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

## Contenido

Introducción Prerequisites Requirements Componentes Utilizados Configurar Diagrama de la red Configuraciones Autenticación vía SMS Autenticación a través de cuentas de redes sociales Autenticación a través del portal personalizado Verificación Troubleshoot

## 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.

cisco	MON	TOR <u>N</u>	(LANs	CONTROL	LER	WIRELESS	<u>s</u>	ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	:	
Security	Acc	ess Cor	ntrol L	ists > Edi	t									
<ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> <li>DNS</li> </ul>	Geno Acces Deny	eral s List Nam Counters	e	CMX_red	lirect									
Downloaded AVP TACACS+	Seq	Action	Sour	ce IP/Mask	D	estination P/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
LDAP Local Net Users	1	Permit	0.0.0	.0 .0	/ 10	0.48.39.100 55.255.255.25	/	ТСР	Any	нттр	Any	Any	0	
MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	2	Permit	10.48 255.2	.39.100 55.255.255	/ 0. 0.	.0.0.0 .0.0.0	/	ТСР	НТТР	Any	Any	Any	0	

### 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 .

cisco	Save Configuration   Ping   Logout   Refresh MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'cmx_sms' < Back Apply
WLANS	General Security QoS Policy-Mapping Advanced
F Advanced	Layer 2       Layer 3       AAA Servers         Layer 2 Security 6       None       +         MAC Filtering?       +         Fast Transition       Disable +
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	General         Security         QoS         Policy-Mapping         Advanced           Layer 2         Layer 3         AAA Servers
<ul> <li>WLANS WLANS</li> <li>Advanced</li> </ul>	Layer 3 Security Web Policy © Captive Network Assistant Bypass None © Authentication Passthrough Conditional Web Redirect Splash Page Web Redirect On MAC Filter failure <sup>19</sup> Web policy done locally on AP <u>warning</u> Preauthentication ACL IPv4 CMX_redirect © IPv6 None © WebAuth FlexAcl None © Qr Code Scanning Email Input Sleeping Client Enable Override Global Config <sup>29</sup> © Enable
	Web Auth type     External(Re-direct to external server)       Redirect URL     http://10.48.39.100/visitor/login

#### B Twilio

CMX proporciona integración <u>Twilio</u> 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.

⊞tw	ilio				docs $\checkmark$	$\sim$
	∨ s	iettings /		UPGRADE	,♀ Go to 🕸 ?	63
ଜ	Dashboard					
Ģ	Billing	Two-Factor Authentication				
	Usage	Add an extra layer of protection to your account, with	h 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 a	ask for verification code every 30 days			
	Manage Users	O EVERY LOG-IN We'll always ask for a verification of	ode			
	User Settings					
	Doer Profile	API Credentials				
	Upgrade	LIVE Credentials	Learn about REST API Credentials 7	TEST Credentials	Learn about Test Credentials	§ 71
		ACCOUNT SID AC3132a0b65f9ac540318a0a576e3f3dbd Used to exercise the REST API AUTH TOKEN		TEST ACCOUNT SID ACb7ec526108f80811b68c6b7b9693e69d Used to exercise the REST API TEST AUTHTOKEN		
		Request a Secondary Token Keep this somewhere safe and secure		<ul> <li>Keep this somewhere safe and secure</li> </ul>		

#### 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.

cisco 10.3.0-62		DETECT & LOCATE	ANALYTICS	CONNECT & ENGAGE	¢; MAN/	} \GE	SYSTEM				•	admin +
								Dashboard	Connect Experiences	Policy Plans	Library <del>-</del>	Settings -
Login Page 🔹 \land	Please enter your number to get Wi-Fi Have SMS Code? X • Phone Number* O ease review and accept our Terms & Condition access to Wi-Fi. SUBMIT		English	• •	- Er	VTENT Have SMS C. Enter Twill Accc Auth From From Mum	BACKGROUND SMS Code? Code Input Placeholder SMS Code o Configuration • • • • O Configuration • • • SMS Code o Configuration • • • • • • • • • • • • • • • • • • •	THEMES LANGU	3dbd	<ul> <li>₽</li> <li>20</li> <li>₽</li> <li>20</li> <li>₽</li> <li>20</li> </ul>	ptional   🗟 ptional   🗟 ptional   🗟	EDIT

