Exemple de configuration de l'enregistrement de portail personnalisé, SMS et social CMX

Contenu

Introduction Conditions préalables Conditions requises Components Used Configuration Diagramme du réseau Configurations Authentification via SMS Authentification via les comptes de réseau social Authentification via le portail personnalisé Vérification Dépannage

Introduction

Ce document a pour but de guider les administrateurs réseau à travers l'enregistrement des clients via la configuration des portails invités sur Connected Mobile eXperience (CMX).

CMX permet aux utilisateurs de s'enregistrer et de s'authentifier sur le réseau à l'aide de Social Registration Login, SMS and Custom Portal. Dans ce document, vous trouverez un aperçu des étapes de configuration sur le contrôleur de réseau local sans fil (WLC) et le CMX.

Conditions préalables

Conditions requises

CMX doit être correctement configuré avec la configuration de base.

L'exportation de cartes à partir de Prime Infrastructure est facultative.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleur sans fil Cisco versions 8.2.166.0, 8.5.110.0 et 8.5.135.0.
- Cisco Connected Mobile Experiences version 10.3.0-62, 10.3.1-35. 10.4.1-22 .

Configuration

Diagramme du réseau

Dans ce document, deux façons différentes d'authentifier les utilisateurs/clients dans le réseau sans fil, à l'aide de CMX, seront décrites.

Tout d'abord, la configuration de l'authentification à l'aide des comptes de réseau social sera décrite, puis l'authentification à l'aide de SMS.

Dans les deux cas, le client tentera de s'enregistrer sur le SSID à l'aide de l'authentification via CMX.

Le WLC redirige le trafic HTTP vers CMX où l'utilisateur est invité à s'authentifier. Le CMX contient la configuration du portail à utiliser pour l'enregistrement du client, à la fois par le biais de comptes sociaux et de SMS.

Le déroulement du processus d'enregistrement est décrit ci-dessous :

- 1. Le client tente de joindre le SSID et ouvre le navigateur.
- 2. Au lieu d'avoir accès au site demandé, est redirigé vers le portail invité par le WLC.
- 3. Le client fournit ses informations d'identification et tente de s'authentifier.
- 4. CMX traite du processus d'authentification.
- 5. En cas de succès, le client bénéficie désormais d'un accès Internet complet.
- 6. Le client est redirigé vers le site initial demandé.

La topologie utilisée est la suivante :



Configurations

Authentification via SMS

Cisco CMX permet l'authentification des clients par SMS. Cette méthode nécessite la configuration d'une page HTML afin que l'utilisateur puisse fournir ses informations d'identification au système.Les modèles par défaut sont fournis nativement par CMX et peuvent être modifiés ou remplacés ultérieurement par un modèle personnalisé.

Le service SMS est réalisé en intégrant CMX à <u>Twilio</u>, une plate-forme de communication en nuage qui permet d'envoyer et de recevoir des messages texte. Twilio permet d'avoir un numéro de téléphone par portail, ce qui signifie que si plus d'un portail est utilisé, un numéro de téléphone par portail est requis.

A. Configuration WLC

Du côté du WLC, un SSID et une ACL seront configurés. L'AP doit être joint au contrôleur et à l'état RUN.

1. ACL

Une liste de contrôle d'accès autorisant le trafic HTTP, configurée sur le WLC, est requise. Pour configurer une liste de contrôle d'accès, accédez à Security->Access Control Lists->Add New Rule.

