# 配置ISE无线CWA和与AireOS和下一代WLCs的热点流

## 目录


简介
先决条件
要求
使用的组件
配置
网络图
配置Unified 5508 WLC
全局配置
配置访客的服务集标识(SSID) ：
配置重定向ACL
HTTPS重定向
积极的故障切换
俘虏旁路
配置聚合3850个NGWC
全局配置
SSID配置
重定向ACL配置
命令行界面(CLI)配置
配置ISE
普通的ISE配置任务
用例1 ：与访客验证的CWA在每用户连接
用例2 ：与一天一次强制执行访客验证的设备已注册的CWA。
用例3 ：Hostspot门户
验证
用例1
用例2
用例3
FlexConnect本地交换在AireOS
外国锚点方案
故障排除
AireOS和聚合的访问WLC的普通的被中断的状态
AireOS WLC
NGWC
ISE
相关信息


## 简介

本文在身份服务引擎(ISE)方面描述如何配置三个访客使用案件有思科的AireOS和下个Generation(NGWC)无线局域网控制器(WLCs)。

# 先决条件

## 要求

Cisco 建议您了解以下主题：

- Cisco无线LAN控制器(统一和聚合的访问)
- 身份服务引擎(ISE)

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科身份服务引擎版本2.1
- Cisco无线LAN控制器5508运行的8.0.121.0
- 运行03.06.04.E的下一代无线控制器(NGWC) Catalyst 3850(WS-C3850-24P)

# 配置

## 网络图

在本文报道的步骤描述在统一的和聚合的访问WLCs的典型配置支持与ISE的所有访客流。

## 配置Unified 5508 WLC

不管在ISE配置的用例，从WLC前景它所有从连接对与作为验证和记帐服务器启用的一个无线终端开始(加上AAA覆盖和RADIUS美洲台)对ISE的该点MAC过滤的一开放SSID。 这保证ISE能动态地推送必要的属性到重定向的成功的实施的WLC到艾斯的访客门户。

### 全局配置

1. 添加ISE全局作为验证和记帐服务器。

   - 导航对**安全>AAA >验证**并且点击**新**

   - 输入ISE服务器IP和共享机密
   - 保证服务器状态和**支持RFC 3676的**(授权或CoA支持更改)是都集对**已启用**。
   - 默认情况下在服务器超时AireOS下WLCs将有2秒。根据网络特性(延迟、ISE和WLC用不同的位置等等)增加服务器超时到至少5秒避免多余的故障切换事件可能是有利的。
   - 单击 **Apply**。
   - 如果有多项策略配置的服务节点(PSN)继续创建额外服务器条目。

     **注意**：此特定配置示例包括2个ISE实例

- 导航对**认为安全的>AAA >的RADIUS>**并且点击**新**
- 输入ISE服务器IP和共享机密
- 保证服务器状态设置对已启用
- 如果需要，增加服务器超时(默认是2秒)。

2. Fallback配置。

在统一的环境，一旦服务器超时被触发WLC移动向下个配置的服务器。从WLAN的下一个。如果没有其他是可用的那么WLC选择下一个在全局Servers列表。当多个服务器在SSID (主要的配置，附属等等)默认情况下，一旦故障切换发生WLC继续发送验证和(或)永久性核算流量到附属实例，即使主服务器回到联机。

为了缓和此行为enable (event) fallback。导航对**安全>AAA > RADIUS> Fallback。**默认行为关闭。恢复的唯一方法从服务器下来事件要求admin干预(全局请重新启动服务器的管理状态)。

要启用fallback您有两个选项：

- **被动**-在被动模式，如果服务器不回答WLC认证请求， WLC移动服务器向非激活队列并且设置计时器(在秒选项的间隔)。当计时器超时时， WLC移动服务器向活动队列不考虑服务器实际状态。如果认证请求导致含义的超时事件(服务器仍然是下来)服务器项再移动向非激活队列，并且计时器再起动。如果服务器成功响应上一步，在活动队列保持。此处可配置的值去从180到3600秒。

- **激活-**在激活模式，当服务器不回答WLC认证请求时， WLC指示服务器如停止，然后移动服务器向非活动服务器池并且开始周期地发送探测器消息，直到该服务器回应。如果服务器回应，则WLC移动死机服务器向活动池并且停止发送探测器消息。

