# CMX互聯體驗 — 社交、SMS和自定義門戶註冊 配置示例

# 目錄

簡介
必要條件
需求
採用元件
設定
網路圖表
組態
通過SMS進行身份驗證
通過自定義門戶進行身份驗證
驗證
疑難排解

# 簡介

本文的目的為指導網路管理員通過互聯移動體驗(CMX)上的訪客門戶配置完成客戶端註冊。

CMX允許使用者使用社交註冊登入、SMS和自定義門戶在網路中註冊和身份驗證。在本文中,可以 找到無線LAN控制器(WLC)和CMX上的組態步驟概觀。

# 必要條件

# 需求

CMX應正確配置基本配置。

從Prime基礎設施匯出地圖是可選的。

#### 採用元件

本文中的資訊係根據以下軟體和硬體版本:

- •思科無線控制器版本8.2.166.0、8.5.110.0和8.5.135.0。
- •思科互連行動體驗版本10.3.0-62、10.3.1-35、10.4.1-22。

# 設定

# 網路圖表

本文檔將介紹使用CMX對無線網路中的使用者/客戶端進行身份驗證的兩種不同方法。

首先介紹使用社交網路帳戶設定身份驗證,然後使用SMS進行身份驗證。

在這兩種情況下,客戶端將嘗試通過CMX使用身份驗證在SSID上註冊。

WLC將HTTP流量重新導向到CMX,系統會提示使用者進行驗證。CMX包含用於客戶註冊的門戶設 定,包括社交帳戶和SMS。

下面介紹了註冊流程:

- 1. 客戶端嘗試加入SSID並開啟瀏覽器。
- 2. WLC會將其重新導向至訪客輸入網站,而不是存取所請求的網站。
- 3. 使用者端會提供其憑證並嘗試進行驗證。
- 4. CMX處理身份驗證過程。
- 5. 如果成功,則現在為客戶端提供完全網際網路訪問。
- 6. 客戶端被重定向到最初請求的站點。

#### 使用的拓撲是:



#### 組態

#### 通過SMS進行身份驗證

Cisco CMX允許通過SMS進行客戶端身份驗證。此方法需要設定HTML頁面,以便使用者可以向系 統提供其憑據。預設模板由CMX原生提供,以後可以編輯或用自定義模板替換。

文本消息服務通過將CMX與<u>Twilio</u>(一個允許傳送和接收文本消息的雲通訊平台)相整合來完成。 Twilio允許每個門戶都有一個電話號碼,這意味著如果使用多個門戶,則每個門戶需要一個電話號碼 。

#### A. WLC組態

在WLC端,將同時配置SSID和ACL。AP應連線到控制器且處於RUN狀態。

1. ACL

需要在WLC上設定允許HTTP流量的ACL。要配置ACL,請轉至Security->Access Control Lists->Add New Rule。 使用的IP是為CMX配置的IP。這允許WLC和CMX之間的HTTP流量。下圖顯示了建立的ACL,其中「10.48.39.100」是指CMX ip地址。

cisco	MONI	TOR <u>N</u>	<u>V</u> LANs	CONTROLLE	R W <u>I</u> RELESS	<u>s</u>	ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	:	
Security	Acc	ess Cor	ntrol L	ists > Edit									
<ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> <li>DNS</li> <li>Downloaded AVP</li> </ul>	Gene Acces Deny Seg	eral s List Nam Counters Action	ne Sour	CMX_redin 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 /	10.48.39.100 255.255.255.25	/	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,與門戶的整合已完成,必須在WLAN上更改安全策略。

