

# 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](#)

[トラブルシューティング](#)

## 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

## 設定

## 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。

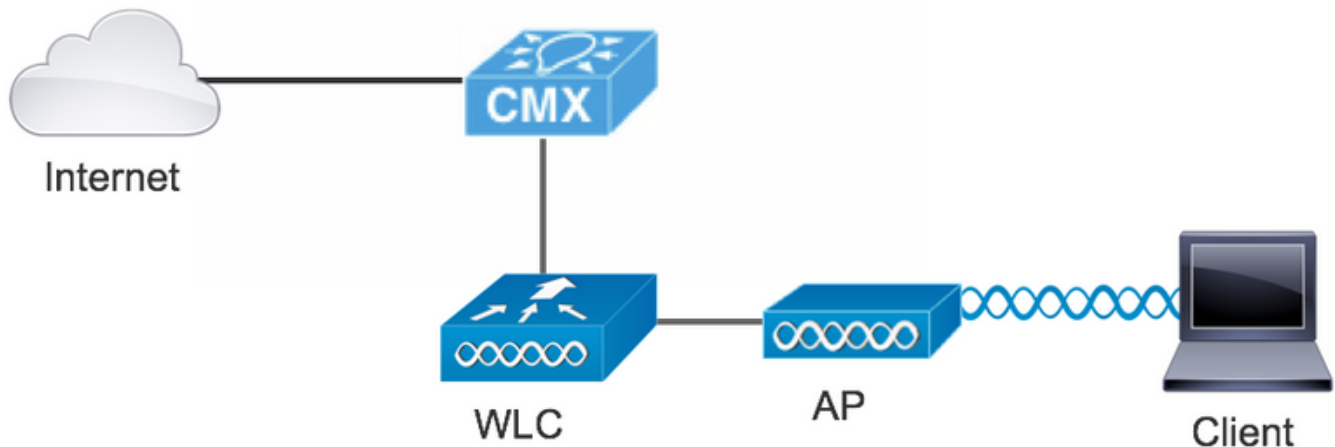
両方のシナリオで、クライアントはCMXによる認証を使用してSSIDへの登録を試みます。

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へ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。
2. 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[Twilio](#)を統合して行われます。[Twilio](#)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。

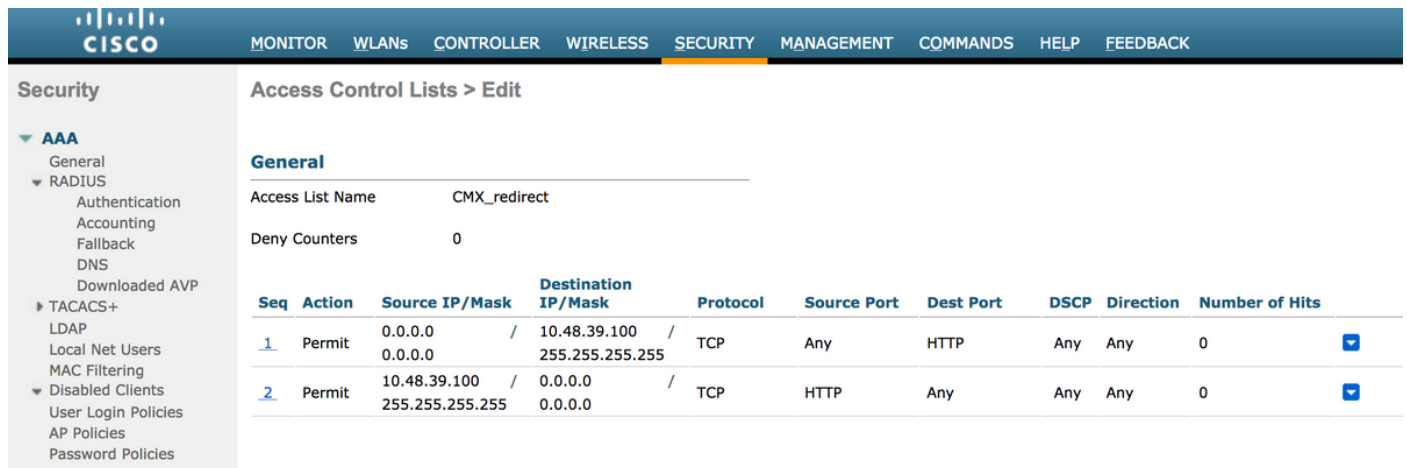
## A. WLC の設定

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。



The screenshot shows the Cisco WLC configuration interface for Access Control Lists. The left sidebar shows the navigation menu with 'Security' selected. The main content area is titled 'Access Control Lists > Edit' and shows the 'General' tab for an ACL named 'CMX\_redirect'. The 'Deny Counters' are set to 0. Below this is a table of rules:

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	10.48.39.100 / 255.255.255.255	TCP	Any	HTTP	Any	Any	0
2	Permit	10.48.39.100 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTP	Any	Any	Any	0