在此模式WLC以秒钟(180到3600)要求您输入一用户名和一个探测器间隔。

> **注意**：WLC探测器不要求成功认证。不管怎样，成功或失败的认证认为是促进服务器的足够对活动队列的服务器响应。

**配置访客的服务集标识(SSID) ：**

- 导航对WLAN选项卡和下创建新选项单击**去**：

- 输入配置文件名称和SSID名称。单击 **Apply**。
- 在常规选项卡下请选择将使用的接口或接口组(访客VLAN)。

- 在**安全> Layer2 >第2层安全下请勿**选择并且启用**过滤**复选框。的**Mac**

- 在**AAA服务器**选项卡集合验证和记帐服务器下**启用**并且选择您的主要的和辅助服务器。

- **临时更新**：这是不添加任何好处到此流的可选配置。如果喜欢启用它， WLC我应该运行8.x或更高的代码：

**已禁用**：功能完全禁用。

**启用与0个间隔：**WLC发送核算更新对ISE，在有在客户端的移动位置控制器Block(MSCB)条目时候(IE上的一个变化。IPv4或IPv6地址分配或者更改、客户端漫游事件等等)没有另外的定期更新被派出。

**启用与一个已配置的临时间隔：**在此模式WLC发送通知对ISE在客户端的MSCB条目更改，并且也

发送另外的定期核算通知在配置的时间间隔(不管任何更改)。

- 在Advanced选项Enable (event)下请**允许AAA覆盖**和在**NAC状态**挑选**RADIUS NAC下**。这保证WLC运用来自ISE的所有属性值对(AVPs)。
- 导航对SSID常规选项卡并且设置SSID状态对**已启用**

- **应用**更改。

### 配置重定向ACL

此ACL由ISE参考，并且确定什么流量重新定向，并且什么流量通过将允许。

- 去**安全选项卡>访问控制列表**并且点击**新**
- 这是ACL示例

此ACL到/从DNS服务和ISE节点如果允许在TCP端口8443。隐式在含义的底部拒绝流量的其余重新定向对艾斯的访客门户URL。

### HTTPS重定向

AireOS版本8.0.x支持此功能并且向上默认情况下，但是被关闭。要启用HTTPS支持请去WLC **Management> HTTP-HTTPS > HTTPS的重定向**并且设置它**启用**或应用此in命令CLI ：

```
(Cisco Controller) >config network web-auth https-redirect enable
```

### 在HTTPS重定向以后的证书警告启用

在https重定向启用后，在重定向期间，用户可能遇到证书信任问题。这被看到，即使有在控制器的一有效被串连的证书，并且，即使此证书由第三方签字委托认证机关。原因是在WLC安装的证书发出对其虚拟接口主机名或IP地址。当客户端试https ：//cisco.com，浏览器盼望证书发出到cisco.com。然而，为了的WLC能拦截客户端发出的GET，它首先需要建立WLC提交其虚拟接口证书的HTTPS会话在SSL握手相位期间。这造成浏览器显示警告，因为在SSL握手期间被提交的证书未发出到客户端尝试访问的原始网站(IE。cisco.com反对WLC's虚拟接口主机名)。您也许发现不同的身份验证错误消息用不同的浏览器，但是全部与同一问题关连。

### 积极的故障切换

默认情况下此功能在AireOS WLCs启用。当积极的故障切换启用时， WLC指示AAA服务器，当无答复和它移动向下个已配置的AAA服务器，在Radius超时事件影响一个客户端后。

当功能禁用时WLC故障切换到下个服务器，只有当RADIUS超时事件发生在至少3客户端会话。此功能可能由此命令禁用(重新启动没有为此命令要求) ：

```
(Cisco Controller) >config radius aggressive-failover disable
```

验证功能的当前状态：

```
(Cisco Controller) >show radius summary

Vendor Id Backward Compatibility..... Disabled
Call Station Id Case..................... lower
Acct Call Station Id Type..................... Mac Address
Auth Call Station Id Type..................... AP's Radio MAC Address:SSID
```

```
Extended Source Ports Support.................. Enabled
Aggressive Failover............................ Disabled
```

### 俘虏旁路

支持一俘虏Network Assistant的终端(CNA)机制发现俘虏PORTAL和自动启动登录页通过在受控的窗口的一个假浏览器通常执行此，当其他终端启动一个充分地有能力浏览器触发此时。对于CNA启动假浏览器的终端，这可能中断流，当重定向对ISE俘虏门户。 这典型地影响苹果公司IOS设备，并且有特别是负面影响在要求设备已注册、VLAN DHCPRlease、标准检查等等的流。

