# 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 <u>配置ISE進行無線身份驗證</u> 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I<u>SE授權配置檔案</u> 為承包商建立ISE授權配置檔案 裝置狀態/分析的授權策略 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

<u>新增Active Directory組</u> <u>新增身份源序列</u> 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

### <u> 簡介</u>

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。

## <u>必要條件</u>

#### <u>需求</u>

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





Name	IP Address	Credential
Vmware Host	10.10.10.2	(Machine used to host the ISE 1.0 MR vmware server files)
Identity Service Engine	10.10.10.70	admin/ default1A
Active Directory/ DNS/ DHCP/ CA Server	10.10.10.10	(Machine used to host Active Directory/ DNS/ DHCP/ CA Server)

#### <u>慣例</u>

如需文件慣例的詳細資訊,請參閱<u>思科技術提示慣例。</u>

## 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。

## <u>無線LAN控制器RADIUS NAC和CoA功能流</u>

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)。
- 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:



#### <u>ISE分析概述</u>

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。



<u>建立內部身份使用者</u>

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。

cisco Identity Services Engi	ne	
A Home Monitor V Policy V	Administration <b>v</b>	
System 🏼 🖓 Identity Manageme	n System	A Identity Management
Identities Groups External	Deployment Licensing	Groups
Identities	Certificates	External Identity Sources

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

💧 Home	Monitor 🔻	Policy 🔻 🚺	dministration	•		
💑 System	And Identity	Management	Network	Resources	🛃 Guest Manag	ement
Identities	Groups	External Iden	tity Sources	Identity So	ource Sequences	Settings
Identities			م چ	Netwo	rk Access Users	nge Status 🔻
Users Endpoint	s		•		1	

💧 Home Monitor 🕶 Policy 🕶 🛛 A	dministration 🔻	
🔆 System 🛛 🖓 Identity Management	Network Resources	🛃 Guest Management
Identities Groups External Iden	tity Sources Identity So	urce Sequences Settings
Identities	Network A	ccess Users > New Network Access User Access User
Users	Name	employee Status
Endpoints	Email	
	▼ Passwo	rd
		* Password
	* Re-En	ter Password
	▼ User Inf	formation

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

Identities	Network Access Users
	/ Edit 🕂 Add 🔯 Change Status 👻 🔂 Impor
♥▼	Status 🔺 Name De
Users	Enabled 🕹 contractor
Endpoints ()	🖸 🖾 Enabled 🖉 employee

## <u>向ISE新增無線LAN控制器</u>

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。

Administration + Policy + Administration +	
🔆 System 🏾 🕂 Identity Management 🛛 🖬 Network P	Resources August Management
Network Devices Network Device Groups External	rnal RADIUS Servers RADIUS Server Sequences SGA AAA Servers
Network Devices	Network Devices List > New Network Device
<u>۹</u>	* Name pod-wic
<b>⊕</b> - ⊗-	Description
Network Devices	
Default Device	* IP Address: 10.10.10.5 / 32
	<b>C</b>
	Model Name
	Software Version
	Network Device Group
	Location All Locations
	Device Type All Device Types Set To Default
🔪 🐪	
	Authentication Settings
	Enable Authentication Settings
	Protocol RADIUS
	Show Show
	SNMP Settings
	Security Group Access (SGA)
	Device Configuration Deployment

- 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。

System       Identity Management       Network Resources       Guest Management         Network Devices       Network Device Groups       External RADIUS Servers       RADIUS Server Sequences       SGA AAA Servers         Network Devices       Imagement       Imagement       Imagement       Imagement         Network Devices       Imagement       Imagement       Imagement         Imagement       Imagement       Imagement       Imagement         Network Devices       Imagement       Imagement       Imagement         Imagement       Imagement       Imagement       Imagement       Imagement         Imagement       Imagement       Imagement <th>🔥 Home Monitor 🔻 Policy 🔻 🗛</th> <th>dministration 🔻</th> <th></th> <th></th> <th></th>	🔥 Home Monitor 🔻 Policy 🔻 🗛	dministration 🔻			
Network Devices       Network Devices       Network Devices       Network Devices         Image: Second sec	System Aldentity Management	Network Resources	E Guest Managemen	t	
Network Devices       Network Devices       Image: Second se	Network Devices Network Device Gr	roups External RADIU	IS Servers RADIUS	Server Sequences SGA	AAA Servers
Image: Construction     Image: Construction     Image: Construction     Image: Construction     Image: Construction       Image: Construction     Image: Construction     Image: Construction     Image: Construction     Image: Construction	Network Devices	Network I	Devices		
Name IP/Mask Location	·	P dit	Add Duplicate	🔂 Import 🛛 🔂 Export 👻	🗙 Deleto 👻
Network Devices	@+	😔 🔪 Name	IP/Mask	Location	
pod-wic 10.10.10.5/32 All Locations	Network Devices	> pod-v	vic 10.10.10.5/	32 All Locations	

## <u>配置ISE進行無線身份驗證</u>

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。

cisco Identity Services Engine	ise admin Log Out Feedba
💧 Home Monitor 🔹 Policy 💌 Administration	ee Task Novigetar
Authentication Authorization Approfiling	🔀 Posture 🔤 Client Provisioning 🔄 Security Group Access 4. Policy Elements
Policy Type O Simple   Rule-Bas	red
* Rule Based	
11 💌 🕶 MAB : H	Wired_MA8 🔶 allow protocols Allowed Protocol : Default Network allow and
E DettX : If	Wired_802.1X - Blow protocols Allowed Protocol : Default Network and ,
🔄 👻 Defsult Rule (If no match) 💠 a	Add All Conditions Below to Library
	Condition Name Expression AND Acid Attribute/Value Acid Attribute/Value Acid Condition from Literary Detete

#### 4. 從條件選擇下拉選單中,選擇**複合條件> Wireless\_802.1X**。

Dot1X : If	Wired_802.1X
Default Rule (If no match) : a	Add All Conditions Below to Library
	Condition Name Expression
	Select Condition
	Compound Condition
	Vired_802.1X
	Wireless_802.1X Switch_Local_Web_A_mentication

#### 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)。

- 🛛	Dot1X	: If	Wired_802.1XA  allow protocols Allowed Protocol : Default Networ  and	
•	Default Rule (If no match)	: a	Add All Conditions Below to Library	<b>1</b>
			Condition Name Expression	OR I
			Wired_802.1X 🕑	OR
			Wireless_802.1X 😒 Acondition to match an 802.1X based authentication reque	

cisi	יוי כס	· 1	den	tity S	ervices Er	ngine					_			
â	н	ome		Monito	or 🔻 🕴 Polic	/ 🔻 🛛 Adi	ministration							
4	Au	ther	nticat	tion	🧕 Authoriza	ation	Profiling	💽 P	osture	🐻 Client Pr	ovisioning	🚍 Sec	urity Group	Access
•	Ru	ile I	Base	Policy ed	/Type 🔿 S	mple 💽	) Rule-Bas	ed		2	22			
	=		•	MAE	9		: If	Wired	_MAB	$\diamondsuit$ all	w protoco	s Allowed	Protocol	Default Net
	1	2	Ŧ	Dot	1X		: If	Wired	802.1X	0 ⇔ allo	w protoco	s Allowed	Protocol	Default Net
				•	Default		:	use	Internal	Users 👄	1			
-			Ŧ	Def	ault Rule (If n	o match)	: all	ow pro	Options If authe If	Identity entication faile user not foun process faile	Source I d Reject d Reject d Drop	nternal Use	irs	

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

#### <u>將WLC連線到網路</u>

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): Ciscol23
   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 dotlq
switchport trunk native VLAN 10
switchport mode trunk
end

### <u>將驗證伺服器(ISE)新增到WLC</u>

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	FEEDBACI			
RADIUS Authentication Server	s > New								
Server Index (Priority)	1 •	1							
Server IP Address	10.10.10.70	10.10.10.70							
Shared Secret Format	ASCII 🔻								
Shared Secret									
Confirm Shared Secret	····· 🔨								
Key Wrap	(Designed fo	r FIPS custome	ers and requires a	key wrap compli	iant RADI	US server)			
Port Number	1812	1812							
Server Status	Enabled 👻	Enabled 👻							
Support for RFC 3576	Enabled 🚽	and the second							
Server Timeout	2 secon	ds							
Network User	🗹 Enable								
Management	🖉 Enable								
IPSec	Enable								

- 3. 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
- 4. 按一下「Apply」以繼續。
- 5. 選擇RADIUS Accounting > Add NEW。

 cısco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	c
Security	RADIUS	Account	ing Servers >	New			
<ul> <li>AAA</li> <li>General</li> <li>RADIUS         <ul> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> </ul> </li> <li>TACACS+         <ul> <li>LOAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disabled Clients</li> <li>User Login Policies</li> <li>AP Policies</li> <li>Password Policies</li> </ul> </li> <li>Local EAP</li> <li>Priority Order</li> </ul>	Server In Server IP Shared S Shared S Confirm S Port Num Server St Server Ti Network U IPSec	dex (Priori Address ecret Form ecret Shared Sec ber atus meout Jser	ty) 2 - 10.10 at ASC •••• 1813 Enab 2 V Er	D.10.70			
Certificate							

