在使用ISE的WLC上配置使用FlexConnect AP的CWA

目录

简介

本文档介绍如何在WLC ISE上以本地交换模式配置FlexConnect AP的集中Web身份验证。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

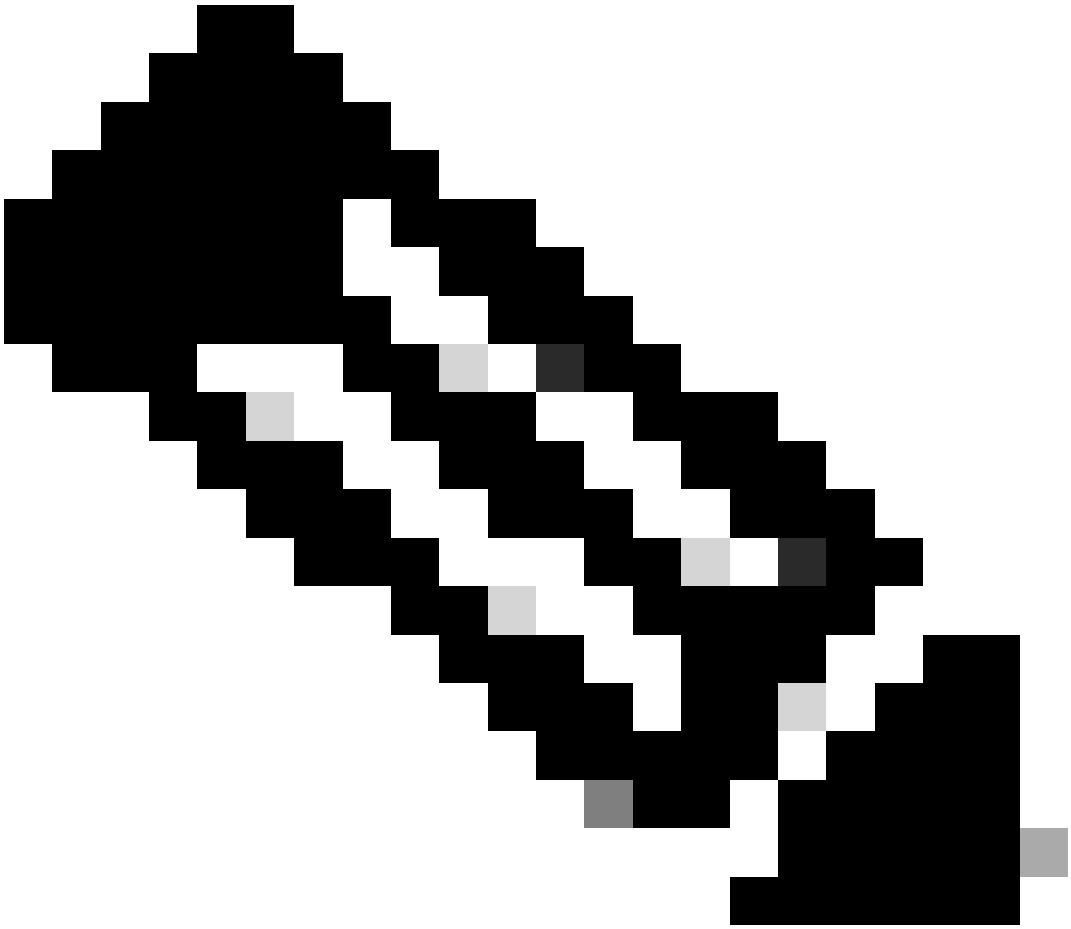
本文档中的信息基于以下软件和硬件版本：

- 思科身份服务引擎(ISE)，版本1.2.1
- 无线局域网控制器(WLC)软件发行版本- 7.4.100.0
- 访问点 (AP)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息



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的集中Web身份验证配置示例
- WLC 和 ISE 上的集中式 Web 身份验证配置示例

配置

在无线局域网控制器(WLC)上配置集中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，并提示用户进行身份验证。然后，WLC提取凭证（在外部服务器的情况下，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. 用户关联到Web身份验证SSID。
2. 用户打开其浏览器。
3. 输入URL后，WLC立即重定向至访客门户（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。

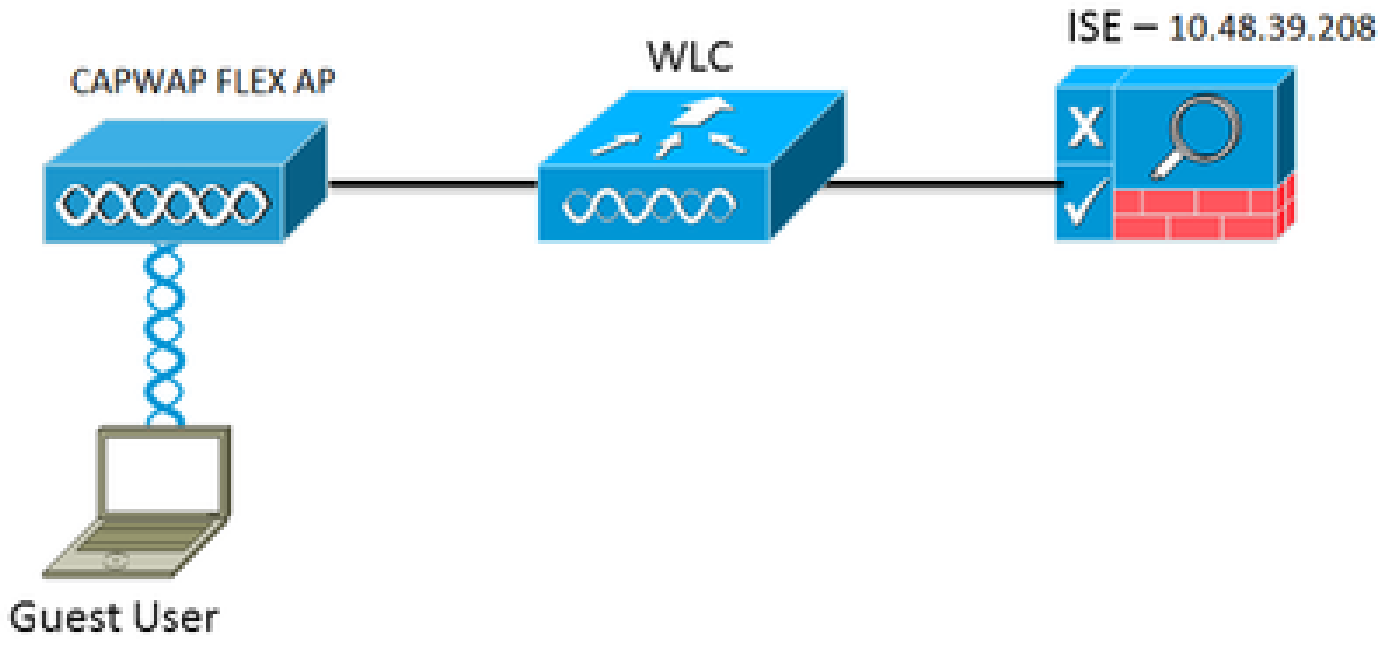
此过程包括许多重定向。新的方法是使用与ISE（高于1.1版本）和WLC（高于7.2版本）配合使用的集中Web身份验证。此过程包括以下步骤：

1. 用户关联到Web身份验证SSID。
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，例如访问控制列表(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Web身份验证的必要步骤。

网络图

此配置使用以下网络设置：



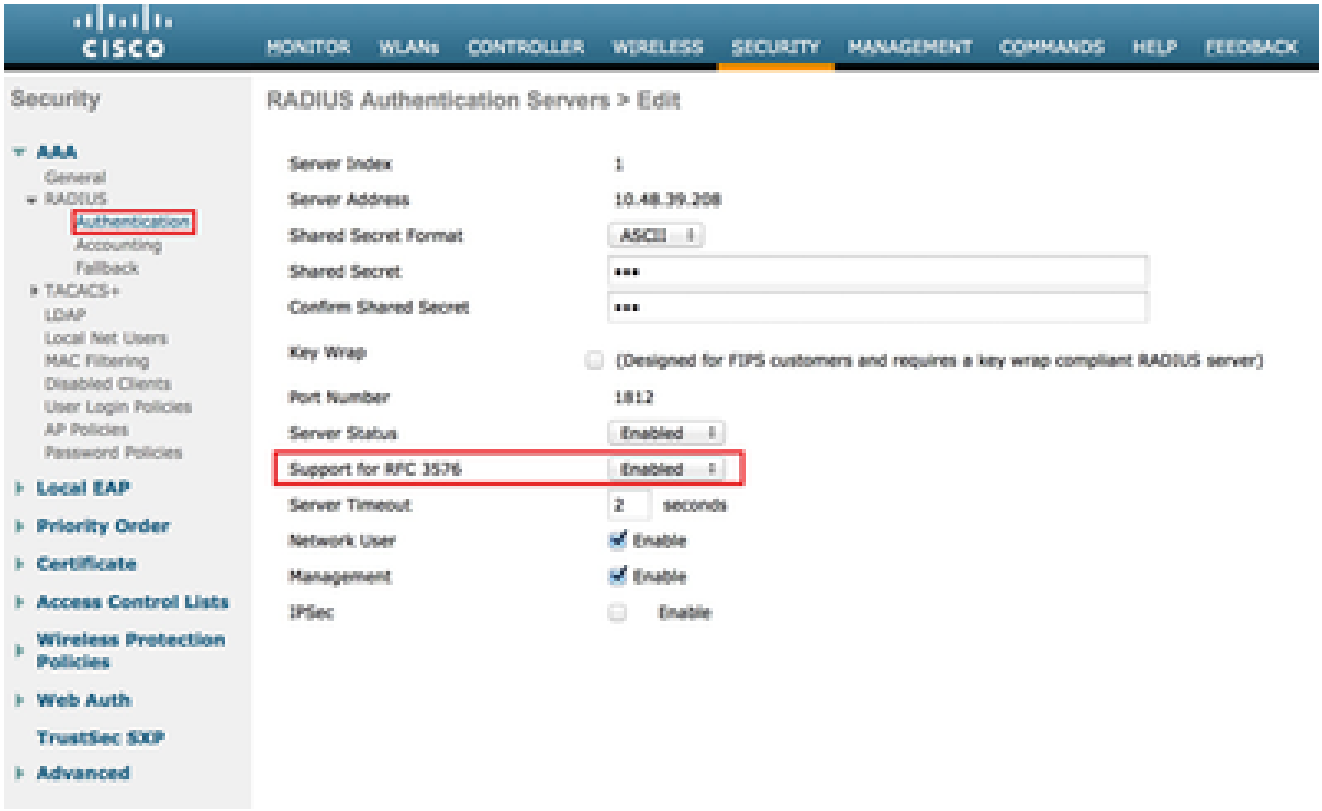
网络设置

WLC 配置

WLC配置相当简单。使用技巧（与交换机上的技巧相同）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配置为即使未找到MAC地址也返回Access-Accept消息，以便为所有用户发送重定向URL。

