CMX Connected Experiences - Social, sms en Custom Portal Registration Voorbeeld

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Configureren Netwerkdiagram Configuraties Verificatie via SMS Verificatie via sociale netwerkrekeningen Verificatie via Aangepaste Portal Verifiëren Problemen oplossen

Inleiding

Dit doel van dit document is om netwerkbeheerders door clientregistratie te sturen via de configuratie van gastportals bij Connected Mobile eXperience (CMX).

CMX stelt gebruikers in staat om zich in het netwerk te registreren en te authentiseren met behulp van Vastlegging sociale registratie, sms en Aangepaste Portal. In dit document kunt u een overzicht vinden van de configuratiestappen in de draadloze LAN-controller (WLC) en CMX.

Voorwaarden

Vereisten

CMX moet correct worden geconfigureerd met de basisconfiguratie.

Het hebben van kaarten van Prime Infrastructuur is optioneel.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco draadloze controller versie 8.2.16.0, 8.5.10.0 en 8.5.135.0.
- Cisco Connected Mobile Experiences versie 10.3.0-62, 10.3.1-35.10.4.1-22.

Configureren

Netwerkdiagram

In dit document worden twee verschillende manieren beschreven om gebruikers/klanten in het draadloze netwerk met CMX te authenticeren.

Ten eerste zal de invoering van een echtheidscontrole met behulp van sociale netwerkrekeningen worden beschreven, en daarna de authenticatie met behulp van sms.

In beide scenario's zal de client proberen om zich op de SSID te registreren door gebruik te maken van verificatie via CMX.

De WLC wijst het HTTP-verkeer terug naar CMX, waar de gebruiker wordt gevraagd om echt te maken. CMX bevat de instellingen van het portal dat de client kan registreren, zowel via sociale accounts als sms.

Hieronder vindt u het verloop van het registratieproces:

- 1. De client probeert zich aan te sluiten bij de SSID en opent de browser.
- 2. In plaats van toegang te hebben tot de gevraagde site, wordt de bezoekersportal door de WLC aangereikt.
- 3. De cliënt verstrekt zijn geloofsbrieven en probeert authentiek te verklaren.
- 4. CMX heeft betrekking op het verificatieproces.
- 5. Indien geslaagd, wordt nu volledige internettoegang aan de klant geboden.
- 6. De cliënt wordt naar de aanvankelijk gevraagde site verwezen.

De gebruikte topologie is:



Configuraties

Verificatie via SMS

Cisco CMX maakt clientverificatie mogelijk via sms. Voor deze methode moet u een HTMLpagina instellen, zodat de gebruiker hun aanmeldingsgegevens aan het systeem kan geven.Standaardsjablonen worden ook door CMX geleverd en kunnen later worden bewerkt of vervangen door een aangepaste pagina.

De service voor tekstberichten wordt uitgevoerd via het integreren van CMX met <u>Twilio</u>, een cloudcommunicatieplatform waarmee tekstberichten kunnen worden verzonden en ontvangen. Hiermee kan een telefoonnummer per portal worden ingevoerd, wat betekent dat als er meer dan één portal wordt gebruikt, er één telefoonnummer per portal nodig is.

A. WLC-configuratie

In de WLC-zijde worden zowel een SSID als ACL ingesteld. Het AP moet worden aangesloten op de controller en op de RUN-staat.

1. ACL

Er is een ACL vereist die HTTP-verkeer toelaat, ingesteld op de WLC. Om ACL te configureren gaat u naar Security->Toegangscontrolelijsten->Nieuwe regel toevoegen.

