# CMX互联体验 — 社交、短信和自定义门户注册配 置示例

# 目录

<u>简介</u> <u>先决条件</u> 要求 使用的组件 配置 网络图 配置 通过SMS进行身份验证 通过社交网络帐户进行身份验证 通过自定义门户进行身份验证 验证 故障排除

# 简介

本文档的目的是通过互联移动体验(CMX)上的访客门户配置引导网络管理员通过客户端注册。

CMX使用户能够使用社交注册登录、SMS和自定义门户注册并验证到网络。在本文档中,可以找到 无线局域网控制器(WLC)和CMX上配置步骤的概述。

# 先决条件

# 要求

CMX应正确配置基本配置。

从Prime基础设施导出映射是可选操作。

## 使用的组件

本文档中的信息基于以下软件和硬件版本:

- •思科无线控制器版本8.2.166.0、8.5.110.0和8.5.135.0。
- •思科互联移动体验版本10.3.0-62、10.3.1-35. 10.4.1-22。

# 配置

网络图

本文档将介绍使用CMX对用户/客户端进行无线网络身份验证的两种不同方法。

首先,将介绍使用社交网络帐户设置身份验证,然后使用SMS进行身份验证。

在这两种情况下,客户端都会尝试通过CMX使用身份验证在SSID上注册。

WLC将HTTP流量重定向到CMX,在CMX中,系统会提示用户进行身份验证。CMX包含用于客户端 注册的门户设置,包括通过社交帐户和SMS。

下面介绍注册流程:

使用的拓扑为:

- 1. 客户端尝试加入SSID并打开浏览器。
- 2. WLC将重定向到访客门户,而不是访问请求的站点。
- 3. 客户端提供其凭证并尝试进行身份验证。
- 4. CMX处理身份验证过程。
- 5. 如果成功,则现在为客户端提供完全互联网访问。
- 6. 客户端被重定向到初始请求的站点。

# Internet

# 配置

#### 通过SMS进行身份验证

思科CMX允许通过SMS进行客户端身份验证。此方法需要设置HTML页面,以便用户向系统提供其 凭证。默认模板由CMX本地提供,稍后可编辑或替换为自定义模板。

文本消息服务通过将CMX与Twilio集成来完<u>成,</u>Twilio是一个允许发送和接收文本消息的云通信平 台。Twilio允许每个门户拥有一个电话号码,这意味着如果使用多个门户,则每个门户需要一个电话 号码。

#### A. WLC 配置

在WLC端,将同时配置SSID和ACL。AP应加入控制器并处于RUN状态。

1. ACL

需要允许WLC上配置的HTTP流量的ACL。要配置ACL,请转至Security -> Access Control Lists -> Add New Rule。

使用的IP是为CMX配置的IP。这允许WLC和CMX之间的HTTP流量。下图显示了创建的ACL,其中 "10.48.39.100"是指CMX IP地址。

cisco	MONI		<u>W</u> LANs		r W <u>I</u> RELESS	<u>s</u>	ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	:	
Security	Acc	ess Co	ntrol L	ists > Edit									
<ul> <li>AAA</li> <li>General</li> <li>RADIUS         <ul> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> <li>DNS</li> <li>Downloaded AVP</li> </ul> </li> </ul>	Gene Acces Deny	eral s List Nar Counters Action	me	CMX_redire 0 ce IP/Mask	ect Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
LDAP Local Net Users	1	Permit	0.0.0	.0 /	10.48.39.100 255.255.255.255	/	ТСР	Any	НТТР	Any	Any	0	
MAC Filtering Disabled Clients User Login Policies	2	Permit	10.48 255.2	.39.100 / .55.255.255	0.0.0.0 0.0.0.0	/	тср	НТТР	Any	Any	Any	0	
AP Policies Password Policies													

## 2. WLAN

因此,与门户的集成完成后,必须对WLAN进行安全策略更改。

首先,转到WLANs ->Edit->Layer 2->Layer 2 Security,然后在下拉列表中选择None,因此Layer 2 Security已禁用。然后,在同一"安全"选项卡中,更改为第3层。在"第3层安全"下拉菜单中,依次选择Web策略和直通。在预身份验证ACL中,选择之前配置的IPv4 ACL,将其绑定到必须提供SMS身份验证的相应WLAN。必须启用Over-ride Global Config(超载全局配置)选项,并且网络身份验证类型必须为External(重定向到外部服务器),因此客户端可以重定向到CMX服务。URL必须与CMX SMS身份验证门户相同,格式为http://<CMX-IP>/visitor/login。

