

Experiências conectadas do CMX - Exemplo de configuração de registro de portal social, SMS e personalizado

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Autenticação via SMS](#)

[Autenticação via Contas de Rede Social](#)

[Autenticação via Portal Personalizado](#)

[Verificar](#)

[Troubleshoot](#)

Introduction

Esta finalidade deste documento é orientar os administradores de rede através do registro de clientes através da configuração de portais convidados no Connected Mobile eXperience (CMX).

O CMX permite que os usuários se registrem e se autentiquem na rede usando o Social Registration Login, SMS e Custom Portal. Neste documento, uma visão geral das etapas de configuração no Wireless LAN Controller (WLC) e no CMX pode ser encontrada.

Prerequisites

Requirements

O CMX deve ser configurado corretamente com a configuração básica.

Ter mapas exportados do Prime Infrastructure é opcional.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Wireless Controller versão 8.2.166.0, 8.5.110.0 e 8.5.135.0.
- Cisco Connected Mobile Experiences versão 10.3.0-62, 10.3.1-35. 10.4.1-22.

Configurar

Diagrama de Rede

Neste documento, serão descritas duas maneiras diferentes de autenticar usuários/clientes na rede sem fio, usando CMX.

Primeiro, será descrita a configuração da autenticação usando Contas de Rede Social e, em seguida, a autenticação usando SMS.

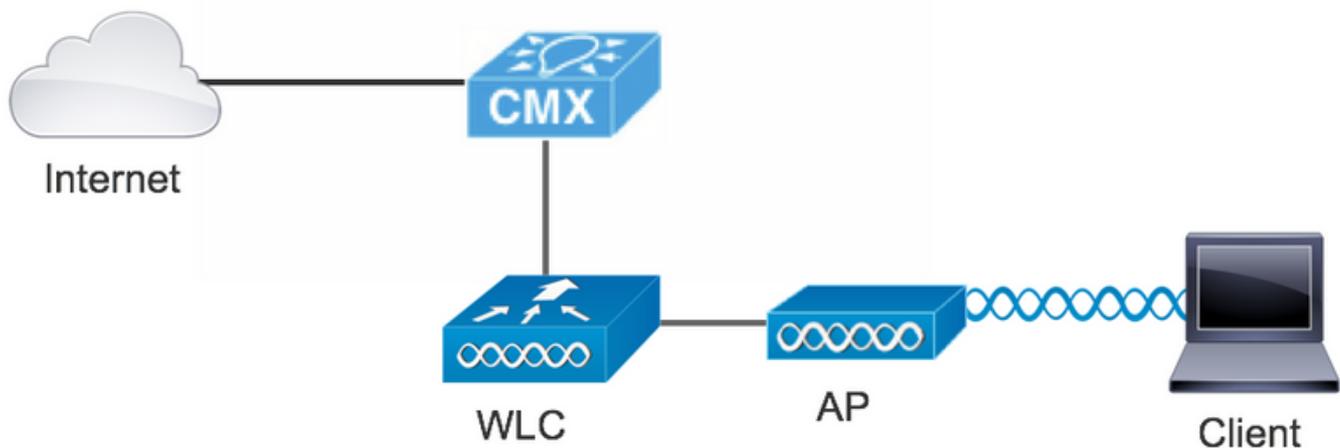
Em ambos os cenários, o cliente tentará se registrar no SSID usando a autenticação via CMX.

A WLC redireciona o tráfego HTTP para o CMX, onde o usuário é solicitado a autenticar. O CMX contém a configuração do portal a ser usado para que o cliente se registre, por meio de contas sociais e SMS.

Abaixo, o fluxo do processo de registro é descrito:

1. O cliente tenta ingressar no SSID e abre o navegador.
2. Em vez de ter acesso ao site solicitado, a WLC redireciona para o portal do convidado.
3. O cliente fornece suas credenciais e tenta autenticar.
4. O CMX lida com o processo de autenticação.
5. Se bem-sucedido, agora o acesso total à Internet é fornecido ao cliente.
6. O cliente é redirecionado para o site solicitado inicialmente.

A topologia usada é:



Configurações

Autenticação via SMS

O Cisco CMX permite a autenticação do cliente através do SMS. Este método requer a configuração de uma página HTML para que o usuário possa fornecer suas credenciais ao sistema. Os modelos padrão são fornecidos nativamente pelo CMX e podem ser editados ou substituídos posteriormente por um personalizado.

O serviço de mensagens de texto é feito por meio da integração do CMX com [Twilio](#), uma plataforma de comunicação em nuvem que permite enviar e receber mensagens de texto. Twilio permite ter um número de telefone por portal, o que significa que, se mais de um portal for usado, um número de telefone por portal será necessário.

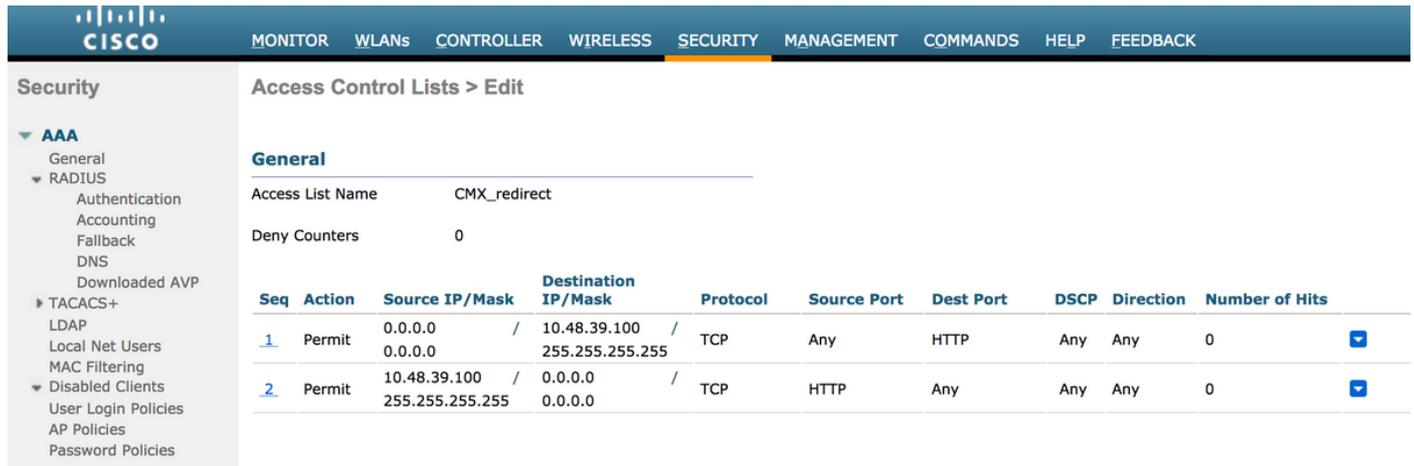
A. Configuração de WLC

No lado da WLC, o SSID e a ACL serão configurados. O AP deve ser associado ao controlador e no estado RUN.

