CMX Connected Experience - Esempio di configurazione della registrazione di social network, SMS e portali personalizzati

Sommario

Introduzione

Questo documento ha lo scopo di guidare gli amministratori di rete nella registrazione dei client tramite la configurazione dei portali guest su Connected Mobile eXperience (CMX).

CMX consente agli utenti di eseguire la registrazione e l'autenticazione nella rete utilizzando Social Registration Login, SMS e Custom Portal. In questo documento è disponibile una panoramica dei passaggi di configurazione sul controller WLC (Wireless LAN Controller) e su CMX.

Prerequisiti

Requisiti

CMX deve essere configurato correttamente con la configurazione di base.

L'esportazione delle mappe da Prime Infrastructure è opzionale.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Wireless Controller versione 8.2.16.0, 8.5.110.0 e 8.5.135.0.
- Cisco Connected Mobile Experience versione 10.3.0-62, 10.3.1-35. 10.4.1-22.

Configurazione

Esempio di rete

In questo documento vengono descritti due diversi modi per autenticare utenti/client nella rete wireless, utilizzando CMX.

In primo luogo, verrà descritta l'impostazione dell'autenticazione tramite account di social network, quindi l'autenticazione tramite SMS.

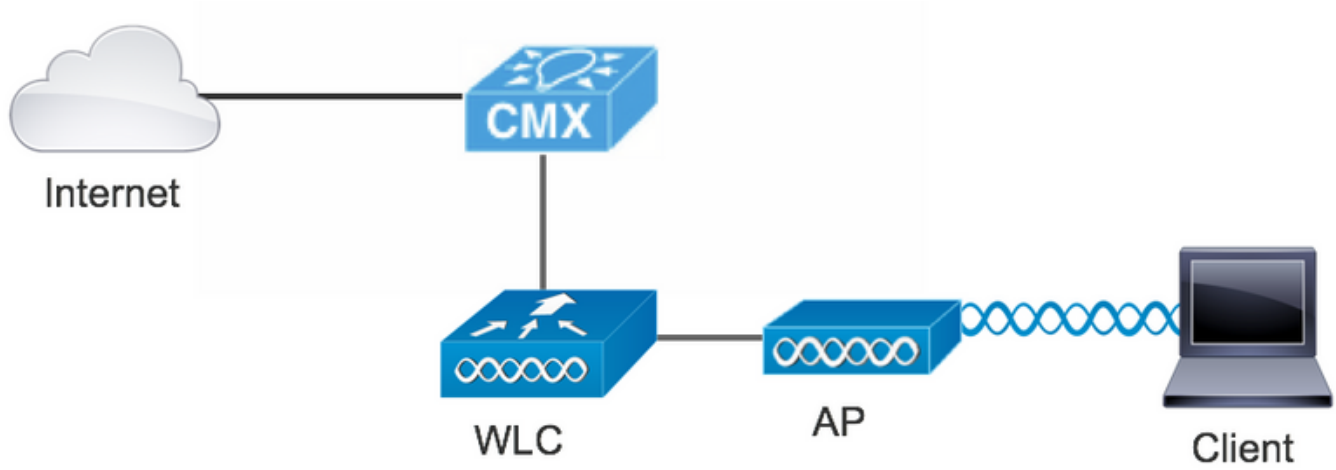
In entrambi gli scenari, il client tenterà di eseguire la registrazione sul SSID utilizzando l'autenticazione tramite CMX.

Il WLC reindirizza il traffico HTTP a CMX, dove all'utente viene richiesto di eseguire l'autenticazione. Il CMX contiene l'impostazione del portale da utilizzare per la registrazione del client, sia tramite account social che tramite SMS.

Di seguito viene descritto il flusso del processo di registrazione:

1. Il client tenta di unirsi all'SSID e apre il browser.
2. Anziché accedere al sito richiesto, viene reindirizzato al portale guest dal WLC.
3. Il client fornisce le credenziali e tenta di eseguire l'autenticazione.
4. CMX si occupa del processo di autenticazione.
5. Se l'operazione ha esito positivo, al client verrà fornito l'accesso completo a Internet.
6. Il client viene reindirizzato al sito richiesto iniziale.

La topologia utilizzata è:



Configurazioni

Autenticazione tramite SMS

Cisco CMX consente l'autenticazione del client tramite SMS. Questo metodo richiede l'impostazione di una pagina HTML in modo che l'utente possa fornire le proprie credenziali al sistema.I modelli predefiniti sono forniti da CMX in modo nativo e possono essere successivamente modificati o sostituiti da un modello personalizzato.

Il servizio SMS viene fornito integrando CMX con Twilio, una piattaforma di comunicazioni cloud

che consente di inviare e ricevere messaggi di testo. Twilio consente di avere un numero di telefono per portale, il che significa che se si utilizza più di un portale, è necessario un numero di telefono per portale.

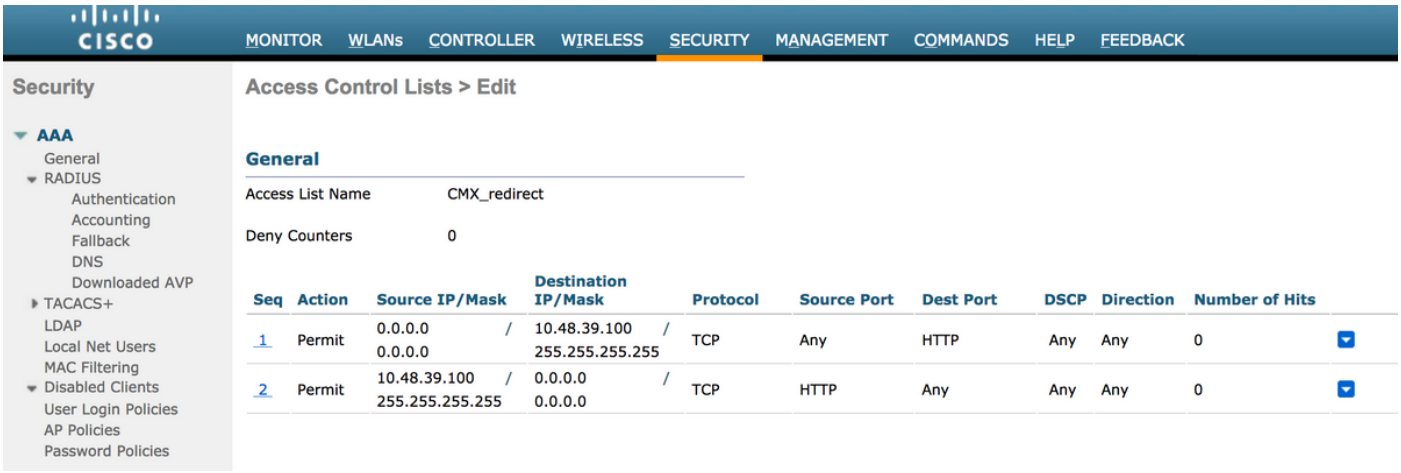
R. Configurazione WLC

Sul lato WLC, verranno configurati sia un SSID che un ACL. L'access point deve essere unito al controller e in stato RUN.

1. ACL

Ènecessario un ACL che consenta il traffico HTTP, configurato sul WLC. Per configurare un ACL, selezionare Protezione->Access Control Lists->Aggiungi nuova regola.