،،۱،،۱۱،، cısco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	Save Configuration   Ping FEEDBACK	Logout   <u>R</u> efresh
WLANs	WLANs > Edit 'cmx_sms'	< Back	Apply
<ul> <li>WLANS</li> <li>WLANS</li> <li>Advanced</li> </ul>	General     Security     QoS     Policy-Mapping     Advanced       Layer 2     Layer 3     AAA Servers       Layer 2 Security & None     \$       MAC Filtering @       Fast Transition       Fast Transition       Disable \$		

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
/LANe	General Security QoS Policy-Mapping Advanced
LANS	Layer 2 Layer 3 AAA Servers
WLANS	
Advanced	Layer 3 Security Web Policy 🗘
	Authentication
	Passthrough
	Conditional Web Redirect
	Splash Page Web Redirect
	On MAC Filter failure <sup>10</sup>
	Web policy done locally on AP warning
	Preauthentication ACL IPv4 CMX_redirect 📀 IPv6 None 📀 WebAuth FlexAcl None ᅌ
	Qr Code Scanning Email Input
	Sleeping Client  Enable
	Override Global Config <sup>20</sup> 🗹 Enable
	Web Auth type External(Re-direct to external server)
	Redirect URL http://10.48.39.100/visitor/login

#### B. Twilio

CMX为文<u>本消</u>息服务提供Twilio集成。在正确配置Twilio上的帐户后,提供凭证。需要ACCOUNT SID和AUTH TOKEN。

Twilio有自己的配置要求,通过设置服务的过程进行记录。在与CMX集成之前,可以测试Twilio服务 ,这意味着在将Twilio设置与CMX结合使用之前,可以检测与Twilio设置相关的问题。

⊕tw	rilio <sup>-</sup>				docs $\sim$			
	✓ 5	iettings /		UPGRADE	, <b>O</b> Go to	¢	?	\$03
ŵ	Dashboard							
Ģ	Billing	Two-Factor Authentication						
	Usage	Add an extra layer of protection to your account, wit	h a verification code sent via SMS or voice call.					
)	Settings	DISABLED Do not require a verification code						
	General Subaccounts	ONCE PER COMPUTER Trust computers and only a	ask for verification code every 30 days					
	Manage Users	O EVERY LOG-IN We'll always ask for a verification of	ode					
	User Settings							
	Doer Profile	API Credentials						
	Upgrade	LIVE Credentials	Learn about REST API Credentials >	TEST Credentials	Learn abo	ut Test Cre	dentials	я
		ACCOUNT SID AC3132a0b65f9ac540318a0a576e3f3dbd Used to exercise the REST API		TEST ACCOUNT SID ACb7ec526108f80811b68c6b7b9693e69d Used to exercise the REST API				
		AUTH TOKEN		TEST AUTHTOKEN				
		Request a Secondary Token						
		Keep this somewhere safe and secure		Keep this somewhere safe and secure				

# C. CMX配置

需要将控制器正确添加到CMX,以及从Prime基础设施导出的映射。

#### •SMS注册页

注册门户有默认模板。可以找到选择CONNECT&ENGAGE->Library的门户。如果需要模板,请在 下拉菜单中选择模板。

要将Twilio与门户集成,请转至Twilio配置并提供帐户ID和身份验证令牌。如果集成成功,Twilio帐

户中使用的号码将弹出。

CISCO 10.3.0-62	DETE 8 LOC	CT ANALYTICS	ÇONNECT & ENGAGE	<b>Ø</b> Manage	SYSTEM				ſ	admin +
							Connect Experiences			
Login Page 🖌 <table-cell></table-cell>	Please enter your number to get WI-FI Have SMS Code? x  Phone Number* C  Please review and accept our <u>Terms &amp; Conditions</u> CUBMIT	English	• 0	CONTENT Have SMS C Enter Twill Acc Aut From Num C Enter Mess Error Mess	BACKGROUND SMS Code? SMS Code SMS Code Input Placeholder SMS Code Configuration CAST32a0b6? Token: Casta Cas	THEMES LANGUA	dbd	<ul> <li>₽</li> <li>♀</li> <li>♀</li></ul>	I Inno	EDIT