#### 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)

CISCO	MONI	TOR W	LANs		R WIRELESS	s	ECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK		
Security	Acce	ess Con	trol Li	sts > Edit									
<ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> </ul>	Gene Access Deny	eral s List Nam Counters	e	CMX_Auth 0									
DNS Downloaded AVP TACACS+	Seq	Action	Sourc	e IP/Mask	Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
LDAP Local Net Users	1	Permit	10.48 255.2	39.100 / 55.255.255	0.0.0.0 0.0.0.0	/	ТСР	HTTPS	Any	Any	Any	0	
MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	_2_	Permit	0.0.0.	) / D	10.48.39.100 255.255.255.25	5	ТСР	Any	HTTPS	Any	Any	0	
Local EAP													

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.

،،۱،،۱،، cısco	<u>M</u> ONITOR <u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	-
Security	ACL > CMX_Auth	> URL List							
<ul> <li>▼ AAA</li> <li>General</li> <li>▼ RADIUS</li> <li>Authentication</li> </ul>	URL String Name					Add			
Fallback	facebook.com								
DNS	m.facebook.com								
<ul> <li>Downloaded AVP</li> <li>TACACS+</li> <li>LDAP</li> </ul>	fbcdn.net								

#### 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.

	Save Configuration   Ping   Logout   Refresh MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'cmxFW' < Back Apply
WLANS WLANS	General         Security         QoS         Policy-Mapping         Advanced           Laver 2         Laver 3         AAA Servers         Image: Contract of the security of the secure security of the secure secure security of the secure
P Advanced	Layer 2 Security § None MAC Filtering 9 Fast Transition Fast Transition Disable \$
ululu cisco	Save Configuration Ping   Logout   <u>R</u> efresh MONITOR <u>W</u> LANS <u>C</u> ONTROLLER W <u>I</u> RELESS <u>S</u> ECURITY M <u>A</u> NAGEMENT C <u>O</u> MMANDS HE <u>L</u> P <u>F</u> EEDBACK <u>home</u>
WLANs	WLANs > Edit 'Facebook' < Back Apply
VLANs	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers

#### B Facebook para desarrolladores

Web Auth type

URL https://10.

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 <u>Facebook para desarrolladores</u> para crear la Aplicación. Hay algunos requisitos de configuración de la aplicación para integrar los servicios.

External(Re-direct to external server) \$

/visitor/login

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.

f = App Dashboard				Docs	Too	is Suppo	t Q Se	arch developers.facebook.com
	🔯 Catarina's first app	•	APP ID:		ON O	Status: Liv	vie 🗸	w Analytics
	音 Dashboard な Settings 四 Roles ▲ Alerts O App Review	•	Make Catarina's first app public? Yes Your app is currently live and available to the public.					
	PRODUCTS 🔶	,	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. 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.

illullu car cisco 1031-95	DETECT & LOCATE	ANALYTICS	CONNECT & ENGAGE	<b>C</b> MANAGE	SYSTEM			6	admin -
						Dashboard	Connect Experiences	Policy Plans Library	- Settings -
RegistrationPage &							Live View D	Portais Library	Save
Login Page 👻 👁		English	• 6	CONTENT	BACKGROUND	THEMES LANGUAGES			EDIT
Login to connect to wife				Social	Login			Remove eler	nent
				Dep	ends on Terms and C	Conditions			- 11
f				- Content					- 11
				<b>Ø</b> 1	acebook 🔗   Scope:	Basic Profile +			- 11
				Ci	atarina's first app	▼ Key:			
				0	Create new				

