适用于FlexConnect的无线BYOD部署指南

目录

简介 先决条件 要求 使用的组件 拓扑 设备注册和请求方调配 资产注册门户 自助注册门户 身份验证和调配 iOS调配(iPhone/iPad/iPod) Android调配 双SSID无线BYOD自助注册 单SSID无线BYOD自助注册 功能配置 WLAN 配置 FlexConnect AP配置 ISE 配置 用户体验—调配iOS 双SSID 单SSID 用户体验—调配Android 双SSID 我的设备门户 参考 — 证书 相关信息

简介

移动设备在计算能力上越来越强大,在消费者中越来越受欢迎。数以百万计的这些设备通过高速Wi-Fi销售给消费者,因此用户可以进行通信和协作。现在,消费者已经习惯了这些移动设备为他们的 生活带来的工作效率提升,并正在寻求将他们的个人体验带入工作空间。这就产生了在工作场所使 用自带设备(BYOD)解决方案的功能需求。

本文档提供BYOD解决方案的分支机构部署。员工使用新iPad连接到企业服务集标识符(SSID),并 被重定向到自助注册门户。思科身份服务引擎(ISE)根据公司Active Directory(AD)对用户进行身份验 证,并将具有嵌入式iPad MAC地址和用户名的证书以及请求方配置文件下载到iPad,该请求方配置 文件强制使用可扩展身份验证协议——传输层安全(EAP-TLS)作为dot1x连接的方法。根据ISE中的授 权策略,用户可以使用dot1x连接并访问适当的资源。 早于7.2.110.0的思科无线局域网控制器软件版本中的ISE功能不支持通过FlexConnect接入点(AP)关 联的本地交换客户端。版本7.2.110.0支持用于本地交换和集中身份验证客户端的FlexConnect AP的 这些ISE功能。此外,与ISE 1.1.1集成的版本7.2.110.0提供(但不限于)以下无线自带设备解决方 案功能:

- 设备分析和状态
- 设备注册和请求方调配
- 个人设备自注册(调配iOS或Android设备)

注意:虽然受支持,但本指南中不包括其他设备,例如PC或Mac无线笔记本电脑和工作站。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本:

- Cisco Catalyst交换机
- •思科无线局域网(WLAN)控制器
- •思科WLAN控制器(WLC)软件版本7.2.110.0及更高版本
- FlexConnect模式下的802.11n AP
- Cisco ISE软件1.1.1版及更高版本
- •带证书颁发机构(CA)的Windows 2008 AD
- DHCP 服务器
- 域名系统 (DNS) 服务器
- 网络时间协议 (NTP)
- •无线客户端笔记本电脑、智能手机和平板电脑(Apple iOS、Android、Windows和Mac)

注意:有关此软件版本的重要信息,请参阅<u>版本7.2.110.0的思科无线LAN控制器和轻量接入</u> <u>点版本说明</u>。在加载和测试软件之前,请登录Cisco.com网站查看最新的版本说明。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

拓扑

要正确实施和测试这些功能,需要最低限度的网络设置,如下图所示:



对于此模拟,您需要具有FlexConnect AP的网络、具有本地DHCP的本地/远程站点、DNS、 WLC和ISE。FlexConnect AP连接到中继以测试多个VLAN的本地交换。

设备注册和请求方调配

必须注册设备,以便其本地请求方可以调配dot1x身份验证。根据正确的身份验证策略,用户被重定 向到访客页面并通过员工凭证进行身份验证。用户将看到设备注册页面,该页面要求用户输入设备 信息。然后开始设备调配过程。如果调配不支持操作系统(OS),则用户将被重定向到资产注册门户 ,以将该设备标记为MAC身份验证绕行(MAB)访问。如果操作系统受支持,注册过程将开始并配置 设备的本地请求方进行dot1x身份验证。

资产注册门户

资产注册门户是ISE平台的元素,允许员工通过身份验证和注册流程启动终端自注册。

管理员可以从终端身份页面删除资产。每位员工都可以编辑、删除已注册的资产并将其列入黑名单 。列入黑名单的终端被分配到黑名单身份组,并且创建授权策略以阻止列入黑名单的终端访问网络 。

自助注册门户

在中心Web身份验证(CWA)流程中,员工被重定向到允许他们输入其凭证、进行身份验证和输入他 们希望注册的特定资产的细节的门户。此门户称为自助调配门户,类似于设备注册门户。它允许员 工输入MAC地址以及有意义的终端描述。

身份验证和调配

一旦员工选择自助注册门户,他们便需要提供一组有效的员工凭证以继续进入调配阶段。身份验证 成功后,终端可以调配到终端数据库中,并为终端生成证书。页面上的链接允许员工下载 Supplicant客户端引导向导(SPW)。

注意:请参阅Cisco<u>的FlexConnect功</u>能矩阵文章,以便查看BYOD的最新FlexConnect功能矩 阵。

iOS调配(iPhone/iPad/iPod)

对于EAP-TLS配置,ISE遵循Apple Over-the-Air(OTA)注册流程:

- •身份验证成功后,评估引擎将评估客户端调配策略,从而生成请求方配置文件。
- 如果请求方配置文件用于EAP-TLS设置,则OTA进程确定ISE是使用自签名还是由未知CA签名
 。如果其中一个条件为true,则要求用户下载ISE或CA的证书,然后才能开始注册过程。
- 对于其他EAP方法,ISE在身份验证成功后推送最终配置文件。

Android调配

出于安全考虑,Android代理必须从Android市场网站下载,并且不能从ISE调配。思科通过Cisco Android marketplace发布者帐户将向导的候选版本上传到Android市场。

这是Android调配过程:

- 1. 思科使用软件开发套件(SDK)创建扩展名为.apk的Android软件包。
- 2. 思科将软件包上传到Android市场。
- 3. 用户使用适当的参数配置客户端调配中的策略。
- 4. 注册设备后,当dot1x身份验证失败时,最终用户将重定向到客户端调配服务。
- 5. 调配门户页面提供将用户重定向到Android市场门户的按钮,用户可以在该门户下载SPW。
- 6. Cisco SPW启动并执行请求方的调配: SPW发现ISE并从ISE下载配置文件。SPW为EAP-TLS创建证书/密钥对。SPW向ISE发出简单证书注册协议(SCEP)代理请求调用并获取证书。 SPW应用无线配置文件。如果成功应用配置文件, SPW将触发重新身份验证。SPW退出。

双SSID无线BYOD自助注册

双SSID无线BYOD自注册过程如下:

- 1. 用户与访客SSID关联。
- 2. 用户打开浏览器并重定向到ISE CWA访客门户。
- 3. 用户在访客门户中输入员工用户名和密码。
- 4. ISE对用户进行身份验证,并根据他们是员工而不是访客的事实,将用户重定向到Employee Device Registration访客页面。
- 5. MAC地址预填充到设备ID的设备注册访客页面中。用户输入说明,并在需要时接受可接受的使 用策略(AUP)。

- 6. 用户选择Accept并开始下载和安装SPW。
- 7. 该用户设备的请求方将与所有证书一起调配。
- 8. 发生CoA,设备重新关联到企业SSID(CORP)并使用EAP-TLS(或用于该请求方的其它授权方 法)进行身份验证。

