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

Inhalt

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.

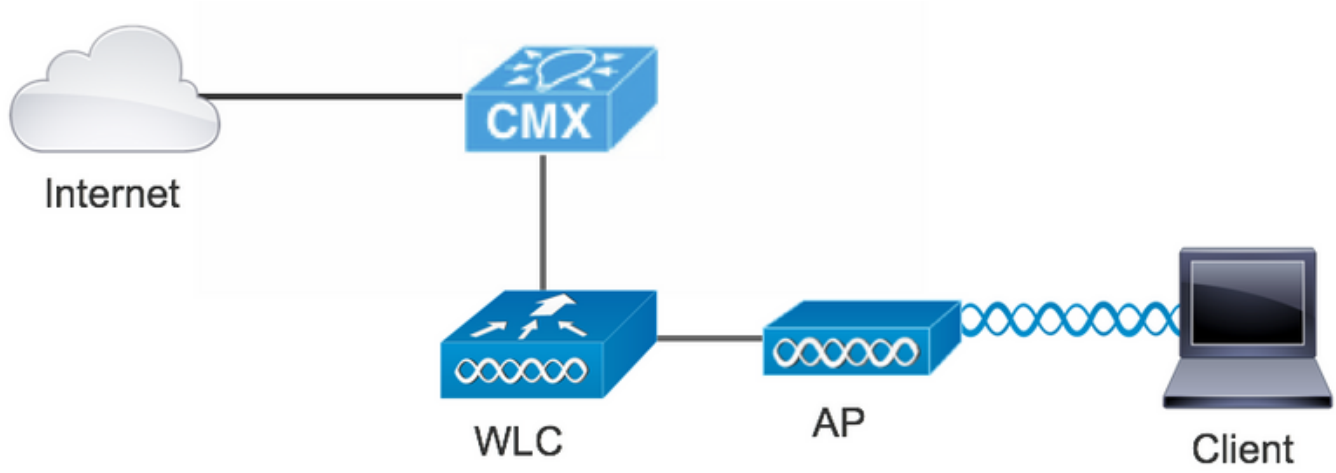
In beiden Szenarien versucht der Client, sich mithilfe der Authentifizierung über CMX auf der SSID zu registrieren.

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 Twilio 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.

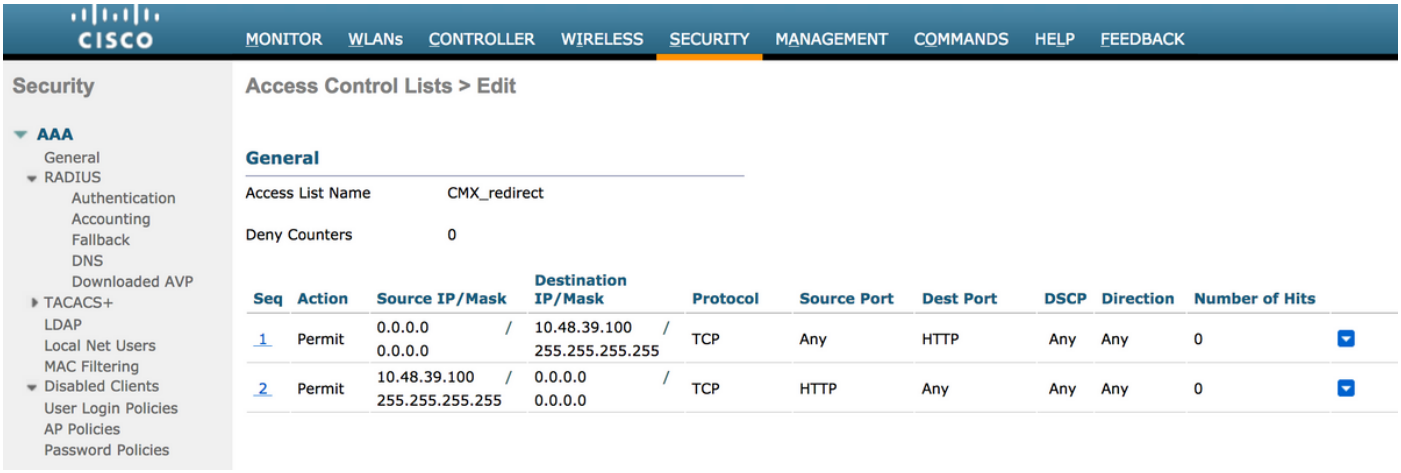
Antwort: WLC-Konfiguration

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.

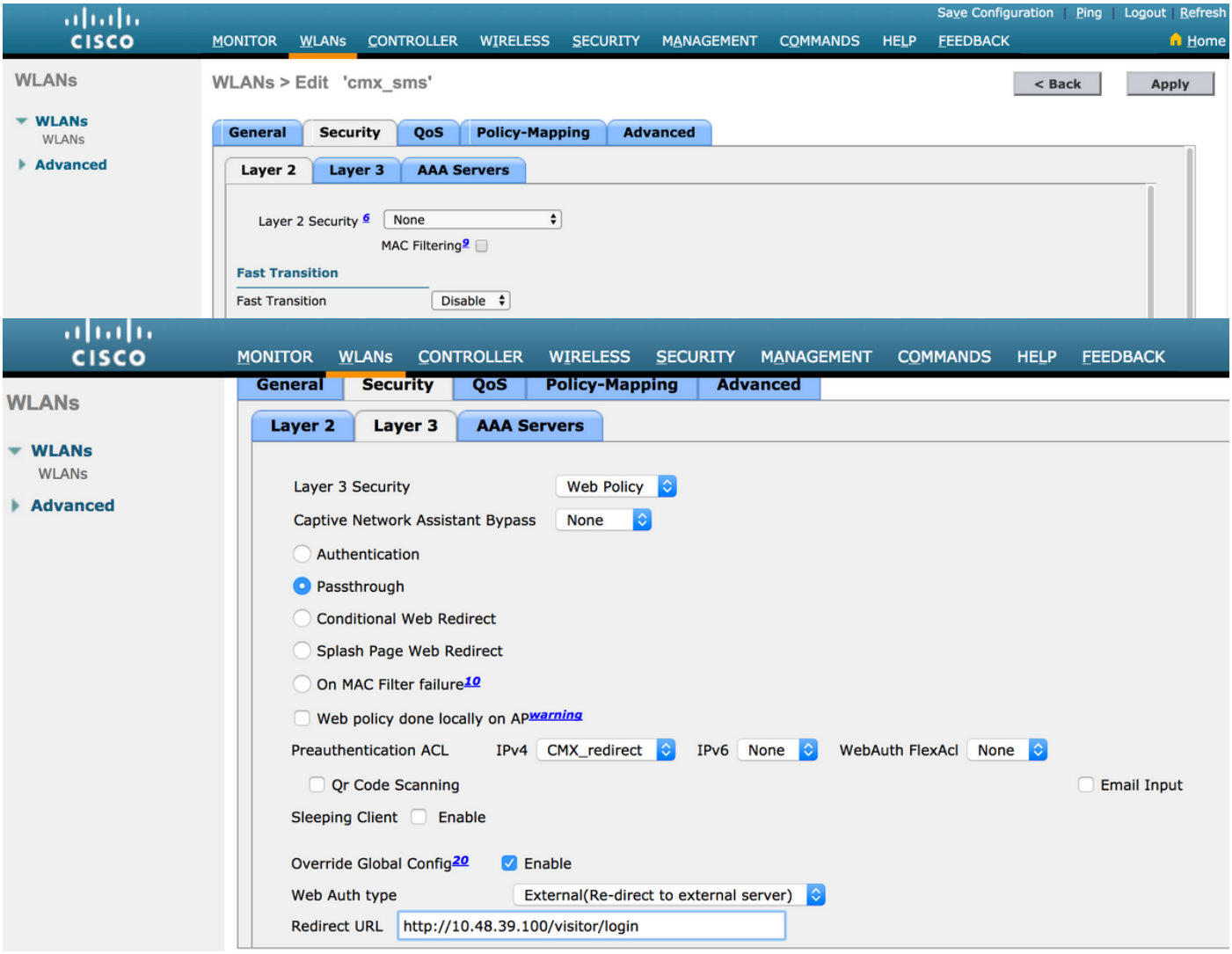
Die verwendete IP ist die für das CMX konfigurierte IP. Dadurch wird HTTP-Datenverkehr zwischen dem WLC und dem CMX zugelassen. Die folgende Abbildung zeigt die erstellte ACL, wobei "10.48.39.100" auf die CMX-IP-Adresse verweist.



