带身份服务引擎的无线BYOD

目录

简介 先决条件 要求 使用的组件 拓扑 规则 无线LAN控制器RADIUS NAC和CoA概述 无线LAN控制器RADIUS NAC和CoA功能流 ISE分析概述 创建内部身份用户 向ISE添加无线LAN控制器 <u>配置ISE进行无线身份验证</u> Bootstrap无线LAN控制器 将WLC连接到网络 将身份验证服务器(ISE)添加到WLC 创建WLC员工动态接口 创建WLC访客动态接口 添加802.1x WLAN 测试WLC动态接口 iOS无线身份验证(iPhone/iPad) 将状态重定向ACL添加到WLC 在ISE上启用分析探测 为设备启用ISE配置文件策略 终端安全评估发现重定向的ISE授权配置文件 为员工创建ISE授权配置文件 为承包商创建ISE授权配置文件 设备状态/分析的授权策略 测试状态补救策略 差异化访问的授权策略 测试CoA以区分访问 WLC访客WLAN 测试访客WLAN和访客门户 ISE无线发起访客接入 赞助访客 测试访客门户访问 证书配置 Windows 2008 Active Directory集成

<u>添加Active Directory组</u> <u>添加身份源序列</u> <u>集成AD的ISE无线赞助访客接入</u> <u>在交换机上配置SPAN</u> <u>参考:Apple MAC OS X的无线身份验证</u> <u>参考:Microsoft Windows XP的无线身份验证</u> <u>参考:Microsoft Windows 7的无线身份验证</u> <u>相关信息</u>

<u>简介</u>

思科身份服务引擎(ISE)是思科的下一代策略服务器,为Cisco TrustSec解决方案提供身份验证和授权基础设施。它还提供另外两项关键服务:

- 第一项服务是提供一种方法,根据思科ISE从各种信息源接收的属性自动分析终端设备类型。此服务(称为Profiler)提供与思科之前通过Cisco NAC Profiler设备提供的相同功能。
- •思科ISE提供的另一项重要服务是扫描终端合规性;例如,AV/AS软件安装及其定义文件有效性 (称为状态)。思科之前仅通过Cisco NAC设备提供此确切的安全评估功能。

思科ISE提供同等级别的功能,并与802.1X身份验证机制集成。

与无线局域网控制器(WLC)集成的思科ISE可提供移动设备(例如Apple iDevices (iPhone、iPad和 iPod)、基于Android的智能手机和其他设备的分析机制。对于802.1X用户,思科ISE可提供相同级 别的服务,例如分析和状态扫描。思科ISE上的访客服务也可通过将Web身份验证请求重定向到思 科ISE进行身份验证而与思科WLC集成。

本文档介绍自带设备(BYOD)的无线解决方案,例如根据已知终端和用户策略提供差异化接入。本文 档不提供BYOD的完整解决方案,但用于演示动态访问的简单使用案例。其他配置示例包括使用 ISE发起人门户,特权用户可以发起访客调配无线访客接入。

<u>先决条件</u>

<u>要求</u>

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:

- •软件版本为7.2.103的思科无线局域网控制器2504或2106
- Catalyst 3560 8端口
- WLC 2504
- •身份服务引擎1.0MR(VMware服务器映像版本)
- Windows 2008 Server(VMware映像) 512M,20GB磁盘Active DirectoryDNSDHCP证书 服务

拓扑



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

<u>规则</u>

有关文档规则的详细信息,请参阅 <u>Cisco 技术提示规则。</u>

无线LAN控制器RADIUS NAC和CoA概述

此设置使WLC能够查找来自ISE RADIUS服务器的URL重定向AV对。这仅适用于绑定到启用了 RADIUS NAC设置的接口的WLAN。当收到用于URL重定向的Cisco AV-Pair时,客户端将进入 POSTURE_REQD状态。这基本上与控制器内部的WEBAUTH_REQD状态相同。

当ISE RADIUS服务器认为客户端符合安全评估时,它会发出CoA ReAuth。Session_ID用于将其连接在一起。使用此新的AuthC(重新身份验证)时,它不会发送URL-Redirect AV-Pairs。由于没有URL重定向AV对,因此WLC知道客户端不再需要安全评估。

如果未启用RADIUS NAC设置,WLC将忽略URL重定向VSA。

CoA-ReAuth:这通过RFC 3576设置启用。ReAuth功能已添加到以前支持的现有CoA命令中。

RADIUS NAC设置与此功能互斥,但CoA需要它才能工作。

Pre-Posture ACL:当客户端处于POSTURE_REQ状态时,WLC的默认行为是阻止除DHCP/DNS之 外的所有流量。Pre-Posture ACL(在url-redirect-acl AV-Pair中称为)应用于客户端,该ACL中允 许的内容是客户端可以到达的内容。 Pre-Auth ACL与VLAN覆盖:7.0MR1不支持与接入VLAN不同的隔离或AuthC VLAN。如果从策略服 务器设置VLAN,它将成为整个会话的VLAN。首次授权后无需更改VLAN。

无线LAN控制器RADIUS NAC和CoA功能流

以下图提供了客户端通过后端服务器身份验证和NAC状态验证时消息交换的详细信息。

- 1. 客户端使用dot1x身份验证进行身份验证。
- 2. RADIUS Access Accept传输端口80的重定向URL和包括允许IP地址和端口或隔离VLAN的预 身份验证ACL。
- 3. 客户端将重定向到access accept中提供的URL,并进入新状态,直到完成状态验证。处于此 状态的客户端与ISE服务器通信,并根据ISE NAC服务器上配置的策略验证自身。
- 4. 客户端上的NAC代理启动状态验证(到端口80的流量):代理向端口80发送HTTP发现请求 ,控制器重定向到访问接受中提供的URL。ISE知道客户端尝试访问并直接响应客户端。这样 ,客户端即可了解ISE服务器IP,从现在起,客户端将直接与ISE服务器进行通信。
- 5. 由于ACL配置为允许此流量,因此WLC允许此流量。如果发生VLAN覆盖,流量会桥接以便到 达ISE服务器。
- 6. ISE客户端完成评估后,RADIUS CoA-Req with reauth service将发送到WLC。这将启动客户端的重新身份验证(通过发送EAP-START)。重新身份验证成功后,ISE会发送包含新ACL(如果有)和无URL重定向或访问VLAN的访问接受。
- 7. 根据RFC 3576,WLC支持CoA-Req和Disconnect-Req。根据RFC 5176,WLC需要支持重新身 份验证服务的CoA-Req。
- 8. WLC上使用的是预配置的ACL,而不是可下载的ACL。ISE服务器仅发送ACL名称,该名称已 在控制器中配置。
- 9. 此设计适用于VLAN和ACL两种情况。如果发生VLAN覆盖,我们只需重定向端口80,并允许 (桥接)隔离VLAN上的其余流量。对于ACL,应用访问接受中收到的预身份验证ACL。



此图直观地显示了此功能流:

<u>ISE分析概述</u>

思科ISE分析器服务提供发现、定位和确定网络上所有连接的终端的功能,无论其设备类型如何 ,以确保和维护对企业网络的适当访问。它主要收集网络上所有终端的一个属性或一组属性,并根 据其配置文件对它们进行分类。

分析器由以下组件组成:

- 传感器包含许多探针。探测功能通过查询网络接入设备来捕获网络数据包,并将从终端收集的 属性及其属性值转发到分析器。
- 分析器使用配置的策略和身份组评估终端以匹配所收集的属性及其属性值,将终端分类到指定 组并将具有匹配配置文件的终端存储在思科ISE数据库中。

对于移动设备检测,建议结合使用以下探针正确识别设备:

- RADIUS(呼叫站ID):提供MAC地址(OUI)
- DHCP(主机名):主机名 默认主机名可以包括设备类型;例如:jsmith-ipad
- DNS(反向IP查找): FQDN 默认主机名可以包括设备类型
- •HTTP(用户代理):有关特定移动设备类型的详细信息

在iPad的此示例中,分析器从User-Agent属性捕获网络浏览器信息,从请求消息捕获其他HTTP属性,并将它们添加到终端属性列表中。



创建内部身份用户

简单概念验证不需要MS Active Directory(AD)。ISE可用作唯一的身份库,其中包括区分用户访问权 限以进行访问和精细策略控制。

在ISE 1.0版本中,使用AD集成,ISE可以在授权策略中使用AD组。如果使用ISE内部用户存储(无AD集成),则不能在策略中与设备身份组一起使用组(已在ISE 1.1中确定需要解决的漏洞)。因此,除了设备身份组外,使用时只能区分个人用户,例如员工或承包商。

请完成以下步骤:

- 1. 打开浏览器窗口访问https://ISEip地址。
- 2. 导航到Administration > Identity Management > Identities。



- 3. 选择**Users**,然后单击**Add**(网络访问用户)。输入以下用户值并分配给Employee组:姓名
 - :employee密码

: XXXX

💧 Home	Monitor 🔻	Policy 🔻 🚺	dministration	•		
🔆 System	And Identity	Management	Network	Resources	🛃 Guest Manag	ement
Identities	Groups	External Iden	tity Sources	Identity So	urce Sequences	Settings
Identities				Networ	rk Access Users	
•			P	/ Edit	🕂 Adg	nge Status 🔻
\$~			\$ <u>\$</u>	Status	Name	
Endopinte						
Endpoints						

🛕 Home Monitor 🔻	Policy V Ac	dministration 🔻	_	-			
🔆 System 🖉 Identit	y Management	Network Re	sources	🛃 Guest Man	agement		
Identities Groups	External Identi	ity Sources	Identity So	urce Sequences	Setting	S	
Identities			Network A	Access Users > Ne	w Network Ac	ccess User	
\$-		ŵ.	* Name	employee	-		Statue
Users		۲	Hame	employee			Oldios
Endpoints		۲	Email				
			Passwo	ord			
				* Password	#		
			* Re-Er	nter Password	•••••		
			VUser In	formation			

- 4. 单击"Submit"。姓名:承包商密码:XXXX
- 5. 确认两个帐户均已创建。

Identities		Network Access Users
(*		/ Edit 🕂 Add 🔯 Change Status 👻 🄂 Imp
\$~	₩ •	Status 🔺 Name 🛛
Users	۲	🕒 🖾 Enabled 🛛 🙆 contractor
Endpoints	۲	🖂 🖾 Enabled 🛛 🖧 employee

<u>向ISE添加无线LAN控制器</u>

向ISE发起RADIUS请求的任何设备都必须在ISE中有定义。这些网络设备是根据其IP地址定义的。 ISE网络设备定义可以指定IP地址范围,从而允许定义代表多个实际设备。

除了RADIUS通信所需的设置,ISE网络设备定义还包含其他ISE/设备通信的设置,例如SNMP和 SSH。

网络设备定义的另一个重要方面是对设备进行适当分组,以便可以在网络访问策略中使用此分组。

本练习将配置实验所需的设备定义。

请完成以下步骤:

1. 从ISE转至Administration > Network Resources > Network Devices。

Administration	•
System 24 Identity Management	k Resources August Management
Network Devices Network Device Groups Ex	ternal RADIUS Servers RADIUS Server Sequences SGA AAA Servers
Network Devices	Network Devices List > New Network Device
	• Name pod-wic
¢•• @•	Description
Network Devices	
Default Device	* IP Address: 10.10.10.5 / 32
	Model Name
	Software Version
	* Network Device Group
	Location All Locations Set To Default
l 🚽	Device Type All Device Types Sar to Denaut
	✓ Authentication Settings
	Enable Authentication Settings
	Protocol RADIUS
	* Shared Secret
	Source Control Section Access (SCA)
	Device Configuration Deployment
	Submit Cancel

- 2. 在Network Devices(网络设备)中,单击Add。输入IP地址,掩码检查Authentication Setting,然后输入cisco作为共享密钥。
- 3. 保存WLC条目,并在列表中确认控制器。

🔥 Home Monitor 🔻 Policy 🛪 🛛 A	dministration 🔻								
System Aldentity Management	Network Resources	🛃 Guest Managemen	t .						
Network Devices Network Device Gr	roups External RADIUS	Servers RADIUS	Server Sequences SGA	AAA Servers					
Network Devices Network Devices									
·	P dit	Add Duplicate	🔛 Import 🛛 🕀 Export 👻	🗙 Delete 🔻					
\$P+	😔 🔪 Name	 IP/Mask 	Location						
Network Devices	> pod-w	c 10.10.10.5/	32 All Locations						