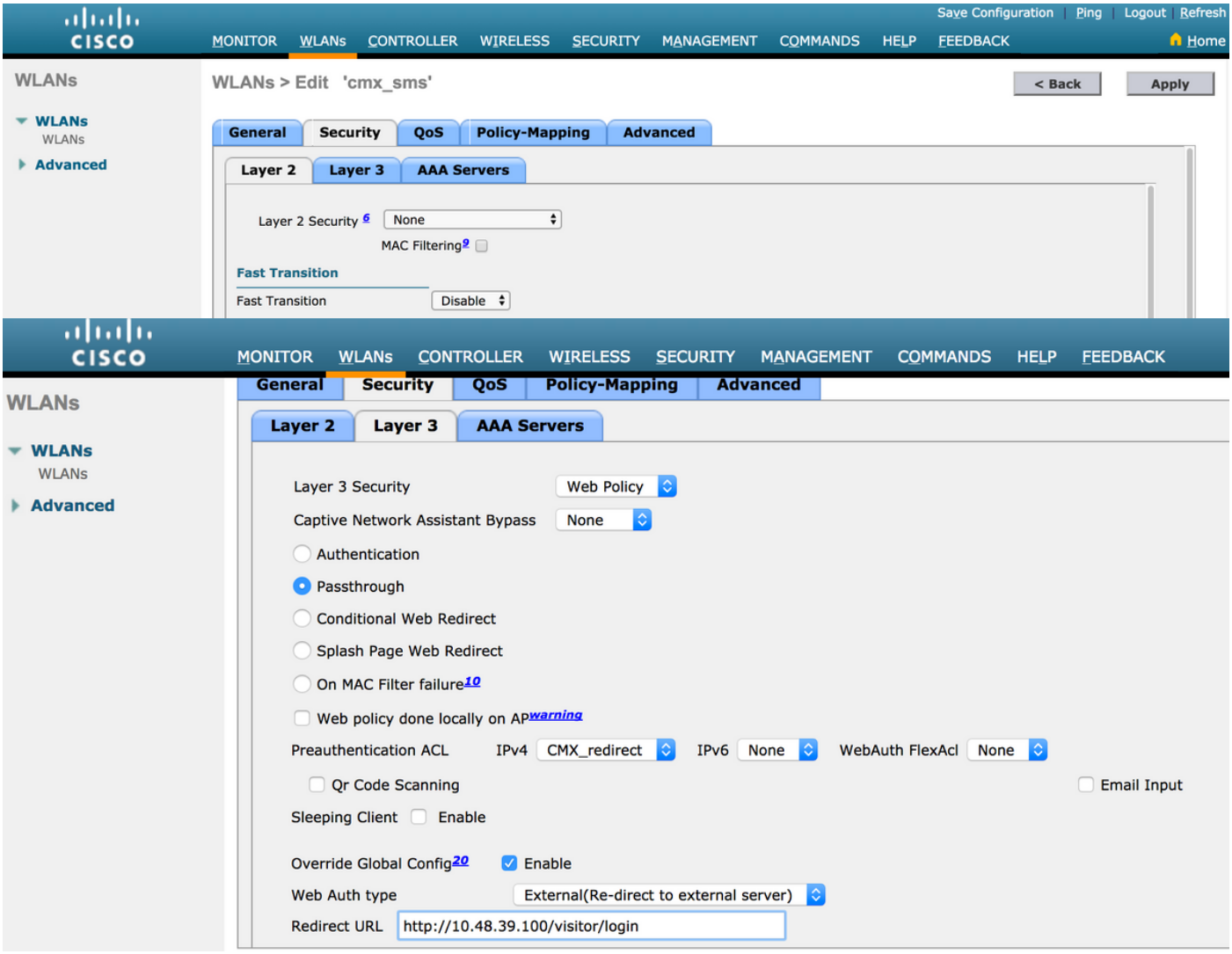
L'indirizzo IP utilizzato è quello configurato per il CMX. Questo consente il traffico HTTP tra il WLC e il CMX. La figura seguente mostra l'ACL creato dove "10.48.39.100" si riferisce all'indirizzo IP CMX.



2. WLAN

In questo modo l'integrazione con il portale è completa, è necessario apportare modifiche alle policy di sicurezza sulla WLAN.

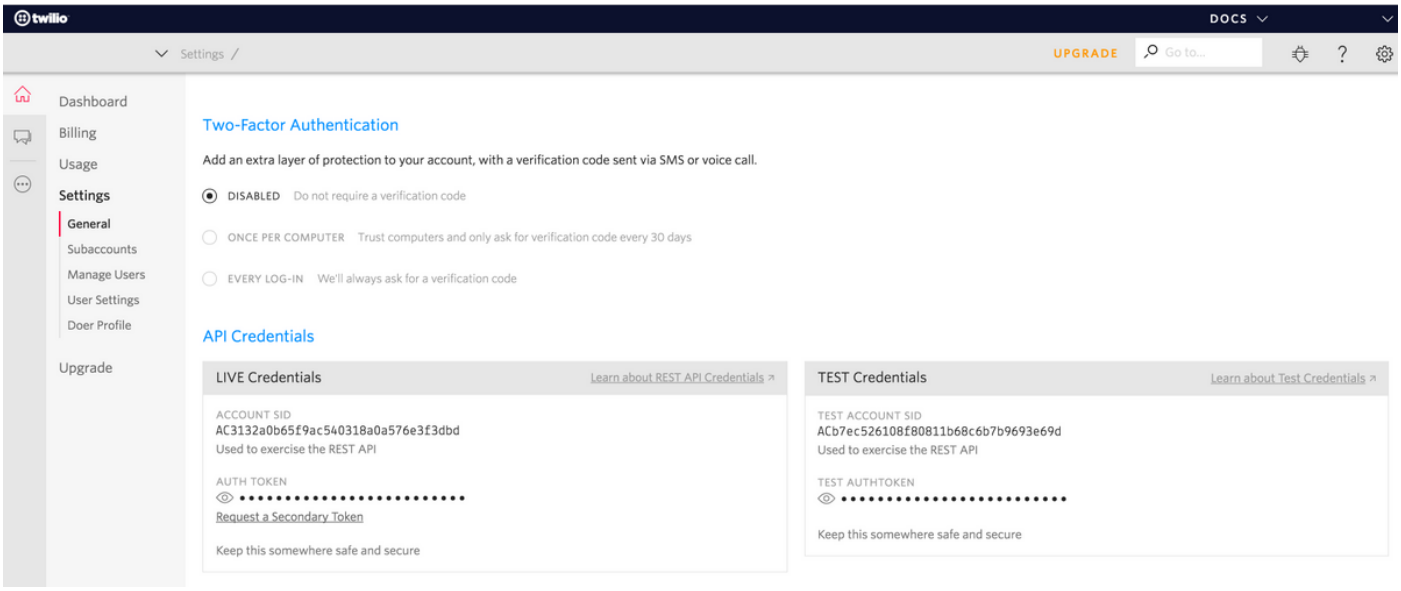
Per prima cosa, accedere alle WLAN->Edit->Layer 2->Layer 2 Security (Sicurezza di livello 2), quindi selezionare None (Nessuno) nell'elenco a discesa, in modo che la sicurezza di livello 2 sia disabilitata. Quindi, nella stessa scheda Protezione, passare al layer 3. Nel menu a discesa Protezione di layer 3, selezionare Criterio Web, quindi Passthrough. In ACL di preautenticazione, selezionare l'ACL IPv4 configurato in precedenza, per associarlo alla rispettiva WLAN in cui deve essere fornita l'autenticazione SMS. È necessario abilitare l'opzione Ignora configurazione globale e il tipo di autenticazione Web deve essere Esterna (reindirizzamento su server esterno), in modo che i client possano essere reindirizzati al servizio CMX. L'URL deve essere lo stesso del portale di autenticazione SMS CMX, nel formato http://<CMX-IP>/visitor/login.



B. Twilio

CMX fornisce integrazione Twilio per i servizi SMS. Le credenziali vengono fornite dopo la corretta configurazione dell'account su Twilio. Sono necessari sia il SID ACCOUNT che il TOKEN AUTH.

Twilio ha i propri requisiti di configurazione, documentati attraverso il processo di configurazione del servizio. Prima dell'integrazione con CMX, è possibile testare il servizio Twilio, il che significa che i problemi relativi all'installazione di Twilio possono essere rilevati prima di utilizzarlo con CMX.