首先,進入WLANs->Edit->Layer 2->Layer 2 Security,然後在下拉選單中選擇None,因此禁用 Layer 2 Security。然後,在同一安全頁籤中,更改為第3層。在第3層安全下拉選單中,選擇Web策 略,然後選擇Passthrough。在預先驗證ACL中,選擇先前設定的IPv4 ACL,將其繫結到必須提供 SMS驗證的各個WLAN。必須啟用Over-ride Global Config選項,且Web Auth型別必須為 External(重定向到外部伺服器),因此客戶端可以重定向到CMX服務。URL必須與CMX SMS身份 驗證門戶相同,格式為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 <u>W</u> LANS <u>C</u> ONTROLLER WIRELESS <u>S</u> ECURITY MANAGEMENT C <u>O</u> MMANDS HELP <u>F</u> EEDBACK
WLANe	General Security QoS Policy-Mapping Advanced
WLANS	Layer 2 Layer 3 AAA Servers
VLANs	Laver 3 Security Web Policy
Advanced	Captive Network Assistant Bypass None 📀
	Authentication     Passthrough
	Conditional Web Redirect
	On MAC Filter failure <sup>10</sup>
	Web policy done locally on Apwarning
	Preauthentication ACL       IPv4       CMX_redirect       IPv6       None       WebAuth FlexAcl       None       IPv6         Qr Code Scanning       Email Input         Sleeping Cliept       Enable
	Override Global Config <sup>20</sup>
	Web Auth type     External(Re-direct to external server)       Redirect URL     http://10.48.39.100/visitor/login

#### B.特維利奧

CMX為文<u>本消</u>息服務提供了Twilio整合。在Twilio上的帳戶配置正確後提供憑據。需要帳戶SID和身 份驗證令牌。

Twilio有自己的配置要求,在設定服務的過程中記錄這些要求。在與CMX整合之前,可以對Twilio服 務進行測試,即在將其與CMX結合使用之前,可以檢測到與Twilio設定相關的問題。

⊕ tw	ilio				DOCS			
	∨ s	ettings /		UPGRADE	, <b>O</b> Go to	¢	?	ŝ
ଇ	Dashboard							
Ģ	Billing	Two-Factor Authentication						
	Usage	Add an extra layer of protection to your account, with	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 as	k for verification code every 30 days					
	Manage Users	O EVERY LOG-IN We'll always ask for a verification co	de					
	User Settings							
	Doer Prome	API Credentials						
	Upgrade	LIVE Credentials	Learn about REST API Credentials 7	TEST Credentials	<u>Learn ab</u>	out Test Cr	edentials	2 71
		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		Vera Mission and a second				
		Keep this somewhere safe and secure		Keep this somewhere sale and secure				

### C. CMX配置

必須將控制器正確新增到CMX中,並從Prime基礎設施匯出對映。

#### • SMS註冊頁面

註冊門戶有一個預設模板。選擇CONNECT&ENGAGE->Library(庫)即可找到門戶。如果需要模板,請在下拉選單中選擇「模板」。

若要將Twilio與門戶整合,請轉到Twilio配置並提供帳戶ID和身份驗證令牌。如果整合成功,將彈出

Twilio帳戶中使用的編號。

cisco 10.3.0-62		OETECT & LOCATE	ANALYTICS		CT Ge	<b>Ø</b> MANAGE	SYSTEM			Î	admin +
									Connect Experiences		
Login Page 🖌 💊	Please enter your number to get Wi-Fi Have SMS Code?	2	English	•	0	CONTENT Have SMS CC Enter Twilin Accco Auth From Norm	BACKGROUND SMS Code? ode Input Placeholder SMS Code? o Configuration 0 0 0 AC3132a0b6 1 AC3132a0b6 1 AC3132a0	THEMES LANGU	AGES 3dbd	tional 🕆	EDIT

#### 通過社交網路帳戶進行身份驗證

使用社交網路帳戶驗證客戶端需要網路管理員在CMX上新增有效的Facebook APP識別符號。

A. WLC配置

在WLC端,將同時配置SSID和ACL。AP應連線到控制器且處於RUN狀態。

1. ACL

由於此處我們使用HTTPS作為驗證方式,因此必須在WLC上設定允許HTTPS流量的ACL。要配置 ACL,請轉至Security->Access Control Lists->Add New Rule。

CMX IP必須用於允許WLC和CMX之間的HTTPS流量。(在本例中,CMX ip為10.48.39.100)