<u>配置ISE进行无线身份验证</u>

需要配置ISE以对802.1x无线客户端进行身份验证,并使用Active Directory作为身份库。

请完成以下步骤:

- 1. 从ISE导航到策略>身份验证。
- 2. 单击展开Dot1x > Wired_802.1X(-)。
- 3. 单击齿轮图标以从库中添加条件。

1	li ili i isco	Iden	tity Services Engine	1						ise	asinin Log-Out Feedis
E	🍐 н	ime I	Vontor 🔹 – Policy 💌	Administration							e Taok Navigator
F	a Au	henticat	on Suthorization	🔀 Profiling	🔀 Posture	Client Provis	ioning	Security Group Access	🐥 Policy Elements		
ſ	1		Policy Type 🔿 Simple	Rule-Bas	ed	7					
	* Ru	le Basi	əd								
	ŧ (• 12	M/B	: H	Wired_MA8	<> allow p	rotocols	Allowed Protocol : Default P	lebvoi 🌚 🛛 and 🖡		🖗 Actions 💌
	E (• 🖻	DettX	: H	Wired_902.1X	- alow p	rotocols	Allowed Protocol : Default P	lebwor 🥑 iand 💡		🎡 Actions 👻
		- 1	Default Rule (If no mat	(8) : a	💾 Add All C	and tions Below to	Library				
					Condition Wired_80	Name 2.1X 💌	Express	sion	-	AND Acid Attribute/Va Acid Condition fr Delete	lue rom Library

4. 从条件选择下拉列表中,选择**复合条件> Wireless_802.1X**。

Dot1X : If	Wired_802.1X
Default Rule (If no match) : a	Add All Conditions Below to Library
	Condition Name Expression
	Select Condition
	Compound Condition
	- ✓ · · · · · · · · · · · · · · · · · ·
	VVired_802.1X
	Switch_Local_Web_A_mentication

5. 将Express条件设置为OR。

6. 展开after allow protocols选项,并接受默认的内部用户(Internal Users)(默认)。

🔽 👻 DottX if	Wired_802.1XA allow protocols Allowed Protocol : Default Networ and	
Default Rule (If no match) : a	Add All Conditions Below to Library	1
	Condition Name Expression	OR 💽
	Wired_802.1X 🕑	OR
	Wireless_802.1X 😒 🗖 Acondition to match an 802.1X based authentication reque	

cisc	0 0	Iden	tity Servi	ces Engine)				_			
ŵ	Hom	e I	Monitor 🔻	Policy V	Administration							
1	Authe	nticat	ion 🧕	Authorization	🛃 Profiling	💽 Po	sture	词 Client Pro	wisioning	🚉 Secu	rity Group	Access
•	Rule	Base	Policy Type	e 🔿 Simple	 Rule-Base 	ed		7				
	-	•	MAB		: If	Wired_	MAB	\Rightarrow allo	w protocols	Allowed	Protocol :	Default Net
	-	•	Dot1X		: If	Wired_	802.1X (D ↔ allo	w protocols	Allowed	Protocol :	Default Net
			▼ Defa	ult	:	use	Internal	Users 👄	Source Int	ernal User	'S	
_		•	Default F	Rule (If no mat	ch) : all	ow pro	Options If authe If	ntication failed user not found process failed	Reject Reject Drop	•		

7. 保留其他所有设置。单击Save完成这些步骤。

Bootstrap无线LAN控制器

<u>将WLC连接到网络</u>

<u>Cisco 2500 Series Wireless Controller Deployment Guide</u>中还提供了Cisco 2500无线LAN控制器部 署指南。

使用启动向导配置控制器

(Cisco Controller) Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup Would you like to terminate autoinstall? [yes]: yes AUTO-INSTALL: process terminated -- no configuration loaded System Name [Cisco_d9:24:44] (31 characters max): ISE-Podx Enter Administrative User Name (24 characters max): admin Enter Administrative Password (3 to 24 characters): Ciscol23 Re-enter Administrative Password: Cisco123 Management Interface IP Address: 10.10.10.5 Management Interface Netmask: 255.255.255.0 Management Interface Default Router: 10.10.10.1 Management Interface VLAN Identifier (0 = untagged): 0 Management Interface Port Num [1 to 4]: 1 Management Interface DHCP Server IP Address: 10.10.10.10 Virtual Gateway IP Address: 1.1.1.1 Mobility/RF Group Name: ISE Network Name (SSID): PODx Configure DHCP Bridging Mode [yes][NO]: no Allow Static IP Addresses [YES][no]: no Configure a RADIUS Server now? [YES][no]: no Warning! The default WLAN security policy requires a RADIUS server. Please see documentation for more details.

Enter Country Code list (enter 'help' for a list of countries) [US]: US Enable 802.11b Network [YES][no]: yes Enable 802.11a Network [YES][no]: yes Enable 802.11g Network [YES][no]: yes Enable Auto-RF [YES][no]: yes Configure a NTP server now? [YES][no]: no Configure the ntp system time now? [YES][no]: yes Enter the date in MM/DD/YY format: mm/dd/yy Enter the time in HH:MM:SS format: hh:mm:ss Configuration correct? If yes, system will save it and reset. [yes][NO]: yes Configuration saved! Resetting system with new configuration... Restarting system. **邻居交换机配置**

控制器连接到相邻交换机(Fast Ethernet 1)的以太网端口。邻居交换机端口配置为802.1Q中继并允 许中继上的所有VLAN。本征VLAN 10允许连接WLC的管理接口。

802.1Q交换机端口配置如下:

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

将身份验证服务器(ISE)添加到WLC

需要将ISE添加到WLC,以便为无线终端启用802.1X和CoA功能。

请完成以下步骤:

1. 打开浏览器,然后连接到Pod WLC(使用安全HTTP)> https://wlc。

2. 导航到**安全>身份验证>新建**。

MONITOR WLANS CONTRO	DLLER WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACI
RADIUS Authentication S	ervers > New					
Server Index (Priority)	1 -	1				
Server IP Address	10.10.10.70	-				
Shared Secret Format	ASCII 👻					
Shared Secret						
Confirm Shared Secret	🔨					
Key Wrap	(Designed for	r FIPS custome	ers and requires a	key wrap compl	iant RADI	US server)
Port Number	1812					
Server Status	Enabled 👻					
Support for RFC 3576	Enabled 👻	and the second s				
Server Timeout	2 secon	ds				
Network User	🗹 Enable					
Management	🗹 Enable					
IPSec	Enable					

- 3. 输入以下值:服务器IP地址:10.10.10.70(检查分配)共享密钥:cisco支持RFC 3576(CoA):启用(默认)其他所有内容:默认
- 4. 单击Apply继续。
- 5. 选择RADIUS Accounting > Add NEW。

cisco	MONITOR	<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	MANAGEMENT	c		
Security	RADIUS /	Accounti dex (Priorit	ng Servers >	New					
RADIUS Authentication Accounting Fallback TACACS+	Server IP Shared S Shared S	Server IP Address Shared Secret Format Shared Secret			10.10.10.70 ASCII -				
LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Confirm S Port Num Server St Server Ti	shared Sec ber atus meout	1813 Enab 2	led 🗸					
 Elocal EAP Priority Order Certificate 	Network IPSec	Jser	V Er	able Enable					

6. 输入以下值:服务器IP地址:10.10.10.70共享密钥:cisco其他所有内容:默认 7. 单击Apply,然后保存WLC的配置。

创建WLC员工动态接口

完成以下步骤,以便为WLC添加新的动态接口并将其映射到Employee VLAN:

1. 从WLC导航到Controller > Interfaces。然后单击 New。

սիսիս					Saye Configuration Min	g Logo
cisco	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY	MANAGEMENT COMM	NDS HELP FEEDBA	ск
Controller	Interfaces	×.				N
General						∕‴
Inventory	Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Managem	ent
Interfaces	management	untagged	10.10.10.5	Static	Enabled	
Interface Groups	virtual	N/A	1.1.1.1	Static	Not Supported	

2. 从WLC导航到**Controller > Interfaces**。输入以下内容:接口名称:EmployeeVLAN ID:11

<u>M</u> ONITOR	<u>W</u> LANs		WIRELESS	<u>s</u> ecur
Interface	s > New			
Interface VLAN Id	Name 🖡	Employee		

- 3. 为员工界面输入以下内容:端口号:1VLAN标识符:11IP地址:10.10.11.5网络掩码
 - :255.255.255.0网关
 - : 10.10.11.1DHCP:10.10.10.10

Configuration	
Quarantine	
Quarantine Vlan Id	0
Physical Information	
Port Number	1
Backup Port	0
Active Port	0
Enable Dynamic AP Mana	igement 🗌
Interface Address	
VLAN Identifier	11
IP Address	10.10.11.5
Netmask	255.255.255.0
Gateway	10.10.11.1
DHCP Information	
Primary DHCP Server	10.10.10
Secondary DHCP Server	

4. 确认已创建新的员工动态接口。

cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	С <u>О</u> ММА
Controller	Interfaces	5					
General Inventory	Interface	Name		/LAN Identifier	IP Addres	s Interfac	е Туре
Interfaces	employee		:	11	10.10.11.5	Dynamic	1
Interface Groups	manageme	nt		untagged	10.10.10.5	Static	
Multicast	virtual			N/A	1.1.1.1	Static	

创建WLC访客动态接口

完成以下步骤,以便为WLC添加新的动态接口并将其映射到访客VLAN:

- 1. 从WLC导航到Controller > Interfaces。然后单击 New。
- 2. 从WLC导航到Controller > Interfaces。输入以下内容:接口名称:访客VLAN
 - ID:12

սիսիս				- K	
CISCO	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLI	LER WIRELESS	<u>s</u> ec
Controller	Interfaces	s > New			
General	Interface	Name	Guest	-	
Interfaces	VLAN Id	I	12		

- 3. 为访客接口输入以下内容:端口号:1VLAN标识符:12IP地址:10.10.12.5网络掩码
 - :255.255.255.0网关
 - : 10.10.12.1DHCP:10.10.10.10

Configuration	
Quarantine 📃	
Quarantine Vlan Id 0	
Physical Information	
Port Number	1
Backup Port	0
Active Port	0
Enable Dynamic AP Manageme	ent 🗔
Interface Address	
VLAN Identifier	12
IP Address	10.10.12.5
Netmask	255.255.255.0
Gateway	10.10.12.1
DHCP Information	
Primary DHCP Server	10.10.10.10
Secondary DHCP Server	
Access Control List	
ACL Name	none
Note: Changing the Interface part temporarily disabled and thus ma some clients.	ameters causes the WLANs to be y result in loss of connectivity for

4. 确认已添加访客接口。

uluili. cisco	MONITOR	<u>W</u> LANs	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMAI
Controller	Interfaces	8				
General Inventory	Interface	Name	VLAN Identifier	IP Address	Interfa	ce Type
Interfaces	employee		11	10.10.11.5	Dynamic	0
Interface Groups	guest		12	10.10.12.5	Dynamic	2
Multicast	manageme	nt	untagged	10.10.10.5	Static	
Internal DHCP Server	virtual		N/A	1.1.1.1	Static	

<u>添加802.1x WLAN</u>

从WLC的初始引导中,可能已创建默认WLAN。如果是,请按照指南中的说明修改它或创建一个新的WLAN以支持无线802.1X身份验证。

请完成以下步骤:

1. 从WLC导航到WLAN > Create New。

արտիս				Sa <u>v</u> e C	onfiguration <u>P</u> ir	ng Logou	t <u>R</u> e
	WLANS CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP E	EEDI
WLANs	WLANS					Entries O	- 0 a
WLANS WLANS	Current Filter: None	[Change F	ilter] (Clear Fil	<u>ter</u>]	Create New Create New	Go	4
Advanced	WLAN ID Type Pro	file Name W	LAN SSID A	dmin Status Se	Disable Selected Enable Selected Remove Selected		

