Experiencias conectadas de CMX: ejemplo de configuración de registro de portal personalizado, SMS y social

Contenido

Introducción

Este documento tiene como objetivo guiar a los administradores de red a través del registro de clientes a través de la configuración de portales invitados en Connected Mobile eXperience (CMX).

CMX permite a los usuarios registrarse y autenticarse en la red a través de Social Registration Login, SMS y Custom Portal. En este documento, se puede encontrar una descripción general de los pasos de configuración en el controlador de LAN inalámbrica (WLC) y CMX.

Prerequisites

Requirements

CMX debe configurarse correctamente con la configuración base.

La exportación de mapas desde Prime Infrastructure es opcional.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

Configurar

Diagrama de la red

En este documento se describen dos formas diferentes de autenticar usuarios/clientes en la red inalámbrica, utilizando CMX.

En primer lugar, se describirá la configuración de la autenticación mediante cuentas de redes sociales y, a continuación, la autenticación mediante SMS.

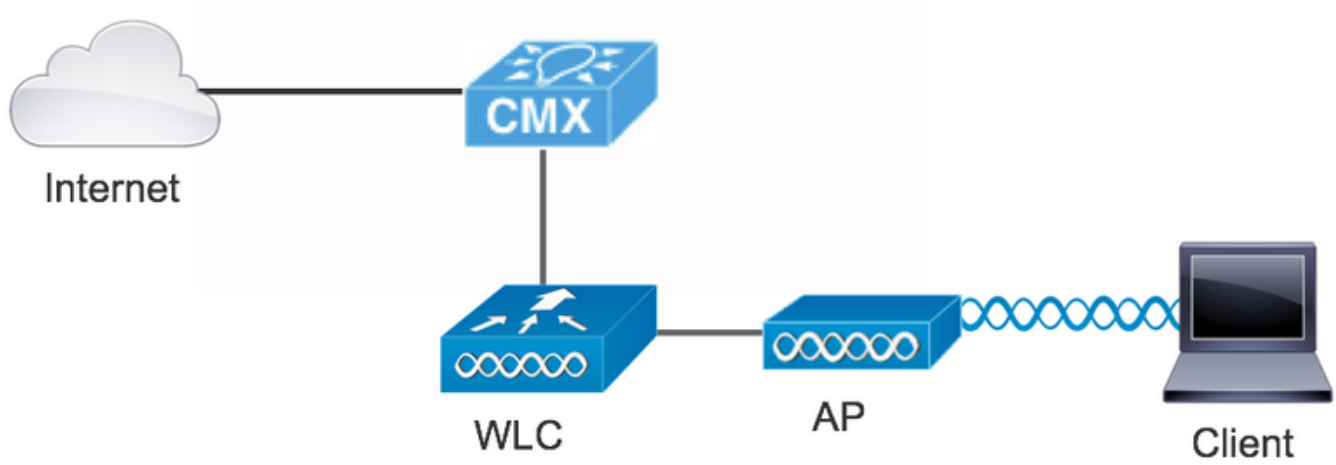
En ambos escenarios, el cliente intentará registrarse en el SSID mediante la autenticación a través de CMX.

El WLC redirige el tráfico HTTP a CMX donde se le pide al usuario que se autentique. El CMX contiene la configuración del portal que se utilizará para que el cliente se registre, tanto a través de cuentas sociales como de SMS.

A continuación se describe el flujo del proceso de registro:

1. El cliente intenta unirse al SSID y abre el navegador.
2. En lugar de tener acceso al sitio solicitado, el WLC redirige al portal de invitados.
3. El cliente proporciona sus credenciales e intenta autenticarse.
4. CMX se ocupa del proceso de autenticación.
5. Si se realiza correctamente, ahora se proporciona acceso completo a Internet al cliente.
6. El cliente se redirige al sitio solicitado inicial.

La topología utilizada es:



Configuraciones

Autenticación vía SMS

Cisco CMX permite la autenticación del cliente a través de SMS. Este método requiere configurar una página HTML para que el usuario pueda proporcionar sus credenciales al sistema.CMX proporciona de forma nativa las plantillas predeterminadas, que pueden editarse posteriormente o reemplazarse por una personalizada.

El servicio de mensajes de texto se realiza mediante la integración de CMX con Twilio, una

plataforma de comunicaciones en la nube que permite enviar y recibir mensajes de texto. Twilio permite tener un número de teléfono por portal, lo que significa que si se utiliza más de un portal, se requiere un número de teléfono por portal.

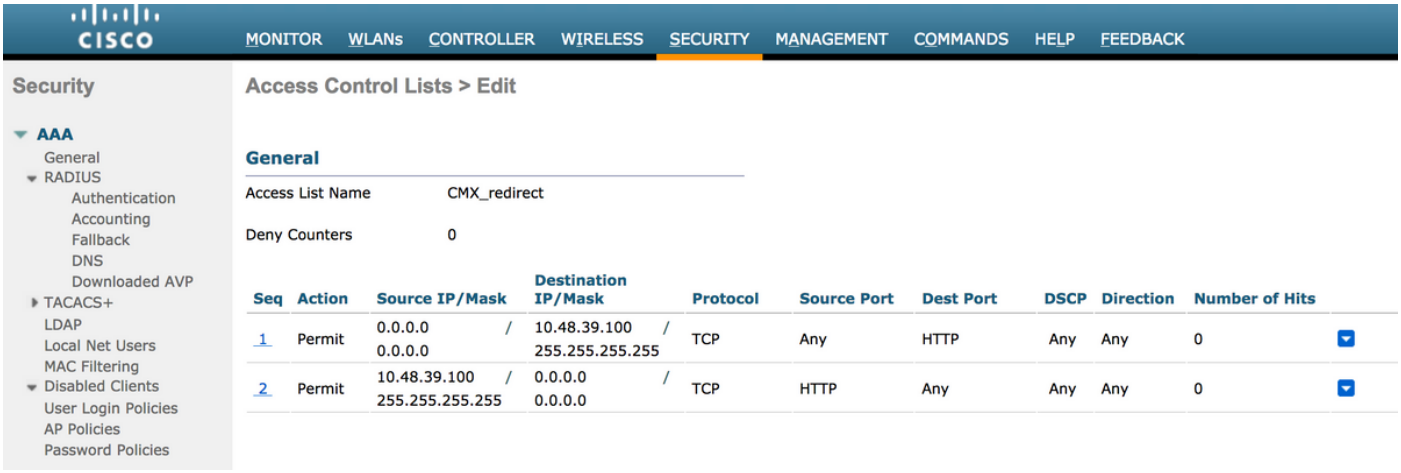
A. Configuración de WLC

En el lado del WLC, se configurará un SSID y una ACL. El AP se debe unir al controlador y en el estado RUN.

1. ACL

Se requiere una ACL que permita el tráfico HTTP, configurada en el WLC. Para configurar una ACL, vaya a Security->Access Control Lists ->Add New Rule (Seguridad->Listas de control de acceso->Agregar nueva regla.

