

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

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[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 authentifieren 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

## Netwerkdigram

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.

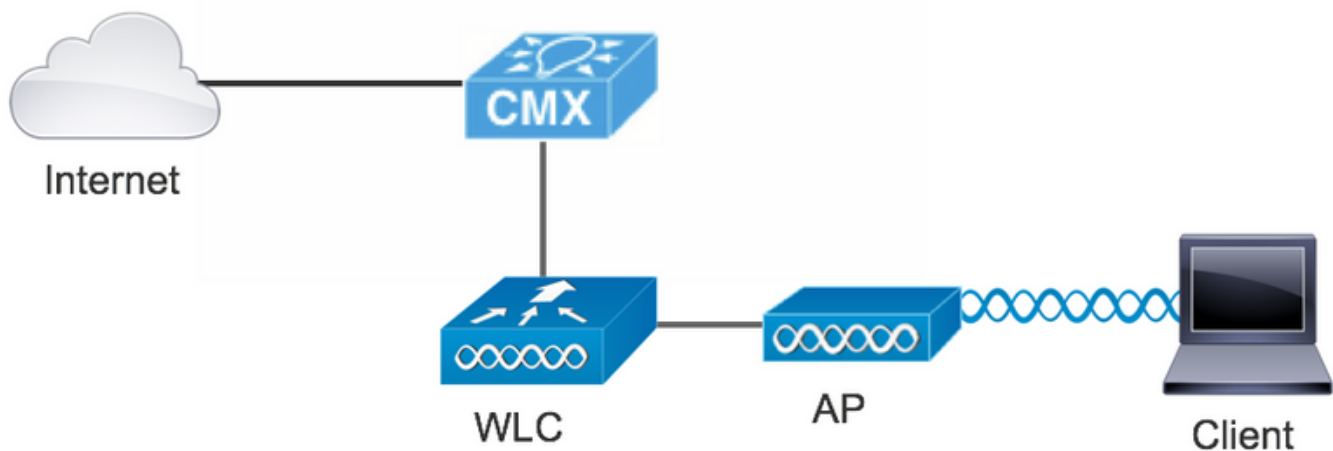
In beide scenario's zal de client proberen om zich op de SSID te registreren door gebruik te maken van verificatie via CMX.

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 HTML-pagina 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 [Twilio](#), 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.

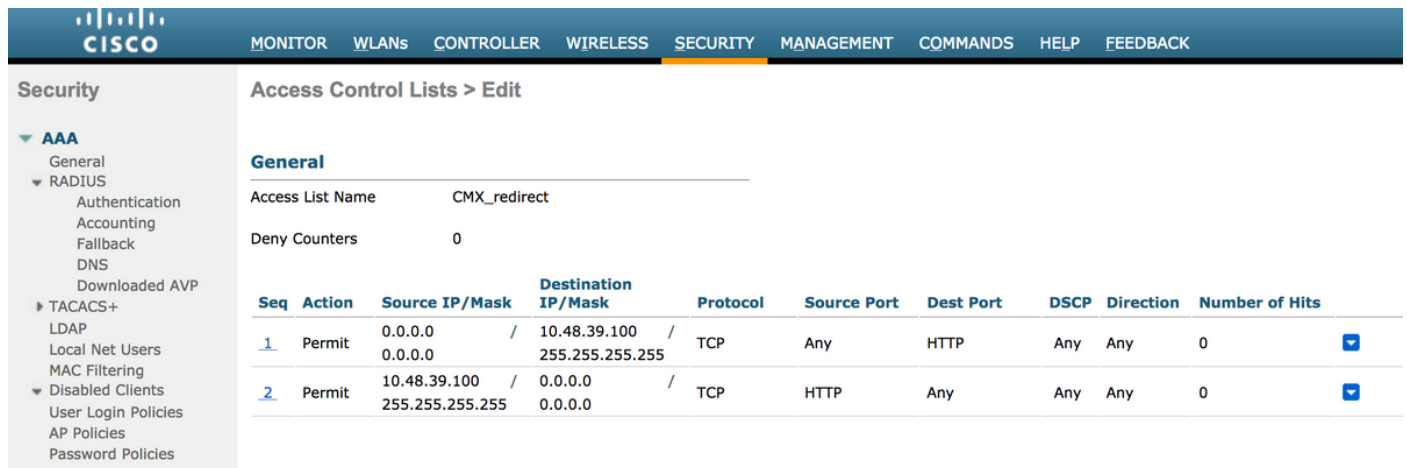
## A. WLC-configuratie

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.



The screenshot shows the Cisco WLC configuration interface for 'Access Control Lists > Edit'. The 'General' tab is active, showing the 'Access List Name' as 'CMX\_redirect' and 'Deny Counters' as '0'. Below this is a table of ACL entries:

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	10.48.39.100 / 255.255.255.255	TCP	Any	HTTP	Any	Any	0
2	Permit	10.48.39.100 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTP	Any	Any	Any	0

