

帶身份服務引擎的無線BYOD

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[拓撲](#)

[慣例](#)

[無線LAN控制器RADIUS NAC和CoA概觀](#)

[無線LAN控制器RADIUS NAC和CoA功能流](#)

[ISE分析概述](#)

[建立內部身份使用者](#)

[向ISE新增無線LAN控制器](#)

[配置ISE進行無線身份驗證](#)

[Bootstrap無線LAN控制器](#)

[將WLC連線到網路](#)

[將驗證伺服器\(ISE\)新增到WLC](#)

[建立WLC員工動態介面](#)

[建立WLC訪客動態介面](#)

[新增802.1x WLAN](#)

[測試WLC動態介面](#)

[適用於iOS的無線驗證\(iPhone/iPad\)](#)

[將狀態重新導向ACL新增到WLC](#)

[在ISE上啟用分析探測](#)

[為裝置啟用ISE配置檔案策略](#)

[狀態發現重定向的ISE授權配置檔案](#)

[為員工建立ISE授權配置檔案](#)

[為承包商建立ISE授權配置檔案](#)

[裝置狀態/分析授權策略](#)

[測試狀態修正策略](#)

[差異化訪問的授權策略](#)

[測試CoA以區分訪問](#)

[WLC訪客WLAN](#)

[測試訪客WLAN和訪客門戶](#)

[ISE無線贊助訪客接入](#)

[贊助訪客](#)

[測試訪客門戶訪問](#)

[憑證組態](#)

[Windows 2008 Active Directory整合](#)

[新增Active Directory組](#)

[新增身份源序列](#)

[整合AD的ISE無線贊助訪客接入](#)

[在交換器上設定SPAN](#)

[參考：Apple MAC OS X的無線身份驗證](#)

[參考：Microsoft Windows XP的無線身份驗證](#)

[參考：Microsoft Windows 7的無線身份驗證](#)

[相關資訊](#)

簡介

思科身份服務引擎(ISE)是思科的下一代策略伺服器，為Cisco TrustSec解決方案提供身份驗證和授權基礎設施。它還提供另外兩項關鍵服務：

- 第一項服務是提供一種方法，根據思科ISE從各種資訊源接收的屬性自動分析終端裝置型別。此服務（稱為Profiler）提供的功能與思科之前提供的Cisco NAC Profiler裝置功能相同。
- 思科ISE提供的另一項重要服務是掃描端點合規性；例如，AV/AS軟體安裝及其定義檔案有效性（稱為狀態）。Cisco以前只通過Cisco NAC裝置提供此確切狀態功能。

思科ISE提供同等級別的功能，並與802.1X身份驗證機制整合。

與無線LAN控制器(WLC)整合的Cisco ISE可提供流動裝置(例如Apple iDevices (iPhone、iPad和 iPod)、基於Android的智慧手機和其他裝置的分析機制。對於802.1X使用者，思科ISE可提供相同級別的服務，如分析和狀態掃描。通過將網路身份驗證請求重定向到思科ISE進行身份驗證，思科ISE上的訪客服務也可以與思科WLC整合。

本文檔介紹自帶裝置(BYOD)的無線解決方案，例如根據已知終端和使用者策略提供差異化接入。本文檔不提供BYOD的完整解決方案，但用於演示動態訪問的簡單使用案例。其他配置示例包括使用ISE發起人門戶，特權使用者可以在其中發起訪客來調配無線訪客接入。

必要條件

需求

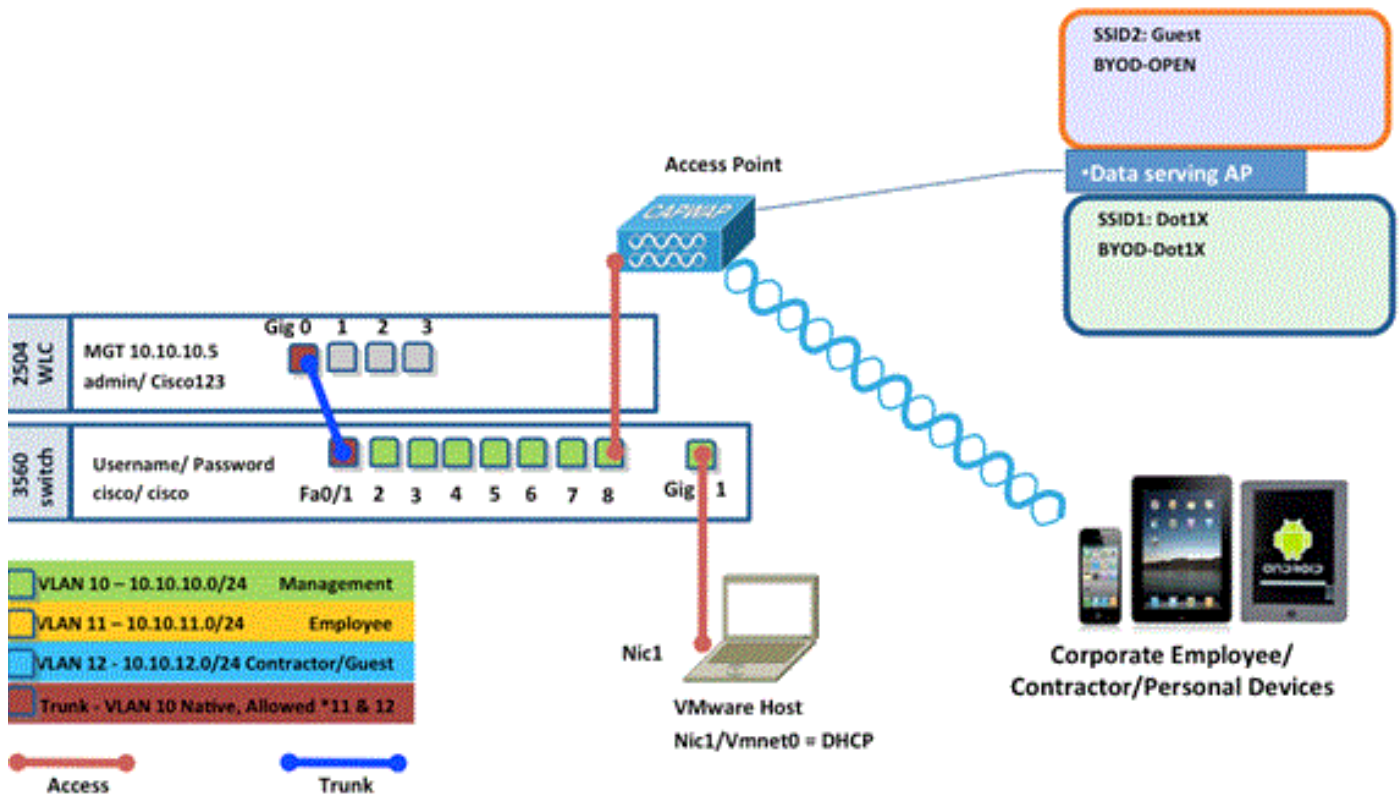
本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 軟體版本為7.2.103的Cisco無線LAN控制器2504或2106
- Catalyst 3560 - 8埠
- WLC 2504
- 身份服務引擎1.0MR (VMware伺服器映像版本)
- Windows 2008 Server (VMware映像) — 512M，20GB磁碟Active DirectoryDNSDHCP憑證服務

拓撲



慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

無線LAN控制器RADIUS NAC和CoA概觀

此設定使WLC能夠查詢來自ISE RADIUS伺服器的URL重定向AV對。這隻發生在連線到已啟用RADIUS NAC設定的介面的WLAN上。收到適用於URL重新導向的Cisco AV配對時，使用者端會進入POSTURE_REQD狀態。這基本上與控制器內部的WEBAUTH_REQD狀態相同。

當ISE RADIUS伺服器判斷使用者端是否符合Posture_Compliant時，會發出CoA ReAuth。Session_ID用於將其連線在一起。使用此新的AuthC (重新驗證) 不會傳送URL-Redirect AV對。由於沒有URL重新導向AV配對，因此WLC知道使用者端不再需要安全狀態。

如果RADIUS NAC設定未啟用，WLC會忽略URL重新導向VSA。

CoA-ReAuth：這是使用RFC 3576設定啟用的。已將ReAuth功能新增到先前支援的現有CoA命令中。

RADIUS NAC設定與此功能互斥，但CoA需要它才能工作。

前狀態ACL：當客戶端處於POSTURE_REQ狀態時，WLC的預設行為是阻止除DHCP/DNS以外的所有流量。預先安全狀態ACL (在url-redirect-acl AV對中稱為) 應用於客戶端，該ACL中允許的內

容是客戶端可以到達的內容。

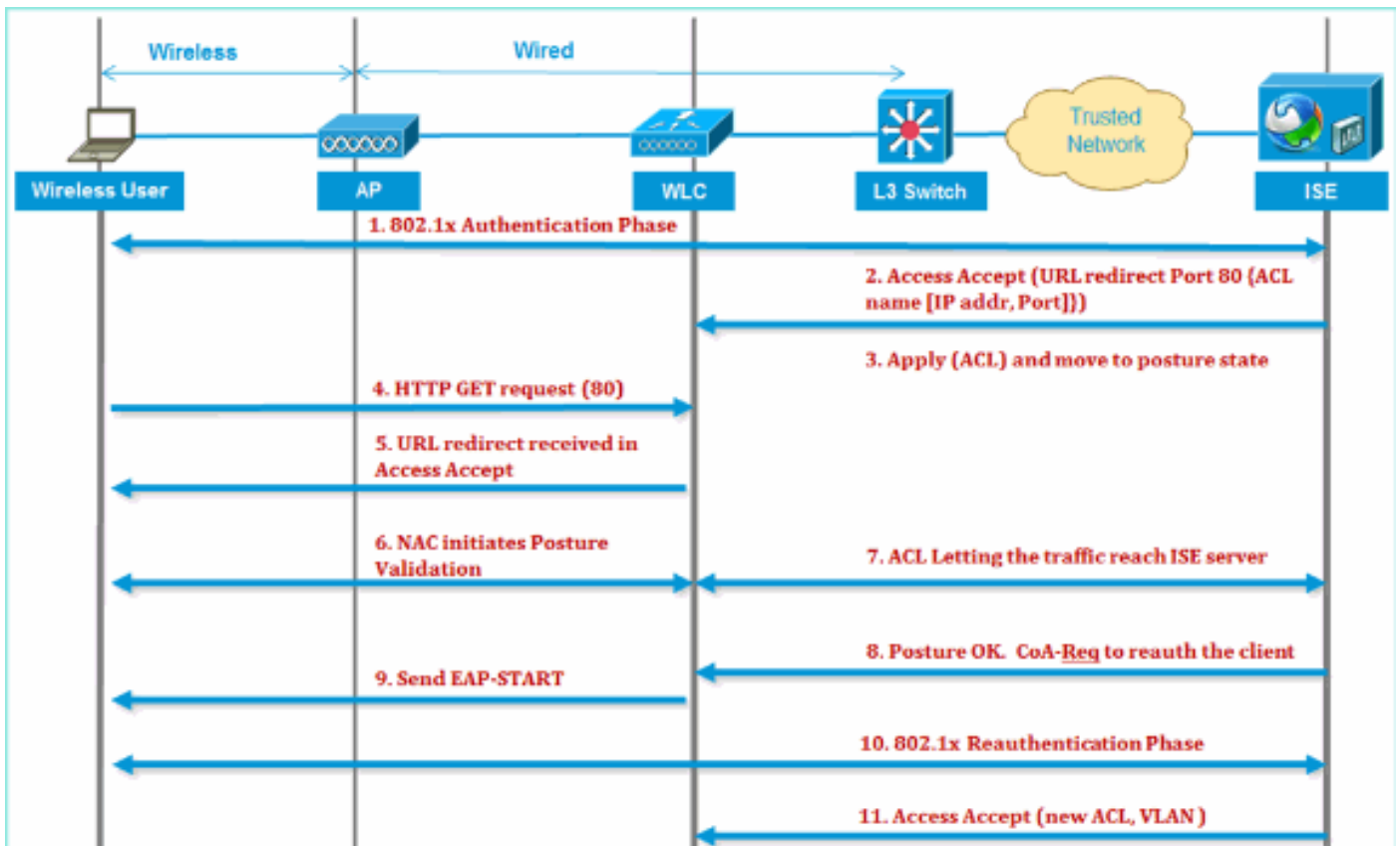
預先驗證ACL與VLAN覆寫：7.0MR1不支援與Access-VLAN不同的隔離或AuthC VLAN。如果從策略伺服器設定VLAN，它將成為整個會話的VLAN。首次授權後無需更改VLAN。

無線LAN控制器RADIUS NAC和CoA功能流

下圖提供當客戶端通過後端伺服器驗證和NAC狀態驗證時消息交換的詳細資訊。

1. 客戶端使用dot1x身份驗證進行身份驗證。
2. RADIUS存取接受傳送連線埠80的重新導向URL和預先驗證ACL (包括允許IP位址和連線埠，或隔離VLAN)。
3. 客戶端將重定向到訪問接受中提供的URL，並進入新狀態，直到完成狀態驗證。處於此狀態的客戶端與ISE伺服器對話並根據ISE NAC伺服器上配置的策略驗證自身。
4. 客戶端上的NAC代理啟動狀態驗證 (流向埠80)：代理向埠80傳送HTTP發現請求，控制器將請求重定向到訪問接受中提供的URL。ISE知道客戶端嘗試聯絡並直接響應客戶端。這樣，客戶端可以瞭解ISE伺服器IP，從現在開始，客戶端將直接與ISE伺服器對話。
5. WLC允許此流量，因為ACL設定為允許此流量。在發生VLAN覆寫的情況下，流量會橋接以便到達ISE伺服器。
6. ISE使用者端完成評估後，會向WLC傳送帶有reauth服務的RADIUS CoA-Req。這將啟動客戶端的重新身份驗證 (通過傳送EAP-START)。重新身份驗證成功後，ISE會傳送訪問接受並帶有一個新的ACL (如果有) 和沒有URL重定向或訪問VLAN。
7. 根據RFC 3576,WLC支援CoA-Req和Disconnect-Req。根據RFC 5176,WLC需要支援重新驗證服務的CoA-Req。
8. WLC上使用的是預配置的ACL，而不是可下載的ACL。ISE伺服器只傳送ACL名稱，該名稱已在控制器中配置。
9. 此設計適用於VLAN和ACL兩種情況。在發生VLAN覆寫的情況下，我們只需將連線埠80重新導向，並允許 (橋接) 隔離VLAN上的其餘流量。對於ACL，會套用在access accept中接收的預先驗證ACL。

下圖直觀地顯示了此功能流程：



ISE分析概述

思科ISE分析器服務提供發現、定位和確定網路上所有連線端點的功能，無論其裝置型別如何，以確保和維護對您的企業網路的適當訪問。它主要收集網路上所有終端的一個屬性或一組屬性，並根據其配置檔案對它們進行分類。

Profiler由以下元件組成：

- 感測器包含多個探測器。探測器通過查詢網路接入裝置來捕獲網路資料包，並將從端點收集到的屬性及其屬性值轉發到分析器。
- 分析器使用配置的策略和身份組評估端點以匹配所收集的屬性及其屬性值，將端點分類到指定的組並將具有匹配配置檔案的端點儲存在思科ISE資料庫中。

對於流動裝置檢測，建議使用以下探針組合來正確識別裝置：


- RADIUS(Calling-Station-ID)：提供MAC地址(OUI)
- DHCP (主機名)：主機名 — 預設主機名可以包括裝置型別；例如：jsmith-ipad
- DNS (反向IP查詢)：FQDN — 預設主機名可以包括裝置型別
- HTTP (使用者代理)：有關特定流動裝置型別的詳細資訊

在iPad的這個示例中，探查器從User-Agent屬性中捕獲Web瀏覽器資訊，以及從請求消息中捕獲其它HTTP屬性，並將它們新增到終端屬性清單中。




Is the MAC Address
from Apple? 



Does the Hostname
contain "iPad"? 



Is the Safari Browser
on an iPad? 



I am
certain it
is an iPad!

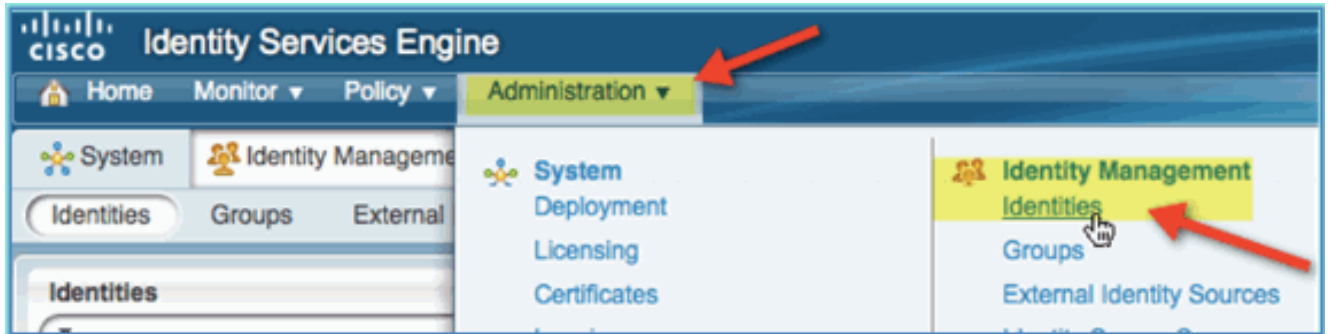
建立內部身份使用者

MS Active Directory(AD)對於簡單的概念驗證不是必需的。ISE可用作唯一身份庫，包括區分使用者訪問和精細策略控制。

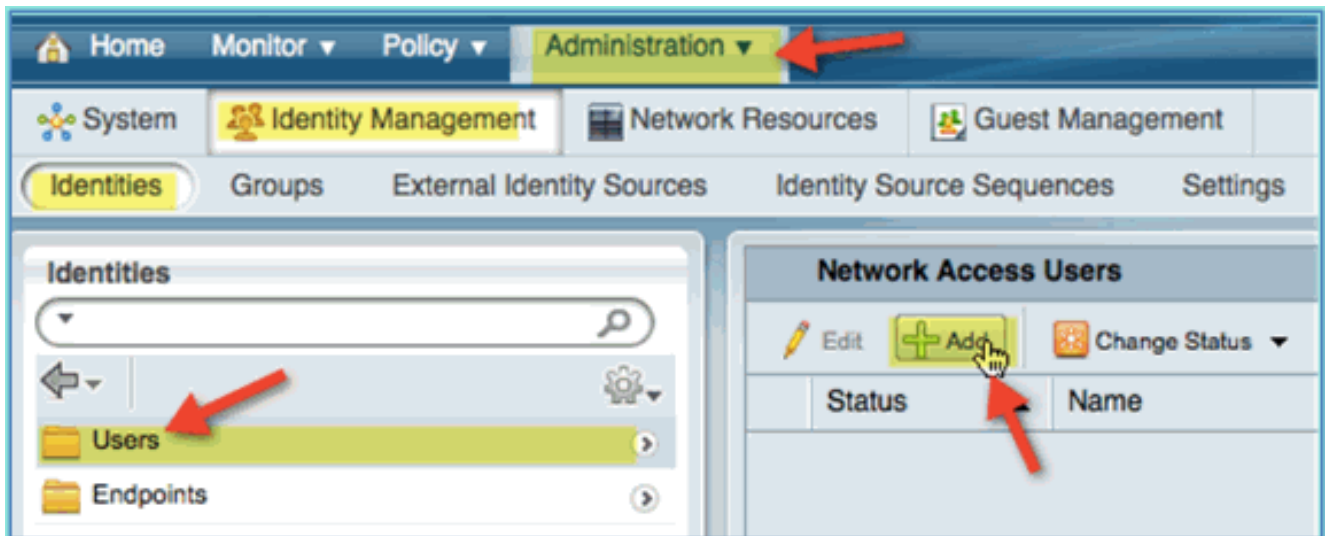
在ISE 1.0發佈時，使用AD整合，ISE可以在授權策略中使用AD組。如果使用ISE內部使用者儲存（無AD整合），則不能將組與裝置身份組一起用於策略（已在ISE 1.1中確定需要解決的錯誤）。因此，除了裝置身份組之外，只有個人使用者才能被區分，如員工或承包商。

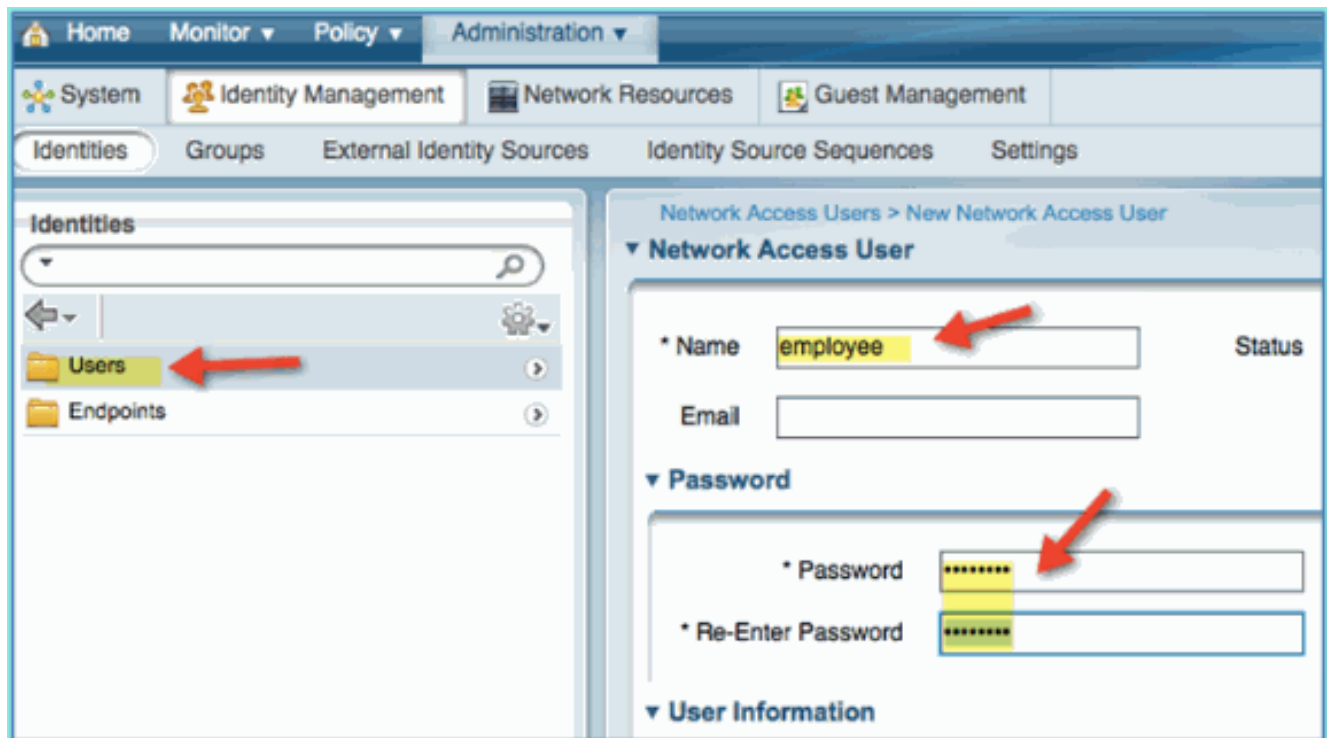
請完成以下步驟：

1. 開啟瀏覽器視窗訪問https://ISEip地址。
2. 導航到**管理>身份管理>身份**。

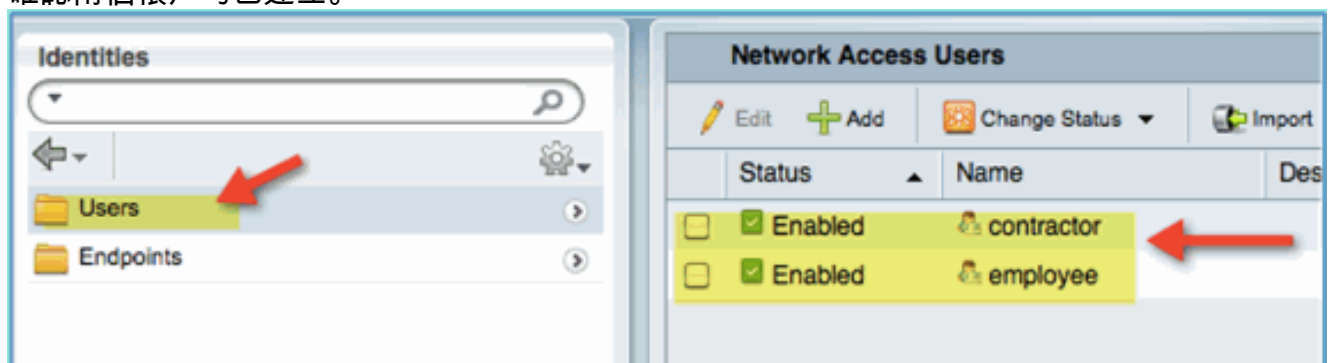


3. 選擇**Users**，然後按一下**Add**（網路訪問使用者）。輸入以下使用者值並分配給Employee組
：姓名：員工密碼
：XXXX





4. 按一下「Submit」。名稱：承包商密碼：XXXX
5. 確認兩個帳戶均已建立。



向ISE新增無線LAN控制器

任何向ISE發起RADIUS請求的裝置都必須在ISE中有一個定義。這些網路裝置是根據其IP地址定義的。ISE網路裝置定義可以指定IP地址範圍，從而允許定義表示多個實際裝置。

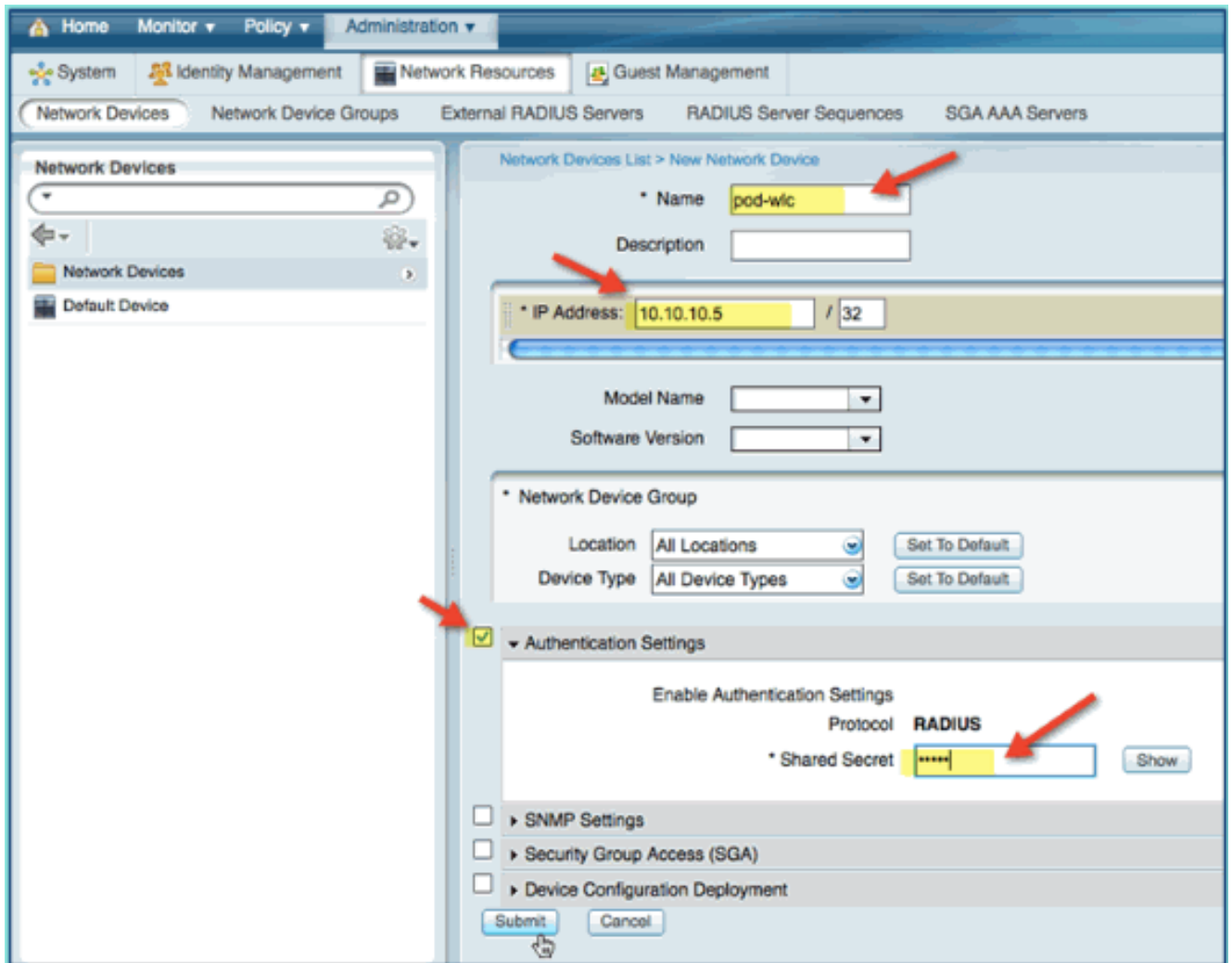
除了RADIUS通訊所需的設定，ISE網路裝置定義還包含其他ISE/裝置通訊的設定，例如SNMP和SSH。

網路裝置定義的另一個重要方面是對裝置進行適當分組，以便可以在網路訪問策略中利用此分組。

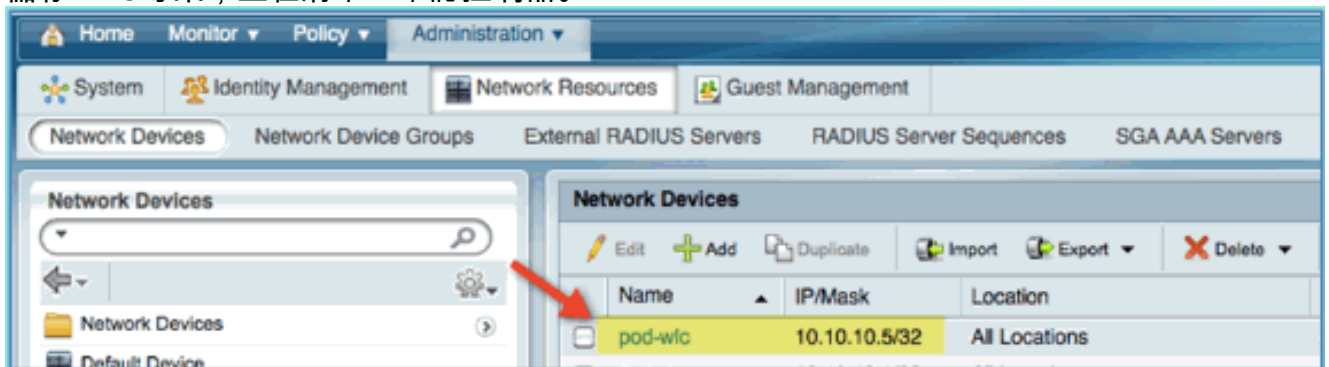
本練習將配置實驗所需的裝置定義。

請完成以下步驟：

1. 從ISE轉至管理>網路資源>網路裝置。



2. 在「Network Devices (網路裝置)」中，按一下Add。輸入IP地址，掩碼檢查身份驗證設定，然後輸入「cisco」作為共用金鑰。
3. 儲存WLC專案，並在清單上確認控制器。

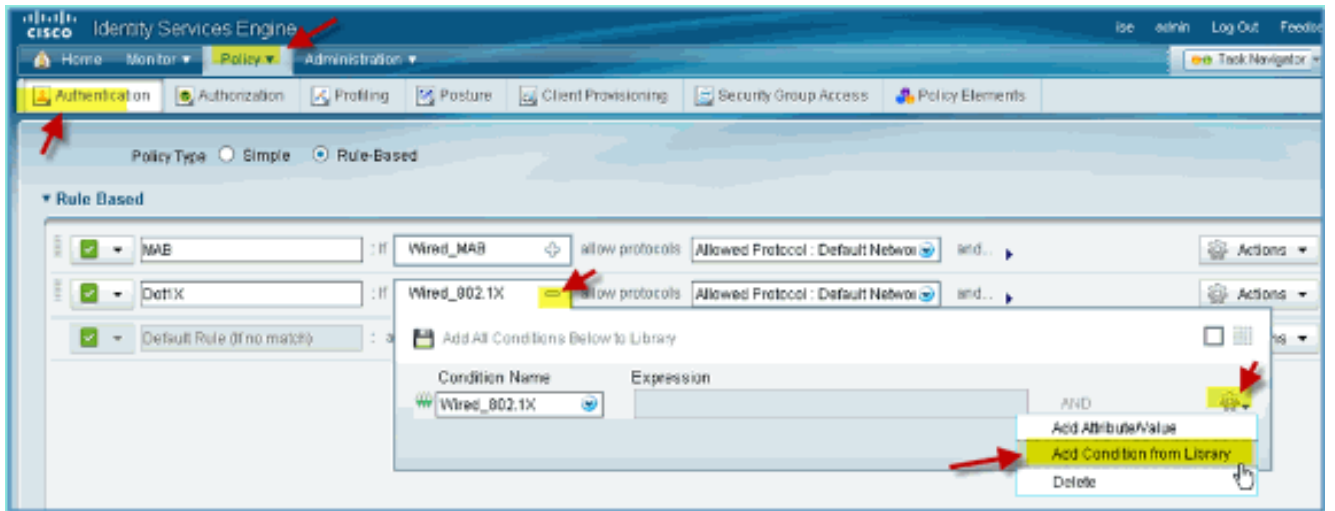


配置ISE進行無線身份驗證

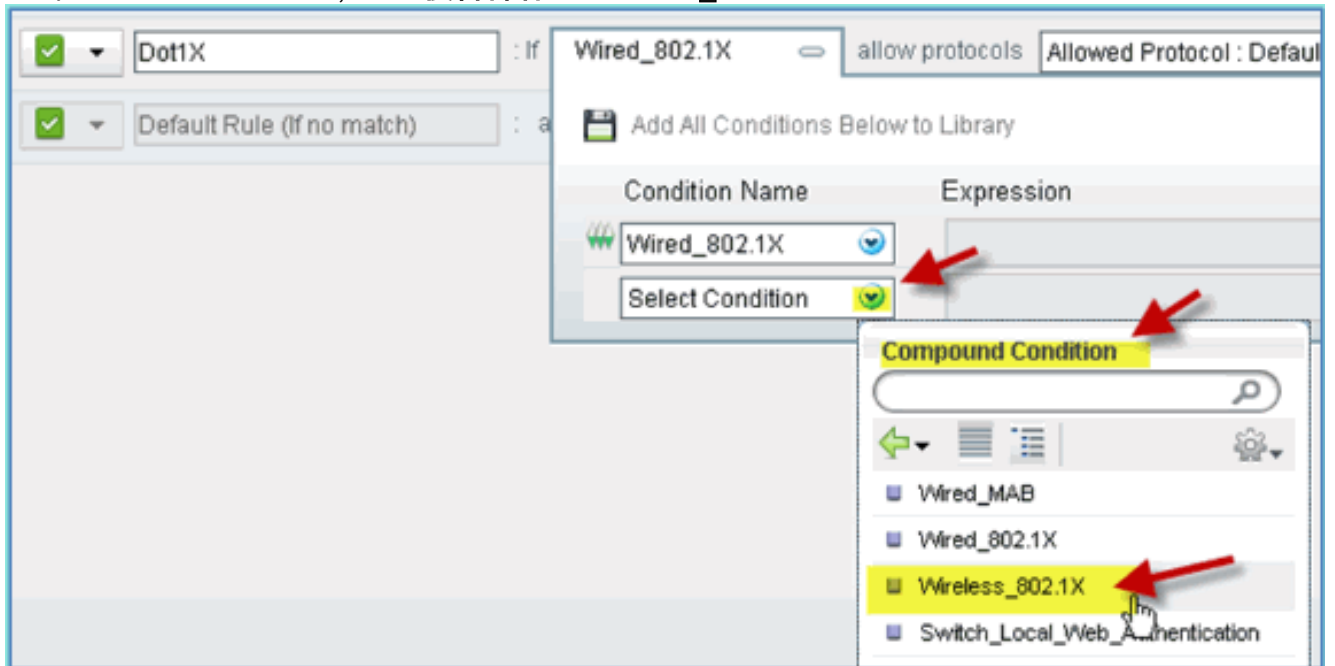
需要配置ISE以驗證802.1x無線客戶端並使用Active Directory作為身份庫。

請完成以下步驟：

1. 從ISE導航到Policy > Authentication。
2. 按一下展開Dot1x > Wired_802.1X(-)。
3. 按一下齒輪圖示以從庫中新增條件。



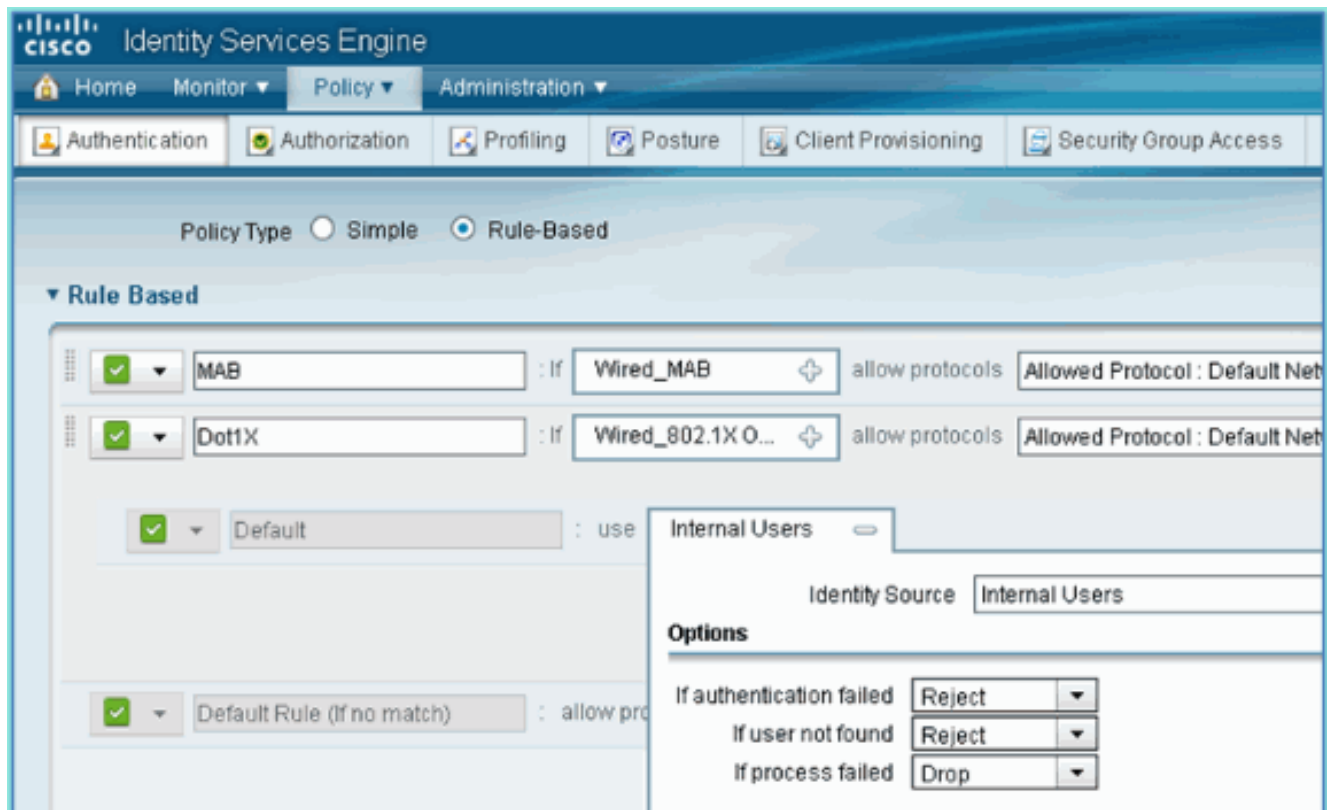
4. 從條件選擇下拉選單中，選擇**複合條件**> **Wireless_802.1X**。



5. 將Express條件設定為**OR**。

6. 展開**after allow protocols**選項，並接受預設的**Internal Users**（預設）。





7. 將其他所有內容保留為預設值。按一下「Save」以完成步驟。

[Bootstrap無線LAN控制器](#)

[將WLC連線到網路](#)

[Cisco 2500系列無線控制器部署指南](#)中也提供Cisco 2500無線LAN控制器部署指南。

使用啟動嚮導配置控制器

(Cisco Controller)

```

Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup
Would you like to terminate autoinstall? [yes]: yes AUTO-INSTALL: process terminated
-- no configuration loaded System Name [Cisco_d9:24:44] (31 characters max):
ISE-Podx Enter Administrative User Name (24 characters max): admin
Enter Administrative Password
(3 to 24 characters): Cisco123
Re-enter Administrative Password: Cisco123
Management Interface IP Address: 10.10.10.5
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.10.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.10.10.10
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: ISE
Network Name (SSID): PODx
Configure DHCP Bridging Mode [yes][NO]: no
Allow Static IP Addresses [YES][no]: no
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code list (enter 'help' for a list of countries) [US]: US

```

```
Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes
Configure a NTP server now? [YES][no]: no
Configure the ntp system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: mm/dd/yy
Enter the time in HH:MM:SS format: hh:mm:ss
Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
Configuration saved!
Resetting system with new configuration...
Restarting system.
```

鄰居交換機配置

控制器已連線到相鄰交換機(Fast Ethernet 1)上的乙太網埠。鄰居交換機埠配置為802.1Q中繼並允許中繼上的所有VLAN。本徵VLAN 10允許連線WLC的管理介面。

802.1Q交換機埠配置如下：

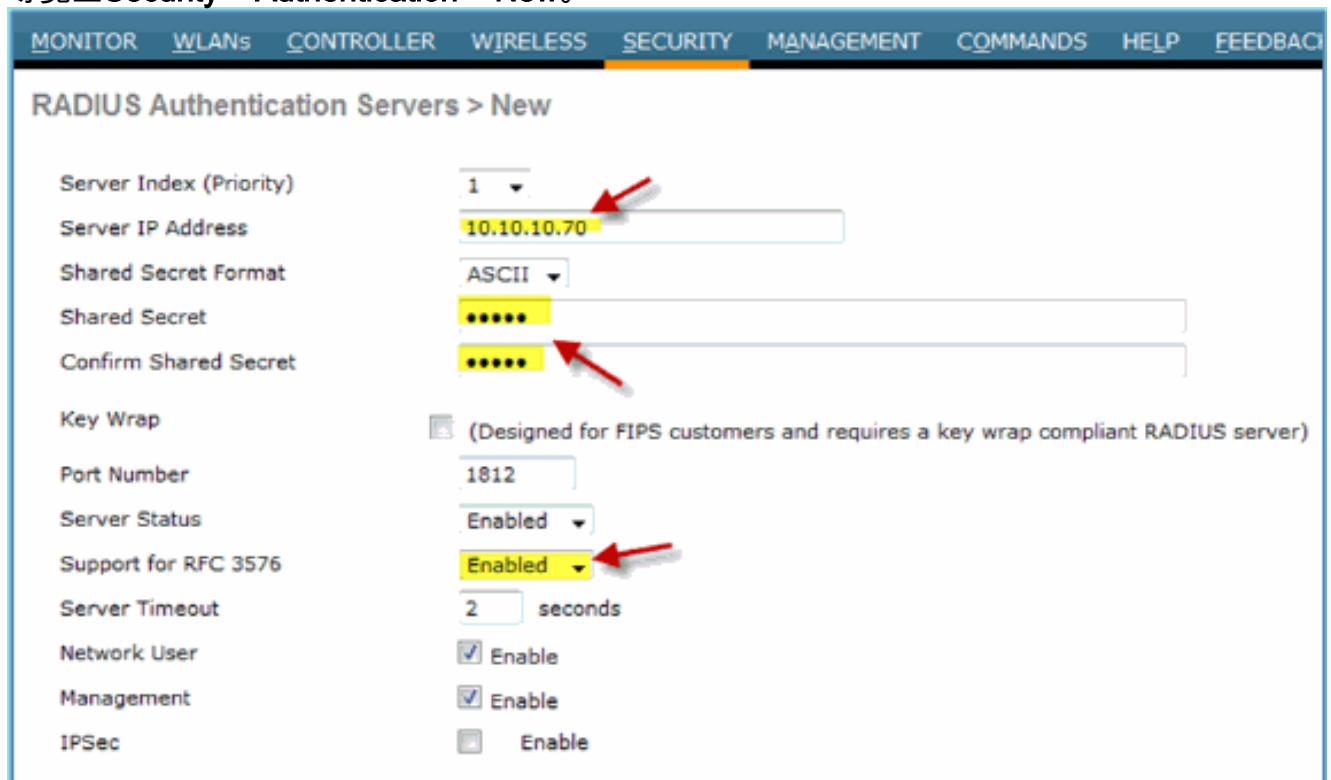
```
switchport
switchport trunk encapsulation dot1q
switchport trunk native VLAN 10
switchport mode trunk
end
```

將驗證伺服器(ISE)新增到WLC

需要將ISE新增到WLC，以便為無線終端啟用802.1X和CoA功能。

請完成以下步驟：

1. 開啟瀏覽器，然後連線到Pod WLC (使用安全HTTP) > <https://wlc>。
2. 導覽至Security > Authentication > New。



MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK

RADIUS Authentication Servers > New

Server Index (Priority)	1
Server IP Address	10.10.10.70
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

- 輸入以下值：伺服器IP地址：10.10.10.70（檢查分配）共用金鑰：cisco支援RFC 3576(CoA)：已啟用（預設）其他所有內容：預設
- 按一下「Apply」以繼續。
- 選擇RADIUS Accounting > Add NEW。

- 輸入以下值：伺服器IP地址：10.10.10.70共用金鑰：cisco其他所有內容：預設
- 按一下「Apply」，然後儲存WLC的組態。

建立WLC員工動態介面

完成以下步驟，以便為WLC新增動態介面，並將其對應到員工VLAN:

- 在WLC中，導覽至Controller > Interfaces。然後，按一下New。

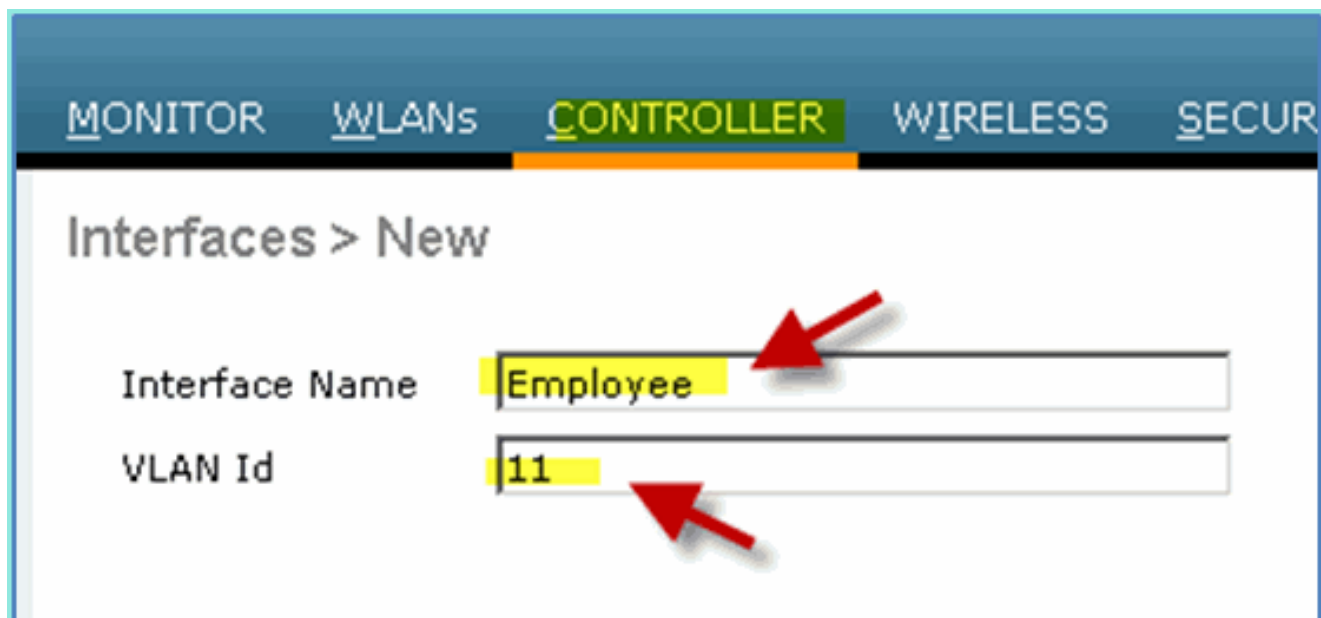
Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
management	untagged	10.10.10.5	Static	Enabled
virtual	N/A	1.1.1.1	Static	Not Supported