6. 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 7. 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:

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

					Sage Configura	stion   <u>P</u> ing   Logout	Retre
CISCO	MONITOR WLANS	CONTROLLER WIRELESS	<u>s</u> ecurity	MANAGEMENT COMM	ANDS HELP	EEEDBACK	
Controller	Interfaces					New.	
General							
Inventory	Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP 1	Management	
Interfaces	management	untagged	10.10.10.5	Static	Enabled		
Interface Groups	virtual	N/A	1.1.1.1	Static	Not Supported		

2. 在WLC中,導覽至**Controller > Interfaces**。輸入以下內容:介面名稱:員工VLAN id: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	0
Physical Information	
Port Number	1
Backup Port	0
Active Port	0
Enable Dynamic AP Mana	gement 🗌
Interface Address	
VLAN Identifier	11
IP Address	10.10.11.5
Netmask	255.255.255.0
Gateway	10.10.11.1
DHCP Information	
Primary DHCP Server	10.10.10
Secondary DHCP Server	

#### 4. 確認已建立新的員工動態介面。

cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	С <u>О</u> ММА
Controller	Interfaces	6					
General Inventory	Interface	Name	,	/LAN Identifier	IP Addres	s Interfac	е Туре
Interfaces	employee		1	11	10.10.11.5	Dynamic	:
Interface Groups	manageme	nt		untagged	10.10.10.5	Static	
Multicast	virtual		1	4/A	1.1.1.1	Static	

### <u>建立WLC訪客動態介面</u>

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

cisco	MONITOR	<u>W</u> LANs		WIRELESS	<u>s</u> ec
Controller	Interfaces	s > New			
General Inventory Interfaces	Interface VLAN Id	Name 🚺	Guest		

- 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	
<b>Physical Information</b>	
Port Number	1
Backup Port	0
Active Port	0
Enable Dynamic AP Managem	ient 🖯
Interface Address	
VLAN Identifier	12
IP Address	10.10.12.5
Netmask	255.255.255.0
Gateway	10.10.12.1
DHCP Information	
Primary DHCP Server	10.10.10.10
Secondary DHCP Server	
Access Control List	
ACL Name	none
Note: Changing the Interface pa temporarily disabled and thus m some clients.	rameters causes the WLANs to be ay result in loss of connectivity for

4. 確認已新增訪客介面。

uluulu cisco		<u>W</u> LANs	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMAN
Controller	Interfaces	6				
General	Interface	Name	VLAN Identifier	IP Address	i Interfac	е Туре І
Interfaces	employee		11	10.10.11.5	Dynamic	1
Interface Groups	quest		12	10.10.12.5	Dynamic	:
Multicast	manageme	nt	untagged	10.10.10.5	Static	
Finternal DHCP Server	virtual		N/A	1.1.1.1	Static	

## <u>新增802.1x WLAN</u>

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。

ականո				Sa <u>v</u> e C	onfiguration <u>P</u> ir	ng Logout	t   <u>R</u> e
	WLANS CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP E	EEDI
WLANs	WLANs					Entries 0	- 0 o
WLANs WLANs	Current Filter: None	[Change F	ilter] (Clear F	ilter)	Create New	Go	
Advanced	WLAN ID Type Pro	ofile Name W	LAN SSID	Admin Status Se	Disable Selected Enable Selected Remove Selected		

2. 對於WLAN,請輸入以下內容:配置檔名稱:pod1xSSID:相同

cisco			WIRELESS	<u>S</u> ECURITY	MANAGEMENT
WLANs	WLANs > New				
WLANS WLANS Advanced	Type Profile Name SSID ID	WLAI pod1: pod1: 1		-	

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

<u>M</u> ONITOR <u>W</u> L	ANs <u>C</u> ON	TROLLER	WIRELESS	<u>S</u> ECURITY
WLANs > Ed	it 'pod1x'			
General	Security	QoS	Advanced	
Profile Nam	e	pod1×		
Туре		WLAN		
SSID		pod1×		
Status		🗆 Enabl	ed	
Security Po	licies	[WPA2] (Modificat	[Auth(802.1X ions done unde	)] r security tab w
Radio Policy	¢.	All	•	
Interface/Ir Group(G)	nterface	manage	ment 💽 🔶	
Multicast VI	an Feature	🗆 Enable	ed	
Broadcast S	SID	🔽 Enable	ed	

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

	MONITOR	<u>W</u> LANs	<u>C</u> ON	TROLLER	WIF	RELESS	<u>S</u> ECUR
	WLANs>	Edit 'po	od1x	b			
	Conoral	Cacuu		O a F	Adus	need	
	General	Secur	ity	Qus	Adad	incea	
	Layer 2	Laye	er 3	AAA Se	ervers		
						-	
	Layer	2 Security	🧕 🚺	PA+WPA2			
				10 MAC Filt	tering		
	WPA+W	PA2 Parai	meter	s			
	WPA I	Policy					
	WPA2	Policy					
	WPA2	Encryption	n	I AES	с Г	ТКІР	
	Auth I	Key Mgmt		802.	1X		and the second s
<sup>.</sup> 802 1X						45	

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

MONITOR	<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS H
WLANs >	Edit 'p	od1x'				
General	Secu	rity QoS	Advanced			
Layer	2 Lay	er 3 AAA Se	ervers			
Select	AAA serve	ers below to ove	rride use of a	lefault serve	rs on this WLAN	
Radius	Servers					
Radi	us Server	Overwrite interfac	e 🗆 Enabled			
			Authentica	tion Servers	Accounting	Servers
			Enabled		Enabled	
Serv	er 1	_	IP:10.10.1	0.70, Port:181	2 💌 IP:10.10.10	.70, Port:1813 👻
Serv	er 2	~	None		<ul> <li>None</li> </ul>	•
Serv	/er 3		None		▼ None	•
Local E	AP Authe	ntication				

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 )						
MONITOR WLANS CONT	ROLLER WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBAC	к
WLANs > Edit 'pod1x'						
General Security	QoS Advanced					
Allow AAA Override	Enabled		DHCP			
Coverage Hole Detection	Enabled		DHC	P Server	Override	
Enable Session Timeout	V 1800 Session Timeout (se	cs)	DHC	P Addr. Assignn	nent 🗖 Required	
Aironet IE	✓ Enabled		Manag	ement Frame	Protection (MFP)	
Diagnostic Channel	Enabled					
IPv6 Enable Z			MFP	Client Protectio	n 🔨 🛛 Optional 💌	
Override Interface ACL	None	*	DTIM P	eriod (in beac	on intervals)	
P2P Blocking Action	Disabled					_
Client Exclusion <sup>2</sup>	Enabled Timeout V	alue (secs)	802	.11a/n (1 - 255) .11b/g/n (1 - 25)	5) 1	_
Maximum Allowed Clients <sup>2</sup>	0		NAC			
Static IP Tunneling 22	Enabled		NAC Load B	State Radius	NAC	

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

WLANs > E	dit 'pod1x			
General	Security	QoS	Advanced	
Profile Na	ame	pod1×		
Туре		WLAN		
SSID		pod1×		¢
Status		Enat	oled	
Security	Policies	۲۶ [WPA2 (Modifica	][Auth(802.1X itions done unde	)] er security tab
Radio Po	licy	All	•	
Interface Group(G)	/Interface )	manag	ement 💌	
Multicast	Vlan Feature	🗆 Enab	led	
Broadcas	t SSID	🔽 Enab	led	

# <u>測試WLC動態介面</u>

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

	Wi-Fi Networks	pod1x	
	Forg	et this Net	work
	IP Address		
	DHCP	BootP	Static
:00. <b>世</b> 军	IP Address		10.10.11.100

4.	確認上一個介面後,將WLAN介	面分配更改為G	uest,然後按	一下Apply。		
	ալալո		- K			
	cisco	MONITOR	WLANS	ONTROLLER	WIRELESS	<u>s</u>
	W/LANS	WI ANS > P	-dit 'pod'	lv'		
	IFE/UIS	ILC/110 / L	- arc pou			
	WLANS	General	Security	QoS	Advanced	
	WLANS					
	Mayanced 1	Profile N	ame	pod1x		
		Туре		WLAN		
		SSID		pod1×		
		Status		🔽 Enabl	led	
		Security	Policies	[WPA2]	[Auth(802.1X	)]
				(Modificat	tions done unde	r se
		Radio Po	dicy	All	-	
		Interface Group(G	e/Interface )	guest		
		Multicast	Vlan Feature	guest		0
		Broadca	st SSID	Manage ✓ Enable	ed	

