# 配置9800 WLC和Aruba ClearPass — 访客接入 和FlexConnect

# 目录

简介 先决条件 要求 使用的组件 背景信息 CWA访客企业部署的流量 网络图 配置 配置访客无线接入C9800参数 C9800 — 访客的AAA配置 <u>C9800 — 配置</u>重定向ACL C9800 — 访客WLAN配置文件配置 <u>C9800 — 访客策略配置文件定义</u> <u>C9800 — 策</u>略标记 C9800 - AP加入配置文件 C9800 - Flex配置文件 C9800 — 站点标记 C9800 - RF配置文件 C9800 — 为AP分配标记 配置Aruba CPPM实例 Aruba ClearPass服务器初始配置 申请许可证 服务器主机名 生成CPPPM Web服务器证书(HTTPS) 将C9800 WLC定义为网络设备 访客门户页面和CoA计时器 <u>ClearPass — 访客CWA配置</u> ClearPass端点元数据属性:允许 — 访客 — 互联网 ClearPass重新验证实施策略配置 ClearPass访客门户重定向实施配置文件配置 ClearPass元数据实施配置文件配置 ClearPass访客互联网访问实施策略配置 ClearPass访客在AUP后实施策略配置 ClearPass MAB身份验证服务配置 ClearPass Webauth服务配置 ClearPass - Web登录 验证 — 访客CWA授权 Appendix

# 简介

本文档介绍Catalyst 9800无线LAN控制器(WLC)与Aruba ClearPass的集成,以提供访客无线服务集标识符(SSID),该SSID利用集中式Web身份验证(CWA)在接入点(AP)部署的Flexconnect模式下向无线客户端进行身份验证。

访客无线身份验证由访客门户支持,带有匿名可接受用户策略(AUP)页面,托管在Aruba Clearpass的安全隔离区(DMZ)网段中。

# 先决条件

本指南假设已配置并验证以下组件:

- •所有相关组件均同步到网络时间协议(NTP),并验证其时间是否正确(证书验证需要)
- •运行DNS服务器(访客流量流需要,证书撤销列表(CRL)验证)
- 可操作的DHCP服务器
- •可选的证书颁发机构(CA)(签署CPPM托管访客门户时需要)
- Catalyst 9800 WLC
- Aruba ClearPass服务器(需要平台许可证、访问许可证、板载许可证)
- Vmware ESXi

### 要求

Cisco 建议您了解以下主题:

- C9800部署和新配置模型
- C9800上的Flexconnect交换
- 9800 CWA身份验证(请参阅:<u>https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213920-central-web-authentication-cwa-on-cata.html</u>)

### 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17.3.4c的Cisco Catalyst C9800-L-C
- 思科Catalyst C9130AX
- Aruba ClearPass, 6-8-0-109592和6.8-3补丁
- MS Windows服务器 Active Directory(GP配置为向受管终端自动发布基于计算机的证书)带选项43和选项60的DHCP服务器DNS 服务器NTP服务器对所有组件进行时间同步CA

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。

## 背景信息

该图显示了访客WiFi接入交换的详细信息,然后允许访客用户访问网络:

1.访客用户与远程办公室中的访客Wifi关联。

2.初始RADIUS访问请求由C9800代理到RADIUS服务器。

3.服务器在本地MAC终端数据库中查找提供的访客MAC地址。 如果未找到MAC地址,则服务器会使用MAC身份验证绕行(MAB)配置文件进行响应。此RADIUS响 应包括:

- URL重定向访问控制列表(ACL)
- URL重定向

4.客户端通过IP Learn过程为其分配IP地址。

5. C9800将访客客户端(由其MAC地址标识)转换为"Web Auth Pending"状态。

6.大多数与访客WLAN关联的现代设备操作系统都执行某种强制网络门户检测。 确切的检测机制取决于具体的操作系统实施。客户端操作系统会打开一个弹出窗口(伪浏览器)对 话框,其中页面由C9800重定向到访客门户URL,由RADIUS服务器托管,作为RADIUS访问接受响 应的一部分提供。

7.访客用户接受显示的弹出窗口ClearPass上的条款和条件,在其终端数据库(DB)中为客户端 MAC地址设置一个标志,以指示客户端已完成身份验证,并通过根据路由表选择接口(如果 ClearPass上存在多个接口)来启动RADIUS授权更改(CoA)。

8. WLC将访客客户端转换为"运行"状态,用户无需进一步重定向即可访问Internet。

**注意:**有关Cisco 9800外部、锚点无线控制器与RADIUS和外部托管访客门户的状态流程图 ,请参阅本文的附录部分。

		Guest CWA flow	
CI	V. V		Radius
	[Client Association]     [1] Assoc Request		
	Guest Client Joh	Mile annotation 1	
		(MAB procedure) Start MAD	
		121 Access Request Clession/D=1E1E1E02000000073/8765699 131 Access Accept (redirect URL: redirect ACL Redirect URL: https://copm.fpdn.com/upuest/cpage.name>.shp?session/d=1E1E1E020000003/378768696portal=134a5780	and )
	[4] Assoc Response		
L		MAB complete	
		(interpretent procedure)	
alt	[webauth procedures] [5] Client Device OS performs Portal Detection		
		HTTPH/TTPS session started to dest is intercepted by controller	
		Controller send HTTP TCP SYN ACK and redirects client to Guest Portal URL on CPPR	
	[6] Redirect to Guest Portal URL: https:// <ccpm.lgdn.com>/guest/<page name="">.php?sessionid=1E1E1E020000003/F3F876898/portal=194a5780</page></ccpm.lgdn.com>	(7)	-
		HTTP/HTTPS session started to Guest Portal Server	
		Coest Portal Server Sends HTTP/HTTPS TCP SYN Ack and displays internal login page	
[9]		10) Meteries to goine portai	
	User enters credential and/or clicks on Accept AUP		
	[10] User ser	nds credential HTTPS post (username.password)	
		[11] Validates Cri	
		[Col procedures]	
		[12] CoA Request (Reauthenticate, SessionID=1E1E1E02000003/F3F876869)	
		[13] CoA Ack (Session/D=1E1E1E02000003/3/8768669)	
		[14] Access Request (SessionID=1E1E1E020000003F3F8768690	-
		[15] Access Accept (No redirect URL, Session/D=1E1E1E02000003F3F876869)	
	1	[16] Landing Logout Page	
		client goes to RUM state	
CI	ient V		Radius

访客中心Web身份验证(CWA)状态图



在具有多个分支机构的典型企业部署中,每个分支机构都设置为在访客接受EULA后通过访客门户 提供对访客的安全分段访问。

在此配置示例中,9800 CWA用于访客接入,通过集成到单独的ClearPass实例,该实例专门为网络 安全DMZ中的访客用户部署。

访客必须接受DMZ ClearPass服务器提供的Web同意弹出门户中列出的条款和条件。此配置示例重 点介绍匿名访客访问方法(即,无需访客用户名/密码即可对访客门户进行身份验证)。

与此部署对应的流量如图所示:

1. RADIUS - MAB阶段

2.访客客户端URL重定向到访客门户

3.访客在访客门户上接受EULA后, RADIUS CoA Reauthenticate从CPPM颁发到9800 WLC

4.允许访客访问互联网



#### 网络图

**注意:**出于实验室演示目的,单个/组合的Aruba CPPPM服务器实例用于同时提供访客和公司 SSID网络访问服务器(NAS)功能。最佳实践实施建议独立NAS实例。



## 配置

在此配置示例中,利用C9800上的新配置模式创建必要的配置文件和标记,为企业分支机构提供 dot1x企业访问和CWA访客访问。下图总结了生成的配置:

	Policy Tag: PT_CAN01	WLAN Profile: WP_Guest SSID: Guest Layer 2: Security None Layer 2: MAC Filtering Enabled Authz List: AAA_Authz-CPPM	Policy Profile: PP_Guest Central Switching: Disabled Central Auth: Enabled Central DHCP: Disabled Vlan: guest (21) AAA Policy: Allow AAA Override Enabled AAA Policy: NAC State Enabled AAA Policy: NAC Type RADIUS AAA Policy Accounting List: Guest_Accounting
AP MAC: 1000KJ000KJ000K	AP MAC: x000C.X000C Site Tag: ST_CAN01 Enable Local Site: Off	AP Join Profile: MyApProfile NTP Server: 10.0.10.4 Flex Profile: FP_CAN01 Native Vlan 2 Policy ACL: CAPTIVE_PORTAL_REDIRECT, ACL CWA: Enabled VLAN: 21 (Guest)	
			SGHz Band RF: Typical_Client_Density_rf_5gh
	RF Tag: Branch_RF		2GHz Band RF: Typical_Client_Density_rf_2gh

