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

Contents

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.

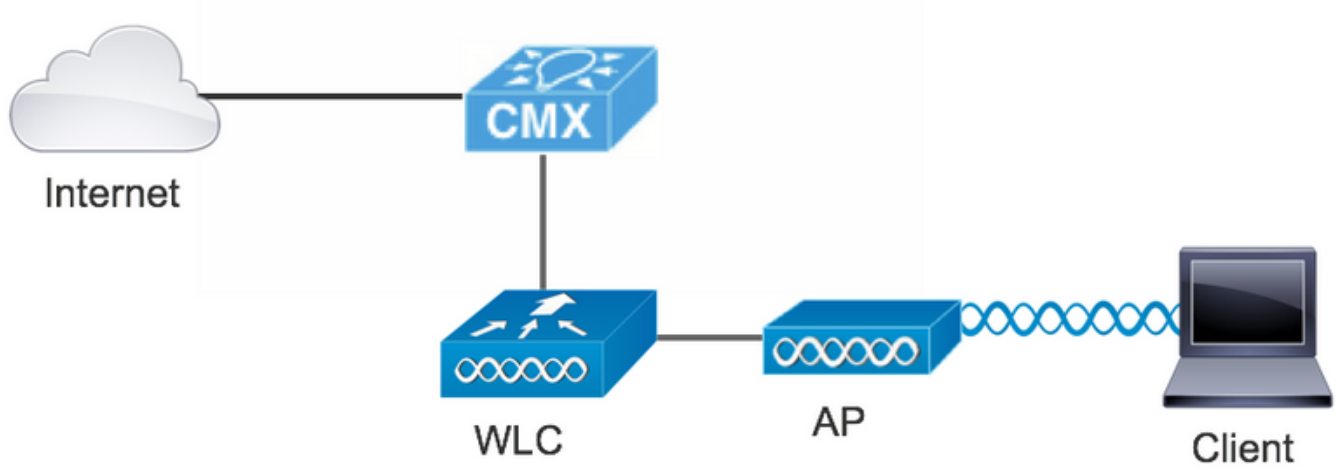
Em ambos os cenários, o cliente tentará se registrar no SSID usando a autenticação via CMX.

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.

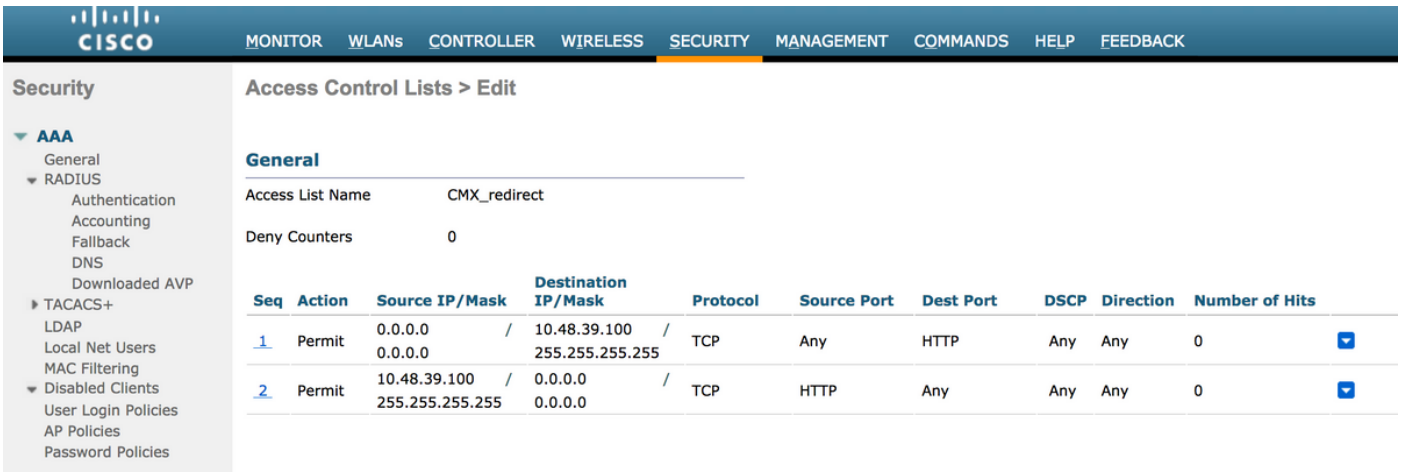
A. Configuração de WLC

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

1. ACL

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

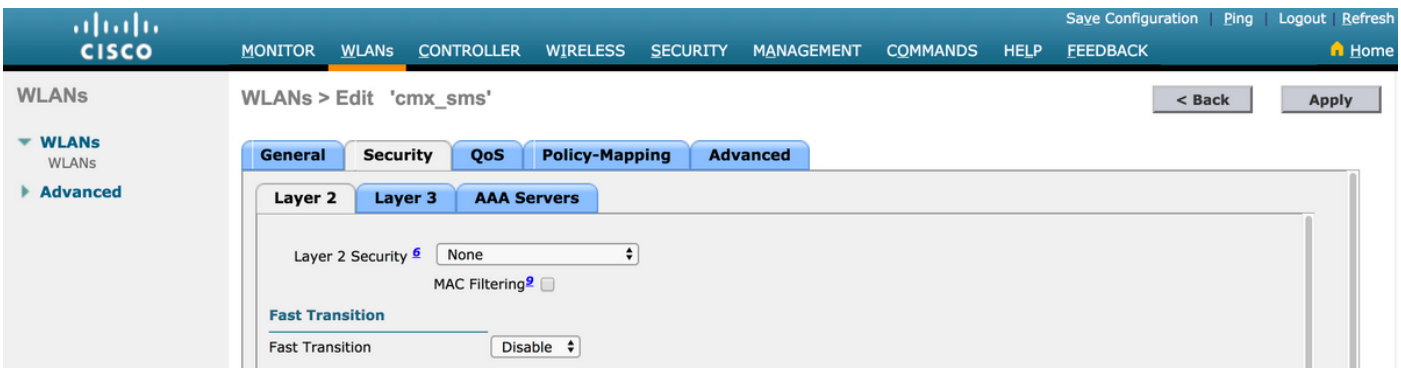
O IP usado é o configurado para o CMX. Isso permite o tráfego HTTP entre a WLC e o CMX. A figura abaixo mostra a ACL criada onde "10.48.39.100" se refere ao endereço ip do CMX.