根据流的复杂性在使用中可能推荐启用俘虏旁路。在这样方案中， WLC忽略CNA门户发现机制，并且客户端需要打开浏览器开始重定向进程。

验证功能的状况：

```
(Cisco Controller) >show network summary

Web Auth CMCC Support ..................... Disabled
Web Auth Redirect Ports ................... 80,3128
Web Auth Proxy Redirect  .................. Disable
Web Auth Captive-Bypass   ................. Disabled
Web Auth Secure Web  ...................... Enable
Web Auth Secure Redirection  .............. Enable
```

启用此功能类型此命令：

```
(Cisco Controller) >config network web-auth captive-bypass enable
Web-auth support for Captive-Bypass will be enabled.

You must reset system for this setting to take effect.
```

WLC警告为了更改能起作用重置系统的用户(重新启动)是需要的。

这时**show network摘要**显示功能如启用，但是对于更改起作用WLC需要重新启动。

## 配置聚合3850个NGWC

### 全局配置

1. **添加ISE全局作为验证和记帐服务器**
   - 导航到**Configuration> Security>RADIUS >服务器**并且点击**新**
   - 输入反射您的环境状况的ISE**服务器IP地址**、**共享机密**、**服务器超时**和**重试计数**。
   - 保证**RFC 3570的**(CoA支持)**支持**启用。
   - 重复进程添加辅助服务器条目。
2. **创建艾斯的服务器组**
   - 导航给**Configuration>安全>Server组**并且点击**新**
   - 分配名称到组并且输入时间值以分钟。这是时间控制器在非激活队列保留服务器，在再促进对活动服务器列表前。
   - 从可用的Servers列表请添加他们到已分配服务器列。
3. **全局请启用Dot1x**

- 导航对**Configuration> AAA >方法列表>General**并且启用**Dot1x系统验证控制**

4. **配置方法列表**

- 导航对**Configuration> AAA >方法列表>验证**并且建立新方法列表。在这种情况下它是类型Dot1x和组ISE_Group (在上一步创建的组)。然后命中数**应用**

- 为认为(**Configuration> AAA >方法列表>核算**)和授权(**Configuration>**执行同样**AAA >方法列表>授权**)。他们如下所示:

5. **创建授权MAC过滤器方法**。

这从SSID设置呼叫后。

- 导航对**Configuration> AAA >方法列表>授权**并且点击**新**。
- 输入**方法列表名称**。选择**Type=网络**和**组类型组**。
- 添加ISE_Group到已分配服务器组字段。

**SSID配置**

1. **创建访客SSID**

- 导航对**Configuration>无线> WLAN**并且点击**新**
- 输入WLAN ID、SSID和配置文件名称并且单击应用。
- 一旦在接口/接口组下的SSID设置请选择访客VLAN第3层接口。

- 在**安全> Layer2下请勿**选择，并且在**过滤**回车的**Mac旁边**您以前配置的Mac过滤器方法列表名称(MacFilterMethod)。
- 在**安全>**AAA **Server选项下请**选择适当的验证和会计方法列表(ISE_Method)。

- 在**Advanced选项**enable (event)下请**允许AAA覆盖**和**NAC状态。**应该根据每部署需求(会话超时、客户端排除、支持Aironet扩展的等等)调节设置的其余。

- 导航对常规选项卡设置状态对已启用。然后命中数**应用。**

**重定向ACL配置**

此ACL由ISE参考后access-accept以回应初始MAB请求。NGWC使用它确定应该通过允许重定向的什么流量，并且什么流量。

- 导航对**配置> Security > ACL >访问控制列表**并且单击**添加新**。
- 选择延长并且输入ACL名称。
- 此图片显示典型的重定向ACL的示例：

**注意**：线路10可选。这为排除故障通常被添加报价。此ACL如果允许对DHCP， DNS服务并且到ISE服务器端口TCP 8443(Deny ACE)。HTTP和HTTPS流量重新定向(Permit ACE)。

### 命令行界面(CLI)配置

在上一个步骤讨论的所有配置可能通过CLI也应用。

### 全局启用的802.1x

```
dot1x system-auth-control
```

### 全局AAA配置

```
aaa new-model
!
aaa authentication dot1x ISE_Method group ISE_Group
aaa authorization network ISE_Method group ISE_Group
aaa accounting Identity ISE_Method start-stop group ISE_Group
!
aaa server radius dynamic-author
 client 14.36.157.210 server-key *****
 client 14.36.157.21 server-key *****
 auth-type any
!
radius server ISE1
 address ipv4 14.36.157.210 auth-port 1812 acct-port 1813
 timeout 5
 retransmit 2
 key *****
!
radius server ISE2
 address ipv4 14.36.157.21 auth-port 1812 acct-port 1813
 timeout 5
 retransmit 2
 key *****
!
!
aaa group server radius ISE_Group
 server name ISE2
 server name ISE1
 deadtime 10
 mac-delimiter colon
!
```