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

Wi-Fi Networks	pod1x	
Forg	get this Net	work
IP Address		
DHCP	BootP	Static
IP Address	-	0.10.12.102

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





4. 確認iOS裝置正在從管理(VLAN10)介面獲取IP地址。

• AT&T 穼 4:31	PM 📼
Wi-Fi Networks POC	l1x
Forget this	s Network
IP Address	
DHCP Boo	otP Static
IP Address	10.10.10.102
Subnet Mask	255.255.255.0
Router	10.10.10.1
DNS	10.10.10.10
Search Domains	corp.rf-demo.com
Client ID	

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

uluilu cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> O	NTROLLER WIRELE	
Monitor	Clients > Detail		
Summary Access Points	Client Properties		
Cisco CleanAir	MAC Address	5c:59:48:40:82:8d	
Statistics	IP Address	10.10.10.102	
▶ CDP	Client Type	Regular	
Rogues	User Name	aduser	
Clients	Port Number	1	
Multicast	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 🔻 Adminis	tration <b>v</b>				
	Authentications 💆 Alarms 🧮 Reports	💊 Troubleshoot				
	🎡 Add or Remove Columns 👻 🛞 Refresh	li li				
	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 <b>Details</b> 圖示可細化到會話以	以獲取會話的深	【入資訊。			
	վերին					
	cisco Identity Servi	ces Engi	ne			
	브, 🛋 📷					
	Showing Page	1 of 1				
	AAA Protocol > RAD	IUS Auth	entication	) Detail		
	RADIUS Audit Session	ID : 0a0a0;	a050000000	ld4e1e2a	45	
	AAA session ID :	ise/99	967658/11			
	Date :	July	13,2011			
	0	044 4 44 4				
	Generated on July 13, 2	011 4:41:1	IPMPUI			
	Authentication Summa	ry				
	Logged At:	July 13,2	011 4:39:36	.573 PM		
	RADIUS Status:	Authentic	ation succe	eded		
	NAS Failure:					
	Username:	<u>aduser</u>				
	MAC/IP Address:	5C:59:48	:40:82:8D			
	Network Device:	<u>WLC</u> : 10	).10.10.5 :			
	Allowed Protocol:	Default N	etwork Acc	ess		
	Identity Store:	AD1				
	Authorization Profiles:	PermitAc	cess			
	SGA Security Group:					
	Authentication Protocol	: PEAP(EA	AP-MSCHA	Pv2)		

# <u>將狀態重新導向ACL新增到WLC</u>

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」。

ahuhu					Save Config	uration <u>P</u> ing	Logout   <u>R</u> efresh
CISCO MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP FEEDE
Security	Ad	ccess Control	Lists		Ĺ	New	Apply
<ul> <li>▼ AAA</li> <li>General</li> <li>▼ RADIUS</li> <li>Authentication</li> </ul>	En	able Counters				-	
Accounting Fallback TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies							•
Local EAP							
Priority Order							
Ecrtificate							
Access Control Lists     CPU Access Control	Lists						

2. 為ACL提供名稱(ACL-POSTURE-REDIRECT)。

cisco		<u>W</u> LANs		WIRELESS	SECURITY	Me
Security	Access (	Control L	ists > New			
<ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> </ul>	Access C	ontrol Lis	t Name ACL-PO	STURE-REDIR	ECT	

 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	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP
Access 0	Control L	ists > Rules >	Edit				
Sequence	•	1					
Source		Any					
Destination		IP Address		IP Addr 10.10.	ess 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 / 0.0.0.0	10.10.10.70 / 255.255.255.255	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:



#### 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 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any
2	Permit	10.10.10.70 / 255.255.255.255	0.0.0.0 / 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:



- 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 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any
2	Permit	10.10.10.70 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any
3	Permit	0.0.0.0 / 0.0.0.0	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:



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 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any
2	Permit	10.10.10.70 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any
4	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any

11. 儲存目前的WLC組態。

# <u>在ISE上啟用分析探測</u>

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。



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

٩



- 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。
| cisco Identity Services Engine              | -   |                                  |
|---|---|----------------------------------|
| 🔺 Home Monitor 🔻 Policy 🔻 🚺 Administrati    | on The second |                                  |
| 🔆 System 🏼 🌺 Identity Management 🖉 🔤 Netwo  | ork Resources 🛛 🛃 Guest Management  |                                  |
| Identities Groups External Identity Sources | s Identity Source Sequences Setting   | 15                               |
| Identities                                  | Endpoints   |                                  |
|   | 🖊 Edit 🕂 Create 🗙 Delete 👻  | 😢 Import 👻 😰 Export 👻 😽 Filter 👻 |
| @•  | Endpoint Profile  | <ul> <li>MAC Address</li> </ul>  |
| Users                                       | Android   | 40:FC:89:75:64:43                |
| Endponts ()                                 | Apple-Device  | 5C:59:48:40:82:8D                |
|   | Apple-Device  | 44:2A:60:F7:3A:4A                |
|   | Microsoft-Workstation   | 00:21:5C:69:9A:39                |
|   | Microsoft-Workstation   | 00:26:C6:0C:33:56                |
|   | Windows7-Workstation  | 00:1B:21:4D:EE:C0                |
|   |   |                                  |

#### <u>為裝置啟用ISE配置檔案策略</u>

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**。
- 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

cisco Identity Services Engine						
A Home Monitor V Policy V	Administration					
Authentication Suthorization	Refiling	Posture	Client Pro	ovisioning	Security Group A	ccess
Profiling		Profiler Polic	y List > Apple-iP	ad	-	
	P		* Name	Apple-iPa	ad	Des
<b>◆</b> - ■ 1		F	olicy Enabled		8	
👻 🚞 Profiling Policies		* Minimum Ce	artainty Factor	20		(Valir
Android			intunity r doitor	20		
👻 🛃 Apple-Device		* Ex	ception Action	NONE		•
Apple-MacBook				Create Mat	ching Identity Group	
Apple-iPad @			0	Lico Hioror	obu	
Apple-iPhone			0	Use hierard	uny	
Apple-iPod			Parent Policy	Apple-De	evice	-
Applera-Device						

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

cisco Identity Services Engine				
🛕 Home 🛛 Monitor 🔻 🛛 Policy 🔻	Administration	ì <b>v</b>		
Authentication SAuthorization	🛃 Profiling	💽 Posture	🛃 Client Provisionii	ng 🔄 Security Group Access
Profiling		Profiler Policy	List > Android	
<b>∲</b> - ≡ ≡	 ⊛•	P	* Name Andro	id C
Profiling Policies     Android		* Minimum Ce	ertainty Factor 30	~
V Apple-Device		* Exc	eption Action NON	E
Apple-MacBook			Create	Matching Identity Group
Apple-iPhone			O Use His	erarchy
Apple-iPod		*	Parent Policy NON	E

# <u>狀態發現重定向的ISE授權配置檔案</u>

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。

cisco Identity Services Engine		
💧 Home Monitor 🔻 Policy 🕇 Administr	ation	ion 🔻
🛃 Authentication 🛛 S Authorization 🔀 Profil	ling	g 💽 Posture 🔂 Client Provisioning 🔂 Security Group Access
Dictionaries Conditions (Results)		-
Results		Standard Authorization Profiles
	Т	/ Edit Add Duplicate X Delete 🖓 Filter 🗸
		Name     Description
Authentication		Cisco_IP_Phones Profile For Cisco Pho
Authorization     Authorization		DenyAccess Default Network Auth
Cisco_IP_Phones		PermitAccess Default Network Auth
😪 DenyAccess		
😪 PermitAccess		
Downloadable ACLs		
Inline Posture Node Profiles		
Profiling		

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

cisco Identity Services Engine					
Administra	ton 🕶				
🛃 Authentication 💽 Authorization 🔀 Profili	ng 💽 Posture 🙀 Client Provisioning 📑 Security Group Access 🐥 Policy Elements				
Dictionaries Conditions Results					
Results	Authorization Profiles > New Authorization Profile				
<u>ج</u>	*Name Posture_Remediation				
◆- 三 Ξ 容-	Description Permit Access To Posture And Remediation Services; Redirect Traffic To Client Provisioning And Posture				
Authentication     Authentization	Services.				
Authorization Profiles	*Acress Type ACCESS_ACCEPT				
Cisco_IP_Phones					
2 DenyAccess					
Permitaccess     Downloadable ACLs	* Common Tasks				
inline Posture Node Profiles	DACI Narra				
Frotting					
Posture					
Client Provisioning	C Voice Domain Permission				
Security Group Access	Posture Discovery ACL ACL-POSTURE-REDIRECT				
	Contrained Web Authentication				
	Centralized Heb Automation				
	Auto Smart Port				
	* Advanced Attributes Settings				
	ii Select an item 💿 = 💮 🚽				
	* Attributes Details				
	Access Type = ACCESS_ACCEPT tisto-aw-pair = url-redirect+ateACL-POSTURE-REDIRECT cisco-aw-pair = url-redirect+https://pr.8443/guestportal/gateway?sessionid=SessionidValue&action=cpp Sdant Cancel				

