在使用ISE的WLC上使用FlexConnect AP配置CWA

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[配置](#)
[网络图](#)
[WLC 配置](#)
[ISE 配置](#)
[创建授权配置文件](#)
[创建身份验证规则](#)
[创建授权规则](#)
[启用IP续订（可选）](#)
[流量传输](#)
[验证](#)

简介

本文档介绍如何在本地交换模式下通过身份服务引擎(ISE)在无线局域网控制器(WLC)上使用FlexConnect接入点(AP)配置集中式Web身份验证。

重要注意：目前，此方案不支持FlexAP上的本地身份验证。

本系列中的其他文档

- 使用交换机和身份服务引擎进行集中Web身份验证的配置示例
- WLC 和 ISE 上的集中式 Web 身份验证配置示例

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科身份服务引擎(ISE)，版本1.2.1
- 无线LAN控制器软件版本 — 7.4.100.0

配置

在无线局域网控制器(WLC)上配置集中式Web身份验证的方法有多种。第一种方法是本地Web身份验证，其中WLC将HTTP流量重定向到内部或外部服务器，提示用户进行身份验证。然后，WLC获取凭证（如果是外部服务器，则通过HTTP GET请求发送回）并进行RADIUS身份验证。对于访客用户，需要外部服务器(例如身份服务引擎(ISE)或NAC访客服务器(NGS))，因为门户提供设备注册和自助调配等功能。此过程包括以下步骤：

1. 用户与Web身份验证SSID关联。
2. 用户打开其浏览器。
3. 一旦输入URL，WLC会重定向到访客门户（例如ISE或NGS）。
4. 用户在门户上进行身份验证。
5. 访客门户使用输入的凭证重定向回WLC。
6. WLC通过RADIUS对访客用户进行身份验证。
7. WLC重定向回原始URL。

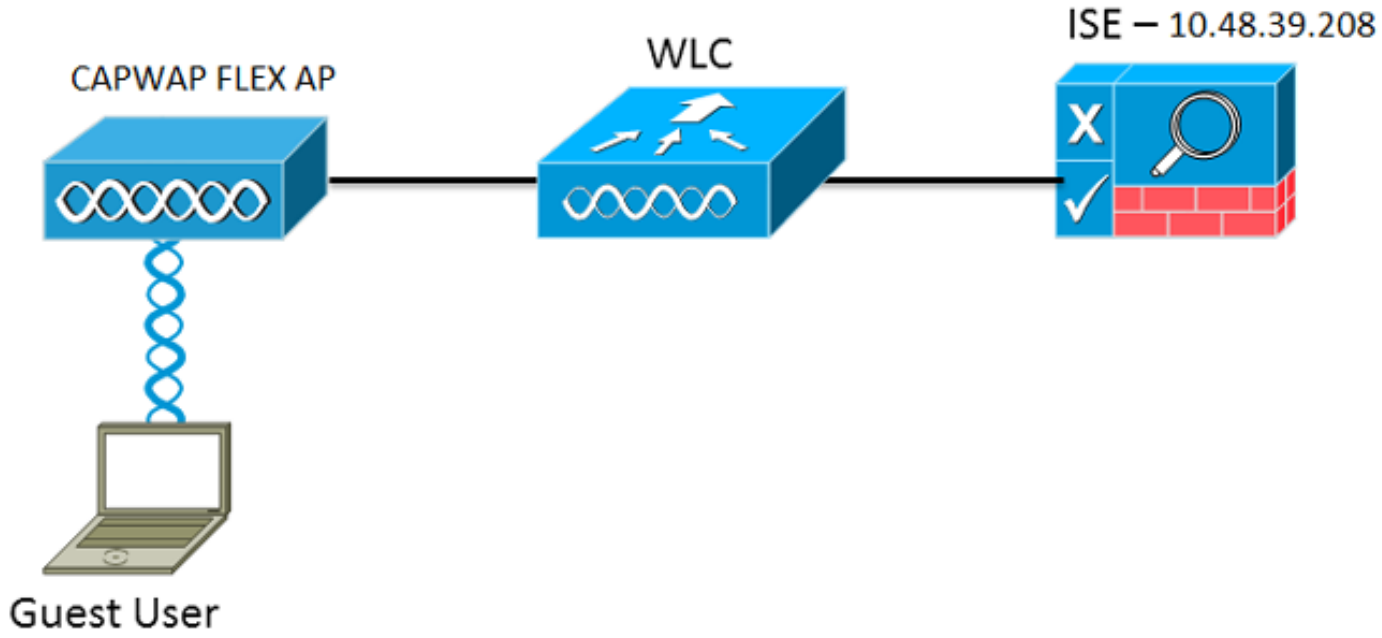
此过程包括许多重定向。新的方法是使用集中式Web身份验证，该身份验证可与ISE（1.1版之后的版本）和WLC（7.2版之后的版本）配合使用。此过程包括以下步骤：

1. 用户与Web身份验证SSID关联。
2. 用户打开其浏览器。
3. WLC重定向到访客门户。
4. 用户在门户上进行身份验证。
5. ISE发送RADIUS授权更改（CoA - UDP端口1700）向控制器指示用户有效，并最终推送RADIUS属性，如访问控制列表(ACL)。
6. 系统将提示用户重试原始URL。