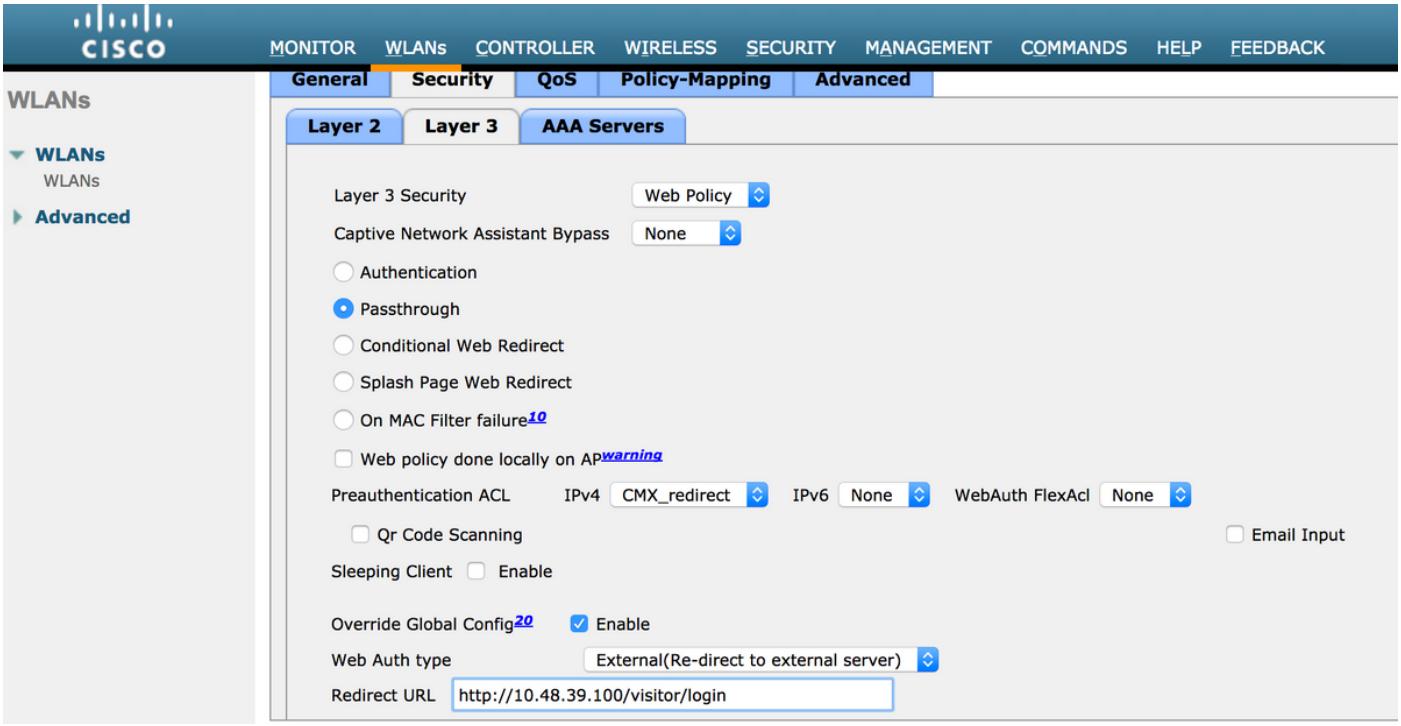


2. WLAN

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 .

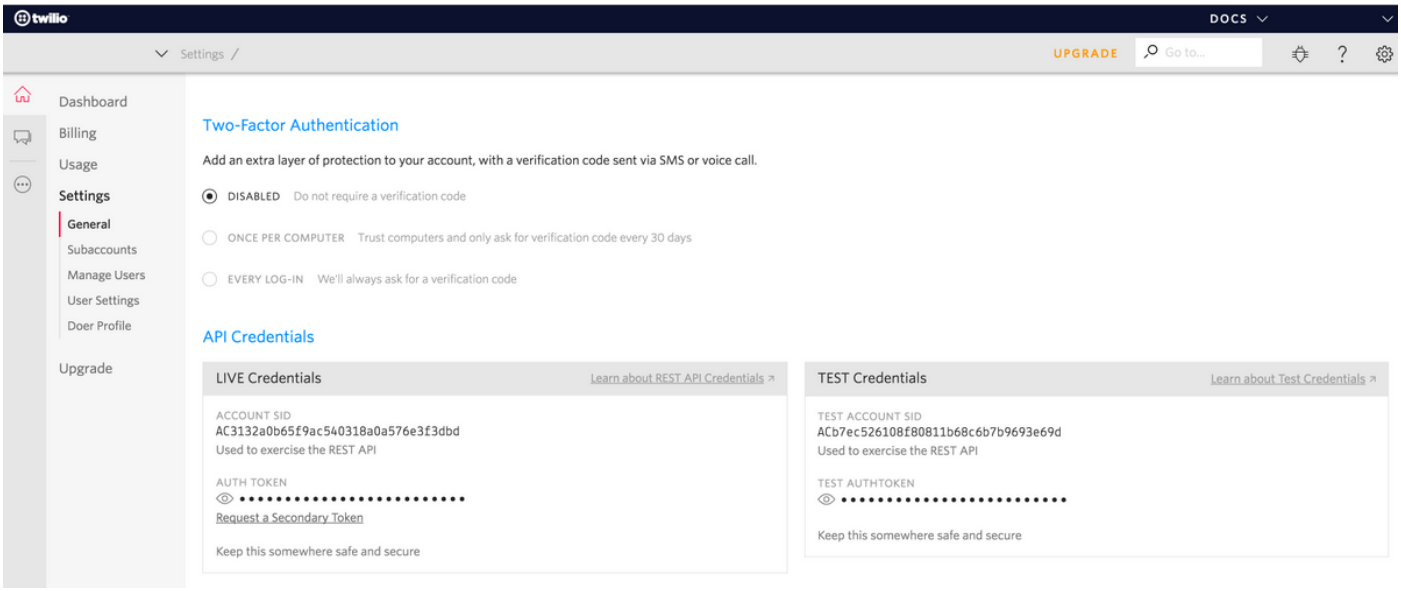




B. Twilio

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.