L'adresse IP utilisée est celle configurée pour le CMX. Ceci autorise le trafic HTTP entre le WLC et le CMX. La figure ci-dessous montre la liste de contrôle d'accès créée où « 10.48.39.100 » fait référence à l'adresse IP CMX.

cisco	MONI	ITOR <u>w</u>	LANs		ER W <u>I</u> RELESS	<u>S</u> ECURI	TY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	:	
Security	Acc	ess Con	itrol Li	ists > Edit									
AAA General RADIUS Authentication Accounting Fallback DNS	Gene Acces Deny	eral s List Nam Counters	e	CMX_redir	rect								
Downloaded AVP TACACS+	Seq	Action	Sourc	e IP/Mask	Destination IP/Mask	Proto	ocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
LDAP Local Net Users	1	Permit	0.0.0. 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 AP Policies 	2	Permit	10.48 255.2	.39.100 / 55.255.255	0.0.0.0 0.0.0.0	/ TCP		НТТР	Any	Any	Any	0	
Password Policies													

2. WLAN

Ainsi, l'intégration au portail se fait, les modifications des politiques de sécurité sur le WLAN doivent être effectuées.

Premièrement, accédez à WLANs ->Edit->Layer 2->Layer 2 Security. Dans la liste déroulante, sélectionnez None, de sorte que Layer 2 Security est désactivé. Dans le même onglet Sécurité, passez ensuite à la couche 3. Dans le menu déroulant Sécurité de couche 3, sélectionnez Stratégie Web, puis Passthrough. Dans la liste de contrôle d'accès de préauthentification, sélectionnez la liste de contrôle d'accès IPv4 configurée précédemment pour la lier au WLAN respectif où l'authentification SMS doit être fournie. L'option Remplacer la configuration globale doit être activée et le type d'authentification Web doit être Externe (Rediriger vers un serveur externe), afin que les clients puissent être redirigés vers le service CMX. L'URL doit être identique au portail d'authentification SMS CMX, au format http://<CMX-IP>/visiteur/login .

սիսիս		Save Configuration Ping	Logout Refresh
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 Disable \$		

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WI ANO	General Security QoS Policy-Mapping Advanced
WLANS	Layer 2 Layer 3 AAA Servers
▼ WLANs	
WLANS	Layer 3 Security Web Policy 📀
Advanced	Captive Network Assistant Bypass None ᅌ
	Passthrough
	Conditional Web Redirect
	Splash Page Web Redirect
	On MAC Filter failure ¹⁰
	Web policy done locally on APwarning
	Preauthentication ACL IPv4 CMX_redirect ᅌ IPv6 None ᅌ WebAuth FlexAcl None ᅌ
	Qr Code Scanning Email Input
	Sleeping Client 🗌 Enable
	Override Global Config ²⁰ 🗹 Enable
	Web Auth type External(Re-direct to external server)
	Redirect URL http://10.48.39.100/visitor/login

B. Twilio

CMX fournit l'intégration <u>Twilio</u> pour les services de messagerie texte. Les informations d'identification sont fournies après la configuration correcte du compte sur Twilio. Le SID du COMPTE et le JETON AUTH sont tous deux nécessaires.

Twilio a ses propres exigences de configuration, documentées au cours du processus de configuration du service. Avant l'intégration avec CMX, le service Twilio peut être testé, ce qui signifie que les problèmes liés à la configuration de Twilio peuvent être détectés avant de l'utiliser avec CMX.

(ii) tw	rilio [.]			DOCS	~		\sim
	∨ s	iettings /	UPGRADE	, O Go to	÷	?	63
	Dashboard Billing Usage Settings General Subaccounts Manage Users	Two-Factor Authentication Add an extra layer of protection to your account, with a verification code sent via SMS or voice call.					
	User Settings Doer Profile Upgrade	API Credentials	TEST Cradentials	Loare ab	out Tast Cr	dantial	6.3
		ACCOUNT SID AC3132a0b65f9ac540318a0a576e3f3dbd Used to exercise the REST API AUTH TOKEN © ••••••••••••••••••••••••••••••••••••	TEST ACCOUNT SID ACb7ec526108f80811b68c6b7b9693e69d Used to exercise the REST API TEST AUTHTOKEN © Keep this somewhere safe and secure	Learn ab	<u>outriest cre</u>	coentiai	20

C. Configuration CMX

Le contrôleur doit être correctement ajouté au CMX et les cartes doivent être exportées depuis Prime Infrastructure.