2. WLAN

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

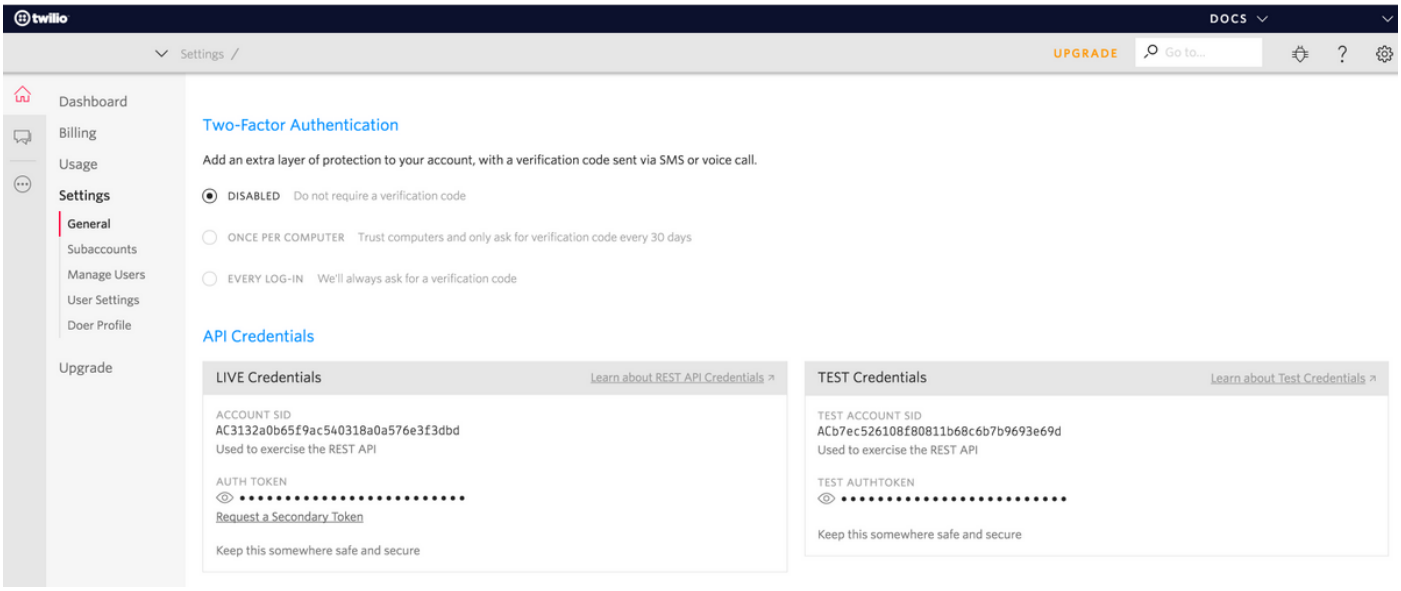
Zuerst wählen Sie WLANs->Edit->Layer 2->Layer 2 Security, und wählen Sie in der Dropdown-Liste None (Keine) aus, um die Layer 2 Security-Funktion zu deaktivieren. Wechseln Sie dann auf der gleichen Registerkarte "Sicherheit" zu Layer 3. Wählen Sie im Dropdownmenü für die Layer-3-Sicherheit die Option 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.



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.