单SSID无线BYOD自助注册

在此方案中,企业接入(CORP)使用单个SSID,同时支持受保护的可扩展身份验证协议(PEAP)和 EAP-TLS。没有访客SSID。

以下是单SSID无线BYOD自注册过程:

- 1. 用户与CORP关联。
- 2. 用户向PEAP身份验证的请求方输入员工用户名和密码。
- 3. ISE对用户进行身份验证,并根据PEAP方法,提供接受授权策略并重定向到Employee Device Registration访客页面。
- 4. 用户打开浏览器并重定向到Employee Device Registration guest页面。
- 5. MAC地址预填充到设备ID的设备注册访客页面中。用户输入说明并接受AUP。
- 6. 用户选择Accept并开始下载和安装SPW。
- 7. 该用户设备的请求方将与所有证书一起调配。
- 8. 发生CoA,设备重新关联到CORP SSID并使用EAP-TLS进行身份验证。

功能配置

完成以下步骤以开始配置:

1. 对于本指南,请确保WLC版本为7.2.110.0或更高版本。

ll cisco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS
Monitor	Summary					
Summary Access Points Cisco CleanAir Statistics CDP Rogues				Cisco 250	D Series Wireless C	Controller Model 2504
Clients	Controller Summa	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 Image Version	1.0.0		A	shoc Rogues	
	System Name	wic-11mm		R	gues on wired Net	WORK

2. 导航到Security > RADIUS > Authentication, 然后将RADIUS服务器添加到WLC。

ululu cisco	MONITOR	WLANS C	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP EEEOBA	CK
Security	RADIUS	Authentica	tion Serve	rs					
AAA General RADIUS Authentication Accounting Fallback TACACS+	Call Stat Use AES MAC Del	ion ID Type I Key Wrap imiter	System M (Designed Hyphen	AC Address 1 for FIPS custome	rs and require	is a key wrap com	oliant RADIUS ser	iver)	
LDAP	User	Management	Index	Server Addre	ss Port	19	Sec	Admin Status	
MAC Filtering Disabled Clients User Login Policies	2	2	1	10.10.10.60	1812	D	sabled	Enabled	

3. 将ISE 1.1.1添加到WLC:

输入共享密钥。将Support for RFC 3576(对RFC 3576的支持)设置为**Enabled**。

MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBAC
RADIUS	Authenti	ication Server	rs > Edit					
Server In	dex		1					
Server A	ddress		10.10.10.60	0				
Shared S	ecret Forma	at	ASCII :					
Shared S	ecret							
Confirm 5	Shared Secr	ret						
Key Wrap		6	(Designed f	or FIPS custom	ers and requires a	key wrap complia	nt RADIU	IS server)
Port Num	ber		1812					
Server St	tatus		Enabled	۵.				
Support f	for RFC 357	6	Enabled	•				
Server Ti	meout		2 secon	nds				
Network	User		S Enable					
Managem	nent		S Enable					
IPSec			Enable	5				

4. 添加与RADIUS记账服务器相同的ISE服务器。

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. 创建稍后在ISE策略中使用的WLC预身份验证ACL。导航到WLC > **Security** > Access Control Lists > **FlexConnect ACLs**,然后创建名为**ACL-REDIRECT**的新FlexConnect ACL(在本例中)。

cisco		<u>W</u> LANs		WIF
Security	FlexConr	nect Aco	cess Control Li	ists
 AAA Local EAP Priority Order Certificate 	Acl Name	ECT		
Access Control Lists Access Control Lists CPU Access Control Lists FlexConnect ACLs Wireless Protection Policies				

6. 在ACL规则中,允许所有流入/流出ISE的流量,并在请求方调配期间允许客户端流量。

对于第一条规则(序列1):

将Source设置为Any。设置IP(ISE地址)/网络**掩码255.255.255.255**。将Action设置为 Permit。

Access Control	Lists > 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 ‡		

对于第二个规则(序列2),将源IP(ISE地址)/掩码255.255.255.255设置为**Any**,将操作设 置为**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	1	Any	Any	Any	Any	

7. 创建名为Flex1的新FlexConnect组(在本例中):

导航到FlexConnect Group > WebPolicies选项卡。在WebPolicy ACL字段下,单击Add,然后 选择ACL-REDIRECT或之前创建的FlexConnect ACL。确认它填充了WebPolicy Access Control Lists 字段。

ululu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBA	Sage Configuration Bing Legout Befi ICK
Wireless	FlexConnect Groups > Edit 'Flex1'	< Back Apply
Access Points All APs Radios Rol 11a/n	General Local Authentication Image Upgrade VLAN-ACL mapping WLAN-ACL mapping	WebPalicies
802.11b/g/h Global Configuration	WebPolicies	
Mesh RF Profiles	WebPolicy ACL ACLARDORECT	
HexConnect Groups HexConnect ACCI > 802.11a/n	WebPolicy Access Control Lists ACL-REDIRECT	
 > 802.11b/g/n > Media Stream 		

8. 单击Apply和Save Configuration。



ſ

- 1. 创建双SSID的开放式WLAN SSID示例:
 - 输入WLAN名称:**DemoCWA**(在本例中)。为Status选择**Enabled**选项。

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. 导航到Security选项卡> Layer 2选项卡,并设置以下属性:

第2层安全: 无 MAC过滤: 启 用	(复选框为选中状态))快速过渡: 禁用 ((未选中框)

eneral	security	Qu5 Advan	ceo
Layer 2	Layer 3	AAA Servers	
Layer 2	Security 🤨 🚺	lone	
	M	AC Filtering2 🔽	
Fast Tran	sition		

3. 转至AAA Servers选项卡,并设置以下属性:

身份验证和帐户服务器:已**启用**服务器1:<ISE IP地址>

LANs > E	dit 'Demo	CWA'			
General	Security	QoS Advanc	ced		
Layer 2	Layer 3	AAA Servers			
Colock AAA	convers hele	who associate uses a	of default concore of	-	Inter MILANI
Radius Se Radius	servers belo rvers Server Overw	w to override use o	of default servers o	nt	his WLAN
Radius Se Radius	servers belo rvers Server Overw	w to override use o ite interface □Enat Authe 愛 Ena	of default servers o bled intication Servers	nt	Accounting Servers
Select AAA Radius Se Radius Server	servers belo rvers Server Overwi 1	ite interface Enat Auther Final Ena	bled ntication Servers abled .10.10.60, Port:1812	:	Accounting Servers Enabled IP:10.10.10.60, Port:1813
Select AAA Radius Se Radius Server Server	servers belo rvers Server Overwi 1 2	ite interface Enat Auther IP:10.	of default servers o bled intication Servers abled .10.10.60, Port:1812	: :	Accounting Servers Enabled IP:10.10.10.60, Port:1813 None

4. 从AAA Servers选项卡向下滚动。在Web-auth用户的Authentication priority order下,确保将 RADIUS用于身份验证,而不使用其他身份验证。

			iutii usei
ication	Order Used For Authenti		Not Used
Up	RADIUS	>	LOCAL LDAP
t	RADIUS	>	LOCAL LDAP