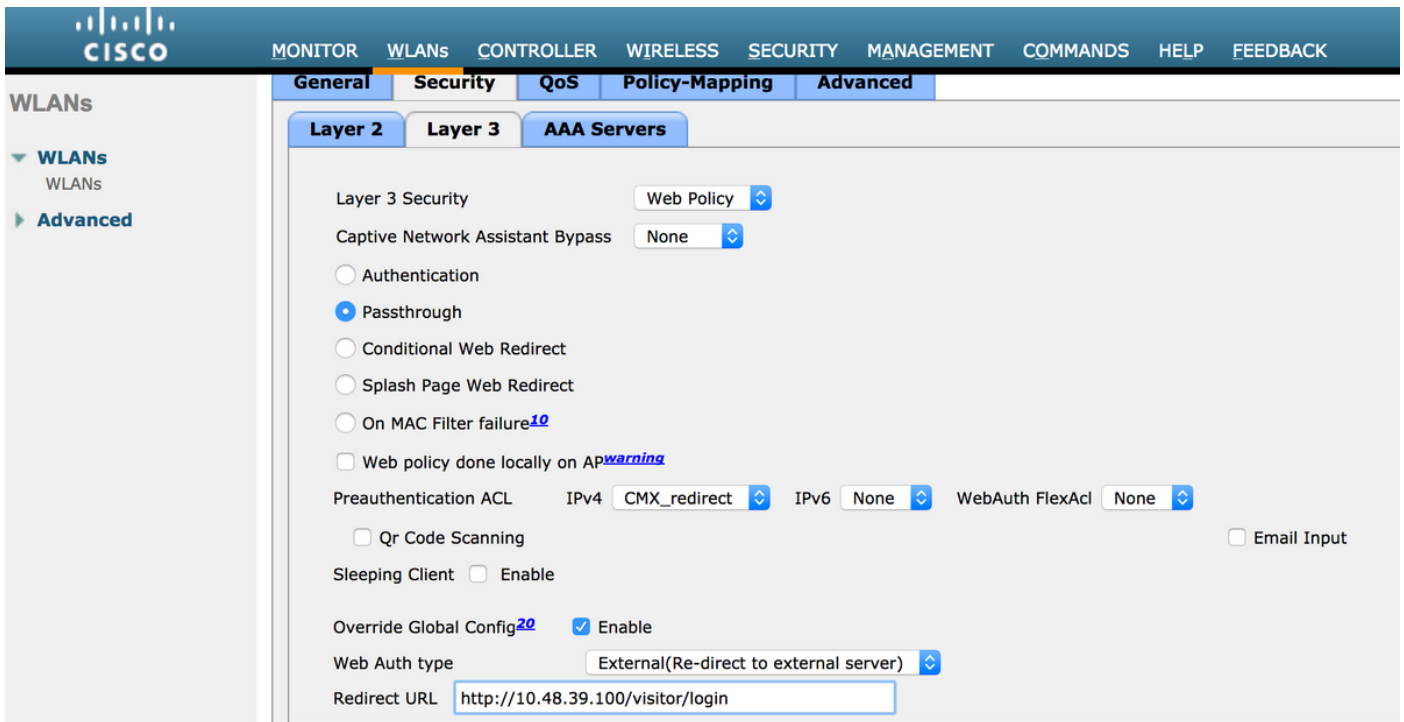
### 2. WLAN

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。



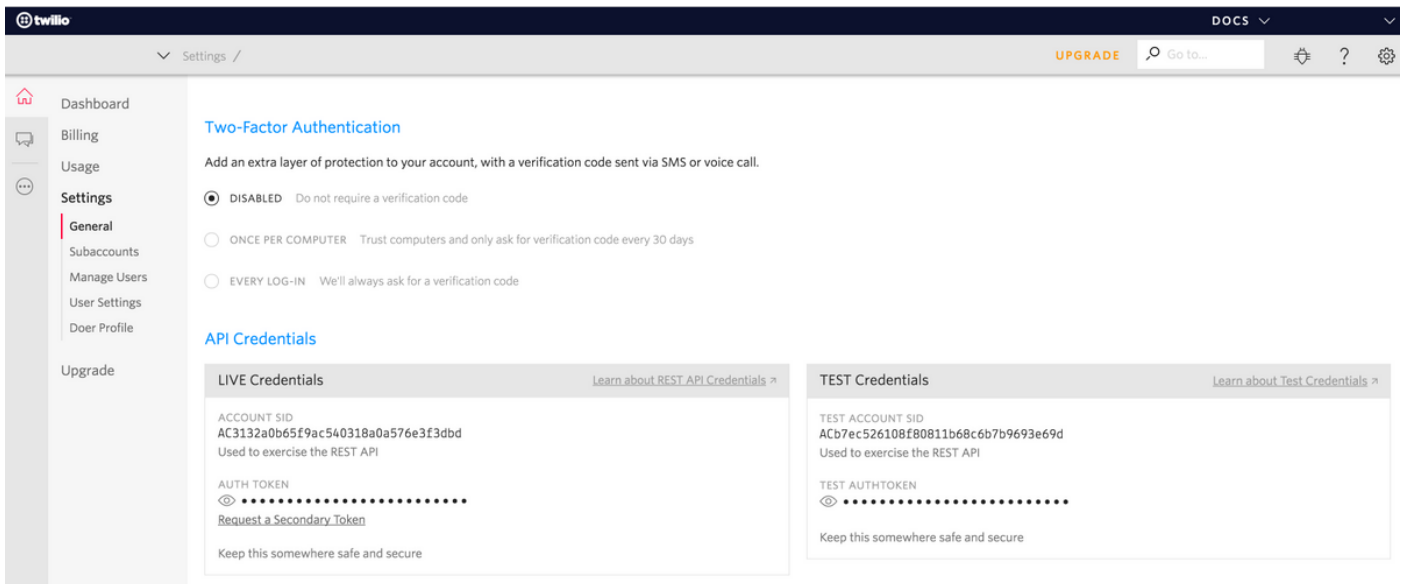
The screenshot shows the Cisco WLC configuration interface for WLANs. The left sidebar shows the navigation menu with 'WLANs' selected. The main content area is titled 'WLANs > Edit 'cmx\_sms'' and shows the 'Security' tab. The 'Layer 2 Security' dropdown is set to 'None'. The 'MAC Filtering' checkbox is unchecked. The 'Fast Transition' dropdown is set to 'Disable'.