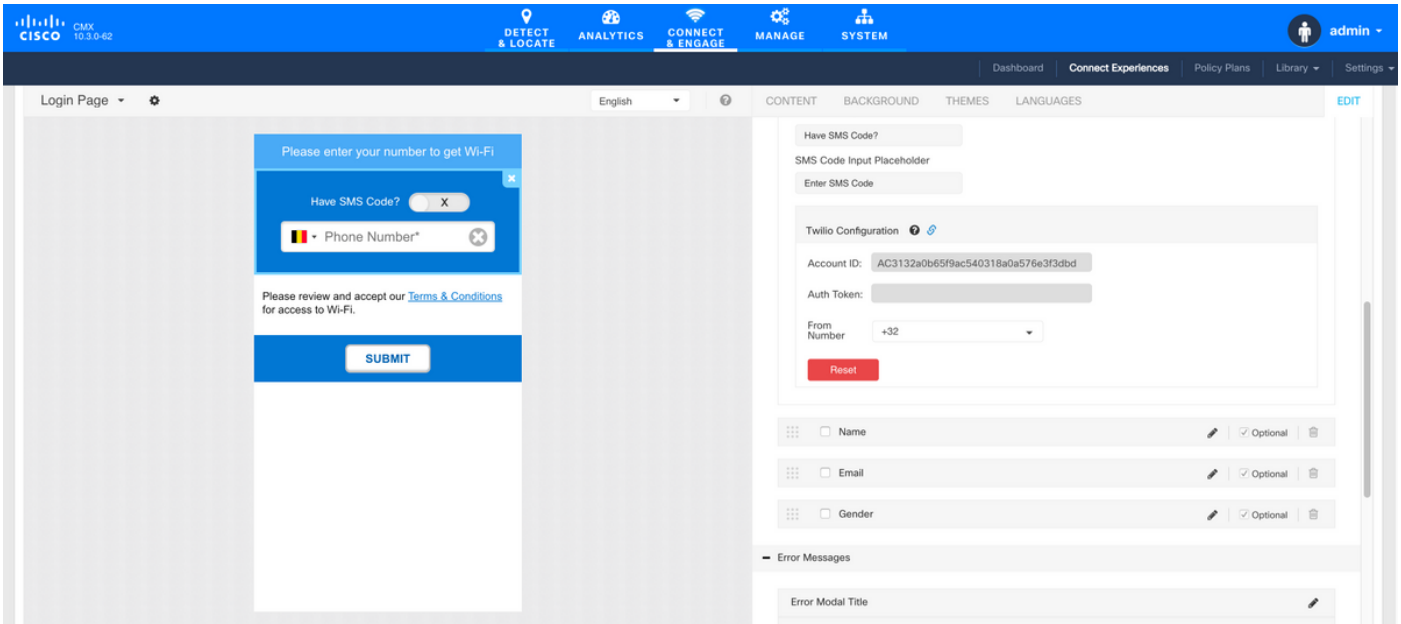
C. CMX-Konfiguration

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.



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.

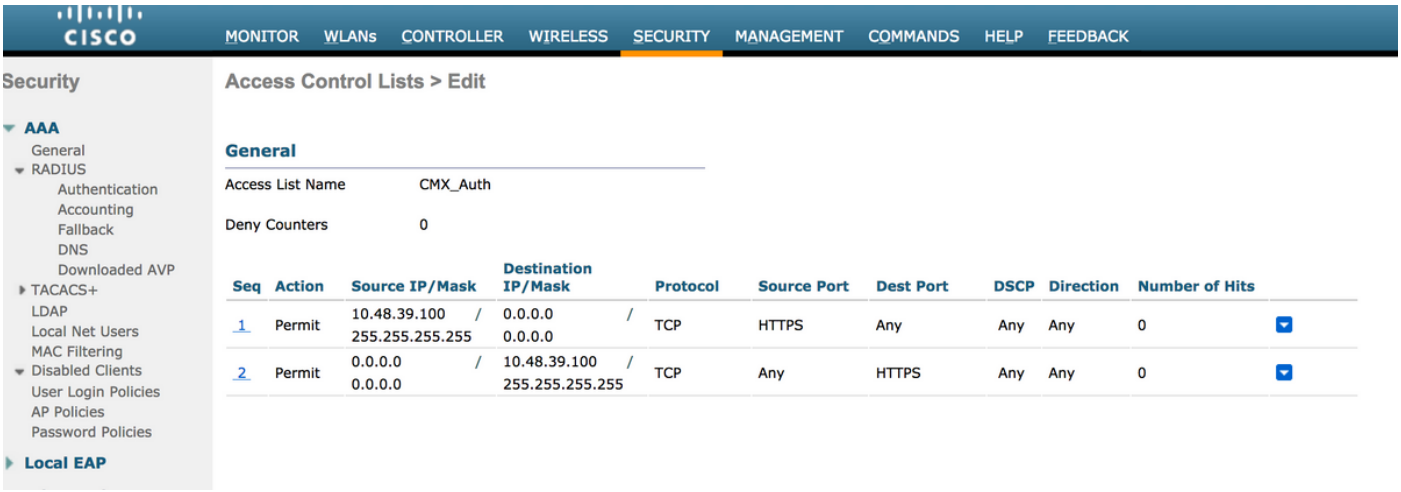
Antwort: WLC-Konfiguration

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.

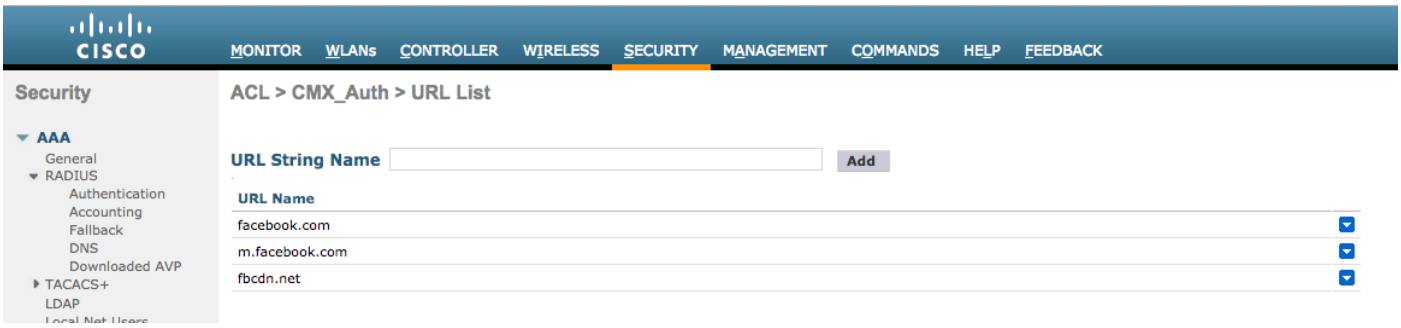
1. ACL

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)



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.

