# 使用基于ISE的WLC配置到Active Directory组映 射的动态VLAN分配

目录
先决条件
要求
使用的组件
<u>规则</u>
使用 RADIUS 服务器执行动态 VLAN 分配
网络图
配置
ISE到AD集成和配置ISE上用户的身份验证和授权策略
<u>支持SSID 'office_hq'的dot1x身份验证和AAA覆盖的WLC配置</u>
<u>验证</u>
<u>故障排除</u>

# 简介

本文档介绍动态VLAN分配的概念。

# 先决条件

本文档介绍如何配置无线LAN控制器(WLC)和身份服务引擎(ISE)服务器,以便动态地将无线LAN (WLAN)客户端分配到特定VLAN。

## 要求

Cisco 建议您了解以下主题:

- 无线局域网控制器(WLC)和轻量接入点(LAP)的基础知识
- 身份验证、授权和记帐(AAA)服务器(例如ISE)的功能知识
- 全面了解无线网络和无线安全问题
- 有关动态VLAN分配的功能和配置知识
- 基本了解Microsoft Windows AD服务以及域控制器和DNS概念
- 具备接入点协议(CAPWAP)控制和调配的基础知识

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 运行固件 8.8.111.0 版本的 Cisco 5520 系列 WLC
- Cisco 4800系列AP
- 本地Windows请求方和Anyconnect NAM
- 思科安全ISE版本2.3.0.298
- 配置为域控制器的 Microsoft Windows 2016 Server
- 运行版本15.2(4)E1的Cisco 3560-CX系列交换机

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。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

规则

有关文档规则的详细信息,请参阅 <u>Cisco 技术提示规则。</u>

# 使用 RADIUS 服务器执行动态 VLAN 分配

在大多数 WLAN 系统中,每个 WLAN 都有适用于与服务集标识符 (SSID) 关联的所有客户端的静态 策略,即以控制器术语表示 WLAN。虽然此方法功能强大,但也具有局限性,这是因为,它要求客 户端与不同的 SSID 相关联以便继承不同的 QoS 和安全策略。

思科WLAN解决方案通过支持身份网络解决了这一限制。 这允许网络通告单个SSID,但允许特定用 户根据用户凭证继承不同的QoS、VLAN属性和/或安全策略。

动态 VLAN 分配便是一项这样的功能,它根据无线用户提供的凭证将该用户置于特定 VLAN 中。将 用户分配到特定VLAN的任务由RADIUS身份验证服务器(例如Cisco ISE)处理。例如,为了让无 线主机在园区网络中移动时保持同一个VLAN上,可以使用此选项。

思科ISE服务器根据多个可能的数据库(包括其内部数据库)之一对无线用户进行身份验证。例如 :

- 内部数据库
- Active Directory
- 通用轻量目录访问协议 (LDAP)
- 与开放式数据库连接 (ODBC) 兼容的关系数据库
- Rivest、Shamir 和 Adelman (RSA) SecurID 令牌服务器
- 与 RADIUS 兼容的令牌服务器

Cisco ISE身份验证协议和支持的外部身份源列出了ISE内部和外部数据库支持的各种身份验证协议

0

本文档重点介绍如何对使用Windows Active Directory外部数据库的无线用户进行身份验证。

身份验证成功后,ISE从Windows数据库中检索该用户的组信息,并将该用户关联到相应的授权配 置文件。

当客户端尝试与注册到控制器的LAP关联时,LAP会在各自EAP方法的帮助下将用户的凭证传递到 WLC。

WLC使用RADIUS协议(封装EAP)将这些凭证发送到ISE,ISE将用户的凭证传递到AD以在 KERBEROS协议的帮助下进行验证。

AD验证用户凭证,并在身份验证成功后通知ISE。

身份验证成功后,ISE服务器会将某些Internet工程任务组(IETF)属性传递给WLC。这些RADIUS属 性决定了必须分配给无线客户端的VLAN ID。客户端的 SSID(WLAN,从 WLC 的角度而言)并不 重要,这是因为,会始终为用户分配此预先确定的 VLAN ID。

用于 VLAN ID 分配的 RADIUS 用户属性包括:

- IETF 64(隧道类型)—将此项设置为VLAN
- IETF 65(隧道介质类型)—将此值设置为802
- IETF 81(隧道专用组ID)—将此项设置为VLAN ID

VLAN ID为12位,取值在1和4094(含)之间。由于Tunnel-Private- Group-ID属于字符串类型(如 用于IEEE 802.1X的RFC2868中所定义),因此VLAN ID整数值被编码为字符串。当发送这些隧道 属性时,需要填写 Tag 字段。