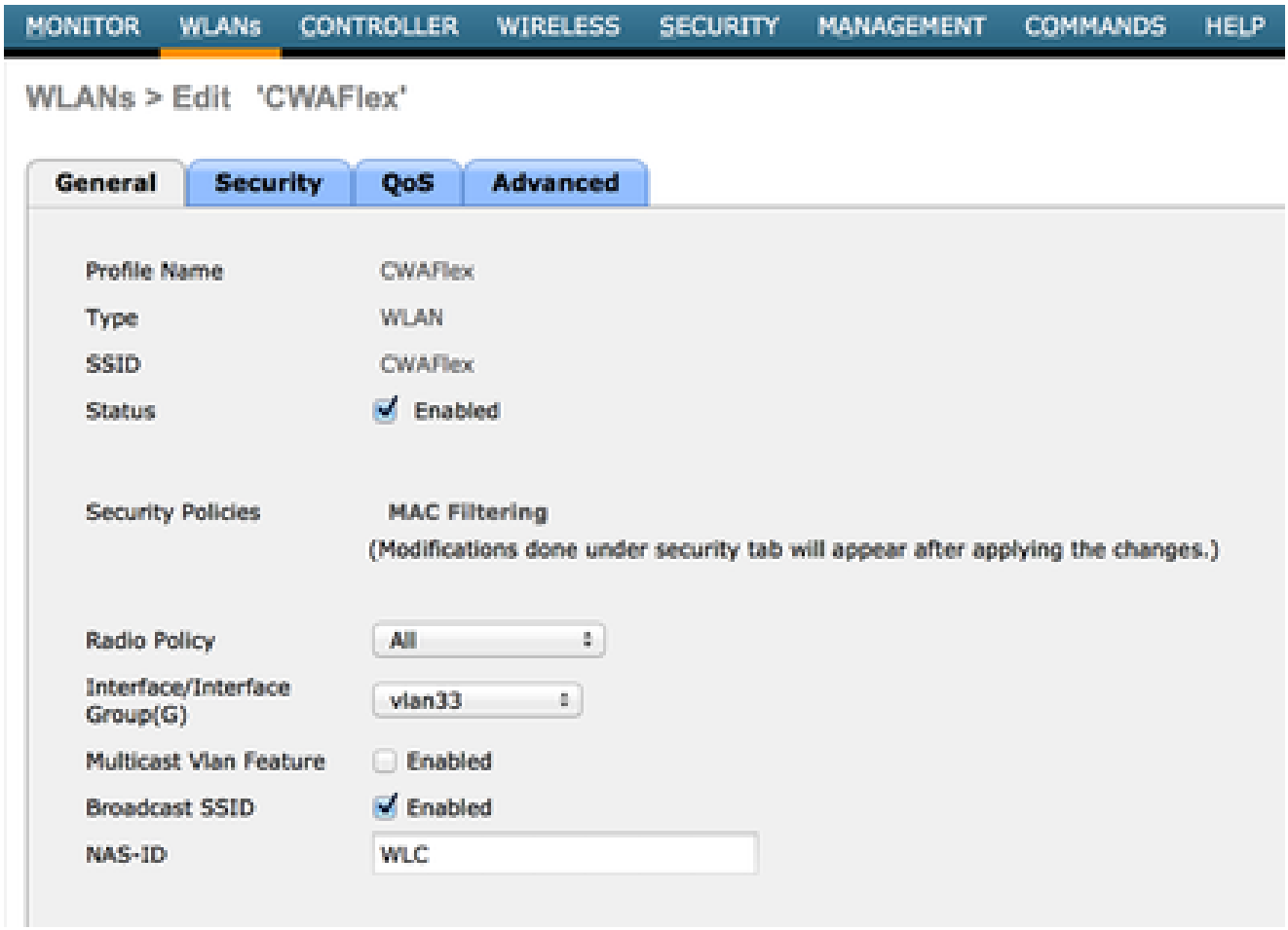
此外，必须启用RADIUS网络准入控制(NAC)和AAA覆盖。RADIUS NAC允许ISE发送CoA请求，指示用户现在已通过身份验证并能够访问网络。它还用于安全评估，其中ISE根据安全评估结果更改用户配置文件。

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



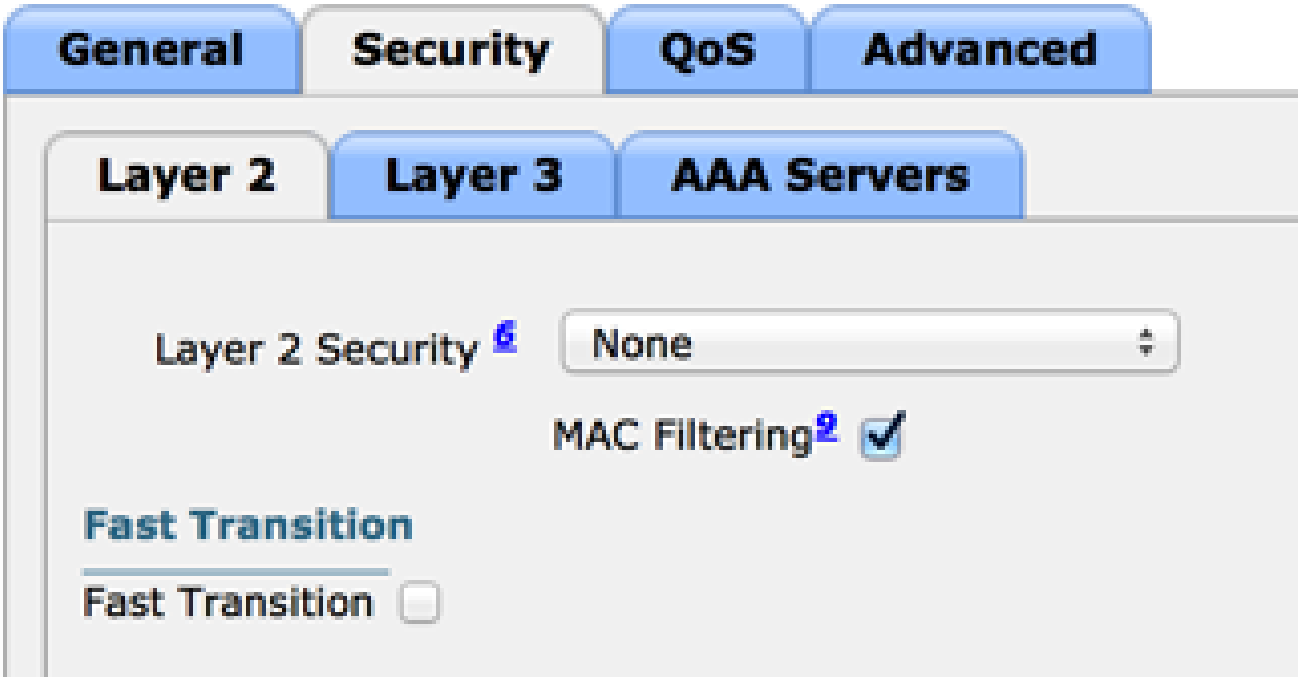
RADIUS服务器有RFC3576

2. 创建新的WLAN。本示例将创建名为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，因此更改不会产生多大影响。）