• Page d'inscription SMS

Il existe un modèle par défaut pour le portail d'inscription. Les portails peuvent être trouvés en sélectionnant CONNECT&ENGAGE->Bibliothèque. Si vous voulez un modèle, choisissez Modèles dans le menu déroulant.

Pour intégrer Twilio au portail, accédez à Configuration Twilio et indiquez l'ID de compte et le jeton d'authentification. Si l'intégration réussit, le numéro utilisé dans le compte Twilio apparaîtra.

cisco 10.3.0-62		DETECT & LOCATE	ANALYTICS	ECT Age	C MANAGE	SYSTEM				•	admin -
							Dashboard	Connect Experiences	Policy Plans	Library -	Settings -
Login Page 🖌 💊	Please enter your number to get Wi-Fi Have SMS Code? X Phone Number* O Please review and accept our Terms & Condition for access to Wi-Fi.		English	0	CONTENT Have SMS C Enter Twill Acc Aut From Nurr	BACKGROUND SMS Code? SMS Code? Configuration Configurati	THEMES LANGU	AGES	 2 ⊙op 2 ⊙op 2 ⊙op 	tional 🔒	EDIT

Authentification via les comptes de réseau social

L'authentification du client à l'aide de comptes de réseau social nécessite que l'administrateur réseau ajoute un identificateur APP Facebook valide sur le CMX.

A. Configuration WLC

Du côté du WLC, un SSID et une ACL seront configurés. L'AP doit être joint au contrôleur et à l'état RUN.

1. ACL

Comme nous utilisons HTTPS comme méthode d'authentification, une liste de contrôle d'accès autorisant le trafic HTTPS doit être configurée sur le WLC. Pour configurer une liste de contrôle d'accès, accédez à Security->Access Control Lists->Add New Rule.

L'adresse IP CMX doit être utilisée pour autoriser le trafic HTTPS entre le WLC et le CMX. (dans cet exemple, l'adresse IP CMX est 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 Disc 	Gene Access Deny	e ral s List Name Counters	2	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. 255.25	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	0.0.0.0	D /	10.48.39.100 255.255.255.25	5	ТСР	Any	HTTPS	Any	Any	0	
Local EAP													

Il est également nécessaire d'avoir une liste de contrôle d'accès DNS avec des URL Facebook. Pour ce faire, dans Security ->Access Control Lists, recherchez l'entrée de la liste de contrôle d'accès précédemment configurée (dans ce cas CMX_Auth) et déplacez la souris vers la flèche bleue à la fin de l'entrée et sélectionnez Add-Remove URL. Après ce type, tapez les URL de Facebook sur l'URL String Name et Add.

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	
Security	ACL > CMX_Auth > URL List	
 ▼ AAA General ▼ RADIUS Authentication 	URL String Name Add	
Fallback	facebook.com	
DNS	m.facebook.com	
► TACACS+ LDAP	fbcdn.net	

2. WLAN

Les modifications apportées aux stratégies de sécurité pour que l'enregistrement fonctionne nécessitent une configuration spécifique sur le WLAN.

Comme précédemment pour l'enregistrement SMS, d'abord, accédez aux WLAN->Edit->Layer 2->Layer 2 Security, et dans la liste déroulante, sélectionnez None, de sorte que la sécurité de couche 2 est désactivée. Dans le même onglet Sécurité, passez à la couche 3. Dans le menu déroulant Sécurité de couche 3, sélectionnez Stratégie Web, puis Passthrough. Dans la liste de contrôle d'accès de préauthentification, sélectionnez la liste de contrôle d'accès IPv4 configurée précédemment pour la lier au WLAN respectif où l'authentification via Facebook doit être fournie. L'option Remplacer la configuration globale doit être activée et le type d'authentification Web doit être Externe (Rediriger vers un serveur externe), afin que les clients puissent être redirigés vers le service CMX. Notez que cette fois, l'URL, doit être au format suivant https ://<CMX-IP>/visiteur/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 +	

cisco	Saye Configuration Ping Logout Br MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'Facebook' < Back Appl
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

B. Facebook pour les développeurs

Pour l'intégration de Facebook et CMX, une application Facebook est nécessaire pour que les jetons appropriés soient échangés entre les deux parties.

