# CMXコネクテッドエクスペリエンス – ソーシャ ル、SMS、およびカスタムポータル登録の設定 例

# 内容

概要
 前提条件
 要件
 使用するコンポーネント
 設定
 ネットワーク図
 設定
 SMSによる認証
 ソーシャルネットワークアカウントによる認証
 カスタムポータルによる認証
 確認
 トラブルシュート

# 概要

このドキュメントの目的は、Connected Mobile eXperience(CMX)のゲストポータル設定を介して クライアント登録を行うことをネットワーク管理者に促すことです。

CMXを使用すると、ユーザはソーシャル登録ログイン、SMS、およびカスタムポータルを使用してネットワークに登録および認証できます。このドキュメントでは、ワイヤレスLANコントローラ(WLC)とCMXの設定手順の概要を示します。

# 前提条件

# 要件

CMXは基本設定で正しく設定されている必要があります。

Prime Infrastructureからマップをエクスポートすることはオプションです。

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

• Cisco Wireless Controllerバージョン8.2.166.0、8.5.110.0、および8.5.135.0。

• Cisco Connected Mobile Experiencesバージョン10.3.0-62、10.3.1-35。10.4.1-22

# ネットワーク図

このドキュメントでは、CMXを使用してユーザ/クライアントをワイヤレスネットワークに認証する2つの異なる方法について説明します。

まず、ソーシャルネットワークアカウントを使用した認証の設定について説明し、次にSMSを使用した認証について説明します。

両方のシナリオで、クライアントはCMXによる認証を使用してSSIDへの登録を試みます。

WLCはHTTPトラフィックをCMXにリダイレクトします。ここで、ユーザは認証を求められます。CMXには、ソーシャルアカウントとSMSの両方を通じて、クライアントの登録に使用するポータルのセットアップが含まれています。

次に、登録プロセスのフローについて説明します。

- 1. クライアントはSSIDへの参加を試み、ブラウザを開きます。
- 要求されたサイトにアクセスする代わりに、WLCによってゲストポータルにリダイレクトされます。
- 3. クライアントは自分のクレデンシャルを提供し、認証を試みます。
- 4. CMXは認証プロセスを扱います。
- 5. 成功すると、完全なインターネットアクセスがクライアントに提供されます。

6. クライアントは最初に要求されたサイトにリダイレクトされます。

使用されるトポロジは次のとおりです。



## 設定

#### SMSによる認証

Cisco CMXは、SMSを介したクライアント認証を可能にします。この方法では、ユーザーがシス テムに資格情報を提供できるようにHTMLページを設定する必要があります。既定のテンプレー トはCMXによってネイティブに提供され、後で編集またはカスタムのテンプレートに置き換える ことができます。

テキストメッセージサービスは、CMXと<u>Twilio</u>を統合して行われ<u>ます。Twilio</u>は、テキストメッ セージの送受信を可能にするクラウドコミュニケーションプラットフォームです。Twilioでは、ポ ータルごとに電話番号を設定できます。つまり、複数のポータルを使用する場合は、ポータルご とに1つの電話番号が必要になります。

# A. WLC の設定

WLC側では、SSIDとACLの両方が設定されます。APはコントローラに加入し、RUN状態である 必要があります。

#### 1. ACL

WLCで設定されたHTTPトラフィックを許可するACLが必要です。ACLを設定するには、 [Security] > [Access Control Lists] > [Add New Rule]の順に選択します。

使用されるIPは、CMX用に設定されたIPです。これにより、WLCとCMX間のHTTPトラフィック が許可されます。次の図は、作成されたACLを示しています。「10.48.39.100」はCMX IPアドレ スを表します。

cisco	MON	ITOR <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> <li>TACACS+</li> <li>LDAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disabled Clients</li> <li>User Login Policies</li> </ul>	Gene Acces Deny	eral s List Nan Counters	ie Sour	CMX_redire 0	Destination	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hite	
	1	Permit	0.0.0	.0 /	10.48.39.100 255.255.255.255	/ тср	Any	нттр	Any	Any	0	
	2	Permit	10.48 255.2	.39.100 / .55.255.255	0.0.0.0	/ тср	НТТР	Any	Any	Any	0	
AP Policies Password Policies												