本节介绍在WLC和ISE上配置集中式Web身份验证的必要步骤。

网络图

此配置使用以下网络设置：

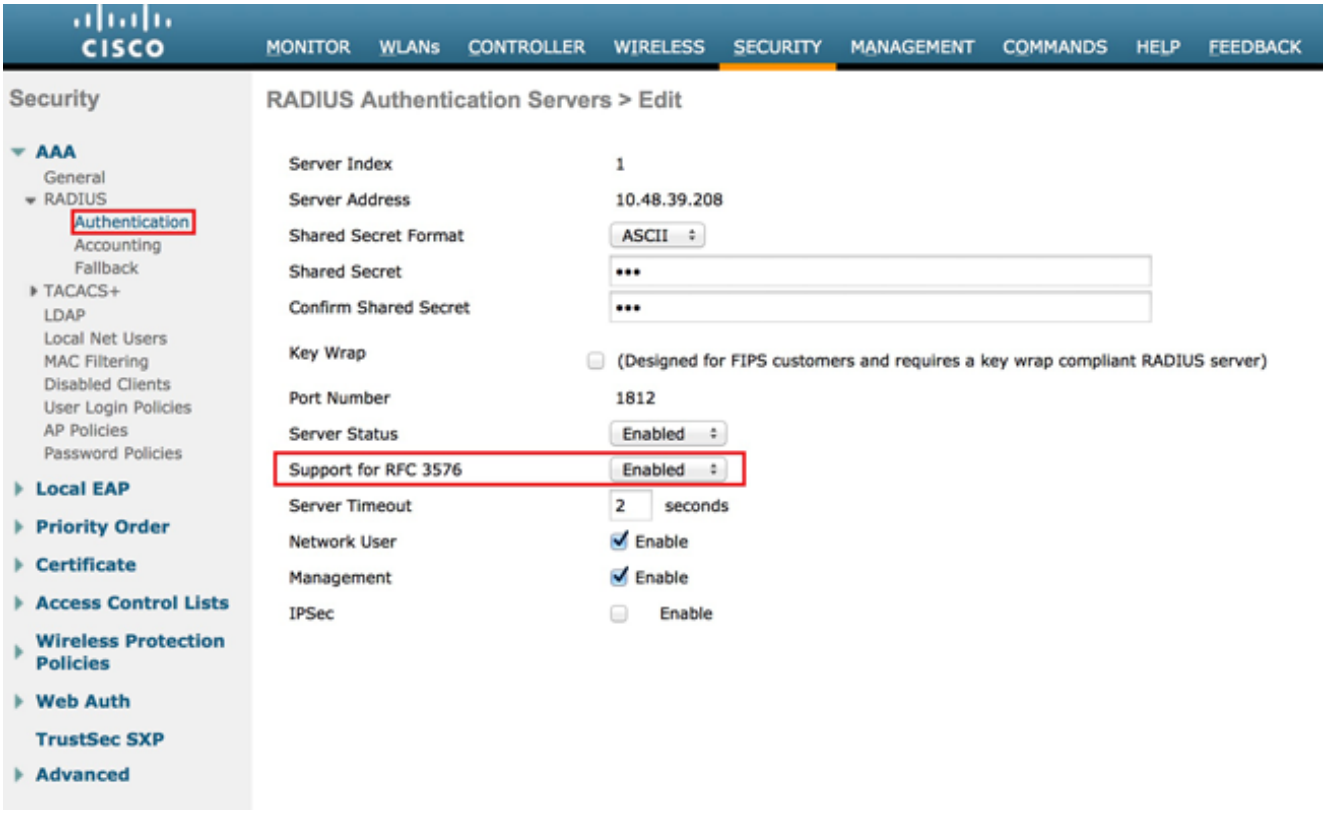


WLC 配置

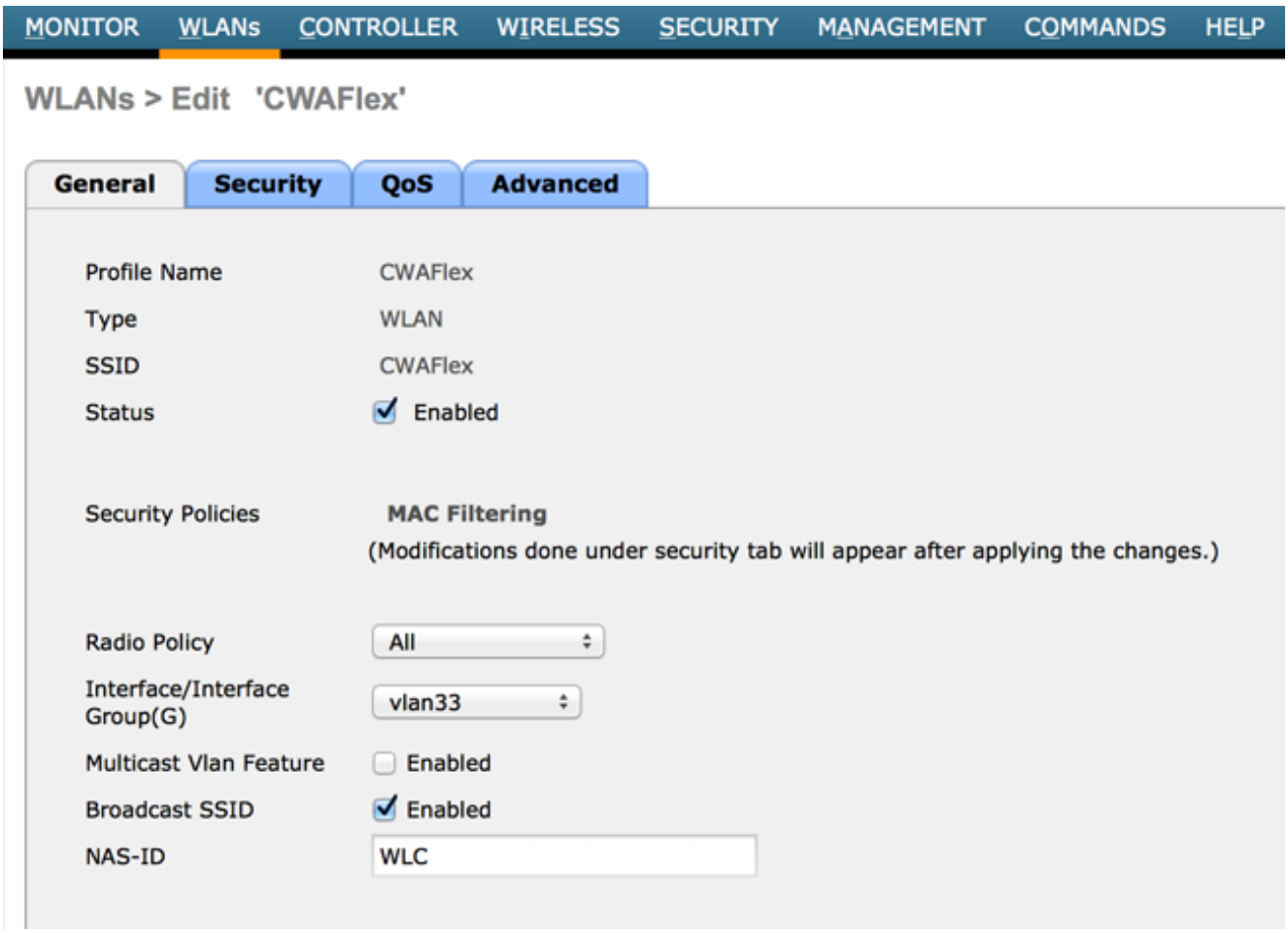
WLC配置非常简单。使用“技巧”（与交换机相同）从ISE获取动态身份验证URL。（由于它使用CoA，因此需要创建会话，因为会话ID是URL的一部分。）SSID配置为使用MAC过滤，并且ISE配置为返回Access-Accept消息，即使MAC地址未找到，它也会为所有用户发送重定向URL。

此外，必须启用RADIUS网络准入控制(NAC)和AAA覆盖。RADIUS NAC允许ISE发送CoA请求，指示用户现在已通过身份验证且能够访问网络。它还用于状态评估，其中ISE根据状态结果更改用户配置文件。

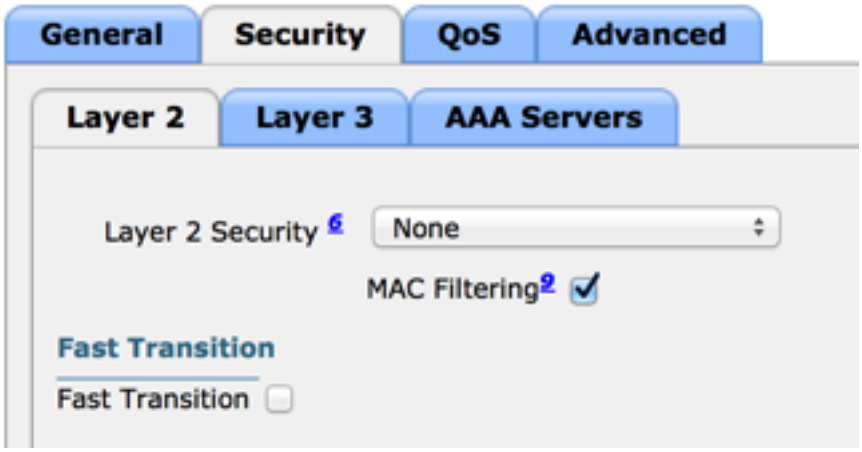
1. 确保RADIUS服务器启用了RFC3576(CoA)，这是默认设置。



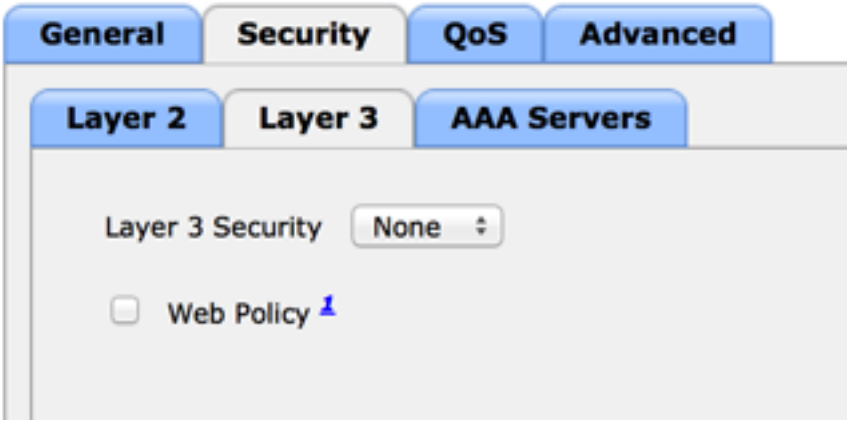
2. 创建新的WLAN。本示例创建一个名为*CWAFlex*的新WLAN，并将其分配给vlan33。（请注意，由于接入点处于本地交换模式，因此它不会产生太大影响。）