#### 通过社交网络帐户进行身份验证

使用社交网络帐户对客户端进行身份验证要求网络管理员在CMX上添加有效的Facebook应用标识 符。

#### A. WLC配置

在WLC端,将同时配置SSID和ACL。AP应加入控制器并处于RUN状态。

1. ACL

正如我们使用HTTPS作为身份验证方法一样,必须在WLC上配置允许HTTPS流量的ACL。要配置 ACL,请转至Security -> Access Control Lists -> Add New Rule。

CMX IP必须用于允许WLC和CMX之间的HTTPS流量。(在本例中,CMX IP为10.48.39.100)

cisco	MONI	ITOR W	LANs		R WIRELESS	s	ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK		
Security	Acc	ess Cor	trol L	ists > Edit									
<ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> </ul>	Gene Acces Deny	eral s List Nam Counters	e	CMX_Auth 0	1								
DNS Downloaded AVP TACACS+	Seq	Action	Sourc	e IP/Mask	Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
LDAP Local Net Users	1	Permit	10.48 255.2	.39.100 / 55.255.255	0.0.0.0 0.0.0.0	/	ТСР	HTTPS	Any	Any	Any	0	
MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	2	Permit	0.0.0. 0.0.0.	0 /	10.48.39.100 255.255.255.25	5	ТСР	Any	HTTPS	Any	Any	0	
Local EAP													

此外,还需要使用带有Facebook URL的DNS ACL。为此,在安全 — >访问控制列表中查找之前配置的ACL(本例中为CMX\_Auth)的条目,并将鼠标移到条目末尾的蓝色箭头,然后选择添加 — 删

除URL。然后在URL字符串名称和添加上键入Facebook的URL。

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS	S HELP FEEDBACK
Security	ACL > CMX_Auth > URL List	
<ul> <li>▼ AAA</li> <li>General</li> <li>▼ RADIUS</li> <li>Authentication</li> </ul>	URL String Name Add	
Fallback	facebook.com	
DNS	m.facebook.com	
TACACS+     LDAP	fbcdn.net	

#### 2. WLAN

安全策略会更改,以便注册生效,需要在WLAN上进行特定配置。

如之前对SMS注册所做的那样,首先转到WLAN ->编辑 — >第2层 — >第2层安全,然后在下拉列 表中选择无,因此禁用第2层安全。在同一Security选项卡中,更改为Layer 3。在Layer 3 Security下拉菜单中,依次选择Web Policy和Passthrough。在预身份验证ACL中,选择之前配置的 IPv4 ACL,将其绑定到必须通过Facebook提供身份验证的相应WLAN。必须启用Over-ride Global Config(超载全局配置)选项,并且网络身份验证类型必须为External(重定向到外部服务器),因 此客户端可以重定向到CMX服务。请注意,此时URL必须采用以下格式https://<CMX-IP>/visitor/login。

	Save Configuration   Ping   Logout Refresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'cmxFW'     < Back     Apply
WLANs	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2       Layer 3       AAA Servers         Layer 2 Security for None       +         MAC Filtering for many for m
	Sa <u>v</u> e Configuration <u>P</u> Ing Logout <u>R</u> efresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'Facebook' < Back Apply
VLANs	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2       Layer 3       AAA Servers         Layer 3 Security 4       Web Policy ‡         Authentication         Passthrough         Conditional Web Redirect         Splash Page Web Redirect         On MAC Filter failure <sup>10</sup> Preauthentication ACL       IPv4         CMX_Auth       ‡         IPv6       None ‡         WebAuth FlexAcl       None ‡         Email Input       Sleeping Client         Sleeping Client       Enable         Over-ride Global Config <sup>2</sup> © Enable         Web Auth type       External(Re-direct to external server) ‡         URL       https://10.

