適用於FlexConnect的無線BYOD部署指南

目錄

簡介 必要條件 需求 採用元件 拓撲 裝置註冊和請求方調配 資產註冊門戶 自助註冊門戶 驗證與布建 iOS布建(iPhone/iPad/iPod) Android調配 雙SSID無線BYOD自註冊 單SSID無線BYOD自註冊 功能配置 WLAN配置 <u>FlexConnect</u> AP配置 ISE 組態 使用者體驗 — 調配iOS 雙SSID 單SSID 使用者體驗 — 調配Android 雙SSID 我的裝置入口網站 引用 — 證書 相關資訊

簡介

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

本文檔提供自帶裝置解決方案的分支機構部署。員工使用新iPad連線到企業服務集識別符號 (SSID),並被重定向到自助註冊門戶。思科身份服務引擎(ISE)根據公司Active Directory(AD)對使用 者進行身份驗證,並將具有嵌入式iPad MAC地址和使用者名稱的證書以及請求方配置檔案下載到 iPad,該請求方配置檔案強制使用可擴展身份驗證協定 — 傳輸層安全(EAP-TLS)作為dot1x連線的 方法。根據ISE中的授權策略,使用者可以使用dot1x連線並訪問適當的資源。 低於7.2.110.0的思科無線區域網控制器軟體版本中的ISE功能不支援通過FlexConnect接入點(AP)關 聯的本地交換客戶端。7.2.110.0版支援用於本地交換和集中身份驗證客戶端的FlexConnect AP的這 些ISE功能。此外,與ISE 1.1.1整合的版本7.2.110.0提供(但不限於)以下無線自帶裝置解決方案 功能:

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

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

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本:

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

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

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

拓撲

若要正確實施和測試這些功能,需要最低限度的網路設定,如下圖所示:



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

裝置註冊和請求方調配

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

資產註冊門戶

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

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

自助註冊門戶

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

驗證與布建

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

注意:請參閱<u>FlexConnect功能表</u>思科文章,檢視BYOD的最新FlexConnect功能表。

iOS布建(iPhone/iPad/iPod)

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

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

Android調配

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

這是Android調配過程:

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

雙SSID無線BYOD自註冊

以下是雙SSID無線BYOD自註冊的過程:

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

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

單SSID無線BYOD自註冊

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

這是單SSID無線BYOD自註冊的過程:

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

功能配置

完成以下步驟即可開始設定:

1. 在本指南中,請確保WLC的版本是7.2.110.0或更高版本。

uluulu cisco		CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS
Monitor	Summary					
Access Points Cisco CleanAir Statistics CDP Rogues	-ili-ili- cisco			Cisco 250	D Series Wireless C	Kodel 2504
Clients	Controller Sumn	ary		Ro	gue Summary	
Multicast	Management IP Address	10.10.10.5		A	tive Rogue APs	
	Software Version	7.2.104.16		A	tive Rogue Clients	
	Field Recovery Imag Version	e 1.0.0		A	dhoc Rogues	
	System Name	wic-11mm		R	igues on wined wet	WORK

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

ululu cisco	MONITOR	WLANS C	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP EEEOBA	cx
Security	RADIUS	Authentica	tion Serve	rs					
General RADIUS Authentication Accounting Fallback	Call Stat Use AES MAC De	tion ID Type ¹ Key Wrap limiter	System M (Designed Hyphen	AC Address 1) for FIPS custome	rs and require	es a key wrap com	pliant RADIUS se	rver)	
TACACS+ LDAP	Network User	Management	Server Index	Server Addre	ss Port	19	Sec	Admin Status	
MAC Filtering			1	10.10.10.60	1812	D	isabled	Enabled	
Disabled Clients User Login Policies									

3. 將ISE 1.1.1新增到WLC:

輸入共用金鑰。將RFC 3576的支援設定為Enabled。

MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBAC
RADIUS Authentic	ation Server	s > Edit					
Server Index		1					
Server Address		10.10.10.60					
Shared Secret Format		ASCII :					
Shared Secret							
Confirm Shared Secre	t						
Key Wrap	6	(Designed fo	r FIPS custom	ers and requires a l	key wrap complia	nt RADIU	IS server)
Port Number		1812					
Server Status		Enabled :					
Support for RFC 3576		Enabled :	0				
Server Timeout		2 second	ds				
Network User		Enable					
Management		Enable					
IPSec		Enable					

4. 新增與RADIUS記帳伺服器相同的ISE伺服器。

MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANA
RADIUS Accountin	ng Servers >	Edit		
Server Index	1			
Server Address	10.10	0.10.60		
Shared Secret Format	ASC	II ÷		
Shared Secret	•••			
Confirm Shared Secre	t			
Port Number	1813			
Server Status	Enal	bled :		
Server Timeout	2	seconds		
Network User	🗹 Er	nable		
IPSec		Enable		

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

cisco		<u>W</u> LANs		WIR
Security	FlexConr	nect Acc	ess Control Li	ists
 AAA Local EAP Priority Order Certificate Access Control Lists Access Control Lists CPU Access Control Lists FlexConnect ACLs Wireless Proto Access Control Lists 	Acl Name	ECT		

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

對於第一條規則(序列1):

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

Access Control Lis	sts > Rules > Edit		
Sequence	1		
Source	Any :		
		IP Address	Netmask
Destination	IP Address ‡	10.10.10.60	255.255.255.255
Protocol	Any		
DSCP	Any ‡		
Direction	Any ÷		
Action	Permit ‡		

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

Gene	ral									
Access	s List Name	ACL-RED	IR	ECT						
Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	,
1	Permit	0.0.0.0 0.0.0.0	/	10.10.10.60 255.255.255.255	/	Any	Any	Any	Any	
2	Permit	10.10.10.60 255.255.255.255	/	0.0.0.0 0.0.0.0	/	Any	Any	Any	Any	

7. 建立一個名為Flex1的新FlexConnect組(在本例中):

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

uluili. cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBA	Sage Configuration Bing Legout Beh CK
Wireless	FlexConnect Groups > Edit 'Flex1'	< Back Apply
Access Points All APs Radios	General Local Authentication Image Upgrade VLAN-ACL mapping WLAN-ACL mapping	WebPalicies
802.11a/n 802.11b/g/n Global Configuration	WebPolicies	
 Advanced Mesh 	WebPolicy ACL ACLAREDIRECT	
FlexConnect Groups HesConnect Accs	WebPolicy Access Control Lists	
> 802.11a/n > 802.11b/g/n	ACL-REDIRECT	
▶ Media Stream		