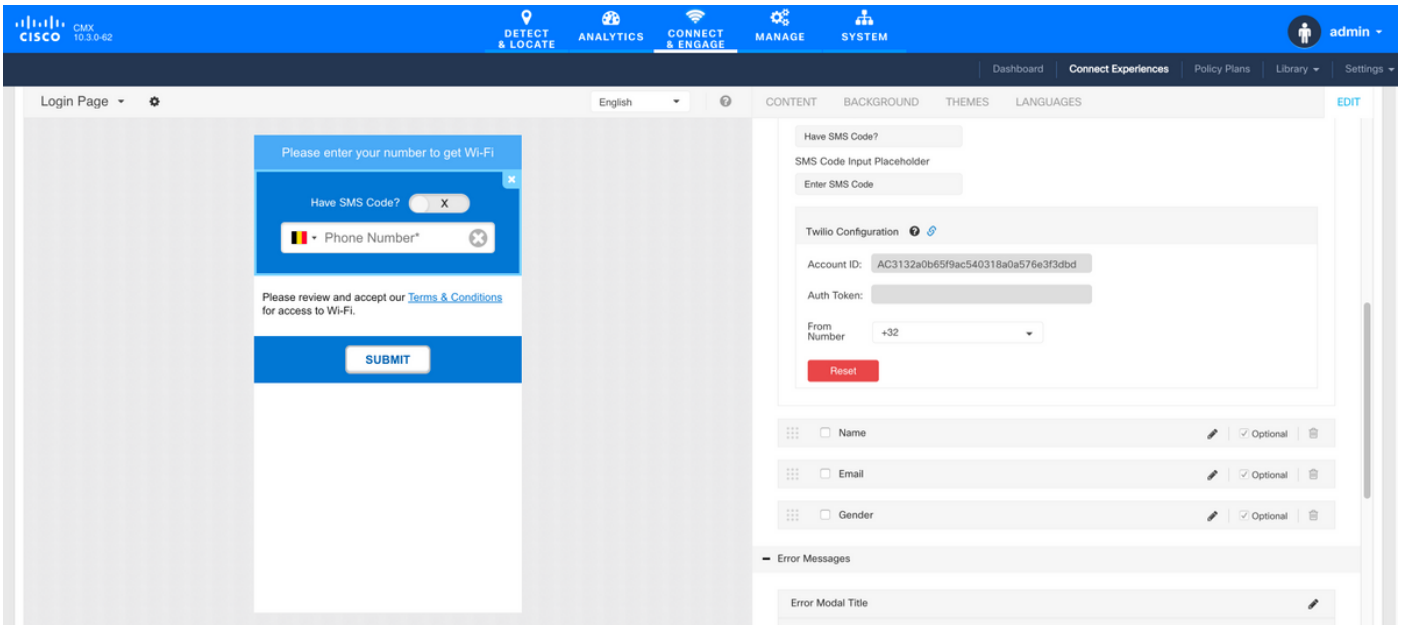
C. Configurazione CMX

Ènecessario che il controller venga aggiunto correttamente al CMX e che le mappe vengano esportate da Prime Infrastructure.

- Pagina di registrazione SMS

Èdisponibile un modello predefinito per il portale di registrazione. I portali possono essere trovati selezionando CONNECT&ENGAGE->Library. Se si desidera un modello, scegliere Modelli dal menu a discesa.

Per integrare Twilio con il portale, andare a Configurazione Twilio e fornire l'ID account e il token Auth. Se l'integrazione ha esito positivo, il numero utilizzato nell'account Twilio verrà visualizzato.



Autenticazione tramite account di social network

L'autenticazione del client tramite account di social network richiede all'amministratore di rete di aggiungere un identificatore APP Facebook valido nel CMX.

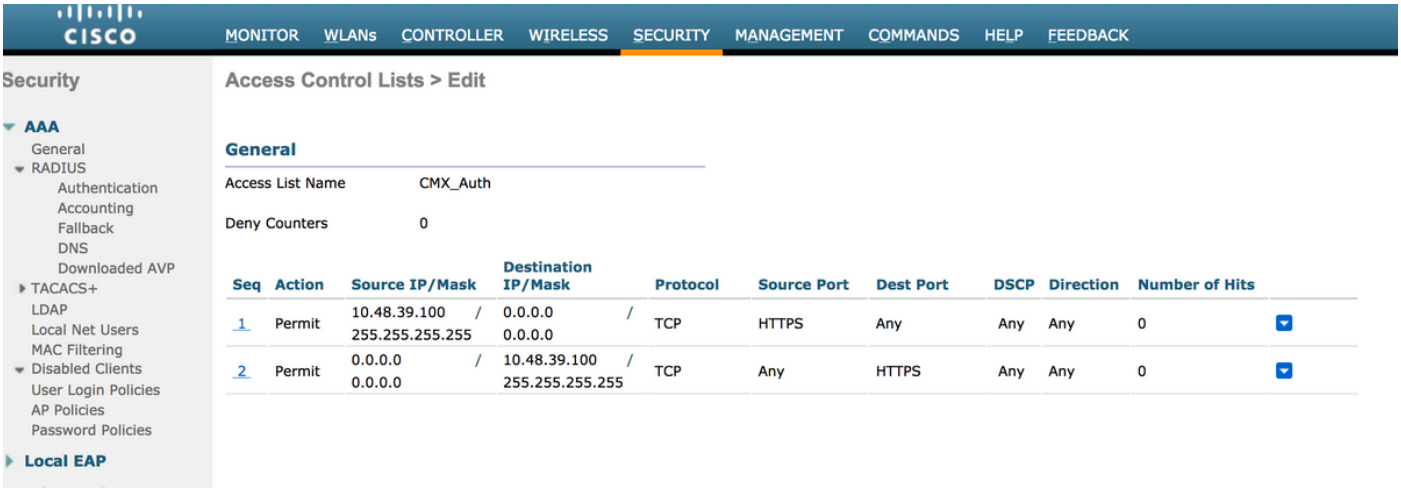
A. Configurazione WLC

Sul lato WLC, verranno configurati sia un SSID che un ACL. L'access point deve essere collegato al controller e in stato RUN.

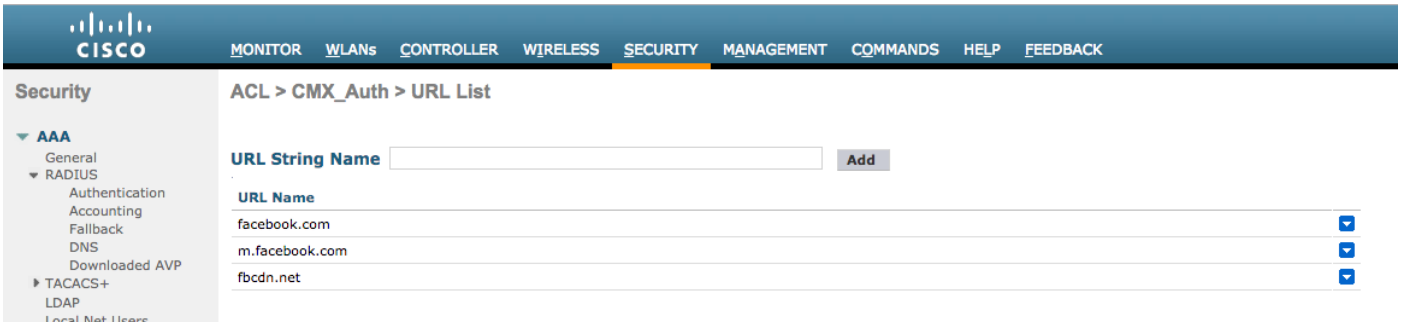
1. ACL

In questo caso si utilizza HTTPS come metodo di autenticazione, è necessario configurare un ACL che consenta il traffico HTTPS sul WLC. Per configurare un ACL, selezionare Protezione->Access Control Lists->Aggiungi nuova regola.