5. 转到Advanced选项卡,并设置以下属性:

ANs > Edit 'DemoC\	QoS Advanced	
Allow AAA Override	₩ Enabled	846.9
Coverage Hole Detection	P Enabled	ENCP Server Covers
Enable Section Timeout	gr (1000 Session Timesult (secs)	DHCP Adds. Assignment C. Annuel
Aironat IE	P Enabled	Nananament France Protection (1973)
Diagnostic Channel	l''Evabled	Construction of Construction of Construction
Override Interface ACL	(Fold None R (Fold None R	MPP Clant Protection # Optional
F2F Blocking Action	Disabled B	BTIPs Period (in beacan intervals)
Client Exclusion	["Evabled	
Maximum Allowed Clients	F	802.33.wh (3 - 250) [3 802.338/g/n (3 - 250) [3
Static IP Tunneling 👪	Finalised	NAC
Wi-Fi Direct Clients Policy	Doubled 1	NAC State Radius NAC 💌
Recimum Allowed Clearly Fer AF Radio	[200	Clast Load Balancing

注意:当FlexConnect AP处于断开模式时,不支持RADIUS网络准入控制(NAC)。因此,如果

FlexConnect AP处于独立模式且失去与WLC的连接,所有客户端都会断开连接,并且不再通告SSID。

6. 在Advanced(高级)选项卡中向下滚动,并将FlexConnect Local Switching(FlexConnect本 地交换)设置为**Enabled**。



7. 单击Apply和Save Configuration。



8. 为单和双SSID场景创建名为Demo1x(在本例中)的802.1X WLAN SSID。

WLANs > Edit 'Demo	1x'
General Security	QoS Advanced
Profile Name	Demo1x
Туре	WLAN
SSID	Demoix
Status	Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under secu
Radio Policy	All
Interface/Interface Group(G)	management 💌
Multicast Vlan Feature	Enabled
Broadcast SSID	F Enabled

9. 导航到Security选项卡> Layer 2选项卡,并设置以下属性:

第2层安全:WPA+WPA2快速过渡:禁用(未选中框)身份验证密钥管理:802.IX:启用

WLANs > E	dit 'Demo	1x'					
General	Security	QoS	Advand	ced			
Layer 2	Layer 3	AAA S	ervers				
Layer 2	Layer 2 Security 🗐 WPA+WPA2						
	M	AC Filtering	2				
Fast Trans	sition						
Fast Transit Over the D	s D						
Reassociati	on Timeout 20						
WPA+WPA	2 Parameter	s					
WPA Po	licy						
WPA2 P	olicy	5					
WPA2 E	WPA2 Encryption RAES TKIP						
Authentica	ation Key Ma	nagemen	t				
802.1X	ع جا	nable					
CCKM	Π ε	nable					
PSK	Πe	nable					

10. 转到Advanced选项卡,并设置以下属性:

允许AAA覆盖:启用NAC状态:Radius NAC

Allow AAA Override	F Enabled	DHCP
Coverage Hole Detection	W Enabled	DHCP Server Coverside
Enable Excelon Timeout	(p) (1800 Session Timeout (sess)	DHCP Adds. Assignment Required
Airunet III	\$ Evalued	Natagement Frame Protection (NFP)
Diagnostic Channel	Cenative	
Dverride Interface ACL	Mod None B Mot None B	MPP Classit Profestion # Optional 18
P2P Blocking Action	Disabled R	BTIPs Period (in beacon intervals)
Client Evolusion 8	P Enabled Tenanut Value (secc)	Million and Annual A
Recimum Alfored Claims	P	802.113/g/h (1 - 299) [1
and a large state of the	English	NAC
Contraction of the second seco		

11. 在Advanced选项卡中向下滚动,并将FlexConnect Local Switching设置为Enabled。

ElexConnect	a. 100
FlexConnect Local Switching ²	Enabled
Shicking	· / manu

12. 单击Apply和Save Configuration。



13. 确认已创建两个新WLAN。

MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
WLANs								Entries 1 - 5 of 2
Current Filt	ter: No	ne [Change	Filter] [Clear	Filter]		Create New	• 6	0
_							Admin	
U WLAN I	D Type	Profile Na	me	v	VLAN SSID		Status	Security Policies
E 1	WLAS	85×			EEH.		Disable	[[w#a2][auth(802.12)]
C 2	WLAN				1		Enabled	[#P&2][Auth(P5x)]
□ <u>2</u>	WLAN	Demo1x		C	Demo1x		Enabled	[WPA2][Auth(802.1X)]
□ <u>4</u>	WLAN	DemoCWA		D	DemoCWA		Enabled	MAC Filtering
E 1	101,475	Her:			la c		Oreables	d Wab-Auth

FlexConnect AP配置

要配置FlexConnect AP,请完成以下步骤:

1. 导航到WLC > Wireless,然后点击目标FlexConnect AP。

	<u>W</u> LANs		WIRELESS
All APs			
Current Fi	lter		None
Number o	of APs		2
AP Name		AP	Model
<u>Site-B-Fley</u>	(AP (b)	AI	R-LAP1262N-A-K

2. 单击FlexConnect选项卡。

MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	EEE
All APs >	Details f	or Site-B-Flex	AP					
General	Cred	nilais Inter	faces Hig	ph Availabilit	a Investory	FlexConne	ct	Advan
						4		

3. 启用VLAN支持(选中此框),设置本地VLAN ID,然后点击**VLAN映射**。

VLAN Support	v	
Native VLAN ID	1	VLAN Mappings
FlexConnect Group Name	Not Confi	gured 62

4. 将SSID的VLAN ID设置为21(在本例中)以用于本地交换。

ONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY
All APs	> Site-B	FlexAP > VLA	N Mapping	S
AP Nam	e	Site-B-FlexAP		
Base Ra	dio MAC	e8:04:62:0a:68:80	0	
WLAN Id	SSID			VLAN ID
3	Demo1x			21
4	DemoCW	A		21
	-			and the second s

5. 单击Apply和Save Configuration。

ISE 配置

完成以下步骤以配置ISE:

1. 登录ISE服务器:<https://ise>。

	Identity Services Engine Uservane admin Paswood Resented Resented Resented Resented Resented Reservane Res
affliates in the U.S and certain other countries.	cisco

2. 导航到管理 > 身份管理 > 外部身份源。



3. 单击Active Directory。



4. 在Connection选项卡中:

添加corp.rf-demo.com的域名(在本例中),并将身份库名称默认为AD1。单击Save Configuration。单击Join,并提供加入所需的AD管理员帐户用户名和密码。"状态"必须为绿色 。启用Connected to:(复选框处于选中状态)。

Connection	Advanced 9	Settings	Groups	Attribut	85	
		* Do	main Name	corp.rf-demo.	com	
		* Identity	Store Name	AD1		
e or more nodes nnection.	may be selec	ted for Join	or Leave ope	rations. If a no	de is joined th	en a leave operation
e or more nodes nnection. È Join 🛛 👷 Leave	may be selec	onnection +	or Leave ope	rations. If a no	de is joined th	en a leave operation
e or more nodes nnection. È Join 92 Leave ISE Node	may be selec	onnection +	or Leave ope	rations. If a no	de is joined th	en a leave operation