### WLAN配置

```
 wlan Guest 1 Guest
 aaa-override
 accounting-list ISE_Method
 client vlan VLAN0301
 mac-filtering MacFilterMethod
 nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security dot1x authentication-list ISE_Method
 no security ft over-the-ds
 session-timeout 28800
 no shutdown
```

### 重定向ACL示例

```
3850#show ip access-lists Guest_Redirect
Extended IP access list Guest_Redirect
    10 deny icmp any any
    20 deny udp any any eq bootps
    30 deny udp any any eq bootpc
    40 deny udp any any eq domain
    50 deny tcp any host 14.36.157.210 eq 8443
    60 deny tcp any host 14.36.157.21 eq 8443
    70 permit tcp any any eq www
    80 permit tcp any any eq 443
```

### HTTP和HTTPS支持

```
3850#show run | inc http
ip http server
ip http secure-server
```

**注意**：如果应用ACL限制对WLC的访问在HTTP，影响重定向。

## 配置ISE

此部分描述在ISE要求的配置支持在本文讨论的所有用途事例。

### 普通的ISE配置任务

1. 登陆对ISE并且导航到**Administration >网络资源>网络设备**并且单击**添加**
2. 输入**名称**关联对WLC和设备**IP地址**。
3. 检查**RADIUS验证设置**方框并且键入在WLC侧配置的**共享塞克雷**。然后请点击**提交**。

4. 导航对**策略>验证**和在**MAB下**单击**编辑**并且保证那在**使用下：内部终端**选项，如果没有**找到用户**设置**继续**默认情况下(应该在那里)。

### 用例1 ：与访客验证的CWA在每用户连接

### 流概述

1. 无线用户连接对访客SSID。
2. WLC验证根据其MAC地址的终端使用ISE作为AAA服务器。
3. ISE回归上一步和access-accept与两属性值对(AVPs) ：url重新定向和url-redirect-acl。一旦WLC应用此AVPs给终端会话，站点在CENTRAL_WEB_AUTH过渡了到DHCP要求，并且，一旦获取IP地址它坚持。在此步骤WLC准备开始重定向客户端的http/HTTPS流量。
4. 最终用户打开Web浏览器，并且，一旦HTTP或HTTPS流量生成， WLC重定向用户到ISE访客门户。
5. 一旦用户到访客门户提示输入访客凭证(在这种情况下赞助商创建)。
6. 在凭证验证ISE显示AUP页，并且，一旦客户端接受，一个动态CoA类型Re-authenticate被派出对WLC。
7. WLC重新处理过滤验证的MAC，无需发出DE验证对移动站点。这应该是无缝的对终端。
8. 一旦再验证事件发生ISE复评授权策略，并且这次终端给Permit访问，因为有一个上一个成功的访客验证事件。

在用户连接对SSID时候，此进程重复操作自己。

### 配置

1. 导航对ISE并且导航对**工作区>访客访问>配置>访客门户**>选择**被赞助的访客门户**(或请创建一新的门户类型赞助访客)。
2. 在**访客设备已注册下**设置不选定所有选项并且点击**"Save"**。

3. 导航对**策略>Policy元素>结果>授权>授权配置文件**。单击 Add。

4. 此配置文件增加对WLC重定向**URL**和重定向URL **ACL**以回应最初的MAC验证旁路(MAB)请求。

- 一旦**Web重定向(CWA， MDM， NSP， CPP)**检查请选择**集中化Web验证**，然后键入重定向ACL名称在**ACL**字段下和在**值下**选择**被赞助的访客Portal(default)** (或在上一个步骤创建的其他特定门户)。

配置文件应该查找类似那个在此图片。然后单击保存。

属性详细信息在页底端属性值Pairs(AVPs)，当他们是推送对WLC

5. 导航对**策略>授权**并且插入新规则。此规则是触发重定向进程以回应从WLC的最初的MAC验证请求的那个。(在这种情况下呼叫**Wireless_Guest_Redirect**)。

6. 在**情况下请**选择**选择从库的现有情况**，然后在**条件名下请**选择**复合条件**。选择呼叫**Wireless_MAB的**一个预定义的复合条件。

> **注意**：此情况包括以访问请求产生的形式预计的2个RADIUS属性WLC (NAS-Port-Type= IEEE 802.11 <present在是指一个特定请求MAC验证bypass>)的所有无线requests>和服务类型=呼叫Check<