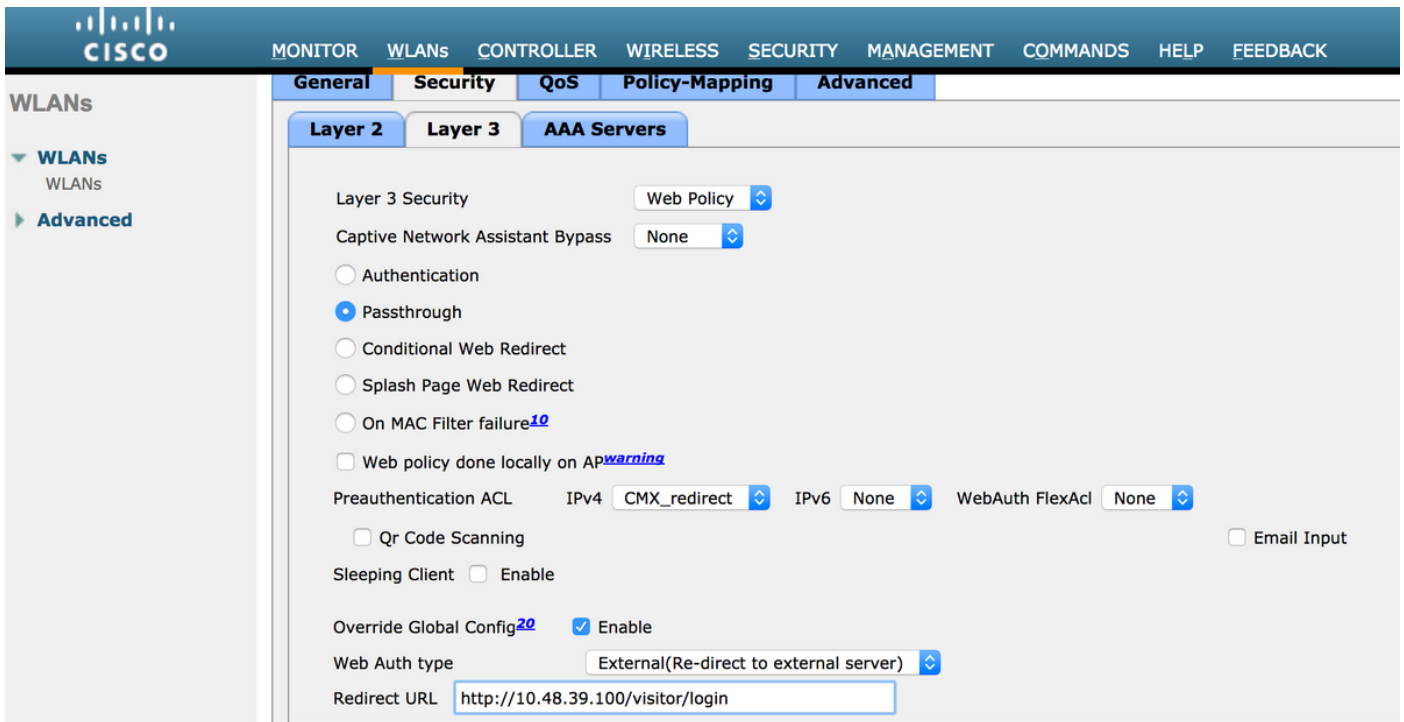
### 2. WLAN

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.



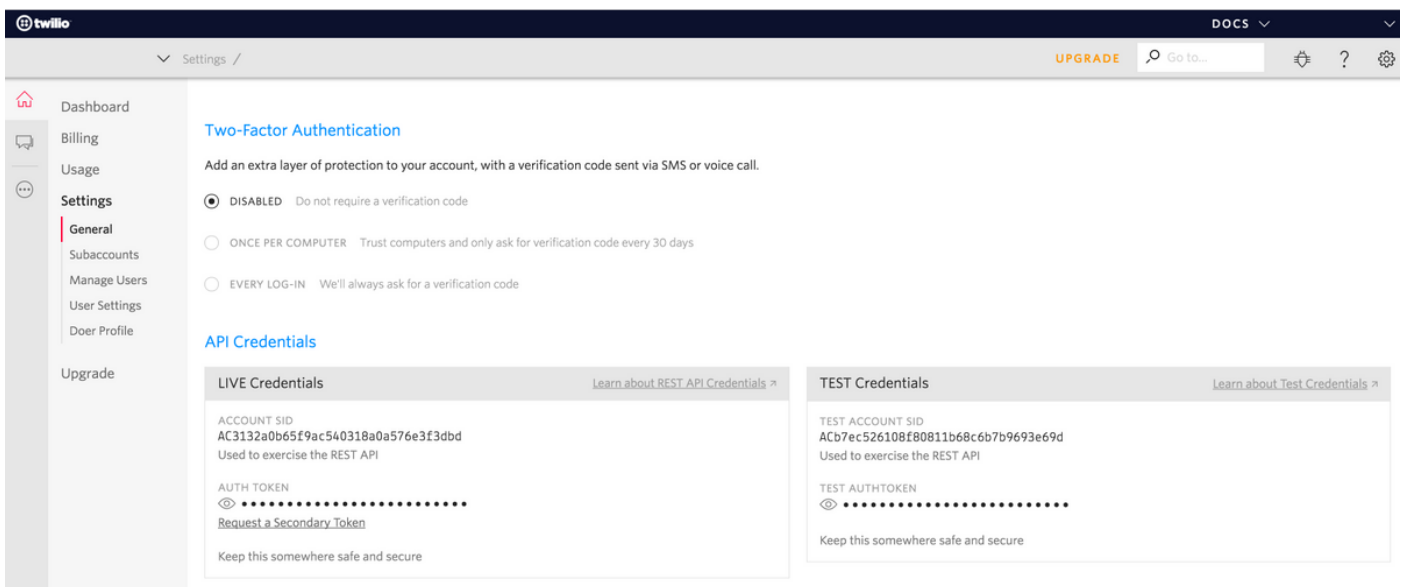
The screenshot shows the Cisco WLC configuration interface for 'WLANs > Edit 'cmx\_sms''. The 'Security' tab is active, and the 'Layer 3' sub-tab is selected. The 'Layer 2 Security' dropdown is set to 'None', and 'MAC Filtering' is disabled. The 'Fast Transition' dropdown is set to 'Disable'.



