使用AireOS和下一代WLC配置ISE无线CWA和热点流

目录

简介

本文档介绍如何在带有Cisco AireOS和下一代无线局域网控制器的身份服务引擎中配置三个访客案例。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科无线局域网控制器（统一和融合接入）
- 身份服务引擎 (ISE)

使用的组件

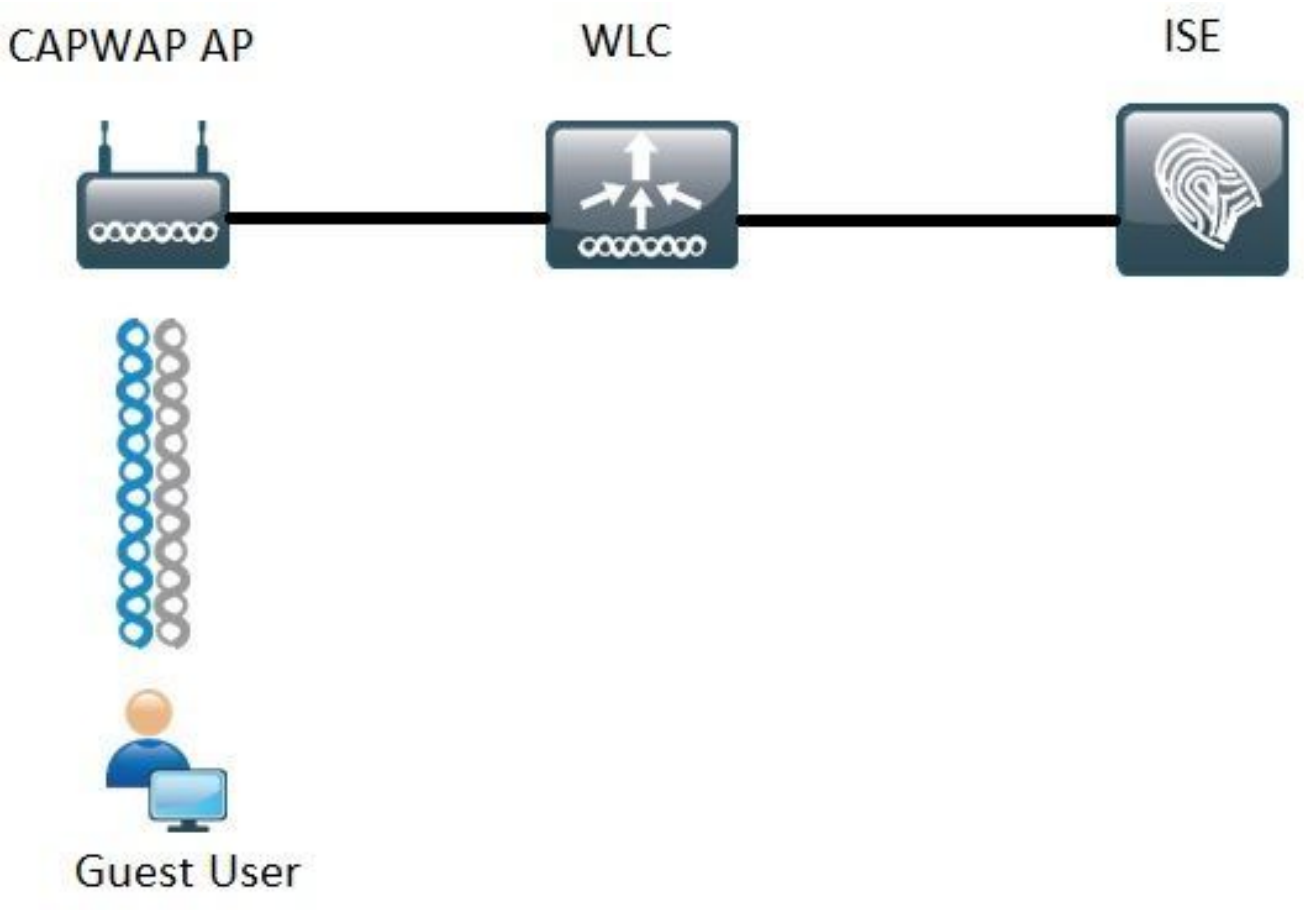
本文档中的信息基于以下软件和硬件版本：

- 思科身份服务引擎版本2.1
- 思科无线局域网控制器5508，带8.0.121.0
- 下一代无线控制器(NGWC)catalyst 3850(WS-C3850-24P)，带03.06.04.E

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。

配置

网络图



本文档介绍的步骤介绍统一接入WLC和融合接入WLC上的典型配置，以支持任何使用ISE的访客流。

配置Unified 5508 WLC

无论在ISE中配置何种使用案例，从WLC的角度来看，它都以无线端点开始，该端点连接到启用了MAC过滤的开放式SSID（以及AAA覆盖和RADIUS NAC），该端点指向ISE作为身份验证和记帐服务器。 这可以确保ISE将必要的属性动态推送到WLC，以便成功实施重定向到ISE的访客门户。

全局配置

1.将ISE全局添加为身份验证和记帐服务器。

- 导航到**安全> AAA >身份验证**，然后点击**新建**

- 输入ISE服务器IP和共享密钥
- 确保服务器状态和**RFC 3676支持**（授权更改或CoA支持）均设置为**启用**。
- 在服务器超时下，默认情况下AireOS WLC有2秒。取决于网络特征（延迟、不同位置的ISE和WLC），将服务器超时至少增加到5秒可避免不必要的故障切换事件。
- 单击 **Apply**。
- 如果有多个要配置的策略服务节点(PSN)，请继续创建其他服务器条目。

注意：此特定配置示例包括2个ISE实例

- 导航到**安全> AAA > RADIUS >记帐**，然后点击**新建**
- 输入ISE服务器IP和共享密钥
- 确保Server Status设置为Enabled
- 如有必要，增加服务器超时（默认值为2秒）。

2.回退配置。

在统一环境中，一旦触发服务器超时，WLC将移至下一个配置的服务器。WLAN中的下一行。如果没有其它可用服务器，则WLC会选择全局服务器列表中的下一个可用服务器。当故障切换发生后，在SSID（主、辅助）上配置多个服务器时，WLC默认继续将身份验证和（或）记帐流量永久发送到辅助实例，即使主服务器重新联机也是如此。

为了缓解此行为，请启用回退。导航到**安全> AAA > RADIUS >回退。**默认行为是关闭的。从服务器关闭事件恢复的唯一方法需要管理员干预（全局退回服务器的管理员状态）。

要启用回退，您有两个选项：

- **被动** — 在被动模式下，如果服务器不响应WLC身份验证请求，则WLC将服务器移至非活动队列并设置计时器（Interval in Sec选项）。当计时器到期时，WLC将服务器移至活动队列，而不考虑服务器的实际状态。如果身份验证请求导致超时事件（这意味着服务器仍然停机），服务器条目会再次移动到非活动队列，并且计时器再次启动。如果服务器成功响应，则它仍保留在活动队列中。此处的可配置值范围为180至3600秒。

- **主用 — 在主用模式**下，当服务器不响应WLC身份验证请求时，WLC将服务器标记为停机，然后将服务器移至非主用服务器池，并定期开始发送探测消息，直到该服务器响应为止。如果服

务器响应，则WLC将失效服务器移至活动池并停止发送探测消息。
在此模式下，WLC要求您输入用户名和探测间隔（以秒为单位）（180到3600）。

注意：WLC探测功能不需要身份验证成功。无论哪种方式，成功或失败的身份验证都被视为服务器响应，足以将服务器提升到活动队列。

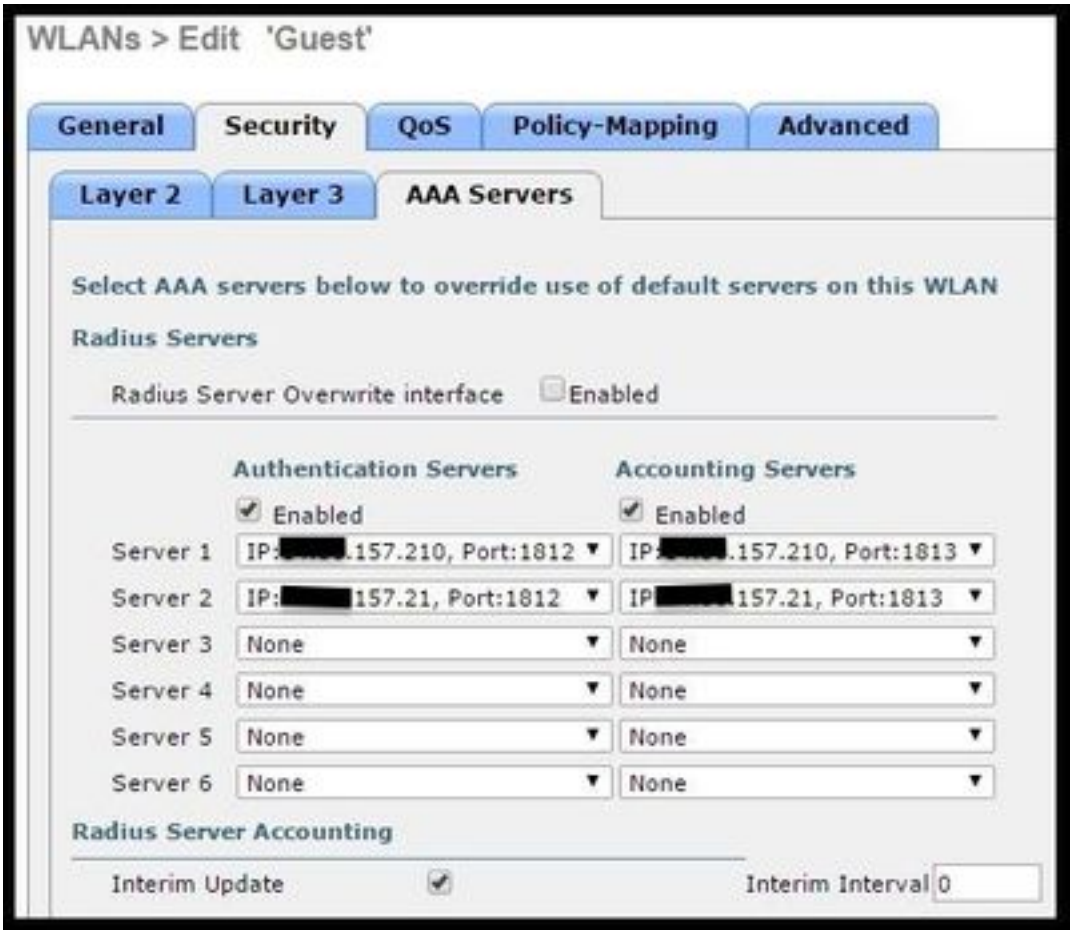
配置访客的服务集标识符(SSID):

- 导航到WLANs选项卡，在Create New选项下单击**Go**:

- 输入配置文件名称和SSID名称。单击 **Apply**。
- 在General选项卡下，选择要使用的接口或接口组（访客VLAN）。

- 在**Security > Layer 2 > Layer 2 Security**下选择**None**并启用**Mac Filtering**复选框。

- 在**AAA Servers**选项卡下，将Authentication and Accounting servers设置为**enabled**，并选择您的主要和辅助服务器。



- **临时更**新：这是一个可选配置，不会为此流程增加任何优势。如果您希望启用它，则WLC必须运行8.x或更高版本的代码：

已禁用：功能已完全禁用。

启用0间隔：每当客户端的移动站控制块(MSCB)条目(即IPv4或IPv6地址分配或更改，客户端漫游事件。) 不会发送额外的定期更新。

使用已配置的临时间隔启用：在此模式下，WLC在客户端的MSCB条目更改时向ISE发送通知，并在已配置的间隔发送其他定期记帐通知（无论任何更改）。

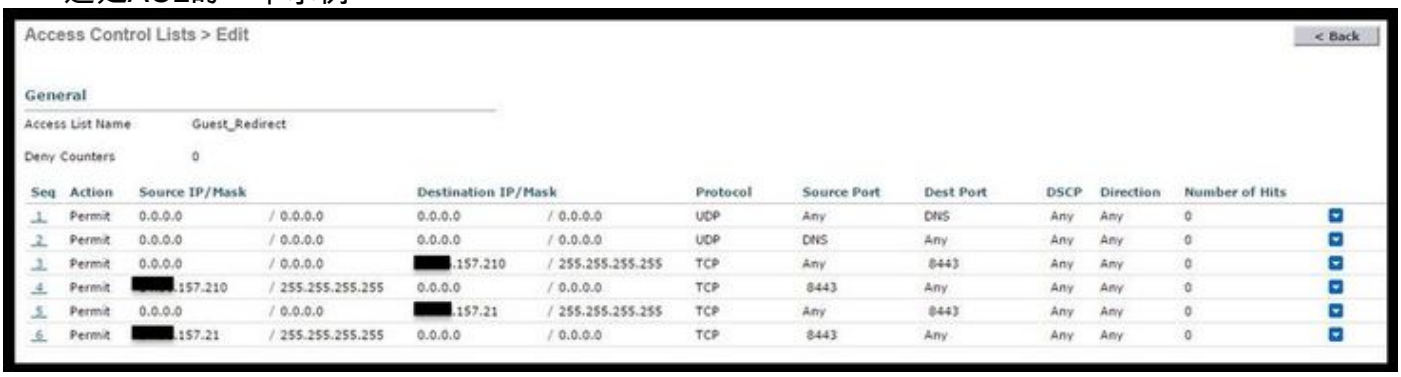
- 在Advanced Tab Enable **Allow AAA Override**下，在**NAC state**下，选择**RADIUS NAC**。这可确保WLC应用来自ISE的任何属性值对(AVP)。
- 导航到SSID常规选项卡，并将SSID状态设置为**Enabled**

- **应**用更改。

配置重定向ACL

此ACL由ISE引用，它确定重定向哪些流量以及允许哪些流量通过。

- 转至**Security**选项卡> **Access Control Lists**，然后单击**New**
- 这是ACL的一个示例


Access Control Lists > Edit

< Back

General

Access List Name Guest_Redirect

Deny Counters 0

Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	UDP	Any	DNS	Any	Any	0
2	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	UDP	DNS	Any	Any	Any	0
3	Permit	0.0.0.0	/ 0.0.0.0	[redacted].157.210	/ 255.255.255.255	TCP	Any	8443	Any	Any	0
4	Permit	[redacted].157.210	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	TCP	8443	Any	Any	Any	0
5	Permit	0.0.0.0	/ 0.0.0.0	[redacted].157.21	/ 255.255.255.255	TCP	Any	8443	Any	Any	0
6	Permit	[redacted].157.21	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	TCP	8443	Any	Any	Any	0

此ACL必须允许通过TCP端口8443访问DNS服务和ISE节点。底部有一个隐式拒绝，表示其余流量重定向到ISE的访客门户URL。

HTTPS重定向

此功能在AireOS版本8.0.x及更高版本中受支持，但默认情况下处于关闭状态。要启用HTTPS支持，请转到WLC **Management > HTTP-HTTPS > HTTPS Redirection**并将其设置为**Enabled**，或在CLI中应用此命令：

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

启用HTTPS重定向后的证书警告

启用https-redirect后，用户可能会在重定向期间遇到证书信任问题。即使控制器上有有效的链式证书，并且即使该证书由第三方受信任证书颁发机构签名，也会出现这种情况。原因是WLC上安装的证书已颁发给其虚拟接口主机名或IP地址。当客户端尝试https://cisco.com时，浏览器期望将证书颁发给cisco.com。但是，为了让WLC能够截取客户端颁发的GET，它首先需要建立HTTPS会话，WLC在SSL握手阶段为其提供其虚拟接口证书。这会导致浏览器显示警告，因为在SSL握手过程中显示的证书尚未颁发给客户端尝试访问的原始网站(即，与WLC的虚拟接口主机名相对cisco.com)。您可以在不同的浏览器中看到不同的证书错误消息，但是这些错误消息都与同一问题有关。