- 在WLC中，導覽至Controller > Interfaces。輸入以下內容：介面名稱：員工VLAN id:11

MONITOR WLANs **CONTROLLER** WIRELESS SECUR

Interfaces > New

Interface Name	<input type="text" value="Employee"/>
VLAN Id	<input type="text" value="11"/>



3. 為Employee介面輸入以下內容：埠號：1VLAN識別符號：11IP地址：10.10.11.5網路掩碼：255.255.255.0網關：10.10.11.1DHCP:10.10.10.10

Configuration

Quarantine

Quarantine Vlan Id

Physical Information

Port Number

Backup Port

Active Port

Enable Dynamic AP Management

Interface Address

VLAN Identifier

IP Address

Netmask

Gateway

DHCP Information

Primary DHCP Server

Secondary DHCP Server

4. 確認已建立新的員工動態介面。

CISCO

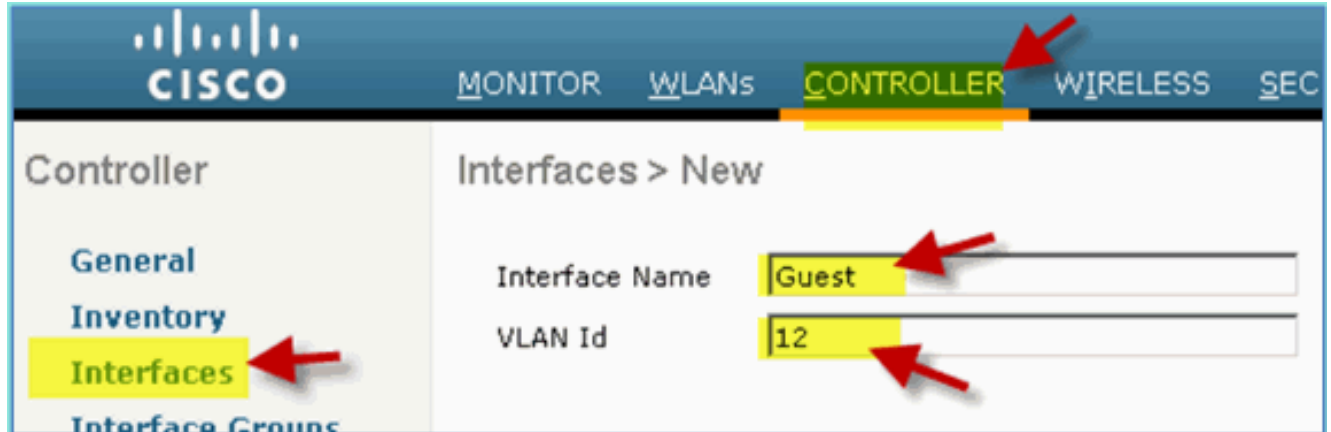
MONITOR WLANs **CONTROLLER** WIRELESS SECURITY MANAGEMENT COMMUNITY

Controller		Interfaces			
		Interface Name	VLAN Identifier	IP Address	Interface Type
General		employee	11	10.10.11.5	Dynamic
Inventory		management	untagged	10.10.10.5	Static
Interfaces		virtual	N/A	1.1.1.1	Static
Interface Groups					
Multicast					

建立WLC訪客動態介面

完成以下步驟，以便為WLC新增動態介面，並將其對應到訪客VLAN:

1. 在WLC中，導覽至**Controller > Interfaces**。然後，按一下**New**。
2. 在WLC中，導覽至**Controller > Interfaces**。輸入以下內容：介面名稱：訪客VLAN id:12



3. 為訪客介面輸入以下內容：埠號：1VLAN識別符號：12IP地址：10.10.12.5網路掩碼：255.255.255.0網關：10.10.12.1DHCP:10.10.10.10

Configuration

Quarantine
Quarantine Vlan Id

Physical Information

Port Number
Backup Port
Active Port
Enable Dynamic AP Management

Interface Address

VLAN Identifier
IP Address
Netmask
Gateway

DHCP Information

Primary DHCP Server
Secondary DHCP Server

Access Control List

ACL Name

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

4. 確認已新增訪客介面。

Interface Name	VLAN Identifier	IP Address	Interface Type
employee	11	10.10.11.5	Dynamic
guest	12	10.10.12.5	Dynamic
management	untagged	10.10.10.5	Static
virtual	N/A	1.1.1.1	Static

新增802.1x WLAN

從WLC的初始啟動中，可能建立了一個預設WLAN。如果是，請按照指南中的說明修改它或建立一個新的WLAN以支援無線802.1X身份驗證。

請完成以下步驟：

1. 在WLC中，導覽至WLAN > Create New。



2. 對於WLAN，請輸入以下內容：配置檔名稱：pod1x SSID：相同



3. 對於WLAN settings > General頁籤，請使用以下內容：無線電策略：全部介面/組：管理所有其他內容：預設

MONITOR WLANs CONTROLLER WIRELESS SECURITY

WLANs > Edit 'pod1x'

General Security QoS Advanced

Profile Name pod1x

Type WLAN

SSID pod1x

Status Enabled

Security Policies [WPA2][Auth(802.1X)]
(Modifications done under security tab w

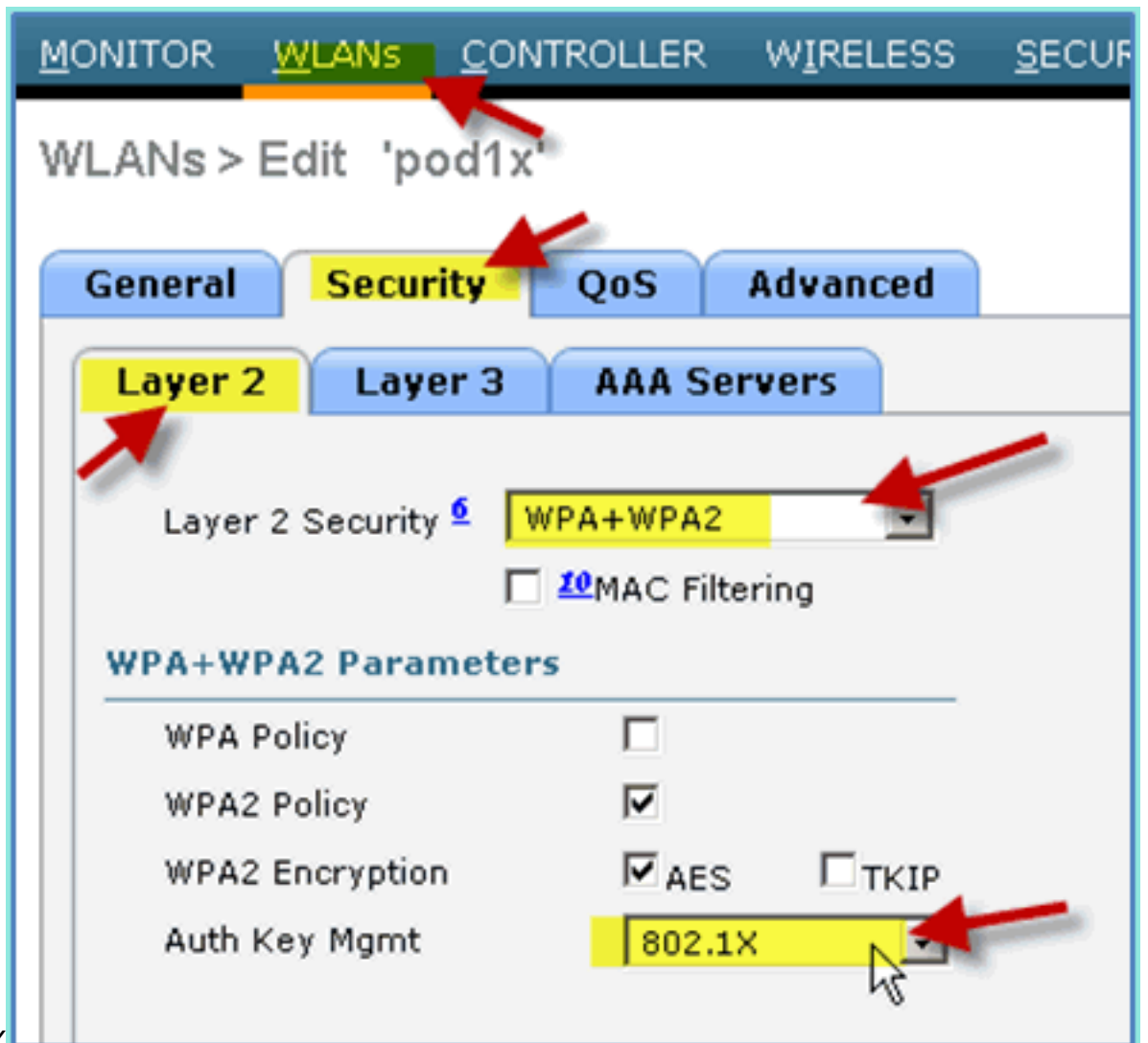
Radio Policy All

Interface/Interface Group(G) management

Multicast Vlan Feature Enabled

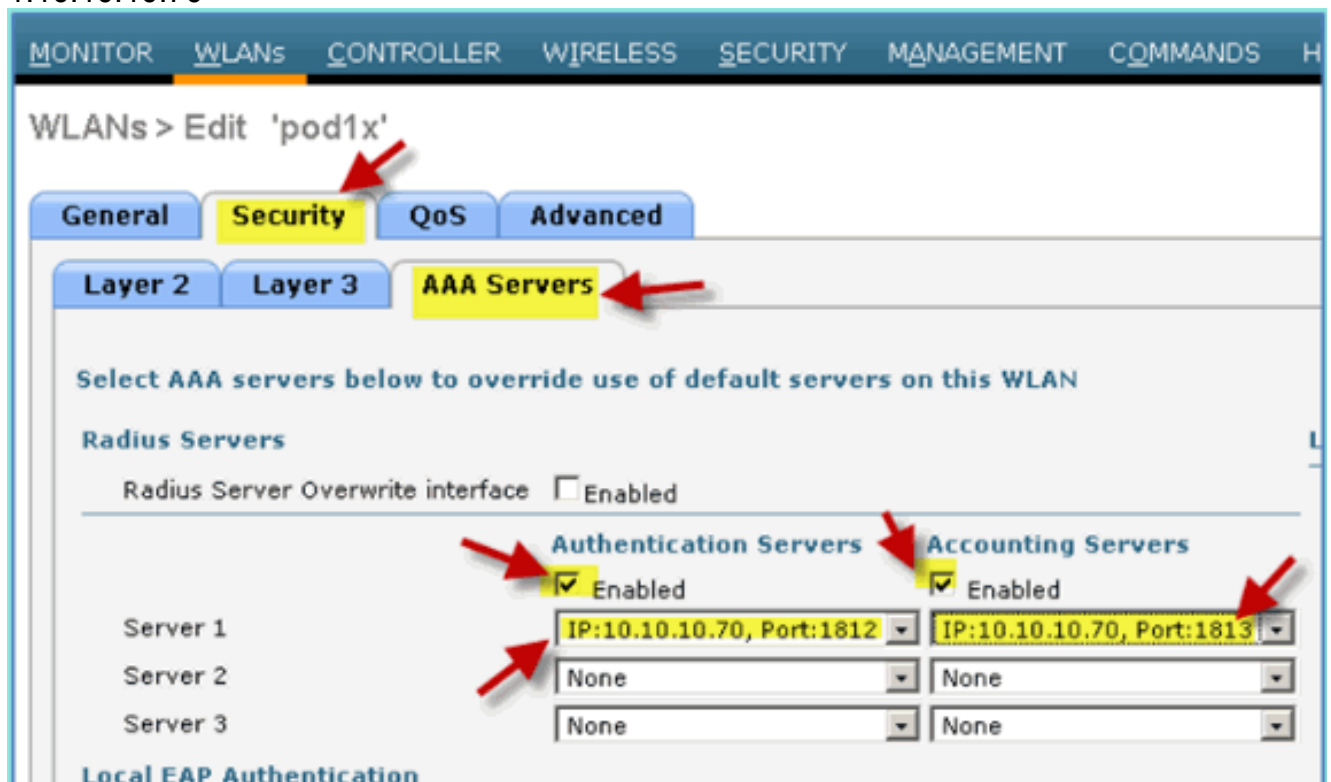
Broadcast SSID Enabled

4. 對於WLAN > Security頁籤>第2層，請設定以下內容：第2層安全：WPA+WPA2WPA2策略/加密：啟用/AES身份驗證金鑰管理



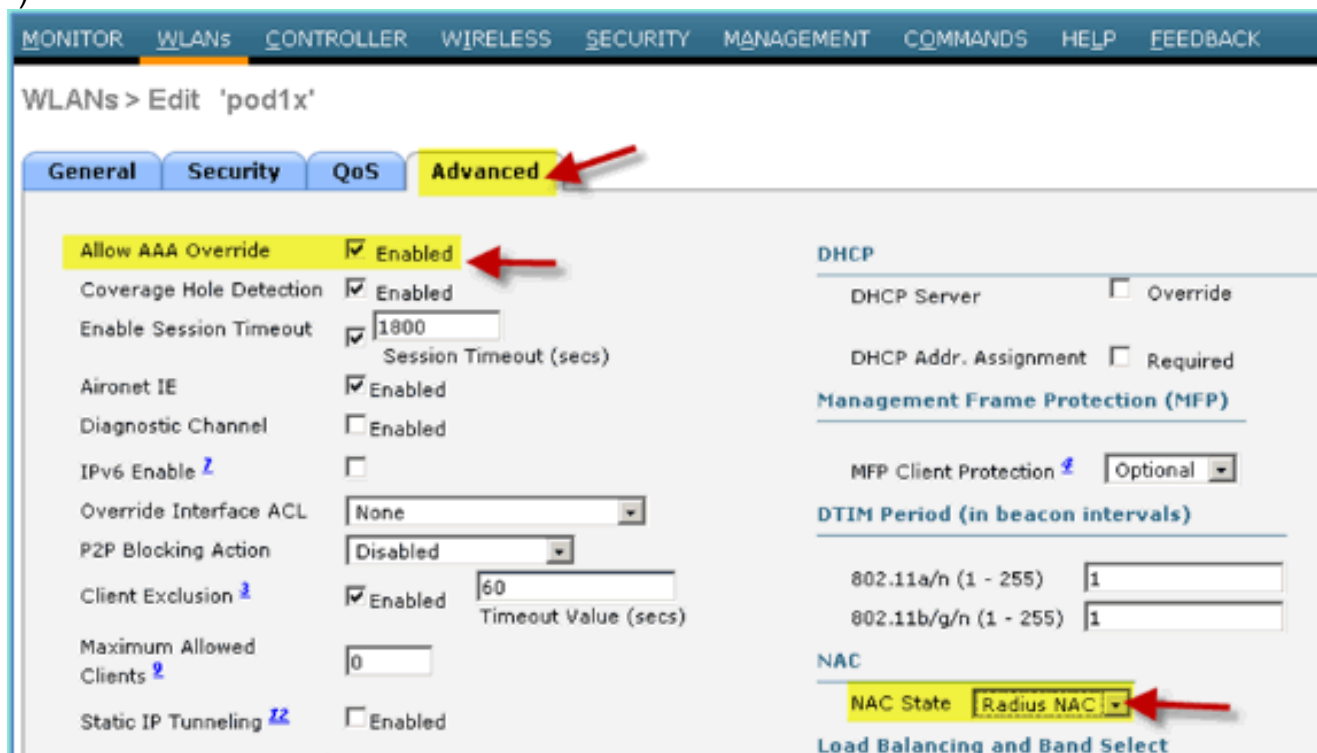
: 802.1X

5. 對於WLAN > Security頁籤> AAA Servers，設定以下內容：無線電伺服器覆蓋介面：已禁用身份驗證/記帳伺服器：已啟用伺服器
1:10.10.10.70



6. 對於WLAN > Advanced頁籤，請設定以下內容：允許AAA覆蓋：已啟用NAC狀態：Radius

NAC (選中)



7. 回到WLAN > General索引標籤> Enable WLAN (覈取方塊)。

WLANs > Edit 'pod1x'

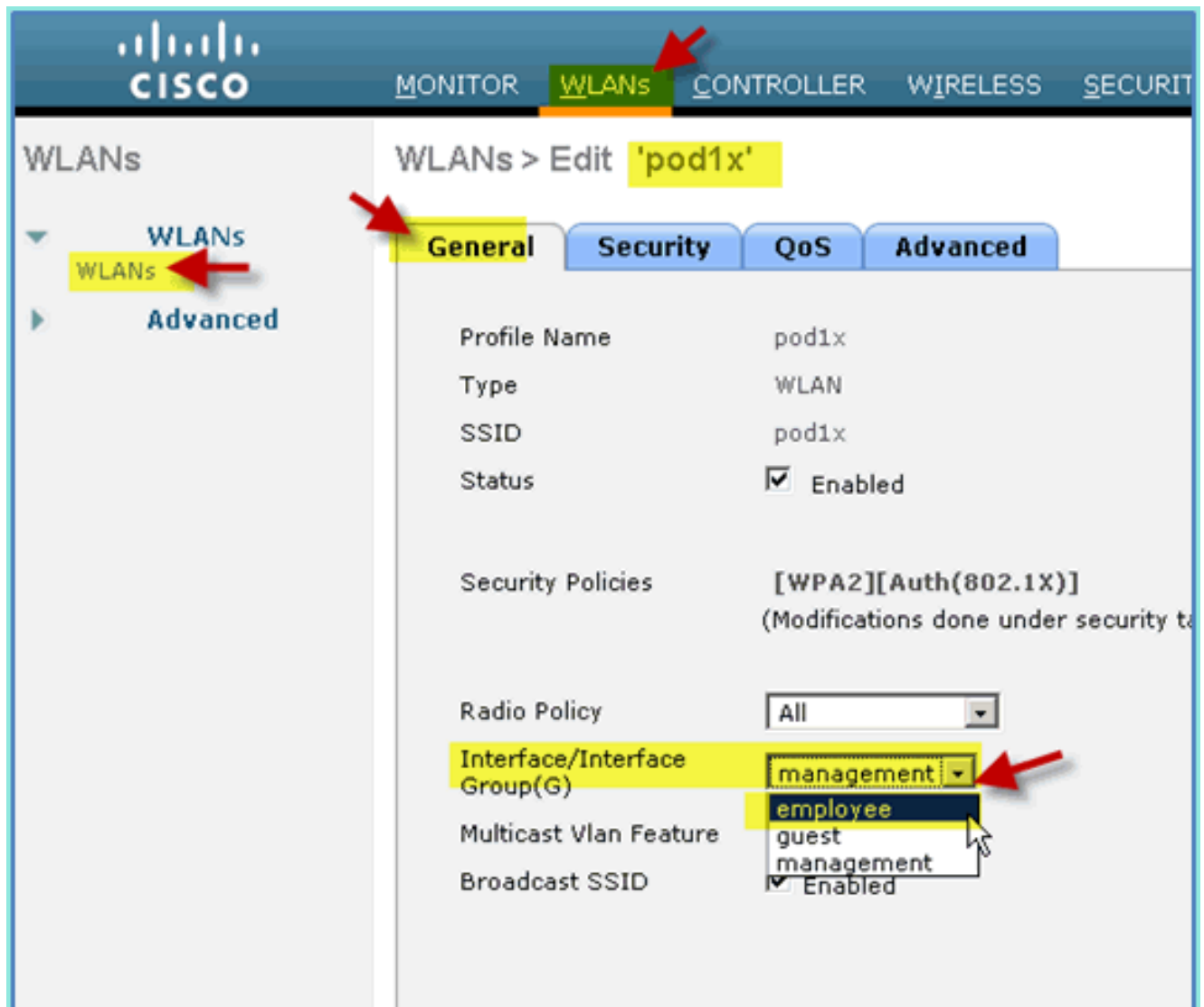
General Security QoS Advanced

Profile Name	pod1x
Type	WLAN
SSID	pod1x
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab)
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

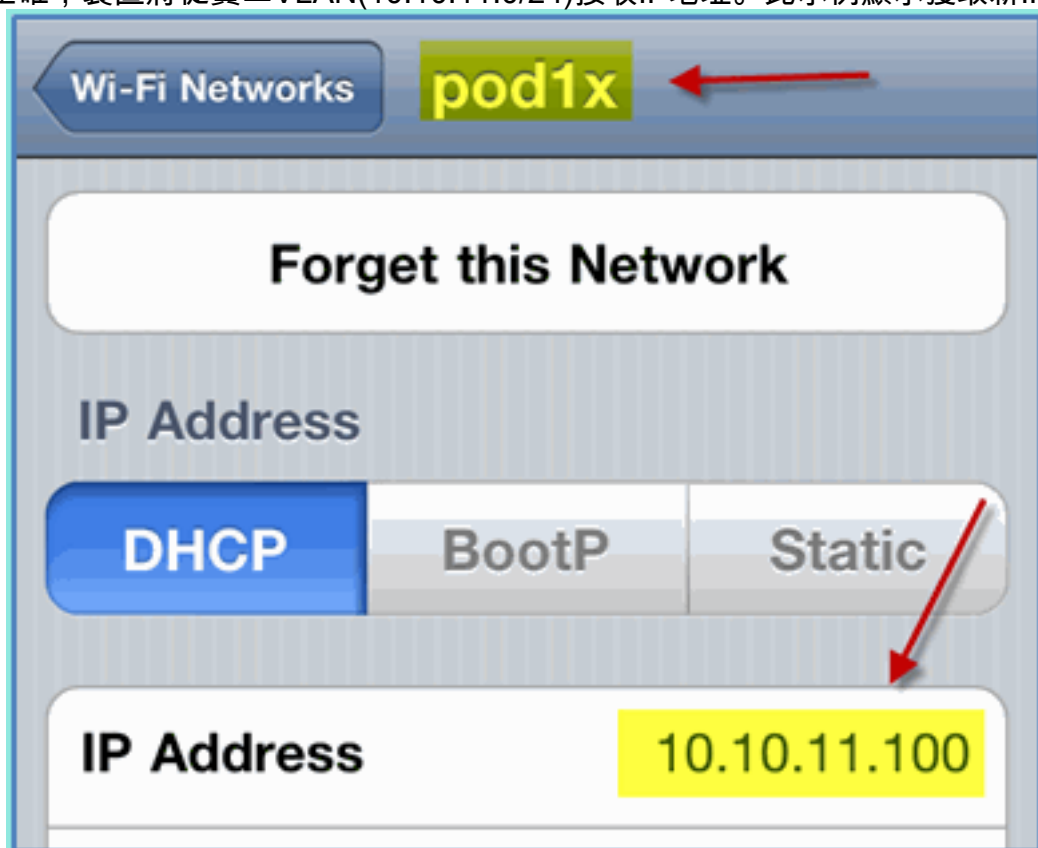
測試WLC動態介面

您需要快速檢查有效的員工和訪客介面。使用任何裝置與WLAN關聯，然後更改WLAN介面分配。

1. 在WLC中，導覽至WLAN > WLANs。按一下以編輯在前面練習中建立的安全SSID。
2. 將介面/介面組更改為Employee，然後按一下Apply。

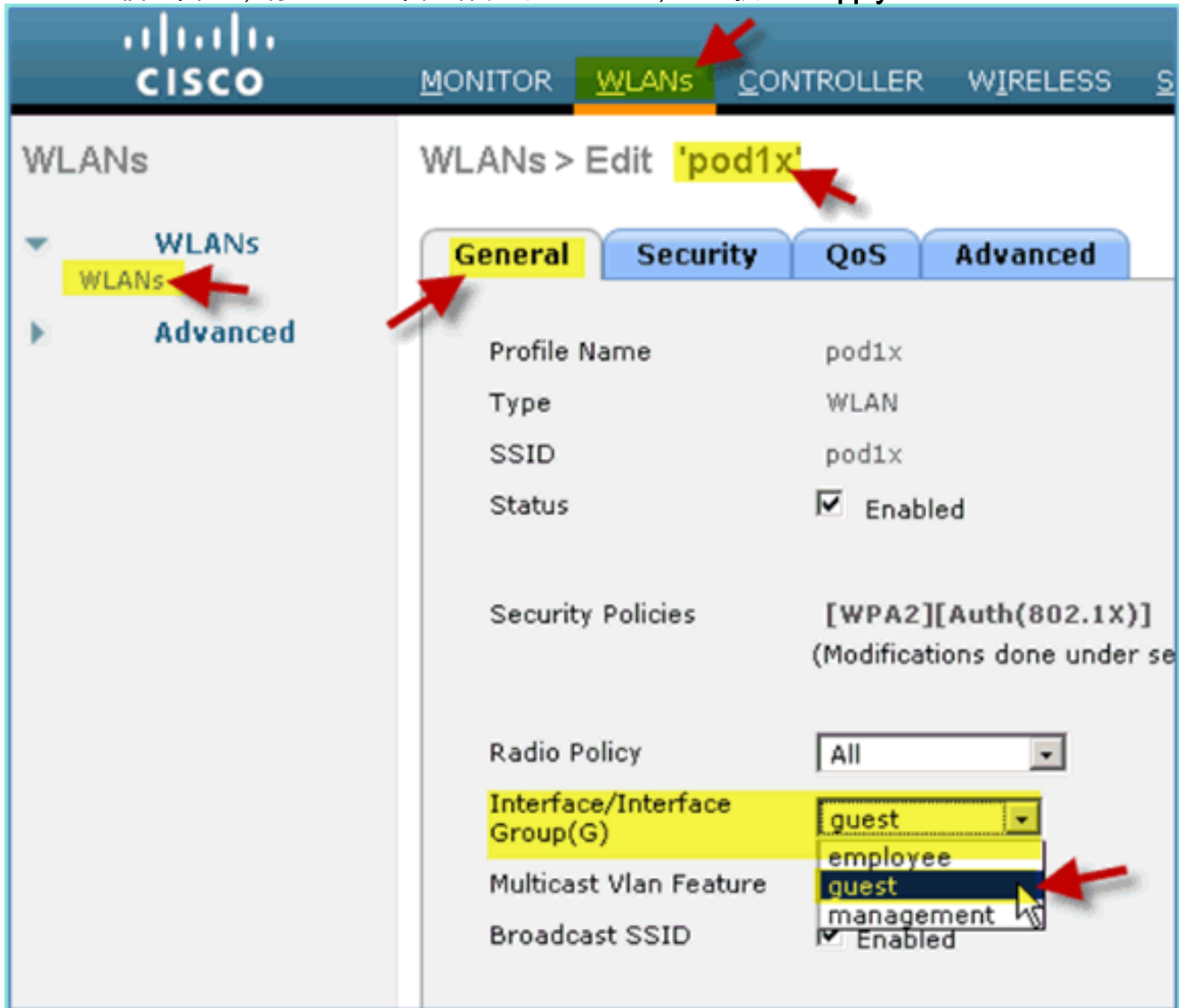


3. 如果配置正確，裝置將從員工VLAN(10.10.11.0/24)接收IP地址。此示例顯示獲取新IP地址的

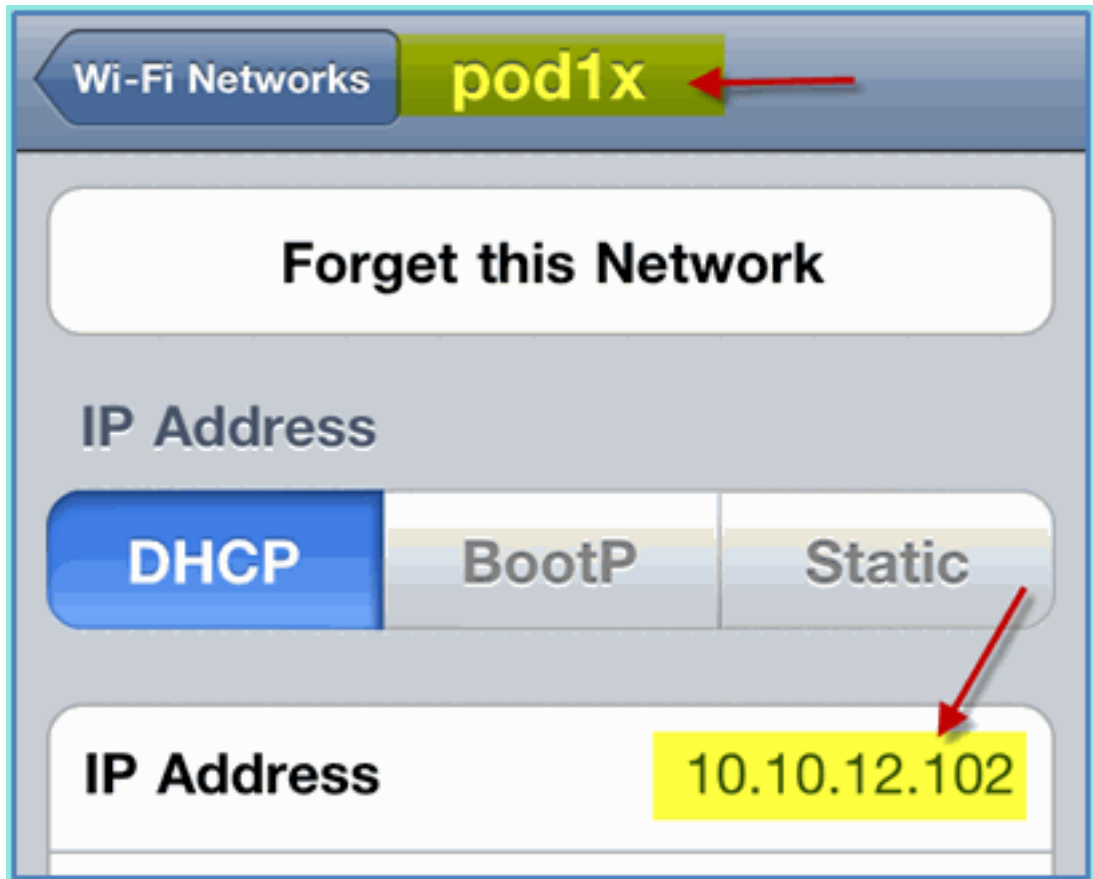


iOS裝置。

4. 確認上一個介面後，將WLAN介面分配更改為Guest，然後按一下Apply。



5. 如果配置正確，裝置將從訪客VLAN(10.10.12.0/24)接收IP地址。此示例顯示獲取新IP地址的



iOS裝置。

6. **重要資訊**：將介面分配更改回原始管理。
7. 按一下「Apply」，並儲存WLC的組態。

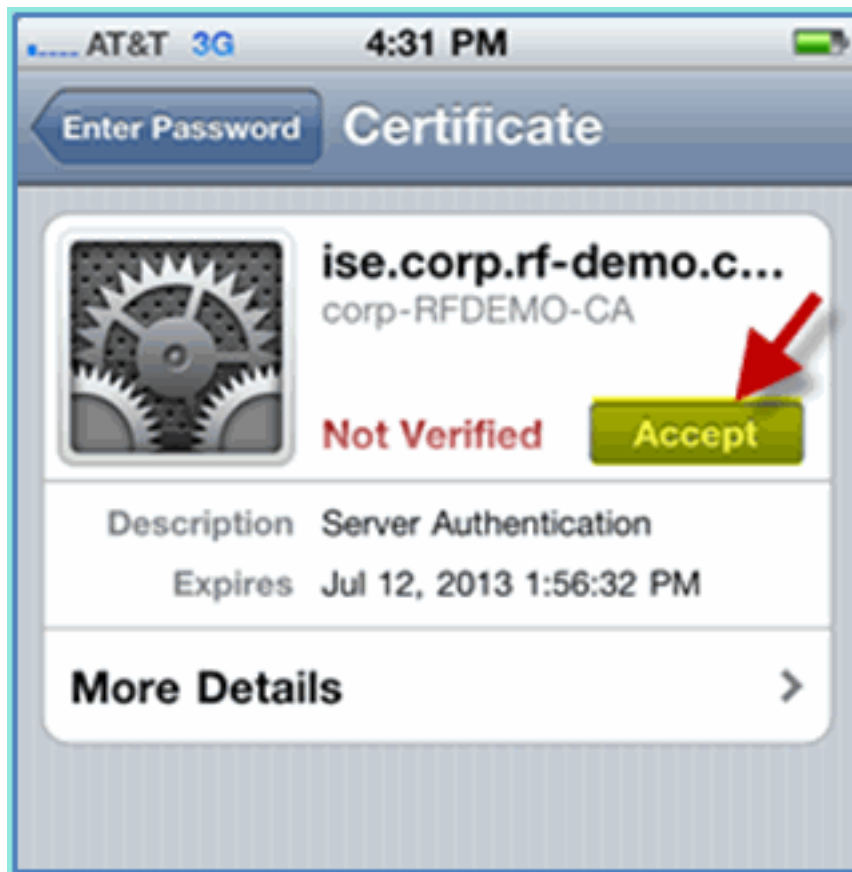
[適用於iOS的無線驗證\(iPhone/iPad\)](#)

使用iPhone、iPad或iPod等iOS裝置，通過經過身份驗證的SSID與內部使用者（或整合的AD使用者）關聯到WLC。如果不適用，請跳過這些步驟。

1. 在iOS裝置上，轉到WLAN設定。啟用WIFI，然後選擇上一節中建立的啟用802.1X的SSID。
2. 提供以下資訊以便連線：使用者名稱：員工（內部 — 員工）或承包商（內部 — 承包商）密碼



: XXXX



3. 按一下接受ISE證書。
4. 確認iOS裝置正在從管理(VLAN10)介面獲取IP地址。



5. 在WLC > Monitor > Clients上，驗證終端資訊，包括使用、狀態和EAP型別。

The screenshot displays the Cisco ISE Monitor interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', and 'WIRELESS'. The left sidebar shows a menu with 'Monitor' selected, and sub-items like 'Summary', 'Access Points', 'Cisco CleanAir', 'Statistics', 'CDP', 'Rogues', 'Clients', and 'Multicast'. The main content area is titled 'Clients > Detail' and is divided into two sections: 'Client Properties' and 'Security Information'.



Client Properties

MAC Address	5c:59:48:40:82:8d
IP Address	10.10.10.102
Client Type	Regular
User Name	aduser
Port Number	1
Interface	management
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Management Frame Protection	No

Security Information

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	PEAP
SNMP NAC State	Access
Radius NAC State	RUN
AAA Override ACL Name	none

6. 同樣，客戶端資訊也可由ISE > Monitor > Authentication頁面提供。

Cisco Identity Services Engine							
Home		Monitor	Policy	Administration			
Authentications		Alarms	Reports	Troubleshoot			
Add or Remove Columns Refresh							
Time	Status	Details	Username	Endpoint ID	Network Device	Authorization Profiles	Ident
Jul 13,11 04:39:36.573 PM	✓		aduser	5C:59:48:40:82:8D	WLC	PermitAccess	
Jul 13,11 04:38:46.285 PM	✓		aduser	5C:59:48:40:82:8D	WLC	PermitAccess	

7. 按一下**Details**圖示可細化到會話以獲取會話的深入資訊。

Cisco Identity Services Engine	
Showing Page 1 of 1 First Prev	
AAA Protocol > RADIUS Authentication Detail	
RADIUS Audit Session ID : 0a0a0a050000000d4e1e2a45	
AAA session ID :	ise/99967658/11
Date :	July 13,2011
Generated on July 13, 2011 4:41:11 PM PDT	
Authentication Summary	
Logged At:	July 13,2011 4:39:36.573 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	<u>aduser</u>
MAC/IP Address:	<u>5C:59:48:40:82:8D</u>
Network Device:	<u>WLC : 10.10.10.5 :</u>
Allowed Protocol:	<u>Default Network Access</u>
Identity Store:	AD1
Authorization Profiles:	PermitAccess
SGA Security Group:	
Authentication Protocol :	PEAP(EAP-MSCHAPv2)

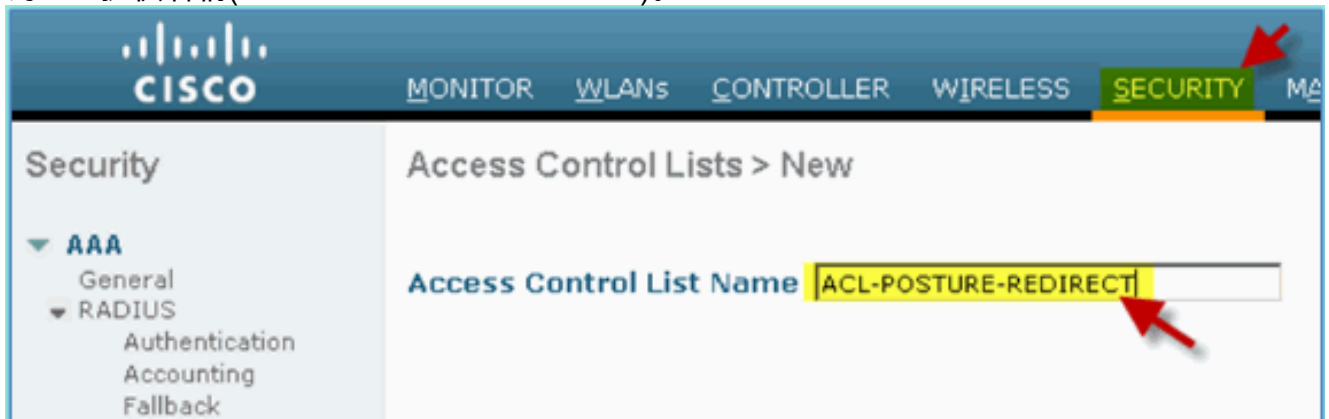
將狀態重新導向ACL新增到WLC

在WLC上配置終端安全評估重定向ACL，ISE將用於限制客戶端安全評估。ACL至少可以有效地允許ISE之間的流量。如果需要，可以在此ACL中新增可選規則。

1. 導覽至WLC > Security > Access Control Lists > Access Control Lists。按一下「New」。



2. 為ACL提供名稱(ACL-POSTURE-REDIRECT)。



3. 點選新ACL的Add New Rule。將以下值設定為ACL序列#1。完成後按一下Apply。來源：任意
目的地：IP地址10.10.10.70、255.255.255協定：任意Action:
Permit

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Access Control Lists > Rules > Edit

Sequence: 1

Source: Any

Destination: IP Address

IP Address: 10.10.10.70

Netmask: 255.255.255.255

Protocol: Any

DSCP: Any

Direction: Any

Action: Permit

4. 已新增確認序列。

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 /	10.10.10.70 /	Any	Any	Any	Any	Any	0

5. 按一下「Add New Rule」。將以下值設定為ACL序列#2。完成後按一下Apply。來源：IP地址 10.10.10.70、255.255.255目標：任意協定：任意Action: Permit

Sequence: 2

Source: IP Address

IP Address: 10.10.10.70

Netmask: 255.255.255.255

Destination: Any

Protocol: Any

DSCP: Any

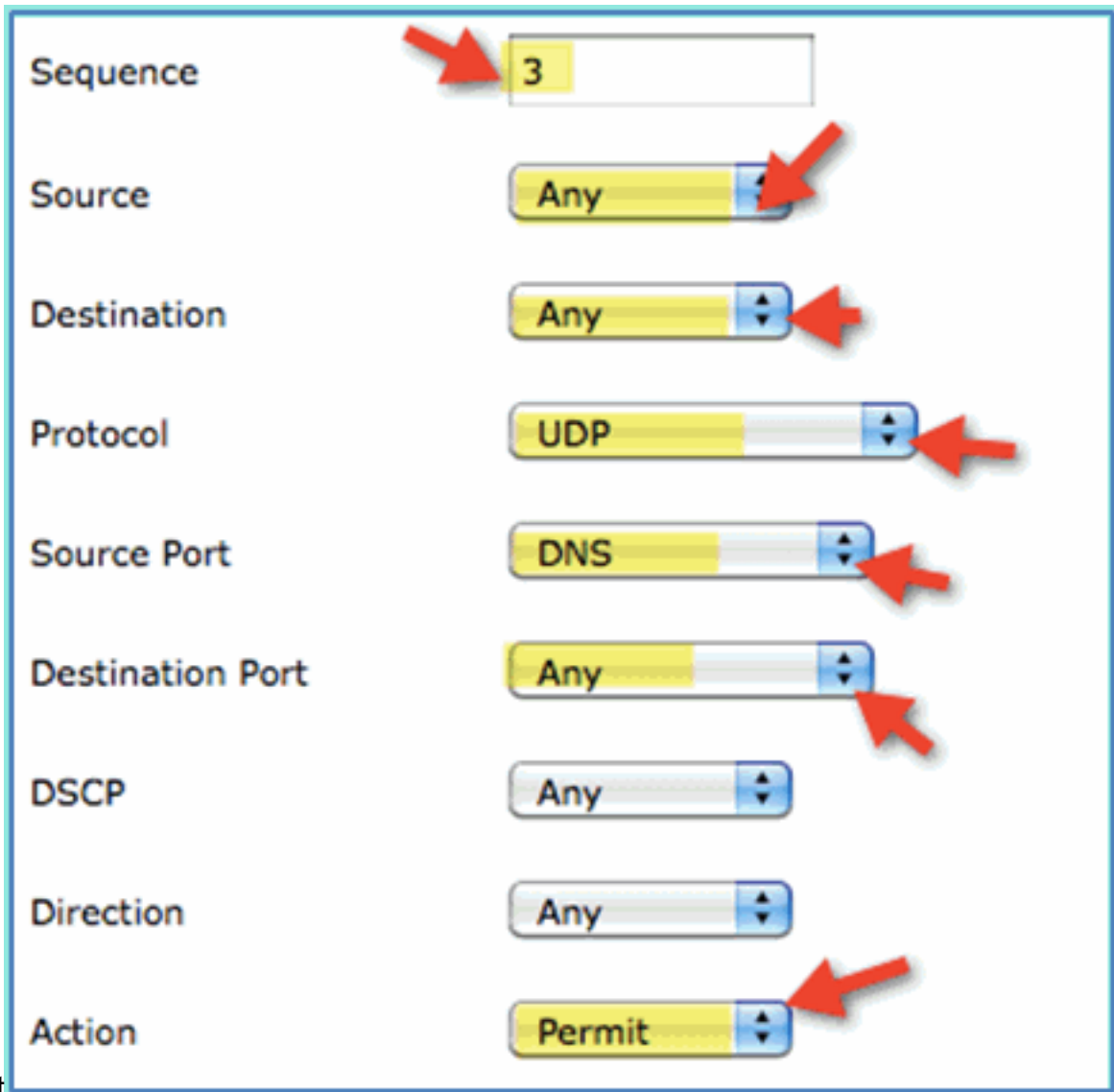
Direction: Any

Action: Permit

6. 已新增確認序列。

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0 /	10.10.10.70 /	Any	Any	Any	Any	Any
2	Permit	10.10.10.70 /	0.0.0.0 /	Any	Any	Any	Any	Any

7. 將以下值設定為ACL序列#3。完成後按一下Apply。來源：任意目標：任意協定：UDP源埠：DNS目的地連線埠：任意Action:



Sequence: 3

Source: Any

Destination: Any

Protocol: UDP

Source Port: DNS

Destination Port: Any

DSCP: Any

Direction: Any

Action: Permit

Permit

8. 已新增確認序列。

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0 /	10.10.10.70 /	Any	Any	Any	Any	Any
2	Permit	0.0.0.0 /	255.255.255.255 /	Any	Any	Any	Any	Any
3	Permit	0.0.0.0 /	0.0.0.0 /	UDP	DNS	Any	Any	Any

9. 按一下「Add New Rule」。將以下值設定為ACL序列#4。完成後按一下Apply。來源：任意目標：任意協定：UDP源埠：任意目的地連線埠：DNSAction:

Sequence: 4

Source: Any

Destination: Any

Protocol: UDP

Source Port: Any

Destination Port: DNS

DSCP: Any

Direction: Any

Action: Permit

Permit

10. 已新增確認序列。

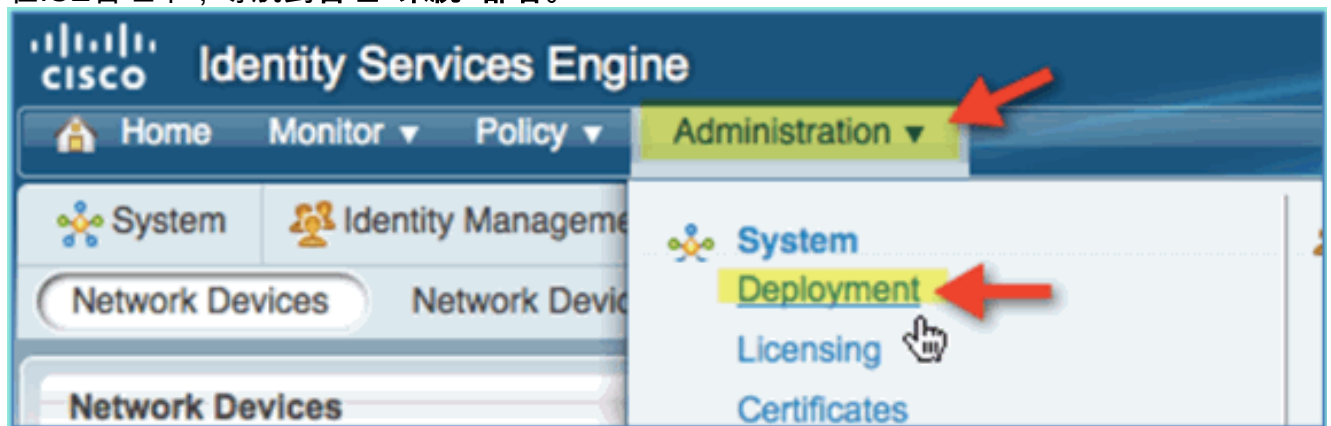
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0 /	10.10.10.70 /	Any	Any	Any	Any	Any
		0.0.0.0 /	255.255.255.255 /					
2	Permit	10.10.10.70 /	0.0.0.0 /	Any	Any	Any	Any	Any
		255.255.255.255 /	0.0.0.0 /					
3	Permit	0.0.0.0 /	0.0.0.0 /	UDP	DNS	Any	Any	Any
		0.0.0.0 /	0.0.0.0 /					
4	Permit	0.0.0.0 /	0.0.0.0 /	UDP	Any	DNS	Any	Any
		0.0.0.0 /	0.0.0.0 /					