如<u>RFC 2868</u>第3.1部分中所述:"标记"字段的长度为一个二进制八位数,它用于提供在同一数据包 中分组引用同一隧道属性的方法。此字段的有效值是 0x01 到 0x1F(包含 0x01 和 0x1F)。如果未 使用 Tag 字段,则它一定为零 (0x00)。有关所有 RADIUS 属性的详细信息,请参阅 <u>RFC 2868。</u>

## 配置

本节提供配置文档中所述功能所需的信息。

#### 网络图



## 配置

下面是此图中使用的组件的配置详细信息:

- ISE (RADIUS)服务器的IP地址是10.48.39.128。
- WLC的管理和AP管理器接口地址为10.48.71.20。
- DHCP服务器驻留在LAN网络中,并且针对各个客户端池进行了配置;如图所示。
- 此配置中使用VLAN1477和VLAN1478。营销部门的用户配置为置于VLAN1477中,HR 部门 的用户配置为由RADIUS服务器置于VLAN1478中 当两个用户连接到同一个SSID时 office\_hq.

VLAN1477:192.168.77.0/24。网关:192.168.77.1 VLAN1478:192.168.78.0/24。网关 :192.168.78.1

• 本文档使用带有PEAP-mschapv2的802.1x作为安全机制。



注意:Cisco建议您使用高级身份验证方法(例如EAP-FAST和EAP-TLS身份验证),以保 护WLAN。 在执行此配置之前已做出以下假设:

- LAP已注册到WLC
- DHCP服务器分配了一个DHCP作用域
- 网络中的所有设备之间存在第3层连接
- 本文档讨论在无线端所需的配置,并假设有线网络已部署到位
- 在AD上配置相应的用户和组

要完成基于ISE到AD组映射的WLC动态VLAN分配,必须执行以下步骤:

- 1. ISE到AD集成和配置ISE上用户的身份验证和授权策略。
- 2. WLC配置,以支持SSID 'office\_hq'的dot1x身份验证和AAA覆盖。
- 3. 最终客户端请求方配置。

ISE到AD集成和配置ISE上用户的身份验证和授权策略

- 1. 使用admin帐户登录到ISE Web UI界面。
- 2. 导航到Administration > Identity management > External Identity Sources > Active directory。

tituti Identity Services Engine Home	Context Visibility     Operations	Policy      Administration      Work Centers	
System      Identity Management     Network F	esources	t pxGrid Service + Feed Service + Threat Centric NAC	
Identities Groups External Identity Sources	Identity Source Sequences	s	
External Identity Sources	Active Directory		
	/ Edit 👷 Add 🗙 Delete 🖌	Node View 🔂 Advanced Tools 👻 Scope Mode	
Certificate Authentication Profile	Join Point Name	<ul> <li>Active Directory Domain</li> </ul>	
Active Directory			No data available
LDAP			
ODBC			
RADIUS Token			
RSA SecurID			
SAML Id Providers			
Social Login			

3. 单击Add, 然后从Active Directory加入点名称设置输入域名和身份库名称。在本例中, ISE注 册到域wlaaan.com, 并且加入点指定为AD.wlaaan.com - ISE的本地重要名称。

External Identity Sources		Connection		
<₽ ▼   ₩ ▼	ŵ. <b>-</b>	* Join Point Name	AD.wlaaan.com	(I)
Certificate Authentication Profile				Ŭ
Active Directory		<ul> <li>Active Directory Domain</li> </ul>	wlaaan.com	(i)
E LDAP				
CDBC				
RADIUS Token		C. L		
C RSA SecurID		Submit Cancel		
SAML Id Providers				
Social Login				

4. 按<sub>Submit</sub>下按钮后,将打开一个弹出窗口,询问您是否要立即将ISE加入AD。按<sub>Yes</sub>并提供具有 管理员权限的Active Directory用户凭据,以将新主机添加到域中。

Connection Whitelisted	Domains Passiv	eID Groups	Attributes	Advanced Settings		
* Join Point Name AD.wi     * Active Directory Domain wlaat	aaan.com		I) I)			
양금 Join 양금 Leave 🧕 Test User 音	Diagnostic Tool 🛛 🛞 Refre	sh Table				
ISE Node	▲ ISE Node Role	Status	Domain Controller	Site		
rmanchur-ise.wlaaan.com	STANDALONE	A Not Joined				
	Join Domain Please specify the creder • AD U Specify Organizat Store Cr	ntials required to Join ISE ser Name () Administrat * Password ••••••••••••••••••••••••••••••••••••	node(s) to the Active Dire	ectory Domain.	×	
				OK Cancel		