8. 按一下「Apply」和「Save Configuration」。

1. 建立雙SSID的開放式WLAN SSID示例:

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

WLANs > Edit 'Demo	CWA'
General Security	QoS Advanced
Profile Name	DemoCWA
Туре	WLAN
SSID	DemoCWA
Status	✓ Enabled
Security Policies	MAC Filtering (Modifications done under se
Radio Policy	All
Interface/Interface Group(G)	management 💌
Multicast Vlan Feature	Enabled
Broadcast SSID	F Enabled

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

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

_ANs > Eq	dit 'Demo(CWA'	
General	Security	QoS	Advanced
Layer 2	Layer 3	AAA S	ervers
Layer 2	Security 🤨 🛛 N MA	lone C Filterin	9 <mark>2</mark> 🔽
Fast Trans	ition		
Fast Transiti	ion		

3. 轉到AAA Servers頁籤,並設定以下屬性:

身份驗證和帳戶伺服器:已**啟用**伺服器1:<ISE IP地址>

eneral	Security	QoS Advanced	
layer 2	Layer 3	AAA Servers	
elect AAA	servers belo	w to override use of default servers on this WLAN	
Radius Se Radius	rvers Server Overw	ite interface Enabled	
Radius Se Radius	rvers Server Overw	ite interface Enabled Authentication Servers Accounting Servers Servers Enabled	
Radius Se Radius Server	rvers Server Overw	ite interface Enabled Authentication Servers Accounting Servers Enabled IP:10.10.10.60, Port:1812 IP:10.10.10.60, Port:18	1
Radius Se Radius Server Server	rvers Server Overwi 1 2	ite interface Enabled Authentication Servers Accounting Servers Enabled IP:10.10.10.60, Port:1812 IP:10.10.10.60, Port:18 None None None	1

0	rder Used For Authent	ication
>	RADIUS	Up
	o >	Order Used For Authent

5. 轉到Advanced索引標籤,並設定以下屬性:

Allow AAA Override	F Enabled	100.7
Correrage Hole Detection	W Enabled	EMCP Server Covers
Enable Session Timeout	pr [1800 Session Timeout (secs)	DHCP Addr. Assignment Exercise
Aironat 18	9 Enabled	Nananament Frame Protection (NF)
Diagnostic Channel	I"Evabled	
Overvide Interface ACL	Shot None R Shot None R	1979 Class Profession # Cottonal
F2F Blacking Action	Disabled B	0104 Period (in beacas intervals)
Clarit Exclusion	C'Evabled	
Maximum Allowed Clients	F	802.33.wh (3 - 295) [3 802.33.b/p/n (3 - 295) [5
Static IF Tunneling 🛤	Finalist	NAC
Wi-Fi Direct Clients Policy	Doubled B	NAC State Radius NAC 💌
		Land References and Rand Refer

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

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

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



7. 按一下「Apply」和「Save Configuration」。

Sa <u>v</u> e Configuration	Logical Batta
< Back	Apply
	6

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

/LANs > Edit 'Demo	o1x'
General Security	QoS Advanced
Profile Name	Demo1x
Туре	WLAN
SSID	Demoix
Status	Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under sec
Radio Policy	All
Interface/Interface Group(G)	management 💌
Multicast Vlan Feature	Enabled
Broadcast SSID	Enabled

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

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

WLANs > E	dit 'Demo	1x'		
General	Security	QoS	Advanc	ed
Layer 2	Layer 3	AAA S	ervers	
Layer 2	Security 😫 🚺	WPA+WPA2	2	
	M	AC Filtering	2 🗆	
Fast Trans	ition			
Fast Transit Over the DS	ion 🗆			
Reassociatio	on Timeout 20)		
WPA+WPA	2 Parameter	rs		
WPA Pol	icy			
WPA2 P	olicy	4		
WPA2 E	ncryption	₩ AES	s 🗖 T	KIP
Authentica	tion Key Ma	nagement	t	
802.1X	ع ب	inable	_	
CCKM	□ e	nable		
PSK	Πe	inable		

10. 轉到Advanced索引標籤,並設定以下屬性:

允許AAA覆蓋	:	啟 用 NAC狀態	:	Radius	NAC
---------	---	------------------	---	--------	-----

Allow AAA Override	F Enabled	0407
Coverage Hole Detection	P Enabled	DHCP Server Coveride
Enable Session Timesul	ge (1.800 Section Tometud (1865)	DHCP Adds. Assignment Remained
Airunet II	\$ Enabled	Nanaparated France Protection (NEP)
Diagnostic Channel	T Evabled	
Override Interface ACL	IPod None B IPod None B	MPP Classit Production # Optional 20
F2F Electring Action	Disatived R	BTIN Period (in beacan intervals)
Client Evolusion 8	PEnabled Timeout Value (secs)	800 11 mb (1 - 1980) 5
Maximum Allowed	P	802.135/ph (1 - 200) [1
Charits *	-	

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

FlexConnect	
FlexConnect Local Switching ²	Enabled
Rectanged user last	· 7 susses

12. 按一下「Apply」和「Save Configuration」。



13. 確認兩個新的WLAN都已建立。

MONI	TOR Y	<u>N</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
WLA	Ns								Entries 1 - 5 of :
Curre	nt Filte	r: Nor	ne [Change	Filter] [Clear	Filter]		Create New	• 6	0
	LAN ID	Туре	Profile Na	me		VLAN SSID		Admin Status	Security Policies
0.1		10,85	8114			EEH		Disabled	[[#FA2[Auth(952.14]]
C 2		WLAN						Enabled	[#PA2][Auth(PSE)]
Π 2		WLAN	Demo1x		C	Demoix		Enabled	[WPA2][Auth(802.1X)]
		WLAN	DemoCWA		C	DemoCWA		Enabled	MAC Filtering
E 1		97,45	fig.s			le r		Creative	i Web-Auth

FlexConnect AP配置

完成以下步驟以設定FlexConnect AP:

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

	<u>W</u> LANs		WIRELESS
All APs			
Current Fi	lter		None
Number o	f APs		2
AP Name		AF	P Model
<u>Site-B-Fley</u>	AP Name Site-B-FlexAP		R-LAP1262N-A-K

2. 按一下FlexConnect選項卡。



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

VLAN Support	•	
Native VLAN ID	1	VLAN Mappings
FlexConnect Group Name	Not Confi	gured