## 2. WLAN

ポータルとの統合が完了したら、WLANのセキュリティポリシーを変更する必要があります。

まず、[WLANs] -> [Edit] -> [Layer 2] -> [Layer 2 Security]に移動し、ドロップダウンで[None]を選 択します。したがって、レイヤ2セキュリティは無効になります。次に、同じ[Security]タブで [Layer 3]に変更します。[Layer 3 Security]ドロップダウンメニューで、[Web Policy]、 [Passthrough]の順に選択します。事前認証ACLで、前に設定したIPv4 ACLを選択し、SMS認証を 提供する必要がある各WLANにバインドします。[Over-ride Global Config]オプションを有効にし 、[Web Auth type]を[External (Re-direct to external server)]に設定して、クライアントをCMXサー ビスにリダイレクトできるようにする必要があります。URLは、CMX SMS認証ポータルと同じ 形式にする必要があります。形式はhttp://<CMX-IP>/visitor/loginです。

ريانيان cısco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	Save Configuration   Ping	Logout <u>R</u> efresh
WLANs	WLANs > Edit 'cmx_sms'	< Back	Apply
<ul> <li>WLANS</li> <li>Mutans</li> <li>Advanced</li> </ul>	General     Security     QoS     Policy-Mapping     Advanced       Layer 2     Layer 3     AAA Servers       Layer 2 Security 6     None     \$       MAC Filtering 2     •       Fast Transition     •       Fast Transition     •		

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

#### バリー・トゥィリオ

CMXはテキストメ<u>ッセージ</u>サービスのTwilio統合を提供します。クレデンシャルは、Twilioのアカ ウントが正しく設定された後で提供されます。アカウントSIDと認証トークンの両方が必要です 。

Twilioには独自の設定要件があり、サービスの設定プロセスで文書化されています。CMXと統合 する前に、Twilioサービスをテストできます。Twilioのセットアップに関連する重大な問題は、 CMXで使用する前に検出できます。

(ii) tw	rilio <sup>.</sup>				DOCS	/		~						
	$\sim$ s	settings /		UPGRADE	, <b>O</b> Go to	Ö	?	ŝ						
ŵ	Dashboard													
Ģ	Billing	Two-Factor Authentication												
	Usage	Add an extra layer of protection to your account, with a verification of	dd 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 ask for verification	ONCE PER COMPUTER Trust computers and only ask for verification code every 30 days											
	Manage Users User Settings	O EVERY LOG-IN We'll always ask for a verification code	EVERY LOG-IN We'll always ask for a verification code											
	Doer Profile	API Credentials												
	Upgrade	LIVE Credentials	Learn about REST API Credentials 7	TEST Credentials	Learn abo	ut Test Cre	dential	<u>s</u> 7						
		ACCOUNT SID AC3132a0b65f9ac540318a0a576e3f3dbd Used to exercise the REST API		TEST ACCOUNT SID ACb7ec526108f80811b68c6b7b9693e69d Used to exercise the REST API										
		AUTH TOKEN O Request a Secondary Token	TEST AUTHTOKEN ③ •											
		Keep this somewhere safe and secure	Keep this somewhere safe and secure											

# C. CMXの設定

コントローラをCMXに正しく追加し、マップをPrime Infrastructureからエクスポートする必要が あります。

#### • SMS登録ページ

登録ポータルにはデフォルトテンプレートがあります。ポータルは、[CONNECT&ENGAGE] ->

[Library]を選択できます。テンプレートが必要な場合は、ドロップダウンメニューから[テンプレート(Templates)]を選択します。

Twilioをポータルと統合するには、[Twilio Configuration]に移動し、アカウントIDと認証トークン を入力します。統合が成功すると、Twilioアカウントで使用されている番号がポップアップ表示さ れます。