主动故障转移

默认情况下，此功能在AireOS WLC中启用。启用主动故障切换时，WLC会将AAA服务器标记为无响应，并在RADIUS超时事件影响一个客户端后移至下一个配置的AAA服务器。

禁用此功能后，仅当至少3个客户端会话发生RADIUS超时事件时，WLC才会故障切换到下一台服务器。此命令可以禁用此功能（此命令不需要重新启动）：

```
(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
```

强制网络旁路

支持强制网络助手(CNA)机制以发现强制网络门户并自动启动登录页的终端通常通过受控窗口中的伪浏览器执行此操作，而其他终端则启动完全功能的浏览器以触发此操作。对于CNA启动伪浏览器的终端，这会中断流 重定向至ISE强制网络门户时。 这通常影响Apple IOS设备，在需要设备注册、VLAN DHCP释放和合规性检查的流中尤其有负面影响。

根据使用的流量的复杂性，建议启用强制绕行。在这种情况下，WLC忽略CNA门户发现机制，客户端需要打开浏览器以启动重定向过程。

验证功能的状态：

```
(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
```

要启用此功能，请键入以下命令：

```
(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提醒用户，要使更改生效，需要重新启动重置系统。

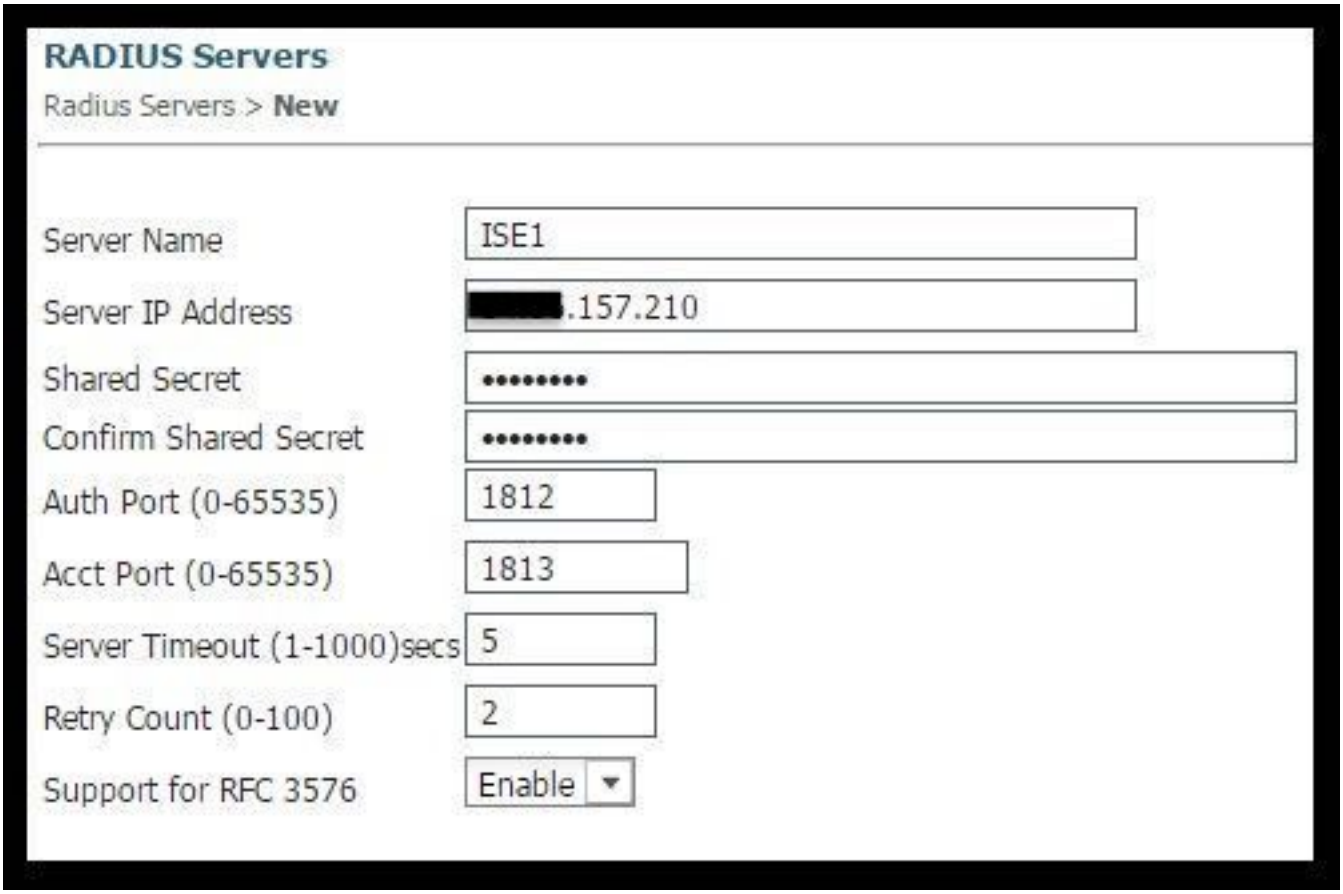
此时，**show network summary**将功能显示为已启用，但是要使更改生效，需要重新启动WLC。

配置融合3850 NGWC

全局配置

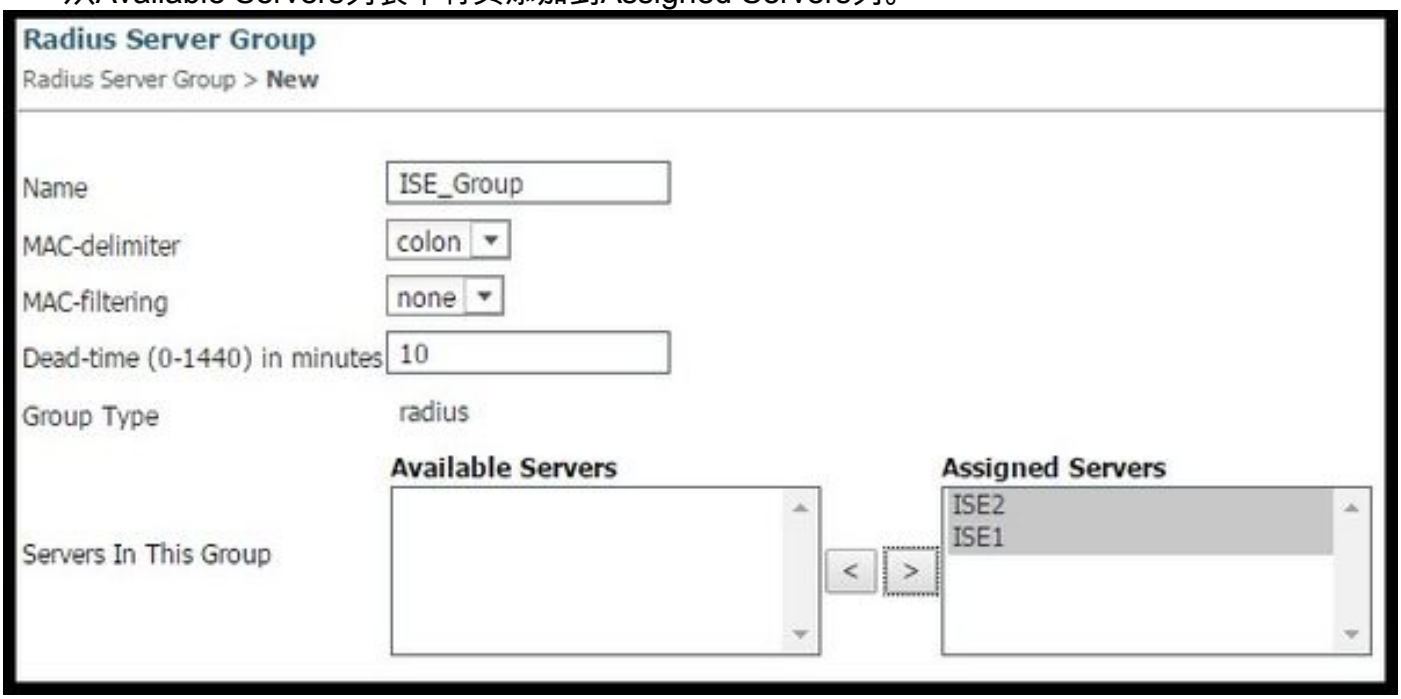
1.全**局添加ISE作为身份验证和记帐服务器**

- 导航到**Configuration > Security > RADIUS > Servers**，然后单击**New**
- 输入反映环境**条件的ISE服务器IP地址、共享密钥、服务器超时**和**重试计数。**
- 确保**支持RFC 3570**（CoA支持）。
- 重复此过程以添加辅助服务器条目。



2.创**建ISE的服务器组**

- 导航到**Configuration > Security > Server Groups**，然后单击**New**
- 为组分配名称并输入**Dead-time**值（分钟）。这是控制器将服务器保留在“非活动”队列中的时间，然后才会将其再次提升到活动服务器列表。
- 从Available Servers列表中将其添加到Assigned Servers列。

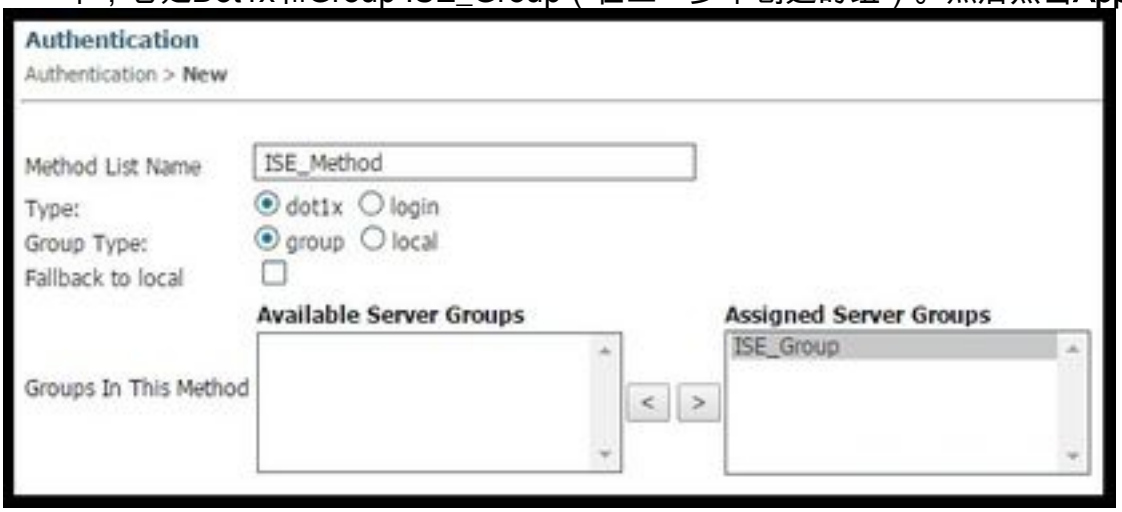


3.全**局启用Dot1x**

- 导航到**Configuration > AAA > Method Lists > General**并启用**Dot1x system Auth Control**

4.配置方法列表

- 导航到Configuration > AAA > Method Lists > Authentication，然后创建新的方法列表。在本例中，它是Dot1x和Group ISE_Group（在上一步中创建的组）。然后点击Apply

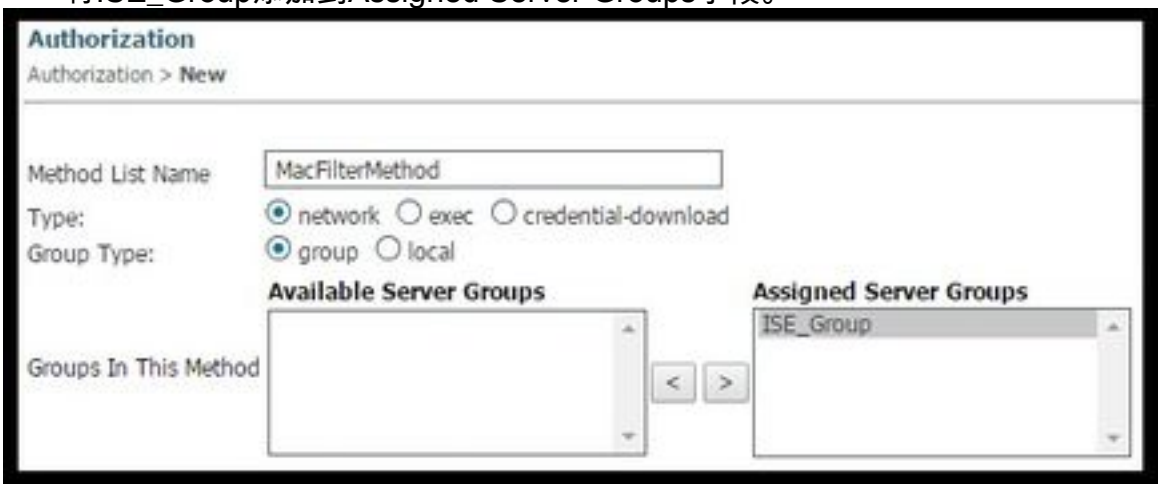


- 对记帐(Configuration > AAA > Method Lists > accounting)和授权(Configuration > AAA > Method Lists > Authorization)执行相同操作。他们一定长这样

5.创**建授权MAC过滤器方法**。

稍后会从SSID设置调用此项。

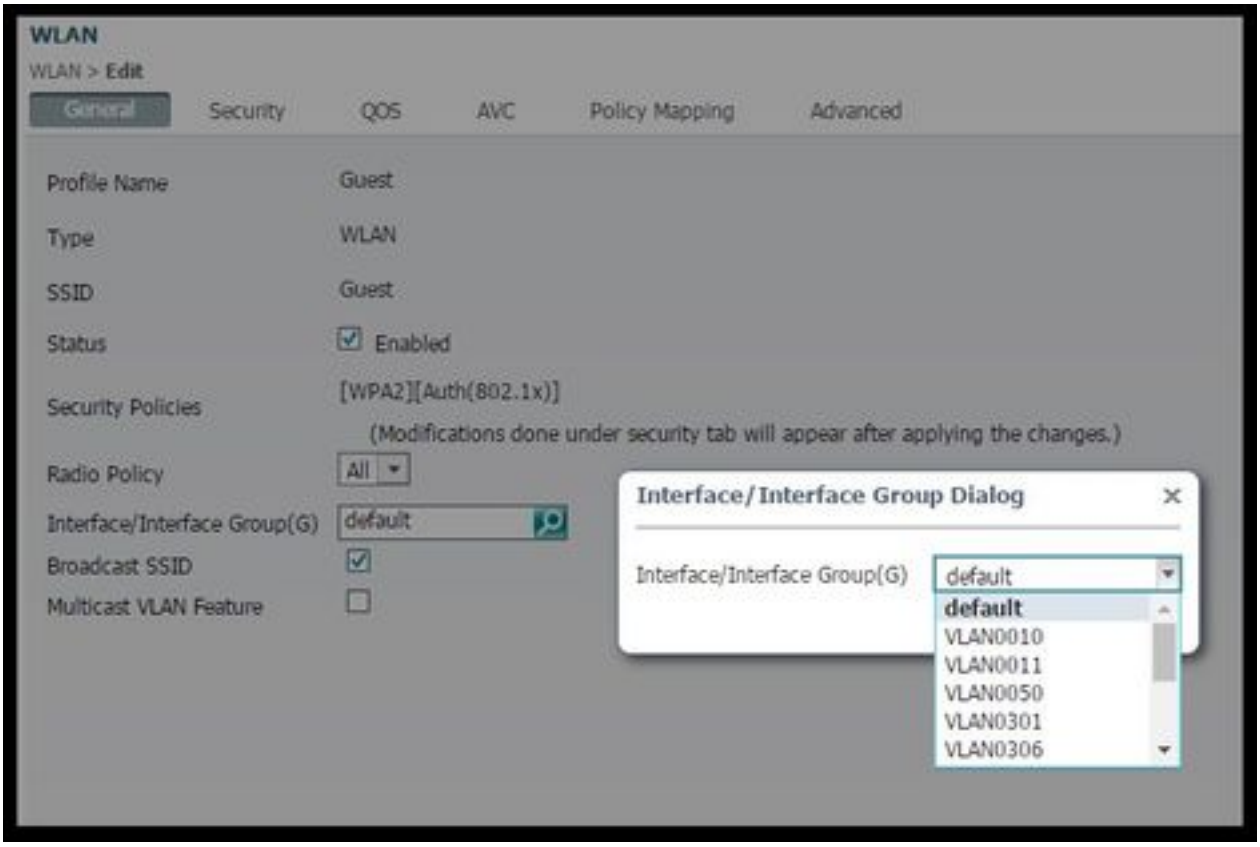
- 导航到**Configuration > AAA > Method Lists > Authorization**，然后单击**New**。
- 输入方**法列表名称**。选择**类型=网络**和**组类型组**。
- 将ISE_Group添加到Assigned Server Groups字段。



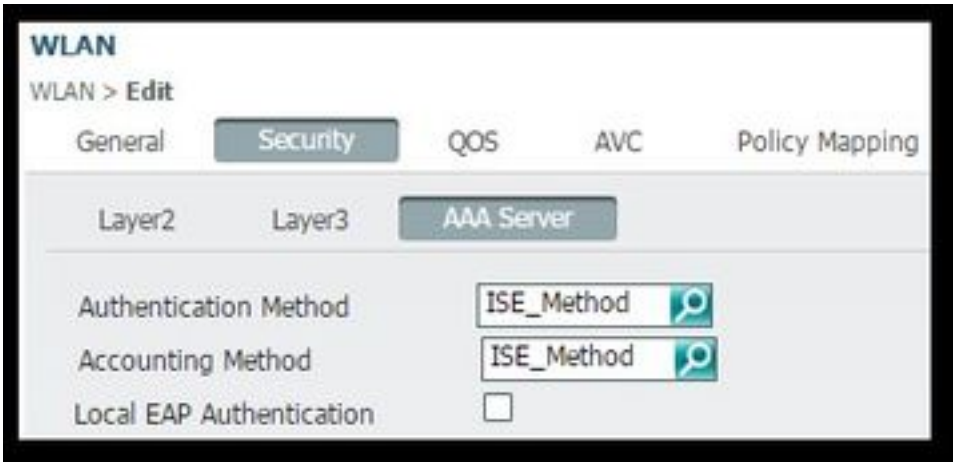
SSID 配置

1.创**建访客SSID**

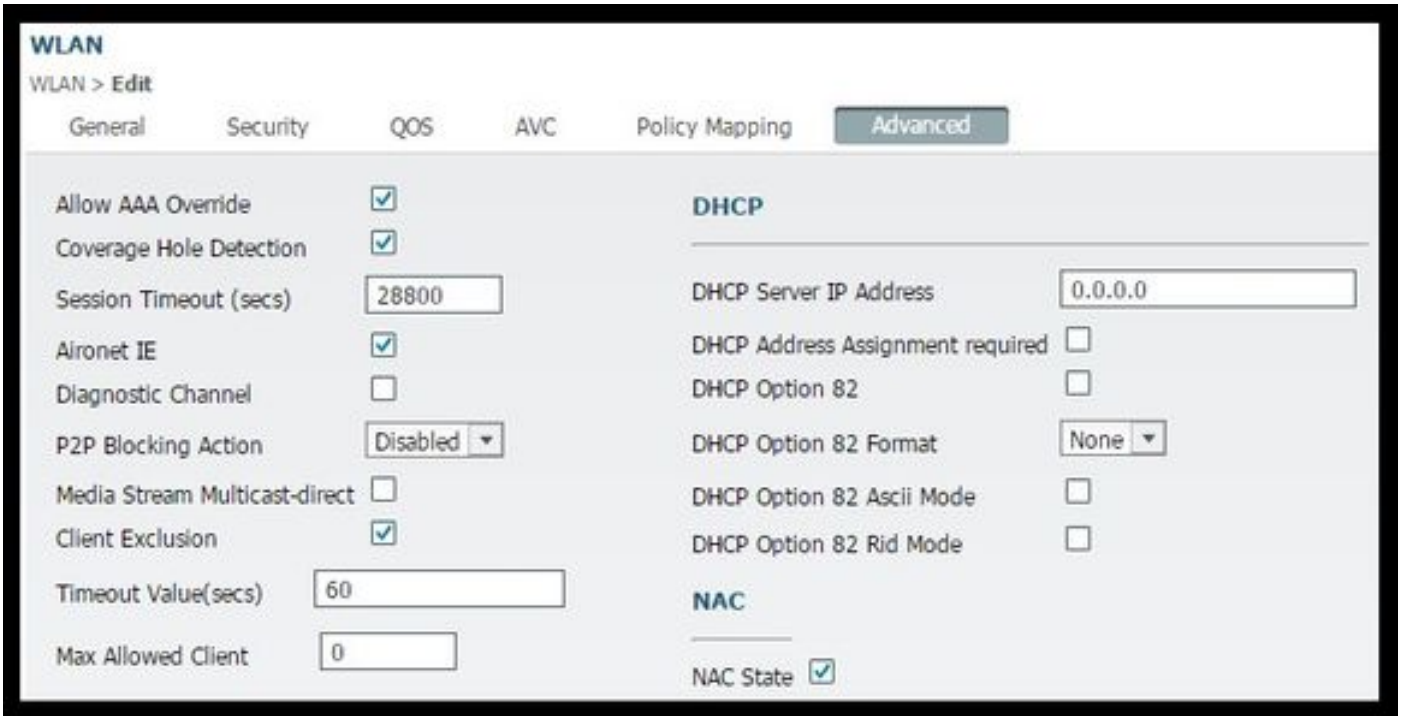
- 导航到**配置>无线> WLANs**，然后单击**新建**
- 输入WLAN ID、SSID和配置文件名称，然后点击Apply。
- 进入Interface / Interface Group下的SSID设置后，选择Guest VLAN Layer 3 interface。



- 在**Security > Layer 2**下，选择**None**，然后在**Mac Filtering**旁边输入先前配置的Mac Filter Method List Name(MacFilterMethod)。
- 在**Security > AAA Server**选项卡下，选择正确的身份验证和记帐方法列表(ISE_Method)。



- 在**Advanced**选项卡下，启用**Allow AAA Override**和**NAC state**。其他设置必须根据每个部署要求（会话超时、客户端排除、支持Aironet扩展）进行调整。



- 导航到General选项卡，将Status设置为Enabled。然后点击**应用。**

重定向 ACL 配置

ISE稍后在响应初始MAB请求的access-accept中引用此ACL。NGWC使用它来确定重定向哪些流量以及必须允许哪些流量通过。

- 导航到**configuration > security > ACL > Access Control Lists**，然后单击**Add New**。
- 选择扩展并输入ACL名称。
- 下图显示典型重定向ACL的示例：

注：行10是可选的。这通常是为建议进行故障排除而添加的。此ACL必须允许访问DHCP、DNS服务以及ISE服务器端口TCP 8443（拒绝ACE）。HTTP和HTTPS流量被重定向（允许ACE）。

命令行界面(CLI)配置

前面步骤中讨论的所有配置也可以通过CLI应用。

802.1x全局启用

