CMX互联体验 — 社交、短信和自定义门户注册配置示例

目录

简介

本文档的目的是通过互联移动体验(CMX)上的访客门户配置引导网络管理员通过客户端注册。

CMX使用户能够使用社交注册登录、SMS和自定义门户注册并验证到网络。在本文档中，可以找到无线局域网控制器(WLC)和CMX上配置步骤的概述。

先决条件

要求

CMX应正确配置基本配置。

从Prime基础设施导出映射是可选操作。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科无线控制器版本8.2.166.0、8.5.110.0和8.5.135.0。
- 思科互联移动体验版本10.3.0-62、10.3.1-35. 10.4.1-22。

配置

网络图

本文档将介绍使用CMX对用户/客户端进行无线网络身份验证的两种不同方法。

首先，将介绍使用社交网络帐户设置身份验证，然后使用SMS进行身份验证。

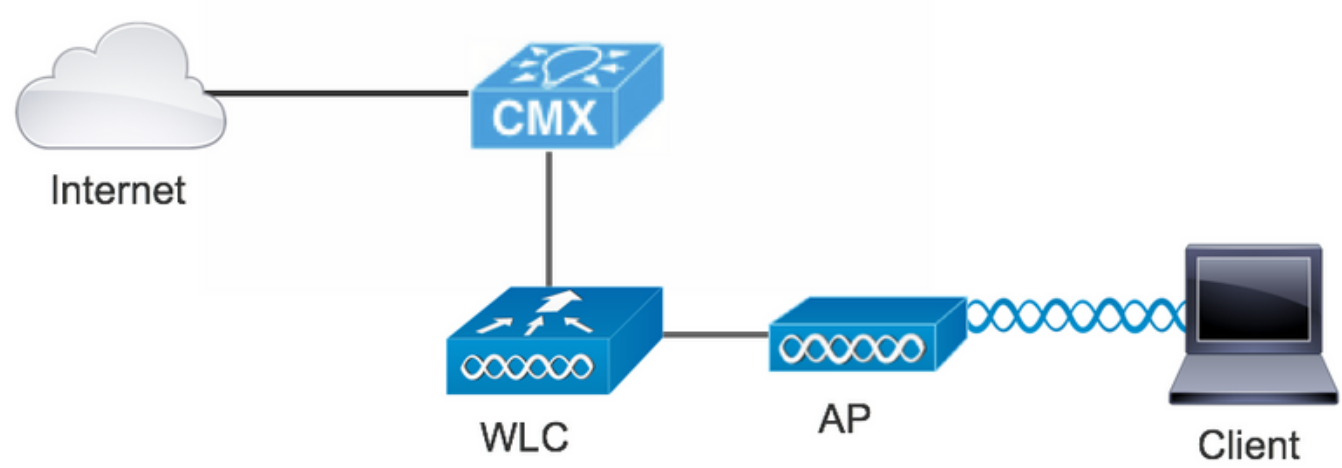
在这两种情况下，客户端都会尝试通过CMX使用身份验证在SSID上注册。

WLC将HTTP流量重定向到CMX，在CMX中，系统会提示用户进行身份验证。CMX包含用于客户端注册的门户设置，包括通过社交帐户和SMS。

下面介绍注册流程：

1. 客户端尝试加入SSID并打开浏览器。
2. WLC将重定向到访客门户，而不是访问请求的站点。
3. 客户端提供其凭证并尝试进行身份验证。
4. CMX处理身份验证过程。
5. 如果成功，则现在为客户端提供完全互联网访问。
6. 客户端被重定向到初始请求的站点。

使用的拓扑为：



配置

通过SMS进行身份验证

思科CMX允许通过SMS进行客户端身份验证。此方法需要设置HTML页面，以便用户向系统提供其凭证。默认模板由CMX本地提供，稍后可编辑或替换为自定义模板。

文本消息服务通过将CMX与Twilio集成来完成，Twilio是一个允许发送和接收文本消息的云通信平台。Twilio允许每个门户拥有一个电话号码，这意味着如果使用多个门户，则每个门户需要一个电话号码。

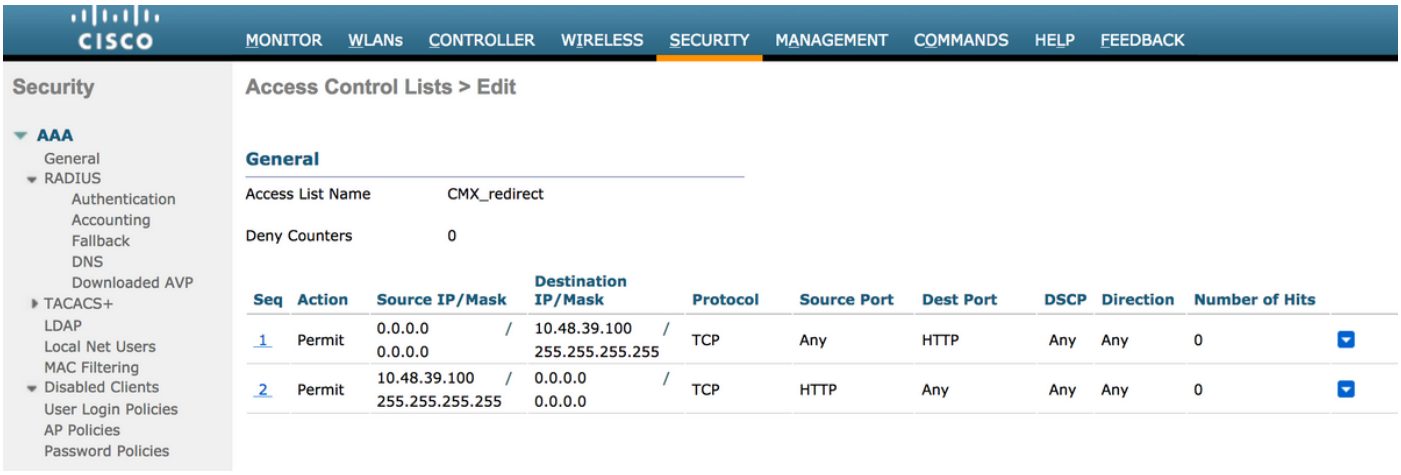
A. WLC 配置

在WLC端，将同时配置SSID和ACL。AP应加入控制器并处于RUN状态。

1. ACL

需要允许WLC上配置的HTTP流量的ACL。要配置ACL，请转至Security -> Access Control Lists -> Add New Rule。

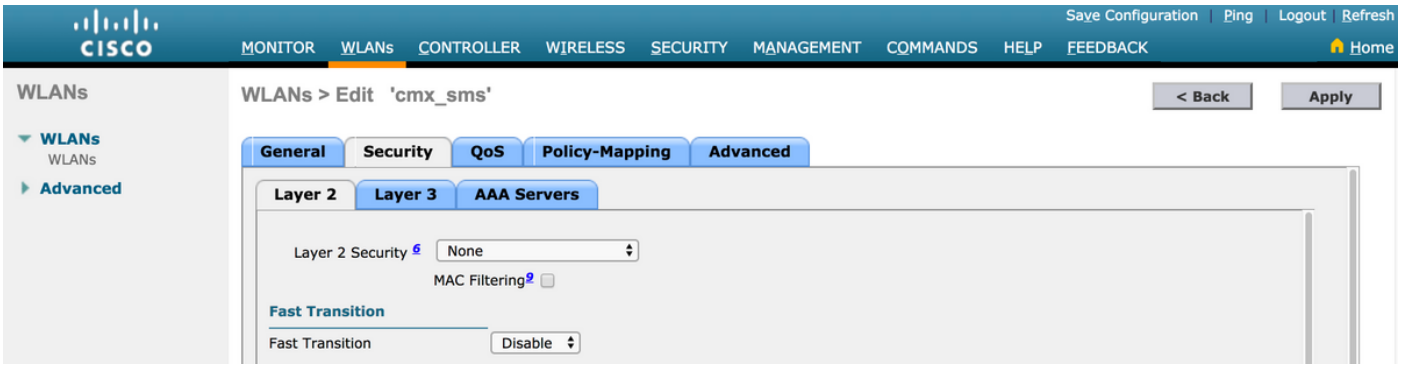
使用的IP是为CMX配置的IP。这允许WLC和CMX之间的HTTP流量。下图显示了创建的ACL，其中“10.48.39.100”是指CMX IP地址。