5. 使用当前域用户对AD执行基本连接测试。

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

6. 如果成功连接到AD,则会显示一个对话框,确认密码正确。



- 7. 导航到管理 > 身份管理 > 外部身份源:
 - 点击**证书身份验证配置文件**。单击Add以获取新的证书身份验证配置文件(CAP)。

CISCO Identity Services Engine	
🛕 Home Operations 🔻 Policy 🔻 A	dministration 🔻
🔆 System 🏾 👰 Identity Management	Network Resources 🛛 🛃 Web Portal Manage
Identities Groups External Identity Sour	ces Identity Source Sequences Settings
External Identity Sources	Certificate Authentication Profile
🔶 🗐 🗐	- I co date Di Dutinta Ma
Certificate Authentication Profile	· · · · · · · · · · · · · · · · · · ·
Active Directory	Name 🐱
CDAP CDAP	
a RADIUS Token	•
RSA Securit	

8. 为CAP输入名称**CertAuth**(在本例中);对于Principal Username X509 Attribute,选择 **Common Name**;然后单击**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 LDAP/AD Instance Name	arison with Certificate retrieved from	n LDAP or Active Directory
Submit Cancel		

9. 确认已添加新的CAP。

CISCO Identity Services Engine	
🍐 Home Operations 🔻 Policy 🔻 Adminis	stration 🔻
🔆 System 🦉 Identity Management 📰 !	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 💿	Certinan
RADIUS Token 💿	
RSA SecurID 🛞	

10. 导航到Administration > Identity Management > Identity Source Sequences,然后单击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. 为序列指定名称TestSequence(在本例中)。

cisco Ide	entity Services Engine
💧 Home 🤇	Operations Policy Administration
🔆 System	Veb Portal Mana
Identities G	Troups External Identity Sources Identity Source Sequences Settings
Identity Source Sequ Identity Source Identity Source	ences List > New Identity Source Sequence rce Sequence urce Sequence
* Name	TestSequence
Description	
 Certificate 	Based Authentication

12. 向下滚动到Certificate Based Authentication:

启用Select Certificate Authentication Profile(复选框处于选中状态)。选择CertAuth(或之前创建的其他CAP配置文件)。

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

13. 向下滚动到Authentication Search List:

将AD1从"可用"移动到"选定"。点击向上按钮将AD1移至最高优先级。

 Authentication Search List 		
A set of identity sources that will be accesse	d in sequence until first authentication succeeds	
Available	Selected	
	Internal Users Internal Endpoints	$\overline{\mathbf{x}}$
×		× ×

14. 单击Submit进行保存。

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: Cancel

15. 确认已添加新的身份源序列。

cisco Identity Services Engine	all all a	0.00
🛕 Home Operations 🔹 Policy 💌 Administrat	tion 🔻	
🔆 System 🛛 🖉 Identity Management 🖉 Netw	vork Resources 🚯 Web Portal Management	
Identities Groups External Identity Sources	Sentity Source Sequences Settings	
Identity Source Sequence		
And deal Departure Martin		
A rost where all orthogon to posts		
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 Endpoint

16. 使用AD验证我的设备门户。导航到ISE > Administration > Identity Management > Identity Source Sequence, 然后编辑MyDevices_Portal_Sequence。

🔆 System 🏾 👰 Identity Management	🖥 Network Resources 🛛 🛃 Web
Identities Groups External Identity Source	s Identity Source Sequences
dentity Source Sequence	
dentry obtaile ocquerice	
dentry oou ce oequence	
/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. 将AD1添加到Selected列表,然后单击up按钮将AD1移动到最高优先级。



18. Click Save.



19. 确认MyDevices_Portal_Sequence的身份库序列包含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. 重复步骤16-19以添加Guest_Portal_Sequence的AD1,然后单击Save。



21. 确认Guest_Portal_Sequence包含AD1。

o

Name .	Description	Identity Stores
Guest_Portal_Sequence	A Built-in Identity Sequence For The Guest Portal	Internal Users, AD1
		and the second second second second

22. 要将WLC添加到网络接入设备(WLC),请导航到管理 > 网络资源 > 网络设备,然后单击添加

CISCO Identity Services Engine	
A Home Operations ▼ Policy ▼ Admin System ♣ Identity Management ♣	Istration V
Network Devices Network Device Groups Ext	ernal RADIUS Servers RADIUS Server Sequences S
Network Devices	Network Devices
به ه.	/ Edit 🚽 Add 🖓 Duplicate 👔 Import 🚱
Network Devices	Name IP/Mask Location
Default Device	

23. 添加WLC名称、IP地址、子网掩码等。

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 	e Group
Location	All Locations 📀 Set To Default
Device Type	All Device Types 📀 Set To Default

24. 向下滚动到Authentication Settings,然后输入Shared Secret。这必须与WLC RADIUS的共 享密钥匹配。

•	▼ Authentication Settings		
	Enable Authentication Settings Protocol	RADIUS	
	* Shared Secret	•••••	Show
	Enable KeyWrap		
	 Key Encryption Key 		Show
	 Message Authenticator Code Key 		Show
	Key Input Format	ASCII HEXADECIM	AL
	SNMP Settings		
	SGA Attributes		
Sub	mit Cancel		

- 25. 单击"Submit"。
- 26. 导航到ISE > Policy > Policy Elements > Results。

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

27. 展开Results和Authorization,单击Authorization Profiles,然后单击Add以获取新的配置文件

cisco Identity Services Engine	
🛕 Home Operations 🔻 Policy 🔻 Adr	ninistration 🔻
其 Authentication 👩 Authorization	Profiling 🕜 Posture 😡 Client Provisioning
Dictionaries Conditions Results	
Results	Standard Authorization Profiles
(+- ■ 1 = 1 · · · · · · · · · · · · · · · · ·	/ Edit Add Duplicate X Delete
Authentication	Blacklist_Access
Authorization	Gisco_IP_Phones
 Authorization Profiles 	ContractV12
🤬 Blacklist_Access	DenvAccess

28. 为此配置文件指定以下值:

名称:CWA

o

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

启用Web身份验证(选中此框):

Web身份验证:集中ACL:**ACL-REDIRECT**(必须与WLC预身份验证ACL名称匹配。)重定 向:默**认**

 Common Tasks 							
DACL Name							
Voice Domain Permissio	n						
Web Authentication	Centralized	•	ACL	ACL-REDIRECT	Redirect	Default	¥

29. 单击Submit,并确认已添加CWA授权配置文件。



30. 单击Add以创建新的授权配置文件。



- 31. 为此配置文件指定以下值:
 - 名称:调**配**

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

启用Web身份验证(选中此框):

Web身份验证值:请求**方调配**

Common Tasks					
DACL Name					
Voice Domain Permission	on				
Veb Authentication	Centralized	Ŧ	ACL		
	Centralized				
Auto Smart Port Device Registration					
Posture Discovery					
- Filter-ID	Supplicant Provisioning	Day			
1		2			

ACL:ACL-REDIRECT(必须与WLC预身份验证ACL名称匹配。)

