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

Contenu

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.

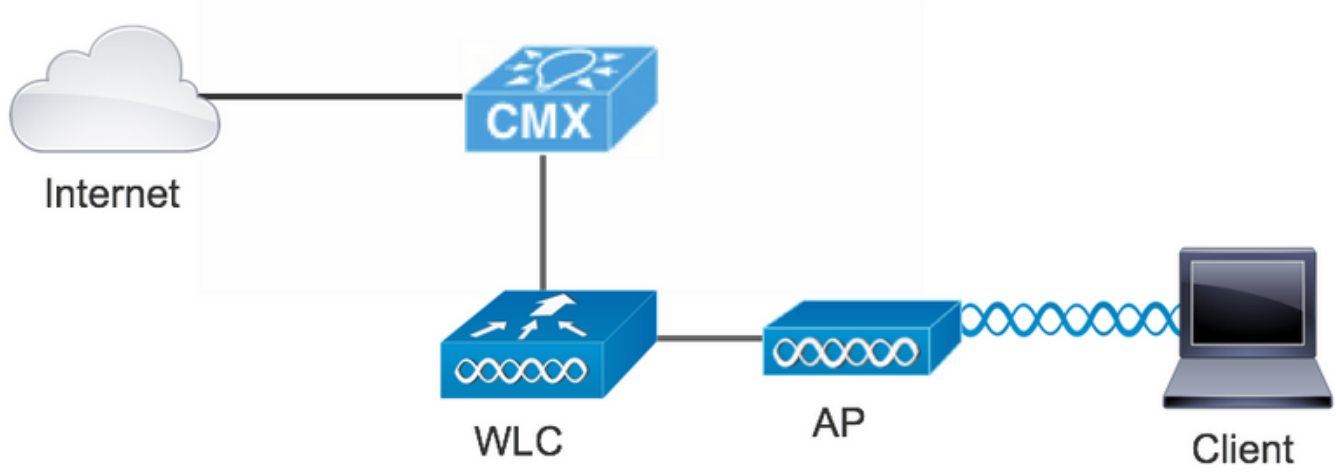
Dans les deux cas, le client tentera de s'enregistrer sur le SSID à l'aide de l'authentification via CMX.

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 Twilio, 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.

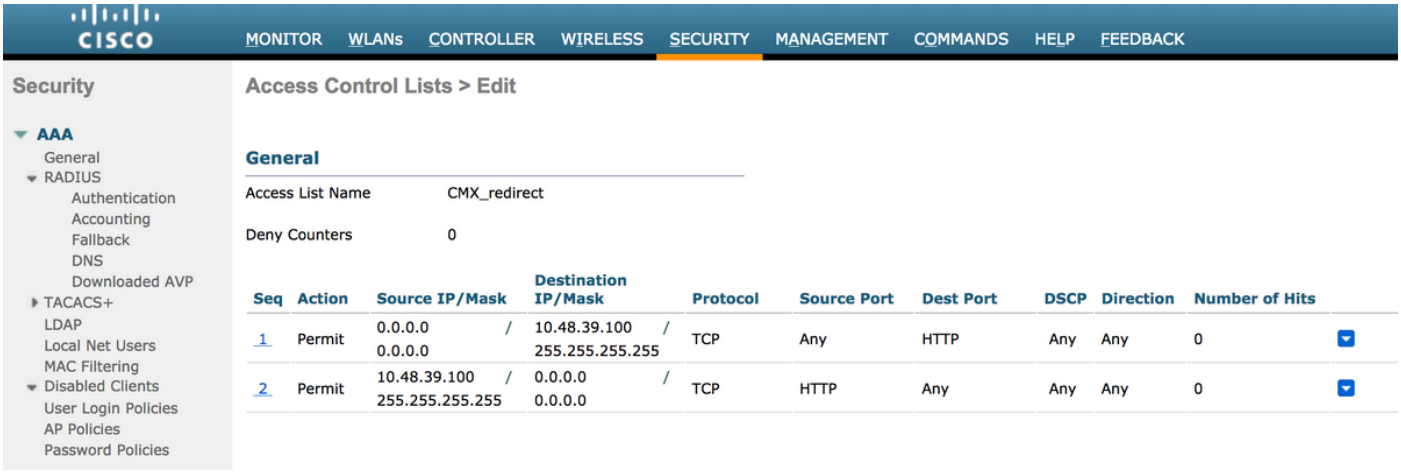
A. Configuration WLC

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.

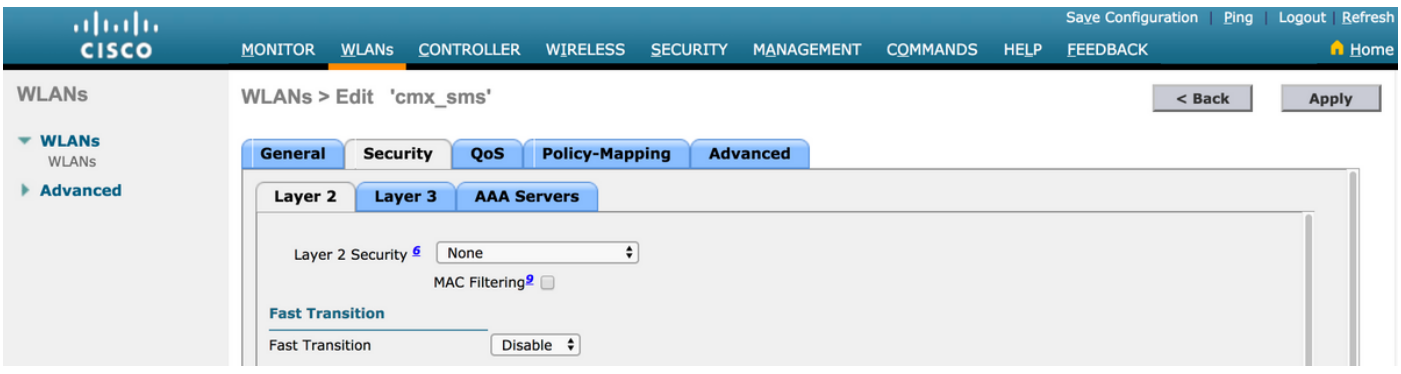
L'adresse IP utilisée est celle configurée pour le CMX. Ceci autorise le trafic HTTP entre le WLC et le CMX. La figure ci-dessous montre la liste de contrôle d'accès créée où « 10.48.39.100 » fait référence à l'adresse IP CMX.