1. ACL

É necessária uma ACL que permita tráfego HTTP, configurada na WLC. Para configurar uma ACL, vá para Security->Access Control Lists ->Add New Rule.

O IP usado é o configurado para o CMX. Isso permite o tráfego HTTP entre a WLC e o CMX. A figura abaixo mostra a ACL criada onde "10.48.39.100" se refere ao endereço ip do CMX.



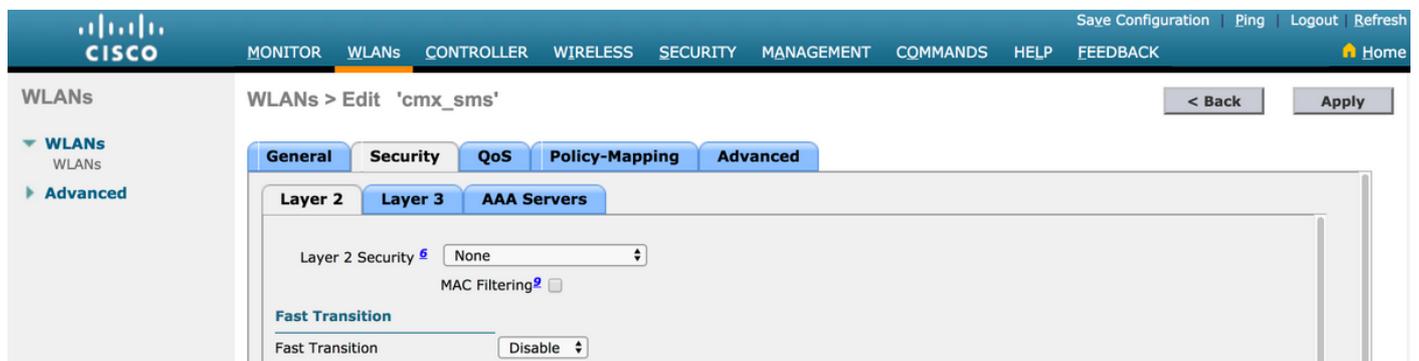
The screenshot shows the Cisco WLC interface for configuring an Access Control List (ACL). The page title is "Access Control Lists > Edit". Under the "General" tab, the "Access List Name" is "CMX_redirect" and "Deny Counters" is 0. A table lists the ACL rules:

| 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 |

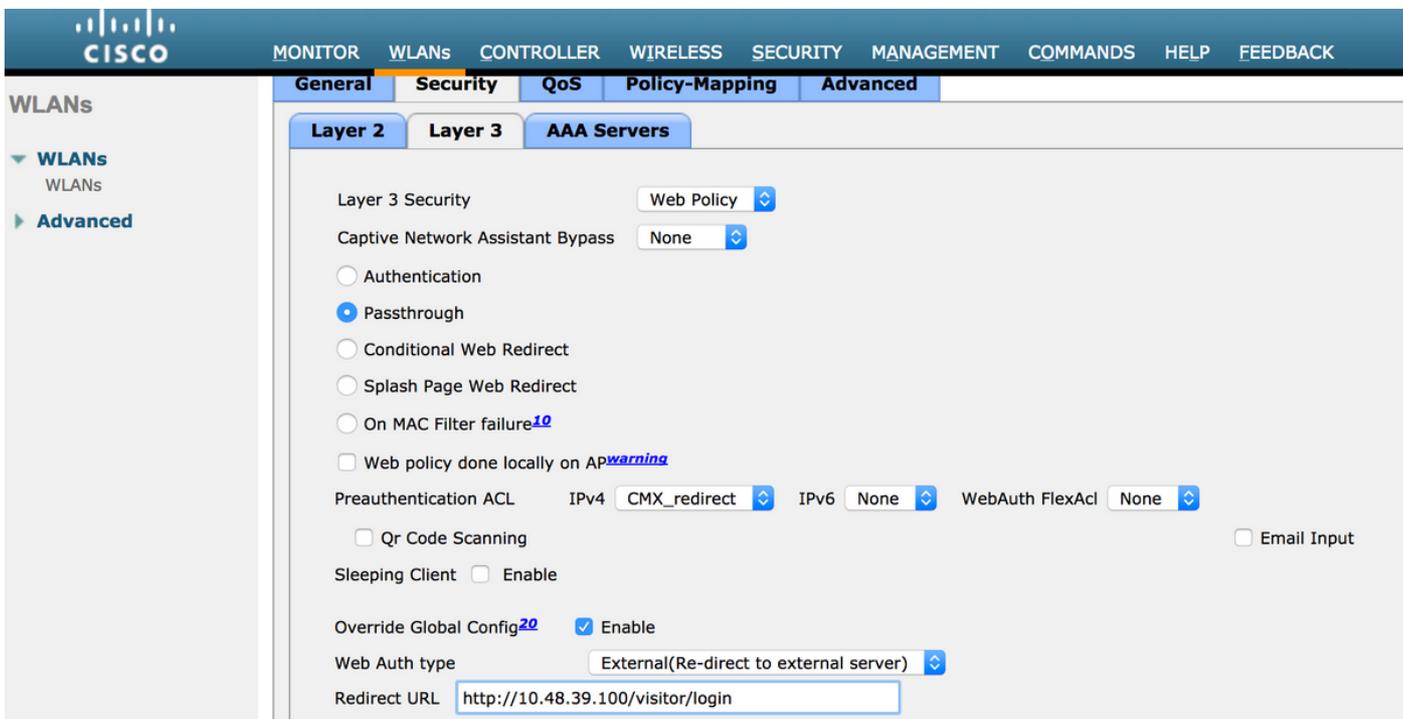
2. WLAN

Assim, a integração com o portal é feita, as alterações nas políticas de segurança na WLAN devem ser feitas.