4. 將SSID的VLAN ID設定為21(在本例中),以便進行本地交換。

MONITOR	t <u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY
All APs	> Site-B	-FlexAP > VLA	N Mapping	S
AP Nam	e	Site-B-FlexAP		
Base Radio MAC		e8:04:62:0a:68:8	0	
WLAN Id	SSID			VLAN ID
3	Demo1x			21
4	DemoCW	A		21
	-			and the second second second

5. 按一下「Apply」和「Save Configuration」。

ISE 組態

完成以下步驟以配置ISE:

1. 登入ISE伺服器: <https://ise>。



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



3. 按一下Active Directory。



4. 在Connection頁籤中:

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

Connection	Advanced S	Settings	Groups	Attri	butes		
		* Do	main Name	corp.rf-der	no.com		
		* Identity	Store Name	AD1			
		recting	onore realine				
ne or more node	s may be selec	ted for Join	or Leave ope	erations. If a	node is joine	d then a lea	ve operation is
he or more node onnection. 같 Join 약을 Lea	s may be select ve 👷 Test Co	ted for Join	or Leave ope	erations. If a	node is joine	d then a lea	ve operation is
ne or more node onnection. 2 Join 9 Lea) ISE Node	s may be select ve 😟 Test Co	ted for Join	or Leave op	ole St	node is joine atus	d then a lea	ve operation is

5. 使用當前域使用者執行與AD的基本連線測試。

connection.	
👷 Join 🛛 👷 Leave	👷 Test Connection 👻
ISE Node	Basic Test
✓ ise11-mnr	Detailed Test
Test Connection * User Name: paul * Password:	×

6. 如果與AD的連線成功,則會出現一個對話方塊,確認密碼正確。



- 7. 導航到Administration > Identity Management > External Identity Sources:
 - 按一下「Certificate Authentication Profile」。按一下「Add」以新增憑證驗證設定檔(CAP)。

CISCO Identity Services	Engine		
🛕 Home Operations 🔻 P	olicy 🔻 Adminis	stration 🔻	
🔆 System 🛛 👰 Identity Mar	nagement 🔛 N	Network Resources	🛃 Web Portal Manage
Identities Groups External	Identity Sources	Identity Source Sequ	iences Settings
External Identity Sources		Certificate Auth	nentication Profile
∲-	ŵ.	In hu	Department You
Certificate Authentication Profile	۲	East oge Add	Duplicate K De
Active Directory		□ Name •	
CDAP LDAP	۲		
RADIUS Token	۲		
PSA SecurID	0		

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

Certificate Authentication Profiles List > New	Certificate Authentication Profile	
Certificate Authentication Pr	rofile	
* Name	CertAuth	
Description		
Principal Username X509 Attribute	Common Name	-
Perform Binary Certificate Comp	arison with Certificate retrieved fro	m LDAP or Active Directory
LDAP/AD Instance Name		
Submit Cancel		

9. 確認已新增新的CAP。

CISCO Identity Services Engine	
🛕 Home Operations 🔻 Policy 🔻 Admini	stration 🔻
🔆 System 🦉 Identity Management 📰 I	Network Resources 🛛 🚇 Web Portal Management
Identities Groups External Identity Sources	Identity Source Sequences Settings
External Identity Sources	Certificate Authentication Profile
Certificate Authentication Profile	🖊 Edit 📲 Add 🕒 Duplicate 🗙 Delete
Active Directory	Name
🚞 LDAP 💿	Cerusan
RADIUS Token 💿	
RSA SecurID 💿	

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

CISCO Identity Services Engine	
🛕 Home Operations 🔻 Policy 🔻 Adm	inistration 🔻
🔆 System 🦉 Identity Management	Network Resources 🛛 🛃 Web Portal Management
Identities Groups External Identity Sources	Identity Source Sequences Settings
Identity Source Sequence	
/ Edit -Add Pa Duplicate X Delete	
Name S	Description
Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal
MyDevices_Portal_Sequence	A built-in Identity Sequence for the My Devices Po
Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal

11. 為序列指定名稱TestSequence(在本例中)。

cisco Id	entity Services Engine
💧 Home	Operations Policy Administration
🔆 System	Veb Portal Mana
Identities (Groups External Identity Sources Identity Source Sequences Settings
Identity Source Sequ Identity Source Identity Source	uences List > New Identity Source Sequence rce Sequence urce Sequence
* Name	TestSequence
Description	
▼ Certificate	e Based Authentication

12. 向下滾動至Certificate Based Authentication:

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

Certificate Based Authentication	
Select Certificate Authentication Profile	CertAuth 💌
 Authentication Search List 	

13. 向下滾動至Authentication Search List:

將AD1從「可用」移動到	「選定」。按一下up按鈕將AD1移至最高優先順序。
 Authentication Search List 	
A set of identity sour	ces that will be accessed in sequence until first authentication succeeds
Available	Selected
	Internal Users

14. 按一下「Submit」以儲存。

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
Submit

15. 確認已新增新的身份源序列。

cisco Identity Services Engine		0. 00
🛕 Home Operations * Policy * Administrati	ion 🔹	
🔆 System 🛛 👰 Identity Management 🖉 Netw	rork Resources 💽 Web Portal Management	
Identities Groups External Identity Sources	entity Source Sequences Settings	
Identity Source Sequence		
/ Edit - Add Duplicate X Delete		
Name .	Description	Identity Stores
Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users
MyDevices_Portal_Sequence	A built-in Identity Sequence for the My Devices Portal	Internal Users
Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal Users
TestSequence		CertAuth, Internal Users, Internal Endpoints

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

🔆 System 🏾 👰 Identity Management	Network Resources 🛛 🛃 Web
Identities Groups External Identity Sources	Identity Source Sequences
dentity Source Sequence	0
dentry obdiec ocquerice	
activity obtained dequetice	
/Edit +Add Duplicate XDelete	
/Edit +Add Duplicate XDelete	Description
Edit +Add Duplicate XDelete Name Guest_Portal_Sequence	Description A Built-in Identity Sequence
Edit Add Duplicate XDelete Name Guest_Portal_Sequence MyDevices_Portal_Sequence	Description A Built-in Identity Sequence A Built-in Identity Sequence

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



18. 按一下「**Save**」。



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

I Guest_Portal_Sequence	A Built-in Identity Sequence For The Guest Portal	Internal Users, AD1
MyDevices_Portal_Sequence	A Built-in Identity Sequence For The My Devices Portal	AD1, Internal Users