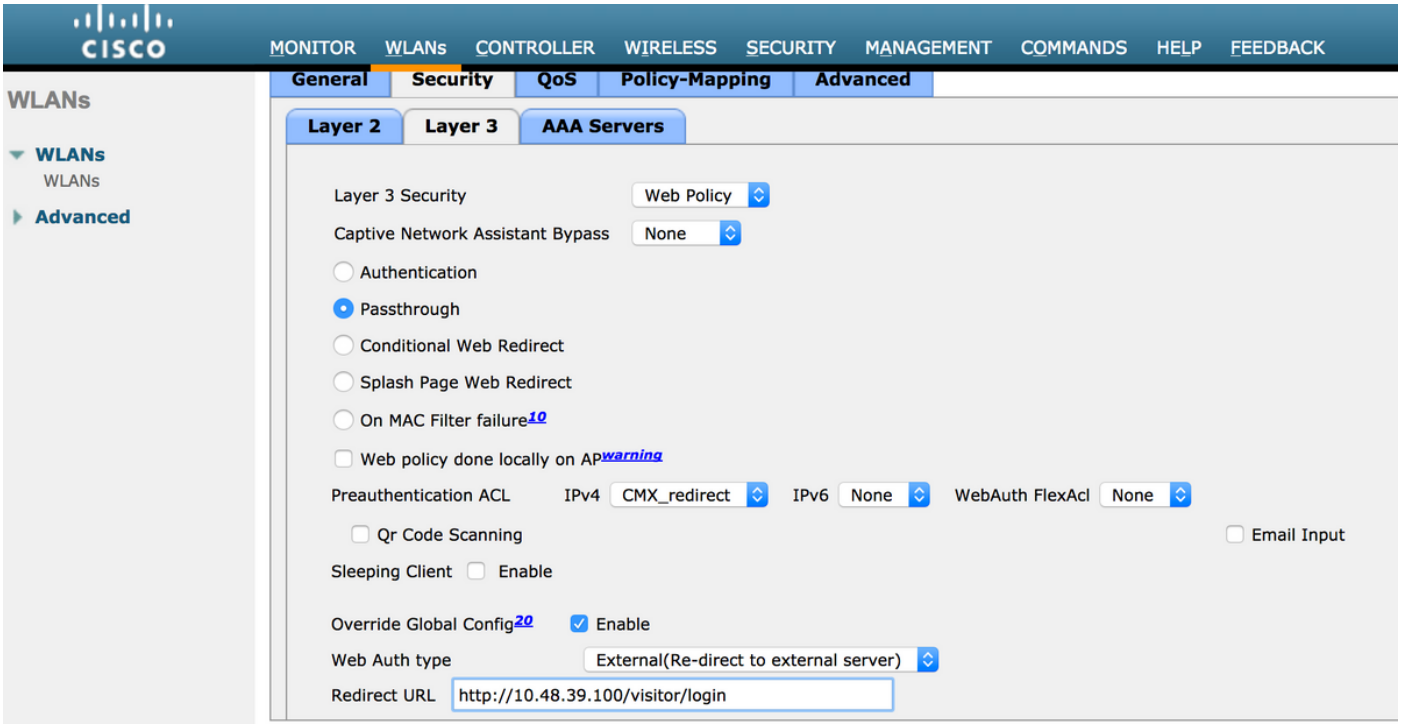


2. WLAN

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 .

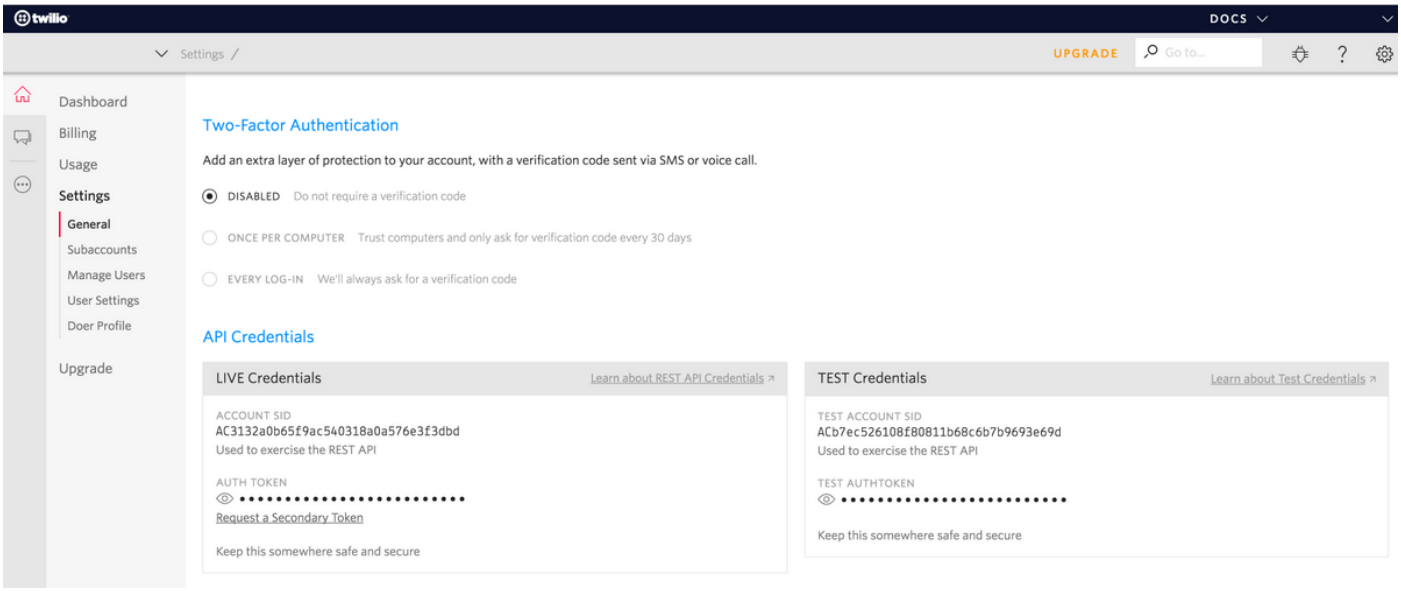




B. Twilio

CMX fournit l'intégration Twilio 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.