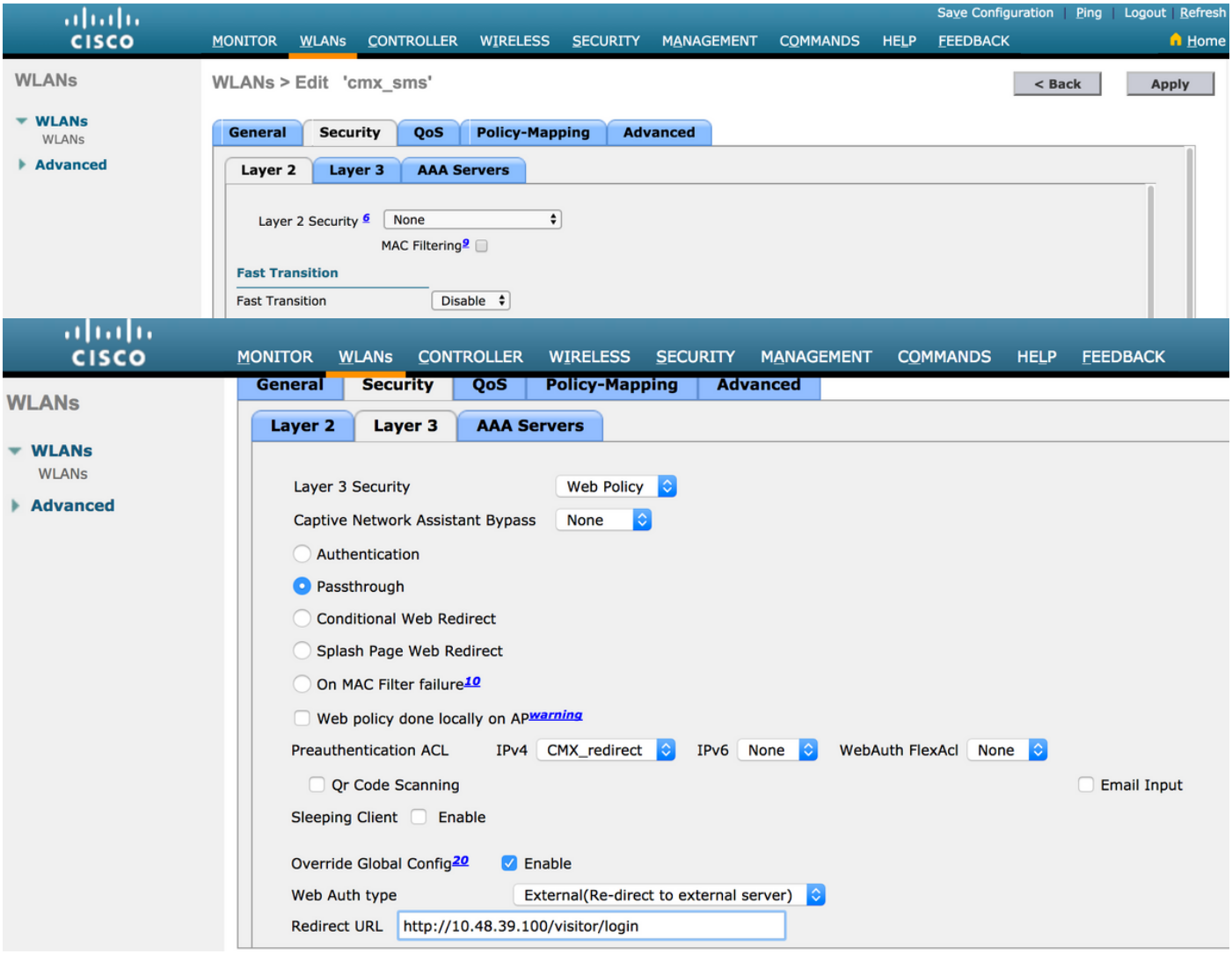
La IP que se utiliza es la configurada para el CMX. Esto permite el tráfico HTTP entre el WLC y el CMX. La siguiente figura muestra la ACL creada donde "10.48.39.100" se refiere a la dirección ip CMX.



2. WLAN

Por lo tanto, se realiza la integración con el portal, se deben realizar cambios en las políticas de seguridad en la WLAN.

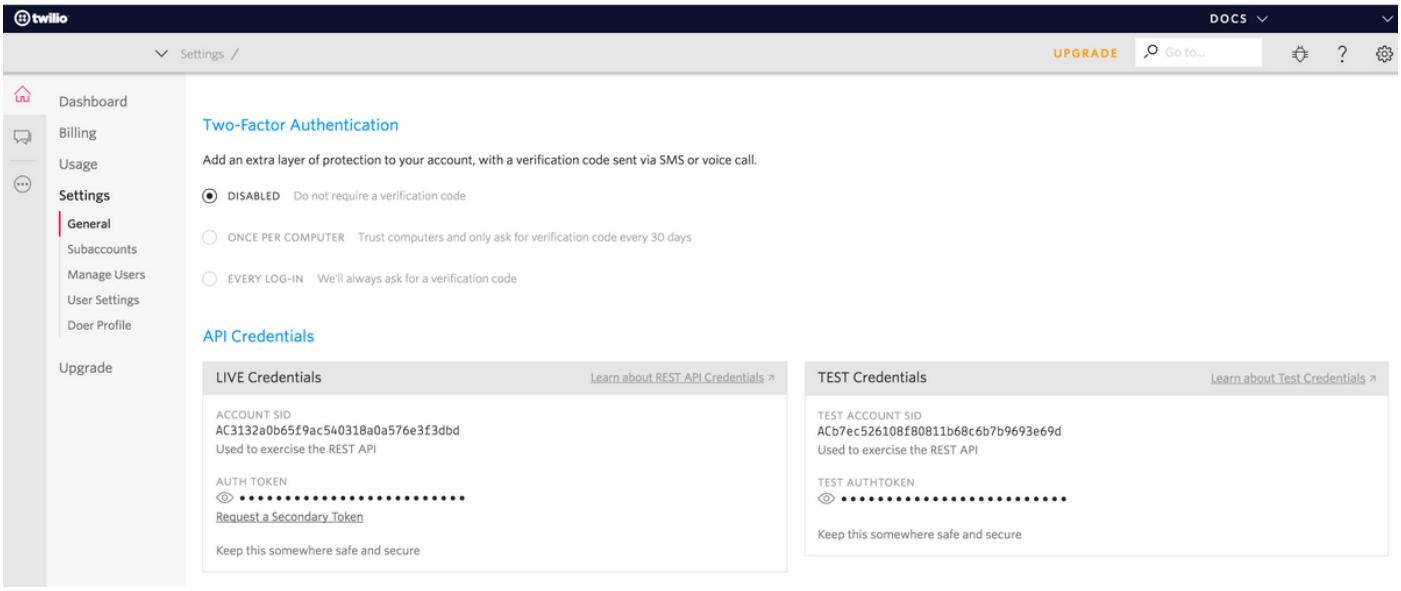
Primero, acceda a WLANs->Edit->Layer 2->Layer 2 Security y, en el menú desplegable, elija None (Ninguno), de modo que la seguridad de la capa 2 esté inhabilitada. A continuación, en la misma ficha Security (Seguridad), cambie a Layer 3 (Capa 3). En el menú desplegable Layer 3 Security (Seguridad de capa 3), seleccione Web Policy (Política web) y, a continuación, Passthrough (Paso a través). En ACL de autenticación previa, seleccione la ACL IPv4 configurada previamente para enlazarla a la WLAN respectiva donde se debe proporcionar la autenticación SMS. La opción Over-ride Global Config debe estar habilitada y el tipo Web Auth debe ser External (Redirigir a servidor externo), para que los clientes puedan ser redirigidos al servicio CMX. La URL debe ser la misma que el portal de autenticación CMX SMS, con el formato http://<CMX-IP>/visitor/login .



B Twilio

CMX proporciona integración Twilio para los servicios de mensajes de texto. Las credenciales se proporcionan después de que la cuenta de Twilio esté configurada correctamente. Se necesitan SID de CUENTA y TOKEN AUTH.

Twilio tiene sus propios requisitos de configuración, documentados a través del proceso de configuración del servicio. Antes de integrarse con CMX, se puede probar el servicio Twilio, lo que significa que se pueden detectar problemas relacionados con la configuración de Twilio antes de utilizarlo con CMX.