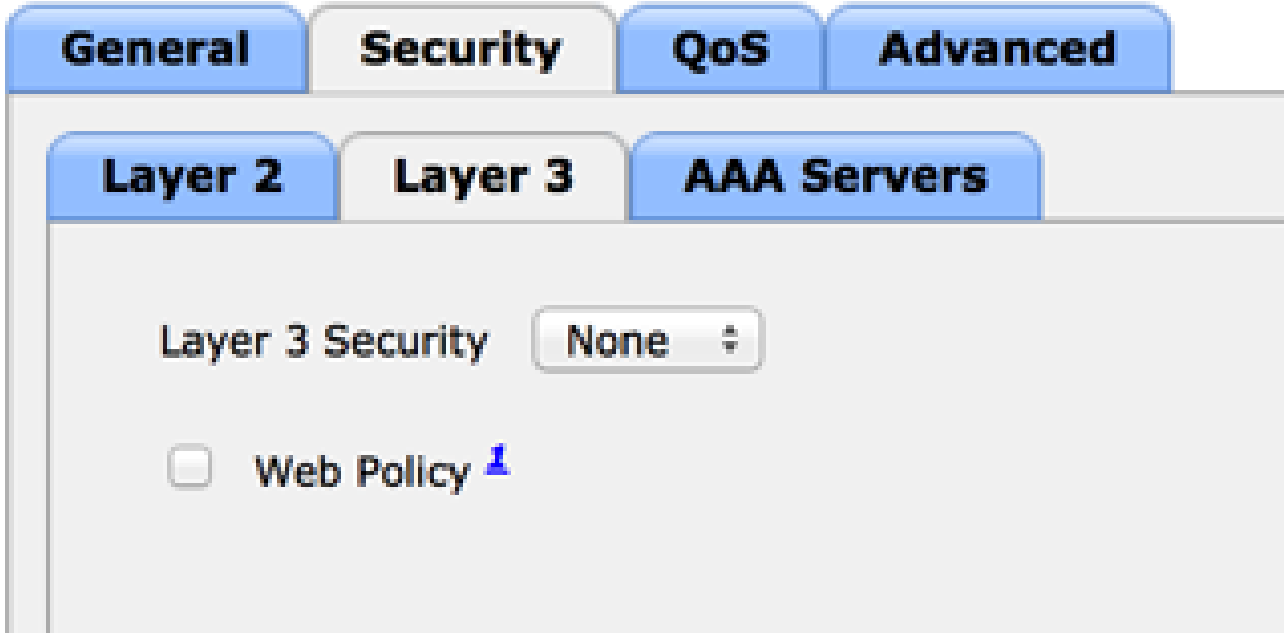
创建新的WLAN

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



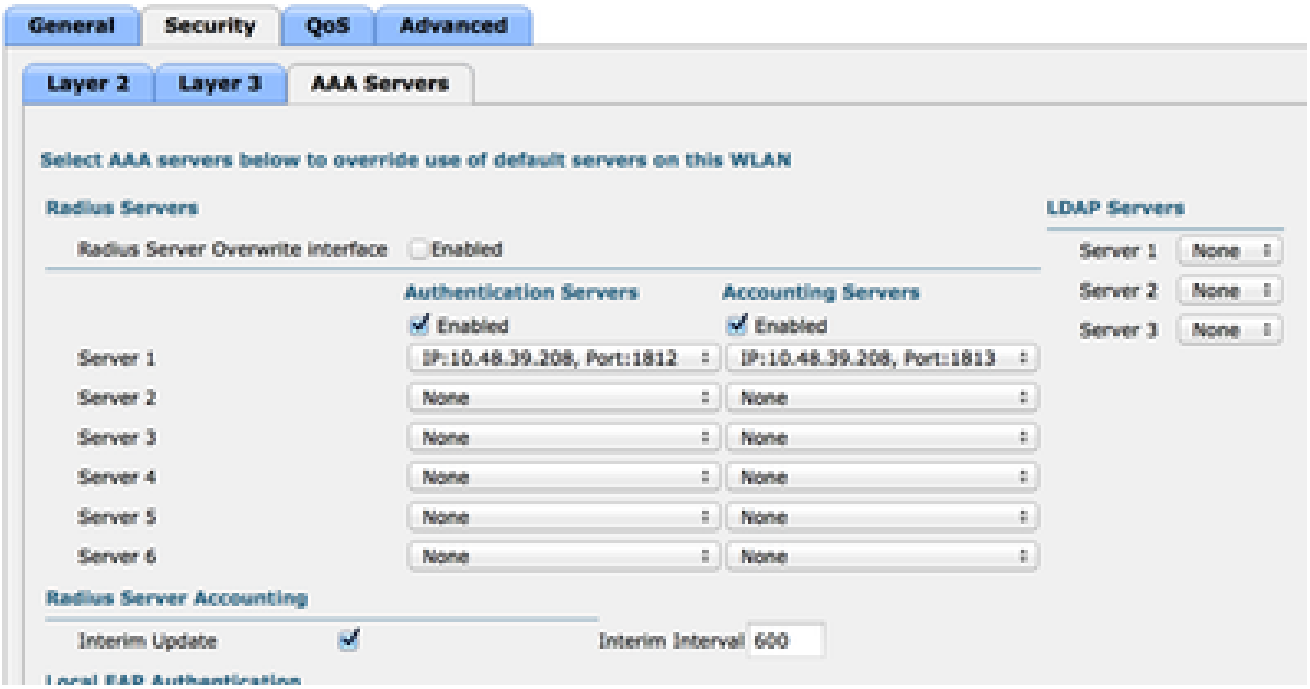
启用MAC过滤

4. 在Layer 3选项卡上，确保禁用了安全性。（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。）



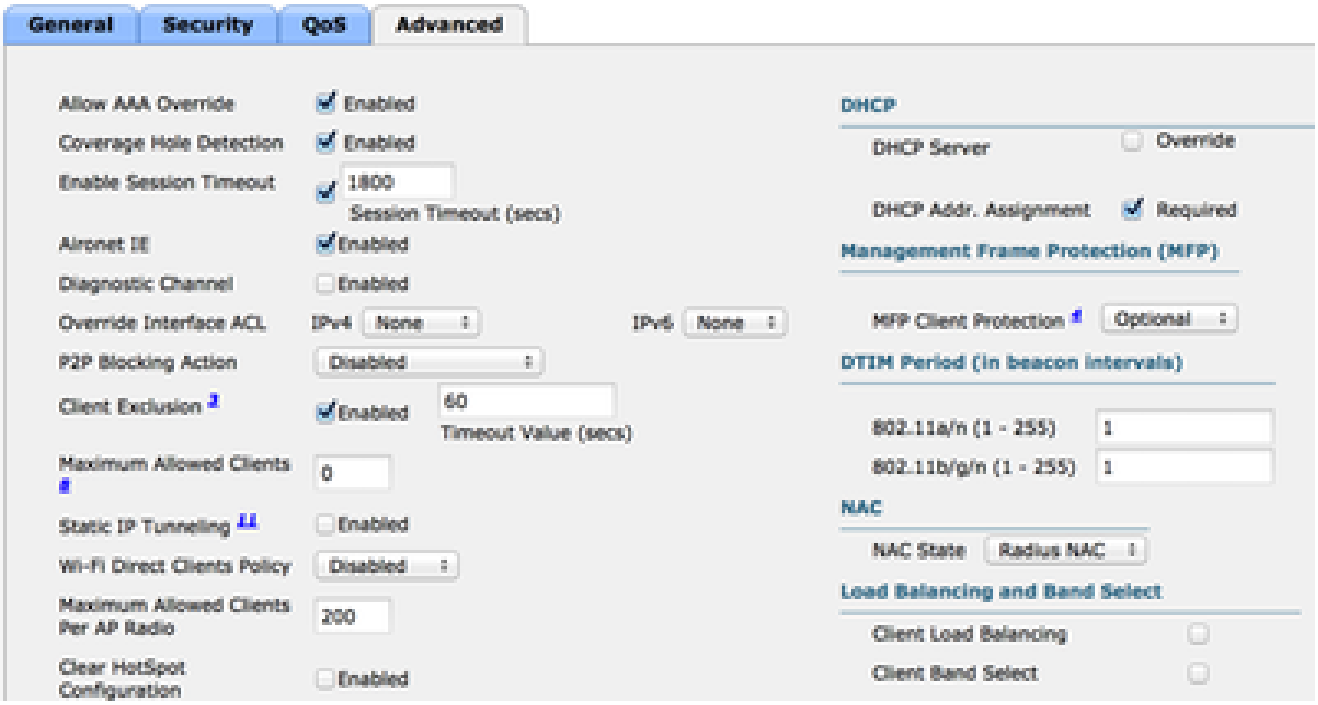
确保已禁用安全性

5. 在AAA Servers选项卡上，为WLAN选择ISE服务器作为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。



选择ISE服务器

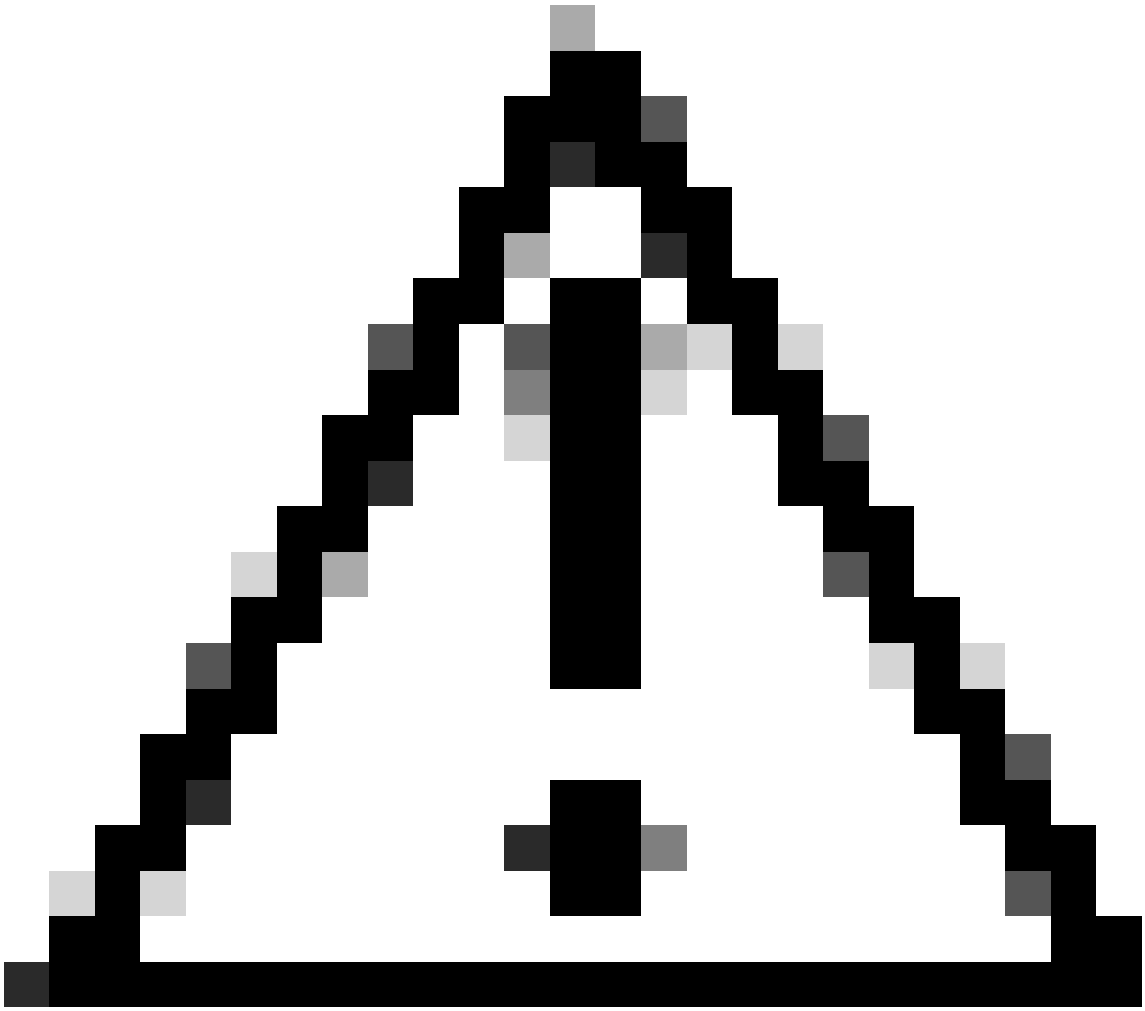
6. 在Advanced选项卡上，确保选中Allow AAA Override并为NAC State选择Radius NAC。