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



21. 確認Guest_Portal_Sequence包含AD1。

	Name	Description	Identity Stores
Ð	Guest_Portal_Sequence	A Built-in Identity Sequence For The Guest Portal	Internal Users, AD1
100			

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

🛕 Home Operations 🔻 Policy 🔻 🖌	Administration 🔻		
🔆 System 🏾 👰 Identity Management	Network Resources	🛃 Web Portal Management	
Network Devices Network Device Groups	External RADIUS Servers	RADIUS Server Sequences	S
Network Devices	Network Device	5	
Network Devices	P Ketwork Device	Ra Duplicate (De Import	

23. 新增WLC名稱、IP地址、子網掩碼等。

Network Devices List > New Net	twork Device	
Network Devices		
* Name Description	WLC	
* IP Address:	10.10.10.5 / 32	
Model Name Software Version	×	
* Network Devic	te Group	
Location	All Locations 📀 Set To Default	
Device Type	All Device Types 📀 Set To Default	

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

~	 Authentication Settings 			
	Enable A	thentication Settings	PADTUC	
		 Shared Secret 	*****	Show
		Enable KeyWrap		
		Key Encryption Key		Show
	 Message Au 	thenticator Code Key		Show
		Key Input Format	ASCII O HEXADEC	IMAL
	SNMP Settings			
	SGA Attributes			
Sub	nit Cancel			

- 25. 按一下「Submit」。
- 26. 導覽至ISE > Policy > Policy Elements > Results。

CISCO Identity Services Engine				
🛕 Home Operations 🔻	Policy Administration			
🔆 System 🛛 😤 Identity I	Authentication			
Network Devices Network	Authorization			
Network Devices	Posture Client Provisioning			
	Security Group Access			
Network Devices	Network Device Authorization			
Default Device	Policy Elements Dictionaries Conditions			
	Results			

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

CISCO Identity Services Engine	
🛕 Home Operations 🔻 Policy 🔻	Administration 🔻
🛃 Authentication 👩 Authorization	Refiling Rosture 🔂 Client Provisioning
Dictionaries Conditions Results	
Results	Standard Authorization Profiles
∲• ≡ 1≣	Edit Add Duplicate X Delete Name
Authentication	Blacklist_Access
Authorization Profiles	Gsco_IP_Phones
Blacklist_Access	ContractV12 DenvAccess

28. 為此配置檔案指定以下值:

名稱:CWA

Authorization Profiles > Authorization I	New Authorization Profile Profile
* Name	CWA
Description	
* Access Type	ACCESS_ACCEPT *

啟用Web驗證(覈取方塊為選中狀態):

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

 Common Tasks 							
DACL Name							
ULAN VLAN							
Voice Domain Permissio	n						
Web Authentication	Centralized	٣	ACL	ACL-REDIRECT	Redirect	Default	٣

29. 按一下Submit, 並確認已新增CWA授權配置檔案。



30. 按一下Add以建立新的授權設定檔。



31. 為此配置檔案指定以下值:

名稱:配**置**

Authorization Profiles > Authorization I	New Authorization Profile Profile
* Name	Provision
Description	
* Access Type	ACCESS_ACCEPT *

啟用Web驗證(覈取方塊為選中狀態):

Web驗證值:請求**方調配**

 Common Tasks 		
DACL Name		
ULAN VLAN		
Voice Domain Permission	on	
Veb Authentication	Centralized *	ACL
	Centralized	
Auto Smart Port	Device Registration	
	Posture Discovery	
Filter-ID	Supplicant Provisioning	
	V2	

ACL: ACL-REDIRECT(必須與WLC預先驗證ACL名稱相符。)

▼ Common Tasks			
DACL Name			
ULAN			
Voice Domain Permission			
Veb Authentication	Supplicant Provisioning *	ACL	ACL-REDIRECT
Auto Smart Bort			

32. 按一下Submit, 並確認已新增Provision授權配置檔案。

Standard Authorization Profiles						
1	Edit -Add	Duplicate	×			
	Name					
	Blacklist_Acces	s				
	CWA					
	Provision					

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



34. 選擇Native Supplicant Profile。



35. 為配置檔案指定名稱WirelessSP(在本例中)。

Native Supplicant Profil	e
* Name	WirelessSP
Description	

36. 輸入以下值:

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

Operating System	ALL 💠		
Connection Type	Wired		
	Vireless		
		*SSID	Demoix
		Security	WPA2 Enterprise +
* Allowed Protocol	PEAP		v
Optional Settings	TLS PEAP	ę	3
Submit Cancel			

- 37. 按一下「Submit」。
- 38. 按一下「**Save**」。

* Allowed Protocol	TLS	-
* Key Size	1024	•
Save Reset		

39. 確認已新增新配置檔案。

Resources						
/ Edit 🕂 Add 👻 🕒 Duplicate	XDelete					
Name	Туре					
Wireless	NativeSPProfile					

40. 導覽至Policy > Client Provisioning。



41. 為iOS裝置的調配規則輸入以下值:

規則名稱:iOS身份組:任意

	Rule Name	Identity Gro	ups	Operating Systems	Other Conditions
. 🖌	IOS	If Any	<> and	Choose a 🗢	and Condition(s)
				Choose an Oper	rating System 👷 🕂
					9

作業系統:MaciOS All

Operating System Grou	ips
	Q
◆- ■ '≣	ŵ
Android	
Mac OSX	
Mac iOS All	
🚞 Windows All	۲

結果:WirelessSP(這是之前建立的本地請求方配置檔案)

Results
then Result 🕀 🥎

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



WizardProfile	
	(م
€- ■ '≣	ŵ .
Clear Selection	
Wireless	

42. 確認已新增iOS設定配置檔案。

			Rule Name	I	(dentity Gr	oups		Operating Systems			Other Conditions		Results	
1	¥.	٠	105	If [Any	\diamond	and	Mac IOS All	Þ	and	Condition(s)	\$ then	WrelessSP	\diamond

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



44. 將新規則的Name更改為Android。

	Rule Name	
•	iOS	
•	Android	

45. 將作業系統更改為Android。

Operating System Gr	oups
	R
🔶 🔳 🗐	ŵ
Android (h)	
· Mac 405 AB	
Windows Al	(8

- 46. 保留其他值不變。
- 47. 按一下Save(左下螢幕)。



48. 導覽至ISE > Policy > Authentication。



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



50. 按一下Condition Name下拉選單。



51. 選擇Dictionaries > Compound Condition。



52. 選擇Wireless_MAB。



53. 在規則的右側,選擇要展開的箭頭。

:	If [Wireless_MAB	¢	allow protocols	Allowed Protocol : Default Netw	and	Ę.