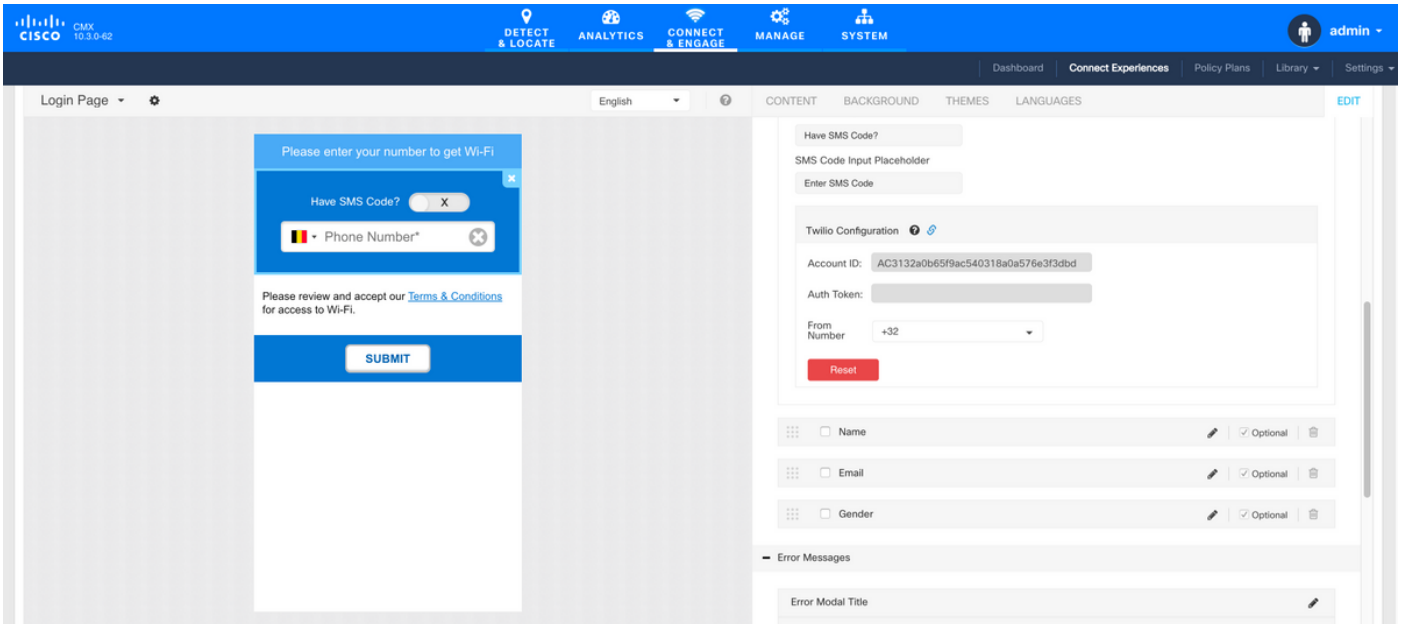
C. Configuração do CMX

Énecessário 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.

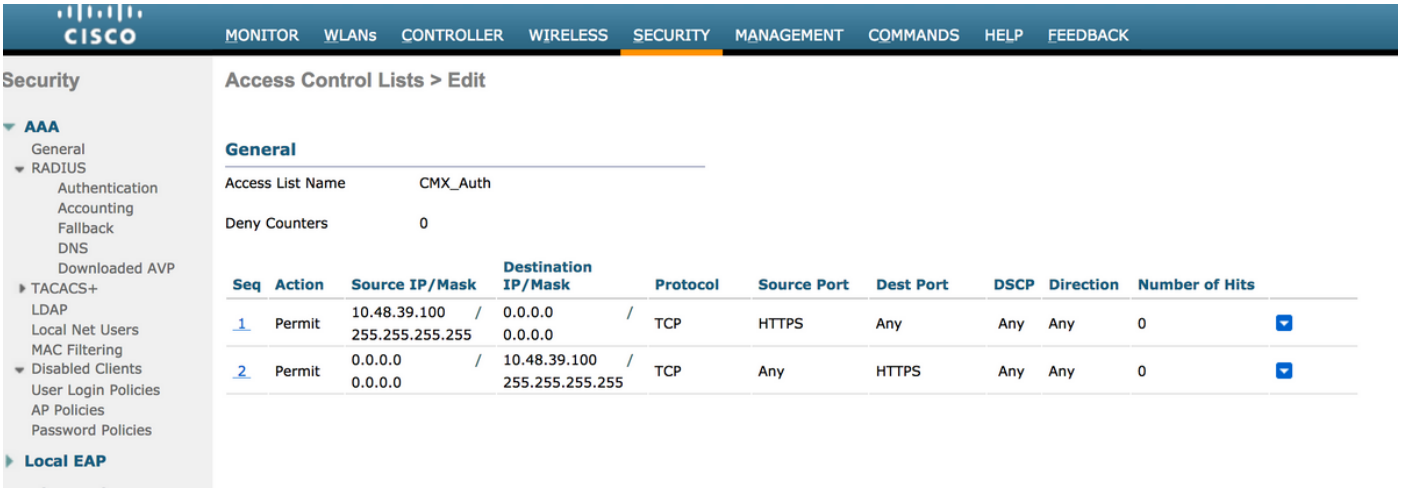
A. Configuração de WLC

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

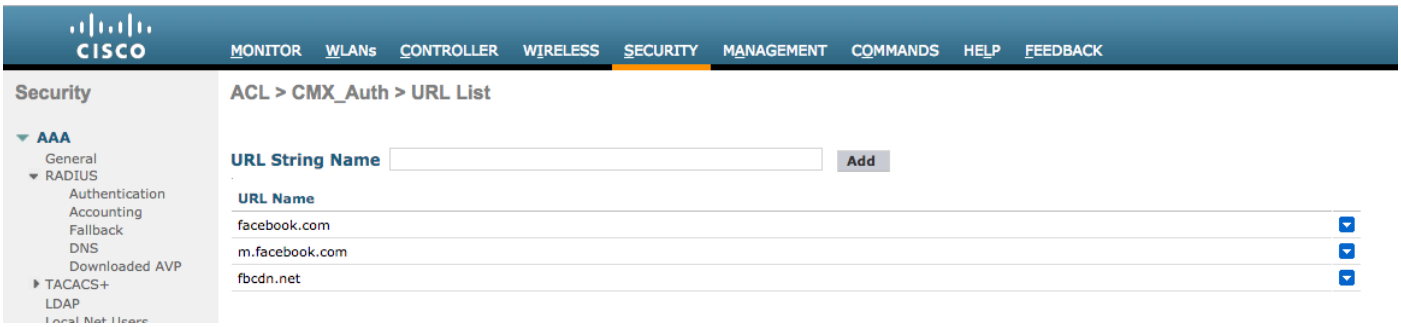
1. ACL

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)