Primeiro, vá para WLANs ->Edit->Layer 2->Layer 2 Security e, no menu suspenso, escolha None, de modo que a Layer 2 Security está desativada. Em seguida, na mesma guia Segurança, altere para Camada 3. No menu suspenso Layer 3 Security, selecione Web Policy e, em seguida, Passthrough. Na ACL de pré-autenticação, selecione a ACL IPv4 configurada anteriormente para vinculá-la à respectiva WLAN onde a autenticação SMS deve ser fornecida. A opção Override Global Config deve ser habilitada e o tipo Web Auth deve ser External (Re-direct to external server) para que os clientes possam ser redirecionados para o serviço CMX. O URL deve ser o mesmo do portal de autenticação SMS do CMX, cujo formato é `http://<CMX-IP>/visitor/login`.



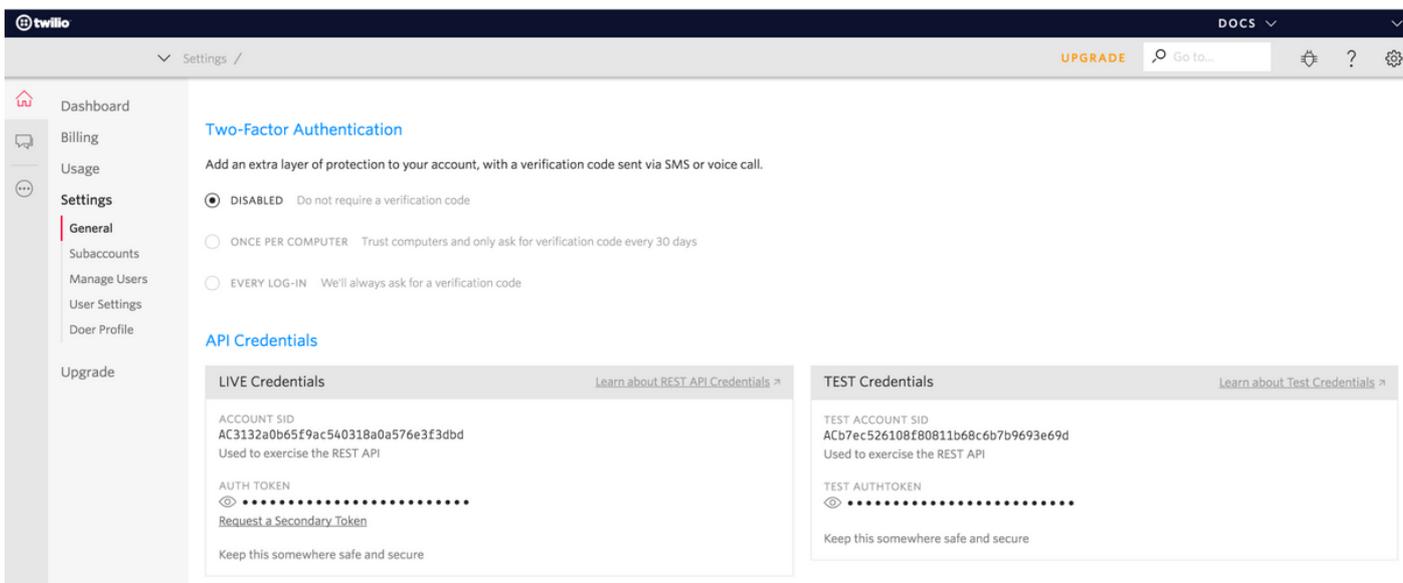
The screenshot shows the Cisco WLC interface for configuring a WLAN named "cmx_sms". The "Security" tab is selected. Under the "Layer 2" sub-tab, "Layer 2 Security" is set to "None" and "MAC Filtering" is disabled. Under the "Layer 3" sub-tab, "Fast Transition" is set to "Disable".



B. Twilio

O CMX oferece integração [Twilio](#) para serviços de mensagem de texto. As credenciais são fornecidas após a configuração correta da conta em Twilio. O SID da CONTA e o TOKEN AUTH são necessários.

Twilio tem seus próprios requisitos de configuração, documentados por meio do processo de configuração do serviço. Antes de integrar com CMX, o serviço Twilio pode ser testado, o que significa que problemas relacionados à configuração do Twilio podem ser detectados antes de usá-lo com CMX.