54. 從下拉選單中選擇以下值:

身份源:**TestSequence**(這是之前建立的值)如果身份驗證失敗:拒**絕**如果找不到使用者 :繼**續**如果進程失敗:**Drop**

use	TestSequence 🗢
	Identity Source TestSequence 📀
	Options
	If authentication failed Reject
Minute	If user not found Continue
	If process failed Drop 🔹

55. 轉到Dot1X規則,然後更改以下值:

	•	Dot1X	: If	Wired_802.	1X ⊕ _î	allow protoco	
T			Default Rule (If no match)	: al	low protocols	Allowed Protocol : Default Ne	

CON	pound Condition
	م
4.	/ 🔳 📜 👘 🌸 🛛
•	Wired_MAB
•	Wireless_MAB
•	Wired_802.1X
ш. М	Mireless_802.1X Jhn
• 3	Switch_Local_Web_Authentication
•	WLC_Web_Authentication
: If	Wired_802.1X allo
: al	Add All Conditions Below t
	Condition Name
	Wireless 802.1X 📀

條件:Wireless_802.1X

身份源:測**試**

Identity Source TestSequence	se for authe	
Options	Identity Source List	
If user not found Reject *	(م	
If process failed Drop *	∲•	
Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS	Internal Endpoints	
it is not possible to continue processing when authentication fails a	Internal Users	
In containue option is selected in these cases, requests will be rejec-	Guest_Portal_Sequence	
	Sponsor_Portal_Sequence	
	MyDevices_Portal_Sequence	
	U TestSequence	
Internal Users 🗢	CertAuth	
	DenyAccess	

56. 按一下「**Save**」。



57. 導覽至ISE > Policy > Authorization。



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

ect	Matched R	ule Annies	oaseo on identity groups anajor other conditions. Urag and drop rules to i	unange one order.	
	- and a second second	an affinia .			
Đ	ceptions (0)			
St	andard				
	Status	Rule Name	Conditions (identity groups and other conditions)	Pr	emissions
		Black List Default	f Blacklist	then B	acklist_Access
		Profiled Cisco IP Phones	if Cisco-IP-Phone	then O	sco_IP_Phone
		Default	If no matches, then PermitAccess		

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



新增新的標準規則編號。

	Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
1		Black List Default	if Blacklist	then Blackist_Access
		Profiled Cisco IP Phones	Cisco-IP-Phone	then Osco_IP_Phones
11	- 🖬	Standard Rule 1	f Any \ominus and Condition(s)	💠 then AuthZ Profil 💠
		Default	If no matches, then PermitAccess	

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



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

Cisco-IP-Phone		then Cisco_IP_Phor		
f Any \diamondsuit and f no matches, then Perm	Select Condition	ng Condition from Library () or Create		

62. 選擇Compound Conditions > Wireless_MAB。

er conditions. Drag and drop	Compound Conditions
	[٩
	∻- ≣ '≣
	Wired_802.1X
	Wired_MA8
	Wireless_802.1X
ups and other conditions)	Wireless_MAB
	Catalyst_Switch_cocal_Web_Authentica
	WLC_Web_Authentication
	1
Select Condition	
Add All Conditions B	
Condition Name	
Select Condition	

63. 在AuthZ配置檔案中,按一下加號(+),然後選擇Standard。
| | Profiles | |
|----------------|-----------------------|----|
| | | P |
| licy Elements | (4 - ≡ '≣ | ÷. |
| | 🚞 Inline Posture Node | ۲ |
| | Security Group | ۲ |
| | Sandard 🗟 | ۲ |
| rmissions | | |
| icklist_Access | | |
| co_IP_Phones | | |
| AuthZ Profil 🗢 | | |
| Select an item | ○ - + | |
| | | |
| | | |

64. 選擇標準CWA(這是之前建立的授權配置檔案)。

Standard	
	Q
∲- 🗐 🗐	ŵ.
Swa Jhn	
Circo D Obser	

65. 確認新增規則時使用了正確的條件和授權。

🖉 🗹 👻 OpenCWA	# Any	♦ m	Wireless_MAB	the	CWA	\$
---------------	-------	-----	--------------	-----	-----	----

66. 按一下**Done**(在規則的右側)。



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

Below(在下面插入新規則)」。



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

1	OpenCWA	if Wineless_MAB	then CWA
1 🖬 -	Standard Rule 1	Any 💠 and Condition(s)	🔶 then Auth2 Profil 💠

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

Condition(s)	- then AuthZ Profil 💠	
🗎 Add All Conditions Belo	w to Library	
Condition Name	Expression	
Wireless_802.1X	Radius:Service-Type EQUALS Framed AND Radius:NAS-Port	ŵ .

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



71. 找到並選擇Network Access。

		-	Dictionaries	
				R
			◆- ■ .≡	\$\$+
os and other conditions)				-
		then		
		then		
		then		
Condition(s)	0	-		
tAccess			· · ·	
Condition Name	Expression			
Wireless_802.1X 📀	Radius:Service-	Type E	Network Access	
٥	Select Attri	oute 🤇		

72. 選擇AuthenticationMethod,然後輸入以下值:

Ne	twork Access
\square	م
¢	🖬 🗐 🗐 👘
	AuthenticationIdentityStore
	AuthenticationMethod
	AuthenticationStatus
۳	Device IP Address

AuthenticationMethod:等於

Network Access:Au🛇	•
	Equals Not Equals

選擇MSCHAPV2。

S Framed AND Radius:NAS-Port			
Equals 💌	•		
	CHAP/MD5		
	Lookup		
	MSCHAPV1		
	MSCHAPV2		
	PAP_ASCII		
	x509_PKI		

這是規則的示例;請務必確認條件是AND。

and [Condition(s)	🗢 then 🛛 AuthZ Profil 💠		
	Our Rine Name	Furnancian	-	
	Wireless 802 1X	Radius:Service.Type EOLIALS Framed AND Radius:NAS.Dort	AND	ŵ.,
	♦ 1000000000000000000000000000000000000	Network Access:Au Equals * MSCHAPV2 *	•	ŵ.