2. 对于WLAN,请输入以下命令:配置文件名称:pod1xSSID:相同

cisco		CONTROLLER WIRELESS SECURITY MANAGEMENT
WLANs	WLANs > New	
WLANs WLANs Advanced	Type Profile Name SSID ID	WLAN pod1x pod1x 1

3. 对于WLAN settings > General选项卡,请使用以下命令:无线电策略:全部接口/组:管理其 他所有内容:默认

<u>M</u> ONITOR <u>W</u> LA	Ns <u>C</u> ONTROLLE	R W <u>I</u> RELESS	<u>S</u> ECURITY
WLANs > Edit	'pod1x'		
		· · · · ·	
General S	ecurity QoS	Advanced	
Profile Name	pod1×		
Туре	WLAN		
SSID	pod1×		
Status	En-	abled	
Security Polic	cies [WPA (Modifie	2][Auth(802.1) ations done und	X)] er security tab w
Radio Policy	All	•	
Interface/Inte Group(G)	erface <mark>mana</mark>	gement 💌 🗲	_
Multicast Vlar	n Feature 🗌 Ena	bled	
Broadcast SS	ID 🔽 Ena	bled	

4. 对于WLAN > Security选项卡> Layer 2,请设置以下内容:第2层安全:WPA+WPA2WPA2策 略/加密:启用/AES身份验证密钥管理

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

 5. 对于WLAN > Security选项卡> AAA Servers,请设置以下内容:无线电服务器覆盖接口:已禁 用身份验证/记帐服务器:已启用服务器
 1:10.10.10.70

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

6. 对于WLAN > Advanced选项卡,请设置以下内容:允许AAA覆盖:已启用NAC状态:Radius

NAC(选中)						
MONITOR WLANS CONT	ROLLER WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
WLANs > Edit 'pod1x'						
General Security	QoS Advanced					
Allow AAA Override	Enabled		DHCP			
Coverage Hole Detection	Enabled		DHC	P Server		Override
Enable Session Timeout	V 1800 Session Timeout (see	cs)	DHC	P Addr. Assignn	ment 🗖	Required
Aironet IE	✓ Enabled		Manag	ement Frame	Protectio	on (MEP)
Diagnostic Channel	Enabled					
IPv6 Enable Z			MFP	Client Protectio	n 🔨 🛛 🖸 🕅	otional 💌
Override Interface ACL	None	×	DTIM P	eriod (in bead	on inter	vals)
P2P Blocking Action	Disabled •					
Client Exclusion ³	Enabled Timeout V	alue (secs)	802.	.11a/n (1 - 255) .11b/g/n (1 - 25	1 5) 1	
Maximum Allowed Clients ²	0		NAC			
Static IP Tunneling 22	Enabled		Load B	State Radius	Band Sel	ect

7. 返回WLAN > General选项卡> Enable WLAN(复选框)。

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

<u>测试WLC动态接口</u>

您需要快速检查有效的员工和访客接口。使用任何设备与WLAN关联,然后更改WLAN接口分配。

- 1. 从WLC导航到WLAN > WLANs。单击以编辑在前面的练习中创建的安全SSID。
- 2. 将Interface/Interface Group更改为**Employee**,然后单击**Apply**。

uluilu cisco		NTROLLER WIRELESS SECURI
CISCO WLANS WLANS MUANS Advanced	MONITOR WLANS COL WLANs > Edit 'pod1> General Security Profile Name Type Type SSID Status Status Radio Policy Interface/Interface Group(G) Multicast Vlan Feature Broadcast SSID SSID	NTROLLER WIRELESS SECURIT X' QoS Advanced pod1x WLAN pod1x MLAN pod1x Membled [WPA2][Auth(802.1X)] (Modifications done under security t All management management Finabled

3. 如果配置正确,设备将从员工VLAN(10.10.11.0/24)接收IP地址。此示例显示获取新IP地址的

~	Wi-Fi Networks	pod1x	
	Forg	et this Netv	work
	IP Address		
	DHCP	BootP	Static
z	IP Address	1	0.10.11.100

iOS设备。

4. 确认之前的接口后,将WLAN接口分配更改为Guest,然后单击Apply。

cisco		NTROLLER WIRELESS S
WLANs	WLANs > Edit 'pod1)	<u></u>
WLANS	General Security	QoS Advanced
▶ Advanced	Profile Name Type SSID Status	podix WLAN podix Enabled
	Security Policies	[WPA2][Auth(802.1X)] (Modifications done under se
	Radio Policy	All
	Interface/Interface Group(G)	guest 💌
	Multicast Vlan Feature Broadcast SSID	guest management ✓ Enabled

5. 如果配置正确,设备将从访客VLAN(10.10.12.0/24)接收IP地址。此示例显示获取新IP地址的

Wi-Fi Networks	pod1x						
Forget this Network							
IP Address							
DHCP	BootP	Static					
IP Address		10.10.12.102					

iOS设备。

6. 重要信息:将接口分配更改回原始管理。

7. 单击Apply并保存WLC的配置。

<u>iOS无线身份验证(iPhone/iPad)</u>

使用iPhone、iPad或iPod等iOS设备,通过经过身份验证的SSID与内部用户(或集成的AD用户)关 联到WLC。如果不适用,请跳过这些步骤。

1. 在iOS设备上,转到WLAN设置。启用WIFI,然后选择上一节中创建的启用802.1X的SSID。 2. 提供以下信息以连接:用户名:员工(内部 — 员工)或承包商(内部 — 承包商)密码





4. 确认iOS设备正在从管理(VLAN10)接口获取IP地址。

3. 单击以接受ISE证书。

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

5. 在WLC > Monitor > Clients上,验证终端信息,包括使用、状态和EAP类型。

uluilu cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> O	NTROLLER WIRELE
Monitor	Clients > Detail	
Summary Access Points	Client Properties	
Cisco CleanAir	MAC Address	5c:59:48:40:82:8d
Statistics	IP Address	10.10.10.102
▶ CDP	Client Type	Regular
Rogues	User Name	aduser
Clients	Port Number	1
Multicast	Interface	management
	Mobility Peer IP Address	N/A
	Policy Manager State	RUN
	Management Frame Protection	No
	Security Information	
	Security Policy Completed	Yes
	Policy Type	RSN (WPA2)
	Encryption Cipher	CCMP (AES)
	EAP Type	PEAP
	SNMP NAC State	Access
	Radius NAC State	RUN
	AAA Override ACL Name	none

6. 同样,客户端信息可以由ISE > Monitor > Authentication页面提供。

Identity Services Engine					
🛕 Home 🛛 Monitor 🔻 Policy 🔻 Adminis	tration 🔻	-7			
Authentications 2 Alarms E Reports	💊 Troubleshoot				_
🎡 Add or Remove Columns 👻 🛞 Refresh	1				
Time • Status Details	Usemame	Endpoint ID	Network Device	Authorization Profiles	Id
Jul 13,11 04:39:36.573 PM	aduser	5C:59:48:40:82:8D	WLC	PermitAccess	
Jul 13,11 04:38:46.285 PM	aduser	5C:59:48:40:82:8D	WLC	PermitAccess	
L击 Details 图标可细化到会话以氡	^夫 取会话的深入	信息。			
duntity Servi	ces Engii	ne			
					_
Showing Page	1 07 1				
AAA Protocol > RAD	IUS Auth	enticatior	n Detail		
RADIUS Audit Session	ID : 0a0a0a	a050000000)d4e1e2a	45	
AAA session ID :	ise/999	967658/11			
Date :	July	13,2011			
Generated on July 13-2	011 4-41-11	I PM PDT			
Authentiection Summer					_
Authentication Summar	y Iulu 12 0	111 4-20-20	572 DM		_
DADIUS Status:	Authoritic	otion cucco			
NAS Epilure:	Authentito	ation succe	seueu		
lleornama:	aducar				
MAC/IP Address	50:59:48	40.82-8D			
Network Device	WLC - 10	10 10 5			
Allowed Protocol:	Default N	etwork Acc	855		
Identity Store:	AD1	011101117100	000		
looning otoro.					
Authorization Profiles:	PermitAc	Cess			
Authorization Profiles: SGA Security Group	PermitAc	cess			

<u>将状态重定向ACL添加到WLC</u>

在WLC上配置终端安全评估重定向ACL,ISE将用于限制客户端的终端安全评估。ACL至少有效地 允许ISE之间的流量。如果需要,可以在此ACL中添加可选规则。

1. 导航到WLC > Security > Access Control Lists > Access Control Lists。单击 New。

ahuhu					Save Config	uration <u>P</u> ing	Logout Refrest
	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP FEEDE
Security	A	ccess Control	Lists			New	Apply
General RADIUS Authentication	En	able Counters				-	
Fallback Fallback TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies							•
E Local EAP							
Priority Order							
Certificate							
Access Control Lits Access Control Lits CPU Access Control	sts Lists						

2. 为ACL提供名称(ACL-POSTURE-REDIRECT)。

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

3. 单击Add New Rule以添加新ACL。将以下值设置为ACL序列#1。完成后单击Apply。来源:任意目的:IP地址10.10.10.70、255.255.255.255协议:任意操作:允许

MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Access 0	control L	ists > Rules >	Edit				
Sequence	•	1					
Source		Any	*				
Destination		IP Address		IP Addr 10.10.	ess 10.70	Vetmask 255.255.255.255	1
Protocol		Any					
DSCP		Any					
Direction		Any					
Action		Permit					

4. 已添加确认序列。

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any	0

5. 单击 Add New Rule。将以下值设置为ACL序列#2。完成后单击Apply。来源:IP地址 10.10.10.70、255.255.255.255目标:任意协议:任意操作:允许

Sequence	2		
Source	ID Address	IP Address	Netmask
Source	IF Address	10.10.10.70	233.233.233.233
Destination	Any		
Protocol	Any	e	
DSCP	Any		
Direction	Any		
Action	Permit		

6. 已添加确认序列。

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

7. 将以下值设置为ACL序列#3。完成后单击**Apply**。来源:任意目标:任意协议:UDP源端口 :DNS目标端口:任意操作:允许



8. 已添加确认序列。

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

9. 单击 Add New Rule。将以下值设置为ACL序列#4。完成后单击Apply。来源:任意目标:任意协议:UDP源端口:任意目标端口:DNS操作:允许



10. 已添加确认序列。

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

11. 保存当前WLC配置。

<u>在ISE上启用分析探测</u>

需要将ISE配置为探测功能以有效地分析终端。默认情况下,这些选项处于禁用状态。本节介绍如 何将ISE配置为探测功能。 1. 从ISE管理,导航到管理>系统>部署。



cisco Identity Services Engine			
🔥 Home 🛃 Monitor 👻 Policy 👻 🗾	Administration		
🔆 System 🖉 Identity Management	Network Resources	4 Guest Management	
Deployment Licensing Certifica	ites Logging Opera	ations Admin Access	Settings
Deployment	Deploymen	nt Nodes	
	🎡 🖌 📝 Edit 🕻	Register 💮 Syncup	💆 Deregister - 🖓 Filter -
Deployment	🗌 Hostna	ime 🔺	Node Type Personas
		P	ISE Administration
	C37		

3. 从Edit Node页中,选择Profiling Configuration并配置以下内容:DHCP:启用、全部(或默认)DHCPSPAN:启用、全部(或默认)HTTP:启用、全部(或默认)RADIUS:已启用,不 适用DNS:已启用,不适用



- 4. 重新关联设备(iPhone/iPad/Droids/Mac等)。
- 5. 确认ISE终端身份。导航到Administration > Identity Management > Identities。点击 Endpoints以列出已分析的内容。**注意:**初始分析来自RADIUS探测器。
| Cisco Identity Services Engine | | |
|-------------------------------------|---|---|
| System Addentity Management Network | ork Resources 🛛 🛃 Guest Management
s Identity Source Sequences Setting | ş |
| Identities
▼ | Endpoints Edit Create X Delete Endpoint Profile | 🚱 Import 👻 🚱 Export 👻 😽 Filter 👻 |
| Users ()
Endpoints () | Android Apple-Device Apple-Device | 40:FC:89:75:64:43
5C:59:48:40:82:8D
44:2A:60:F7:3A:4A |
| | Microsoft-Workstation Microsoft-Workstation Windows7-Workstation | 00:21:5C:69:9A:39
00:26:C6:0C:33:56
00:1B:21:4D:EE:C0 |