确保选中Allow AAA Override

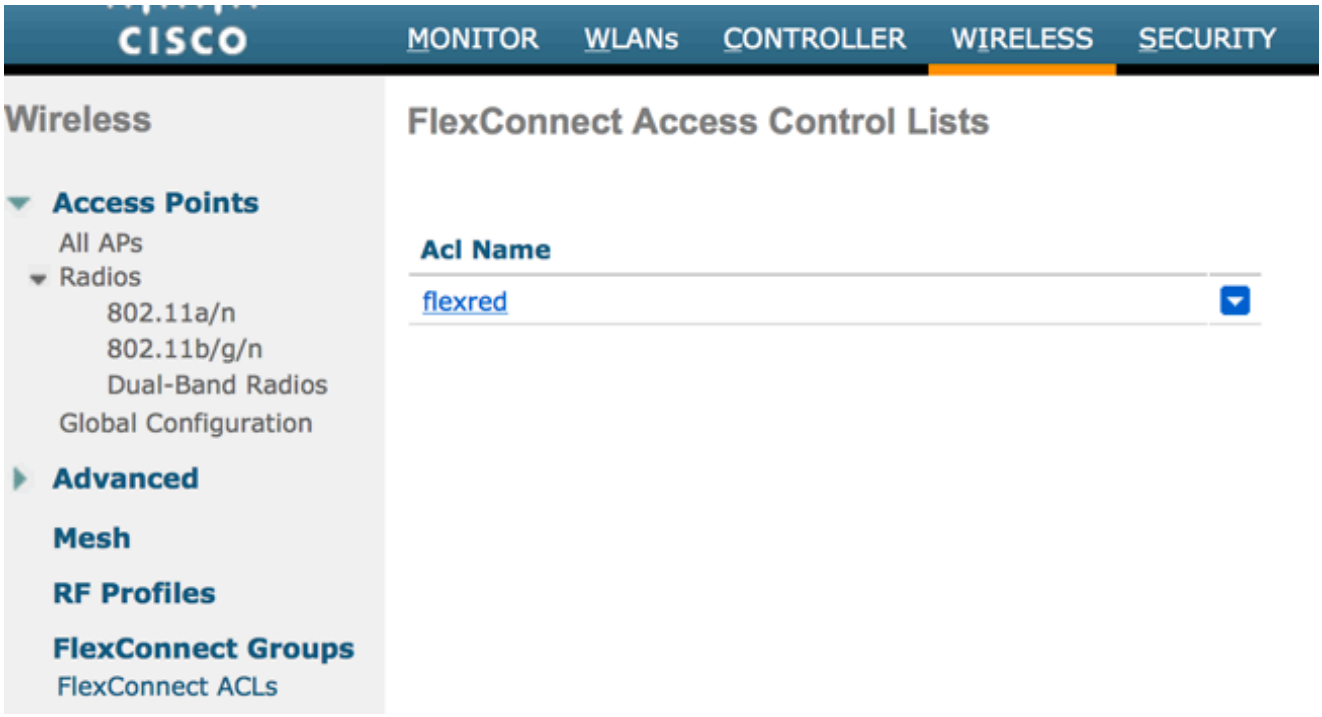
7. 创建重定向ACL。

此ACL在ISE的Access-Accept消息中引用，并定义哪些流量必须重定向（被ACL拒绝）以及哪些流量不能重定向（被ACL允许）。基本上，需要允许DNS流量和从ISE传入/传出流量



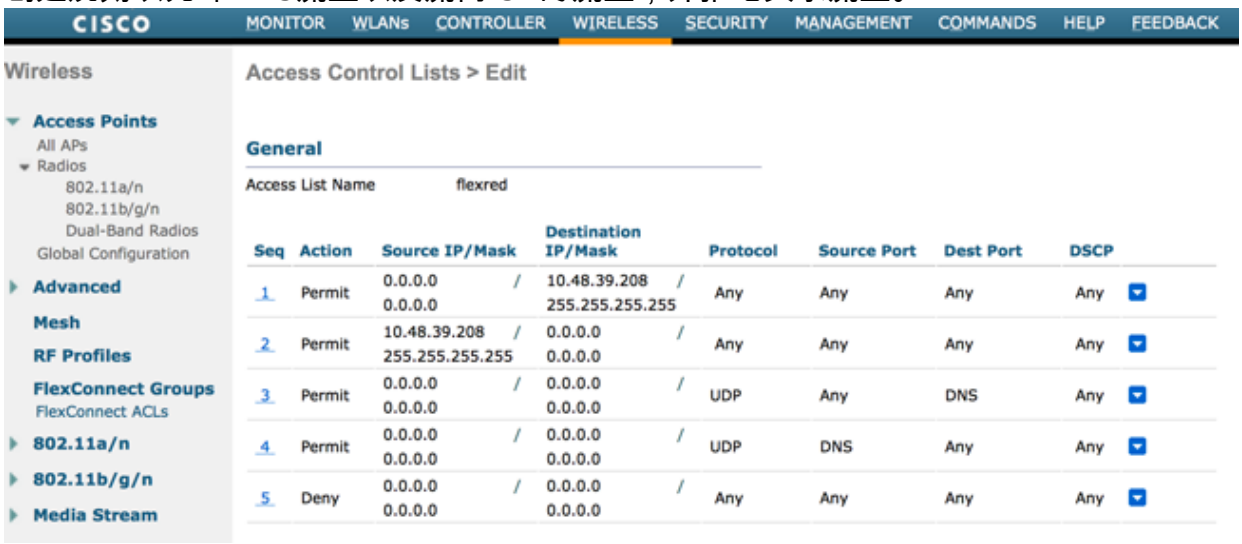
注意：FlexConnect AP的一个问题是您必须创建与普通ACL分开的FlexConnect ACL。此问题记录在Cisco Bug ID CSCue68065中，并在版本7.5中进行了修复。在WLC 7.5及更高版本中，仅需要FlexACL，不需要标准ACL。WLC预期ISE返回的重定向ACL是普通ACL。但是，为确保它正常工作，您需要应用与FlexConnect ACL相同的ACL。（只有注册的思科用户才能访问内部思科工具和信息。）