### 配置访客无线接入C9800参数

C9800 — 访客的AAA配置

**注意:**关于Cisco Bug ID <u>CSCvh03827</u>,请确保定义的身份验证、授权和记帐(AAA)服务器未 进行负载均衡,因为机制依赖WLC中的SessionID持续性进行ClearPass RADIUS交换。

步骤1.将Aruba ClearPass DMZ服务器添加到9800 WLC配置并创建身份验证方法列表。导航到 Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > +Add并输入RADIUS服 务器信息。

Create AAA Radius Server		×
Name*	СРРМ	
Server Address*	10.85.54.98	
PAC Key		
Кеу Туре	Clear Text 🔻	
Key* (i)	••••••	
Confirm Key*		
Auth Port	1812	
Acct Port	1813	
Server Timeout (seconds)	5	
Retry Count	3	
Support for CoA		
Cancel		Apply to Device

步骤2.定义访客的AAA服务器组,并将步骤1中配置的服务器分配给此服务器组。导航到 Configuration > Security > AAA > Servers/Groups > RADIUS > Groups > +Add。

Create AAA Radius Serve	r Group	×
Name*	AAA_Radius_CPPM	
Group Type	RADIUS	
MAC-Delimiter	none 🔹	
MAC-Filtering	none 🔹	
Dead-Time (mins)	5	
Source Interface VLAN ID	1	
Available Servers	Assigned Servers	
	CPPM	
<b>D</b> Cancel	Apply to Device	

步骤3.定义访客访问的授权方法列表并映射在步骤2中创建的服务器组。导航到**配置>安全> AAA >** 

AAA方法列表>授权> +添加。选择Type Network,然后选择步骤2中配置的AAA Server Group。

Quick Setup: AAA Authoriza	tion	×
Method List Name*	AAA_Authz_CPPM	
Type*	network 🔹	
Group Type	group 🔹 🤅	
Fallback to local		
Authenticated		
Available Server Groups	Assigned Server Groups	
radius Idap tacacs+	AAA_Radius_CPPM   <	
Cancel	Apply to Device	

第4步:为访客访问创建记账方法列表并映射在步骤2中创建的服务器组。导航到**配置>安全> AAA > AAA方法列表>记账> +添加**。从下拉菜单中选择**Type Identity**,然后选择**步骤2中配置的AAA Server** Group。

Quick Setup: AAA Accounti	ng		×
Method List Name* Type*	AAA_Accounting_C	CPPM	
Available Server Groups	Assigne	ed Server Groups	
radius Idap tacacs+	> < > «	AAA_Radius_CPPM	<ul> <li></li> &lt;</ul>
Cancel			Apply to Device

### C9800 — 配置重定向ACL

重定向ACL定义必须重定向到访客门户的流量与允许无重定向通过的流量。在这里,ACL拒绝意味 着绕过重定向或通过,而允许意味着重定向到门户。对于每个流量类,在创建访问控制条目 (ACE)并创建与入口和出口流量均匹配的ACE时,您需要考虑流量的方向。

导航到**Configuration > Security > ACL**,然后定义名为**CAPTIVE\_PORTAL\_REDIRECT**的新ACL。 使用以下ACE配置ACL:

- ACE1:允许双向互联网控制消息协议(ICMP)流量绕过重定向,主要用于验证可达性。
- ACE10、ACE30:允许双向的DNS流量流向DNS服务器10.0.10.4,并且不会重定向到门户。触发访客流需要DNS查找和响应拦截。
- ACE70、ACE80、ACE110、ACE120:允许用户通过门户对访客强制网络门户进行HTTP和 HTTPS访问。
- ACE150:所有HTTP流量(UDP端口80)都会被重定向。

Sequence v	Action ~	Source v	Source v Wildcard	Destination ~ IP	Destination ~ Wildcard	Protocol 🖂	Source V Port	Destination ~ Port
1	deny	any		a)ey		icmp		
10	deny	any		10.0.10.4		udp		eq domain
30	deny	10.0.10.4		any		udp	eq domain	
70	deny	any		10.85.54.98		tcp		eq 443
80	deny	10.85.54.98		any		tcp	eq 443	
110	deny	any		10.85.54.98		tcp		eq www
120	deny	10.85.54.98		any		tcp	eq www	
150	permit	any		any		tcp		eq www

#### C9800 — 访客WLAN配置文件配置

步骤1.导航到**配置>标记和配置文件>无线> +添加**。创建新的SSID配置文件WP\_Guest,并广播访客 客户端与之关联的SSID 'Guest'。

Add WLAN × General Security Advanced All Profile Name\* WP\_Guest Radio Policy • Broadcast SSID ENABLED SSID\* Guest 3 WLAN ID\* ENABLED Status

在同一Add WLAN对话框下,导航到Security > Layer 2选项卡。

— 第2层安全模式:无

-MAC 过滤:启用

— 授权列表:AAA\_Authz\_CPPPM(在步骤3下配置,作为AAA配置的一部分)

A	dd WLAN					×
	General	Security	Advanced			
	Layer2	Layer3	AAA			
	Laver 2 Sec	urity Mode		None	Lobby Admin Access	
	MAC Eilterin	,			Fast Transition	Adaptive Enab 🔻
					Over the DS	
	OWE Transit	tion Mode			Reassociation Timeout	20
	Transition M	lode WLAN ID	)*	1-4096		
	Authorizatio	n List*		AAA_Authz_C 🗸 (i)		
	Cancel	]				Apply to Device

### C9800 — 访客策略配置文件定义

在C9800 WLC GUI上,导航到配置>标记和配置文件>策略> +添加。

名称:PP\_Guest

状态:启用

集中交换:禁用

集中身份验证:启用

中央DHCP:禁用

中央协会:禁用

Ad	d Policy	Profile							×
Ge	eneral	Access Policies	QOS and AVC	Mobility	Ad	vanced			
		A Configuri	ng in enabled state will re	esult in loss of	conn	ectivity for clients associated with	this profile	9.	
	Name*		PP_Guest			WLAN Switching Policy			
	Descrip	tion	Policy Profile for G	iuest		Central Switching		DISABLED	
	Status		ENABLED			Central Authentication	ENAB		
	Passive	Client	DISABLED			Central DHCP		DISABLED	
	Encrypt	ed Traffic Analytics	DISABLED			Central Association		DISABLED	
	CTS P	olicy				Flex NAT/PAT		DISABLED	
	Inline Ta	agging							
	SGACL	Enforcement							
	Default	SGT	2-65519						

Cancel

Apply to Device

Add Polic	cy Profile						×
	A Configur	ing in enabled state wil	l result in loss o	of conr	nectivity for clients associated with t	his profile.	
General	Access Policies	QOS and AVC	Mobility	Ad	vanced		
Name	*	PP_Guest			WLAN Switching Policy		
Descr	iption	Profile for Branch	Guest		Central Switching	DISABLED	
Status	3	DISABLED			Central Authentication	ENABLED	
Passiv	ve Client	DISABLED			Central DHCP	DISABLED	
Encry	oted Traffic Analytics	DISABLED			Central Association	DISABLED	
CTS	Policy				Flex NAT/PAT	DISABLED	
Inline	Tagging						
SGAC	L Enforcement						
Defau	It SGT	2-65519					
Cance	el					Apply to Device	,

导航到同一Add Policy Profile对话框中的Access Policies选项卡。

- RADIUS分析:启用

- VLAN/VLAN组:210(即,VLAN 210是每个分支机构位置的访客本地VLAN)

**注意:**在9800 WLC上的VLAN下,必须在VLAN/VLAN组类型VLAN编号中定义Flex的访客 VLAN。

已知缺陷:如果在WLC下和Flex配置文件中定义了相同的Flex访客VLAN,则Cisco bug ID <u>CSCvn48234</u>会导致不广播SSID。

Add Policy Profile			
A Configuring in en	nabled state will result in loss of connectivity for o	clients associated w	with this profile.
General Access Policies QOS	S and AVC Mobility Advanced		
RADIUS Profiling		WLAN ACL	
HTTP TLV Caching		IPv4 ACL	Search or Select
DHCP TLV Caching		IPv6 ACL	Search or Select 🚽
WLAN Local Profiling		URL Filters	
Global State of Device Classification	í	Pre Auth	Search or Select 🗸
Local Subscriber Policy Name	Search or Select	Post Auth	Search or Select
VLAN			
VLAN/VLAN Group	210 🔹		
Multicast VLAN	Enter Multicast VLAN		

Cancel

在同一Add Policy Profile对话框中,导航到Advanced选项卡。

— 允许AAA覆盖:启用

- NAC状态:启用

- NAC类型: RADIUS

— 记帐列表:AAA\_Accounting\_CPPPM(在步骤4中定义。作为AAA配置的一部分)