CISCO	MON	ITOR M	(LANs		LER	WIRELESS	<u>S</u> I	ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK		
Security	Acc	ess Cor	ntrol Li	sts > Ed	it									
<ul> <li>AAA</li> <li>General</li> <li>RADIUS         <ul> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> <li>DNS</li> </ul> </li> </ul>	Geno Acces Deny	<b>eral</b> s List Nam Counters	e	CMX_Au	th									
Downloaded AVP TACACS+	Seq	Action	Sourc	e IP/Mask	D	Destination P/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	/	тср	HTTPS	Any	Any	Any	0	
MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	2	Permit	0.0.0.0	0	/ 1	0.48.39.100 55.255.255.255	/	ТСР	Any	HTTPS	Any	Any	0	
Local EAP														

還必須使用帶有Facebook URL的DNS ACL。為此,請在Security -> Access Control Lists中查詢先 前配置的ACL條目(本例中為CMX\_Auth),並將滑鼠移動到條目末尾的藍色箭頭上,然後選擇 Add-Remove URL。然後,在URL字串名稱和新增上鍵入Facebook的URL。

،،ا،،،ا،، cısco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLLE	R W <u>I</u> RELESS <u>S</u> ECURITY	M <u>a</u> nagement C <u>o</u> mmands	HELP <u>F</u> EEDBACK	
Security	ACL > CMX_Auth > URL Lis	t			
<ul> <li>▼ AAA</li> <li>General</li> <li>▼ RADIUS</li> <li>Authentication</li> </ul>	URL String Name		Add		
Accounting Fallback	facebook.com				
DNS	m.facebook.com				
<ul> <li>TACACS+</li> <li>LDAP</li> </ul>	fbcdn.net				

## 2. WLAN

安全策略更改以使註冊生效,需要對WLAN進行特定配置。

與之前的SMS註冊一樣,首先進入WLAN -> Edit -> Layer 2 -> Layer 2 Security,然後在下拉選單 中選擇None,這樣將禁用Layer 2 Security。在同一個「安全」頁籤中,更改為「第3層」。在「第 3層安全」下拉選單中,選擇「Web策略」,然後選擇「傳遞」。在預先驗證ACL中,選擇先前設定 的IPv4 ACL,將其繫結到必須提供透過Facebook驗證的各個WLAN。必須啟用Over-ride Global Config選項,且Web Auth型別必須為External(重定向到外部伺服器),因此客戶端可以重定向到 CMX服務。請注意,這次的URL必須採用以下格式https://<CMX-IP>/visitor/login。