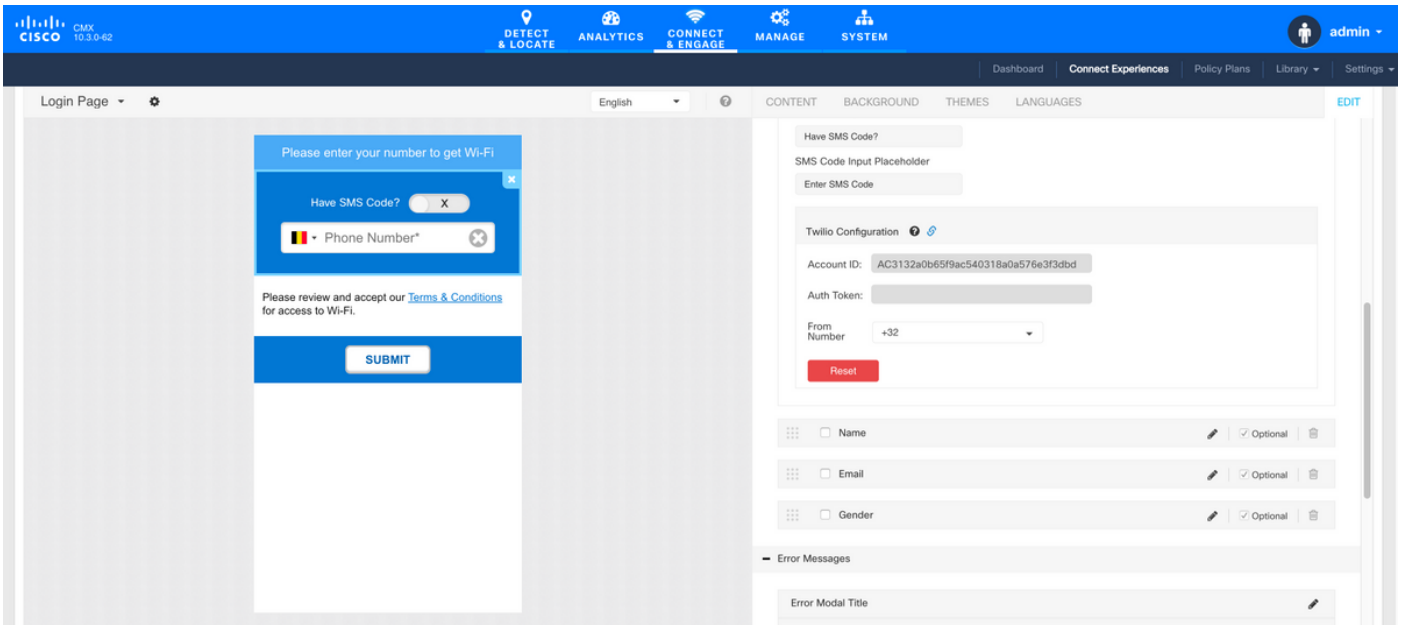
C. Configuración CMX

Es necesario que el controlador se agregue correctamente al CMX y que los mapas se exporten desde Prime Infrastructure.

- Página de registro de SMS

Hay una plantilla predeterminada para el portal de registro. Se pueden encontrar portales seleccionando CONNECT&ENGAGE->Library. Si desea una plantilla, seleccione Plantillas en el menú desplegable.

Para integrar Twilio con el portal, vaya a Configuración de Twilio y proporcione el ID de cuenta y el token de autenticación. Si la integración se realiza correctamente, aparecerá el número utilizado en la cuenta Twilio.



Autenticación a través de cuentas de redes sociales

La autenticación del cliente mediante cuentas de redes sociales requiere que el administrador de

la red agregue un identificador de APP de Facebook válido en el CMX.

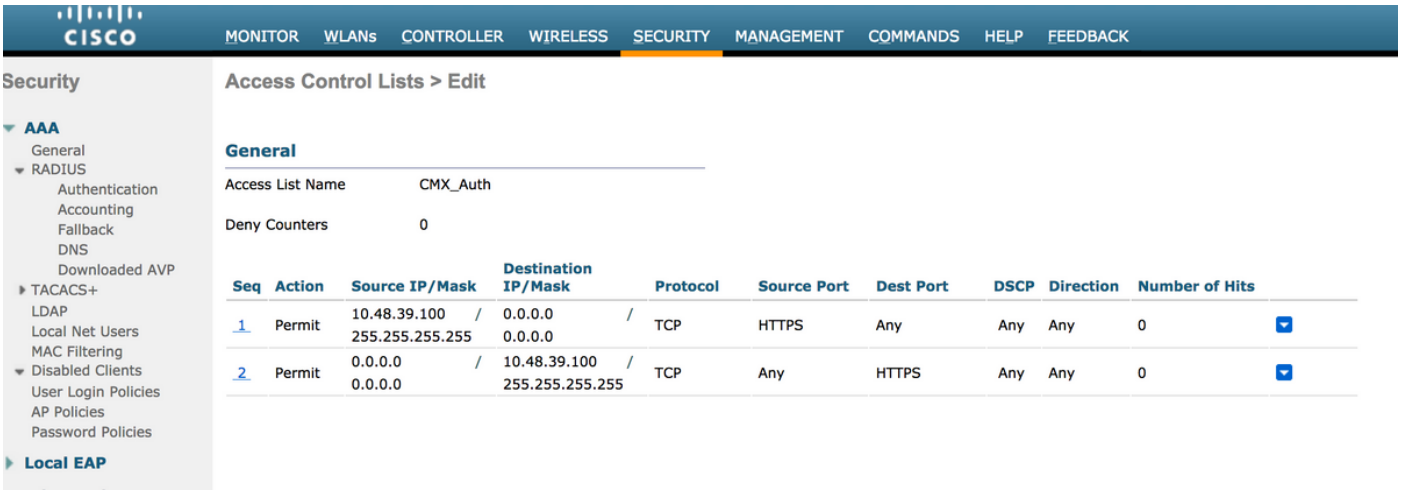
A. Configuración de WLC

En el lado del WLC, se configurará un SSID y una ACL. El AP debe unirse al controlador y en el estado RUN.

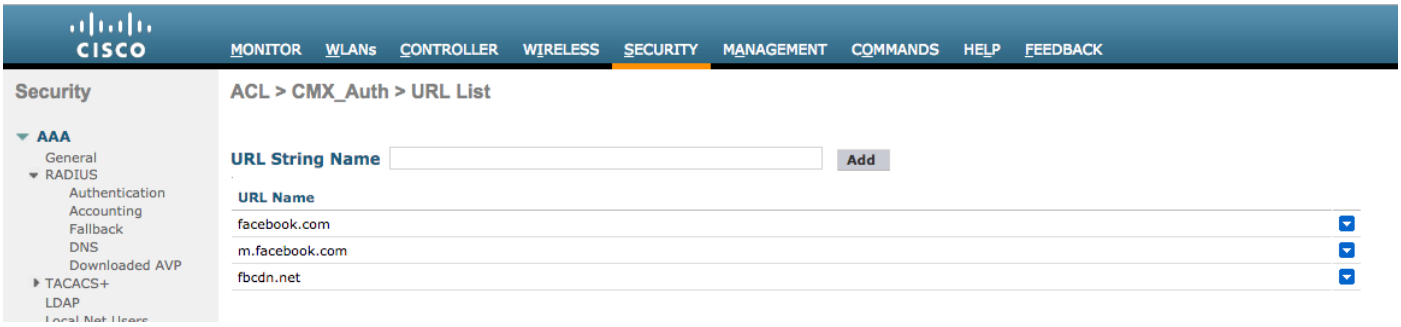
1. ACL

Como aquí estamos usando HTTPS como método de autenticación, una ACL que permita el tráfico HTTPS se debe configurar en el WLC. Para configurar una ACL, vaya a Security->Access Control Lists ->Add New Rule (Seguridad->Listas de control de acceso->Agregar nueva regla.