#### Add Policy Profile

A Configuring in enabled state will result in loss of connectivity for clients associated with this profile.				
General Access Polici	es QOS and AVC	Mobility	Advanced	
WLAN Timeout			Fabric Profile     Search or Select	
Session Timeout (sec)	1800		mDNS Service Search or Select	
Idle Timeout (sec)	300		Hotspot Server Search or Select 🔹	
Idle Threshold (bytes)	0		User Defined (Private) Network	
Client Exclusion Timeout (	sec) 🗹 <u>60</u>		Status	
Guest LAN Session Timeo	ut 📋		Drop Unicast	
DHCP			Umbrella	
IPv4 DHCP Required DHCP Server IP Address			Umbrella Parameter Map	
how more >>>			Flex DHCP Option ENABLED	
AAA Policy			DNS Traffic Redirect	
Allow AAA Override			WLAN Flex Policy	
NAC State			VLAN Central Switching	
NAC Type	RADIUS	•	Split MAC ACL Search or Select	
Policy Name	default-aaa-policy	/ × •	Air Time Fairness Policies	
Accounting List	AAA_Accounting_	<b>. ( , ( ) x</b>	2.4 GHz Policy Search or Select	

**注意:**要启用C9800 WLC以接受RADIUS CoA消息,需要"网络准入控制(NAC)状态 — 启用 "。

### C9800 — 策略标记

在C9800 GUI上,导航到配置>标记和配置文件>标记>策略> +添加。

-姓名 :PT\_CAN01

-描述:CAN01分支站点的策略标签

在同一个对话框Add Policy Tag中,在WLAN-POLICY MAPS下,单击+Add,并将之前创建的 WLAN配置文件映射到策略配置文件: ×

### - WLAN配置文件: WP\_Guest

### — 策略配置文件:PP\_Guest

Add Policy Tag			×
Name*	PT_CAN01		
Description	Policy Tag for CAN01		
VUAN-POLICY	/ Maps: 0		
+ Add × Dele	ete		
WLAN Profile		V Policy Profile	₩.
	10 🔻 items per page		No items to display
Map WLAN and Pol	icy		
WLAN Profile*	WP_Guest	Policy Profile*	PP_Guest
	×	<b>~</b>	
RLAN-POLICY	Maps: 0		
Cancel			Apply to Device

### C9800 - AP加入配置文件

在C9800 WLC GUI上,导航到**配置>标记和配置文件> AP加入> +添加**。

-姓名 :Branch\_AP\_Profile

-NTP 服务器:10.0.10.4(请参阅实验拓扑图)。 这是Branch中的AP用于同步的NTP服务器。

Add AP J	oin Profile								×
General	Client	CAPWAP	AP	Management	Sec	urity	ICap	QoS	
Name*		Branch	_AP_Pro	ofile		Office	Extend A	P Configuratio	on
Descrip	otion	Branch	AP Join	Profile		Local	Access	<ul> <li></li> </ul>	
LED St	ate	$\checkmark$				Link Er	ncryption	~	
LAG M	ode					Rogue	Detection		
NTP Se	erver	10.0.1	0.4						
GAS A	P Rate Limit								
Appho	st								
Cance									Apply to Device

### C9800 - Flex配置文件

配置文件和标签是模块化的,可以重复用于多个站点。

对于FlexConnect部署,如果所有分支机构站点使用相同的VLAN ID,您可以重复使用相同的Flex配置文件。

步骤1.在C9800 WLC GUI上,导航到**配置>标记和配置文件> Flex > +Add**。

-姓名 :FP\_Branch

— 本征VLAN ID:10(仅在您有一个非默认本地VLAN且要有AP管理接口时需要)

Add Flex Profile				×
General Local Authentica	tion Policy ACL VI	AN Umbrella		
Name*	FP_Branch	Fallback Radio Shut		
Description	Branch Flex Profile	Flex Resilient		
Native VLAN ID	10	ARP Caching		
HTTP Proxy Port	0	Efficient Image Upgrade		
HTTP-Proxy IP Address	0.0.0.0	OfficeExtend AP		
CTS Policy		Join Minimum Latency		
Inline Tagging		IP Overlap		
SGACL Enforcement		mDNS Flex Profile	Search or Select	
CTS Profile Name	default-sxp-profile x			
Cancel				Apply to Device

在同一添加Flex Profile对话框中,导航到策略ACL选项卡,然后单击+添加。

-ACL 名称:CAPTIVE\_PORTAL\_REDIRECT

— 集中Web身份验证:启用

在Flexconnect部署中,当重定向发生在AP而不是C9800上时,预期每个托管AP都将在本地下载重定向ACL。

Add Flex P	rofile				×
General	Local Authentication	Policy ACL VLAN	Umbrella		
+ Add	× Delete				
ACL Nam	ne v.	Central Web Auth 🗸	Pre Auth URL 🛛 💉	ACL Name*	CAPTIVE_PORTAL_F
H 4	0 ► ► 10 v ite	ms per page N	lo items to display	Central Web Auth	
				Pre Auth URL Filter	Search or Select
				✓ Save	Cancel
Cancel					Apply to Device

在Add Flex Profile对话框中,导航到VLAN选项卡,然后单击+Add(请参见实验拓扑图)。

### -VLAN 名称:访客

#### -VLAN ID:210

Add Flex P	Profile				×
General	Local Authentication Policy AC		Imbrella		
+ Add	× Delete				
VLAN	Name v ID v ACL Name	×.			
data	2		VLAN Name*	guest	
H	1 ► ► 10 ¥ items per pag	е	VLAN Id*	210	
		1 - 1 of 1 items	ACL Name	Select ACL	
			✓ Save	ວ Cancel	
	_				
Cancel					Apply to Device

### C9800 — 站点标记

在9800 WLC GUI上,导航到配置>标签和配置文件>标签>站点>添加。

注意:为每个需要支持两个无线SSID的远程站点创建唯一的站点标记(如所述)。

地理位置、站点标签和Flex Profile配置之间有1-1映射。

FlexConnect站点必须具有与其关联的FlexConnect配置文件。每个flex connect站点最多可以有 100个接入点。

-姓名 :ST\_CAN01

- AP加入配置文件: Branch\_AP\_Profile
- Flex配置文件: FP\_Branch
- 启用本地站点:禁用

Add Site Tag	
Name*	ST_CAN01
Description	Site Tag for Branch CA
AP Join Profile	Branch_AP_Profile
Flex Profile	FP_Branch
Fabric Control Plane Name	•
Enable Local Site	
Cancel	

### C9800 - RF配置文件

在9800 WLC GUI上,导航到Configuration > Tags & Profiles > Tags > RF > Add。

-姓名:Branch\_RF

- 5 GHz频段射频(RF)配置文件: Typical\_Client\_Density\_5gh(系统定义的选项)

- 2.4 GHz频段RF配置文件:Typical\_Client\_Density\_2gh(系统定义的选项)

Add RF Tag		×
Name*	Branch_RF	
Description	Typical Branch RF	
5 GHz Band RF Profile	Client_Density_rf_5gh	
2.4 GHz Band RF Profile	Typical_Client_Densi	
Cancel		Apply to Device

有两个选项可用于将定义的标记分配到部署中的单个AP:

— 基于AP名称的分配,利用regex规则匹配AP名称字段中的模式(**Configure > Tags & Profiles >** Tags > AP > Filter)

— 基于AP以太网MAC地址的分配(配置>标记和配置文件>标记> AP >静态)

在使用DNA Center的生产部署中,强烈建议使用DNAC和AP PNP工作流程,或使用9800中提供的 静态批量逗号分隔值(CSV)上传方法,以避免手动分配每个AP。导航到Configure > Tags & Profiles > Tags > AP > Static > Add(注意Upload File选项)。

- AP MAC地址: < AP\_ETHERNET\_MAC>

— 策略标记名称:PT\_CAN01

— 站点标记名称:ST\_CAN01

- RF标记名称: Branch\_RF

**注意:**从Cisco IOS®-XE 17.3.4c开始,每个控制器最多有1,000个正则表达式规则限制。如果 部署中的站点数量超过此数量,则必须使用静态的每MAC分配。

Associate Tags to	AP	
AP MAC Address*	aaaa.bbbb.cccc	
Policy Tag Name	PT_CAN01	•
Site Tag Name	ST_CAN01	•
RF Tag Name	Branch_RF	•
Cancel		

**注意:**或者,要利用基于AP名称正则表达式的标签分配方法,请导航到**配置>标签和配置文件** >标签> AP >过滤器>添加。

-姓名:BR\_CAN01

- AP名称正则表达式:BR-CAN01-.(7)(此规则与组织中采用的AP名称约定匹配。在本示例中,标签 被分配给具有"AP名称"字段的AP,该字段包含"BR\_CAN01 — ",后跟任意七个字符。)

-优先级:1

— 策略标记名称:PT\_CAN01(如定义)

— 站点标记名称:ST\_CAN01

- RF标记名称: Branch\_RF

A Rule "BR-CAN01" has this priority. Assigning it to the current rule will swap the priorites.



