CMX Connected Experiences -Konfigurationsbeispiel zur Registrierung von Social Networking, SMS und benutzerdefiniertem Portal

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Netzwerkdiagramm Konfigurationen Authentifizierung über SMS Authentifizierung über Konten im sozialen Netzwerk Authentifizierung über ein benutzerdefiniertes Portal Überprüfen Fehlerbehebung

Einführung

Dieses Dokument soll Netzwerkadministratoren durch die Client-Registrierung über die Konfiguration von Gastportalen auf Connected Mobile eXperience (CMX) führen.

CMX ermöglicht Benutzern die Registrierung und Authentifizierung im Netzwerk mithilfe von Social Registration Login, SMS und Custom Portal. In diesem Dokument finden Sie eine Übersicht über die Konfigurationsschritte für den Wireless LAN Controller (WLC) und CMX.

Voraussetzungen

Anforderungen

CMX sollte ordnungsgemäß mit der Basiskonfiguration konfiguriert werden.

Maps aus der Prime-Infrastruktur zu exportieren ist optional.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

Konfigurieren

Netzwerkdiagramm

In diesem Dokument werden zwei verschiedene Methoden zur Authentifizierung von Benutzern/Clients im Wireless-Netzwerk mithilfe von CMX beschrieben.

Zunächst wird das Einrichten der Authentifizierung mithilfe von Social Network Accounts beschrieben, dann die Authentifizierung mithilfe von SMS.

In beiden Szenarien versucht der Client, sich mithilfe der Authentifizierung über CMX auf der SSID zu registrieren.

Der WLC leitet den HTTP-Datenverkehr an CMX um, wo der Benutzer zur Authentifizierung aufgefordert wird. Das CMX enthält die Einrichtung des Portals, das der Kunde für die Registrierung verwenden soll, sowohl über soziale Konten als auch SMS.

Im Folgenden wird der Ablauf des Registrierungsprozesses beschrieben:

- 1. Der Client versucht, der SSID beizutreten und öffnet den Browser.
- 2. Anstelle des Zugriffs auf die angeforderte Website wird vom WLC zum Gastportal umgeleitet.
- 3. Der Client stellt seine Anmeldeinformationen bereit und versucht, eine Authentifizierung vorzunehmen.
- 4. CMX behandelt den Authentifizierungsprozess.
- 5. Bei erfolgreicher Nutzung wird dem Kunden nun ein vollständiger Internetzugang zur Verfügung gestellt.
- 6. Der Client wird an die ursprünglich angeforderte Site umgeleitet.

Die verwendete Topologie ist:



Konfigurationen

Authentifizierung über SMS

Cisco CMX ermöglicht die Client-Authentifizierung über SMS. Für diese Methode muss eine HTML-Seite eingerichtet werden, damit der Benutzer seine Anmeldeinformationen für das System angeben kann.Standardvorlagen werden von CMX nativ bereitgestellt und können später bearbeitet oder durch eine benutzerdefinierte Vorlage ersetzt werden. Der SMS-Service wird durch die Integration von CMX mit <u>Twilio</u> realisiert, einer Cloud-Kommunikationsplattform, die das Senden und Empfangen von Textnachrichten ermöglicht. Twilio ermöglicht eine Telefonnummer pro Portal, d. h., wenn mehr als ein Portal verwendet wird, ist pro Portal eine Telefonnummer erforderlich.

Antwort: WLC-Konfiguration

Auf der Seite des WLC werden sowohl eine SSID als auch eine ACL konfiguriert. Der Access Point muss mit dem Controller und im RUN-Status verbunden sein.

1. ACL

Eine auf dem WLC konfigurierte ACL für HTTP-Datenverkehr ist erforderlich. Um eine ACL zu konfigurieren, gehen Sie zu Sicherheit > Zugriffskontrolllisten > Neue Regel hinzufügen.

Die verwendete IP ist die für das CMX konfigurierte IP. Dadurch wird HTTP-Datenverkehr zwischen dem WLC und dem CMX zugelassen. Die folgende Abbildung zeigt die erstellte ACL, wobei "10.48.39.100" auf die CMX-IP-Adresse verweist.