La IP CMX debe usarse para permitir el tráfico HTTPS entre el WLC y el CMX. (en este ejemplo, la ip CMX es 10.48.39.100)



También es necesario tener una ACL DNS con URL de Facebook. Para ello, en Security ->Access Control Lists (Seguridad -> Listas de control de acceso) busque la entrada de la ACL configurada previamente (en este caso CMX_Auth) y mueva el ratón a la flecha azul al final de la entrada y seleccione Add-Remove URL (Agregar-Eliminar URL). Después de ese tipo, escriba las URL de Facebook en el nombre de cadena de URL y Agregar.

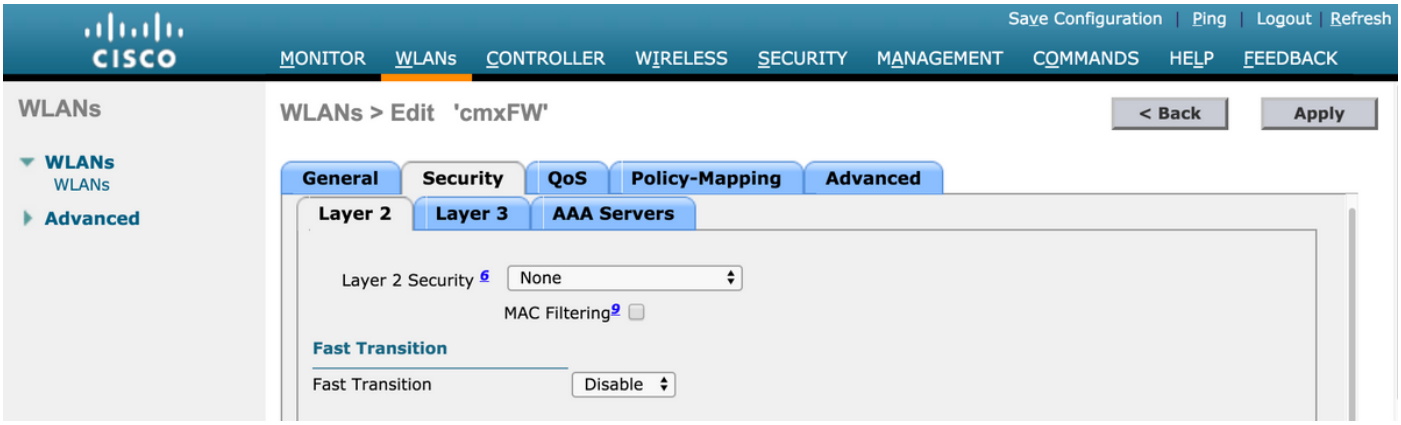


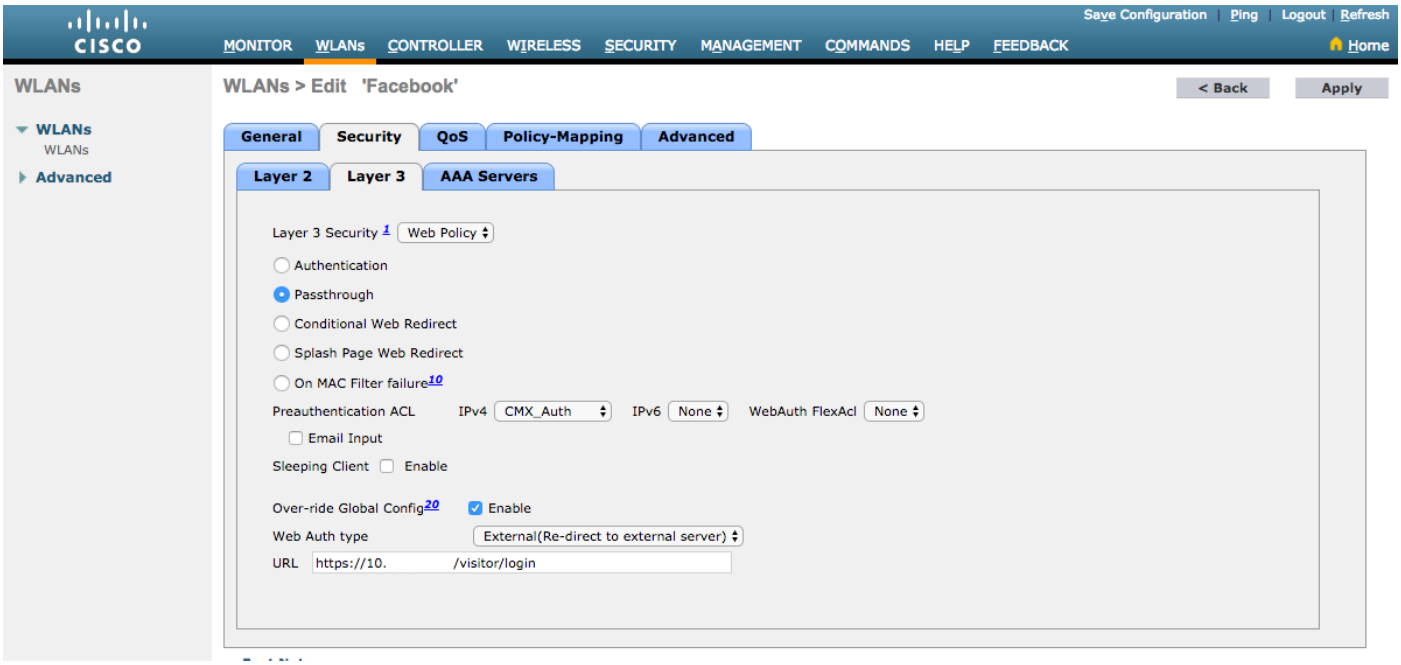
2. WLAN

Las políticas de seguridad cambian para que el Registro funcione y requieren que se realice una configuración específica en la WLAN.

Como se hizo anteriormente para el registro de SMS, primero, llegó a WLANs ->Edit->Layer 2->Layer 2 Security y, en el menú desplegable, elija None, por lo que la seguridad de la capa 2 está desactivada. En la misma ficha Seguridad, cambie a Capa 3. En el menú desplegable Layer 3

Security (Seguridad de capa 3), seleccione Web Policy (Política web) y, a continuación, Passthrough (Paso a través). En ACL de autenticación previa, seleccione la ACL IPv4 configurada previamente para enlazarla a la WLAN respectiva donde se debe proporcionar la autenticación a través de Facebook. La opción Over-ride Global Config debe estar habilitada y el tipo Web Auth debe ser External (Redirigir a servidor externo), para que los clientes puedan ser redirigidos al servicio CMX. Tenga en cuenta que esta vez, la URL, debe tener el siguiente formato **https**://<CMX-IP>/visitor/login.