#### 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.

ဂါ၊ဂါ၊ င၊sco	MONITOR W	LANs <u>C</u> ONTRO	LLER WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK					
ecurity	Access Con	trol Lists > Ed	dit										
AAA General ▼ RADIUS	General												
Authentication Accounting Fallback DNS	Access List Name	≥ CMX_H 0	ITTPS										
Downloaded AVP	Seq Action	Source IP/Mas	k	Destinatio	n IP/Mask	Pro	otocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
IDAP	1 Permit	10.48.71.122	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	TCF	<b>&gt;</b>	HTTPS	Any	Any	Any	0	-
Local Net Users MAC Filtering Disabled Clients	2 Permit	0.0.0.0	/ 0.0.0.0	10.48.71.1	22 / 255.255.	255.255 TCF	, ,	Any	HTTPS	Any	Any	0	

#### 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.

WLANs WLANs > Edit 'cmx_login'	
WLANs         MAdvanced         Layer 2       Layer 3       AAA Servers         Layer 2       Security 6       None       \$         MAC Filtering 9       Fast Transition       Disable \$         Lobby Admin Configuration       Lobby Admin Access	Advanced

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'cmx_login'
VLANs	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>1,2</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>2,2</sup> Enable Web Auth type External(Re-direct to external server) ‡ Redirect URL https://10.48.71.122/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:

MONITOR WLANS CONTROLLER WIRELESS SECURITY	MANAGEMENT COMMANDS HELP FEEDBACK						Sa <u>v</u> e Co	infiguration	Ping   Logou	.t <u>B</u> efresh
Clients									Entries 1	- 1 of 1
Current Filter None [Change Filter]	[Clear Filter]									
Client MAC Addr IP Address(Ipv4/Ipv6)	AP Name	WLAN Profile	WLAN SSID	User Name	Protocol	Status	Auth	Port Slot I	d Tunnel	Fastland
<u>f4:</u> 64.	AP3-37021	Facebook	WiFi_Facebook	Unknown	802.11ac	Associated	Yes	1 1	No	No
Foot Notes RLAN Clients connected to AP702w. will not show Client IP details.										
	MONTOR WLANS CONTROLLER WIRELESS SECURITY Clients Current Filter None [Charge Filter] Client NAC Addr IP Address(Tpv4/Tpv6) 55: 64.	MONTTOR         WLANS         CONTROLLER         WIRELESS         SECURITY         MANAGEMENT         COMMANDS         HELP         FEEDBACK           Clients         Current Filter         None         ICharope Eilter]         ICharope Eilter]	MONTOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Clients Current Filter None EChaoge Filter] Client MAC Addr IP Address(Tpv4/Tpv6) AP Name WLAN Profile ES: 64. AP3-37021 Facebook Foot Notes RUAN Contes connected to AP702m, will not show Client IP detasts.	MONTROR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP PEEDBACK Clients Current Filter None [Charge Filter] Client NAC Addr IP Address(Tpv4/Tpv6) AP Name WLAN Profile WLAN SSID ES: 64. AP3-37021 Facebook Wifi_Facebook Foot Notes RLAN Clients connected to AP7Conv, will not show Client IP details.	MONTROR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Clients Current Filter None [Chaope Filter] Client NAC Addr IP Address(Tpv4/Tpv6) AP Name WLAN Profile WLAN SSID User Name Es 64. AP3-37021 Feedbook WiRL/Faeebook Unknown Foot Notes RUAN Clients connected to AP702m, will not show Client IP details.	MONTROR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP PEEDBACK Clients Current Filter None [Chaope_Filter] [Clear_Filter] Client MAC Addr IP Address(Tpr4/Tpr6) AP Name WLAN Profile WLAN SSTD User Name Protocol ES 64. AP3-37021 Facebook Wifi_Facebook Unknown B02.11ac	MONTROR WLANG CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Clients Current Filter None [Chaope Filter] Client NAC Addr IP Address(Tpv4/Tpv6) AP Name WLAN Profile WLAN SSID User Name Protocol Status f5: 64. AP3-37021 Facebook Wilf_Facebook Urknown 802.11ac Associated Foot Notes RUAN Clients connected to AP7Com, will not show Client IP details.	MONTROR       WLANS       CONTROLLER       WIRELESS       SECURITY       MANAGEMENT       COMMANDS       HELP       peedback         Clients       Current Filter       None       [Chaope_Filter]       Control       Clients       Current Filter       WLAN Frofile       WLAN SSID       User Name       Protocol       Blatus       Auth         Els       64.       AP3-37021       Facebook       Wifl_Tacebook       Unknown       802.112c       Associated       Yes	MONTROR       WLANS       CONTROLLER       WIRELESS       SECURITY       MANAGEMENT       COMMANDS       HELP       geedback         Clients       Current Filter       None       [Chaope_Filter]       Courrent Filter       User Name       WLAN Frofile       WLAN SSID       User Name       Protocol       Status       Auth       Pert       Sint 1         Els       64.       AP3-37021       Facebook       WiRL/Facebook       Unknown       802-112c       Associated       Yes       1       1	MONTROR       WLANS       CONTROLLER       WIRELESS       SECURITY       MANAGEMENT       COMMANDS       HELP       PEEDBACK         Clients            Entries 1         Current Filter       None       (Sharpe Filter)