 Common Tasks 			
DACL Name			
U VLAN			
Voice Domain Permission			
✓ Web Authentication	Supplicant Provisioning	ACL	ACL-REDIRECT
C Auto Smort Bort			

32. 单击Submit,并确认已添加调配授权配置文件。

Standard Authorization Profiles							
1	Edit -Add	Duplicate	×				
	Name						
	Blacklist_Access	3					
	CWA						
	-						
	Provis. m						

33. 在Results(结果)中向下滚动,展开Client Provisioning,然后单击Resources。



34. 选择Native Supplicant Profile。



35. 为配置文件指定名称WirelessSP(在本例中)。

Native Supplicant Profi	e
* Name	WirelessSP
Description	

36. 输入以下值:

连接类型:无**线**SSID:**Demo1x**(此值来自WLC 802.1x WLAN配置)允许的协议:**TLS**密钥 大小:**1024**

Operating System	ALL 💠		
Connection Type	Wired		
	Vireless		
		*SSID	Demoix
		Security	WPA2 Enterprise +
* Allowed Protocol	PEAP		v
Optional Settings	TLS PEAP	ę	9
Submit Cancel			

- 37. 单击"Submit"。
- 38. Click Save.

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

39. 确认已添加新配置文件。

/ Edit 🕂 Add 🗸	Duplicate	XDelete
Name		Туре
Menter		NativeSDDrefil

40. 导航到**策略 > 客户端调配**。



41. 为iOS设备的调配规则输入以下值:

规则名称:iOS身份组: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

操作系统:Mac iOS All

Operating System Group	ps
	Q
∲•	\$\$~
Android	
Mac OSX	1
Mac iOS All	
🚞 Windows All	۲

结果:WirelessSP(这是之前创建的本地请求方配置文件)

Results
then Result 🕀 🦿

导航到**结果 > 向导配置文件**(下拉列表) > WirelessSP。



WizardProfile							
	R						
◆ • ■ '≣	<u>`</u> `						
Clear Selection							
Wireless							

42. 确认已添加iOS调配配置文件。

		Rule Name	I	Identity G	roups		Operating System	ms		Other Conditions		Results	
2	٠	IOS	If [Any	\diamond	and	Mac IOS All	\diamond	and	Condition(s)	\$ then	WrelessSP	\diamond

43. 在第一个规则的右侧,找到Actions下拉列表,然后选择**Duplicate below(或**above)。



44. 将新规则的Name更改为Android。



45. 将操作系统更改为Android。



- 46. 保留其他值不变。
- 47. 单击**Save**(左下屏幕)。



48. 导航到ISE > Policy > Authentication。



49. 修改条件以包括Wireless_MAB,然后展开Wired_MAB。



50. 单击Condition Name下拉列表。



51. 选择Dictionaries > Compound Condition。



52. 选择Wireless_MAB。



53. 在规则右侧,选择要展开的箭头。

: If	Wireless_MAB	¢	allow protocols	Allowed Protocol : Default Netw	and	R

54. 从下拉列表中选择以下值:

身份源:**TestSequence**(这是之前创建的值)如果身份验证失败:拒**绝**如果找不到用户:继 **续**如果进程失败:丢**弃**

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

55. 转到Dot1X规则,然后更改以下值:

	2	٠	Dot1X	: If	Wired_802	.1X ⊕	allow protocol
L			Default Rule (If no match)	: al	low protocols	Allowed Protocol : Default Ne	

Con	npound Condition		
	(م		
4	/ 🔳 📜 👘 🎡 -		
	Wired_MAB		
	Wireless_MAB		
	Wired_802.1X		
Wireless_802.1X Switch_Local_Web_Authentication			
: If : all	Wired_802.1X allo		
	Condition Name Wireless_802.1X		

条件:Wireless_802.1X

身份源:TestSequence

Identity Source TestSequence	se for authe
Options	Identity Source List
If authentication failed Reject	
If user not found Reject	
If process failed Drop 💌	€• ■ 1 =
Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS	Internal Endpoints
it is not possible to continue processing when authentication fails	Internal Users
If continue option is selected in these cases, requests will be reject	Guest_Portal_Sequence
	Sponsor_Portal_Sequence
	MyDevices_Portal_Sequence
	TestSequence
Internal Users	CertAuth
	DenyAccess

56. Click Save.



57. 导航到ISE > Policy > Authorization。



58. 默认规则(例如Black List Default、Profiled和Default)已在安装中配置;前两个规则可以忽略;默认规则将在以后进行编辑。

rst M	latched R	ule Applies 🔹			
Exc	eptions (0)			
Sta	ndard				
	Status	Rule Name	Conditions (identity groups and other conditions)		Permissions
		Black List Default	f Blacklist	then	Blacklist_Access

59. 在第二条规则(已分析的思科IP电话)的右侧,点击编辑旁边的向下箭头,然后选择Insert New Rule Below。



添加新的标准规则编号。

St	tatus	Rule Name	Conditions (identity groups and other conditions)	Permissions
•		Black List Default	f Blacklist	then Blacklet_Access
	3	Profiled Cisco IP Phones	Cisco-IP-Phone	then Osco_JP_Phones
12	- [Standard Rule 1	f Any \Diamond and Condition(s) \Diamond	then AuthZ Profil 💠
2	1	Default	if no matches, then PermitAccess	

60. 将Rule Name从Standard Rule #更改为**OpenCWA**。此规则在开放式WLAN(双SSID)上为 进入访客网络的用户启动注册过程,以便调配设备。



61. 单击"条件"的**加号**(+),然后单击"从库中选择现有条件"(Select Existing Condition from Library)。

t Cisco-IP-Phone then Cis					
f Any	¢	and	Select Condition	then AuthZ Pro	
i no matches, t		Perm	Select Ex	isting Condition from Library 👔 🕜 Create	

62. 选择**复合条件 > Wireless_MAB**。

er conditions. Drag and drop	Compound Conditions
	(م
	🔶 🗐 🗐 🛞 🔬
	Wired_802.1X
	Wired_MA8
	Wireless_802.1X
ups and other conditions)	Wireless_MAB
	Catalyst_Switch_cocal_Web_Authentica
	WLC_Web_Authentication 5
Select Condition	h
Add All Conditions B	
Condition Name	
Select Condition	

63. 在AuthZ配置文件中,点击加号(+),然后选择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. 选择标准CWA(这是之前创建的授权配置文件)。

Standard	
	<u>م</u>
⇔- ≣ '≣	ŵ ∙
CWA flm	
Circo D Dhanar	

65. 确认添加的规则具有正确的条件和授权。

1 -	OpenCWA	Any	0 and	Wireless MAB	O the	CWA	4
# 0100 mm 00000							

66. 单击Done(在规则的右侧)。



67. 在同一规则的右侧,点击Edit旁边的向下箭头,然后选择Insert New Rule Below。

Edit I 👻	
Insert New Rule Above	
Insert New Rule Below	
Duplicate Above 🛛 🖤	

68. 将Rule Name从Standard Rule #更改为**PEAPrule**(在本例中)。此规则用于PEAP(也用于 单SSID方案)检查没有传输层安全(TLS)的802.1X身份验证,并且网络请求方调配由之前创 建的调配授权配置文件启动。

🖉 🗹 OpenCWA	f Wireless_MAB	then CWA
🖉 👻 🔹 Standard Rule 1	Any 💠 and Condition(s) 🔶	then AuthZ Profil 💠

69. 将Condition(条件)更改为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	- ∰•

70. 单击条件右侧的齿轮图标,然后选择**添加属性/值**。这是一个"and"条件,而不是"or"条件。



71. 找到并选择Network Access。

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

72. 选择AuthenticationMethod,然后输入以下值:

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

AuthenticationMethod:等于

Network Access:Au💟	-
	Equals
	Not Equals 💟

选择MSCHAPV2。

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

这是规则的示例;请务必确认Condition为AND。

and	Condition(s)	🗢 then AuthZ Profil 💠		
	Condition Name	Expression	AND	
	Wireless_802.1X 📀	Radius:Service-Type EQUALS Framed AND Radius:NAS-Port		ŵ .
	♦	Network Access:Au Equals MSCHAPV2	0	ŵ .