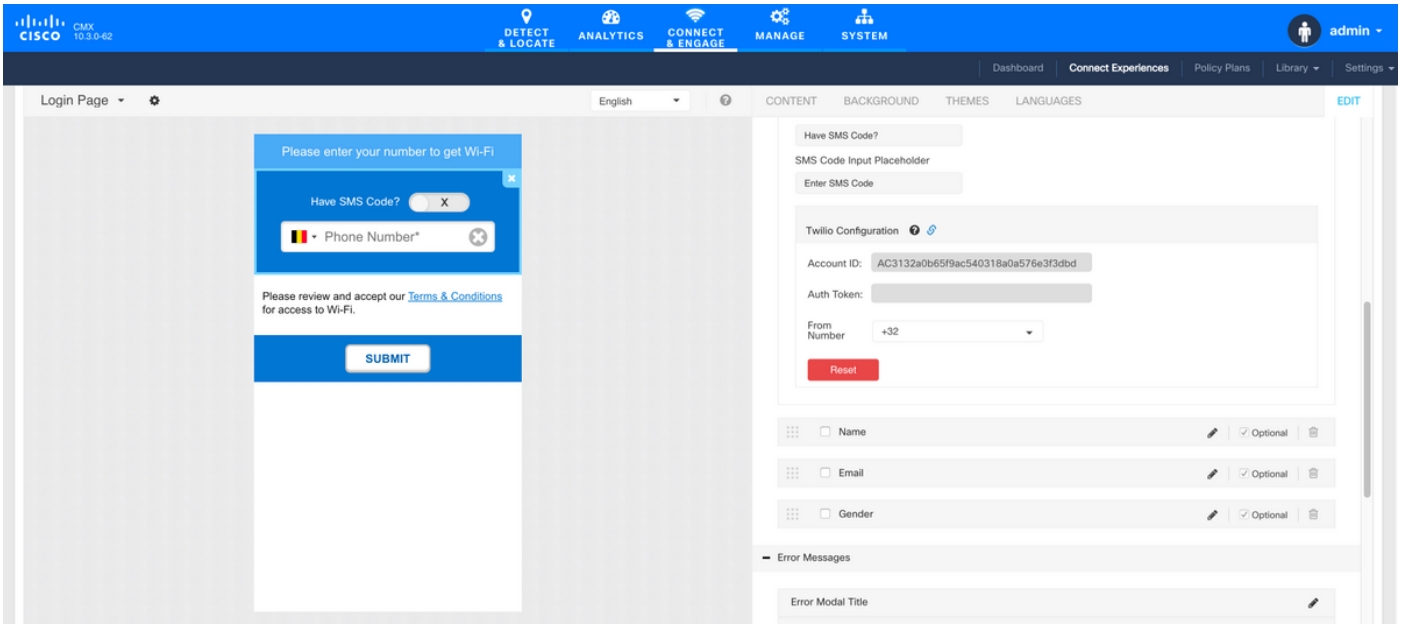
C. Configuration CMX

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.



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.

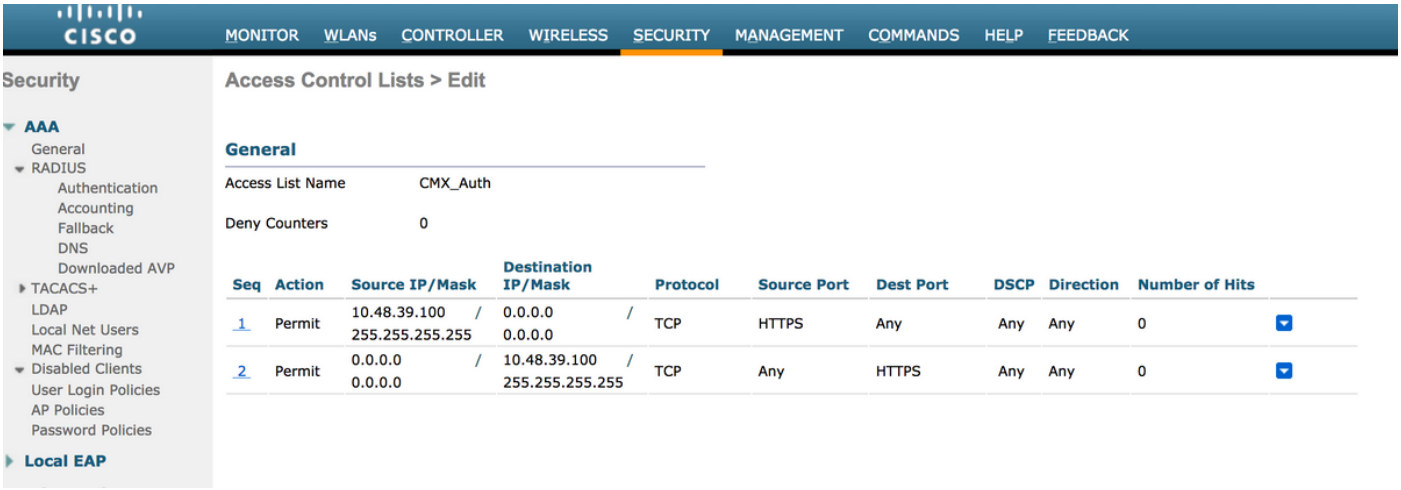
A. Configuration WLC

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

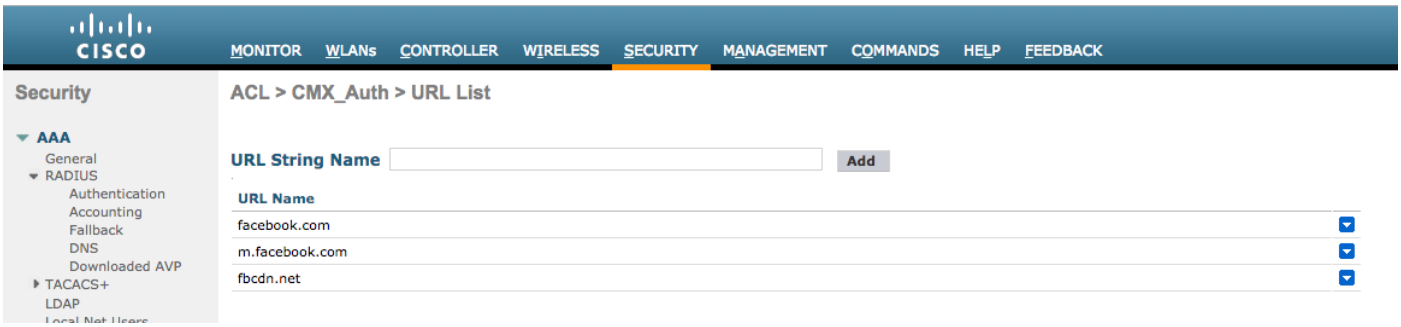
1. ACL

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)