11. 儲存目前的WLC組態。

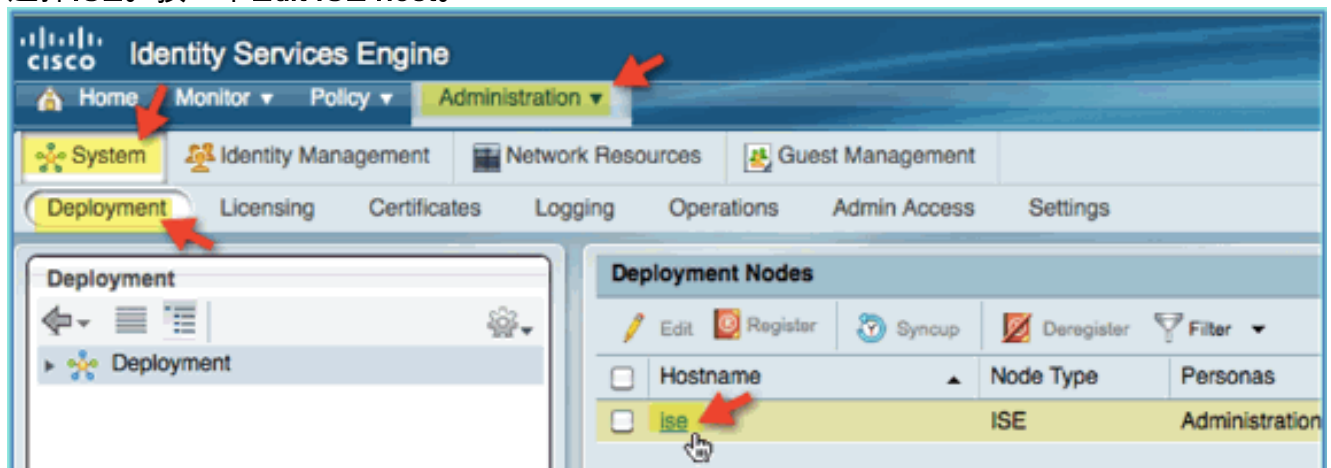
在ISE上啟用分析探測

需要將ISE配置為探測器，以有效地分析端點。預設情況下，這些選項處於禁用狀態。本節介紹如何將ISE配置為探測。

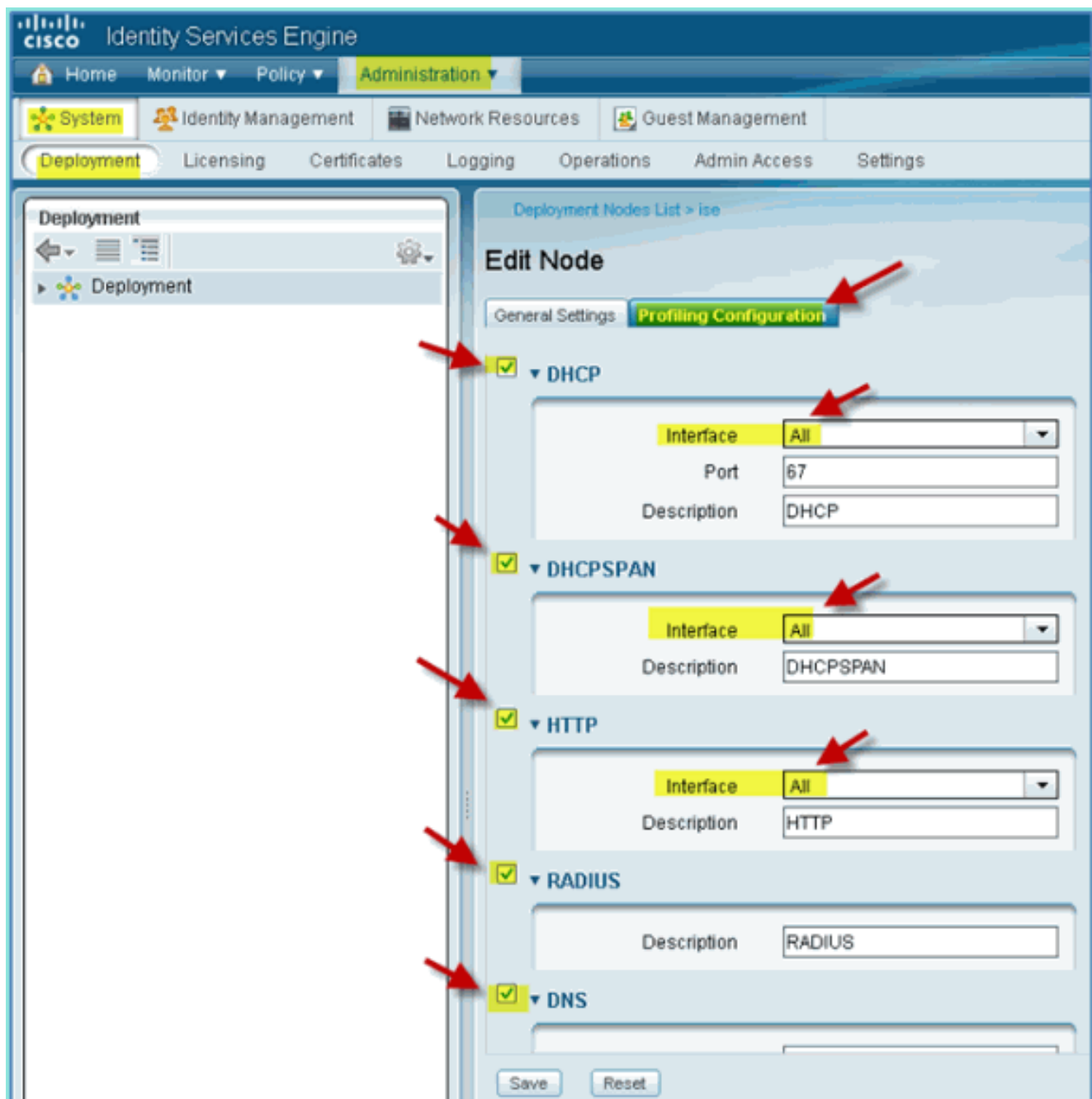
1. 在ISE管理中，導航到**管理>系統>部署**。



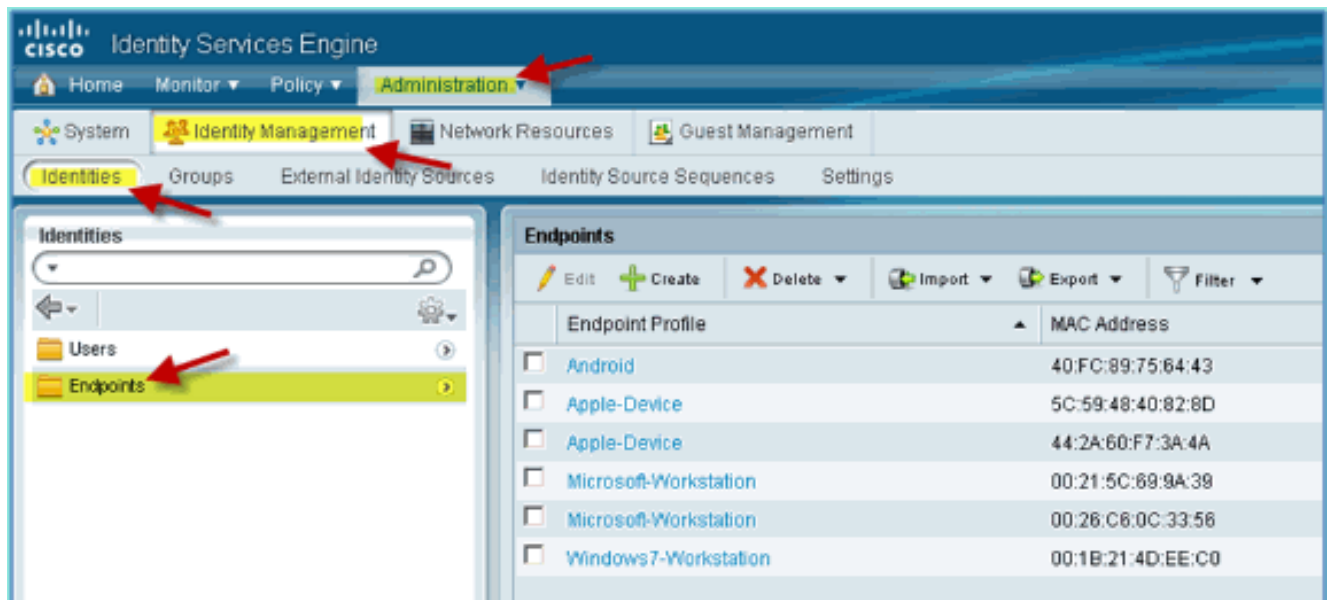
2. 選擇ISE。按一下**Edit ISE host**。



3. 從「編輯節點」頁中，選擇分析配置並配置以下內容：
DHCP：啟用、全部（或預設）
DHCPSPAN：啟用、全部（或預設）
HTTP: Enabled, All（或預設）
RADIUS：已啟用，不適用
DNS：已啟用，不適用



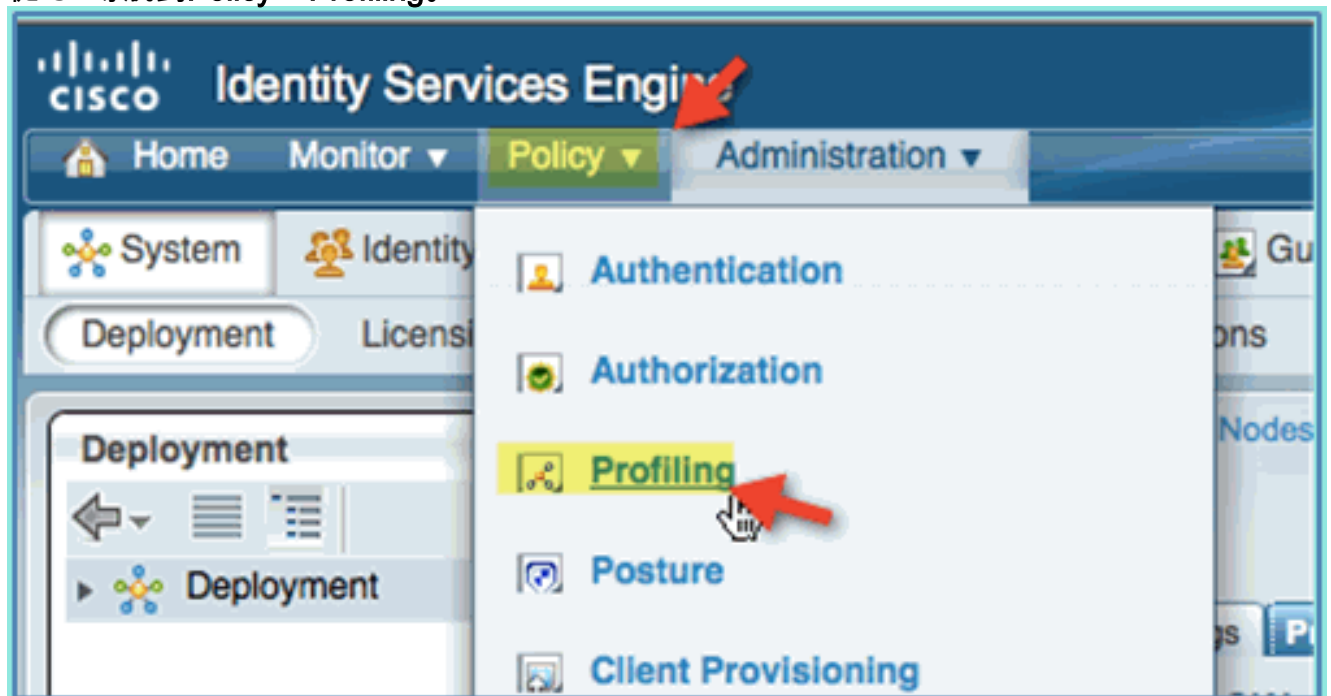
4. 重新關聯裝置 (iPhone/iPad/Droids/Mac等)。
5. 確認ISE終端標識。導航到**管理>身份管理>身份**。點選Endpoints以列出已分析的內容。**注意**：初始分析來自RADIUS探測器。



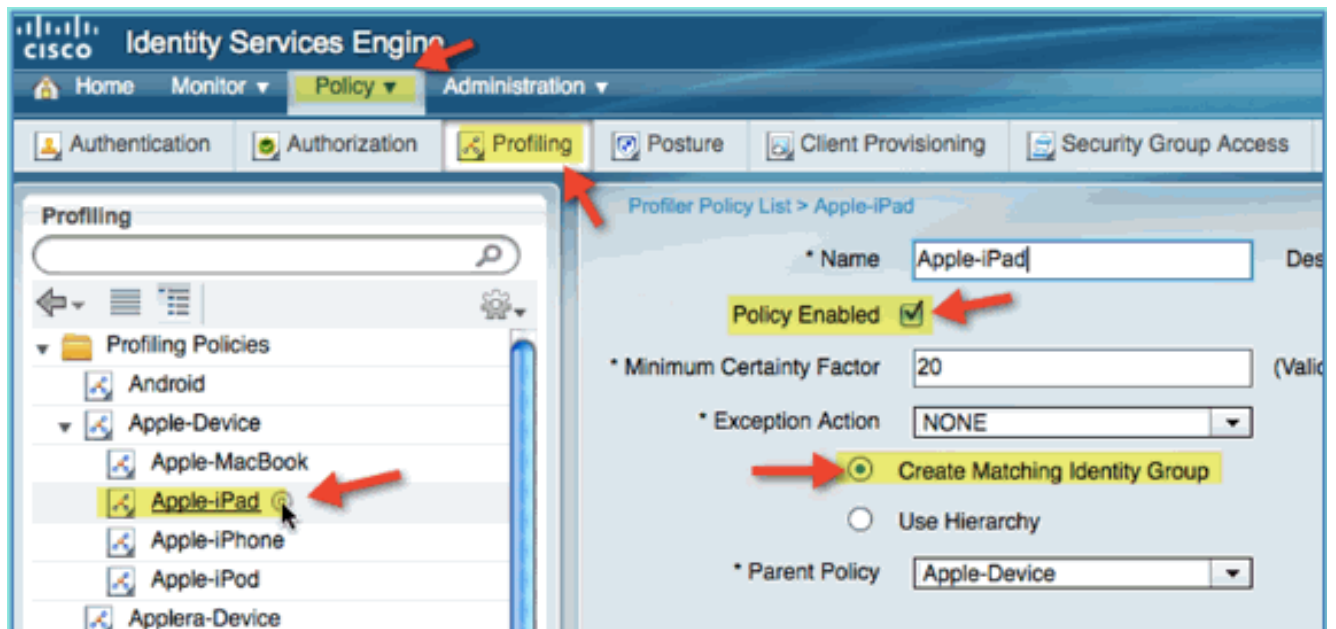
為裝置啟用ISE配置檔案策略

ISE開箱即用提供各種終端配置檔案庫。完成以下步驟，為裝置啟用設定檔：

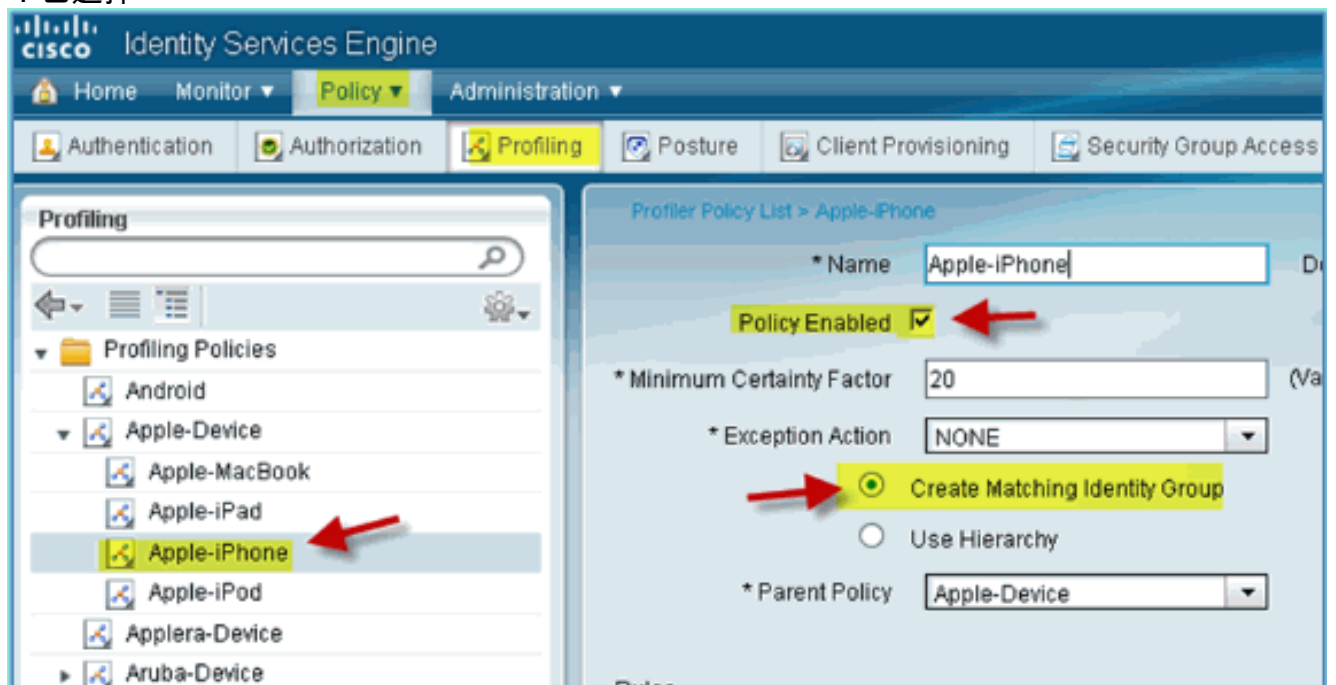
1. 從ISE導航到Policy > Profiling。



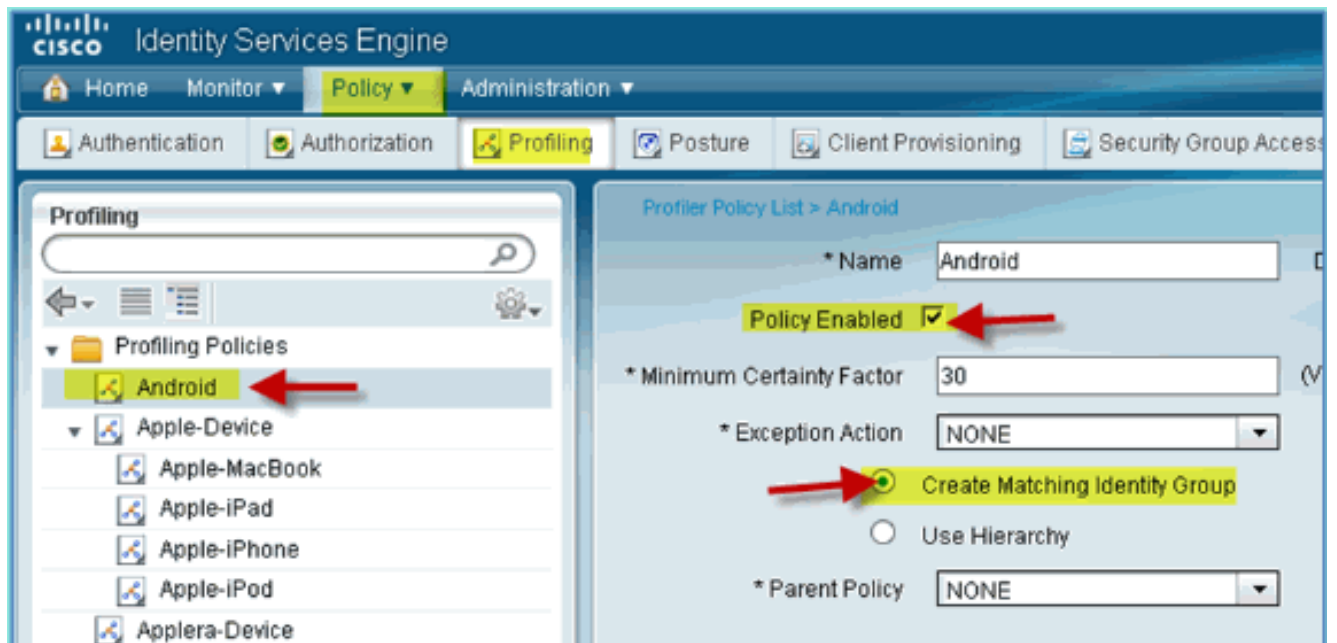
2. 在左窗格中，展開分析策略。
3. 按一下Apple Device > Apple iPad，然後設定以下內容：已啟用策略：已啟用建立匹配的身份組：已選擇



4. 按一下**Apple Device > Apple iPhone**，設定以下內容：已啟用策略：已啟用建立匹配的身份組：已選擇



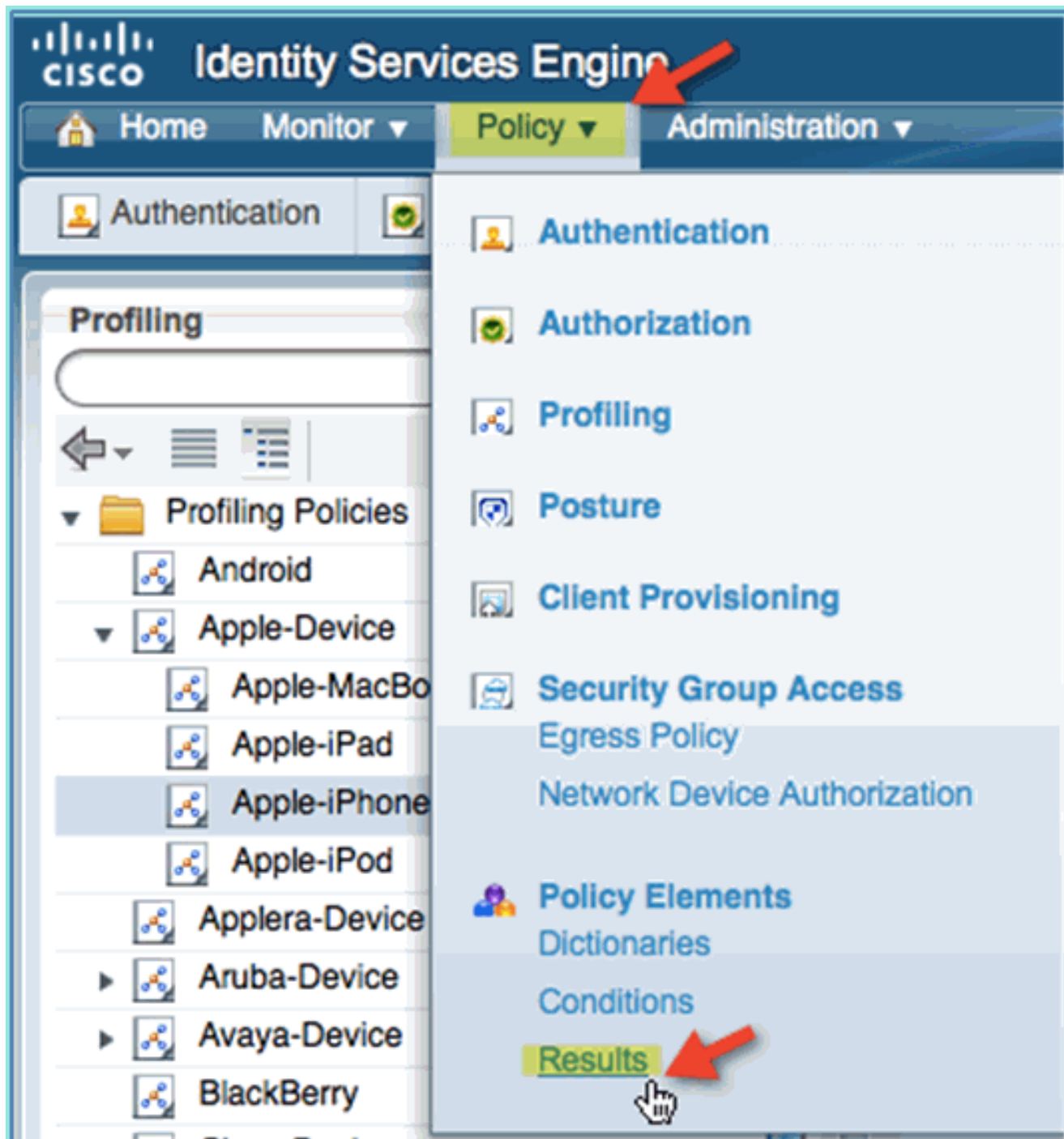
5. 按一下**Android**，設定以下內容：已啟用策略：已啟用建立匹配的身份組：已選擇



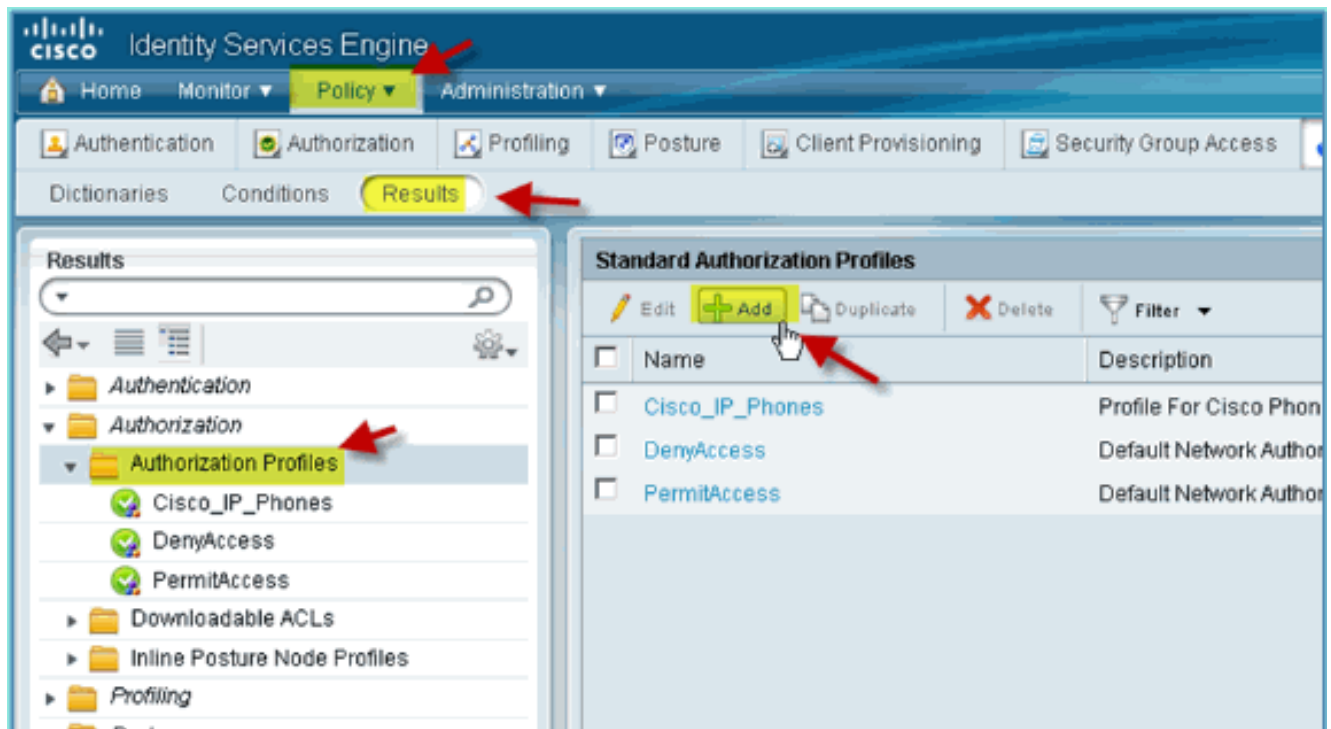
狀態發現重定向的ISE授權配置檔案

完成以下步驟，配置授權策略狀態重定向允許將新裝置重定向到ISE以進行正確發現和分析：

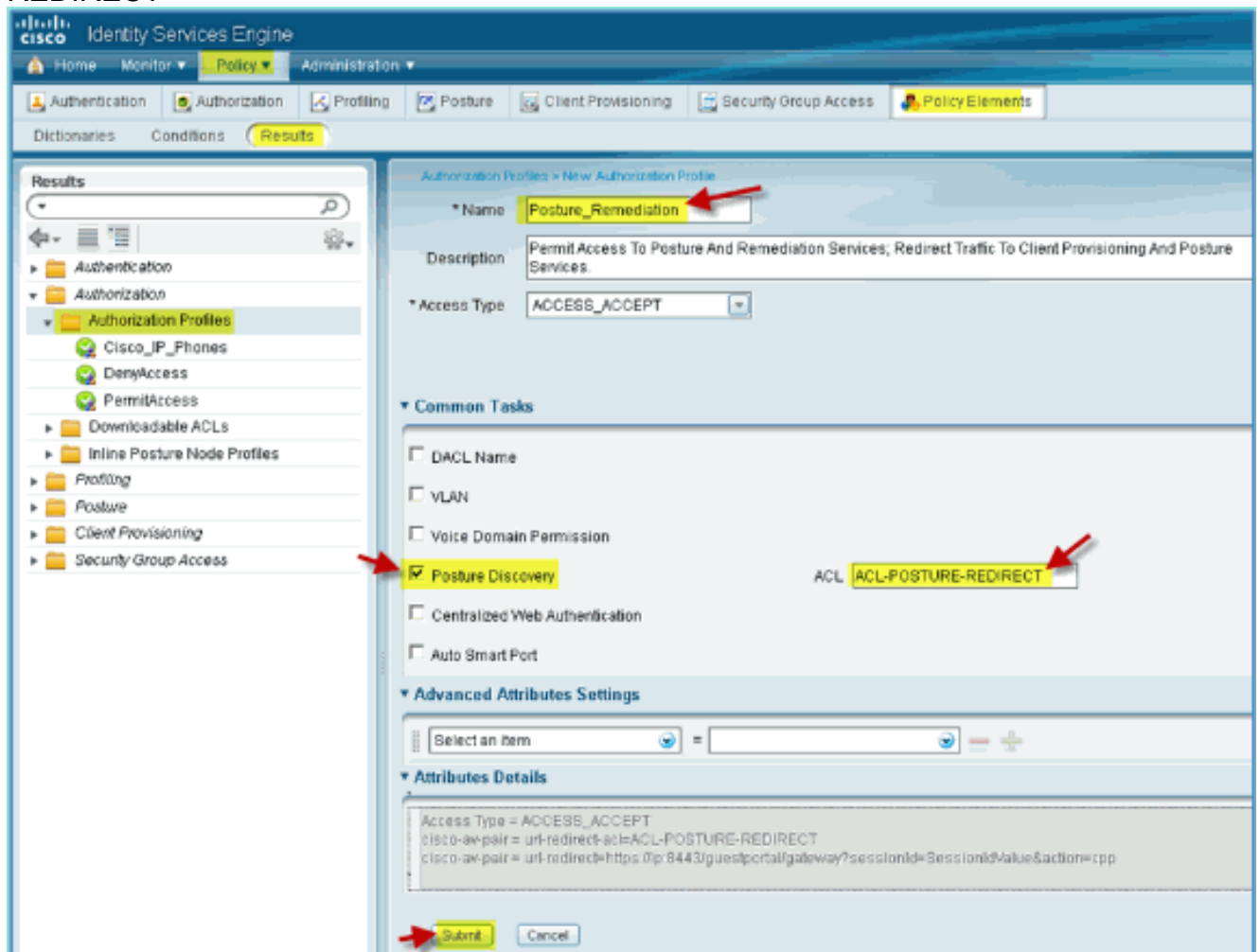
1. 從ISE導航到Policy > Policy Elements > Results。



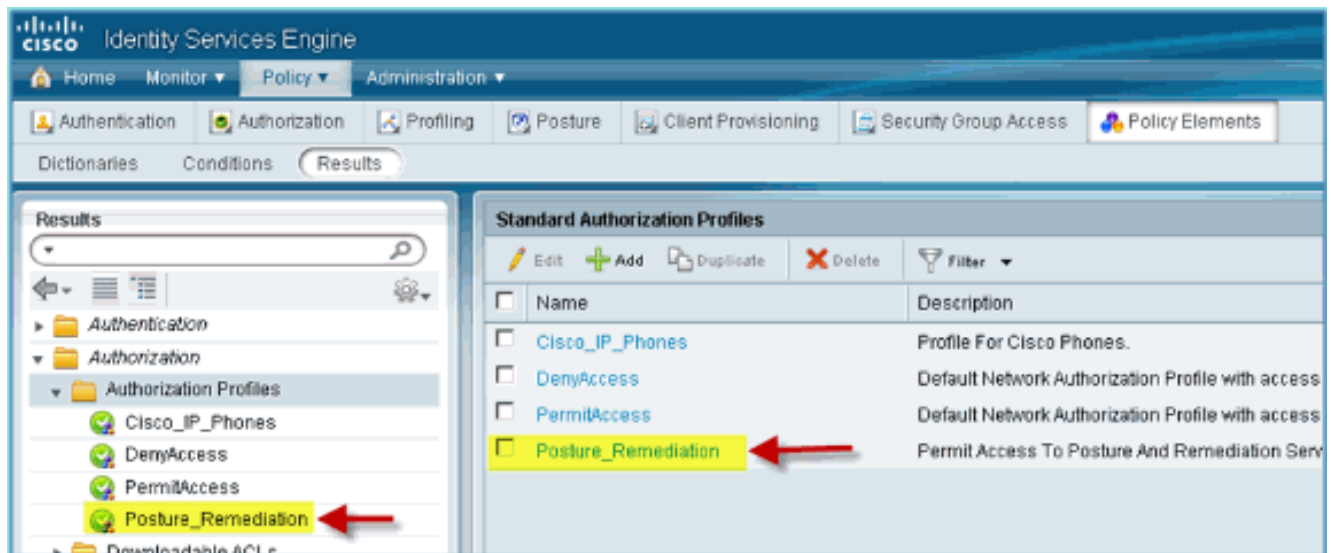
2. 展開授權。按一下Authorization Profiles (左窗格)，然後按一下Add。



3. 使用以下內容建立授權配置檔案：名稱：Posture_Remediation 訪問型別：Access_Accept 常用工具：狀態發現，已啟用狀態發現、ACL ACL-POSTURE-REDIRECT



4. 按一下提交以完成此任務。
5. 確認已新增新的授權配置檔案。

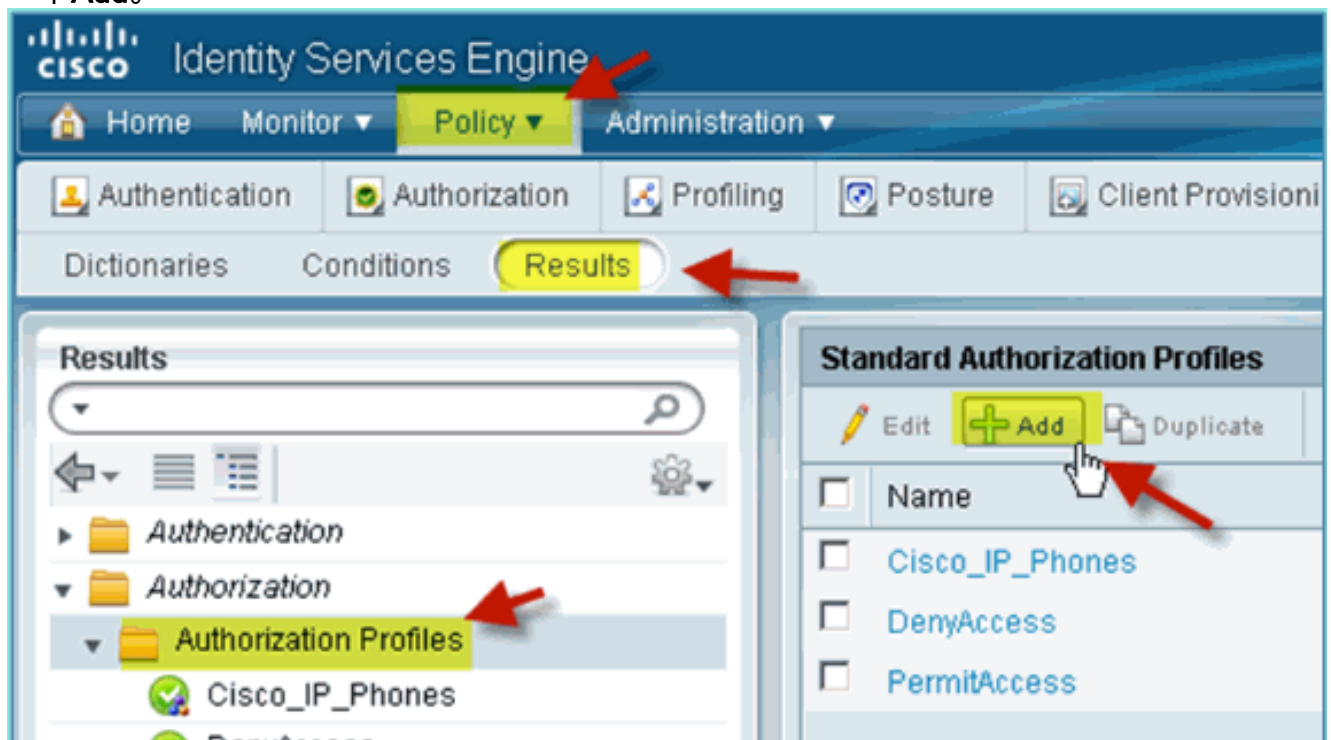


為員工建立ISE授權配置檔案

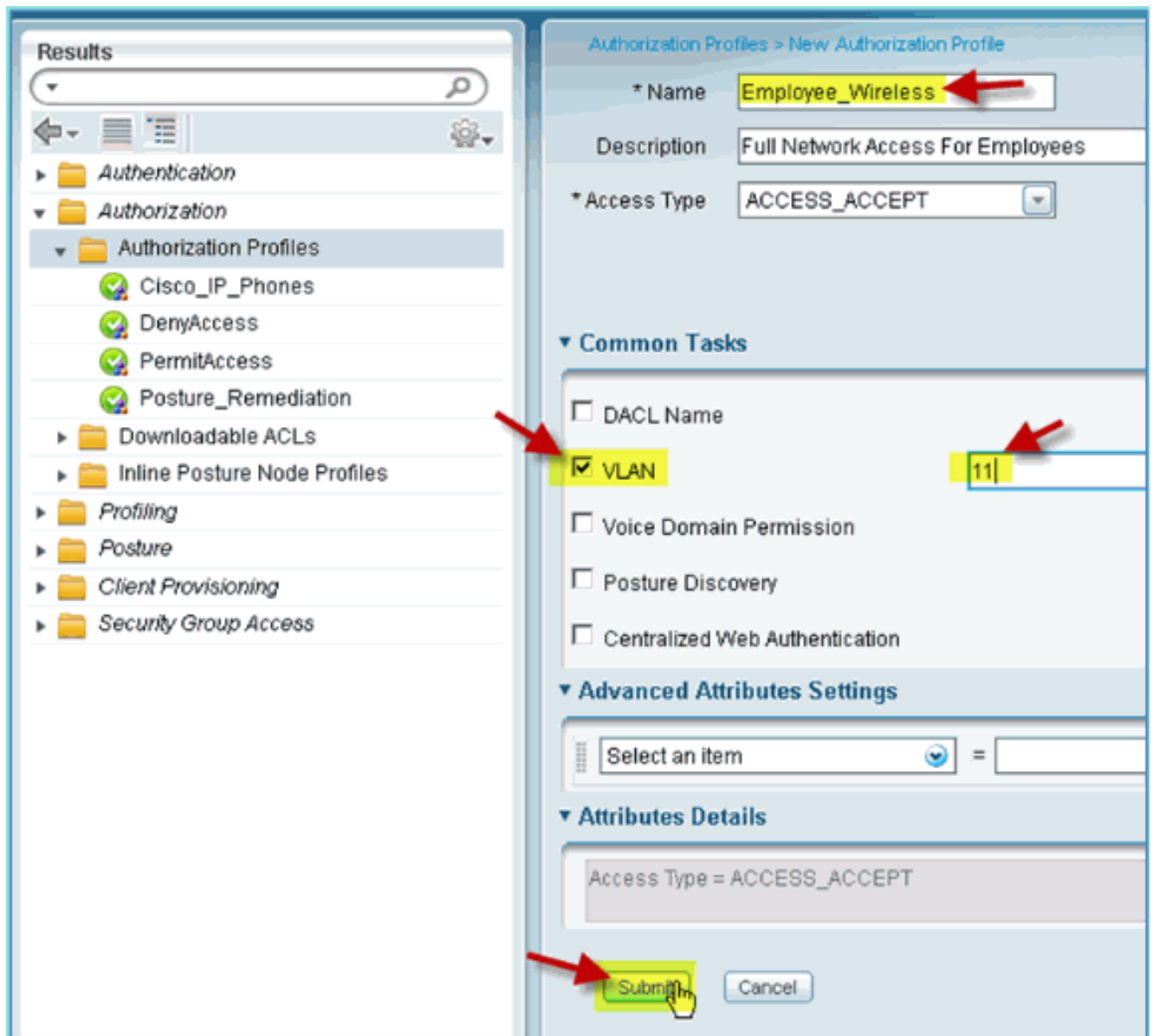
為員工新增授權配置檔案允許ISE使用分配的屬性授權和允許訪問。在此案例中分配了員工VLAN 11。

請完成以下步驟：

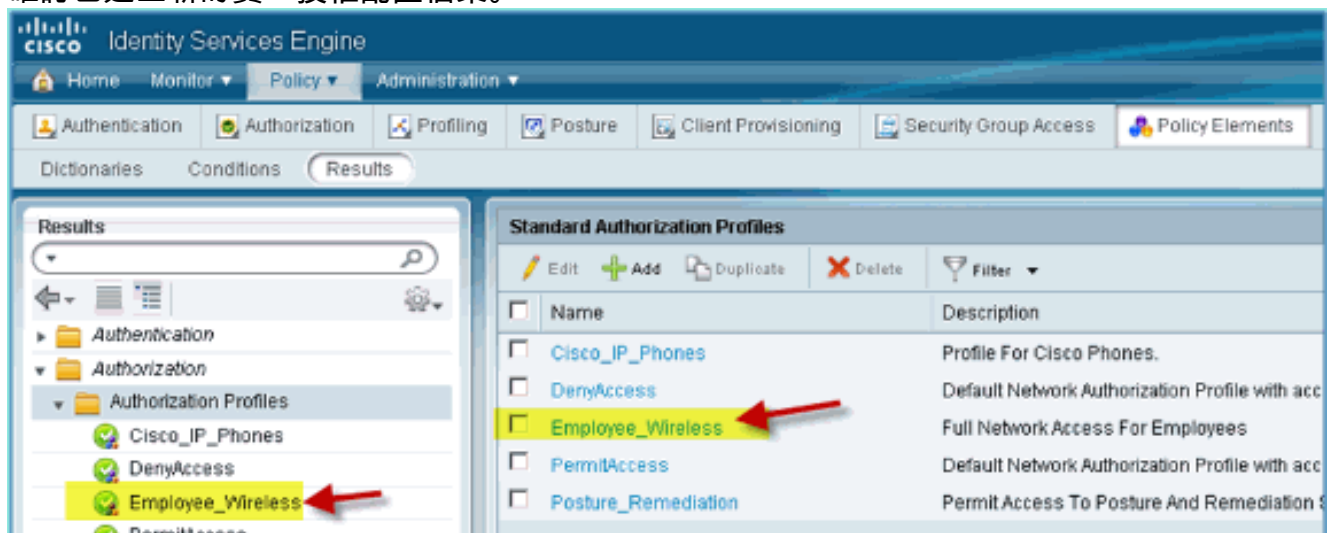
1. 從ISE導航到**Policy > Results**。展開**Authorization**，然後按一下**Authorization Profiles**，然後按一下**Add**。



2. 為員工授權配置檔案輸入以下內容：名稱：Employee_Wireless常見任務：VLAN，已啟用VLAN，子值11
3. 按一下**提交**以完成此任務。



4. 確認已建立新的員工授權配置檔案。

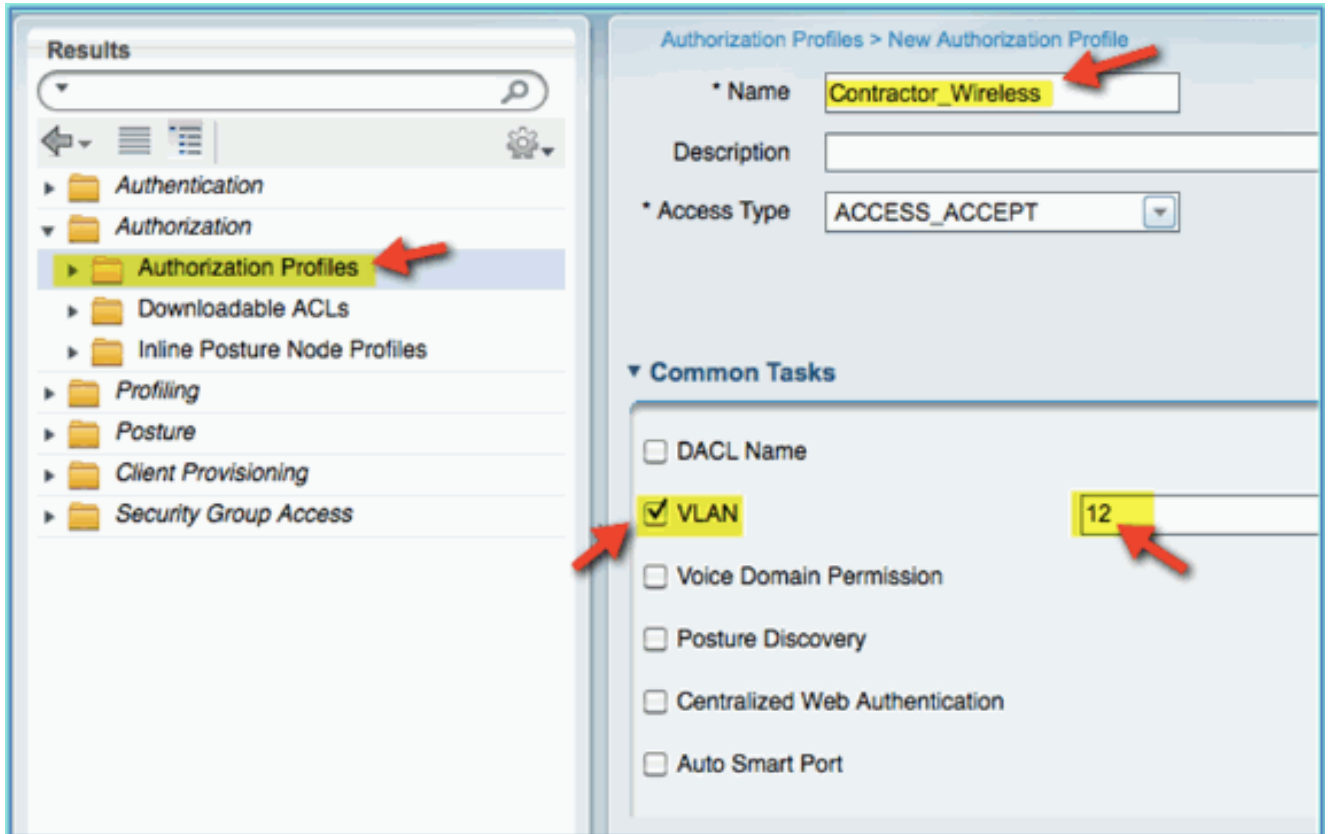


為承包商建立ISE授權配置檔案

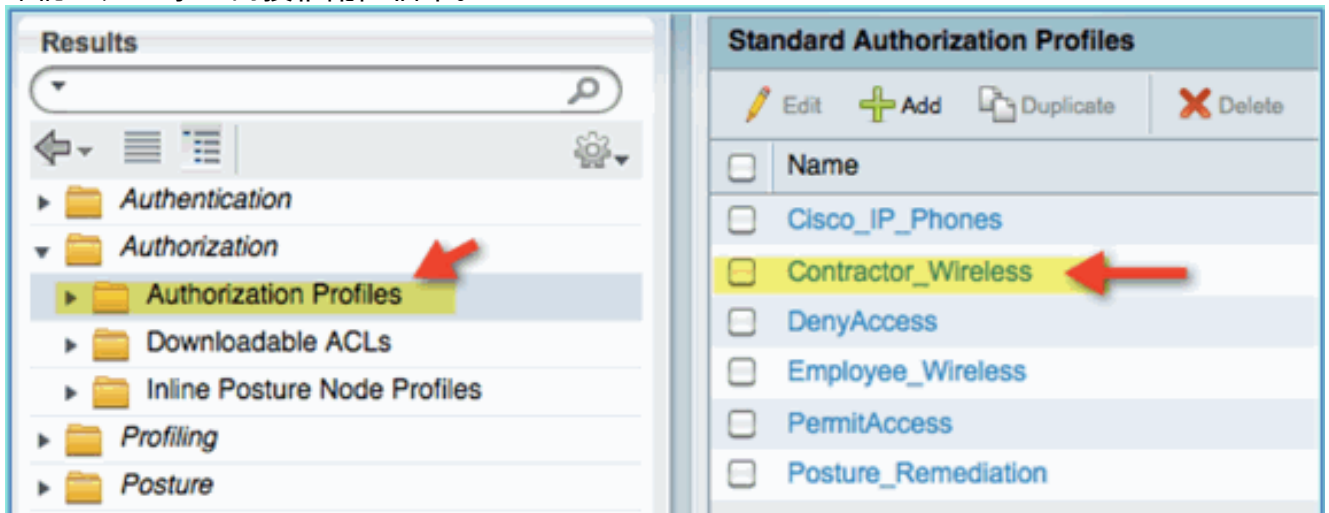
為承包商新增授權配置檔案允許ISE授權和允許具有指定屬性的訪問。在此案例中分配承包商VLAN 12。