- ahaha	Sa <u>v</u> e Configuration   <u>P</u> ing   Logout   <u>R</u> efresh
cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLLER 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
WLANs	WLANs > Edit 'cmxFW' < Back Apply
WLANs WLANs	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 2 Security  None MAC Filtering? Fast Transition Fast Transition Disable
	Saye Configuration Ping Logout Refresh
CISCO 🖻	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs V	WLANs > Edit 'Facebook' < Back Apply
WLANS WLANS	WLANs > Edit     'Facebook'     < Back     Apply       General     Security     QoS     Policy-Mapping     Advanced
WLANS WLANS WLANS Advanced	WLANs > Edit     'Facebook'     < Back     Apply       General     Security     QoS     Policy-Mapping     Advanced       Layer 2     Layer 3     AAA Servers
WLANS WLANS WLANS Advanced	WLANs > Edit     'Facebook'     < Back     Apply       General     Security     QoS     Policy-Mapping     Advanced       Layer 2     Layer 3     AAA Servers       Layer 3 Security ½     Web Policy ‡
WLANS WLANS WLANS Advanced	General     Security     QoS     Policy-Mapping     Advanced       Layer 2     Layer 3     AAA Servers       Layer 3 Security 1     Web Policy 2       Authentication
WLANS WLANS WLANS Advanced	WLANs > Edit 'Facebook' < Back Apply     General Security QoS Policy-Mapping Advanced     Layer 2 Layer 3     Layer 3 AAA Servers     Layer 3 Security 1 Web Policy 2     Authentication   Passthrough
WLANS V VLANS WLANS Advanced	General     Security     QoS     Policy-Mapping     Advanced       Layer 2     Layer 3     AAA Servers       Layer 3 Security 1     Web Policy 2       Authentication       Passthrough       Conditional Web Redirect       Seleta Pace Web Redirect
WLANS WLANS WLANS Advanced	WLANS > Edit 'Facebook'     < Back Apply       General     Security     QoS     Policy-Mapping     Advanced       Layer 2     Layer 3     AAA Servers       Layer 3 Security 1     Web Policy ‡       Authentication       • Passthrough       Conditional Web Redirect       • Splash Page Web Redirect       • On MAC Filter failure <sup>10</sup>
WLANS WLANS WLANS Advanced	General     Security     QoS     Policy-Mapping     Advanced       Layer 2     Layer 3     AAA Servers       Layer 3 Security 4     Web Policy 2       Authentication       Passtbrough       Conditional Web Redirect       Splash Page Web Redirect       On MAC Filter failure <sup>£9</sup> Preauthentication ACL     IPv4       CMX_Auth     IPv6       None 2
WLANS V WLANS WLANS Advanced	General     Security     QoS     Policy-Mapping     Advanced       Layer 2     Layer 3     AAA Servers       Layer 3 Security 1     Web Policy ‡       Authentication       Passthrough       Conditional Web Redirect       Splash Page Web Redirect       On MAC Filter failure 12       Presuthentication ACL       IPv4       CMX_Auth     ‡       IPv6       None ‡
WLANS WLANS WLANS Advanced	WLANS > Edit     'Facebook'     < Back
WLANS WLANS WLANS Advanced	WLANS > Edit 'Facebook'     < Back Apply       General Security QoS Policy-Mapping 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>1,0</sup> Preauthentication ACL       IPv4 CMX_Auth ‡ IPv6 None ‡ WebAuth FlexAcl None ‡       Email Input       Sleeping Client _ Enable       Over-ride Global Config <sup>2</sup> 2 Enable
WLANS WLANS WLANS Advanced	WLANS > Edit 'Facebook'     < Back
WLANS WLANS WLANS Advanced	WLANS > Edit 'Facebook'     < Back Apply         General Security QoS Policy-Mapping Advanced         Layer 2 Layer 3 AAA Servers         Layer 3 Security 1 Web Policy ?         Authentication         Passthrough         Conditional Web Redirect         Splash Page Web Redirect         On MAC Filter failure <sup>4,9</sup> Preauthentication ACL IPv4 (MX_Auth ?) IPv6 None ? WebAuth FlexAcl None ?       Email Input   Sleeping Client         Soleping Client         Over-ride Global Config <sup>2</sup> Web Auth type     External(Re-direct to external server) ? URL https://10. /visitor/login

#### B.面向開發者的Facebook

對於Facebook和CMX的整合,需要使用Facebook應用來在兩部分之間交換正確的令牌。

在「應用設定」中,確保啟用客戶端OAuth登入和Web OAuth登入。此外,請驗證有效的OAuth重 定向URI是否具有**https**://<CMX-IP>/visitor/login格式的CMX URL。