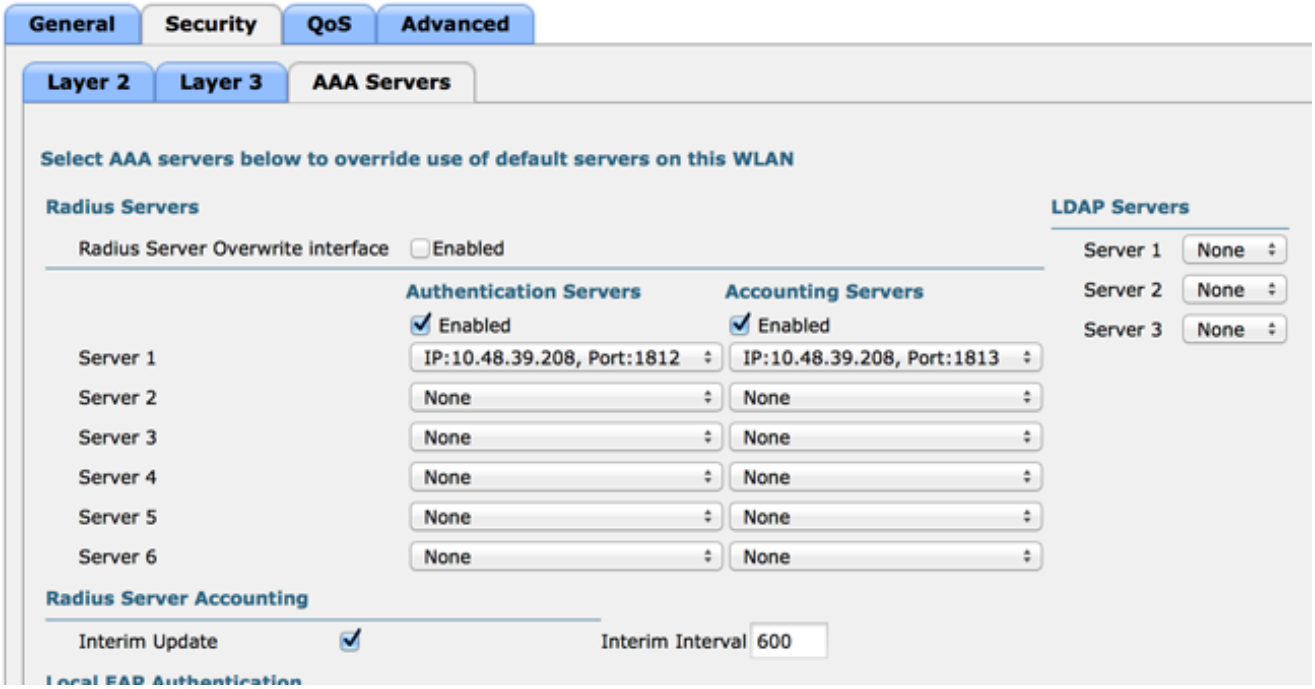
3. 在Security选项卡上，启用MAC Filtering as Layer 2 Security。



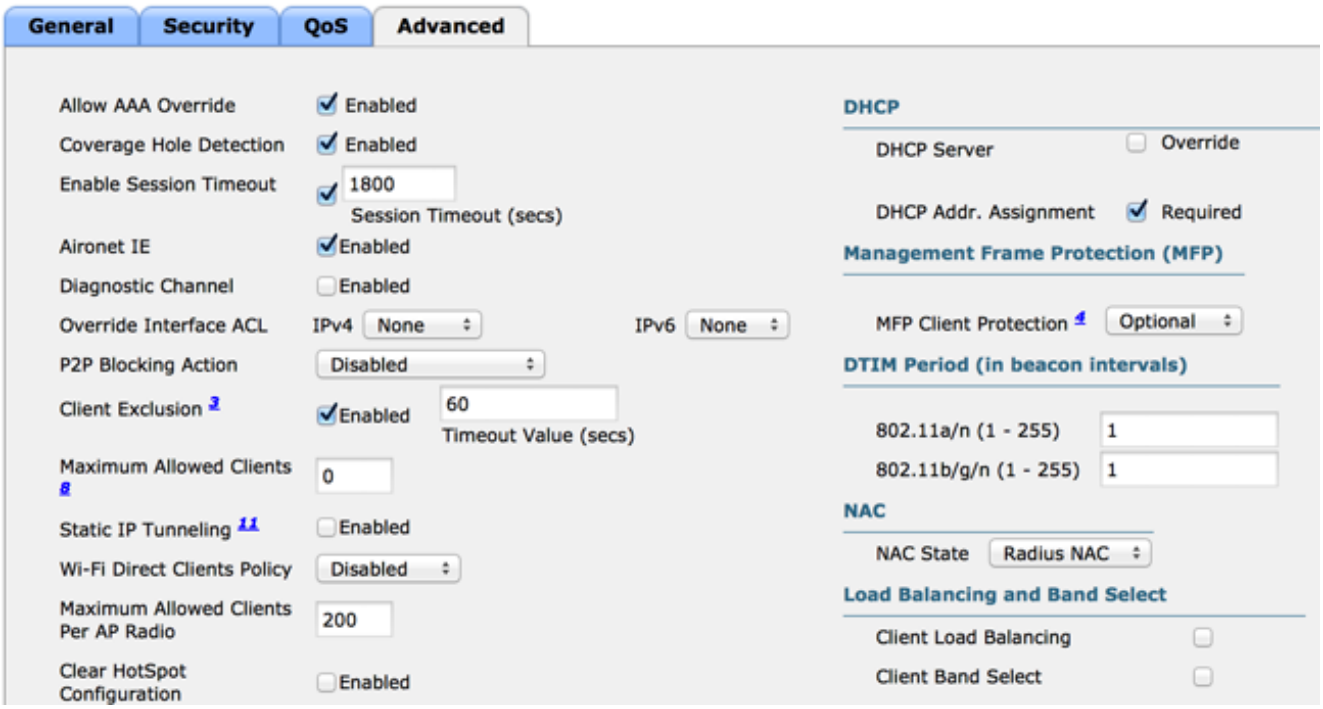
4. 在第3层选项卡上，确保已禁用安全性。（如果在第3层启用Web身份验证，则启用本地Web身份验证，而不是集中式Web身份验证。）