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

then	AuthZ Profil	Done
	Select an item 📀	- +

Standard	ž.
	و م
∲- ■ 1≣	<u>§</u> ≩.
and the second second	
and the second	
and the state of the state of	
and a subsection of the	
(and the state of	
and the second se	
Servision (h)	

74. 按一下「**完成**」。



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



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

💉 🗹 🔹 Standard Rule 1	# [Any	\diamond	nd [Condition(s)] then [AuthZ Profil	\$

77. 在「條件」下,選擇**複合條件**。

	Dictionaries	
		P
	♦ • ■ '≣	\@+
lant Dravicionina	Simple Conditions	۲
	Compound Conditions	A.
	Time and Date Conditions	82
twork Access:Authentica		
Condiaon(s)		1
💾 Add All Conditions B		
Add All Conditions E Condition Name		

78. 選擇Wireless_802.1X。



79. 新增AND屬性。

Wireless_802.1X		
💾 Add All Conditions Bel	ow to Library	
Condition Name	Expression	
Wireless_802.1X 📀	Radius:Service-Type EQUALS Framed AND Radius:NAS-Port	- B

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



81. 找到並選擇Radius。

			Dictionaries	
	10		¢• 🔳 🗉	
Client Provisioning 🛛 🚊 Sect	urity Group Ac	cess	🛄 diter	-
			Caco-detter	
		thee	🛄 Caco-officialit	
		then	📴 DEHICE	
		then	🛄 EndPointe	
	- the d		📴 Guest	
etwork Access:AuthenticationM	lethod	then	a Mentlyling	
Wireless 802.1X Network Acc	ess:A.	5	🔛 Internal.teer	
			Moreault	
Condition Name	Expressio	on	Retwork Access	AND V
			🚞 Radius	
Wireless_802.1X 📀	Radius:Ser	vice-Type E	Section 1	20-
٥	Select /	Attribute 📀		o

82. 選擇Calling-Station-ID---[31]。



83. 選擇Equals。

Radius:Service-Type EQUAL	S Framed AND Radius:NAS-	Port
Radius:Calling-Statio	Equals Not Equals	⊙

84. 轉到CERTIFICATE,然後按一下右箭頭。



85. 選擇Subject Alternative Name。



86. 對於AuthZ配置檔案,請選擇Standard。

	Profiles	
		۵.
	∲-	ŵ
v Elements	🔜 John Posture Toole	
,,	🛄 ficarty irrup	
	Standard	R
o_IP_Phones		
4		
ision	-	
AuthZ Profil 🗢		
Select an item	2	

87. 選擇Permit Access。



88. 按一下「**完成**」。



以下是規則的範例:

1	OpenCHA /	Weeks, Mill	there	CHR
-	Kiha I	Winker, 802.51 (10) Network Access Authenticator/Hethod 8/234L5 HSDNIPV2)		Provision
1	AllowRule if	Wireless_802.1X Radus:Caling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name		PermitAccess

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



90. 按一下「Edit」以編輯「Default」規則。



91. 轉到PermitAccess的現有AuthZ配置檔案。



92. 選擇Standard。



93. 選擇**DenyAccess**。

Standard		
4	• 🗐 🗉 🗌	
8	Balikt_Access Cask	
õ	Caso, JP , Phones	
	DepyAccess 0	
G	Contraction (D)	

94. 如果找不到匹配項,請確認預設規則具有DenyAccess。



95. 按一下「**完成**」。



這是此測試所需的主要規則的示例;它們適用於單SSID或雙SSID方案。

OpenCWA	if Wireless_MAB	then	CWA
PEAPrule	If (Wireless_802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	then	Provision
AllowRule	Wireless_802.1X AND Radius:Caling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name)	then	PermitAccess
Default	if no matches, then DenyAccess		

96. 按一下「**Save**」。



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



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



99. 按一下「Add」。



100. 為此配置檔案輸入以下值:

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

P Certificat	e Authority	
* Name	mySCEP	
Description		
* URL	https://10.10.10.10/certsrv/mscep/	Test Connectivit

101. 按一下測試連線以測試SCEP連線的連線。



102. 此響應顯示伺服器連線成功。



103. 按一下「Submit」。



104. 伺服器響應已成功建立CA配置檔案。



105. 確認已新增SCEP CA配置檔案。

SCEP CA Profiles			♦ @ .
/Edt +Add XDelete		Show All	- 8
Name Name	Description	URL	CA Cert Name
MySCEP		https://10.10.10.10/certsrv/mscep	RFDemo-MSCE

使用者體驗 — 調配iOS

雙SSID

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

完成以下步驟,以便在雙SSID場景中調配iOS:

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



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

Web Authentication Redirect
Cannot Verify Server Identity Safari cannot verify the identity of
Would you like to continue anyway?
Details
Continue

3. 系統會將您重新導向至訪客輸入網站以登入。



4. 使用AD使用者帳戶和密碼登入。出現提示時,安裝CA配置檔案。



5. 按一下Install CA伺服器的受信任證書。



6. 配置式安裝完成後,按一下Done。



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



8. 按一下「Install」以安裝已驗證的設定檔。



9. 按一下「Install Now」。



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

Profile Installed Done							
X. K.	WirelessSP Cisco						
	♥ Verified						
Description	ISE Profile desc						
Signed	ise11-mnr.corp.rf-demo.com						
Received	Mar 24, 2012						
Contains	Certificate SCEP enrollment request Wi-Fi Network						
More Detai	ls >						

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



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

A Home Operations • Policy • Administration •									
Authentications	🤨 Endpo	ant Prote	ection Service 🛛 🕎	Alams 🚊 Report	s 💊 Trouble	shoot			
Live Authentications									
🙀 Add or Remove Columns 🔹	🔂 Refi	resh					Refresh Every 3 secon	ds • 9ow	Latest 20 records * within L
Time	Status	Detais	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25,12 12:27:57.052 AM		.0	paul	E8:06:80:97:09:41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25,12 12:27:21.714 AM			68:06:88:97:09:41	E8:05:88:97:09:41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25,12 12:27:20.438 AM		à			WLC				Dynamic Authorization succeeded
Mar 25,12 12:26:56.187 AM		à	paul	E8:06:88:97:09:41	WLC	CWA	Any,Profiled:Apple-Pad	Pending	

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

🛕 Home Operations 🔻 Policy 💌 Admir	inistration 🔻
🔆 System 🦞 Identity Management	Network Resources 🛛 🛃 Web Portal Management
Identities Groups External Identity Sources	s Identity Source Sequences Settings
Identity Groups	Endpoint Group List > RegisteredDevices Endpoint Group * Name RegisteredDevices Description Asset Registered Endpoints Identity Group Parent Group Save Reset * Endpoints Identity Group Endpoints MAC Address Es:06:88:97:09:41