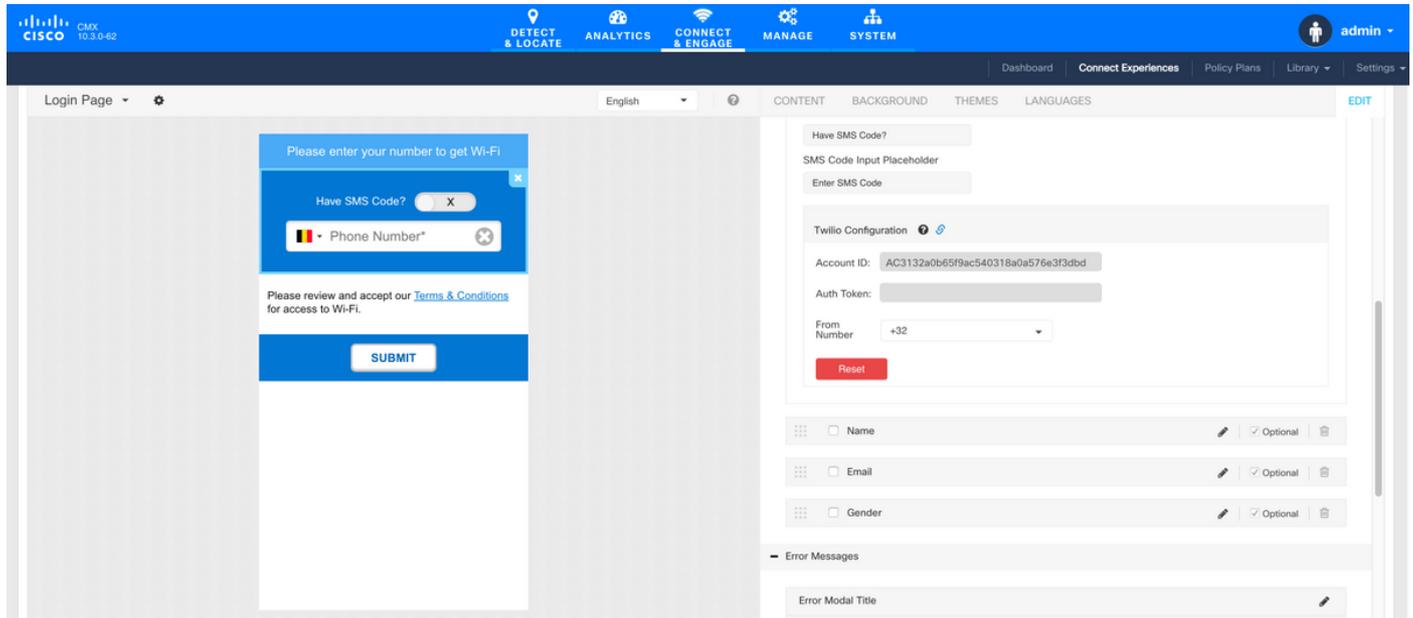
C. Configuração do CMX

É necessário que o controlador seja corretamente adicionado ao CMX e os mapas exportados do Prime Infrastructure.

- Página de registro SMS

Há um modelo padrão para o portal de registro. É possível encontrar os portais selecionando CONNECT&ENGAGE->Biblioteca. Se quiser um modelo, escolha Modelos no menu suspenso.

Para integrar Twilio ao portal, acesse Twilio Configuration e forneça a ID da conta e o Token de autenticação. Se a integração for bem-sucedida, o número usado na conta Twilio será exibido.



Autenticação via Contas de Rede Social

A autenticação do cliente usando Contas de Rede Social exige que o administrador de rede adicione um identificador de APP do Facebook válido no CMX.

A. Configuração de WLC

No lado da WLC, o SSID e a ACL serão configurados. O AP deve ser associado ao controlador e ao estado RUN.

1. ACL

Como aqui estamos usando HTTPS como método de autenticação, uma ACL que permite o tráfego HTTPS deve ser configurada na WLC. Para configurar uma ACL, vá para Security->Access Control Lists ->Add New Rule.

O CMX IP deve ser usado para permitir o tráfego HTTPS entre a WLC e o CMX. (neste exemplo, o ip do CMX é 10.48.39.100)

Security

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 |

Também é necessário ter uma ACL DNS com URLs do Facebook. Para isso, em Security ->Access Control Lists (Segurança ->Listas de controles de acesso), localize a entrada da ACL configurada anteriormente (neste caso, CMX_Auth) e mova o mouse para a seta azul no final da entrada e selecione Add-Remove URL (Adicionar/remover URL). Depois desse tipo de URLs do Facebook no URL String Name e Add.

Security

ACL > CMX_Auth > URL List

URL String Name:

URL Name

| | |
|----------------|-------------------------------------|
| facebook.com | <input checked="" type="checkbox"/> |
| m.facebook.com | <input checked="" type="checkbox"/> |
| fbcdn.net | <input checked="" type="checkbox"/> |

2. WLAN

As alterações nas políticas de segurança para que o registro funcione exigem que seja feita uma configuração específica na WLAN.

Como feito anteriormente para o registro de SMS, primeiro, fui para WLANs ->Edit->Layer 2->Layer 2 Security e, no menu suspenso, escolha None, de modo que a segurança de camada 2 está desativada. O, na mesma guia Segurança, é alterado para Camada 3. No menu suspenso Layer 3 Security, selecione Web Policy e, em seguida, Passthrough. Na ACL de pré-autenticação, selecione a ACL IPv4 configurada anteriormente para vinculá-la à respectiva WLAN onde a autenticação através do Facebook deve ser fornecida. A opção Override Global Config deve ser habilitada e o tipo Web Auth deve ser External (Re-direct to external server) para que os clientes possam ser redirecionados para o serviço CMX. Note que desta vez, a URL deve estar no seguinte formato **https://<CMX-IP>/visitor/login**.

The screenshot shows the Cisco WLAN configuration interface for a WLAN named 'cmxFW'. The 'Security' tab is selected, and the 'Layer 2' sub-tab is active. The 'Layer 2 Security' dropdown is set to 'None', and 'MAC Filtering' is disabled. Under the 'Fast Transition' section, the 'Fast Transition' dropdown is set to 'Disable'. The interface includes a navigation menu on the left with 'WLANs' and 'Advanced' options, and a top navigation bar with 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. Utility links for 'Save Configuration', 'Ping', 'Logout', and 'Refresh' are in the top right.