```
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 authorization network MacFilterMethod group ISE_Group
aaa accounting Identity ISE_Method start-stop group ISE_Group
!
aaa server radius dynamic-author
 client 172.16.157.210 server-key *****
 client 172.16.157.21 server-key *****
 auth-type any
!
radius server ISE1
 address ipv4 172.16.157.210 auth-port 1812 acct-port 1813
 timeout 5
 retransmit 2
 key *****
!
radius server ISE2
 address ipv4 172.16.157.21 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 172.16.157.210 eq 8443
    60 deny tcp any host 172.16.157.21 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
```

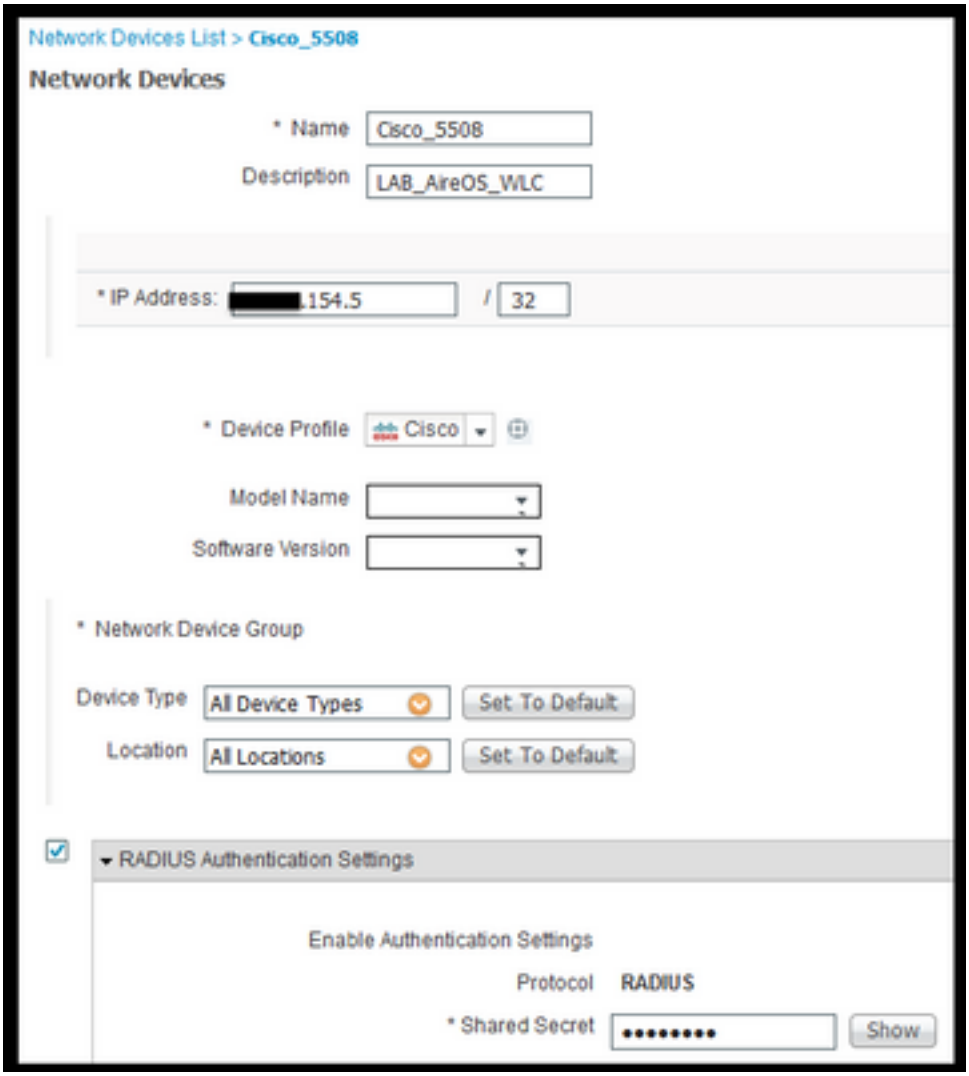
注意：如果应用ACL以限制通过HTTP访问WLC，则会影响重定向。

配置ISE

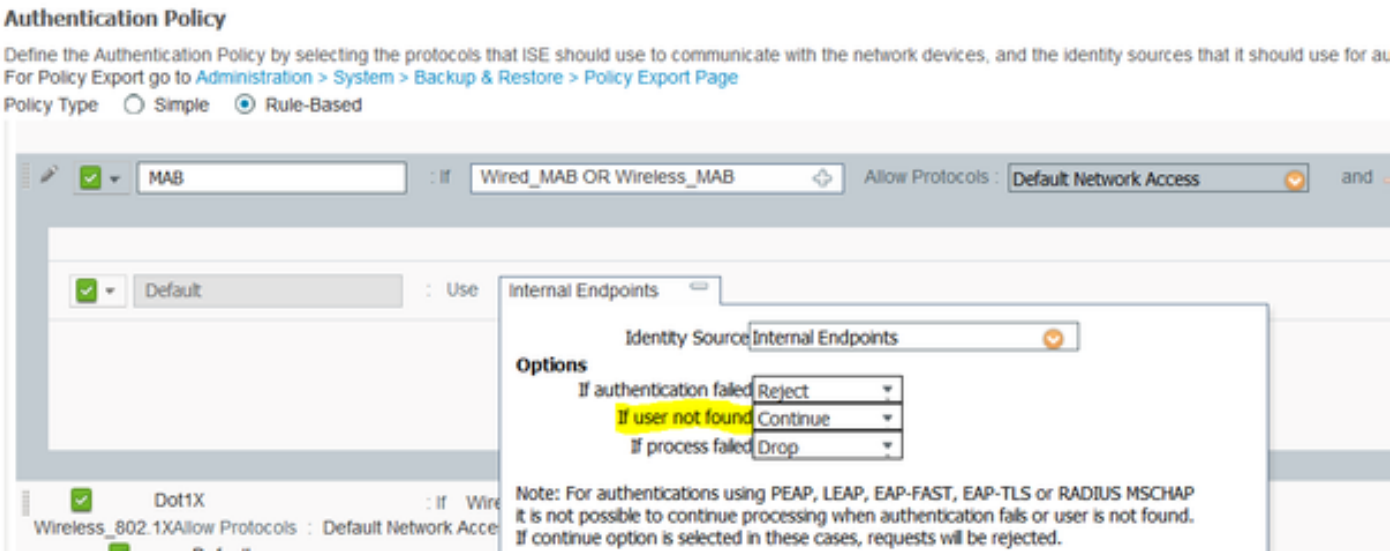
本节介绍ISE上支持本文档中讨论的所有使用案例所需的配置。

常见ISE配置任务

1. 登录到ISE并导航到**管理>网络资源>网络设备**，然后点击**添加**
2. 输入与WLC关联的**Name**和设备IP**地址**。
3. 选中**RADIUS身份验证设置**框，并键入WLC端配置的**共享密钥**。然后请点击**提交**。



4.定位至“策略”>“验证”，在“MAB”下单击“编辑”，并确保在**使用：内部终端**下，选项如果未找到用户设置为继续（默认情况下必须存在）。



使用案例1：在每个用户连接中具有访客身份验证的CWA

流概述

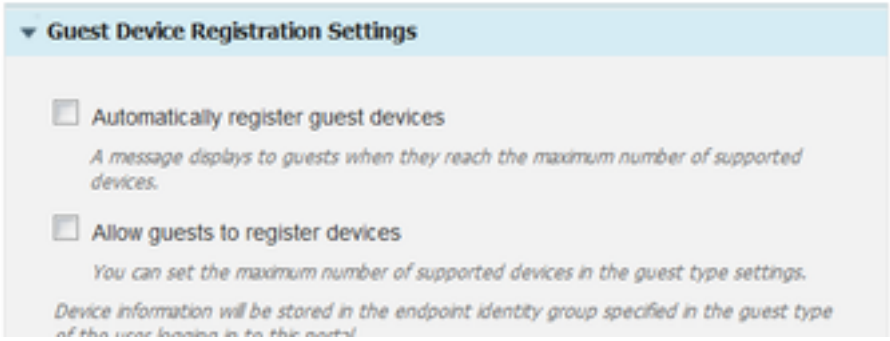
1. 无线用户连接到访客SSID。

2. WLC根据终端在ISE上的MAC地址作为AAA服务器对终端进行身份验证。
3. ISE返回back和access-accept两个属性值对(AVP):url-redirect和url-redirect-acl。一旦WLC将此AVP应用于终端会话，该站点将转换为DHCP-Required，一旦它获取了IP地址，它将保留在CENTRAL_WEB_AUTH中。在此步骤中，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，一旦生成HTTP或HTTPS流量，WLC会将用户重定向到ISE访客门户。
5. 用户进入访客门户后，会提示输入访客凭证（在本例中为发起人创建）。
6. 凭证验证后，ISE显示AUP页面，客户端接受后，会向WLC发送动态CoA类型重新身份验证。
7. WLC重新处理MAC过滤身份验证，而不向移动站发出取消身份验证。这对终端必须是无缝的。
8. 发生重新身份验证事件后，ISE会重新评估授权策略，并且此次，终端被授予允许访问权限，因为之前有一个成功的访客身份验证事件。

每次用户连接到SSID时，此过程都会重复。

配置

1. 导航至ISE并导航至**工作中心(Work Centers)>访客接入(Guest Access)>配置(Configure)>访客门户(Guest Portals)**>选择**发起人访客门户(Select Sponsored Guest Portal)**（或创建新的门户类型Sponsored-Guest）。
2. 在**Guest Device Registration** settings下，取消选中所有选项，然后单击**Save**。

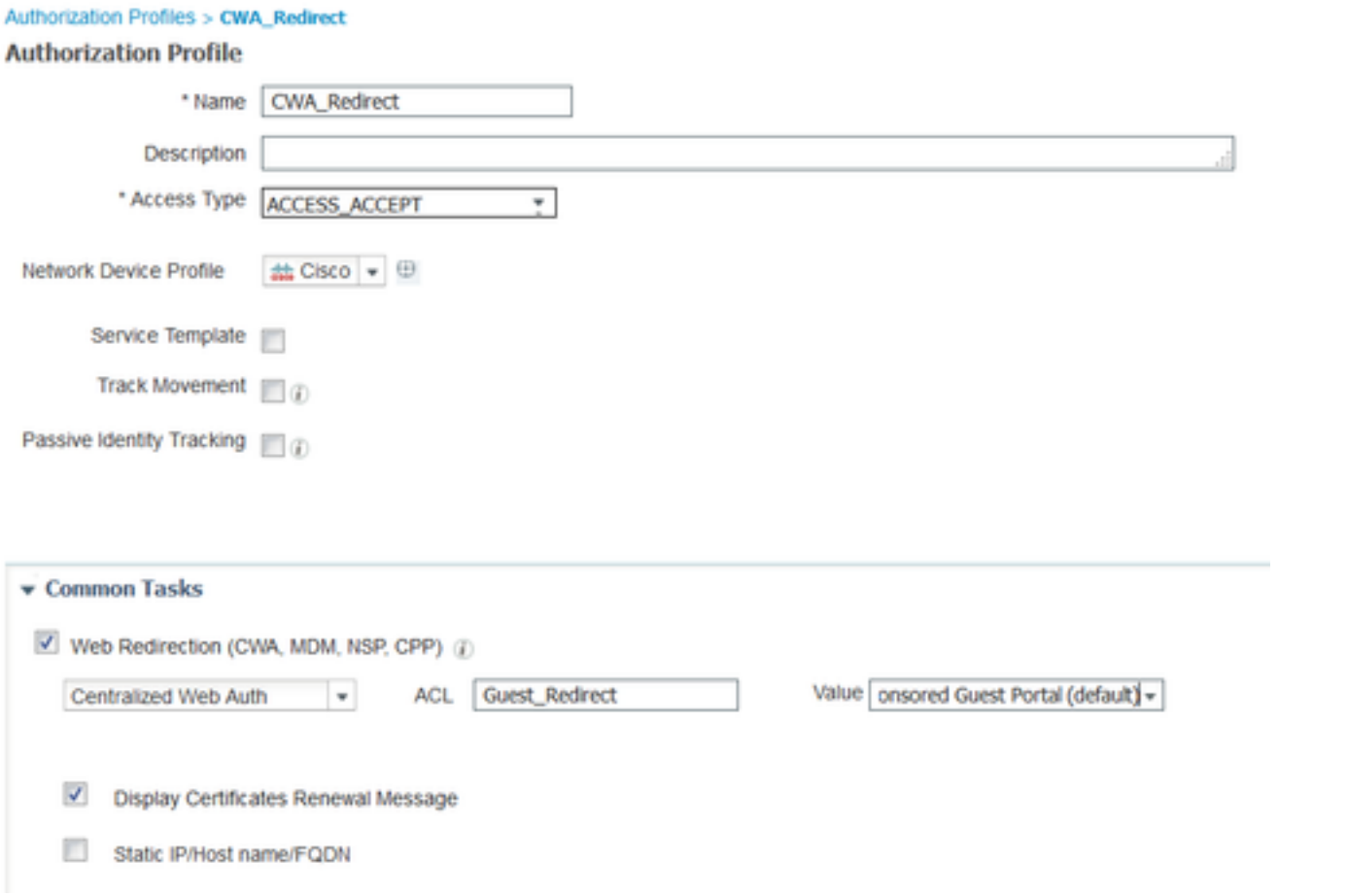


3.定位至“策**略”>“策略要素”>“结果”>“授权”>“授权配置文件**”。单击 **Add**。

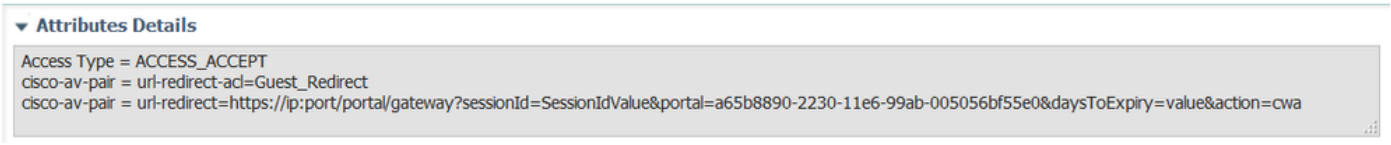
4.响应初始Mac身份验证绕行(MAB)请求，此配置文件通过**Redirect-URL**和**Redirect-URL-ACL**推送到WLC。

- 选中Web重定向(CWA、MDM、NSP、CPP)后，选择Centralized Web Auth，然后在ACL字段下键入Redirect ACL name，并在**Value**下选择**Sponsored** Guest Portal(default)（或之前步骤中创建的任何其他特定门户）。

配置文件必须与此图片中的配置文件类似。然后单击保存。



页面底部的Attribute Details（属性详细信息）将属性值对(AVP)推送到WLC

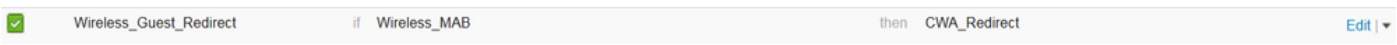


5.定位至**Policy > Authorization**，然后插入新规则。此规则是触发重定向进程以响应来自WLC的初始MAC身份验证请求的规则。(在本例中称为**Wireless_Guest_Redirect**)。