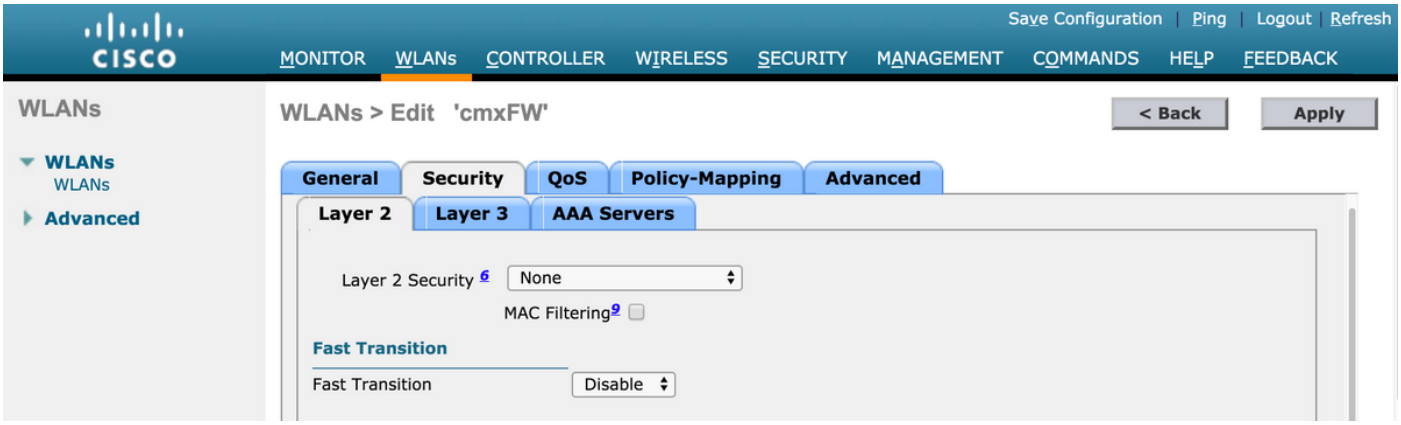


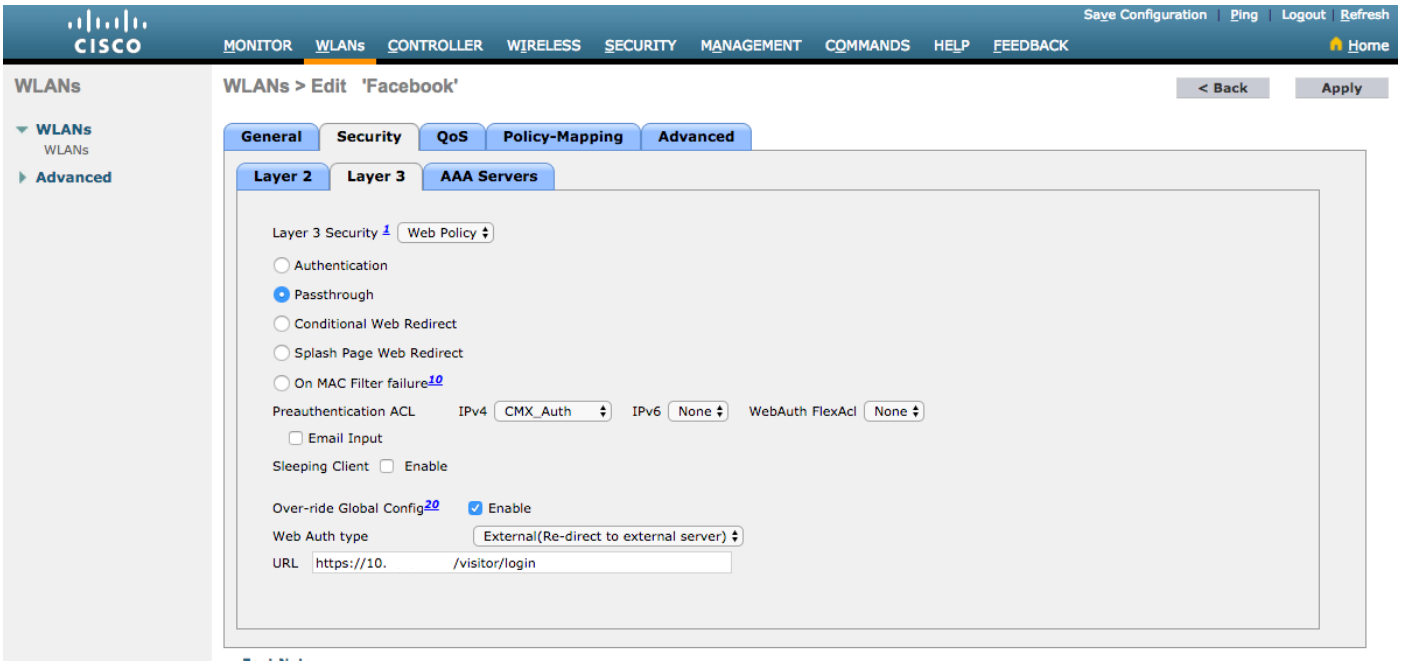
2. WLAN

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.