L'IP CMX deve essere utilizzato per consentire il traffico HTTPS tra il WLC e il CMX. (nell'esempio, l'IP CMX è 10.48.39.100)



Èanche necessario avere un ACL DNS con URL di Facebook. A tale scopo, in Protezione ->Access Control Lists individuare la voce dell'ACL precedentemente configurato (in questo caso CMX_Auth) e spostare il mouse sulla freccia blu alla fine della voce e selezionare Add-Remove URL (Aggiungi/Rimuovi URL). Quindi digitare gli URL di Facebook in Nome stringa URL e Aggiungi.

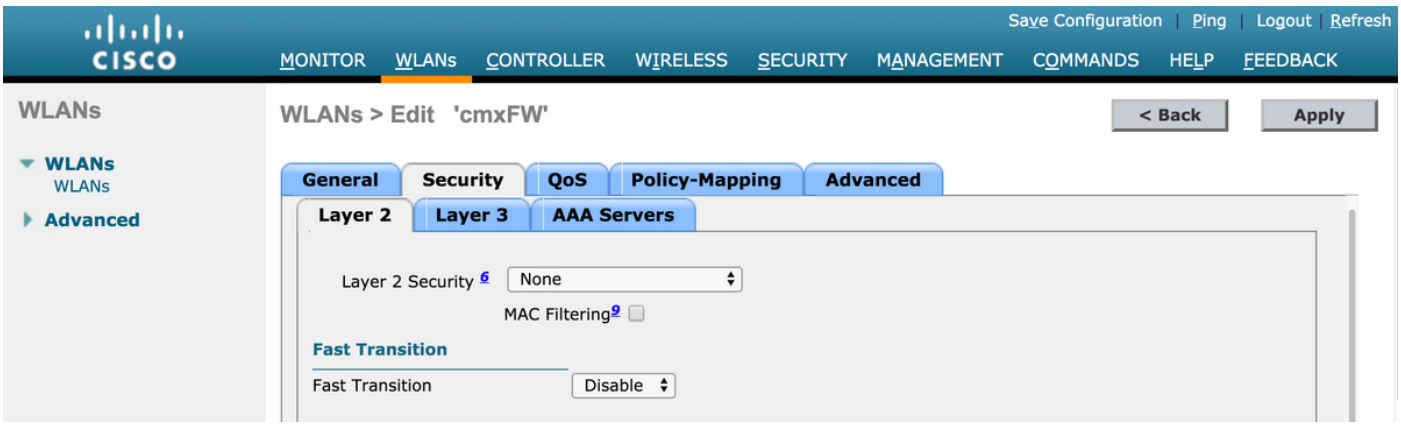


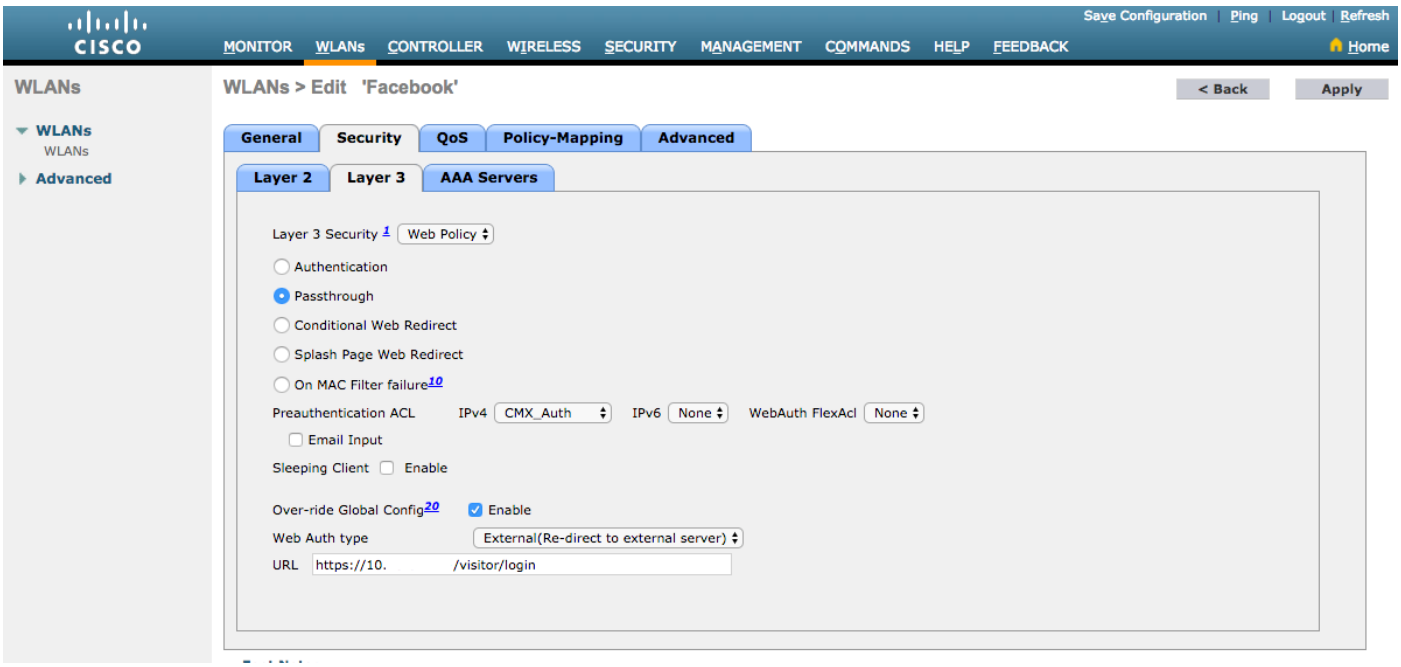
2. WLAN

Le modifiche apportate ai criteri di sicurezza per consentire la registrazione richiedono una configurazione specifica sulla WLAN.

Come già fatto per la registrazione SMS, prima di tutto è arrivato alle WLAN->Edit->Layer 2->Layer 2 Security, e nell'elenco a discesa scegliere None (Nessuno), quindi la sicurezza Layer 2 è disabilitata. Nella stessa scheda Protezione, passare al layer 3. Nel menu a discesa Protezione di layer 3, selezionare Criteri Web, quindi Passthrough. In ACL di preautenticazione, selezionare l'ACL IPv4 configurato in precedenza, per associarlo alla rispettiva WLAN su cui deve essere

fornita l'autenticazione tramite Facebook. È necessario abilitare l'opzione Ignora configurazione globale e il tipo di autenticazione Web deve essere Esterna (reindirizzamento su server esterno), in modo che i client possano essere reindirizzati al servizio CMX. Notare che questa volta, l'URL, deve essere nel seguente formato **https**://<CMX-IP>/visitor/login.



