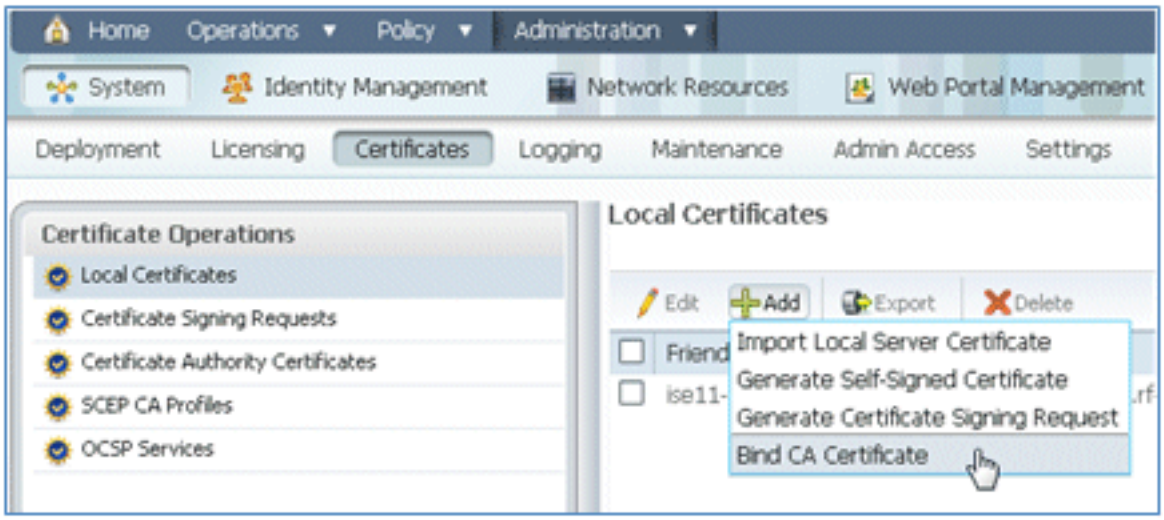


15. 按一下「**Download certificate**」。

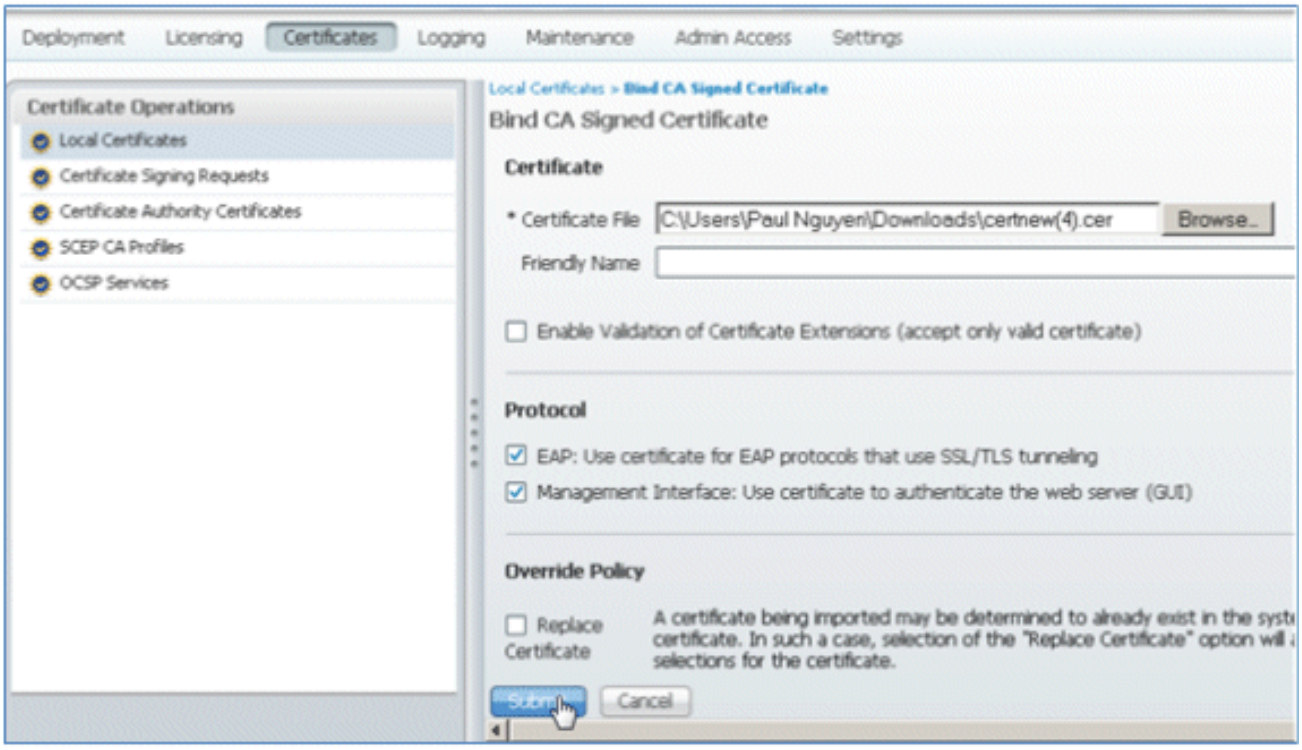


16. 儲存certnew.cer檔案；稍後將使用該檔案與ISE繫結。

17. 在ISE **Certificates**中，導航到**Local Certificates**，然後點選**Add > Bind CA Certificate**。



18. 瀏覽到在上一步中儲存到本地電腦的證書，啟用**EAP**和**Management Interface**協定（覈取方塊處於選中狀態），然後按一下**Submit**。ISE可能需要幾分鐘或更長時間才能重新啟動服務。