7. 在结果下，请选择**英文虎报> CWA_Redirect** (在上一步创建的授权配置文件)。然后请单击**完成**和**"Save"**

**8.** 导航对结尾的**CWA_Redirect**规则并且单击箭头在旁边**编辑**。然后请选择**上面重复项**。

9. 请修改名称，因为这是终端匹配会话一次重新鉴别在艾斯的CoA的策略(在这种情况下Wireless_Guest_Access)。

10. 在**Wireless_MAB**复合条件旁边请点击**+**展开条件的符号，并且在**Wireless_MAB**情况以前请单击**添加属性/值**。

11. 下面"请选择属性"选择**网络访问> UseCase等于访客流**

**12.** 在**权限下请**选择**PermitAccess**。然后请单击**完成**和**"Save"**

两项策略应该看起来类似于此：

**用例2 ：与一天一次强制执行访客验证的设备已注册的CWA。**

**流概述**

1. 无线用户连接对访客SSID。

2. WLC验证根据其MAC地址的终端使用ISE作为AAA服务器。
3. ISE回归上一步和access-accept与两属性值对(AVPs) (url重新定向和url-redirect-acl)。
4. 一旦WLC应用此AVPs给终端会话，站点在CENTRAL_WEB_AUTH过渡了到DHCP要求，并且，一旦获取IP地址它坚持。在此步骤WLC准备开始重定向客户端的http/HTTPS流量。
5. 最终用户打开Web浏览器，并且，一旦HTTP或HTTPS流量生成， WLC重定向用户到ISE访客门户。
6. 一旦用户到访客门户，他得到提示输入赞助商创建的凭证。
7. 在凭证验证ISE添加此终端到一特定(已经预配置)终端标识组(设备已注册)。
8. AUP页显示和，一旦客户端接受，一个动态CoA类型重新鉴别。被派出对WLC。
9. 重新处理MAC的WLC过滤验证，不用发出DE验证对移动站点。这应该是无缝的对终端。
10. 一旦再验证事件发生ISE复评授权策略。这次，因为终端是正确终端标识组ISE的成员返回访问接受没有限制。
11. 因为终端在步骤6注册，每次那用户回来，他在网络允许，直到从ISE手工删除，或者终端清除策略运行冲洗满足标准的终端。

在此实验室情形中，验证一天一次被强制执行。再验证触发是终端每天删除被使用的终端标识组所有终端的清除策略。

**注意**：强制执行根据消逝的时间的访客验证事件从最后AUP接受是可能的。这可能是选项，如果需要经常强制执行一天一次的访客登录(在示例每4个小时)。

## 配置

1. 在ISE请导航对**工作区>访客访问>配置>访客门户>**选择**被赞助的访客门户**(或请创建一新的门户类型赞助访客)。
2. 在**访客设备已注册**设置下请验证选项**自动地注册设备**被检查的**访客**。单击 **Save**。

3. 导航对**工作区>访客访问>配置>访客类型**或点击快捷方式指定在访客设备已注册设置下在门户。

4. 当赞助商用户创建访客帐户时，他分配访客类型到它。每个单个访客类型能有属于一不同的终端标识Group.To分配终端标识组应该添加对，选择访客类型这些来宾用户的赞助商用途设备的一个已注册终端(此用例根据每星期(默认))。

5. 一旦在访客类型，在**洛金选项下请**选择从下拉菜单**终端标识组的**终端组**访客设备已注册的**

**6.** 导航对**策略>Policy元素>结果>授权>授权配置文件**。单击 **Add**。

7. 此配置文件增加对WLC重定向**URL**和重定向URL **ACL**以回应最初的MAC验证旁路(MAB)请求。

- 一旦**Web重定向(CWA， MDM， NSP， CPP)**检查请选择**集中化Web验证**，然后键入重定向ACL名称在**ACL**字段下和在**值下**选择为此流创建的门户(**CWA_DeviceRegistration**)。

8. 导航对**策略>授权**并且插入新规则。此规则是触发重定向进程以回应从WLC的最初的MAC验证请求的那个。(在这种情况下呼叫**Wireless_Guest_Redirect**)。

9. 在**情况下**选择**选择从库的现有情况**，然后在**条件名下请**选择**复合条件**。选择呼叫**Wireless_MAB的**一个预定义的复合条件。

10. 在结果下，请选择**英文虎报> CWA_DeviceRegistration** (在上一步创建的授权配置文件)。然后请单击**完成**和**"Save"**