## B. Twilio

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

Twilio 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 Twilio-instelling. Deze kunnen worden gedetecteerd voordat u de service met CMX gebruikt.



## C. CMX-configuratie

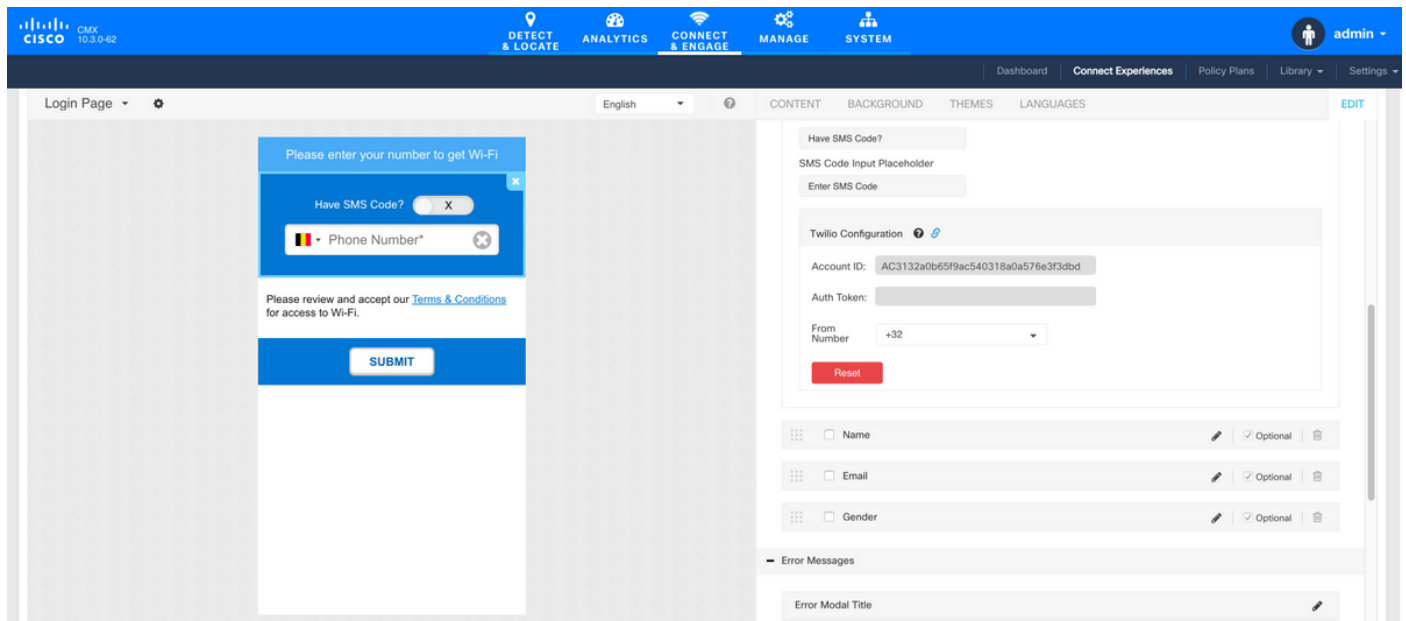
De controller moet naar behoren aan de CMX worden toegevoegd en de kaarten moeten worden geëxporteerd uit de Prime-infrastructuur.

- Sms-registratiepagina

Er is een standaardjabloon 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.



## 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)

**Security** | Access Control Lists > Edit

**General**

Access List Name: CMX\_Auth

Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	10.48.39.100 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTPS	Any	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	10.48.39.100 / 255.255.255.255	TCP	Any	HTTPS	Any	Any	0

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.

**Security** | ACL > CMX\_Auth > URL List

URL String Name:  Add

URL Name
facebook.com
m.facebook.com
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**.