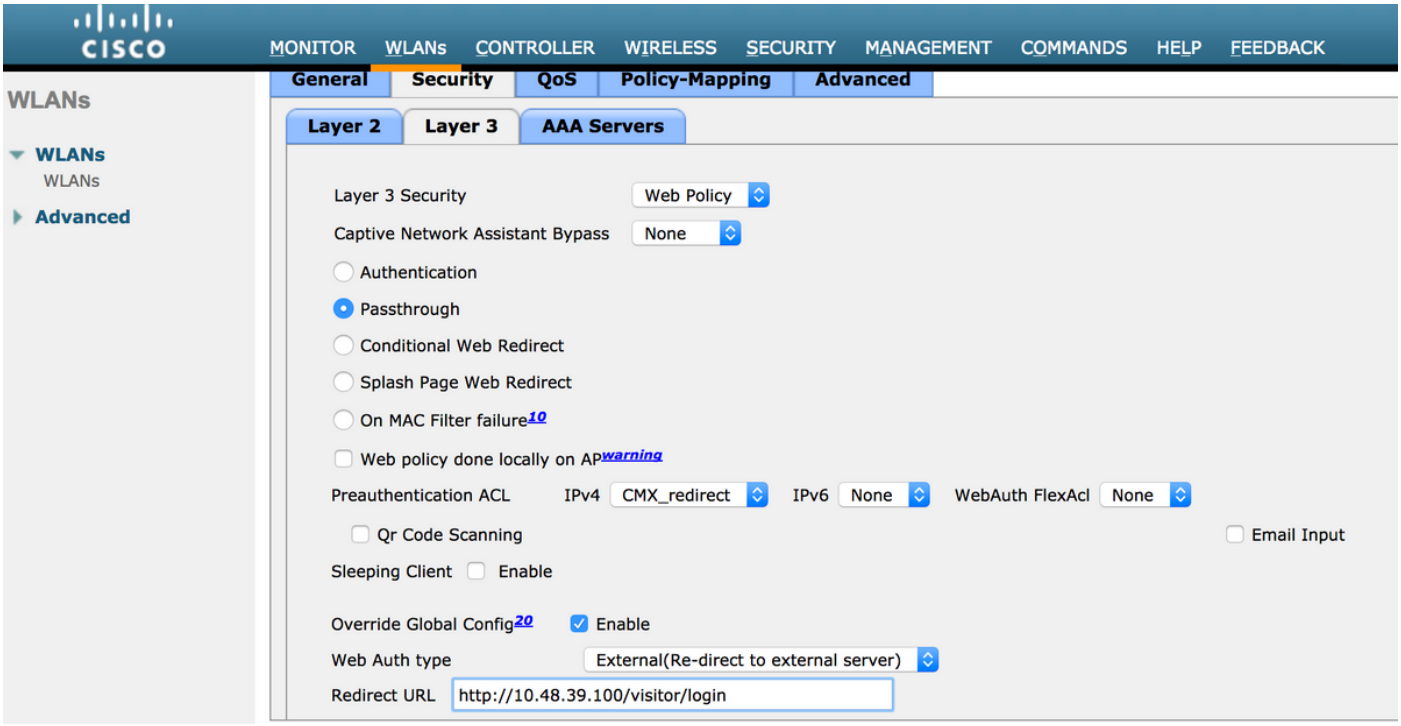


2. WLAN

因此，与门户的集成完成后，必须对WLAN进行安全策略更改。

首先，转到WLANs ->Edit->Layer 2->Layer 2 Security，然后在下拉列表中选择None，因此Layer 2 Security已禁用。然后，在同一“安全”选项卡中，更改为第3层。在“第3层安全”下拉菜单中，依次选择Web策略和直通。在预身份验证ACL中，选择之前配置的IPv4 ACL，将其绑定到必须提供SMS身份验证的相应WLAN。必须启用Over-ride Global Config（超载全局配置）选项，并且网络身份验证类型必须为External（重定向到外部服务器），因此客户端可以重定向到CMX服务。URL必须与CMX SMS身份验证门户相同，格式为http://<CMX-IP>/visitor/login。

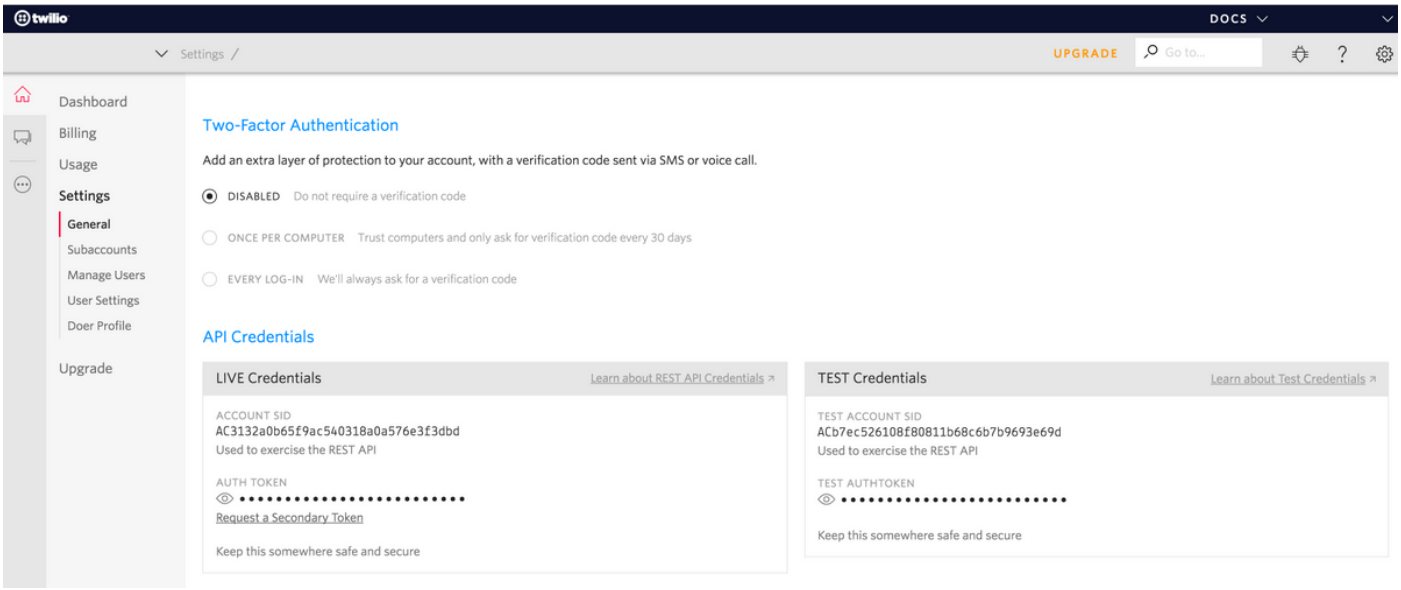




B. Twilio

CMX为文本消息服务提供Twilio集成。在正确配置Twilio上的帐户后，提供凭证。需要ACCOUNT SID和AUTH TOKEN。

Twilio有自己的配置要求，通过设置服务的过程进行记录。在与CMX集成之前，可以测试Twilio服务，这意味着在将Twilio设置与CMX结合使用之前，可以检测与Twilio设置相关的问题。