73. 在AuthZ Profile中,选择**Standard > Provision**(这是之前创建的授权配置文件)。

then	AuthZ Profil	Done
	Select an item 📀 🔤 a	<u>f</u>

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. 单击Done。



75. 在PEAPrule的右侧,点击Edit旁边的向下箭头,然后选择Insert New Rule Below。



- 76. 将Rule Name从Standard Rule #更改为**AllowRule**(在本例中)。此规则将用于允许访问安装 了证书的已注册设备。
 - Any 💠 and Condition(s) 💠 then AuthZ Profil... 💠
- 77. 在Conditions(s)下,选择Compound Conditions。



78. 选择Wireless_802.1X。



79. 添加AND属性。

Wireless_802.1X	⇔ then the	
Add All Conditions Below	w to Library	
Condition Name	Expression	
Wireless_802.1X 📀	Radius:Service-Type EQUALS Framed AND Radius:NAS-Port	B -

80. 单击条件右侧的齿轮图标,然后选择添加属性/值。



81. 找到并选择Radius。

A			Dictionaries	
	U.S.		ۥ	
Client Provisioning 🔄 Sec	urity Group Ac	cess 🧠 🙇	Care	
			Caco-dettre	
			Caco-sPACKER	
		then	anace -	
		then	EndPoints	
			iuest 😜	
etwork Access:AuthenticationN	lethod	then	Likelity-Group	
Wireless 802.1X Network Acc	ess A	5	2 Internal.teer	
			Moreault	
Condition Name	Expressio	on	Retwork Access	AND V
			Radius	
Wireless_802.1X 📀	Radius:Ser	vice-Type E	Sectors 1	20-
♦	Select /	Attribute 📀		o

82. 选择Calling-Station-ID---[31]。



83. 选择**Equals**。

Radius:Service-Type EQUALS	5 Framed AND Radius:NAS-	Port
Radius:Calling-Statio	Equals h	•

84. 转到CERTIFICATE,然后单击向右箭头。



85. 选择Subject Alternative Name。



86. 对于授权配置文件,请选择**标准**。

	Profiles	
		٩
	◆- ■ '≡	ŵ.,
Elements	🔜 Julie Posture Node	
,	📒 Incety Group	
	Standard	R
_IP_Phones		0
sion		
AuthZ Profil 🗢		
Select an item	4	

87. 选择**允许访问**。



88. 单击**Done**。



以下是规则示例:

1	OpenCHA /	Weeks, Mill	ther	CHR
-	Riha i	Windex, 802.51 (10) Network Access Authenticator/Hethod 802.04.5 HIGHNIPV2)		Provision
1	AllowRule	Wireless_802.1X Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name	then	PermitAccess

89. 找到Default规则以将PermitAccess更改为DenyAccess。



90. 单击Edit以编辑Default规则。



91. 转到PermitAccess的现有授权配置文件。



92. 选择Standard。



93. 选择DenyAccess。

Sta	ndard
4	· 🗐 🗉
8	Bacillet_Access Cash
õ	Caco, JP , Phones
	DenyAccess
9	Decovery V

94. 如果找不到匹配项,请确认Default规则具有DenyAccess。



95. 单击**Done**。



这是此测试所需的主要规则的示例;适用于单SSID或双SSID场景。

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

96. Click Save.



97. 导航到**ISE > Administration > System > Certificates**,以便使用SCEP配置文件配置ISE服务 器。



98. 在Certificate Operations中,单击SCEP CA Profiles。



99. 单击 Add。



100. 为此配置文件输入以下值:

名称:**mySCEP**(在本示例中)URL: **https://**<*ca-server*>/**CertSrv/mscep/**(请检查CA服务 器配置中的正确地址。)

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

101. 单击测试连接以测试SCEP连接的连接。



102. 此响应显示服务器连接成功。



103. 单击"Submit"。



104. 服务器响应已成功创建CA配置文件。

1		d	XX
1	~	Server Response	
4	arms	CA Profile created successibility	(0)

105. 确认已添加SCEP CA配置文件。

SCEP CA Profiles			4 8
/Edt +Add XDelete		Show All	- 8
Name Name	Description	URL	CA Cert Name
MySCEP		https://10.10.10.10/certsrv/mscep	RFDemo-MSCE

用户体验 — 调配iOS

双SSID

本节介绍双SSID,并介绍如何连接到要调配的访客,以及如何连接到802.1x WLAN。

完成以下步骤,以便在双SSID场景中调配iOS:

1. 在iOS设备上,转到**Wi-Fi Networks**,然后选择**DemoCWA**(在WLC上配置了开放式 WLAN)。



2. 在iOS设备上打开Safari浏览器,并访问可访问的URL(例如,内部/外部Web服务器)。ISE会 将您重定向到门户。单击 **Continue**。



3. 您将重定向到访客门户进行登录。



4. 使用AD用户帐户和密码登录。出现提示时,安装CA配置文件。



5. 单击Install CA服务器的受信任证书。



6. 配置文件安装完成后,单击Done。



7. 返回浏览器,然后单击Register。记下包含设备MAC地址的设备ID。



8. 单击Install以安装已验证的配置文件。



9. 单击Install Now。



10. 完成此过程后,WirelessSP配置文件确认已安装该配置文件。单击Done。

Pro	ofile 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 Details >		

11. 转到Wi-Fi网络,将网络更改为Demo1x。您的设备现已连接并使用TLS。



12. 在ISE上,导航到**操作 > 身份验证**。事件显示设备连接到开放访客网络的过程,通过请求方 调配完成注册过程,并在注册后允许访问。

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. 导航至ISE >管理>身份管理> Groups > Endpoint Identity Groups > RegisteredDevices。 MAC地址已添加到数据库。

🛕 Home Operations 🔻 Policy 💌 Admir	nistra	ation	-	
🔆 System 🦉 Identity Management	Ne	etwork	k Resource:	es 🛛 🛃 Web Portal Management
Identities Groups External Identity Sources		Ident	tity Source	e Sequences Settings
Identity Groups		Endpoi Endp Pare Saw Ide	Add MAC Addr MAC Addr	t > RegisteredDevices RegisteredDevices Asset Registered Endpoints Identity Group set p Endpoints x Remove ▼ tress 9:97:09:41 ↓