請完成以下步驟：

1. 從ISE導航到Policy > Results。展開Authorization，然後按一下Authorization Profiles，然後按一下Add。
2. 為員工授權配置檔案輸入以下內容：名稱：Employee_Wireless常見任務：VLAN，已啟用VLAN，子值12



3. 按一下提交以完成此任務。
4. 確認已建立承包商授權配置檔案。

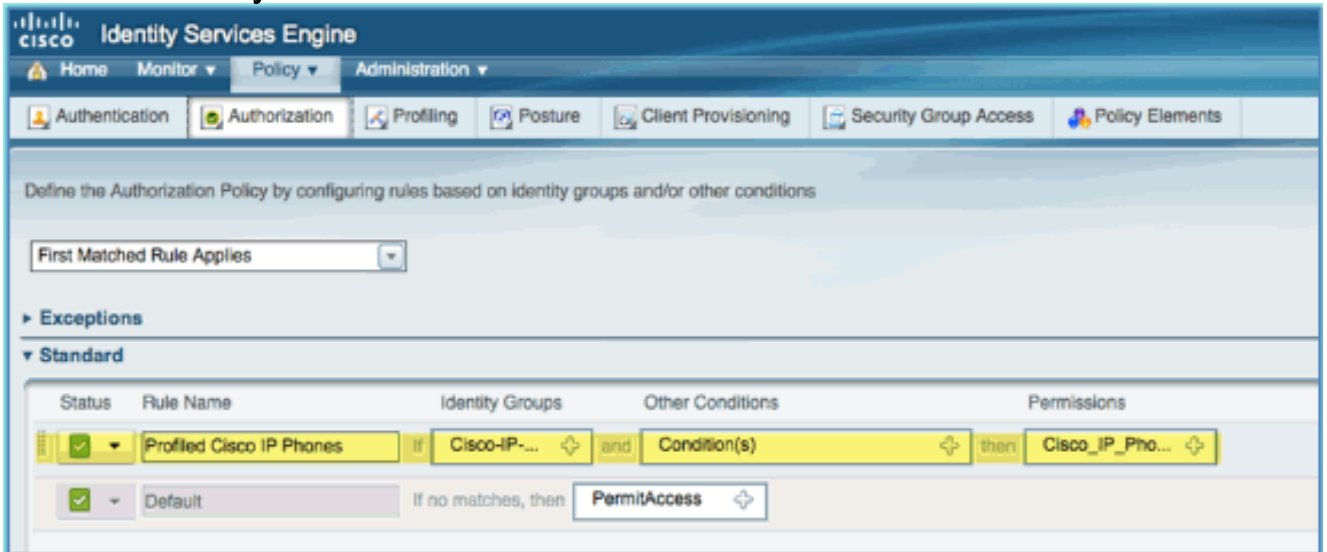


裝置狀態/分析的授權策略

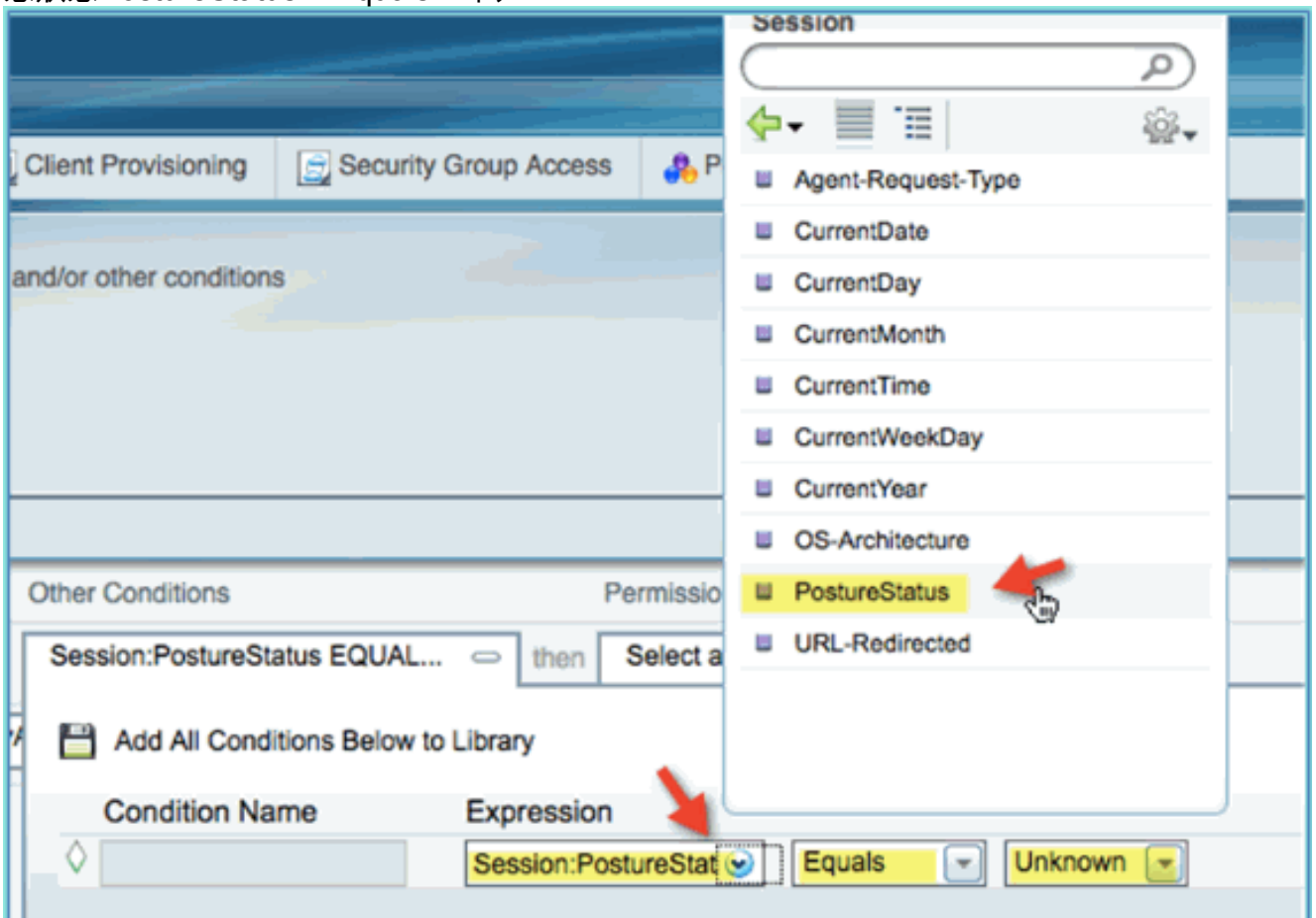
新裝置首次進入網路時，幾乎沒有關於它的資訊，管理員會建立相應的策略，以便在允許訪問之前識別未知端點。在本練習中，將建立授權策略，以便將新裝置重定向到ISE進行狀態評估（對於流動裝置是無代理的，因此僅與分析相關）；終端將重定向到ISE強制網路門戶並識別。

請完成以下步驟：

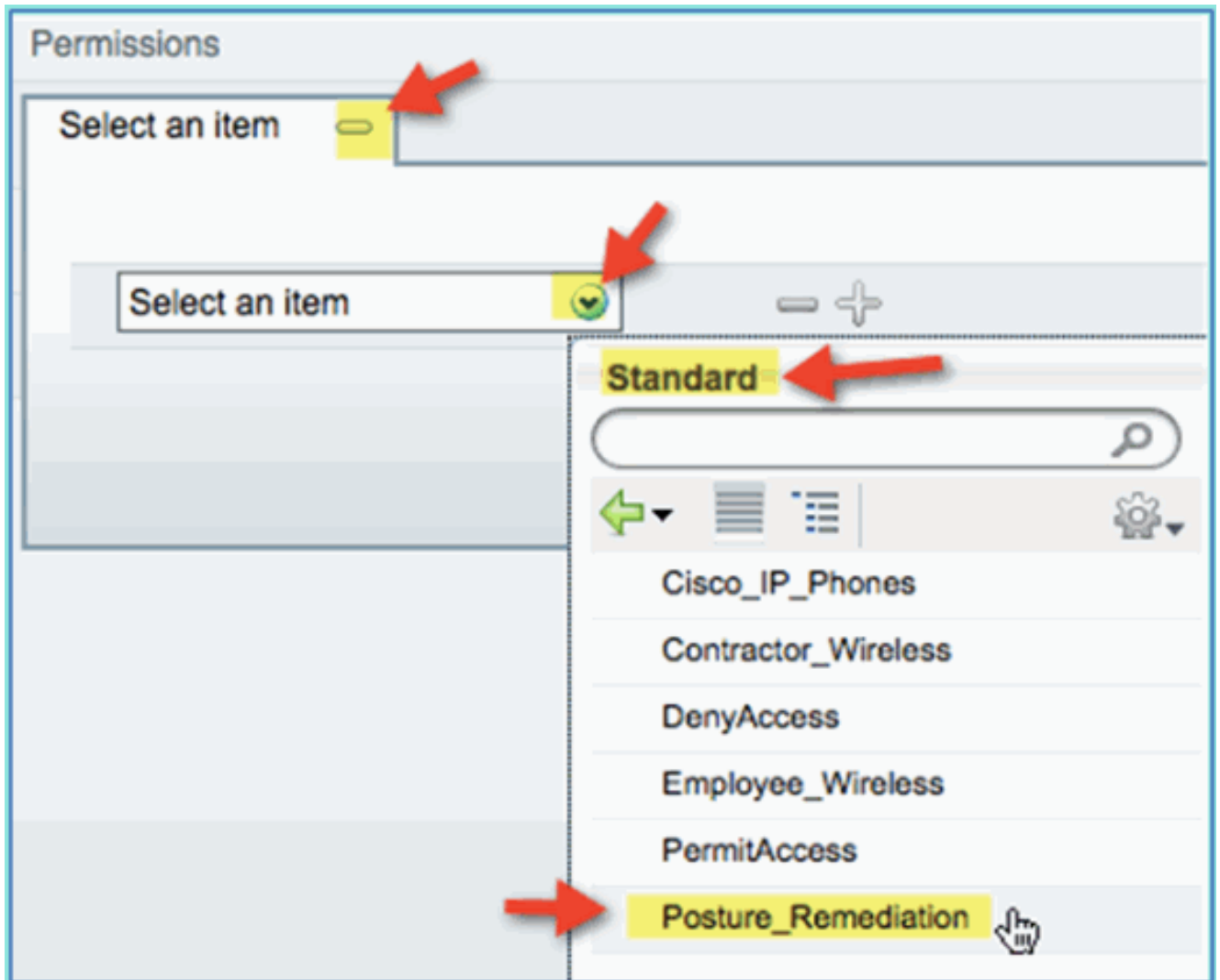
1. 從ISE導航到Policy > Authorization。



2. 已分析的Cisco IP電話有一個策略。這是開箱即用的。將此項編輯為狀態策略。
3. 為此策略輸入以下值：規則名稱：狀態_補救身份組：任意其他條件>新建：（高級）會話>狀態PostureStatus > Equals：未知



4. 設定以下許可權：Permissions > Standard:
Posture_Remediation

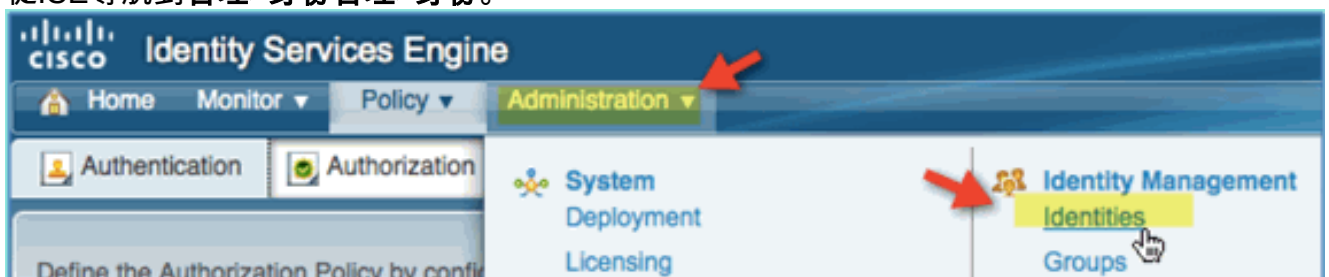


5. 按一下「Save」。注意：或者，可以建立自定義策略元素以增加易用性。

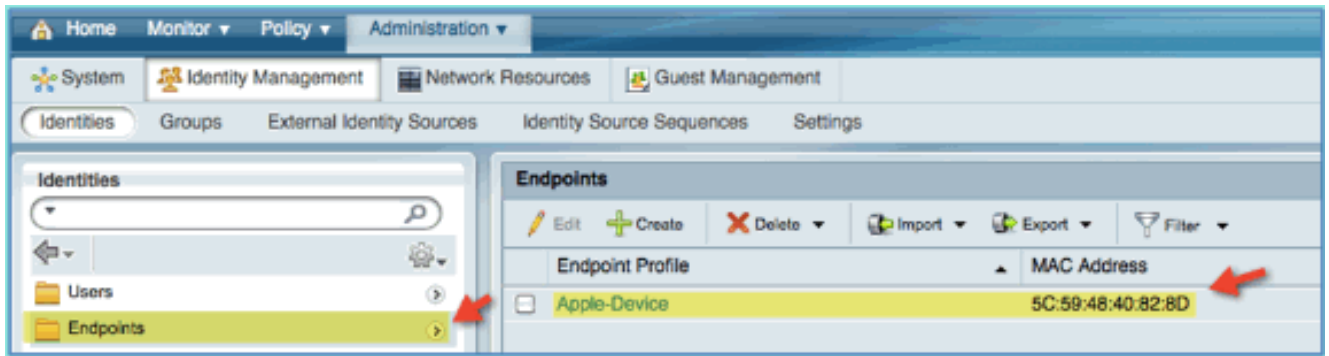
測試狀態修正策略

可以執行簡單演示，以顯示ISE正在根據終端安全評估策略正確分析新裝置。

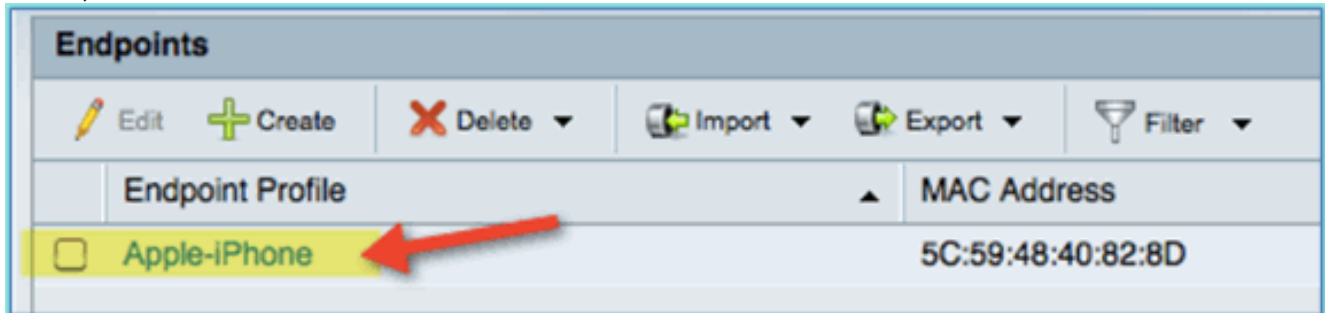
1. 從ISE導航到**管理>身份管理>身份**。



2. 按一下「Endpoints」。關聯並連線裝置（本例中為iPhone）。



3. 刷新端點清單。觀察給出的資訊。
4. 從終端裝置瀏覽到：URL:http://www (或10.10.10.10) 裝置已重定向。接受證書的任何提示。
5. 流動裝置完全重定向後，從ISE再次刷新終端清單。觀察已更改的內容。上一個終結點 (例如 , Apple-Device) 應更改為「Apple-iPhone」等。原因是HTTP探測器有效地獲取使用者代理資訊，這是重定向到強制網路門戶的過程的一部分。



差異化訪問的授權策略

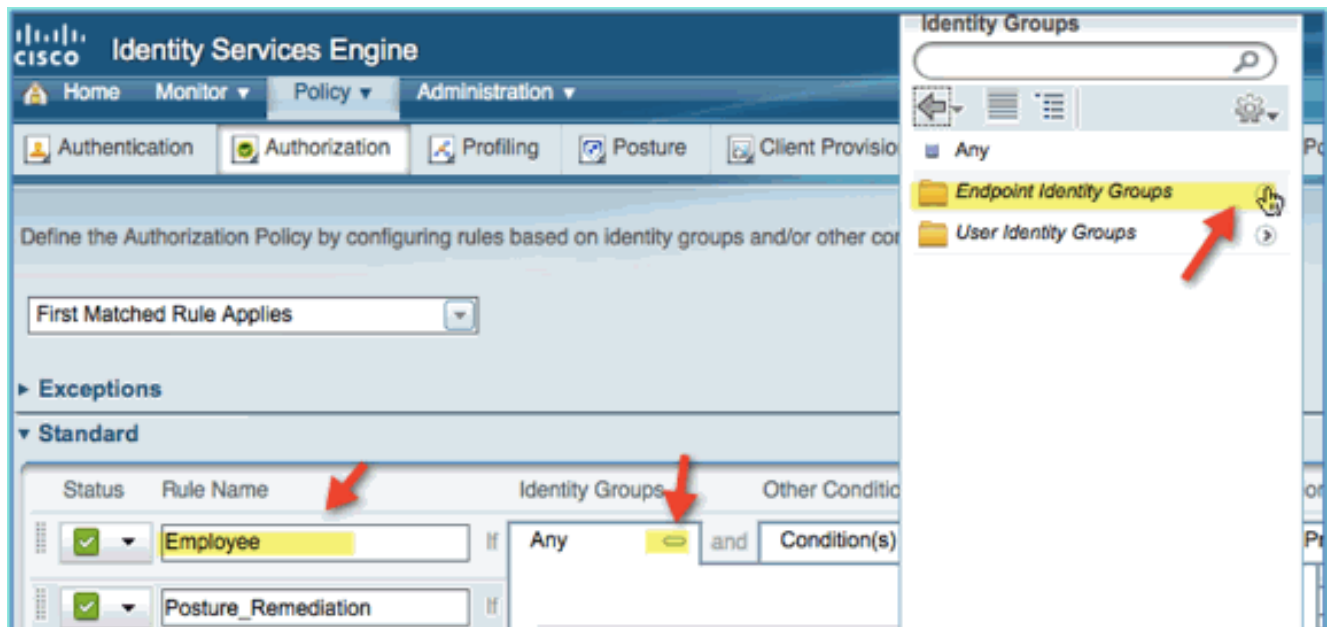
成功測試安全狀態授權後，繼續構建策略以支援員工和承包商的差異化訪問，包括已知裝置和特定於使用者角色的不同VLAN分配 (在此方案中，為員工和承包商)。

請完成以下步驟：

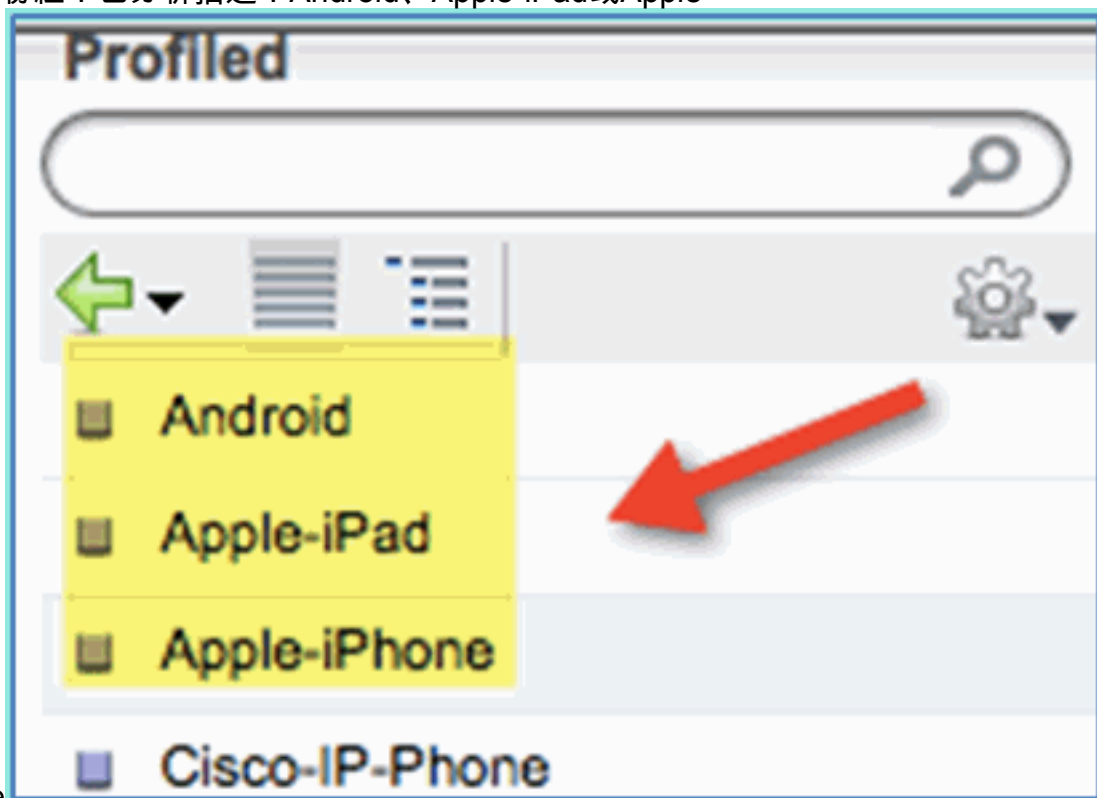
1. 導航到ISE > Policy > Authorization.
2. 在Posture Remediation policy/line上方新增/插入新規則。



3. 為此策略輸入以下值：規則名稱：員工身份組 (擴展)：終端身份組

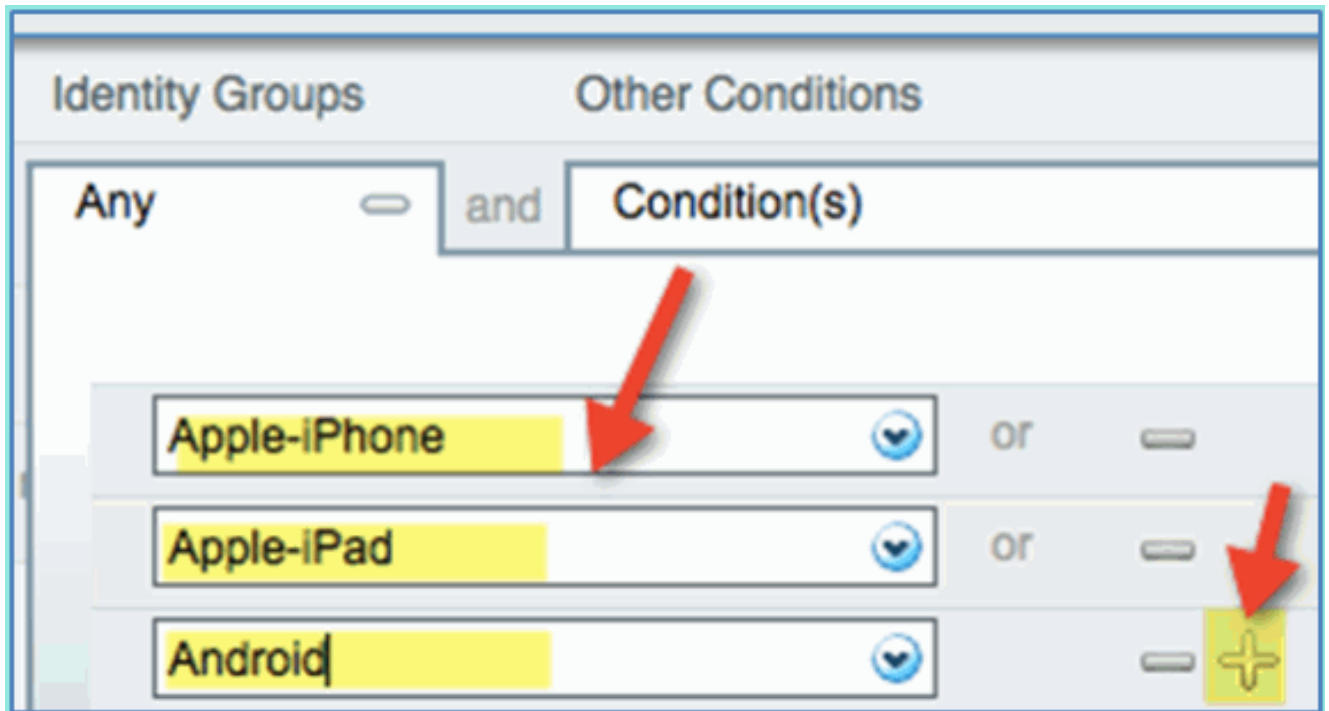


終端身份組：已分析描述：Android、Apple-iPad或Apple-

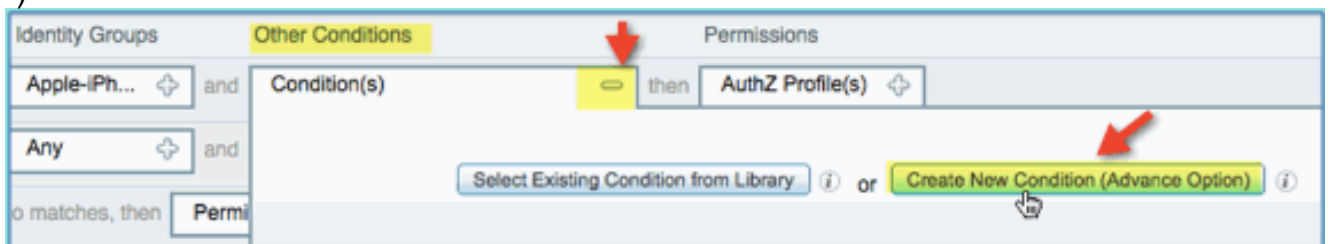


iPhone

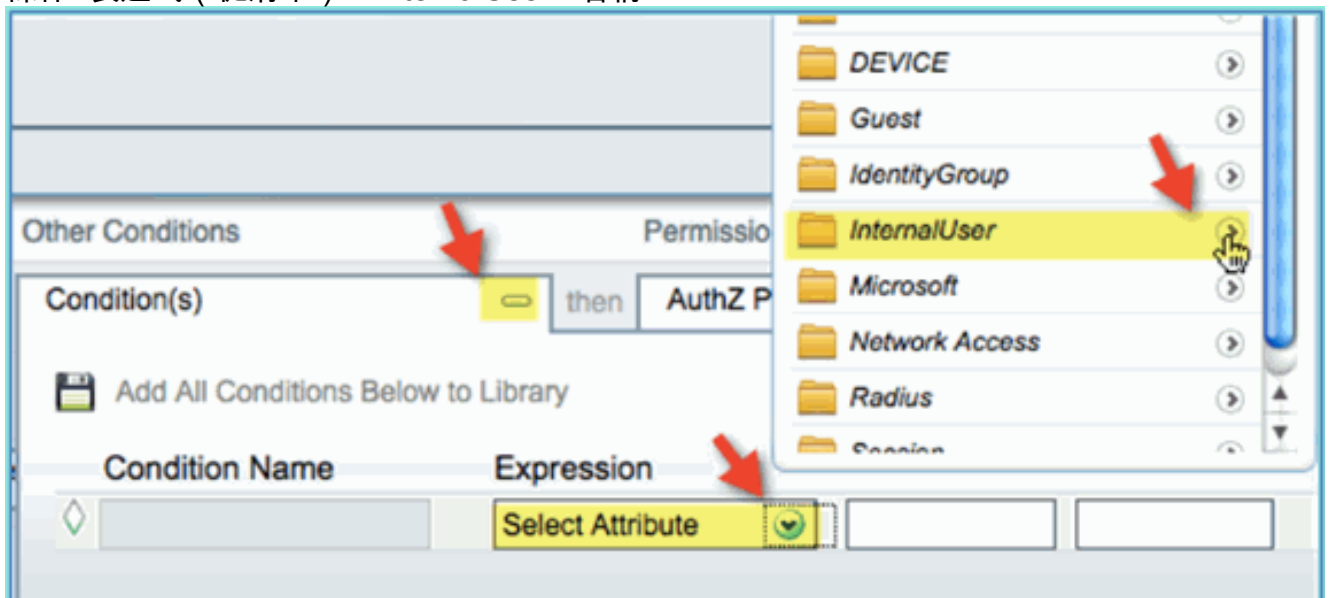
4. 若要指定其他裝置型別，請按一下+並新增更多裝置（如果需要）：終端身份組：已分析描述：Android、Apple-iPad或Apple-iPhone



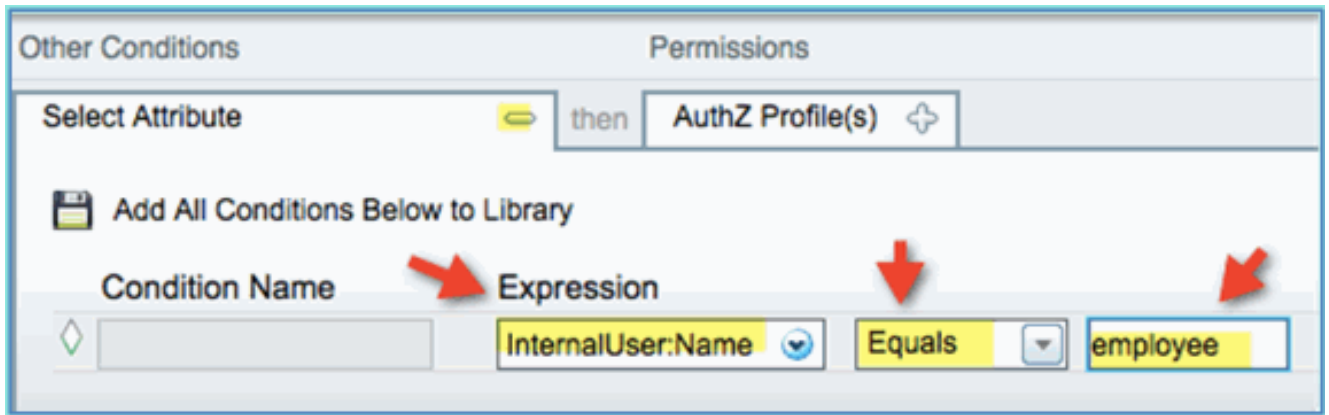
5. 為此策略指定以下「許可權」值：其他條件（展開）：建立新條件（高級選項）



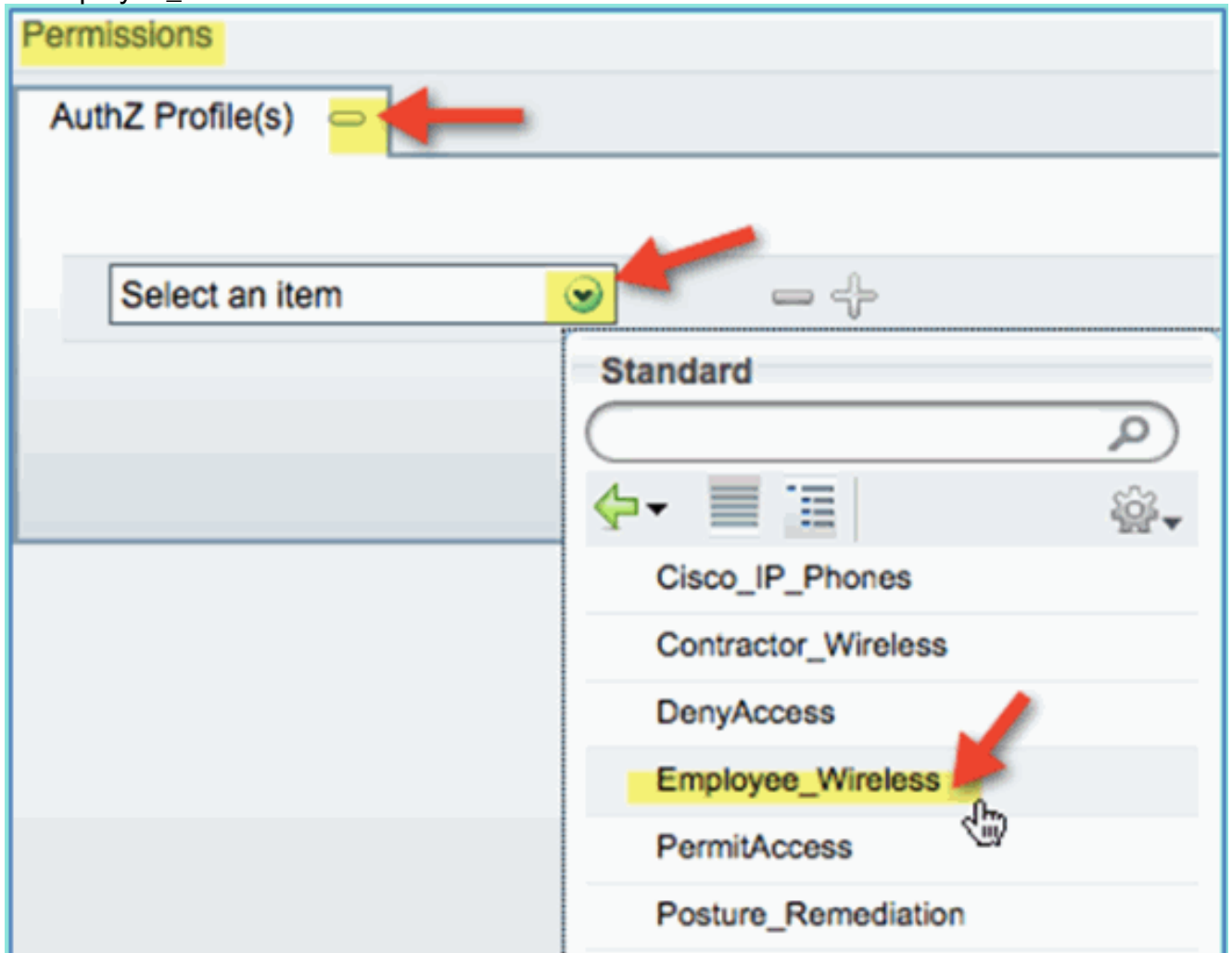
條件>表達式（從清單）：InternalUser >名稱



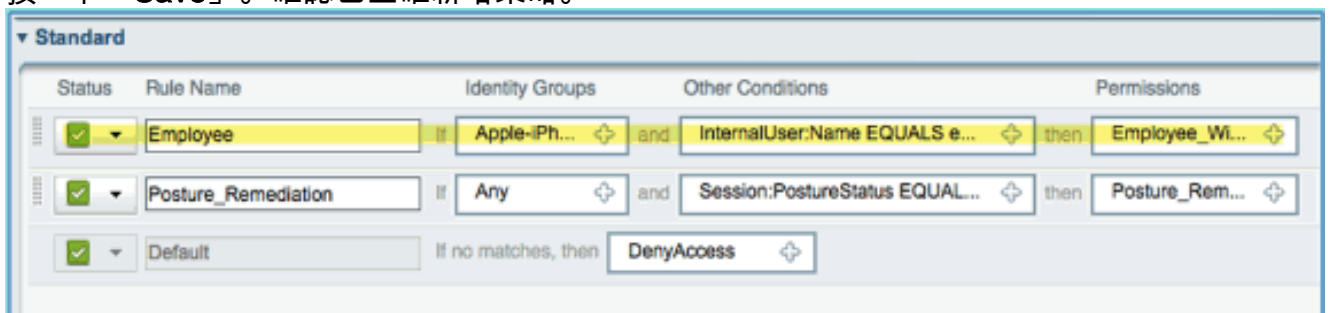
InternalUser > Name：員工



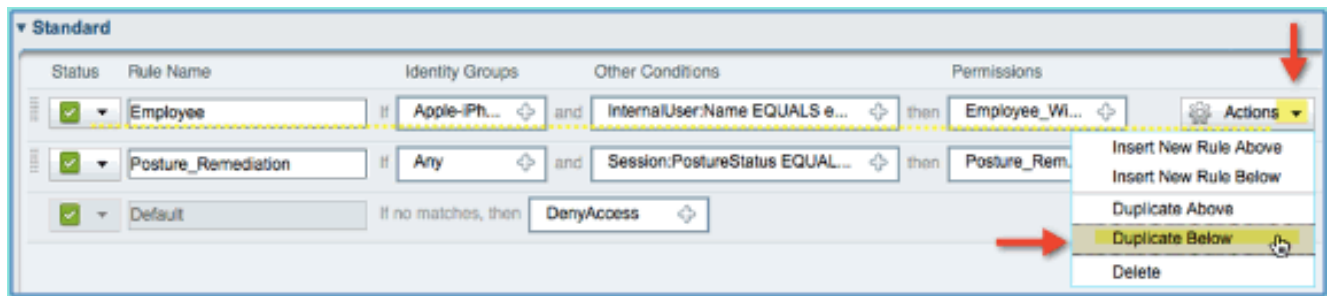
6. 為符合安全狀態會話新增條件：許可權>配置檔案>標準
：Employee_Wireless



7. 按一下「Save」。確認已正確新增策略。

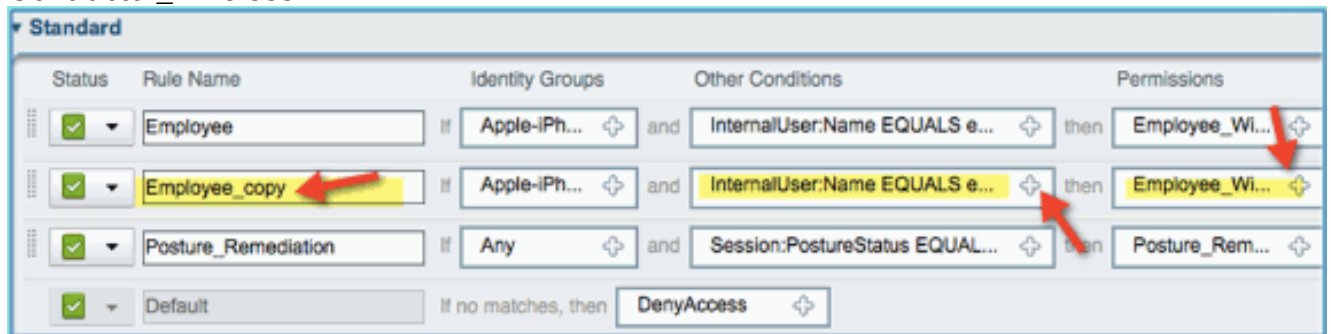


8. 繼續新增承包商策略。在本文檔中，複製了先前的策略以加快處理速度（或者可以手動配置以採用良好的做法）。在Employee policy > Actions中，按一下Duplicate Below。

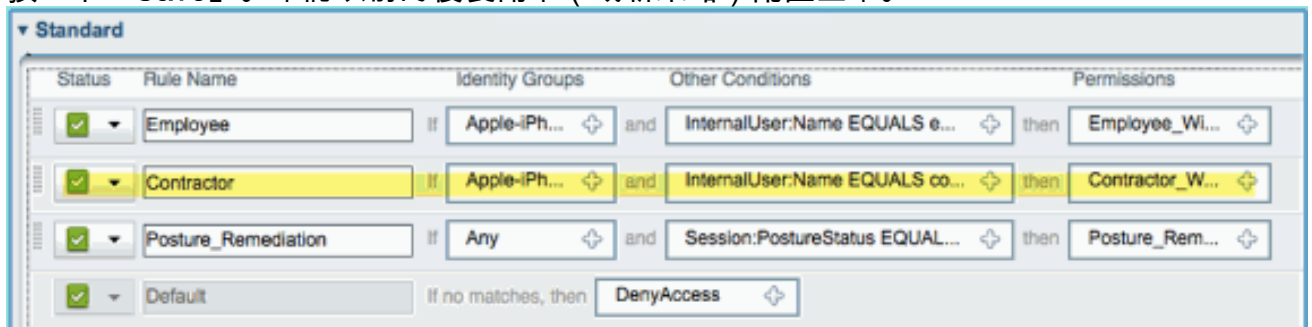


9. 編輯此策略的以下欄位 (複製副本) : 規則名稱 : 承包商其它條件>內部使用者>名稱 : 承包商許可權 :

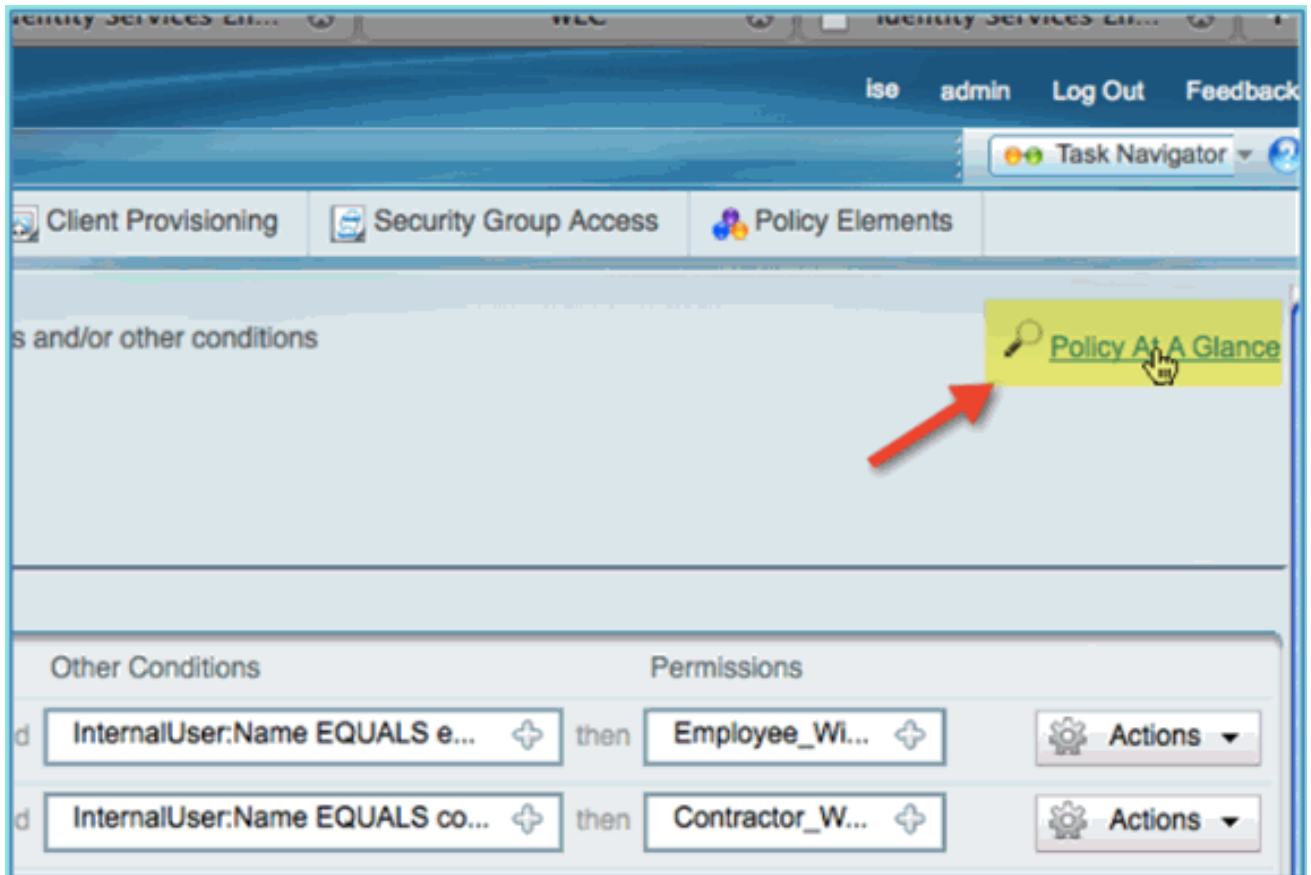
Contractor_Wireless



10. 按一下「Save」。確認以前的複製副本 (或新策略) 配置正確。



11. 要預覽策略，請按一下Policy-at-a-Glance。



「策略概覽」檢視提供彙總的策略摘要和易於檢視的策略。

Authorization Policy At A Glance				
First Matched Rule Applies				
Exceptions				
Status	Rule Name	Identity Groups	Other Conditions	Permissions
No data available				
Standard				
Status	Rule Name	Identity Groups	Other Conditions	Permissions
Enabled	Employee	Android OR Apple-iPad OR Apple-iphone	InternalUser.Name EQUALS employee	Employee_Wireless
Enabled	Contractor	Android OR Apple-iPad OR Apple-iphone	InternalUser.Name EQUALS contractor	Contractor_Wireless
Enabled	Posture_Remediation	Any	Session.PostureStatus EQUALS Unknown	Posture_Remediation
Enabled	Default	Any		DenyAccess

測試CoA以區分訪問

利用為區分訪問而準備的授權配置檔案和策略，現在正是進行測試的時候。如果使用單個安全WLAN，則將為員工分配員工VLAN，並為承包商分配VLAN。下一個示例中使用的是Apple iPhone/iPad。

請完成以下步驟：

1. 使用流動裝置連線到安全的WLAN(POD1x)並使用以下憑證：使用者名稱：employee密碼：XXXXX



2. 按一下「Join」。確認為員工分配了VLAN 11 (員工VLAN)。



3. 按一下Forget this Network。按一下Forget進行確認。



4. 前往WLC並移除現有使用者端連線（如果前面的步驟使用相同的連線）。導覽至Monitor > Clients > MAC address，然後按一下Remove。

Monitor

Clients

Summary

Current Filter

▶ Access Points

▶ Cisco CleanAir

▶ Statistics

▶ CDP

▶ Rogues

Clients

Multicast

Client MAC Addr

[44:2a:60:f7:3a:4a](#)