以下示例演示如何创建名为flexred的FlexConnect ACL：



创建名为Flexred的FlexConnect ACL

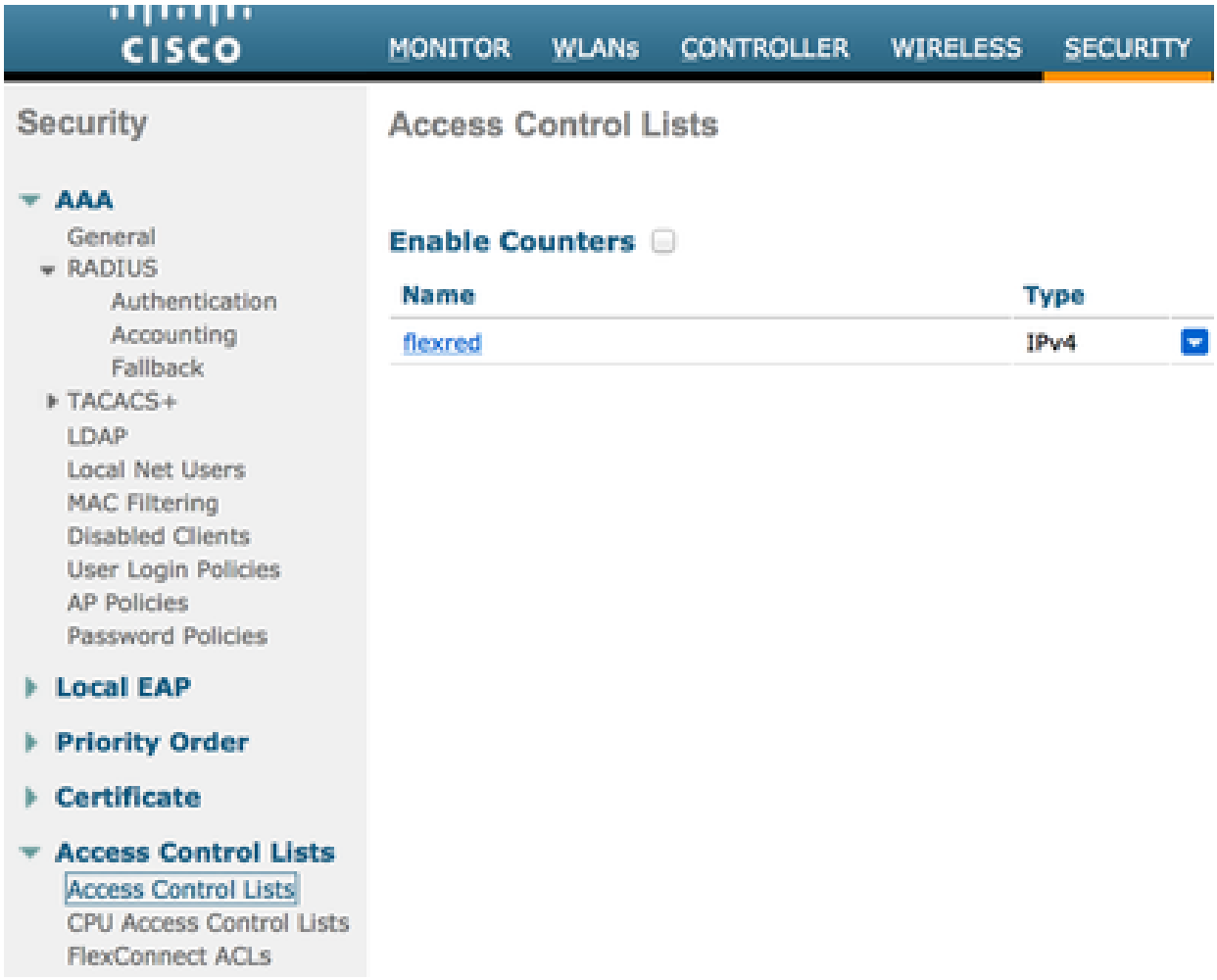
a. 创建规则以允许DNS流量以及流向ISE的流量，并拒绝其余流量。



允许DNS流量

如果您希望获得最高安全性，可以仅允许端口8443指向ISE。（如果进行安全评估，则必须添加典型的安全评估端口，例如8905,8906,8909,8910。）

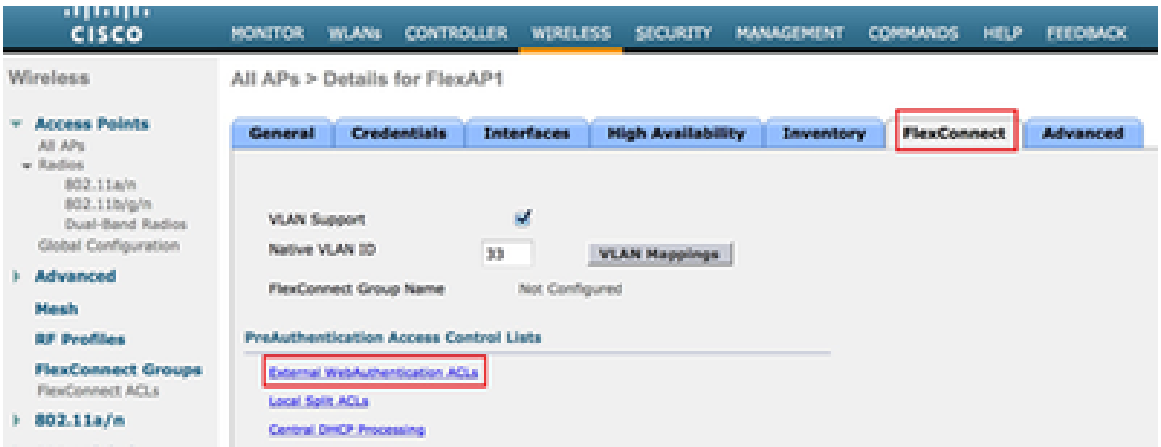
b. (仅限于7.5版本之前的代码，因为Cisco bug IDCSCue68065)选择Security > Access Control Lists以创建具有相同名称的相同ACL。



创建相同的ACL

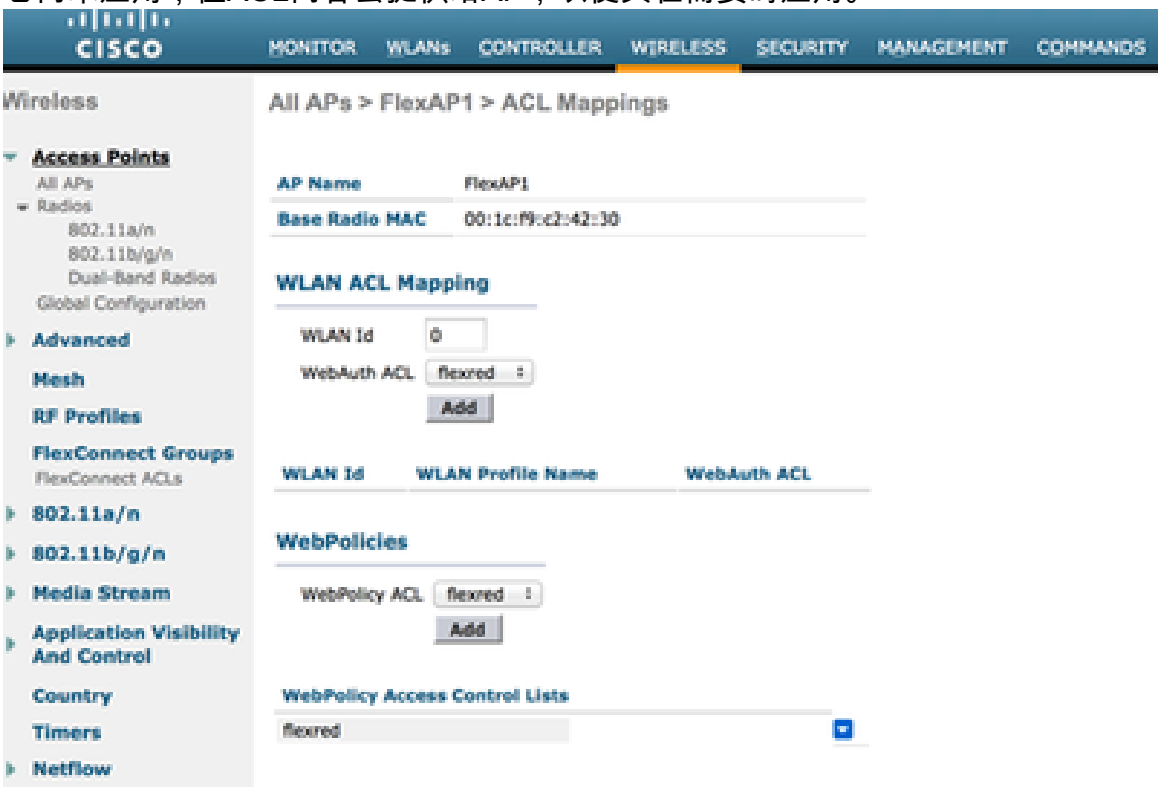
c. 准备特定FlexConnect AP。请注意，对于较大型的部署，通常会使用FlexConnect组，出于可扩展性原因，不会逐个AP执行这些项目。

1. 单击Wireless ，然后选择特定的接入点。
2. 点击FlexConnect选项卡，然后点击外部Web身份验证ACL。(在版本7.4之前，此选项被命名为Web policies。)



点击FlexConnect选项卡

3. 将ACL(在本例中为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ACL内容会提供给AP，以便其在需要时应用。



“将ACL添加到Web策略”区域

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Web身份验证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。

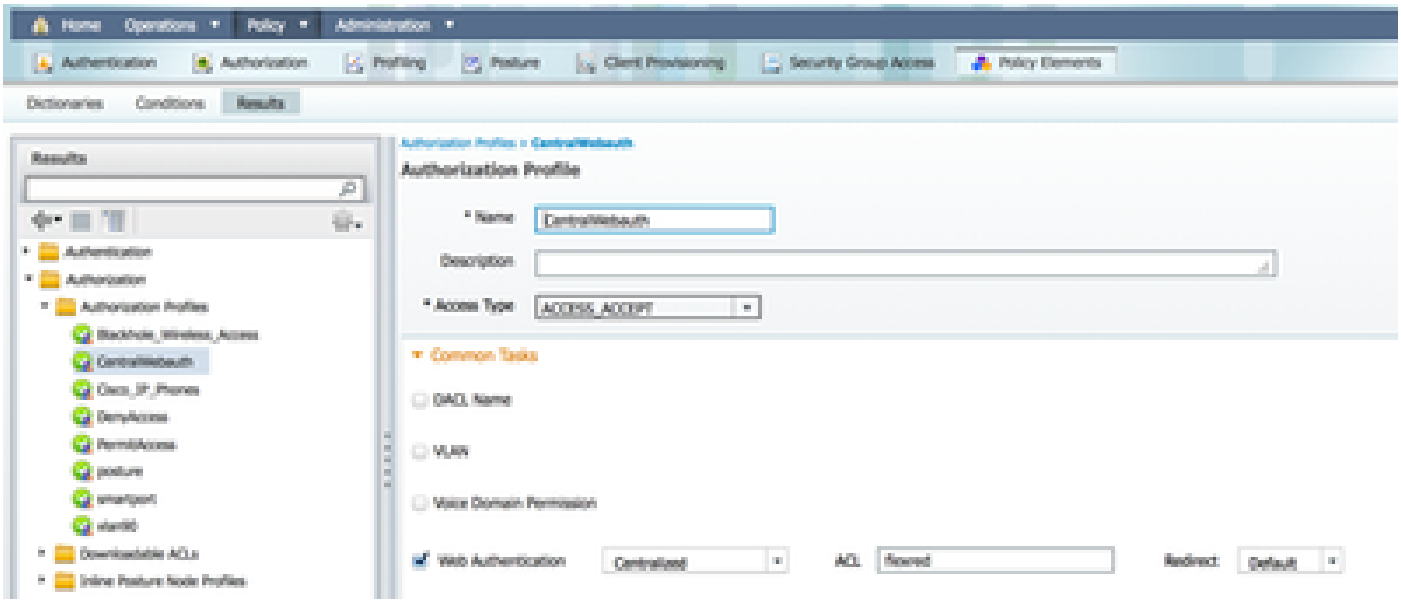
6. 从Access Type下拉列表中选择ACCESS_ACCEPT。

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的名称。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可在HTTP流量从客户端重定向到任意位置时触发。