6.在**Conditions**下，选择**Select Existing Condition from Library**，然后在**condition name**下，选择**Compound condition**。选择名为**Wireless_MAB**的预定义复合条件。

> **注**：此条件包含源自WLC的访问请求中预期的2个Radius属性(NAS-Port-Type= IEEE 802.11 <存在于所有无线请求中>和Service-Type = Call Check<（表示特定的mac身份验证绕行请求））

7.在结果下，选择**Standard > CWA_Redirect**（在上一步中创建的授权配置文件）。然后单击**完成**并保存

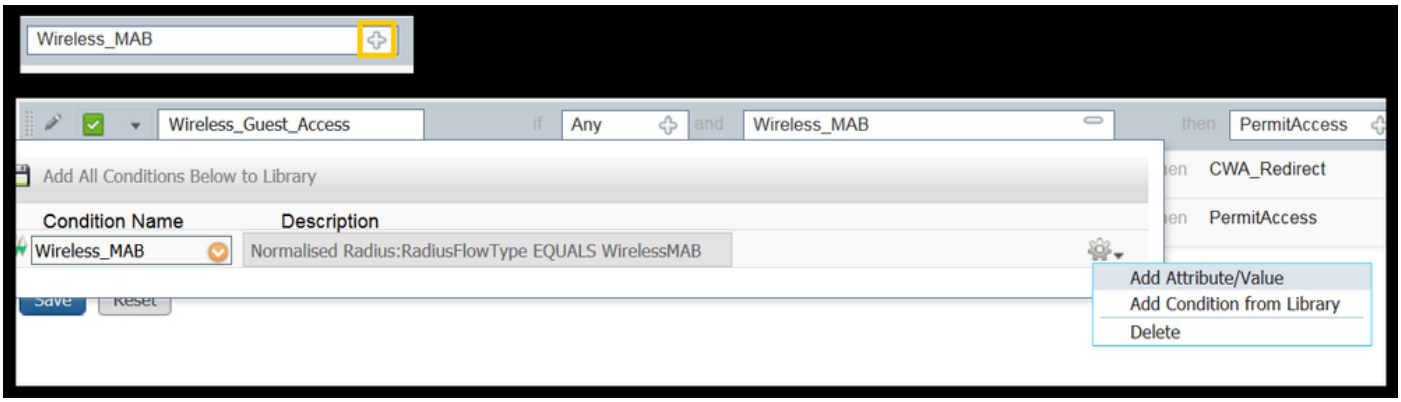


8.导航到**CWA**_Redirect规则**的结尾**，然后点击**Edit**旁边的箭头。然后选择**duplicate above**。

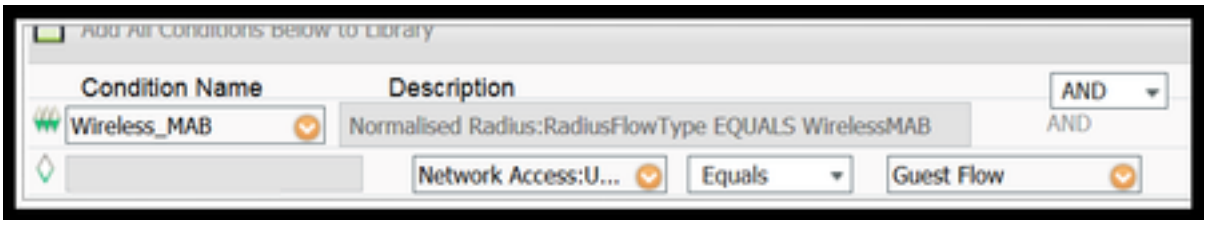
9.修改名称，因为这是ISE的CoA重新验证会话后终端匹配的策略（本例中为Wireless_Guest_Access）。

10.在**Wireless_MAB**复合条件旁边，单击**+**符号展开条件，并在**Wireless_MAB**条件结束时单击**添加**

属性/值。

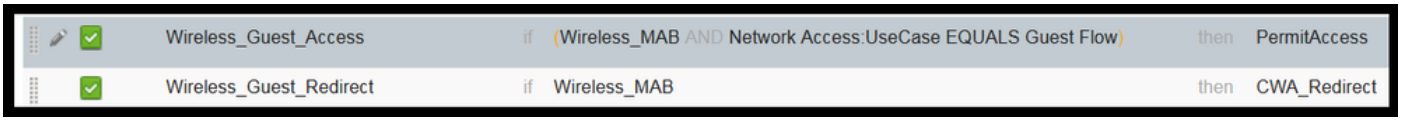


11.在“选择属性”下，选择**网络访问>用例等于访客流**



12.在**权限**下，选择**PermitAccess**。然后单击**完成**并保存

两个策略必须如下所示：



使用案例2:CWA with Device Registration enforcing guest authentication everyday.（带设备注册的CWA每天执行一次访客身份验证。）

流概述

1. 无线用户连接到访客SSID。
2. WLC根据终端在ISE上的MAC地址作为AAA服务器对终端进行身份验证。
3. ISE返回back和access-accept并包含两个属性值对(AVP)（url-redirect和url-redirect-acl）。
4. 一旦WLC将此AVP应用于终端会话，该站点将转换为DHCP-Required，一旦它获取了IP地址，它将保留在CENTRAL_WEB_AUTH中。在此步骤中，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，一旦生成HTTP或HTTPS流量，WLC会将用户重定向到ISE访客门户。
6. 用户进入访客门户后，系统会提示他输入发起人创建的凭证。
7. 凭证验证后，ISE会将此终端添加到特定（预配置的）终端身份组（设备注册）。
8. 显示AUP页面，一旦客户端接受，动态CoA类型重新进行身份验证。发送到WLC。
9. WLC重新处理MAC过滤身份验证，而不向移动站发出取消身份验证。这对终端必须是无缝的。
10. 发生重新身份验证事件后，ISE会重新评估授权策略。这次，由于终端是正确终端身份组的成

员，ISE返回无限制的访问接受。

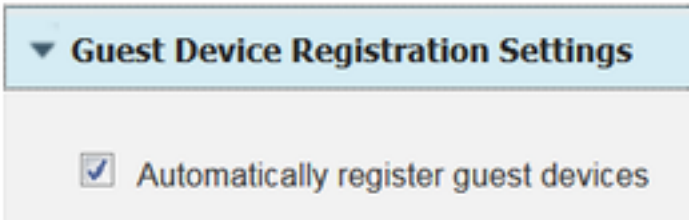
11. 由于终端已在步骤6中注册，因此每次用户返回时，都允许其在网络上，直到从ISE手动将其删除，或者终端清除策略运行刷新符合条件的终端。

在本实验场景中，身份验证每天执行一次。重新身份验证触发器是终端清除策略，它每天删除已使用的终端身份组的所有终端。

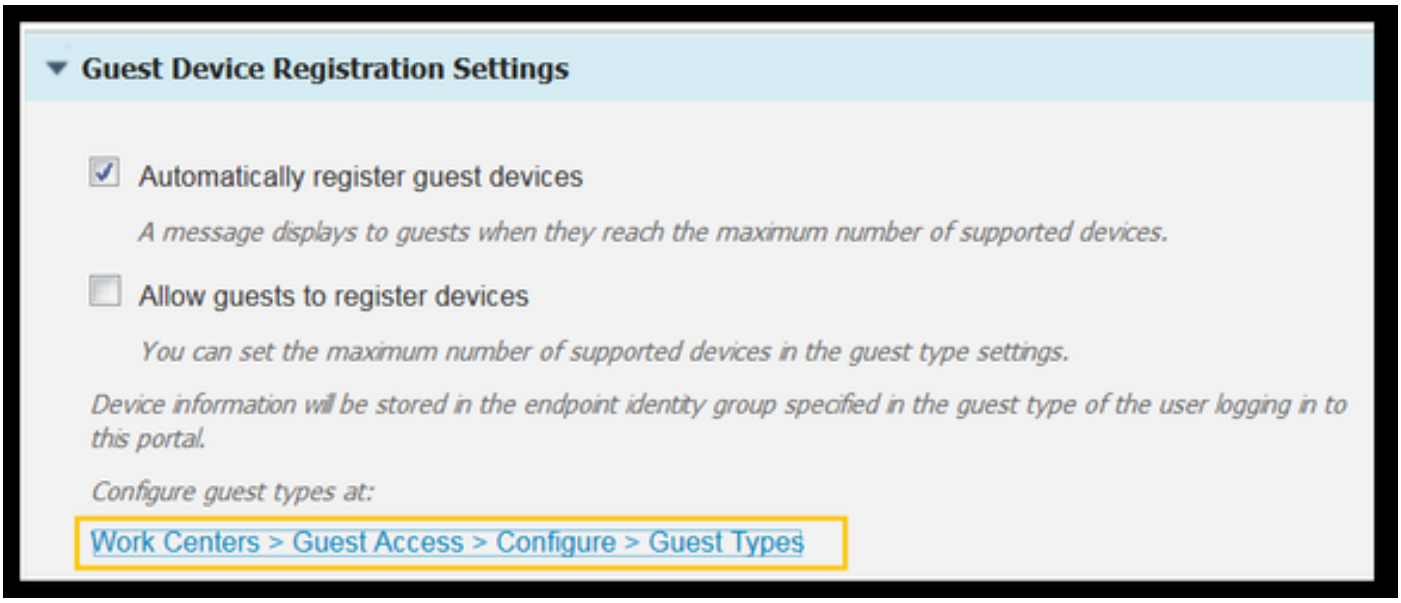
注意：可以根据自上次AUP接受以来经过的时间实施访客身份验证事件。如果您需要更频繁地实施Guest Logon（例如每4小时），则可以选择此选项。

配置

1. 在ISE上，导航至**工作中心(Work Centers)>访客接入(Guest Access)>配置(Configure)>访客门户(Guest Portals)**>选择**发起人访客门户(Select Sponsored Guest Portal)**（或创建新的门户类型Sponsored-Guest）。
2. 在**Guest Device Registration**设置下，验证选中**Automatically register guest devices**选项。Click **Save**.

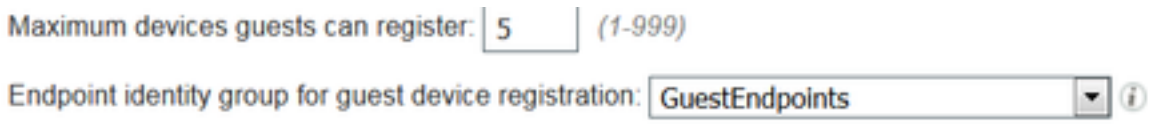


3.导航到**工作中心>访客接入>配置>访客类型**，或只需单击门户中“访客设备注册设置”下指定的快捷方式。



4.发起人用户创建访客帐户时，会为其分配访客类型。每个访客类型可以有一个属于不同终端身份组的注册终端。要分配设备必须添加到的终端身份组，请选择发起人用于这些访客用户的访客类型(此使用案例基于每周（默认）)。

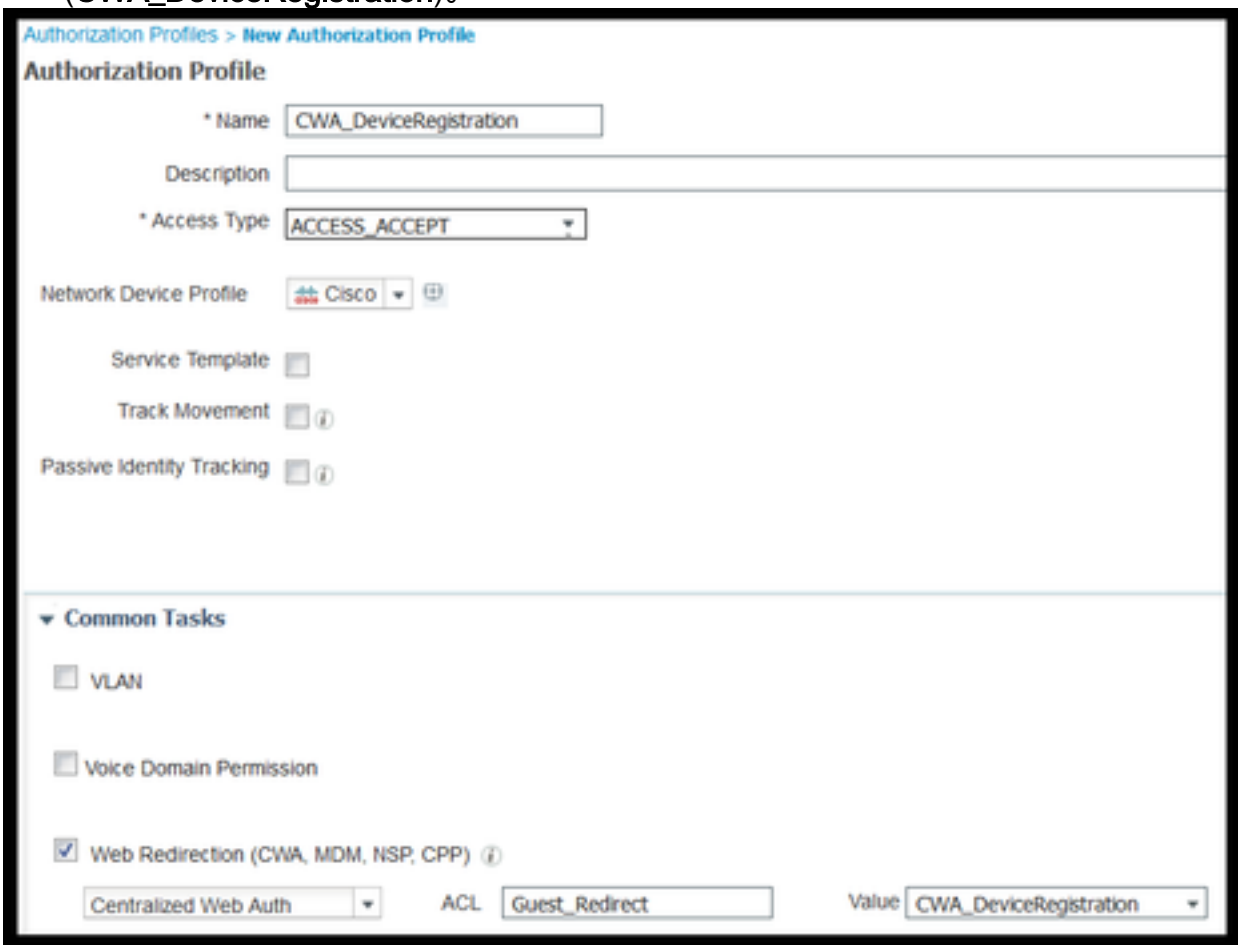
5.进入访客类型后，在**Login Options**下，从下拉菜单**Endpoint Identity group for guest device registration**中选择Endpoint Group



6.定位至“策略”>“策略要素”>“结果”>“授权”>“授权配置文件”。单击 Add。

7.响应初始Mac身份验证绕行(MAB)请求，此配置文件通过Redirect-URL和Redirect-URL-ACL推送到WLC。