5. 在AAA Servers选项卡上，选择ISE服务器作为WLAN的radius服务器。或者，您可以选择它进行记帐，以便获得有关ISE的更多详细信息。

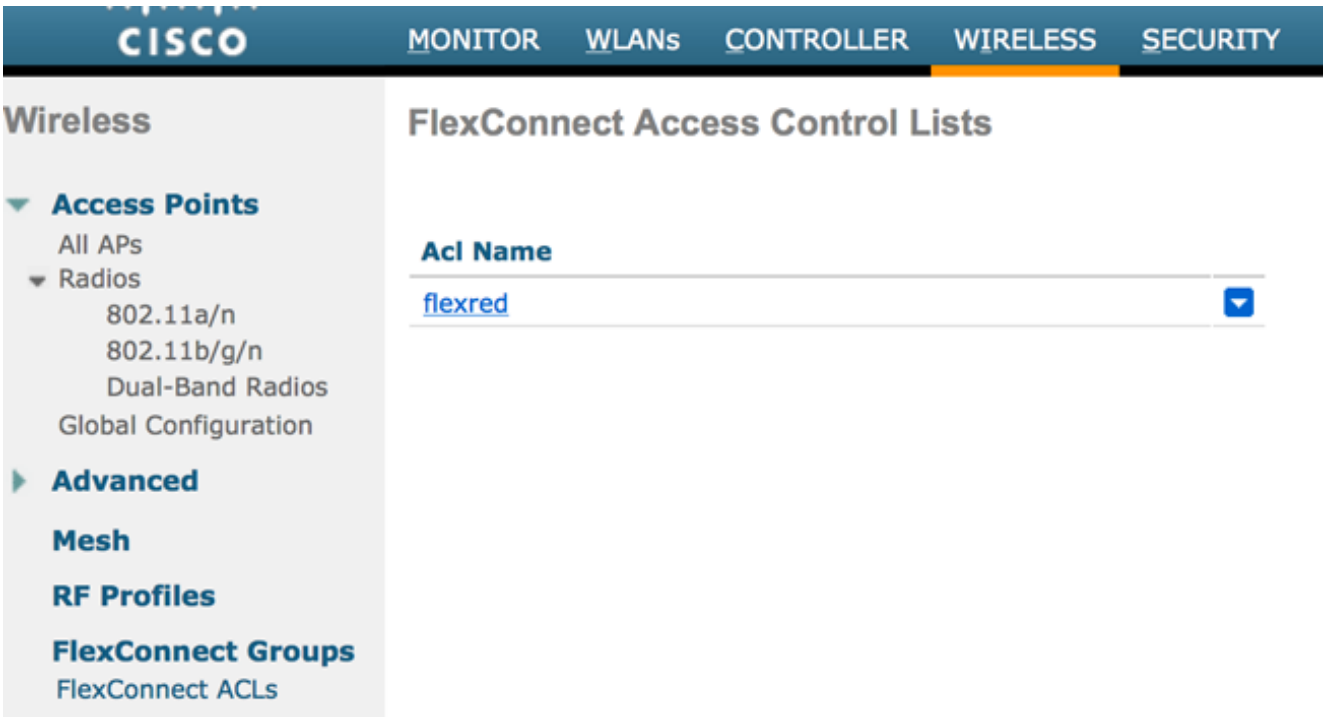


6. 在Advanced选项卡上，确保选中Allow AAA Override并为NAC State选择Radius NAC。

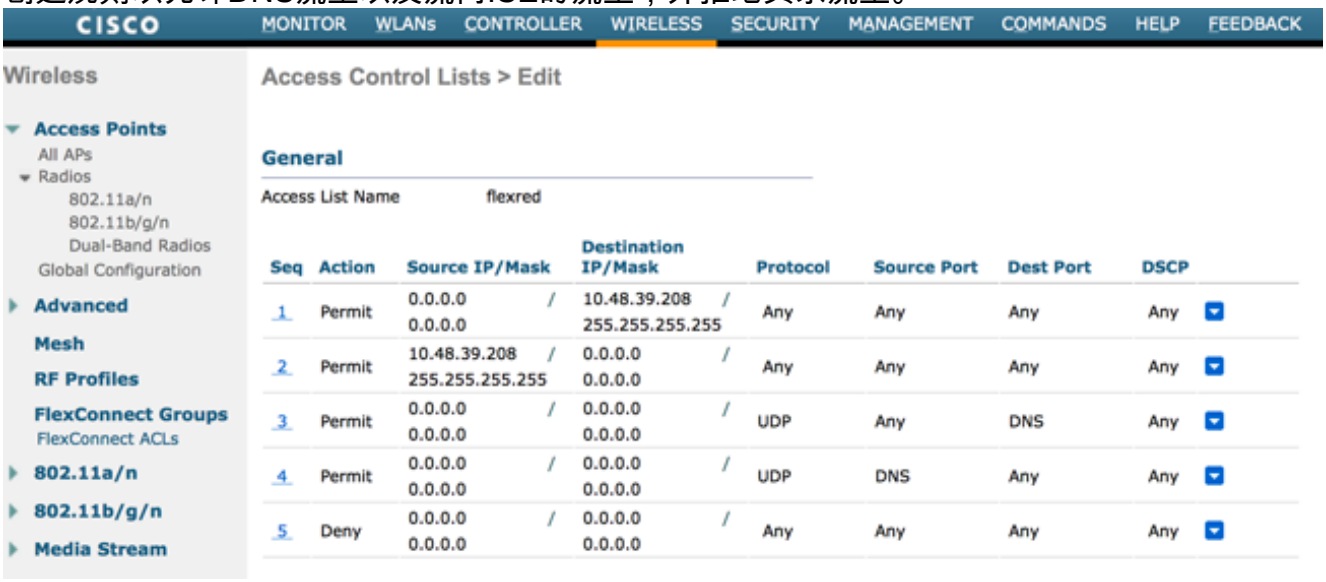


7. 创建重定向ACL。

此ACL在ISE的Access-Accept消息中引用，并定义哪些流量应重定向（被ACL拒绝）以及哪些流量不应重定向（被ACL允许）。基本上，需要允许DNS和流入/流出ISE的流量。 **注**:FlexConnect AP的问题是您必须创建独立于正常ACL的FlexConnect ACL。此问题记录在Cisco Bug CSCue68065中，并在版本7.5中得到修复。在WLC 7.5及更高版本中，仅需要FlexACL，不需要标准ACL。WLC期望ISE返回的重定向ACL是正常ACL。但是，要确保它正常工作，您需要应用与FlexConnect ACL相同的ACL。
此示例显示如何创建名为flexred的*FlexConnect* ACL:

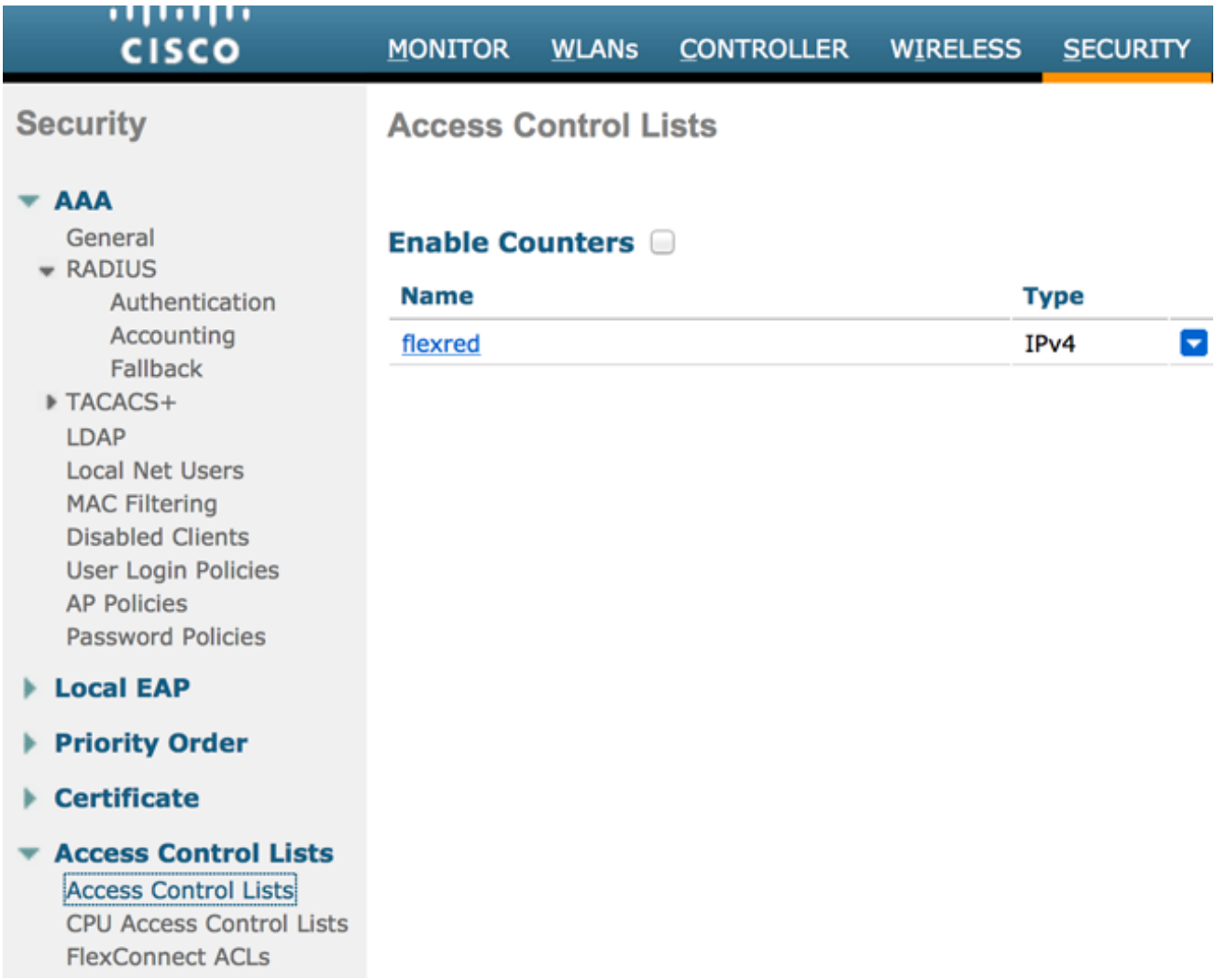


创建规则以允许DNS流量以及流向ISE的流量，并拒绝其余流量。



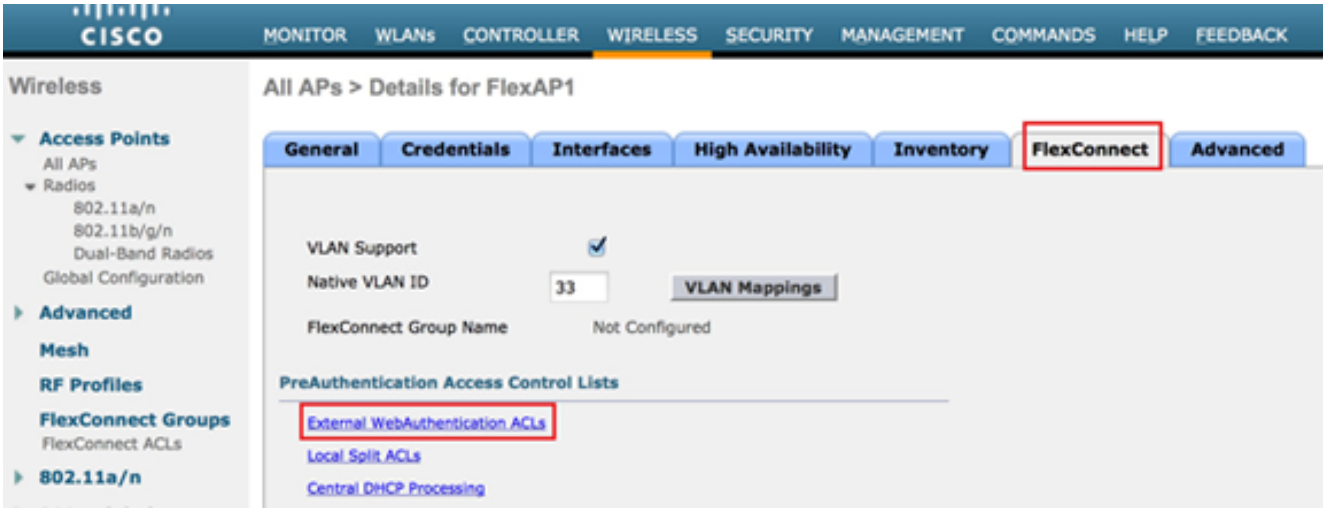
如果您希望获得最高安全性，则只能允许端口8443到达ISE。（如果进行安全评估，必须添加典型的安全评估端口，例如8905、8906、8909、8910。）

(由于CSCue68065，仅限于7.5版之前的代码)选择**Security > Access Control Lists**以创建具有相同名称的相同ACL。

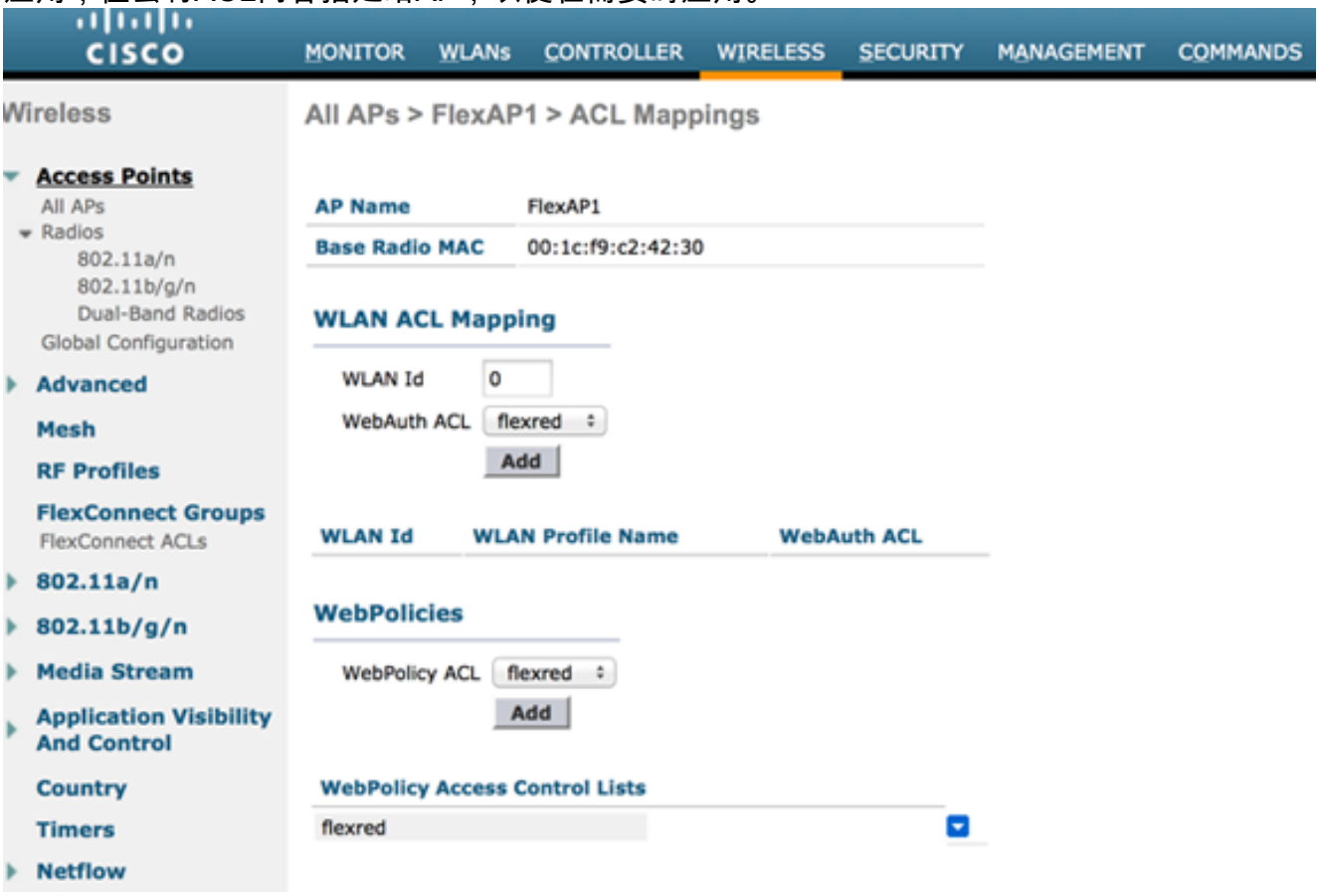


准备特定FlexConnect AP。请注意，对于较大的部署，通常使用FlexConnect组，出于可扩展性原因，不会逐个AP执行这些项目。

单击**Wireless**，然后选择特定的接入点。单击**FlexConnect**选项卡，然后单击**External Webauthentication ACLs**。(在7.4版之前，此选项被命名为*web policies*。)