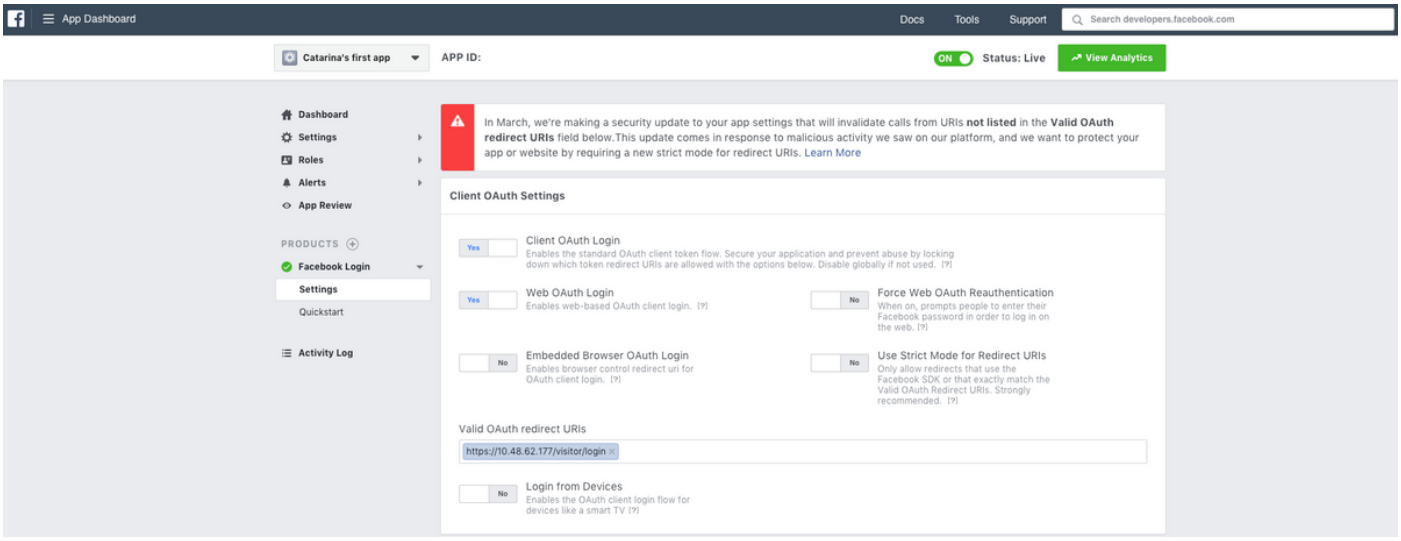


B. Facebook für Entwickler

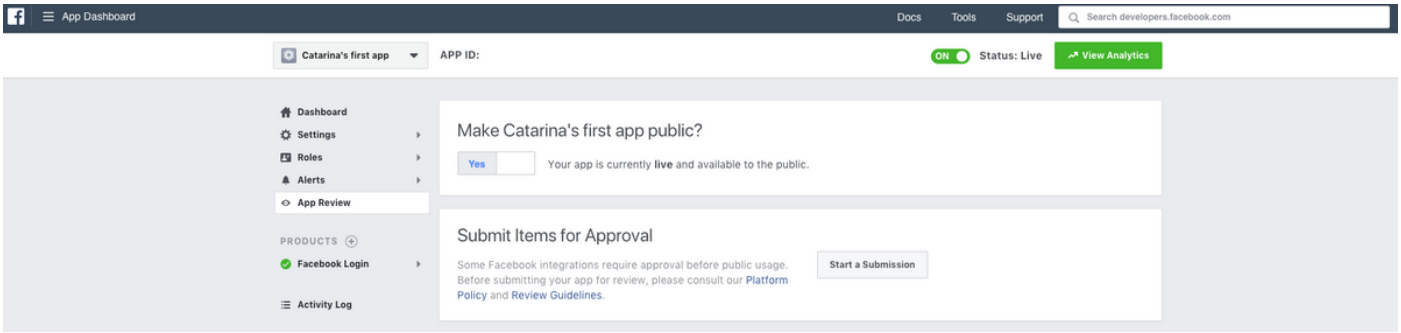
Für die Integration von Facebook und CMX ist eine Facebook-App erforderlich, damit die richtigen Token zwischen den beiden Teilen ausgetauscht werden können.

Auf Facebook für Entwickler 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.



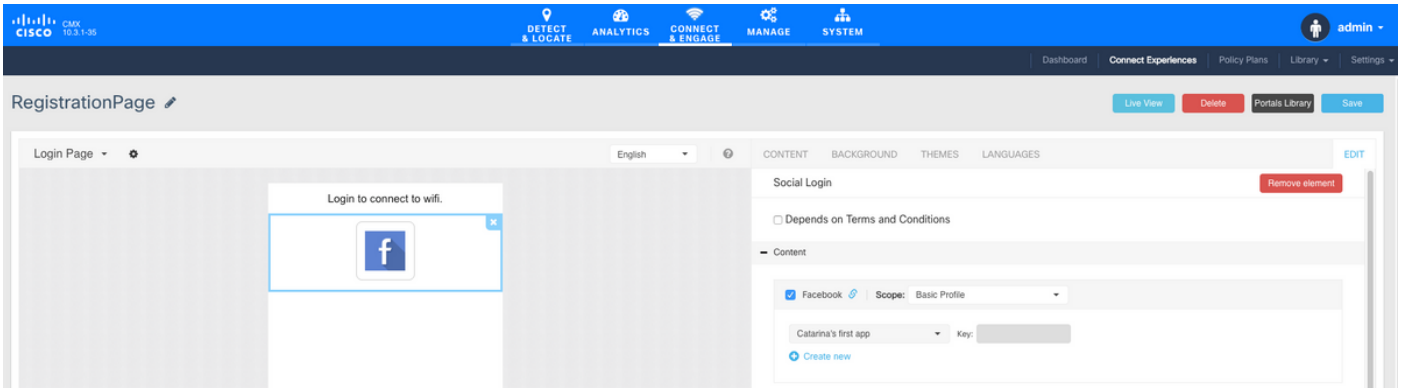
C. CMX-Konfiguration

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.



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

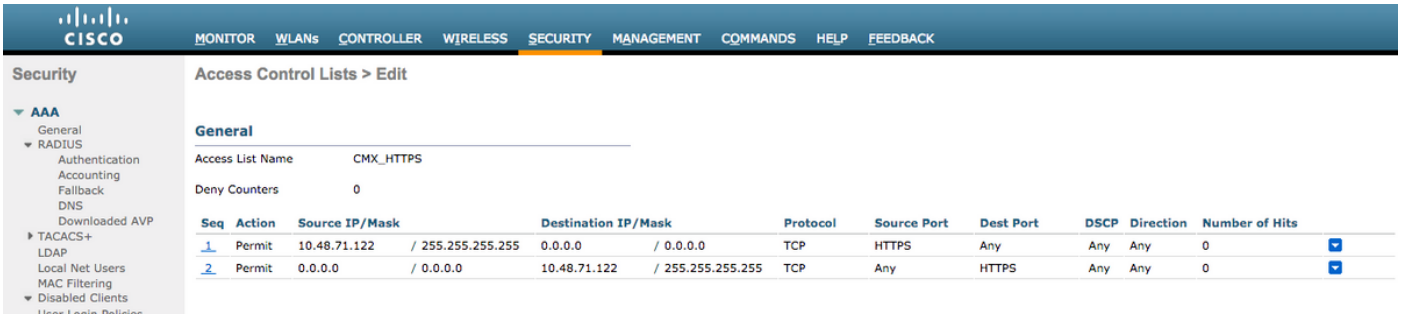
Auf der Seite des WLC werden sowohl eine SSID als auch eine ACL konfiguriert. Der Access Point muss dem Controller und im RUN-Status angeschlossen sein.

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.