### 配置Aruba CPPM实例

有关基于生产/最佳实践的Aruba CPPM配置,请联系您当地的HPE Aruba SE资源。

#### Aruba ClearPass服务器初始配置

Aruba ClearPass使用开放式虚拟化格式(OVF)模板部署在ESXi <>服务器上,该服务器分配以下资 源:

- •两个保留的虚拟CPU
- 6 GB RAM
- •80 GB磁盘(必须在初始虚拟机部署后手动添加,然后才能启动计算机)

#### 申请许可证

通过以下方式应用平台许可证:**管理(Administration)>服务器管理器(Server Manager)>许可** (Licensing)。添加**平台、访问**和板载**许可证**。

#### 服务器主机名

导航到管理>服务器管理器>服务器配置,然后选择新调配的CPPM服务器。

-主机名:cppm

- FQDN:cppm.example.com
- 验证管理端口IP编址和DNS

×

Administration » Server Manager » Server Configuration - cppm

#### Server Configuration - cppm (10.85.54.98)

System Services Control	Service	Parameters	System Monitoring	Network	FIPS			
Hostname:		cppm						
FQDN:		cppm.example	.com					
Policy Manager Zone:		default	~				Manage F	
Enable Performance Monitoring	Display:	Enable this	server for performan	ice monitoring	display			
Insight Setting:		🗹 Enable Insi	ght 🔽 E	nable as Insigh	nt Master	Current Master:cppm(10.85.54.98)		
Enable Ingress Events Process	ing:	🗌 Enable Ing	ress Events processir	g on this serve	er			
Master Server in Zone:		Primary maste	er v					
Span Port:		None	~					
			IP	v4	_	IPv6	Action	
	IP Add	IP Address Subnet Mask Default Gateway		85.54.98				
Management Port	Subnet			5.255.255.224	· .	Cont		
	Defaul			.85.54.97				
	IP Add	ress			_			
Data/External Port	Subnet	Subnet Mask					Configure	
	Defaul	Default Gateway						
	Primar	у	10	.85.54.122				
DNS Settings	Second	lary					Configure	
ono octango	Tertian	y					oomiguro	
	DNS C	aching	Dis	abled				

### 生成CPPPM Web服务器证书(HTTPS)

当ClearPass Guest Portal页面通过HTTPS呈现给连接到分支中的访客Wifi的访客客户端时,使用此 证书。

步骤1.上传CA发布链证书。

导航到管理>证书>信任列表>添加。

-使用率:启用其他

Subject DN:	
Issuer DN:	
Issue Date/Time:	Dec 23, 2020 16:55:10 EST
Expiry Date/Time:	Dec 24, 2025 17:05:10 EST
Validity Status:	Valid
Signature Algorithm:	SHA256WithRSAEncryption
Public Key Format:	X.509
Serial Number:	86452691282006080280068723651711271611
Enabled:	true
Usage:	🗹 EAP 🗹 RadSec 🗹 Database 🗹 Others
	Update Disable Export Close

步骤2.创建证书签名请求。

导航到管理>证书>证书存储>服务器证书>用法:HTTPS服务器证书。

- 单击Create Certificate Signing Request
- 公用名:CPPM
- 组织: cppm.example.com

确保填充SAN字段(SAN中必须存在通用名称,IP和其他FQDN必须根据需要存在)。格式为 DNS:**<fqdn1>、DNS:<fqdn2>、IP<ip1>**。

### **Create Certificate Signing Request**

Common Name (CN):	cppm
Organization (O):	Cisco
Organizational Unit (OU):	Engineering
Location (L):	Toronto
State (ST):	ON
Country (C):	CA
Subject Alternate Name (SAN):	DNS:cppm.example.com
Private Key Password:	•••••
Verify Private Key Password:	•••••
Private Key Type:	2048-bit RSA ~
Digest Algorithm:	SHA-512 ~
	Submit Cancel

第3步:在所选的CA中,签署新生成的CPPM HTTPS服务CSR。

步骤4.导航到证书模板> Web服务器>导入证书。

— 证书类型:服务器证书

-使用率:HTTP服务器证书

-证书文件:浏览并选择CA签名的CPPM HTTPS服务证书

Import Certificate		8
Certificate Type:	Server Certificate	
Server:	cppm v	
Usage:	HTTPS Server Certificate	
Upload Method:	Upload Certificate and Use Saved Private Key	
Certificate File:	Browse No file selected.	
	Import	

### 将C9800 WLC定义为网络设备

导航到Configuration > Network > Devices > Add。

8

-姓名:WLC\_9800\_Branch

- IP或子网地址:10.85.54.99(请参阅实验拓扑图)

- RADIUS共享思科: <WLC RADIUS密码>

-供应商名称: 思科

— 启用RADIUS动态授权:1700

Add Device						
Device SNMP Read Settings	SNMP Write Settings	CLI Settings	OnConnect Enfor	cement	Attributes	
Name:	WLC_9800_Branch					
IP or Subnet Address:	10.85.54.99	(e.	g., 192.168.1.10 or	192.168.	1.1/24 or 192.	168.1.1-20)
Description:	Cisco 9800 WLC f	or Branch Gue	st <u>Wifi</u>			
			11.			
RADIUS Shared Secret:			Verify:			
TACACS+ Shared Secret:			Verify:			
Vendor Name:	Cisco	Ŧ				
Enable RADIUS Dynamic Authorizati	on: 🗹 Port: 1700					
Enable RadSec:						

Add Cancel	Add	Cancel
------------	-----	--------

### 访客门户页面和CoA计时器

在整个配置中设置正确的计时器值非常重要。如果未调整计时器,您可能会遇到客户端未处于"运行 状态"的循环Web门户重定向。 要注意的计时器:

- 门户Web登录计时器:此计时器将延迟重定向页面,然后才允许访问访客门户页面通知 CPPPM服务状态转换、注册终端自定义属性"Allow-Guest-Internet"值,并触发从CPPPM到 WLC的CoA进程。导航到Guest > Configuration > Pages > Web Logins。
   选择访客门户名称:实验室匿名访客注册(此访客门户页面配置如图所示)
   单击Edit
  - 登录延迟:6秒

\* Login Delay: 6 C The time in seconds to delay while displaying the login message.

ClearPass CoA延迟计时器:这会延迟CoA消息从ClearPass发送到WLC。在CoA确认(ACK)从WLC返回之前,CPPM在内部成功转换客户端终端状态时需要此步骤。实验室测试显示来自WLC的亚毫秒响应时间,如果CPPM尚未完成终端属性的更新,则来自WLC的新RADIUS会话将与未经身份验证的MAB服务实施策略相匹配,并且客户端将再次获得重定向页面。导航到CPPM > Administration > Server Manager > Server Configuration,然后选择CPPM Server > Service Parameters。

- RADIUS动态授权(DM/CoA)延迟 — 设置为6秒

aruba	ClearPass Policy Manager					
Dashboard O Monitoring O Configuration O Administration O	Administration » Server Manager » Server Configuration - cppm Server Configuration - cppm (10.85.54.98)					
	System         Services Control         Service Parameters         System Monitoring         Network         FIPS           Select Service:         Async network services					
Cog Configuration      Conf	Parameter Name Ingress Event Batch Processing Interval Command Control	Parameter Value     30	seconds			
	RADIUS Dynamic Authorization (DM/CoA) Delay Enable SNMP Bounce Action	6 s FALSE v	seconds			
Guturate Solid     For Trust List    }     Revocation Lists     Guturate Solid     Agents and Software Updates     Support	Post Auth Number of request processing threads Lazy handler polling frequency Eager handler polling frequency Connection Timeout Palo Alto User Identification Timeout	20 t 5 r 30 s 10 s	threads minutes seconds seconds minutes			

### ClearPass — 访客CWA配置

ClearPass-side CWA配置包括(3)服务点/阶段:

ClearPass组件	服务类型	目的
1.策略管理器	服务:MAC 验证	如果自定义属性Allow-Guest-In = TRUE,则允许它进入网络。 ,触发Redirect和COA: <b>重新验</b> 语
2.访客	Web登录	显示匿名登录AUP页面。 Post-auth set custom attribute <b>Allow-Guest-Internet</b> = TRUE。
3.策略管理器	服务:基于Web的身份验证	将终端更新为 <b>已知</b> 设置自定义 <b>属性Allow-Guest-In</b> = TRUE <b>COA:重新验证</b>

### ClearPass端点元数据属性:允许 — 访客 — 互联网

创建类型为Boolean的元数据属性,以在客户端在"Webauth Pending"和"Run"状态之间转换时跟踪 访客终端状态:

— 连接到wifi的新访客将默认元数据属性设置为Allow-Guest-Internet=false。基于此属性,客户端身 份验证通过MAB服务

— 当您点击AUP Accept按钮时,访客客户端的元数据属性更新为Allow-Guest-Internet=true。随后 基于此属性设置为True的MAB允许对互联网进行非重定向访问

导航到ClearPass > Configuration > Endpoints,从列表中选择任何终端,点击Attributes选项卡,使 用值false添加Allow-Guest-Internet并Save。

**注意:**您也可以编辑同一端点,并在之后删除此属性 — 此步骤仅创建可在策略中使用的端点 元数据数据库中的字段。

Ed	it Endpoint				8
	Endpoint Attributes				
	Enapoint Attributes				
	Attribute		Value		
1	Allow-Guest-Internet	=	false	۳)	Ť
2	. Click to add				