C. CMX配置

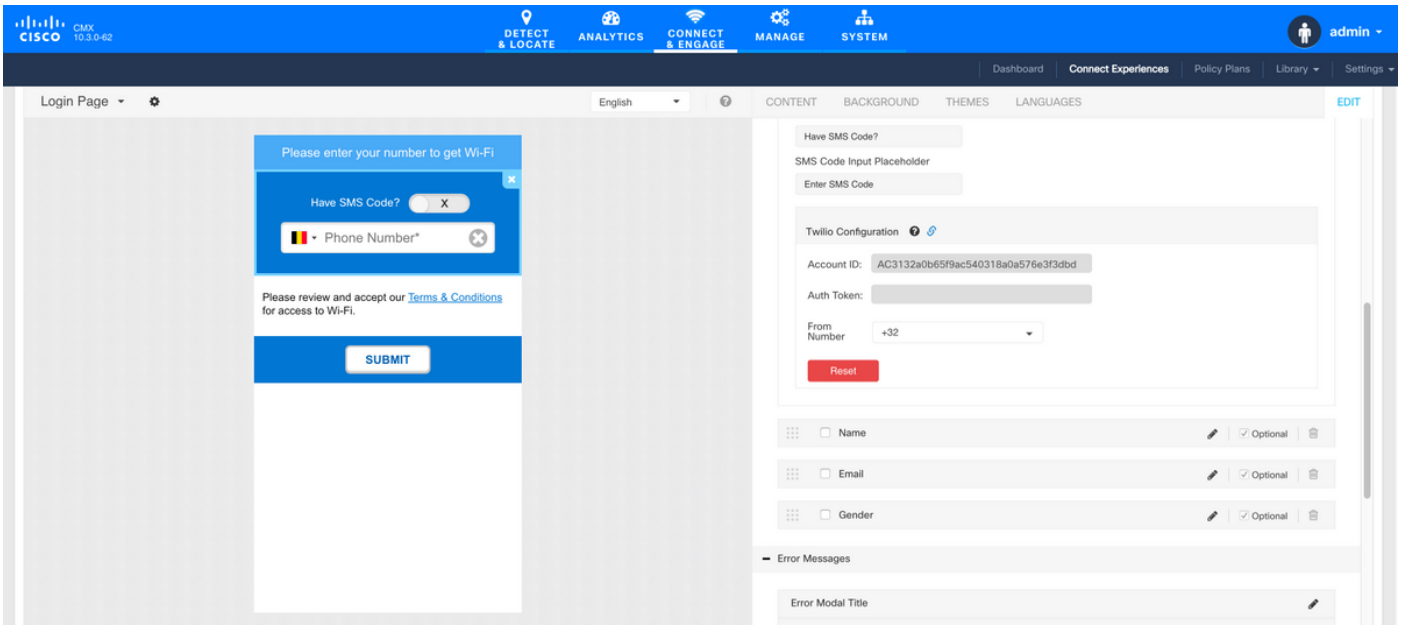
需要将控制器正确添加到CMX，以及从Prime基础设施导出的映射。

- SMS注册页

注册门户有默认模板。可以找到选择CONNECT&ENGAGE->Library的门户。如果需要模板，请在下拉菜单中选择模板。

要将Twilio与门户集成，请转至Twilio配置并提供帐户ID和身份验证令牌。如果集成成功，Twilio帐

户中使用的号码将弹出。



通过社交网络帐户进行身份验证

使用社交网络帐户对客户端进行身份验证要求网络管理员在CMX上添加有效的Facebook应用标识符。

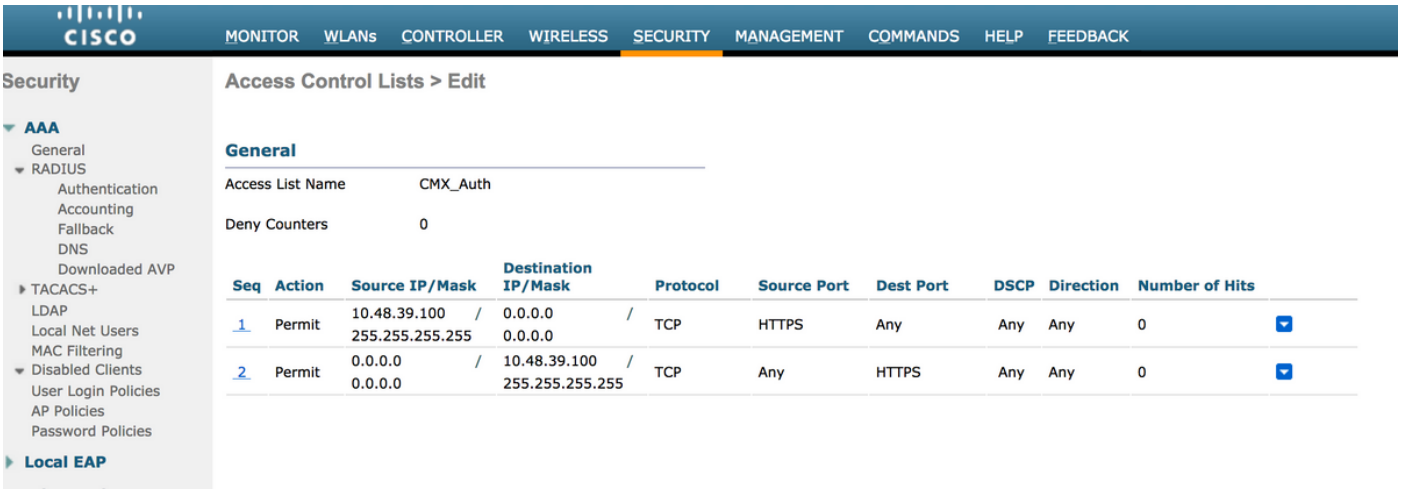
A. WLC配置

在WLC端，将同时配置SSID和ACL。AP应加入控制器并处于RUN状态。

1. ACL

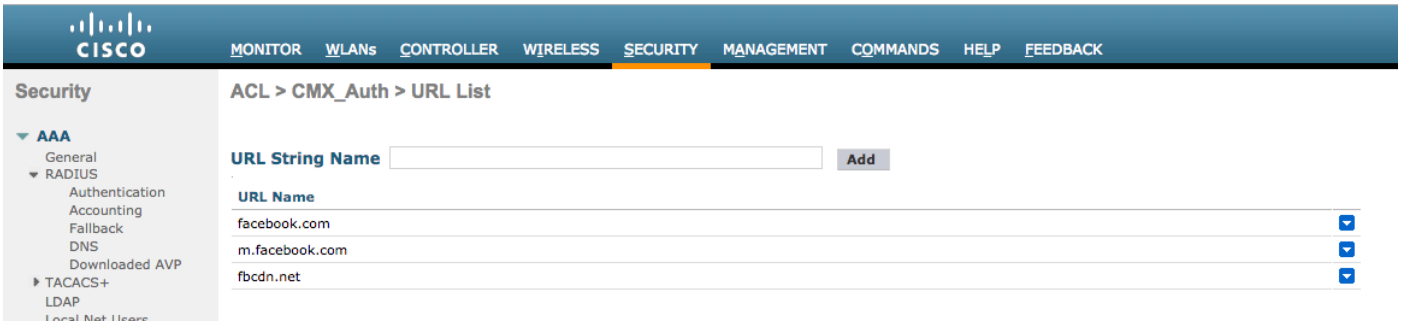
正如我们使用HTTPS作为身份验证方法一样，必须在WLC上配置允许HTTPS流量的ACL。要配置ACL，请转至Security -> Access Control Lists -> Add New Rule。