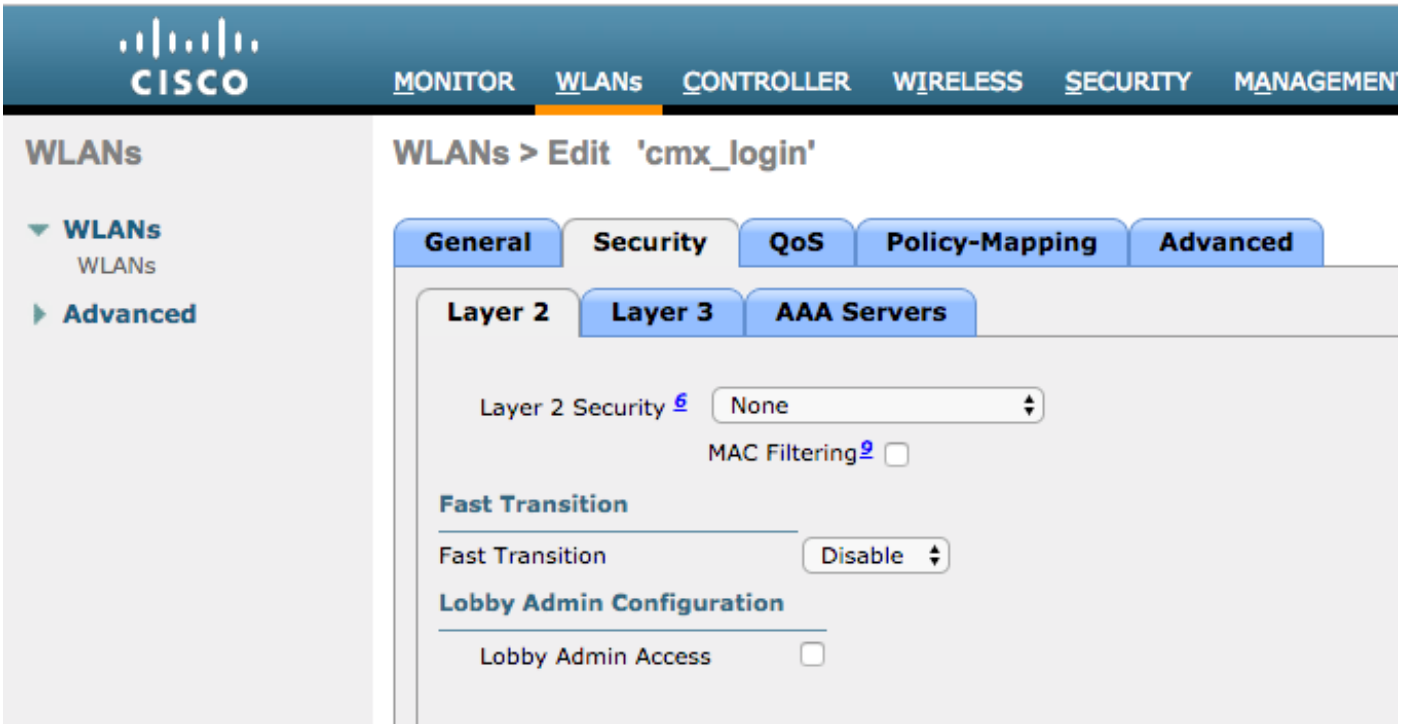


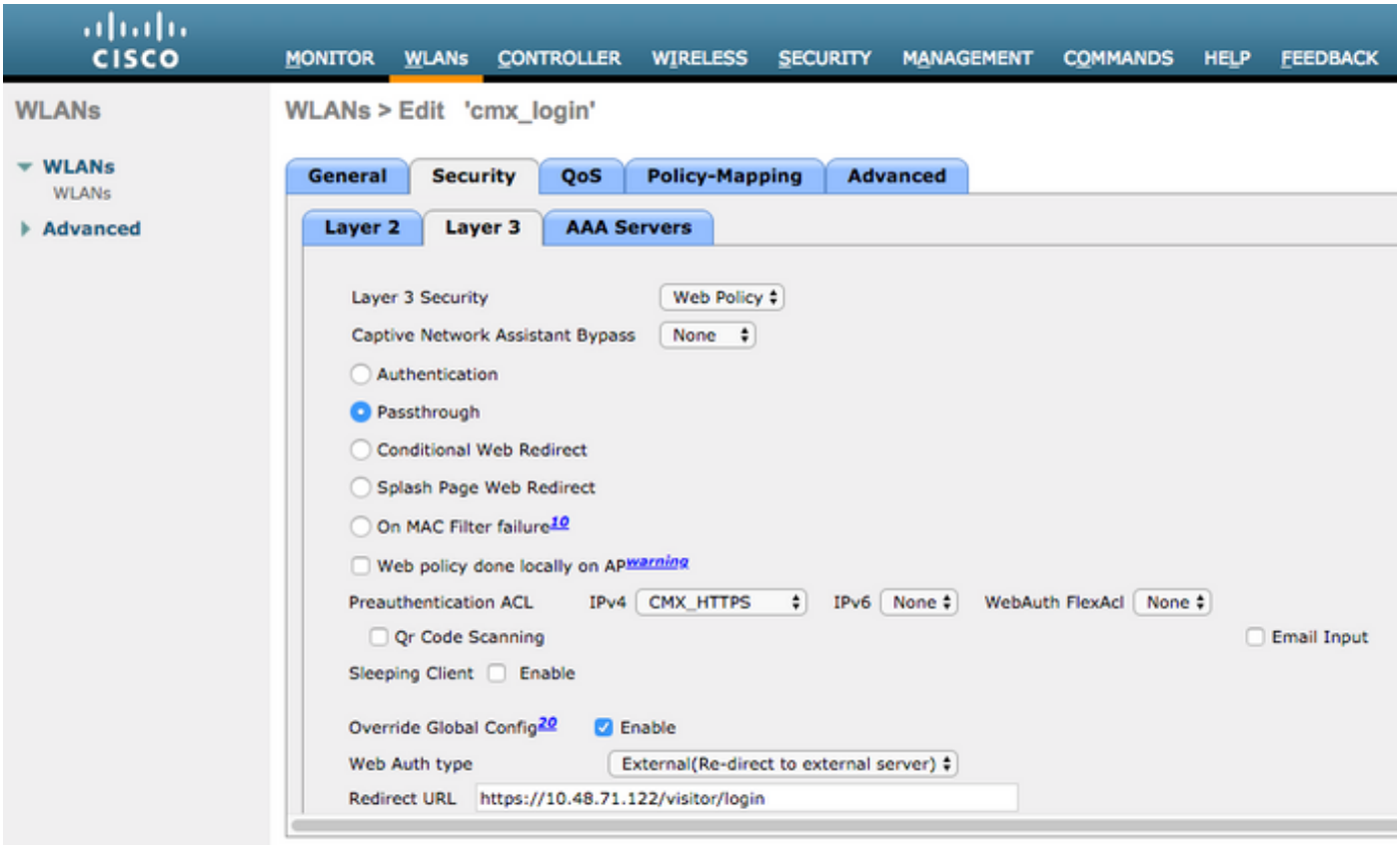
2. WLAN

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.