5. 在此之后,您必须将ISE成功注册到AD。

al Identity Sources	Connection Whitelisted Dom	ains PassiveID Group	os Attributes Advanced	Settings
Er V @v Certificate Authentication Profile Active Directory LDAP ODRC	Join Point Name     AD.wlaaan     Active Directory Domain     wlaaan.co	.com	Ū.	
RADIUS Token	👷 Join 🔮 Leave 👤 Test User 💼 Diag	nostic Tool 🛛 🛞 Refresh Table		
RSA SecurID	ISE Node	ISE Node Role Status	Domain Controller	Site
SAML Id Providers	rmanchur-ise.wlaaan.com	STANDALONE Operational	WIN-CFA29CSRIL9.wlaaan.com	Default-First-Site-Name

如果注册过程中有任何问题,可以使用Diagnostic Tool 来运行AD连接所需的测试。 6. 您必须检索用于分配相应授权配置文件的活动目录组。导航到Administration > Identity management >

External Identity Sources > Active directory >

>Groups ,然后点击Add并选择Select Groups from Active Directory。

	sources	
Identities Groups External Identity Sources	Identity Source Sequences	
External Identity Sources	Connection Whitelisted Domains PassiveID Groups Attributes	Advanced Settings
(= ▼   E ▼ _ ② <sub>▼</sub>	/ Edit + Add - X Delete Group Update SID Values	
Certificate Authentication Profile     Active Directory	Nam Select Groups From Directory	
2 AD.wlaaan.com		No data available
LDAP		
ODBC		
RADIUS Token		
SAML Id Providers		
Social Login		

7. 将打开一个新的弹出窗口,您可以在其中指定过滤器以检索特定组或从AD检索所有组。 从AD组列表中选择相应的组,然后按OK。

Select Directory Groups This dialog is used to select groups from the Director	ory.			х
Domain wlaaan.com	-	-]		
Name Filter *	SID Filter *	Type Filter GLOBAL	*	
	Group SID		Group Type	
wlaaan.com/Users/Cloneable Domain Control	llers S-1-5-21-2222429329-41080851	64-3220345271-522	GLOBAL	
wlaaan.com/Users/DnsUpdateProxy	S-1-5-21-2222429329-41080851	64-3220345271-1102	GLOBAL	
wlaaan.com/Users/Domain Admins	S-1-5-21-2222429329-41080851	64-3220345271-512	GLOBAL	
wlaaan.com/Users/Domain Computers	S-1-5-21-2222429329-41080851	64-3220345271-515	GLOBAL	
wlaaan.com/Users/Domain Controllers	S-1-5-21-2222429329-41080851	64-3220345271-516	GLOBAL	
wlaaan.com/Users/Domain Guests	S-1-5-21-2222429329-41080851	64-3220345271-514	GLOBAL	
wlaaan.com/Users/Domain Users	S-1-5-21-2222429329-41080851	64-3220345271-513	GLOBAL	
wlaaan.com/Users/Group Policy Creator Own	ers S-1-5-21-2222429329-41080851	64-3220345271-520	GLOBAL	
vlaaan.com/Users/HR	S-1-5-21-2222429329-41080851	64-3220345271-1105	GLOBAL	
wlaaan.com/Users/Key Admins	S-1-5-21-2222429329-41080851	64-3220345271-526	GLOBAL	
✓ wlaaan.com/Users/Marketing	S-1-5-21-2222429329-41080851	64-3220345271-1104	GLOBAL	
wlaaan.com/Users/Protected Users	S-1-5-21-2222429329-41080851	64-3220345271-525	GLOBAL	
wlaaan.com/Users/Read-only Domain Control	llers S-1-5-21-2222429329-41080851	64-3220345271-521	GLOBAL	

OK Cancel

8. 相应的组会添加到ISE中并可保存。按。Save

	C	Connectio	on		Whiteliste	d Domains	PassiveID	Groups	Attributes	Advanced Settings	
1	Edit	جالے م	Id -	YR	loto Croup	Lindate SID Value					
_	Eult	Tw	JU Ŧ		sete Group	opuble SID value					
	Na	ame					-	SID			
	w	aaan.co	m/Use	ers/HR				S-1-5-21-2222	2429329-4108085164-322	20345271-1105	
	wl	aaan.co	m/Use	ers/Ma	rketing			S-1-5-21-2222	2429329-4108085164-322	20345271-1104	
_	_		_								
Sa	ve	Reset	:								

9. 将WLC添加到ISE网络设备列表-导航到Administration > Network Resources > Network Devices, 然后按Add。 通过在WLC和ISE之间提供WLC管理IP地址和RADIUS共享密钥来完成配置。

dentity Services Engine	Home + Context Visibility + Operations + Policy - Administration + Work Centers
System      Identity Management	Network Resources     Device Portal Management     pxGrid Services     Feed Service     Threat Centric NAC
Network Devices Network Device G	iroups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services
0	
Network Devices	Notwork Devices List > New Network Device Network Device Network Devices
Default Device	• Name 148-5520
Device Security Settings	
	[IP Address + 'IP: 10.48.71.20 / 32
	IPV6 is supported only for TACACS At least one IPv6 must be defined when RADULS is selected
	Device Profile      disco v     (     (     )     (     )
	Model Name v
	Software Version +
	Network Device Group
	Location LAB O Set To Default
	IPSEC Is IPSEC Device O Set To Default
	Device Type V/LC-lab O Set To Default
	RADIUS Authentication Settings
	RADIUS UDP Settings
	Protocol RADIUS
	Shared Secret     Show
	CoA Port 1700 Set To Default
	RADIUS DTLS Settings (7)