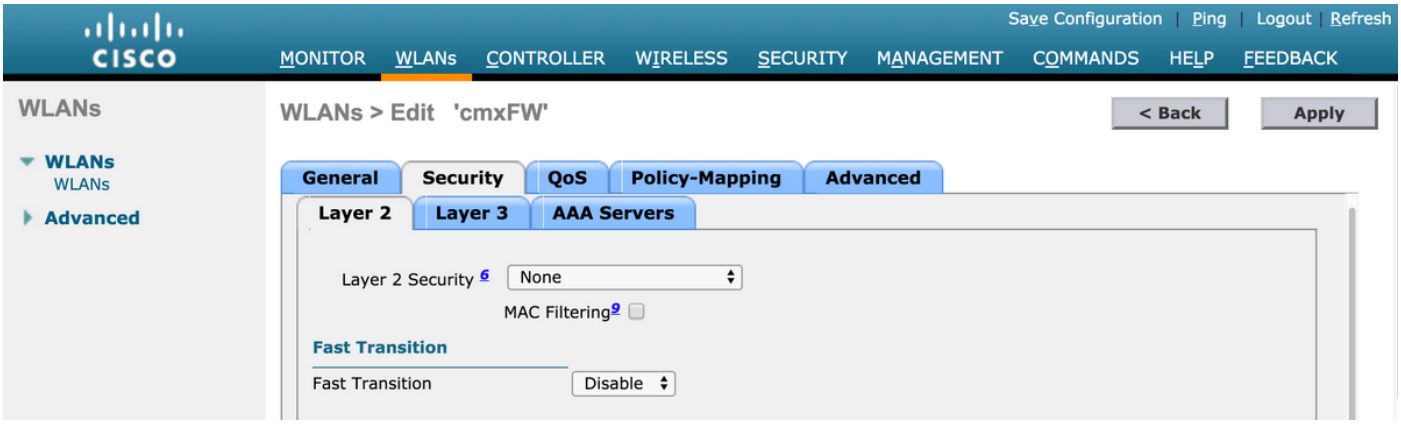
Também é necessário ter uma ACL DNS com URLs do Facebook. Para isso, em Security ->Access Control Lists (Segurança ->Listas de controles de acesso), localize a entrada da ACL configurada anteriormente (neste caso, CMX_Auth) e mova o mouse para a seta azul no final da entrada e selecione Add-Remove URL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

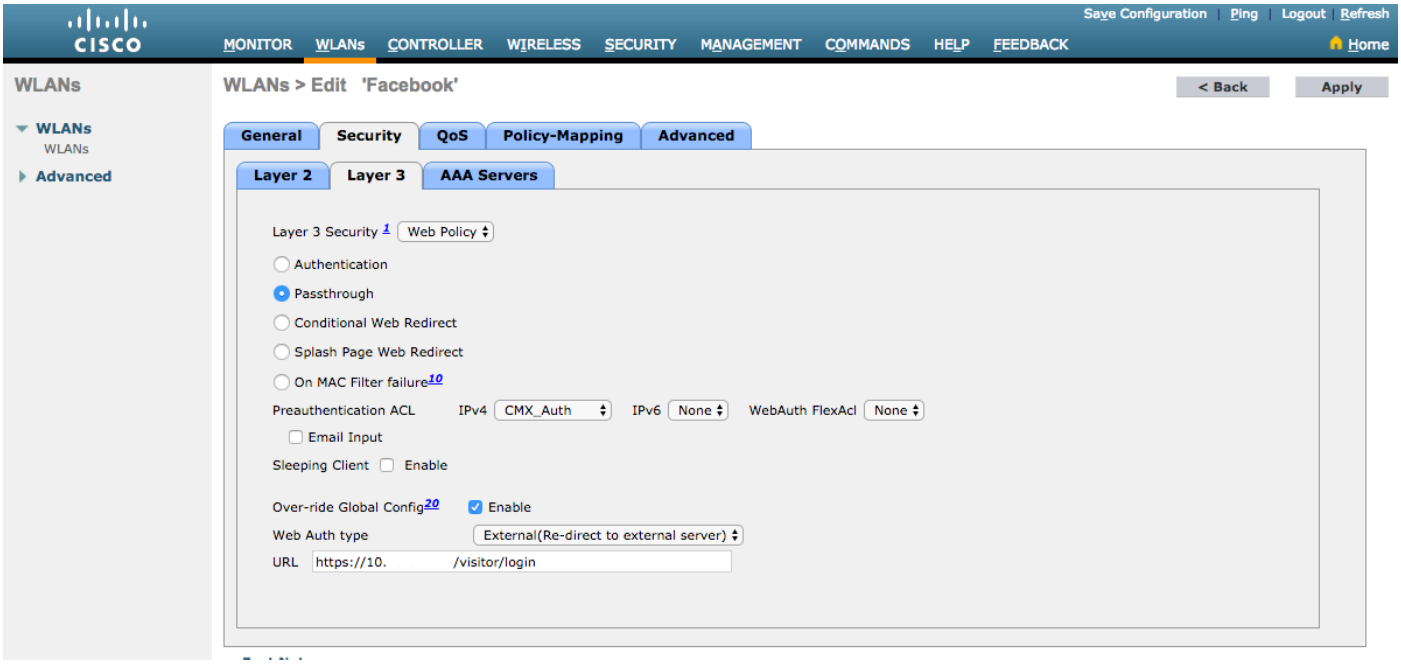


2. WLAN

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.