**WLANs** | WLANs > Edit 'cmxFW'

Save Configuration | Ping | Logout | Refresh

MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK

**WLANs** | **Advanced**

General | Security | QoS | Policy-Mapping | Advanced

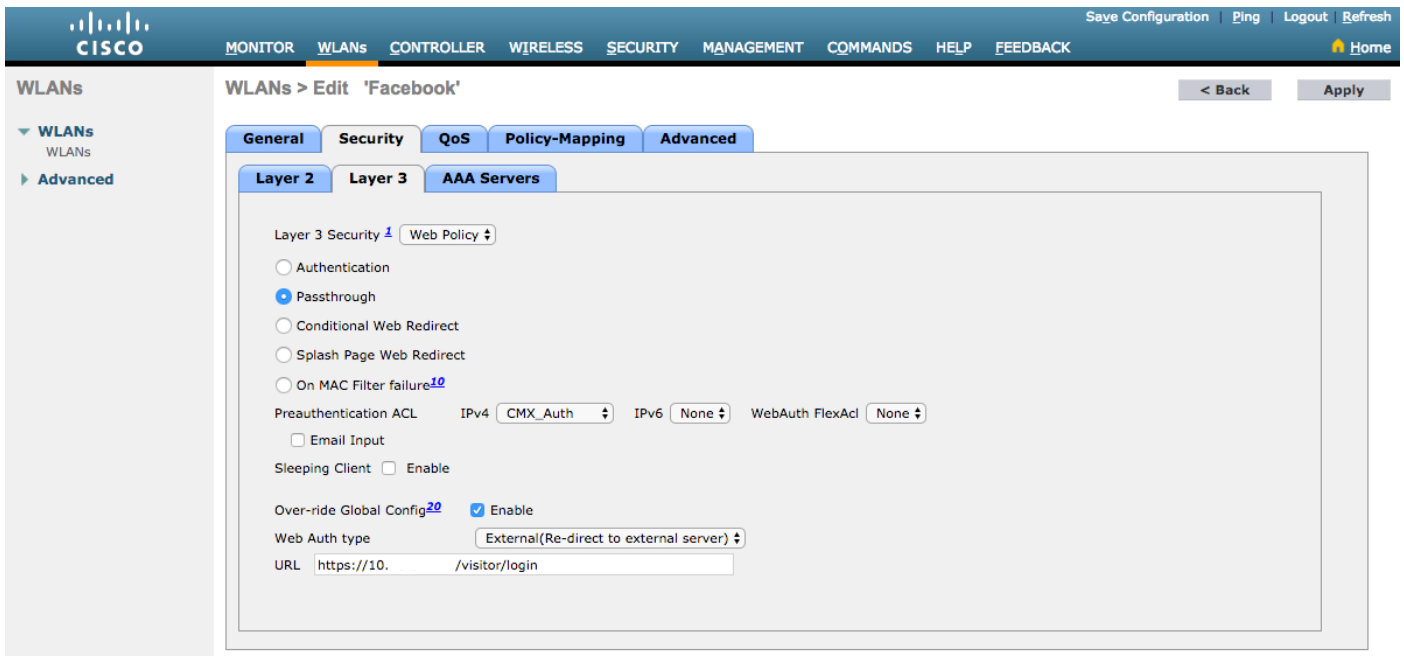
Layer 2 | Layer 3 | AAA Servers

Layer 2 Security: None

MAC Filtering:

Fast Transition

Fast Transition: Disable

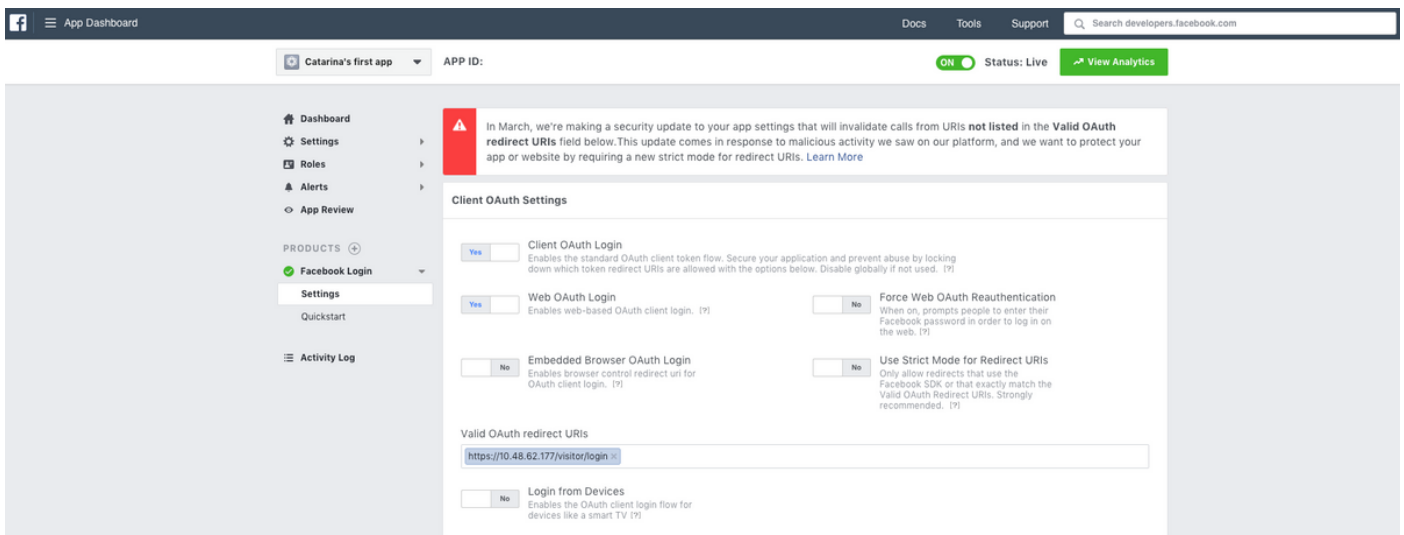


## B. Facebook voor Ontwikkelaars

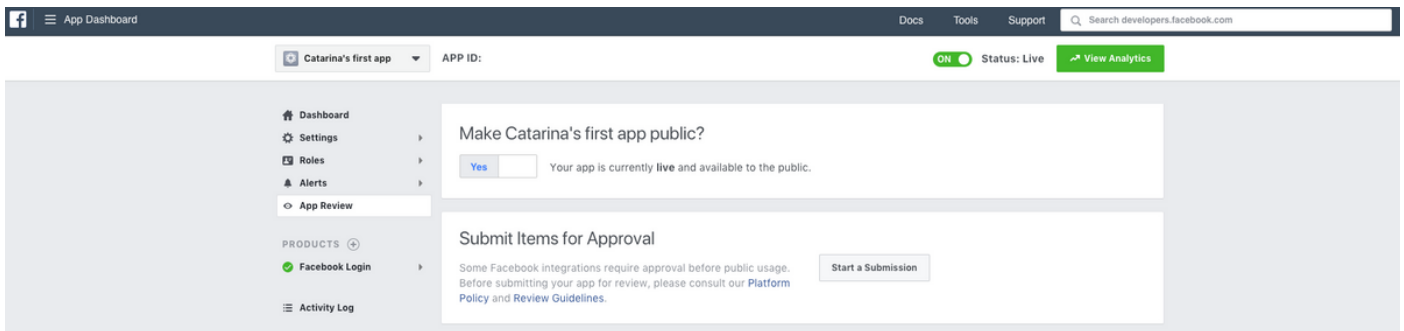
Voor de integratie van Facebook en CMX is een app van Facebook nodig om de juiste penningen tussen de twee partijen te laten ruilen.