### ClearPass重新验证实施策略配置

创建在客户端接受Guest Portal页面上的AUP后立即分配给访客客户端的强制配置文件。

导航到ClearPass > Configuration > Profiles > Add。

— 模板:RADIUS动态授权

-姓名 :Cisco\_WLC\_Guest\_COA

Configuration » Enforcement » Profiles » Add Enforcement Profile

### **Enforcement Profiles**

Profile	Attributes	Summary
Template:		RADIUS Dynamic Authorization
Name:		Cisco_WLC_Guest_COA
Description	1:	
Type:		RADIUS_CoA
Action:		Accept O Reject O Drop
Device Gro	oup List:	Remove
		View Details
		Modify
		Select v
Radius:IETI	=	Calling-Station-Id %{Radius:IETF:Calling-S

RadiustietF	Calling-Station-Id	%{Radius:1ETF:Calling-Station
Radius:思科	Cisco-AVPair	subscriber:command=reauther e
Radius:思科	Cisco-AVPair	%{Radius:Cisco:Cisco- AVPair:subscriber:audit-sessic
Radius:思科	Cisco-AVPair	subscriber:reauthenticate-type type=last

### ClearPass访客门户重定向实施配置文件配置

在CPPM终端数据库中找不到MAC地址且"Allow-Guest-Internet"设置为"**true"**时,创建在初始MAB阶 段应用于访客的强制配置文件。

这会导致9800 WLC将访客客户端重定向到CPPM访客门户进行外部身份验证。

#### 导航到ClearPass > Enforcement > Profiles > Add。

-姓名 :Cisco\_Portal\_Redirect

-类型:RADIUS

-动作:Accept(接受)

Configuration » Enforcement » Profiles » Add Enforcement Profile

### **Enforcement Profiles**

Profile Attrib	Ites Summary
Template:	Aruba RADIUS Enforcement
Name:	Cisco_Portal_Redirect
Description:	
Гуре:	RADIUS
Action:	💿 Accept 🔘 Reject 🔘 Drop
Device Group List:	Remove       View Details       Modify

ClearPass重定向实施配置文件

### 在同一对话框的**属性**选项卡下,根据此映像配置两个属性:

Enforcement Profiles - Cisco\_Portal\_Redirect

_					
	Туре	Name		Value	
1.	Radius:Cisco	Cisco-AVPair	-	url-redirect-acl=CAPTIVE_PORTAL_REDIRECT	6
2.	Radius:Cisco	Cisco-AVPair	=	url-redirect=https://cppm.example.com/guest/iaccept.php?cmd- login&mac=%{Connection:Client-Mac-Address-Hyphen}&switchip=% {Radius:IETF:NAS-IP-Address}	8

ClearPass重定向配置文件属性

url-redirect-acl属性设置为CAPTIVE-PORTAL-REDIRECT,这是在C9800上创建的ACL的名称。

**注意:**RADIUS消息中只传递对ACL的引用,而不传递ACL内容。在9800 WLC上创建的 ACL的名称必须与此RADIUS属性的值完全匹配,这一点很重要。

- •托管访客门户的目标URL,<u>https://cppm.example.com/guest/iaccept.php</u>
- •访客客户端MAC,宏%{Connection:Client-Mac-Address-Hyphen}
- •身份验证器IP(9800 WLC触发重定向),宏%{Radius:IETF:NAS-IP-Address}
- cmd-login操作

导航到**CPPM > Guest > Configuration > Pages > Web Logins > Edit**时,会看到ClearPass Guest Web Login Page的URL。

在本例中,CPPM中的访客门户页面名称定义为iaccept。

**注意**:访客门户页面的配置步骤如中所述。

aruba		(
💱 Guest 🔹 📀	Home » Configuration	n » Pages » Web Logins
il Devices 🔹 💿	Web Login (La	b Anonynous Guest Regist
📳 Onboard 🔹 💿		
🔨 Configuration 📀	Use this form to make	e changes to the Web Login <b>Lab Anon</b> j
- 🍣 Authentication		
🗄 🎯 Content Manager	* Name:	Lab Anonynous Guest Registration
– 🚝 Guest Manager	Nume.	Enter a name for this web login page.
🗄 靲 Hotspot Manager		iaccept
🚽 😩 Pages	Page Name:	Enter a page name for this web login.
— 🌆 Fields		The web login will be accessible from /guest/
- 🛅 Forms		
List Views	Description:	
Self-Registrations		Comments or descriptive text about the web I
- Keb Logins	* Vendor Settings	Aruba Networks
Web Pages	venuor Settings.	Select a predefined group of settings suitable

注意:对于思科设备,通常使用audit\_session\_id,但其他供应商不支持该功能。

#### ClearPass元数据实施配置文件配置

配置实施配置文件,以更新用于CPPM跟踪状态转换的终端元数据属性。

此配置文件应用于终端数据库中的访客客户端MAC地址条目,并将"**Allow-Guest-Internet**"参数设置为"**true**"。

导航到ClearPass > Enforcement > Profiles > Add。

— 模板: ClearPass实体更新实施

-类型:Post\_Authentication

### **Enforcement Profiles**

Profile	Attributes	Summary
Template:		ClearPass Entity Update Enforcement
Name:		Make-Cisco-Guest-Valid
Descriptior	1:	
Туре:		Post_Authentication
Action:		Accept O Reject O Drop
Device Gro	oup List:	Remove       View Details       Modify

在同一对话框中,选择Attributes选项卡。

-类型:终端

-姓名 :允许 — 访客 — 互联网

**注意:**要将此名称显示在下拉菜单中,您必须手动为至少一个终端定义此字段,如步骤中所述 。

### -价值:true

Co	nfiguration » Enforcement » Profiles » Add Enfor	cement Profile		
Er	nforcement Profiles			
P	rofile Attributes Summary			
	Туре	Name		Value
1.	Type Endpoint	Name Allow-Guest-Internet	=	Value true

#### ClearPass访客互联网访问实施策略配置

#### 导航到ClearPass > Enforcement > Policies > Add。

-姓名:WLC思科访客允许

- 实施类型:RADIUS
- -缺省配置文件:Cisco\_Portal\_Redirect

Configuration » Enforcement » Policies » Add

Enforceme	Enforcement Policies								
Enforcement	Rules	Summary							
Name:		WLC Cisco Guest Allow							
Description:									
Enforcement Typ	e:	● RADIUS → TACACS+ ○ WEBAUTH (SNMP/Agent/CLI/CoA) ○ Application ○ Event							
Default Profile:		Cisco_Portal_Redirect View Details Modify							

在同一对话框中,导航到Rules选项卡,然后单击Add Rule。

- -类型:终端
- -姓名 :允许 访客 互联网
- 操作员:等于
- 值为True

— 配置文件名称/选择添加: [RADIUS] [允许访问配置文件]

Rules Editor				
		Conditions		
Match ALL of the following	conditions:			
Туре	Name	Operator	Value	
1. Endpoint	Allow-Guest-Interne	t 💌 EQUALS	▼ true	<b>v</b> 🖱 ti
2. Click to add				
		Enforcement Profiles		
Profile Names:	[RADIUS] [Allow Access Profile] Move Ren	Up † Down ↓		
	Select to Add	~		
				Save Cancel

ClearPass访客在AUP后实施策略配置

导航到ClearPass > Enforcement > Policies > Add。

-姓名:Cisco WLC Webauth实施策略

- 实施类型:WEBAUTH(SNMP/Agent/CLI/CoA)
- -缺省配置文件:[RADIUS\_CoA] Cisco\_Reauthenticate\_Session

#### **Enforcement Policies**

Enforcement	Rules	Summary
Name:		Cisco WLC Webauth Enforcement Policy
Description:		
Enforcement Type:		○ RADIUS ○ TACACS+
Default Profile:		[RADIUS_CoA] Cisco_Reautl > View Details Modify

#### 在同一对话框中,导航到**规则>添加**。

- -条件:身份验证
- -姓名:状态
- 操作员:等于

-价值:用户

- 配置文件名称:<add each>:
- [身份验证后] [更新终端已知]
- [Post Authentication] [Make-Cisco-Guest-Valid]
- [RADIUS\_CoA] [Cisco\_WLC\_Guest\_COA]

Rules Editor				· · · · · · · · · · · · · · · · · · ·
		Conditions		
Match ALL of the following conditions:				
Туре	Name	Operator	Value	
1. Authentication	Status	EQUALS	User	Ba #
2. Click to add				
		Enforcement Profiles		
Profile Names: [Post Auther	tication] [Update Endpoint Known]			
[Post Auther	tication] Make-Cisco-Guest-Valid	Move Up ↑		
[RADIUS_Co	A] Cisco_WLC_Guest_COA	Move Down ↓		
		Remove		
Select to A	dd	~		
				Save