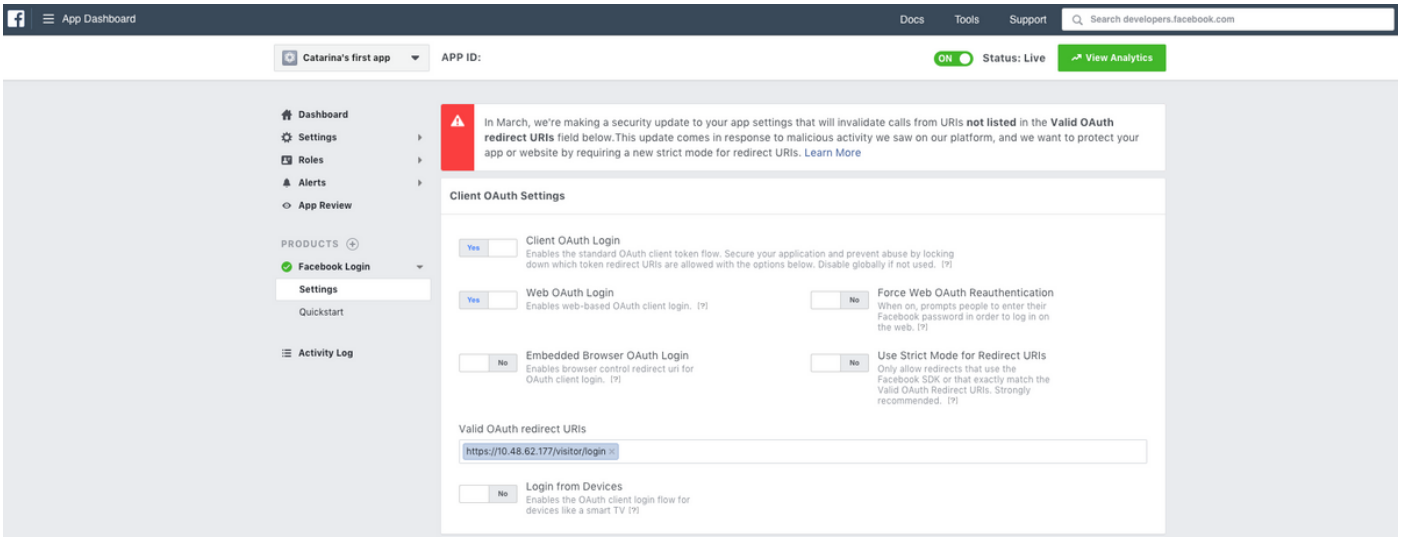


B. Facebook para desenvolvedores

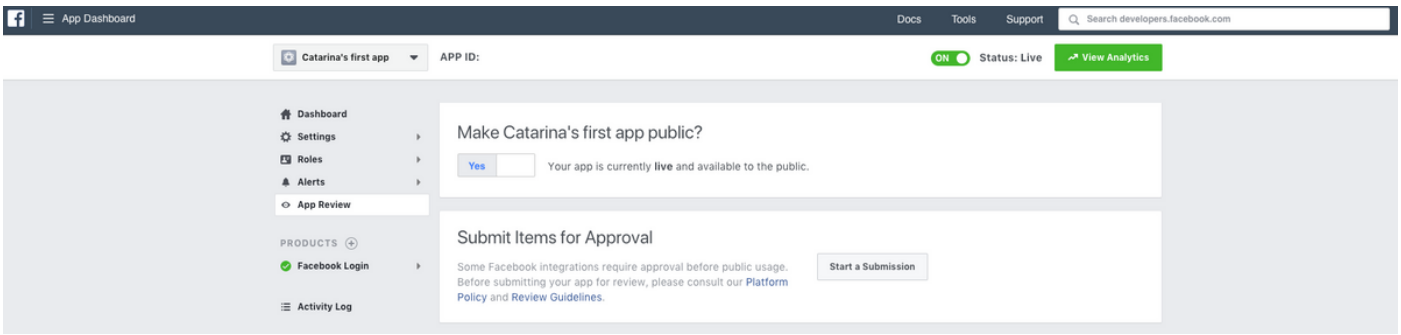
Para a integração do Facebook e CMX, é necessário um aplicativo do Facebook para que os tokens corretos sejam trocados entre as duas partes.

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.



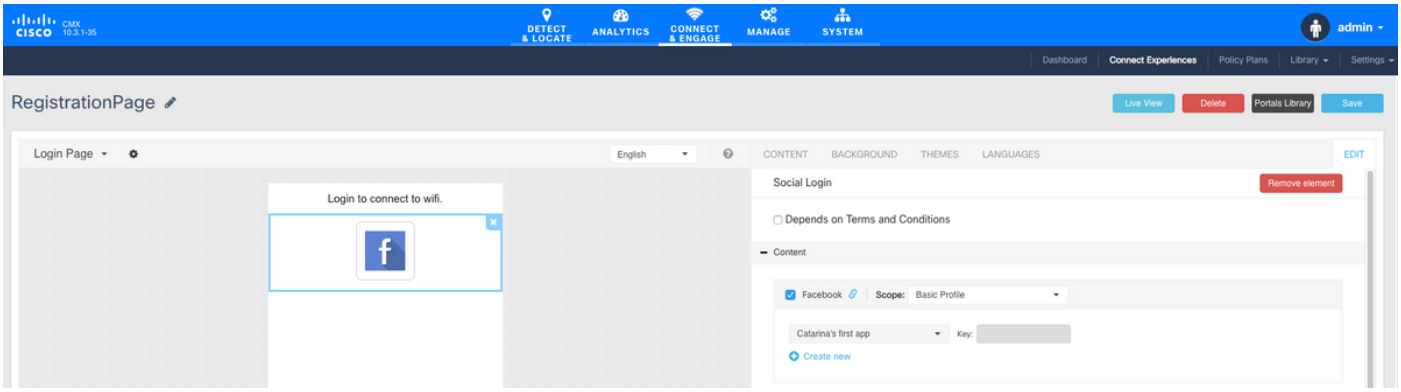
C. Configuração do CMX

Énecessário 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

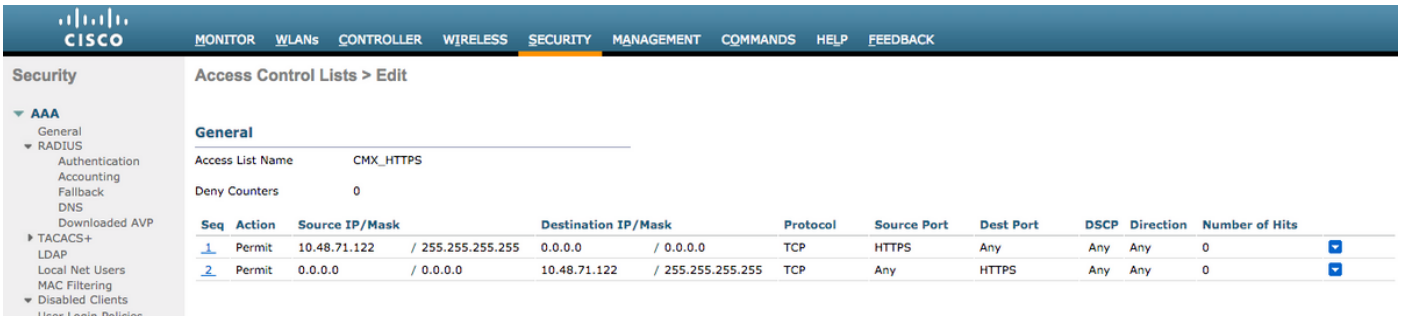
No lado da WLC, o SSID e a ACL serão configurados. O AP deve ser associado ao controlador e ao estado RUN.

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.