Ga naar [Facebook voor Ontwikkelaars](#) 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.



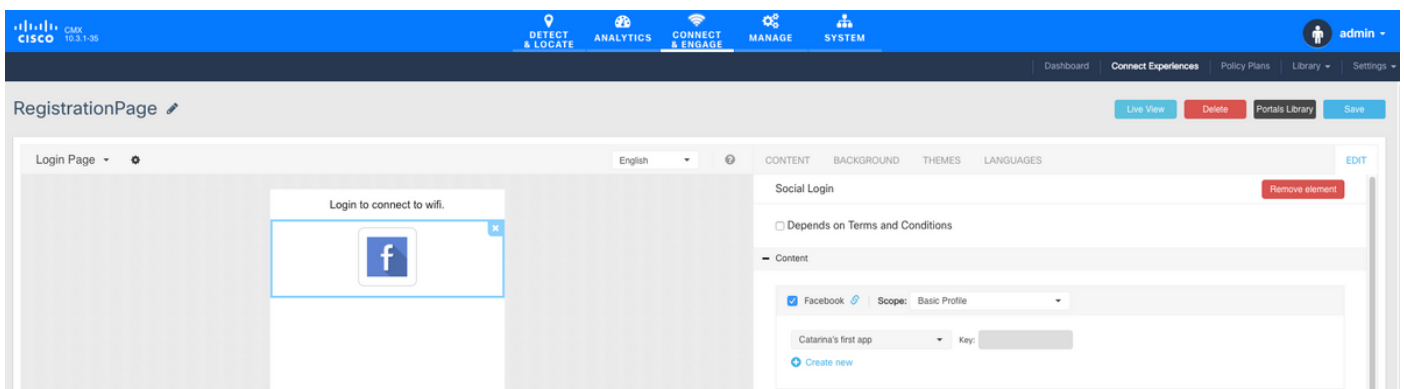
### C. CMX-configuratie

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.



### 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

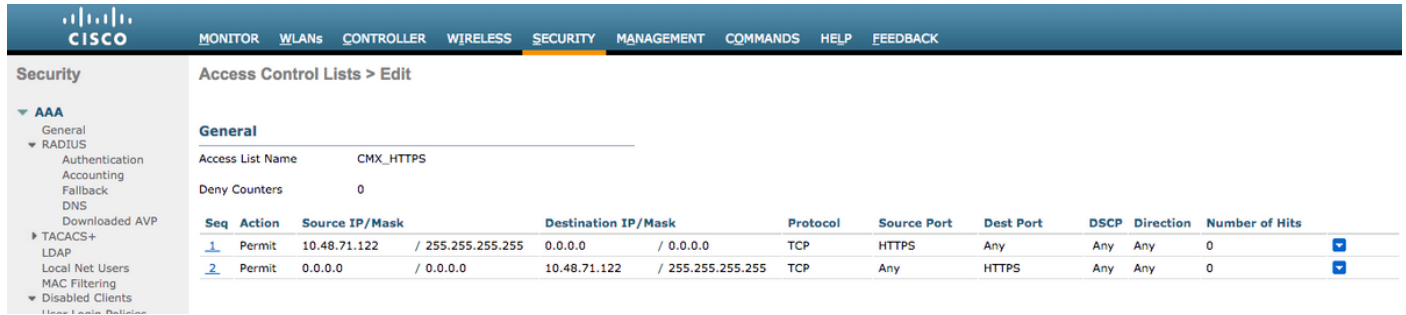
Zoals hier gebruik we HTTPS als authenticatiemethode, moet een ACL die HTTPS verkeer toelaat op de WLC worden geconfigureerd. Om ACL te configureren gaat u naar Security-



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.



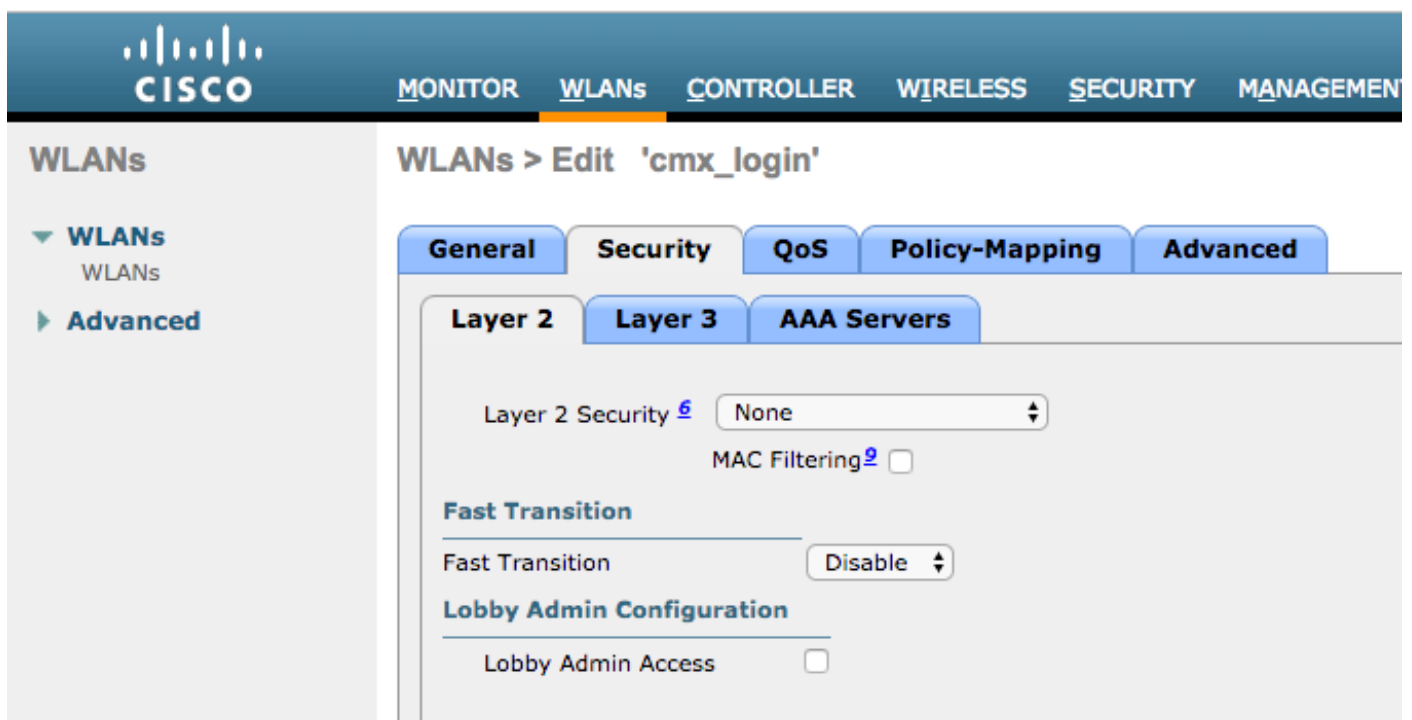
The screenshot shows the Cisco WLC Security configuration page for Access Control Lists. The 'General' tab is selected, showing the 'Access List Name' as 'CMX\_HTTPS' and 'Deny Counters' as '0'. A table lists the configured rules:

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	10.48.71.122 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTPS	Any	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	10.48.71.122 / 255.255.255.255	TCP	Any	HTTPS	Any	Any	0

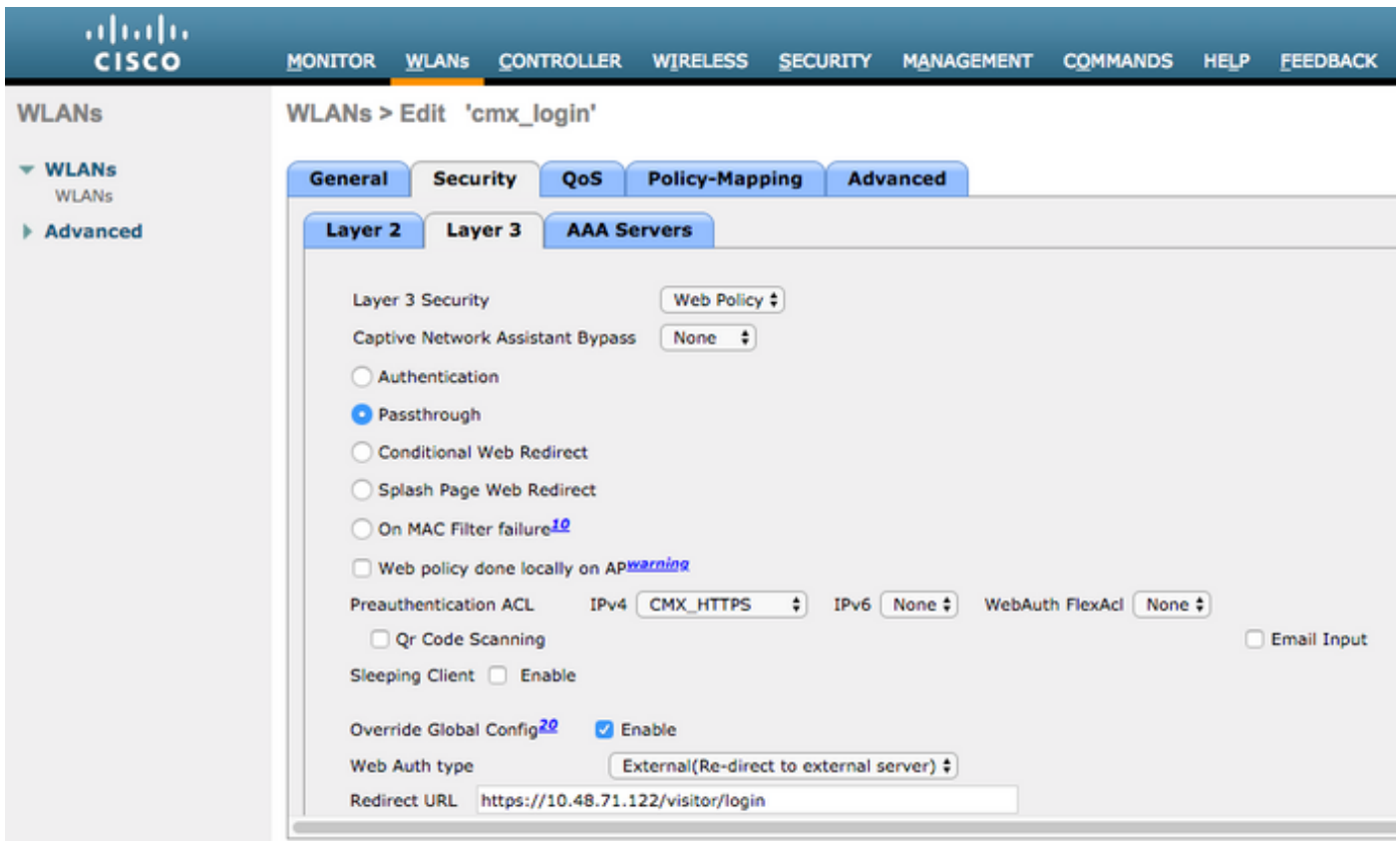
## 2. WLAN

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 2-beveiliging 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**.