将ACL(在本示例中名为*flexred*)添加到Web策略区域。这会将ACL预先推送到接入点。它尚未应用，但会将ACL内容指定给AP，以便在需要时应用。



WLC配置现已完成。

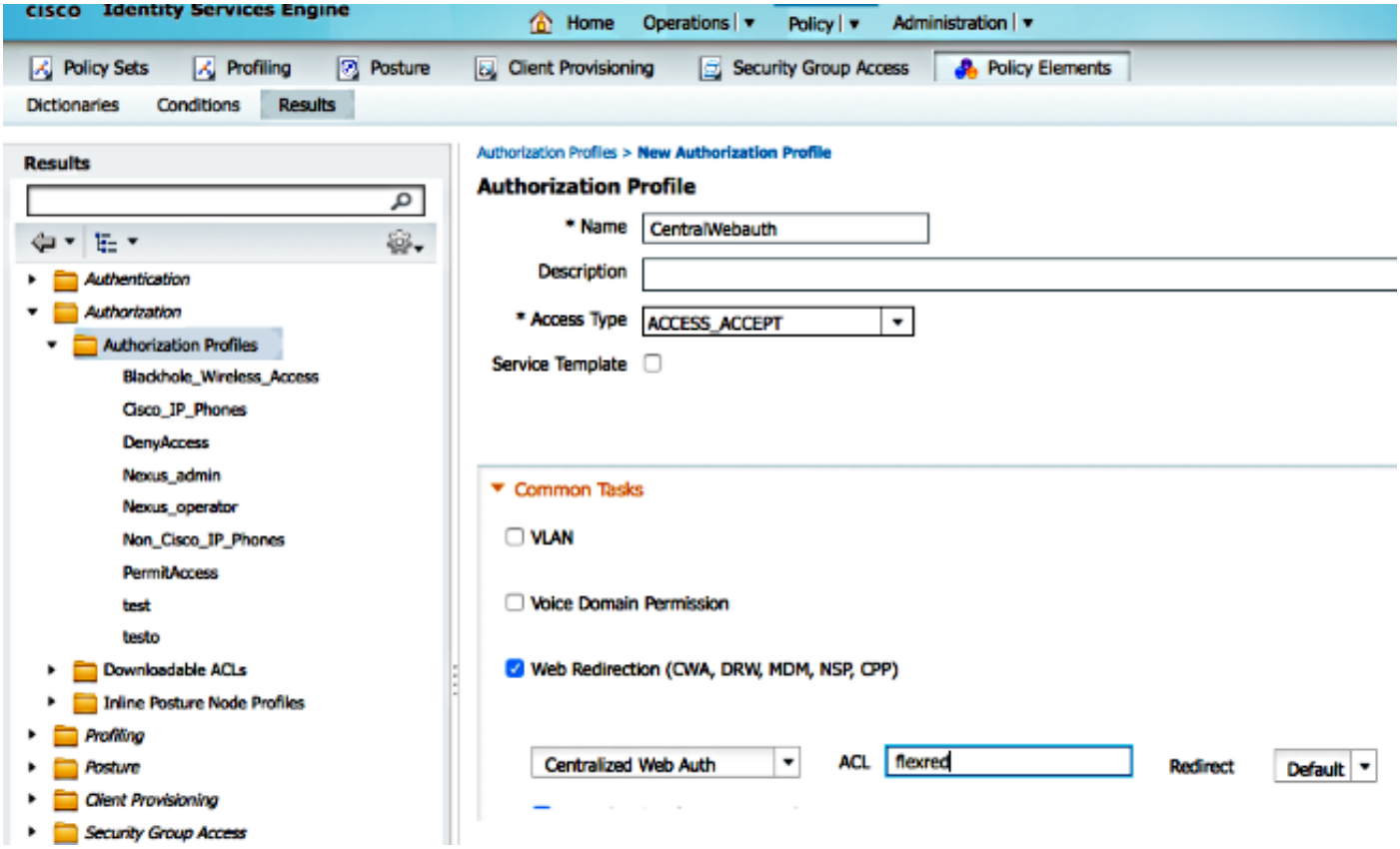
ISE 配置

创建授权配置文件

完成以下步骤以创建授权配置文件：

1. 单击**Policy**，然后单击**Policy Elements**。
2. 单击**Results**。
3. 展开**Authorization**，然后单击**Authorization profile**。
4. 单击**Add**按钮为集中Webauth创建新的授权配置文件。
5. 在**名称**字段中，输入配置文件的名称。本示例使用*CentralWebauth*。
6. 从Access Type下拉列表中选择**ACCESS_ACCEPT**。
7. 选中**Web Authentication**复选框，然后从下拉列表中选择**Centralized Web Auth**。
8. 在ACL字段中，输入WLC上用于定义将被重定向的流量的ACL名称。本示例使用*flexred*。
9. 从Redirect下拉列表中选择**Default**。

Redirect属性定义ISE看到默认Web门户还是ISE管理员创建的自定义Web门户。例如，本示例中的*flexred* ACL会触发从客户端到任何位置的HTTP流量重定向。



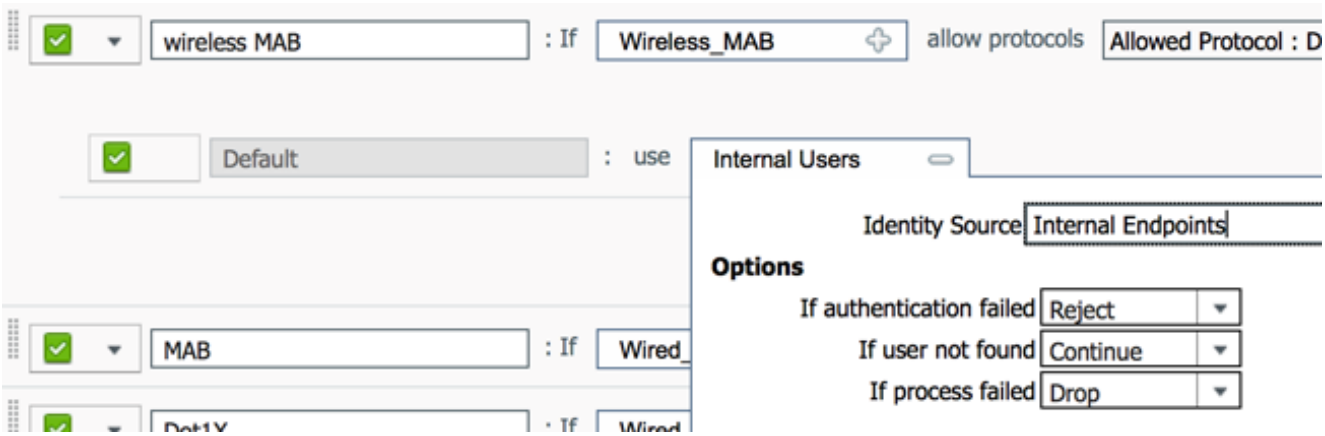
创建身份验证规则

完成以下步骤以使用身份验证配置文件创建身份验证规则：

1. 在Policy菜单下，单击**Authentication**。 下图显示如何配置身份验证策略规则的示例。在本示例中，配置了一个规则，当检测到MAC过滤时将触发该规则。