單SSID

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

完成以下步驟,以便在單SSID場景中調配iOS:

1. 如果您使用的是同一個iOS裝置,請從已註冊裝置中刪除終端。

Endpoir Endp	Endpoint Group List > RegisteredDevices Endpoint Group						
	* Name	RegisteredDevices					
De	escription	Asset Registered Endpoint					
Pare	nt Group						
Sav	Res	et					
▼ E	ndpoints						
Ide	ntity Grou	up Endpoints					
	+ Add	×Remove •					
	MAC Add	Remove Selected					
	E8:06:88	9 Remove All					

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



3. 按一下「Remove」以移除先前的設定檔。





4. 使用現有的(已清除)裝置或新的iOS裝置直接連線到802.1x。

5. 連線到Dot1x,輸入使用者名稱和密碼,然後按一下Join。

Enter the password for "Demo1x" Cancel Enter Password Join						
Username paul						
Password ••••••3						
Mode	Automatic >					

- 6. 從ISE配置部分重複步驟90和on,直到完全安裝相應的配置檔案。
- 7. 導覽至ISE > Operations > Authentications以監控流程。此範例顯示使用TLS來布建、斷開並 重新連線到同一WLAN時,直接連線到802.1X WLAN的客戶端。

Live Authentications									
🎼 Add or Remove Columns 🗢	😵 Refi	resh					Refresh Every	3 seconds *	Show Latest 20 records
Tme •	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25,12 12:40:03:593 AM		ò	piul	E8 06 88 97 09 41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25,12 12:39:53.353 AM	2	ò	E8:06:88:97:09:41	E8:06:88:97:09:41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25,12 12:39:08.867 AM		à	paul	E8:06:88:97:09:41	WLC	Provision	RegisteredDevices	Pending	Authentication succeeded

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

Live Authentications									
🎼 Add or Remove Columns 👻	😵 Refi	resh					Refresh Every	3 seconds *	Show Latest 20 records
Time •	Status	Detais	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25,12 12:40:03.593 AM		ò	paul	E8.06.88.97.09.41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25,12 12:39:53.353 AM	2	ò	E8:06:88:97:09:41	E8:06:88:97:09:41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25,12 12:39:08.867 AM	1		piul	E8-06-88-97:09-41	WLC	Provision	RegisteredDevices	Pending	Authentication succeeded

使用者體驗 — 調配Android

雙SSID

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

Android裝置的連線過程與iOS裝置(單或雙SSID)的連線過程非常相似。然而,一個重要的區別是 ,Android裝置需要訪問Internet才能訪問Google Marketplace(現在是Google Play)和下載請求者 代理。 完成以下步驟,以便在雙SSID場景中調配Android裝置(如本示例中的Samsung Galaxy):

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



2. 接受任何證書以連線到ISE。



3. 在訪客門戶輸入使用者名稱和密碼以登入。



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

🕝 https://market.androi 🔾	×
CISCO Identity Services Engine 1.1 Self-Provisioning Portal	peul Log Cut Abo
Device Registration This device has not been registered. To register this device, please enter the Device ID (MAC Address format nonnexe either A-F or a digit 0-19) and a description (optional). Please click the "Register" button to install and run the Cisco W-FI Setup Assistant application. This application will insi certificates and configures your device to use secure will network. Clicking the "Register" button will redirect you to an where you can download the Cisco W-FI Setup Assistant application.	unionion where in is tall all the necessary drold market place,
Device ID 98-0C-82-40-31-A9 Description	

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



6. 登入Google,然後點選**安裝**。



7. 按一下「**OK**」(確定)。



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



- 9. 確保您仍然從您的Android裝置登入到訪客門戶。
- 10. 按一下開始以啟動Wi-Fi設定助手。



11. Cisco SPW開始安裝證書。



12. 出現提示時,設定憑據儲存的密碼。



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

Certificate name							
Certificate name:							
paul							
Package contains One user key One user certificate							
ОК	Cancel						
Can	cel						

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

	111					
Certificate na	ame					
Certificate name: iseca Package contains One CA certificate						
ОК	Cancel					
paul is installed.						
Can	cel					

15. Android裝置現已連線。



我的裝置入口網站

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

完成以下步驟以將裝置列入黑名單:

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

CISCO My Devices Portal		
	Username Password	paul

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

Add a	New De	evice	To add a device, please ente (optional); then click submit	r the Device ID (MAC . to add the device.	Address) and a descrip	tion
		* Device ID				
			Submit	_		
Your De	vices					0
State	Device ID	Des	alption	Ac	tion	
	EB:06:88:97:0	9:41		Ed	n I Logez I 🗐	
					0	

3. 當ISE提示警告時,按一下Yes繼續。



4. ISE確認裝置已標籤為lost。



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

Live Authentications										
🚔 Add or Remove Columns =	😵 Raf	resh					Refresh Every	3 seconds *	Show Latest 20 records	*
Time •	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event	
Mar 25,12 12:49:07.851 AM	•	ò	paul	E8:06:88:97:09:41	WLC	Blacklist_Access	Blacklet		Authentication failed	
Mar 25,12 12:40:59.057 AM	•	ò	E8:06:08:97:09:41	EB-06-88:97:09-41	WLC	Blacklist_Access	Blacklet		Authentication falled	
Mar 95 10 10-40-54 107 AM		-		F0-04-00-00-01	WEC	Blackfet Access	Backlet		Authentication faled	

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

Identity Groups	Endpoint Group			
(م •	*Name Blacklist			
🗣 📰 📳 🚱 -	Description Blacklist Identity Group Parent Group Save Reset. Endpoints			
Endpoint Identity Groups				
💾 Blackåst				
Profiled				
RegisteredDevices	Identity Group Endpoints	Identity Group Endpoints		
	Add KRemove -			
	MAC Address			
	D			

完成以下步驟以恢復列入黑名單的裝置:

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



2. 當ISE提示警告時,按一下Yes繼續。



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



引用 — 證書

ISE不僅需要有效的CA根證書,還需要由CA簽署的有效證書。

完成以下步驟,以便新增、繫結和匯入新的受信任CA證書:

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

🛕 Home Operations 🔻 Policy 🔻	Administration 🔻			
🔆 System 🛛 👰 Identity Management	Network Resources	🛃 Web Portal Management		
Deployment Licensing Certificates	Logging Maintenance	Admin Access Settings		
Certificate Operations	/ Edit Add	Export XDelete		
🚭 Local Certificates	Friendly Name			
💩 Certificate Signing Requests	Default self-sig	Default self-signed server certificate		
S Certificate Authority Certificates				