The screenshot shows the Cisco WLC WLAN configuration page for 'cmx\_login'. The 'Security' tab is selected, and the 'Layer 3' sub-tab is active. The 'Layer 2 Security' is set to 'None', and 'MAC Filtering' is disabled. The 'Fast Transition' is set to 'Disable', and 'Lobby Admin Access' is also disabled.



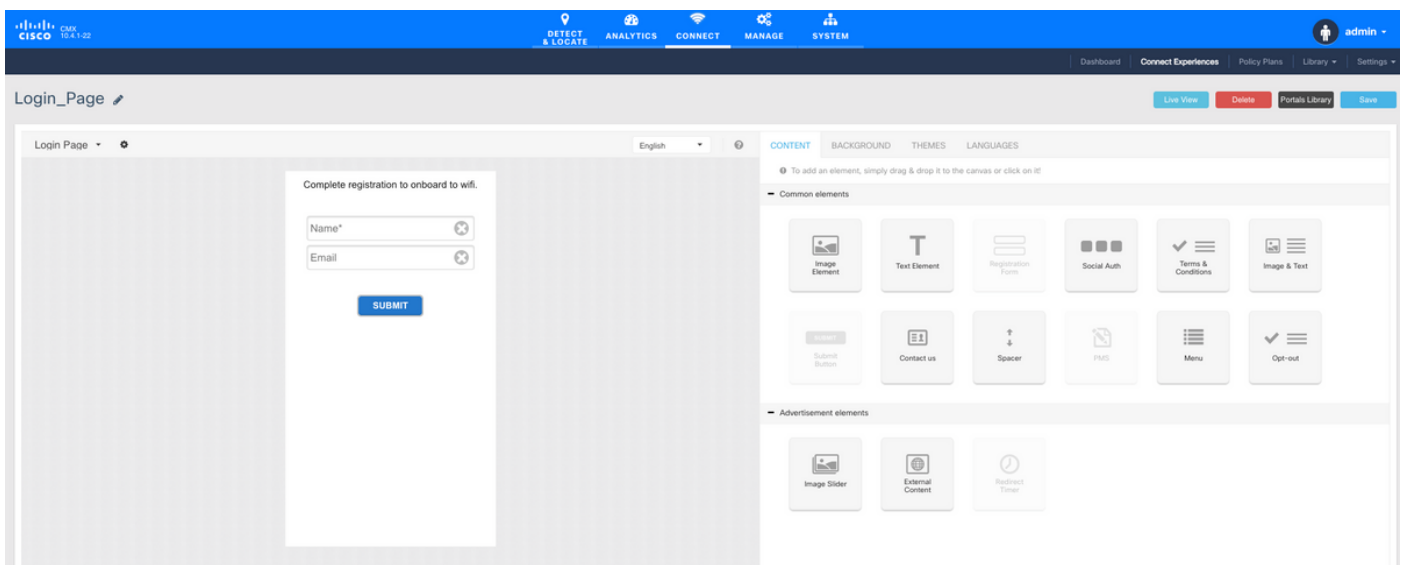
### C. CMX-configuratie

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.

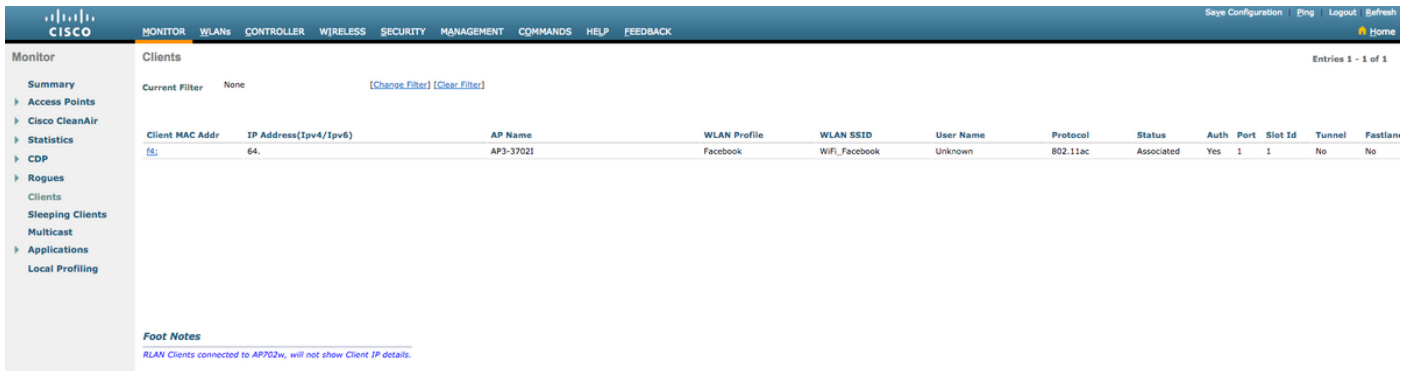
Het portal voor normale registratie kan vanaf het begin worden gebruikt (selecteer "Aangepast") of aangepast aan de sjabloon "Registratieformulier" die in de CMX-bibliotheek beschikbaar is.