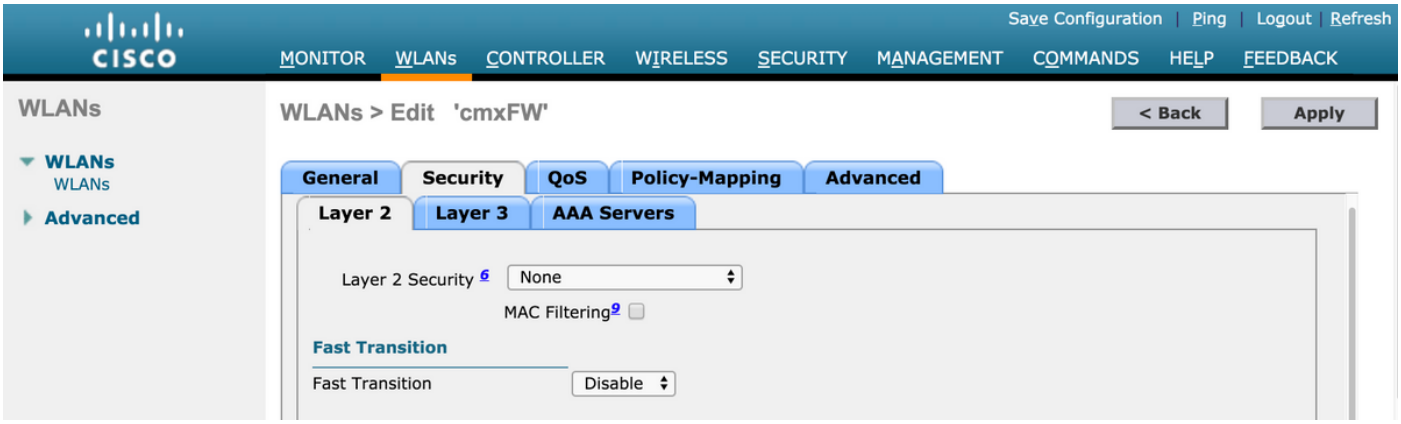
Il est également nécessaire d'avoir une liste de contrôle d'accès DNS avec des URL Facebook. Pour ce faire, dans Security ->Access Control Lists, recherchez l'entrée de la liste de contrôle d'accès précédemment configurée (dans ce cas CMX_Auth) et déplacez la souris vers la flèche bleue à la fin de l'entrée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

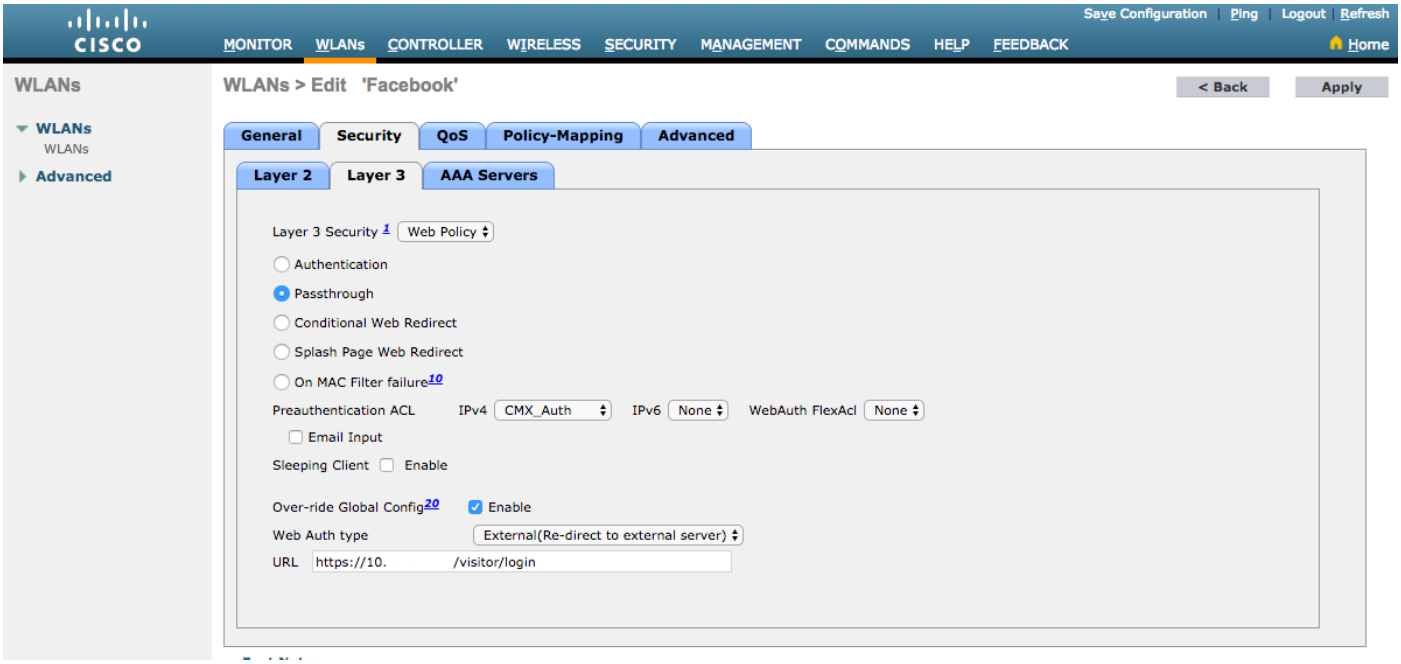


2. WLAN

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.