CMX IP必须用于允许WLC和CMX之间的HTTPS流量。（在本例中，CMX IP为10.48.39.100）



此外，还需要使用带有Facebook URL的DNS ACL。为此，在安全 — >访问控制列表中查找之前配置的ACL（本例中为CMX_Auth）的条目，并将鼠标移到条目末尾的蓝色箭头，然后选择添加 — 删

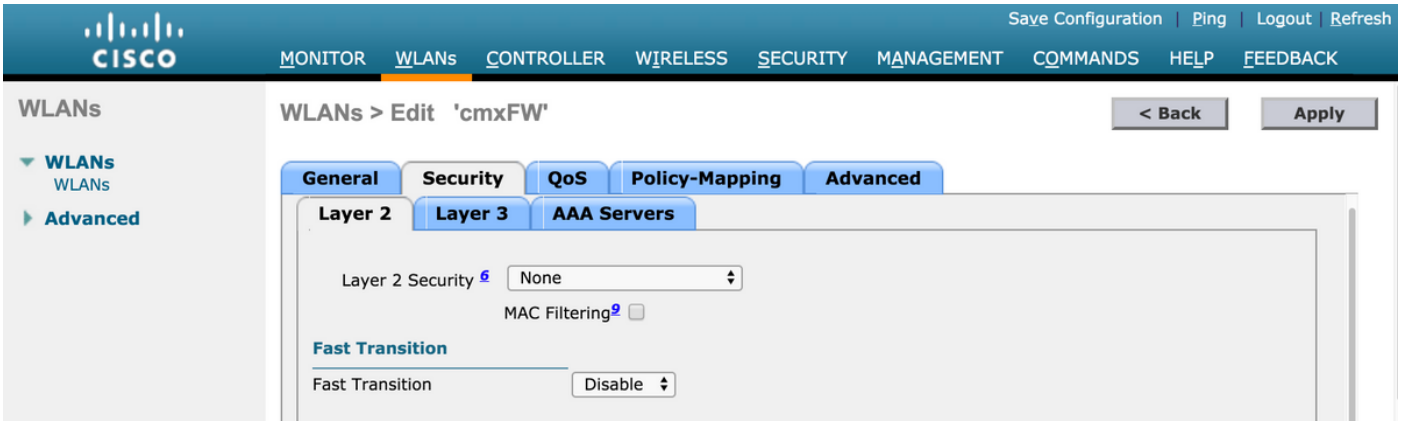
除URL。然后在URL字符串名称和添加上键入Facebook的URL。

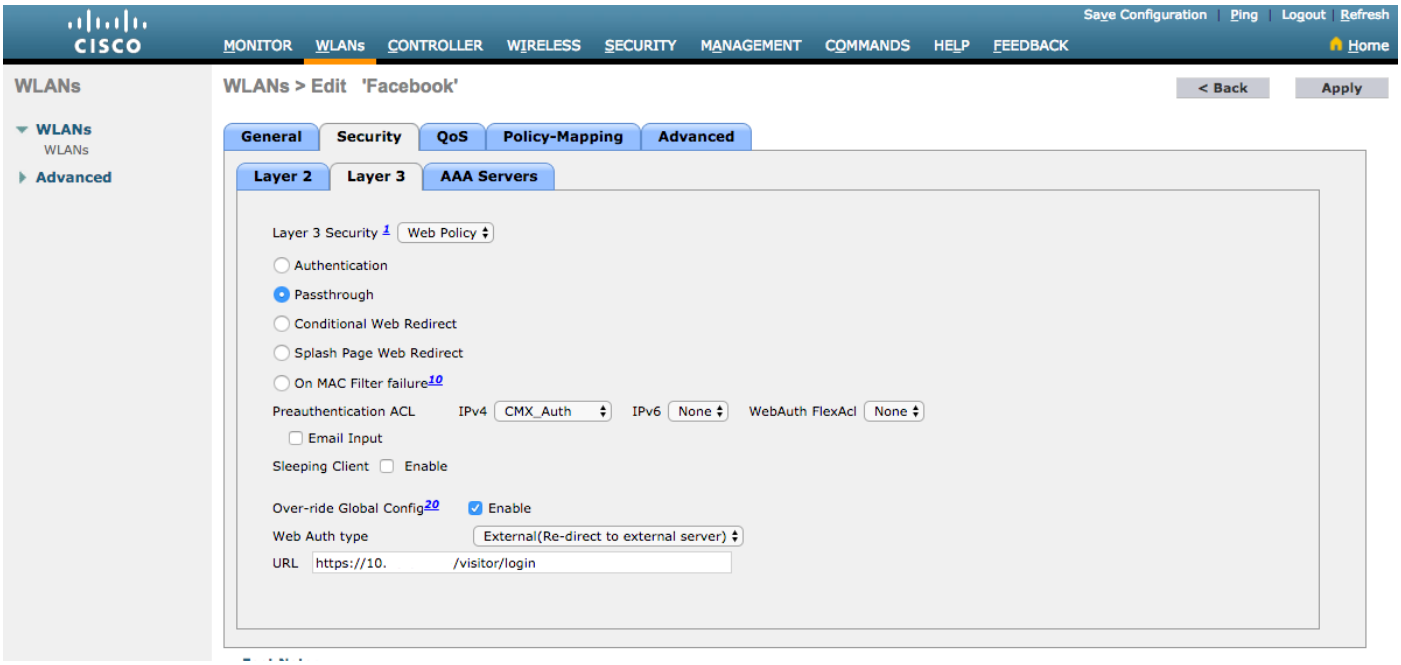


2. WLAN

安全策略会更改，以便注册生效，需要在WLAN上进行特定配置。

如之前对SMS注册所做的那样，首先转到WLAN ->编辑 — >第2层 — >第2层安全，然后在下拉列表中选择无，因此禁用第2层安全。在同一Security选项卡中，更改为Layer 3。在Layer 3 Security下拉菜单中，依次选择Web Policy和Passthrough。在预身份验证ACL中，选择之前配置的IPv4 ACL，将其绑定到必须通过Facebook提供身份验证的相应WLAN。必须启用Over-ride Global Config（超载全局配置）选项，并且网络身份验证类型必须为External（重定向到外部服务器），因此客户端可以重定向到CMX服务。请注意，此时URL必须采用以下格式**https**://<CMX-IP>/visitor/login。