CISCO	MONI	TOR W	LANs	<u>C</u> ONTROL	LER.	WIRELESS	<u>S</u> E(CURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK		
Security	Acce	ess Con	trol Li	ists > Ed	it									
 AAA General RADIUS Authentication Accounting Fallback DNS Downloaded AVP 	Gene Access Deny	s List Name Counters	e	CMX_re 0	direc	t Destination		Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
LDAP Local Net Users	1	Permit	0.0.0.	0	/ 1	10.48.39.100 255.255.255.255	/ .	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	HTTP	Any	Any	Any	0	

2. WLAN

Die Integration mit dem Portal erfolgt, daher müssen Sicherheitsrichtlinien im WLAN geändert werden.

Zuerst wählen Sie WLANs->Edit->Layer 2->Layer 2 Security, und wählen Sie in der Dropdown-Liste None (Keine) aus, um die Layer 2 Security-Funktion zu deaktivieren. Wechseln Sie dann auf der gleichen Registerkarte "Sicherheit" zu Layer 3. Wählen Sie im Dropdownmenü für die Layer-3-Sicherheit die Option Webrichtlinie und dann Passthrough aus. Wählen Sie unter Preauthentication ACL die zuvor konfigurierte IPv4-ACL aus, um diese an das entsprechende WLAN zu binden, in dem die SMS-Authentifizierung bereitgestellt werden muss. Die Option Globale Konfiguration überschreiben muss aktiviert sein, und der Web Auth-Typ muss extern sein (Umleitung zum externen Server), damit die Clients zum CMX-Dienst umgeleitet werden können. Die URL muss mit dem CMX SMS-Authentifizierungsportal identisch sein. Das Format lautet http://<CMX-IP>/visitor/login.

alulu cisco	Save Configuration Ping Logout Refresh MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'cmx_sms' < Back Apply
VLANS	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers Layer 2 Security [©] None + MAC Filtering ² + + 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 Advanced 	Layer 3 Security Web Policy © Captive Network Assistant Bypass None © Authentication Passthrough Conditional Web Redirect Splash Page Web Redirect On MAC Filter failure ^{1,0} Web policy done locally on Ap <u>exacrains</u> Preauthentication ACL IPv4 CMX_redirect © IPv6 None © WebAuth FlexAcl None © Qr Code Scanning Email Input Sleeping Client Enable Override Global Config ²⁰ Z Enable
	Web Auth type External(Re-direct to external server) Redirect URL http://10.48.39.100/visitor/login

B. Twilio

CMX bietet Twilio-Integration für Textnachrichtendienste. Die Anmeldeinformationen werden bereitgestellt, nachdem das Konto auf Twilio richtig konfiguriert wurde. Es werden sowohl ACCOUNT SID als auch AUTH TOKEN benötigt.

Twilio hat eigene Konfigurationsanforderungen, die durch den Prozess der Einrichtung des Service dokumentiert sind. Vor der Integration in CMX kann der Twilio-Service getestet werden, sodass Probleme im Zusammenhang mit der Twilio-Einrichtung erkannt werden können, bevor dieser Service mit CMX verwendet wird.

(ii) tw	ilio				docs \checkmark			~					
	∨ s	iettings /		UPGRADE	, O Go to	\Leftrightarrow	?	\$					
☆	Dashboard Billing	Two-Factor Authentication											
\odot	Usage Settings	Add an extra layer of protection to your account, w DISABLED Do not require a verification code	layer of protection to your account, with a verification code sent via SMS or voice call.										
	General Subaccounts	ONCE PER COMPUTER Trust computers and only	E 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	code										
	Doer Profile	API Credentials											
	Upgrade	LIVE Credentials	Learn about REST API Credentials 7	TEST Credentials	Learn abou	t Test Cre	dentials	я					
		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		W Keep this somewhere safe and secure									

C. CMX-Konfiguration

Der Controller muss dem CMX ordnungsgemäß hinzugefügt und die Karten aus der Prime-Infrastruktur exportiert werden.

SMS-Registrierungsseite

Es gibt eine Standardvorlage für das Registrierungsportal. Portale finden Sie unter CONNECT&ENGAGE->Library. Wenn Sie eine Vorlage möchten, wählen Sie im Dropdown-Menü die Option Vorlagen.