<u>为设备启用ISE配置文件策略</u>

ISE开箱即用提供各种终端配置文件库。要启用设备的配置文件,请完成以下步骤:

1. 从ISE导航到**策略>分析**。

cisco Identity Serv	ices Engind	
A Home Monitor V	Policy Administration	
🔆 System 🏼 🖓 Identity	Authentication	🛃 Gu
Deployment Licensi	Authorization	ons
Deployment	Refiling	Nodes
♥▼ ■ Ⅲ ▶ 2 Deployment	Posture	
	Client Provisioning	IS P

- 2. 在左侧窗格中,展开分析策略。
- 3. 单击Apple Device > Apple iPad,然后设置以下项:策略已启用:已启用创建匹配的身份组
 :已选择

cisco Identity Services Engine	2					
A Home Monitor T Policy T	Administration				and the second se	
Authentication SAuthorization	Refiling	Posture	Client Pro	visioning	Security Group Ac	cess
Profiling		Profiler Polic	y List > Apple-iP	ad		
	\sim		* Name	Apple-iPa	ad	Des
↓ = 1	- 🙀	P	olicy Enabled		8	
👻 🪞 Profiling Policies		* Minimum Ce	artainty Factor	20		(Valid
Android						
		* Exc	ception Action	NONE	-	
Apple-MacBook				Create Mat	ching Identity Group	
Apple-iPad @			0	Lise Hieran	chy	
Apple-iPhone						
Apple-iPod			Parent Policy	Apple-De	evice	
Applera-Device						

4. 单击Apple Device > Apple iPhone,设置以下项:策略已启用:已启用创建匹配的身份组:已 选择



5. 单击Android,设置以下项:策略已启用:已启用创建匹配的身份组:已选择

cisco Identity Services Engin	e				
💧 Home 🛛 Monitor 🔻 📄 Policy 🔻	Administration	î ▼			
Authentication 💿 Authorization	Refiling	💽 Posture	Client Pro	visioning	🚊 Security Group Acces
Profiling		Profiler Policy	List > Android		
	P		* Name	Android	
◆ - ≡ '≡	- Q-	P	nlicy Enabled		
👻 🚞 Profiling Policies			Shoy Endored		
🔣 Android 🚽 🚃		* Minimum Ce	rtainty Factor	30	0
		* Exc	eption Action	NONE	•
Apple-MacBook				create Matri	hing Identity Group
Apple-iPad				violate mater	
Apple-iPhone			0.	Jse Hierarci	hy
🛃 Apple-iPod		*	Parent Policy	NONE	-
Applera-Device					

<u>终端安全评估发现重定向的ISE授权配置文件</u>

完成以下步骤以配置授权策略状态重定向,允许将新设备重定向到ISE进行适当的发现和分析:

1. 从ISE,导航到**策略>策略元素>结果**。



2. 展开**授权**。单击Authorization Profiles(左窗格),然后单击Add。

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

3. 使用以下内容创建授权配置文件:名称:Posture_Remediation访问类型:Access_Accept常用工具:状态发现,已启用状态发现、ACL ACL-POSTURE-REDIRECT

cisco Identity Services Engine	
🐴 Home Monitor 🕶 Policy 💌 Administ	aton 🔹
Authentication Authorization 🔀 Prof	ling 🖉 Posture 🙀 Client Provisioning 📑 Security Group Access 🦨 Policy Elements
Dictionaries Conditions Results	
Deceder	Automation Profiles > New Automation Profile
(* P)	*Name Posture Remediation
4 - ≡ 1 8.	
Authentication	Description Permit Access To Posture And Remediation Services; Redirect Traffic To Client Provisioning And Posture Services.
+ 🧰 Authorization	*Access Type ACCESS ACCEPT
 Authorization Profiles 	
Cisco_IP_Phones	
DemyAccess DemyAccess	
Downloadable ACLs	* Common Tasks
Inline Posture Node Profiles	DACL Name
Profiling	E
Posture	L. VLAN
Client Provisioning	Voice Domain Permission
Security Group Access	Posture Discovery ACL ACL-POSTURE-REDIRECT
	Cantralizad Wah Authoritication
	C Auto Smart Port
	* Advanced Attributes Settings
	🔢 Select an item 💿 = 💼 💿 🗕 🛨
	* Attributes Details
	Access Type = ACCESS_ACCEPT cisco-aw-pair = url-redirect-acl=ACL-POSTURE-REDIRECT cisco-aw-pair = url-redirect=https://pii/8443/guestportal/gateway?sessionid=SessionidMatue&action=cpp

4. 单击Submit完成此任务。

5. 确认已添加新的授权配置文件。

CISCO Identity Services Engine	on 🔻		
Authentication Authorization Profilin Dictionaries Conditions Results	g 😰 Posture 🛃 Client Provisioning	🚉 Security Group Access	A Policy Elements
Results	Standard Authorization Profiles	lete 🖓 Filter 👻	
	Cisco_IP_Phones	Description Profile For Cisco Pho	ones.
Authorization Profiles Cisco_IP_Phones Dominance	DenyAccess PermitAccess Dentre Dementiation	Default Network Auth Default Network Auth	orization Profile with access orization Profile with access sture and Pernediation Serv
Originaccess PermitAccess Original Construction Posture_Remediation		- Tennin Access To Po	

<u>为员工创建ISE授权配置文件</u>

添加员工的授权配置文件允许ISE授权和允许具有已分配属性的访问。本例中分配了员工VLAN 11。

请完成以下步骤:

1. 从ISE导航到**策略>结果**。展开Authorization,然后单击Authorization Profiles,然后单击 Add。

ture 🛛 🗔 Client Provisioni
Authorization Profiles
r

- 2. 为员工授权配置文件输入以下内容:名称:Employee_Wireless常见任务:VLAN,已启用 VLAN,子值11
- 3. 单击Submit完成此任务。

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

4. 确认已创建新的员工授权配置文件。

cisco Identity Services Engine		
🍐 Home 🛛 Monitor 🔻 📴 Policy 💌 👔 Administratio	in 🔻	
🛃 Authentication 🛛 S Authorization 🔀 Profiling	Posture 🕞 Client Provisioning 🚊 Se	curity Group Access 🔒 Policy Elements
Dictionaries Conditions Results		
Results	Standard Authorization Profiles	
(٩)	🖉 Edit 🕂 Add 🖓 Duplicate 🗙 Delete	₩ Filter +
(∲ • <u>≡</u> <u>≣</u> <u>⊗</u> •	Name	Description
Authentication	Cisco_IP_Phones	Profile For Cisco Phones.
Authorization Authorization	DenyAccess	Default Network Authorization Profile with acc
Cisco IP Phones	Employee_Wireless	Full Network Access For Employees
Q DenyAccess	PermitAccess	Default Network Authorization Profile with acc
Employee_Wireless	Posture_Remediation	Permit Access To Posture And Remediation
Permitàrrese		

<u>为承包商创建ISE授权配置文件</u>

为承包商添加授权配置文件允许ISE授权和允许具有已分配属性的访问。在本例中,分配了承包商 VLAN 12。 请完成以下步骤:

- 1. 从ISE导航到**策略>结果**。展开Authorization,然后单击Authorization Profiles,然后单击 Add。
- 2. 为员工授权配置文件输入以下内容:名称:Employee_Wireless常见任务:VLAN,已启用 VLAN,子值



- 3. 单击Submit完成此任务。
- 4. 确认已创建承包商授权配置文件。

Results	Standard Authorization Profiles
٩ ٠	/ Edit 🕂 Add 🖓 Duplicate 🗙 Delete
�- ≡ ≡ ÷	Name
Authentication	
👻 🚞 Authorization 🛛 🖊 🎽	
Authorization Profiles	Contractor_Wireless
	DenvAccess
Downloadable ACLs	
Inline Posture Node Profiles	Employee_Wireless
- Profiling	PermitAccess
Froming	
Posture	Posture_Remediation

<u>设备状态/分析的授权策略</u>

新设备首次进入网络时,其相关信息很少,管理员会创建适当的策略,以允许未知终端在允许访问 之前被识别。在本练习中,将创建授权策略,以便将新设备重定向到ISE进行终端安全评估(对于 无代理的移动设备,因此仅分析相关);终端将重定向到ISE强制网络门户并识别。 1. 从ISE导航到**策略>授权**。

isco idditalij	Services Engin	0				and the second secon
🔥 Home Mon	lter V Policy V	Administration				
Authentication	 Authorization 	Ref Profiling	Posture	Client Provisioning	Security Group Access	Policy Elements
Define the Authoria	ration Policy by config	uring rules based	on identity group	os and/or other conditions	5	
First Matched Ru	le Applies	T				
-						
Exceptions						
Exceptions						
Exceptions Standard Status Rule	e Name	identi	ty Groups	Other Conditions	P	ermissions
Exceptions Standard Status Rule Pro	e Name filed Cisco IP Phones	Identi If Cisc	ty Groups xo-IP 💠 ar	Other Conditions	P 💠 Then	ermissions Cisco_IP_Pho 4

- 2. 有一个策略用于分析的Cisco IP电话。这是开箱即用的。将此编辑为状态策略。
- 3. 为此策略输入以下值:规则名称:Posture_Remediation身份组:任意Other Conditions > Create New:(Advanced)Session > PostureStatusPostureStatus > Equals:未知

	Session
	<u>م</u>
the second se	🖕 - 🗏 📜 🚳 - 📥
Client Provisioning 📄 Security Group Access 🚯 P	Agent-Request-Type
	CurrentDate
and/or other conditions	CurrentDay
	CurrentMonth
	CurrentTime
	CurrentWeekDay
	CurrentYear
	U OS-Architecture
Other Conditions Permissio	PostureStatus
Session:PostureStatus EQUAL then Select a	URL-Redirected
Add All Conditions Below to Library	
Condition Name Expression	
Session:PostureStat	Equals Vinknown

4. 设置以下权限:Permissions > Standard: Posture_Remediation



5. Click Save.注意:或者,可以创建自定义策略元素来增加易用性。

<u>测试状态补救策略</u>

可以执行简单演示,以显示ISE正根据终端安全评估策略正确分析新设备。

1. 从ISE,导航到管理>身份管理>身份。



2. 点击终端。关联并连接设备(本示例中为iPhone)。

Administration		
System Aldentity Management Network	Resources Age Guest Management	
Identities Groups External Identity Sources	Identity Source Sequences Settings	
Identities	Endpoints	
<u>(م</u>	/ Edit 🕂 Create 🗙 Delete 👻 😭 Import 👻	Export ▼ Filter ▼
₽- ₩-	Endpoint Profile	MAC Address
Users 💿 🛺	Apple-Device	5C:59:48:40:82:8D
Endpoints 📀 👕		

- 3. 刷新终端列表。观察给出的信息。
- 4. 从终端设备浏览到: URL:http://www(或10.10.10.10)设备被重定向。接受证书的任何提示。
- 5. 移动设备完全重定向后,从ISE再次刷新终端列表。观察变化。上一个终端(例如,Apple-Device)应更改为"Apple-iPhone"等。原因是HTTP探测功能在重定向到强制网络门户的过程 中有效地获取用户代理信息。

	Endpoints						
	🥖 Edit	Create	🔀 Delete 👻	🛃 Import 👻		Export 🔻	🖓 Filter 📼
	Endp	oint Profile			•	MAC Addr	ess
I	Apple	-iPhone				5C:59:48:4	40:82:8D

<u>差异化访问的授权策略</u>

成功测试安全评估授权后,继续构建策略,以支持员工和承包商的差异化访问,包括已知设备和特定于用户角色的不同VLAN分配(在此场景中,员工和承包商)。

请完成以下步骤:

- 1. 导航到ISE > Policy > Authorization。
- 2. 在Posture Remediation policy/line上方添加/插入新规则。

Standard		
Status Rule Name	Identity Groups Other Conditions	Permissions
Posture_Remediation	If Any I and Condition(s)	🔷 then Posture_Rem 💠 🔯 Actions
🗹 👻 Default	If no matches, then PermitAccess	Insert New Rule Above Insert New Rule Below
		Duplicate Above