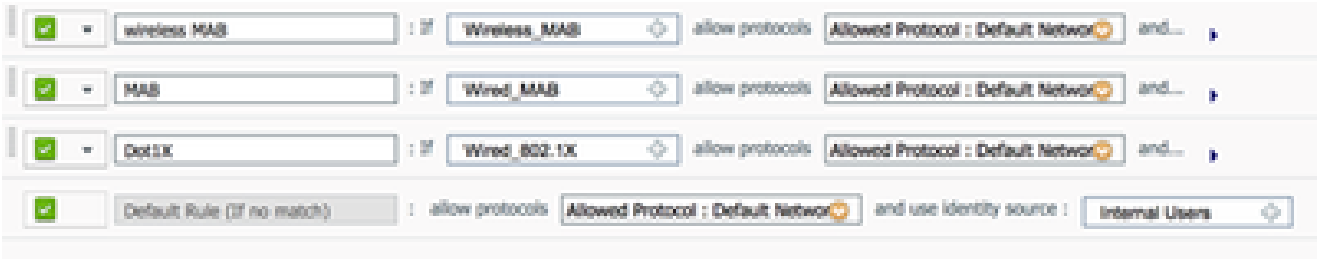
ACL触发从客户端到任何位置的HTTP流量重定向

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。

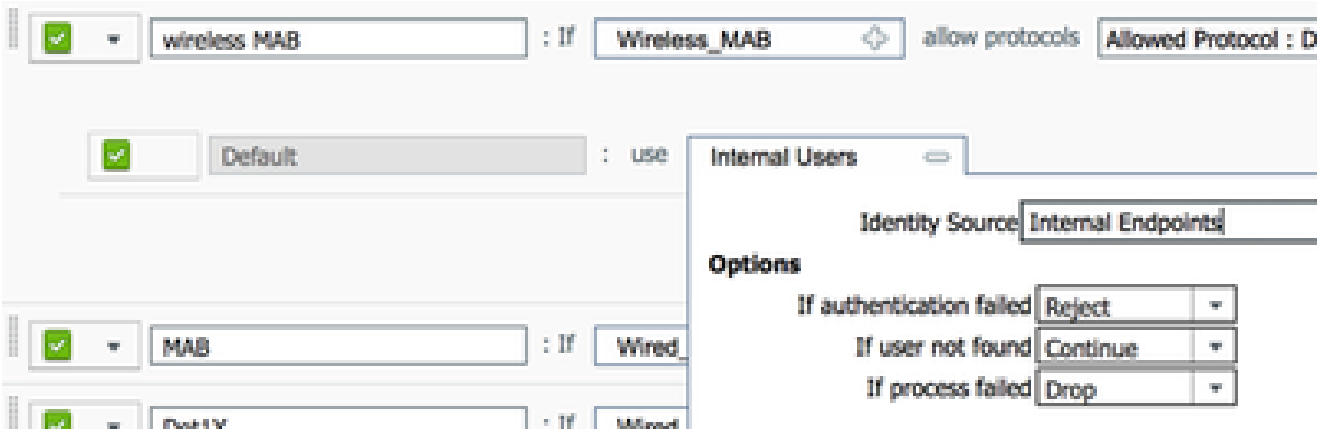
   下图展示了如何配置身份验证策略规则的示例。在本示例中，配置了当检测到MAC过滤时将触发的规则。



如何配置策略规则

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Default network access 作为允许的协议。
6. 点击位于和……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。

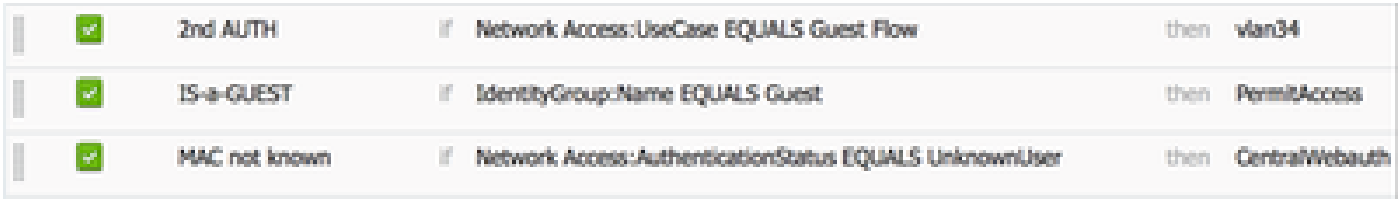


点击“继续”

此选项允许设备（通过webauth）进行身份验证，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，并且切勿关注此配置。

创建授权规则

现在，授权策略中有多个规则需要配置。关联PC后，它将通过mac过滤；假设MAC地址未知，则返回webauth和ACL。此MAC未知规则在下图中显示，并在本部分中配置。



MAC未知

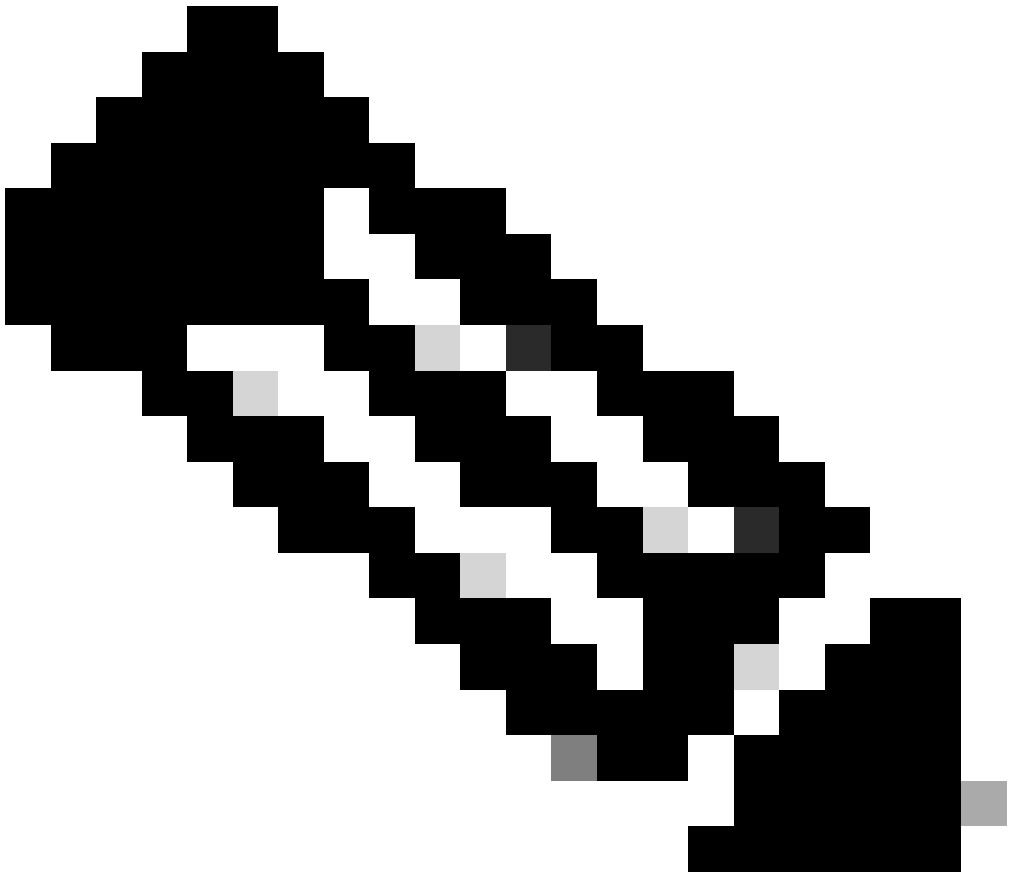
要创建授权规则，请完成以下步骤：

1. 创建新规则，然后输入名称。本示例使用MAC未知。
2. 点击条件字段中的加号(+)图标，并选择创建新条件。
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”页上，然后在词语右侧的字段中选择CentralWebauth(Authorization Profile)。

   此步骤允许ISE在用户（或MAC）未知的情况下继续。

   此时将向未知用户显示“登录”页面。但是，一旦他们输入其凭证，他们在ISE上会再次显示身份验证请求；因此，必须为另一个规则配置一个条件，如果用户是访客用户，则必须满足该条件。在本示例中，如果UseridentityGroup等于已使用的Guestis，并且假设所有访客都属于此组。
8. 点击MAC未知规则末尾的actions按钮，并选择在上方插入新规则。