[5c:59:48:40:82:8d](#)

Status	Auth	Port	WGB
--------	------	------	-----

Associated	Yes	1	No
------------	-----	---	----

Associated	No	1	
------------	----	---	--

LinkTest

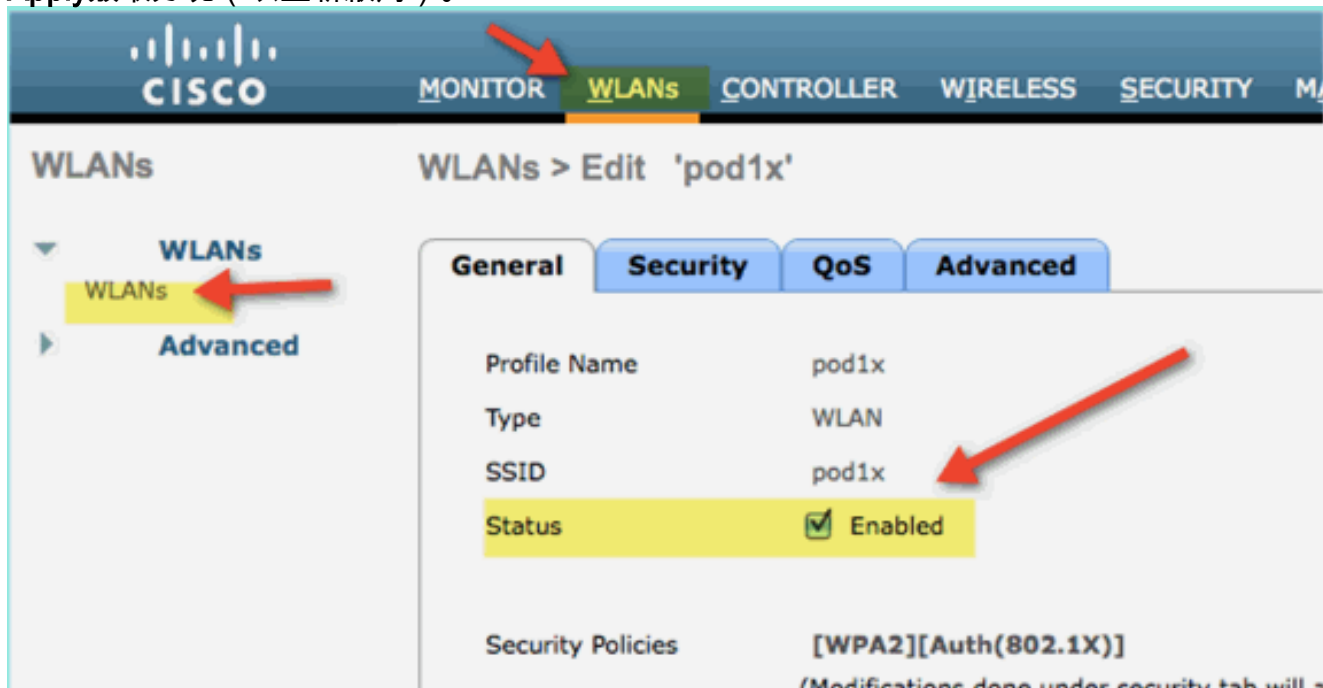
Disable

Remove

802.11aTSM

802.11b/gTSM

5. 清除先前使用者端作業階段的另一種可靠方法是停用/啟用WLAN。前往WLC > WLANs > WLAN，然後按一下WLAN以進行編輯。取消選中Enabled > Apply (禁用)。選中Enabled > Apply覈取方塊 (以重新啟用)。



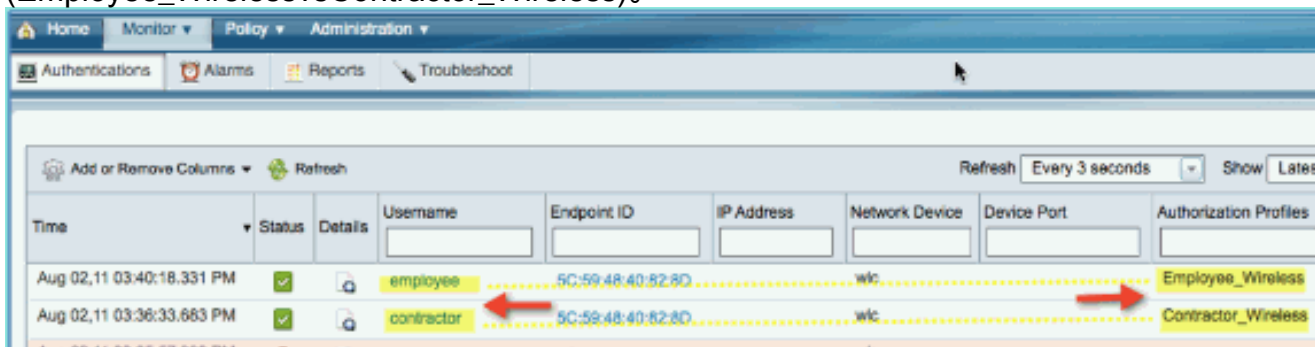
6. 返回流動裝置。使用以下憑證重新連線到同一個WLAN:使用者名稱：contractor密碼：XXXX



7. 按一下「Join」。確認為承包商使用者分配了VLAN 12 (承包商/訪客VLAN)。



8. 您可以在ISE > Monitor > Authorizations中檢視ISE即時日誌檢視。您應該會看到各個使用者 (員工、承包商) 在不同的VLAN中獲得不同的授權配置檔案 (Employee_WirelessvsContractor_Wireless)。



[WLC訪客WLAN](#)

完成以下步驟，新增訪客WLAN以允許訪客訪問ISE發起人訪客門戶：

1. 在WLC中，導覽至WLANs > WLANs > Add New。
2. 為新的訪客WLAN輸入以下內容：配置檔名稱
： pod1guestSSID:pod1guest



3. 按一下「Apply」。
4. 在訪客WLAN > General頁籤下輸入以下命令：狀態：已禁用介面/介面組：訪客

WLANs > Edit 'pod1guest'

General

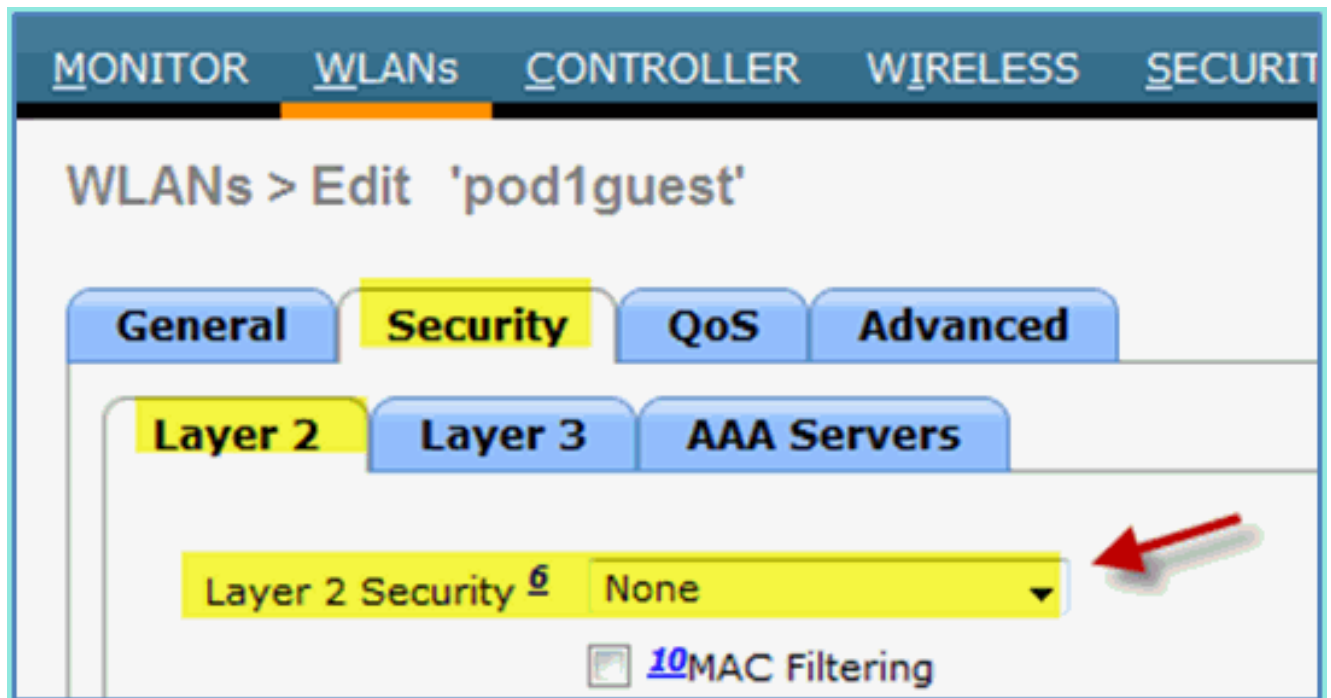
Security

QoS

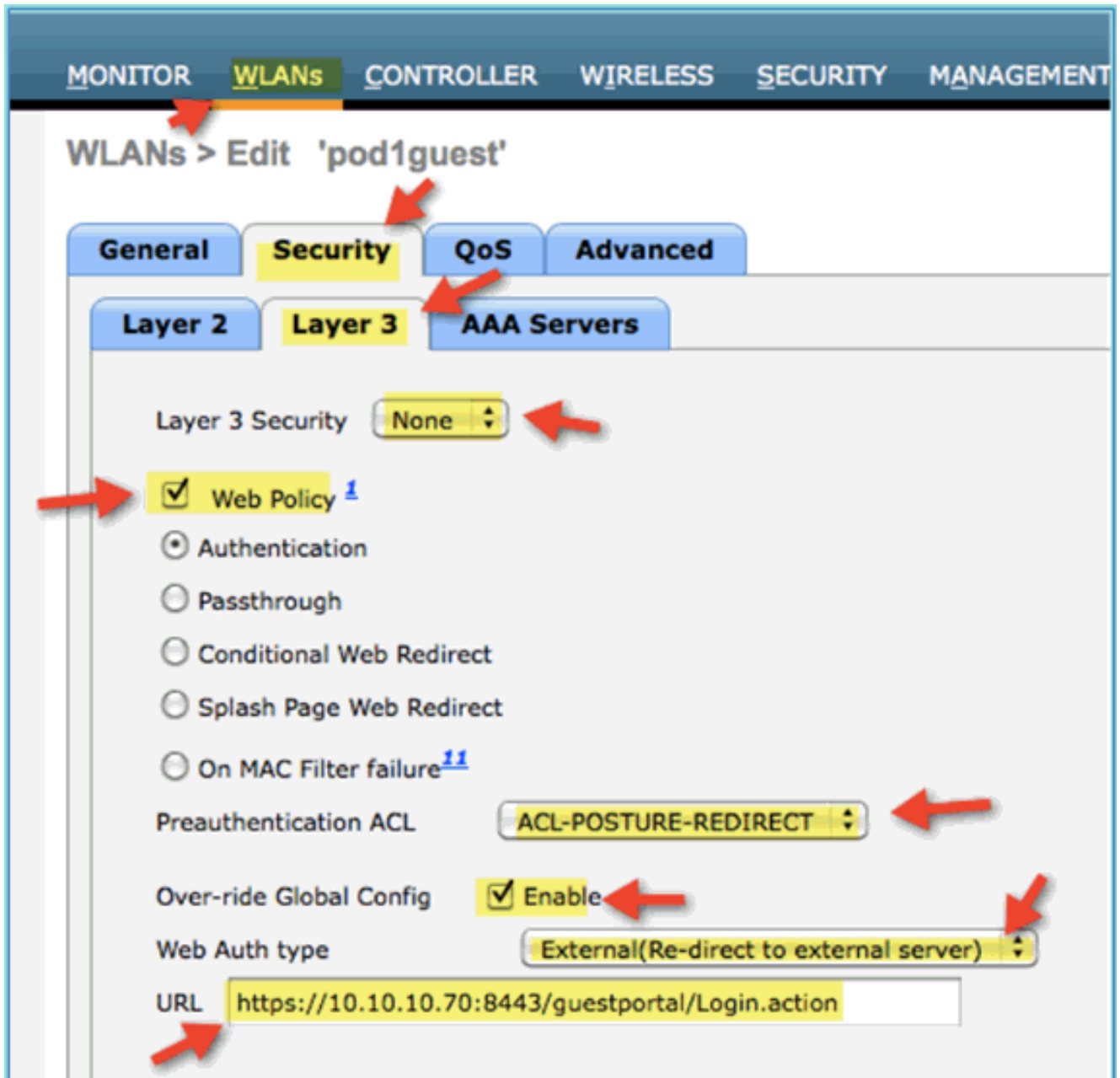
Advanced

Profile Name	pod1guest
Type	WLAN
SSID	pod1guest
Status	<input type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security)
Radio Policy	All
Interface/Interface Group(G)	guest
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

5. 導覽至guest WLAN > Security > Layer2，然後輸入以下內容：第2層安全：無



6. 導覽至guest WLAN > Security > Layer3索引標籤，然後輸入以下內容：第3層安全：無Web策略：已啟用Web策略子值：身份驗證預身份驗證ACL:ACL-POSTURE-REDIRECTWeb身份驗證型別：外部 (重定向到外部伺服器)
) URL:https://10.10.10.70:8443/guestportal/Login.action



7. 按一下「Apply」。

8. 請確保儲存WLC組態。

測試訪客WLAN和訪客門戶

現在，您可以測試訪客WLAN的組態。應將訪客重新導向至ISE訪客門戶。

請完成以下步驟：

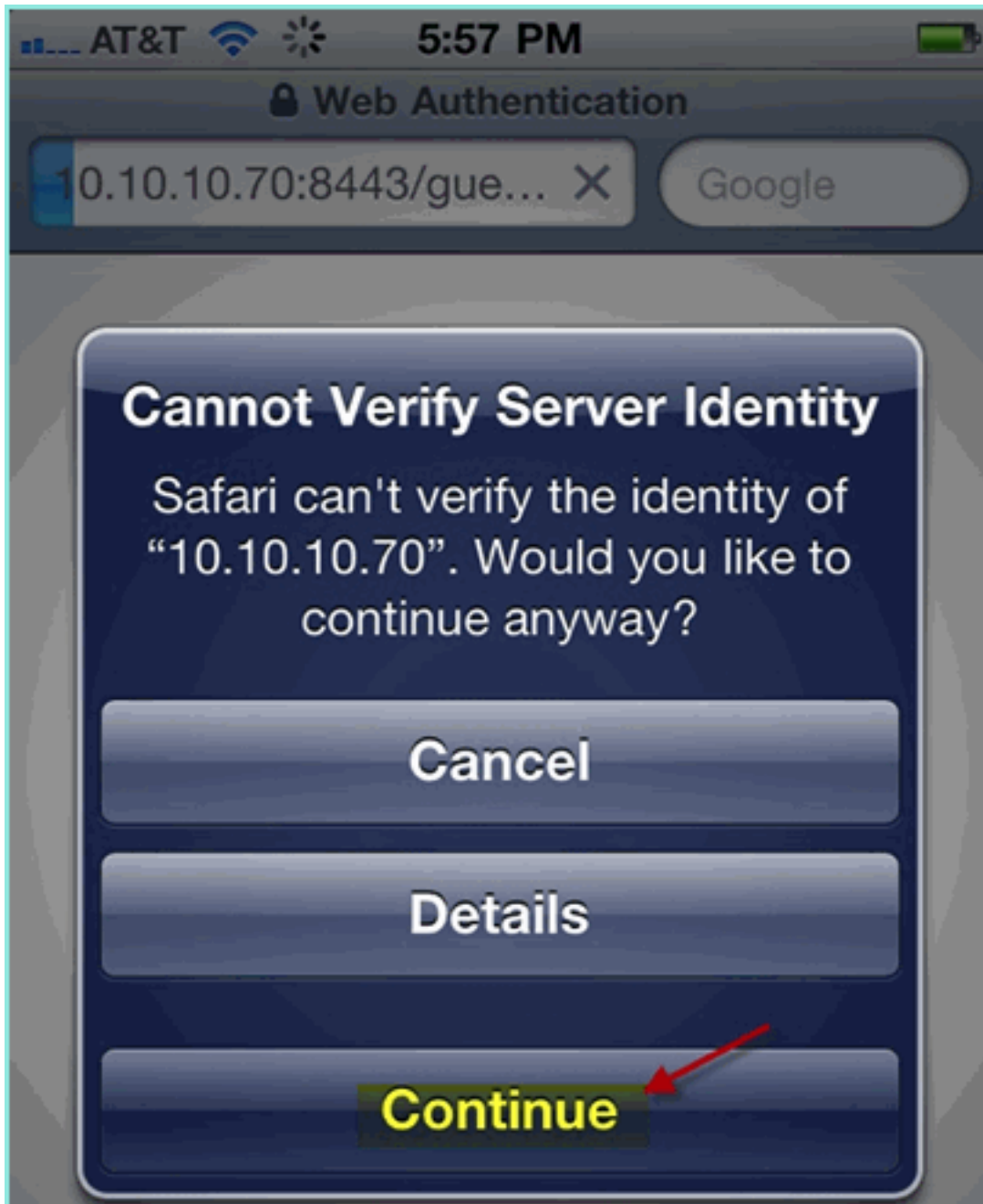
1. 從iPhone等iOS裝置導航至Wi-Fi Networks > Enable。然後選擇POD訪客網路。



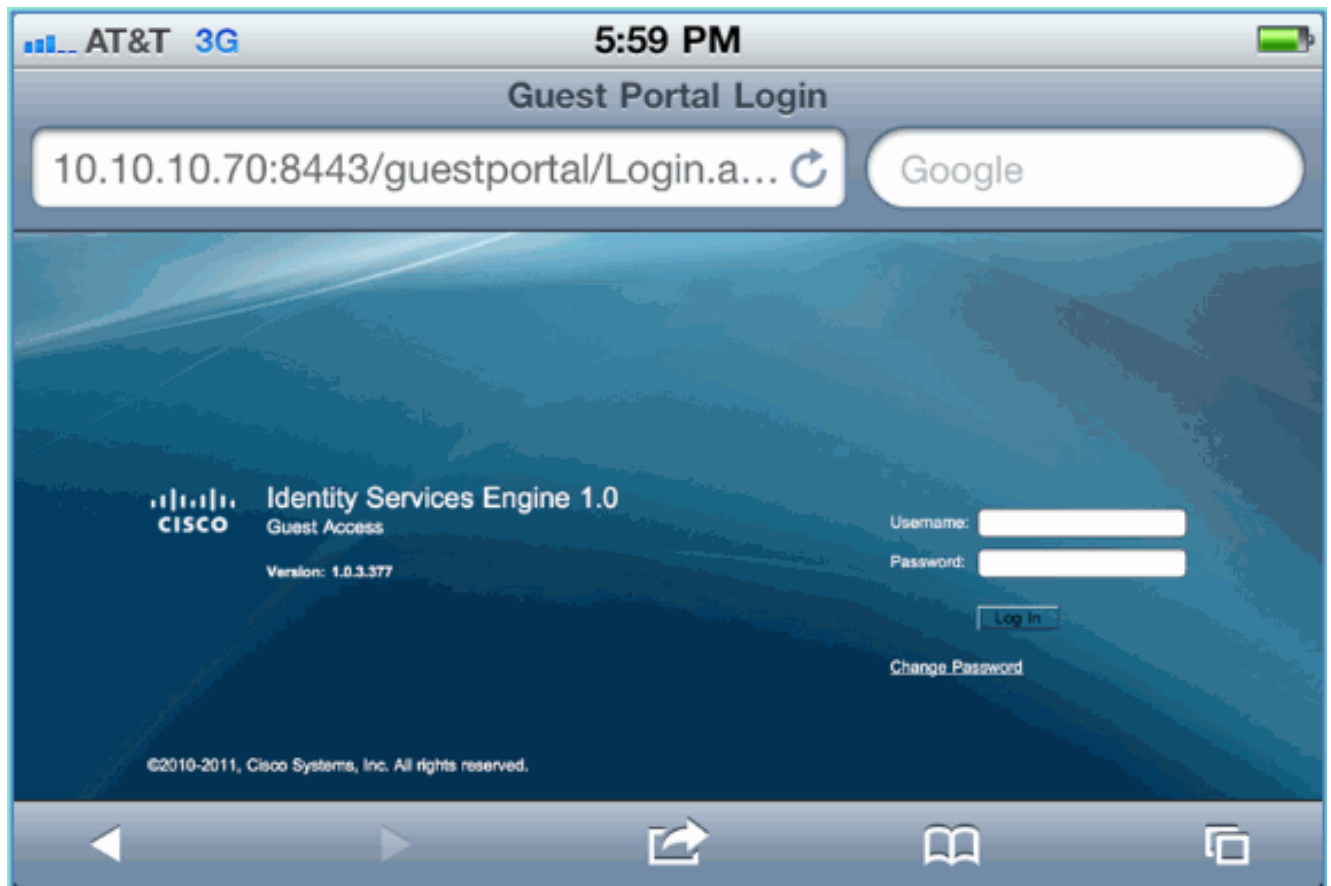
2. 您的iOS裝置應顯示來自訪客VLAN(10.10.12.0/24)的有效IP地址。



3. 開啟Safari瀏覽器並連線到：URL:<http://10.10.10.10>出現「Web Authentication redirect (Web身份驗證重定向)」。
4. 點選Continue，直到您到達ISE訪客門戶頁面。



。 下一個示例螢幕截圖顯示了訪客門戶登入上的iOS裝置。這確認WLAN和ISE訪客門戶的正確設定處於活動狀態。

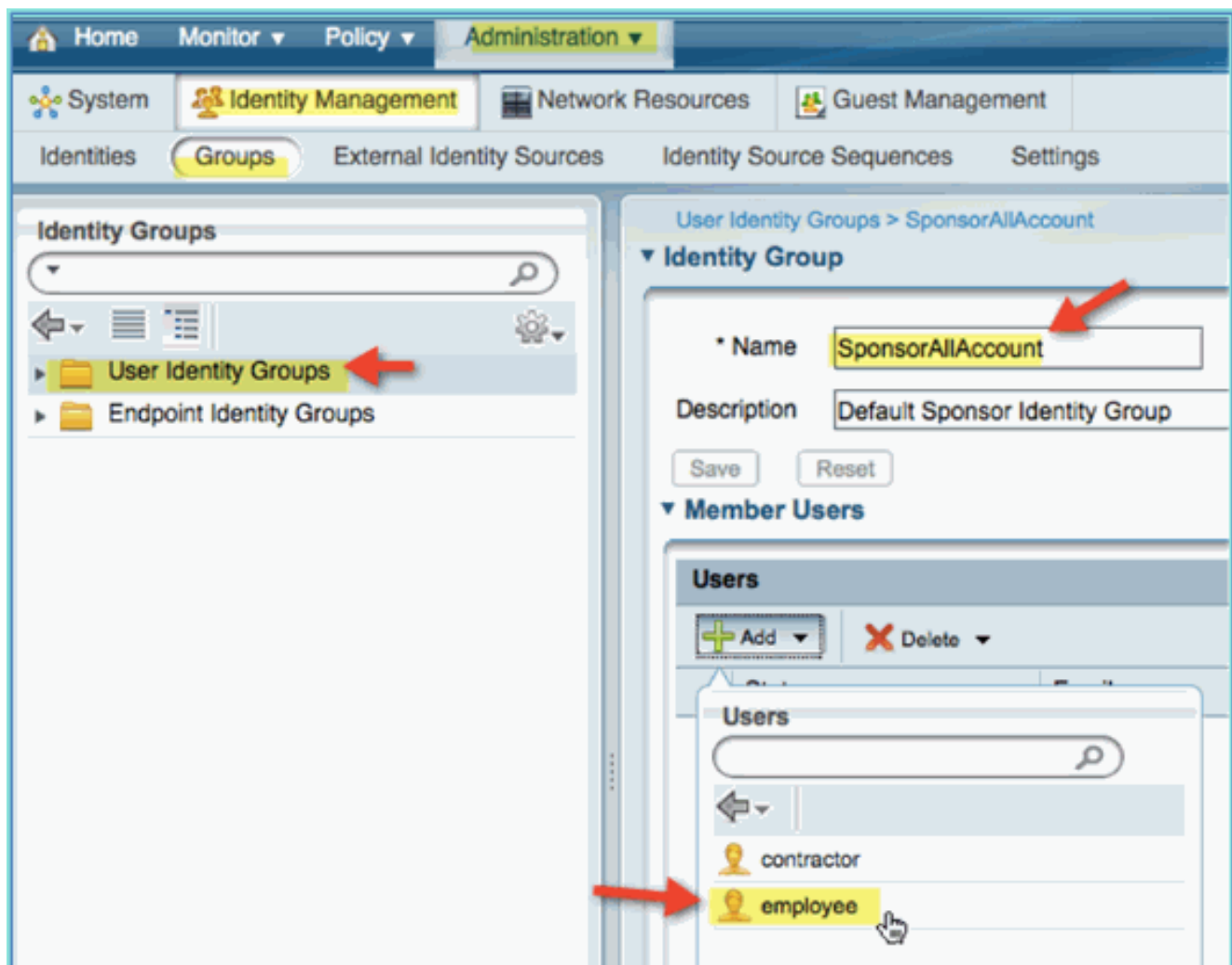


ISE無線贊助訪客接入

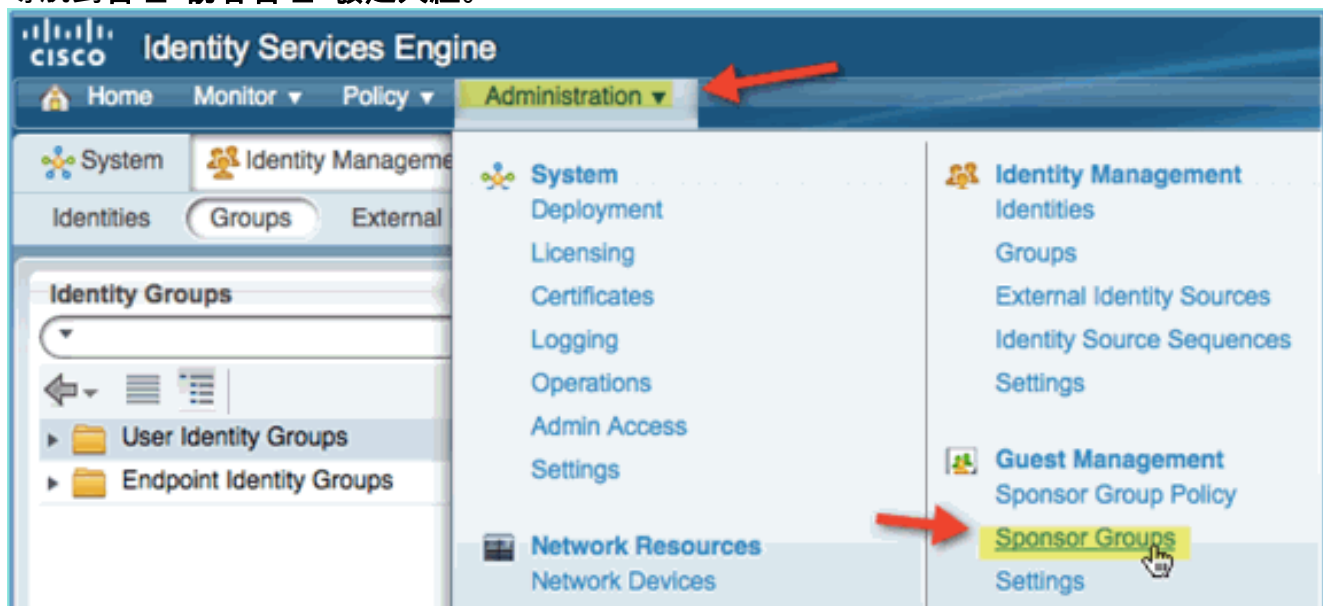
可以將ISE配置為允許贊助訪客。在這種情況下，您將配置ISE訪客策略以允許內部或AD域（如果整合）使用者發起訪客訪問。您還將配置ISE以允許發起人檢視訪客密碼（可選），這對本實驗很有幫助。

請完成以下步驟：

1. 將員工使用者新增到SponsorAllAccount組。可以使用不同的方法執行此操作：直接轉到組，或編輯使用者和分配組。在本例中，導航到**管理>身份管理>組>使用者身份組**。然後，按一下**SponsorAllAccount**並新增員工使用者。



2. 導航到管理>訪客管理>發起人組。



3. 按一下Edit，然後選擇SponsorAllAccounts。

CISCO Identity Services Engine

Home Monitor Policy Administration

System Identity Management Network Resources Guest Management

Sponsor Group Policy Sponsor Groups Settings

Guest Sponsor Groups

Edit Add Delete Filter

<input type="checkbox"/>	Sponsor Group Name	Description
<input checked="" type="checkbox"/>	SponsorAllAccounts	Default SponsorGroup
<input type="checkbox"/>	SponsorGroupGrpAccounts	Default SponsorGroup

4. 選擇Authorization Levels並設定以下內容：檢視訪客密碼：是

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is 'Sponsor Group List > SponsorAllAccounts'. The 'Authorization Levels' tab is selected. The configuration table is as follows:

Allow Login	Yes
Create Accounts	Yes
Create Bulk Accounts	Yes
Create Random Accounts	Yes
Import CSV	Yes
Send Email	Yes
Send SMS	No
View Guest Password	Yes
Allow Printing Guest Details	Yes
View/Edit Accounts	All Accounts
Suspend/Reinstate Accounts	All Accounts
* Account Start Time	1 Days (Valid Range 1 to 999999999)
* Maximum Duration of Account	5 Days (Valid Range 1 to 999999999)

Buttons for 'Save' and 'Reset' are visible at the bottom.

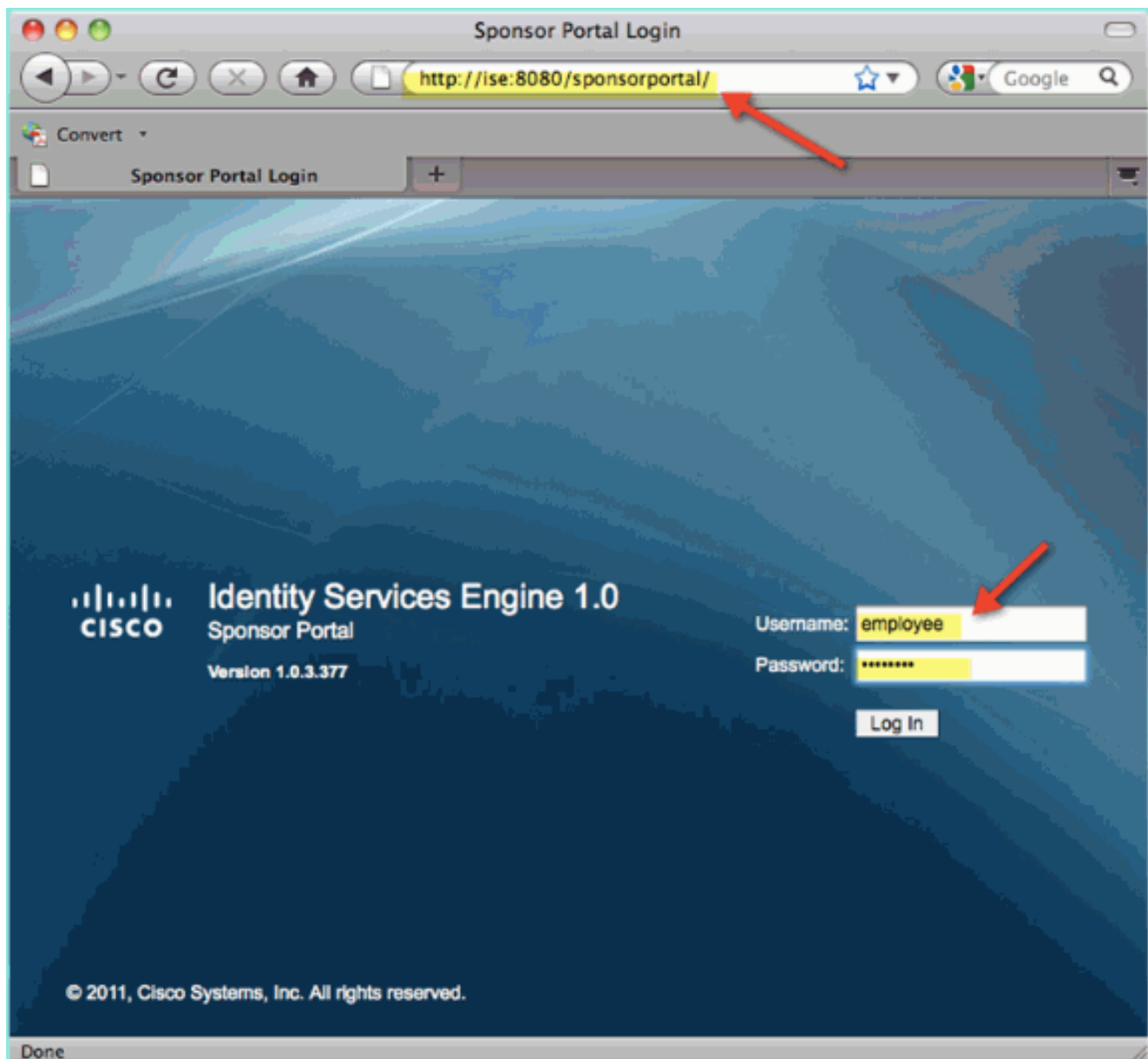
5. 按一下「Save」以完成此任務。

贊助訪客

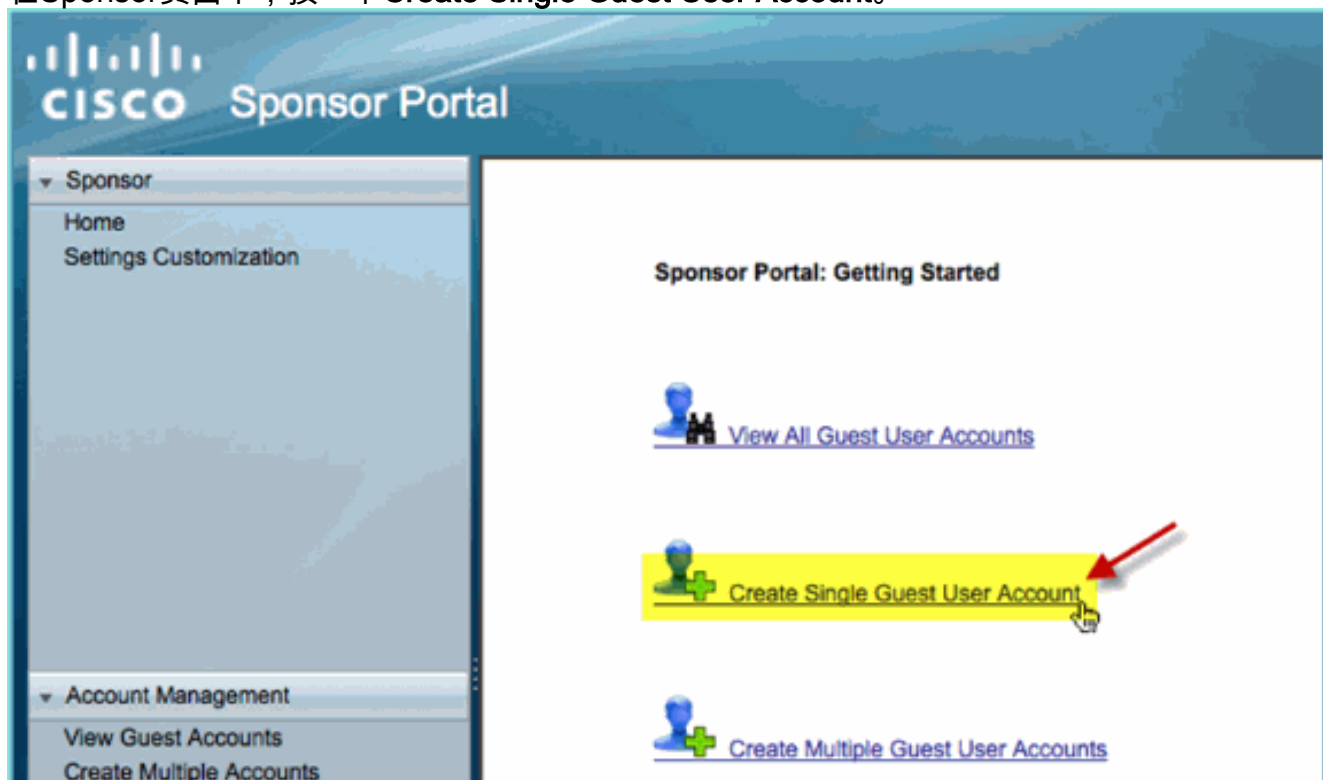
以前，您已配置相應的訪客策略和組，以允許AD域使用者發起臨時訪客。接下來，您將訪問發起人門戶並建立臨時訪客訪問許可權。

請完成以下步驟：

1. 在瀏覽器中，導航到以下URL之一：<http://<ise ip>:8080/sponsorportal/> 或 <https://<ise ip>:8443/sponsorportal/>。然後，使用以下內容登入：使用者名稱：aduser(Active Directory)、employee (內部使用者) 密碼：XXXX



2. 在Sponsor頁面中，按一下Create Single Guest User Account。



- 對於臨時訪客，新增以下內容：名字：必填（例如，Sam） 姓氏：必填（例如，Jones） 組角色：訪客時間配置檔案：DefaultOneHour 時區：任意/預設

Sponsor Portal

Account Management > View All Guest Accounts > Create Guest Account

Create Guest Account

First Name:

Last Name:

Email Address:

Phone Number:

Company:

Optional Data 1:

Optional Data 2:

Optional Data 3:

Optional Data 4:

Optional Data 5:

Group Role:

Time Profile:

Timezone:

⚙ = Required fields

- 按一下「Submit」。
- 系統會根據您之前的輸入建立訪客帳戶。請注意，密碼可見（從上一個練習中），與雜湊密碼相***。
- 保持此視窗處於開啟狀態，顯示訪客的使用者名稱和密碼。您將使用它們測試訪客門戶登入（下一步）。



Successfully Created Guest Account **siam0002**

Username: **siam0002** ←
Password: **5_5g6d7Kx** ←
First Name: Sam ←
Last Name: iAm
Email Address:
Phone Number:
Company:
Status: AWAITING INITIAL LOGIN
Suspended: false
Optional Data 1:
Optional Data 2:
Optional Data 3:
Optional Data 4:
Optional Data 5:
Group Role: Guest
Time Profile: DefaultOneHour

Timezone: EST
Account Start Date: 2011-07-15 13:56:04 EST
Account Expiration Date: 2011-07-15 14:56:04 EST

Email

Print

Create Another Account

View All Accounts

測試訪客門戶訪問

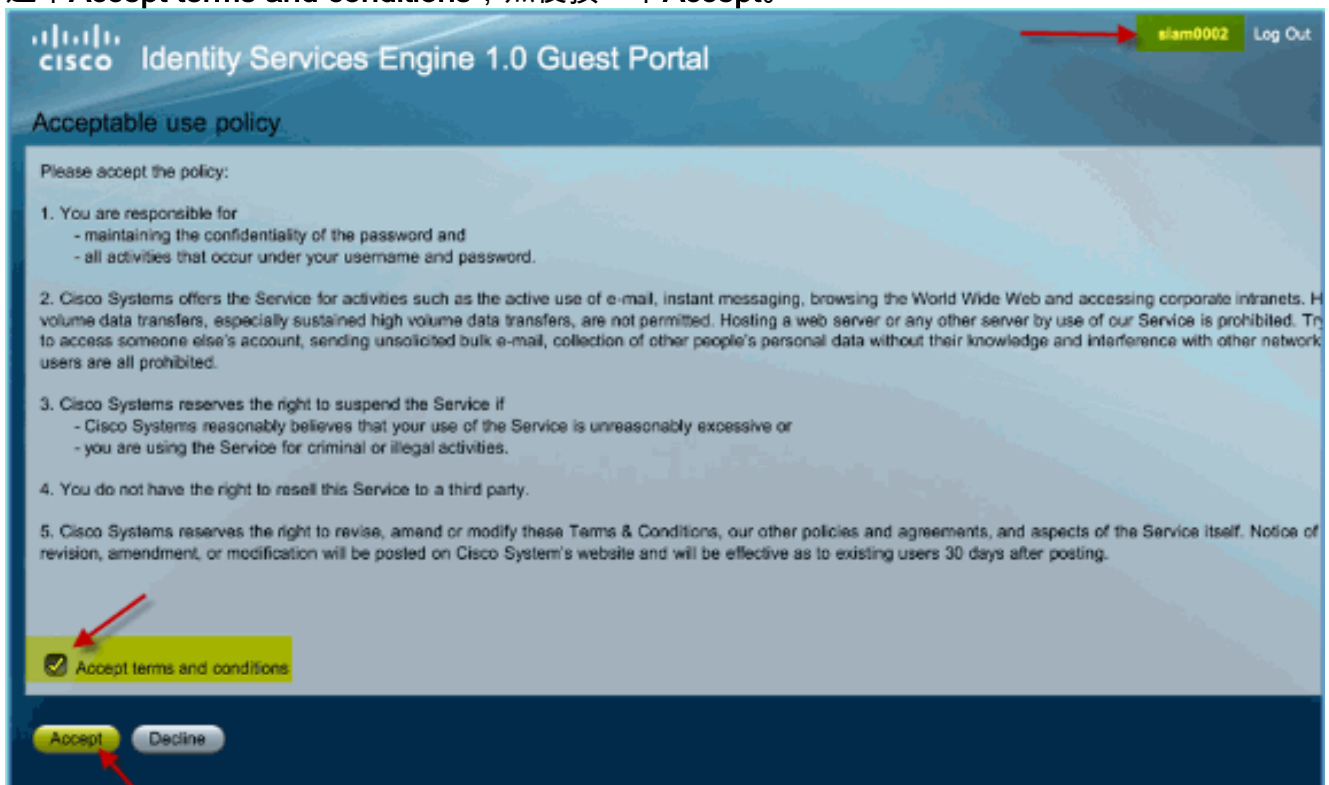
使用由AD使用者/發起人建立的新訪客帳戶，是時候測試訪客門戶和訪問許可權了。

請完成以下步驟：

1. 在首選裝置（本例中為Apple iOS/iPad）上，連線到Pod訪客SSID並檢查IP地址/連線。
2. 使用瀏覽器並嘗試導航至http://www。系統會將您重新導向至訪客入口登入頁面。



3. 使用在上一個練習中建立的訪客帳戶登入。如果成功，將顯示「可接受的使用策略」(Acceptable use policy)頁面。
4. 選中Accept terms and conditions，然後按一下Accept。



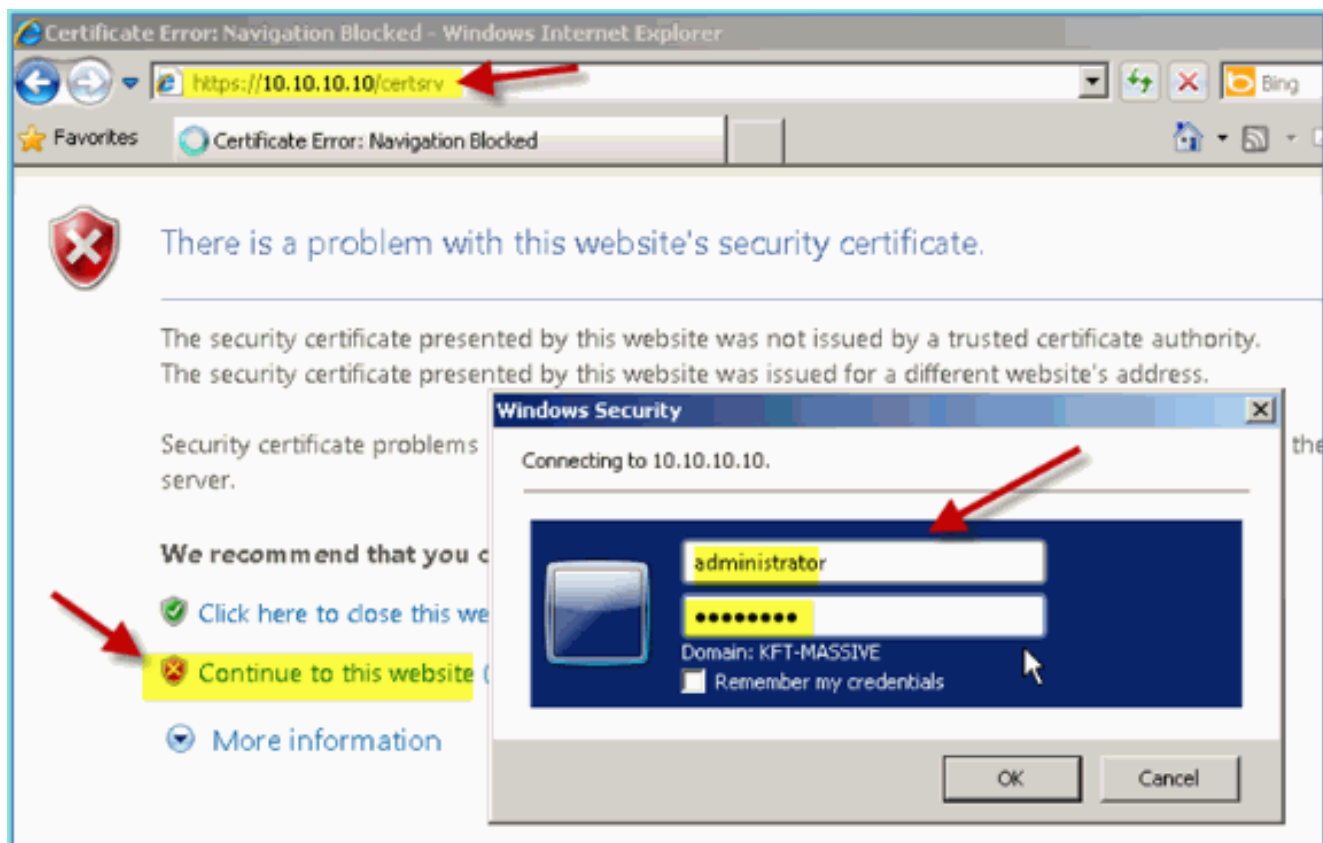
原始URL已完成，且允許終端作為訪客訪問。

憑證組態

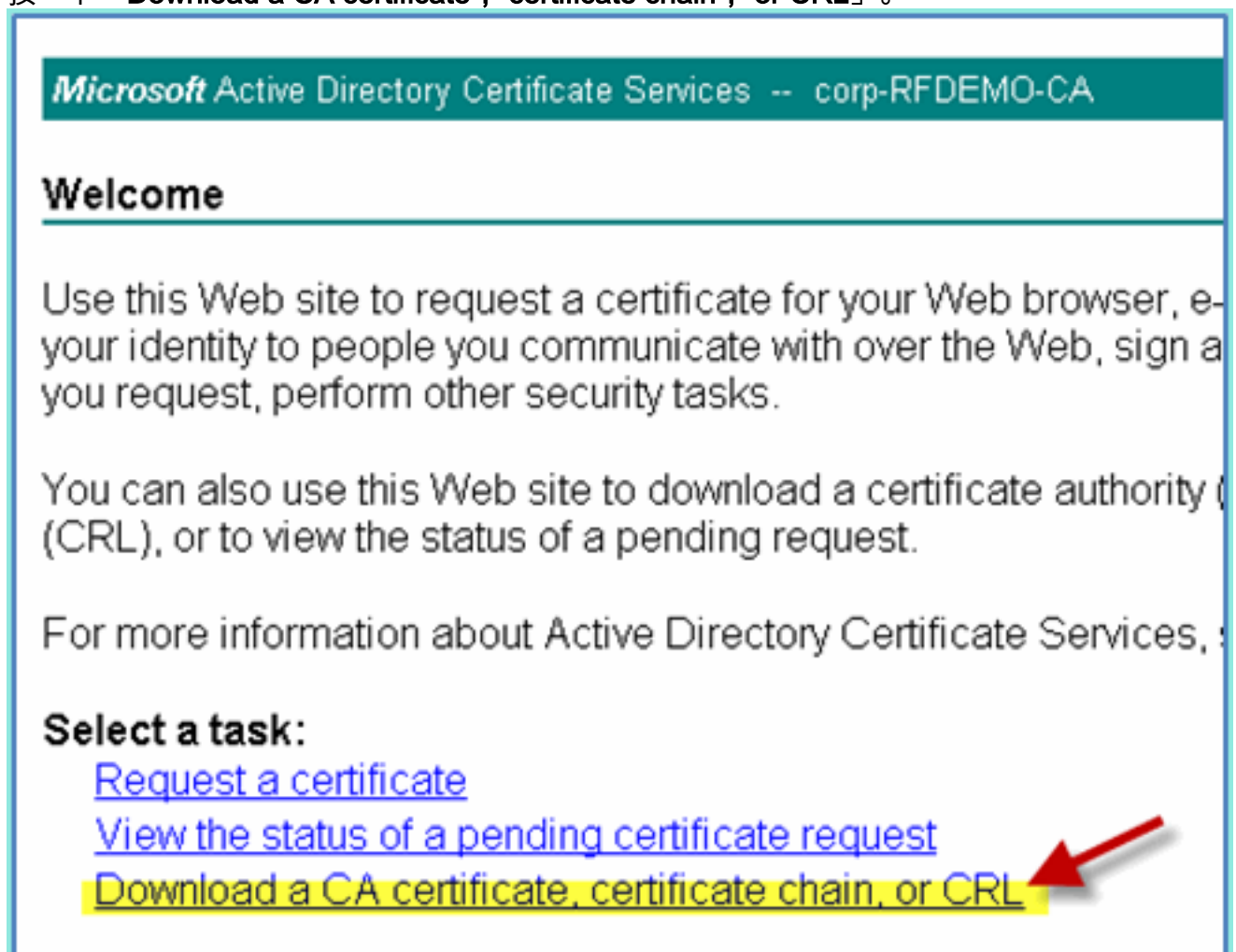
為了保護與ISE的通訊，請確定該通訊是身份驗證相關還是用於ISE管理。例如，對於使用ISE Web UI的配置，需要配置X.509證書和證書信任鏈以啟用非對稱加密。