3. 为此策略输入以下值:规则名称:员工身份组(扩展):终端身份组

de.	Interview Services Engine													
CIS	cisco identity Services Engine										Q)		
â	Home	Monito	r v 📄	Policy v	Administr	ation 🔻				(· 🗏 🗉		- S	4
Ŀ	Authent	tication	🧔 Aut	horization	🔀 Profil	ing 🦉	Posture		Client Provisio		Any			P
							-				Endpoint Ident	tity Groups		в 🗂
De	Define the Authorization Policy by configuring rules based on identity groups and/or other cor 📒 User Identity Groups													
													•	
E	irst Matc	hed Rule	Applies											
	_													
► E	Exceptio	ons												
¥ \$	Standaro	d												
Γ	Status	Rule I	Name	1		Identity	Groups	,	Other Condition					o
	-	Empl	oyee		lf	Any	-	and	Condition(s)	1				P
1		Postu	re_Rem	ediation	If									

终端身份组:已分析已分析:Android、Apple-iPad或Apple-

	Profiled	
	\bigcirc	Q
	∲- 🗏 🗄	÷
	Android	
	Apple-iPad	
	Apple-iPhone	
iPhone	Cisco-IP-Phone	9

4. 要指定其他设备类型,请点击+并添加更多设备(如果需要):终端身份组:已分析已分析 :Android、Apple-iPad或AppleiPhone

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

5. 为此策略指定以下"权限"值:其他条件(展开):创建新条件(高级选项

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

条件>表达式(从列表):InternalUser >名称

			DEVICE	•
			Guest	۲
			IdentityGroup	۱ ک
Other Conditions	Permissio		InternalUser	R.
Condition(s)	then AuthZ P		Microsoft	3
			Network Access	ی 🖢
Add All Conditions Below to	Library		Radius	ک ا
Condition Name	Expression	-	Cassian	~ L.
	Select Attribute	9		

InternalUser > Name:employee

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

6. 为安全评估会话合规添加条件:权限>配置文件>标准

: Employee_Wireless	
Permissions	
AuthZ Profile(s)	
Select an item	<u>●</u>
	Standard
	🔶 - 📃 🔚 🙀 🎡 -
	Cisco_IP_Phones
	Contractor_Wireless
	DenyAccess
	Employee_Wireless
	PermitAccess
	Posture_Remediation

7. Click Save.确认已正确添加策略。

r Standard		
Status Rule Name	Identity Groups Other Conditions	Permissions
Employee	If Apple-IPh 🔶 and InternalUser:Name EQUALS	e 💠 then Employee_Wi 💠
Posture_Remediation	Any 🔶 and Session:PostureStatus EQUA	NL 💠 then Posture_Rem 💠
Pefault	If no matches, then DenyAccess	

8. 继续添加承包商策略。在本文档中,复制了之前的策略以加快流程(或者,您可以手动配置以 实现良好实践)。从Employee policy > Actions中,单击**Duplicate Below**。

ſ	Standard					
I	Status Rule Na	me	Identity Groups	Other Conditions	Permissions	•
I	Employ	ee H	Apple-IPh 🔶 and	InternalUser:Name EQUALS e 🔶 then	Employee_Wi	🔶 🎡 Actions 🗸
	Posture	Remediation	Any \diamondsuit and	Session:PostureStatus EQUAL 💠 then	Posture_Rem.	Insert New Rule Above Insert New Rule Below
	Vefault	H I	no matches, then Deny	Access 💠	-	Duplicate Above Duplicate Below

9. 编辑此策略的以下字段(复制副本):规则名称:承包商其它条件>内部用户>姓名:承包商权
 限

:	: Contractor_Wireless										
* S	* Standard										
Γ	Status	Rule Name	Identity Groups	Other Conditions	Permissions						
1	-	Employee	If Apple-iPh 🗇 and	InternalUser:Name EQUALS e	💠 then Employee_Wi						
1	- 2	Employee_copy	If Apple-iPh 💠 and	InternalUser:Name EQUALS e	💠 then Employee_Wi 💠						
1	-	Posture_Remediation	If Any 💠 and	Session:PostureStatus EQUAL	🔶 🐜 Posture_Rem 🔶						
		Default	If no matches, then Deny	Access 🔶							

10. <u>Click **Save**</u>.确认之前的复制副本(或新策略)已正确配置。

73	Standard		
Γ	Status	Rule Name	Identity Groups Other Conditions Permissions
	-	Employee	If Apple-IPh \diamondsuit and InternalUser:Name EQUALS e \diamondsuit then Employee_Wi \diamondsuit
	-	Contractor	If Apple-IPh 🔶 and InternalUser:Name EQUALS co 💠 then Contractor_W 💠
	-	Posture_Remediation	If Any \diamondsuit and Session:PostureStatus EQUAL \diamondsuit then Posture_Rem \diamondsuit
	-	Default	If no matches, then DenyAccess

11. 要预览策略,请单击Policy-at-a-Glance。

remarky bervices ch	ω L	THE		ucitury	SCIVICES EII	wj.+
			is	e adm	nin Log Out	Feedback
					ee Task Nav	igator 👻 🕗
Client Provisioning	Security Gr	roup Access	🖧 Policy Eler	nents		
s and/or other condition	ns				Policy At	A Glance
d InternalUser:Nam	e EQUALS e	then □	Employee_Wi	¢	Actio	ons 🗸
d InternalUser:Nam	e EQUALS co	⇔ then	Contractor_W	\$	Actio	ons 👻

策略概览(Policy at Glance)视图提供汇总的策略摘要和易于查看的策略。

Authorization Policy At A Glance First Matched Rule Applies										
Exceptions	Exceptions									
Status Rule Name Identity Groups Other Conditions Permission										
	Nn riste available									
Standard										
Status	Rule Name	Identity Groups	Other Conditions	Permissions						
C Enabled	Employee	Android OR Apple-IPad OR Apple- iPhone	InternalUser:Name EQUALS employee	Employee_Wireless						
Enabled	Contractor	Android OR Apple-IPad OR Apple- iPhone	InternalUser:Name EQUALS contractor	Contractor_Wireless						
Enabled	Posture_Remediation	Алу	Session:PostureStatus EQUALS Unknown	Posture_Remediation						
Enabled	Default	Any		DenyAccess						

<u>测试CoA以区分访问</u>

利用为区分访问而准备的授权配置文件和策略,是时候进行测试了。如果使用单个安全WLAN,则员工将被分配员工VLAN,承包商将被分配为承包商VLAN。下一个示例中使用的是Apple iPhone/iPad。

请完成以下步骤:

1. 使用移动设备连接到安全的WLAN(POD1x)并使用以下凭证:用户名:employee密码 :XXXXX



2. 单击Join。确认已为员工分配了VLAN 11(员工VLAN)。

Wi-Fi Networks	pod1x						
Forget this Network							
IP Address							
DHCP	BootP	Static					
	4						
IP Address		0.10.11.100					
Subnet Mas	k 25	5.255.255.0					
Router		10.10.11.1					
DNS		10.10.10.10					

3. 单击Forget this Network。单击Forget进行确认。



4. 转到WLC并删除现有的客户端连接(如果在前面的步骤中使用了相同的连接)。导航到**监控** >**客户端> MAC地址**,然后单击**删除**。



5. 另一种清除以前客户端会话的可靠方法是禁用/启用WLAN。转到WLC > WLANs > WLAN,然 后单击要编辑的WLAN。取消选中Enabled > Apply(以禁用)。选中Enabled > Apply复选框 (以重新启用)。

cisco		<u>w</u> lans	CON	TROLLER	WIRELESS	SECURITY	Mį
WLANs	WLANs > E	Edit 'p	od1x				
WLANS	General	Secur	rity	QoS	Advanced		
Advanced	Profile Name			podix			
	Туре	Type SSID			N		
	SSID				11x		
	Status	Status		Enabled			
	Security	Policies		[WPA2]][Auth(802.1X)]	will a

6. 返回移动设备。使用以下凭证重新连接到同一WLAN:用户名:contractor密码 :XXXX

Enter the password for "pod1x" Cancel Enter Password					
Username	contractor				
Password	•••••••				
Mode	Automatic >				
1 2 3 4 5 6 7 8 9 0					

7. 单击Join。确认为承包商用户分配了VLAN 12(承包商/访客VLAN)。

Wi-Fi Networks	pod1x						
Forget this Network							
IP Address							
DHCP	BootP	Static					
IP Address		10.10.12.100					
Subnet Mas	k	255.255.255.0					
Router		10.10.12.1					

8. 您可以在ISE >监控>授权中查看ISE实时日志视图。您应该看到个人用户(员工、承包商)在 不同的VLAN中获得不同的授权配置文件(Employee_WirelessContractor_Wireless)。

A Home Monitor V Policy V Administration V									
Authentications	Authentications 💆 Alarms 👖 Reports 🔨 Troubleshoot								
Add or Remove Columns	🙀 Add or Remove Columns 👻 🏀 Refresh 💽 Show Lates								
Time	Status	Details	Usemame		Endpoint ID	IP Address	Network Device	Device Port	Authorization Profile
Aug 02,11 03:40:18.331 PM	×	a	employee		5C:59:48:40:82:8D		.wic		Employee_Wireless
Aug 02,11 03:36:33.663 PM	1	à	contractor		5C:59:48:40:82:8D		.wic		Contractor_Wireles
1	-						and a		

<u>WLC访客WLAN</u>

完成以下步骤以添加访客WLAN以允许访客访问ISE保证人访客门户:

- 1. 从WLC导航到WLANs > WLANs > Add New。
- 2. 为新的访客WLAN输入以下命令:配置文件名称
 - : pod1guestSSID:pod1guest

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

- 3. 单击 Apply。
- 4. 在访客WLAN > General选项卡下输入以下命令:状态:已禁用接口/接口组:访客

	ls <u>C</u> ON	NTROLLER	WIRELESS	<u>s</u> ecur					
WLANs > Edit ' <mark>pod1guest</mark> '									
General Se	curity	QoS	Advanced						
Profile Name Type		podigu WLAN	est						
SSID		podigu	est						
Status Security Polici	Enabled [WPA2][Auth(802.1X)] (Modifications done under security								
Radio Policy		All	-						
Interface/Inter Group(G)	rface	guest		-					
Multicast Vlan	Feature	🗆 Enabl	ed						
Broadcast SSI	D	🔽 Enabl	ed						

5. 导航到访客WLAN > Security > Layer2,然后输入以下内容:第2层安全:无

MONITOR	<u>W</u> LANs		ROLLER	WIREL	ESS	<u>S</u> ECURIT
WLANs >	Edit 'p	od1g	uest'			
Genera	Secu	rity	QoS	Advanc	ed	
Layer	2 Lay	ver 3	AAA S	ervers		
Laye	er 2 Securit	y <mark>₫</mark> N	one		-	and the second s
MAC Filtering						

6. 导航到访客WLAN > Security > Layer3选项卡,然后输入以下内容:第3层安全:无Web策略
 : 已启用Web策略子值:身份验证预身份验证ACL:ACL-POSTURE-REDIRECTWeb身份验证
 类型:外部(重定向到外部服务器
 > UDL: https://10.10.10.70:9442/guestnettel/Legin.setion

) URL:https://10.10.10.70:8443/guestportal/Login.action

M		LANS CON	TROLLER	WIRELESS	SECURITY	MANAGEMENT
v	VLANs > E	dit 'pod1g	juest'			
	General	Security	QoS	Advanced		
	Layer 2	Layer 3	AAA Se	ervers		
	Layer 3	Security No	ine 🗘 🔨	-		
-	🕨 🗹 We	b Policy ¹				
	 Auth 	entication				
	O Pass	through				
	O Conc	ditional Web Re	direct			
	🖯 Spla	sh Page Web R	edirect			
	O On M	AC Filter failu	re ¹¹			
	Preauth	entication ACL		-POSTURE-RE	DIRECT	-
	Over-rid	le Global Confi	g 🗹 En	able 🛑 👘		1
	Web Aut	th type	(E	xternal(Re-dir	ect to external s	server)
		ttps://10.10.1	0.70:8443/	guestportal/Lo	gin.action	