10. 现在,在您将ISE加入AD并将WLC添加到设备列表后,您可以开始为用户配置身份验证和授 权策略。

#### • 创建授权配置文件,以将市场营销用户分配到VLAN1477,并将HR组用户分配到 VLAN1478。

导航到Policy > Policy Elements > Results > Authorization > Authorization profiles并单击Add按钮以创建新配置 文件。

cisco Identity Services Engine Hor	me   Context Visibility   Operations   Policy	Administration     Work Centers	
Policy Sets Profiling Posture Client Pr	rovisioning - Policy Elements		
Dictionaries + Conditions - Results			
G			
Authentication	Standard Authorization Profiles		
- Authorization	For Policy Export go to Administration > System > Backup &	Restore > Policy Export Page	
Authorization Profiles	🖌 Edit 🕂 Add 🕞 Duplicate 🗙 Delete		
Authonization Profiles	Name	Profile	Description
Downloadable ACLs	Blackhole_Wireless_Access	誌 Cisco 🕀	Default profile used to blacklist wireless dev
<ul> <li>Profiling</li> </ul>	Cisco_IP_Phones	🖮 Cisco 🕀	Default profile used for Cisco Phones.
Posture	Cisco_Temporal_Onboard	誌 Cisco 🕀	Onboard the device with Cisco temporal ag
	Cisco_WebAuth	🗰 Cisco 🕀	Default Profile used to redirect users to the
Client Provisioning	NSP_Onboard	誌 Cisco 🕀	Onboard the device with Native Supplicant
	Non_Cisco_IP_Phones	🔐 Cisco 🕀	Default Profile used for Non Cisco Phones.
	DenyAccess		Default Profile with access type as Access-
	PermitAccess		Default Profile with access type as Access-

• 使用相应组的VLAN信息完成授权配置文件配置;示例显示了Marketing组配置设置。

Dictionaries + Conditions - Result	
G	
Authentication	Authorization Profile
▼ Authorization	* Name Marketing
Authorization Profiles	Description Marketing
Downloadable ACLs	* Access Type ACCESS ACCEPT *
Profiling	Network Device Profile 🛛 👘 Gisco 🛛 🗣
▶ Posture	Service Template
Client Provisioning	Track Movement
	Passive Identity Tracking 📋 🕡
	▼ Common Tasks
	DACL Name
	ACL (Filter-ID)
	Security Group
	VLAN     Tag ID 1     Edit Tag     ID/Name     1477
	▼ Advanced Attributes Settings
	🛿 Select an item 📀 = 💽 — 🕂
	▼ Attributes Details
	Access Type = ACCESS_ACCEPT Tunnel-Private-Group-ID = 1:1477 Tunnel-Ype = 1:13 Tunnel-Medium-Type = 1:6
	Submit Cancel

必须为其他组执行类似配置,并且必须配置各自的VLAN标记属性。

• 配置授权配置文件后,您可以定义无线用户的身份验证策略。这可以通过配置Custom或修

改Default策略集来实现。在本示例中,Default策略集被修改。导航到Policy > Policy Sets > Default。默认情况下,对于dot1x身份验证类型,ISE将使用All\_User\_ID\_Stores,尽管它使用当前默认设置,因为AD是All\_User\_ID\_Stores的身份源列表的一部分,此示例对该相应LAB控制器使用更具体的规则WLC\_lab,并使用AD作为身份验证的唯一源。

	Haidning Policy Clement		Click here to do wireless setup and visibility setup Do not show this agr
cy Sets → Default			Resot
Status Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
arch			
Oefault	Default policy set		Default Network Access 🔺 * 🕈
Authentication Policy (4)			
+ Status Rule Name	Conditions		Use Hits Ar
earch			
Ø MAR	08	JMAB	Internal Endpoints × v
0		ss_MAB	> Options
	<b>•</b> •	ns_802.1X	
/ @ WLC_MB	AND & C	ype EQUALS AI Device Types#WLC-lab	AD Wasan.com
	E 0	DE Location EQUALS AI Locations#LAB	> Options
() Derix	0P 0	_802.1X	Al_User_ID_Stores * *
		995_802.1X	> Options
(a) Defect			M_User_ID_Stores × *
0 0000			> Options
Authorization Policy - Local Exceptions			
Authorization Policy - Global Exception	5		
Authorization Policy (12)			