注意：此新规则必须位于MAC未知规则之前，这一点非常重要。

---

9. 在Name字段中输入2nd AUTH。
10. 选择身份组作为条件。本示例选择Guest。

11. 在condition字段中，点击加号(+)图标，然后选择创建新条件。

12. 选择Network Access ，然后单击UseCase。

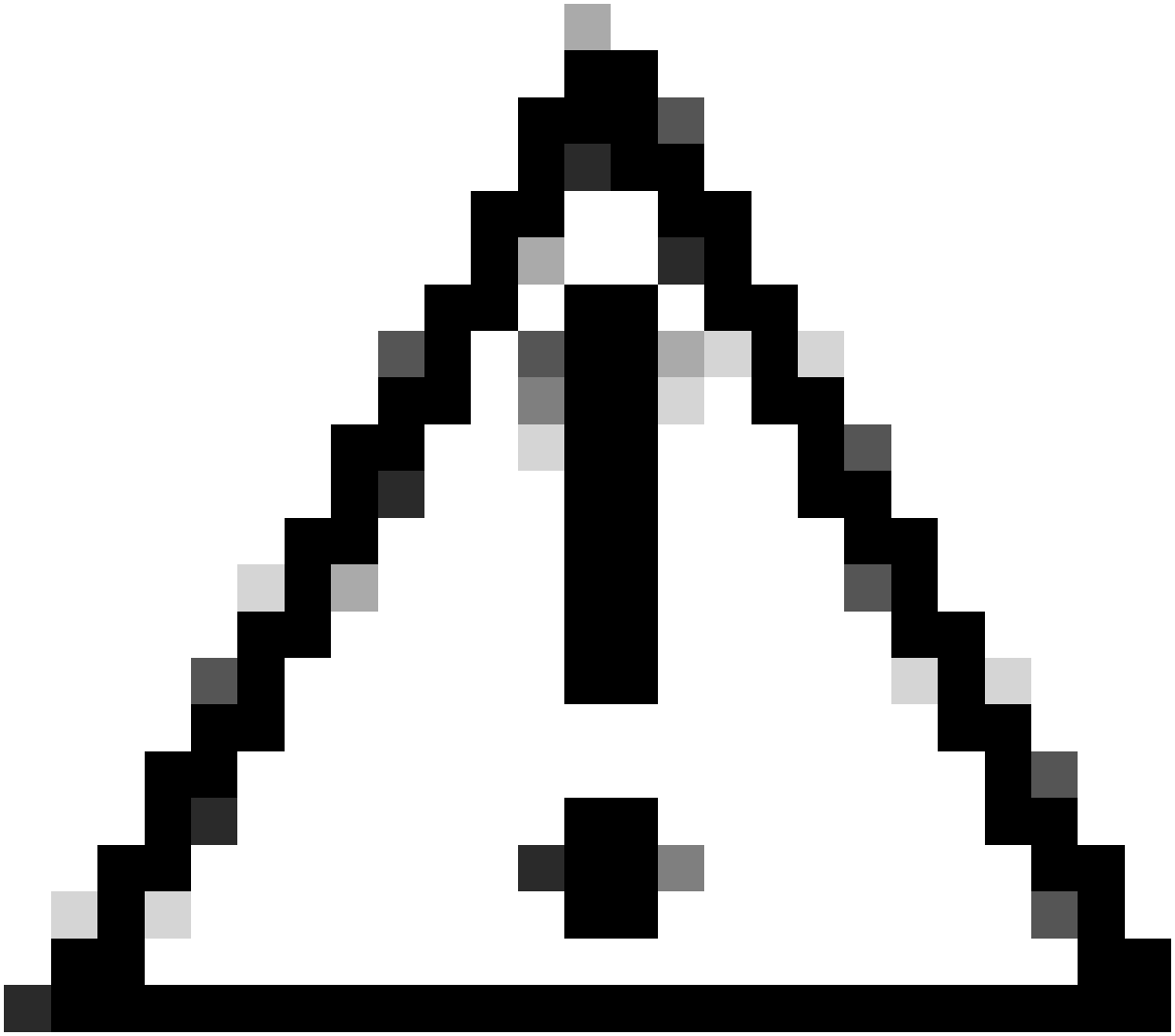
13. 选择Equals作为运算符。

14. 选择GuestFlow作为正确的操作数。这意味着您将捕获刚刚登录网页并在授权更改（规则的访客流部分）后返回的用户，并且仅当他们属于访客身份组时。

15. 在授权页面上，点击加号(+)图标(位于然后旁边)以选择规则的结果。

    在本示例中，分配了预配置的配置文件(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。



注意：在ISE版本1.3中，无法再遇到访客流使用案例，具体取决于Web身份验证的类型。然后，授权规则必须包含访客用户组作为唯一可能的条件。

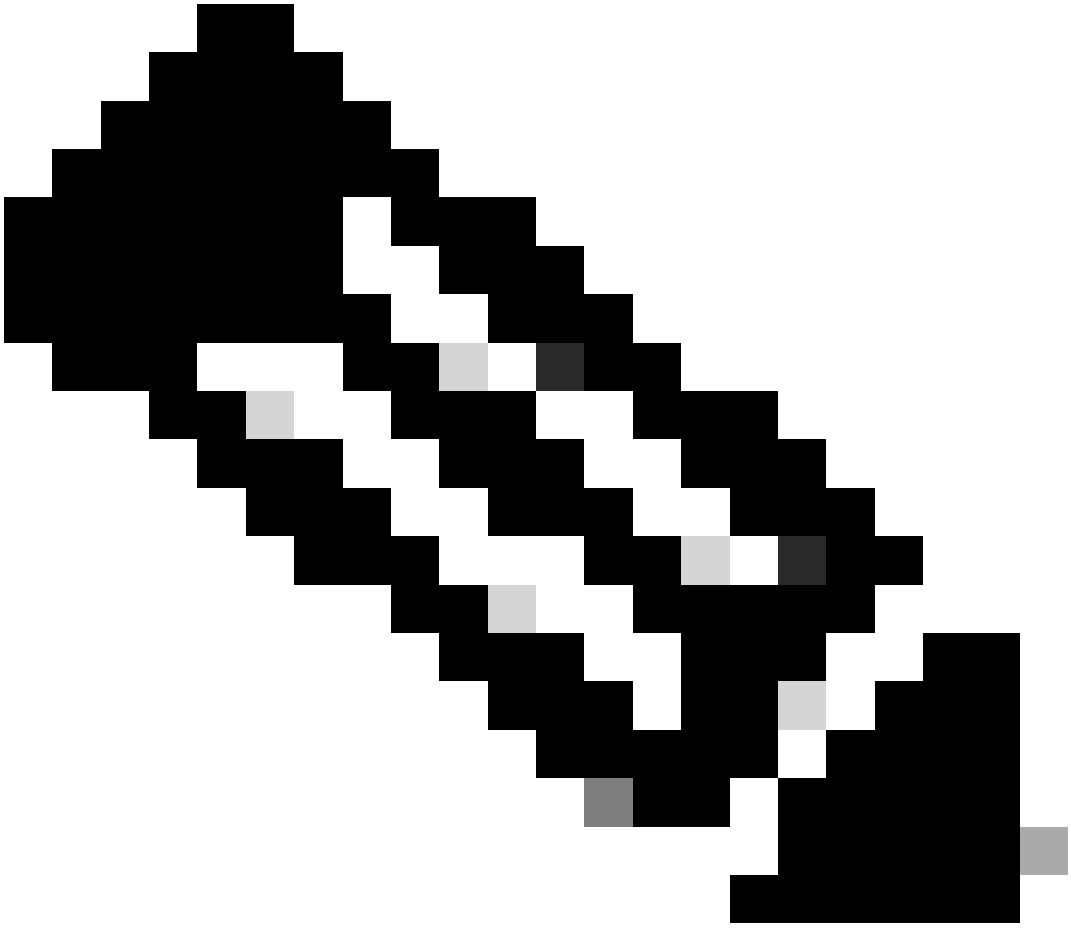
启用IP续订（可选）

如果分配VLAN，最后一步是让客户端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次身份验证规则设置VLAN，则可以跳过此步骤。

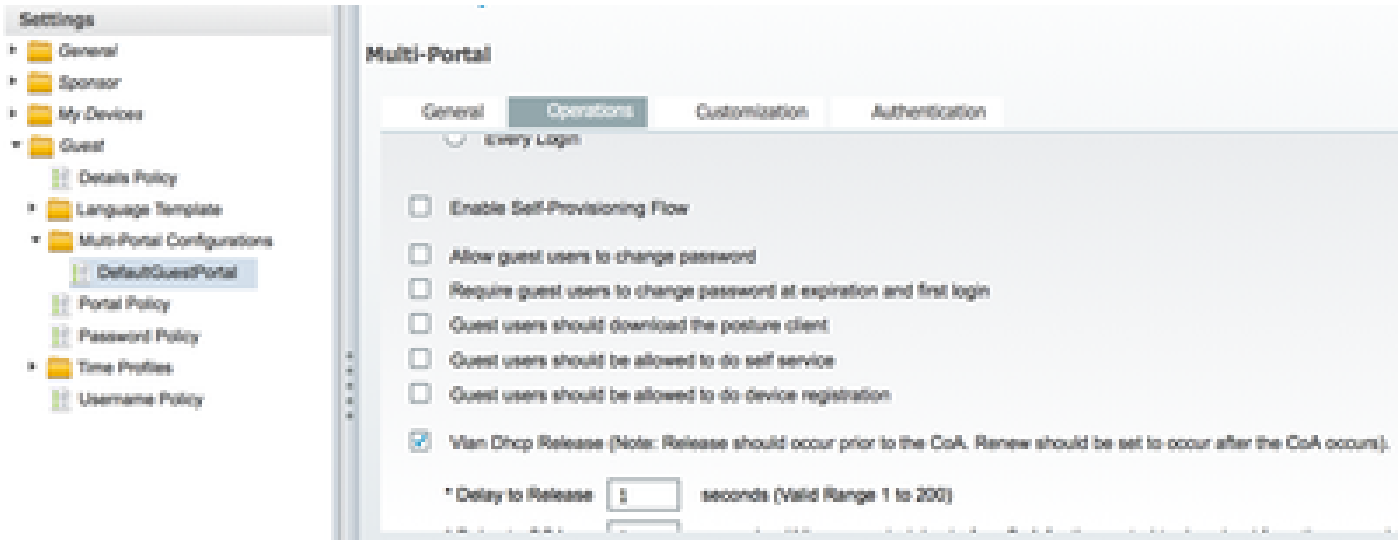
请注意，在FlexConnect AP上，VLAN需要预先存在于AP上。因此，如果没有，您可以在AP自身或您不为要创建的新VLAN应用任何ACL的flex组上创建VLAN-ACL映射。这实际上会创建一个VLAN（没有ACL）。