Wenn Sie Twilio in das Portal integrieren möchten, rufen Sie Twilio Configuration auf, und geben Sie die Konto-ID und das Auth-Token an. Wenn die Integration erfolgreich ist, wird die im Twilio-Konto verwendete Nummer angezeigt.

cisco 10.3.0.62	Q DETECT & LOCATE	ANALYTICS	CONNECT 8 ENGAGE	¢¢ MANAGE	SYSTEM				(admin +
						Dashboard	Connect Experiences	Policy Plans	Library v	Settings -
Login Page • •	e enter your number to get Wi-Fi tave SMS Code? X Phone Number* C iew and accept our Terms & Conditions to Wi-Fi. SUBMIT	English	• 0	CONTENT Haw SMS 4 Enter Aut Fro Num Enter C Error Mes	BACKGROUND	THEMES LANGU	AGES 3dbd	 ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? <lp>? </lp> ? <lp>? <!--</th--><th>nal B lan lan</th><th>EDIT</th></lp>	nal B lan lan	EDIT

Authentifizierung über Konten im sozialen Netzwerk

Bei der Authentifizierung des Clients mithilfe von Social-Network-Konten muss der

Netzwerkadministrator eine gültige Facebook-APP-Kennung für das CMX hinzufügen.

Antwort: WLC-Konfiguration

Auf der Seite des WLC werden sowohl eine SSID als auch eine ACL konfiguriert. Der Access Point muss dem Controller und im RUN-Status angeschlossen sein.

1. ACL

Da hier HTTPS als Authentifizierungsmethode verwendet wird, muss eine ACL, die HTTPS-Datenverkehr zulässt, auf dem WLC konfiguriert werden. Um eine ACL zu konfigurieren, gehen Sie zu Sicherheit > Zugriffskontrolllisten > Neue Regel hinzufügen.

Die CMX-IP muss verwendet werden, um HTTPS-Datenverkehr zwischen dem WLC und dem CMX zuzulassen. (in diesem Beispiel lautet die CMX-IP 10.48.39.100)

cisco	MONI	TOR W	(LANs		ER WIRELESS	5	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK		
Security	Acce	ess Cor	ntrol Li	sts > Edi	:								
 AAA General RADIUS Authentication Accounting Fallback DNE 	Gene Access Deny	eral s List Nam Counters	e	CMX_Aut	h								
Downloaded AVP TACACS+	Seq	Action	Source	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) ()	10.48.39.100 255.255.255.2	/ 55	ТСР	Any	HTTPS	Any	Any	0	
Local EAP													

Außerdem ist eine DNS-ACL mit Facebook-URLs erforderlich. Dazu suchen Sie unter Security - >Access Control Lists (Sicherheit ->Zugriffskontrolllisten) nach dem Eintrag der zuvor konfigurierten ACL (in diesem Fall CMX_Auth) und bewegen die Maus am Ende des Eintrags zum blauen Pfeil und wählen Add-Remove URL aus. Nach diesem Typ die URLs von Facebook auf dem URL-Zeichenfolgennamen und dem Hinzufügen.

،،ا،،،ا،، cısco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLLER WIRELESS <u>S</u> ECURITY MANAGEMENT C <u>O</u> MMANDS HELP <u>F</u> EEDBACK	
Security	ACL > CMX_Auth > URL List	
 ▼ AAA General ▼ RADIUS Authentication Accounting 	URL String Name	
Fallback	facebook.com	
DNS	m.facebook.com	
TACACS+ LDAP	fbcdn.net	

2. WLAN

Die Sicherheitsrichtlinien ändern sich, damit die Registrierung funktioniert. Es muss eine spezifische Konfiguration im WLAN vorgenommen werden.

Wie bereits bei der SMS-Registrierung, zuerst auf WLANs->Edit->Layer 2->Layer 2 Security, und in der Dropdown-Liste "None" (Keine), wird die Layer 2 Security deaktiviert. Ändern Sie auf der Registerkarte "Sicherheit" die Option "Layer 3". Wählen Sie im Dropdownmenü für die Layer-3-

Sicherheit die Option Webrichtlinie und dann Passthrough aus. Wählen Sie unter "Preauthentication ACL" die zuvor konfigurierte IPv4-ACL aus, um diese an das entsprechende WLAN zu binden, in dem die Authentifizierung über Facebook bereitgestellt werden muss. Die Option Globale Konfiguration überschreiben muss aktiviert sein, und der Web Auth-Typ muss extern sein (Umleitung zum externen Server), damit die Clients zum CMX-Dienst umgeleitet werden können. Beachten Sie, dass sich die URL diesmal im folgenden Format befinden muss: https://<CMX-IP>/visitor/login.

ululu cisco	Sa <u>v</u> e Configuration <u>P</u> ing 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 HELP <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 ^g None + MAC Filtering ^g + Fast Transition + Fast Transition +
cisco	Save Configuration Ping Logout Refresh MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK nh Home
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 +
	OAuthentication
	O Passthrough
	O Conditional Web Redirect
	○ Splash Page Web Redirect
	On MAC Filter failure ¹⁰
	Preauthentication ACL IPv4 CMX_Auth IPv6 None WebAuth FlexAcl None
	Email Input
	Sleening Client Enable
	Sleeping Client Enable

B. Facebook für Entwickler

URL https://10.