De IP die wordt gebruikt, is degene die voor de CMX is geconfigureerd. Dit staat HTTP verkeer tussen de WLC en de CMX toe. De grafiek toont de gemaakte ACL waar "10.48.39.100" naar het CMX IP adres verwijst.

cisco	MON	ITOR <u>V</u>	<u>/</u> LANs	CONTROLL	ER W <u>I</u> RELESS	SE	CURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	:	
Security	Acc	ess Col	ntrol L	ists > Edit									
AAA General RADIUS	Gen	eral											
Authentication	Acces	s List Nan	ne	CMX_redi	rect								
Fallback	Deny	Counters		0									
Downloaded AVP TACACS+	Seq	Action	Sour	ce IP/Mask	Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
LDAP Local Net Users	1	Permit	0.0.0	.0 / .0	10.48.39.100 255.255.255.255	/	ТСР	Any	нттр	Any	Any	0	
 MAC Filtering Disabled Clients User Login Policies 	2	Permit	10.48 255.2	3.39.100 / 255.255.255	0.0.0.0 0.0.0.0	/	ТСР	НТТР	Any	Any	Any	0	
AP Policies Password Policies													

2. WLAN

Dus de integratie met het portal wordt gedaan, het beveiligingsbeleid moet worden aangepast aan de WLAN.

Eerst moet u WLAN's ->Bewerken->Layer 2->Layer 2-beveiliging inschakelen en moet u in de vervolgkeuzelijst Geen kiezen, zodat Layer 2-beveiliging wordt uitgeschakeld. Wijzig vervolgens in hetzelfde tabblad Security naar Layer 3. Selecteer in het vervolgkeuzemenu Layer 3 Security de optie Webbeleid en vervolgens Passthrough. In Verificatie vooraf ACL, selecteer de IPv4 ACL die eerder is geconfigureerd om het aan de respectievelijke WLAN te binden waar sms-verificatie moet worden geleverd. De optie Over-ride Global Config moet worden ingeschakeld en het type webverbinding moet extern zijn (Re-direct naar externe server), zodat klanten kunnen worden omgeleid naar de CMX-service. De URL moet gelijk zijn aan de CMX-portal voor sms-verificatie, met de bestandsindeling http://<CMX-IP>/bezoeker/aanmelding.

սիսիս		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 None MAC Filtering		
	Fast Transition 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
WLANS WLANS Advanced	Layer 3 Security Web Policy 🗘 Captive Network Assistant Bypass None 🗘
	Authentication Passthrough Conditional Web Redirect Callack Data Web Redirect
	Splash Page web Redirect On MAC Filter failure ¹² Web policy done locally on AP <u>warning</u> Presuthentication ACl IPv4 CMX radirect IPv6 None 2 WebAuth ElevAcl None 2
	Qr Code Scanning Email Input Sleeping Client Enable
	Override Global Config20 Image: Config20 Image: Config20 Web Auth type External(Re-direct to external server) Image: Config20 Redirect URL http://10.48.39.100/visitor/login

B. Twilio

CMX biedt integratie van Twitlio voor tekstberichten. Credentials worden geleverd nadat de account op Twitlio correct is ingesteld. Zowel ACCOUNT SID als AUTH TOKEN zijn nodig.

Twio heeft zijn eigen configuratievereisten, gedocumenteerd door het proces van het opzetten van de service. Voordat u de Twilio-service met CMX installeert, kan deze getest worden op problemen die te maken hebben met Twio-instelling. Deze kunnen worden gedetecteerd voordat u de service met CMX gebruikt.