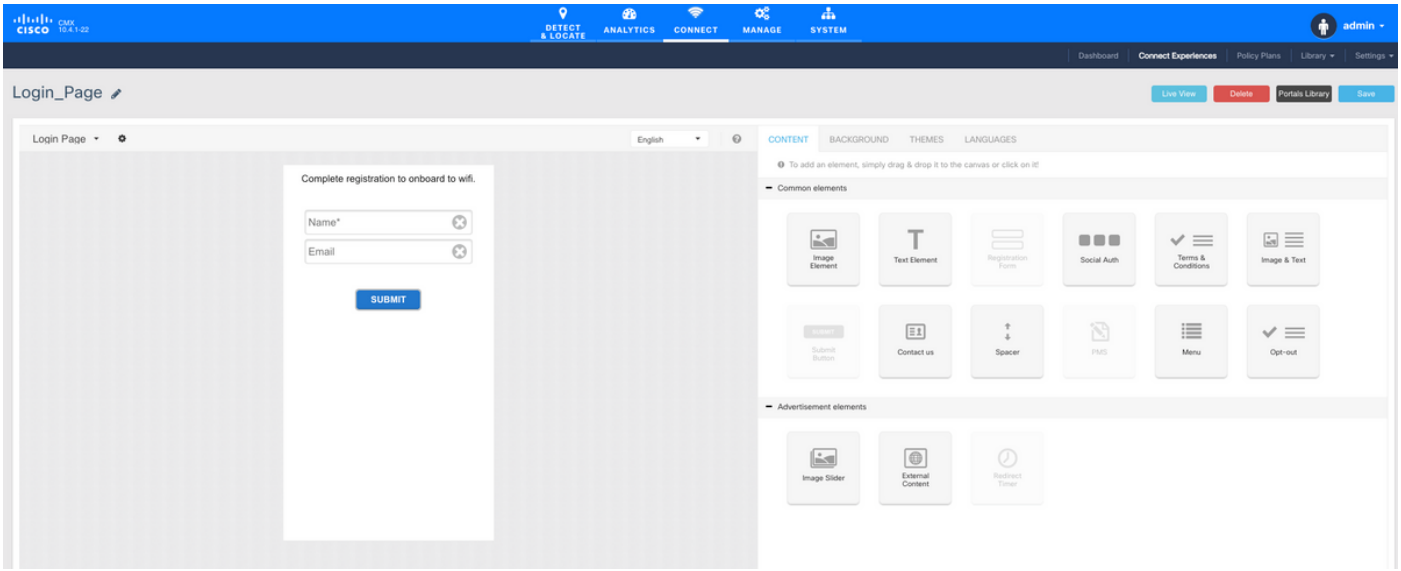
C. CMX-Konfiguration

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.

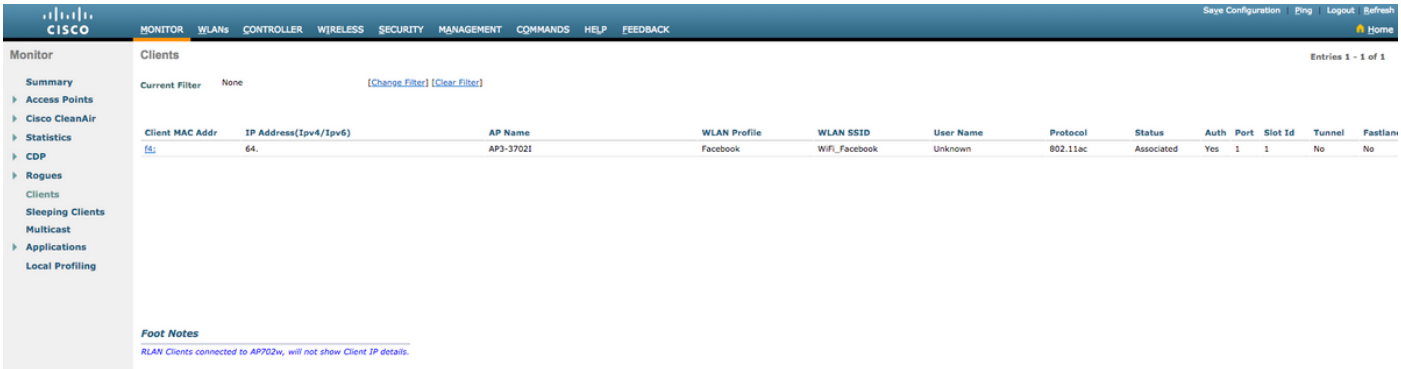
Das Portal für die normale Registrierung kann von Grund auf (wählen Sie "Benutzerdefiniert") oder angepasst aus der Vorlage "Registrierungsformular" in der CMX-Bibliothek verfügbar gemacht werden.