## バリー・トウィリオ

CMXはテキストメッセージサービスの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。



## C. CMXの設定

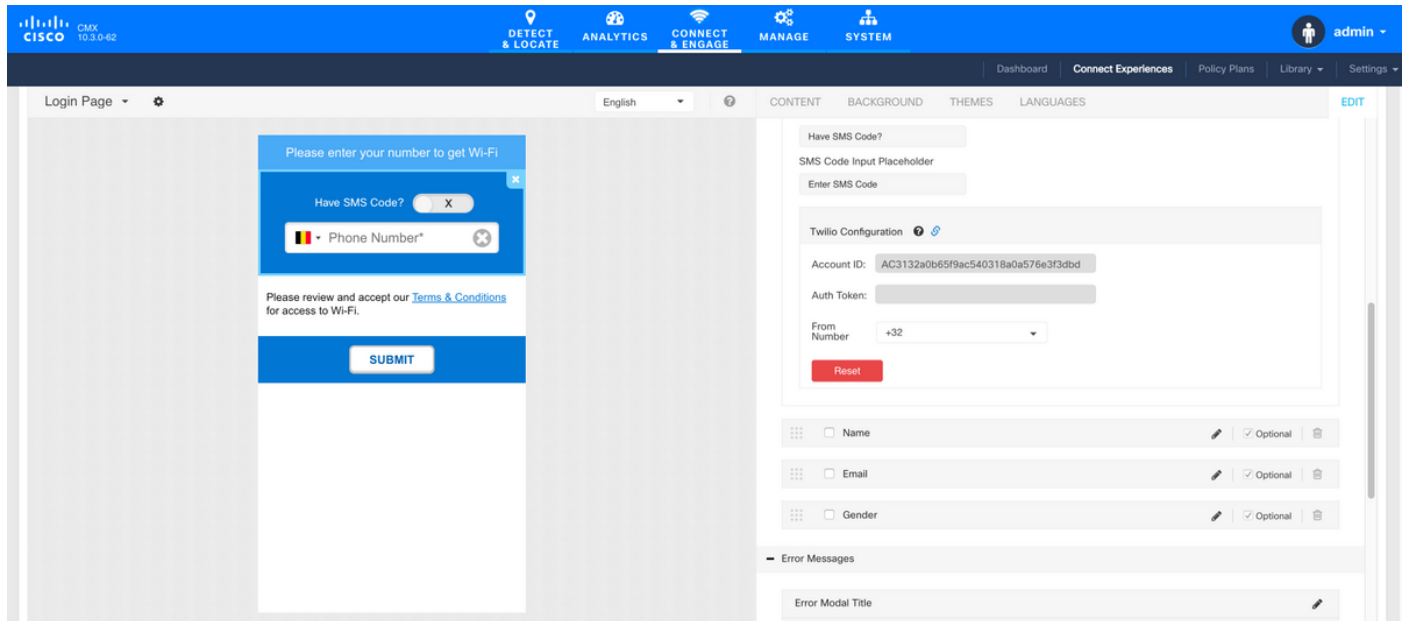
コントローラをCMXに正しく追加し、マップをPrime Infrastructureからエクスポートする必要があります。

- 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。



## 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)。

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Security

AAA  
 General  
 RADIUS  
 Authentication  
 Accounting  
 Fallback  
 DNS  
 Downloaded AVP  
 TACACS+  
 LDAP  
 Local Net Users  
 MAC Filtering  
 Disabled Clients  
 User Login Policies  
 AP Policies  
 Password Policies  
 Local EAP

Access Control Lists > Edit

General

Access List Name CMX\_Auth

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	10.48.39.100 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTPS	Any	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	10.48.39.100 / 255.255.255.255	TCP	Any	HTTPS	Any	Any	0

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。

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Security

AAA  
 General  
 RADIUS  
 Authentication  
 Accounting  
 Fallback  
 DNS  
 Downloaded AVP  
 TACACS+  
 LDAP  
 Local Net Users

ACL > CMX\_Auth > URL List

URL String Name  Add

URL Name
facebook.com
m.facebook.com
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。