- 选中Web重定向(CWA、MDM、NSP、CPP)后，选择Centralized Web Auth，然后在ACL字段下键入Redirect ACL name，然后在Value下选择为此流创建的门户(CWA_DeviceRegistration)。



8.定位至策略>授权，然后插入新规则。此规则是触发重定向进程以响应来自WLC的初始MAC身份验证请求的规则。(在本例中称为Wireless_Guest_Redirect)。

9.在Conditions下，选择Select Existing Condition from Library，然后在condition name下，选择Compound。选择名为Wireless_MAB的预定义复合条件。

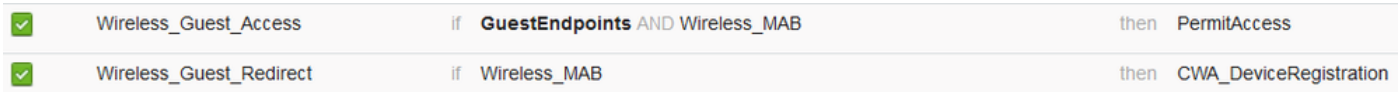
10.在结果下，选择Standard > CWA_DeviceRegistration（在上一步中创建的授权配置文件）。然后单击完成并保存

11.复制上述策略，修改其名称，因为这是终端从重新身份验证事件（称为Wireless_Guest_Access）返回后触发的策略。

12.在Identity Group Details框中，选择Endpoint Identity Group，然后在Guest

Type(GuestEndpoints)下选择您引用的组。

13.在“结果”下，选择**PermitAccess**。单击**Done**并**Save**更改。



14.创建并清除每天清除访客终端组的终端策略。

- 导航到**管理>身份管理>设置>**终端清除
- 在**Purge**规则下，默认情况下，如果经过时间超过30天，则必须有一个触发访客终端删除的规则。
- 修改GuestEndpoints的现有策略或创建新策略（如果默认策略已删除）。请注意，清除策略在定义的时间里每天运行。

在这种情况下，条件为已用天数小于1天的访客终端的成员

使用案例3:HostSpot门户

流概述

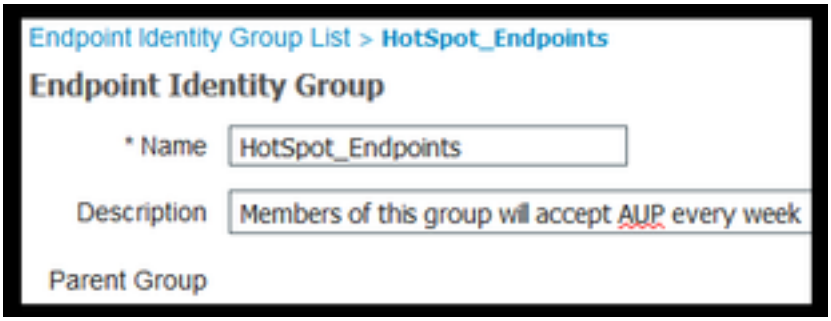
1. 无线用户连接到访客SSID。
2. WLC使用ISE作为AAA服务器，根据终端的MAC地址对终端进行身份验证。
3. ISE返回具有两个属性值对(AVP)的access-accept:url-redirect和url-redirect-acl。
4. 一旦WLC将此AVP应用于终端会话，该站点将转换为DHCP-Required，一旦它获取了IP地址，它将保留在CENTRAL_WEB_AUTH中。在此步骤中，WLC已准备好重定向客户端的http/https流量。
5. 最终用户打开Web浏览器，一旦生成HTTP或HTTPS流量，WLC会将用户重定向到ISE热点门户。
6. 进入门户后，系统会提示用户接受可接受的使用策略。
7. ISE将终端MAC地址（终端ID）添加到已配置的终端身份组。
8. 处理请求的策略服务节点(PSN)向WLC发出动态CoA类型**Admin-Reset**。
9. WLC处理完传入CoA后，会向客户端发出取消身份验证（连接丢失，客户端返回所需的时间很长）。
10. 客户端重新连接后，会创建新的会话，因此ISE端没有会话连续性。这意味着身份验证将作为新线程处理。
11. 由于终端已添加到已配置的终端身份组，并且存在检查终端是否属于该组的授权策略，因此新身份验证与此策略匹配。结果是对访客网络的完全访问权限。
12. 除非终端身份对象因终端清除策略而从ISE数据库中清除，否则用户不得再次接受AUP。

配置

1. 创建新终端身份组以在注册后将这些设备移动到。导航到**工作中心(Work Centers)>访客接入(Guest Access)>身份组(Identity Groups)>终端身份组(Endpoint Identity Groups)**，然后单击 

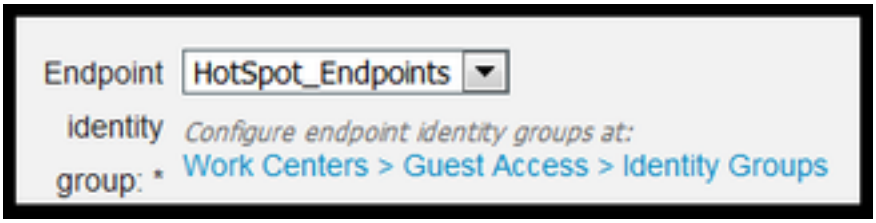
.

- 输入组名称（本例中为HotSpot_Endpoints）。添加说明，无需父组。



2.定位至**工作中心>访客访问权限>配置>访客门户**>选择**热点门户(默认)**。

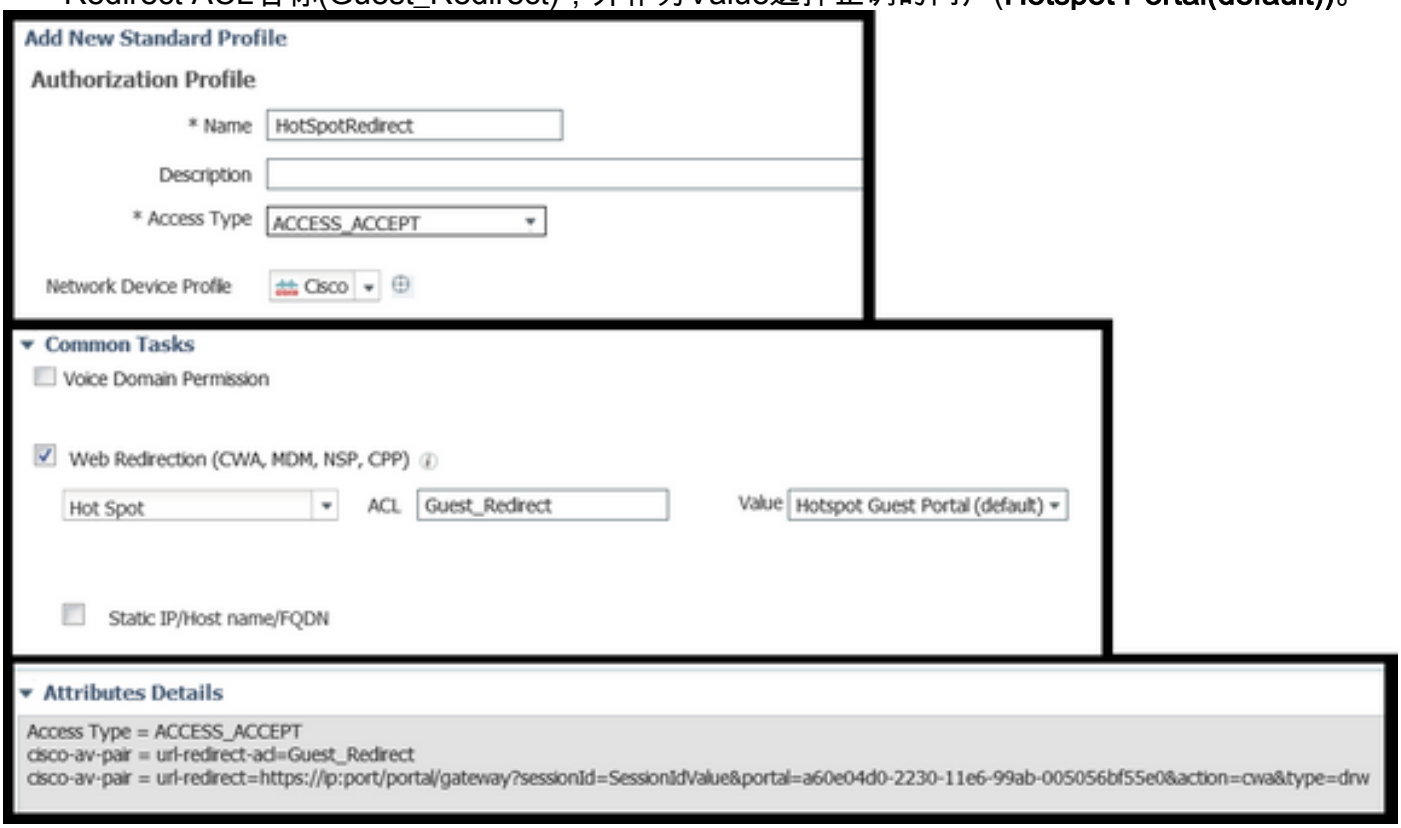
3.展开Portal Settings，然后在Endpoint Identity Group下**选择Endpoint** Identity Group下**的HostSpot_Endpoints组。**这会将注册设备发送到指定的组。



4.**保存**更改。

5.创建在WLC发起的MAB身份验证时调用HotSpot门户的授权配置文件。

- 导航到**Policy > Policy elements > Results > authorization > Authorization Profiles**并创建一个(HotSpotRedirect)。
- 选中**Web redirection(CWA， MDM， NSP， CPP)**后，选择**Hot Spot**，然后在ACL字段中键入Redirect ACL名称(Guest_Redirect)，并作为Value选择正确的门户(**Hotspot Portal(default))**。

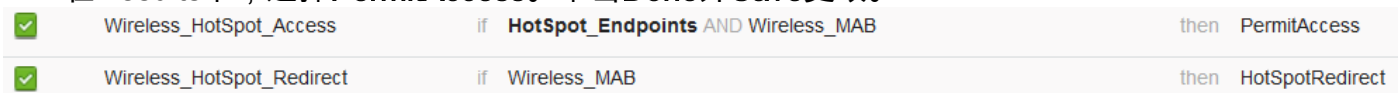


6.创建授权策略，在WLC发出初始MAB请求时触发HotSpotRedirect结果。

- 导航到**Policy > Authorization**并插入新规则。此规则是触发重定向过程以响应来自WLC的初始MAC身份验证请求的规则。(在本例中称为**Wireless_HotSpot_Redirect**)。