(ii) tw	ilio				DOCS	/		~					
	∨ s	ettings /		UPGRADE	, O Go to	¢	?	ŝ					
ଇ	Dashboard												
	Billing	Two-Factor Authentication	Factor Authentication										
	Usage	Add an extra layer of protection to your account, w	n extra layer of protection to your account, with a verification code sent via SMS or voice call.										
)	Settings	DISABLED Do not require a verification code	ISABLED Do not require a verification code										
	General Subaccounts	ONCE PER COMPUTER Trust computers and only	ONCE PER COMPUTER Trust computers and only ask for verification code every 30 days										
	Manage Users User Settings	O EVERY LOG-IN We'll always ask for a verification	EVERY LOG-IN We'll always ask for a verification code										
	Doer Profile	API Credentials											
	Upgrade	LIVE Credentials	Learn about REST API Credentials 7	TEST Credentials	Learn abo	ut Test Cre	edential	<u>s</u> 7					
		ACCOUNT SID AC3132a0b65f9ac540318a0a576e3f3dbd Used to exercise the REST API AUTH TOKEN Concept Autor Account Action Action Request a Secondary Token Keep this somewhere safe and secure		TEST ACCOUNT SID ACD7ec526108f80811b68c6b7b9693e69d Used to exercise the REST API TEST AUTHTOKEN © Keep this somewhere safe and secure									

C. CMX-configuratie

De controller moet naar behoren aan de CMX worden toegevoegd en de kaarten moeten worden geëxporteerd uit de Prime-infrastructuur.

Sms-registratiepagina

Er is een standaardsjabloon voor het registratieportal. Portals kunt u vinden bij het selecteren van

CONNECT&ENGAGE-X>Library. Als u een sjabloon wilt hebben, kiest u sjablonen in het uitrolmenu.

Om Twitlio met het portal te integreren, gaat u naar Twitlio Configuration en geeft u de account-ID en de auth Token. Als de integratie succesvol is zal het aantal dat in Twitlio-account wordt gebruikt verschijnen.

CISCO 10.3.0-62	DETECT & LOCATE	ANALYTICS	CONNECT & ENGAGE	MANAGE	SYSTEM					admin -
							Connect Experiences			
Login Page - I	ease enter your number to get Wi-Fi Have SMS Code? x Phone Number &	English	•	CONTENT Haw SMS Enh Tw Ac Au Fri Nu Enh Enh SMS Content Tw Ac Au Enh SMS Content Tw Ac Au Enh SMS Content Tw Ac Content Tw Ac Content Tw Ac Content Co	BACKGROUND e SMS Code? Code Input Placeholder er SMS Code illio Configuration • • • illio Configuration • • illio Configuration • • AC3132a0R • +32 • +32 • - Reset • - - - - - - - - - - - - - -	THEMES LANGU	IAGES I3dbd	 ₽ ≥ α ₽ ≥ α 	ztional @	EDIT

Verificatie via sociale netwerkrekeningen

Voor het authenticeren van de client met behulp van socialenetwerkrekeningen is het nodig dat de netwerkbeheerder een geldig Facebook APP-identificator aan CMX toevoegt.

A. WLC-configuratie

In de WLC-zijde worden zowel een SSID als ACL ingesteld. AP moet worden aangesloten bij de controller en op de RUN-staat.

1. ACL

Zoals hier gebruik we HTTPS als authenticatiemethode, moet een ACL die HTTPS verkeer toelaat op de WLC worden geconfigureerd. Om ACL te configureren gaat u naar Security->Toegangscontrolelijsten->Nieuwe regel toevoegen.

CMX IP moet worden gebruikt voor HTTPS-verkeer tussen de WLC en de CMX. (In dit voorbeeld is de CMX-ip 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									
 AAA General RADIUS Authentication Accounting Fallback Dice 	Gene Access Deny	e ral s List Name Counters	e	CMX_Auth									
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 / D	10.48.39.100 255.255.255.255	5	ТСР	Any	HTTPS	Any	Any	0	
Local EAP													

Het is ook nodig om een DNS ACL met Facebook URLs te hebben. Om dit te doen, in Beveiliging ->Toegangscontrolelijsten vinden de ingang van de eerder geconfigureerd ACL (in dit geval CMX_Auth) en verplaats de muis naar de blauwe pijl aan het eind van de ingang en selecteer Add-Remove URL. Nadat dat type heeft Facebook URL's op de URL String String Name en Add.