Save Configuration Ping Logout Refresh

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs

WLANs  
 Advanced

WLANs > Edit 'cmxFW' < Back Apply

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

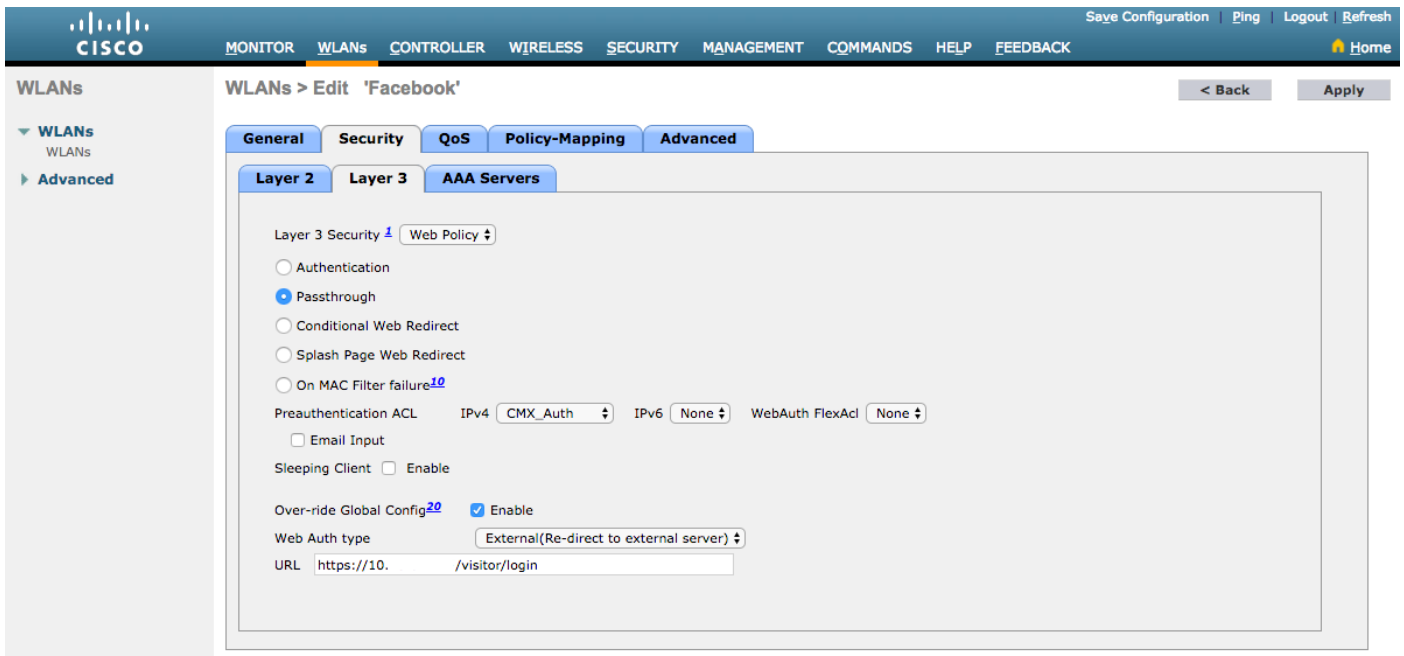
Layer 2 Security

MAC Filtering

Fast Transition

Fast Transition



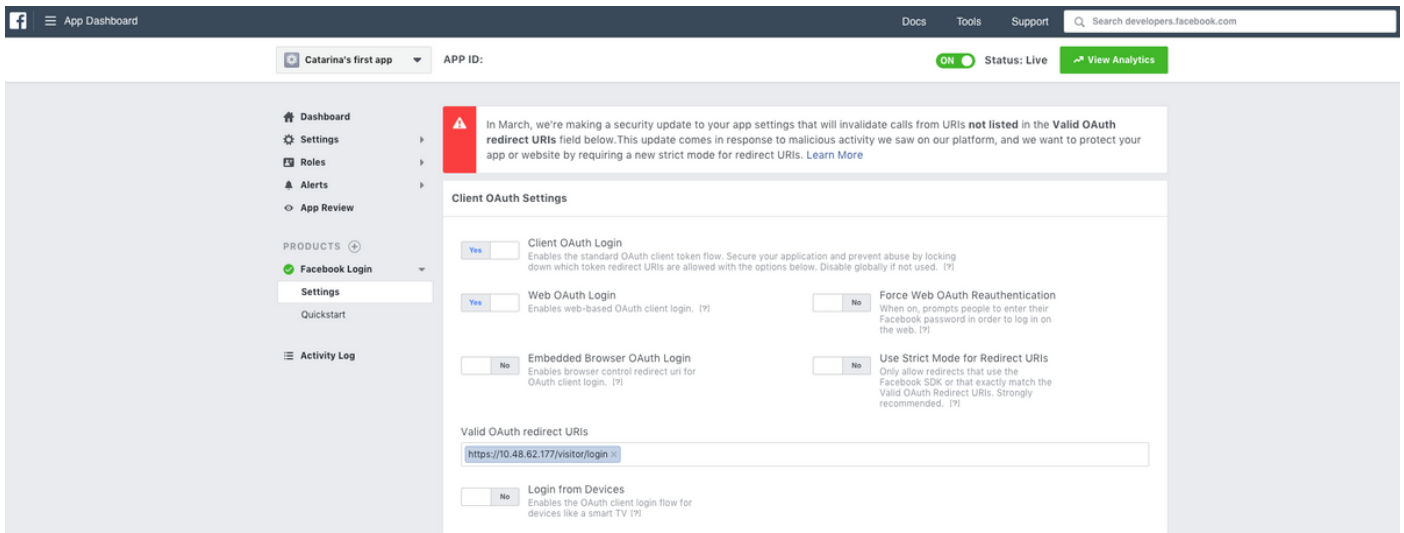


## B. Facebook for Developers

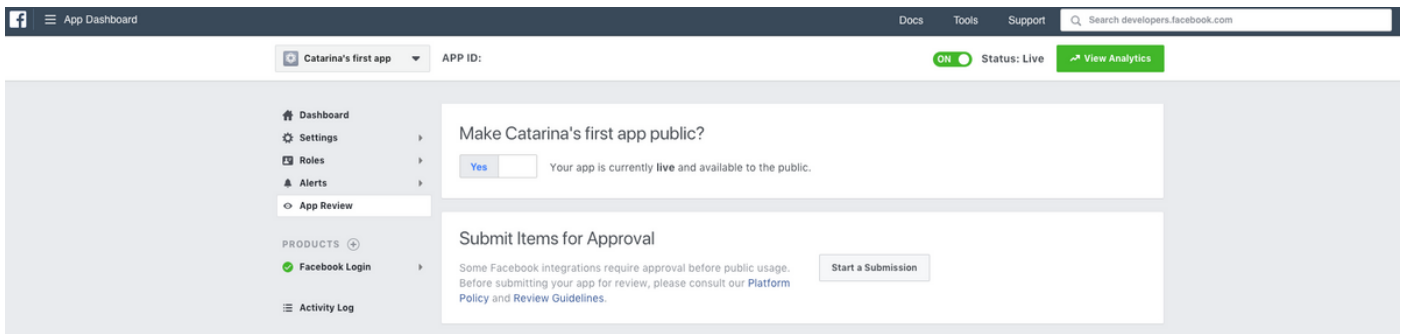
FacebookとCMXの統合では、2つのパーツ間で適切なトークンを交換するためにFacebookアプリが必要です。

アプリを作成するには、[Facebook for Developers](#)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。