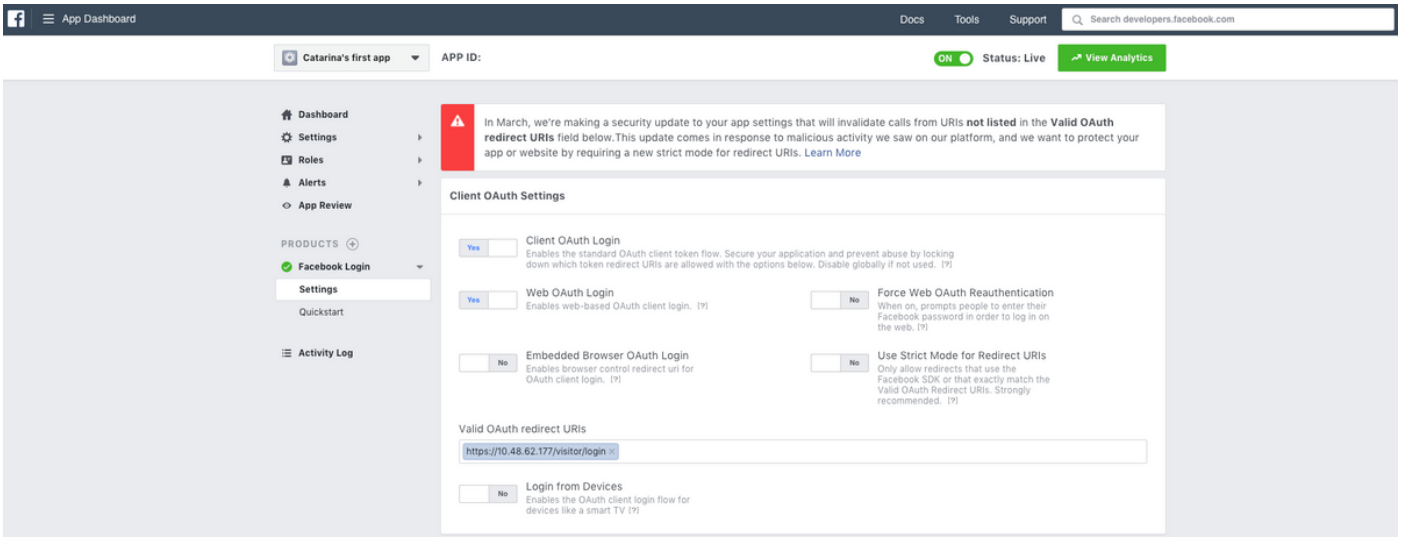


B. Facebook per gli sviluppatori

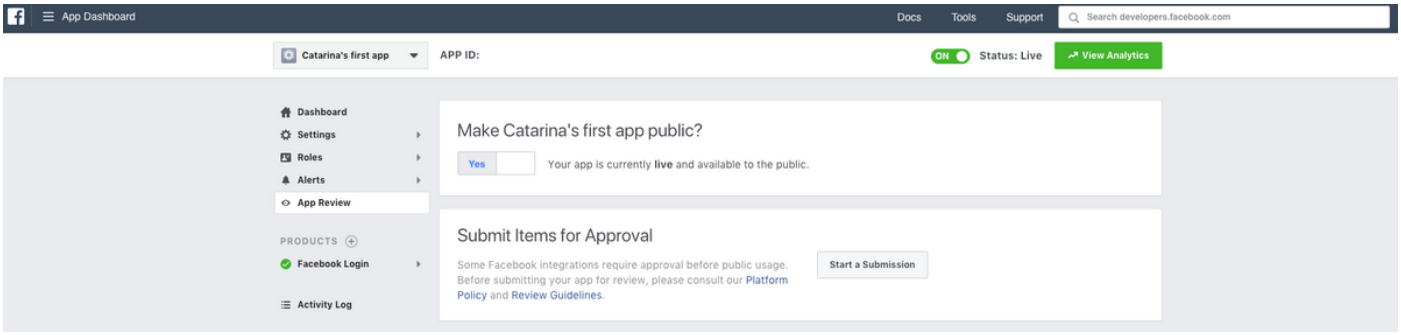
Per l'integrazione di Facebook e CMX, è necessaria un'app di Facebook per poter scambiare i token corretti tra le due parti.

Vai a Facebook per gli sviluppatori per creare l'App. Per integrare i servizi sono previsti alcuni requisiti di configurazione dell'app.

Nelle impostazioni dell'app verificare che le opzioni Accesso OAuth client e Accesso OAuth Web siano abilitate. Verificare inoltre che gli URI di reindirizzamento OAuth validi dispongano dell'URL CMX nel formato **https**://<CMX-IP>/visitor/login.



Per pubblicare l'app e renderla pronta per l'integrazione con CMX, è necessario renderla pubblica. A tale scopo, passare a Revisione app->Rendi <App-Name> pubblico? e impostare lo stato su Sì.



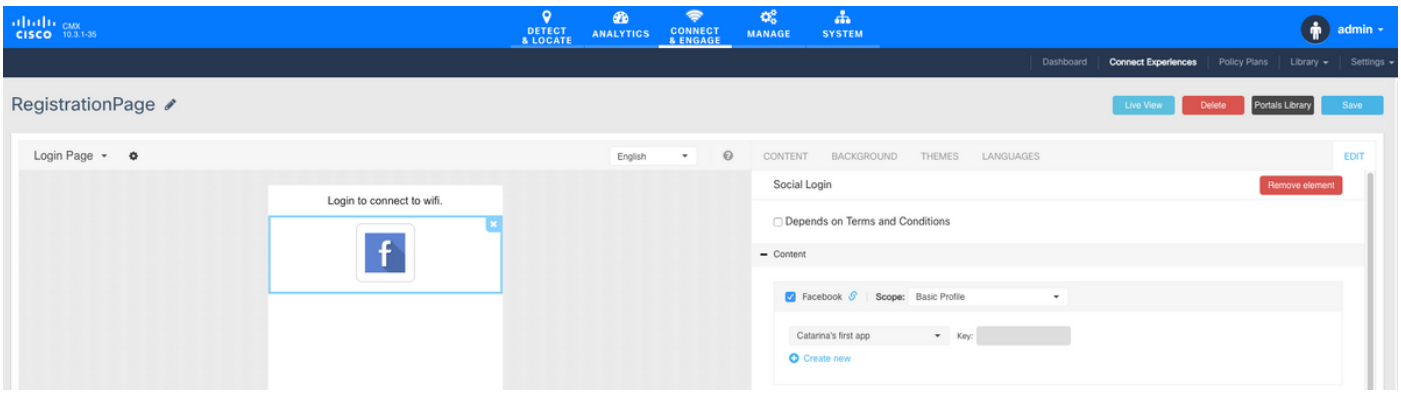
C. Configurazione CMX

Ènecessario che il controller venga aggiunto correttamente al CMX e che le mappe vengano esportate da Prime Infrastructure.

- Pagina di registrazione

Per creare una pagina di registrazione su CMX, è necessario seguire la stessa procedura utilizzata in precedenza per creare la pagina di registrazione SMS. Selezionando CONNECT&ENGAGE->Library (Libreria), è possibile trovare portali modello pronti per la modifica scegliendo Modelli dal menu a discesa.

Per la registrazione tramite le credenziali di Facebook è necessario che il portale disponga della connessione Account social. Per farlo da zero, quando si crea un portale personalizzato, arrivare a CONTENT->Common Elements->Social Auth, e selezionare Facebook. Quindi inserisci il Nome app e l'ID app (Chiave) ottenuti da Facebook.



Autenticazione tramite portale personalizzato

L'autenticazione del client tramite il portale personalizzato è simile alla configurazione dell'autenticazione Web esterna. Il reindirizzamento verrà eseguito sul portale personalizzato ospitato in CMX.

A. Configurazione WLC

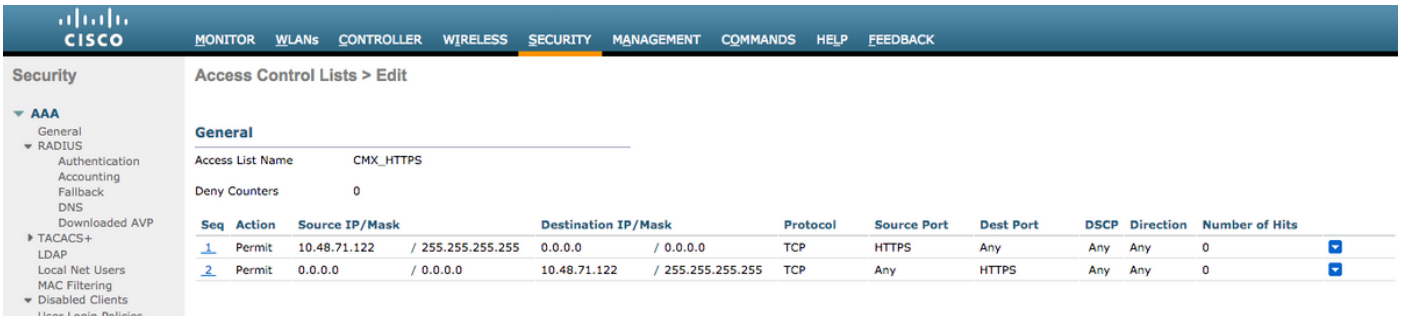
Sul lato WLC, verranno configurati sia un SSID che un ACL. L'access point deve essere collegato al controller e in stato RUN.