/visitor/login

Für die Integration von Facebook und CMX ist eine Facebook-App erforderlich, damit die richtigen Token zwischen den beiden Teilen ausgetauscht werden können.

Auf <u>Facebook für Entwickler</u> können Sie die App erstellen. Zur Integration der Services sind einige App-Konfigurationsanforderungen erforderlich.

Stellen Sie in den Anwendungseinstellungen sicher, dass Client-OAuth-Anmeldung und Web-OAuth-Anmeldung aktiviert sind. Überprüfen Sie außerdem, ob die gültigen OAuth-Umleitungs-URIs die CMX-URL im Format **https**://<CMX-IP>/visitor/login enthalten.



Damit die App veröffentlicht und in CMX integriert werden kann, muss sie veröffentlicht werden. Gehen Sie dazu zu "App Review->Make <App-Name> public?" (Anwendungsprüfung >> öffentlich machen). und den Status auf Yes (Ja) ändern.

App Dashboard		Docs Tools Support	Q Search developers.f
Catarina's first app 🔻	APP ID:	ON Status: Live	A View Analytics
☆ Dashboard ☆ Settings >> Eg Roles >> ▲ Alerts >>	Make Catarina's first app public? Your app is currently live and available to the public.		
 App Review PRODUCTS ⊕ © Facebook Login → Ξ 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. CMX-Konfiguration

Der Controller muss dem CMX ordnungsgemäß hinzugefügt und die Karten aus der Prime-Infrastruktur exportiert werden.

Registrierungsseite

Um eine Registrierungsseite für CMX zu erstellen, müssen die gleichen Schritte wie zuvor ausgeführt werden, um die Seite für die SMS-Registrierungsseite zu erstellen. Wählen Sie CONNECT&ENGAGE->Library, Template Portals ready to be edited aus, indem Sie im Dropdown-Menü Templates (Vorlagen) auswählen.

Für die Registrierung über Facebook-Anmeldeinformationen muss das Portal über eine Verbindung mit Social Accounts verfügen. Um dies von Grund auf zu erledigen, müssen Sie beim Erstellen eines benutzerdefinierten Portals CONTENT->Common Elements->Social Auth angeben und Facebook auswählen. Geben Sie dann den von Facebook erhaltenen App-Namen und die App-ID (Schlüssel) ein.

cisco 10.8.1-86		DETECT & LOCATE	ANALYTICS	CONNECT 8 ENGAGE	¢ Manage	SYSTEM			(†	admin -
							Dashboard	Connect Experiences	Policy Plans Library	Settings -
RegistrationPage &								Live View	Portals Library	Save
Login Page 👻 🌣			English	• 6	CONTENT	BACKGROUND	THEMES LANGUAGES			EDIT
	Legis le seggest le uif				Social	.ogin			Remove eleme	int
	×				Depe	ends on Terms and C	Conditions			- 11
	f				- Content					
					Ca	acebook 🧬 Scope: tarina's first app	Basic Profile Key:			
					0	create new				- 11

Authentifizierung über ein benutzerdefiniertes Portal

Das Authentifizieren des Clients mithilfe des Benutzerdefinierten Portals ähnelt dem Konfigurieren der externen Webauthentifizierung. Die Umleitung erfolgt an das auf CMX gehostete benutzerdefinierte Portal.

Antwort: WLC-Konfiguration

Auf der Seite des WLC werden sowohl eine SSID als auch eine ACL konfiguriert. Der Access Point muss dem Controller und im RUN-Status angeschlossen sein.

1. ACL

Da hier HTTPS als Authentifizierungsmethode verwendet wird, muss eine ACL, die HTTPS-Datenverkehr zulässt, auf dem WLC konfiguriert werden. Um eine ACL zu konfigurieren, gehen Sie zu Sicherheit > Zugriffskontrolllisten > Neue Regel hinzufügen.