# B.面向开发人员的Facebook

为了实现Facebook和CMX的集成,需要Facebook应用才能在两部分之间交换正确的令牌。

转到Facebook<u>供开发人员</u>创建应用。要集成这些服务,需要一些应用配置要求。

在"应用设置"中,确保已启用"客户端OAuth登录"和"Web OAuth登录"。此外,验证有效OAuth重定向URI,您的CMX URL为**https:**//<CMX-IP>/visitor/login格式。



要发布应用并准备好与CMX集成,需要将其公开。为此,请转至"应用审阅" — >"使<应用名称>为公 共"?并将状态更改为"是"。

f = App Dashboard				Docs	Too	ls Support	Q Search developers.facebook.com
	🔯 Catarina's first app	•	APP ID:		ON O	Status: Live	✓ View Analytics
	# Dashboard						
	∯ Settings		Make Catarina's first app public?				
	Roles	+	Yes Your and is currently live and available to the public				
	Alerts	÷	real approcartering we and available to the public.				
	PRODUCTS (+)		Submit Items for Approval				
	S Facebook Login	÷	Some Facebook integrations require approval before public usage. Before submitting your app for review, please consult our Platform	art a Submission			
	≅ Activity Log		Policy and Review Guidelines.				

# C. CMX配置

需要将控制器正确添加到CMX,以及从Prime基础设施导出的映射。

• 注册页面

要在CMX上创建注册页,应执行与之前创建SMS注册页相同的步骤。选择CONNECT&ENGAGE->库,可通过在下拉菜单中选择模板找到准备编辑的模板门户。

通过Facebook凭证注册要求门户具有社交帐户连接。要从头开始,在创建自定义门户时,请转至 CONTENT->Common Elements->Social Auth,然后选择Facebook。然后插入从Facebook获取的 应用名称和应用ID(密钥)。

cisco 10.8.1-86		DETECT & LOCATE	ANALYTICS	CONNECT 8 ENGAGE	<b>¢</b> Manage	SYSTEM			(†	admin -
							Dashboard	Connect Experiences	Policy Plans Library	Settings -
RegistrationPage &								Live View	Portals Library	Save
Login Page 👻 💁			English	• 6	CONTENT	BACKGROUND	THEMES LANGUAGES			EDIT
	Legis le seggest le uif				Social	.ogin			Remove eleme	int
	×				Depe	ends on Terms and C	Conditions			- 11
	f				- Content					
					Ca	acebook 🧬   Scope: tarina's first app	Basic Profile     Key:			
					0	create new				- 11

## 通过自定义门户进行身份验证

使用自定义门户对客户端进行身份验证类似于配置外部Web身份验证。重定向将完成到CMX上托管 的自定义门户。

## A. WLC配置

在WLC端,将同时配置SSID和ACL。AP应加入控制器并处于RUN状态。

1. ACL

正如我们使用HTTPS作为身份验证方法一样,必须在WLC上配置允许HTTPS流量的ACL。要配置 ACL,请转至Security(安全) — > Access Control Lists(访问控制列表) — >Add New Rule(添 加新规则)。

CMX IP必须用于允许WLC和CMX之间的HTTPS流量。(在本例中,CMX IP为10.48.71.122)。

注意:确保在CMX CLI上发出命令"cmxctl node ssimode enable",在CMX上启用ssl。

،، ،،، ،، cısco	MONITOR W	LANs <u>C</u> ONTROL	LER WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK					
Security	Access Con	trol Lists > Edi	t										
General	General												
<ul> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> <li>DNS</li> </ul>	Access List Nam Deny Counters	е СМХ_НТ 0	TPS										
Downloaded AVP	Seq Action	Source IP/Mask		Destinatio	n IP/Mask	Pr	otocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
▶ TACACS+ LDAP	1 Permit	10.48.71.122	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	тс	P	HTTPS	Any	Any	Any	0	
Local Net Users MAC Filtering Disabled Clients	2 Permit	0.0.0.0	/ 0.0.0.0	10.48.71.1	22 / 255.255.2	255.255 TC	P	Any	HTTPS	Any	Any	0	

2. WLAN

安全策略会更改,以便注册生效,需要在WLAN上进行特定配置。

如之前对SMS和社交网络注册所做的那样,首先,转到WLANs->Edit->Layer 2->Layer 2 Security,然后在下拉列表中选择None,因此Layer 2 Security被禁用。在同一Security选项卡中 ,更改为Layer 3。在Layer 3 Security下拉菜单中,依次选择Web Policy和Passthrough。在预身份 验证ACL中,选择之前配置的IPv4 ACL(本例中命名为CMX\_HTTPS),并将其绑定到相应的 WLAN。必须启用Over-ride Global Config(超载全局配置)选项,并且网络身份验证类型必须为 External(重定向到外部服务器),因此客户端可以重定向到CMX服务。请注意,此时URL必须采 用以下格式https://<CMX-IP>/visitor/login。