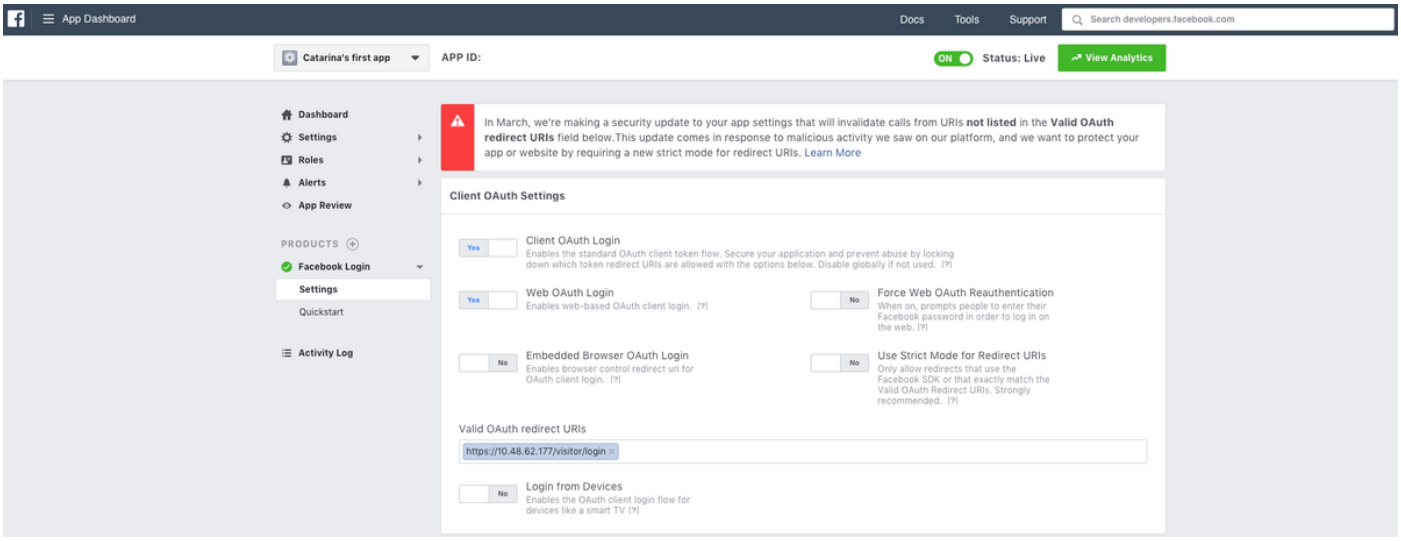


B. Facebook pour les développeurs

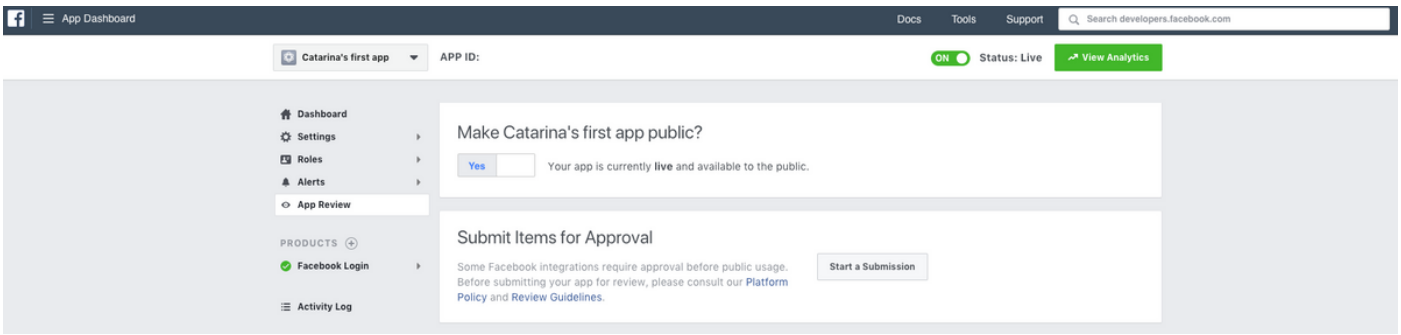
Pour l'intégration de Facebook et CMX, une application Facebook est nécessaire pour que les jetons appropriés soient échangés entre les deux parties.

Accédez à Facebook for Developers 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.



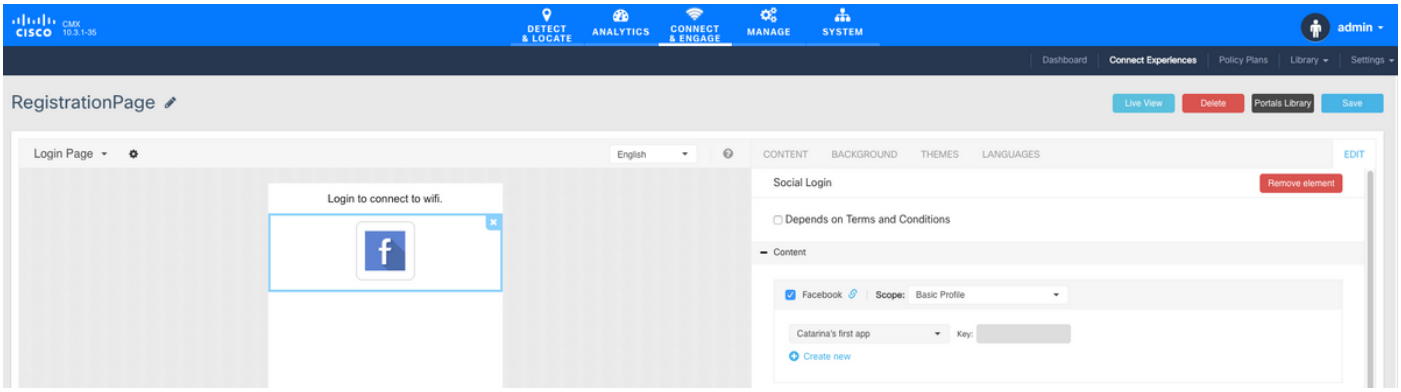
C. Configuration CMX

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.



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

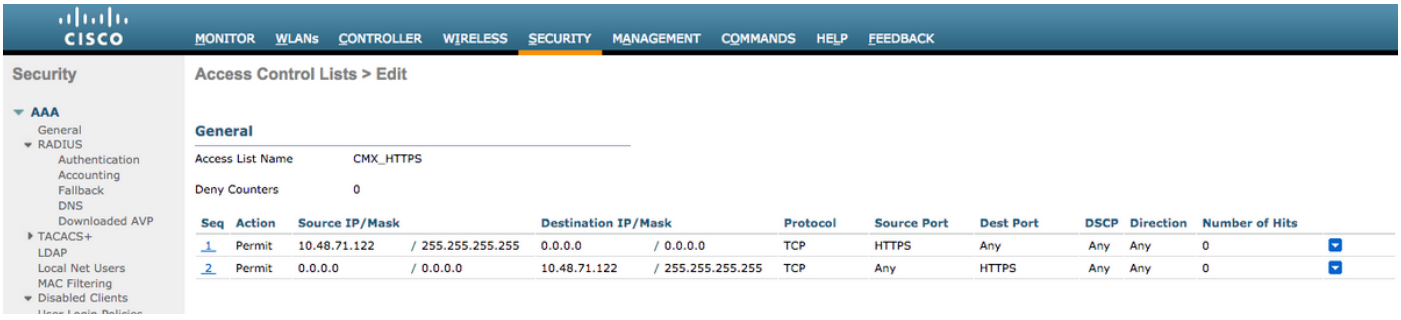
Du côté du WLC, un SSID et une ACL seront configurés. L'AP doit être joint au contrôleur et à l'état RUN.

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.