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:

ahaha						Saye Cor	igural	tion	tion   <u>P</u> in	tion   Ping	tion   <u>P</u> ing   L	tion   Ping   Log	tion Ping Logo
cisco 🔤	ONITOR WLANS C	ONTROLLER WIRELESS SECURITY MANAGEMENT	T COMMANDS HELP	FEEDBACK			ļ						
Monitor C	lients > Detail					< B.	nck	ack Link	ack Link Tes	ack Link Test	ack Link Test	ack Link Test P	ack Link Test Re
Summary M	fax Number of Records	10 Clear AVC Stats											
Access Points	General AVC Sta	tistics											
Cisco CleanAir													
Statistics	Client Properties		AP Properties										
CDP .	MAC Address	<b>1</b> 4	AD Address	79.									
Rogues	MAC Address	14:	AP Address	/8:									
ients	IPv6 Address	64. fe80:	AP Name	AP3-37021									
eping Clients			AP type	802.118c									
lticast			AP radio slot to	1 Frankrik									
pplications			WLAN Profile	Facebook									
cal Profiling			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	N/A	Allowed (URL)IP add	iress									
	Mobility Move Count	0											
	Policy Manager State	RUN											
	Management Frame	No											
	UpTime (Sec)	71											
	Current TxRateSet	m8 ss2											

### CMX

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

cisco 10.31-85	DETECT 8 LOCATE	ANALYTICS	CONNECT 8 ENGAGE	<b>¢</b> Manage	SYSTEM						idmin +
							Dashboard	Connect Experiences	Policy Plans	Library 👻	Settings ·
Cocation     Global      No locations available	•	Ø Int Last	terval t 7 Days		•	Visitor Search Please enter search patte	m	<b>v</b>	٩		
Global Dashboard											
Today at a Glance - Feb 22, 2018											
<b>203</b> 1			Visi	itor Trend co	mpared to:		Data Usa	ge:			
Total Visitors		New Visitor	s : 1	Yesterday	6	Average	1	0 O	Dowr	)	
			<b>^</b>								~
Column   Column   New and Repeat Visitors		Repeat Visito	Area	8	•	Netwo	rk Usage				Û

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

							<b>9</b>	<u>&amp;</u>	¢\$									
CISCO 10.3.1-35	Visitor Searc	h														×	Plans   Librar	
Q Location	Please enter search q	uery			Q	Downloa	d as CSV 💩											_
Global	Use Search Filter C	Options																
Global Dash	Search on								From		-	To	0010 0.11 0					
	19 of 19 selected							•	02/21/2018 3:41 P	M		02/22	/2018 3:41 PN	a				
Today at a Glance	Export Preview (U	Jp to 100	results show	m, 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	RegistrationPag	ge CustomPorta	REGISTRATION	PC	Windows 10	0	0	Catarina Silva	female	0	
Column	Previous 1	Next																(1
	Showing 1 of 1																	
4																		
visitors									Jsage									
aber of									Vio Bytes					_				_
Ling (									ž									

## 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 webauth)

>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.