**11.** 请复制以上的策略，修改其名称，因为这是终端点击的策略，在从再验证事件后返回(呼叫

Wireless_Guest_Access)。

12. 在**标识组下选派**方框，选择**终端标识组**并且选择您参考在访客Type(GuestEndpoints)下的组。

13. 在结果下请选择**PermitAccess**。点击**完成**并且**保存**更改。

14. 创建和终端清除GuestEndpoint组日报的清除策略。

- 导航对**Administration >身份管理>设置>终端清除**
- 默认情况下根据**清除**规则，如果消逝的时间比30天，极大应该有一个该触发GuestEndpoints删除。
- (万一默认删除)，请修改GuestEndpoints的现有策略或创建新的。注意清除策略每天运行定义的时间。

在这种情况下情况是GuestEndpoints的成员与经过天数的少于1天

**用例3 ：Hostspot门户**

**流概述**

1. 无线用户连接对访客SSID。
2. WLC验证根据其MAC地址的终端使用ISE作为AAA服务器。
3. ISE回归返回与两属性值对(AVPs)的一access-accept ：url重新定向和url-redirect-acl。
4. 一旦WLC应用此AVPs给终端会话，站点在CENTRAL_WEB_AUTH过渡了到DHCP要求，并且，一旦获取IP地址它坚持。在此步骤WLC准备重定向客户端的http/HTTPS流量。
5. 最终用户打开Web浏览器，并且，一旦HTTP或HTTPS流量生成， WLC重定向用户到ISE热点门户。
6. 一旦在门户提示用户接受可接受的使用规定。
7. ISE添加终端MAC地址(端点ID)到配置的终点标识组。
8. Services节点的策略(PSN)该处理请求发出动态CoA类型Admin**重置**对WLC。
9. 一旦WLC完成处理流入CoA，发出DE验证给客户端(连接是用为了客户端能回来)时间的损耗。
10. 一旦客户端重新连接，个新会话创建那么那里是在ISE侧的没有会话连续性。意味着验证处理，当一个新的线索。
11. 因为终端被添加到配置的终点标识组，并且有检查的授权策略终端是否是该组的一部分，新证书匹配此策略。结果是全部存取的对访客网络。
12. 由于终端清除策略，除非终端标识对象从ISE数据库清除用户不应该必须再接受AUP。

**配置**

1. 创建一新的终端标识组移动这些设备向在注册。导航给**工作区>访客访问>标识Groups>终端标识组**并且单击 。

- 输入组名(在这种情况下HotSpot_Endpoints)。添加一说明，并且父组不是需要的。

2. 导航对**工作区>访客访问>配置>访客门户**>选择**热点门户(默认**)。

3. 展开门户设置，并且在终端标识组下请选择**HostSpot_Endpoints**组在**终端标识组下。**这发送注册的设备给指定的组。

4.**保存**更改。

5. 创建要求热点门户WLC产生的MAB验证的授权配置文件。

- 导航对**策略>Policy元素>结果>授权>授权配置文件**并且创建一(HotSpotRedirect)。
- 一旦**Web重定向(CWA， MDM， NSP， CPP)**被检查请在ACL字段(Guest_Redirect)选择**热点**，然后键入重定向ACL名称和，值挑选正确门户(**热点门户(默认)**)。

6. 创建触发HotSpotRedirect结果在从WLC的初始MAB请求的授权策略。

- 导航对**策略>授权**并且插入新规则。此规则是触发重定向进程以回应从WLC的最初的MAC验证请求的那个。(在这种情况下呼叫**Wireless_HotSpot_Redirect**)。
- 在**情况下请**选择**选择从库的现有情况**，然后在**条件名下请**选择**复合条件**
- 在结果下，请选择**英文虎报> HotSpotRedirect** (在上一步创建的授权配置文件)。然后请单击**完成**和**"Save"**

7. 创建第二项授权策略。

- 请复制以上的策略，修改其名称，因为这是终端点击的策略，在从再验证事件后返回(呼叫Wireless_HotSpot_Access)。
- 在**标识组下选派**方框，选择**终端标识组**然后您及早创建的组(**HotSpot_Endpoints**)。
- 在结果下请选择**PermitAccess**。点击**完成**并且**保存**更改。

8. 配置清除与消逝的时间了不起的比5天的终端的清除策略。

- 导航对**Administration >身份管理>设置>终端清除，**并且在清除下规则创建新的。
- 在**标识组详细信息**方框下请选择**终端标识组> HotSpot_Endpoints**
- 在**情况下请**单击**创造新的条件(Advanced选项)**。
- 下面请选择属性选择*ENDPOINTPURGE ：ElapsedDays GREATERTHAN* 5天