CISCO 10.3.0-62		DETECT & LOCATE	ANALYTICS		ECT AGE	<b>Ø</b> MANAGE	SYSTEM				Î	admin 👻
								Dashboard	Connect Experiences	Policy Plans	Library 👻	Settings 🗸
Login Page • 🔶	Please enter your number to get Wi-Fi Have SMS Code? X  Phone Number* Condition Please review and accept our Terms & Condition for access to Wi-Fi.  SUBMIT		English	•	0	CONTENT Have I SMS C( Enter I Accc Auth From Num	BACKGROUND SMS Code? SMS Code a Configuration a Configuration	THEMES LANGU	AGES		otional 🛛 🕾	ΕΟΤ

#### ソーシャルネットワークアカウントによる認証

ソーシャルネットワークアカウントを使用してクライアントを認証するには、ネットワーク管理 者がCMXに有効なFacebook APP IDを追加する必要があります。

#### A. WLCの設定

WLC側では、SSIDとACLの両方が設定されます。APはコントローラに加入し、RUN状態である 必要があります。

#### 1. ACL

ここでHTTPSを認証方式として使用しているため、HTTPSトラフィックを許可するACLを WLCで設定する必要があります。ACLを設定するには、[Security] > [Access Control Lists] > [Add New Rule]の順に選択します。

CMX IPは、WLCとCMX間のHTTPSトラフィックを許可するために使用する必要があります(この 例では、CMX ipは10.48.39.100です)。

cisco	MON	ITOR <u>w</u> i	ANs 🤇	ONTROLLER	R WIRELESS	SE	CURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK		
Security	Acc	ess Cont	rol Lis	ts > Edit									
<ul> <li>AAA         <ul> <li>General</li> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> <li>DNS</li> <li>Downloaded AVP</li> </ul> </li> <li>TACACS+</li> <li>LDAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disabled Clients</li> <li>User Login Policies</li> <li>AP Policies</li> </ul> <li>Password Policies</li>	Gene	eral s List Name		CMX_Auth									
	Deny	Counters		0	Destination								
	Seq	Action Permit	Source 10.48.39 255.255	IP/Mask 9.100 / .255.255	IP/Mask 0.0.0.0 0.0.0.0	/	Protocol TCP	Source Port	Dest Port	Any	Direction	Number of Hits	
	2	Permit	0.0.0.0 0.0.0.0	/	10.48.39.100 255.255.255.255	/	ТСР	Any	HTTPS	Any	Any	0	
Local EAP													

また、Facebook URLを含むDNS ACLも必要です。これを行うには、[Security] -> [Access Control Lists]で、以前に設定したACL(この場合はCMX\_Auth)のエントリを検索し、エントリの 最後にある青い矢印にマウスを移動して、[Add-Remove URL]を選択します。その後、[URL String Name]と[Add]にFacebookのURLを入力します。

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

# 2. WLAN

登録のセキュリティポリシーが変更されると、WLAN上で特定の設定を行う必要があります。

SMSの登録に関して以前に行ったように、最初に[WLANs] -> [Edit] -> [Layer 2] -> [Layer 2 Security]に移動し、ドロップダウンで[None]を選択したため、レイヤ2セキュリティは無効になり ます。同じ[Security]タブで、[Layer 3]に変更します。[Layer 3 Security]ドロップダウンメニュー で、[Web Policy]、[Passthrough]の順に選択します。事前認証ACLで、前に設定したIPv4 ACLを 選択し、Facebook経由の認証を提供する必要がある各WLANにバインドします。[Over-ride Global Config]オプションを有効にし、[Web Auth type]を[External (Re-direct to external server)]に設定して、クライアントをCMXサービスにリダイレクトできるようにする必要があり ます。この場合、URLはhttps://<CMX-IP>/visitor/loginの形式である必要があります。

