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 <u>Twilio</u>, 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.

cisco	MON	ITOR <u>N</u>	/LANs	<u>C</u> ONTROL	LER.	WIRELESS	<u>s</u>	ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK		
Security	Acc	ess Cor	ntrol Li	ists > Ed	it									
 AAA General RADIUS Authentication Accounting Fallback DNS Downloaded AVP TACACS+ 	Gene Acces Deny Seq	eral s List Nam Counters Action	ne Sourc	CMX_re 0 ce IP/Mask	direct	estination P/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
LDAP Local Net Users	1	Permit	0.0.0.	0 0	/ 1	0.48.39.100 55.255.255.255	/	ТСР	Any	НТТР	Any	Any	0	
MAC Filtering Disabled Clients User Login Policies AP Policies	2	Permit	10.48 255.2	.39.100 55.255.255	/ 0	.0.0.0 .0.0.0	/	ТСР	НТТР	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 .

արտիս		Save Configuration Ping	Logout <u>R</u> efresh
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	<u>F</u> EEDBACK	n <u>H</u> ome
WLANs	WLANs > Edit 'cmx_sms'	< Back	Apply
WLANS WLANS	General Security QoS Policy-Mapping Advanced		
Advanced	Layer 2 Layer 3 AAA Servers		
	Layer 2 Security ⁶ None MAC Filtering ⁹		
	Fast Transition Fast Transition		

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
AND AND	General Security QoS Policy-Mapping Advanced
WLANS	Layer 2 Layer 3 AAA Servers
WLANS	
Advanced	Layer 3 Security Web Policy Captive Network Assistant Bypass None Authentication Passthrough Conditional Web Redirect Splash Page Web Redirect On MAC Filter failure ¹² Web policy done locally on Apwarning
	Preauthentication ACL IPv4 CMX_redirect IPv6 None WebAuth FlexAcl None IPv6 Qr Code Scanning Email Input Sleeping Client Enable Override Global Config ² IPv6 Enable Web Auth type External(Re-direct to external server) Redirect URL http://10.48.39.100/visitor/login IPv6 IPv6

B. Twilio

O CMX oferece integração <u>Twilio</u> 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.

(ii) tw	rilio				DO	cs 🗸			
	✓ 5	iettings /		UPGRAI	DE Co to		Ø	?	¢3
۵	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 >>	TEST Credentials	Lea	rn about Te	st Crede	entials :	n
		ACCOUNT SID AC3132a0b65f9ac540318a0a576e3f3dbd Used to exercise the REST API AUTH TOKEN		TEST ACCOUNT SID ACb7ec526108f80811b68c6b7b9693e69d Used to exercise the REST API					
		© •••••		© •••••					
		Request a Secondary Token		Keep this somewhere safe and secure					
		Keep this somewhere safe and secure							

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.

cisco 10.3.0-62		DETECT & LOCATE	ANALYTICS		T I 3E	O MANAGE	SYSTEM				•	admin +
								Dashboard	Connect Experiences	Policy Plans	Library 👻	Settings -
Login Page 🔸 \land	Please enter your number to get Wi-Fi Have SMS Code? X Phone Number' O Please review and accept our Terms & Condition Please review and accept our Terms & Condition SUBMIT		English	•	0	CONTENT Have SMS C Enter Twili Accu Auth Fron Nurr	BACKGROUND TH SMS Code? SMS Code o Configuration O O o Configuration O O a Token: There +32	HEMES LANGU	AGES		ptional 🛛 😁 ptional 🔹 😁	EDT

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)

cisco	MONI	TOR WI	LANs (SECUR	ITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK		
Security	Acce	ess Con	trol Lis	ts > Edit									
 AAA General RADIUS Authentication Accounting Fallback DNC 	Gene Access Deny	e ral s List Name Counters	2	CMX_Auth									
Downloaded AVP TACACS+	Seq	Action	Source	IP/Mask	Destination IP/Mask	Prot	tocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
LDAP Local Net Users	1	Permit	10.48.3 255.255	9.100 / 5.255.255	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	0.0.0.0 0.0.0.0	/	10.48.39.100 255.255.255.255	[/] тср		Any	HTTPS	Any	Any	0	
Local EAP													

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.

ແມ່ນເມ່ນ cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLLER WIRELESS <u>SECURITY</u> M <u>A</u> NAGEMENT C <u>O</u> MMANDS HELP <u>F</u> EEDBACK	
Security	ACL > CMX_Auth > URL List	
 AAA General RADIUS Authentication 	URL String Name Add	
Fallback	facebook.com	
DNS	m.facebook.com	
TACACS+ LDAP Local Net Lisers	fbcdn.net	

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.

uluilu cisco	s MONITOR WLANS <u>C</u> ONTROLLER WIRELESS <u>S</u> ECURITY MANAGEMENT	Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> efresh C <u>O</u> MMANDS HE <u>L</u> P <u>F</u> EEDBACK
WLANs	WLANs > Edit 'cmxFW'	< Back Apply
 WLANs WLANs Advanced 	General Security QoS Policy-Mapping Advanced Layer 2 Layer 3 AAA Servers Layer 2 Security None + MAC Filtering? + Fast Transition Filtering? Fast Transition Disable +	

cisco	Save Configuration Ping Logout Re MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'Facebook' < Back Apple
VLANs	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 3 Security 1 Web Policy Authentication Passthrough Conditional Web Redirect Splash Page Web Redirect On MAC Filter failure19 Preauthentication ACL IPv4 CMX_Auth ; IPv6 None; WebAuth FlexAcl None; Email Input Sleeping Client Enable Over-ride Global Config29 Senable Web Auth type External(Re-direct to external server); URL https://10. /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 <u>Facebook para desenvolvedores</u> 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 tornálo público. Para isso, vá para App Review->Tornar a <App-Name> pública? e altere o estado para Sim.