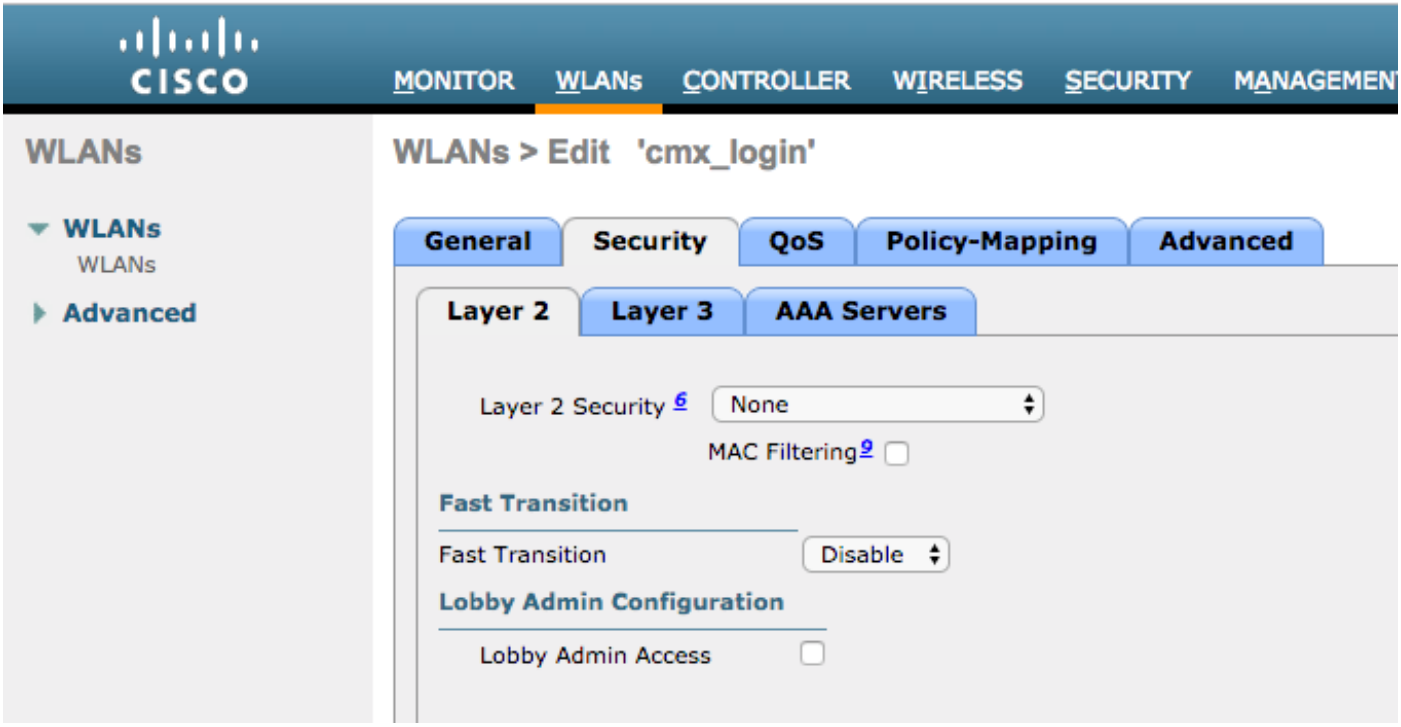


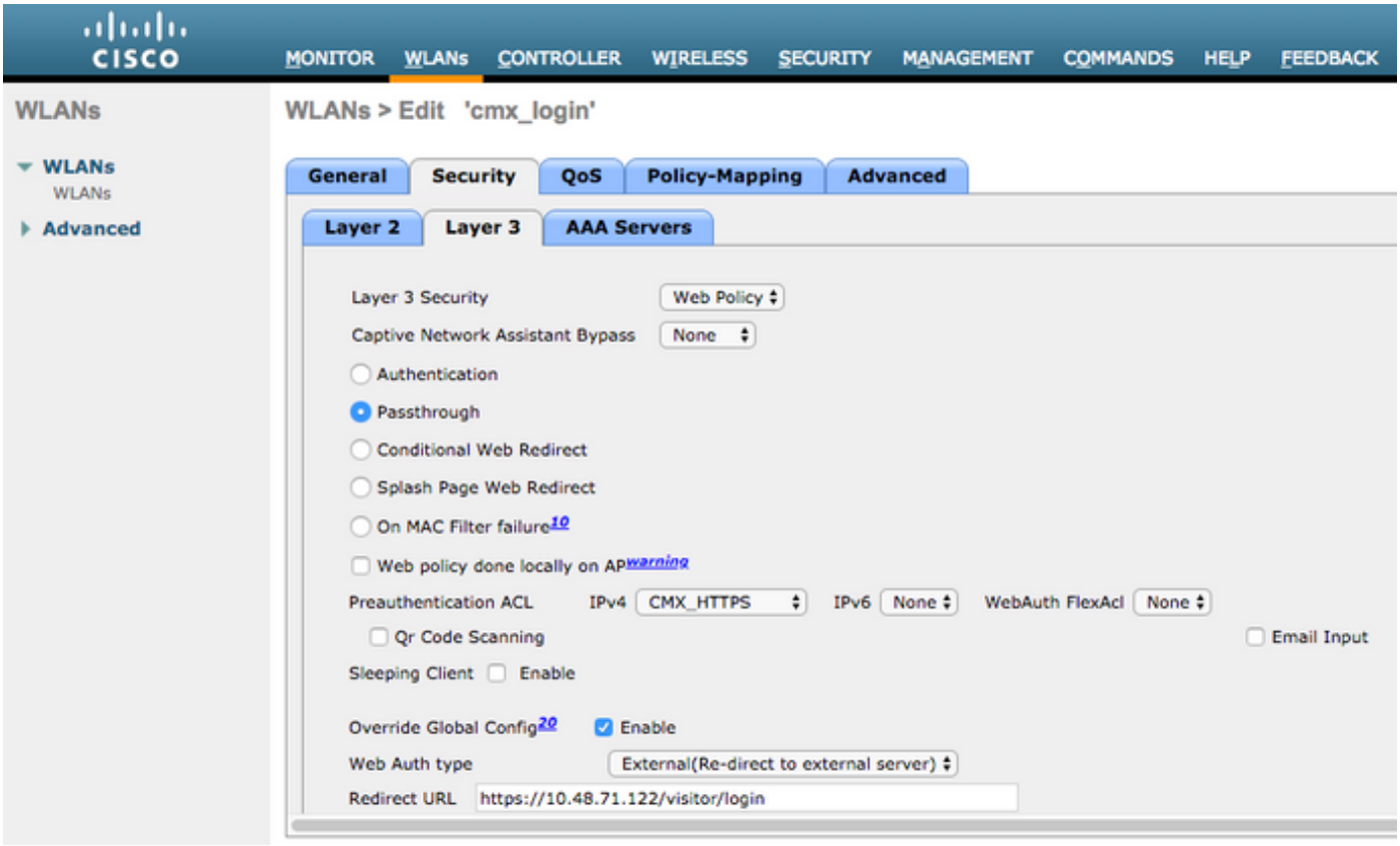
2. WLAN

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.