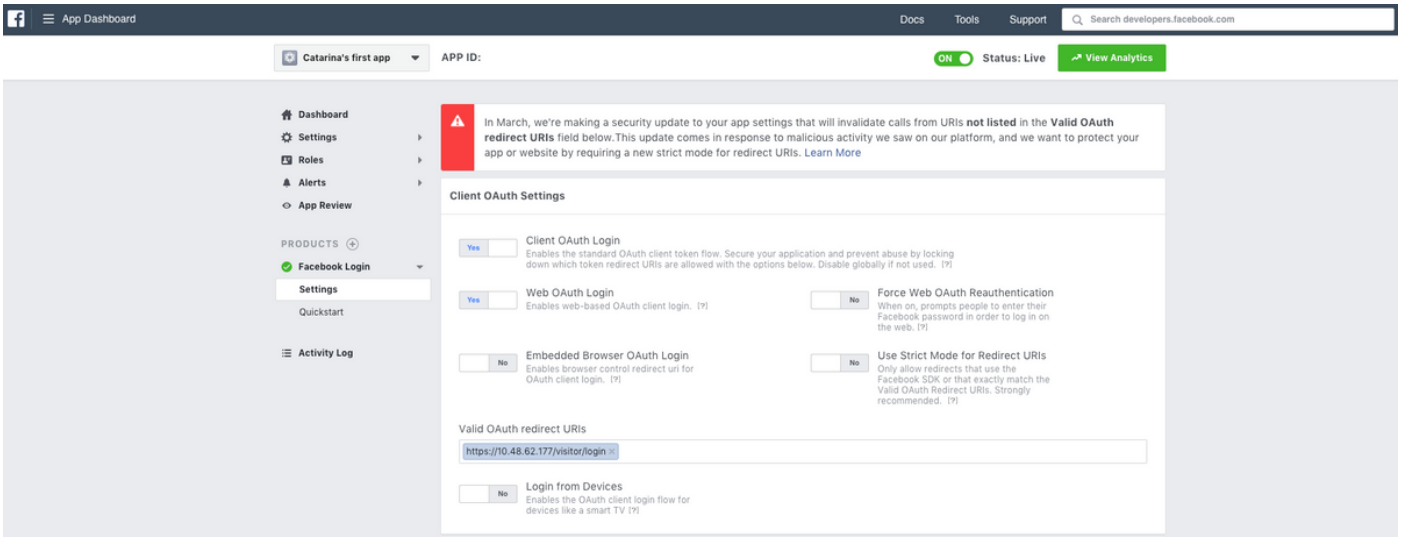


B Facebook para desarrolladores

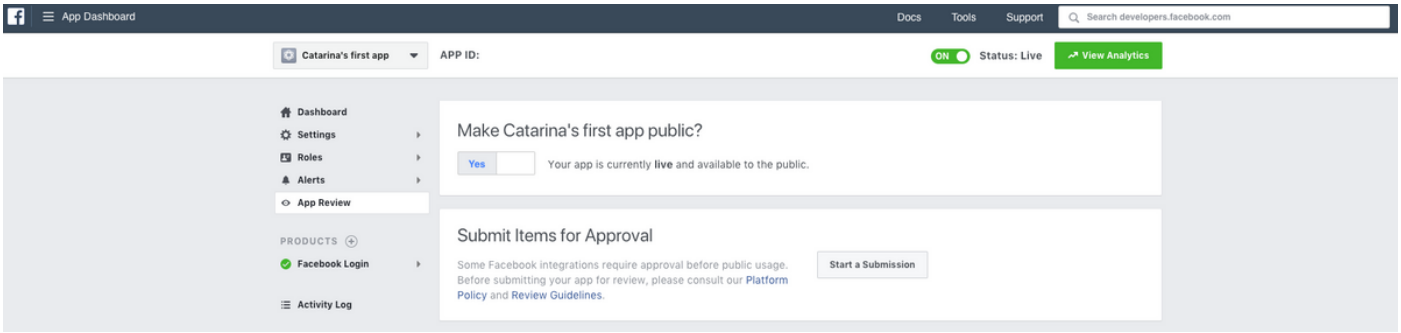
Para la integración de Facebook y CMX, se requiere una aplicación de Facebook para que se intercambien los tokens adecuados entre las dos partes.

Vaya a Facebook para desarrolladores para crear la Aplicación. Hay algunos requisitos de configuración de la aplicación para integrar los servicios.

En la configuración de la aplicación, asegúrese de que el inicio de sesión de Client OAuth y el inicio de sesión de Web OAuth estén habilitados. Además, verifique que los URI de redirección de OAuth válidos, tenga la URL CMX en el formato **https**://<CMX-IP>/visitor/login.



Para que la Aplicación se publique y esté lista para integrarse con CMX, es necesario que se haga pública. Para ello, vaya a App Review->¿Hacer público <App-Name>? y cambie el estado a Sí.



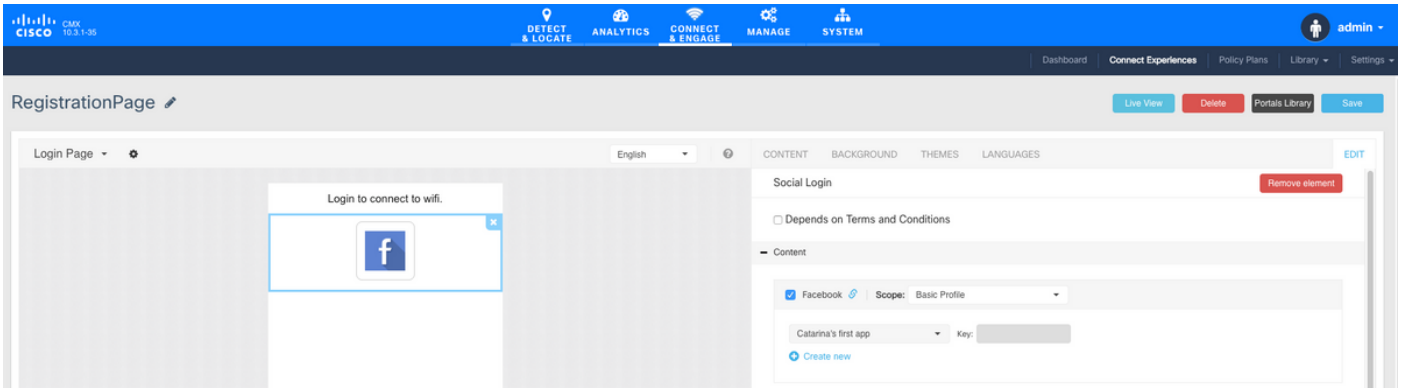
C. Configuración CMX

Es necesario que el controlador se agregue correctamente al CMX y que los mapas se exporten desde Prime Infrastructure.

- Página de registro

Para crear una página de registro en CMX, se deben realizar los mismos pasos que se hicieron anteriormente para crear la página de registro de SMS. Al seleccionar CONNECT&ENGAGE->Library, los portales de plantillas listos para editar se pueden encontrar eligiendo Plantillas en el menú desplegable.

Para registrarse a través de las credenciales de Facebook, es necesario que el portal tenga conexión a las cuentas sociales. Para hacerlo desde cero, al crear un portal personalizado, vaya a CONTENIDO->Elementos comunes->Autenticación social y seleccione Facebook. A continuación, introduzca el nombre de la aplicación y la ID de la aplicación (clave) obtenidos de Facebook.



Autenticación a través del portal personalizado

La autenticación del cliente mediante el portal personalizado es similar a la configuración de la autenticación Web externa. La redirección se realizará en el portal personalizado alojado en CMX.

A. Configuración de WLC

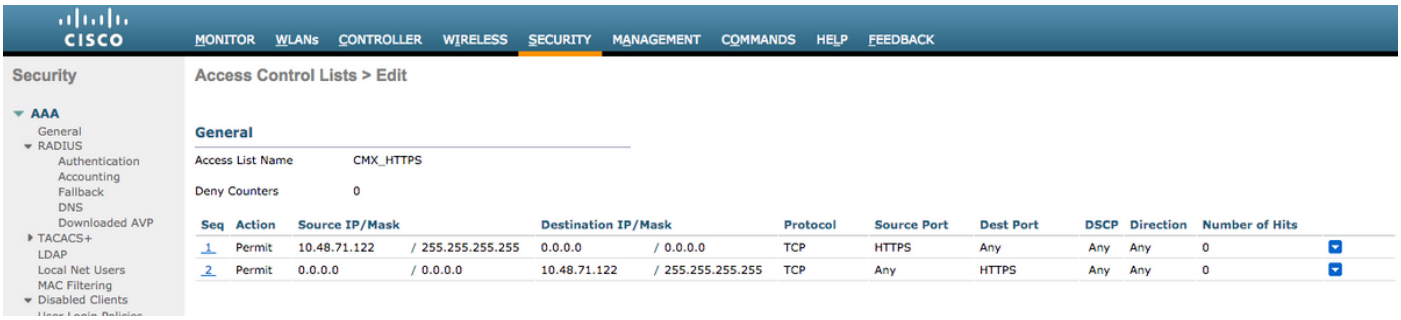
En el lado del WLC, se configurará un SSID y una ACL. El AP debe unirse al controlador y en el estado RUN.