- ahaha	S	a <u>v</u> e Configuration   <u>P</u> ing   Logout   <u>R</u> efresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT	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 Security None MAC Filtering Fast Transition Fast Transition Disable	

									Save Configura	ation   <u>P</u> ing	Logout <u>R</u> efree
cisco	<u>M</u> ONITOR <u>V</u>	VLANs <u>C</u> ON	TROLLER W	<u>i</u> reless <u>s</u> ecur	ITY M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK			n <u>H</u> om
WLANs	WLANs > E	dit 'Faceb	ook'							< Back	Apply
VLANs	General	Security	QoS Po	licy-Mapping	Advanced						
Advanced	Layer 2	Layer 3	AAA Serve	rs							
	Layer 3 Auth Pass Cone Spla On N Preauth En Sleeping Over-ric Web Au URL	Security 1 W entication through ditional Web Re sh Page Web R MAC Filter failur entication ACL nail Input g Client C En de Global Config th type ttps://10.	eb Policy ‡ direct edirect e10 IPv4 CM able 20 V Enab Extern /visitor/log	IX_Auth + IPv le hal(Re-direct to exte	6 None 🕈 WebAuth	n FlexAcl None ‡	)				

# B. Facebook for Developers

FacebookとCMXの統合では、2つのパーツ間で適切なトークンを交換するためにFacebookアプリが必要です。

アプリを作<u>成するには、Facebook for Developers</u>に移動します。サービスを統合するためのアプ リケーションの設定要件がいくつかあります。

[App Settings]で、[Client OAuth Login]と[Web OAuth Login]が有効になっていることを確認しま す。また、有効なOAuthリダイレクトURIが**https**:/<CMX-IP>/visitor/login形式のCMX URLである ことを確認します。

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>Settings</li> <li>Alerts</li> <li>App Review</li> <li>PRODUCTS (*)</li> <li>Facebook Login Settings</li> <li>Quickstart</li> <li>Activity Log</li> </ul>	In March, we're making a security update to your app settings that will invalidate calls from URIs not listed in the Valid OAuth redirect URIs field below. This update comes in response to malicious activity we saw on our platform, and we want to protect your apport website by requiring a new strict mode for redirect URIs. Learn More  Client OAuth Settings  Client OAuth Login Chieft Client Count network from Secure your application and prevent abuse by locking down which been redirect URIs and aved with the doors below. Disable globably if not used. Tri Web OAuth Login Chieft Secure Your Chieft Client Count Login Chieft Secure Your application and prevent abuse by locking down which been redirect URIs and aved with the colors below. Disable globably if not used. Tri Chieft Secure Your application and prevent abuse by locking down which been redirect URIs and aved with the colors below. Disable globably if not used. Tri Chieft Secure Your application and prevent abuse by locking down which been redirect URIs and web with the colors below. Disable globably if not used. Tri Chieft Secure Your Application and prevent abuse by locking down which been redirect URIs and web with the colors below. Disable globably if not used. Tri Chieft Secure Your Application and prevent abuse by locking down which been redirect URIs to play and the redirect URIs to play abor redirect that use the Secure Your Your Your Your Your Your Your Your	
	Valid OAuth redirect URIs https://10.48.62.177/visitor/login ×	
	No Cognies the Out-cleant login flow for devices like a smart TV (?)	