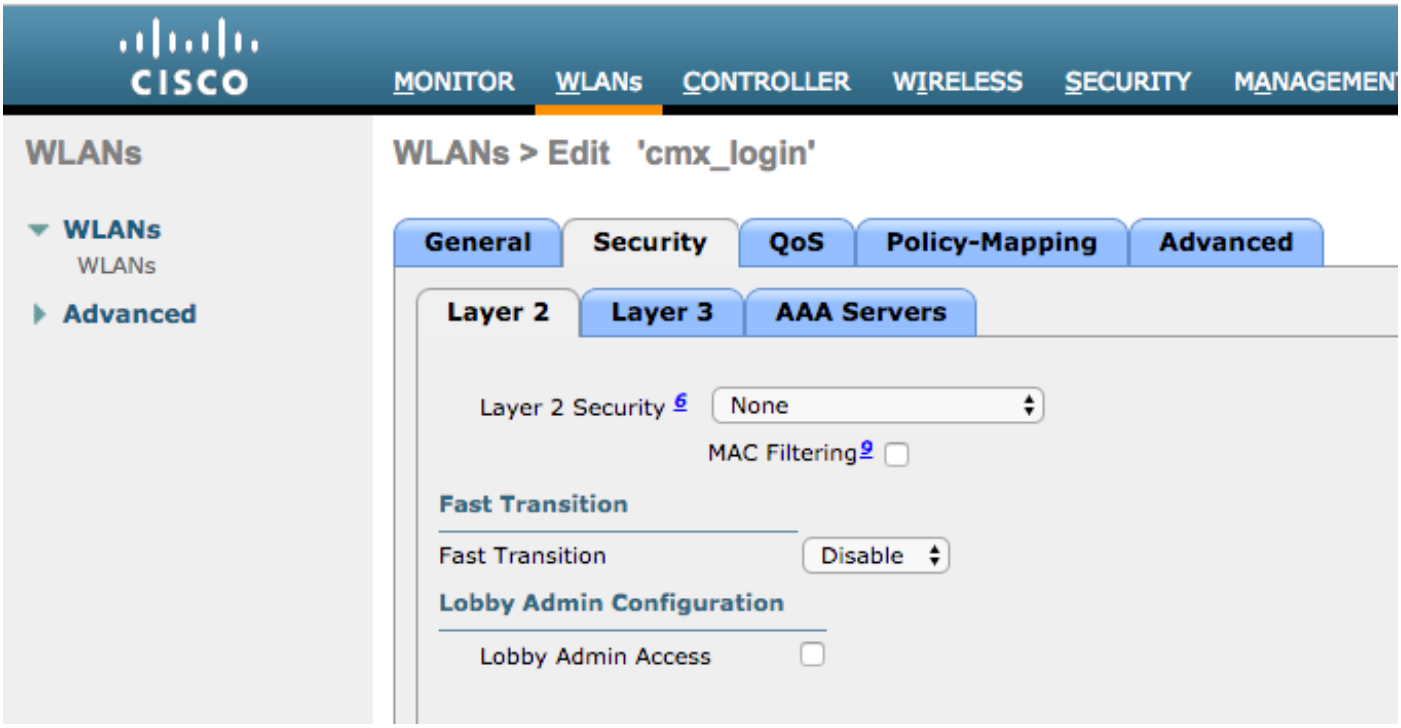


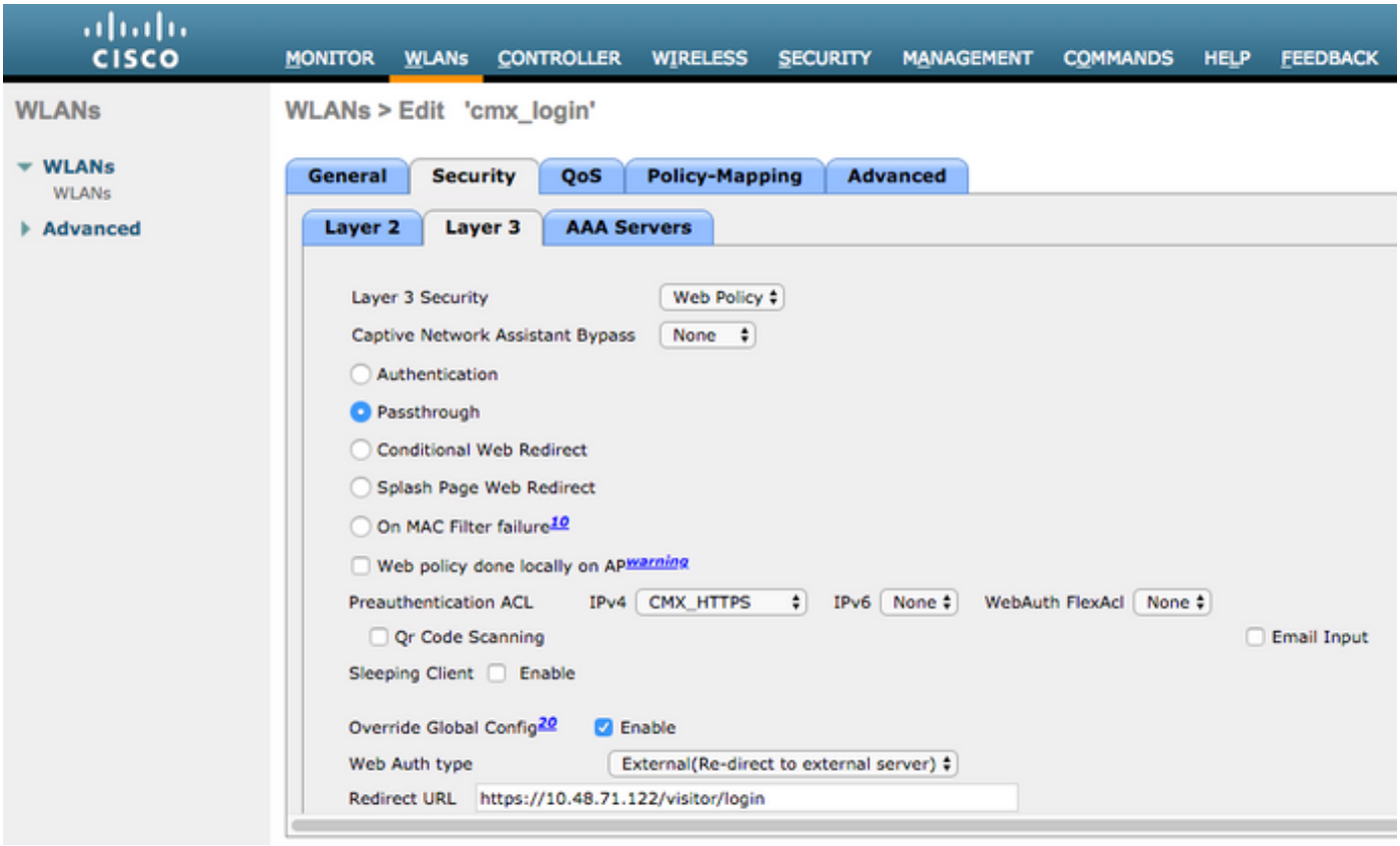
2. WLAN

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.