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。



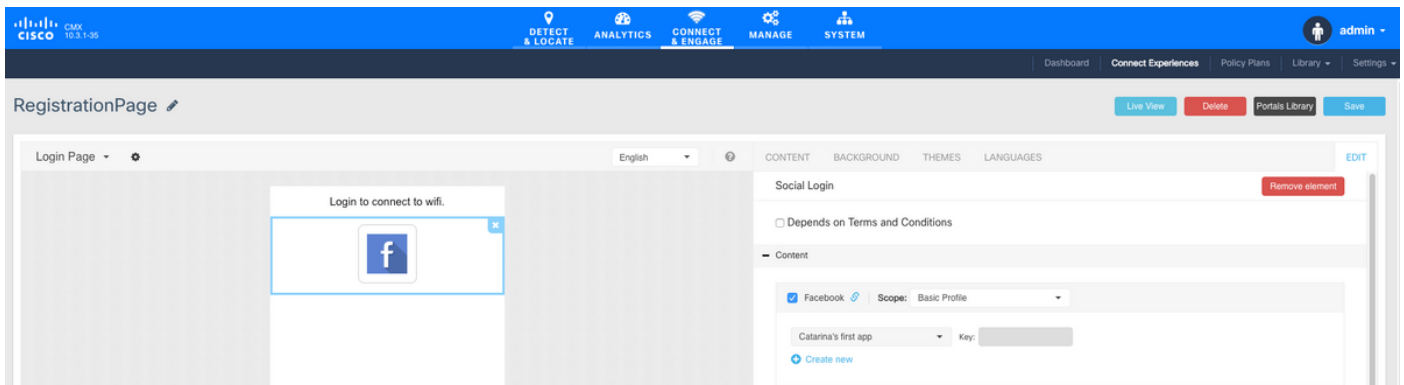
## C. CMXの設定

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。



## 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

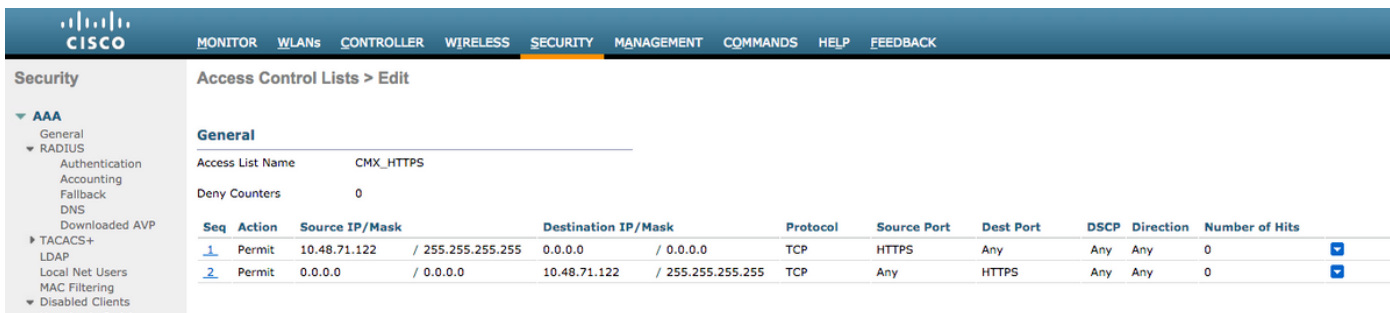
ここでHTTPSを認証方式として使用しているため、HTTPSトラフィックを許可するACLをWLCで設定する必要があります。ACLを設定するには、[Security] > [Access Control Lists] > [Add New Rule]に移動します。

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



の例では、CMX IPは10.48.71.122です)。

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。



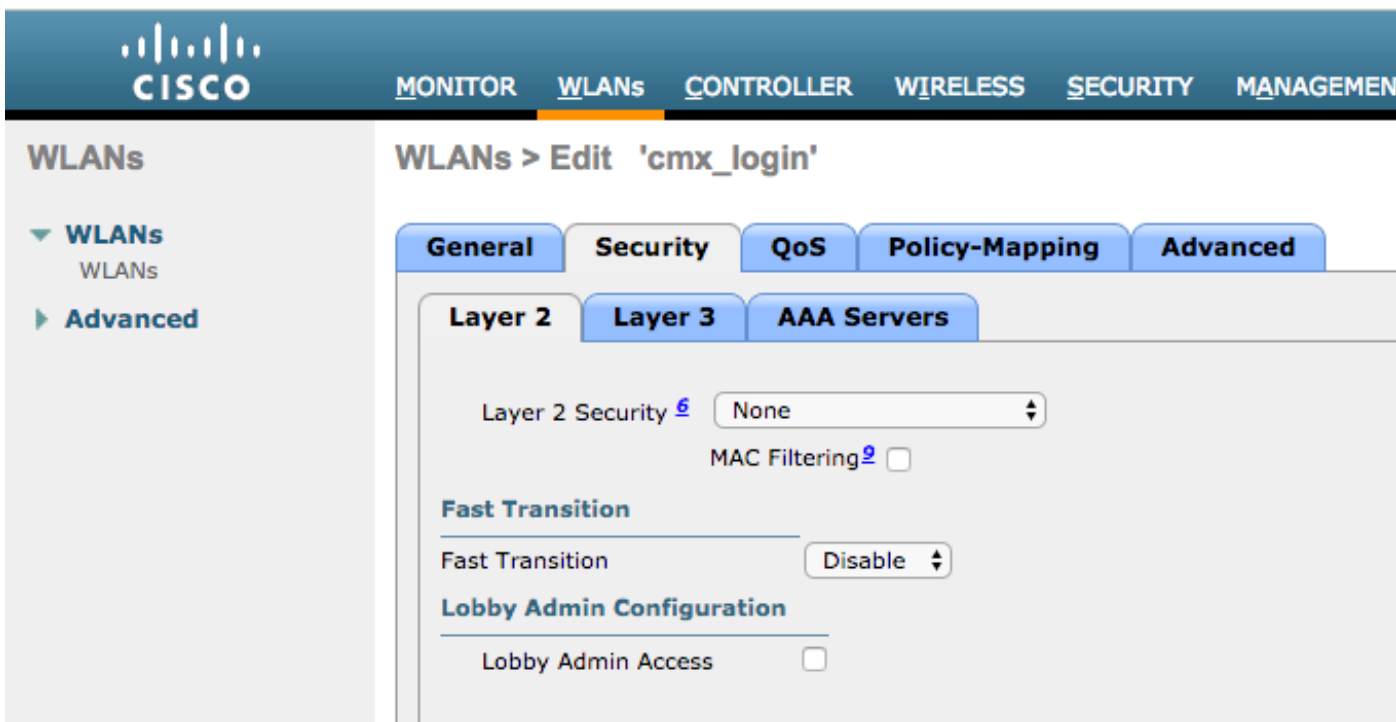
The screenshot shows the Cisco Security configuration interface for an Access Control List (ACL) named 'CMX\_HTTPS'. The 'General' tab is active, showing the ACL name and a deny counter of 0. Below this is a table of ACL entries.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	10.48.71.122 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTPS	Any	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	10.48.71.122 / 255.255.255.255	TCP	Any	HTTPS	Any	Any	0