• 现在,您必须为根据组成员身份分配相应授权配置文件的用户创建授权策略。导航到 Authorization policy部分并创建策略以完成此要求。

Policy Sets Pr	ofiling Posture Client Provision	ing		(	Click here to do wireles	s setup and visibility setup Do n	ot show this	again. ×
Policy Sets +	Default						Reset	Savo
Status	Policy Set Name	Description	Conditions		1	Nowed Protocols / Server 5	Sequence	Hits
Search	Default	Default policy set				Default Network Access	×* +	•
> Authenticatio	on Policy (4)							
> Authorization	n Policy - Local Exceptions							
> Authorization	n Policy - Global Exceptions							
✓ Authorization	n Policy (14)							
+ Statu	s Rule Name	Conditions		Results Profiles	Security Gro	ups	Hits	Actions
search	Wreless_Marketing	AND E AD wlasan o	nss In ExternalGroups EQUALS wlaaan.com/Users/Marketing	× Marketing	Select from	<b>.</b>	۰	۰
I, 0	Wireless_HR	AND E AD.wissen.co	oss m ExternalGroups EQUALS wisaan com/UsersHR	HR	+ Select from		۰	۰

支持SSID 'office\_hq'的dot1x身份验证和AAA覆盖的WLC配置

1. 将ISE配置为WLC上的RADIUS身份验证服务器。导航到Web UI界面中的Security > AAA > RADIUS > Authentication部分,并提供ISE IP地址和共享密钥信息。

cisco	MONITOR WLANS CONTROLLER	r W <u>i</u> reless <u>s</u> ecurity m <u>a</u> nagement c <u>o</u> mmands he <u>l</u> p <u>f</u> eedback
Security	RADIUS Authentication Serve	ers > New
Security  AAA General RADIUS Authentication Accounting Auth Cached Users Fallback DNS Downloaded AVP TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies Password Policies Local EAP Advanced EAP Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec Local Policies Umbrella Advanced Advanced	RADIUS Authentication Server Server Index (Priority) Server IP Address(Ipv4/Ipv6) Shared Secret Format Shared Secret Confirm Shared Secret Apply Cisco ISE Default settings Apply Cisco ACA Default settings Key Wrap Port Number Server Status Support for CoA Server Timeout Network User Management Management Retransmit Timeout Tunnel Proxy PAC Provisioning IPSec Cisco ACA	<pre>ers &gt; New 2  2  10.48.39.128 ASCII  ASCII  ASCII  COMPARIANCE ASC</pre>

2. 在WLC上的wLANs部分下配置SSIDoffice\_hq;此示例使用wPA2/AES+dot1x和AAA覆盖配置SSID。 已为WLAN选择接口Dummy,因为仍会通过RADIUS分配正确的VLAN。必须在WLC上创建此虚 拟接口并给予IP地址,但IP地址不必是有效的,而且上行链路交换机中无法创建放置该虚拟接 口的VLAN,因此如果没有分配VLAN,客户端将无法访问任何位置。

cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK			
WLANs	WLANs											
WLANS	Current Filter	n: Nor	ne	[Change Filte	er] [Clear Filter	1				[	Create New	\$ Go
Advanced	WLAN ID	Туре	Profile Na	me		WLAN SSID		,	Admin Status	Security Policies		
	01	WLAN	test			test		6	Enabled	[WPA2][Auth(802.1X	)]	
	C 2	WLAN	AndroidAP			AndroidAP		E	Enabled	[WPA2][Auth(PSK)]		
	253	WLAN	BTER-BTwi	fi-public		BTwifi-public		E	Enabled	[WPA2][Auth(PSK)]		
advada.											Say	e Configuration Ping Lo

cisco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK	1								A Home
WLANs	WLANs > New															< Back	Apply
✓ WLANS WLANS ► Advanced	Type Profile Name SSID ID	with office 3	N E														

WL	ANs > Edit 'office_hq	
G	eneral Security Q	oS Policy-Mapping Advanced
	Profile Name Type SSID Status	office_hq WLAN office_hq Imabled
	Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
	Radio Policy Interface/Interface Group(G Multicast Vlan Feature	All dummy Enabled
	Broadcast SSID NAS-ID	Enabled  none

WLANs > Edit 'office\_hq'