アプリを公開し、CMXと統合できるようにするためには、公開する必要があります。そのために は、App Review->Make <App-Name> public?状態を[Yes]に変更します。

f = App Dashboard			Docs Tools Support	Q Search developers.facebook.com
	🔯 Catarina's first app 🛛 🔻	APP ID:	ON Status: Live	View Analytics
		Make Catarina's first app public?		
	PRODUCTS ↔ Sacebook Login → E Activity Log	Submit Items for Approval Some Facebook integrations require approval before public usage. Before submitting your app for review, please consult our Platform Policy and Review Guidelines.	Start a Submission	

# C. CMXの設定

コントローラをCMXに正しく追加し、マップをPrime Infrastructureからエクスポートする必要があります。

•登録ページ

CMXで登録ページを作成するには、SMS登録ページのページを作成する手順と同じものを実行す る必要があります。CONNECT&ENGAGE->ライブラリを選択すると、ドロップダウンメニュー から[テンプレート]を選択して編集できます。

Facebook資格情報を使用して登録するには、ポータルでソーシャルアカウントに接続する必要が あります。これを最初から行うには、カスタムポータルを作成するときに、[CONTENT] -> [Common Elements] -> [Social Auth]に移動し、[Facebook]を選択します。次に、Facebookから取 得したアプリ名とアプリID(キー)を挿入します。

cisco 10.3.1-35		DETECT & LOCATE	ANALYTICS	CONNECT & ENGAGE	<b>¢</b> Manage	SYSTEM			•	admin -
							Dashboard	Connect Experiences	Policy Plans Library -	Settings -
RegistrationPage &								Live View De	Portals Library	Save
Login Page 👻 🔹			English	• 6	CONTENT	BACKGROUND	THEMES LANGUAGES			EDIT
	Legis to segreest to will				Social	Login			Remove element	
	Edgin to connect to win.				Dep	ends on Terms and C	Conditions			- 11
					- Content					- 11
					🔽 F	acebook 🔗   Scope:	Basic Profile •			11
					Ci	tarina's first app	• Key:			111
					0	Create new				

#### カスタムポータルによる認証

カスタムポータルを使用したクライアントの認証は、外部Web認証の設定に似ています。リダイ レクトは、CMXでホストされるカスタマイズされたポータルに対して実行されます。

#### A. WLCの設定

WLC側では、SSIDとACLの両方が設定されます。APはコントローラに加入し、RUN状態である 必要があります。

#### 1. ACL

ここでHTTPSを認証方式として使用しているため、HTTPSトラフィックを許可するACLを WLCで設定する必要があります。ACLを設定するには、[Security] > [Access Control Lists] > [Add New Rule]に移動します。

CMX IPは、WLCとCMXの間のHTTPSトラフィックを許可するために使用する必要があります(こ

**注**:CMX CLIで「cmxctl node sslmode enable」コマンドを発行して、CMXでsslを有効にし てください。

ာါကျက cisco	MONI	TOR	<u>W</u> LANs	CONTROLL	ER WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMAND	s he <u>l</u> p	FEEDBACK					
curity	Acce	ess Co	ontrol L	ists > Edit											
A Seneral (ADIUS Authentication Accounting Fallback	Gene Access Deny (	e <b>ral</b> 5 List Na Counter	ime s	CMX_HTT 0	PS										
DNS Downloaded AVP	Seq	Action	Sour	ce IP/Mask		Destinatio	on IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
CACS+	1	Permit	10.48	8.71.122	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	1	TCP	HTTPS	Any	Any	Any	0	
cal Net Users C Filtering sabled Clients	2	Permit	0.0.0	.0	/ 0.0.0.0	10.48.71.1	22 / 255.255	5.255.255	ГСР	Any	HTTPS	Any	Any	0	