請完成以下步驟：

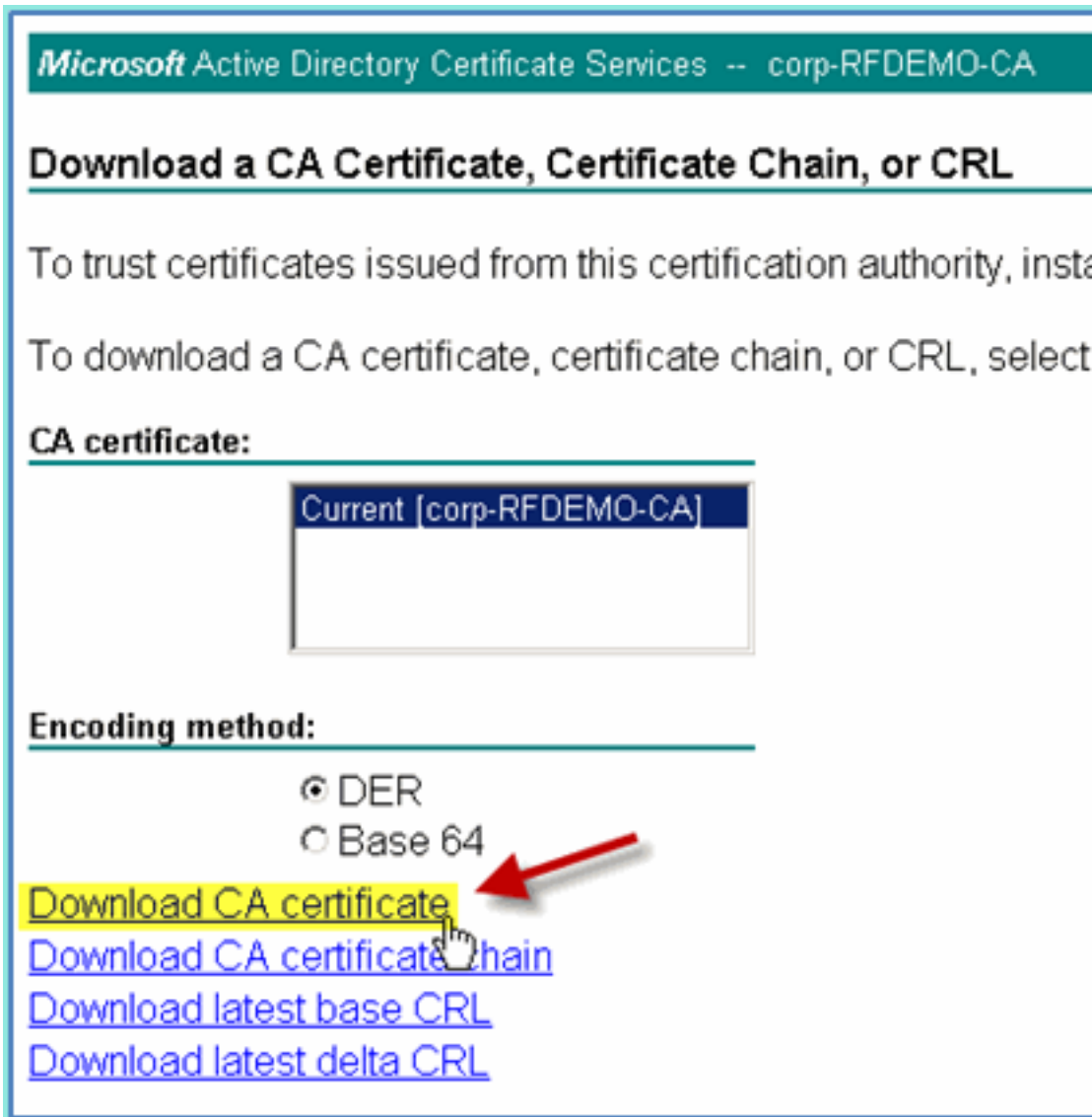
1. 在有線連線的PC上，開啟一個瀏覽器視窗訪問https://AD/certsrv。注意：使用安全HTTP。注意：使用Mozilla Firefox或MS Internet Explorer訪問ISE。
2. 以管理員/Cisco123身份登入。



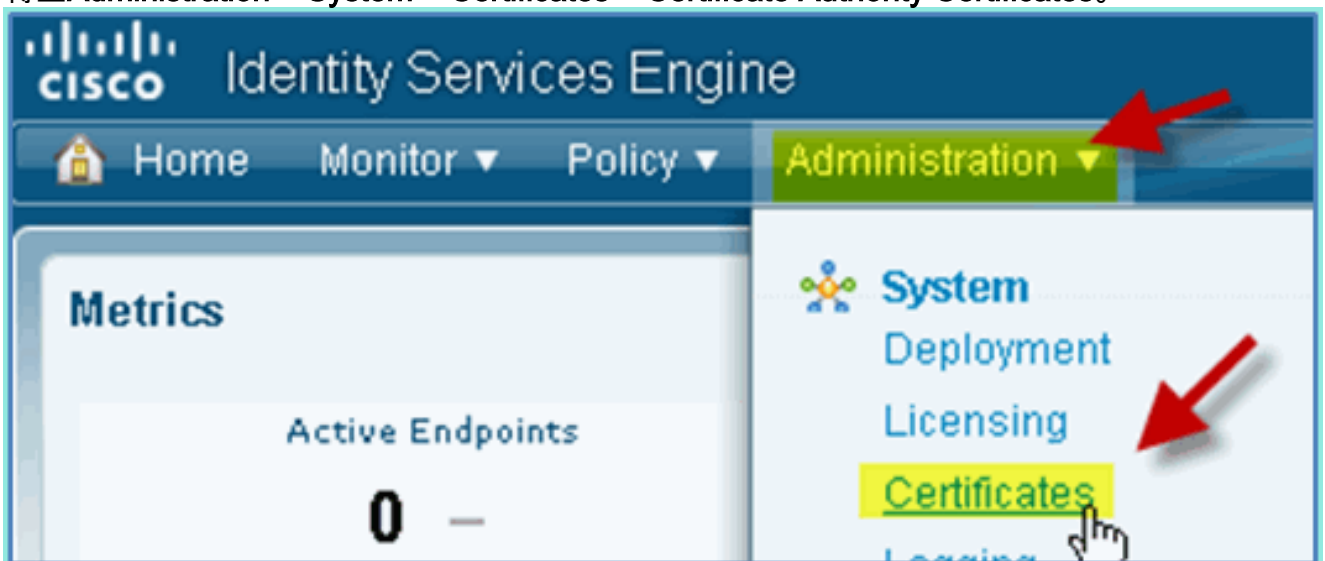
3. 按一下「Download a CA certificate , certificate chain , or CRL」。



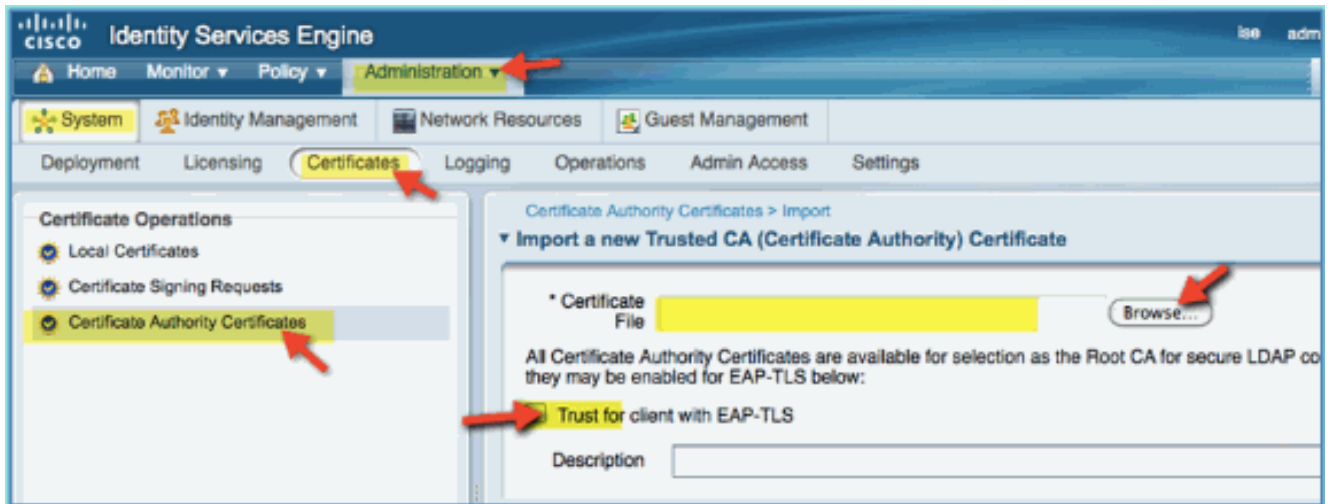
4. 按一下「Download CA certificate」，然後儲存該憑證（請注意儲存位置）。



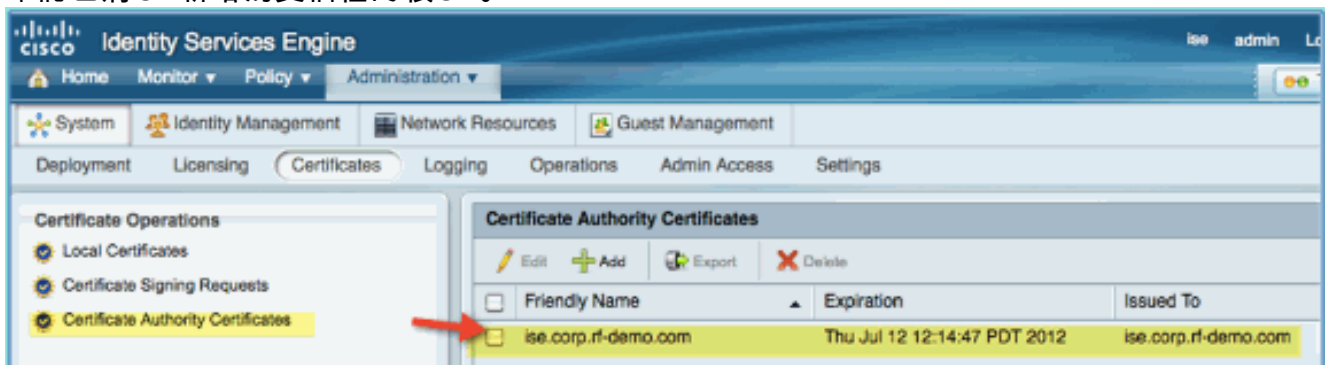
5. 開啟瀏覽器視窗訪問https://<Pod-ISE>。
6. 轉至Administration > System > Certificates > Certificate Authority Certificates。



7. 選擇Certificate Authority Certificates操作，並瀏覽到以前下載的CA證書。
8. 選擇Trust for client with EAP-TLS，然後提交。

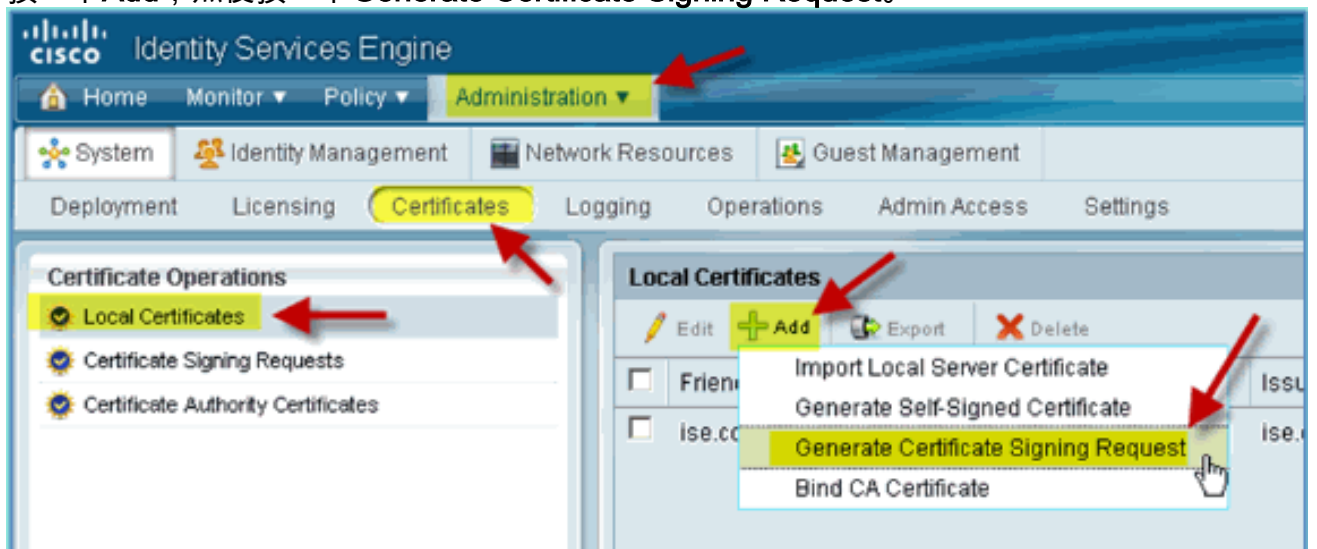


9. 確認已將CA新增為受信任的根CA。



10. 從瀏覽器中，轉至Administration > System > Certificates > Certificate Authority Certificates。

11. 按一下Add，然後按一下Generate Certificate Signing Request。



12. 提交以下值：證書主題：CN=ise.corp.rf-demo.com金鑰長度：2048

Local Certificates > Generate Certificate Signing Request

▼ **Generate Certificate Signing Request**

Certificate

* Certificate Subject

* Key Length

Digest to Sign With SHA1

13. ISE提示在CSR頁面中提供CSR。按一下「OK」(確定)。



14. 從ISE CSR頁面選擇CSR，然後按一下Export。

15. 將檔案儲存到任何位置(例如下載等)

16. 檔案將另存為*.pem。

Identity Services Engine

Home Monitor Policy Administration

System Identity Management Network Resources Guest Management

Deployment Licensing Certificates Logging Operations Admin Access Settings

Certificate Operations

- Local Certificates
- Certificate Signing Requests
- Certificate Authority Certificates

Certificate Signing Requests

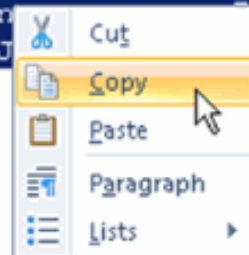
Export Delete

<input checked="" type="checkbox"/>	Friendly Name	Certificate Subject	Key Length
<input checked="" type="checkbox"/>	ise.corp.rf-demo.com	CN=ise.corp.rf-demo.com	2048

17. 找到CSR檔案並使用記事本/寫字板/TextEdit進行編輯。

18. 複製內容(「全選」>「複製」)。

```
-----BEGIN CERTIFICATE REQUEST-----
MIICyTCCAAbECAQAwHzEdMBSGA1UEAxMUaXNlLmNvcnAucmYtZGVtby5jb20wggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDXaeWDSqfI64K59dyRLm8JAXan
WYTaAJ6S/Ke206ws/K3BFAFJQhndQQ0hYVmGcJLVN03pXtRln/q/HBuglLIItIvbe
86FADPq3kUNb48UHcdR9b5rUs7B8T5E6banZia6eHSXjIzX4f0U7mVOrzALeAPDK
HXU+/y/gleyNL6P8zC4bvi/SZXhZp1OvtQpi+8lh14M5ROChhbPUnB3EGVaIVRiN
wYn8Ojvejbtg//k0CItGARlG2IFbBbgUpkMVhDQqgixp3wrlm3hi9JXgffEI f4BO
sirLrhvMSuSNESnIVWYrRLz5Xt4dMct+bu08xaEYPqgoukYjxsA9gn0bRDMJAgMB
AAGgZTBjBqkqhkiG9w0BCQ4xVjBUMASGA1UdDwQEAwICrDAdBgNVHQ4EFgQU2jmj
715rSw0yVb/vlWAYkK/YBwkWewYDVR0lBAwwCgYIKwYBBQUHAWewEQYJYIZIAYb4
QgEBBAQDAgZAMA0GCSqGSIb3DQEBBQUAA4IBAQBz4YPO9sN7WF2HtG+48300mw9q
gA/MMZsTioEPekcunrm+ZFtlAXajB32uwHHi1lc9Rn93TgOWPFxKEX9E89fzSWDK
J4qsQM7KEYOpQt4bia07188Lm6BBTk9mRhiTBwSF3dx0tlzfgiHc72kjWvxsgg/c
k8a7LHYgkgLRYBnpu15RjQ7wWijArH8cK1OrVT42riz7vK0g0nkWRHF52uiu3AkP
LPKQ72N2XYIXfu0jdgoaJjmsk6T9nLABVYQ6n...KDJTHchcwx6I1k/
V5QYBOjTYHXIPG8/ned9z3M0iZd2sm4XNS2bJ...W1ZuB6drHg9
-----END CERTIFICATE REQUEST-----
```



19. 開啟瀏覽器視窗訪問`https://<Pod-AD>/certsrv`。
20. 按一下「Request a certificate」。

Microsoft Active Directory Certificate Services -- corp-RFDEMO-CA

Welcome

Use this Web site to request a certificate for your Web browser to communicate with over the Web, sign and encrypt messages.

You can also use this Web site to download a certificate and a pending request.

For more information about Active Directory Certificate Services, click the following link:

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

21. 按一下以提交高級證書請求。

Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#)



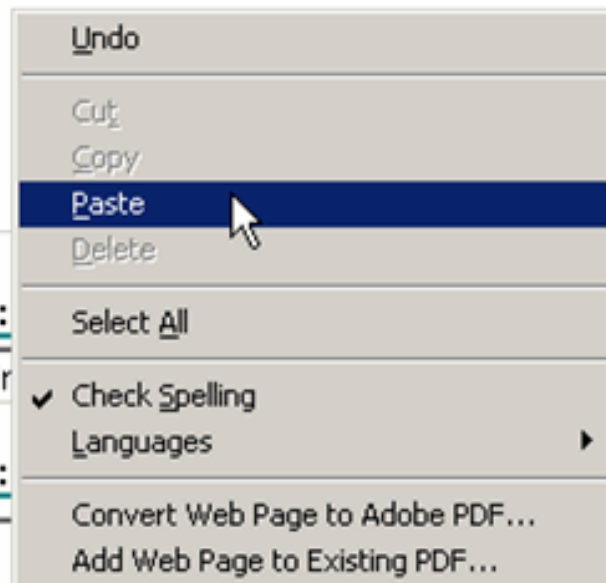
22. 將CSR內容貼上到「儲存的請求」欄位中。

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CM source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):



Certificate Template:

Adr

Additional Attributes:

Attributes:

23. 選擇Web Server作為證書模板，然後按一下Submit。

Microsoft Active Directory Certificat...

Microsoft Active Directory Certificate Services -- corp-RFDEMO-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CM source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
gA/MMZsTioEPekcunm+2Ft1AXajB32uwHH11c9
J4qsQM7KEYOpQt4bia071S8Lm6BBTk9mRhiTBwSF
kSa7LHYgkgLRYBnpul5RjQ7wWijArH8cK1OrVT42
LPKQ72N2XYIXfu0jdgaoJjmsk6T9nLABVYQ6nKQx
V5QYBOjTYHXIPG8/ned9z3M0iZd2sm4XNS2bJfO/
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

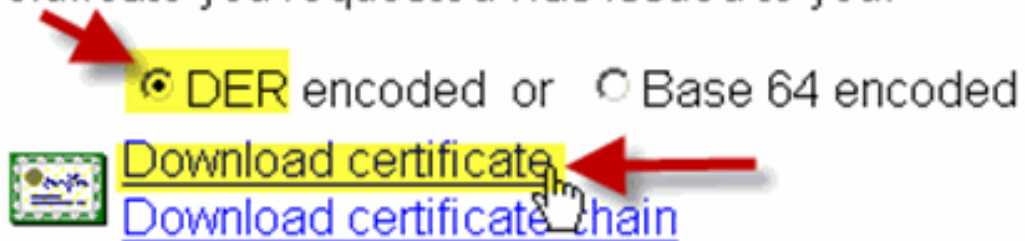
Attributes:

Submit >

24. 選擇DER encoded，然後按一下Download certificate。

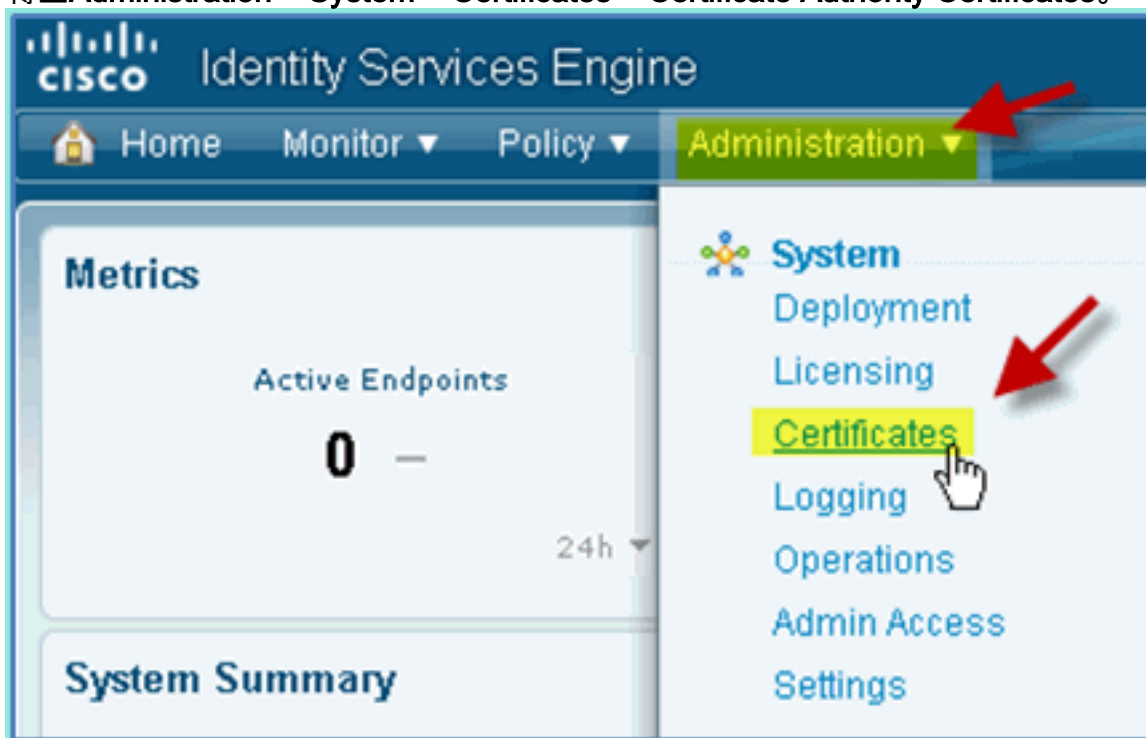
Certificate Issued

The certificate you requested was issued to you.

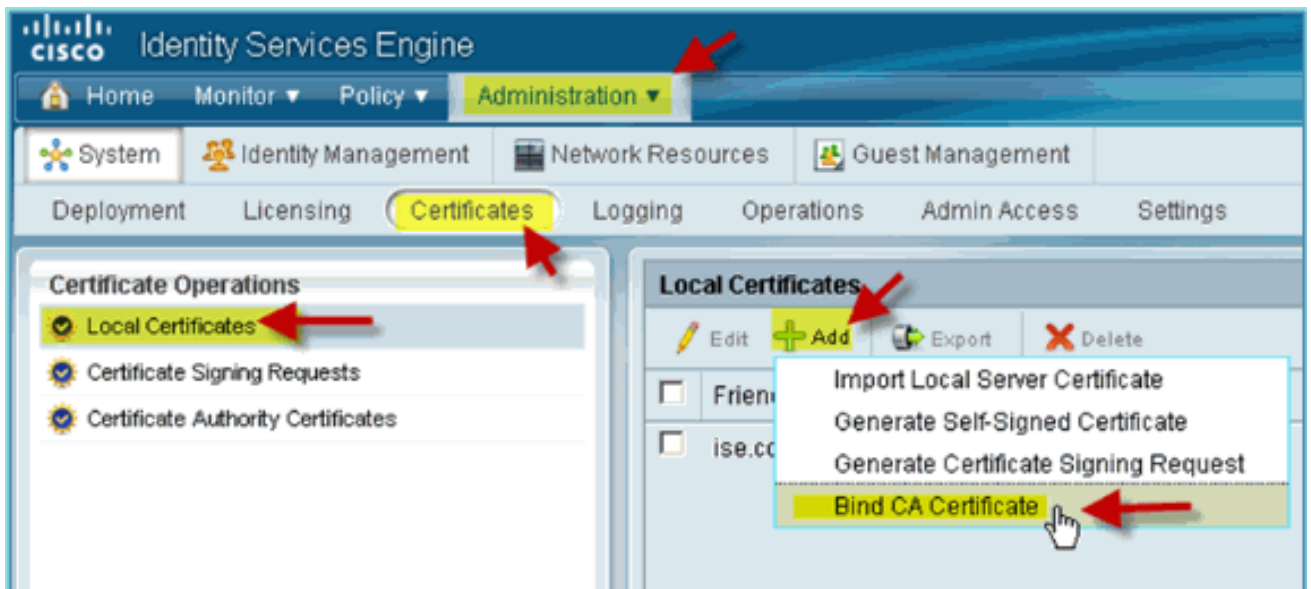


25. 將檔案儲存到已知位置 (例如下載)

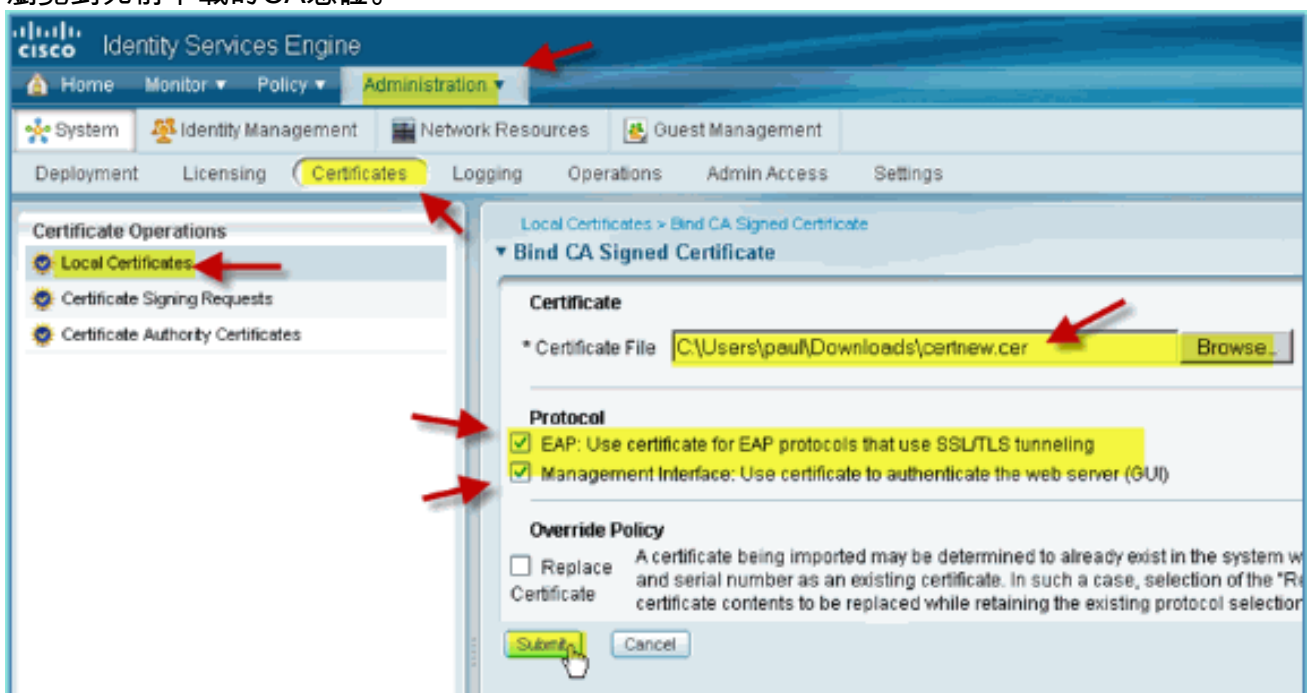
26. 轉至Administration > System > Certificates > Certificate Authority Certificates。



27. 按一下Add > Bind CA Certificate。

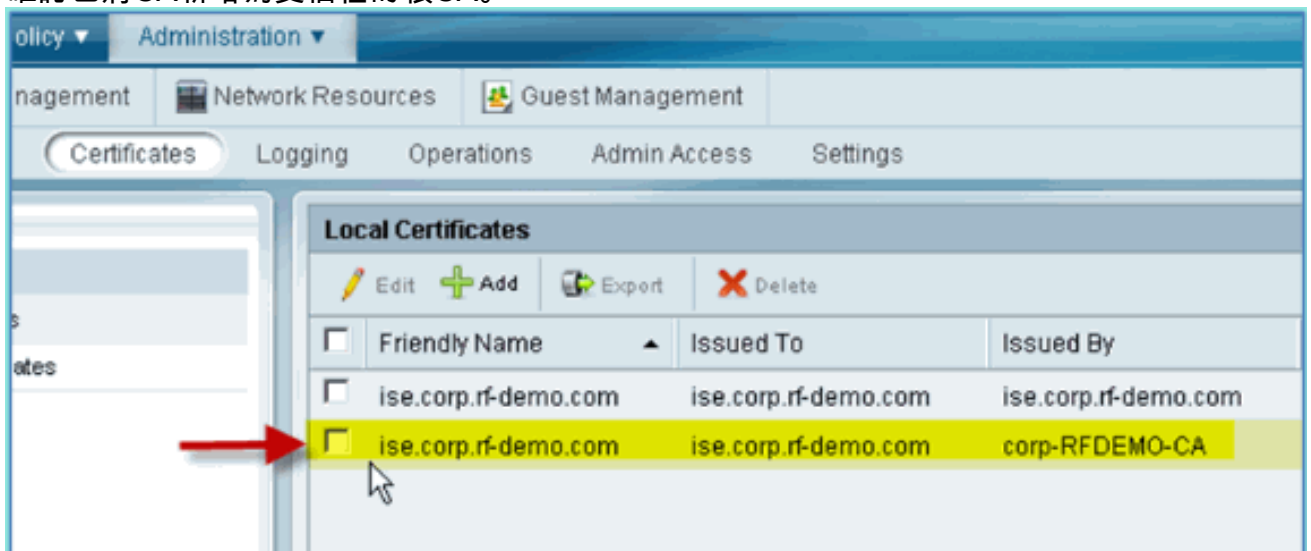


28. 瀏覽到先前下載的CA憑證。



29. 選擇Protocol EAP和Management Interface，然後按一下Submit。

30. 確認已將CA新增為受信任的根CA。

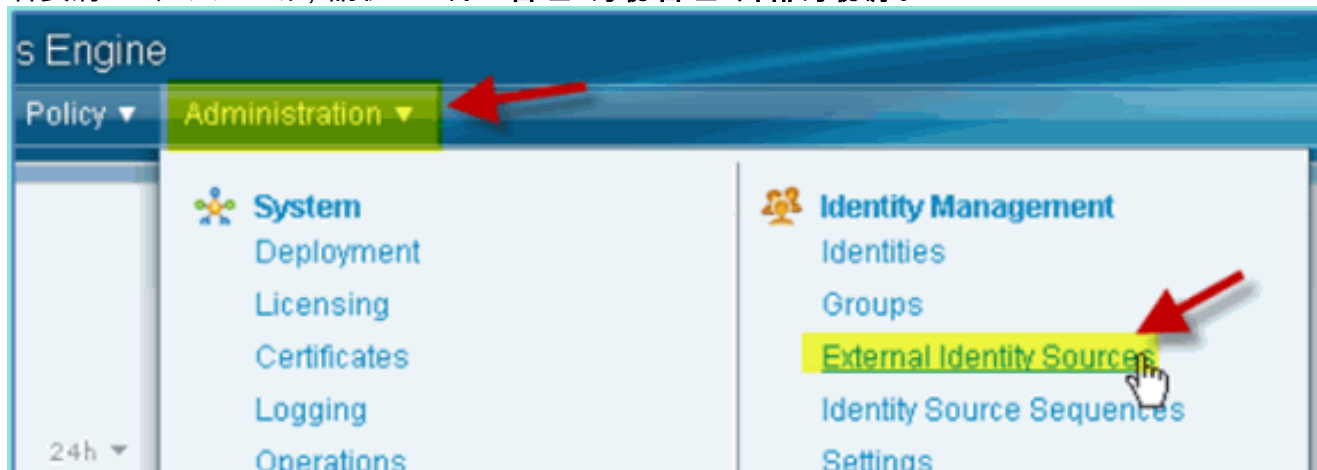


Windows 2008 Active Directory整合

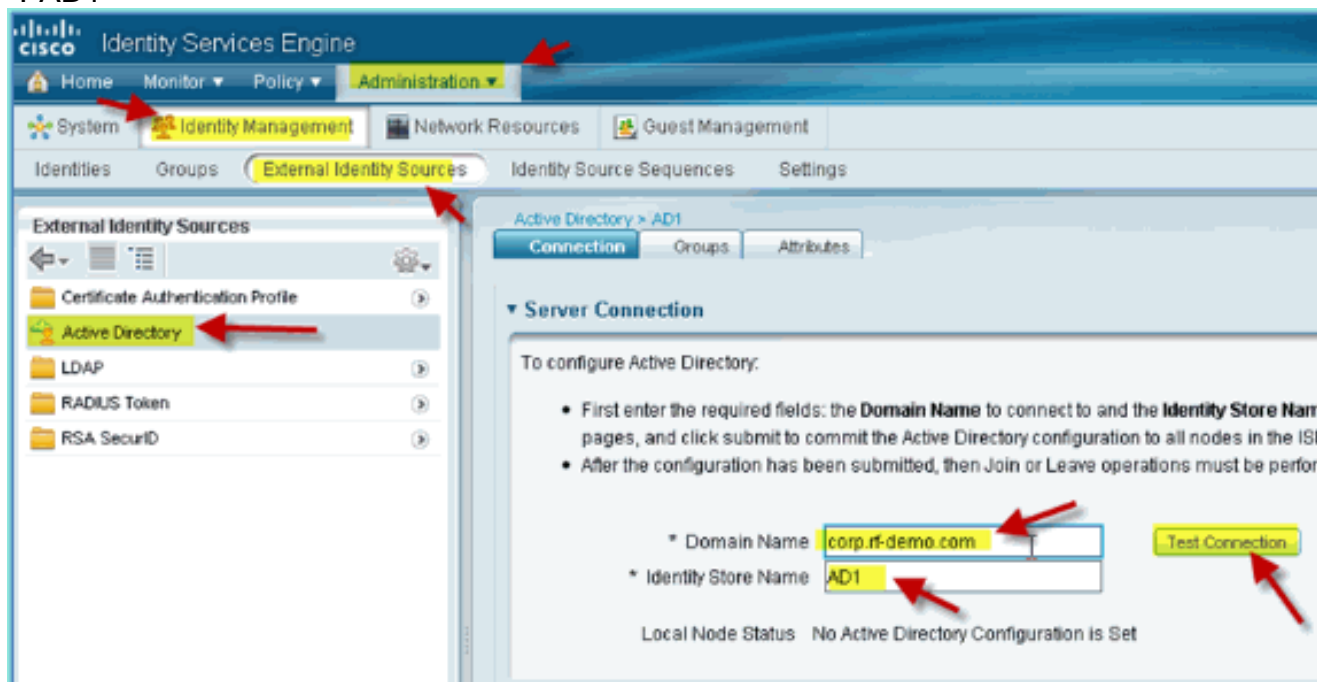
ISE可以直接與Active Directory(AD)進行通訊，用於使用者/機器身份驗證或用於檢索授權資訊使用者屬性。為了與AD通訊，必須將ISE「加入」到AD域。在本練習中，您將將ISE加入AD域，並確認AD通訊是否正常工作。

請完成以下步驟：

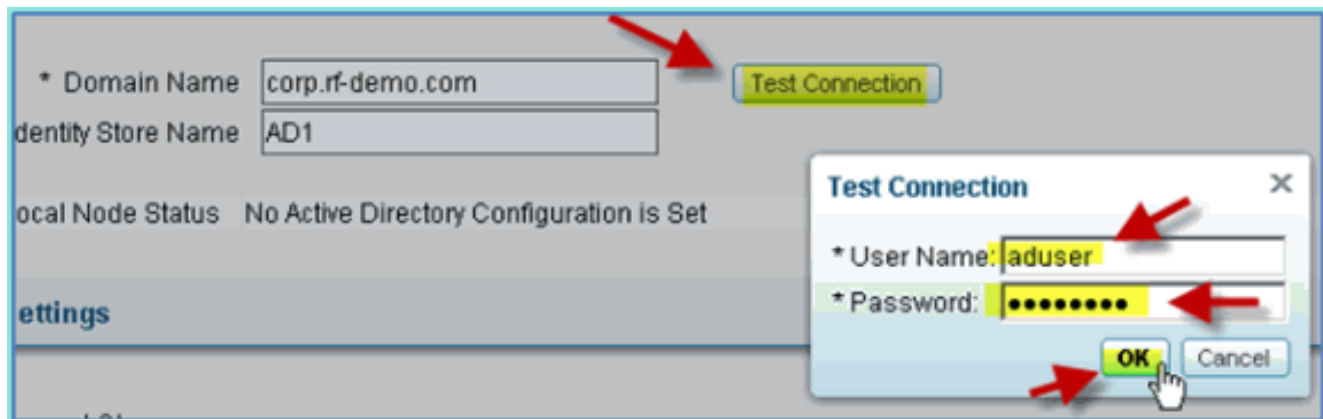
1. 若要將ISE加入AD域，請從ISE轉至**管理>身份管理>外部身份源**。



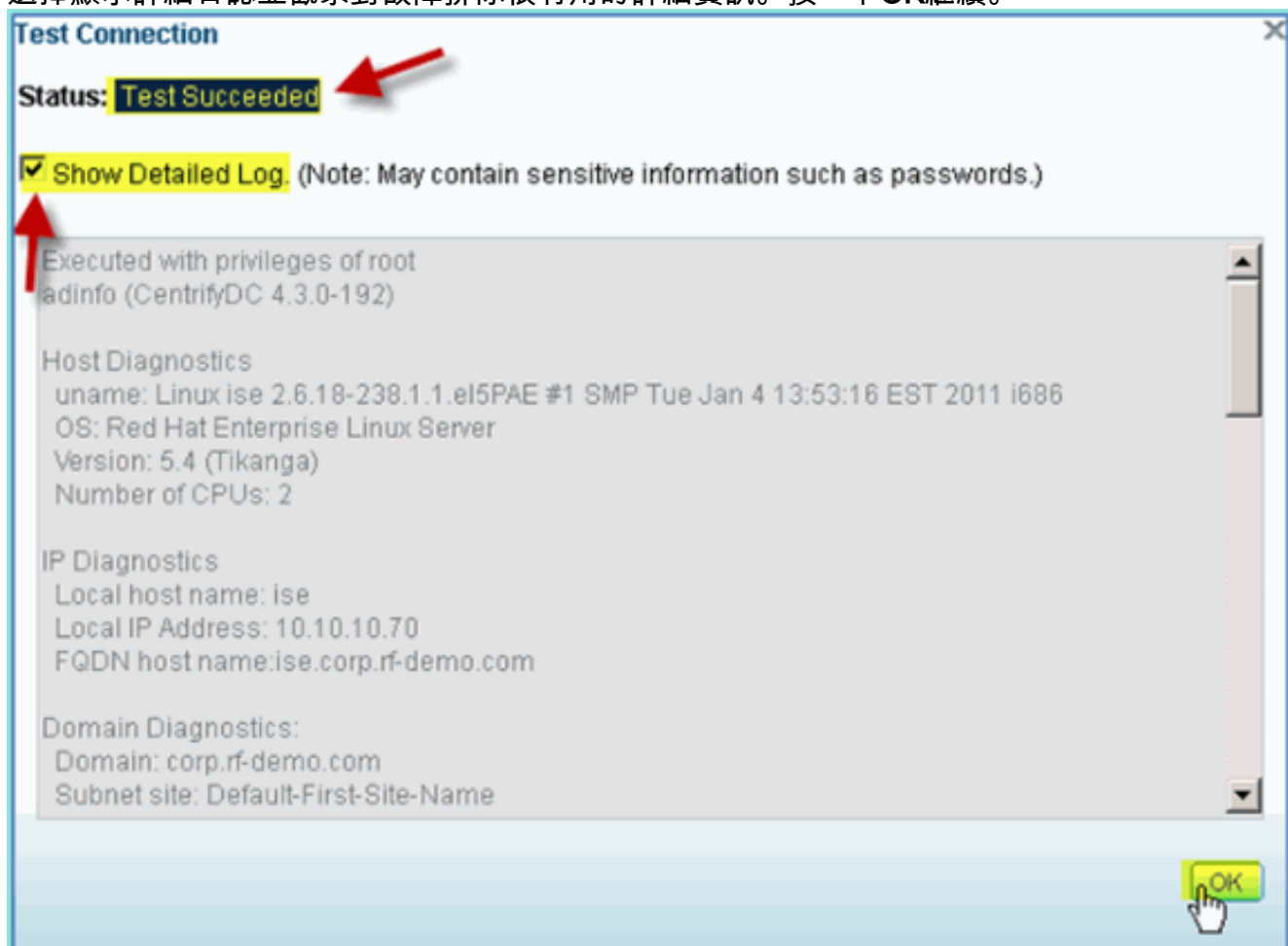
2. 從左側窗格 (外部身份源) 中選擇**Active Directory**。
3. 在右側，選擇**Connection**頁籤並輸入以下內容：域名：corp.rf-demo.com標識儲存名稱：AD1



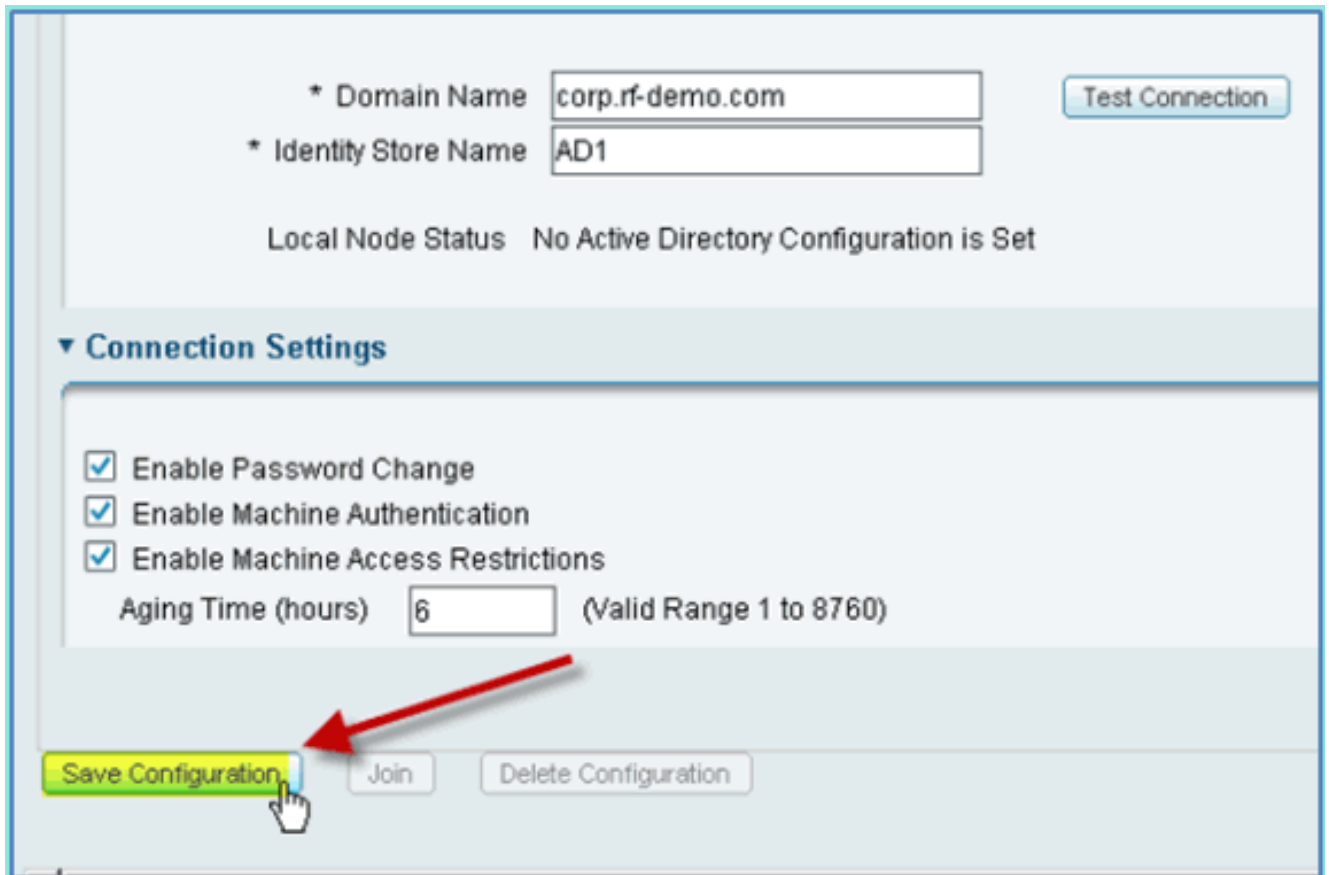
4. 按一下「**Test Connection**」。輸入AD使用者名稱(aduser/Cisco123)，然後按一下OK。