General See	curity QoS	Policy-Map	ping Adva	nced			
Layer 2	ayer 3 AAA Se	ervers					
Layer 2 Secur	rity <sup>6</sup> WPA+WPA2 MAC Filtering	2 ÷	)				
Fast Transition							
Fast Transition Over the DS Reassociation Tin	Ada aneout 20 Seconds	ptive 🕈					
Protected Mana	gement Frame						
PMF	Disa	abled \$					
WPA+WPA2 Pa	rameters						
WPA Policy							
WPA2 Policy	<b>V</b>						
WPA2 Encrypt	tion 🗸 🗹 AES	5 TKIP	CCMP256	GCMP128	GCMP256		
OSEN Policy							
Authentication	Key Management	<u>19</u>					
802.1X	🕑 Enable						

WLANs	WLANs > Edit 'office_h	q'		
WLANs	General Security	QoS Policy-Mapping	Advanced	
Advanced	Layer 2 Layer 3	AAA Servers		
	Select AAA servers below RADIUS Servers RADIUS Server Overwrite Apply Cisco ISE Default S Authentication Server 2 None Server 3 None Server 4 None Server 5 None Server 6 None Server 6 None Server 7 None 2 Server 7 None	to override use of default serv e interface Enabled settings Enabled DN Servers Accounting Set 128, Port: 1812 ¢ None ¢ None ¢ None	rvers EAP Pau 28, Port:1813 ¢	rameters le

ANs > Edit 'office_hq'			
eneral Security QoS Po	licy-Mapping Advanced		
Allow AAA Override	Enabled		DHCP
Coverage Hole Detection	Enabled		DHCP Server Override
Enable Session Timeout 2 1800 Aironet IE	Timeout (secs)		DHCP Addr. Assignment CRequired Management Frame Protection (MFP)
Override Interface ACL	IPv4 None \$	IPv6 None \$	MFP Client Protection 4 Optional \$
Layer2 Aci	None Ŧ		DTIM Period (in beacon intervals)
P2P Blocking Action	Disabled \$		802.11a/n (1 - 255) 1 802.11b/a/n (1 - 255) 1
Client Exclusion <sup>2</sup>	Enabled 180 Timeout Value (secs)		NAC
Maximum Allowed Clients 8	0		NAC State None +
Static IP Tunneling 11	Enabled		Load Balancing and Band Select
Wi-Fi Direct Clients Policy	Disabled \$		Client Load Balancing
Maximum Allowed Clients Per AP Radio	200		Client Band Select
Clear HotSpot Configuration	Enabled		Passive Client
Client user idle timeout(15-100000)			

3. 您还必须在WLC上创建用户VLAN的动态接口。导航至Controller > InterfacesUI菜单。如果WLC在该 VLAN中具有动态接口,则它只能执行通过AAA收到的VLAN分配。

.ı ı.ı ı. cısco	<u>M</u> ONITOR <u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Controller								
General	General Informatio	on						
Icons	Interface Name	vlan14	77					
Inventory	MAC Address	00:a3	8e:e3:5a:1a					
Interfaces Interface Groups	Configuration				_			
Multicast	Guest Lan							
Network Routes	Quarantine							
Fabric Configuration	Quarantine Vlan Id	0						
Redundancy	NAS-ID	none						
Mobility Management	Physical Information	on						
Ports	Port Number		1					
▶ NTP	Backup Port		0					
> CDP	Active Port		1					
PMIPv6	Enable Dynamic AP M	anagement						
Tunneling	Tatoufaco Adduoco							
▶ IPv6	Interface Address							
mDNS	VLAN Identifier		1477					
Advanced	IP Address		192.168.77.5	_				
Lawful Interception	Netmask		255.255.255.0					
	Gateway		192.168.77.1					
	Profix Longth		120					
	IPv6 Gateway							
	Link Local IPv6 Addre	ss	fe80::2a3:8eff:1	ee3:5a1a/64				
	DHCP Information			,,				
	Primary DHCP Server		192.168.77.1					
	Secondary DHCP Serv	/er						
	DHCP Proxy Mode		Global 🛊					

# 验证

使用Windows 10本地请求方和Anyconnect NAM测试连接。

由于您使用的是EAP-PEAP身份验证且ISE使用自签名证书(SSC),您必须同意证书警告或禁用证书 验证。在企业环境中,必须在ISE上使用签名和受信任证书,并确保最终用户设备在"受信任 CA"(Trusted CA)列表下安装了相应的根证书。

测试与Windows 10和本地请求方的连接:

1. 打开Network & Internet settings > Wi-Fi > Manage known networks并通过按Add new network钮创建新的网络配置文件;填写所需信息。

← Settings	
命 Wi-Fi	
Manage known networks	
Add a new network	Add a new network
	Network name
Search this list	office_hq
Sort by: Preference $ \checkmark $ Filter by: All $ \checkmark $	Security type
	WPA2-Enterprise AES ~
	EAP method
111 W	Protected EAP (PEAP) V
11.	Authentication method
lic	Secured password (EAP-MSCHAP v2)
lic	Connect automatically
	Connect even if this network is not broadcasting
	Save Cancel