**注意:**如果您遇到具有连续访客门户重定向伪浏览器弹出窗口的方案,则表明CPPM计时器需 要调整或RADIUS CoA消息在CPPM和9800 WLC之间无法正确交换。检验这些站点。

— 导航到**CPPPM > Monitoring > Live Monitoring > Access Tracker**,并确保RADIUS日志条目包含 RADIUS CoA详细信息。

— 在**9800 WLC**上,导航到**故障排除>数据包捕获**,在预期接收RADIUS CoA数据包的接口上启用 pcap,并验证是否从CPPM收到RADIUS CoA消息。

#### ClearPass MAB身份验证服务配置

服务在属性值(AV)对Radius: 思科 | CiscoAVPair | cisco-wlan-ssid

导航到ClearPass > Configuration > Services > Add。

"**服务"**选项卡:

-姓名:访客门户 — Mac身份验证

-类型 :MAC 验证

-更多选项:选择授权,配置文件终端

添加匹配规则:

-类型:RADIUS: 思科

-姓名:Cisco-AVPair

— 操作员:等于

-价值:cisco-wlan-ssid=Guest(匹配配置的访客SSID名称)

注意:"Guest"是通过9800 WLC广播的访客SSID的名称。

Configuration » Services » Add Services Authentication Authorization Roles Enforcement Profiler Summary Service Type: MAC Authentication GuestPortal - Mac Auth Name Description: MAC-based Authentication Service Monitor Mode: Enable to monitor network access without enforcement 🗹 Authorization 🗌 Audit End-hosts 🗹 Profile Endpoints 🚺 Accounting Proxy More Options: Service Rule Matches O ANY or 
 ALL of the following conditions: Туре Name Operator Value 1. Radius:IETF NAS-Port-Type BELONGS\_TO Ethernet (15), Wireless-802.11 (19) Radius:IETF 66 ÷ 2. BELONGS TO Service-Type Login-User (1), Call-Check (10) 3. Connection Client-Mac-Address EQUALS %{Radius:IETF:User-Name} 6 ŝ Cisco-AVPai EQUALS 4. Radius:Cisco cisco-wlan-ssid=Guest 6 8

在同一对话框中,选择Authentication选项卡。

— 身份验证方法:删除[MAC AUTH],添加[允许所有MAC AUTH]

— 身份验证源:[终端存储库][本地SQL数据库],[访客用户存储库][本地SQL数据库]

aruba	ClearPass Policy Manager					
Dashboard O	Configuration » Services >	> Edit - GuestPortal - Mac Auth				
Monitoring O	Services - Guest	Portal - Mac Auth				
Configuration 📀	Summary Service	Authentication Authorization	Roles	Enforcement	Profiler	
<ul> <li>         → Service Templates &amp; Wizards         → Services         Authentication         → Methods         → Sources         → Single Sign-On (SSO)         → Local Users      </li> </ul>	Authentication Methods:	[Allow All MAC AUTH]		Move Up ↑ Move Down ↓ Remove View Details Modify	] ] ]	
-☆ Endpoints         -☆ Static Host Lists         -☆ Roles         -☆ Role Mappings         -☆ Posture         -☆ Policies         -☆ Profiles	Authentication Sources:	[Endpoints Repository] [Local SQL D] [Guest User Repository] [Local SQL I Select to Add	B] DB]	Move Up ↑ Move Down ↓ Remove View Details Modify		
Operation of the second s	Strip Username Rules:	Enable to specify a comma-sep	parated lis	st of rules to strip	o username prefixes or suffixes	

### 在同一对话框中,选择Enforcement选项卡。

#### — 实施策略:WLC思科访客允许

Configuration » Services » Add

#### Services

Service	Authentication	Roles	Enforcement	Summary				
Use Cached	Results:	🗌 Use cach	ed Roles and Pos	ture attributes f	from prev	vious session	IS	
Enforcemen	t Policy:	WLC Cisco	Guest Allow	~	Modify ]			
						Enforce	ment Policy	Details
Description	:	MAB Enfor	cement Redirect					
Default Prof	file:	Cisco_Port	al_Redirect					
Rules Evaluation Algorithm:		first-applic	able					
Conc	litions							Enforcement Profiles
1. (Endpoint:Allow-Guest-Internet EQUALS true)								[Allow Access Profile]

### 在同一对话框中,选择Enforcement选项卡。

Configuration » Services » Add

### Services

Service	Authentication	Authorization	Roles	Enforceme	nt	Profiler	Summary	
Endpoint Classification:		Select the classifica	ation(s) af	ter which an	Rei	on must be	triggered -	
RADIUS Co.	A Action:	Cisco_Reauthentica	te_Sessio	า	~	View Deta	ails Modify	

### ClearPass Webauth服务配置

### 导航到ClearPass > Enforcement > Policies > Add。

-姓名 :Guest\_Portal\_Webauth

### -类型:基于Web的身份验证

Configuration » Services » Add

### Services

Ser	vice	Authentication	Roles	Enforcement	Summary		
Type:	:		Web-based	d Authentication		~	
Name	e:		Guest				
Desci	ription	:					
Monit	tor Mod	de:	Enable to monitor network access without enforcement				
More	Optior	ns:	🗌 Authoriz	ation 🗌 Posture	Compliance		
						S	
Match	nes 🔿	ANY or 🧿 ALL	of the follo	wing conditions:			
	Туре			Na	ame		
1.	Host			Ch	neckType		
2.	Click	to add					

在同一对话框中,在Enforcement选项卡下,Enforcement Policy:Cisco WLC Webauth实施策略。

Configurati	Configuration » Services » Add						
Service	s						
Service	Authentication	Roles	Enforcement	Summary			
Use Cacheo	d Results:	Use cach	ed Roles and Po	sture attribute	s from previo	ous sessions	
Enforceme	nt Policy:	Cisco WLC	Webauth Enforce	ment Policy	✓ Modify		Add New Enforcement Poli
						Enforcement Policy Details	5
Description	6						
Default Pro	file:	Cisco_Rea	uthenticate_Ses	sion			
Rules Evalu	uation Algorithm:	first-applic	cable				
Con	ditions						Enforcement Profiles
1. (At	thentication:Stat	us EQUALS	User)				[Update Endpoint Known], Make-Cisco-Guest-Valid, Cisco_Reauthenticate_Session

### ClearPass - Web登录

对于Anonymous AUP Guest Portal页面,请使用没有密码字段的单个用户名。

使用的用户名必须定义/设置以下字段:

username\_auth |用户名身份验证: | 1

要设置用户的"username\_auth"字段,必须首先在"edit user"表单中显示该字段。导航到ClearPass >

### Guest > Configuration > Pages > Forms,然后选择create\_user表单。

aruba	Cle	arPass Guest			
🔮 Guest 🛛 0	Home » Configuration » Pages » Forms				
👔 Devices 🔹 📀	Customize Forms				
🕞 Onboard 🔹 📀	Use this list view to customize the forms within the application.				
- 🍣 Authentication	△ Name	Title			
Content Manager	change_expiration Change the expiration time of a single guest account.	Change Expiration			
Public Files	create_multi Create multiple guest accounts.	Create Multiple Guest Accounts			
- 🛃 Guest Manager 🖅 🇣 Hotspot Manager	create_multi_result Create multiple accounts results page.	Create Multiple Accounts Results			
Pages  Fields	Create a single guest account.	Create New Guest Account			
	Edit Edit Fields     Accent by Control Contro Control Control Control Control Control Con	🍕 Show Usage 🤯 Translations			
- (a) Self-Registrations	Create_user_receipt Create single guest account receipt.	Create New Guest Account Receipt			
- Web Logins	= nuest edit				

### 选择visitor\_name(第20行),然后单击Insert After。

Home » Configuration » Pages » Forms

### Customize Form Fields (create\_user)

Use this list view to modify the fields of the form create\_user.

0	Quick Help		Preview Form				
 Rank	Field	Туре	Label	Description			
1	enabled	dropdown	Account Status:	Select an option for changing the status of this account.			
10	sponsor_name	text	Sponsor's Name:	Name of the person sponsoring this account.			
13	sponsor_profile_name	text	Sponsor's Profile:	Profile of the person sponsoring this account.			
15	sponsor_email	text	Sponsor's Email:	Email of the person sponsoring this account.			
20	visitor_name	text	Guest's Name:	Name of the guest.			
<b>P</b>	dit 🛯 🛅 Edit Base Field	😵 Remove	📤 Insert Before 🗔	Insert After Disable Field			

### Customize Form Field (new)

Use this form to add a new field to the form create\_user.

	Form Field Editor
* Field Name:	username_auth
Form Display Prope These properties control the	user interface displayed for this field.
Field:	Enable this field When checked, the field will be included as part of the form.
* Rank:	22 Number indicating the relative ordering of user interface fields, which are displayed in order of increasing rank.
* User Interface:	No user interface   Revert  Re
Form Validation Pro	the value of this field is checked.
Field Required:	Field value must be supplied Select this option if the field cannot be omitted or left blank.
Initial Value:	Revert to initialize this field with when the form is first displayed.
* Validator:	IsValidBool   The function used to validate the contents of a field.
Validator Param:	(None)  V Optional name of field whose value will be supplied as the argument to a validator.
Validator Argument:	Ontional value to supply as the argument to a validator.
Validation Error:	The error message to display if the field's value fails validation and the validator does not return an error message directly.