1. ACL

In questo caso si utilizza HTTPS come metodo di autenticazione, è necessario configurare un ACL che consenta il traffico HTTPS sul WLC. Per configurare un ACL, passare a Protezione->Access Control Lists->Aggiungi nuova regola.

L'IP CMX deve essere utilizzato per consentire il traffico HTTPS tra il WLC e il CMX. (nell'esempio, l'IP CMX è 10.48.71.122).

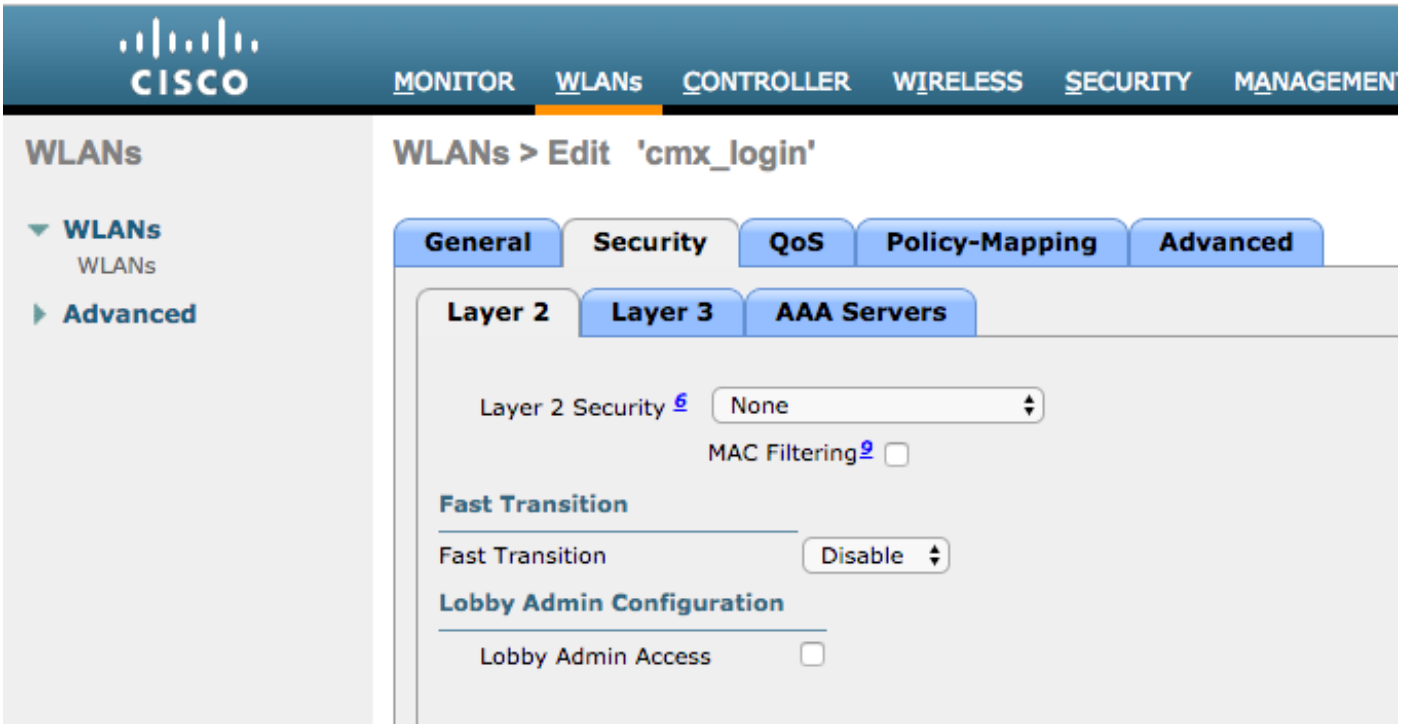
Nota: abilitare ssl sul CMX usando il comando "cmxctl node sslmode enable" sul CLI CMX.

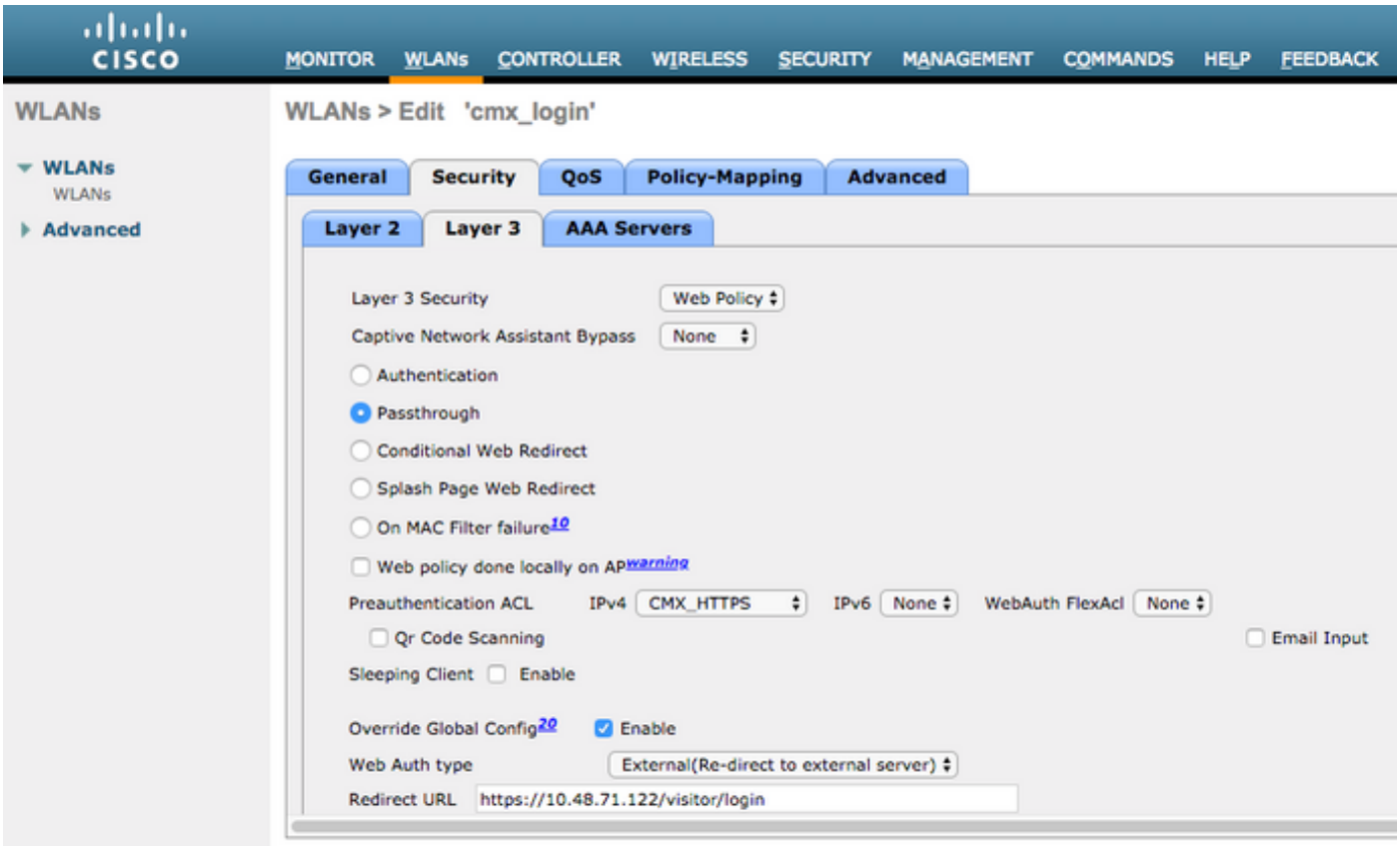


2. WLAN

Le modifiche apportate ai criteri di sicurezza per consentire la registrazione richiedono una configurazione specifica sulla WLAN.