# 验证

## 用例1

1. 用户连接对访客SSID。
2. 他打开浏览器，并且，当HTTP数据流生成，访客门户显示。
3. 一旦来宾用户验证并且接受AUP，成功页显示。
4. 重新鉴别CoA被派出(透明对客户端)。
5. 终端会话重新鉴别与对网络的完全权限。
6. 所有随后的访客连接必须在获得访问前通过访客验证到网络。

从ISE RADIUS Live日志的流：

## 用例2

1. 用户连接对访客SSID。
2. 他打开浏览器，并且，当HTTP数据流生成，访客门户显示。
3. 一旦来宾用户验证并且接受AUP，设备注册。
4. 成功页显示，并且重新鉴别CoA被派出(透明对客户端)。
5. 终端会话重新鉴别与对网络的完全权限。
6. 所有随后的阵风连接9s允许，无需强制执行访客验证，只要终端仍然在配置的终点标识组中。

从ISE RADIUS Live日志的流：

### 用例3

1. 用户连接对访客SSID。
2. 他打开浏览器，并且，当HTTP数据流生成， AUP页显示。
3. 一旦来宾用户接受AUP，设备注册。
4. 成功页显示，并且Admin重置CoA被派出(透明对客户端)。
5. 终端与对网络的完全权限重新连接。
6. 所有随后的阵风连接允许，无需强制执行AUP接受(除非配置)为，只要终端在配置的终点标识组中依然是。

## FlexConnect本地交换在AireOS

当FlexConnect本地交换配置时网络Admin需要以保证那：

- 重定向ACL配置作为FlexConnect ACL。
- 不管怎样重定向ACL应用作为一项策略通过在**FlexConnect**选项卡下的AP **>外部WebAuthentication ACL >策略>**选择重定向ACL并且单击**应用**

或者通过添加策略ACL到FlexConnect组属于对(**无线> FlexConnect Groups>**选择正确**映射的**组>的**ACL >策略**选择重定向ACL并且单击添加)

策略ACL新增内容触发WLC增加已配置的ACL到FlexConnect组的AP成员。疏忽执行此导致Web重定向问题。

## 外国锚点方案

在自动锚点中(外国–锚点)方案突出显示以下事实是重要的：

- 重定向ACL在外国和锚点WLC需要定义。既使当它在锚点只被强制执行。
- Layer2验证由外国WLC总是处理。这在设计阶段期间是关键(也排除故障)作为所有RADIUS验证，并且认为的流量发生在ISE和外国WLC之间。

- 一旦重定向AVPs应用给客户端会话外国WLC通过移动性移交消息更新锚点的客户端会话。
- 这时锚点WLC开始强制执行预先了配置的重定向使用重定向ACL。
- 在锚点WLC SSID应该完全关闭核算避免去往ISE的认为的更新(参考同一个验证事件)来自两个锚点和外国。
- URL外国锚点方案不支持基于ACL。

# 故障排除

## AireOS和聚合的访问WLC的普通的被中断的状态

1. **客户端无法加入访客SSID**

“请**显示客户端被选派的xx: xx ： xx ： xx ： xx ： xx**”表示客户端在**开始**被滞留。 通常这是无法的WLC的指示器适用属性AAA服务器返回。

验证ISE推送的重定向ACL名称完全地匹配预定义的ACL的名称在WLC的。

同一个原理适用对其他属性您配置ISE增加到WLC (VLAN ID、接口名称、Airespace ACL等等)。客

户端应该然后过渡到DHCP然后CENTRAL_WEB_AUTH。

2. **重定向AVPs应用给客户端会话，但是重定向不工作**

验证客户端的Policy Manager状态是与有效IP地址的CENTRAL_WEB_AUTH根据SSID的已配置的动态接口并且重定向ACL和Url重新定向属性应用给客户端会话。

**重定向ACL**

在AIreOS WLCs重定向ACL应该明显地允许不应该重定向的在TCP端口8443的流量，类似DNS和ISE在两个方向，并且隐式deny ip any any触发将重定向的流量的其余。

在聚合的访问逻辑是对面。当permit ACE触发重定向时，请拒绝ACE旁路重定向。这就是为什么明确地推荐给permit tcp端口80和443。

验证对ISE的访问在从访客VLAN的端口8443。如果一切看起来好从配置方面移动向前的简便的方法是获取一个捕获在客户端的无线适配器背后和验证重定向中断的地方。

- DNS resoultion是否发生？
- TCP 3方式握手完成请求的页？
- 在客户端启动GET后， WLC是否返回重定向操作？
- ISE的TCP 3方式握手8443完成？