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	
Security	ACL > CMX_Auth > URL List	
 ▼ AAA General ▼ RADIUS Authentication 	URL String Name Add	
Fallback	facebook.com	
DNS	m.facebook.com	
TACACS+	fbcdn.net	

2. WLAN

Het beveiligingsbeleid verandert zodat de Registratie kan werken, waardoor een specifieke configuratie van het WLAN moet worden uitgevoerd.

Zoals eerder voor de sms-registratie gedaan, eerst bij WLAN's->Bewerken>Layer 2->Layer 2 security, en in de vervolgkeuzelijst Geen kiezen, zodat Layer 2 security uitgeschakeld is. In het tabblad Security verandert dit in Layer 3. Selecteer in het vervolgkeuzemenu Layer 3 Security de optie Webbeleid en vervolgens Passthrough. In Verificatie vooraf ACL selecteert u de IPv4 ACL die u eerder ingesteld heeft, om deze te verbinden met de respectievelijke WLAN's waar verificatie via Facebook moet worden geleverd. De optie Over-ride Global Config moet worden ingeschakeld en het type webverbinding moet extern zijn (Re-direct naar externe server), zodat klanten kunnen worden omgeleid naar de CMX-service. Merk op dat de URL deze keer op het volgende formaat moet staan: https://<CMX-IP>/bezoeker/login.

արտիս					S	a <u>v</u> e Configuratior	n <u>P</u> ing	Logout <u>R</u> efresh
CISCO	<u>M</u> ONITOR <u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS	SECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK
WLANs	WLANs > Edit '	:mxFW'				<	Back	Apply
VLANs	General Secu	rity QoS	Policy-Mapp	ing Adv	anced			
Advanced	Layer 2	er 3 AAA Se	rvers					
	Layer 2 Securit	y 🧕 None	\$					
		MAC Filtering ⁹						
	Fast Transition							
	Fast Transition	Disat	ble 🕈					

	Sa <u>v</u> e Configuration <u>P</u> ing Logo	ut <u>R</u> efres
cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLLER WIRELESS <u>S</u> ECURITY M <u>A</u> NAGEMENT C <u>O</u> MMANDS HELP <u>F</u> EEDBACK	n Hom
WLANs	WLANs > Edit 'Facebook' < Back	Apply
WLANS	General Security QoS Policy-Mapping Advanced	
Advanced	Layer 2 Layer 3 AAA Servers	
	Layer 3 Security 1 Web Policy \$	
	Authentication	
	O Passthrough	
	Conditional Web Redirect	
	Splash Page Web Redirect	
	On MAC Filter failure ¹⁰	
	Preauthentication ACL IPv4 CMX_Auth + IPv6 None + WebAuth FlexAcl None +	
	Email Input	
	Sleeping Client 🗌 Enable	
	Over-ride Global Config ²⁰ 🗹 Enable	
	Web Auth type External (Re-direct to external server) ‡	
	URL https://10. /visitor/login	

B. Facebook voor Ontwikkelaars

Voor de integratie van Facebook en CMX is een app van Facebook nodig om de juiste penningen tussen de twee partijen te laten ruilen.

Ga naar <u>Facebook voor Ontwikkelaars</u> om de app te maken. Er zijn enige configuratievereisten voor de app om de services te integreren.

In de App-instellingen moet u ervoor zorgen dat de inlognaam van de client en de aanmelding van het web worden ingeschakeld. Controleer ook of de geldige OAuth URIs, u de CMX URL in de https://<CMX-IP>/bezoeker/inlogindeling hebben.



Om de app te laten publiceren en klaar te maken voor integratie met CMX moet deze openbaar worden gemaakt. Ga om dat te doen naar App Review->Make <App-naam>? en verander de staat in Ja.



C. CMX-configuratie

De controller moet naar behoren aan de CMX worden toegevoegd en de kaarten moeten worden geëxporteerd uit de Prime-infrastructuur.