如果分配了VLAN，请完成以下步骤以启用IP续订：

1. 点击管理，然后点击访客管理。
2. 单击设置。
3. 展开Guest，然后展开Multi-Portal Configuration。
4. 点击DefaultGuestPortal或您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。



单击Vlan DHCP释放复选框

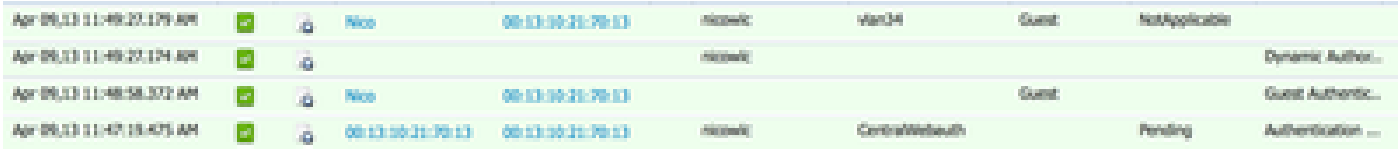
流量传输

在此场景中，可能很难理解将哪些流量发送到何处。以下是简要回顾：

- 客户端通过空中为SSID发送关联请求。
- 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过滤完成后收到相关响应。
- 客户端提交DHCP请求，并由接入点在本地交换DHCP以获得远程站点的IP地址。
- 在Central_webauth状态下，重定向ACL（通常为HTTP）上标记为拒绝的流量将进行集中交换。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会将此信息发送到CAPWAP中封装的WLC，WLC会欺骗该网站IP地址并重定向至ISE。
- 客户端被重定向到ISE重定向URL。这将再次在本地交换（因为它在Flex重定向ACL上命中permit）。
- 一旦进入RUN状态，流量将在本地交换。

验证

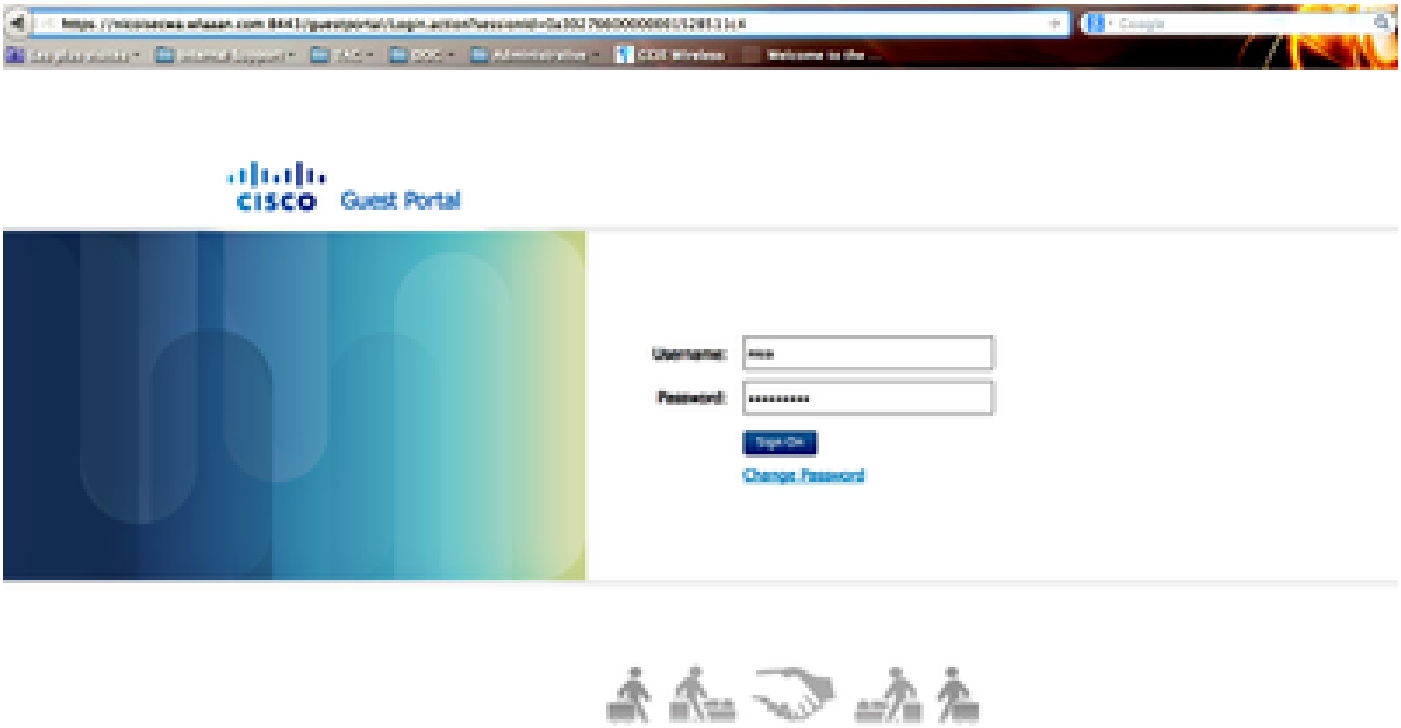
用户与SSID关联后，授权将显示在ISE页面中。



显示授权

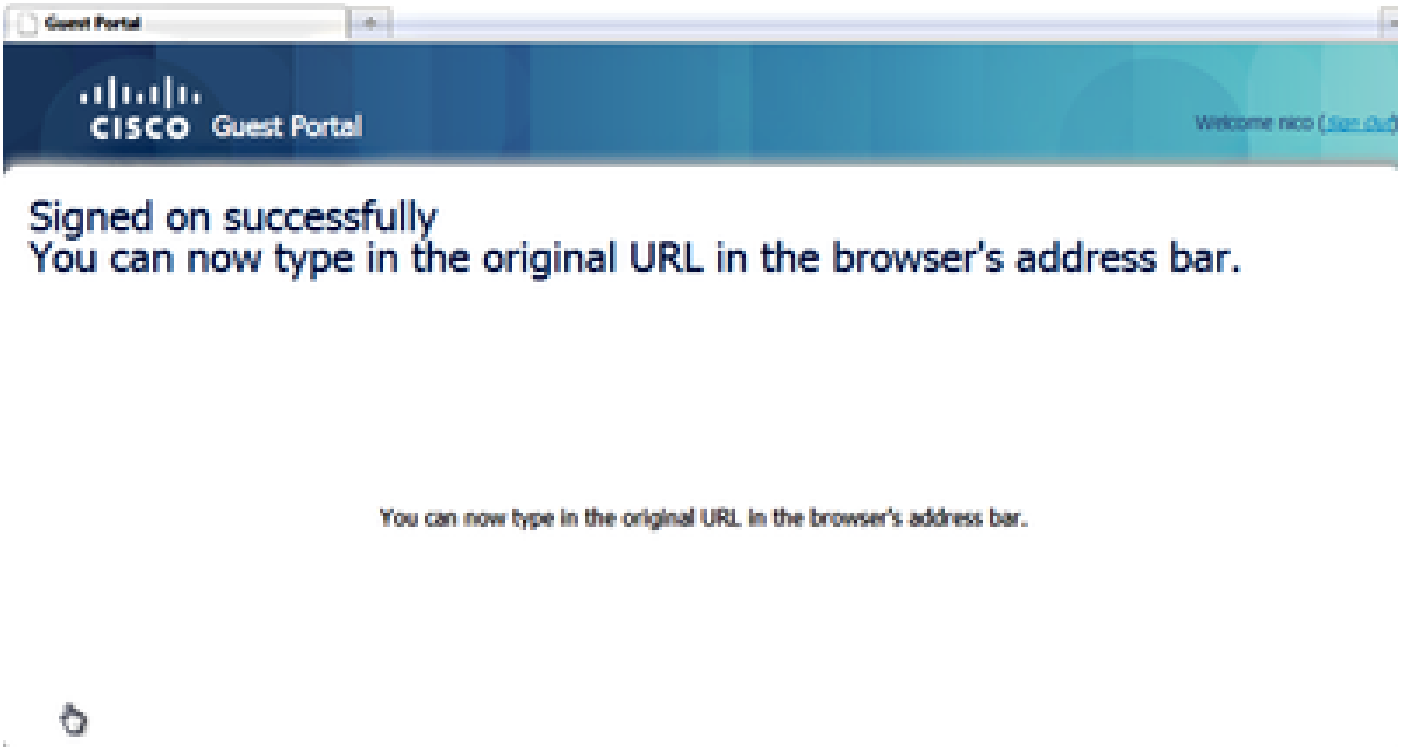
从下到上，您可以看到返回CWA属性的MAC地址过滤身份验证。接下来是门户使用用户名登录。然后，ISE向WLC发送CoA，最后身份验证是在WLC端的第2层mac过滤身份验证，但ISE会记住客户端和用户名并应用我们在本示例中配置的必要VLAN。

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。



已重定向至ISE

用户接受策略后，网络访问即被授予。



授予的网络访问权限

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

相关信息

- 思科技术支持和下载

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）。