2. WLAN

登録のセキュリティポリシーが変更されると、WLAN上で特定の設定を行う必要があります。

SMSとソーシャルネットワークの登録に関して以前に行ったように、最初に[WLANs] -> [Edit] -> [Layer 2] -> [Layer 2 Security]に移動し、ドロップダウンで[None]を選択すると、レイヤ2セキュ リティは無効になります。同じ[Security]タブで、[Layer 3]に変更します。[Layer 3 Security]ドロ ップダウンメニューで、[Web Policy]、[Passthrough]の順に選択します。事前認証ACLで、前に 設定したIPv4 ACL(この例ではCMX\_HTTPSという名前)を選択し、対応するWLANにバインド します。[Over-ride Global Config]オプションを有効にし、[Web Auth type]を[External (Re-direct to external server)]に設定して、クライアントをCMXサービスにリダイレクトできるようにする必 要があります。この場合、URLはhttps://<CMX-IP>/visitor/loginの形式である必要があります。

iliilii cisco	<u>M</u> ONITOR <u>W</u> LAN	5 <u>C</u> ONTROLLER	W <u>I</u> RELESS <u>S</u> EC	CURITY M <u>a</u> nagemen
WLANs	WLANs > Edit	'cmx_login'		
<ul> <li>WLANS</li> <li>Advanced</li> </ul>	General Sec Layer 2 La Layer 2 Secur Fast Transition Fast Transition Lobby Admin Co Lobby Admin	curity QoS ayer 3 AAA S ity <sup>6</sup> None MAC Filtering Dis onfiguration Access	Policy-Mapping	Advanced

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'cmx_login'
VLANs WLANs	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 AP <u>warning</u> 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の設定

コントローラをCMXに正しく追加し、マップをPrime Infrastructureからエクスポートする必要があります。

•登録ページ

CMXで登録ページを作成するには、他の認証方法のページを作成した手順と同じです。 [CONNECT&ENGAGE->ライブラリ]を選択すると、編集できるテンプレートポータルがドロップ ダウンメニューから[テンプレート]を選択できます。

通常の登録のためのポータルは、最初から行うか([カスタム]を選択)、またはCMXライブラリ で利用可能な[登録フォーム]テンプレートから適用できます。

cisco 1041-22		DETECT ANALYTICS	<del>ç</del> connect	¢8 MANA	GE SYSTEN	и				6	admin +
								Dashboard	Connect Experiences	Policy Plans Library	• Settings •
Login_Page &									Live View	Delete Portals Library	Save
Login Page 👻 🗢		English	• •	Θ	CONTENT	CKGROUND THEMES	LANGUAGES				
	Complete registration to enhand to wife				O To add an elem	ment, simply drag & drop it to t	he canvas or click on it!				
	Complete registration to ontotard to with.			•	Common element	ts					
	Name* 📀 Email				image Element	T Text Element		Social Auth	Terms & Conditions	image & Text	
	SUBMIT					(≣±) Contact us	† ÷ Spacer		Menu	✓ == Opt-out	
					Advertisement ele	ements					
					image Side	r External Content					



ユーザがシステムで正常に認証されたかどうかを確認するには、WLC GUIで[MONITOR] -> [Clients]に移動し、リストでクライアントのMACアドレスを検索します。

սիսիս						Save Configuration	ing   Logout   <u>R</u> efresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY	MANAGEMENT COMMANDS HELP FEEDBACK					<mark>n H</mark> ome
Monitor	Clients						Entries 1 - 1 of 1
Summary Access Points	Current Filter None [Change Filter]	Clear Filter)					
Cisco CleanAir							
Statistics	Client MAC Addr IP Address(Ipv4/Ipv6)	AP Name	WLAN Profile WLAN SS	ID User Name	Protocol Status	Auth Port Slot Id	Tunnel Fastiane
> CDP	<u>[4:</u> 64.	AP3-37021	Facebook WiFi_Faceb	book Unknown	802.11ac Associated	Yes 1 1	No No
Rogues							
Clients							
Sleeping Clients							
Multicast							
Applications							
Local Profiling							
	Foot Notes						
	RLAN Clients connected to AP702w, will not show Client IP details.						