2. 检查ISE上的身份验证日志并确保为用户选择了正确的配置文件。

c	Refresh © Reset Repeat Counts	Export To •														,	Filter •	۰۰
	Time	Status	Details	Repeat	Identity		Endpoint ID	Endpoint P	Authenticat	Authorization Policy	Authorizati	IP Address	Network Device	Device Port	Identity Group	Posture St	Server	
×					Bob	×	Endpoint ID	Endpoint Profi	Authentication	Authorization Policy	Authorization I	IP Address	Network Device	Device Port	Identity Group	Posture Statur	Server	
	Feb 15, 2019 02 16:43 300 PM	0	à	3	Bob		F4.8C 50.62.14.68	Unknown	Default >> W	Default >> Wireless_HR	HR						manchur	ise
	Feb 15, 2019 02:09:56.389 PM		0		800		F4.8C 50:62:14:68	Unknown	Default >> W	Default >> Wireless_HR	HR		WLC5520		Unknown		manchur	ise

3. 检查WLC上的客户端条目,确保它已分配到正确的VLAN并处于RUN状态。

،، ،،، ،، cısco	MONITOR WLANS	CONTROLLER V	WIRELESS SECURIT	Y MANAGEMENT	COMMANDS	HELP	FEEDBACK						Saya C	onfiguration	Bing   Log	out   Befresh
Monitor	Clients														Entries	1 - 1 of 1
Summary Access Points Cisco CleanAir	Current Filter N	one	[Charge_Eits	er] [Clear.Filter]												
Statistics     CDP	Client MAC Addr (4:8c:50:62:14:6b	IP Address(Jov4 192.168.78.36	(lav6)	AP N AP4C	ame 77.6D9E.6162			WLAN Profile office_hq	WLAN SSID office_hq	User Name Bob	Protocol 802.11ac(5 GHz)	Status Associated	Auth Yes	Port Slot	Id Tunne No	No No
Rogues     Clients																
Sleeping Clients Multicast																
Applications																

4. 从WLC CLI,可使用show client dertails 命令检查客户端状态:

show client detail f4:8c:50:62:14:6b	
Client MAC Address	f4:8c:50:62:14:6b
Client Username	Bob
Client Webauth Username	N/A
Hostname:	
Device Type:	Intel-Device

AP MAC Address	70:69:5a:51:4e:c0
AP Name	AP4C77.6D9E.6162
AP radio slot Id	1
Client State	Associated
User Authenticated by	RADIUS Server
Client User Group	Bob
Client NAC OOB State	Access
Wireless LAN Id	3
Wireless LAN Network Name (SSID)	office_hq
Wireless LAN Profile Name	office_hq
Hotspot (802.11u)	Not Supported
Connected For	242 secs
BSSID	70:69:5a:51:4e:cd
Channel	36
IP Address	192.168.78.36
Gateway Address	192.168.78.1
Netmask	255.255.255.0
Policy Manager State	RUN
EAP Type	PEAP
Interface	vlan14/8
VLAN	14/8
Quarantine VLAN	0
ACCESS VLAN	14/8

测试与Windows 10和Anyconnect NAM的连接:

1. 从available SSIDs列表和相应的EAP身份验证类型(在本示例PEAP中)以及内部身份验证表 单中选择SSID。

	Cisco AnyConnect Secure Mobility Client -   VPN: Use a browser to gain access.  Connect Web Authentication Required
	Network: Connected (10.103.150.57) internet III V III
Cisco AnyConnect	× curity:
Enter info	rmation for the connection.
Media:	Wi-Fi Hidden Network
Descriptive Name:	office_hq Scan:
SSID:	office_hq can not required on current Wi-Fi.
Security:	WPA2 Enterprise AES 🗸
802. 1X Configuration	PEAP     g Security:       ot currently protected by Umbrella.       Missing.

2. 提供用于用户身份验证的用户名和密码。



3. 由于ISE正在向客户端发送SSC,您必须手动选择信任证书(在生产环境中,强烈建议在 ISE上安装受信任证书)。

Cisco AnyConnect X		
The server certificate for the network 'office_hq' has failed validation. Do you want to trust it?	VPN: Verify your network connection.	
Certificate Name: rmanchur-ise.wlaaan.com@		
Issued To: rmanchur-ise.wlaaan.com	No Network Connectivity	
Issued By: rmanchur-ise.wlaaan.com Expiration Date: 2020-02-13 15:03:40 UTC	Network: Authenticating	
Trust Do Not Trust	office_hq 🗎 ııll 🗸 🗎	
	Web Security: No License Key.	