f ≡ App Dashboard		Docs Tools Support Q Search developers.facebook.com
Catarina's first app	APP ID:	ON 🔵 Status: Live 🥕 View Analytics
<ul> <li>♣ Dashboard</li> <li>♣ Settings</li> <li>➡ Roles</li> <li>▲ Alerts</li> <li>&gt; App Review</li> <li>PRODUCTS</li> <li>● Facebook Login</li> <li>Settings</li> <li>Quickstart</li> <li>※ Activity Log</li> </ul>	In March, we're making a security update to your app settings that redirect URIs field below. This update comes in response to malicic app or website by requiring a new strict mode for redirect URIs. Least app or website by requiring a new strict mode for redirect URIs. Least Client OAuth Settings Client OAuth Settings Client OAuth Login Enables the standard OAuth client token flow. Secure your application down which token redirect URIs are allowed with the options below. Web OAuth Login Enables web-based OAuth client login. (?) Web OAuth Login Enables browser Control redirect un for OAuth client login. (?) Valid OAuth redirect URIs Into:://10.48.62.177/visitor/login >> Login from Devices Enables browser Coater Login flow for devices like a smart TV 171	will invalidate calls from URIs not listed in the Valid OAuth         loss activity we saw on our platform, and we want to protect your         arm More         on and prevent abuse by locking         Disable globally if not used. [9]         Proce Web OAuth Reauthentication         We Receive prevent species to enter their facebook password in order to log in on the web. [9]         We Use Strict Mode for Reduitet URIs         Only allow redirects that use the Facebook SDA or that exactly match the Valebook OAuth Reduct URIs. Strongly recommended. [7]

要發佈該應用並準備好與CMX整合,必須將其公開。要執行此操作,請轉到「應用審閱 — >公開 <App-Name>?」並將狀態更改為「是」。

f = App Dashboard				Docs	s	Tools	s Support	Q Sear	ch developers.facebook.com
	🔯 Catarina's first app	•	APP ID:		6	DN O	Status: Live	→ <sup>■</sup> View	Analytics
	# Dashboard								
	貸 Settings		Make Catarina's first app public?						
	🖾 Roles	+	Yes Your app is currently live and available to the public.						
	Alerts								
	<ul> <li>App Review</li> </ul>								
			Submit Itoma for Approval						
	PRODUCTS 🕂		Submit items for Approval						
	Facebook Login		Some Facebook integrations require approval before public usage.	Start a Submission					
			Before submitting your app for review, please consult our Platform						
	i Activity Log		Policy and Review Guidennes.						

#### C. CMX配置

必須將控制器正確新增到CMX中,並從Prime基礎設施匯出對映。

#### • 註冊頁面

要在CMX上建立註冊頁面,應執行與之前為SMS註冊頁面建立頁面相同的步驟。選擇 CONNECT&ENGAGE->庫,可通過選擇下拉選單中的「模板」找到準備編輯的模板門戶。

通過Facebook憑據註冊需要門戶具有社交帳戶連線。若要從頭開始操作,在建立自定義門戶時,請 轉到CONTENT->Common Elements->Social Auth,然後選擇Facebook。然後插入從Facebook獲 得的應用名稱和應用ID(金鑰)。

cisco 10.31.55	DETECT & LOCATE	ANALYTICS	CONNECT & ENGAGE	<b>¢</b> Manage	SYSTEM			i	admin -
						Dashboard	Connect Experiences	Policy Plans Library	- Settings -
RegistrationPage 🖋							Live View C	Portals Library	Save
Login Page 👻 🗢		English	•	CONTENT	BACKGROUND	THEMES LANGUAGES			EDIT
Logis to connect to wife				Social I	ogin			Remove eleme	ent
				Depe	nds on Terms and C	Conditions			- 11
f				- Content					
				🗹 F	cebook 🔗   Scope:	Basic Profile -			- 11
				Ca	arina's first app	▼ Key:			- 11
				0 0	reate new				

### 通過自定義門戶進行身份驗證

使用自定義門戶對客戶端進行身份驗證類似於配置外部Web身份驗證。重新導向將完成至CMX上託 管的自定義門戶。

#### A. WLC配置

在WLC端,將同時配置SSID和ACL。AP應連線到控制器且處於RUN狀態。

1. ACL

由於此處我們使用HTTPS作為驗證方式,因此必須在WLC上設定允許HTTPS流量的ACL。要配置 ACL,請轉至Security->Access Control Lists->Add New Rule。