f	App Dashboard				Docs	Тоо	s S	upport	Q Search developers
		Catarina's first app	•	APP ID:		ON O	Status	: Live	A View Analytics
		 査 Dashboard 菜 Settings ☑ Roles ▲ Alerts ◇ App Review 	> >	Make Catarina's first app public? Yes Your app is currently live and available to the public.					
		PRODUCTS (+) Facebook Login Activity Log	,	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. 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.

cisco 10.3.1-35		DETECT & LOCATE	ANALYTICS	CONNECT 8 ENGAGE	C MANAGE	SYSTEM			i	admin -
							Dashboard	Connect Experiences	Policy Plans Library	Settings
RegistrationPage 🖋								Live View D	elete Portals Library	Save
Login Page 👻 🛛 🕹			English	• 6	CONTENT	BACKGROUND	THEMES LANGUAGES			EDIT
	Login to connect to wife				Social	Login			Remove eleme	nt
					Dep	ends on Terms and C	Conditions			- 11
	f				- Content					-11
					2 F	acebook 🔗 Scope	: Basic Profile •			11
					Ci	tarina's first app	▼ Key:			- 11
					0	Create new				- 11

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.

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	>	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

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 préautenticação, 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.

،،ا،،،ا،، cısco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLLER WIRELESS <u>S</u> ECURITY M <u>A</u> NAGEMEN
WLANs	WLANs > Edit 'cmx_login'
VLANs	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 2 Security MAC Filtering
	Fast Transition
	Fast Transition Disable 🛊
	Lobby Admin Configuration
	Lobby Admin Access
ludu	
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
	Have 2 County
	Captive Network Assistant Bypass None
	Authentication
	Passthrough
	Conditional Web Redirect
	Splash Page Web Redirect
	On MAC Filter failure ⁴²
	Preauthentication ACL IPv4 CMX_HTTPS + IPv6 None + WebAuth FlexAcl None +
	Qr Code Scanning Email Input Email Input
	Sleeping Client Enable
	Override Global Config ²⁰ 🛛 Enable
	Web Auth type External(Re-direct to external server) \$

C. Configuração do CMX

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

Redirect URL https://10.48.71.122/visitor/login

• 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:

،،۱۱،،۱۱، cısco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK						Saye	Configur	ation <u>P</u> i	ng Logout	t <u>B</u> efresh
Monitor	Clients																Entries 1	- 1 of 1
Summary Access Points Cisco CleanAir	Current Filter Nor	se .		hange Filter) (f	Clear Filter]													
 Statistics 	Client MAC Addr	IP Address(Ipv/	4/Ipv6)		AP N	Name			WLAN Profile	WLAN SSID	User Name	Protocol	Status	Auth	Port	Slot Id	Tunnel	Fastland
> CDP	<u>f4:</u>	64.			AP3-	37021			Facebook	WiFi_Facebook	Unknown	802.11ac	Associated	Yes	1	1	No	No
 Rogues Clients Steeping Clients Multicast Applications Local Profiling 																		
	Foot Notes RLAN Clients connected	1 to AP702w, will not	t show Client IP	details.														

Clique no endereço MAC do cliente e, nos detalhes, confirme se o estado do Policy Manager do cliente está no 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	1 4	AD Address	79.									
Rogues	MAC Address	14:	AP Address	78:									
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

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

cisco 10.3.135	DETECT & LOCATE	ANALYTICS	CONNECT & ENGAGE	Ø MANAGE	SYSTEM					•	admin +
							Dashboard	Connect Experiences	Policy Plans	Library 👻	Settings
Cocation Global	•	Ø In Las	terval t 7 Days		•	Visitor Search Please enter search patte	m	- (2		
Global Dashboard											
Today at a Glance - Feb 22, 2018											
203 1			Vis	itor Trend co	mpared to:		Data Usa	ige:			
Total Visitors Repeat Visitors : 0		New Visitor	rs : 1	Yesterday	0	Average		0	Download Download Compared Download Compared Dow		
Column -			(i) Area	a	•						(j)
5 New and Repeat Visitors		Repeat Visit	ors 5			Netwo	rk Usage				

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

							9	<u> 8</u> 🗢	¢	.								
CISCO 10.3.1-35	Visitor Searc	h														×	Plans Librar	n - s
Q Location	Please enter search q	uery			٩	Downloa	d as CSV 🛓											
Global	Use Search Filter C	Options																
Global Dashl	Search on 19 of 19 selected							*	From 02/21/2018 3:41 PI	и		To 02/22	/2018 3:41 PI	И				
Today at a Glance	Export Preview (U	Jp to 100	results show	n, 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	e CustomPortal	REGISTRATION	PC	Windows 10	0	0	Catarina Silva	female	0	
Column	Previous 1	Next																(1
	Showing 1 of 1																	
4																		
visitors									Usage									
per of									L 0 Bytes									

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.