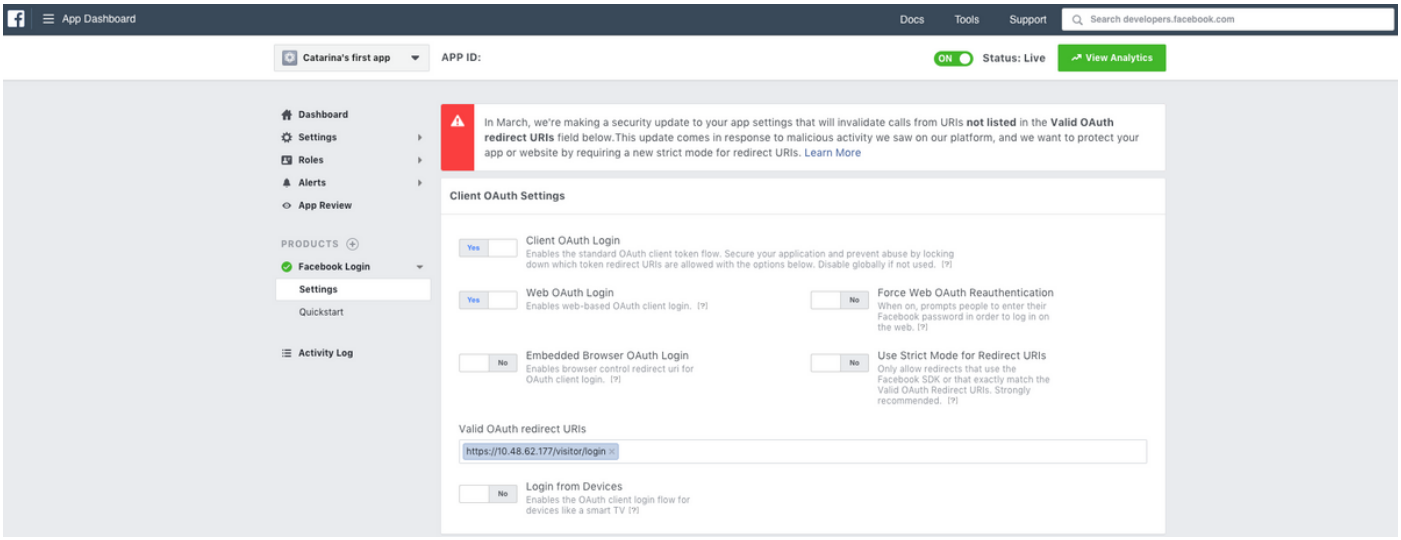


B.面向开发人员的Facebook

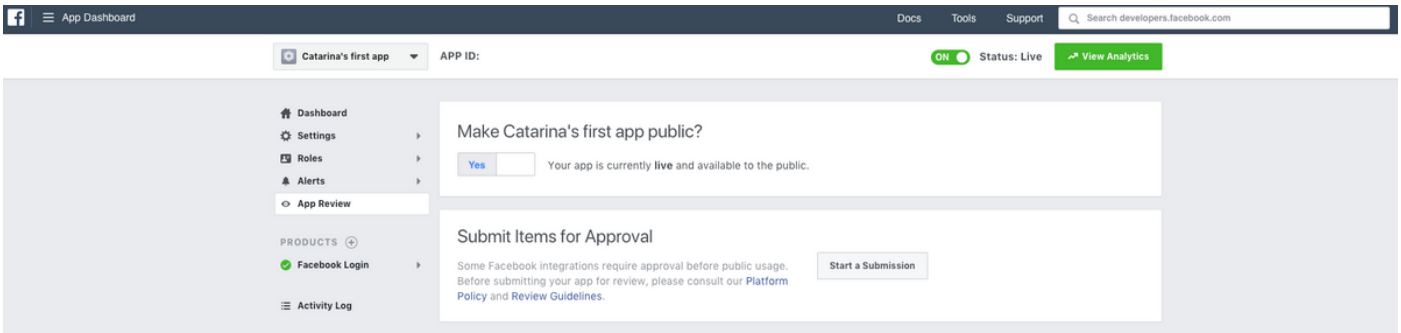
为了实现Facebook和CMX的集成，需要Facebook应用才能在两部分之间交换正确的令牌。

转到Facebook供开发人员创建应用。要集成这些服务，需要一些应用配置要求。

在“应用设置”中，确保已启用“客户端OAuth登录”和“Web OAuth登录”。此外，验证有效OAuth重定向URI，您的CMX URL为**https://<CMX-IP>/visitor/login**格式。



要发布应用并准备好与CMX集成，需要将其公开。为此，请转至“应用审阅” — >“使<应用名称>为公共”？并将状态更改为“是”。



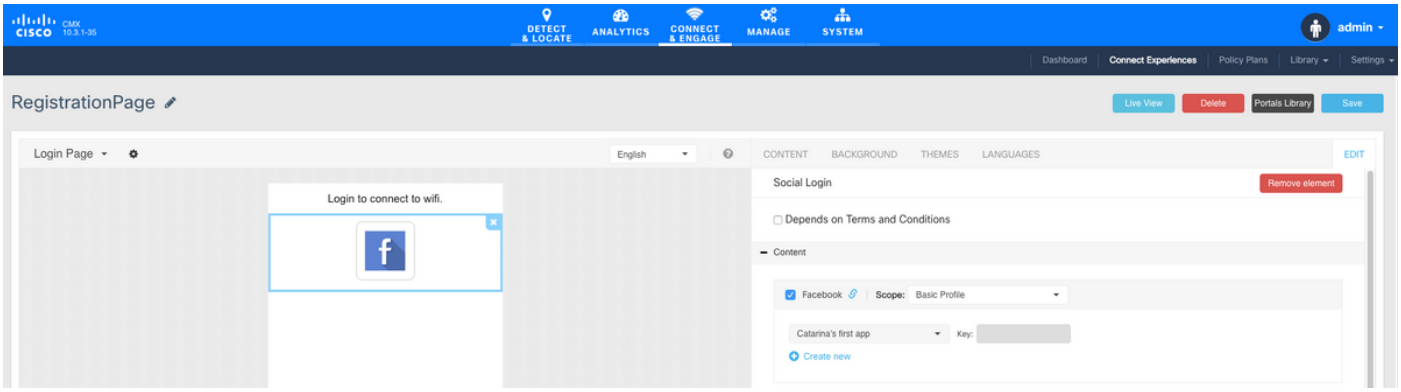
C. CMX配置

需要将控制器正确添加到CMX，以及从Prime基础设施导出的映射。

- 注册页面

要在CMX上创建注册页，应执行与之前创建SMS注册页相同的步骤。选择CONNECT&ENGAGE->库，可通过在下拉菜单中选择模板找到准备编辑的模板门户。

通过Facebook凭证注册要求门户具有社交帐户连接。要从头开始，在创建自定义门户时，请转至CONTENT->Common Elements->Social Auth，然后选择Facebook。然后插入从Facebook获取的应用名称和应用ID（密钥）。



通过自定义门户进行身份验证

使用自定义门户对客户端进行身份验证类似于配置外部Web身份验证。重定向将完成到CMX上托管的自定义门户。

A. WLC配置

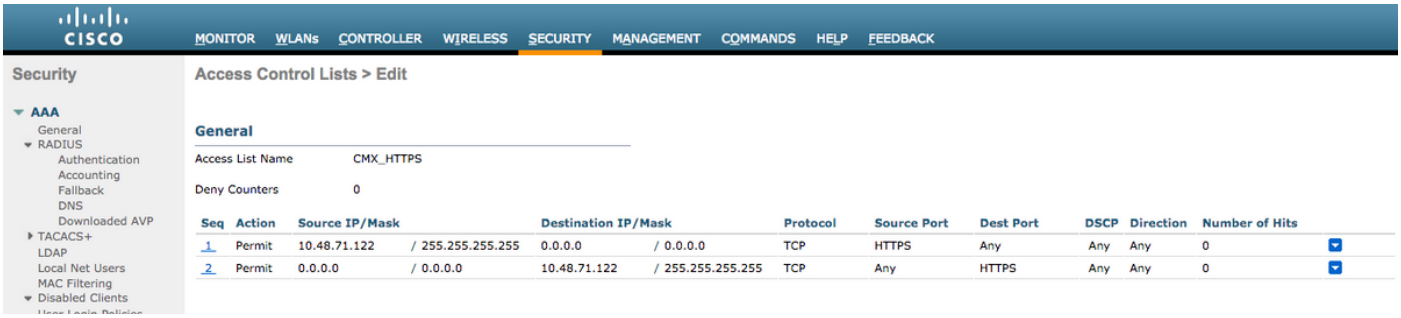
在WLC端，将同时配置SSID和ACL。AP应加入控制器并处于RUN状态。

1. ACL

正如我们使用HTTPS作为身份验证方法一样，必须在WLC上配置允许HTTPS流量的ACL。要配置ACL，请转至Security（安全）— > Access Control Lists（访问控制列表）— >Add New Rule（添加新规则）。