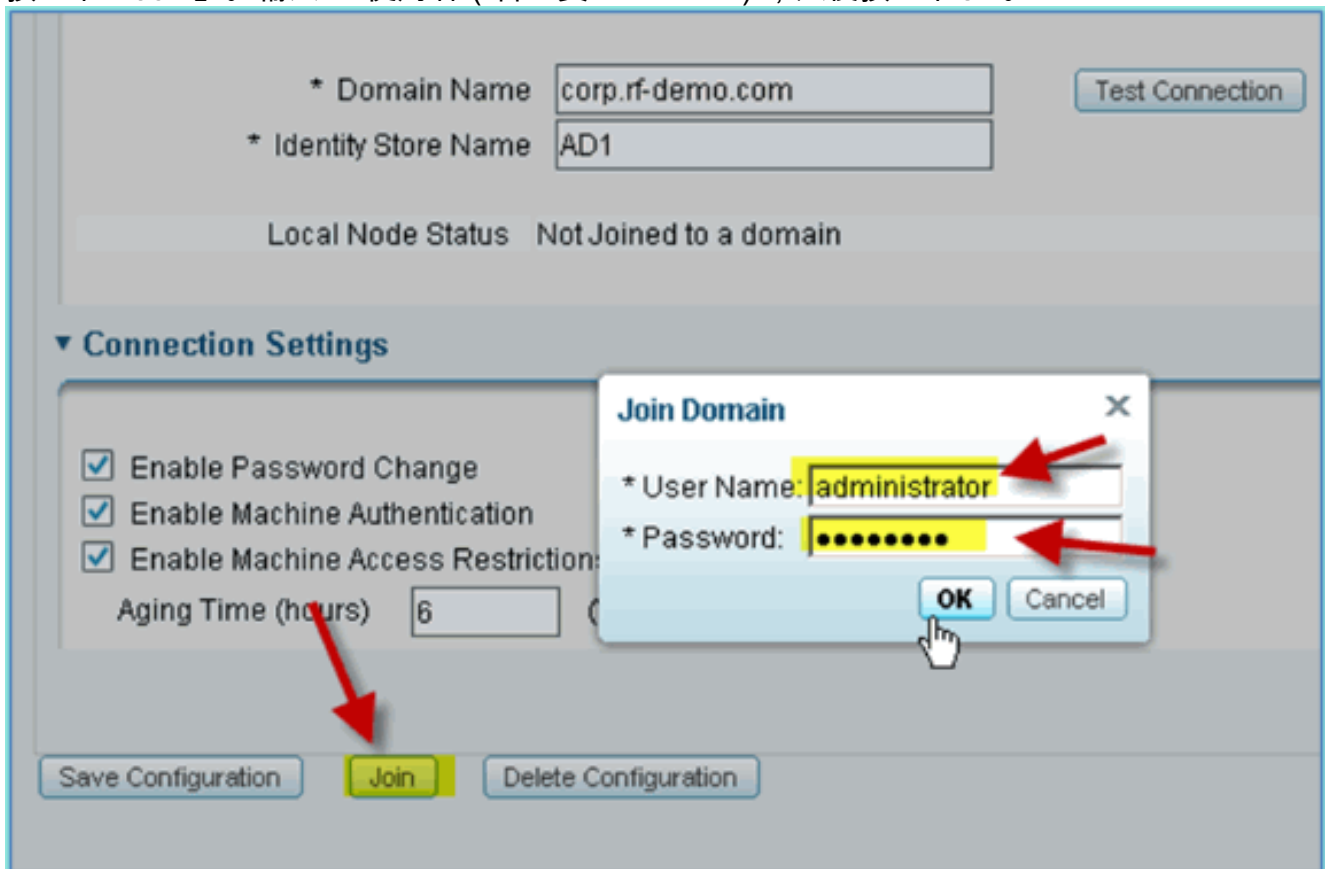
5. 確認「Test Status (測試狀態)」顯示「Test Succeeded(測試成功)」。
6. 選擇顯示詳細日誌並觀察對故障排除很有用的詳細資訊。按一下OK繼續。



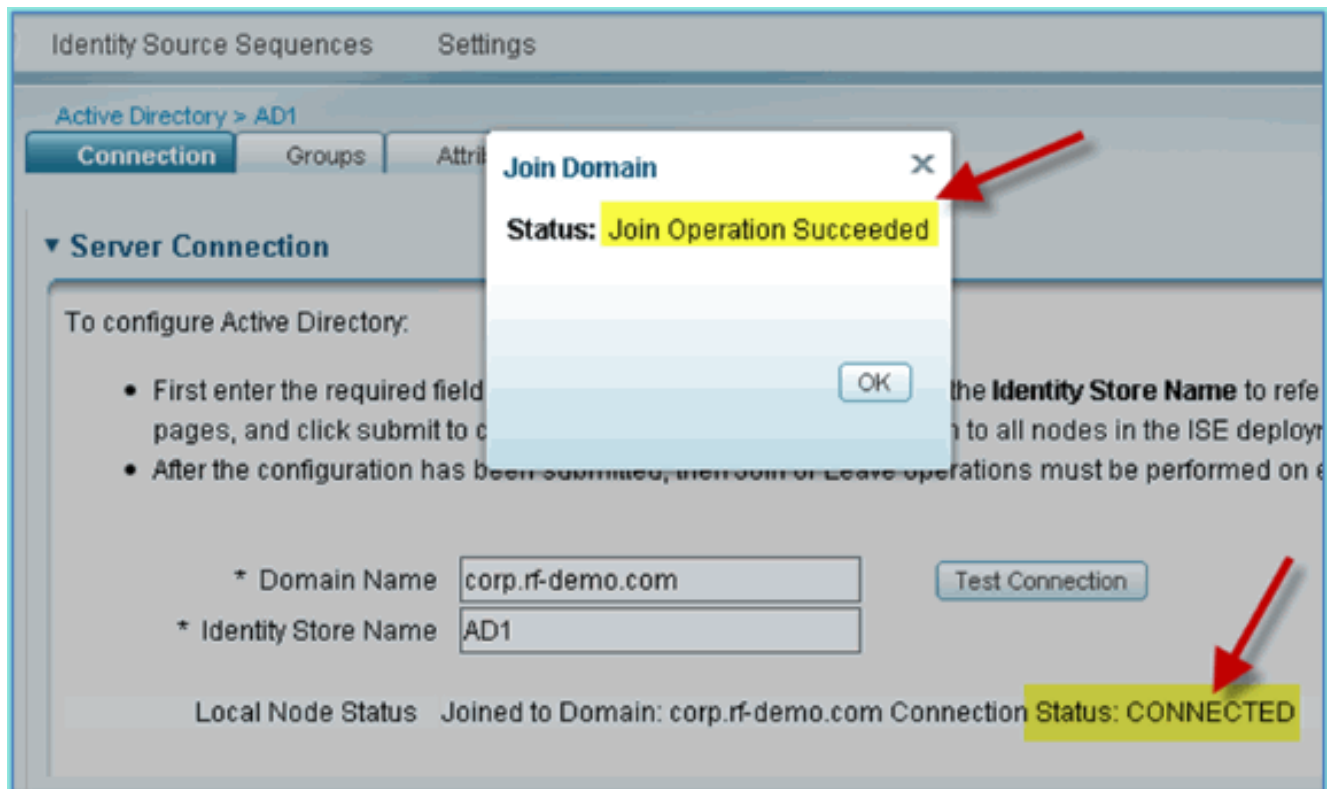
7. 按一下「Save Configuration」。



8. 按一下「Join」。輸入AD使用者（管理員/Cisco123），然後按一下OK。



9. 確認「加入操作狀態」顯示**成功**，然後按一下**確定**繼續。伺服器連線狀態顯示**CONNECTED**。如果此狀態隨時更改，測試連線將幫助排除AD操作問題。



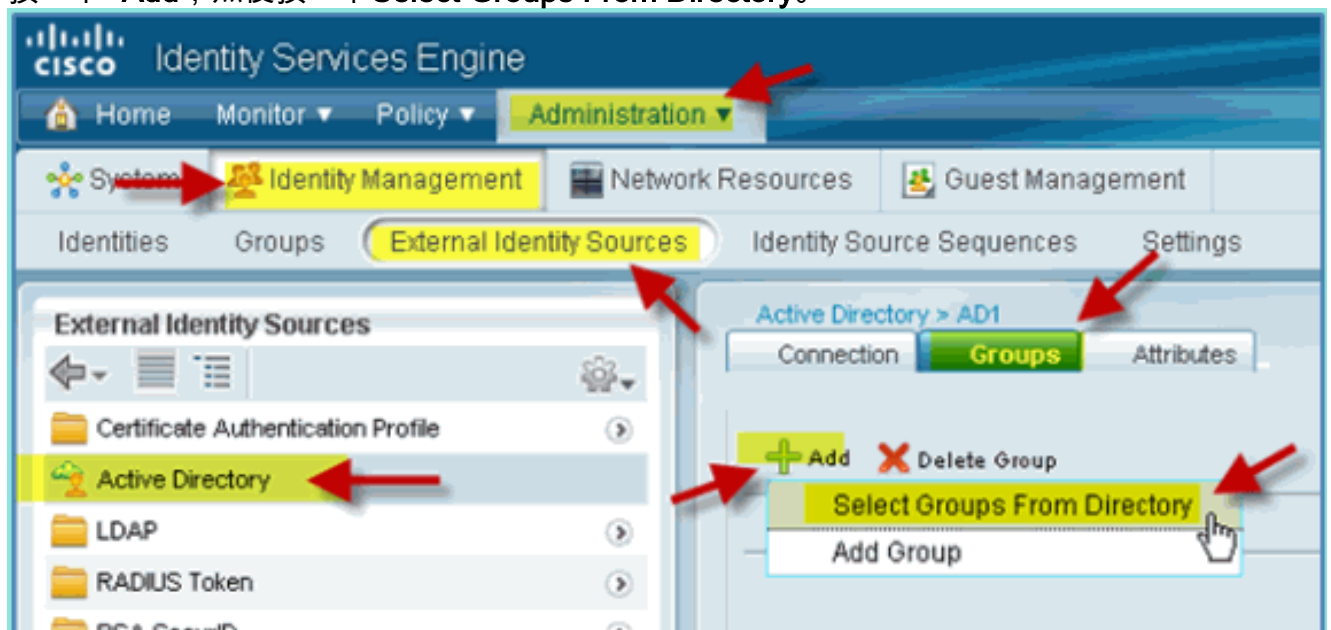
新增Active Directory組

新增AD組時，允許對ISE策略進行更精細的控制。例如，AD組可以按功能角色（如員工或承包商組）區分，而不會在以前的ISE 1.0練習中遇到相關錯誤，在此練習中，策略僅限於使用者。

在本實驗中，僅使用Domain Users和/或Employee組。

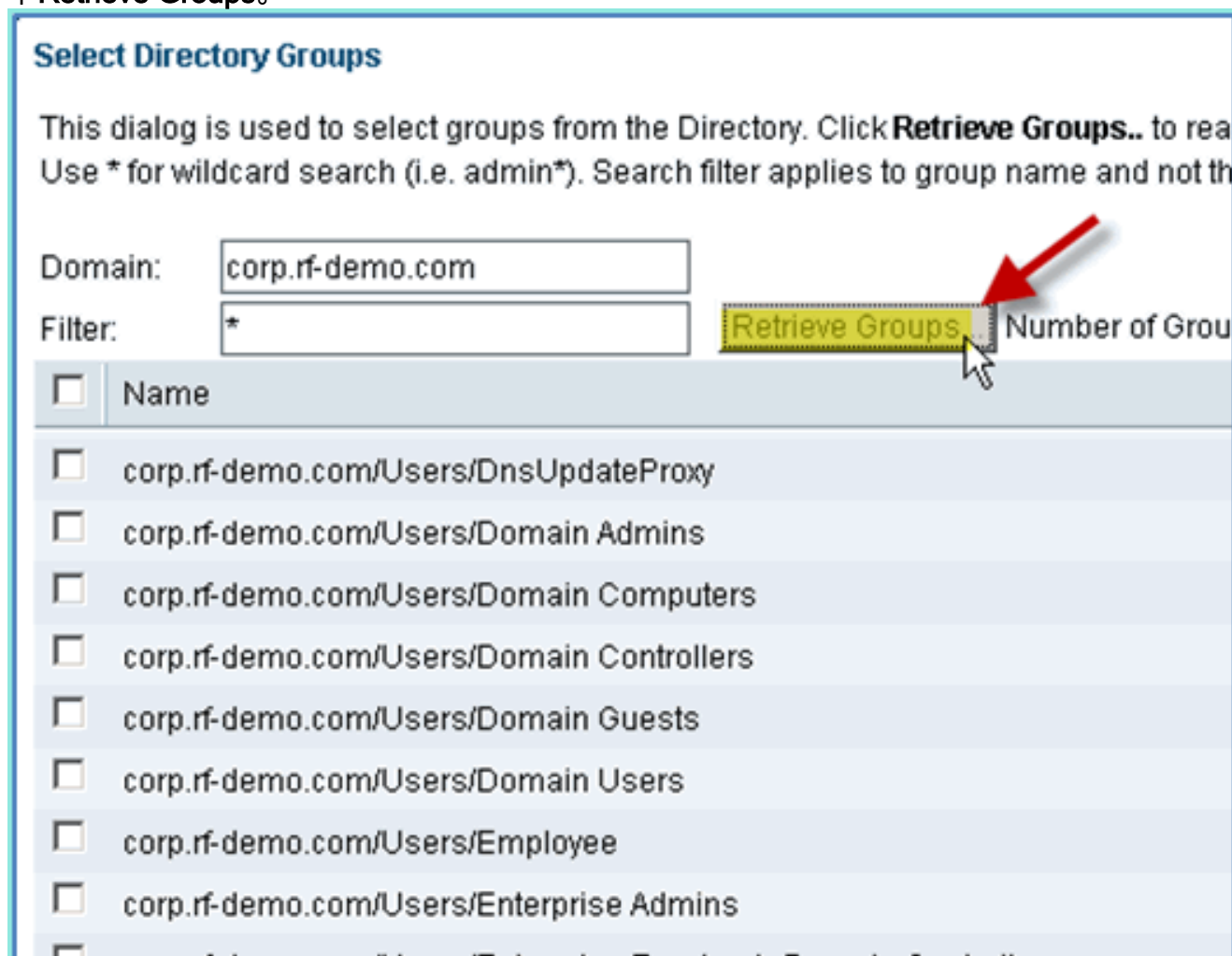
請完成以下步驟：

1. 從ISE轉至**管理>身份管理>外部身份源**。
2. 選擇**Active Directory > Groups**頁籤。
3. 按一下**+Add**，然後按一下**Select Groups From Directory**。



4. 在後續視窗（選擇目錄組）中，接受域(corp-rf-demo.com)和過濾器(*)的預設值。然後，按一

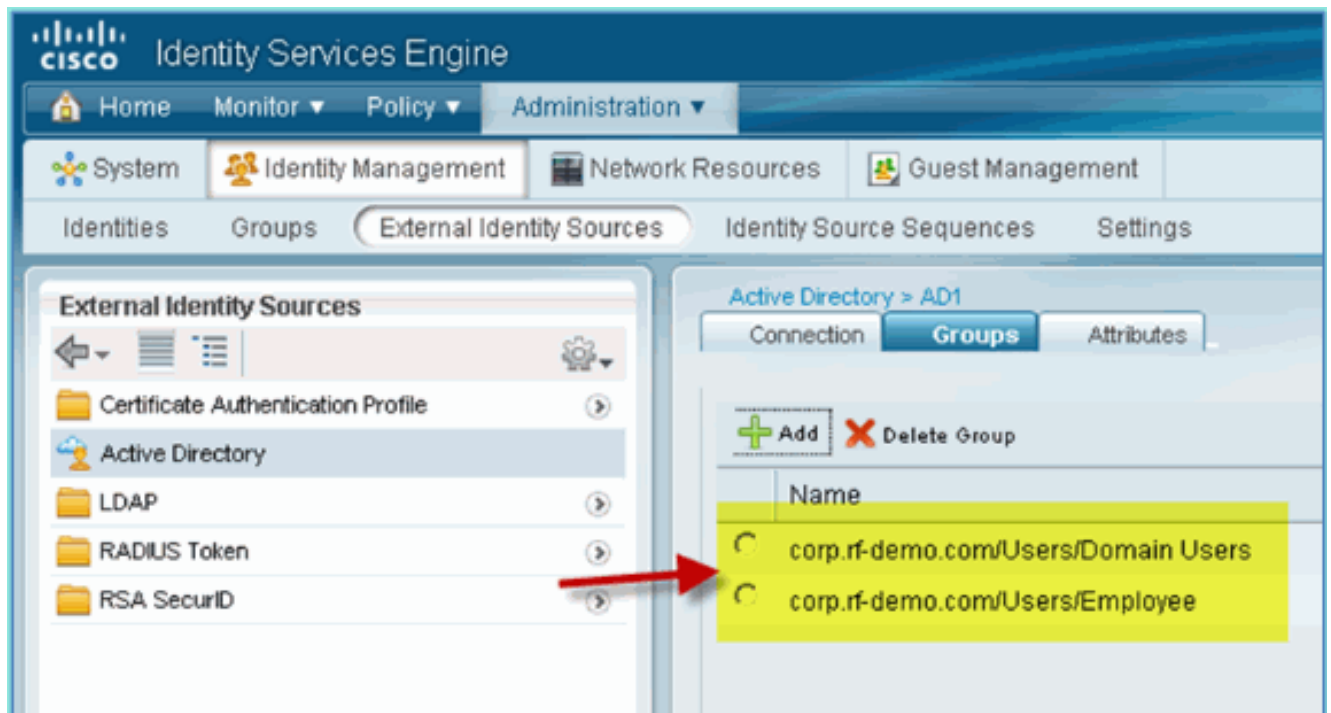
下Retrieve Groups。



5. 選中Domain Users和Employee組的框。完成後按一下OK。



6. 確認已將這些組新增到清單中。

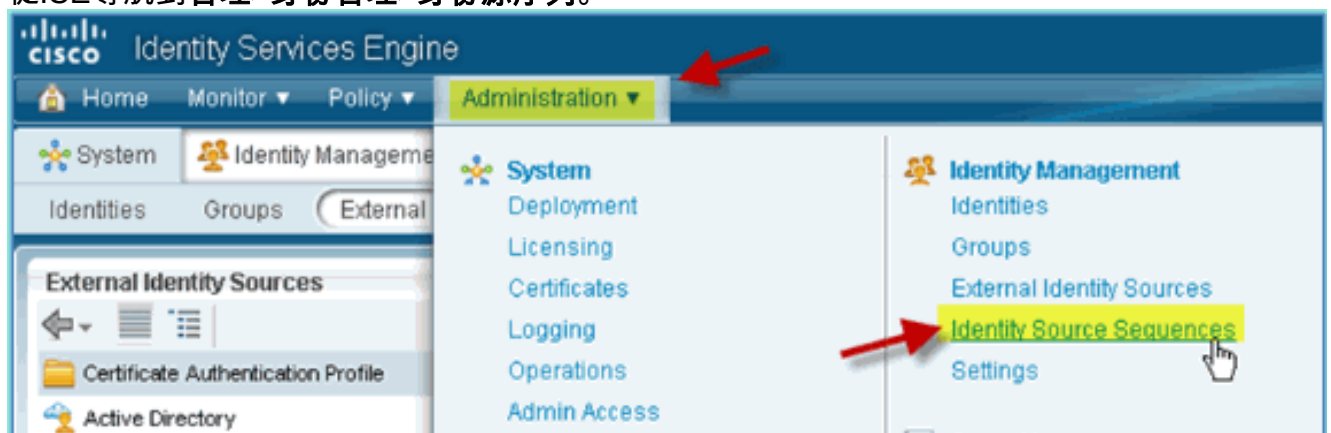


新增身份源序列

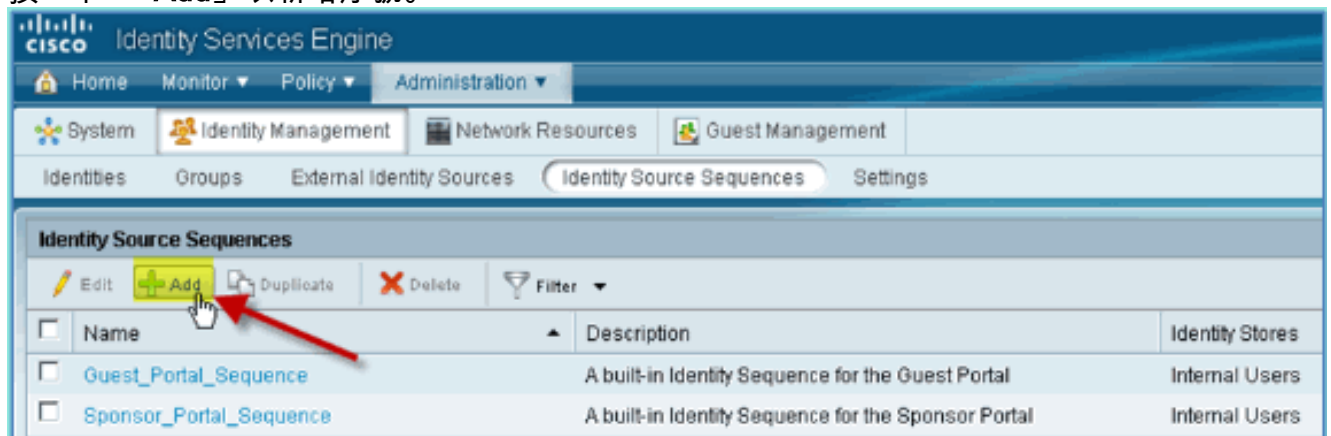
預設情況下，ISE設定為使用內部使用者進行身份驗證儲存。如果新增AD，可以建立優先順序順序以包括ISE將用於檢查身份驗證的AD。

請完成以下步驟：

1. 從ISE導航到**管理>身份管理>身份源序列**。



2. 按一下「+Add」以新增序號。



3. 輸入新名稱：AD_Internal。將所有可用源新增到「選定」欄位。然後，根據需要重新排序，以便將AD1移至清單頂部。按一下「Submit」。

Identities Groups External Identity Sources Identity Source Sequences Settings

Identity Source Sequences List > New Identity Source Sequence

▼ Identity Source Sequence

* Name

Description

▼ Certificate Based Authentication

Select Certificate Authentication Profile

▼ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
	AD1
	Internal Users
	Internal Endpoints

▼ Advanced Search List Settings

Select the action to be performed if a selected identity store cannot be accessed for authentication

Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"

Treat as if the user was not found and proceed to the next store in the sequence

4. 確認序列已新增到清單中。

Identity Services Engine

Home Monitor Policy Administration

System Identity Management Network Resources Guest Management

Identities Groups External Identity Sources Identity Source Sequences Settings

Identity Source Sequences

Edit Add Duplicate Delete Filter

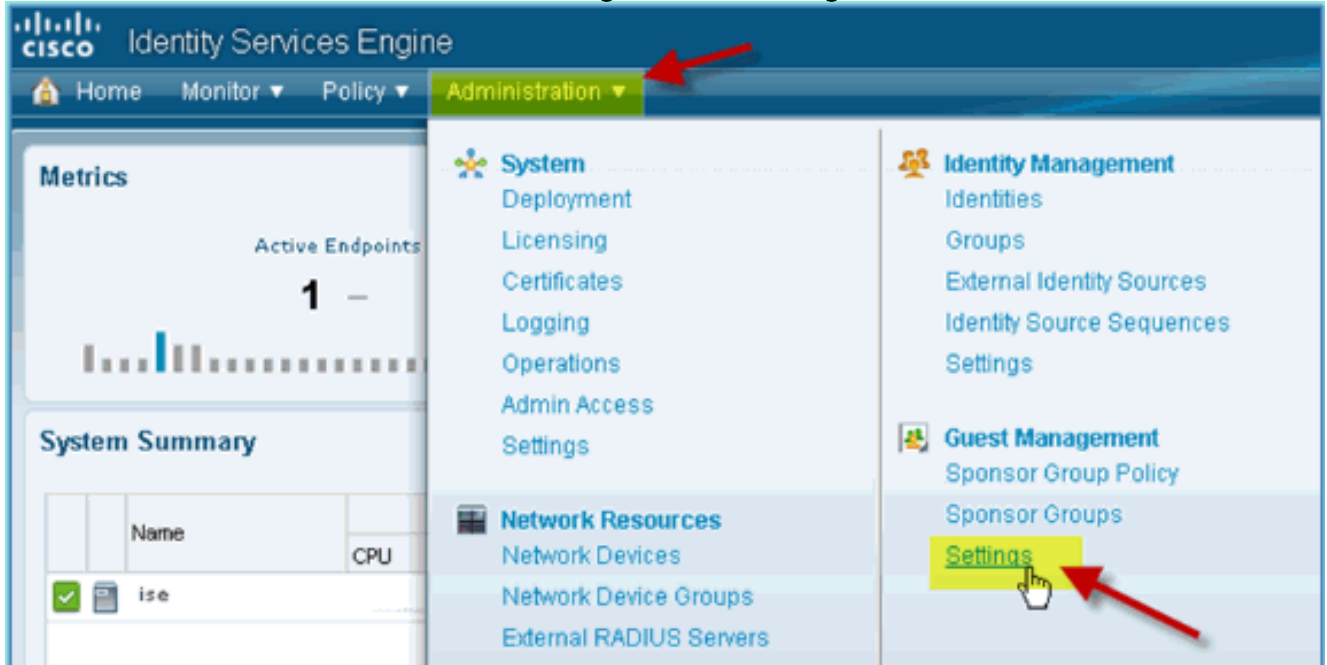
Name	Description	Identity Stores
AD_Internal		AD1, Internal Endpoints, Internal Users
Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users
Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal Users

整合AD的ISE無線贊助訪客接入

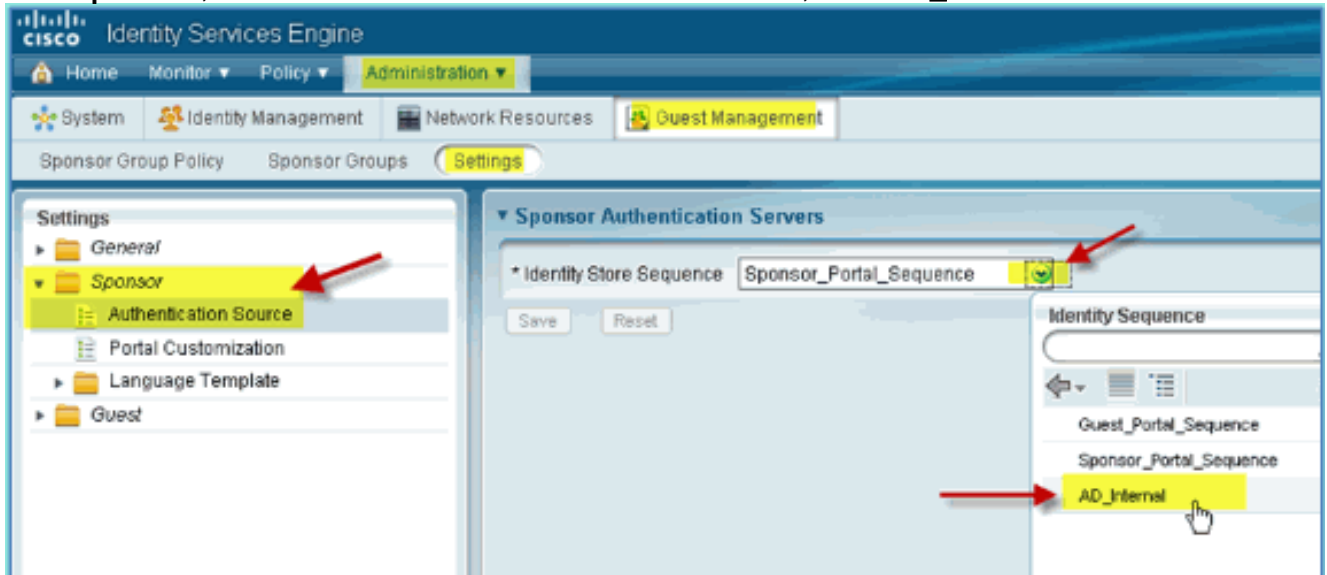
可以將ISE配置為允許使用策略贊助訪客，以便允許AD域使用者贊助訪客訪問。

請完成以下步驟：

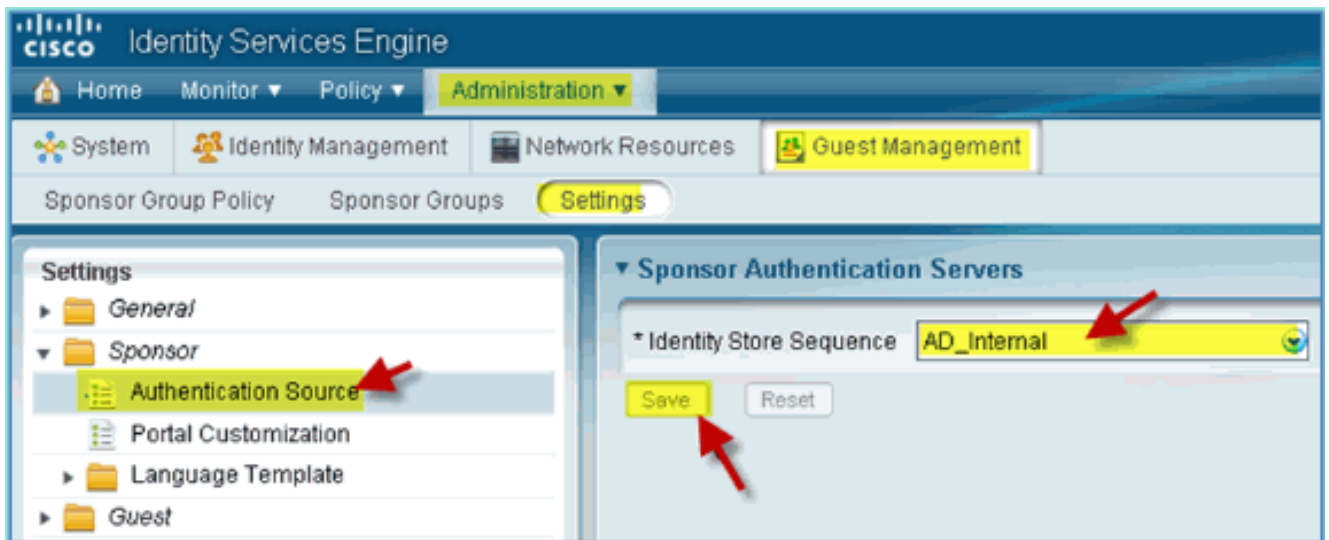
1. 從ISE導航到Administration > Guest Management > Settings。



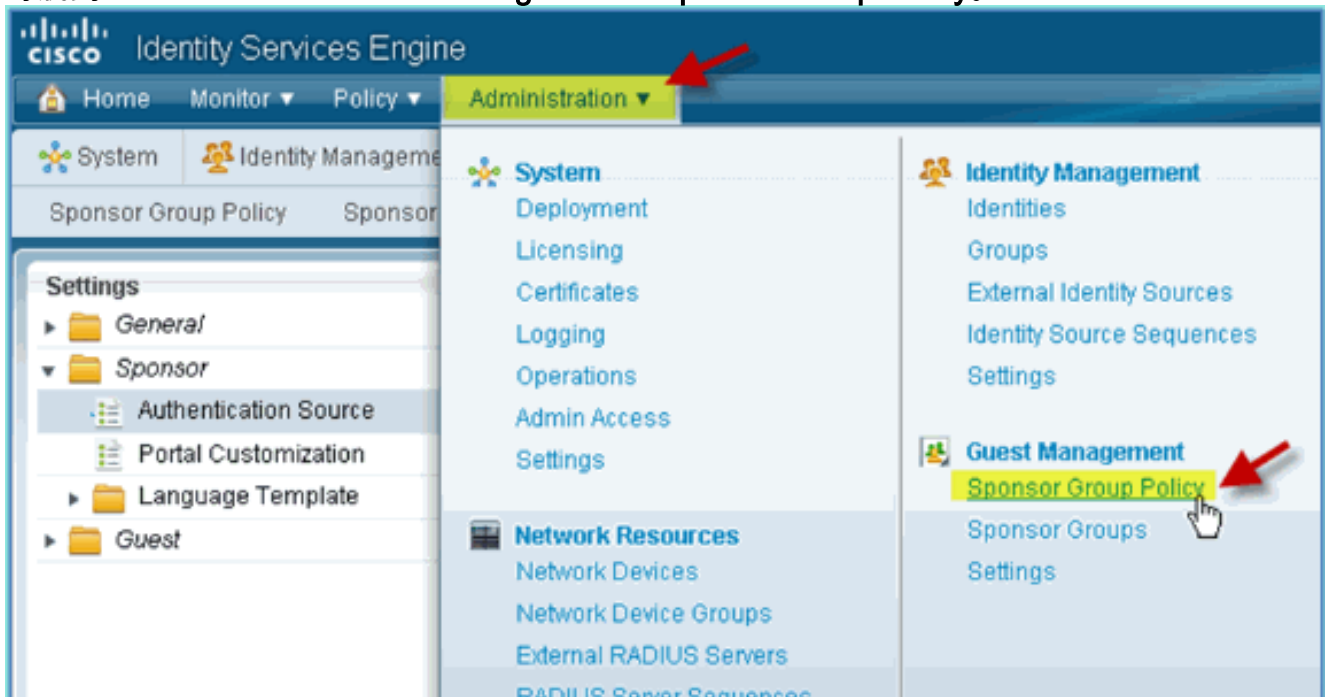
2. 展開Sponsor，然後按一下Authentication Source。然後，選擇AD_Internal作為身份庫序列。



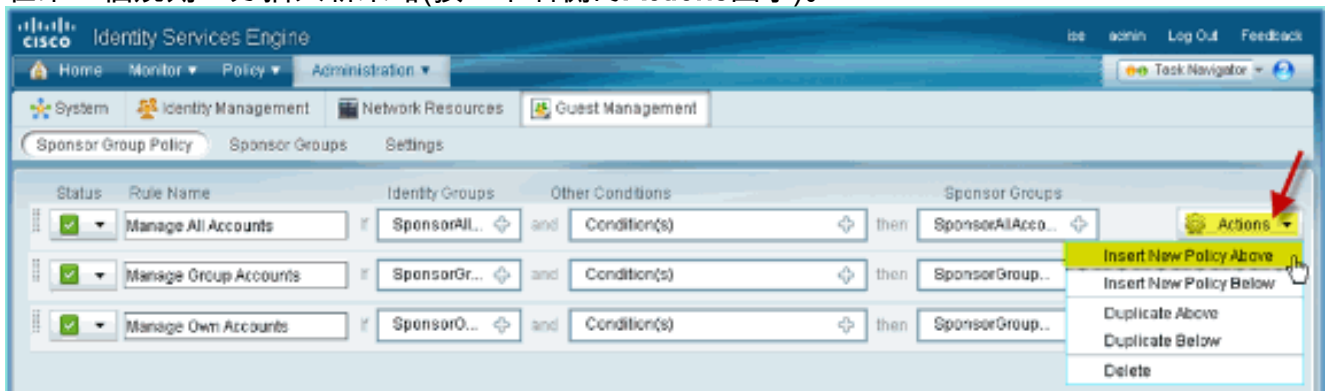
3. 確認AD_Internal為身份庫序列。按一下「Save」。



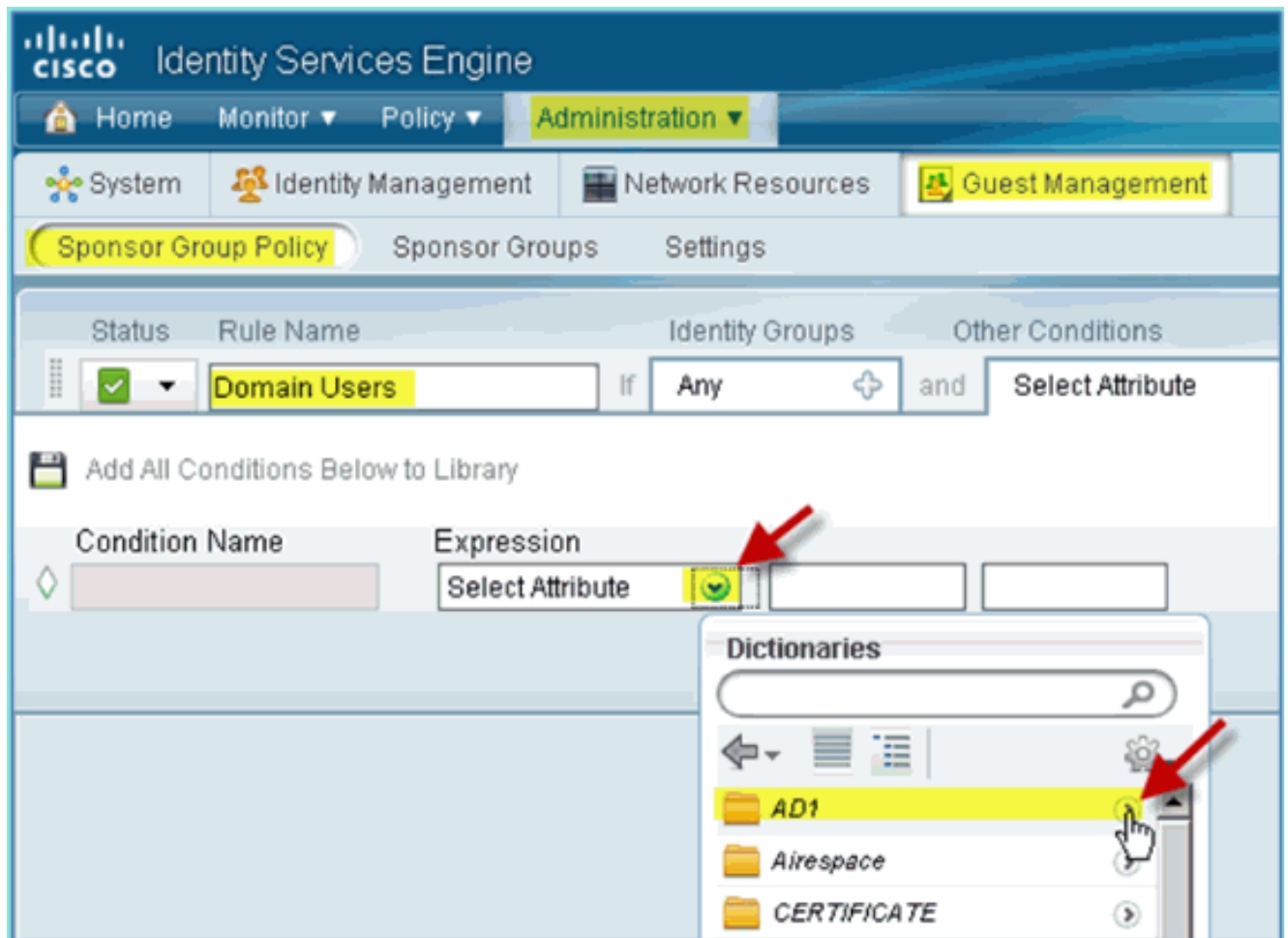
4. 導航到Administration > Guest Management > Sponsor Group Policy。



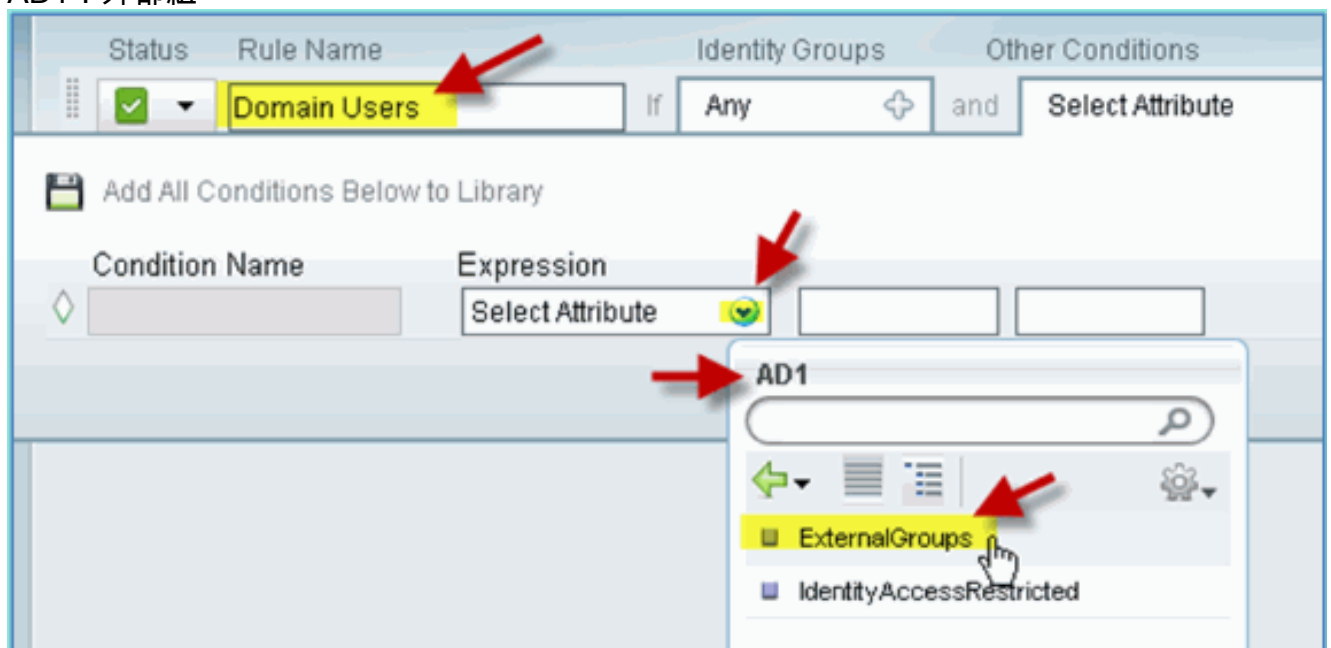
5. 在第一個規則上方插入新策略(按一下右側的Actions圖示)。



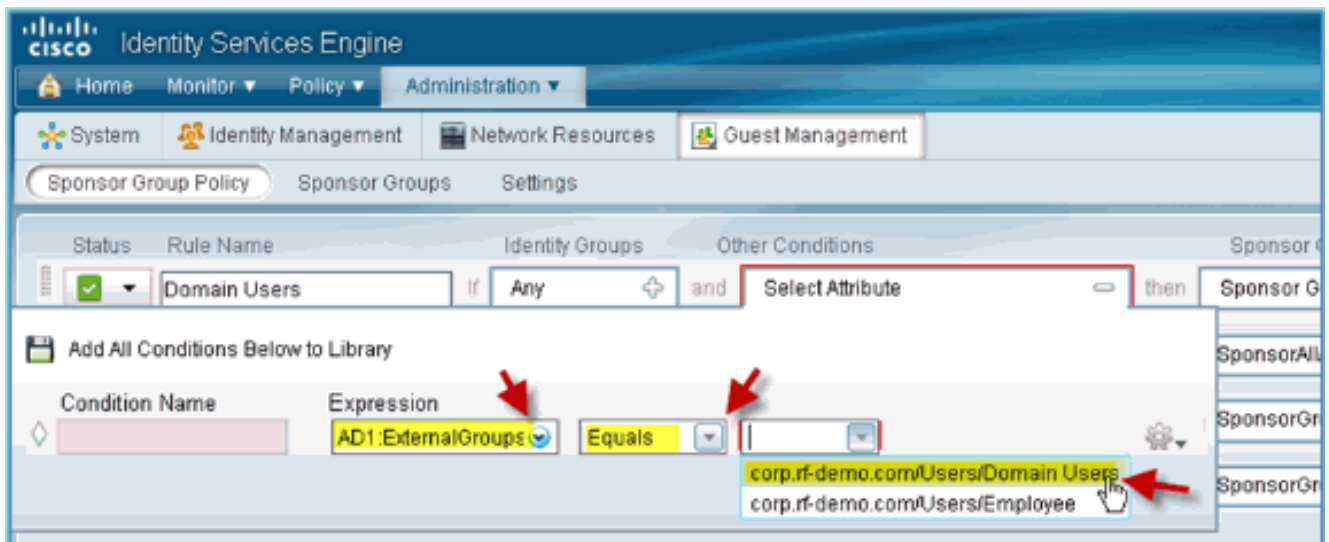
6. 對於新的發起人組策略，請建立以下內容：規則名稱：域使用者身份組：任意其他條件：（新建/高級）> AD1



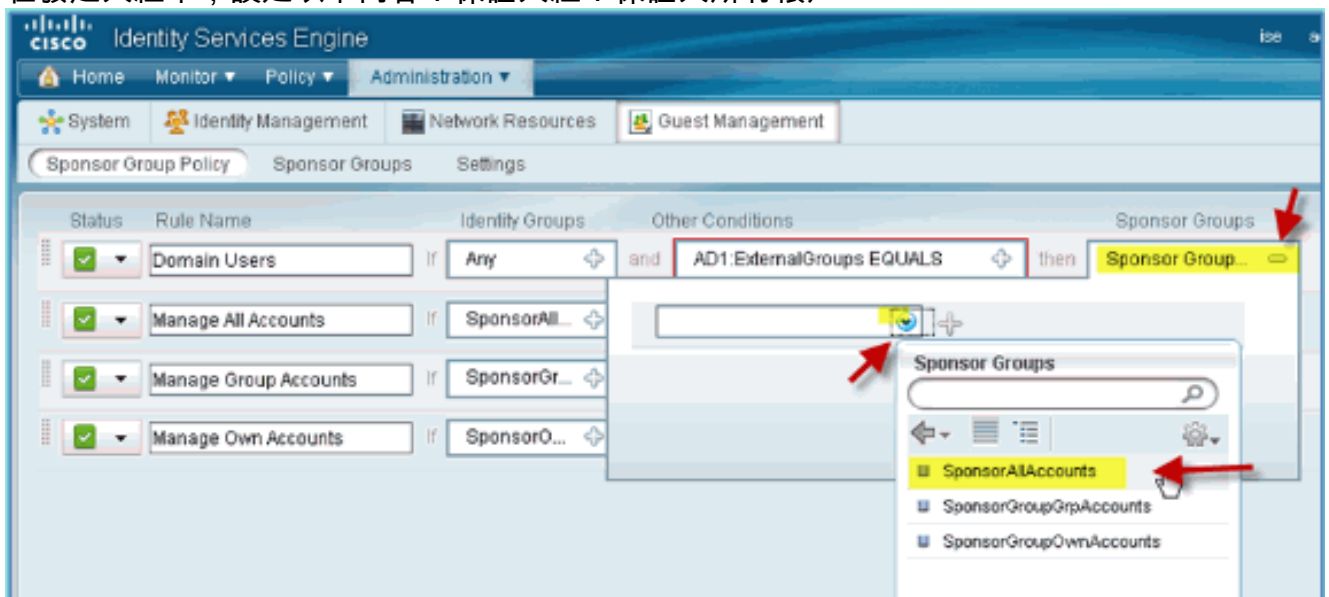
AD1 : 外部組



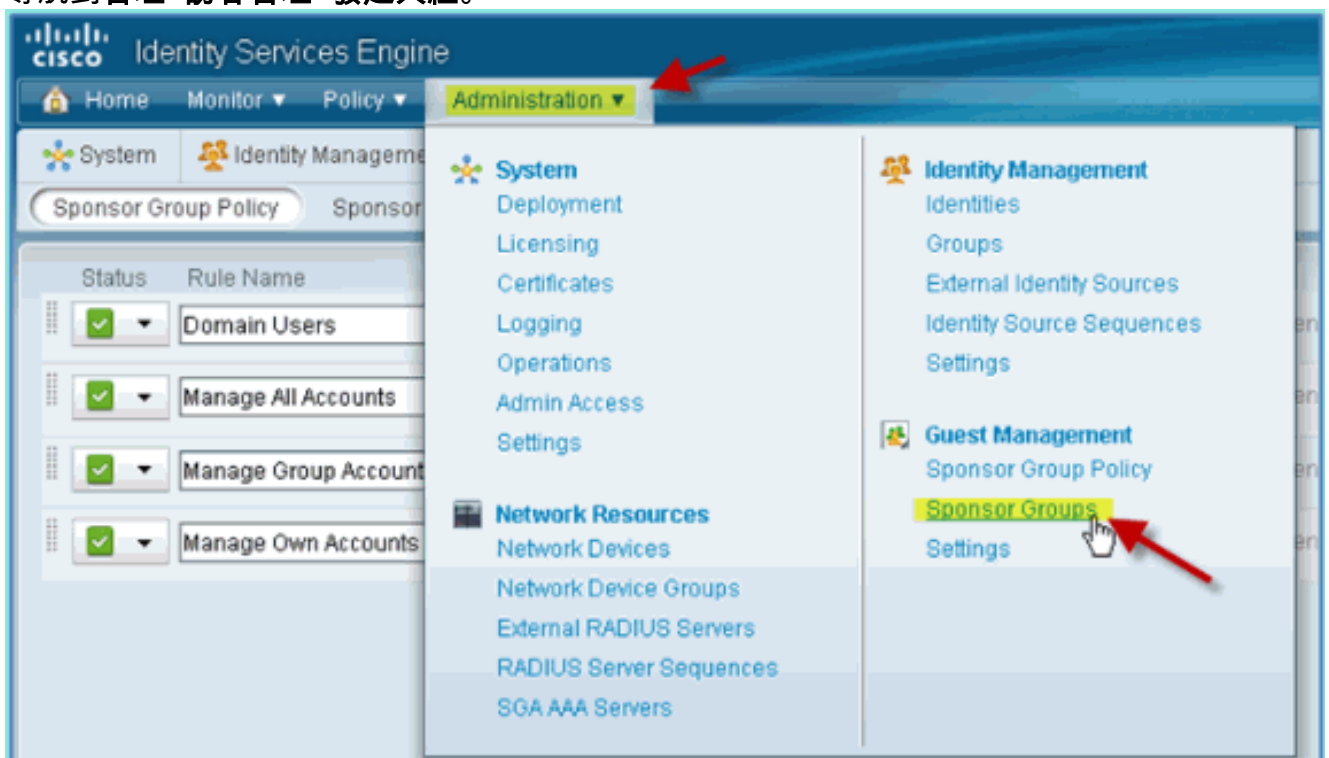
AD1外部組>等於> corp.rf-demo.com/Users/Domain使用者



7. 在發起人組中，設定以下內容：保證人組：保證人所有帳戶



8. 導航到管理>訪客管理>發起人組。



9. 選擇以編輯>SponsorAllAccounts。

CISCO Identity Services Engine

Home Monitor Policy Administration

System Identity Management Network Resources Guest Management

Sponsor Group Policy Sponsor Groups Settings

Guest Sponsor Groups

Edit Add Delete Filter

<input type="checkbox"/>	Sponsor Group Name	Description
<input checked="" type="checkbox"/>	SponsorAllAccounts	Default SponsorGroup
<input type="checkbox"/>	SponsorGroupGrpAccounts	Default SponsorGroup

10. 選擇Authorization Levels並設定以下內容：檢視訪客密碼：是

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes Home, Monitor, Policy, and Administration. The main menu has System, Identity Management, Network Resources, and Guest Management. The current page is 'Sponsor Group Policy' > 'Sponsor Groups' > 'Settings'. The 'Sponsor Group List' shows 'SponsorAllAccounts'. The 'Authorization Levels' tab is selected, and the 'View Guest Password' option is highlighted in yellow with a red arrow pointing to it. The configuration table is as follows:

Allow Login	Yes
Create Accounts	Yes
Create Bulk Accounts	Yes
Create Random Accounts	Yes
Import CSV	Yes
Send Email	Yes
Send SMS	No
View Guest Password	Yes
Allow Printing Guest Details	Yes
View/Edit Accounts	All Accounts
Suspend/Reinstate Accounts	All Accounts
* Account Start Time	1 Days (Valid Range 1 to 999999999)
* Maximum Duration of Account	5 Days (Valid Range 1 to 999999999)

Buttons for 'Save' and 'Reset' are located at the bottom of the configuration area.