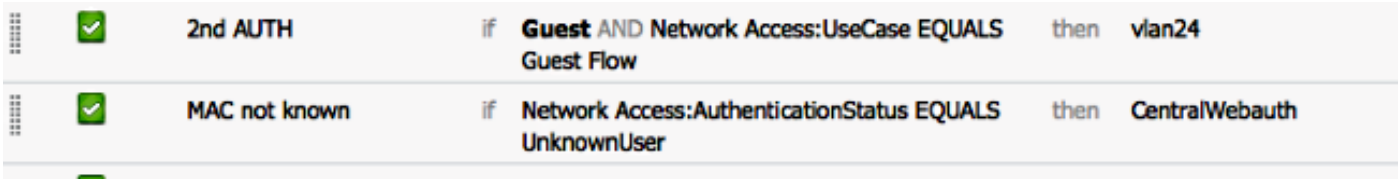
2. 输入身份验证规则的名称。本示例使用*Wireless mab*。
3. 在If条件字**段中**选择加号(+)图标。
4. 选择**Compound condition**，然后选择**Wireless_MAB**。
5. 选择“默认网络访问”作为允许的协议。
6. 单击位于**和……**旁边的箭头以进一步展开规则。
7. 点击Identity Source字段中的**+图标，然后选择Internal endpoints**。
8. 从If user not found下拉列表中选择**Continue**。



此选项允许对设备进行身份验证（通过webauth），即使其MAC地址未知。Dot1x客户端仍然可以使用其凭证进行身份验证，因此不应关注此配置。

创建授权规则

现在，在授权策略中有几个规则需要配置。当PC关联时，它将通过mac过滤；假设MAC地址未知，因此会返回webauth和ACL。此*MAC未知*规则显示在下图中，并且在此部分中进行配置。



要创建授权规则，请完成以下步骤：

1. 创建新规则，然后输入名称。本示例使用*未知的MAC*。
2. 点击条件字段**中**的加号(+)图标，然后选择创建新条件。
3. 展开**表达式**下拉列表。
4. 选择**Network access**，然后展开它。
5. 单击**AuthenticationStatus**，然后选择**Equals**运算符。

6. 在右侧字段中选择**UnknownUser**。
7. 在General Authorization页面上，然后在单词右侧的字段中选择**CentralWebauth**(Authorization Profile)。此步骤允许ISE继续，即使用户（或MAC）未知。现在，系统向未知用户显示“登录”页面。但是，一旦他们输入其凭证，他们就会再次在ISE上收到身份验证请求；因此，如果用户是访客用户，则必须使用满足的条件配置另一个规则。在本示例中，如果使用*UseridentityGroup equals Guest*，并且假定所有访客都属于此组。
8. 点击MAC未知规则末尾的actions按*钮，然*后选择在上方插入新规则。**注意：**此新规则必须出现在MAC未知规*则之前，很*重要。
9. 在名称字段中输入**第2次AUTH**。
10. 选择身份组作为条件。本示例选择**Guest**。
11. 在条件字段中，点击加号**(+)**图标，然后选择创建新条件。
12. 选择**网络访问**，然后单击**使用案例**。
13. 选择**Equals**作为运算符。
14. 选择**GuestFlow**作为正确的操作数。这意味着您将捕获刚刚登录该网页的用户，并在授权更改（规则的访客流部分）后返回该网页，并且仅当这些用户属于访客身份组时。
15. 在授权页面上，点击加号(+)图标(位于*then*旁)以选择规则的结果。

    在本例中，已分配预配置的配置文件(vlan34)；本文档中未显示此配置。

    您可以选择**Permit Access**选项或创建自定义配置文件以返回您喜欢的VLAN或属性。

重要注意：在ISE版本1.3中，根据网络身份验证的类型，“访客流”使用案例可能不再出现。然后，授权规则必须包含访客用户组作为唯一可能的条件。

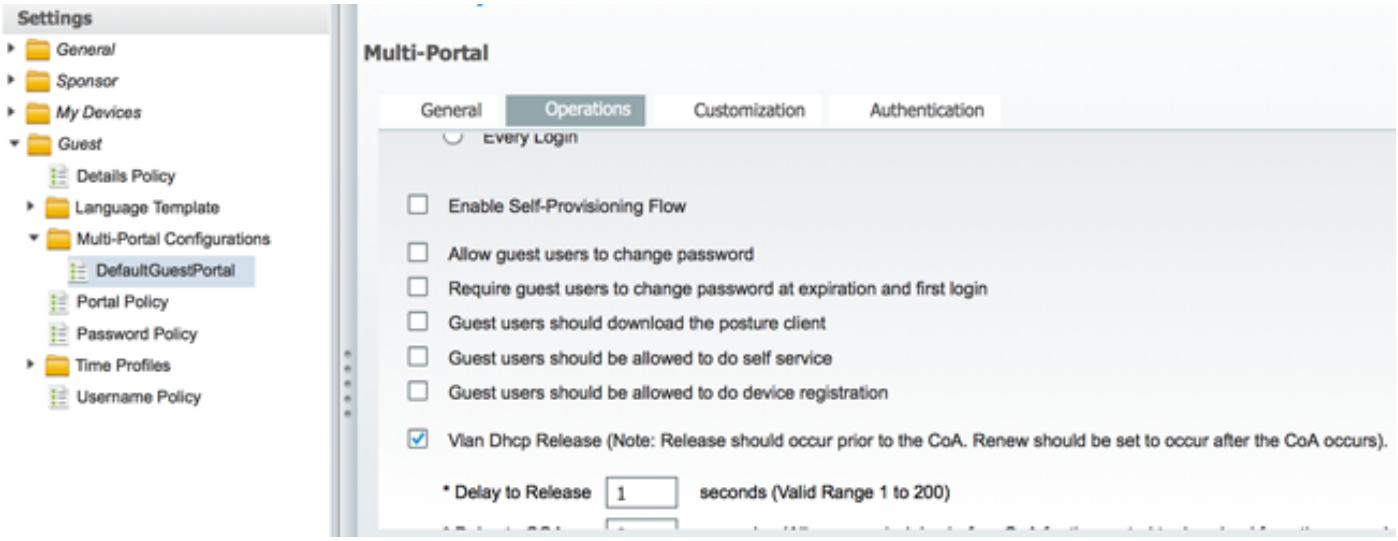
启用IP续订（可选）

如果分配VLAN，最后一步是客户端PC更新其IP地址。此步骤由Windows客户端的访客门户实现。如果之前没有为第2个AUTH规*则设置*VLAN，则可以跳过此步骤。

请注意，在FlexConnect AP上，VLAN需要预先存在于AP上。因此，如果没有，您可以在AP本身或您不为要创建的新VLAN应用任何ACL的flex组上创建VLAN-ACL映射。实际上会创建VLAN（没有ACL）。

如果分配了VLAN，请完成以下步骤以启用IP续订：

1. 单击**Administration**，然后单击**Guest Management**。
2. 单击**设置**。
3. 展开**Guest**，然后展开**Multi-Portal Configuration**。
4. 单击**DefaultGuestPortal**或您可能已创建的自定义门户的名称。
5. 单击**Vlan DHCP Release**复选框。**注意：**此选项仅适用于Windows客户端。



流量传输

在此场景中，可能很难理解将哪些流量发送到何处。下面是快速回顾：

- 客户端通过无线发送针对SSID的关联请求。
- WLC使用ISE（接收重定向属性）处理MAC过滤身份验证。
- 客户端只在MAC过滤完成后收到关联响应。
- 客户端提交DHCP请求，即 **本地** 由接入点交换，以获得远程站点的IP地址。
- 在Central_webauth状态下，重定向ACL（因此通常为HTTP）上标记为拒绝的流量为 **集中** 交换。因此，执行重定向的不是AP，而是WLC；例如，当客户端请求任何网站时，AP会将此消息发送到CAPWAP中封装的WLC，WLC则欺骗该网站IP地址并重定向到ISE。
- 客户端被重定向到ISE重定向URL。这是 **本地** 再次交换（因为它在flex redirect ACL上命中permit）。
- 一旦进入RUN状态，流量将在本地交换。