4. 检查ISE上的身份验证日志并确保为用户选择了正确的授权配置文件。

C Refresh O Reset Repeat	Counts 🛓 Export To-																	¥ Filter •	۰۰
Time	Status	Details	Repeat	Identity		Endpoint ID		Endpoint P	Authenticat	Authorization Policy	Authorizati	IP Address		Network Device	Device Port	Identity Group	Posture St	Server	Mdm
×		•		Alice	×	65	×	Endpoint Prof	Authentication	Authorization Policy	Authorization	IP Address		Network Device	Device Port	Identity Group	Posture Statu	Server	Mdm
Feb 15, 2019 02:51:27.163	РМ 😑	ò	0	Alice		F4:8C:50:62:14:68		Microsoft-W	Default >>	Default >> Wireless_Marketing	Marketing	192.168.77.32						manchur-ise	
Feb 15, 2019 02:51:24.837	PM 🖸	• *		Alice	٠	F4:8C:50:62:14:68	*	Morosoft-W	Default >>	Default >> Wireless_Marketing	Marketing		*	WLC5520		Workstation 💠		manchur-ise 🕈	۶

5. 检查WLC上的客户端条目,确保它已分配到正确的VLAN并处于RUN状态。

Clients										Entries 1 - :
Current Filter No	ne [Change_Filter] [Clear_Fil	ter]								
Client MAC Addr	IP Address(Ipv4/Ipv6)	AP Name	WLAN Profile	WLAN SSID	User Name	Protocol	Status	Auth P	ort Slot Id	Tunnel
f4:8c:50:62:14:6b	192.168.77.32	AP4C77.6D9E.6162	office_hq	office_hq	Alice	802.11ac(5 GHz)	Associated	Yes 1	1	No
14:80:50:62:14:60	192.168.77.32	AP4C77.6D9E.6162	omce_nq	emce_hq	Alice	802-11ac(5 GH2)	Associated	Tes 1	1	NO

6. 从WLC CLI,可使用show client dertails 命令检查客户端状态:

Client MAC Address Client Username Client Webauth Username Hostname:	f4:8c:50:62:14:6b Alice N/A
Device Type: AP MAC Address. AP Name. AP radio slot Id. Client State. User Authenticated by	Intel-Device 70:69:5a:51:4e:c0 AP4C77.6D9E.6162 1 Associated RADIUS Server
Client User Group	Alice
Client NAC OOB State Wireless LAN Id Wireless LAN Network Name (SSID) Wireless LAN Profile Name Hotspot (802.11u) Connected For BSSID Channel IP Address Gateway Address Netmask	Access 3 office_hq office_hq Not Supported 765 secs 70:69:5a:51:4e:cd 36 192.168.77.32 192.168.77.1 255.255.255.0
Policy Manager State	RUN
Policy Type Authentication Key Management Encryption Cipher Protected Management Frame Management Frame Protection EAP Type Interface	WPA2 802.1x CCMP-128 (AES) No No PEAP vlan1477 1477

故障排除

### 1. 使用test aaa radius username

password

wlan-id

#### 可测试WLC和ISE之间的RADIUS连接,使用test aaa show radius可显示结果。

test aaa radius username Alice password <removed> wlan-id 2

Radius Test Request	
Wlan-id	2
ApGroup Name	none
····	× 7
Attributes	Values
User-Name	Alice
Called-Station-Id	00-00-00-00-00-00:AndroidAP
Calling-Station-Id	00-11-22-33-44-55
Nas-Port	0x0000001 (1)
Nas-Ip-Address	10.48.71.20
NAS-Identifier	0x6e6f (28271)
Airespace / WLAN-Identifier	0x0000002 (2)
User-Password	cisco!123
Service-Type	0x0000008 (8)
Framed-MTU	0x00000514 (1300)
Nas-Port-Type	0x0000013 (19)
Cisco / Audit-Session-Id	1447300a000003041d5665c
Acct-Session-Id	5c66d541/00:11:22:33:44:55/743

test radius auth request successfully sent. Execute 'test aaa show radius' for response

(Cisco Controller) >test aaa show radius

	-	
10.48.39.128	1	Success

Authentication Response: Result Code: Success

Attributes	Values
User-Name	Alice
State	ReauthSession:1447300a000003041d5665c
Class	CACS:1447300a000003041d5665c:rmanchur-ise/339603379/59

Tunnel-Type Tunnel-Medium-Type Tunnel-Group-Id 0x000000d (13) 0x0000006 (6) 0x00005c5 (1477)

(Cisco Controller) >

- 2. 使用debug client 排除无线客户端连接问题。
- 3. 使用debug aaa all enable对WLC上的身份验证和授权问题进行故障排除。



注意:请仅对debug mac addr使用此命令,以便根据完成调试的MAC地址限制输出。

4. 请参阅ISE实时日志和会话日志,以确定身份验证失败和AD通信问题。

#### 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)。