Accédez à <u>Facebook for Developers</u> pour créer l'application. Il existe certaines exigences de configuration d'application afin d'intégrer les services.

Dans les paramètres de l'application, assurez-vous que la connexion au client OAuth et la connexion au Web OAuth sont activées. Vérifiez également que les URI de redirection OAuth valides, vous avez l'URL CMX dans le format https://<CMX-IP>/visiteur/login.



Pour que l'application soit publiée et prête à s'intégrer à CMX, il est nécessaire de la rendre publique. Pour ce faire, accédez à App Review->Rendre <App-Name> public ? et passez à l'état Oui.

F = App Dashboard				Docs	т	ools	Support	Q Search developers.facebook.com
	🔯 Catarina's first app	•	APP ID:		ON	D	Status: Live	M View Analytics
	 ∯ Dashboard ☆ Settings ⊡ Roles ▲ Alerts ◇ App Review 	> >	Make Catarina's first app public? Yes Your app is currently live and available to the public.					
	PRODUCTS (*) Ø 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. Configuration CMX

Le contrôleur doit être correctement ajouté au CMX et les cartes doivent être exportées depuis Prime Infrastructure.

Page d'inscription

Pour créer une page d'inscription sur CMX, procédez comme précédemment pour créer la page d'inscription SMS. Pour sélectionner CONNECT&ENGAGE->Bibliothèque, les portails de modèles prêts à être modifiés, sélectionnez Modèles dans le menu déroulant.

L'enregistrement via des informations d'identification Facebook nécessite que le portail dispose d'une connexion aux comptes sociaux. Pour le faire à partir de zéro, lors de la création d'un portail personnalisé, accédez à CONTENT->Éléments communs->Authentification sociale, et sélectionnez Facebook. Insérez ensuite le nom de l'application et l'ID de l'application (clé) obtenus de Facebook.

cisco 10.8.1-86		DETECT & LOCATE	ANALYTICS	CONNECT & ENGAGE	O MANAGE	SYSTEM			6	admin -
							Dashboard	Connect Experiences	Policy Plans Library	- Settings -
RegistrationPage &								Live View De	Portals Library	Save
Login Page 👻 🌣			English	•	CONTE	NT BACKGROUND	THEMES LANGUAGES			EDIT
	Login to connect to wife				Socia	al Login			Remove elem	ent
	×				□ De	epends on Terms and C	Conditions			- 11
	f				- Conte	int				
						Facebook 🔗 Scope	: Basic Profile -			- 11
						Catarina's first app	• Key			111
					c	Create new				- 11
										- 11

Authentification via le portail personnalisé

L'authentification du client à l'aide du portail personnalisé est similaire à la configuration de l'authentification Web externe. La redirection sera effectuée sur le portail personnalisé hébergé sur CMX.

A. Configuration WLC

Du côté du WLC, un SSID et une ACL seront configurés. L'AP doit être joint au contrôleur et à l'état RUN.

1. ACL

Comme nous utilisons HTTPS comme méthode d'authentification, une liste de contrôle d'accès autorisant le trafic HTTPS doit être configurée sur le WLC. Pour configurer une liste de contrôle d'accès, accédez à Security->Access Control Lists->Add New Rule.

L'adresse IP CMX doit être utilisée pour autoriser le trafic HTTPS entre le WLC et le CMX. (dans cet exemple, l'adresse IP CMX est 10.48.71.122).

Remarque : Assurez-vous d'activer ssl sur le CMX en exécutant la commande « cmxctl node sslmode enable » sur l'interface de ligne de commande CMX.