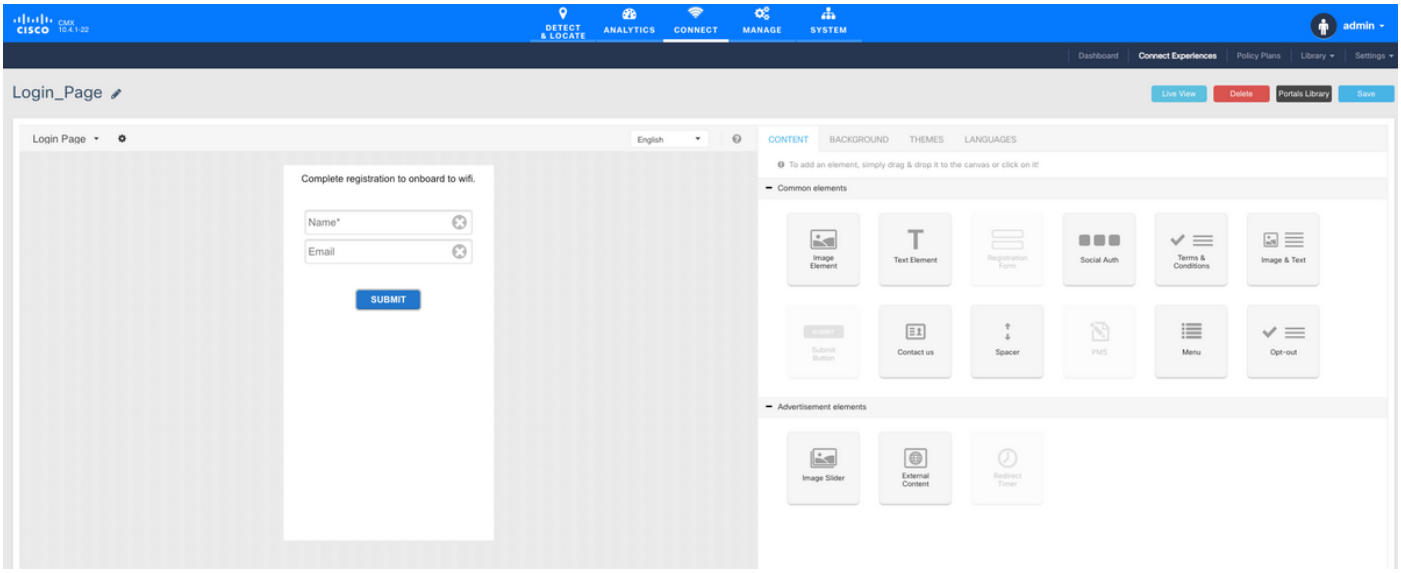
C. Configuração do CMX

Énecessário 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.

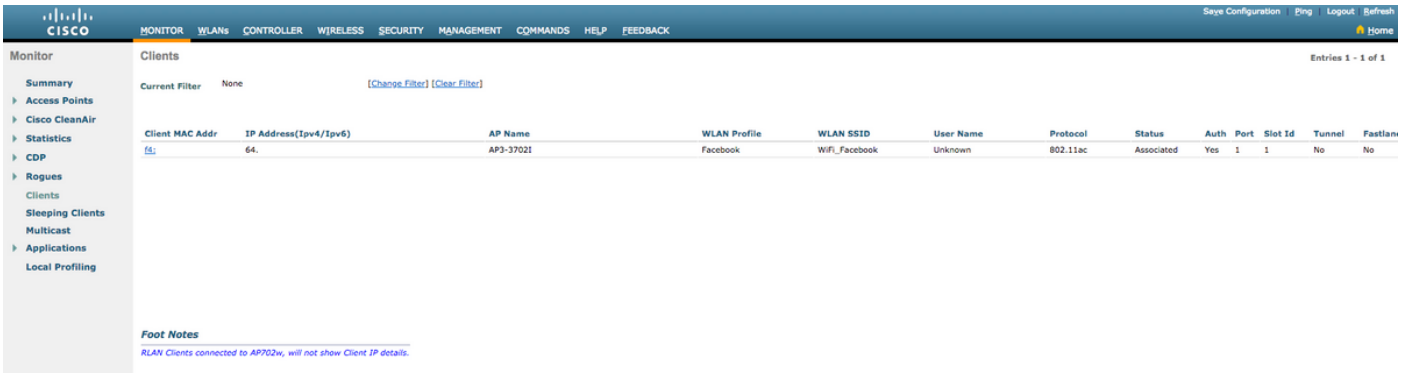
O portal para registro normal pode ser feito do zero (selecione "Personalizado") ou adaptado do modelo "Formulário de registro" disponível na biblioteca CMX.