رابیاب cısco	<u>M</u> ONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>s</u> ecurity	M <u>A</u> NAGEMEN
WLANs	WLANs >	Edit 'c	mx_login'			
WLANs	General	Secu	rity QoS	Policy-Map	ping Adv	vanced
Advanced	Layer 2 Layer Fast Tra Fast Trar Lobby A Lobby	2 Lay 2 Security nsition dmin Con 7 Admin Ac	er 3 AAA S	ervers	)	

ululu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'cmx_login'
VLANs	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 3 Security Web Policy ‡ Captive Network Assistant Bypass None ‡ Authentication Passthrough Conditional Web Redirect Splash Page Web Redirect On MAC Filter failure <sup>10</sup> Web policy done locally on APW2rning Preauthentication ACL IPv4 CMX_HTTPS ‡ IPv6 None ‡ WebAuth FlexAcl None ‡ Qr Code Scanning Email Input Sleeping Client Enable Override Global Config <sup>20</sup> © Enable Web Auth type External(Re-direct to external server) ‡ Redirect URL https://10.48.71.122/visitor/login

## C. CMX配置

需要将控制器正确添加到CMX,以及从Prime基础设施导出的映射。

# • 注册页面

要在CMX上创建注册页,所执行的步骤与之前为其他身份验证方法创建该页的步骤相同。选择 CONNECT&ENGAGE->库,可通过在下拉菜单中选择模板找到准备编辑的模板门户。

正常注册的门户可以从头开始(选择"自定义")或从CMX库上提供的"注册表"模板进行修改。



# 验证

# WLC

要验证用户是否已在系统上成功通过身份验证,请在WLC GUI中,转到MONITOR->Clients并在列 表中搜索客户端的MAC地址:

MONITOR WLANS CONTROLLER WIRELESS SECURITY MAN	GEMENT COMMANDS HELP FEEDBACK						Save Con	iguration j	ing Logout	<ul> <li>Berresh</li> <li>Home</li> </ul>
Clients									Entries 1	- 1 of 1
Current Filter None [Change Filter] [Clear F	iter]									
Client MAC Addr IP Address(Ipv4/Ipv6)	AP Name	WLAN Profile	WLAN SSID	User Name	Protocol	Status	Auth Po	ort Slot Id	Tunnel	Fastian
<u>f4:</u> 64.	AP3-37021	Facebook	WiFi_Facebook	Unknown	802.11ac	Associated	Yes 1	1	No	No
Foot Notes RLAN Clients connected to AP702w, will not show Client IP details.										
	MONITOR     WLANS     CONTROLLER     WIRELESS     SECURITY     MANA       Clients	MONITOR         WLANS         CONTROLLER         WIRELESS         SECURITY         MANAGEMENT         COMMANDS         HELP         PEEDBACK           Clients	MONITOR     WLAN     CONTROLLER     WIRELESS     SECURITY     MANAGEMENT     COMMANDS     HELP     PEEDBACK       Clients     Current Filter     None     [Chaopa Filter]     [Clear Filter]       Client MAC Addr     IP Address(Tpv4/Tpv6)     AP Name     WLAN Profile       Eg:     64.     AP3-37021     Factbook	MONITOR       VIANa       CONTROLLER       VIRELESS       SECURITY       MANAGEMENT       COMMANDS       HE,P       PEEDBACK         Clients	MONITOR         MAR         CONTROLLER         MIRELES         SECURITY         MANAGEMENT         COMMANDS         HELP         PEEDBACK           Clients	MONTOR         WAN         CONTROLLER         WIRELESS         SECURITY         MANAGEMENT         COMMANDS         HELP         EEEDBACK           Clients	MONTOR         WLAN         CONTROLLER         WIRELES         SECURITY         MANAGEMENT         COMMANDS         HELP         FEEDBACK    Clients  Current Filter           Current Filter         None         Chaopa Filter]         Clear Filter]         Filter         Filter         Filter]         Filter         Filter]         Filter] <td>MONTOR         MAR CONTROLLER         WIRELESS         SECURITY         MANAGEMENT         COMMANDS         HE.p         PEDDACX             Clients             Current Filter         None         Chaope Filter   Clear Filter]             Client MaC Addr         IP Address(Ipr4/Ipr4)         AP Name         WLAN Profile         WLAN SSID         User Name         Protocol         Status         Auth         Put             Client MaC Addr         IP Address(Ipr4/Ipr4)         AP Name         WLAN Profile         WLAN SSID         User Name         Protocol         Status         Auth         Put             Foot Notes         RUM Cloent connected to AP702n, will not show Client IP details.         Status         Status         Status         Status         Status         Status         Auth         Put         Status         Status         Auth         Put         <th< td=""><td>MONTOR         MAR CONTROLLER         WIRELESS         SECURITY         MANAGEMENT         COMMANDS         HE.p.         PEEDBACK    Clients  Current Filter           None         Chaope Filter]         Cleare Filter]         Mane         WLAN Profile         WLAN SSID         User Name         Protocol         Status         Auth         Port         Stot Id           Client MAC Addr         1P Address(Ipv4/Ipv6)         AP Name         WLAN Profile         WLAN SSID         User Name         Protocol         Status         Auth         Port         Stot Id         To    Foot Notes RUM Cloare connected to AP702n, will not show Cloare IP details.</td><td>MONTOR         MARLES         SECURITY         MARLERS         SECURITY         MARLERS         RECOMPANDS         HEP         PEDDACK</td></th<></td>	MONTOR         MAR CONTROLLER         WIRELESS         SECURITY         MANAGEMENT         COMMANDS         HE.p         PEDDACX             Clients             Current Filter         None         Chaope Filter   Clear Filter]             Client MaC Addr         IP Address(Ipr4/Ipr4)         AP Name         WLAN Profile         WLAN SSID         User Name         Protocol         Status         Auth         Put             Client MaC Addr         IP Address(Ipr4/Ipr4)         AP Name         WLAN Profile         WLAN SSID         User Name         Protocol         Status         Auth         Put             Foot Notes         RUM Cloent connected to AP702n, will not show Client IP details.         Status         Status         Status         Status         Status         Status         Auth         Put         Status         Status         Auth         Put <th< td=""><td>MONTOR         MAR CONTROLLER         WIRELESS         SECURITY         MANAGEMENT         COMMANDS         HE.p.         PEEDBACK    Clients  Current Filter           None         Chaope Filter]         Cleare Filter]         Mane         WLAN Profile         WLAN SSID         User Name         Protocol         Status         Auth         Port         Stot Id           Client MAC Addr         1P Address(Ipv4/Ipv6)         AP Name         WLAN Profile         WLAN SSID         User Name         Protocol         Status         Auth         Port         Stot Id         To    Foot Notes RUM Cloare connected to AP702n, will not show Cloare IP details.</td><td>MONTOR         MARLES         SECURITY         MARLERS         SECURITY         MARLERS         RECOMPANDS         HEP         PEDDACK</td></th<>	MONTOR         MAR CONTROLLER         WIRELESS         SECURITY         MANAGEMENT         COMMANDS         HE.p.         PEEDBACK    Clients  Current Filter           None         Chaope Filter]         Cleare Filter]         Mane         WLAN Profile         WLAN SSID         User Name         Protocol         Status         Auth         Port         Stot Id           Client MAC Addr         1P Address(Ipv4/Ipv6)         AP Name         WLAN Profile         WLAN SSID         User Name         Protocol         Status         Auth         Port         Stot Id         To    Foot Notes RUM Cloare connected to AP702n, will not show Cloare IP details.	MONTOR         MARLES         SECURITY         MARLERS         SECURITY         MARLERS         RECOMPANDS         HEP         PEDDACK

点击客户端的MAC地址,在详细信息中,确认客户端策略管理器状态处于RUN状态:

ահահո						
cisco	MONITOR WLANS	ONTROLLER WIRELESS	SECURITY MANAG	EMENT COMMANDS HE	LP FEEDBACK	
Monitor	Clients > Detail					
Summary <ul> <li>Access Points</li> <li>Cisco CleanAir</li> </ul>	Max Number of Records General AVC Sta	tistics				
Statistics     CDP	<b>Client Properties</b>			AP Properties		
Bogues	MAC Address	f4:		AP Address	78:	
Clients	IPv4 Address	64.		AP Name	AP3-3702I	
Sleening Clients	IPv6 Address	fe80:		AP Type	802.11ac	
Multicast				AP radio slot Id	1	
Applications	WONTROR         WUARS         C           Clients > Detail         Max Number of Record         General         AVC St           General         AVC St         Client Properties         MAC Address           IPv4 Address         IPv4 Address         IPv6 Address           IPv6 Address         IPv6 Address         IPv6 Address           User Name         Port Number         Interface           VLAN ID         Quarantine VLAN ID         CCX version           E2E Version         Mobility Role         Mobility Role For IP           Address         Mobility Role         Mobility Role           Mobility More (Sec)         Uptimum (Sec)         VLAN ID			WLAN Profile	Facebook	
Local Profiling				WLAN SSID	WiFi_Facebook	
				Data Switching	Central	
				Authentication	Central	
				Status	Associated	
				Association ID	1	
				802.11 Authentica	tion Open System	
	Client Type	Regular		Reason Code	1	
	Client Tunnel Type	Unavailable		Status Code	0	
	User Name			CF Pollable	Not Implemented	
	Port Number	1		CF Poll Request	Not Implemented	
	Interface	internet_access		Short Preamble	Not Implemented	
	VLAN ID	129		PBCC	Not Implemented	
	Quarantine VLAN ID	0		Channel Anility	Not Implemented	
	CCX Version	CCXv4		Timeout	1800	
	E2E Version	E2Ev1		WEP State	WED Disable	
	Mobility Role	Local		WEP State	WLP Disable	
	Mobility Peer IP Address	N/A		Allowed (URL)I	P address	
	Mobility Move Count	0				
	Policy Manager State	RUN				
	Management Frame	No				
	UpTime (Sec)	71				
	Current TxRateSet	m8 ss2				

CMX

通过打开CONNECT&ENGAGE选项卡,可以验证CMX上有多少用户经过身份验证:

-ol ci	Hilli cux SCO 1031-05	DETECT & LOCATE	ANALYTICS	ÇONNECT 8 ENGAGE	<b>Ø</b> MANAGE	SYSTEM					•	admin +
								Dashboard	Connect Experiences	Policy Plans	Library 👻	Settings 👻
	Clobal     V No locations available	•	© Ir   Las	nterval st 7 Days		÷	Visitor Search Please enter search patte	m	- (	<b>X</b>		
(	Global Dashboard											
	Today at a Glance - Feb 22, 2018											
	<b>201</b> 1			Vi	isitor Trend co	mpared to:		Data Us	age:			
	Total Visitors				Yesterday		Average		Upload	Dow	nload	
	Repeat Visitors : 0		New Visito	ors : 1	<b>₩</b> ∞9	6	<b>O</b> 17%		0		C	
	Column +			() Ar	rea	•						<b>i</b>
	New and Repeat Visitors		Repeat Visit	tors 's			Netwo	rk Usage				

要检查用户详细信息,请在右上角的同一选项卡中点击Visitor Search:

							<b>9</b>	£6 🗢	¢ŝ	<b>Å</b>								admin
CISCO 10.3.1-35	Visitor Searc	h														×	Plans   Library	
♀ Location Global	Please enter search o	query Options			۹	Downloa	d as CSV 🛓											
Global Dashl	Search on 19 of 19 selected							•	From 02/21/2018 3:41 PI	и		To 02/22/	'2018 3:41 PM	4				
Today at a Glance	Export Preview (	Up to 100 r	esults show	n, please ex	port CSV to	view all)												
	Mac Address	State	First Login Time	Last Login Time	Last Accept Time	Last Logout Time	Location/Site	Portal	Туре	Auth Type	Device	Operating System	Bytes Received	Bytes Sent	Social Facebook Name	Social Faceboo Gender	Download	
Repeat Visitors : 0	f4:	active	Feb 22, 2018 3:37:59 PM	Feb 22, 2018 3:38:22 PM	Feb 22, 2018 3:38:22 PM	Feb 22, 2018 3:38:22 PM	Global	RegistrationPag	e CustomPortal	REGISTRATION	PC	Windows 10	0	0	Catarina Silva	female	0	
Column	Previous 1	Next																(i)
4	Showing 1 of 1								age									
Number of V									N 0 Bytes									

# 故障排除

为了检查元素之间交互的流,可以在WLC中执行一些调试:

>debug client<MAC addr1> <MAC addr2> (输入一个或多个客户端的MAC地址)

>debug web-auth redirect enable mac <MAC addr> (输入web-auth客户端的MAC地址)

>debug web-auth webportal-server enable

>debug aaa all enable

此调试将允许进行故障排除,如果需要,可以使用某些数据包捕获来补充故障。