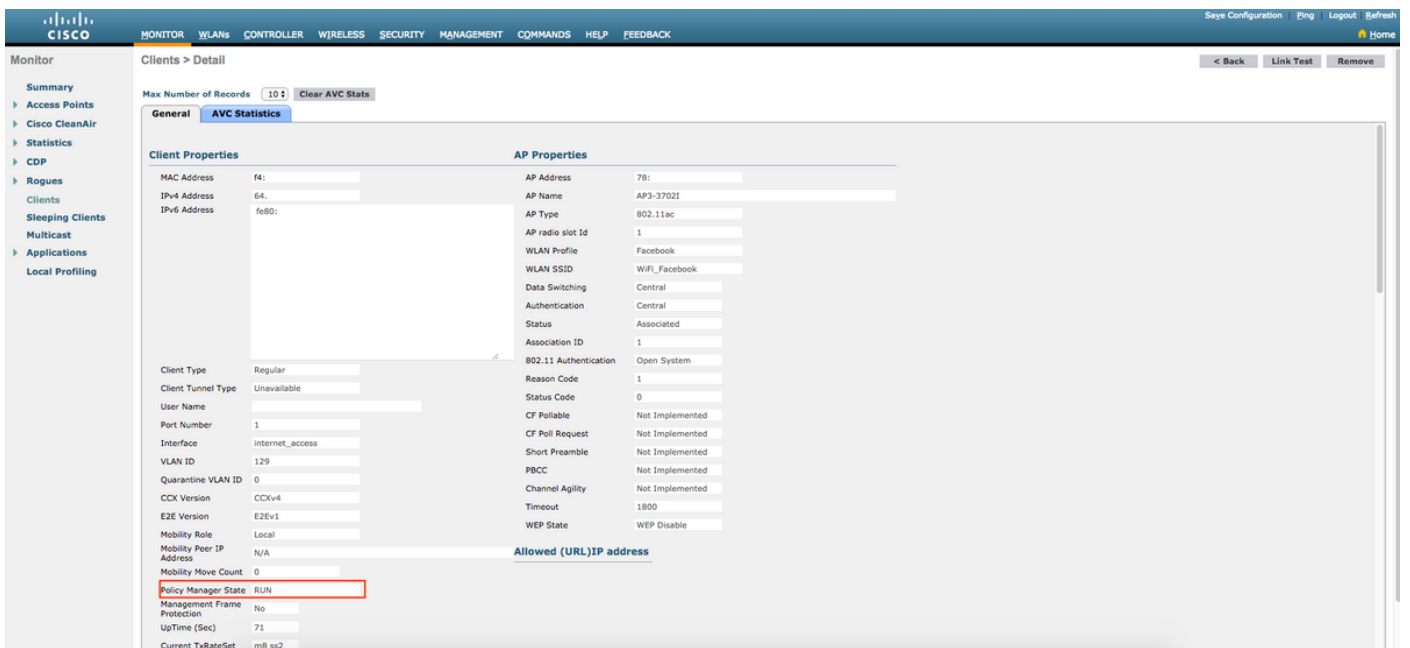
## Verifiëren

# 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:

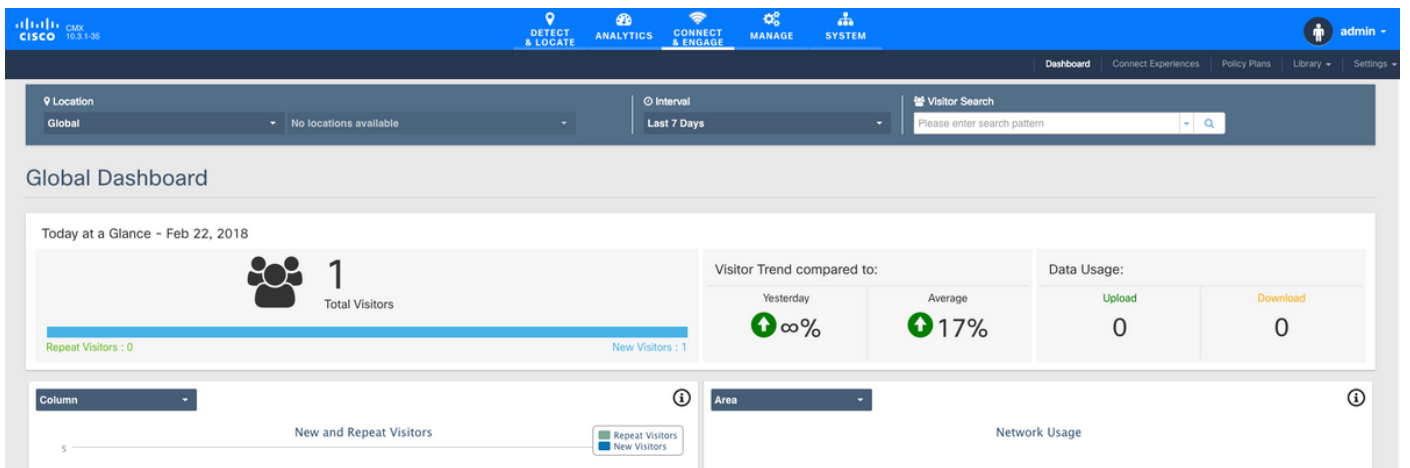


Klik op het MAC-adres van de client en bevestig in de details dat de client Policy Manager-status heeft:



# CMX

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



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

The screenshot shows the Cisco Visitor Search interface. At the top, there is a search bar with the text "Please enter search query" and a "Download as CSV" button. Below the search bar, there is a "Use Search Filter Options" button. The search results are displayed in a table with the following columns: Mac Address, State, First Login Time, Last Login Time, Last Accept Time, Last Logout Time, Location/Site, Portal, Type, Auth Type, Device, Operating System, Bytes Received, Bytes Sent, Social Facebook Name, and Social Facebook Gender. The table shows one result for Mac Address "f4:" with State "active". The background shows a dashboard with various charts and graphs.

Mac Address	State	First Login Time	Last Login Time	Last Accept Time	Last Logout Time	Location/Site	Portal	Type	Auth Type	Device	Operating System	Bytes Received	Bytes Sent	Social Facebook Name	Social Facebook Gender
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	RegistrationPage	CustomPortal	REGISTRATION	PC	Windows 10	0	0	Catarina Silva	female

## 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.