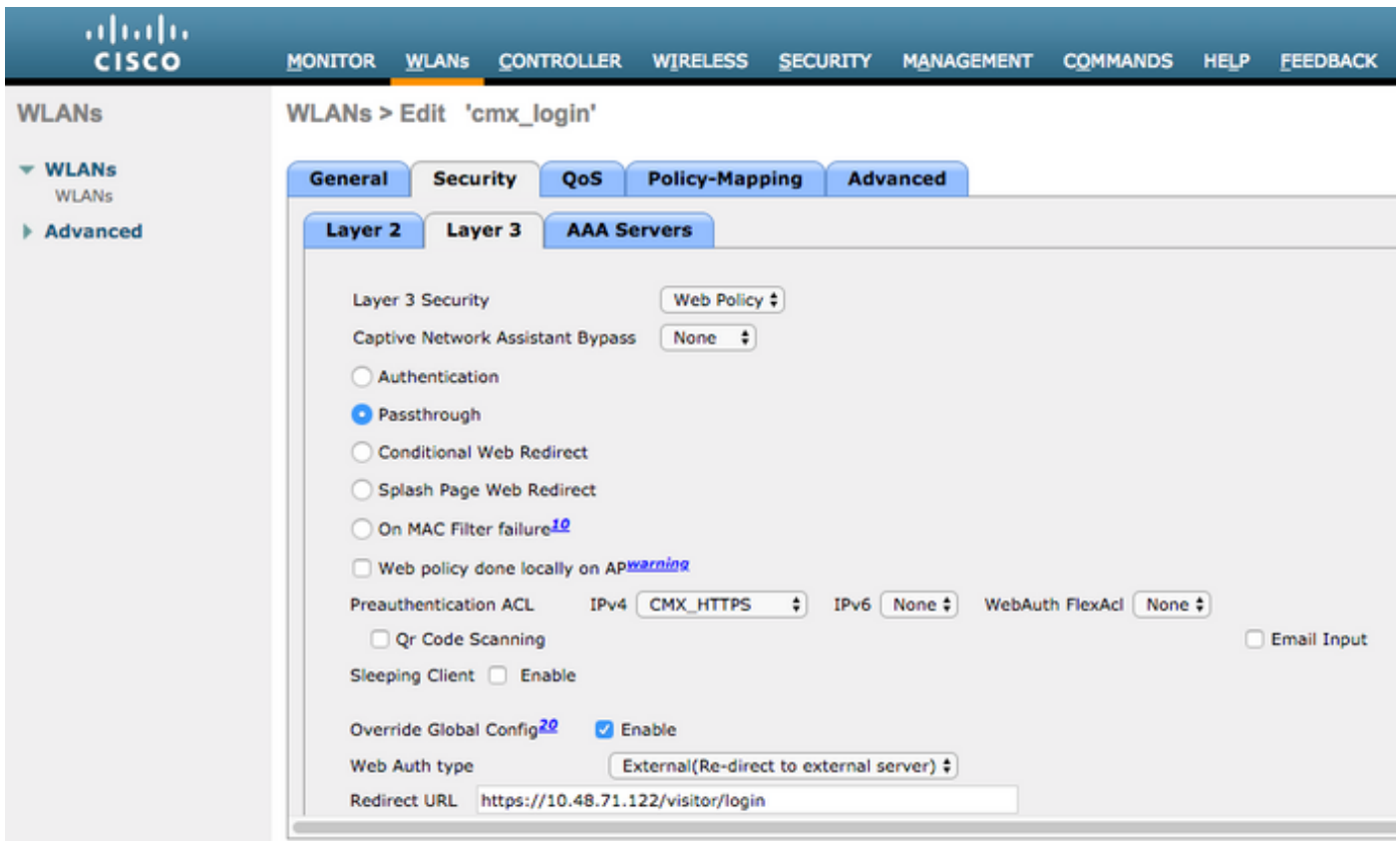
## 2. WLAN

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。



The screenshot shows the Cisco WLAN configuration interface for a WLAN named 'cmx\_login'. The 'Security' tab is active, and the 'Layer 3' sub-tab is selected. The 'Layer 2 Security' dropdown is set to 'None', and 'MAC Filtering' is disabled. The 'Fast Transition' dropdown is set to 'Disable', and 'Lobby Admin Access' is also disabled.