单SSID

本节介绍单SSID,并介绍如何直接连接到802.1x WLAN、提供AD用户名/密码进行PEAP身份验证、通过访客帐户调配以及重新连接TLS。

完成以下步骤,以便在单SSID场景中调配iOS:

1. 如果使用同一iOS设备,请从已注册设备中删除终端。

Endpoir Endp	Endpoint Group List > RegisteredDevices Endpoint Group							
	* Name	RegisteredDevices						
De	Description Asset Registered Endpoint							
Pare	Parent Group							
Sav	Res	et						
▼ E	ndpoints							
Ide	ntity Grou	up Endpoints						
	+ Add	XRemove -						
	MAC Add	e Remove Selected						
	E8:06:88	9 Remove All						

2. 在iOS设备上,导航到**设置 > General > Profiles**。删除本示例中安装的配置文件。



3. 单击Remove以删除以前的配置文件。





4. 使用现有(已清除)设备或新iOS设备直接连接到802.1x。

5. 连接到Dot1x,输入用户名和密码,然后单击**加入**。

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

- 6. 从ISE配置部分重复第90步和第页直到完全安装适当的配置文件。
- 7. 导航到ISE > Operations > Authentications以监控进程。此示例显示使用TLS调配、断开并重 新连接到同一WLAN时直接连接到802.1X WLAN的客户端。

Live Authentications									
🙀 Add or Remove Columns 💌 🍓 Refresh Refresh Refresh Refresh 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	2	à	paul	E8:06:88:97:09:41	WLC	Provision	RegisteredDevices	Pending	Authentication succeeded

8. 导航到WLC > Monitor > [Client MAC]。在客户端详细信息中,请注意客户端处于RUN状态,其数据交换被设置为本地,而身份验证被设置为中心。对于连接到FlexConnect AP的客户端而言,情况也是如此。

Live Authentications									
🙀 Add or Remove Columns 💌 🍪 Refresh Refresh Refresh Refresh Show Latest 20 records									
Time •	Status	Details	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	2	à	piul	E8:06:08:97:09:41	WLC	Provision	RegisteredDevices	Pending	Authentication succeeded

用户体验—调配Android

双SSID

本节介绍双SSID,并介绍如何连接到要调配的访客,以及如何连接到802.1x WLAN。

Android设备的连接过程与iOS设备的连接过程非常相似(单或双SSID)。但是,一个重要的区别是 ,Android设备需要访问Internet才能访问Google Marketplace(现为Google Play)和下载请求方代 理。 完成以下步骤,以便在双SSID场景中调配Android设备(如本示例中的Samsung Galaxy):

1. 在Android设备中,使用Wi-Fi连接到DemoCWA,然后打开访客WLAN。



2. 接受任何证书以连接到ISE。



3. 在访客门户输入用户名和密码以登录。



4. 单击**Register**。设备尝试访问Internet以访问Google市场。将任何其他规则添加到控制器中的 预身份验证ACL(例如ACL-REDIRECT),以允许访问互联网。

🕝 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 number either A-F or a digt 0-79 and a description (optional). Please click the 'Register' button to install and run the Cisco WI-FI Setup Assistant application. This application will ins certificates and configures your device to use secure with network. Clicking the 'Register' button will redirect you to an where you can download the Cisco WI-FI Setup Assistant application.	unionion where in is tall all the necessary drold market place,
Device 10 98-0C-82-40-31-A9 Description	

5. Google将思科网络设置列为Android应用。单击 Install。



6. 登录Google,然后单击INSTALL。



7. Click OK.



8. 在Android设备上,找到已安装的**思科SPW**应用,然后将其打开。



- 9. 确保您仍然从Android设备登录到访客门户。
- 10. 单击Start以启动Wi-Fi设置助手。



11. Cisco SPW开始安装证书。



12. 出现提示时,设置凭据存储的密码。



13. Cisco SPW返回证书名称,其中包含用户密钥和用户证书。点击确定以确认。

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

14. Cisco SPW继续并提示输入另一个包含CA证书的证书名称。输入名称**iseca**(在本例中),然后单击**OK**以继续。

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

15. Android设备现已连接。



我的设备门户

My Devices Portal允许用户在设备丢失或被盗的情况下将之前已注册的设备列入黑名单。它还允许 用户在需要时重新登记。

完成以下步骤以将设备列入黑名单:

1. 要登录My Devices Portal,请打开浏览器,连接到https://ise-server:8443/mydevices(注意端 口号8443),然后使用AD帐户登录。

CISCO My Devices Portal		
	Username	paul
	Password	••••••

2. 在Device ID(设备ID)下找到设备,然后单击Lost?以启动设备的黑名单。

Add a	New De	evice	To add a device, please ente (optional); then click submit	r the Device ID (MAC Addres to add the device.	is) and a descriptio	ń
		* Device ID]		
			Submit	_		
Your De	vices					•
State	Device ID	Desc	nption	Action		
	E8:06:88:97:0	9:41		Edit	Loge I	
					0	

3. 当ISE提示警告时,单击Yes以继续。



4. ISE确认设备已标记为lost。



5. 即使安装了有效的证书,使用之前注册的设备连接到网络的任何尝试现在都会被阻止。以下是 身份验证失败的黑名单设备示例:

Live Authentications									
🥁 Add or Remove Columns * 🔮 Refresh Refresh Every 3 seconds * Show Latest 20 records *									
Time •	Status	Detals	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25,12 12:49:07.851 AM	•	à	paul	E8:06:88:97:09:41	WLC	Blacklist_Access	Blacklet		Authentication failed
Mar 25,12 12:40:59.057 AM	•	ò	E0:06:00:97:09:41	EB-06-88-97:09-41	WLC	Blacklist_Access	Blacklist		Authentication falled
Mar 95 10 12-40-54 197 AM				1000-00-00-01	WEC	Blacklet Access	Backlet		Authentication faled

6. 管理员可以导航到ISE > Administration > Identity Management > **Groups**,点击**Endpoint Identity Groups** > Blacklist,然后看到设备已列入黑名单。

	Identity Groups	Endpoint Group
	<u>۹</u>	*Name Blacklist
Endpoint Identity Groups Endpoints Endpoints Endpoints Identity Group Endpoints MAC Address Ec:06:88:97:09:41		Description Blacklist Identity Group
Bladåst Badåst BegisteredDevices Unknown MAC Address Beso6:80:97:09:41	Endpoint Identity Groups	Parent Group
Add Remove MAC Address Beside::97:09:41	Blackist.	Save Reset
Identity Group Endpoints Identity Group Endpoints Add XRemove MAC Address E8:06:88:97:09:41	 Profiled Desident Desident 	▼ Endpoints
Add XRemove + MAC Address E8:06:88:97:09:41	Linknown	Identity Group Endpoints
* MAC Address E8:06:88:97:09:41		Add XRemove -
E8:06:88:97:09:41		MAC Address
		E8:06:88:97:09:41

要恢复列入黑名单的设备,请完成以下步骤:

1. 从My Devices Portal中,点击该设备的Reinstate。



2. 当ISE提示警告时,单击**Yes**以继续。



3. ISE确认设备已成功恢复。将恢复后的设备连接到网络,以测试该设备现在是否被允许。



参考 — 证书

ISE不仅需要有效的CA根证书,还需要由CA签署的有效证书。

要添加、绑定和导入新的受信任CA证书,请完成以下步骤:

1. 导航到ISE > Administration > System > Certificates,点击Local Certificates,然后点击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-siç	aned server certificate
S Certificate Authority Certificates		

2. 选择Generate Certificate Signing Request(CSR)。



3. 输入证书主**题CN=**<*ISE-SERVER hostname.FQDN>*。对于其他字段,您可以使用CA设置所 需的默认值或值。单击"Submit"。



4. ISE验证已生成CSR。



5. 要访问CSR,请点击**证书签名请求**操作。



6. 选择最近创建的CSR,然后单击Export。



7. ISE将CSR导出到.pem文件。单击Save File,然后单击OK将文件保存到本地计算机。



8. 使用文本编辑器查找并打开ISE证书文件。



9. 复制证书的全部内容。

· ·
BEGIN CERTIFICATE
MIICMzCCAZygAwIBAgIQT1/lPzR9C0W/lqfcJ2a4zTANBgkqhkiG9w0BAQUFADA1
MSMwIQYDVQQDExppc2UxMS1tbnIuY29ycC5yZi1kZW1vLmNvbTAeFw0xMjAzMTQw
MDIOMzFaFw0xMzAzMTQwMDIOMzFaMCUxIzAhBgNVBAMTGmlzZTExLW1uci5jb3Jw
LnJmLWRlbW8uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCnXTshW3Qu
BcvWrtGhB2pTJ19hHVOI607XH6AMlzrbYB/0b5wDW+QFixpgE+tLSn2gOKiieGJT
yGRvymY1HSBIz8QrW1+jBQPKxQ9ossvG98w7s/WQwnP7dKI0oK6kslTNRJZBnG48
U6GquDq/5VZ+LmAVQyQfhluRdFD9PUkNTwIDAQABo2QwYjAMBgNVHRMEBTADAQH/
MAsGA1UdDwQEAwICrDAdBgNVHQ4EFgQUBJa5qgBccwF10GK0YwaGQB10qS0wEwYD
VR01BAwwCgYIKwYBBQUHAwEwEQYJYIZIAYb4QgEBBAQDAgZAMA0GCSqGSIb3DQEB
${\tt BQUAA4GBAKS+tyTCZiNKcXIygxHTWjepfDqWdoSZwFpYnGIwzoTzecGFRzfraZDi}$
1/t65UI0KQAyBRUp21TpHf+o27eDTVwW83bCmbDln0PpwhoKBMP7N8t+9uKuVcP1
osMN8EmLCVz2RPOTE4aKtkJe5oHF10Y/+vPrb1pMhPP2hbyekAIC
END CERTIFICATE
Security Cus
Coba

10. 连接到CA服务器,并使用管理员帐户登录。服务器是Microsoft 2008 CA,其地址为 https://10.10.10.10/certsrv(在本例中)。

G • 6	https://10.10.10.10/certsrv/	ې 😧 💌
Windows Securi	ty	×
Connecting to 1	0.10.10.10.	
	administrator •••••• Domain: KF17 Remember my credentials	
	ОК	Cancel

11. 点击**申请证书**。



12. 单击高级证书请求。



13. 单击第二个选项以使用base-64编码的CMC或......提交证书请求.



14. 将ISE证书文件(.pem)中的内容粘贴到已保存请求字段,确保证书模板为**Web Server**,然后 点击**提交**。

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+tyTCZiNKcXIygxHTW1epfDqWdoSZ 1/t65UI0KQAyBRUp21TpHf+o27eDTVwW83bCmbD1 osMN8EmLCVz2RPOTE4aKtkJe5oHF10Y/+vPrb1pM END CERTIFICATE			
Certificate Template:				
	Web Server			
Additional Attribu	utes:			
Attributes:				
	Submit >			

15. 单击Download certificate。



16. 保存certnew.cer文件;稍后将使用该文件与ISE绑定。



17. 从ISE Certificates,导航到Local Certificates,然后单击Add > Bind CA Certificate。
| 🛕 Home Operations 🔻 Policy 🔻 Adminis | stration 🔻 |
|--|--|
| 🔆 System 🛛 👰 Identity Management | Network Resources 🛛 🛃 Web Portal Management |
| Deployment Licensing Certificates Loggin | ig Maintenance Admin Access Settings |
| Certificate Operations | Local Certificates |
| Certificate Signing Requests 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. 浏览到在上一步中保存到本地计算机的证书,启用**EAP**和**管理接口**协议(复选框处于选中状态),然后点击**提交**。ISE可能需要几分钟或更长时间才能重新启动服务。

Deployment Licensing Certificates Logg	ing Maintenance Admin Access Settings
Certificate Operations Certificates Certificate Signing Requests Certificate Authority Certificates SCEP CA Profiles OCSP Services	Local Certificate > Bind CA Signed Certificate Bind CA Signed Certificate Certificate * Certificate File C:\Users\Paul Nguyen\Downloads\certnew(4).cer Browse. Friendly Name Enable Validation of Certificate Extensions (accept only valid certificate) 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 syste certificate Selections for the certificate. Cancel

19. 返回CA的登录页(https://CA/certsrv/),然后点击下载CA证书、证书链或CRL。



20. 单击下载 CA 证书。

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:			
Current [corp-RFDEMO-CA]			
@ DER			
C Base 64			
Download CA certificate			
Download CA certification chain			
Downkoad latest delta CRL			

21. 将文件保存到本地计算机。



22. 在ISE服务器联机时,转到证书,然后单击证书颁发机构证书。



23. 单击 Import。



24. 浏览CA证书,启用Trust for client authentication(复选框为选中状态),然后单击Submit。

Certificate Authority Certificates > In Import a new Trusted C	^{nport} 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 LDA
Enable Validation of	Certificate Extensions (accept only valid certificate)
Description	

25. 确认已添加新的受信任CA证书。

🔆 System 🏾 👰 Identity Management	Network Resources	🛃 Web Portal Managemer	
Deployment Licensing Certificates	Logging Maintenance	Admin Access Settings	
Certificate Operations	Certificate Aut	nority Certificates	
Certificate Signing Requests	/ Edit 🕂 Imp	ort 💽 Export 🗙 Delete	
Certificate Authority Certificates	Friendly Name	9	
SCEP CA Profiles	Corp-RFDEMC)-CA#corp-RFDEMO-CA#00002	
🚭 OCSP Services	ise11-mnr.co	ise11-mnr.corp.rf-demo.com#ise11-mnr.corp	

相关信息

- <u>思科身份服务引擎硬件安装指南,版本1.0.4</u>
- Cisco 2000 系列无线局域网控制器
- Cisco 4400 系列无线局域网控制器
- Cisco Aironet 3500 系列
- Flex 7500无线分支机构控制器部署指南
- 自带设备 统一设备身份验证和一致的访问体验
- 带身份服务引擎的无线BYOD
- <u>技术支持和文档 Cisco Systems</u>

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。