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。

CISCO Identity Services Engine	on 🔻		
🛃 Authentication 💽 Authorization 🔀 Profilin	g 🔯 Posture 🔯 Client Provisioning	🚉 Security Group Access	🐥 Policy Elements
Dictionaries Conditions Results			
Results	Standard Authorization Profiles	elete 🛛 🖓 Filber 👻	
<b>∲</b> • <u>≡</u> <u>⊞</u> <u>@</u> •	Name	Description	
Authentication     Authorization	Cisco_IP_Phones	Profile For Clsco Pho	ones.
👻 🚞 Authorization Profiles	DemyAccess	Default Network Aufr	orization Profile with access
Cisco_IP_Phones	Posture Remediation	Permit Access To Pr	voture and Remediation Serv
PermitAccess		1 01111/200800 1011	
Posture_Remediation			

### <u>為員工建立ISE授權配置檔案</u>

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。

cisco Identity Services Engine	
🕼 Home 🛛 Monitor 🔻 🔽 Policy 🔻 🗍 Administra	tion <b>v</b>
🚨 Authentication 🛛 🧔 Authorization 🔀 Profili	ng 👩 Posture 😡 Client Provisioni
Dictionaries Conditions Results	
Results	Standard Authorization Profiles         ✓ Edit       Add       Duplicate         □ Name       Cisco_IP_Phones         □ DenyAccess       PermitAccess

- 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。

Results	Authorization Profiles > New Authorization Profile		
	* Name Employee_Wireless		
♦- ■ "■	Description Full Network Access For Employees		
Authentication			
🔻 🪞 Authorization	* Access Type ACCESS_ACCEPT		
👻 🚞 Authorization Profiles			
Cisco_IP_Phones			
😋 DenyAccess	= Common Toolo		
🚱 PermitAccess	Common Tasks		
Posture_Remediation	DACI Name		
Downloadable ACLs			
Inline Posture Node Profiles	VLAN 11		
Profiling	Voice Domain Permission		
🕨 🚞 Posture	- voice Domain Fernission		
Client Provisioning	Posture Discovery		
Security Group Access	Centralized Web Authentication		
	▼ Advanced Attributes Settings		
	Select an item 🕥 =		
	▼ Attributes Details		
	Access Type = ACCESS_ACCEPT		
	Submitter Cancel		

4. 確認已建立新的員工授權配置檔案。

cisco Identity Services Engine		
🏠 Home 🛛 Monitor 🔻 📴 Policy 💌 🖕 Administratio	n <b>T</b>	
🛃 Authentication 🛛 💿 Authorization 🔀 Profiling	🐼 Posture 🙀 Client Provisioning 🚊 Se	curity Group Access 🔒 Policy Elements
Dictionaries Conditions Results		
Results	Standard Authorization Profiles	
(٩)	🖊 Edit 🕂 Add 🗅 Duplicate 🗙 Delete	₩ Filter ▼
	Name	Description
Authentication	Cisco_IP_Phones	Profile For Cisco Phones.
* Authorization	DerryAccess	Default Network Authorization Profile with acc
Authonization Profiles	Employee Wireless	Full Network Access For Employees
Obruiterass	PermitAccess	Default Network Authorization Profile with acc
Employee_Wireless	Posture_Remediation	Permit Access To Posture And Remediation 8
Permitérose		

## <u>為承包商建立ISE授權配置檔案</u>

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



- 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。

Results	Standard Authorization Profiles
٩ ٠	/ Edit 🕂 Add 🖓 Duplicate 🗙 Delete
�- ≡ ≡ ÷	Name
Authentication	
👻 🚞 Authorization 🥢 🎽	
Authorization Profiles	Contractor_Wireless
	DenyAccess
Downloadable ACLs	
Inline Posture Node Profiles	Employee_wireless
Profiling	PermitAccess
P roming	Desture Remediation
▶ 🚞 Posture	- Posture_remediation

#### <u>裝置狀態/分析的授權策略</u>

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。

Indue Identity Services Engine							
🏠 Home 🛛 Ma	Home Monitor   Policy  Administration						
🔔 Authenticatio	n 👩 Authorization	Ref Profiling	Posture	Client Provisioning	Security Group Access	Policy Elements	
Define the Autho	Define the Authorization Policy by configuring rules based on identity groups and/or other conditions						
First Matched Rule Applies							
* Standard							
Status R	ule Name	Identity	/ Groups	Other Conditions	Pe	rmissions	
Profiled Cisco IP Phones If Cisco-IP 💠 and Condition(s) 💠 then Cisco_IP_Pho 💠							
Cefault If no matches, then PermitAccess							

- 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 態狀態PostureStatus > Equals:未知

	Session
	🔶 - 🗏 📜 🙀
Client Provisioning 📄 Security Group Access	Agent-Request-Type
	CurrentDate
and/or other conditions	CurrentDay
	CurrentMonth
	CurrentTime
	CurrentWeekDay
	CurrentYear
	OS-Architecture
Other Conditions Permissio	U PostureStatus
Session:PostureStatus EQUAL   then Select a	URL-Redirected
Add All Conditions Below to Library	
Condition Name Expression	
Session:PostureStat	Equals 🕞 Unknown 💽

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。

#### <u>測試狀態修正策略</u>

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)。

Administration						
System Addentity Management Network	Resources August Management					
Identities Groups External Identity Sources	Identity Source Sequences Settings					
Identities Endpoints						
<u>(م</u>	/ Edit 🕂 Create 🗙 Delete 👻 Import 🗸	🚱 Export 👻 🖓 Filter 👻				
₽- ₩-	Endpoint Profile	MAC Address				
Users 💿 🕌	Apple-Device	5C:59:48:40:82:8D				
Endpoints 📀 🧮						

- 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。

Endpoint	ts					
🥖 Edit 🕂 Create 🗙 Delete 👻 🎲 Import 👻 🔂					Export 👻	🖓 Filter 🔻
Endpoint Profile				•	MAC Add	ress
Apple-iPhone				5C:59:48:	40:82:8D	

## <u>差異化訪問的授權策略</u>

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。

¥ S	tandard				
	Status	Rule Name	Identity Groups Other Co	nditions Permissio	ns 🚽
1	-	Posture_Remediation	If Any 💠 and Conditi	on(s) $\diamondsuit$ then Posture	_Rem 💠 🔯 Actions 👻
	•	Default	If no matches, then PermitAccess	¢ —	Insert New Rule Above Insert New Rule Below
					Duplicate Above

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

dentity	Services Engin	Identity Groups	Ø						
A Home Monit	or V Policy V	Administration	1 🔻	and the second data		- 			
Authentication	S Authorization	Refiling	Posture	Client Provisio	■ Any	P			
					Endpoint Identity Groups	<b>A</b>			
Define the Authoriza	ation Policy by config	uring rules bas	ed on identity gro	oups and/or other cor	User Identity Groups	7 5			
First Matched Rule	First Matched Rule Applies								
<ul> <li>Standard</li> </ul>									
Status Rule	Status Rule Name K Identity Groups Other Conditio								
Emp	loyee	If A	ny 🧰	and Condition(s)		P			
🛛 🔽 👻 Post	ure_Remediation	lf							

終端身份組:已分析描述:Android、Apple-iPad或Apple-

	Profiled							
	∲- 🗏 🗄	÷						
	Android							
	Apple-iPad							
	Apple-iPhone							
iPhone	Cisco-IP-Phone	э						

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AppleiPhone

Identity Groups	Other Conditions		
Any 🗢 and	Condition(s)		
Apple-iPhone	9	or	-
Apple-iPad	۲	or	-
Android	۲		- +

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

)		
Identity Groups	Other Conditions	Permissions
Apple-IPh $\diamondsuit$ and	Condition(s)	then AuthZ Profile(s)
Any 💠 and		Select Existing Condition from Library (a) as Create New Condition (Advance Option) (b)
o matches, then Permi		

條件>表達式(從清單):InternalUser >名稱

		DEVI	CE	•
		🚞 Gues	t	۲
		🚞 Identi	ityGroup	٠.
Other Conditions	Permissio	intern	alUser	B
Condition(s)	then AuthZ P	Micro	soft	3
		Netw	ork Access	ی 🖢
Add All Conditions Below to	Library	📄 Radiu	IS	۰ 🛓
Condition Name	Expression	- Cana	ian	~ L.
	Select Attribute	9		

InternalUser > Name:員工

Other Conditions	Permissions	
Select Attribute	👄 then AuthZ Profile(s) 🔶	
Add All Conditions Below	v to Library	
Condition Name	Expression	
$\diamond$	InternalUser:Name 🕤 Equals 💽 employee	