Die CMX-IP muss verwendet werden, um HTTPS-Datenverkehr zwischen dem WLC und dem CMX zuzulassen. (in diesem Beispiel lautet die CMX-IP 10.48.71.122).

Hinweis: Aktivieren Sie SSL auf dem CMX, indem Sie in der CMX-CLI den Befehl "cmxctl node sslmode enable" eingeben.

ဂျကျက cisco	MONIT	OR <u>W</u> I	LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMAND	S HELP	FEEDBACK					
urity	Acces	s Con	trol Li	sts > Edit											
eneral	Gener	al													
Authentication Accounting	Access	.ist Name	2	CMX_HTTPS	;										
Fallback DNS Downloaded AVP	Deny Co	ounters	Source	0 e TP/Mask		Destinatio	on TP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
CACS+	1	Permit	10.48.	71.122 /	255.255.255.255	0.0.0.0	/ 0.0.0.0		CP	HTTPS	Any	Any	Any	0	
ocal Net Users AC Filtering isabled Clients	2	Permit	0.0.0.0	0 /	0.0.0.0	10.48.71.1	22 / 255.255	5.255.255 1	CP	Any	HTTPS	Any	Any	0	

2. WLAN

Die Sicherheitsrichtlinien ändern sich, damit die Registrierung funktioniert. Es muss eine spezifische Konfiguration im WLAN vorgenommen werden.

Wie bereits bei der Registrierung von SMS und sozialen Netzwerken wurde zuerst WLANs->Edit->Layer 2->Layer 2 Security (WLANs->Edit->Layer 2->Layer 2 Security) ausgewählt. Wählen Sie in der Dropdown-Liste None (Keine) aus, um die Layer 2 Security-Funktion zu deaktivieren. Ändern Sie auf der Registerkarte "Sicherheit" die Option "Layer 3". Wählen Sie im Dropdownmenü für die Layer-3-Sicherheit die Option Webrichtlinie und dann Passthrough aus. Wählen Sie in der ACL für die Vorauthentifizierung die zuvor konfigurierte IPv4-ACL (in diesem Beispiel CMX_HTTPS genannt) aus, und binden Sie sie an das entsprechende WLAN. Die Option Globale Konfiguration überschreiben muss aktiviert sein, und der Web Auth-Typ muss extern sein (Umleitung zum externen Server), damit die Clients zum CMX-Dienst umgeleitet werden können. Beachten Sie, dass sich die URL diesmal im folgenden Format befinden muss: https://<CMX-IP>/visitor/login.

،، ،،، ،، cısco	MONITOR	<u>W</u> LANs		WIRELESS	<u>s</u> ecurity	M <u>A</u> NAG	SEMEN
WLANs	WLANs >	Edit 'o	:mx_login'				
▼ WLANs	General	Secu	rity QoS	Policy-Map	ping Ad	vanced	
Advanced	Layer	2 Lay	er 3 AAA	Servers			
	Laye	r 2 Security	∕ ⁶ None MAC Filterin	\$ 9 <mark>9</mark> _)		
	Fast Tra	ansition					
	Fast Tra	nsition	Di	sable 🛊			
	Lobby A Lobb	y Admin Admin Ad	ccess				

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 ^{1,2} Web policy done locally on AP <u>Macrima</u> Preauthentication ACL IPv4 CMX_HTTPS ‡ IPv6 None ‡ WebAuth FlexAcl None ‡ Preauthentication ACL IPv4 CMX_HTTPS ‡ IPv6 None ‡ WebAuth FlexAcl None ‡ Coverride Global Config ² 2 Enable Web Auth type External(Re-direct to external server) ‡ Redirect URL https://10.48.71.122/visitor/login

C. CMX-Konfiguration

Der Controller muss dem CMX ordnungsgemäß hinzugefügt und die Karten aus der Prime-Infrastruktur exportiert werden.

Registrierungsseite

Zum Erstellen einer Registrierungsseite für CMX gehen Sie wie zuvor vor, um die Seite für andere Authentifizierungsmethoden zu erstellen. Wählen Sie CONNECT&ENGAGE->Library, Template Portals ready to be Edit (Zur Bearbeitung bereite Vorlagenportale) aus, indem Sie im Dropdown-Menü die Option Templates (Vorlagen) auswählen.