CMX IP必须用于允许WLC和CMX之间的HTTPS流量。（在本例中，CMX IP为10.48.71.122）。

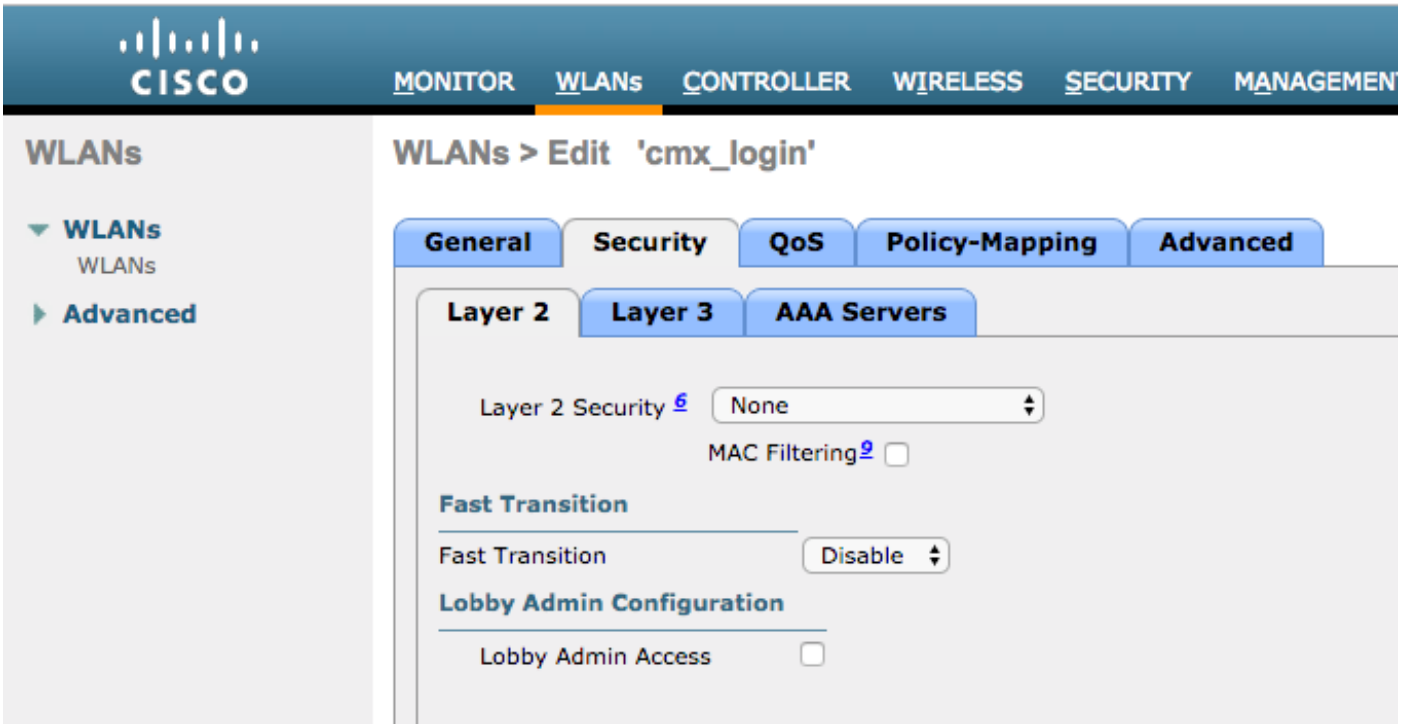
注意: **确保在CMX CLI上发出命令"cmxctl node sslmode enable"，在CMX上启用ssl。**