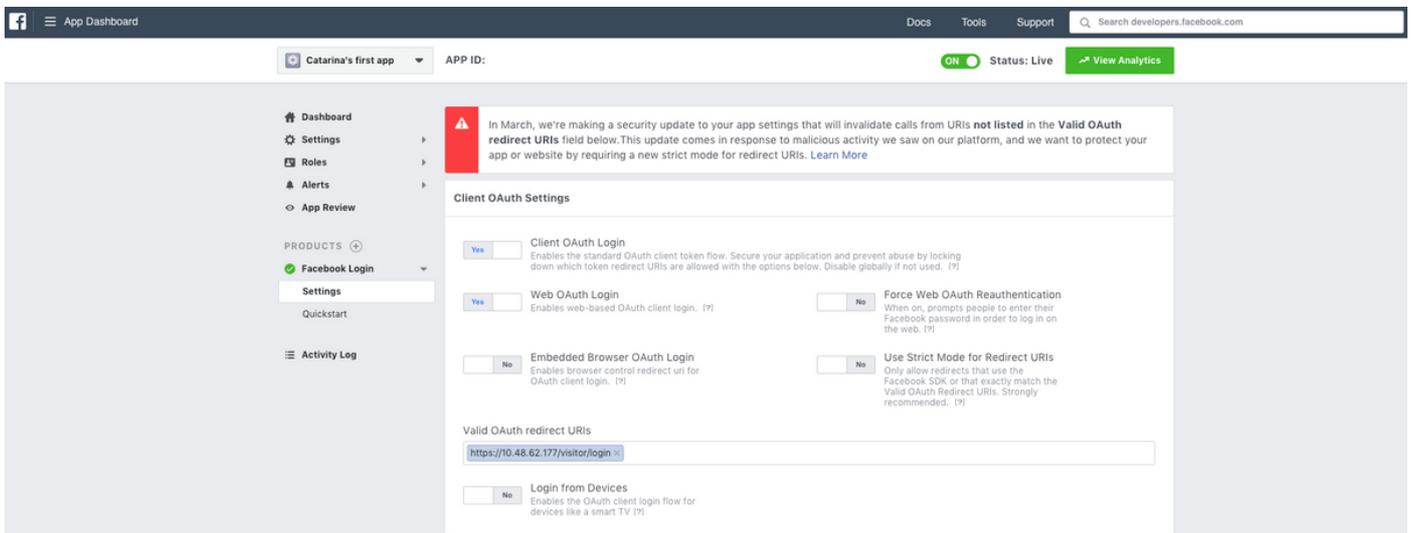
The screenshot shows the Cisco WLAN configuration interface for a WLAN named 'Facebook'. The 'Security' tab is selected, and the 'Layer 3' sub-tab is active. The 'Layer 3 Security' dropdown is set to 'Web Policy'. Under the 'Authentication' section, 'Passthrough' is selected. The 'Preauthentication ACL' section shows 'IPV4' set to 'CMX_Auth', 'IPV6' set to 'None', and 'WebAuth FlexAcl' set to 'None'. The 'Email Input' checkbox is unchecked, and 'Sleeping Client' is disabled. The 'Over-ride Global Config' checkbox is checked and labeled 'Enable'. The 'Web Auth type' dropdown is set to 'External(Re-direct to external server)'. The 'URL' field contains 'https://10. /visitor/login'. The interface includes a navigation menu on the left with 'WLANs' and 'Advanced' options, and a top navigation bar with 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. Utility links for 'Save Configuration', 'Ping', 'Logout', and 'Refresh' are in the top right, along with a 'Home' icon.

B. Facebook para desenvolvedores

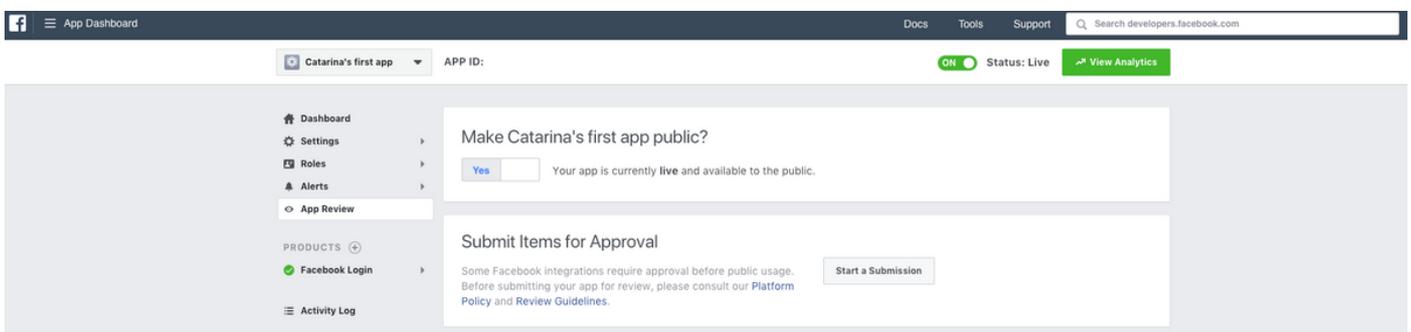
Para a integração do Facebook e CMX, é necessário um aplicativo do Facebook para que os tokens corretos sejam trocados entre as duas partes.

Vá para [Facebook para desenvolvedores](#) para criar o aplicativo. Há alguns requisitos de configuração do aplicativo para integrar os serviços.

Nas Configurações do aplicativo, verifique se o login OAuth do cliente e o login OAuth da Web estão ativados. Além disso, verifique se as URIs de redirecionamento OAuth válidas estão no URL do CMX no formato **https://<CMX-IP>/visitor/login**.



Para que o aplicativo seja publicado e esteja pronto para se integrar ao CMX, é necessário torná-lo público. Para isso, vá para App Review->Tornar a <App-Name> pública? e altere o estado para Sim.



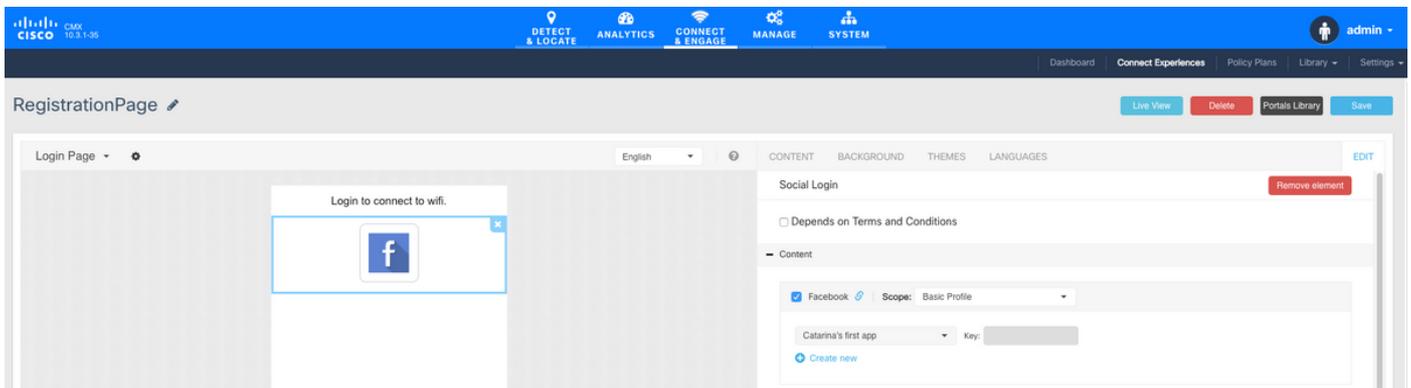
C. Configuração do CMX

É necessário que o controlador seja corretamente adicionado ao CMX e os mapas exportados do Prime Infrastructure.

- Página de registro

Para criar uma página de registro no CMX, as mesmas etapas feitas anteriormente para criar a página para a página de registro do SMS devem ser feitas. A seleção de CONNECT&ENGAGE->Biblioteca, portais de modelos prontos para edição pode ser encontrada selecionando Modelos no menu suspenso.