Registratiepagina

Om een Registratiepagina op CMX te maken, moeten de zelfde stappen worden gezet als eerder om de pagina voor de Registratie van sms te maken zou moeten worden gedaan. Voor het selecteren van de bibliotheek van CONNECT&ENGAGE-M, kunnen de sjablonen voor sjablonen die klaar zijn voor bewerking worden gevonden in het uitrolmenu.

Voor het registreren via Facebook-aanmeldingsgegevens is het toegangspoort nodig om verbinding te maken met je sociale accounts. Om dit vanaf het begin te doen, moest bij het maken van een aangepast portal de website CONTENT->Common Elements->Social Auth worden gestart en Facebook worden geselecteerd. Plaats vervolgens de App Name en App ID (Key) die van Facebook zijn verkregen.

	DETECT & LOCATE	ANALYTICS	CONNECT 8 ENGAGE	C Manage	SYSTEM			Ģ	admin -
						Dashboard	Connect Experiences	Policy Plans Library	✓ Settings ✓
RegistrationPage 🖋							Live View De	Portais Library	Save
Login Page 👻 🌣		English	• 6	CONTENT	BACKGROUND	THEMES LANGUAGES			EDIT
Logis to connect to wife				Social	Login			Remove elem	ent
				Dep	ends on Terms and C	conditions			- 11
f				- Content					
				💟 F	acebook 🔗 Scope:	Basic Profile +			11
				Ca	tarina's first app	▼ Key:			- 11
				0	Create new				

Verificatie via Aangepaste Portal

Het Verifiëren van de client met Custom Portal is gelijk aan het configureren van externe Web Authentication. De omleiding wordt uitgevoerd naar het aangepaste portaal dat op CMX wordt gehost.

A. WLC-configuratie

In de WLC-zijde worden zowel een SSID als ACL ingesteld. AP moet worden aangesloten bij de controller en op de RUN-staat.

1. ACL

Zoals hier gebruik we HTTPS als authenticatiemethode, moet een ACL die HTTPS verkeer toelaat op de WLC worden geconfigureerd. Om ACL te configureren gaat u naar Security-

to>Toegangscontrolelijsten->Nieuwe regel toevoegen.

CMX IP moet worden gebruikt voor HTTPS-verkeer tussen de WLC en de CMX. (in dit voorbeeld is de CMX IP 10.48.71.122).

Opmerking: Zorg ervoor dat u ssl op CMX kunt inschakelen door de opdracht "cmxctl Nogmaals activeren" op de CMX CLI uit te geven.

cisco	MONI	TOR	<u>W</u> LANs	CONTROLLI	R WIRELESS	SECURITY	MANAGEMENT	COMMAND:	S HELP	FEEDBACK					
Security	Acce	ess Co	ontrol L	ists > Edit											
AAA															
General	Gene	eral													
Authentication	Access	s List Na	ame	CMX_HTT	s										
Accounting	Deer	C	-												
DNS	Deny	Counter	5	U											
Downloaded AVP	Seq	Action	Sour	ce IP/Mask		Destinati	on IP/Mask	F	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
▶ TACACS+	1	Permit	10.48	3.71.122	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	т	CP	HTTPS	Any	Any	Any	0	
Local Net Users	2	Permit	0.0.0	.0	/ 0.0.0.0	10.48.71.1	22 / 255.255	.255.255 T	CP	Any	HTTPS	Any	Any	0	
MAC Filtering Disabled Clients															

2. WLAN

Het beveiligingsbeleid verandert zodat de Registratie kan werken, waardoor een specifieke configuratie van het WLAN moet worden uitgevoerd.