ဂျက်က cisco	MONI	tor <u>v</u>	<u>/</u> LANs		N WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMAND	IS HELP	FEEDBACK					
Security	Acce	ess Cor	ntrol Li	sts > Edit											
General	Gene	eral													
Authentication Accounting Solution	Access	s List Nam	ne	CMX_HTTP:	3										
DNS Downloaded AVP	Seq	Action	Sourc	e IP/Mask		Destinatio	on IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
LDAP	1	Permit	10.48	.71.122 /	255.255.255.255	0.0.0.0	/ 0.0.0.0	1	TCP	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	TCP	Any	HTTPS	Any	Any	0	

2. WLAN

Les modifications apportées aux stratégies de sécurité pour que l'enregistrement fonctionne nécessitent une configuration spécifique sur le WLAN.

Comme précédemment pour l'enregistrement des réseaux sociaux et SMS, tout d'abord, accédez à WLAN->Edit->Layer 2->Layer 2 Security (Modifier la sécurité de couche 2) et, dans la liste déroulante, sélectionnez None (Aucun), de sorte que la sécurité de couche 2 est désactivée. Dans le même onglet Sécurité, passez à la couche 3. Dans le menu déroulant Sécurité de couche 3, sélectionnez Stratégie Web, puis Passthrough. Dans la liste de contrôle d'accès de préauthentification, sélectionnez la liste de contrôle d'accès IPv4 configurée précédemment (nommée CMX_HTTPS dans cet exemple) et liez-la au WLAN respectif. L'option Remplacer la configuration globale doit être activée et le type d'authentification Web doit être Externe (Rediriger vers un serveur externe), afin que les clients puissent être redirigés vers le service CMX. Notez que cette fois, l'URL, doit être au format suivant https ://<CMX-IP>/visiteur/login.

	<u>M</u> ONITOR <u>W</u> LANS	CONTROLLER	WIRELESS SEC	CURITY M <u>A</u> NAGEMEN
WLANs	WLANs > Edit	'cmx_login'		
WLANS WLANS	General Sec	urity QoS	Policy-Mapping	Advanced
Advanced	Layer 2 La	yer 3 AAA S	ervers	
	Layer 2 Secur Fast Transition Fast Transition Lobby Admin Co Lobby Admin	ity <u>6</u> None MAC Filtering Disa Infiguration	2 - able \$	

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'cmx_login'
VLANs WLANs	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####################################

C. Configuration CMX

Le contrôleur doit être correctement ajouté au CMX et les cartes doivent être exportées depuis Prime Infrastructure. • Page d'inscription

Pour créer une page d'enregistrement sur CMX, procédez comme précédemment pour créer la page pour d'autres méthodes d'authentification. Pour sélectionner CONNECT&ENGAGE->Bibliothèque, les portails de modèles prêts à être modifiés, sélectionnez Modèles dans le menu déroulant.

Le portail pour l'enregistrement normal peut être fait à partir de zéro (sélectionnez " " personnalisé) ou adapté à partir du modèle " formulaire d'enregistrement " disponible dans la bibliothèque CMX.



Vérification

WLC

Pour vérifier si l'utilisateur a été authentifié correctement sur le système, dans l'interface graphique du WLC, accédez à MONITOR->Clients et recherchez l'adresse MAC du client dans la liste :

սիսիս												Sa <u>v</u> e C	configurat	ion <u>P</u> in	g Logout	Befresh
CISCO	MONITOR WLANS	CONTROLLER WIR	ELESS SECURITY	MANAGEMENT CO	MMANDS HELP	P FEEDBACK										Home
Monitor	Clients														Entries 1	1 of 1
Summary Access Points	Current Filter Nor	ne	[Change Filter]	[Clear Filter]												
Cisco CleanAir																
Statistics	Client MAC Addr	IP Address(Ipv4/Ip	r6)	AP Name			WLAN Profile	WLAN SSID	User Name	Protocol	Status	Auth	Port 5	lot Id	Tunnel	Fastland
> CDP	<u>f4</u> ;	64.		AP3-3702			Facebook	WiFi_Facebook	Unknown	802.11ac	Associated	Yes	1 1		No	No
Rogues																
Clients																
Sleeping Clients																
Multicast																
Applications																
Local Profiling																
	Foot Notes															
	RLAN Clients connected	to AP702w, will not show	v Client IP details.													