O registro através de credenciais do Facebook exige que o portal tenha conexão com as Contas Sociais. Para fazer isso do zero, ao criar um portal personalizado, acesse CONTEÚDO->Elementos comuns->Autenticação social e selecione Facebook. Em seguida, insira o nome do aplicativo e a ID do aplicativo (chave) obtidos do Facebook.



Autenticação via Portal Personalizado

Autenticar o cliente usando o Portal Personalizado é semelhante a configurar a Autenticação da Web externa. O redirecionamento será feito para o portal personalizado hospedado no CMX.

A. Configuração de WLC

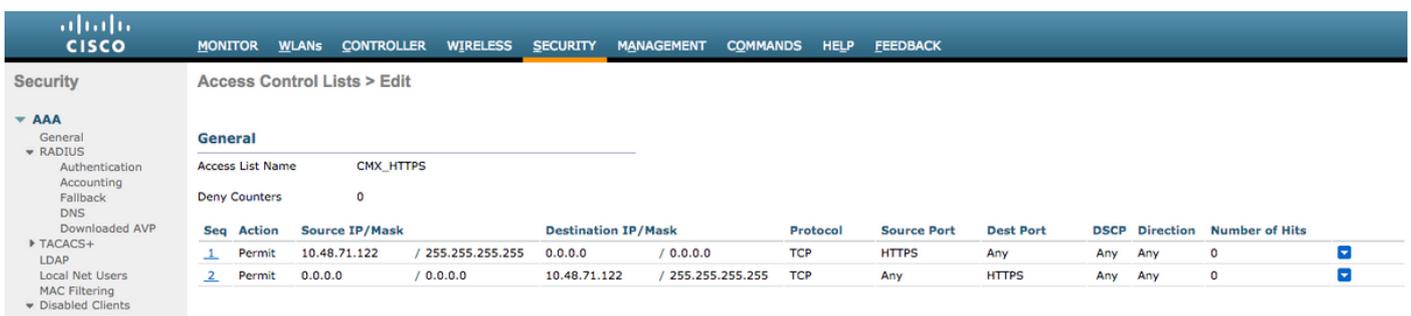
No lado da WLC, o SSID e a ACL serão configurados. O AP deve ser associado ao controlador e ao estado RUN.

1. ACL

Como aqui estamos usando HTTPS como método de autenticação, uma ACL que permite o tráfego HTTPS deve ser configurada na WLC. Para configurar uma ACL, vá para Security->Access Control Lists->Add New Rule.

O CMX IP deve ser usado para permitir o tráfego HTTPS entre a WLC e o CMX. (neste exemplo, o IP do CMX é 10.48.71.122).

Observação: certifique-se de habilitar o ssl no CMX emitindo o comando "cmxctl node sslmode enable" na CLI do CMX.