- 在**Conditions**下选择**Select Existing Condition from Library**，然后在**condition name**下选择**Compound condition**
- 在results下，选择**Standard > HotSpotRedirect**（在上一步中创建的授权配置文件）。然后单击**完成**并保存

7.创建第二个授权策略。

- 复制上述策略，修改其名称，因为这是终端从重新身份验证事件（称为Wireless_HotSpot_Access）返回后触发的策略。
- 在**Identity Group Details**框中，选择**Endpoint Identity Group**，然后选择之前创建的组(**HotSpot_Endpoints**)。
- 在Results下，选择**PermitAccess**。单击**Done**并**Save**更改。



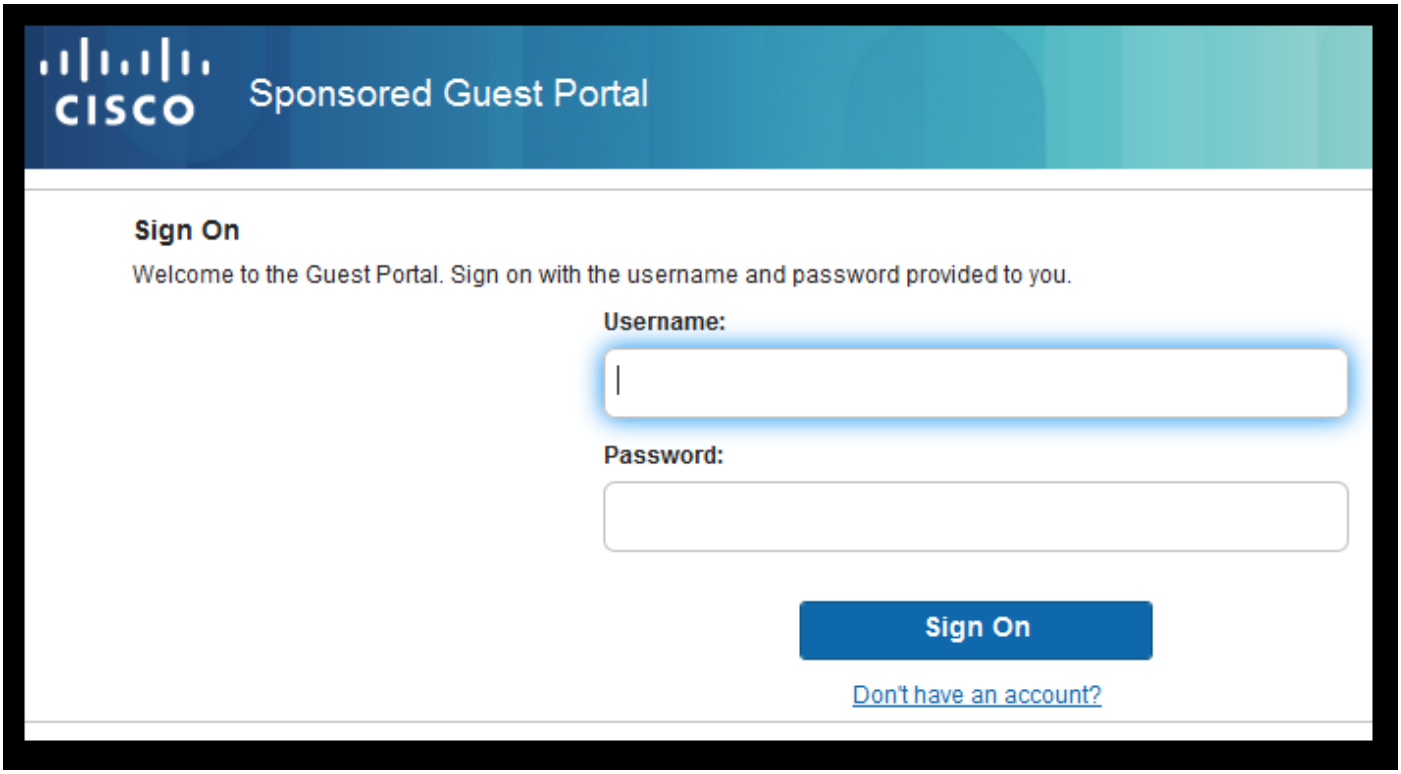
8.配置清除策略，清除运行时间超过5天的终端。

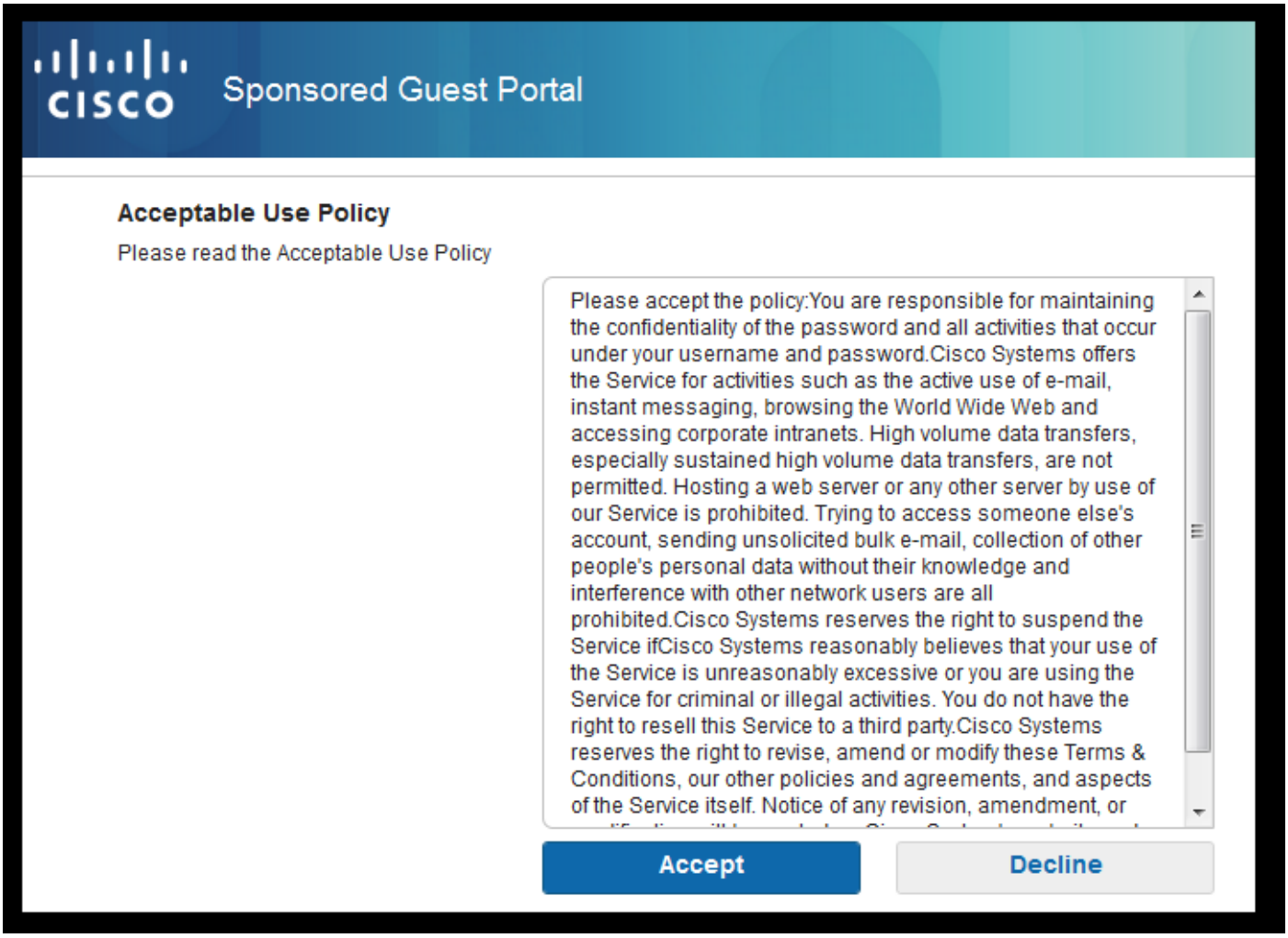
- 导航到**Administration > Identity Management > Settings > Endpoint Purge**，然后在Purge rules下创建新策略。
- 在**Identity Group Details**框中，选择**Endpoint Identity Group > HotSpot_Endpoints**
- 在**conditions**下，单击**Create New Condition(Advanced Option)**。
- 在“选择属性”(Select Attribute)下*选择“终端清除：已用天数”(ENDPOINTPURGE: ElapsedDays GREATERETHAN* 5天)

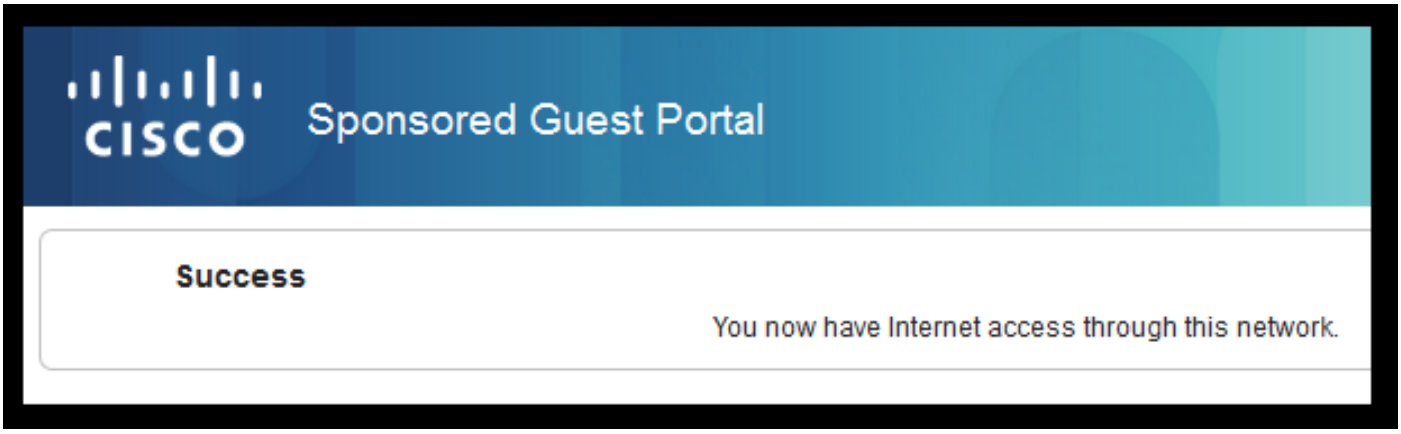
验证

使用案例1

1. 用户连接到访客SSID。
2. 他打开浏览器，一生成HTTP流量，就会显示访客门户。
3. 访客用户验证并接受AUP后，将显示成功页面。
4. 重新验证CoA发送出去（对客户端透明）。
5. 终端会话将重新进行身份验证，具有对网络的完全访问权限。
6. 任何后续访客连接都必须通过访客身份验证，才能获得网络访问权限。


Sponsored Guest Portal
Sign On
Welcome to the Guest Portal. Sign on with the username and password provided to you.
Username:
Password:
Sign On
Don't have an account?

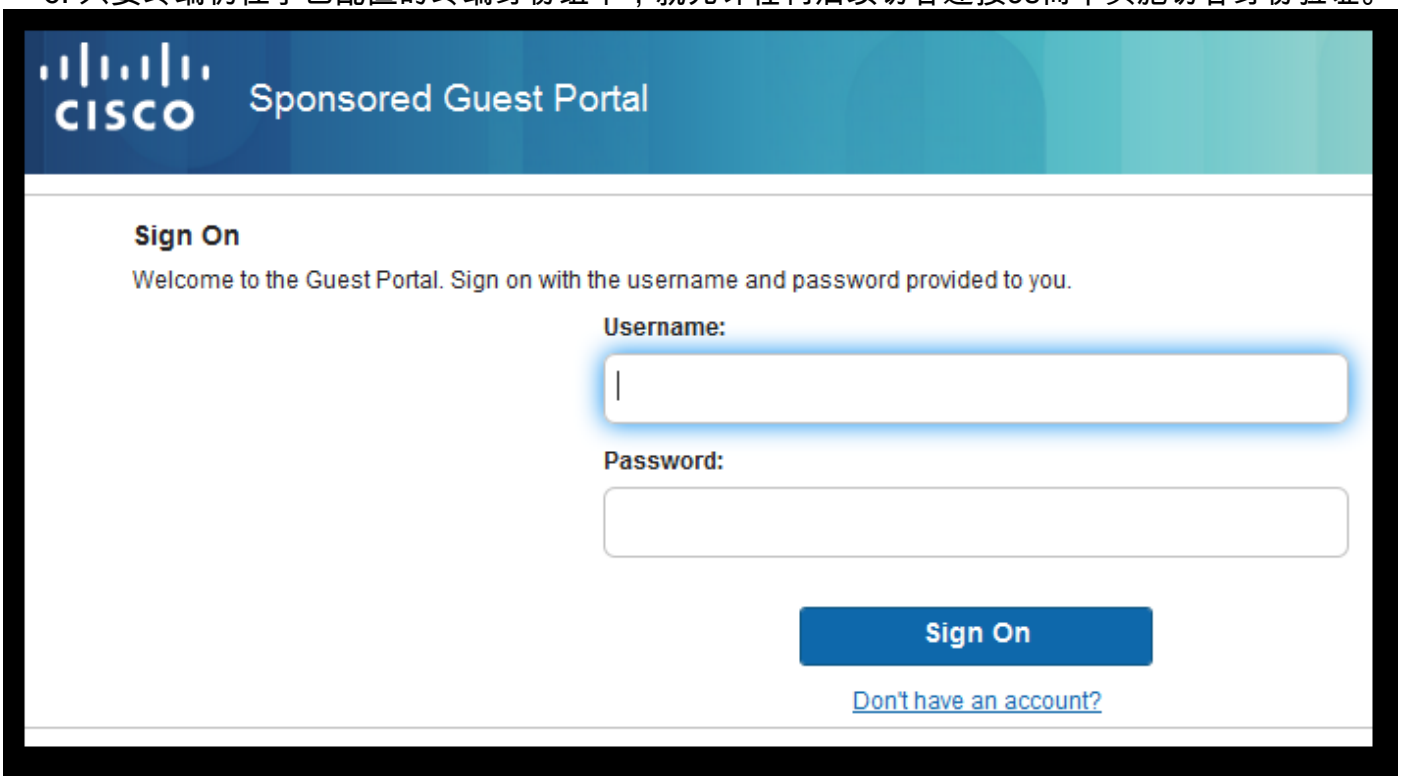

Sponsored Guest Portal
Acceptable Use Policy
Please read the Acceptable Use Policy
Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited.Cisco Systems reserves the right to suspend the Service ifCisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party.Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or
Accept
Decline

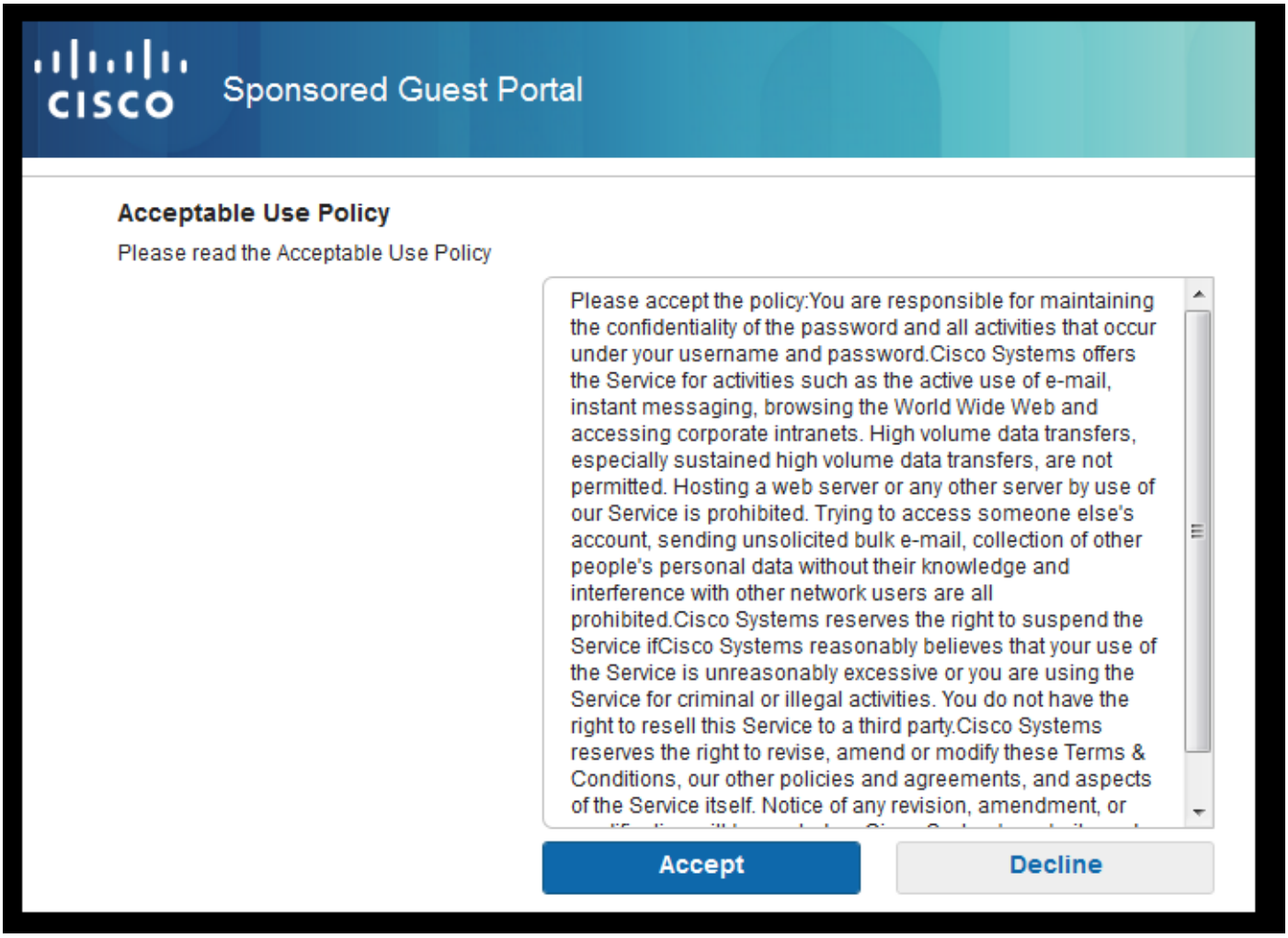


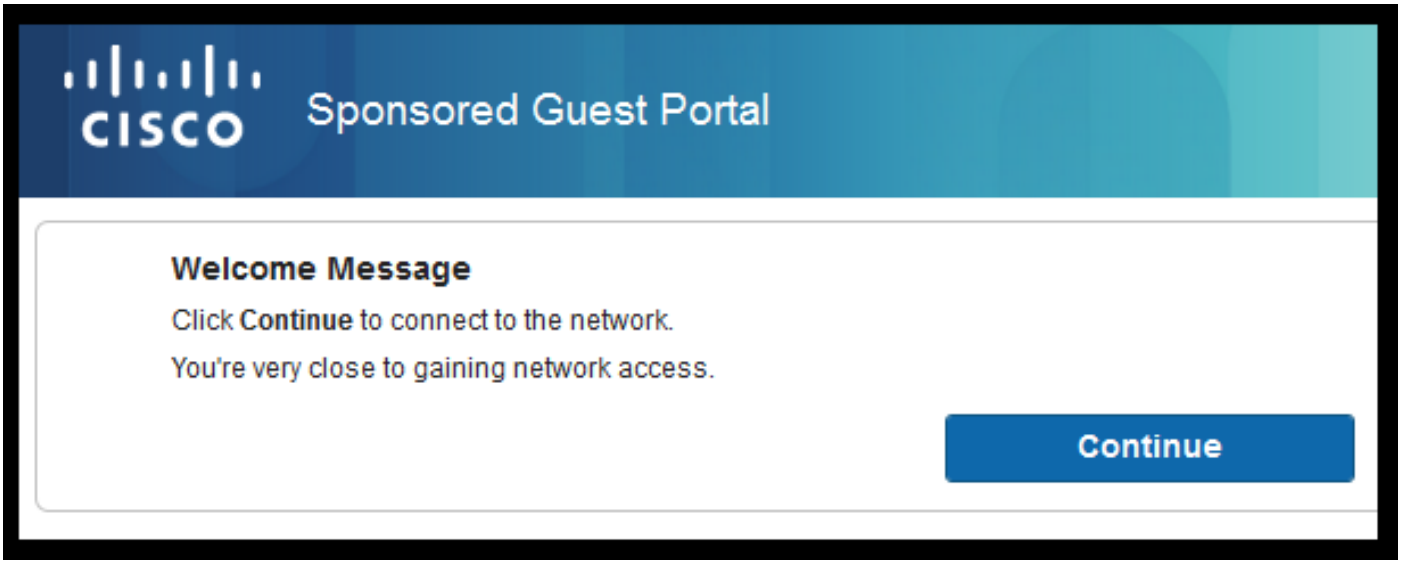
来自ISE RADIUS实时日志的流量：

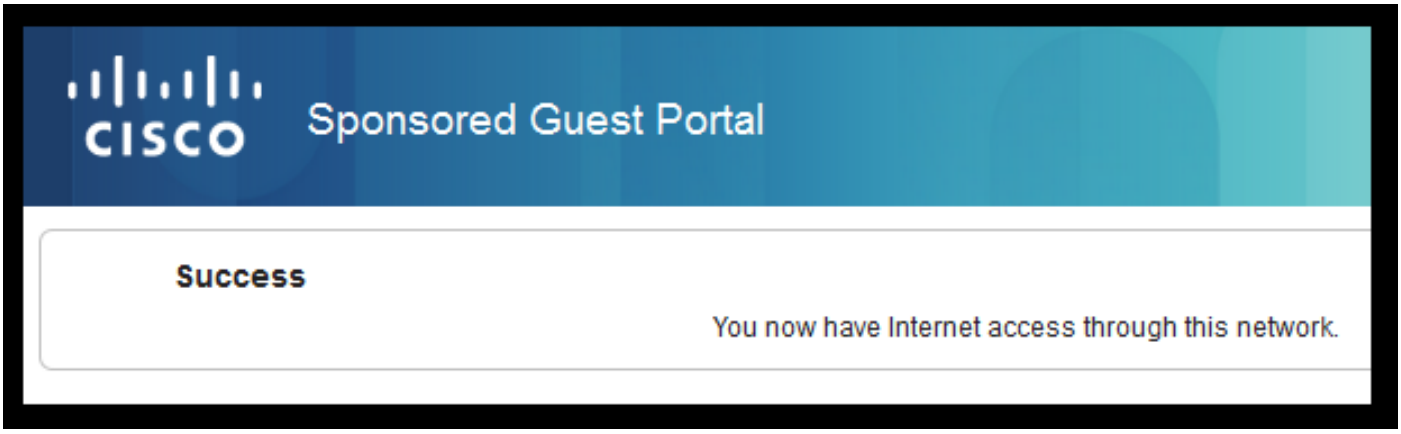
使用案例2

1. 用户连接到访客SSID。
2. 他打开浏览器，一生成HTTP流量，就会显示访客门户。
3. 访客用户验证并接受AUP后，设备即注册。
4. 系统将显示成功页面，并发送Re-authenticate CoA（对客户端透明）。
5. 终端会话将重新进行身份验证，具有对网络的完全访问权限。
6. 只要终端仍位于已配置的终端身份组中，就允许任何后续访客连接9s而不实施访客身份验证。

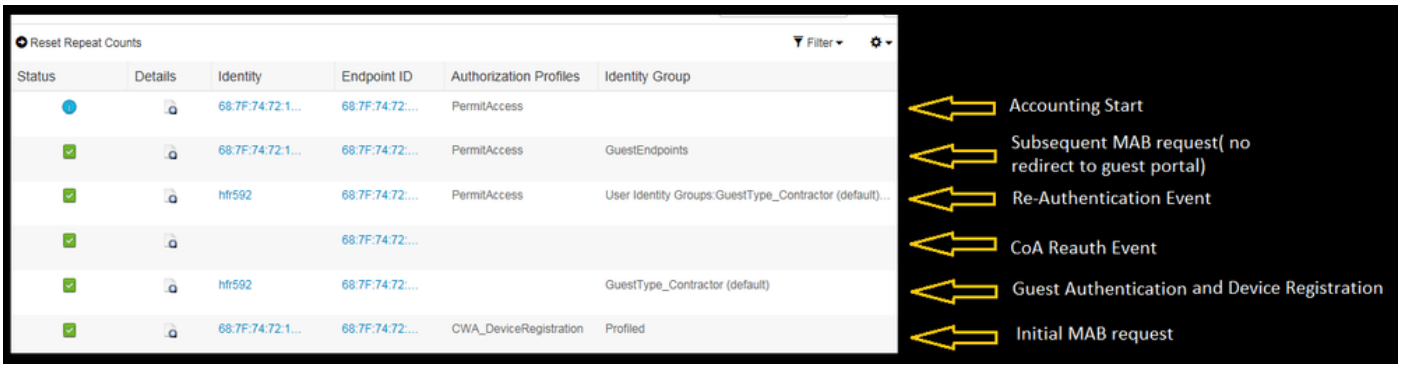



Sponsored Guest Portal
Acceptable Use Policy
Please read the Acceptable Use Policy
Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited.Cisco Systems reserves the right to suspend the Service ifCisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party.Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or
Accept
Decline


Sponsored Guest Portal
Welcome Message
Click Continue to connect to the network.
You're very close to gaining network access.
Continue