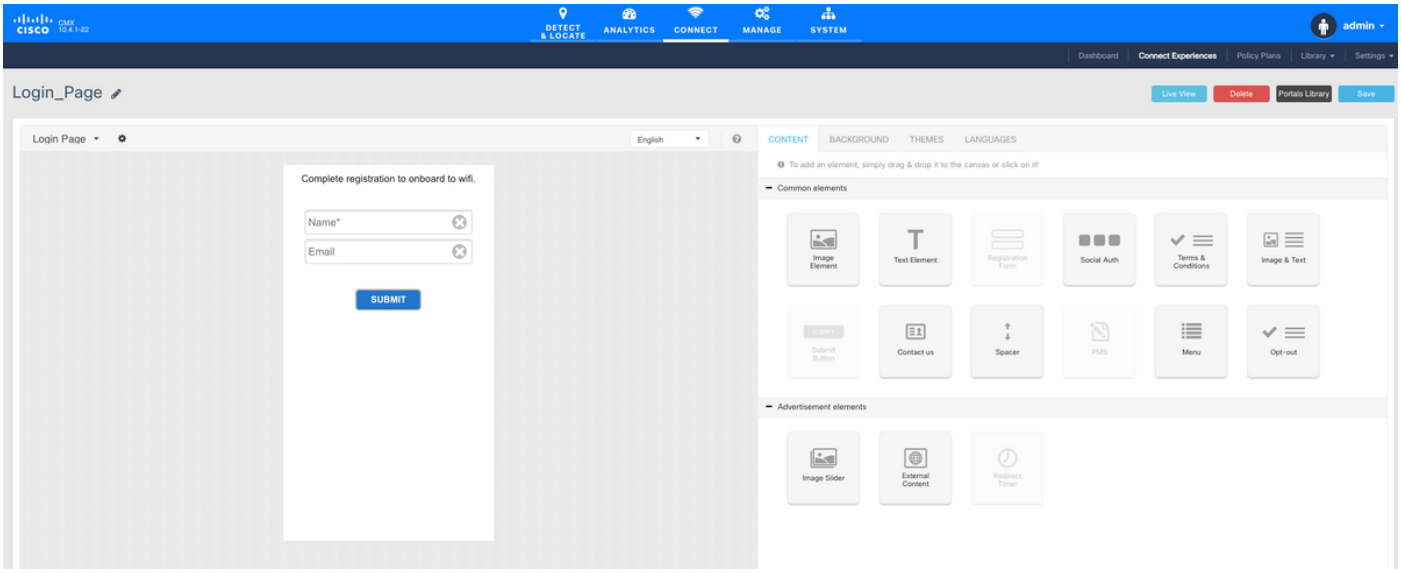
C. Configuration CMX

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.

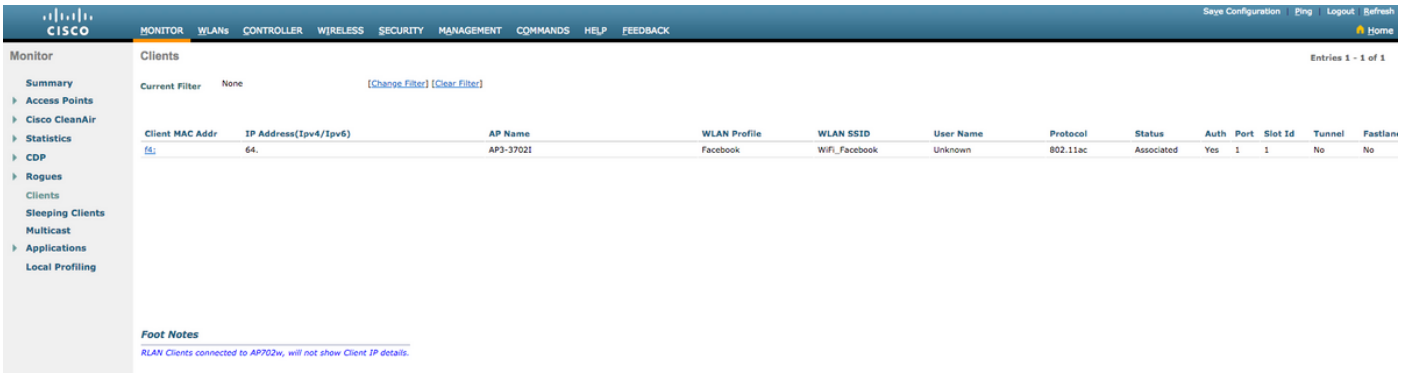
Le portail pour l'enregistrement normal peut être fait à partir de zéro (sélectionnez “ ” personnalisé) ou adapté à partir du modèle “ formulaire d'enregistrement ” disponible dans la bibliothèque CMX.