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							
Permissions							
AuthZ Profile(s)							
Select an item							
	Standard						
	🔶 - 📃 🔚 🙀 🎡 -						
	Cisco_IP_Phones						
	Contractor_Wireless						
	DenyAccess						
	Employee_Wireless						
	PermitAccess						
	Posture_Remediation						

7. 按一下「Save」。確認已正確新增策略。

▼ Standard								
Status	Rule Name	Identity Groups Other Conditions	Permissions					
-	Employee	Apple-IPh 🔶 and InternalUser:Name EQUALS e 💠	then Employee_Wi <					
-	Posture_Remediation	If Any 🔶 and Session:PostureStatus EQUAL 🔆	then Posture_Rem <					
-	Default	If no matches, then DenyAccess						

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**。

ſ	• Standard					
I	Status	Rule Name	Identity Groups	Other Conditions	Permissions	•
I	1 🛛 🔹	Employee	if Apple-IPh 🔶 and	InternalUser:Name EQUALS e 💠 the	n Employee_Wi	🔶 🏭 Actions 👻
		Posture_Remediation	If Any 🔶 and	Session:PostureStatus EQUAL $\diamondsuit$ the	n Posture_Rem.	Insert New Rule Above Insert New Rule Below
		Default	If no matches, then Der	yAccess 💠	-	Duplicate Above Duplicate Below

 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:

v Stan	tracto							
Sta	atus	Rule Name	ld	lentity Groups		Other Conditions		Permissions
1	- 1	Employee	п I	Apple-iPh 💠	and	InternalUser:Name EQUALS e	↔ then	Employee_Wi
	- 1	Employee_copy	1 H 🗸	Apple-iPh 🔶	and	InternalUser:Name EQUALS e	🗘 then	Employee_Wi 🔶
	•	Posture_Remediation	1 If 🖌	Any 💠	and	Session:PostureStatus EQUAL	. 🗘 ten	Posture_Rem 💠
		Default	If no r	matches, then	Deny/	Access 💠		
 . 按-	┛ - 下「	Default 「 <b>Save</b> 」。確認以前	∎ f的複	matches, then [ 製副本(或	Deny/ 成新贫	Access ↔ 策略)配置正確。		
. 按一	┛ ァ 一下「 tandard	Default 「Save」。確認以前	┃ <b># no</b> i 前的複	matches, then [ 製副本(或	Deny/ 战新闭	Access		
. 按-	┛ ァ 一下「 tandard Status	Default Save」。確認以前 Rule Name	╹nor f的複 k	matches, then [ 製副本(或 Jentity Groups	Deny/ 戊新贫	Access	P	<sup>2</sup> ermissions
. 按一	2 ▼ 一下「 tandard Status	Default Save」。確認以前 Rule Name Employee	」 <b>* no</b>	matches, then [ 製副本(或 Jentity Groups Apple-IPh 今	Deny/ 戊新贫	Access	P ¢ then	Permissions Employee_Wi 💠
. 按一	□ ▼ 一下「 tandard Status □ ▼	Default Save」。確認以前 Rule Name Employee	前的複 " 」" 」"	matches, then [ 製副本(或 Sentity Groups Apple-iPh 令 Apple-iPh 令	Deny/ 戊新分 and [ and [	Access 策略)配置正確。 Other Conditions InternalUser:Name EQUALS co	P \$ then	Permissions Employee_Wi $\diamondsuit$ Contractor_W $\diamondsuit$
. 按一 ▼ St	□ ▼ - 下「 tandard Status □ ・ □ ・	Default Save」。確認以前 Rule Name Employee Contractor Posture_Remediation		matches, then [ 製副本(或 Sentity Groups Apple-iPh ◇ Apple-iPh ◇	Deny/ 戈新分 and [ and [ and ]	Access 家略)配置正確。 Other Conditions InternalUser:Name EQUALS co InternalUser:Name EQUALS co Session:PostureStatus EQUAL	P	Permissions Employee_Wi

11. 要預覽策略,請按一下Policy-at-a-Glance。

ientity se	IVICES EII	Ψ.L		TLC.	w l	iue		JEIV	ICCS LIL.	<u></u>
						ise	adr	nin	Log Out	Feedback
								00	Task Nav	vigator 👻 🕗
灵 Client f	Provisioning	📑 S	ecurity Group	Acces	is 🔒 Polic	y Eleme	nts			
								-		-
s and/or o	ther condition	ns						P	Policy A	AGlance
								1	Ì	<u> </u>
						-				
Other	Conditions				Permissions					
d Inter	nalUser:Nam	e EQUA	LS e 🔶	then	Employee_	<b>Wi</b> <	>		🚔 Acti	ons 👻
d Inter	nalUser:Nam	e EQUA	LS co 🔶	then	Contractor_	_w <	Þ	[	🚔 Acti	ons 👻
							_			
╵朿略熌	覓」忸倪提	供東總	的束略摘要	和易於	·	)				
Authorization First Matched	Policy At A Glance Rule Applies									
Exceptions										
Status	Rule Name	ld	entity Groups		Other Conditions				Perm	nissions
Standard										
Status	Rule Name	II.	entity Groups		Other Conditions				Perm	nissions

	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
1	Enabled	Posture_Remediation	Any	Session:PostureStatus EQUALS Unknown	Posture_Remediation
l	Enabled	Default	Any		DenyAccess

# <u>測試CoA以區分訪問</u>

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



Wi-Fi Networks	pod1x	
Forge	et this Netv	vork
IP Address		
DHCP	BootP	Static
IP Address	1	0.10.11.100
Subnet Mas	<b>k</b> 25	5.255.255.0
Router		10.10.11.1
DNS		10.10.10.10

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。



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)。

cisco		WLANs C	ONTROLLER	WIRELESS	<u>S</u> ECURITY	Mį
WLANs	WLANs > E	Edit 'pod	1x'			
WLANS	General	Security	QoS	Advanced		
Advanced	Profile Na	ame	pod1x	podix		
	Туре		WLAN	AN		
	SSID		pod1x			
	Status		Enabled			
	Security	Policies	[WPA2	][Auth(802.1X	)]	will a

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

Enter the Cancel Ent	e password for "pod1x" er Password
Username	contractor
Password	•••••••
Mode	Automatic >
1234	567890

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)。

Wi-Fi Networks	pod1x							
Forget this Network								
IP Address								
DHCP	BootP	Static						
IP Address		10.10.12.100						
Subnet Mask	<b>x</b> 2	255.255.255.0						
Router		10.10.12.1						

(員工、承包商)在不同的VLAN中獲得不同的授權配置檔案

Home Monitor V P	aloy 🕶	Administr	ation v					
Authentications 💆 Alarms 🛒 Reports 🔪 Troubleshoot								
🙀 Add or Remove Columns	🕶 🛞 Ri	afresh				Ru	afresh Every 3 second	s 💽 Show Lat
Time	Cintur	Datala	Usemame	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles
title.	• Glaida	Lietara						
Aug 02,11 03:40:18.331 PM	×	ò	employee	50:59:48:40:82:80		.wic		Employee_Wireless
Aug 02,11 03:36:33.663 PM	<b>~</b>	à	contractor 🚍	5C:59:48:40:82:8D		.wic		Contractor_Wireless
A	-					and a		



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

cisco	MONITOR WLANS CON	NTROLLER WIRELESS SECUR
WLANs	WLANs > New	
WLANS WLANS Advanced	Type Profile Name SSID ID	WLAN  pod1guest 2

- 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

	<u>V</u> LANS <u>C</u> OI	NTROLLER	WIRELESS	<u>s</u> ecur					
WLANs > Edit   ' <mark>pod1guest</mark> '									
General	Security	QoS	Advanced						
Profile Na Type SSID Status	me	podigue WLAN podigue	est est l <b>ed</b>						
Security F	olicies	[WPA2] (Modifica	][Auth(802.1X tions done unde	)] r security					
Radio Poli	су	All	•						
Interface/ Group(G)	'Interface	guest	•	-					
Multicast	Vlan Feature	🗖 Enabl	ed						
Broadcast	SSID	🔽 Enabl	ed						

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

<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONT	ROLLER	WIREL	ESS	<u>S</u> ECURIT			
WLANs >	WLANs > Edit 'pod1guest'								
General	Secu	rity	QoS	Advanc	ed				
Layer	2 Lay	ver 3	AAA S	ervers					
Laye	er 2 Securit	y <u>∮</u> N	one		- 1	-			
			10MAC Fi	tering					