现在创建要在AUP访客门户页面后面使用的用户名。

### 导航到CPPPM > Guest > Guest > Manage Accounts > Create。

-来宾姓名:访客WiFi

-公司名称: 思科

- 电子邮件地址:guest@example.com

— 用户名身份验证: 仅允许访客使用其用户名访问: 启用

-账户激活:现在

-帐户有效期限:帐户未过期

— 使用条款:我是发起人:启用

### Create Guest Account

New guest account being created by admin.

Create New Guest Account					
* Guest's Name:	GuestWiFi Name of the guest.				
* Company Name:	Cisco Company name of the guest.				
* Email Address:	guest@example.com The guest's email address. This will become their username to log into the network.				
Username Authentication:	Allow guest access using their username only Guests will require the login screen setup for username-based authentication as well.				
Account Activation:	Now  Select an option for changing the activation time of this account.				
Account Expiration:	Account will not expire   Select an option for changing the expiration time of this account.				
* Account Role:	[Guest] ~ Role to assign to this account.				
Password:	281355				
Notes:					
* Terms of Use:	I am the sponsor of this account and accept the terms of use				
	Create				

创建Web登录表单。导航到CPPM > Guest > Configuration > Web Logins。

身份验证后部分中的终端属性:

用户名 |用户名 visitor\_name |访问者姓名 cn |访问者姓名 visitor\_phone |访客电话 邮件 |电子邮件 邮件 |电子邮件 sponsor\_name |保证人姓名 sponsor\_email |发起人电子邮件 **允许 — 访客 — 互联网 | true** 

aruba		ClearPass Guest					
Guest 0		Web Login Editor					
Onboard 0	* Name:	e-microsoftwareau shares installand and a second seco					
Configuration 0	Page Name:	lacençi Telar a paga xaara tur tela avda taga.					
Nutheritication		The and Taple will be assessible from '/participage_same.php'.					
Content Hanager	Description:						
Role Files		Conversion or descriptive text almost the web logic.					
Guest Manager	* Vendor Settings:	Pruba Natworks					
Pages	inch Mathema	"Server-strated — Charge of authorization (RFC 1619) even to cardiolar 🔍					
- Trelds	Lagin Method:	benet how the user's relation toget with be transfer. Senser-instructed togets expanse the user's RMC address to be available, usually from the captive portal redirection process.					
- The Porties	Page Redirect	manufactor in the second second					
Self-Reportations		Co net sheek - login will always be permitted w					
Web Logins	Becarity Hashi	Robert Mie level of cheating in apply in 2011, parameters paramit is the anti-legic page. Size this splim in detext often URL parameters have leave modified by the aver, for example their MAC address.					
Net Pages	Login Form	a balancies and context of the bala face.					
SHS Services		Anarymour - De torrequire a username or password V					
R Translations	Automotion	sident the sufficientiation requirement. Access Carlo requires a single code (userment) to be entered.					
		Anotestess a stake a Mark form requiring just the tame or a Lip In Sutton. A pre-existing account is required. Auto is a jointlar to anonymous but the ceap is automatically submitted.					
		Constant Caller and Antonymous account to have the operating Automotization need and					
	Auta-Generate:	The account will be oriented without a section limit or expendion time, and with the Guest rule (35.2), bitar a value for "Wronviews been" to use a specific username, or leave blank to randomly generate a username.					
		O.mtWP1					
	* Anenymous Users	The ansard to use for startyments addentication. The parameter will be whith the HTML.					
	<u> </u>	A reconversion to normal the assess takan crist to the number of parks pix with the apport.					
	Prevent CNA:	The Apple Captive Network Assistant (DM) is the pop-up browser shown when joining a network that has a captive portal.					
Administration 0		Note that this option may not work with all ventions, depending on how the captive partie is implemented.					
	Qualitain Form:	If salesland, you must supply your own HTHL login form in the Headler or Foular HTHL areas.					
	Custore Labels:	Override the default labels and error messages if selected, you will be able to alter labels and error messages for the summit legis form.					
	* Pro-Auth Check:	Lacal — match a local account v					
		areas now on contrasts and password shallo be checked before proceeding to the MS automobilities.					
	Pre-Auth Error:	The left is display if the converses and parameter leslop fails. Leave black to use the default Devald converses or parameterial.					
	Termer	Require a Terms and Conditions confirmation					
		If checked, the user will be forced to accept a Terms and Candilians checkbox.					
	Terma Label:	The form label for the tarms checkber.					
		AND THE AND THE AND					
	Terms Text)						
		#TML case cardiering your terms and Conditions. Lases Mark to use the default () eccept the rs heaf-r (new, global name-guest_accent_barre_of_use_ar()* target="block"+terms af use-v/ar-).					
	Terms Layout:	Display before terms checklos *					
	Tems Bron	The text to display if the terms are not accepted. Leave blank to use the default (In order to leg in, yes must accept the terms and conditions.)-					
	CAPTOHA	CATCHI, ROM V					
		accept and comment					
	Leg to Label 1	The form table for the log in buttor. Leaser blank to use the default (Leg In).					
	Translations	Skip automatic translation handling					
	Default Destination						
	Options for controlling to	he destination clients will redirect to after legin.					
	* Default URL	Propulsive. Entar the default URL to redirect clients.					
	0	Porce dolauit destination for all clients					
	Dvertice Destination:	If satisfied, the silent's default destruction will be avereighter regardless of its value.					
	Login Page Options for controlling It	he look and hed of the logic page.					
	* Skin:	ClearPass Guet Skin v					
		Anonymous durest W-Fi Class					
	Title:	The stille to display on the web legin page. Labor blank to use the default (Login).					
		(ww.muklenkerk)					
		Chead?- Cheat salar = "savy"?					
		Cardeleuse to Dares Wi-FLIC/Ar- Card-					
	Readwint to 1	Gao Gao					
		None sale - "black"> Gofferes and Conditionar(/b)					
		opression succe you review the Terms and Conditions in the link below because by sharehing the tick how and					
		networking the endlesing the put've					
		NTRS. Inexplain and a shapleyed induce like ingin form.					
		inva_test id=25751-pp Contect a staff member if you are experienting					
		#ifficulty logging in. */p=(/me_text)					
	* Lagin Delays	and their we accords to delay shife displaying the legit message.					
	Advertising Service	ni an ihar lagin paga.					
	Advertising	Drable Advertising Services content					
	Cloud Identity	is with surface cloud identity ( assistance,					
	Enabled	D trable logics with claud identity / social network codestails					
	Hulti-Pastor Authen	diation					
	Repurse a secondary fac	ter met autentualité.					
	Network Login Acce	10					
	Carticols access to the lo	da tela-					
	Allowed Access						
		Enter the IP addresses and networks from which lopins are permitted.					
	Provide A						
	Denied Access:						
		Inder the IP addresses and networks that are deened legin access. Rand HTTP 404 Met Pascel states w					
	* Deny Behaviari	Rebeil the requirer of the system is a required that is not prevailed.					
	Post-Authentication Actions to perform after	a summalia pre-subtrestination.					
	Health Check	Require a successful On/Guard health check					
		It appends the substitution is a basis of the second of the second					
	Update Endpoint:	If selected, the endpoint's attributes will also be updated with other details from the user account.					
	Advanced	Contamics with theirs stored with the endpoint					
		vision para Vision Sone					
	Endpoint Attributes:	Visitor shope Visitor Here					
		List of namebyalus pairs to pass along.					