Zoals eerder voor de Registratie van sms en sociaal netwerk gedaan, eerst bij WLAN's ->Bewerken>Layer 2->Layer 2-beveiliging, en in de uitrollijst kiezen u Geen, zodat Layer 2beveiliging wordt uitgeschakeld. In het tabblad Security verandert dit in Layer 3. Selecteer in het vervolgkeuzemenu Layer 3 Security de optie Webbeleid en vervolgens Passthrough. In Voorgaande authenticatie ACL, selecteer IPv4 ACL die eerder ingesteld was (genaamd CMX_HTTPS op dit voorbeeld) en verbind het aan respectieve WLAN. De optie Over-ride Global Config moet worden ingeschakeld en het type webverbinding moet extern zijn (Re-direct naar externe server), zodat klanten kunnen worden omgeleid naar de CMX-service. Merk op dat de URL deze keer op het volgende formaat moet staan: https://<CMX-IP>/bezoeker/login.

راریان cısco	<u>MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMEN</u>
WLANs	WLANs > Edit 'cmx_login'
 WLANS Advanced 	General Security QoS Policy-Mapping Advanced Layer 2 Layer 3 AAA Servers Layer 2 Security None + MAC Filtering ? • • Fast Transition Disable + Lobby Admin Configuration • •
	Lobby Admin Access

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 ¹² 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 ²² Enable Web Auth type External(Re-direct to external server) ‡ Redirect URL https://10.48.71.122/visitor/login

C. CMX-configuratie

De controller moet naar behoren aan de CMX worden toegevoegd en de kaarten moeten worden geëxporteerd uit de Prime-infrastructuur.

• Registratiepagina

Om een Registratie-pagina op CMX te maken, volgt u dezelfde stappen als eerder om de pagina voor andere authenticatiemethoden te maken. Selecteren van CONNECT&ENGAGE->Library kunnen sjablonen die bewerkt kunnen worden gevonden in het uitrolmenu.

Het portal voor normale registratie kan vanaf het begin worden gebruikt (selecteer "Aangepast") of aangepast aan de sjabloon "Registratieformulier" die in de CMX-bibliotheek beschikbaar is.

cisco 10.4.1-22		DETECT ANALYTICS	Ç Connect		SYSTEM					1	admin -
								Dashboard	Connect Experiences	Policy Plans Library -	Settings +
Login_Page 🖋									Live View	Delete Portals Library	Save
Login Page 👻 🍳		Engl	sh 🔹	0 COM	TENT BACKGR	ROUND THEMES	LANGUAGES				
	Complete registration to onboard to wifi.			0	To add an element,	simply drag & drop it to the	carwas or click on it				
				- c	ommon elements						
	Name*				image Element	T Text Element		Social Auth	Terms & Conditions	ing ing & Text	
	SUBMIT										
	_					E.t. Contact us	† ÷ Spacer		i IIII Menu	✓ == Opt-out	
				- A	vertisement element	ts					
					Image Sider	External Content					

Verifiëren

WLC

Ga in de lijst om te controleren of de gebruiker op het systeem succesvol bevonden is, met behulp van de WLC GUI, naar MONITOR->Clients en zoek naar het MAC-adres van de client:

uhuhu cisco		SECURITY MANAGEMENT COMMANDS HELP	FFEDBACK			Say	e Configuration	Ping Logou	t Befresh
Monitor Summary	Clients Current Filter None	(Change Filter) (Clear Filter)	Lessen					Entries 1	- 1 of 1
 Cisco CleanAir Statistics CDP 	Client MAC Addr IP Address(Ipv4/Ipv6)	AP Name AP3-37021	WLAN Profile Facebook	WLAN SSID WiFi_Facebook	User Name Protocol Unknown 802.11ac	Status Au Associated Yes	th Port Slot I	d Tunnel No	Fastland
 Rogues Clients Sleeping Clients 									
Applications Local Profiling									
	Foot Notes RLAN Clients connected to AP702w, will not show Client	1P details.							