- 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

M		LANS CON	TROLLER	WIRELESS	SECURITY	MANAGEMENT
٧	VLANs > E	dit 'pod1g	juest'			
	General	Security	QoS	Advanced		
	Layer 2	Layer 3	AAA Se	ervers		
	Layer 3	Security No	ine 🗘	-		
-	🔶 🗹 Wel	b Policy <sup>1</sup>				
	<ul> <li>Auth</li> </ul>	entication				
	O Pass	through				
	O Cond	ditional Web Re	direct			
	🖯 Spla	sh Page Web R	edirect			
	O On M	IAC Filter failu	re <sup>11</sup>			
	Preautho	entication ACL		-POSTURE-R	EDIRECT 🛟	-
	Over-rid	e Global Confi	g 🗹 En	able 🛑		<b>2</b>
	Web Aut	th type	(E	xternal(Re-di	rect to external s	server)
		ttps://10.10.1	0.70:8443/	guestportal/L	ogin.action	

- 7. 按一下「Apply」。
- 8. 請確保儲存WLC組態。

## <u>測試訪客WLAN和訪客門戶</u>

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

o



#### 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:

 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。

	A Home Monitor - Policy -	Administration	-	-		
	🔆 System 🏼 🖓 Identity Managem	ent 🔛 Networ	k Resources	🛃 Guest N	lanagement	
	Identities Groups External	Identity Sources	Identity So	urce Sequen	ces Setting	gs
	Identity Groups	٩	User Ident	ity Groups > S Froup	ponsorAllAccou	nt
		<u>ي</u> .	* Nam	Sponso	rAllAccount	
	Endpoint Identity Groups		Descriptio	Default	Sponsor Identi	ty Group
			Save Member	Reset		
			Users			
				<b>~</b> × D	elete 🔻	
					-	
			User	5		٩
		1	¢-			
			<u>2</u> co	ontractor		
		1	🤶 er	nployee 👆		
2. <sup>3</sup>	尊航到 <b>管理&gt;訪客管理&gt;發起人維</b>	l。				
	illulu Identity Services Eng	ine				
	A Home Monitor - Policy -	Administration •				
	System Manageme Identities Groups External	System Deployment Licensing		<u>19</u> 8	Identity Manager Identities	gement
	Identity Groups	Certificates			External Identit	ty Sources
	(*	Logging			Identity Source	Sequences
	<b>∲</b> - <b>≡ ≡</b>	Operations	00		Settings	
	User Identity Groups	Settings	55	4	Guest Manage	ement
	Endpoint identity Groups			-	Sponsor Group	Policy
		Network De	vices		Settings	
		Network De	1003		Journas	

3. 按一下Edit,然後選擇SponsorAllAccounts。

dentity Services Engine				
💧 Home	Monitor 🔻 Poli	cy 🔻 🕴 Ad	dministration 🔻	
🔆 System	👰 Identity Mana	agement	🔛 Network Resources	🛃 Guest Management
Sponsor Group Policy Sponsor Groups Settings				
Guest Spon	sui Groups			
💙 Edit 🚽	Add 🔀 Delet	te 🍸 Filt	er 🔻	
🗖 Sponso	or Group Name	•	Description	
Sponso	orAllAccounts 🔩		Default SponsorGroup	
🗖 Sponso	orGroupGrpAccoun	its	Default SponsorGroup	

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

dentity Services Engi	ne			
🛕 Home Monitor 🔻 Policy 🔻	Administration <b>v</b>			
🔆 🔆 System 🛛 🏄 Identity Managem	ent 🔛 Network Resources 🛃 Guest Management			
Sponsor Group Policy Sponsor	Sponsor Group Policy Sponsor Groups Settings			
Sponsor Group List > SponsorAllAccounts				
	v 7			
General Authorization Leve	Guest Roles Time Profiles			
Contrait Provident Cont				
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)			
Save Reset				

5. 按一下「Save」以完成此任務。

## <u> 贊助訪客</u>

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:

 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。

cisco Sponsor Port	al
Home Settings Customization	Sponsor Portal: Getting Started
	View All Guest User Accounts
	Create Single Guest User Account
View Guest Accounts Create Multiple Accounts	Create Multiple Guest User Accounts

3. 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	
mization	Create Guest Account	
	First Name: Sam	
	Last Name:	
defense and	Email Address:	
	Phone Number:	
and the second se	Company:	
	Optional Data 1:	
	Optional Data 2:	
	Optional Data 3:	
	Optional Data 4:	
gement	Optional Data 5:	
counts Accounts	🜣 Group Role: Guest ≑	
n Accounts s	Contraction Contra	
	• Timezone: EST	
	✿ = Required fields	
	Submit	

- 4. 按一下「Submit」。
- 5. 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\*\*\*。
- 6. 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)。

Account Management	t > View All Guest Accounts > Create Guest Account
Cura	eastully Created Cuest Assount sigm0002
Succ	essiuny created Guest Account slamoouz
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
Timezon	e: 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

### <u>測試訪客門戶訪問</u>

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。

### <u> 憑證組態</u>

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」。

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

### Welcome

Use this Web site to request a certificate for your Web browser, eyour identity to people you communicate with over the Web, sign a you request, perform other security tasks.

You can also use this Web site to download a certificate authority ( (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services,

### Select a task:

Request a certificate View the status of a pending certificate request 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)。

Microsoft Active Directory Certificate Services corp-RFDEMO-CA
Download a CA Certificate, Certificate Chain, or CRL
To trust certificates issued from this certification authority, insta
To download a CA certificate, certificate chain, or CRL, select
CA certificate:
Current [corp-RFDEMO-CA]
© DER
C Base 64
Download CA certificate
Download CA certificate 2hain
Download latest delta CRL

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

cisco Identity Services Engi	ne
💧 Home 🛛 Monitor 🔻 Policy 🔻	Administration
Metrics	🔆 System Deployment
Active Endpoints	Licensing
0 –	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。

cisco Identity Services Engine		ise admin Li
Administra		
🔆 System 🖉 Identity Management 🖉 Net	ork Resources 🛃 Guest Management	
Deployment Licensing Certificates L	gging Operations Admin Access Settings	
Certificate Operations	Certificate Authority Certificates	
Local Certificates	🖊 Edit 🕂 Add 🔀 Export 🗙 Delete	
Certificate Signing Requests	Friendly Name     Expiration	Issued To
ger Certificate Automity Certificates	ise.corp.rf-demo.com Thu Jul 12 12:14:47 PDT 2012	ise.corp.rf-demo.com

- 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 > Ge   Generate Certificat	nerate Certificate Signing Request e Signing Request
Certificate	
* Certificate Subject	CN=ise.corp.rf-demo.com
* Key Length	2048
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。



- 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」)。



- 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 brow communicate with over the Web, sign and encrypt message

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

For more information about Active Directory Certificate Ser

### Select a task:

Request a certificate

View the status of a Centificate request

Download a CA certificate, certificate chain, or CRL



22. 將CSR內容貼上到「儲存的請求」欄位中。

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.



23. 選擇Web Server作為證書模板,然後按一下Submit。

Microsoft Activ	e Directory Certificat
Microsoft Active	Directory Certificate Services corp-RFDEMO-CA
Submit a Certi	ficate Request or Renewal Request
To submit a say source (such as <b>Saved Request:</b>	ved request to the CA, paste a base-64-encoded CN a Web server) in the Saved Request box.
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	gA/MMZsTIoEPekcunnm+ZFt1AXajB32uwHH.11c9 ▲ J4qsQM7KEYOpQt4biaO71S8Lm6BBTk9mRhiTBwSF kSa7LHYgkgLRYBnpu15RjQ7wWijArH8cK1OrVT42 LPKQ72N2XYIXfu0jdgoaJjmsk6T9nLABVYQ6nKQx V5QYBOjTYHXIPG8/ned9z3M0iZd2sm4XNS2bJfO/ END CERTIFICATE REQUEST
Certificate Temp	late:
	Web Server
Additional Attribu	utes:
Attributes:	
	Submit >

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



- 25. 將檔案儲存到已知位置(例如下載)
- 26. 轉至Administration > System > Certificates > Certificate Authority Certificates。

cisco Identity Services Engine		
💧 Home Monitor 🔻 Policy 🔻	Administration	
Metrics Active Endpoints 0 - 24h • System Summary	System Deployment Licensing Certificates Logging Operations Admin Access Settings	

27. 按一下Add > Bind CA Certificate。



#### 28. 瀏覽到先前下載的CA憑證。

cisco Identity Services Engine	
Administration	
🔆 System 🖉 Identity Management 📲 Network	Resources 🛃 Guest Management
Deployment Licensing Certificates Log	ging Operations Admin Access Settings
Certificate Operations	Local Certificates > Bind CA Signed Certificate
Certificate Authority Certificates	* Certificate File C:\Users\paul\Downloads\certnew.cer Browse_
	Protocol     EAP: Use certificate for EAP protocols that use SSL/TLS tunneling     Management Interface: Use certificate to authenticate the web server (GUI)
	Override Policy Replace Certificate Cert
	Submit