CMX IP必須用於允許WLC和CMX之間的HTTPS流量。(在本示例中,CMX IP為10.48.71.122)。

註:在CMX CLI上發出「cmxctl node sslmode enable」命令,確保在CMX上啟用ssl。

،، ،،، ،، cısco	MONITO	or <u>w</u> l	ANs	CONTROLLE	R WIRELESS	SECURITY	MANAGEMENT	COMMANDS	5 HELP	FEEDBACK					
Security	Acces	s Cont	rol Li	sts > Edit											
<ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>Authentication</li> </ul>	Genera	al ist Name			2										
Accounting Fallback DNS Downloaded AVP	Deny Co	unters	Sourc	0 e IP/Mask	-	Destinatio	on IP/Mask	Р	rotocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
▶ TACACS+	<u>1</u> P	ermit	10.48.	71.122	255.255.255.255	0.0.0.0	/ 0.0.0.0	т	CP	HTTPS	Any	Any	Any	0	
LDAP Local Net Users MAC Filtering Disabled Clients	<u>2</u> P	ermit	0.0.0.0	ο ,	0.0.0.0	10.48.71.1	22 / 255.255	.255.255 T	CP	Any	HTTPS	Any	Any	0	

2. WLAN

安全策略更改以使註冊生效,需要對WLAN進行特定配置。

正如之前在SMS和Social Network Registration中所做的那樣,首先進入WLANs->Edit->Layer 2->Layer 2 Security,然後在下拉選單中選擇None,因此禁用第2層安全。在同一個「安全」頁籤中 ,更改為「第3層」。在「第3層安全」下拉選單中,選擇「Web策略」,然後選擇「傳遞」。在預 先驗證ACL中,選擇先前設定的IPv4 ACL(在本範例中命名為CMX\_HTTPS),並將其繫結到各自 的WLAN。必須啟用Over-ride Global Config選項,且Web Auth型別必須為External(重定向到外部 伺服器),因此客戶端可以重定向到CMX服務。請注意,這次的URL必須採用以下格式 https://<CMX-IP>/visitor/login。

راریاری cisco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	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		

uluili. 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>12</sup> Web policy done locally on APwarning Preauthentication ACL IPv4 CMX_HTTPS ‡ IPv6 None ‡ WebAuth FlexAcl None ‡ Qr Code Scanning Email Input Sleeping Client Enable Override Global Config <sup>22</sup> € Enable Web Auth type External(Re-direct to external server) ‡ Redirect URL https://10.48.71.122/visitor/login	

### C. CMX配置

必須將控制器正確新增到CMX中,並從Prime基礎設施匯出對映。

#### • 註冊頁面

要在CMX上建立註冊頁,與以前為其他身份驗證方法建立該頁時執行的步驟相同。選擇「連線&參 與」—>「庫」,可通過選擇下拉選單中的「模板」找到準備編輯的模板門戶。

用於正常註冊的門戶可以從頭開始(選擇「自定義」),也可以從CMX庫上提供的「登錄檔」模板 中進行修改。



# 驗證

# WLC

若要確認使用者是否已在系統上成功通過驗證,請在WLC GUI上,前往MONITOR->Clients,並在 清單中搜尋使用者端的MAC位址:

cisco	MONITOR WLANS	CONTROLLER WIREL	ESS SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK						Saye	Configur	ation P	ng Logou	Home
Monitor	Clients															Entries 1	- 1 of 1
Summary Access Points Circo Close Air	Current Filter Non	e	[Change_Filter]	[Clear Filter]													
<ul> <li>Statistics</li> </ul>	Client MAC Addr	IP Address(Ipv4/Ipv6	•)	AP N	iame			WLAN Profile	WLAN SSID	User Name	Protocol	Status	Auth	Port	Slot Id	Tunnel	Fastland
> CDP	<u>f4:</u>	64.		AP3-	37021			Facebook	WiFi_Facebook	Unknown	802.11ac	Associated	Yes	1	1	No	No
<ul> <li>Rogues</li> <li>Clients</li> <li>Sleeping Clients</li> <li>Multicast</li> <li>Applications</li> <li>Local Profiling</li> </ul>																	
	Foot Notes																
	RLAN Clients connected	to AP702w, will not show 0	Sient IP details.														