3. **客户端无法在ISE以后访问网络推送VLAN更改在访客流结束时**

一旦客户端在流(前重定向状态)初获取IP地址，如果VLAN更改增加，在访客验证发生(发表物CoA后请重新鉴别)，强制DHCP版本的唯一方法/在流的访客更新(没有状态代理程序)是通过Java程序在移动设备不工作。

这留给客户端黑洞在VLAN x用VLAN Y.的IP地址。 应该考虑这，当计划解决方案时。

4. **在重定向期间， ISE显示"HTTP 500内部错误，在访客客户端浏览器的Radius会话没被找到的"消息**

这通常是会话丢失指示器在ISE的(会话终止)。当外国锚点部署时，此的多数常见原因在锚点WLC认为配置。 修复认为在锚点的此禁用和留下外国把柄验证和核算。

5.**客户端在艾斯的热点门户断开并且保持断开或连接对一不同的SSID在接受AUP以后。**

这在热点可能预计由于在此流涉及的授权(CoA)的动态崔凡吉莱(CoA重置的Admin)该原因WLC发出deauth对无线站点。多数无线终端没有任何问题回来到SSID，在DE验证发生后，但是客户端在某些情况下连接对另一首选的SSID以回应DEauthenitcate事件。什么都不可以从ISE或WLC完成防止此，当是至坚持的无线客户端原始SSID，或者连接到另一可用的(首选的) SSID。

在这种情况下无线用户应该手工连接回到热点SSID。

## AireOS WLC

```
(Cisco Controller) >debug client <MAC addr>
```

调试调试在客户端状态系统涉及的一套的客户端集组件更改。

```
(Cisco Controller) >debug client <MAC addr>
```

Debug aaa组件

```
(Cisco Controller) >debug client <MAC addr>
```
这可能是影响资源根据通过MAB或Dot1x SSID连接的相当数量用户。 在调试级别的这些组件记录在WLC和ISE之间的AAA处理并且打印在屏幕的RADIUS信息包。

这是关键，如果您ISE可能不提供预计属性，或者，如果WLC不正确地处理他们。

Web-auth重定向

```
(Cisco Controller) >debug client <MAC addr>
```
这可以用于验证WLC顺利地触发重定向。这是示例重定向如何应该看起来象从调试：

```
(Cisco Controller) >debug client <MAC addr>
```

## NGWC

调试调试在客户端状态系统涉及的一套的客户端集组件更改。

```
(Cisco Controller) >debug client <MAC addr>
```
此组件打印RADIUS信息包(验证和核算)在屏幕。这是方便的，当您需要验证时ISE传送正确AVPs并且验证CoA正确地发送并且处理。

```
(Cisco Controller) >debug client <MAC addr>
```
这所有AAA转变(验证、授权和核算)无线客户端是包含的地方。这是关键验证WLC正确地解析AVPs并且应用他们给客户端会话。

```
(Cisco Controller) >debug client <MAC addr>
```
当您怀疑在NGWC时的重定向问题这能已启用。

```
(Cisco Controller) >debug client <MAC addr>
```

## ISE

### RADIUS Live日志

验证最初的MAB请求正确地处理在ISE，并且ISE推回预计属性。导航对**操作> RADIUS> Live日志**并且过滤输出使用客户端MAC在**端点ID下**。一旦找到验证事件，请点击详细信息然后验证结果推送作为接受一部分。

### Tcpdump

此功能，当一更深的调查在ISE和WLC之间的RADIUS信息包交换是需要的时，可以使用。这样您能证明， ISE发送在access-accept的正确属性，不用必须在WLC侧的关闭调试。要开始捕获使用TCDDump导航到**操作>请排除故障>诊断工具>General Tools> Tcpdump。**

这是通过Tcpdump捕获的一个正确流的示例

这是AVPs发送以回应初始MAB请求(在以上的屏幕画面的第二数据包)。

```
(Cisco Controller) >debug client <MAC addr>
```
**终端调试：**

如果需要潜水深到介入政策决策的ISE进程，门户选择、访客验证、CoA处理等等接近此的简便的方法是启用**Endpoit调试**而不是必须设置完整组件为调试级别。

要启用此，请导航对**操作>故障排除> DiagnosticTools >General Tools>终端调试。**

一旦在终端调试页，请输入终端MAC地址并且点击开始，当准备好时再创问题。

一旦调试被终止了请点击识别端点ID下载debug输出的链路。

# 相关信息

TAC推荐了AireOS修造

Cisco无线控制器配置指南，版本8.0。

思科身份服务引擎管理员指南，版本2.1

通用NGWC无线配置用身份服务引擎