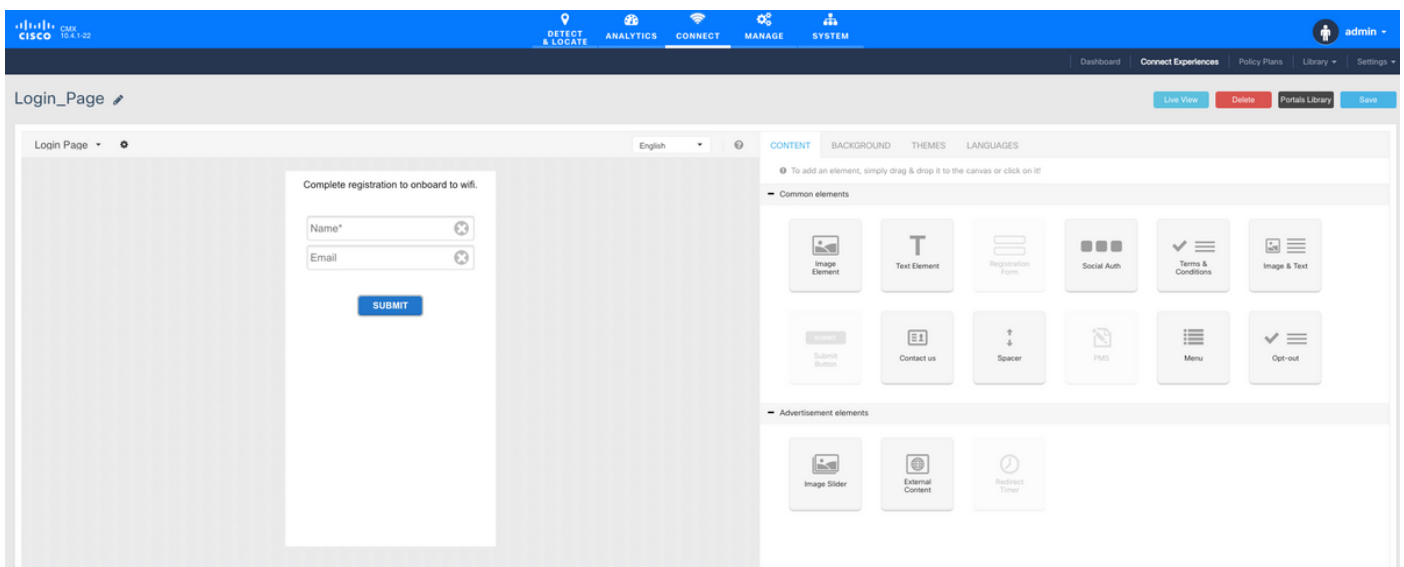
### C. CMXの設定

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。

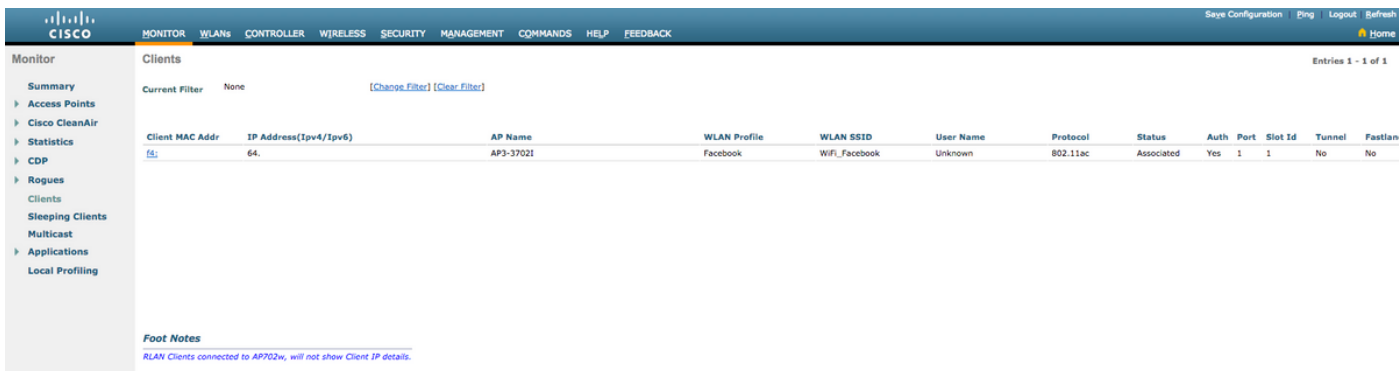
通常の登録のためのポータルは、最初から行うか ([カスタム]を選択)、またはCMXライブラリで利用可能な[登録フォーム]テンプレートから適用できます。



**確認**

## WLC

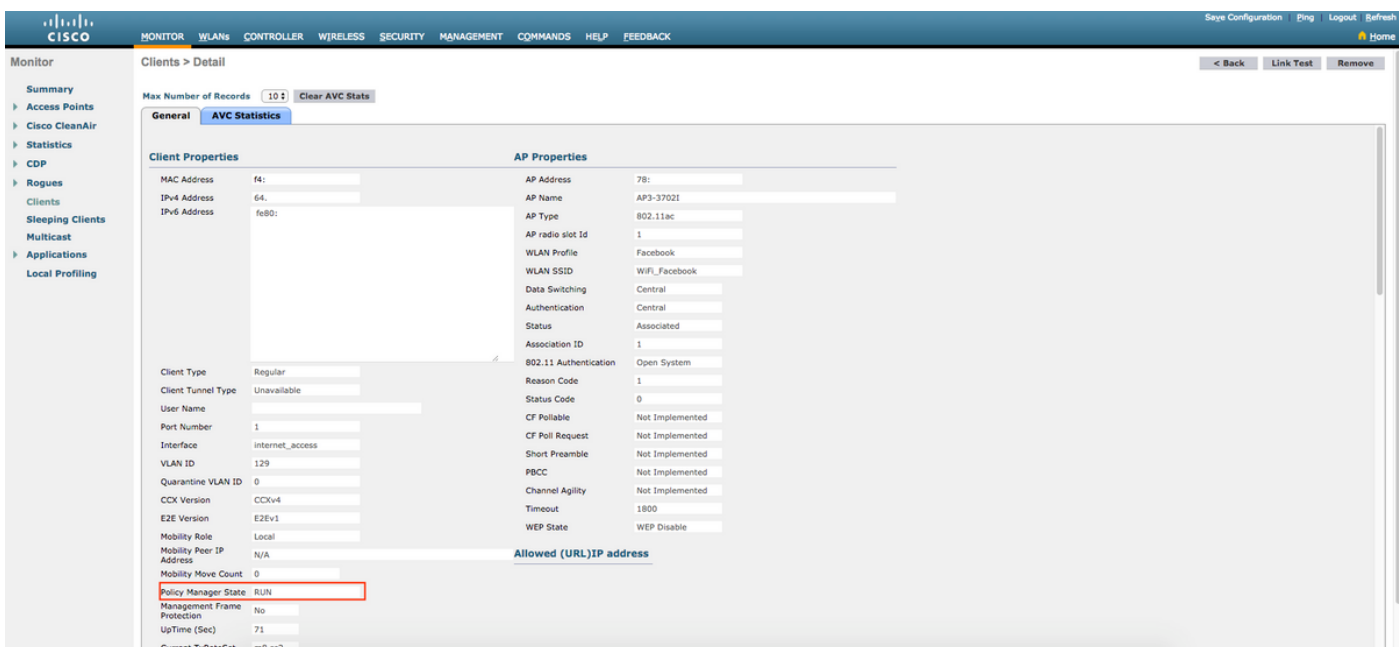
ユーザがシステムで正常に認証されたかどうかを確認するには、WLC GUIで[MONITOR] -> [Clients]に移動し、リストでクライアントのMACアドレスを検索します。



The screenshot shows the Cisco WLC Monitor interface. The 'Clients' tab is active, displaying a table of client information. The table has columns for Client MAC Addr, IP Address (IPv4/IPv6), AP Name, WLAN Profile, WLAN SSID, User Name, Protocol, Status, Auth, Port, Slot Id, Tunnel, and Fastlan. One client is listed with MAC address f4, IP address 64, and AP name AP3-37021. The status is 'Associated'.

Client MAC Addr	IP Address (IPv4/IPv6)	AP Name	WLAN Profile	WLAN SSID	User Name	Protocol	Status	Auth	Port	Slot Id	Tunnel	Fastlan
f4	64	AP3-37021	Facebook	WiFi_Facebook	Unknown	802.11ac	Associated	Yes	1	1	No	No