7. 单击 Apply。

8. 确保保存WLC配置。

<u>测试访客WLAN和访客门户</u>

现在,您可以测试访客WLAN的配置。它应将访客重定向到ISE访客门户。

请完成以下步骤:

1. 从iPhone等iOS设备导航到Wi-Fi Networks > Enable。然后,选择POD访客网络。



2. 您的iOS设备应显示来自访客VLAN(10.10.12.0/24)的有效IP地址。



3. 打开Safari浏览器并连接到: URL:http://10.10.10.10系统将显示Web身份验证重定向。 4. 点击继续,直到您到达ISE访客门户页面。



截图显示访客门户登录上的iOS设备。这可以确认WLAN和ISE访客门户的正确设置处于活动状 态。



<u>ISE无线发起访客接入</u>

可以将ISE配置为允许发起访客。在这种情况下,您将配置ISE访客策略以允许内部或AD域(如果 集成)用户发起访客访问。您还将配置ISE以允许发起人查看访客密码(可选),这对本实验很有 帮助。

请完成以下步骤:

 将员工用户添加到SponsorAllAccount组。有不同的方法可以执行此操作:直接转到组,或编辑用户并分配组。在本示例中,导航到管理>身份管理>组>用户身份组。然后,单击 SponsorAllAccount并添加员工用户。

🔥 Home Monitor v Policy v	Administration	-		
🐝 System 🛛 🏄 Identity Manager	nent Network	Resources	Guest Management	
Identities Groups Externa	al Identity Sources	Identity Source	Sequences Setti	ings
Identity Groups		User Identity G	iroups > SponsorAllAcco	punt
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	- <u></u>	* Name	SponsorAllAccount	
Endpoint Identity Groups		Description	Default Sponsor Ider	ntity Group
		Save F Member Us	Reset	
		Users		
		Add 🔻	🗙 Delete 👻	
		<u></u>		
	:	Users		2
		👤 contra	ctor	
	T	👤 emplo	yee 🐣	
2. 导航到 管理>访客管理>保证人 组	L 。			
dentity Services Eng	gine			
A Home Monitor V Policy V	Administration V	-		
System Aldentity Managem Identities Groups External	System Deployment Licensing		Identity Man Identities Groups	agement
Identity Groups	Certificates		External Iden	tity Sources
	Logging		Identity Sour	ce Sequences
Ver Ver Identity Groups	Admin Access	3	Jetungs	
Endpoint Identity Groups	Settings		Guest Mana	gement
	Network Res	ources	Sponsor Gro	ups
	Network Devic	ces	Settings	

3. 点击**编辑**,然后选择**发起人所有帐户**。

cisco ide	ntity Services I	Engine		
💧 Home	Monitor 🔻 Poli	icy 🔻 🕴 Ad	dministration 🔻	
🔆 System	👰 Identity Mana	agement	🔛 Network Resources	🛃 Guest Management
Sponsor Gr	oup Policy Sp	onsor Grou	ups Settings	
Guart Enon	cor Groupe			
Guest Spon	sui Groups			
💙 Edit 🚽	Add 🔀 Delet	te 🍸 Filt	er 🔻	
🗖 Sponso	or Group Name	•	Description	
Sponso	orAllAccounts 🔩		Default SponsorGroup	
🗖 Sponso	rGroupGrpAccoun	its	Default SponsorGroup	

4. 选择Authorization Levels并设置以下内容:查看访客密码:是

dentity Services Engi	ne
🛕 Home Monitor 🔻 Policy 🔻	Administration v
🔆 System 🛛 👰 Identity Managem	ent 🔛 Network Resources 🛃 Guest Management
Sponsor Group Policy Sponsor	r Groups Settings
Sponsor Group List > SponsorAllAcco	ounts
	× 7
General Authorization Leve	Guest Roles Time Profiles
Allow Login	Yes
Create Accounts	Yes
Create Bulk Accounts	Yes
Create Random Accounts	Yes
Import CSV	Yes
Send Email	Yes
Send SMS	No
View Guest Password	Yes 🚽
Allow Printing Guest Details	Yes
View/Edit Accounts	All Accounts
Suspend/Reinstate Accounts	All Accounts
* Account Start Time	1 Days (Valid Range 1 to 999999999)
* Maximum Duration of Account	5 Days (Valid Range 1 to 999999999)
Save Reset	

5. 单击Save以完成此任务。

<u>赞助访客</u>

以前,您已配置相应的访客策略和组,以允许AD域用户发起临时访客。接下来,您将访问发起人门 户并创建临时访客访问权限。

请完成以下步骤:

 从浏览器导航至以下URL:http://<ise ip>:8080/sponsorportal/或https://<ise ip>:8443/sponsorportal/。然后,使用以下内容登录:用户名:aduser(Active Directory)、 employee(内部用户)密码 :XXXX



2. 在"发起人"(Sponsor)页面中,单击**创建单个访客用户帐户**。

cisco Sponsor Port	al
Home Settings Customization	Sponsor Portal: Getting Started
Connects 2nd Protocol	View All Guest User Accounts
	Create Single Guest User Account
View Guest Accounts Create Multiple Accounts	Create Multiple Guest User Accounts

3. 对于临时访客,添加以下内容:名字:必填(例如,Sam)姓氏:必填(例如,Jones)组角 色:访客时间配置文件:DefaultOneHour时区:任意/默认

Sponsor Port	al
	Account Management > View All Guest Accounts > Create Guest Account
mization	Create Guest Account
	First Name:
	Last Name:
Sec	Email Address:
2.4	Phone Number:
et al second	Company:
	Optional Data 1:
	Optional Data 2:
	Optional Data 3:
	Optional Data 4:
gement	Optional Data 5:
counts Accounts	Guest
n Accounts s	Time Profile:
	Timezone: EST EST
	A = Required fields
	Submit Cancel

- 4. 单击"Submit"。
- 5. 访客帐户根据您之前的输入创建。请注意,密码可见(从上一个练习中),与散列密码相***。
- 6. 保持此窗口打开,显示访客的用户名和密码。您将使用它们测试访客门户登录(下一步)。

Account Management	t > View All Guest Accounts > Create Guest Account
	a set alle Case at a different discussion alle second
Succ	essfully Created Guest Account slam0002
Username:	siam0002
Password:	5_5g6d7Kx
First Name:	Sam 🔨
Last Name:	iAm
Email Address:	
Phone Number:	
Company:	
Status:	AWAITING INITIAL LOGIN
Suspended:	false
Optional Data 1:	
Optional Data 2:	
Optional Data 3:	
Optional Data 4:	
Optional Data 5:	
Group Role:	Guest
Time Profile:	DefaultOneHour
Timezon	e: EST
Account	Start Date: 2011-07-15 13:56:04 EST
Account	Expiration Date: 2011-07-15 14:56:04 EST
Email Print	Create Another Account View All Accounts

<u>测试访客门户访问</u>

使用AD用户/发起人创建的新访客帐户,测试访客门户和访问权限的时机到了。

请完成以下步骤:

- 1. 在首选设备(本例中为Apple iOS/iPad)上,连接到Pod访客SSID并检查IP地址/连接。
- 2. 使用浏览器并尝试导航至http://www。您将重定向到"访客门户登录"页面。


- 3. 使用在上一个练习中创建的访客帐户登录。如果成功,系统将显示Acceptable use policy页面
- 4. 选中Accept terms and conditions, 然后单击Accept。



原始URL已完成,并且允许终端作为访客访问。

要保护与ISE的通信,请确定该通信是身份验证相关还是用于ISE管理。例如,对于使用ISE Web UI的配置,需要配置X.509证书和证书信任链以启用非对称加密。

请完成以下步骤:

- 从有线连接的PC上,打开一个浏览器窗口,转到https://AD/certsrv。注意:使用安全HTTP。
 注:请使用Mozilla Firefox或MS Internet Explorer访问ISE。
- 2. 以管理员/Cisco123身份登录。



3. 单击 Download a CA certificate, certificate chain, or CRL。

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

Welcome

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

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

For more information about Active Directory Certificate Services,

Select a task:

Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

4. 单击Download CA certificate并保存它(注意保存位置)。

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

- 5. 打开浏览器窗口访问https://<Pod-ISE>。
- 6. 转至Administration > System > Certificates > Certificates Authority Certificates。

cisco Identity Services Engine		
💧 Home 🛛 Monitor 🔻 Policy 🔻	Administration	
Metrics	🔆 System Deployment	
Active Endpoints	Licensing	
0 –	Certificates	

- 7. 选择Certificate Authority Certificates操作并浏览到以前下载的CA证书。
- 8. 选择**Trust for client with EAP-TLS**,然后提交。

cisco Identity Services Engine		ise adm
A Home Monitor V Policy V Administration		
System Aldentity Management	rk Resources 🛛 🛃 Guest Management	
Deployment Licensing Certificates Log	ging Operations Admin Access	Settings
Certificate Operations	Certificate Authority Certificates > Impo Timport a new Trusted CA (Certifi	icate Authority) Certificate
Certificate Signing Requests Certificate Authority Certificates	* Certificate File	Browse
	All Certificate Authority Certificates a they may be enabled for EAP-TLS t	are available for selection as the Root CA for secure LDAP co below:
	Trust for client with EAP-TLS	
	Description	

9. 确认已将CA添加为受信任的根CA。

cisco Identity Services Engine		ise admin L		
Administration Administration		••••••••••••••••••••••••••••••••••••••		
System & Identity Management Network Resources & Guest Management				
Deployment Licensing Certificates Logging Operations Admin Access Settings				
Certificate Operations Certificate Authority Certificates				
S Local Certificates	🖊 Edit 🕂 Add 🕢 Export 🗙 Delete			
Certificate Signing Requests	Friendly Name Expiration	Issued To		
Certificate Autoonty Certificates	ise.corp.rf-demo.com Thu Jul 12 12:14	4:47 PDT 2012 ise.corp.rf-demo.com		

- 10. 从浏览器转到Administration > System > Certificates > Certificates Authority Certificates。
- 11. 单击Add,然后单击Generate Certificate Signing Request。

cisco Identity Services Engine	
👍 Home Monitor 🔻 Policy 🔻 📗 Administrat	tion •
🔆 System 🖉 Identity Management 📱 Netw	vork Resources 🛛 🛃 Guest Management
Deployment Licensing Certificates L	ogging Operations Admin Access Settings
Certificate Operations	Local Certificates
Cocal Certificates	/ Edit Add Export X Delete
Certificate Signing Requests	Friend Import Local Server Certificate Iss
	Generate Certificate Signing Request
	Bind CA Certificate

12. 提交以下值:证书主题:CN=ise.corp.rf-demo.com密钥长度 :2048

Local Certificates > Generate Certificate Signing Request Generate Certificate Signing Request		
Certificate		
Certificate Subject	CN=ise.corp.rf-demo.com	
* Key Length	2048	
Digest to Sign With	SHA1	

13. ISE提示在CSR页面中提供CSR。Click



- 14. 从ISE CSR页面选择CSR并点击导出。
- 15. 将文件保存到任何位置(例如,下载等)
- 16. 文件将另存为*.pem。

cisco Identity Services Engine	4			
A Home Monitor Policy Administration	•			
🔆 System 😤 identity Management 🛛 🗮 Network	Resources 🛛 🛃 Guest Management			
Deployment Licensing Certificates Logo	ging Operations Admin Access	: Settings		
Certificate Operations Certificate Signing Requests				
Cocal Certificates				
Certificate Signing Requests	Friendly Name	Certificate Subject	Key Length	
Certificate Authority Certificates	🔽 ise.corp.rf-demo.com	CN=ise.corp.rf-demo.com	2048	
^				

- 17. 找到CSR文件并使用记事本/写字板/文本编辑进行编辑。
- 18. 复制内容("全选">"复制")。



- 19. 打开浏览器窗口访问https://<Pod-AD>/certsrv。
- 20. <u>点击**申请证书**。</u>

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

Welcome

Use this Web site to request a certificate for your Web brow communicate with over the Web, sign and encrypt message

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

For more information about Active Directory Certificate Ser

Select a task:

Request a certificate,

View the status of a Centificate request

Download a CA certificate, certificate chain, or CRL



22. 将CSR内容粘贴到已保存请求字段中。

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

Submit a Certificate Request or Renewal Request

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



23. 选择Web Server作为证书模板,然后单击Submit。

Microsoft Activ	e Directory Certificat
Microsoft Active	Directory Certificate Services corp-RFDEMO-CA
Submit a Certi	ficate Request or Renewal Request
To submit a sav source (such as Saved Request:	ved request to the CA, paste a base-64-encoded CN a Web server) in the Saved Request box.
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	GA/MMZsTIoEPekcunnm+ZFt1AXajB32uwHHL11c9 ▲ J4qsQM7KEYOpQt4biaO71S8Lm6BBTk9mRhiTBwSF kSa7LHYgkgLRYBnpu15RjQ7wWijArH8cK1OrVT42 LPKQ72N2XYIXfu0jdgoaJjmsk6T9nLABVYQ6nKQx VSQYBOjTYHXIPG8/ned9z3M0iZd2sm4XNS2bJfO/ END CERTIFICATE REQUEST
Certificate Temp	ate:
	Web Server
Additional Attribu	ites:
Attributes:	
	Submit >

24. 选择DER encoded,然后单击Download certificate。



- 25. 将文件保存到已知位置(例如,下载)
- 26. 转至Administration > System > Certificates > Certificates Authority Certificates。

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

27. 单击Add > Bind CA Certificate。



28. 浏览到以前下载的CA证书。

cisco Identity Services Engine					
💧 Home Monitor 🔻 Policy 🔻 🔤 Admi	nistration •				
🔆 System 👰 Identity Management 📱	Network Resources 😸 Guest Management				
Deployment Licensing Certificates	Logging Operations Admin Access Settings				
Depinyment Eldepiny Operations Settings Certificate Operations Local Certificates > Bind CA Signed Certificate Bind CA Signed Certificate Certificate Signing Requests Certificate Authority Certificates Certificate File C\Users\pau\Downloads\certnew.cer Browse_ Protocol EAP: Use certificate for EAP protocols that use SSL/TLS tunneling Management Interface: Use certificate to authenticate the web server (GUI) Override Policy Replace A certificate being imported may be determined to already exist in the system w Replace Certificate being imported may be determined to already exist in the system w Replace Certificate being imported may be determined to already exist in the system w Replace Certificate being imported may be determined to already exist in the system w Replace Certificate being imported may be determined to already exist in the system w Certificate being imported may be determined to already exist in the system w Certificate being imported may be determined to already exist in the system w Certificate being imported may be determined to already exist in the system w Certificate being imported may be determined to already exist in the system w Certificate being imported may be determined to already exist in the system w Certificate being imported may be determined to already exist in the system w Certificate being imported may be determined to already exist in the system w Certificate bei					
	Certificate Certificate contents to be replaced while retaining the existing protocol selection				

- 29. 选择Protocol EAP和Management Interface, 然后单击Submit。
- 30. 确认已将CA添加为受信任的根CA。



<u>Windows 2008 Active Directory集成</u>

ISE可以直接与Active Directory(AD)进行通信,以进行用户/机器身份验证或检索授权信息用户属性 。为了与AD通信,ISE必须"加入"到AD域。在本练习中,您将将ISE加入AD域,并确认AD通信是否 正常工作。

请完成以下步骤:

1. 要将ISE加入AD域,请从ISE转至管理>身份管理>外部身份源。

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

- 2. 从左侧窗格(外部身份源)中选择Active Directory。
- 3. 在右侧,选择**Connection**选项卡并输入以下内容:域名:corp.rf-demo.com身份库名称 :AD1

cisco Identity Services Engine		
🛕 Home Monitor 🔻 Policy 🔻 🔜	Iministration 💌	
System	Network Resources 🛃 Guest Management	
Identities Groups External Iden	ty Sources Identity Source Sequences Settings	
External Identity Sources	Active Directory > AD1 Connection Oroups Attributes	
Certificate Authentication Profile	Server Connection	
LDAP	To configure Active Directory:	
RADIUS Token	First enter the required fields: the Domain Name to connect to and the Identity S	tore Nam
RSA SecuriD	pages, and click submit to commit the Active Directory configuration to all nodes After the configuration has been submitted, then Join or Leave operations must	be perfor
	* Domain Name corp.rf-demo.com	ection
	* Identity Store Name AD1	
	Local Node Status No Active Directory Configuration is Set	

4. 单击**Test Connection**。输入AD用户名(aduser/Cisco123),然后单击**OK**。

* Domain Name	corp.rf-demo.com	Test (Connection
dentity Store Name			Test Connection ×
ocal Node Status 🕴	No Active Directory Configuration is	set	* User Name <mark>: aduser</mark>
ettings			* Password:

- 5. 确认"测试状态"显示测试成功(Test Succeeded)。
- 6. 选择Show Detailed Log并观察对故障排除有用的详细信息。单击 OK 继续。

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

7. 单击Save Configuration。

	* Domain Name corp.rf-demo.com Test Connection * Identity Store Name AD1 Local Node Status No Active Directory Configuration is Set
	▼ Connection Settings
	 Enable Password Change Enable Machine Authentication Enable Machine Access Restrictions Aging Time (hours) 6 (Valid Range 1 to 8760)
	Save Configuration Join Delete Configuration
8.	单击 Join 。输入AD用户(管理员/思科123),然后单击 OK 。
	* Domain Name corp.rf-demo.com Test Connection * Identity Store Name AD1 Local Node Status Not Joined to a domain
	▼ Connection Settings
	 Enable Password Change Enable Machine Authentication Enable Machine Access Restriction Aging Time (hours) Monte Configuration Save Configuration

9. 确认Join Operation Status显示为**Succeeded**,然后单击**OK**继续。服务器连接状态显示 CONNECTED。如果此状态随时更改,测试连接将帮助排除AD操作问题。

Identity Source Sequences Settings	
Active Directory > AD1 Connection Groups Attrib Join Stat	Domain ×
To configure Active Directory:	
 First enter the required field pages, and click submit to c After the configuration has been a 	OK the Identity Store Name to referre to all nodes in the ISE deploys
* Domain Name corp.rf-	demo.com Test Connection
* Identity Store Name AD1	
Local Node Status Joined to	Domain: corp.rf-demo.com Connection Status: CONNECTED

添加Active Directory组

添加AD组时,允许对ISE策略进行更精细的控制。例如,AD组可以按功能角色(如员工或承包商组)区分,而不会在以前的ISE 1.0练习中遇到相关漏洞,在此练习中,策略仅限于用户。

在本实验中,仅使用Domain Users和/或Employee组。

请完成以下步骤:

- 1. 从ISE,转至管理>身份管理>外部身份源。
- 2. 选择Active Directory > Groups选项卡。
- 3. 单击+Add,然后单击Select Groups From Directory。



4. 在后续窗口(选择目录组)中,接受域(corp-rf-demo.com)和过滤器(*)的默认值。然后,单击

Retrieve Groups。

Select Directory Groups				
This dialog is used to select groups from the Directory. O Use * for wildcard search (i.e. admin*). Search filter appli	lick Retrieve Groups to rea ies to group name and not t			
Domain: corp.rf-demo.com Filter: * Retriev	e Groups Number of Grou			
Name	NE			
corp.rf-demo.com/Users/DnsUpdateProxy				
corp.rf-demo.com/Users/Domain Admins				
corp.rf-demo.com/Users/Domain Computers				
Corp.rf.demo.com/Lisers/Domain Controllers				
Corp. if domo.com/Users/Domain Cupete				
Corp.rf-demo.com/Users/Domain Users				
Corp.n-demo.com/Osers/Domain Osers				
Corp.n-demo.com/Users/Employee				
corp.rf-demo.com/Users/Enterprise Admins				
选中Domain Users和Emplovee组的框。完成后单击 OK。				
Corp.n-demo.com/Users/Domain Computers	GLOBAL			
corp rf-demo.com/Users/Domain Guests	GLOBAL			
corp.rf-demo.com/Users/Domain Users	GLOBAL			
Corp.rf-demo.com/Users/Employee	GLOBAL			
corp.rf-demo.com/Users/Enterprise Admins	UNIVERSAL			
Corp.rf-demo.com/Users/Enterprise Read-only Domain Controllers	UNIVERSAL			
Corp.rf-demo.com/Users/Group Policy Creator Owners	GLOBAL			
Corp.rf-demo.com/Users/RAS and IAS Servers	LOCAL			
C corp.rf-demo.com/Users/Read-only Domain Controllers	GLOBAL			
Corp.rf-demo.com/Users/Schema Admins	UNIVERSAL			
•)			

OK Cancel

6. 确认已将组添加到列表中。

Identity Services Engine						
A Home	Monitor V	Policy V	Administration			
🔆 System	Identity	/ Managemer	nt 🔛 Network	Resources	🛃 Guest Manageme	nt
Identities	Groups	External lo	dentity Sources	Identity So	urce Sequences S	ettings
External Identity Sources Active Directory > AD1 Certificate Authentication Profile Certificate Authentication Profile Active Directory > AD1 Connection Groups Attributes Connection Groups Attributes Active Directory > AD1 Connection Groups Attributes Connection Groups Attributes Active Directory > AD1 Connection Groups Attributes Connection Groups Attributes Active Directory > AD1 Connection Groups Attributes Connection Groups Attributes Connection Groups Attributes 						
👻 Active Dir	rectory			P Add	👗 Delete Group	
E LDAP			۲	Nam	10	
🚞 RADIUS T	oken		•	C corp.	.rf-demo.com/Users/Do	main Users
🚞 RSA Sec	urID			C corp.	.rf-demo.com/Users/Em	ployee

添加身份源序列

默认情况下,ISE设置为使用内部用户进行身份验证存储。如果添加AD,可以创建优先级顺序以包括ISE将用于检查身份验证的AD。

请完成以下步骤:

1. 从ISE,导航到管理>身份管理>身份源序列。

cisco Identity Services Engin	Administration
System System Identity Manageme Identities Groups External External Identity Sources	Administration * Main Stration * Main Stration * Deployment Licensing Certificates Logging Operations Admin Access
单击+Add以添加新序列。 Cisco Identity Services Engine	nistration v

	System The nutry management	(63)	ources		
l	Identities Groups External Identity Sources Identity Source Sequences Settings				
	Identity Source Sequences				
	/ Edit Add Duplicate X Delete V Filter -				
	□ Name	•	Description	Identity Stores	
	Guest_Portal_Sequence		A built-in Identity Sequence for the Guest Portal	Internal Users	
	Sponsor_Portal_Sequence		A built-in Identity Sequence for the Sponsor Portal	Internal Users	

3. 输入新名称:AD_Internal。将所有可用源添加到Selected字段。然后,根据需要重新排序,将 AD1移至列表顶部。单击"Submit"。

Identities Groups External Identity Sources (Identity Source Sequences) Settings			
Identity Source Sequences List > New Identity Source Sequence			
▼ Identity Source Sequence			
* Name AD_Internal			
Description			
▼ Certificate Based Authentication			
Select Certificate Authentication Profile			
▼ Authentication Search List			
A set of identity sources that will be accessed in sequence until first authentication succeeds Available Selected AD1 Internal Users Internal Endpoints INTERNAL EN			
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			

4. 确认序列已添加到列表。

cisco Identity Services Engine		and the second
🚖 Home Monitor 🔻 Policy 🔻 🗚dministration 💌		
System 😵 Identity Management 🔛 Network Res	ources 🛃 Guest Management	
Identities Groups External Identity Sources 🚺	dentity Source Sequences Settings	
Identity Source Sequences		
🖊 Edit 🕂 Add 🖓 Duplicate 🗙 Delete 🖓 Filte	•	
□ Name ▲	Description	Identity Stores
AD_Internal		AD1,Internal Endpoints,Internal Users
Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users
Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal Users

<u>集成AD的ISE无线赞助访客接入</u>

ISE可配置为允许使用策略发起访客,以允许AD域用户发起访客访问。

请完成以下步骤:

1. 从ISE导航到管理>访客管理>设置。

cisco Identity Services Engine						
💧 Home Monitor 🔻 Policy 🔻	Administration V					
Metrics	System Deployment	Identity Management				
Active Endpoints 1 -	Certificates Logging Operations	Bitemal Identity Sources Identity Source Sequences Settings				
System Summary	Admin Access Settings	Guest Management Sponsor Group Policy				
Name	Network Resources	Sponsor Groups Settings				
🗹 🕋 ise	Network Device Groups External RADIUS Servers					

2. 展开Sponsor,然后单击Authentication Source。然后,选择AD_Internal作为身份库序列。

cisco Identity Services Engine	
🔥 Home Monitor 🔻 Policy 🛪 🗌 Administratio	
🔆 System 🖉 Identity Management 🖀 Netwo	ork Resources 📳 Guest Management
Sponsor Group Policy Sponsor Groups	ettings
Settings	Sponsor Authentication Servers
General Sponsor	* Identity Store Sequence Sponsor_Portal_Sequence
E Authentication Source	Save Reset Mentity Sequence
12 Portal Customization	
Canguage Template	
Guest	Guest_Portal_Sequence
	Sponsor_Portal_Sequence
	AD_Internal 0

3. 确认AD_Internal作为身份库序列。Click **Save**.