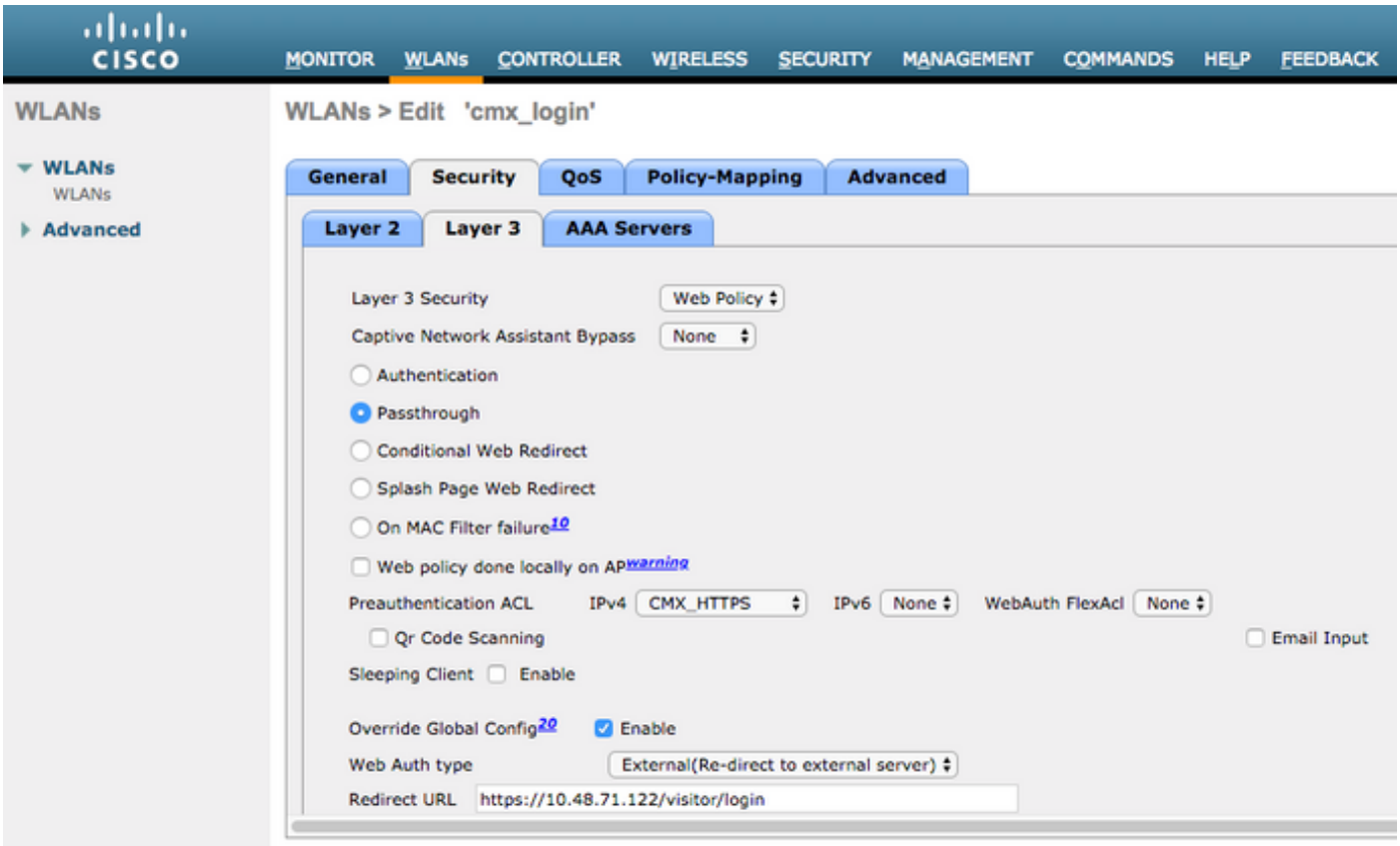


2. WLAN

安全策略会更改，以便注册生效，需要在WLAN上进行特定配置。

如之前对SMS和社交网络注册所做的那样，首先，转到WLANs->Edit->Layer 2->Layer 2 Security，然后在下拉列表中选择None，因此Layer 2 Security被禁用。在同一Security选项卡中，更改为Layer 3。在Layer 3 Security下拉菜单中，依次选择Web Policy和Passthrough。在预身份验证ACL中，选择之前配置的IPv4 ACL（本例中命名为CMX_HTTPS），并将其绑定到相应的WLAN。必须启用Over-ride Global Config（超载全局配置）选项，并且网络身份验证类型必须为External（重定向到外部服务器），因此客户端可以重定向到CMX服务。请注意，此时URL必须采用以下格式**https**://<CMX-IP>/visitor/login。





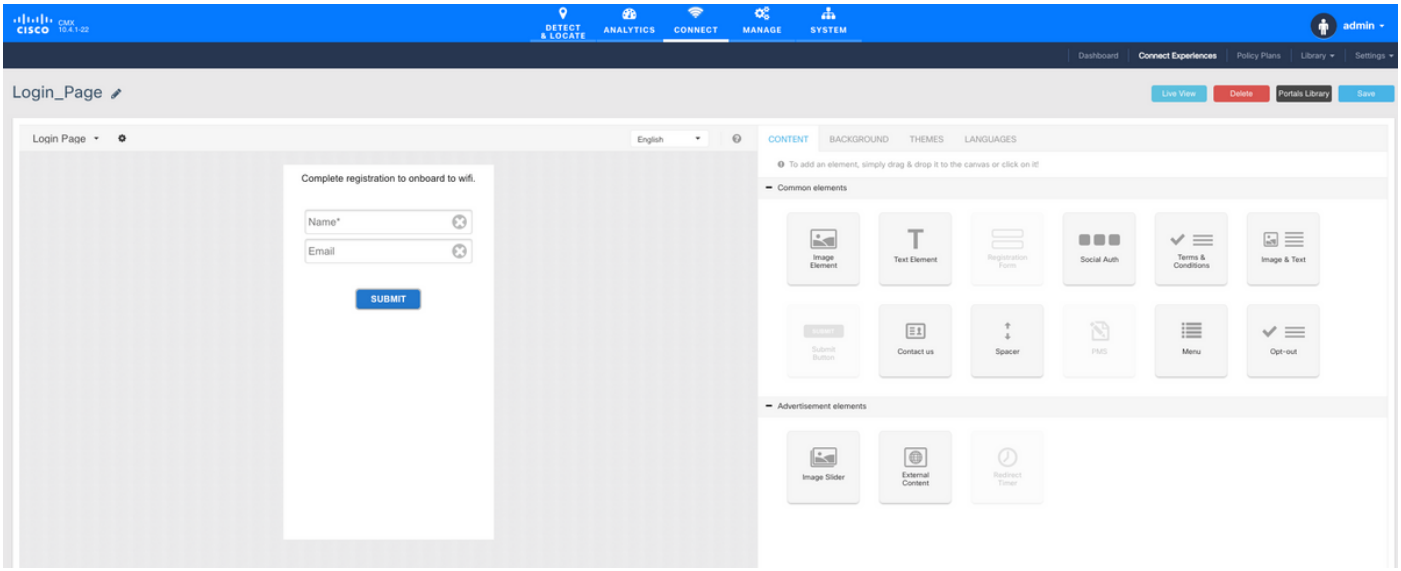
C. CMX配置

需要将控制器正确添加到CMX，以及从Prime基础设施导出的映射。

- 注册页面

要在CMX上创建注册页，所执行的步骤与之前为其他身份验证方法创建该页的步骤相同。选择CONNECT&ENGAGE->库，可通过在下拉菜单中选择模板找到准备编辑的模板门户。

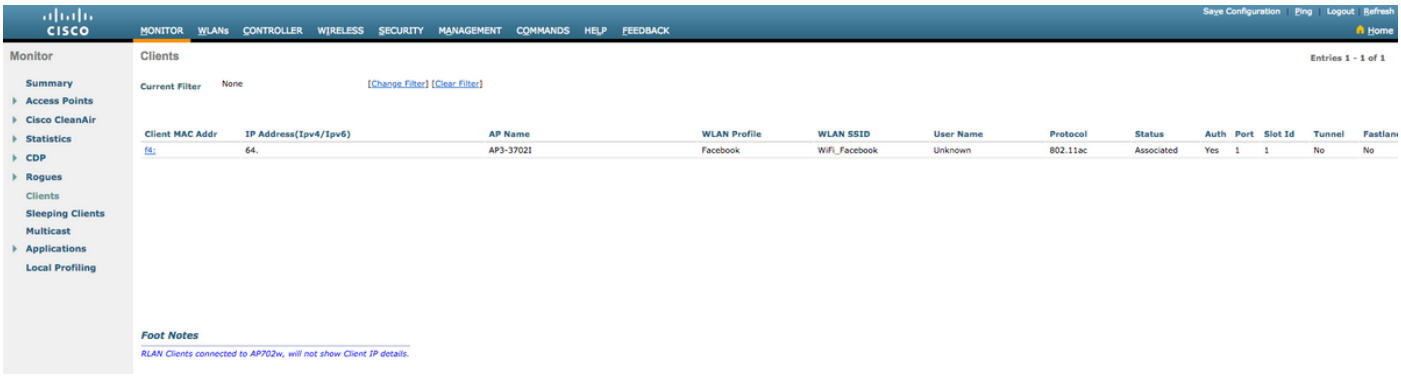
正常注册的门户可以从头开始（选择“自定义”）或从CMX库上提供的“注册表”模板进行修改。