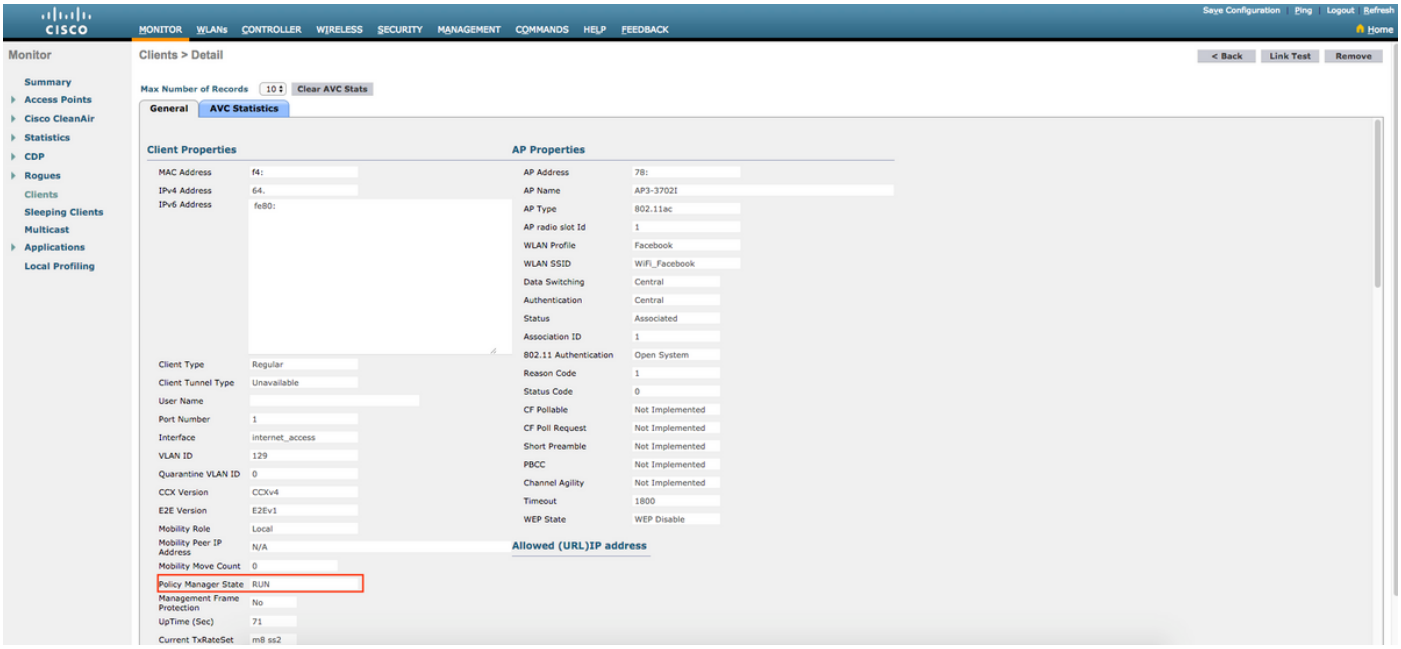
Verificar

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:

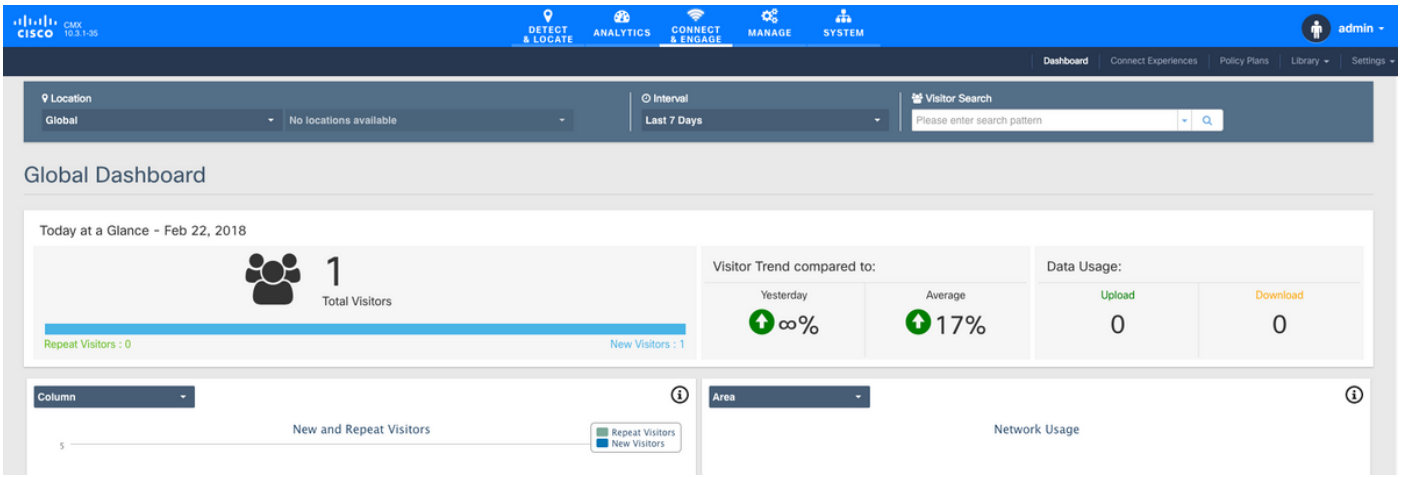


Clique no endereço MAC do cliente e, nos detalhes, confirme se o estado do Policy Manager do cliente está no estado RUN:

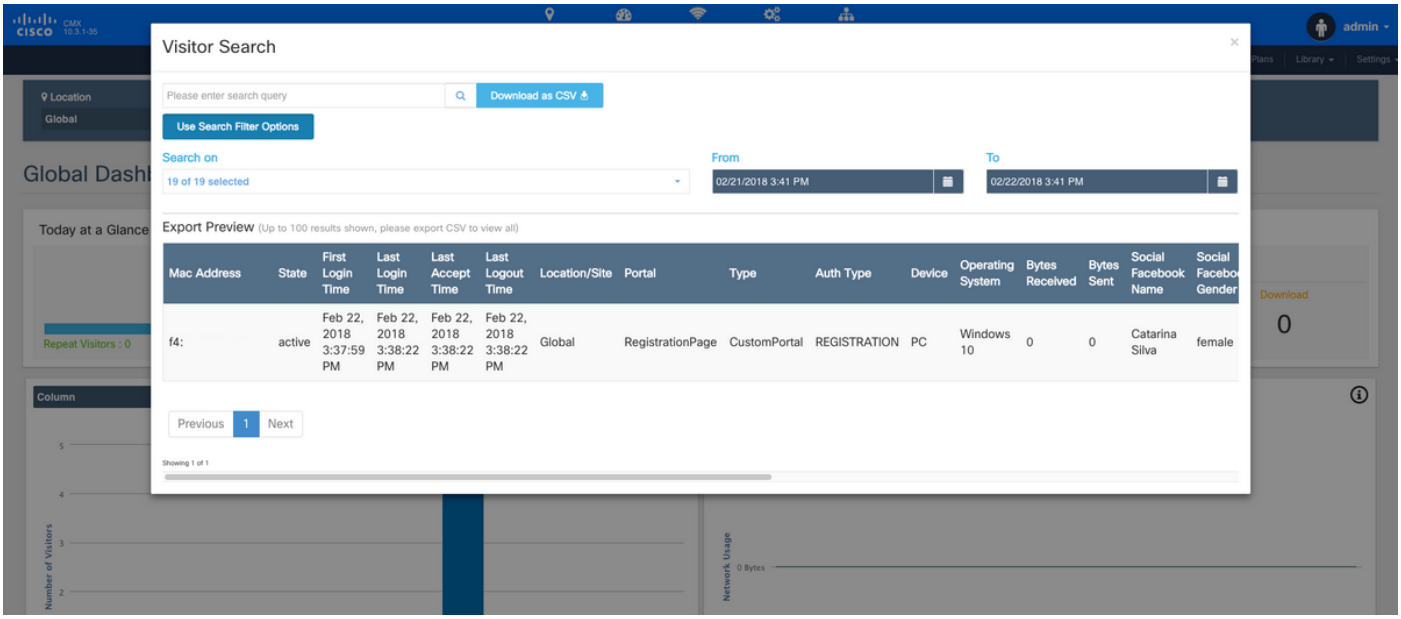


CMX

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



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



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.