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。

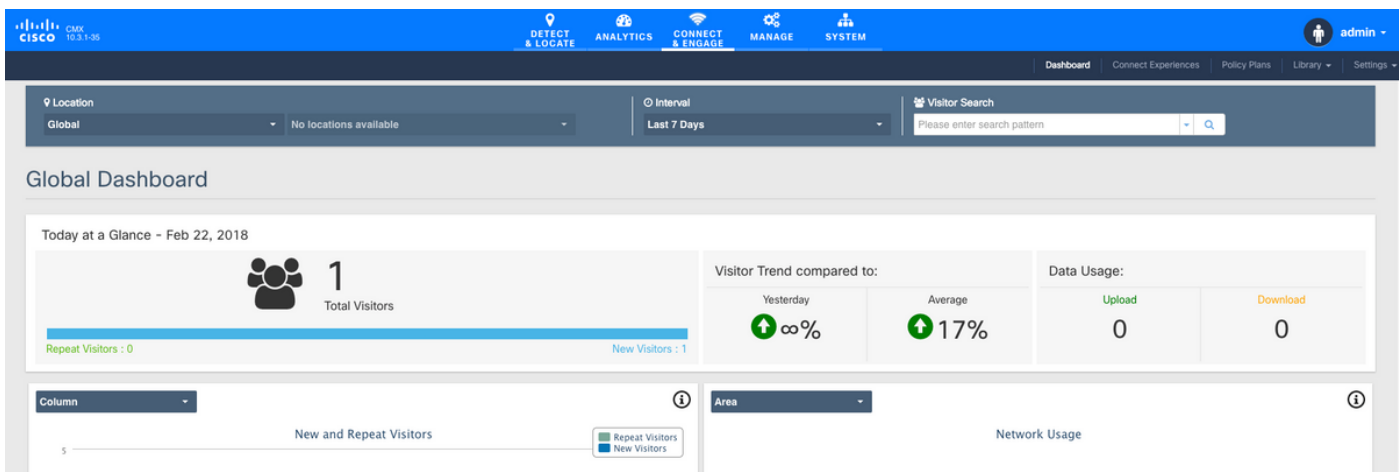


The screenshot shows the 'Clients > Detail' page in the Cisco WLC GUI. The 'AVC Statistics' tab is selected. The 'Client Properties' and 'AP Properties' sections are visible. The 'Policy Manager State' is highlighted in red and shows 'RUN'.

Client Properties	AP Properties
MAC Address: f4	AP Address: 78
IPV4 Address: 64	AP Name: AP3-37021
IPV6 Address: fe80:	AP Type: 802.11ac
	AP radio slot Id: 1
	WLAN Profile: Facebook
	WLAN SSID: WiFi_Facebook
	Data Switching: Central
	Authentication: Central
	Status: Associated
	Association ID: 1
Client Type: Regular	802.11 Authentication: Open System
Client Tunnel Type: Unavailable	Reason Code: 1
User Name:	Status Code: 0
Port Number: 1	CF Pollable: Not Implemented
Interface: internet_access	CF Poll 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 Address: N/A	
Mobility Move Count: 0	
Policy Manager State: RUN	
Management Frame Protection: No	
UpTime (Sec): 71	
Current TxRateSet: m8 ss2	

## CMX

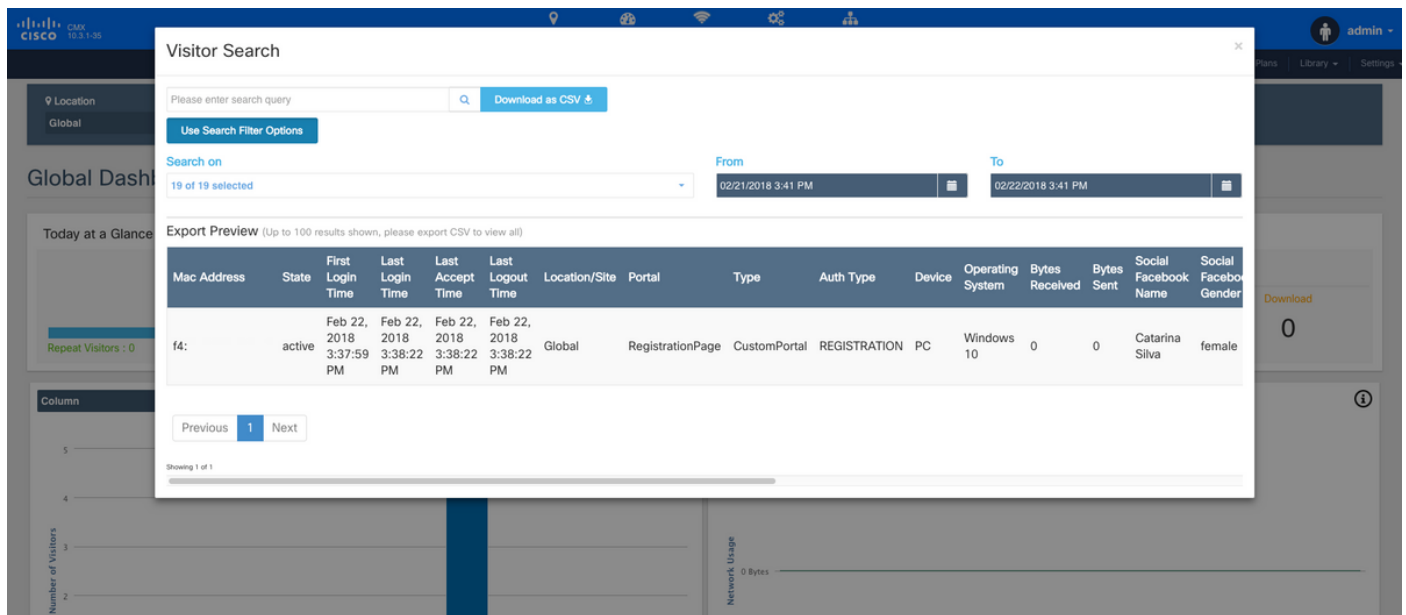
[CONNECT&ENGAGE]タブを開くと、CMXで認証されているユーザ数を確認できます。



The screenshot shows the Cisco CMX dashboard. The 'CONNECT & ENGAGE' tab is active. The 'Global Dashboard' section displays visitor statistics for Feb 22, 2018. The total number of visitors is 1. The visitor trend compared to yesterday is 100% (indicated by a green up arrow). The average visitor trend is 17% (indicated by a green up arrow). The data usage shows 0 upload and 0 download.

Visitor Trend compared to:	Data Usage:
Yesterday: 100%	Upload: 0
Average: 17%	Download: 0

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。



The screenshot shows the Cisco Visitor Search interface. At the top, there is a search bar with the text "Please enter search query" and a "Download as CSV" button. Below the search bar, there is a "Use Search Filter Options" button. The search results are displayed in a table with the following columns: Mac Address, State, First Login Time, Last Login Time, Last Accept Time, Last Logout Time, Location/Site, Portal, Type, Auth Type, Device, Operating System, Bytes Received, Bytes Sent, Social Facebook Name, and Social Facebook Gender. The table shows one result for a user with Mac Address f4: and State active. The user's login and logout times are listed as Feb 22, 2018. The user's location is Global, and the portal is RegistrationPage. The user's device is PC, and the operating system is Windows 10. The user's social media information is listed as Catarina Silva, female.

Mac Address	State	First Login Time	Last Login Time	Last Accept Time	Last Logout Time	Location/Site	Portal	Type	Auth Type	Device	Operating System	Bytes Received	Bytes Sent	Social Facebook Name	Social Facebook Gender
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

## トラブルシューティング

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。