- 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。

olicy  Administration	Y	
nagement 🔛 Network	Resources 🛛 🛃 Guest Management	
Certificates Log	ging Operations Admin Access Settings	
	Local Certificates	
	🖊 Edit 🕂 Add 🐼 Export 🗙 Delete	
stae	Friendly Name 🔺 Issued To	Issued By
0.05	ise.corp.rf-demo.com ise.corp.rf-demo.com	ise.corp.rf-demo.com
	ise.corp.rf-demo.com ise.corp.rf-demo.com	corp-RFDEMO-CA
	13	

## <u>Windows 2008 Active Directory整合</u>

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。

s Engine	)	
Policy 🔻	Administration 🔻	
	System Deployment	Identity Management
	Licensing	Groups
	Certificates	External Identity Sources
	Logging	Identity Source Sequences
24h 🔻	Operations	Settings

- 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

cisco Identity Services Engine	
🛕 Home Monitor 🔻 Policy 🔻 🗖 Adm	inistration •
System 🔤 Identity Management	Network Resources 🔣 Guest Management
Identities Groups External Identity	Sources Identity Source Sequences Settings
External Identity Sources	Active Directory > AD1
Certificate Authentication Profile	Server Connection
LDAP	To configure Active Directory:
RADIUS Token	First enter the required fields: the Domain Name to connect to and the Identity Store Name pages, and click submit to commit the Active Directory configuration to all nodes in the IS     After the configuration has been submitted, then Join or Leave operations must be performed.
	* Domain Name Corp.rf-demo.com
	Local Node Status No Active Directory Configuration is Set

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

* Domain Name	corp.rf-demo.com		Connection
dentity Store Name ocal Node Status	AD1	Set	Test Connection × * User Name: aduser
ettings			* Password:

- 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。

atus: Test Succeeded	
Show Detailed Log. (Note: May contain sensitive information such as passwords.)	
Executed with privileges of root adinfo (CentrifyDC 4.3.0-192)	
Host Diagnostics uname: Linux ise 2.6.18-238.1.1.el5PAE #1 SMP Tue Jan 4 13:53:16 EST 2011 i686 OS: Red Hat Enterprise Linux Server Version: 5.4 (Tikanga) Number of CPUs: 2	
P Diagnostics Local host name: ise Local IP Address: 10.10.10.70 FQDN host name:ise.corp.rf-demo.com	
Domain Diagnostics: Domain: corp.rf-demo.com Subnet site: Default-First-Site-Name	
	J.

7. 按一下「Save Configuration」。

	* Domain Name corp.rf-demo.com Test Connection * Identity Store Name AD1 Local Node Status No Active Directory Configuration is Set
	▼ Connection Settings
	<ul> <li>Enable Password Change</li> <li>Enable Machine Authentication</li> <li>Enable Machine Access Restrictions</li> <li>Aging Time (hours)</li> <li>(Valid Range 1 to 8760)</li> </ul>
	Save Configuration Join Delete Configuration
8.	按一下「 <b>Join</b> 」。輸入AD使用者(管理員/Cisco123),然後按一下 <b>OK</b> 。
	* Domain Name corp.rf-demo.com Test Connection * Identity Store Name AD1 Local Node Status Not Joined to a domain
	T Connection Settings
	<ul> <li>✓ Enable Password Change</li> <li>✓ Enable Machine Authentication</li> <li>✓ Enable Machine Access Restriction</li> <li>Aging Time (hours)</li> </ul>
	Save Configuration Join Delete Configuration

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。

	Identity Source Sequences Settings
1	Active Directory > AD1         Connection       Groups       Attri         Join Domain       ×         Server Connection       Status:       Join Operation Succeeded
	<ul> <li>First enter the required field pages, and click submit to c</li> <li>After the configuration has been submited, men com or Leave operations must be performed on a submited of the configuration has been submited.</li> </ul>
	* Domain Name corp.rf-demo.com Test Connection     * Identity Store Name AD1      Local Node Status Joined to Domain: corp.rf-demo.com Connection Status: CONNECTED

### 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

 $\top \mathbf{Retrieve \ Groups}_{\circ}$ 

This dial Use * for Domain: Filter:	log is used to select groups from the Directory. Click r wildcard search (i.e. admin*). Search filter applies corp.rf-demo.com *	k <b>Retrieve Groups</b> to re to group name and not t
Domain: Filter:	corp.rf-demo.com * Retrieve G	
	me	Number of Gro
	rn rf.demo.com/ilisers/Dnel IndateBrow	
	Ip.in-demo.com/osers/Dirsopdaterioxy	
L co	rp.rf-demo.com/Users/Domain Admins	
🗆 co	rp.rf-demo.com/Users/Domain Computers	
<b>—</b>	rn rf-demo comil IsersiDomain Controllers	
	p.n-demo.com/osers/Domain Controllers	
L co	rp.rf-demo.com/Users/Domain Guests	
C co	rp.rf-demo.com/Users/Domain Users	
C co	rp.rf-demo.com/Users/Employee	
🗆 co	rp.rf-demo.com/Users/Enterprise Admins	
_		
† Domai	n Users和Employee組的框。完成後按一下OK。	
corp.ri-de	mo.com/osers/Domain Computers	GLOBAL
corp.rf-de	mo.com/Users/Domain Controllers	GLOBAL
corp.rF.de	mo.com/lisers/Domain Lisers	GLOBAL
corp.rf-de		GLOBAL
corp.rf-de	mo.com/Users/Enterprise Admins	UNIVERSAL
corp.rf-de	mo.com/Users/Enterprise Read-only Domain Controllers	UNIVERSAL
corp.rf-de	mo.com/Users/Group Policy Creator Owners	GLOBAL
corp.rf-de	mo.com/Users/RAS and IAS Servers	LOCAL
corp.rf-de	mo.com/Users/Read-only Domain Controllers	GLOBAL
corp.rf-de	mo.com/Users/Schema Admins	UNIVERSAL
	COL COL COL COL COL COL COL COL COL COL	Corp.rf-demo.com/Users/Domain Admins corp.rf-demo.com/Users/Domain Computers corp.rf-demo.com/Users/Domain Controllers corp.rf-demo.com/Users/Domain Guests corp.rf-demo.com/Users/Domain Users corp.rf-demo.com/Users/Employee corp.rf-demo.com/Users/Employee corp.rf-demo.com/Users/Enterprise Admins Domain Users和Employee組的框。完成後按一下OK。 Corp.rf-demo.com/Users/Enterprise corp.rf-demo.com/Users/

6. 確認已將這些組新增到清單中。

dentity Services Engine							
💧 Home	Monitor 🔻	Policy 🔻	Administration	•			
🔆 System	Identity	Managemen	t 🔛 Network	Resources	🛃 Guest Management		
Identities	Groups	(External Id	entity Sources	Identity So	urce Sequences Settir	ngs	
External Identity Sources						tes	
RADIUS T	oken urlD		•	C corp.	rf-demo.com/Users/Domai rf-demo.com/Users/Emplo	in Users yee	

# <u>新增身份源序列</u>

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。

cisco Identity Services Engin	e 💋						
🛕 Home Monitor 🔻 Policy 🔻	Administration •						
System Vertication Profile	Identity Management       Deployment       Licensing       Certificates       Logging       Operations       Admin Access	igement tity Sources ie Sequences					
2. 按一下「 <b>+Add</b> 」以新增序號。							
cisco Identity Services Engine							
Admitter ▼ Policy ▼ Admit	nistration 🔻						
🔆 System 🖉 Identity Management 📱	Network Resources 🛛 🛃 Guest Management						
Identities Groups External Identity	Sources (Identity Source Sequences) Settings						
Identity Source Sequences							
/ Edit -Add Duplicate X Dele	de 🖓 Filter 👻						
□ Name	<ul> <li>Description</li> </ul>	Identity Stores					
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					

### 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									
· Identity Source Sequence									
* Name AD_Internal									
Description									
▼ Certificate Based Authentication									
Select Certificate Authentication Profile									
▼ Authentication Search List									
Available Available Selected AD1 Internal Users Internal Endpoints Available AD1 Internal Endpoints Available AD1 Internal Users Internal Endpoints Available AD1 Internal Endpoints Available AD1 Internal Endpoints Available AD1 Internal Endpoints Available Available AD1 Internal Endpoints Available Ava									
Select the action to be performed if a selected identity store cannot be accessed for authentication <ul> <li>Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError</li> <li>Treat as if the user was not found and proceed to the next store in the sequence</li> </ul> Submit Cancel									
確認序列已新增到清單中。									
cisco Identity Services Engine									