1. ACL

Como aquí estamos usando HTTPS como método de autenticación, una ACL que permita el tráfico HTTPS se debe configurar en el WLC. Para configurar una ACL, vaya a Seguridad->Listas de control de acceso->Agregar nueva regla.

La IP CMX debe usarse para permitir el tráfico HTTPS entre el WLC y el CMX. (en este ejemplo, la IP de CMX es 10.48.71.122).

> **Nota**: Asegúrese de habilitar ssl en el CMX ejecutando el comando "cmxctl node sslmode enable" en la CLI de CMX.

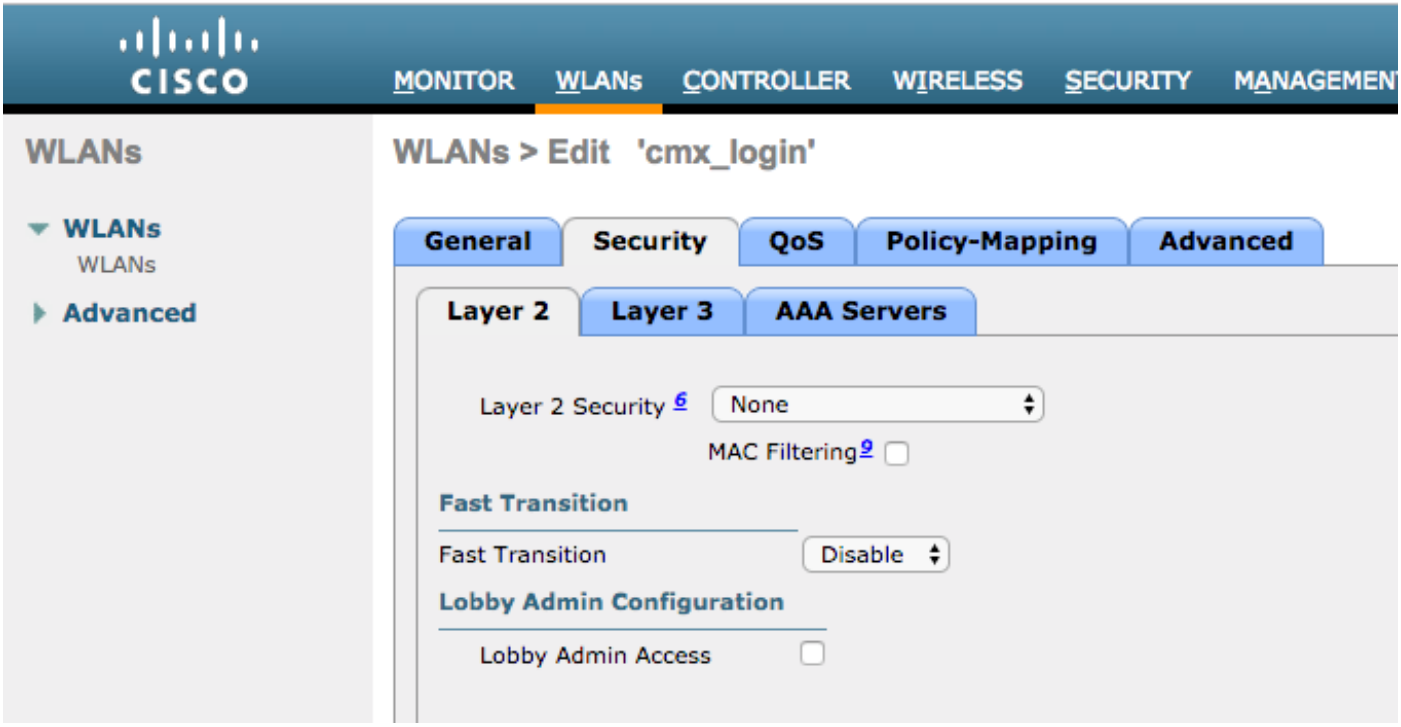


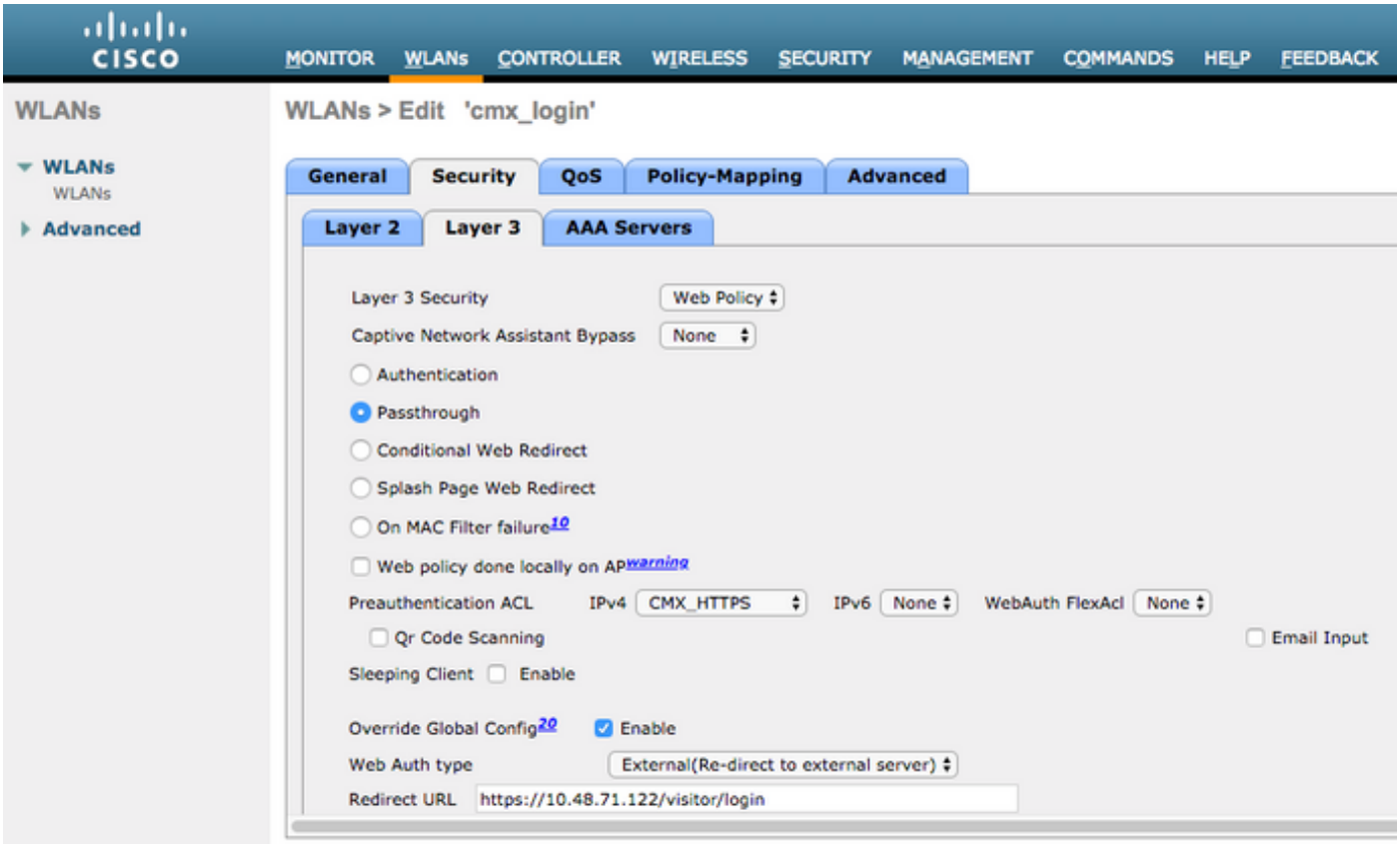
2. WLAN

Las políticas de seguridad cambian para que el Registro funcione y requieren que se realice una configuración específica en la WLAN.