Come già fatto per la registrazione di SMS e social network, in primo luogo è stato raggiunto WLAN->Edit->Layer 2->Layer 2 Security, e nell'elenco a discesa scegliere Nessuno, quindi la sicurezza Layer 2 è disabilitata. Nella stessa scheda Protezione, passare al layer 3. Nel menu a discesa Protezione di layer 3, selezionare Criteri Web, quindi Passthrough. In ACL di preautenticazione, selezionare l'ACL IPv4 configurato in precedenza (nell'esempio, denominato CMX_HTTPS) e associarlo alla rispettiva WLAN. È necessario abilitare l'opzione Ignora configurazione globale e il tipo di autenticazione Web deve essere Esterna (reindirizzamento su server esterno), in modo che i client possano essere reindirizzati al servizio CMX. Notare che questa volta, l'URL, deve essere nel seguente formato **https**://<CMX-IP>/visitor/login.





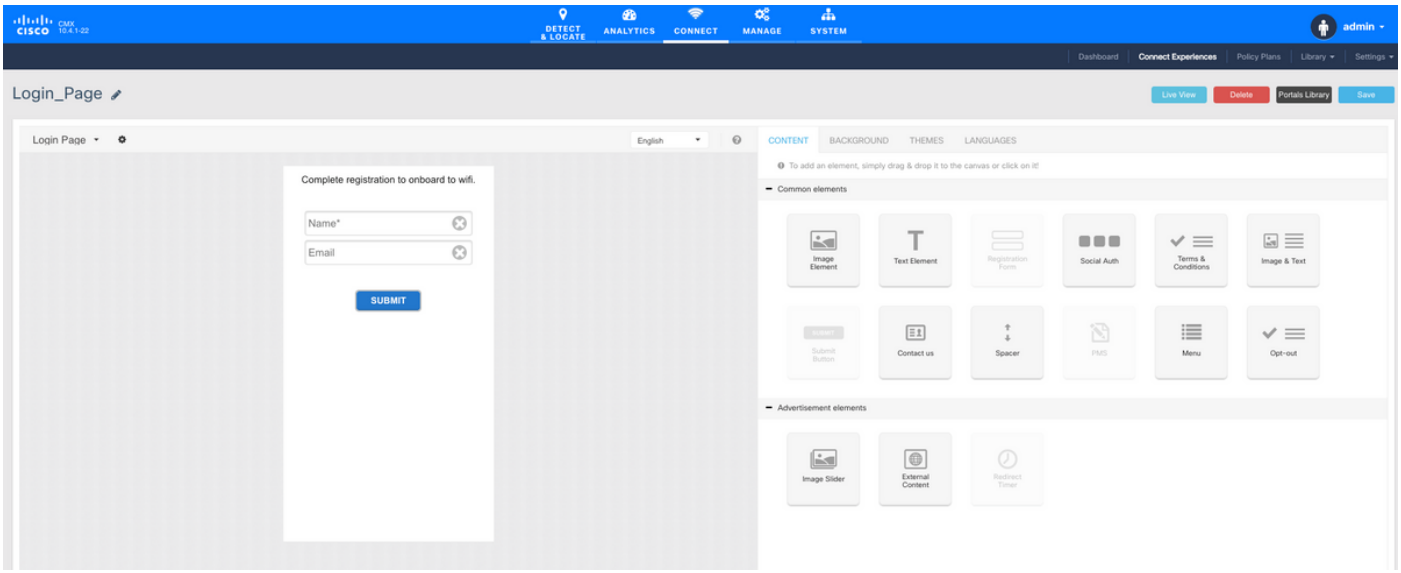
C. Configurazione CMX

Ènecessario che il controller venga aggiunto correttamente al CMX e che le mappe vengano esportate da Prime Infrastructure.

- Pagina di registrazione

Per creare una pagina di registrazione su CMX, seguire la stessa procedura utilizzata in precedenza per creare la pagina per altri metodi di autenticazione. Se si seleziona CONNECT&ENGAGE->Libreria, è possibile trovare i portali dei modelli pronti per la modifica scegliendo Modelli dal menu a discesa.

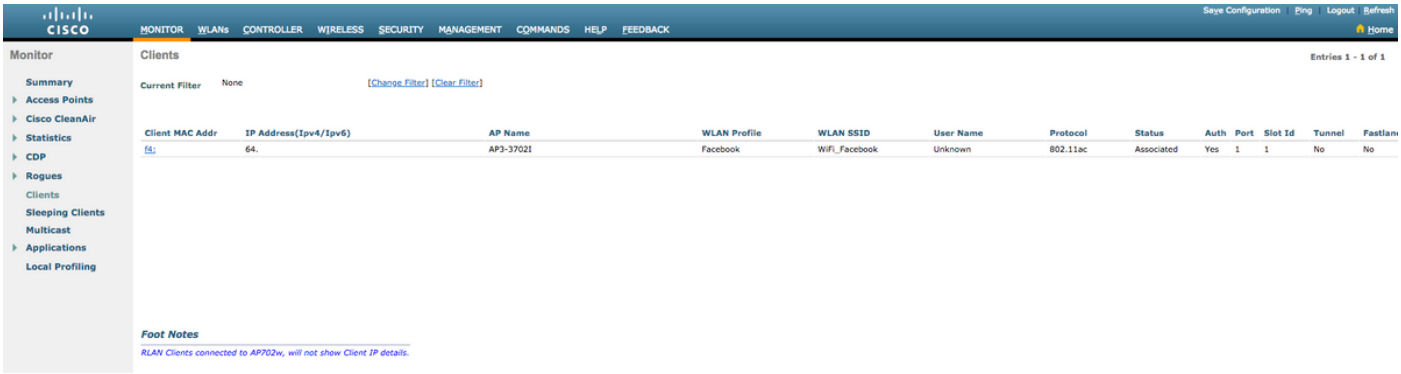
Il portale per la normale registrazione può essere creato da zero (selezionare "Personalizzato") o adattato dal modello "Modulo di registrazione" disponibile nella libreria CMX.