Das Portal für die normale Registrierung kann von Grund auf (wählen Sie "Benutzerdefiniert") oder angepasst aus der Vorlage "Registrierungsformular" in der CMX-Bibliothek verfügbar gemacht werden.

cisco 10.41-22		ANALYTICS	ç connect	MAN	AGE SI	STEM						•	admin -
									Dashboard	Connect Experiences	Policy Plans	Library 👻	Settings 👻
Login_Page 🖋										Live View	Delete Porta	is Library	Save
Login Page 🔹 🔹		English	•	Θ	CONTENT	BACKGRO	OUND THEMES	LANGUAGES					
	Constitute and interface to exchange the set				O To add a	in element, si	imply drag & drop it to the	e canvas or click on it!					
	Complete registration to onboard to will.				- Common el	ements							
	Name* 📀 Email 📀				in Ele	hage ment	T Text Element		Social Auth	V Terms & Conditions	image & Te	= ort	
	_						<u>≣∄</u> Contact us	‡ ↓ Spacer		Menu	Cpt-out	=	
					- Advertisem	ent elements							
					imag	e Sider	External Content						

Überprüfen

WLC

Um zu überprüfen, ob der Benutzer erfolgreich auf dem System authentifiziert wurde, gehen Sie in der WLC-GUI zu MONITOR->Clients, und suchen Sie in der Liste nach der MAC-Adresse des Clients:

սիսիս								Sa <u>v</u> e Co	nfiguration	Ping Logou	t <u>B</u> efresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGE	MENT COMMANDS HELP FEEDBACK									Home
Monitor	Clients									Entries 1	- 1 of 1
Summary	Current Filter None [Change Filter] [Clear Filter]	d									
Access Points											
Cisco CleanAir											
Statistics	Client MAC Addr IP Address(Ipv4/Ipv6)	AP 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											
Sleeping Clients											
Multicast											
Applications											
Local Profiling											
	Foot Notes										
	RLAN Clients connected to AP702w, will not show Client IP details.										

Klicken Sie auf die MAC-Adresse des Clients, und bestätigen Sie in den Details, dass der Status des Client Policy Manager den Status "RUN" aufweist:

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	/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

Sie können überprüfen, wie viele Benutzer in CMX authentifiziert werden, indem Sie die Registerkarte CONNECT&ENGAGE öffnen:

cisco 10.31-36	DETECT AN	ALYTICS CON	ECT MANAGE	SYSTEM			C	admin -
						Dashboard Connect Experien	ces Policy Plans Library	- Settings
Q Location Global • No locations available	Ŧ	O Interval	ys		Visitor Search Please enter search patte	m	- Q	
Global Dashboard								
Today at a Glance - Feb 22, 2018								
201 1			Visitor Trend c	ompared to:		Data Usage:		
Total Visitors			Yesterda	, %	Average	Upload O	Download	
Repeat Visitors : 0		New Visitors : 1						
Column +		(i)	Area	•				(i)
New and Repeat Visitors		Repeat Visitors New Visitors			Netwo	rk Usage		

Um die Benutzerdetails zu überprüfen, klicken Sie auf der gleichen Registerkarte oben rechts auf "Visitor Search:" (Besuchersuche):

							9	<u>&</u> 🗢	•\$.									
	Visitor Searc	h	Control of the c																
Q Location	Please enter search q	uery			۹	Downloa	id as CSV 🕭												
Global	Use Search Filter C	options																	
Global Dash	Search on 19 of 19 selected							•	From 02/21/2018 3:41 PI	И		To 02/22	/2018 3:41 PN	И		=			
Today at a Glance	Export Preview (U	lp to 100 i	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 CustomPortal	REGISTRATION	PC	Windows 10	0	0	Catarina Silva	female	0		
Column	Previous 1	Next																((m)
,	Showing 1 of 1																		
4																			
of Visitor									Caster -										
2									Networ										

Fehlerbehebung

Um den Fluss der Interaktionen zwischen den Elementen zu überprüfen, gibt es einige Debuggen, die mithilfe des WLC durchgeführt werden können:

>Debug-Client<MAC-Adresse1> <MAC-Adresse2> (Geben Sie die MAC-Adresse eines oder mehrerer Clients ein)

>Web-Authentifizierungs-Umleitung debug enable mac <MAC-Adresse> (Geben Sie die MAC-Adresse des Web-Authentifizierungs-Clients ein)

>Webportal-Server für die Webauthentifizierung debug aktivieren

>debuaa all enable

Dieses Debuggen ermöglicht die Fehlerbehebung, und bei Bedarf können einige Paketerfassungen als Ergänzung verwendet werden.