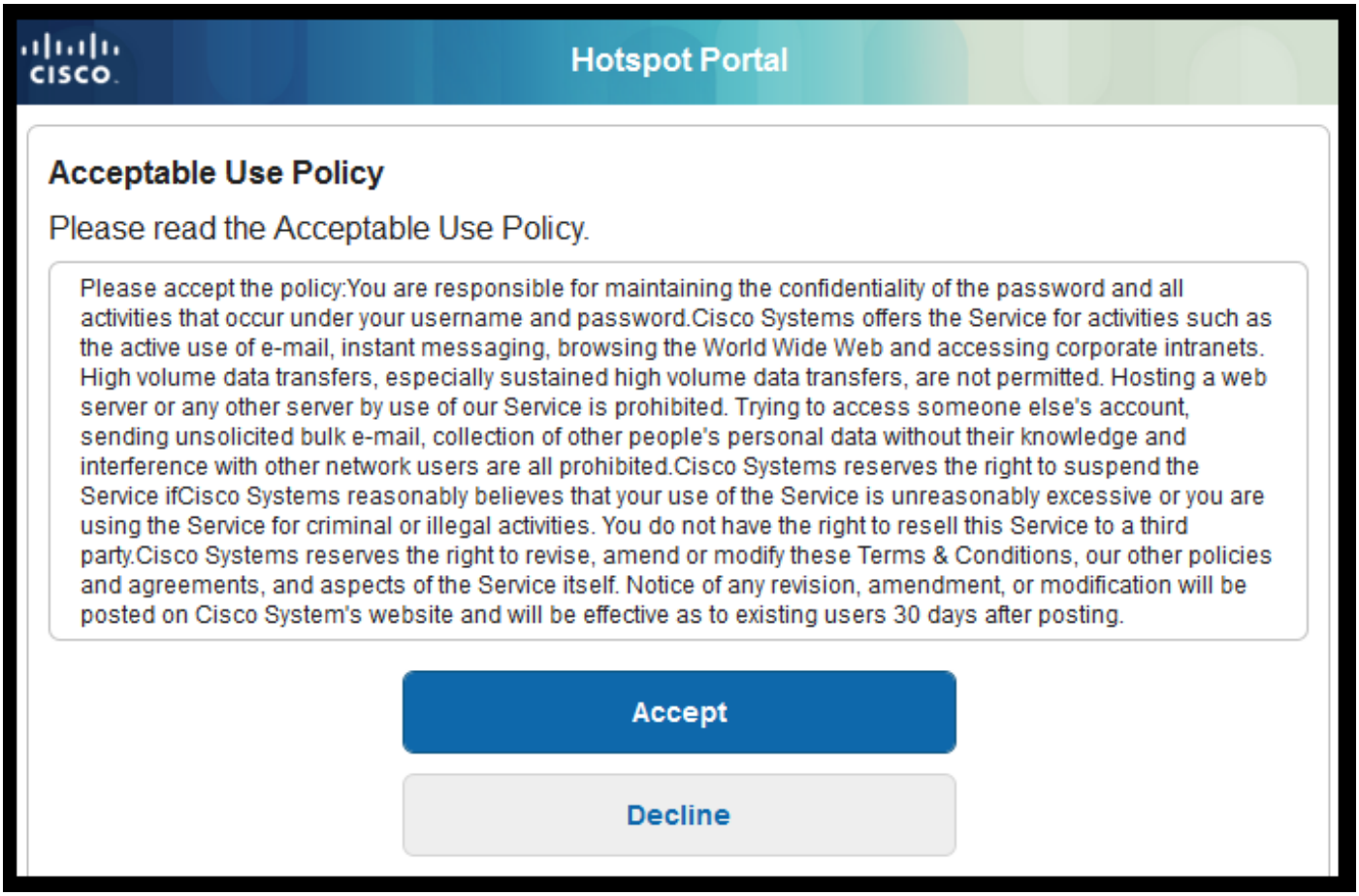


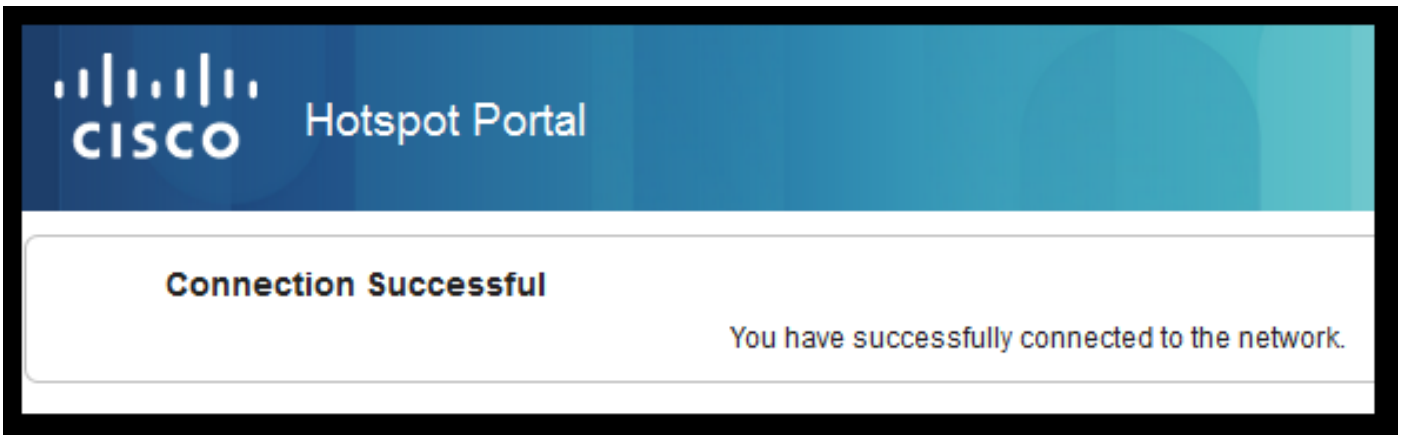
来自ISE RADIUS实时日志的流量：



使用案例3

1. 用户连接到访客SSID。
2. 他打开浏览器，一生成HTTP流量，就会显示AUP页面。
3. 访客用户接受AUP后，即注册设备。
4. 系统将显示成功页面，并发送Admin-Reset CoA（对客户端透明）。
5. 终端以完全访问网络的方式重新连接。
6. 只要终端保留在已配置的终端身份组中，就允许任何后续突风连接，而无需执行AUP接受（除非另外配置）。

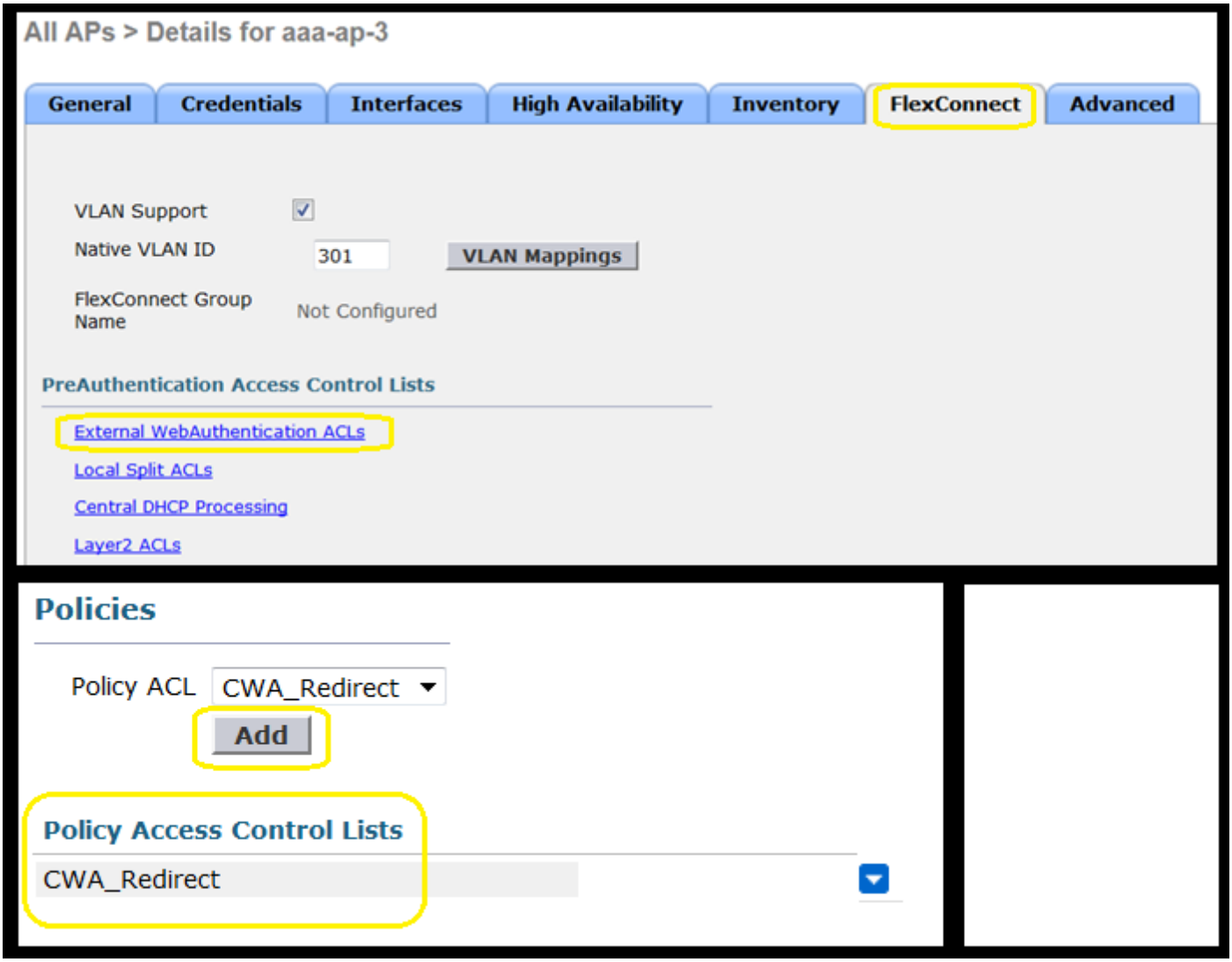




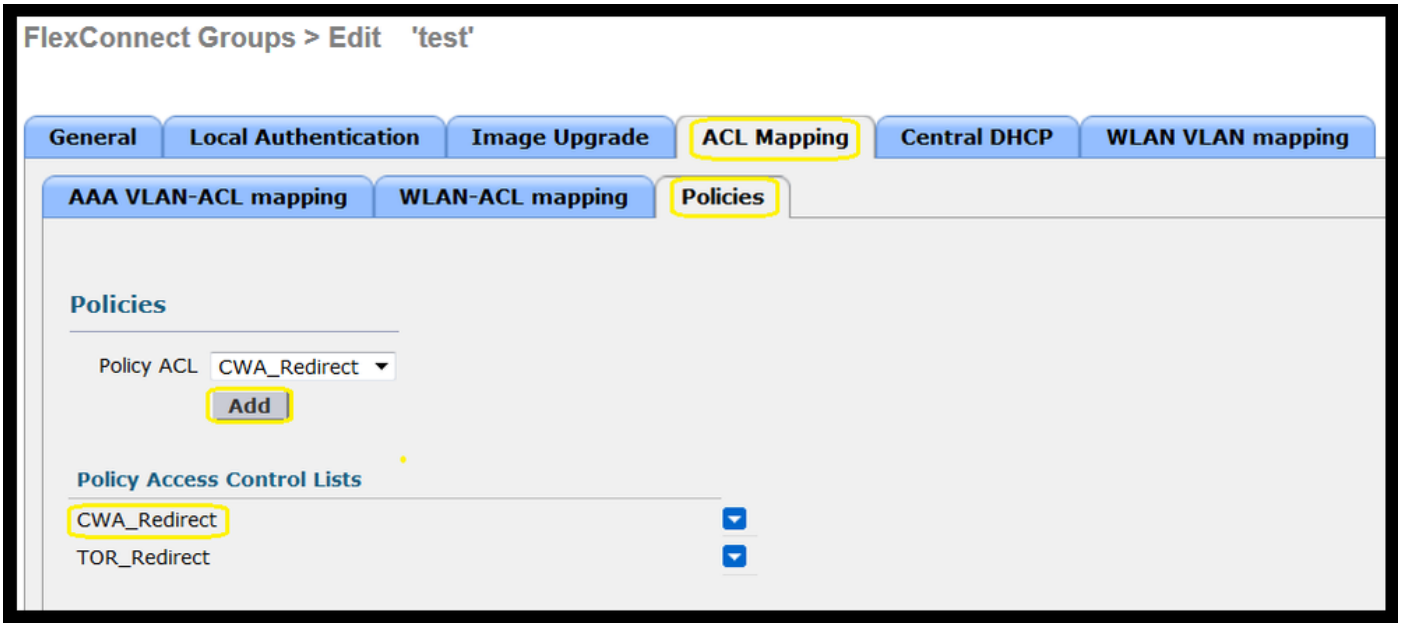
AireOS中的FlexConnect本地交换

配置FlexConnect本地交换时，网络管理员需要确保：

- 重定向ACL配置为FlexConnect ACL。
- 重定向ACL已作为策略应用通过AP自身在**FlexConnect**选项卡> **External WebAuthentication ACLs** > **Policies** >选择重定向ACL下并点击**Apply**



或者通过将策略ACL添加到FlexConnect组所属的(**Wireless > FlexConnect Groups >选择正确的组> ACL Mapping > Policies**选择重定向ACL并点击Add)



添加策略ACL会触发WLC将配置的ACL向下推送到FlexConnect组的AP成员。否则会导致Web重定向问题。

外部锚点方案

在自动锚点（外部锚点）场景中，必须强调以下事实：

- 需要在外部和锚点WLC上定义重定向ACL。即使仅在锚点上强制执行。
- 第2层身份验证始终由外部WLC处理。这在设计阶段（对于故障排除也很重要）非常重要，因为所有RADIUS身份验证和记帐流量都发生在ISE和外部WLC之间。

- 重定向AVP应用于客户端会话后，外部WLC通过移动切换消息更新锚点中的客户端会话。
- 此时，锚点WLC开始使用已预配置的重定向ACL实施重定向。
- 必须在锚点WLC SSID上完全关闭记账，以避免来自锚点和外部的指向ISE的记账更新（引用相同的身份验证事件）。
- 基于URL的ACL在外部锚点场景中不受支持。

故障排除

AireOS和融合接入WLC上的常见断开状态

1. **客户端无法加入访客SSID**

show client detailed xx:xx:xx:xx:xx:xx显示客户端卡在**START**中。 通常，这是指示WLC无法应用AAA服务器返回的属性。

验证ISE推送的重定向ACL名称与WLC上预定义ACL的名称完全匹配。

同样的原理适用于已配置ISE向下推送到WLC的任何其他属性（VLAN ID、接口名称、Airespace-ACL）。然后，客户端必须转换到DHCP，然后转换到CENTRAL_WEB_AUTH。

2. **重定向AVP已应用于客户端会话，但重定向不起作用**

验证客户端的策略管理器状态为CENTRAL_WEB_AUTH，其中有效的IP地址与为SSID配置的动态接口一致，并且重定向ACL和URL重定向属性已应用于客户端的会话。

重定向ACL

在AIreOS WLC中，重定向ACL必须明确允许不得重定向的流量，例如TCP端口8443上的DNS和ISE两个方向，并且隐式deny ip any any any会触发其余的流量重定向。

在融合接入中，逻辑正好相反。拒绝ACE绕过重定向，而允许ACE触发重定向。这就是为什么建议明确允许TCP端口80和443。

验证从访客VLAN通过端口8443对ISE的访问。如果从配置角度看一切正常，最简单的前进方法是获取客户端无线适配器后面的捕获并验证重定向中断的位置。

- 是否发生DNS解析？
- TCP三次握手是否已针对请求的页面完成？
- 客户端启动GET后，WLC是否返回重定向操作？
- 是否完成了通过8443与ISE的TCP三次握手？

3. **在ISE推送访客流结束时的VLAN更改后，客户端无法访问网络**

一旦客户端在流开始时抓取了IP地址（Pre Redirect状态），如果发生Guest身份验证（CoA重新身份验证后）后推下VLAN更改，强制在访客流中进行DHCP释放/续约的唯一方法（无状态代理）是通过Java小程序，在移动设备中该小程序不起作用。

这会使客户端在VLAN X中保持黑洞，IP地址为VLAN Y。 规划解决方案时必须考虑这一点。

4. **在重定向期间，ISE在访客客户端的浏览器中显示"HTTP 500 Internal error， Radius session not found"消息**

这通常是ISE上会话丢失的指示符（会话已终止）。最常见的原因是部署了外部锚点后，在锚点WLC上配置了记账。 要修复此在锚点上禁用记帐，并保留外部句柄Authentication and Accounting。

5. **客户端在ISE的热点门户中接受AUP后会断开连接并保持断开连接或连接到不同的SSID。**

由于此流程中涉及的授权动态更改(CoA)导致WLC向无线站发出取消身份验证，因此在HotSpot中可能会出现这种情况。大多数无线终端在取消身份验证后没有任何问题可返回到SSID，但在某些情况下，客户端会连接到另一个首选SSID以响应取消身份验证事件。从ISE或WLC中无法进行任何操作来阻止此过程，因为要由无线客户端将原始SSID粘贴或连接到另一个可用（首选）SSID。

在这种情况下，无线用户必须手动连接回热点SSID。

AireOS WLC