🙆 Home Monitor 🔻 Policy 🔻 Administration 💌								
🔆 System 🛛 🖓 identity Management 🖉 Network Res	sources 🛃 Guest Management							
Identities Groups External Identity Sources (Identity Source Sequences) Settings								
Identity Source Sequences								
/ Edit 🕂 Add 🖓 Duplicate 🗙 Defete 👻								
□ 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。

cisco Identity Services Engine	
💧 Home Monitor 🔻 Policy 🔻 🔒 Administrat	ion T
🔆 System 🕂 Identity Management 🖀 Netw	vork Resources 🛃 Guest Management
Sponsor Group Policy Sponsor Groups	lettings
Settings	* Sponsor Authentication Servers
General     General     Sponsor	* Identity Store Sequence Sponsor_Portal_Sequence
E Authentication Source	Save Reset Identity Sequence
Portal Customization	
Language Template	
Guest	Guest_Portal_Sequence
	Sponsor_Portal_Sequence
	AD_Internal
	(U)

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)。

cisco Identity Service	es Engine				ibe	acinin Log Out Feedbac
🛕 Home Monitor 🔻	Policy 🔻 🔽 Adminis	stration 💌				\varTheta Task Navigator 👻 🕑
🔆 System 🛛 😤 identity 🛙	lanagement 🖀 t	Network Resources	🛃 Guest Management			
Sponsor Group Policy	Sponsor Groups	Settings				
Status Rule Name		Identity Groups	Other Conditions		Spansor Groups	
🗄 🔽 💌 Manage All Ar	counts	SponsorAlL 🔶	and Condition(s)	them	SponsorAlAcco 💠	😂 Actions
Manage Grou	IP Accounts	SponsorGr 🔶	and Condition(s)	🔶 then	SponsorGroup	Insert New Policy Above Insert New Policy Below
Manage Own	Accounts	SponsorO 🔶	and Condition(s)	💠 then	SponsorGroup	Duplicate Above Duplicate Below
						Delete

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

dentity Services Engine							
🛕 Home Monitor 🔻 Policy	Administration V						
🔆 🔆 System 🦉 Identity Manag	ement 📲 Network Resources 🛃 Guest Management						
Sponsor Group Policy Spor	nsor Groups Settings						
Status Rule Name	Identity Groups Other Conditions						
🛛 🔽 👻 Domain Users	If Any 💠 and Select Attribute						
Add All Conditions Below to L	ibrary						
Condition Name E	xpression						
	Select Attribute						
	Dictionaries						
	Airespace						
AD1:外部組							

Status Rule Name	-	Identity Groups Other Conditions						
🛛 🖉 👻 Domain Users	if it	Any 💠 and Select Attribute						
Add All Conditions Below to Library								
Condition Name	Expression	×						
$\diamond$	Select Attribute							
	_	AD1						
		\$- III 🖌 🖗.						
		ExternalGroups						
		IdentityAccessRestricted						

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

cisco Identity Services Engine						
Administration 💌		-				
🔆 System 🖉 Identity Management 🔛 Network Resources 🛃 Guest Management						
Sponsor Group Policy Sponsor Groups Settings						
Status Rule Name Identity Groups Other Conditions		Sponsor				
Domain Users If Any 🔶 and Select Attribute	🗢 then	Sponsor G				
Add All Conditions Below to Library SponsorA						
Condition Name Expression AD1:ExternalGroups	<b>≙</b> .	SponsorGr				
corp.rf-demo.com/Users/Employe	Users	SponsorGr				

### 7. 在發起人組中,設定以下內容:保證人組:保證人所有帳戶

cisco Identity Services Engine		and the second division of the second divisio	ise
👍 Home Monitor 🔻 Policy 🔻 📝	Administration 🔻		
🔆 System 🛛 😤 Identity Management	Network Resources	🛃 Guest Management	
Sponsor Group Policy Sponsor Gro	ups Settings		
Status       Rule Name         Image       Domain Users         Image       Manage All Accounts         Image       Manage Group Accounts         Image       Manage Own Accounts	Identity Groups	Other Conditions and AD1:ExternalGroups	Sponsor Groups

8. 導航到管理>訪客管理>發起人組。



9. 選擇以編輯>SponsorAllAccounts。

cisco ide	ntity Services En	gine		
💧 Home	Monitor <b>v</b> Policy	<ul> <li>Administration</li> </ul>	•	
🔆 System	👰 Identity Manage	ment 🔛 Network	Resources	🛃 Guest Management
Sponsor Gr	oup Policy Spons	sor Groups Setti	ngs	
Guest Snon	ear Graune			
ouest spon		<b>1</b>		
W Edit	PAdd 🕺 K Delete	¥ Filter ▼		
🗖 Sponso	or Group Name	<ul> <li>Description</li> </ul>		
🗹 Sponso	arAllAccounts	Default Spor	sorGroup	
🗖 Sponso	orGroupGrpAccounts	Default Spor	sorGroup	

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

ululu cisco Identity Services Engi	ne
💧 Home Monitor 🔻 Policy 🔻	Administration T
🔆 🔆 System 🛛 🕸 Identity Managem	ent 📲 Network Resources 🛃 Guest Management
Sponsor Group Policy Sponso	r Groups Settings
Sponsor Group List > SponsorAllAcco	punts
	and the second second
General Authorization Lev	als Guest Roles Time Profiles
Autorization Lev	
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 99999999)
* Maximum Duration of Account	5 Days (Valid Range 1 to 999999999)
Save Reset	

# <u>在交換器上設定SPAN</u>

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

Tx: 254B/s	<b>•</b>	Thu	10:4	7
A.Port: On				
Turn AirPort Off				
√blizzard				(in
3ss				
alpha				
alpha_phone				
Branch				6
Branch-PSK				lie.
BranchVoice				ĉ
Demo2-Rogue				í.
Demo5-Rogue				ĥ
Employee				Ċ,
FlexDemo				ĥ
guest-test			1	lie.
guestnet			1	•
J_test			1	ĉ
Lab				í.
mi-demo-1x				÷
mi-rf-mgt				ĉ
open			1	-
podlx			<b>A</b> 3	2
PodX				•
rt-COA				
rf-management				2
secure-ipv6			•	(c)
Join Other Network Create Network				
Open Network Prefer	ences	i		

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

The network "pod1x" requires a password.
User Name: aduser
oser Name. aduser
Password:
802.1X: Automatic
TLS Certificate: None
Remember this network
Cancel OK

,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

AirPort	
AirPort TCP/IP	DNS WINS 802.1X Proxies Ethernet
▼User Profiles ✓ WPA: alpha	User Name: aduser
WPA: blizzard	Password: •••••
PEAP - Enabled Everything else = DIS	Always prompt for password  Authentication:  Enable Protocol  TLS  ABLED  PEAP  TTLS  EAP-FAST  Configure  Configure Trust
+ -	Wireless Network: pod1x Security Type: WPA2 Enterprise
?	Cancel OK

- 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。



## 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。

<sup>((</sup> p))Wifi1-Intel		×
Network Tasks	Choose a wireless network	
💋 Refresh network list	Click an item in the list below to connect to a wireless network in range or to get r information.	more
Set up a wireless nei for a home or small o	twork ((p)) pod1x	<u>د</u> الارب
Related Tasks	Wireless Network Connection	38898
Learn about wireles: networking		
Change the order of preferred networks	Please wait while Windows connects to the 'pod1x' network.	
Change advanced settings	Detecting network type	
	Cancel	
	Unsecured wireless network	
	((Q)) Demo2-Rogue	
	Security-enabled wireless network (WPA2)	
	((Q)) J_test	
		Connect

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)。

🔔 Wifi1-Intel Properties	pod1x properties	? ×
General Witeless Networks Advanced	Association Authentication Connection	
Use Windows to configure my wireless network settings	Select this option to provide authenticated network access for wireless Ethernet networks.	
To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.	Enable IEEE 802.1x authentication for this network	
View Wireless Networks	EAP type: Protected EAP (PEAP)	
Preferred networks: Automatically connect to available networks in the order listed below:	Authenticate as computer when computer information is available     Authenticate as guest when user or computer information is unavailable	ן ו
Add Remove Properties Learn about <u>setting up wireless network</u> Advanced OK Car		
	OK Cance	1

- 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)

Protected EAP Properties	
When connecting:	
Validate server certificate	
Connect to th EAP MSCHAPv2 Properties	×
When connecting: Trusted Root Cer	
Automatically use my Windows logon name and password (and domain if anu)	I
a.demo.loca	
Certiposte C	
Certisign - Ar	
Certisign - Autoridade Certificadora - AC4	F
	F
Do not prompt user to authorize new servers or trusted	
certification authorities.	
Secured password (EAP-MSCHAP v2)	
Enable Fast Reconnect	
Enable Quarantine checks	

- 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)。

# <u>參考: Microsoft Windows 7的無線身份驗證</u>

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

Currently connected to: secure-ipv6 No Internet access	÷ŋ	
Wireless Network Connection	^	m
secure-ipv6 Connected	he.	
Branch-PSK	m.	
pod1x		
Connect automatically	ect	
FlexDemo	.1	
alpha_phone	Me.	

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)。