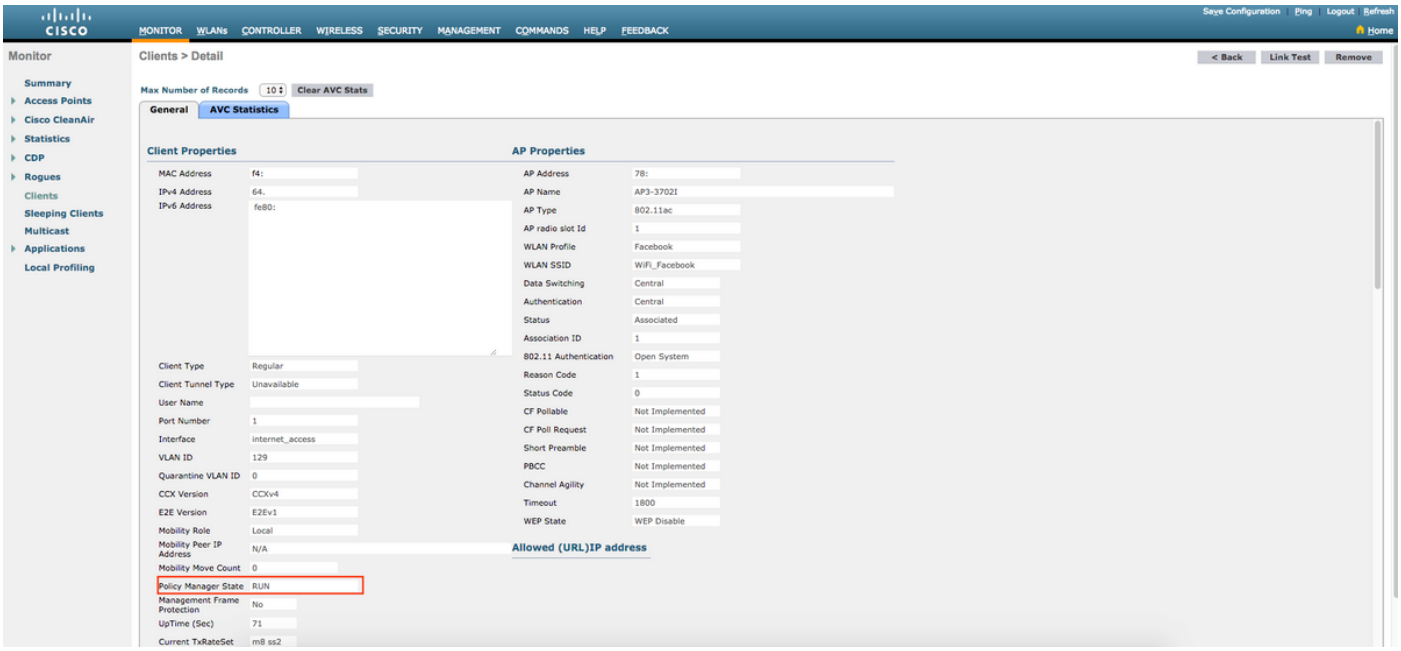
验证

WLC

要验证用户是否已在系统上成功通过身份验证，请在WLC GUI中，转到MONITOR->Clients并在列表中搜索客户端的MAC地址：

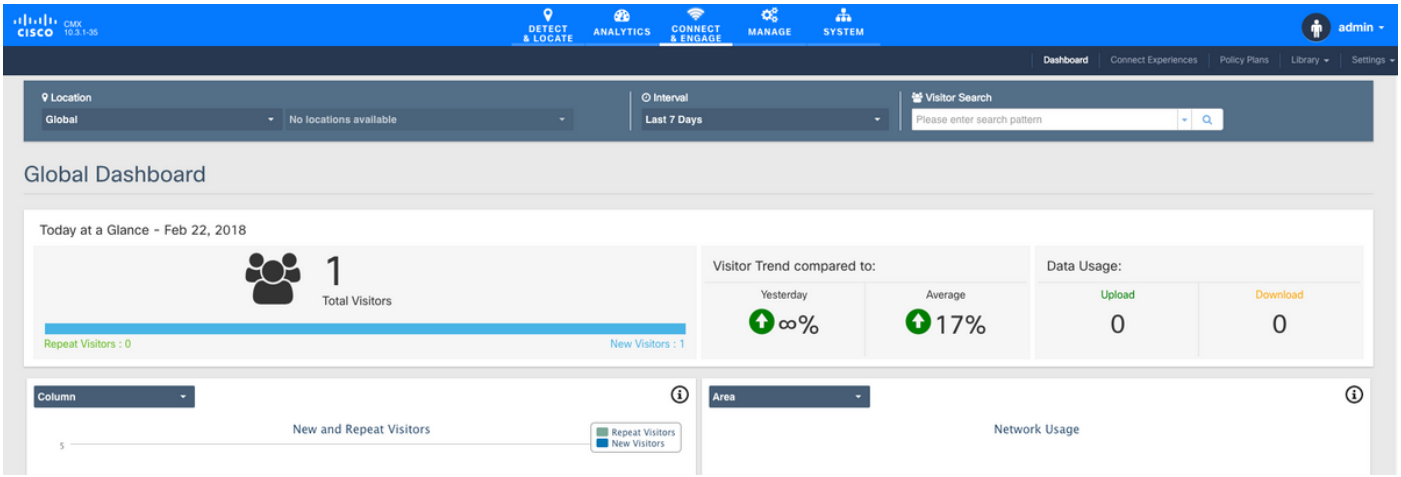


点击客户端的MAC地址，在详细信息中，确认客户端策略管理器状态处于RUN状态：

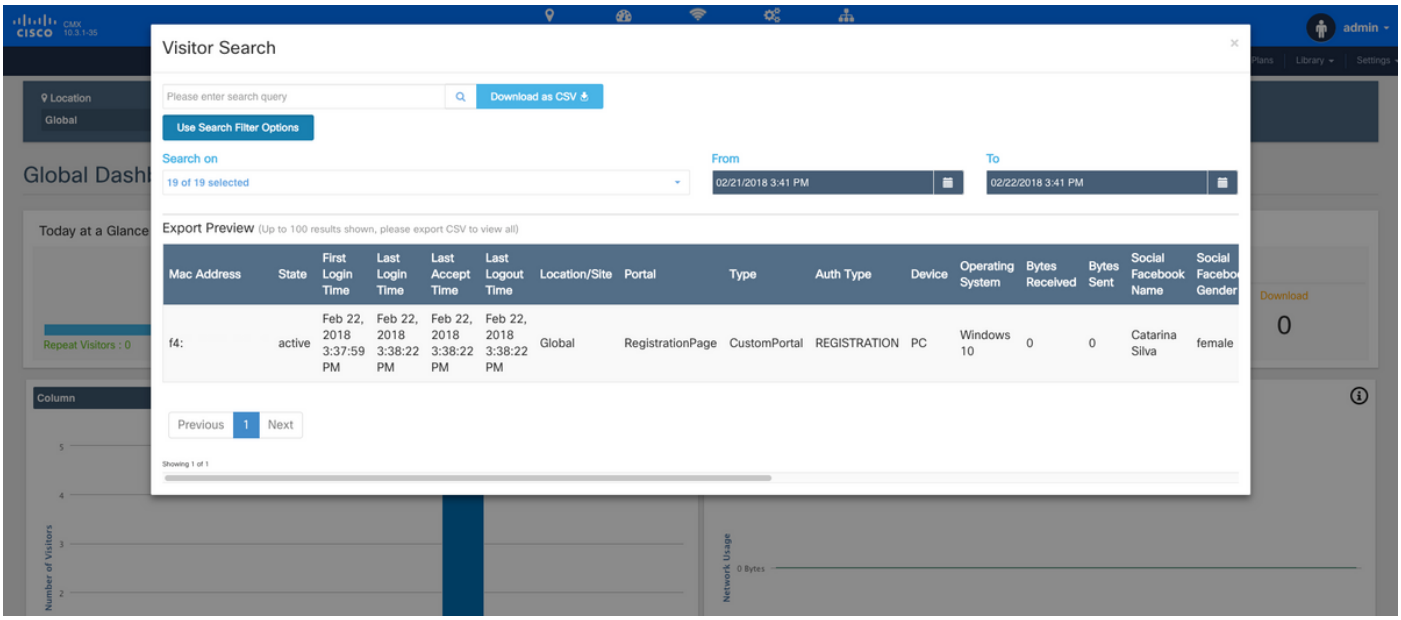


CMX

通过打开CONNECT&ENGAGE选项卡，可以验证CMX上有多少用户经过身份验证：



要检查用户详细信息，请在右上角的同一选项卡中点击Visitor Search:



故障排除

为了检查元素之间交互的流，可以在WLC中执行一些调试：

>debug client<MAC addr1> <MAC addr2>（输入一个或多个客户端的MAC地址）

>debug web-auth redirect enable mac <MAC addr>（输入web-auth客户端的MAC地址）

>debug web-auth webportal-server enable

>debug aaa all enable

此调试将允许进行故障排除，如果需要，可以使用某些数据包捕获来补充故障。