Como se hizo anteriormente para el registro de SMS y redes sociales, primero, llegó a WLAN->Edit->Layer 2->Layer 2 Security y, en el menú desplegable, seleccione None (Ninguno), por lo que la seguridad de capa 2 está desactivada. En la misma ficha Seguridad, cambie a Capa 3. En el menú desplegable Layer 3 Security (Seguridad de capa 3), seleccione Web Policy (Política web) y, a continuación, Passthrough (Paso a través). En ACL de autenticación previa, seleccione

la ACL IPv4 configurada previamente (denominada CMX_HTTPS en este ejemplo) y enlace la ACL a la WLAN respectiva. La opción Over-ride Global Config debe estar habilitada y el tipo Web Auth debe ser External (Redirigir a servidor externo), para que los clientes puedan ser redirigidos al servicio CMX. Tenga en cuenta que esta vez, la URL, debe tener el siguiente formato **https**://<CMX-IP>/visitor/login.





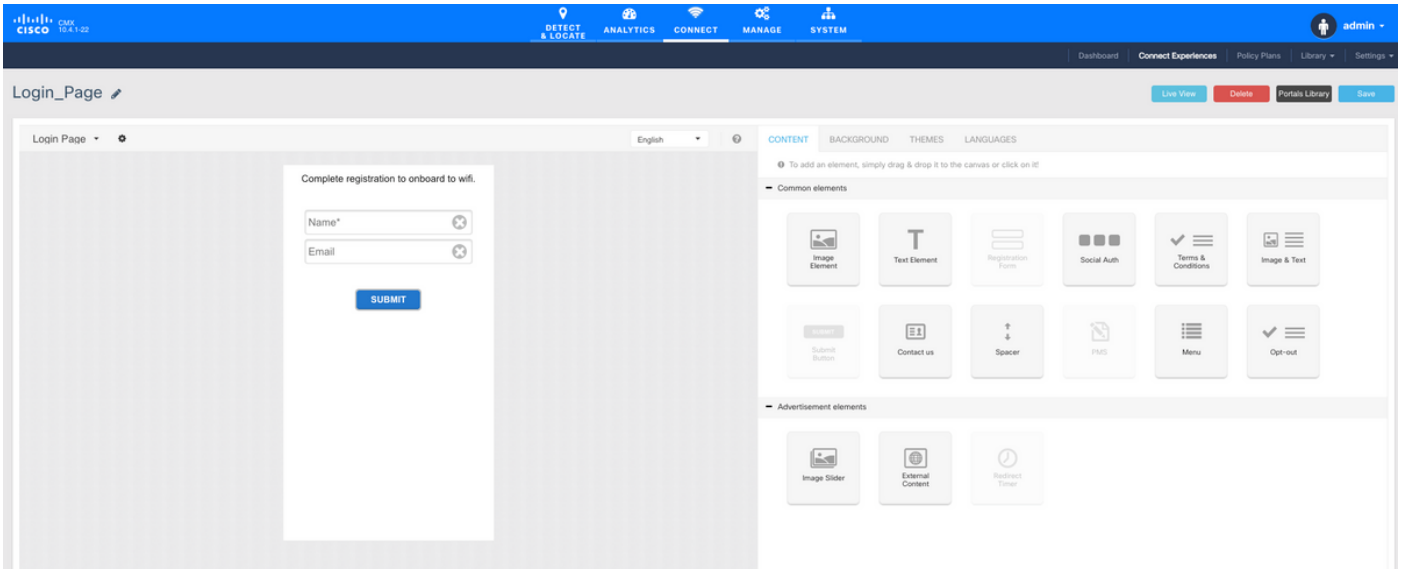
C. Configuración CMX

Es necesario que el controlador se agregue correctamente al CMX y que los mapas se exporten desde Prime Infrastructure.

- Página de registro

Para crear una página de registro en CMX, realice los mismos pasos que antes para crear la página para otros métodos de autenticación. Al seleccionar CONNECT&ENGAGE->Library, los portales de plantillas listos para ser editados se pueden encontrar eligiendo Plantillas en el menú desplegable.

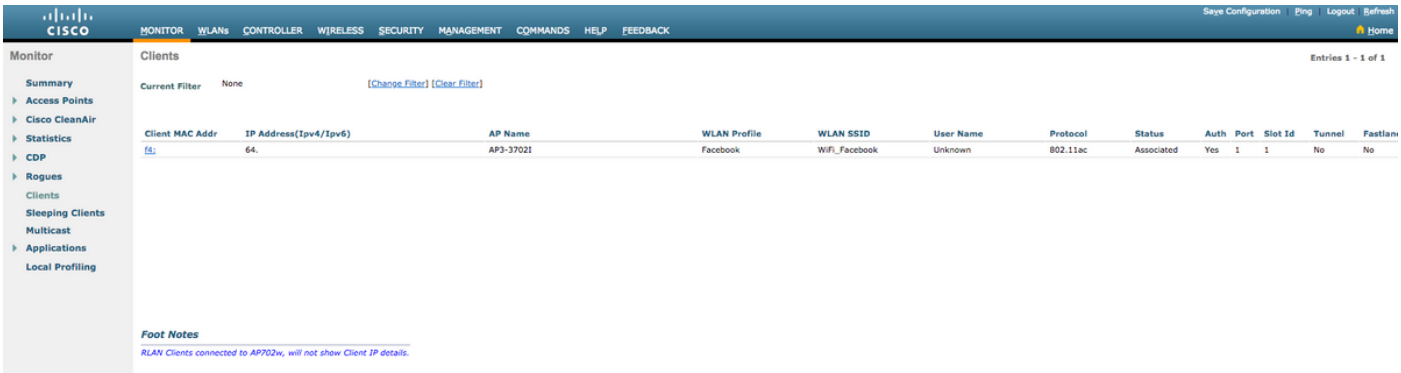
El portal para el registro normal se puede realizar desde el principio (seleccione "Personalizado") o se puede adaptar desde la plantilla "Formulario de registro" disponible en la biblioteca CMX.