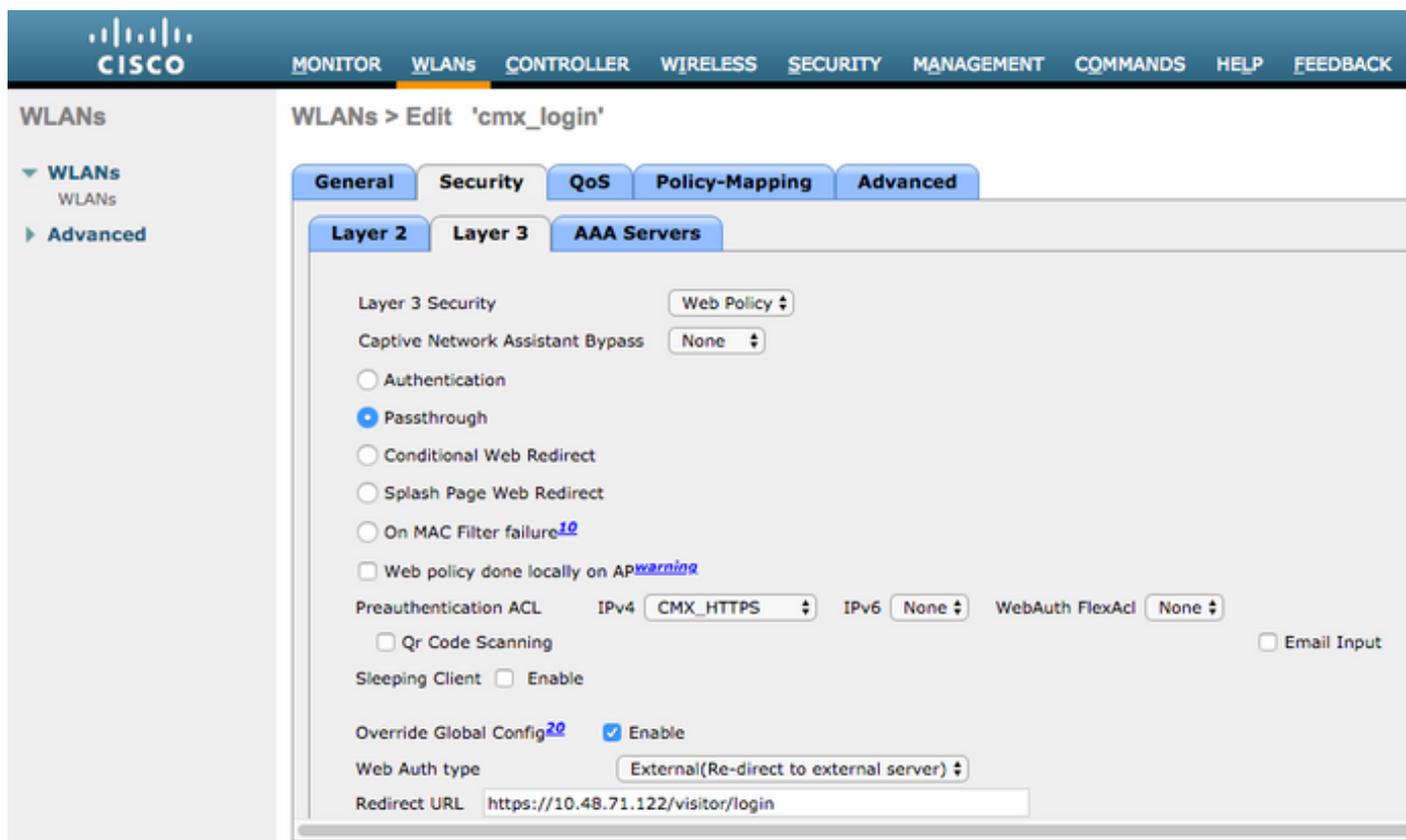
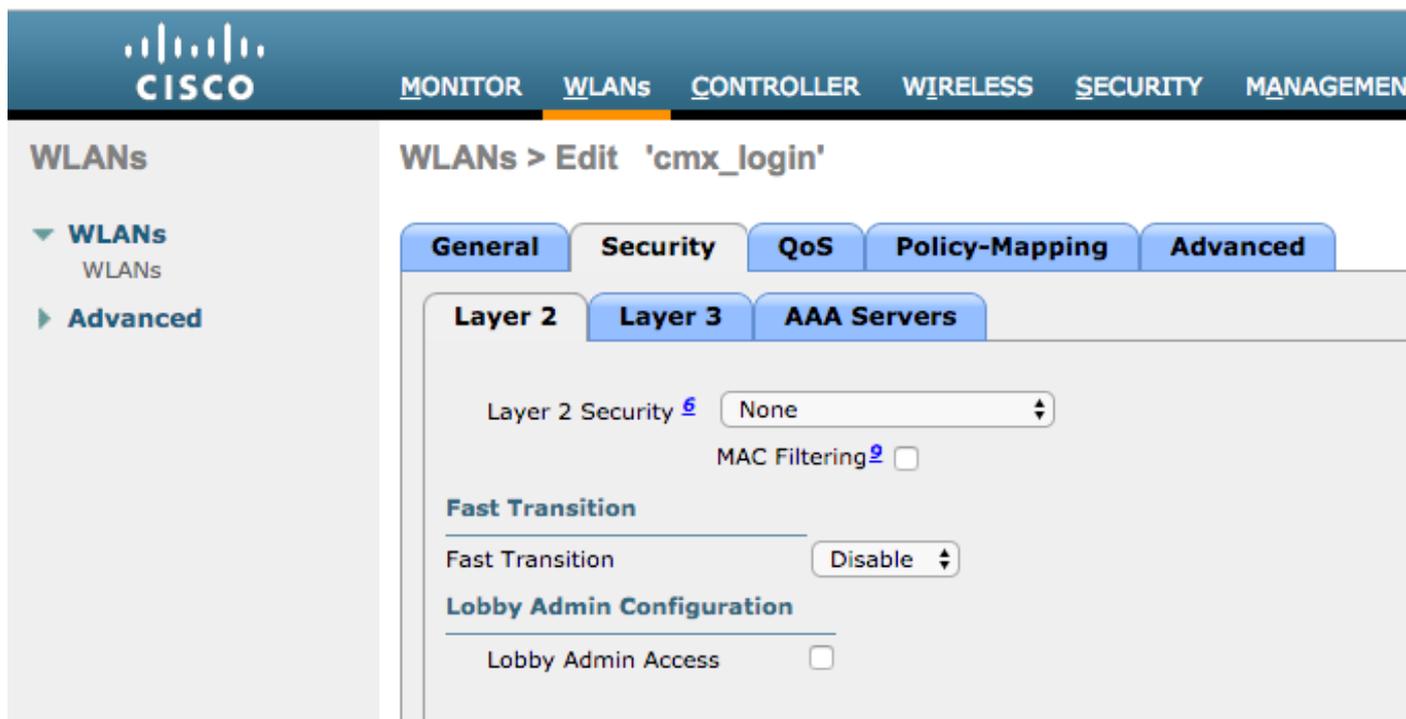


2. WLAN

As alterações nas políticas de segurança para que o registro funcione exigem que seja feita uma configuração específica na WLAN.

Como feito anteriormente para o registro de rede social e SMS, primeiro, fui para WLANs->Edit->Layer 2->Layer 2 Security e, no menu suspenso, escolha None, de modo que a segurança de camada 2 está desativada. O, na mesma guia Segurança, é alterado para Camada 3. No menu suspenso Layer 3 Security, selecione Web Policy e, em seguida, Passthrough. Na ACL de pré-autenticação, selecione a ACL IPv4 configurada anteriormente (denominada CMX_HTTPS neste

exemplo) e vincule-a à respectiva WLAN. A opção Override Global Config deve ser habilitada e o tipo Web Auth deve ser External (Re-direct to external server) para que os clientes possam ser redirecionados para o serviço CMX. Note que desta vez, a URL deve estar no seguinte formato <https://<CMX-IP>/visitor/login>.