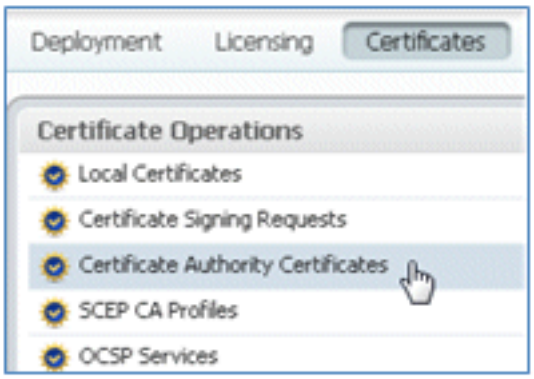


19. 返回CA的登入頁面(https://CA/certsrv/)，然後點選**下載CA證書、證書鏈或CRL**。

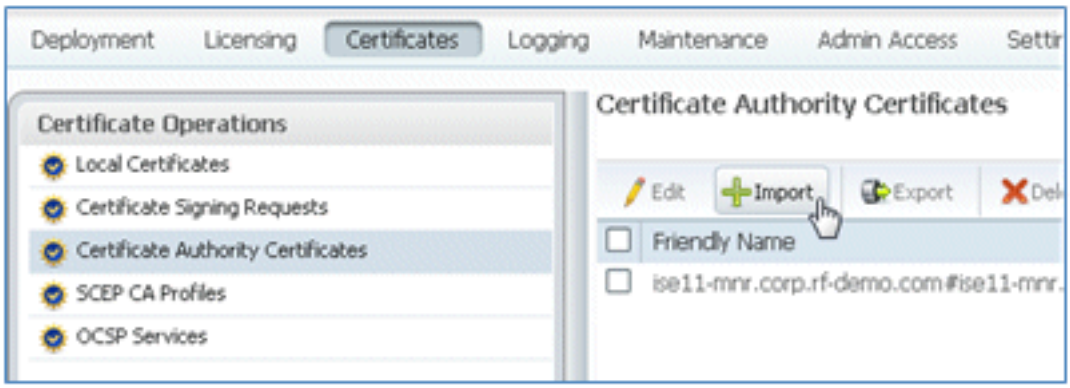
20. 按一下「**Download CA certificate**」。

21. **將檔**案儲存到本機電腦中。

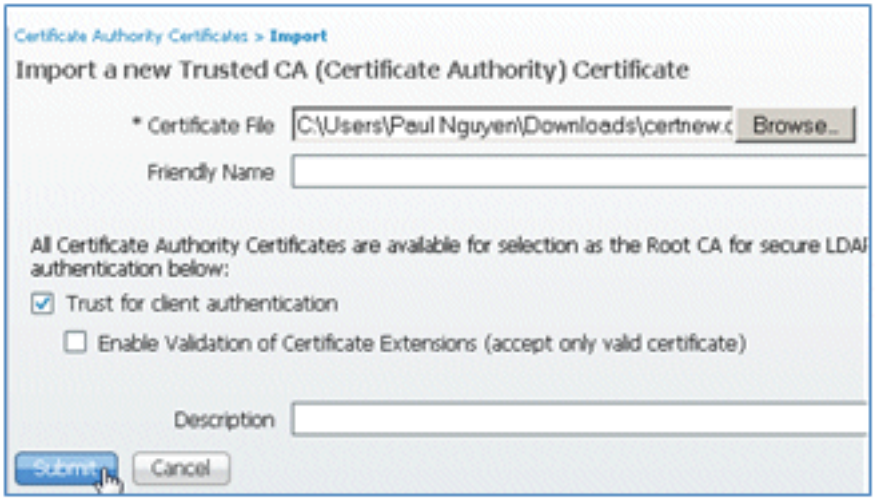
22. 在ISE伺服器聯機時，轉到**證書**，然後按一下**證書頒發機構證書**。



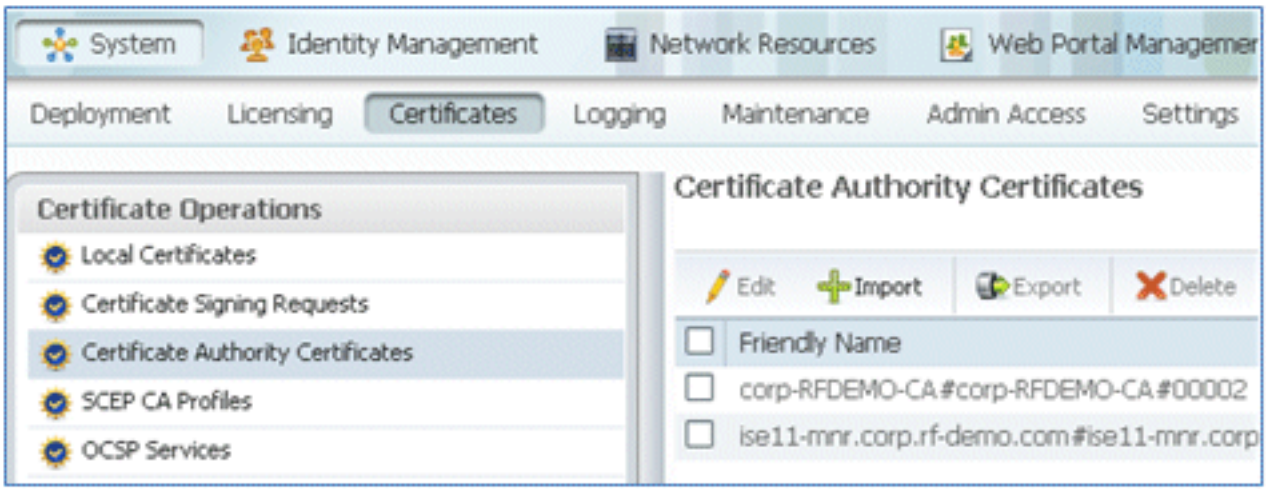
23. 按一下「**Import**」（匯入）。



24. 瀏覽CA證書，啟用**Trust for client authentication**（選中框），然後按一下**Submit**。



25. 確認已新增新的受信任CA證書。



相關資訊

- 思科身份服務引擎硬體安裝指南1.0.4版
- Cisco 2000系列無線LAN控制器
- Cisco 4400系列無線LAN控制器
- Cisco Aironet 3500 系列
- Flex 7500無線分支機構控制器部署指南
- 自帶裝置 — 統一裝置身份驗證和一致的訪問體驗
- 帶身份服務引擎的無線BYOD
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。