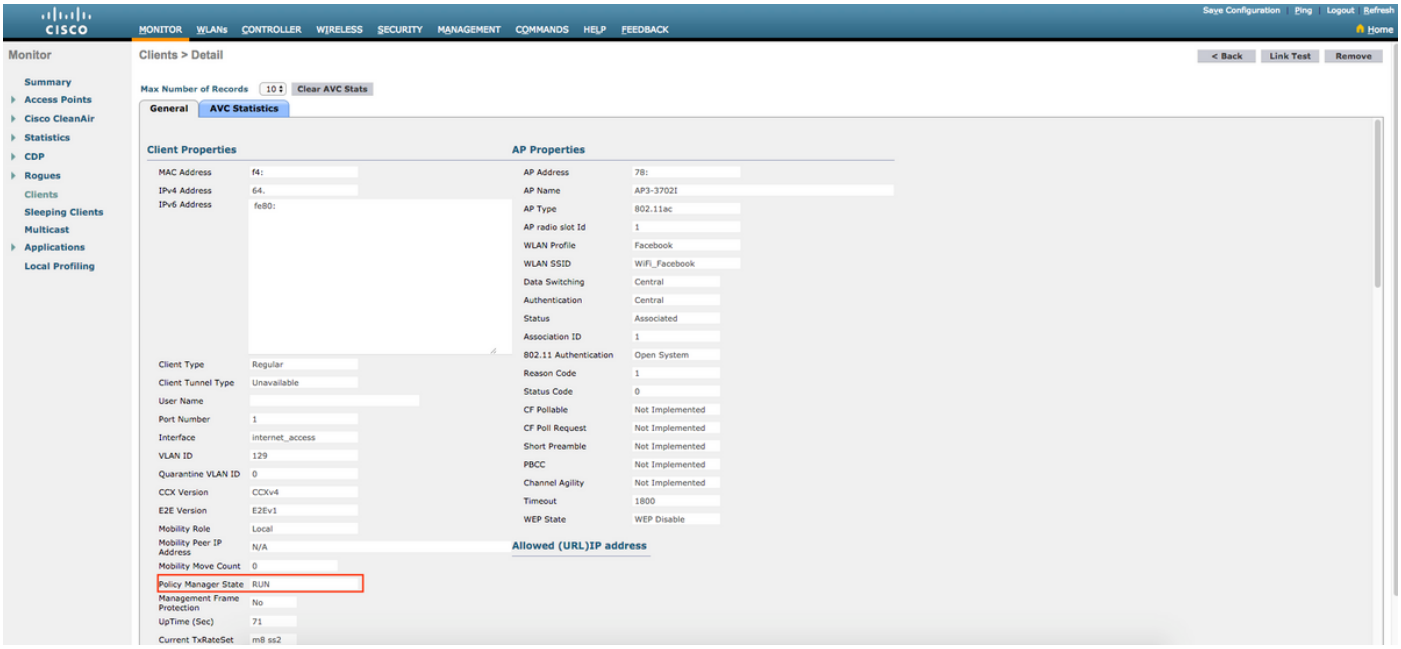
Verifica

WLC

Per verificare se l'utente è stato autenticato correttamente sul sistema, dalla GUI del WLC, selezionare MONITOR->Clients (Client) e cercare l'indirizzo MAC del client nell'elenco:

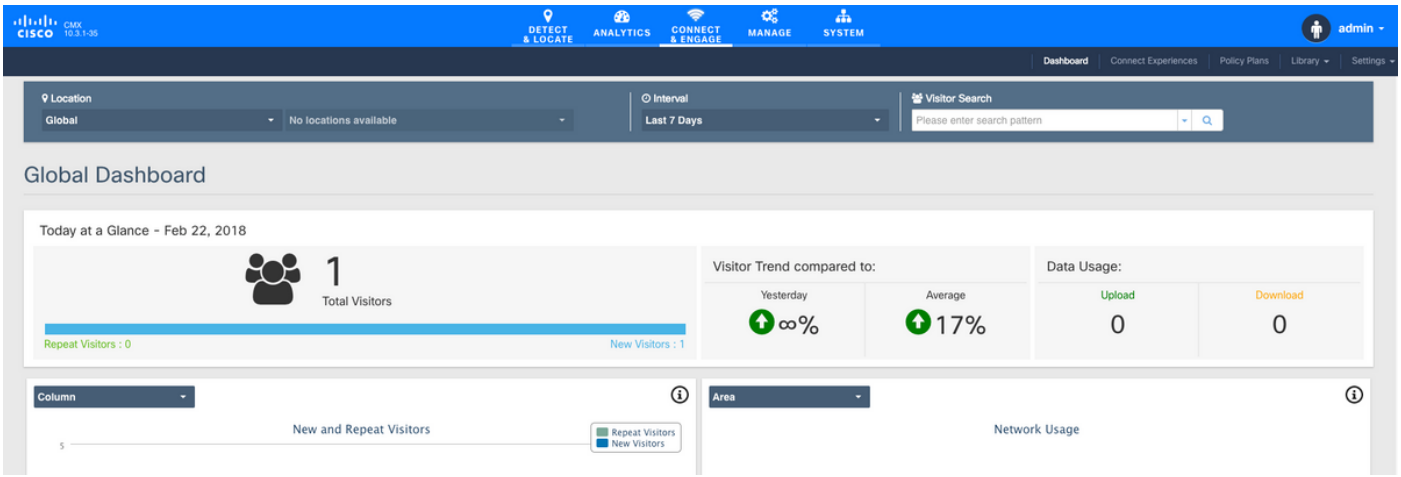


Fare clic sull'indirizzo MAC del client e, nei dettagli, confermare che lo stato di gestione dei criteri del client sia impostato su RUN:

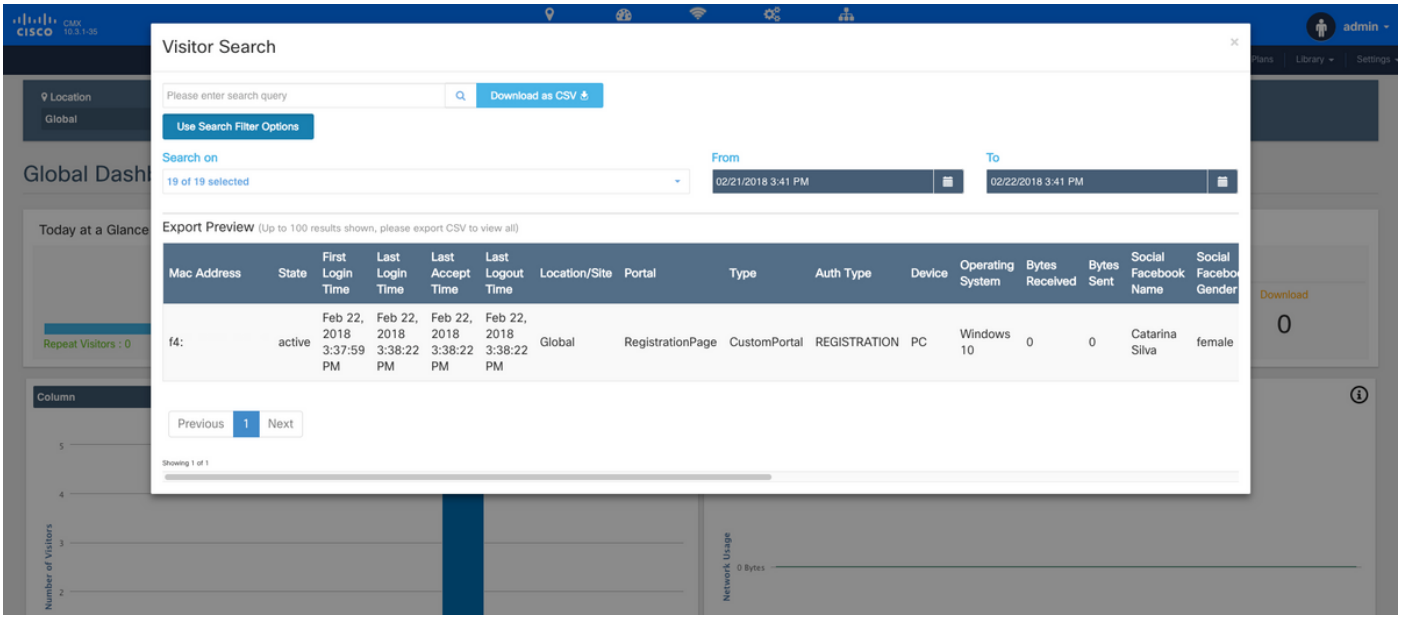


CMX

Èpossibile verificare il numero di utenti autenticati su CMX aprendo la scheda CONNECT&ENGAGE:



Per controllare i dettagli dell'utente, nella stessa scheda, in alto a destra, fare clic su Visitor Search:



Risoluzione dei problemi

Per controllare il flusso delle interazioni tra gli elementi, è possibile eseguire alcuni debug sul WLC:

>client di debug<MAC addr1> <MAC addr2> (Immettere l'indirizzo MAC di uno o più client)

>debug web-auth redirect enable mac <indirizzo MAC> (Immettere l'indirizzo MAC del client web-auth)

>debug attivazione web-auth webportal-server

>debug aaa all enable

I debug consentono di risolvere i problemi e, se necessario, è possibile integrare alcune acquisizioni di pacchetti.