5. 在第一个规则上方插入新策略(点击右侧的操作图标)。

cisco Ide	ntity Services Engine				ise	ecinin Log Out Feedback
💧 Home	Monitor 🔻 Policy 🔻	Administration *				😐 Task Navigator 👻 🙆
🔆 System	😤 Identity Management	🔛 Network Resources	🛃 Guest Management			
(Sponsor Gr	oup Policy Sponsor Gr	roups Settings				
Status	Rule Name	Identity Groups	Other Conditions		Spansor Groups	
I 🔽 🔹	Manage All Accounts	🛛 🕈 SponsorAll 💠	and Condition(s)	💠 them	SponsorAlAcco	😂 Actions 두
	Manage Group Accounts	r SpansorGr 🔶	and Condition(s)	then	SponsorGroup	Insert New Policy Above
	Manage Own Accounts	Y Sponsor0 🔶	and Condition(s)	💠 then	SponsorGroup	Duplicate Above Duplicate Below
						Delete

6. 对于新的发起人组策略,请创建以下内容:规则名称:域用户身份组:任意其他条件:(新建/高级)>

AD1

cisco Identity Services Engine					
💧 Home 🛛 Ma	onitor 🔻 🛛 Policy 🔻 📃 🥂	dministration v			
🔆 System 🛛	🕺 Identity Management	🔛 Network	Resources	🛃 Guest Managem	ent
(Sponsor Group	Policy Sponsor Gro	ups Settin	gs		
Status Ru	ule Name	Ident	ity Groups	Other Conditions	
	omain Users	If Any	¢	and Select Attribu	ute
Add All Cond	litions Below to Library				
Condition Nat	me Expressi Select At	on tribute 💽			
			Dictionaries	م	
		<	⊱- 🗏 🗎	- Â	1
			AD1	Jun	
		1	📄 Airespace	Ŷ	
		(CERTIFICA	TE 🕥	
AD1 · 外部组					

AD1:外部组

Status Rule Name	-	Identity Groups	Other Conditions				
🛛 📱 👻 👻 Domain Users	if 👘	Any 💠	and Select Attribute				
Add All Conditions Below to Library							
Condition Name	Expression						
\diamond	Select Attribute						
		AD1					
			(م				
		🔶 + 🗐 🗄	🖌 🖗				
		ExternalGro	ups				
		IdentityAcce	essRestricted				

AD1外部组>等于> corp.rf-demo.com/Users/Domain用户

cisco Identity Services Engine	
Administration 🕶	
🔆 System 🖉 Identity Management 🔛 Network Resources 🛃 Guest Management	
Sponsor Group Policy Sponsor Groups Settings	
Status Rule Name Identity Groups Other Conditions	Sponsor (
Domain Users If Any 🔶 and Select Attribute 🗢 then	Sponsor G
Add All Conditions Below to Library	SponsorAll
Condition Name Expression	SponsorGr
corp.rf-demo.com/Users/Domain Users corp.rf-demo.com/Users/Employee	SponsorGr

7. 在保证人组中,设置以下内容:保证人组

: SponsorAllAccounts	
cisco Identity Services Engine	ize a
A Home Monitor T Policy Administration T	
🔆 System 🖉 Identity Management 📱 Network Resources 🛃 Guest Management	
Sponsor Group Policy Sponsor Groups Settings	
Status Rule Name Identity Groups Other Conditions	Sponsor Groups
Domain Users If Any 💠 and AD1:ExternalGroups E	EQUALS 💠 then Sponsor Group 🗢
Manage All Accounts If SponsorAll 💠	
🛛 🗹 🔹 Manage Group Accounts 🔤 🖉 SponsorGr 💠	Sponsor Groups
Manage Own Accounts If SponsorO 🗇	♦- ■ 1 @.
	II SponsorAlAccounts
	SponsorGroupGrpAccounts SponsorGroupGrpAccounts
	a sponsororoupownuccounts

8. 导航到管理>访客管理>保证人组。



9. 选择以编辑>SponsorAllAccounts。

cisco Identity Services Engine						
💧 Home	Monitor 🔻 Policy 🔻 📙	Administration 💌				
🔆 System	Identity Management	Network Resources	🛃 Guest Management			
Sponsor Gr	oup Policy (Sponsor Gr	oups Settings				
Guart Enon	cor Groupo					
Guest Spon	sur Groups					
💙 Edit 🚽	💙 Edit 🕂 Add 🗙 Delete 🖓 Filter 👻					
🗖 Sponsor Group Name 🔺 Description						
🔽 Sponso	IrAllAccounts	Default SponsorGroup				
🗖 Sponso	rGroupGrpAccounts	Default SponsorGroup				

10. 选择Authorization Levels并设置以下内容:查看访客密码:是

cisco Identity Services Engine					
🛕 Home Monitor 🔻 Policy 🔻	Administration v				
🔆 🔆 System 🛛 🏄 Identity Managem	ent 🔛 Network Resources 🛃 Guest Management				
Sponsor Group Policy Sponsor	r Groups Settings				
Sponsor Group List > SponsorAllAcco	ounts				
	×				
General Authorization Leve	Guest Roles Time Profiles				
Allow Login	Yes				
Create Accounts	Yes				
Create Bulk Accounts	Yes				
Create Random Accounts	Yes				
Import CSV	Yes				
Send Email	Yes				
Send SMS	No				
View Guest Password	Yes 🚽				
Allow Printing Guest Details	Yes				
View/Edit Accounts	All Accounts				
Suspend/Reinstate Accounts	All Accounts				
* Account Start Time	1 Days (Valid Range 1 to 999999999)				
* Maximum Duration of Account	5 Days (Valid Range 1 to 999999999)				
Sava Danat					
Jave					

<u>在交换机上配置SPAN</u>

配置SPAN - ISE管理/探测接口与WLC管理接口相邻的第2层。交换机可配置为SPAN和其他接口 ,例如员工和访客接口VLAN。

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

参考: Apple MAC OS X的无线身份验证

使用Apple Mac OS X无线笔记本电脑,通过经过身份验证的SSID作为内部用户(或集成的AD用户)关联到WLC。如果不适用,请跳过。 1. 在Mac上,转到WLAN设置。启用WIFI,然后选择并连接到在上一个练习中创建的启用

Tx: 254B/s Rx: 6.7KB/s S Tx: 254B/s Tx: 2	Thu 10:47
A. Port: On	
Turn AirPort Off	
√blizzard	ê 🔶
355	ê 🔶
alpha	ê 😤
alpha_phone	ê 🔶
Branch	ê 🔶
Branch-PSK	ê 🔶
BranchVoice	ê 🔶
Demo2-Rogue	ê 🛜
Demo5-Rogue	£ 🛜
Employee	9
FlexDemo	ê 🔶
guest-test	(()
guestnet	(0
J_test	(¢
Lab	ê 🛜
mi-demo-1x	ê 🔶
mi-rf-mgt	ê 🔶
open	((6
pod1x	🔒 🛜
PodX	((¢
rf-COA	ê 🔶
rf-management	ê 🤶
secure-ipv6	ê 🔶
Join Other Network Create Network Open Network Preferences	
open netholk rieleleles	

802.1X的POD SSID。

2. 提供以下连接信息:用户名:aduser(如果使用AD)、employee(内部 — 员工)、 contractor(内部 — 承包商)密码:XXXX802.1X:自动TLS证书:无

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

,笔记本电脑可能无法连接。此外,ISE可以引发失败事件,如下所示: Authentication failed :12514 EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client certificates chain

3. 转到**System Preference > Network > Airport > 802.1X**设置并将新的POD SSID/ WPA配置文 件身份验证设置为:TLS:已禁用PEAP:已启用TTLS:已禁用EAP-FAST:已禁用

AirPort TCP/IP	DNS WINS 802.1X Proxies Ethern	net
▼User Profiles		
🗹 WPA: alpha	User Name: aduser	
WPA: pod1x	Password:	
WPA: DIIZZard	Always prompt for	nassword
		passitora
DEAD Enable	Authentication: Enable Protocol	
FEAF - Enable		
Everything else = Dis		Ų.
	EAP-FAST	÷.
	Configure	
	Configure Trus	it
	Wireless Network: pod1x	
	Security Type: WPA2 Enterprise	•
+ -		

4. 单击**OK**继续并允许保存设置。

5. 在Network屏幕上,选择适当的SSID + 802.1X WPA配置文件,然后单击Connect。



6. 系统可能会提示输入用户名和密码。输入AD用户和密码(aduser/XXXX),然后单击**OK**。

	Authenticating to network "pod1x"
-	Please enter your name: aduser Please enter your password:
	Cancel OK



参考: Microsoft Windows XP的无线身份验证

使用Windows XP无线笔记本电脑通过经过身份验证的SSID作为内部用户(或集成AD用户)关联到WLC。如果不适用,请跳过。

请完成以下步骤:

1. 在笔记本电脑上,转到WLAN设置。启用WIFI并连接到在上一个练习中创建的启用802.1X的 POD SSID。



2. 访问WIFI接口的网络属性。



3. 导航到**无线网络**选项卡。选择Pod SSID网络属性>身份验证选项卡> EAP类型=受保护的 EAP(PEAP)。

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

- 4. 点击EAP属性。
- 5. 设置以下项:验证服务器证书:已禁用身份验证方法:安全密码(EAP-MSCHAP v2)

Protected EAP Properties		
When connecting:		
Validate server certificate		
Connect to th EAP MSCHAPv2 Properties		
When connecting:		
CA 1 CA 1 Ca demo loci Automatically use my Windows logon name and password (and domain if any).		
Certiposte C		
Certiposte Si		
Certisign - A		
Certisign - Autoridade Certificadora - AC4		
Do not prompt user to authorize new servers or trusted		
certification authorities.		
Select Authentication Method:		
Secured password (EAP-MSCHAP V2)		
Enable Fast Reconnect		
Enable Quarantine checks Disconnect if server does not present studiobinding TLV		

- 6. 在所有窗口中单击OK以完成此配置任务。
- 7. Windows XP客户端提示输入用户名和密码。在本例中,它是aduser/XXXX。
- 8. 确认网络连通性、IP编址(v4)。

参考: Microsoft Windows 7的无线身份验证

使用Windows 7无线笔记本电脑通过经过身份验证的SSID作为内部用户(或集成AD用户)关联到 WLC。 1. 在笔记本电脑上,转到WLAN设置。启用WIFI并连接到在上一个练习中创建的启用802.1X的

Currently connected to:	43	
No Internet access		
Wireless Network Connection	^	10
secure-ipv6 Connected	I	
Branch-PSK	m,	
pod1x		
Connect automatically Conn	ect	
FlexDemo	lle.	
alpha_phone	In.	

POD SSID。

- 2. 访问Wireless Manager并编辑新的POD无线配置文件。
- 3. 设置以下项:身份验证方法:PEAP记住我的凭据……:已禁用验证服务器证书(高级设置):已禁用身份验证方法(高级设置):EAP-MSCHAP v2自动使用我的Windows登录 ……:已禁用



相关信息

• <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)。