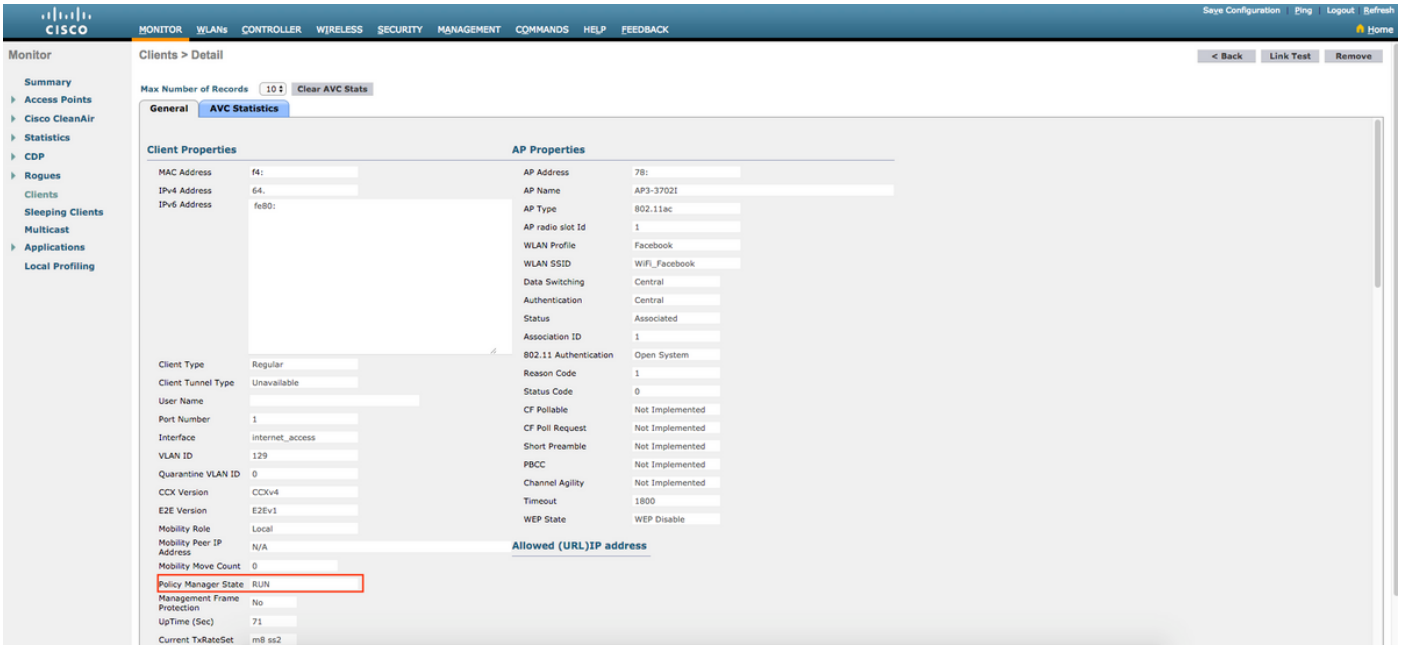
Verificación

WLC

Para verificar si el usuario se autenticó correctamente en el sistema, en la GUI del WLC, vaya a MONITOR->Clientes y busque la dirección MAC del cliente en la lista:

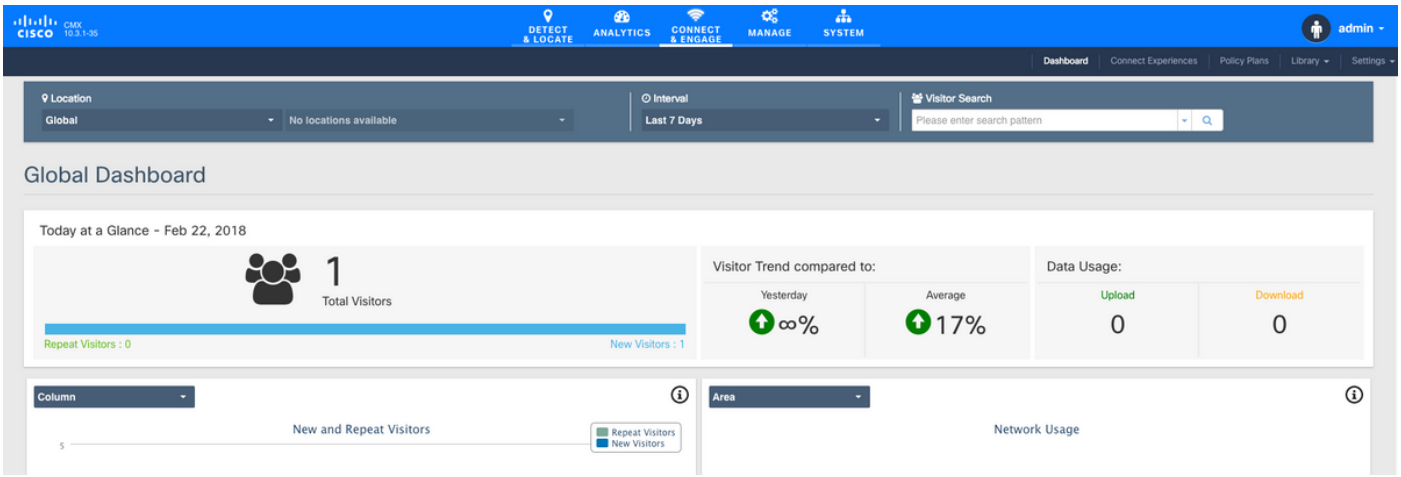


Haga clic en la dirección MAC del cliente y, en los detalles, confirme que el estado del administrador de políticas del cliente está en estado RUN:

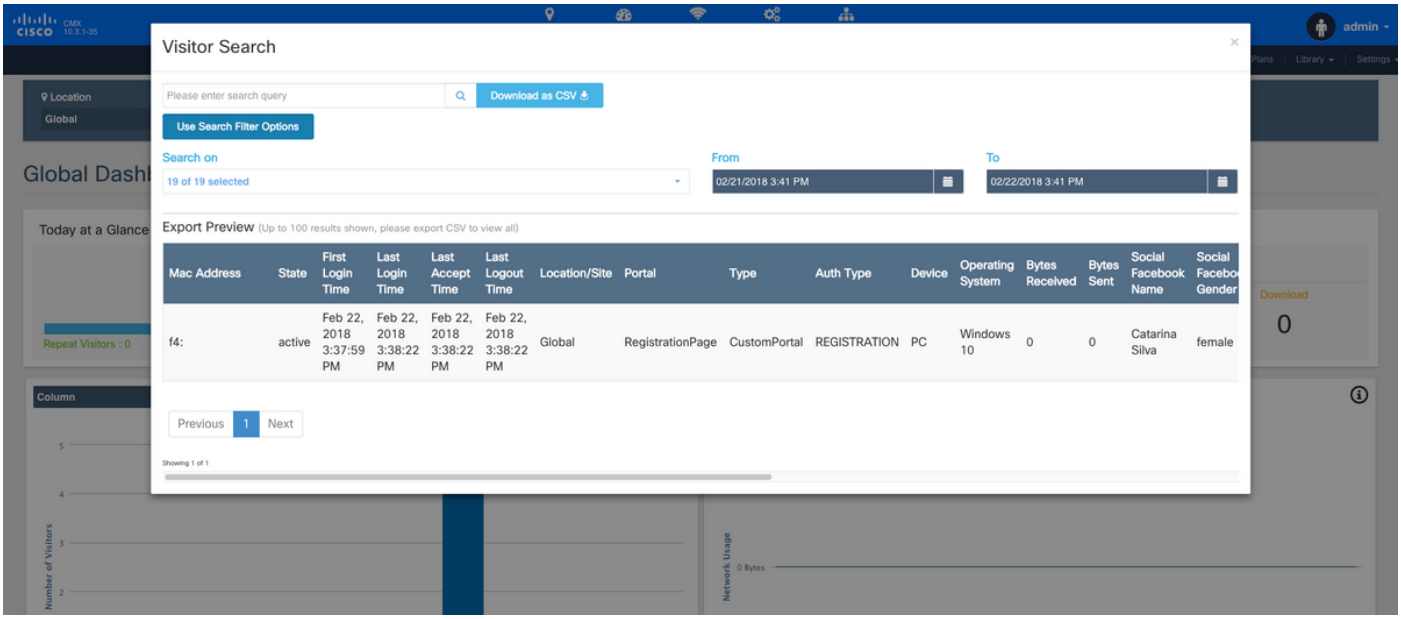


CMX

Es posible verificar cuántos usuarios se autentican en CMX, abriendo la ficha CONNECT&ENGAGE:



Para comprobar los detalles del usuario, en la misma ficha, arriba a la derecha, haga clic en Búsqueda de visitantes:



Troubleshoot

Para verificar el flujo de las interacciones entre los elementos, hay algunas depuraciones que se pueden hacer en el WLC:

>debug client<MAC addr1> <MAC addr2> (Introduzca la dirección MAC de uno o más clientes)

>debug web-auth redirect enable mac <MAC addr> (Introduzca la dirección MAC del cliente web-auth)

>debug web-auth webportal-server enable

>debug aaa all enable

Estas depuraciones permitirán la resolución de problemas y, si es necesario, se pueden utilizar algunas capturas de paquetes para complementar.