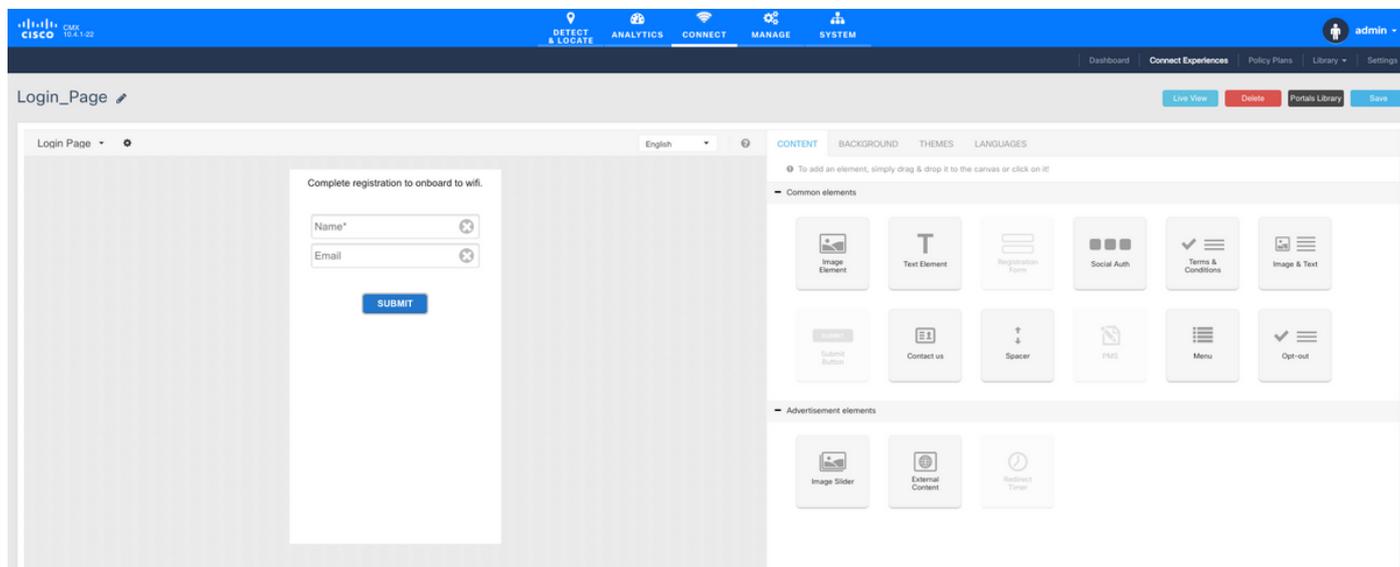
C. Configuração do CMX

É necessário que o controlador seja corretamente adicionado ao CMX e os mapas exportados do Prime Infrastructure.

- Página de registro

Para criar uma página de registro no CMX, siga as mesmas etapas feitas anteriormente para criar a página para outros métodos de autenticação. A seleção de CONNECT&ENGAGE->Biblioteca, portais de modelos prontos para edição pode ser encontrada selecionando Modelos no menu suspenso.

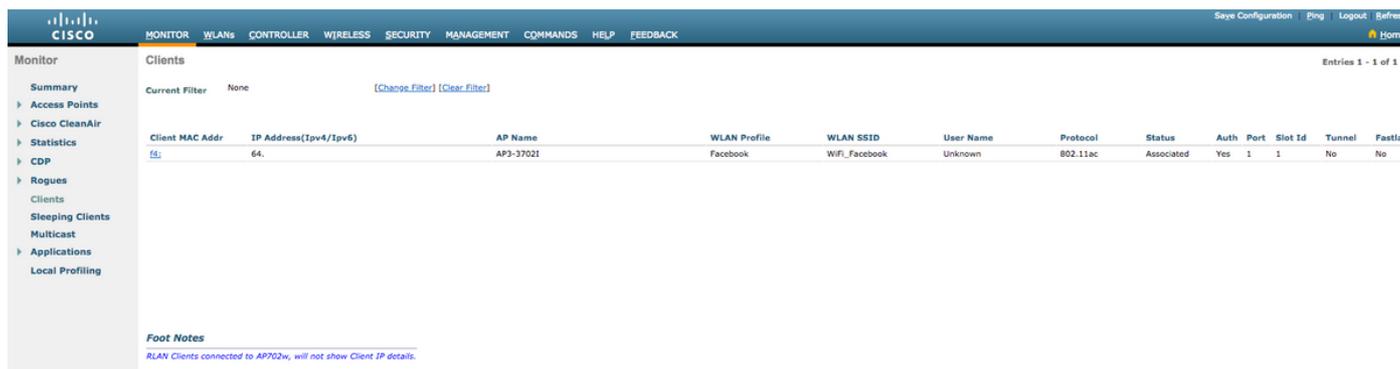
O portal para registro normal pode ser feito do zero (selecione "Personalizado") ou adaptado do modelo "Formulário de registro" disponível na biblioteca CMX.



Verificar

WLC

Para verificar se o usuário foi autenticado com êxito no sistema, na GUI da WLC, vá para MONITOR->Clientes e procure o endereço MAC do cliente na lista:



Clique no endereço MAC do cliente e, nos detalhes, confirme se o estado do Policy Manager do cliente está no estado RUN:

The screenshot shows the Cisco Meraki Monitor interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The main content area is titled 'Clients > Detail' and shows 'AVC Statistics' for a specific client. The 'Client Properties' section includes fields for MAC Address (f4:), IP Address (64:), IPv6 Address (fe80:), Client Type (Regular), Client Tunnel Type (Unavailable), User Name, Port Number (1), Interface (internet_access), VLAN ID (129), Quarantine VLAN ID (0), CCX Version (CCXv4), E2E Version (E2Ev1), Mobility Role (Local), Mobility Peer IP Address, and Mobility Move Count (0). The 'AP Properties' section includes fields for AP Address (78:), AP Name (AP3-37021), 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), 802.11 Authentication (Open System), Reason Code (1), Status Code (0), CF Pollable (Not Implemented), CF Poll Request (Not Implemented), Short Preamble (Not Implemented), PBCC (Not Implemented), Channel Agility (Not Implemented), Timeout (1800), and WEP State (WEP Disable). A red box highlights the 'Policy Manager State' field, which is set to 'RUN'.

CMX

É possível verificar quantos usuários são autenticados no CMX, abrindo a guia CONNECT&ENGAGE:

The screenshot shows the Cisco Meraki CMX interface. The top navigation bar includes 'DETECT & LOCATE', 'ANALYTICS', 'CONNECT & ENGAGE', 'MANAGE', and 'SYSTEM'. The main content area is titled 'Global Dashboard' and shows 'Today at a Glance - Feb 22, 2018'. The dashboard displays '1 Total Visitors' with a bar chart showing 'Repeat Visitors : 0' and 'New Visitors : 1'. The 'Visitor Trend compared to:' section shows 'Yesterday' at ∞% and 'Average' at 17%. The 'Data Usage:' section shows 'Upload' at 0 and 'Download' at 0. The bottom of the dashboard features a 'Column' dropdown set to 'New and Repeat Visitors' and an 'Area' dropdown set to 'Network Usage'.

Para verificar os detalhes do usuário, na mesma guia, na parte superior direita, clique em Pesquisa do Visitante:

The screenshot shows the Cisco WLC Visitor Search interface. The search query is 'f4:'. The search results table is as follows:

| 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 |

Troubleshoot

Para verificar o fluxo das interações entre os elementos, há algumas depurações que podem ser feitas no WLC:

>debug client<MAC addr1> <MAC addr2> (Insira o endereço MAC de um ou mais clientes)

>debug web-auth redirect enable mac <MAC addr> (Insira o endereço MAC do cliente web-auth)

>debug web-auth webportal-server enable

>debug aaa all enable

Essas depurações permitirão a solução de problemas e, se necessário, algumas capturas de pacotes podem ser usadas para complementar.