## 按一下客戶端的MAC地址,並在詳細資訊中確認客戶端策略管理器狀態為運行狀態:

սիսիս						
cisco	MONITOR WLANS	ONTROLLER WIRELESS	SECURITY M	ANAGEMENT	COMMANDS HELP	FEEDBACK
Monitor	Clients > Detail					
Summary  Access Points  Cisco CleanAir	Max Number of Records General AVC Sta	tistics	s			
Statistics	<b>Client Properties</b>				AP Properties	
h Roques	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					WLAN Profile	Facebook
Local Profiling					WLAN SSID	WiFi Facebook
Local Profiling					Data Switching	Central
					Authentication	Central
					Status	Associated
					Association ID	1
				11	802.11 Authentication	Open System
	Client Type	Regular			Reason Code	1
	Client Tunnel Type	Unavailable			Status Code	0
	User Name				CE Pollable	Not Implemented
	Port Number	1			CE Poll Request	Not Implemented
	Interface	internet_access			CF Poli Request	Not Implemented
	VLAN ID	129			Short Preamble	Not Implemented
	Quarantine VLAN ID	0			PBCC	Not Implemented
	CCX Version	CCXv4			Channel Agility	Not Implemented
	E2E Version	E2Ev1			Timeout	1800
	Mobility Role	Local			WEP State	WEP Disable
	Mobility Peer IP	N/A			Allowed (URL)IP add	dress
	Address Mobility Move Count	0				
	Policy Manager State	RUN	1			
	Management Frame	No				
	Protection	71				
	Oprime (Sec)	71				
	Current TxRateSet	m8 ss2				

CMX

通過開啟CONNECT&ENGAGE頁籤,可以驗證在CMX上驗證的使用者數:

ultulu cux CISCO 1831-36	DETECT & LOCATE	ANALYTICS	CONNECT & ENGAGE	<b>Ø</b> MANAGE	SYSTEM					<b>()</b>	admin +
							Dashboard	Connect Experiences	Policy Plans	Library 🗸	Settings 🗸
♥ Location		0	nterval			📽 Visitor Search					
Global • No locations available	•	La	st 7 Days		•	Please enter search path	ern	- C			
Global Dashboard											
Today at a Glance - Feb 22, 2018											
<b>203</b> 1			Vi	sitor 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>1</b> 7%		0	(	C	
Column 👻			(i) Ar	ea	•						<b>i</b>
5 New and Repeat Visitors	Netwo										

要檢查使用者詳細資訊,請在同一頁籤右上角按一下Visitor Search:

							<b>9</b>	<b>&amp;</b> 🗢	¢\$	å								
Visitor Search  Visitor Search  Please enter search query  C Download as CSV 4  C Download as CSV 4  C Download as CSV 4  C Do					×	Plans   Library	-    i											
Q Location	Please enter search o	query			۹	Downloa	id as CSV 🛓											
Global	Use Search Filter	Options																
Global Dash	Search on 19 of 19 selected								rom 02/21/2018 3:41 PM	л		To 02/22	2018 3:41 PM	Л				
Today at a Glance	Export Preview (	Up to 100 i	results 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	RegistrationPage	CustomPortal	REGISTRATION	PC	Windows 10	0	0	Catarina Silva	female	0	
Column	Previous 1	Next																(
	Showing 1 of 1																	
4																		
of Visito									C Rytes									
2									Netwo									

# 疑難排解

為了檢查元素之間的互動流,可以在WLC中進行一些調試:

>debug client<MAC addr1> <MAC addr2> (輸入一個或多個客戶端的MAC地址)

>debug web-auth redirect enable mac <MAC addr> ( 輸入web-auth客戶端的MAC地址 )

>debug web-auth webportal-server enable

>debug aaa all enable

此調試允許進行故障排除,如果需要,可以使用某些資料包捕獲作為補充。