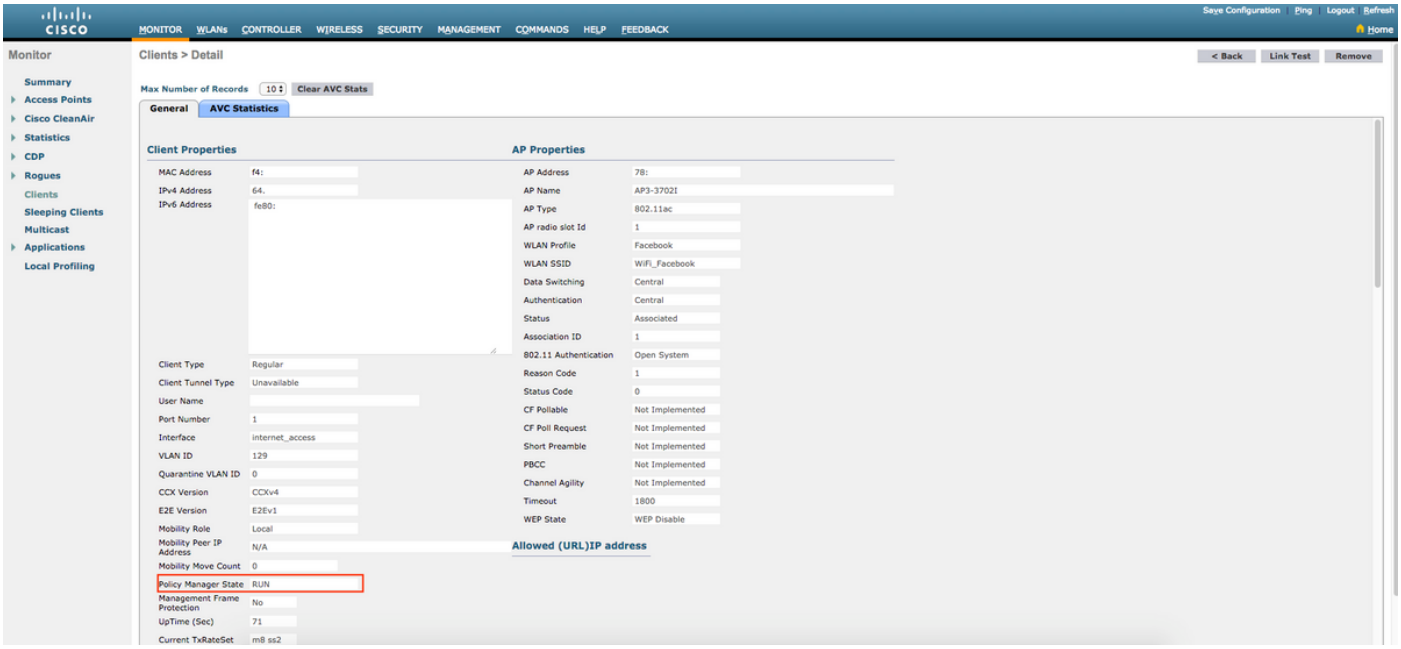
Überprüfen

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:

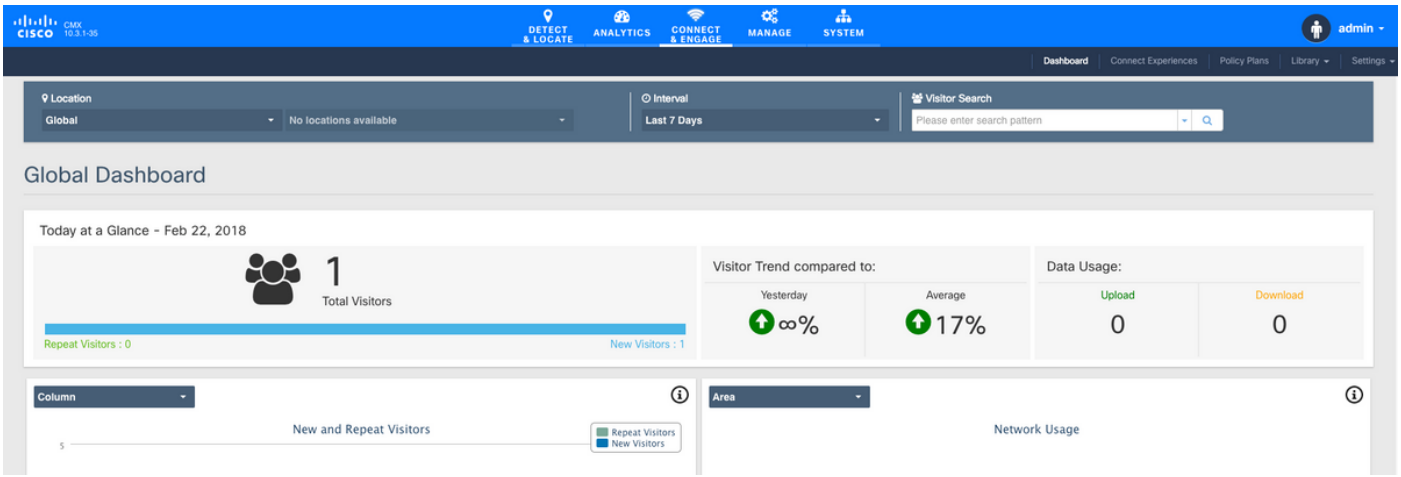


Klicken Sie auf die MAC-Adresse des Clients, und bestätigen Sie in den Details, dass der Status des Client Policy Manager den Status "RUN" aufweist:

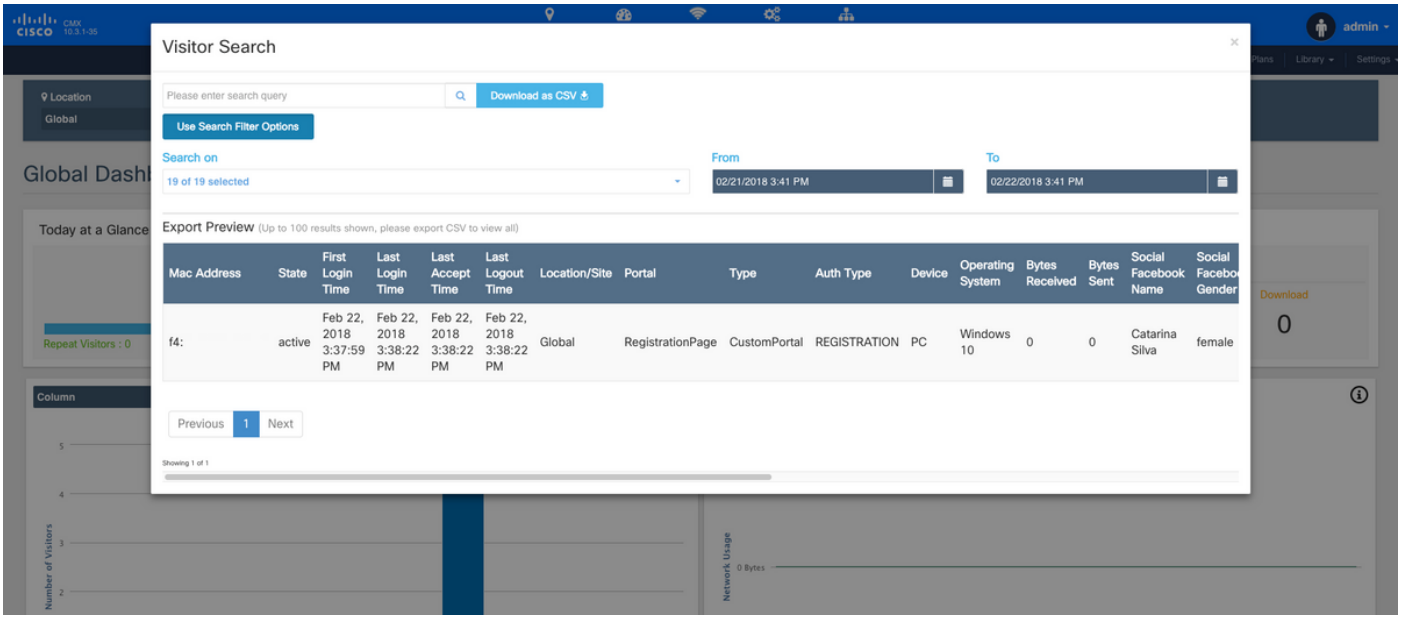


CMX

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



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



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.