2. 選擇Generate Certificate Signing Request(CSR)。



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



4. ISE驗證是否已生成CSR。



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



6. 選擇最近建立的CSR,然後按一下**匯出**。



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



8. 使用文本編輯器查詢並開啟ISE證書檔案。



9. 複製證書的整個內容。

· ·
BEGIN CERTIFICATE
MIICMzCCAZygAwIBAgIQT1/lPzR9C0W/lqfcJ2a4zTANBgkqhkiG9w0BAQUFADA1
MSMwIQYDVQQDExppc2UxMS1tbnIuY29ycC5yZi1kZW1vLmNvbTAeFw0xMjAzMTQw
MDIOMzFaFw0xMzAzMTQwMDIOMzFaMCUxIzAhBgNVBAMTGmlzZTExLW1uci5jb3Jw
LnJmLWR1bW8uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCnXTshW3Qu
BcvWrtGhB2pTJ19hHVOI607XH6AMlzrbYB/0b5wDW+QFixpgE+tLSn2gOKiieGJT
yGRvymY1HSBIz8QrW1+jBQPKxQ9ossvG98w7s/WQwnP7dKI0oK6kslTNRJZBnG48
U6GquDq/5V2+LmAVQyQfhluRdFD9PUkNTwIDAQABo2QwYjAMBgNVHRMEBTADAQH/
MAsGA1UdDwQEAwICrDAdBgNVHQ4EFgQUBJa5qgBccwF10GK0YwaGQB10qS0wEwYD
VR01BAwwCgYIKwYBBQUHAwEwEQYJYIZIAYb4QgEBBAQDAgZAMA0GCSqGSIb3DQEB
${\tt BQUAA4GBAKS+tyTCZiNKcXIygxHTWjepfDqWdoSZwFpYnGIwzoTzecGFRzfraZDi}$
1/t65UI0KQAyBRUp21TpHf+o27eDTVwW83bCmbDln0PpwhoKBMP7N8t+9uKuVcP1
osMN8EmLCVz2RPOTE4aKtkJe5oHF10Y/+vPrb1pMhPP2hbyekAIC
END CERTIFICATE
a cut
Coby Coby

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

G • Ø	https://10.10.10.10/certsrv/	Cer 😵 Cer
Windows Securit	y .	×
Connecting to 1	0.10.10.10.	
	administrator	
	Domain: KF17	
	Remember my credentials	
	ОК	Cancel

11. 按一下「Request a certificate」。



12. 按一下「advanced certificate request」。



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



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

Microsoft Certific	ate Services labsrv.corp.rf-demo.com		
Submit a Certificate Request or Renewal Request			
To submit a sav Saved Request	ved request to the CA, paste a base-64-encoded CN t box.		
Saved Request:			
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	MAsGA1UdDwQEAwICrDAdBgNVHQ4EFgQUBJa5qgBc VR01BAwwCgYIKwYBBQUHAwEwEQYJYIZIAYb4QgEB BQUAA4GBAKS+ <u>tyTCZiNKcXIygxHTWjepfDqWdoSZ</u> 1/t65UIOKQAyBRUp21TpHf+o27eDTVwW83bCmbD1 osMN8EmLCVz2RPOTE4aKtkJe5oHF10Y/+vPrb1pM END CERTIFICATE		
Certificate Temp	late:		
	Web Server		
Additional Attrib	ites:		
Attributes:			
	Submit >		

15. 按一下「Download certificate」。

Microsoft Active Directory Certificate Services corp-RFDEMO-CA
Certificate Issued
The certificate you requested was issued to you.
DER encoded or Base 64 encoded
Download certificate Download certificate chain

16. 儲存certnew.cer檔案;稍後將使用該檔案與ISE繫結。



17. 在ISE Certificates中,導航到Local Certificates,然後點選Add > Bind CA Certificate。
| 🛕 Home Operations 🔻 Policy 💌 Admin | istration 🔻 |
|---|--|
| 🔆 System 🛛 🖉 Identity Management 🛛 🔛 | Network Resources 🛛 🛃 Web Portal Management |
| Deployment Licensing Certificates Loggi | ng Maintenance Admin Access Settings |
| Certificate Operations | Local Certificates |
| Certificate Authority Certificates SCEP CA Profiles | Friend Import Local Server Certificate
Generate Self-Signed Certificate
Generate Certificate Signing Request |
| OCSP Services | Bind CA Certificate |

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

o

Certificate Operations Certificate Service Requests Certificate Service Requests	Local Certificates > Bind CA Signed Certificate Bind CA Signed Certificate Certificate
Certificate Authority Certificates SCEP CA Profiles	* Certificate File C:\Users\Paul Nguyen\Downloads\certnew(4).cer Browse_ Friendly Name
	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 A certificate being imported may be determined to already exist in the syst certificate Selections for the certificate. Cancel Cancel

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



20. 按一下「Download CA certificate」。

Microsoft Active Directory Certificate Services - cor				
Download a CA Certificate, Certificate Ch				
To trust certificates issued from this certification				
To download a CA certificate, certificate chair				
CA certificate:				
Encoding method:				
© DER				
Download CA certificate				

21. 將檔案儲存到本機電腦中。



22. 在ISE伺服器聯機時,轉到證書,然後按一下證書頒發機構證書。



23. 按一下「Import」(匯入)。



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

Certificate Authority Certificates > In Import a new Trusted (neort CA (Certificate Authority) Certificate
* Certificate File Friendly Name	C\Users\Paul Nguyen\Downloads\certnew.c Browse
All Certificate Authority Cert authentication below:	ificates are available for selection as the Root CA for secure LDAJ
Enable Validation of	Certificate Extensions (accept only valid certificate)
Description	

25. 確認已新增新的受信任CA證書。

🔆 System 🏼 🖉 Identity Management	Network Resources	🛃 Web Porta	al Managemer	
Deployment Licensing Certificates	.ogging Maintenance	Admin Access	Settings	
Certificate Operations	Certificate Authority Certificates			
Certificate Signing Requests	🖊 Edit 📲 Imp	ort Export	XDelete	
Sertificate Authority Certificates	Friendly Name			
🔹 SCEP CA Profiles	Corp-RFDEMO	corp-RFDEMO-CA#corp-RFDEMO-CA#00002		
🚭 OCSP Services	ise11-mnr.corp.rf-demo.com#ise11-mnr.corp			

相關資訊

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