クライアントのMACアドレスをクリックし、詳細で、クライアントのポリシーマネージャの状態 がRUN状態であることを確認します。

սիսիս							Save Configuration Ping Logo
	R WLANS CO	ONTROLLER WIRELESS SECUI	UTY MANAGEMENT	COMMANDS HELP !	FEEDBACK		
itor Clients	> Detail						< Back Link Test Re
seco CleanAir Max Num	al AVC Stat	10 2 Clear AVC Stats					
Client	Properties			AP Properties			
MAC A	Address	f4:		AP Address	78:		
IPv4 A	Address	64.		AP Name	AP3-3702I		
IPv6 /	Address	fe80:		AP Type	802.11ac		
rast				AP radio slot Id	1		
cations				WLAN Profile	Facebook		
Profiling				WLAN SSID	WiFi_Facebook		
				Data Switching	Central		
				Authentication	Central		
				Status	Associated		
				Association ID	1		
			h	802.11 Authentication	Open System		
Client	t Type	Regular		Reason Code	1		
Client	t Tunnel Type	Unavailable		Status Code	0		
User M	Name			CF Pollable	Not Implemented		
Port N	Number	1		CF Poll Request	Not Implemented		
Interf	face	internet_access		Short Preamble	Not Implemented		
VLAN	ID	129		PBCC	Not Implemented		
Quara	antine VLAN ID	0		Channel Apility	Not Implemented		
CCX V	Version	CCXv4		Timeout	1800		
E2E V	Version	E2Ev1		WEP State	WEP Disable		
Mobili	lity Role	Local					
Addre	ity Peer IP ess	N/A		Allowed (URL)IP add	ress		
Mobili	lity Move Count	0					
Policy	y Manager State	RUN					
Manag Protec	gement Frame	No					
UpTim	me (Sec)	71					
Curren	ent TxRateSet	m8 ss2					

# CMX

[CONNECT&ENGAGE]タブを開くと、CMXで認証されているユーザ数を確認できます。

cisco 10.31-35	DETECT & LOCATE	ANALYTICS	CONNECT & ENGAGE	CC MANAGE	SYSTEM						admin +
							Dashboard	Connect Experiences	Policy Plans	Library 👻	Settings ·
Q Location     Global      • No locations available	•	©     La	interval Ist 7 Days		Ŧ	Visitor Search Please enter search patte	ern	<b>v</b> 1	٩		
Global Dashboard											
Today at a Glance - Feb 22, 2018											
<b>201</b> 1			Vis	sitor Trend co	mpared to:		Data Usag	le:			
Total Visitors		New Visit	ors : 1	Yesterday € ∞%	6	Average	U	0	Dow (	nload )	
Column •			(i) Are	a							<b>(</b> )
New and Repeat Visitors		Repeat Vis New Visito	itors irs			Netwo	rk Usage				

ユーザの詳細を確認するには、同じタブで右上の[Visitor Search]をクリックします。

							<b>9</b>	<u>66 </u>	<b>Q</b> ;									
SCO 10.3.1-35	Visitor Search	'n														×	Plans   Library •	
Q Location	Please enter search q	uery			Q	Download	d as CSV 🛓											
Global	Use Search Filter C	ptions																
Jobal Dashl	Search on								rom			То						
	19 of 19 selected							*	02/21/2018 3:41 PN	4		02/22	2018 3:41 PN	И				
Today at a Glance	Export Preview (U	p 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	RegistrationPage	CustomPortal	REGISTRATION	PC	Windows 10	0	0	Catarina Silva	female	0	
Column																		(
5	Previous 1	Next																

# トラブルシュート

要素間のインタラクションのフローを確認するには、WLCで実行できるデバッグがあります。

>debug client<MAC addr1> <MAC addr2>(1つ以上のクライアントのMACアドレスを入力します)

>debug web-auth redirect enable mac <MAC addr>(Web-authクライアントのMACアドレスを入 力します)

>debug web-auth webportal-server enable

>debug aaa all enable

このデバッグによりトラブルシューティングが可能になり、必要に応じて、一部のパケットキャ プチャを補完するために使用できます。