[在交換器上設定SPAN](#)

配置SPAN - ISE管理/探測介面是L2，與WLC管理介面相鄰。可將交換器設定為SPAN和其他介面，例如僱員和訪客介面VLAN。

```
Podswitch(config)#monitor session 1 source vlan10 , 11 , 12
Podswitch(config)#monitor session 1 destination interface Fa0/8
ISE virtual probe interface.
```

[參考：Apple MAC OS X的無線身份驗證](#)

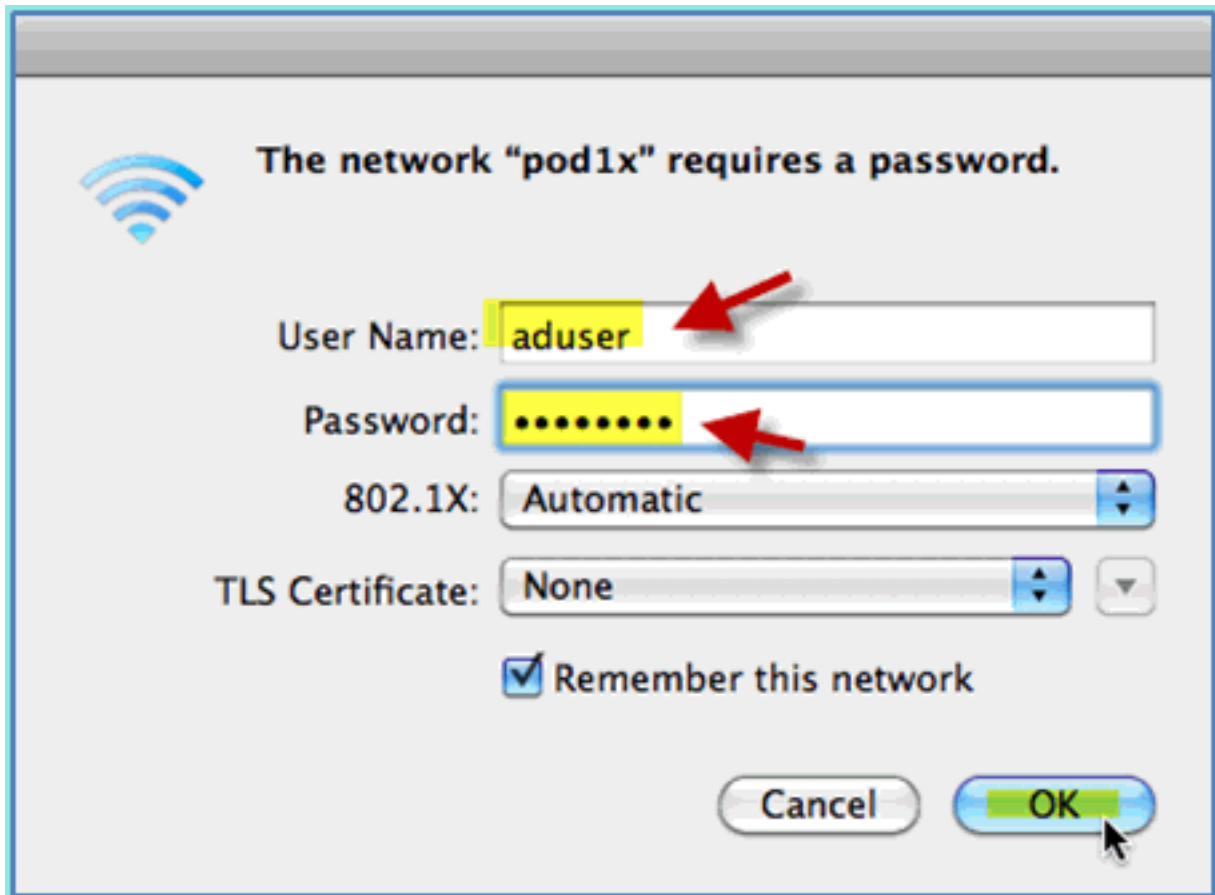
使用Apple Mac OS X無線筆記型電腦，作為內部使用者（或整合的AD使用者），通過經過身份驗證的SSID與WLC關聯。如果不適用，請跳過。

1. 在Mac上，轉到WLAN settings。啟用WIFI，然後選擇並連線到在上一個練習中建立的啟用



802.1X的POD SSID。

2. 提供以下要連線的資訊：使用者名稱：aduser（如果使用AD）、員工（內部 — 員工）、承包商（內部 — 承包商）密碼：XXXX802.1X：自動TLS證書：無

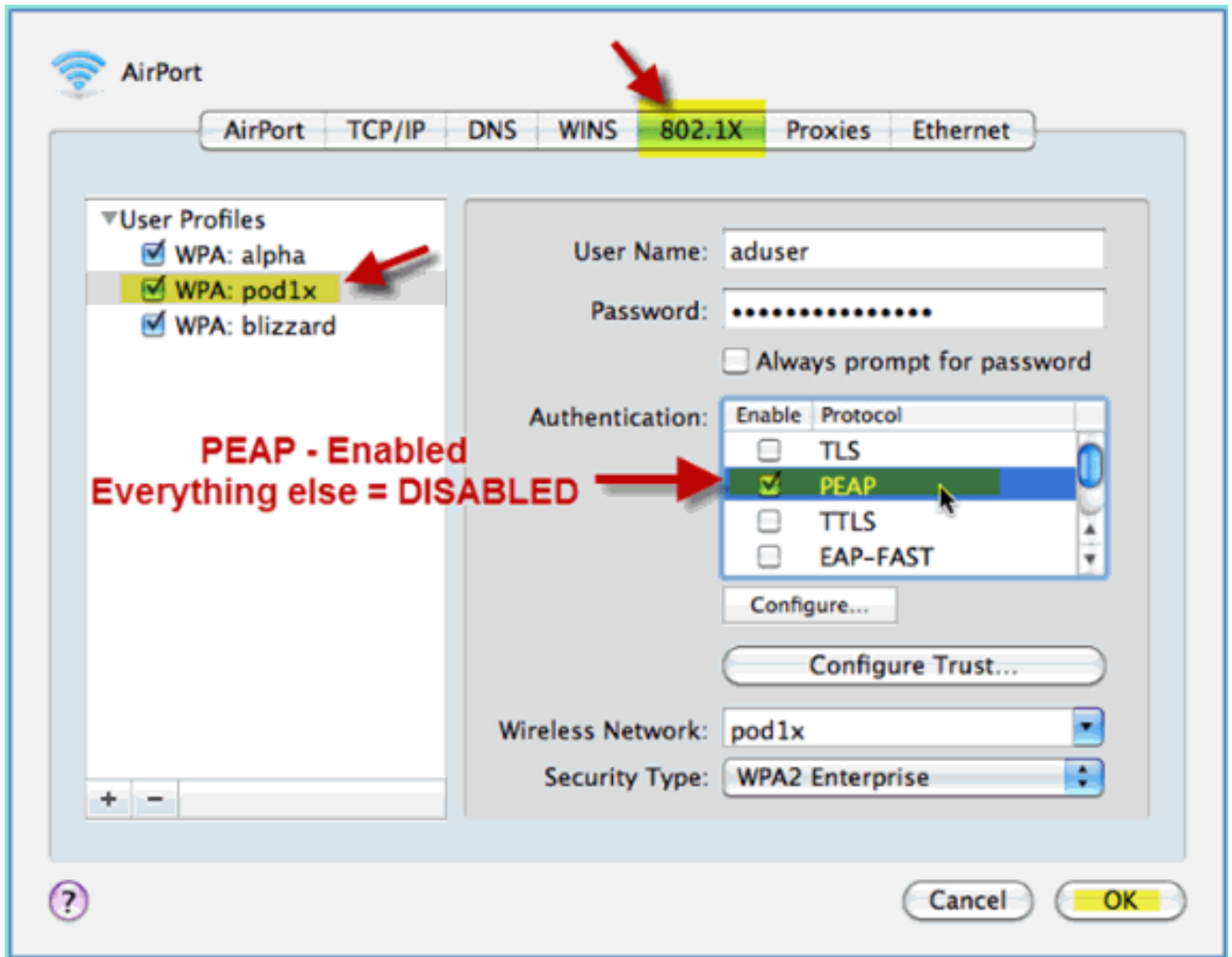


此時

，筆記型電腦可能無法連線。此外，ISE可以按如下方式引發失敗事件：

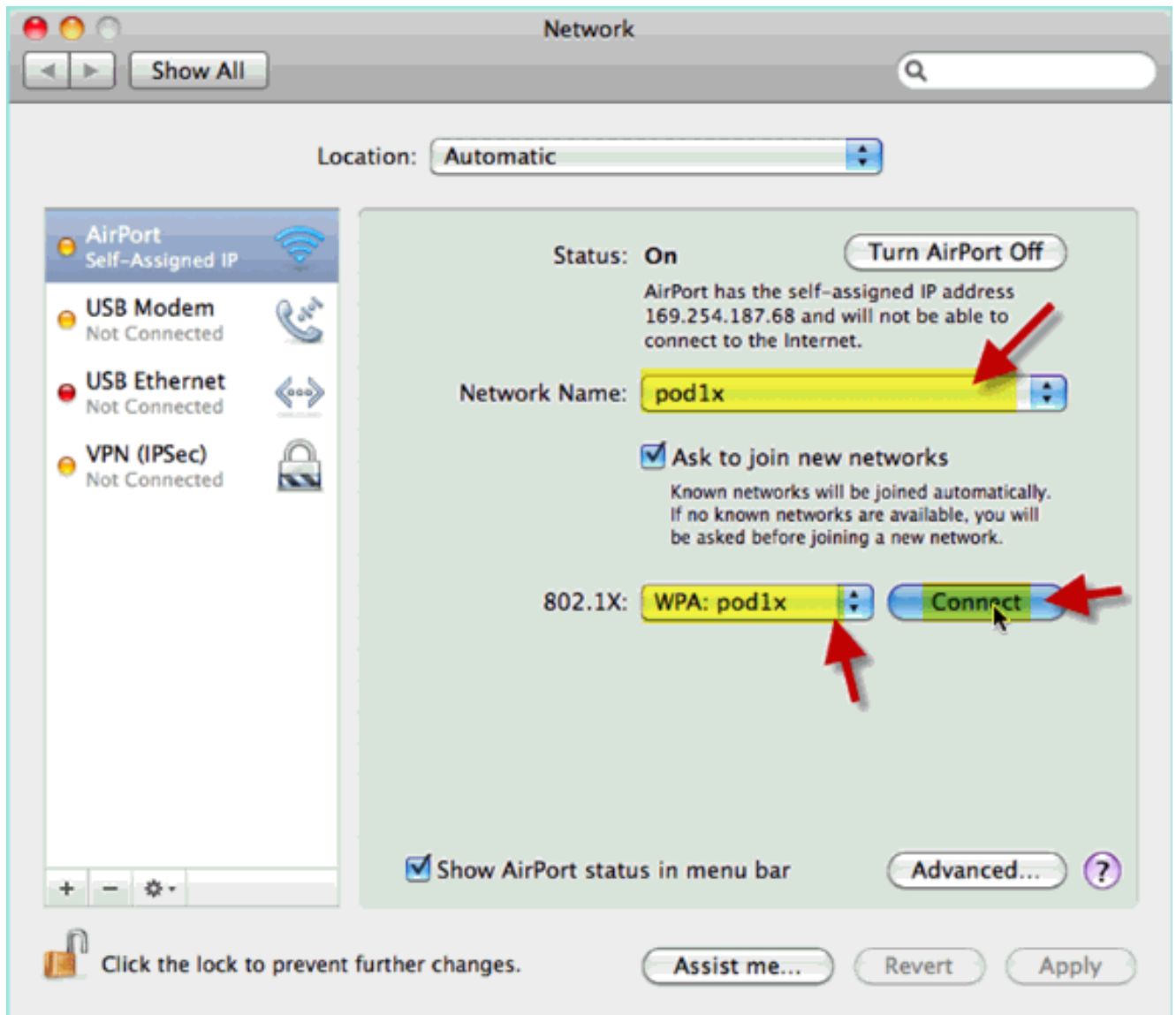
Authentication failed :12514 EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client certificates chain

3. 轉到**System Preference > Network > Airport > 802.1X**設定並將新的POD SSID/WPA配置檔案身份驗證設定為：TLS：已禁用PEAP：已啟用TTLS：已禁用EAP-FAST：已禁用

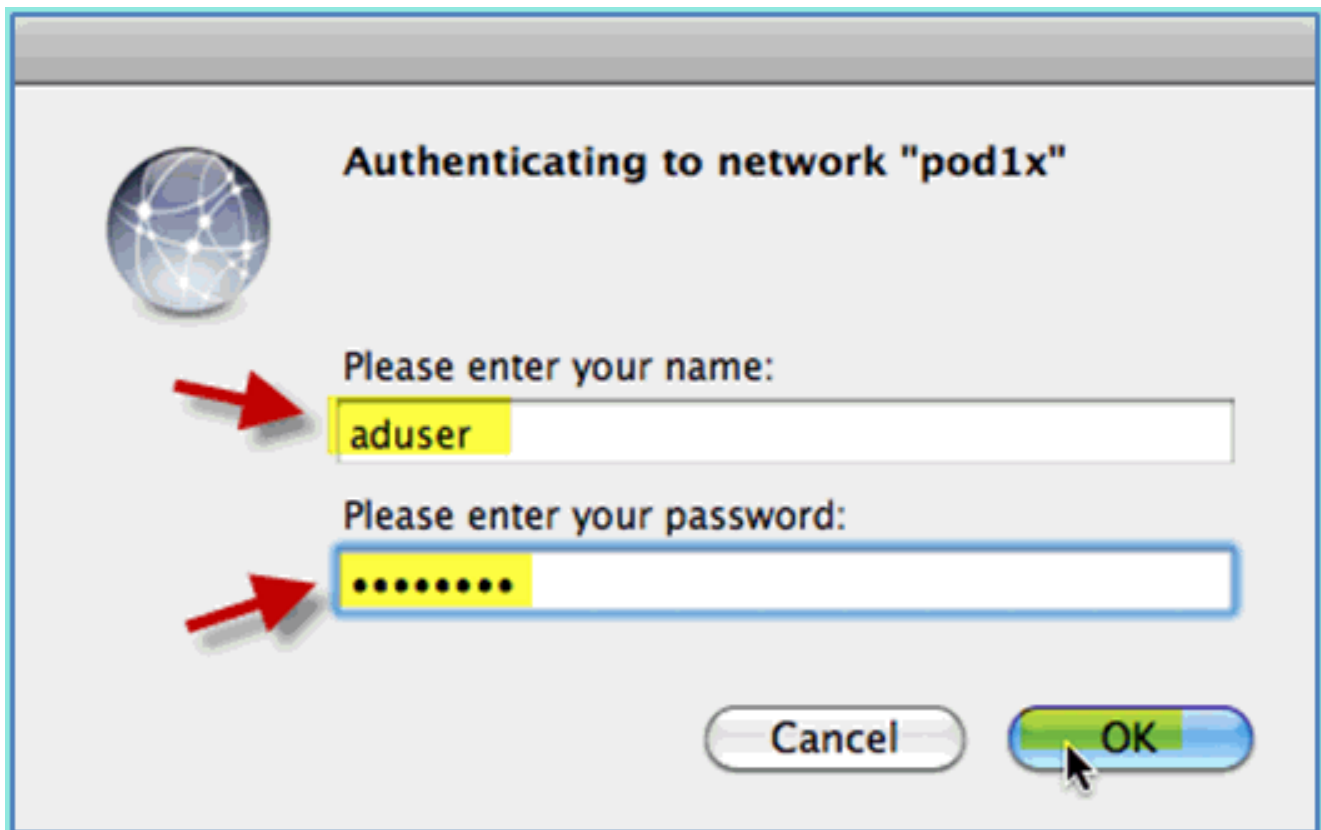


4. 按一下**OK**繼續操作並允許儲存設定。

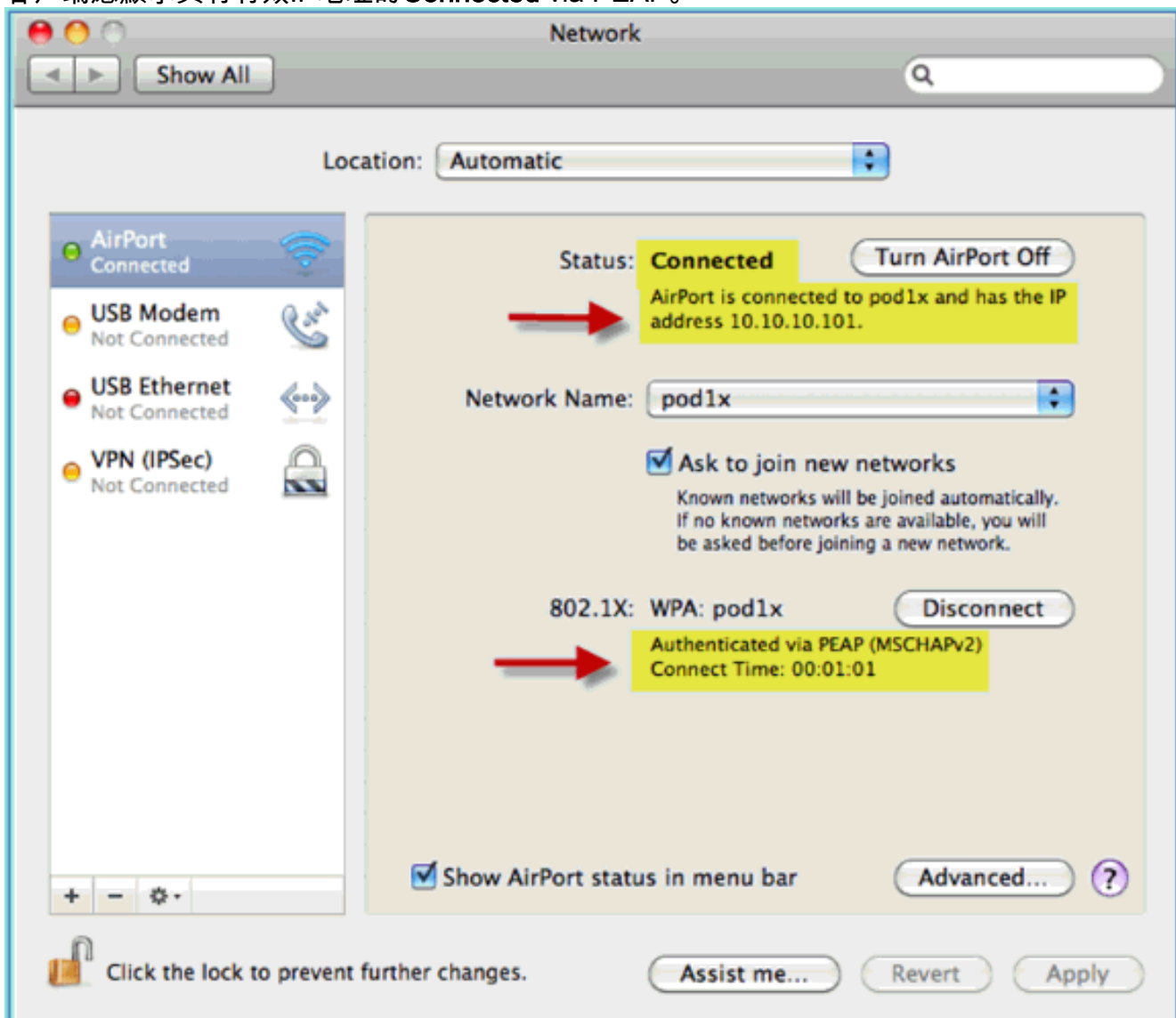
5. 在「Network (網路)」螢幕上，選擇適當的SSID + 802.1X WPA配置檔案，然後按一下**Connect**。



6. 系統可能會提示輸入使用者名稱和密碼。輸入AD使用者和密碼(aduser/XXXX)，然後按一下OK。



客戶端應顯示具有有效IP地址的**Connected** via PEAP。

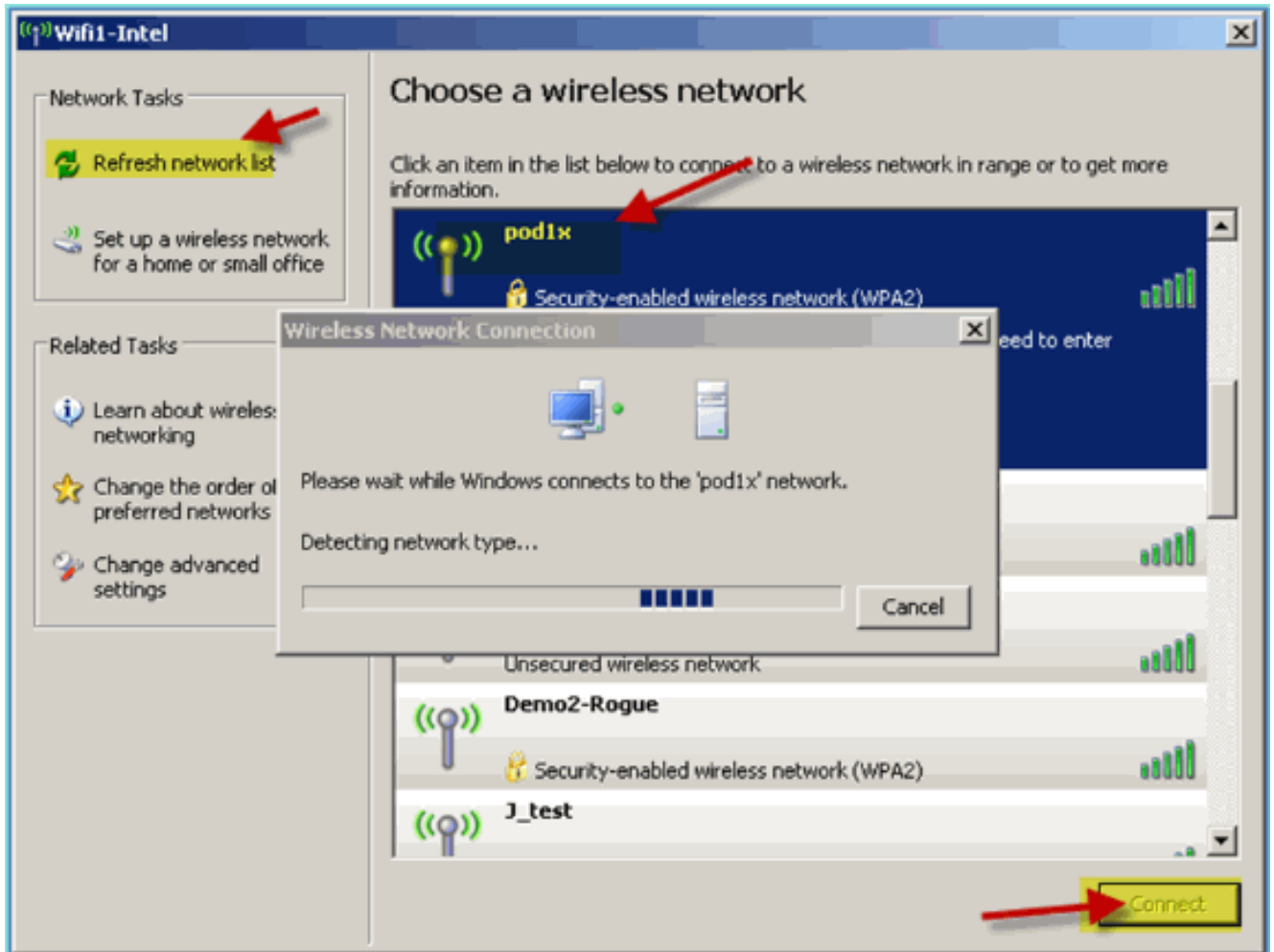


參考：Microsoft Windows XP的無線身份驗證

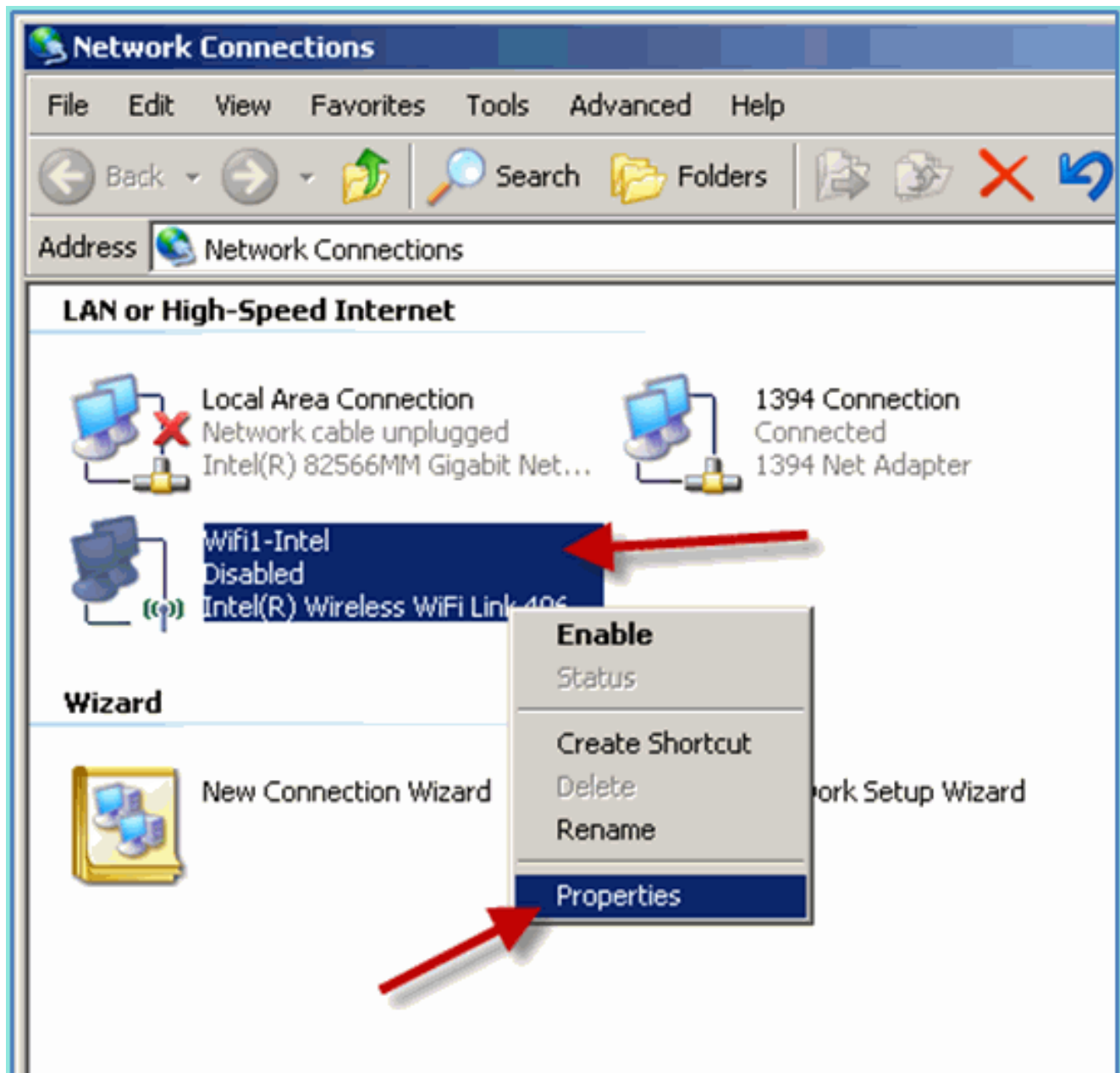
使用Windows XP無線筆記型電腦通過經過身份驗證的SSID作為內部使用者（或整合的AD使用者）與WLC關聯。如果不適用，請跳過。

請完成以下步驟：

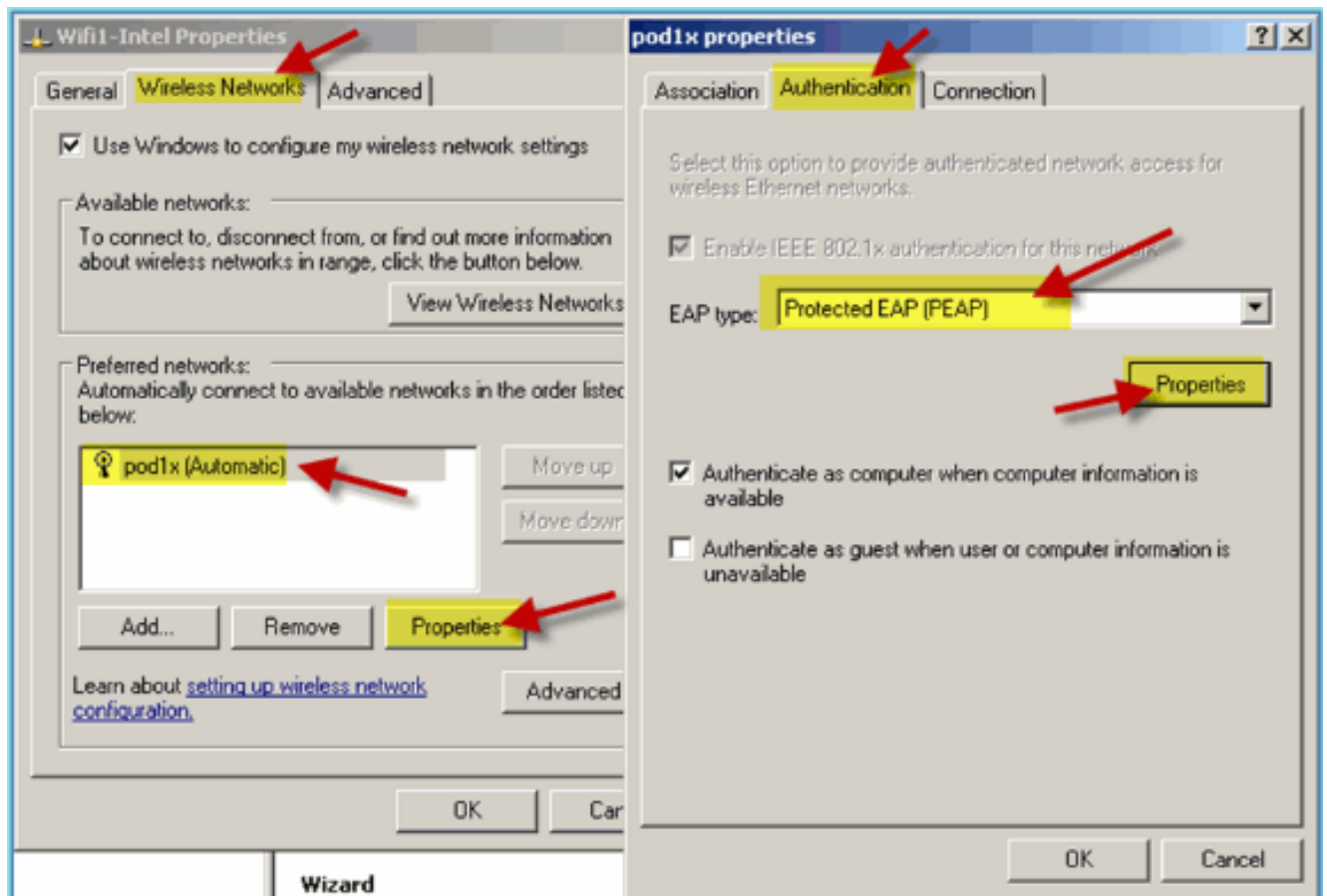
1. 在筆記型電腦上，轉到WLAN設定。啟用WIFI並連線到在上一個練習中建立的啟用802.1X的POD SSID。



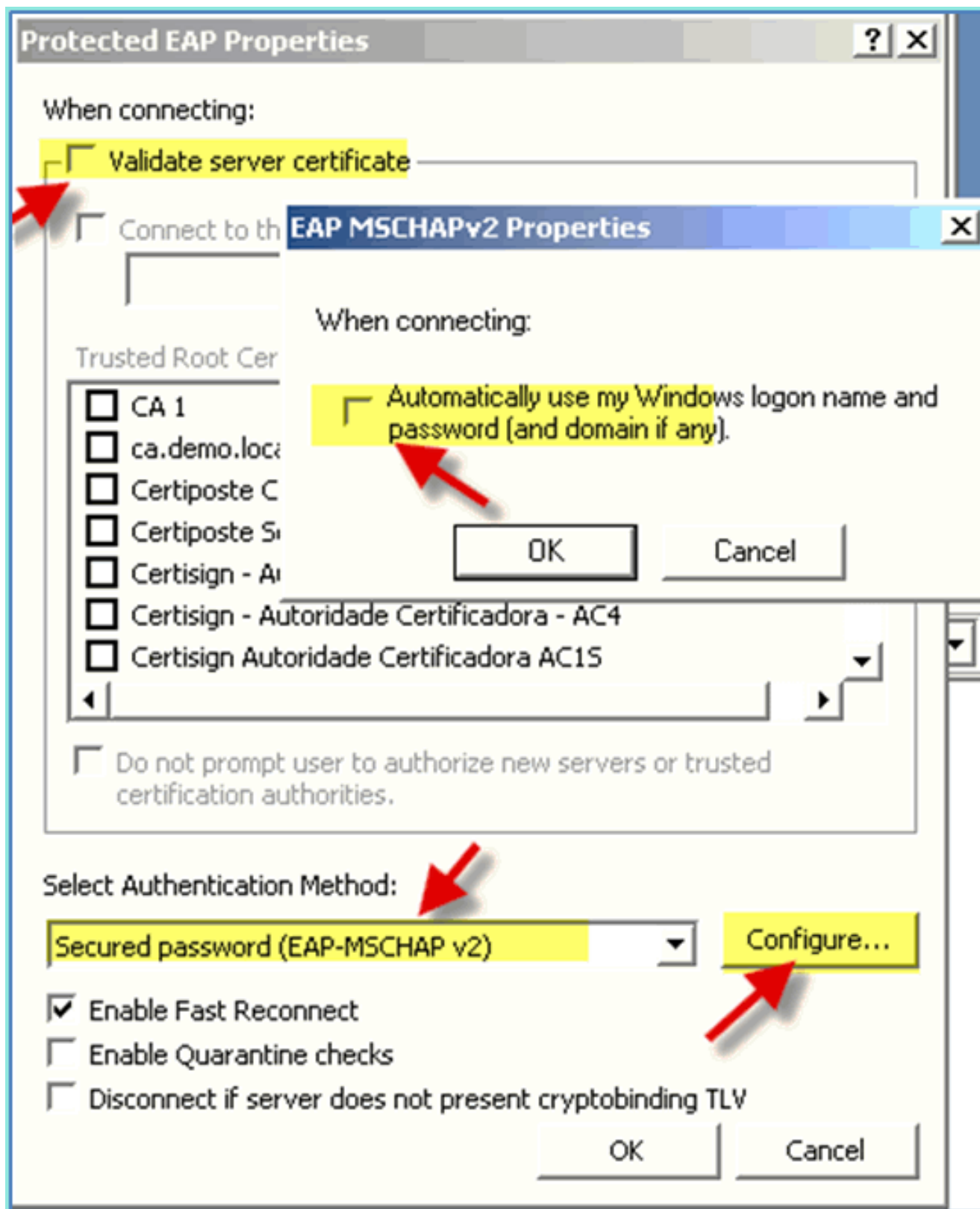
2. 訪問WIFI介面的網路屬性。



3. 導航到無線網路頁籤。選擇Pod SSID網路屬性>身份驗證頁籤> EAP型別=受保護的EAP(PEAP)。



4. 按一下EAP屬性。
5. 設定以下內容：驗證伺服器證書：已禁用身份驗證方法：安全密碼(EAP-MSCHAP v2)

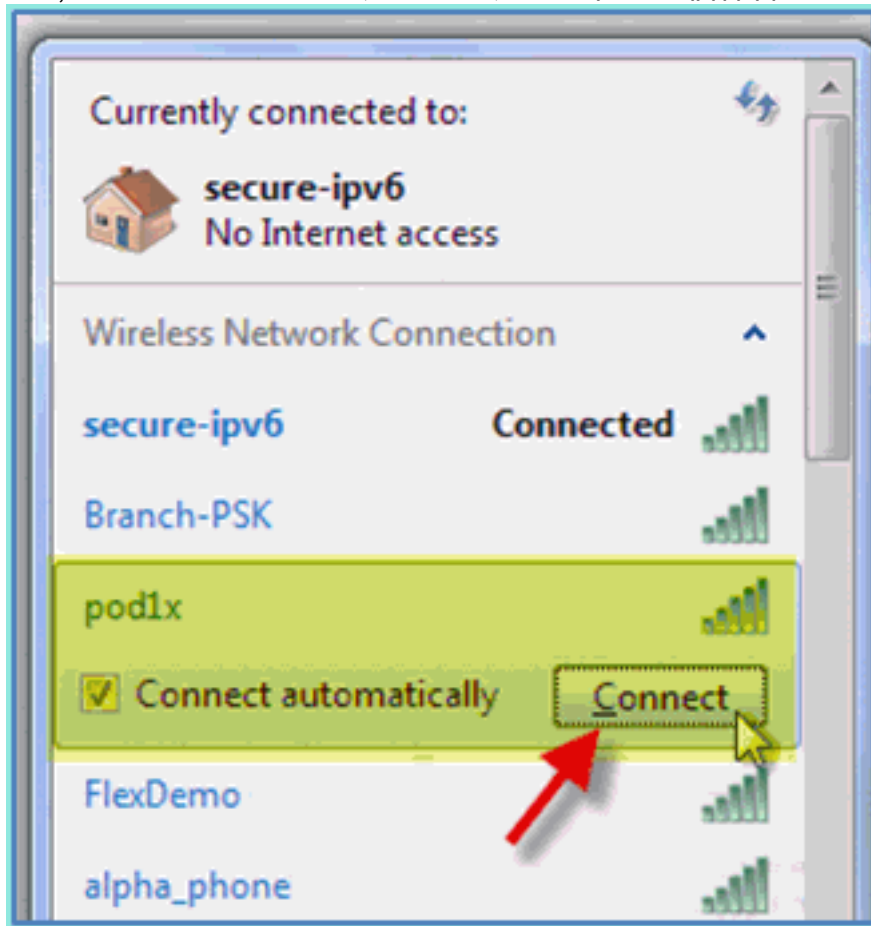


6. 在所有視窗中按一下OK以完成此配置任務。
7. Windows XP客戶端提示輸入使用者名稱和密碼。在本例中，它是aduser/XXXX。
8. 確認網路連線和IP編址(v4)。

[參考：Microsoft Windows 7的無線身份驗證](#)

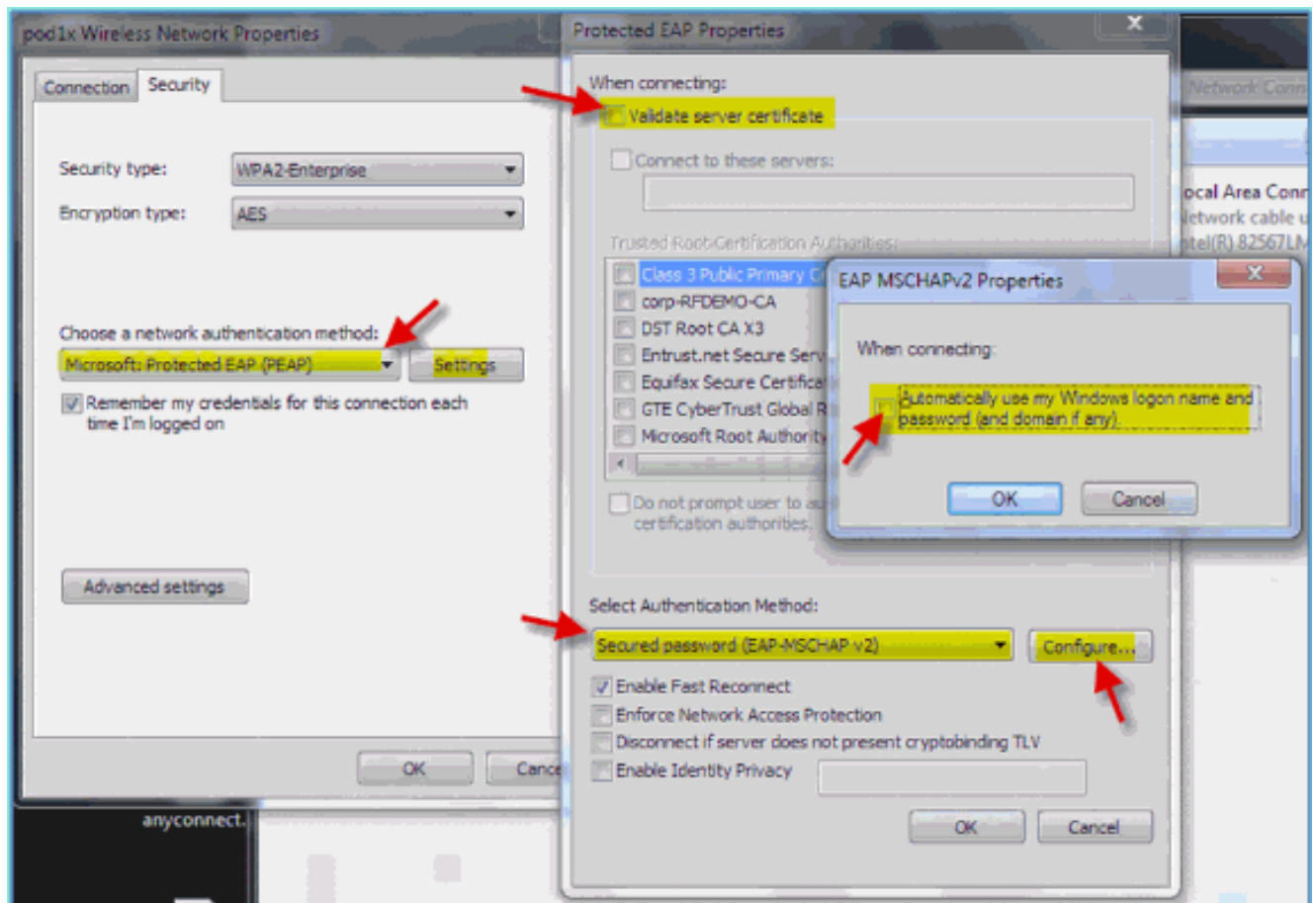
使用Windows 7無線筆記型電腦通過經過身份驗證的SSID作為內部使用者（或整合的AD使用者）與WLC關聯。

1. 在筆記型電腦上，轉到WLAN設定。啟用WIFI並連線到在上一個練習中建立的啟用802.1X的



POD SSID。

2. 訪問Wireless Manager並編輯新的POD無線配置檔案。
3. 設定以下內容：身份驗證方法：PEAP記住我的憑據.....：已禁用驗證伺服器證書（高級設定）：已禁用身份驗證方法（高級設定）：EAP-MSCHAP v2自動使用我的Windows登入.....：已禁用



相關資訊

- [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）。