Cliquez sur l'adresse MAC du client et dans les détails, vérifiez que l'état du gestionnaire de stratégies client est en cours d'exécution :

ahaha			
CISCO MONITOR WLANS	CONTROLLER WIRELESS SECURI	ITY MANAGEMENT COMMANDS HELP	FEEDBACK
itor Clients > Detail			
sco CleanAir	cords 10 Clear AVC Stats		
tatistics Client Properti	es	AP Properties	
MAC Address	f4:	AP Address	78:
IPv4 Address	64.	AP Name	AP3-3702I
IPv6 Address	fe80:	AP Type	802.11ac
ast		AP radio slot Id	1
tions		WLAN Profile	Facebook
rofiling		WLAN SSID	WiFi_Facebook
		Data Switching	Central
		Authentication	Central
		Status	Associated
		Association ID	1
Client Tune	Regular	// 802.11 Authentication	Open System
Client Type	no Unavailable	Reason Code	1
Liter Name		Status Code	0
Port Number		CF Pollable	Not Implemented
Interface	internet access	CF Poll Request	Not Implemented
VI AN ID	129	Short Preamble	Not Implemented
Quarantine VLA2	NID 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	dress
Address Mobility Move Cr	aunt 0		
Policy Manager 5	state RUN		
Management Fra	ime No		
UpTime (Sec)	71		
Current TxRateS	et m8 ss2		

CMX

Il est possible de vérifier le nombre d'utilisateurs authentifiés sur CMX en ouvrant l'onglet CONNECT&ENGAGE :

cisco 1031-05	DETECT & LOCATE	ANALYTICS CC	CNNECT MANAGE	SYSTEM						admin +
					1	Dashboard	Connect Experiences	Policy Plans	Library 👻	Settings
Q Location Global • No locations available	•	O Interva	al Days	÷	Visitor Search Please enter search patte	m	- 0	۹.		
Global Dashboard										
Today at a Glance - Feb 22, 2018										
203 1			Visitor Trend	compared to:		Data Usa	age:			
Total Visitors Repeat Visitors : 0		New Visitors : 1	Yesterd	ay %	Average		Upload O	Down	load	
Column -		(Area	•						(1)
s — New and Repeat V	isitors	Repeat Visitors New Visitors			Networ	k Usage				

Pour vérifier les détails de l'utilisateur, dans le même onglet, en haut à droite, cliquez sur Visitor Search :

							9	£6 🗢	¢;	Å								
	Visitor Searc	ch														×	Plans Library) a -
Q Location	Please enter search o	query			٩	Downloa	d as CSV 🛓											
Global	Use Search Filter	Options																
alobal Dashl	Search on 19 of 19 selected							*	From 02/21/2018 3:41 PI	М		To 02/22	/2018 3:41 PM	И				
Today at a Glance	Export Preview (Up to 100	results show	m, please e	(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																(
4	-	_	_	_				_	_	_	-	-	-		-	_		
Visitors									Usage									
2									Network O Bytes									

Dépannage

Afin de vérifier le flux des interactions entre les éléments, il y a quelques débogages qui peuvent être effectués le WLC :

>debug client<MAC addr1> <MAC addr2> (saisissez l'adresse MAC d'un ou de plusieurs clients)

>debug web-auth redirect enable mac <adresse MAC> (saisissez l'adresse MAC du client d'authentification Web)

>debug web-auth webportal-server enable

>debug aaa all enable

Ces débogages permettront le dépannage, et si nécessaire, certaines captures de paquets peuvent être utilisées pour compléter.