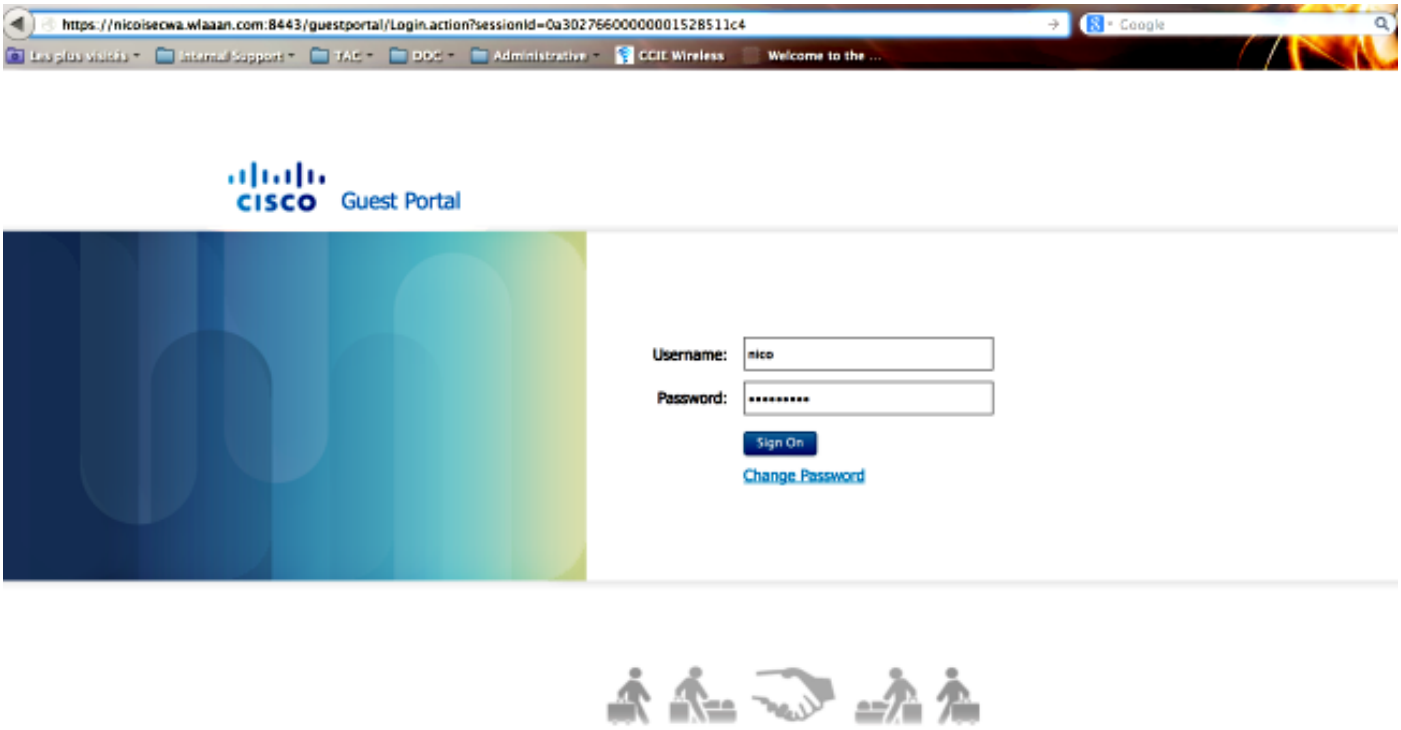
验证

用户与SSID关联后，授权将显示在ISE页面。

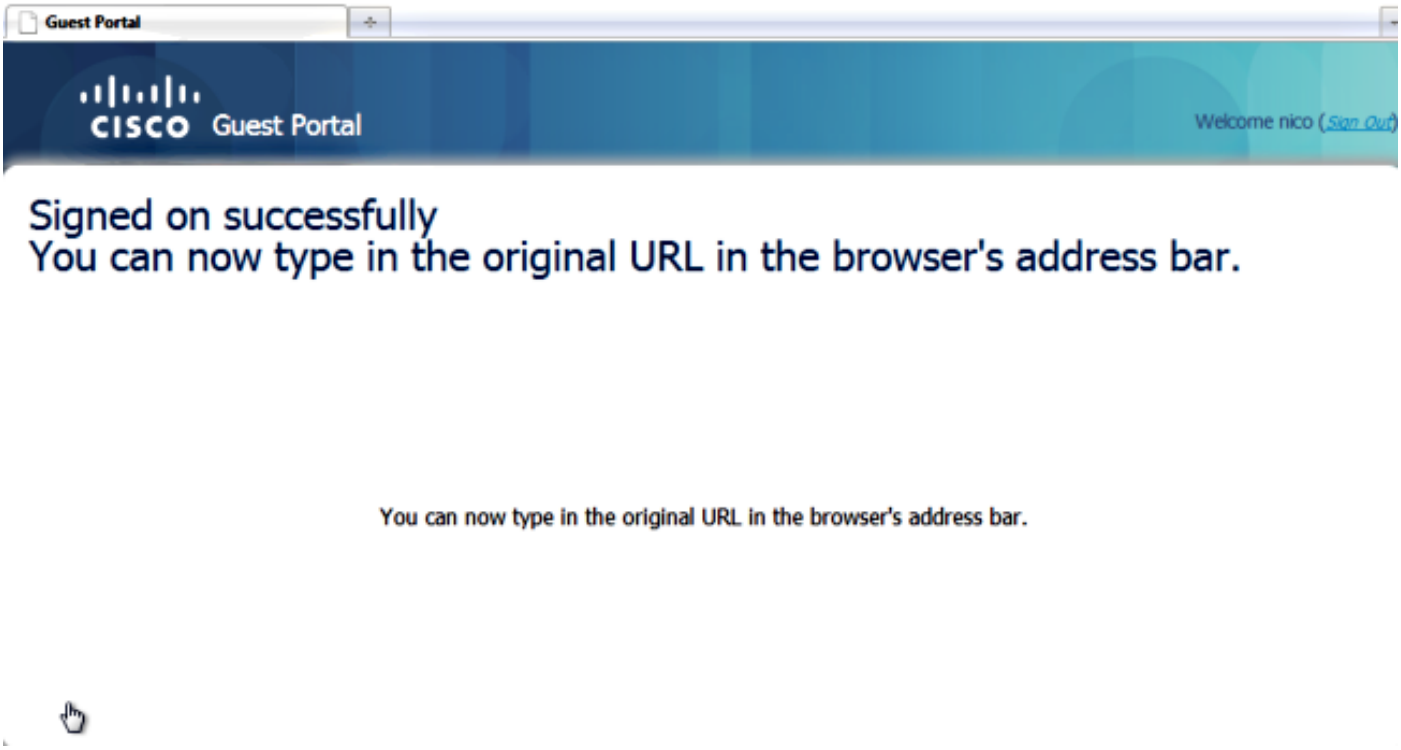
Apr 09,13 11:49:27.179 AM	✓		Nico	00:13:10:21:70:13	nicowlc	vlan34	Guest	NotApplicable	
Apr 09,13 11:49:27.174 AM	✓				nicowlc				Dynamic Author...
Apr 09,13 11:48:58.372 AM	✓		Nico	00:13:10:21:70:13			Guest		Guest Authentic..
Apr 09,13 11:47:19.475 AM	✓		00:13:10:21:70:13	00:13:10:21:70:13	nicowlc	CentralWebauth		Pending	Authentication ...

从下到上，您可以看到返回CWA属性的MAC地址过滤身份验证。接下来是使用用户名的门户登录。然后，ISE向WLC发送CoA，最后身份验证是WLC端的第2层mac过滤身份验证，但ISE记住客户端和用户名并应用我们在本示例中配置的必要VLAN。

当在客户端上打开任何地址时，浏览器将重定向到ISE。确保域名系统(DNS)配置正确。



在用户接受策略后授予网络访问权限。



在控制器上，策略管理器状态和RADIUS NAC状态从*POSTURE_REQD*更改为*RUN*。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。