Klik op het MAC-adres van de client en bevestig in de details dat de client Policy Manager-status heeft:

սիսիս							Sayı	Configuration Ping	Logout
cisco	MONITOR WLANS	ONTROLLER WIRELESS	SECURITY MANAGEME	NT COMMANDS HELP	FEEDBACK				
Monitor	Clients > Detail						<	Back Link Test	Rer
Summary Access Points Cisco CleanAir	Max Number of Records	Clear AVC Stats	5			 			
Statistics	Client Properties			AP Properties					
Roques	MAC Address	f4:		AP Address	78:				
Clients	IPv4 Address	64.		AP Name	AP3-3702I				
Sleeping Clients	IPv6 Address	fe80:		AP Type	802.11ac				
Multicast				AP radio slot Id	1				
Applications				WLAN Profile	Facebook				
Local Profiling				WLAN SSID	WiFi_Facebook				
				Data Switching	Central				
				Authentication	Central				
				Status	Associated				
				Association ID	1				
				802.11 Authentication	Open System				
	Client Type	Regular		Reason Code	1				
	Client Tunnel Type	Unavailable		Status Code	0				
	User Name			CF Pollable	Not Implemented				
	Port Number	1		CF Poll Request	Not Implemented				
	Interface	internet_access		Short Preamble	Not Implemented				
	VLAN ID	129		PBCC	Not Implemented				
	Quarantine VLAN ID	0		Channel Agility	Not Implemented				
	CCX Version	CCXv4		Timeout	1800				
	E2E Version	E2Ev1		WEP State	WEP Disable				
	Mobility Role	Local							
	Address	N/A		Allowed (URL)IP add	dress				
	Mobility Move Count	0							
	Policy Manager State	RUN							
	Management Frame Protection	No							
	UpTime (Sec)	71							
	Current TxRateSet	m8 ss2							

СМХ

Het is mogelijk om te controleren hoeveel gebruikers op CMX geauthentiseerd zijn door het tabblad CONNECT&ENGAGE te openen:

	DETECT & LOCATE	ANALYTICS	CONNECT 8 ENGAGE	C MANAGE	SYSTEM						admin -
						l	Dashboard	Connect Experiences	Policy Plans	Library 👻	Settings
Q Location Global Vo focations available	-	0 L	Interval ast 7 Days		•	Visitor Search Please enter search patte	m	- (λ		
Global Dashboard											
Today at a Glance - Feb 22, 2018											
1			Vis	Visitor Trend compared to:			Data Usage:				
Total Visitors Repeat Visitors : 0	New Visitors : 1		tors : 1	Yesterday € ∞%		Average 17%	Upload O		Download O		
Column		Repeat Visit	Are	a	•	Networ	k Usage				(

U kunt de gebruikersgegevens in hetzelfde tabblad met de rechtermuisknop op Bezoeker controleren:

dhallo cax							9	£9 🗢	¢\$	ሐ								admin -
CISCO 10.3.1-35	Visitor Searc	h														×	Plans Library	
♥ Location Global	Please enter search o	uery Options			٩	Downloa	d as CSV 🛓											
Global Dashl	Search on 19 of 19 selected							•	From 02/21/2018 3:41 P	М		To 02/22	/2018 3:41 PN	И		=		
Today at a Glance	Export Preview (Jp to 100 r	esults 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 CustomPorta	REGISTRATION	PC	Windows 10	0	0	Catarina Silva	female	0	
Column 5	Previous 1 Showing 1 of 1	Next																(j)
A Mumber of Visitors									Network Change Change Notes								_	_

Problemen oplossen

Om de stroom van de interacties tussen de elementen te controleren, zijn er een aantal uitwerpselen die het WLC kunnen doen:

>debug client<MAC-adres1> <MAC-adres2> (Voer het MAC-adres van een of meer clients in)

>debug web-auth redirect activeren CAC <MAC addr> (Voer het MAC-adres van de web-auth client in)

>debug webportaalserver

>Schakel deze optie uit

Deze cijfers maken het mogelijk om problemen op te lossen en indien nodig kunnen sommige pakketvastlegging worden gebruikt ter aanvulling van de applicaties.