验证—访客CWA授权

在CPPPM中,导航到Live Monitoring > Access Tracker。

连接并触发MAB服务的新访客用户。

### **摘要选**项卡:

Request Details	Request Details							
Summary Input	Output F	RADIUS CoA						
Login Status:	ACCEPT							
Session Identifier:	R000047	71a-01-6282a	a110					
Date and Time:	May 16,	2022 15:08:	00 EDT					
End-Host Identifier:	d4-3b-04	4-7a-64-7b	(Computer / Windows / Windo	ows)				
Username:	d43b047	7a647b						
Access Device IP/Port:	10.85.54	4.99:73120	(WLC_9800_Branch / Cisco)					
Access Device Name:	wlc01							
System Posture Status:	UNKNOV	VN (100)						
Policies Used -								
Service:	Guest S	SID - GuestPo	ortal - Mac Auth					
Authentication Method:	MAC-AU	тн						
Authentication Source:	None							
Authorization Source:	[Guest L	Jser Reposito	ry], [Endpoints Repository]					
Roles:	[Employ	ee], [User Au	thenticated]					
Enforcement Profiles:	Cisco_Po	ortal_Redirect						
I ◄ Showing 8 of 1-8 rec	ords 🕨 ы	Change Stat	tus Show Configuration	Export Show Logs	Close			

在同一对话框中,导航到Input(输入)选项卡。

Request Details							
Summary Input	Output RA	ADIUS CoA					
Username:	d43b047a647	b					
End-Host Identifier:	d4-3b-04-7a-6	64-7b (Computer / Windows / Windows)					
Access Device IP/Port:	10.85.54.99:7	73120 (WLC_9800_Branch / Cisco)					
RADIUS Request			•				
Radius:Airespace:Air	espace-Wlan-Id	1 4					
Radius:Cisco:Cisco-A	VPair	audit-session-id=6336550A00006227CE452457					
Radius:Cisco:Cisco-A	VPair	cisco-wlan-ssid=Guest					
Radius:Cisco:Cisco-A	VPair	client-iif-id=1728058392					
Radius:Cisco:Cisco-A	VPair	method=mab					
Radius:Cisco:Cisco-A	VPair	service-type=Call Check					
Radius:Cisco:Cisco-AVPair		vlan-id=21					
Radius:Cisco:Cisco-A	VPair	wlan-profile-name=WP_Guest					
Radius:IETF:Called-S	station-Id	14-16-9d-df-16-20:Guest					
Radius:IETF:Calling-	Station-Id	d4-3b-04-7a-64-7b					
I ◄ Showing 8 of 1-8 r	records 🕨 📔	Change Status Show Configuration Export Show Logs	Close				

### 在同一对话框中,导航到**输出**选项卡。

Request Details								
	Summary	Input	Output	RADIUS CoA				
Enforcement Profiles: Cisc			Cisco_Po	rtal_Redirect				
System Posture Status: UNKNOWN (100)				/N (100)				
Audit Posture Status: UN			UNKNOW	/N (100)				
	RADIUS Response							
Radius:Cisco:Cisco-AVPair			/Pair url-r	url-redirect-acl=CAPTIVE_PORTAL_REDIRECT				
Radius:Cisco:Cisco-AVPair		/Pair url-r 04-7	edirect=https://cppm.example.com/guest/iaccept.php?cmd-login&mac=d4-3b- 7a-64-7b&switchip=10.85.54.99					

8

# Appendix

为便于参考,此处提供了思科9800外部锚点控制器与RADIUS服务器和外部托管访客门户交互的状

K < Showing 8 of 1-8 records ► ► Change Status Show Configuration Export Show Logs Close

### 态流程图。

		_			9800 Foreign-WEC Guest Portal CWA now					
Clie	nt A	P WL	C-Foreign	WLC-	Anchor	DHCP D	NS Ra	dius	Guest	
<b>E</b>	[Client Assocication]								-	
1	[1] Assoc Res	west								
1.5	A CONTRACT OF A		1							
	Guest Crient Join									
			[MAB pro	cedure]		1				
				[2	Access-Request (sessionid+1E1E1E020000003F3F876869)					
							[3] <redirect_url> = <redirect_url> + <?sessionid:</p></redirect_url></redirect_url>			
			[4	I] Access-Accept ([ <redirect url="">, <redirect acl=""> ] <redirect< td=""><td>T URL&gt;: https://<cppm.fgdn.com>/guest/<page name="">.phg?sessio</page></cppm.fgdn.com></td><td>nid+1E1E1E021</td><td>000003F3F8768696gortal=194a5780)</td><td></td><td></td><td></td></redirect<></redirect></redirect>	T URL>: https:// <cppm.fgdn.com>/guest/<page name="">.phg?sessio</page></cppm.fgdn.com>	nid+1E1E1E021	000003F3F8768696gortal=194a5780)			
			4-							
	121 4035, 905	portse	If a Research to a	The Research College of the state of the second states of the second sta						
			Teg Export we	(1) Front Andre Browner						
1				1/1 March Marrier Magazine	1			1		1
			Foreign: Client g	pes to run state. Traffic is forwarded on Mobility Tunnel (CAPWAP)						
- 12	Wetween Web Auth					_		-		
	(External meanword)			181 Redent 1/1 referenced for Clerk care addre						
				Introduction of supportant of colors study and	$\overline{}$					
alt	[Client IP DHCP Process]							1		
					Client goes to DHCP-Required state					
			-	And a second state and a second state to a second state of the sec						
			MCDOOLC	crumes only subtriters around price, price, reced to quest Portal						
	[9] DHCP Hand	shake	-	[10] DHCP Handshake	[11] OHCP Handshake	+				
			4	[12] <ip_update> MSG: <client.ip></client.ip></ip_update>						
					Client goes to webauth pending state					
14			-							
alt	[Client OS Guest Portal Detection	n)								
111	[13] DNS Query www.msftconn	ecttest.com (CAPWAP)	*	[14] DNS Query (CAPVIAP)	[15] DNS Query	$\rightarrow$				
	[18] DNS Response www.msftconnecttest	com is at IP <x.x.x.x.f (capwia)<="" td=""><td>" <b>i 4</b></td><td>[17] DNS Response</td><td>[16] DNS Response</td><td>-</td><td></td><td></td><td></td><td></td></x.x.x.x.f>	" <b>i 4</b>	[17] DNS Response	[16] DNS Response	-				
1 5	[19] TCP SYN IP <x.x.x.x>:8</x.x.x.x>	0 (msftconnecttest)	*	[20] TCP SYN (CAPWAP)						
					Anchor: «REDIRECT_ACL»: redirect enforced					
	[22] TCP SYN-A	скаск	[21] TCP	SYN ACK/ACK speefing <x.x.x.x> (WebAuth <global> VIP)</global></x.x.x.x>						1
110	[23] HTTP GET http://www.msftconn	ecttest.com/connecttest.txt	1	[24] HTTP GET (CAPWAP)						
110	[26] HTTP-302 Redirect Location-Guest	Portal(CPPM) «REDIRECT URL»	1	[25] HTTP-302 (CAPWAP)	]					
116	Circles Result Emeral									
	[27] DNS Query <red< td=""><td>NRECT URL&gt;</td><td></td><td>[28] DNS Query (CAPNIAP)</td><td>[29] DNS Query</td><td></td><td></td><td></td><td></td><td></td></red<>	NRECT URL>		[28] DNS Query (CAPNIAP)	[29] DNS Query					
	(32) DNS Response <redirect< td=""><td>URL&gt; IS AT IP &lt; y y y y y&gt;</td><td>1.</td><td>[31] DNS Response (CAPWAP)</td><td>[30] DNS Response</td><td></td><td></td><td></td><td></td><td></td></redirect<>	URL> IS AT IP < y y y y y>	1.	[31] DNS Response (CAPWAP)	[30] DNS Response					
	Clean must must Guest Produit certificant									
					Anchor: <redirect_acl>: redirect bypass <y.y.y.y> (Guest Port</y.y.y.y></redirect_acl>	-h				
	[33] Guest Portal/CPPHD TCP-SYN/SYN AC	KACK <y y="">:443 (CAPWAP</y>		[34] TCP-SYN/SYN-ACK/ACK (CAPWAP)		-	[35] TCP-SYN/SYN-ACK/ACK			
1 0	[36] HTTP GET «REDIREC	T URL/sessionid>	1	[37] HTTP GET (CAPWAP)			[38] HTTP GET			3
	[41] HTTP/1.1.2	99 OK	1	[40] HTTP/1.1 200 OK (CAPWAP)			[39] HTTP/1.1.200 OK			
	Client clicks 'Accest' AUP burns									
1	[42] HTTP POST/HTT	F1.1 200 DK	***	1431 HTTP POSTARTTP1.1 200 OK	14		Teelerine hozositettet 1 500 OK	Language and		-
								[45] Update I	unopoint us: «client_mac>:AllowinterhetAccess»)	
									[46] Captive Portal page refresh d	elay
		E.	It (CoA Reauth	N						
							[47] CoA delay time			
					48] CoA Request (Type= <reauthenticate>, <sessionid>)</sessionid></reauthenticate>			_		
					[49] CoA Ack ( <session d="">)</session>			]		
			(MAB)					h I		
					[50] Access Request ( <sessionid>)</sessionid>					
					[51] Access Accept (No redirect URL, «sessionid»)					
			4					2		
			-	(5v) Export Anchor Request						
			<ul> <li>[33] Export</li> </ul>	INCOME RESPONDE. NO [CREDINECT_UNLS, CREDINECT_ACLS]						
					Anchor: Client goes to run state					
					In all with California Source Landon Bana					
	•				Contraction of the contraction of the second s					•
					client goes to RUN state					
	-					-				
Clie	nt A	P WL	C-Foreign	WLC-	Anchor	DHCP D	NS Re	dius	Guest	

具有锚点WLC的访客中心Web身份验证状态图

# 相关信息

- Cisco 9800部署最佳实践指南
- 了解Catalyst 9800无线控制器配置模型
- 了解Catalyst 9800无线控制器上的FlexConnect
- <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)。