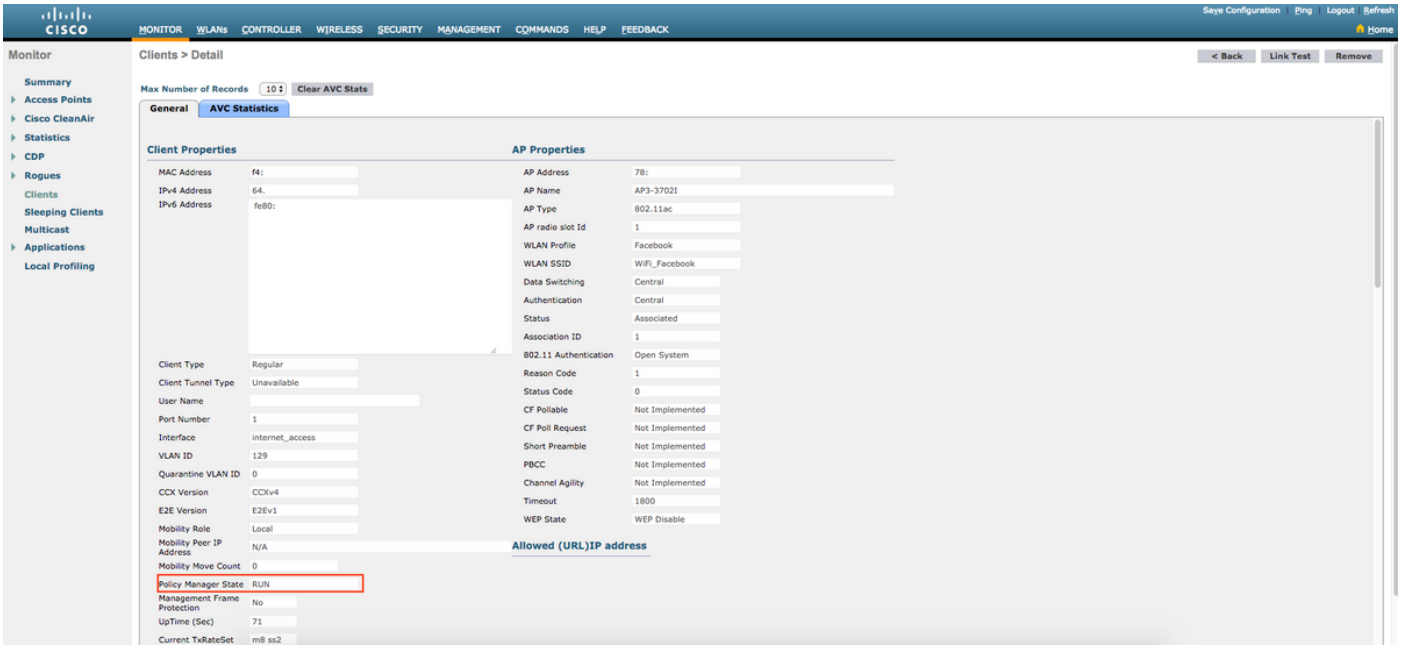
Vérification

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 :

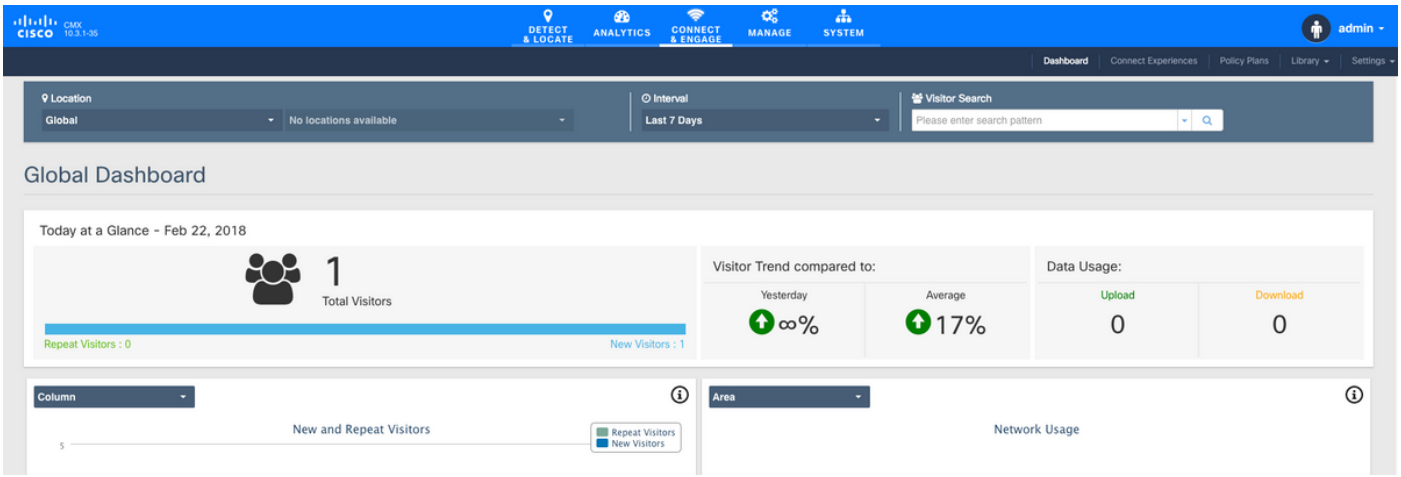


Cliquez sur l'adresse MAC du client et dans les détails, vérifiez que l'état du gestionnaire de stratégies client est en cours d'exécution :

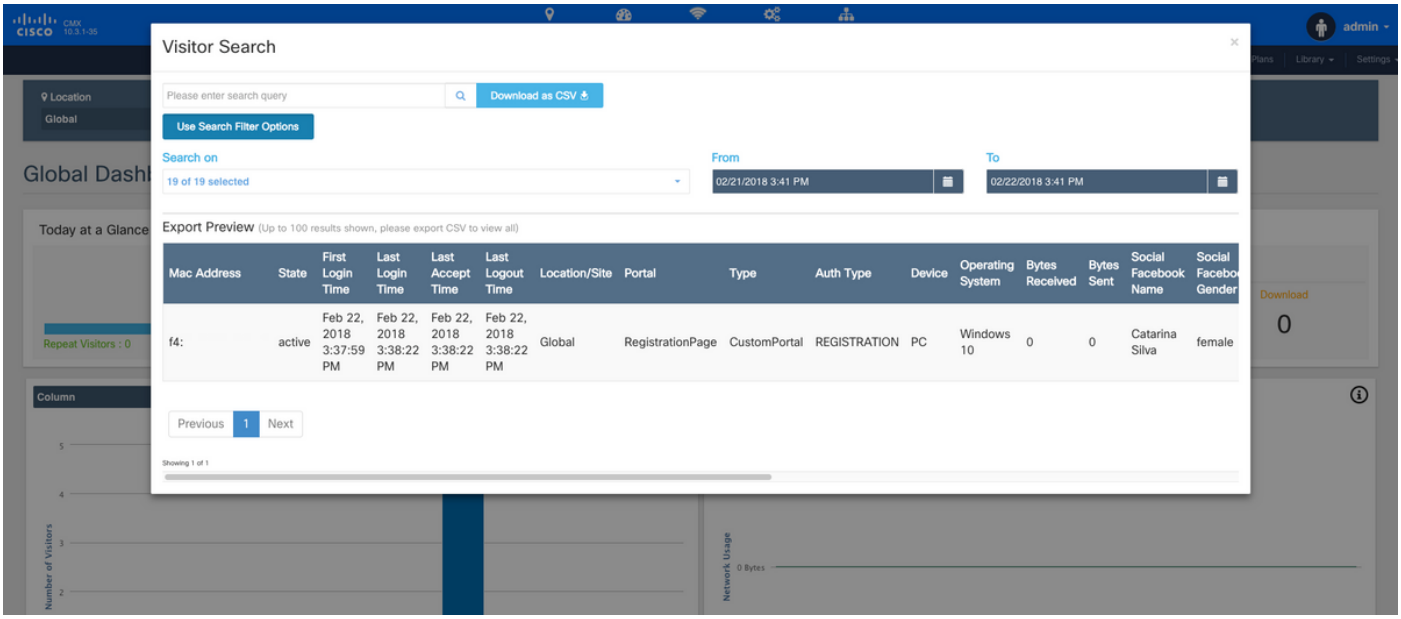


CMX

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



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



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.