```
(Cisco Controller) >debug client
```

Debug client set to DEBUG a set involved in Client State Machine changes。

```
(Cisco Controller) >show debug

MAC Addr 1..................................... AA:AA:AA:AA:AA:AA

Debug Flags Enabled:
  dhcp packet enabled.
  dot11 mobile enabled.
  dot11 state enabled
  dot1x events enabled.
  dot1x states enabled.
  mobility client handoff enabled.
  pem events enabled.
  pem state enabled.
  802.11r event debug enabled.
  802.11w event debug enabled.
  CCKM client debug enabled.
```

调试AAA组件

```
(Cisco Controller) >debug aaa {events, detail and packets} enable
```

这可能影响资源，具体取决于通过MAB或Dot1X SSID连接的用户数量。 DEBUG级别的这些组件记录WLC和ISE之间的AAA事务，并在屏幕上打印RADIUS数据包。

如果ISE无法提供预期属性，或者WLC无法正确处理这些属性，则这一点至关重要。

Web-Auth redirect

```
(Cisco Controller) >debug web-auth redirect enable mac aa:aa:aa:aa:aa:aa
```

这可用于检验WLC是否成功触发重定向。以下示例说明了从调试中重定向必须是什么样子：

```
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e-  parser host is 10.10.10.10
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- parser path is /
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- added redirect=, URL is now
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-005056a15f11&action=cwa&to
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- str1 is now
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-005056a15f11&action=cwa&token=c455b075d20c
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- clen string is Content-Length: 430


*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- Message to be sent is
 HTTP/1.1 200 OK
Location:
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-0050
```

NGWC

Debug client set to DEBUG a set involved in Client State Machine changes。

```
3850#debug client mac-address <client MAC>
```

此组件在屏幕上打印RADIUS数据包（身份验证和记帐）。当您需要验证ISE是否提供正确的AVP以及验证CoA是否正确发送和处理时，这非常方便。

```
3850#debug radius
```

这将涉及无线客户端的所有AAA过渡（身份验证、授权和记帐）。这对于验证WLC正确解析AVP并将其应用于客户端会话至关重要。

```
3850#debug aaa wireless all
```

当您怀疑NGWC上存在重定向问题时，可以启用此功能。

```
3850#debug epm plugin redirect all
3850#debug ip http transactions
3850#debug ip http url
```

ISE

RADIUS实时日志

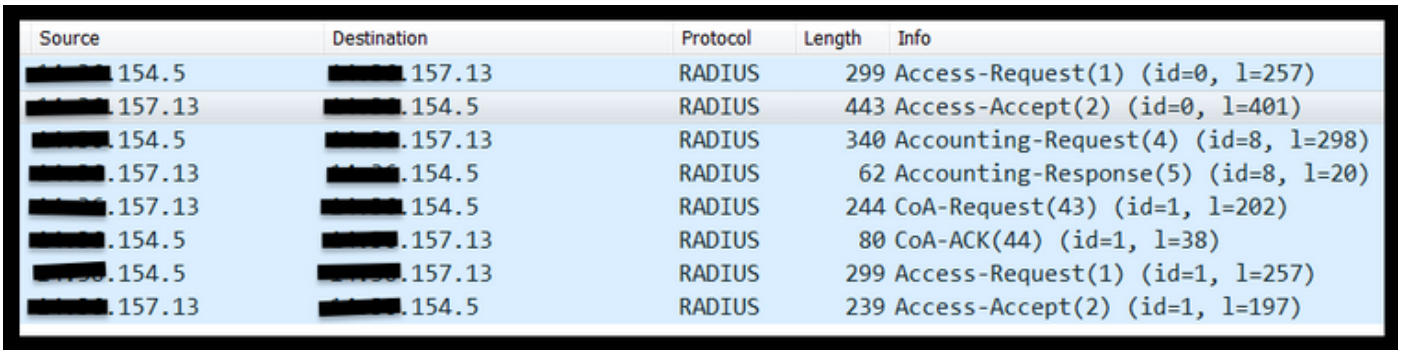
验证初始MAB请求已在ISE中正确处理且ISE回推预期属性。导航到**操作> RADIUS >实时日志**，并使用**终端ID**下的客户端MAC过滤输出。找到身份验证事件后，单击详细信息，然后验证作为接受的

一部分推送的结果。

TCPDump

此功能可用于深入研究ISE和WLC之间的RADIUS数据包交换。这样，您可以证明ISE在access-accept中发送正确的属性，而无需在WLC端启用调试。要使用TCDump启动捕获，请导航到**操作>故障排除>诊断工具** >常规工具> TCPDump。

这是通过TCPDump捕获的正确流的示例



Source	Destination	Protocol	Length	Info
[redacted]154.5	[redacted]157.13	RADIUS	299	Access-Request(1) (id=0, l=257)
[redacted]157.13	[redacted]154.5	RADIUS	443	Access-Accept(2) (id=0, l=401)
[redacted]154.5	[redacted]157.13	RADIUS	340	Accounting-Request(4) (id=8, l=298)
[redacted].157.13	[redacted].154.5	RADIUS	62	Accounting-Response(5) (id=8, l=20)
[redacted].157.13	[redacted]154.5	RADIUS	244	CoA-Request(43) (id=1, l=202)
[redacted].154.5	[redacted].157.13	RADIUS	80	CoA-ACK(44) (id=1, l=38)
[redacted].154.5	[redacted].157.13	RADIUS	299	Access-Request(1) (id=1, l=257)
[redacted].157.13	[redacted].154.5	RADIUS	239	Access-Accept(2) (id=1, l=197)

以下是响应初始MAB请求而发送的AVP（以上屏幕截图中的第二个数据包）。

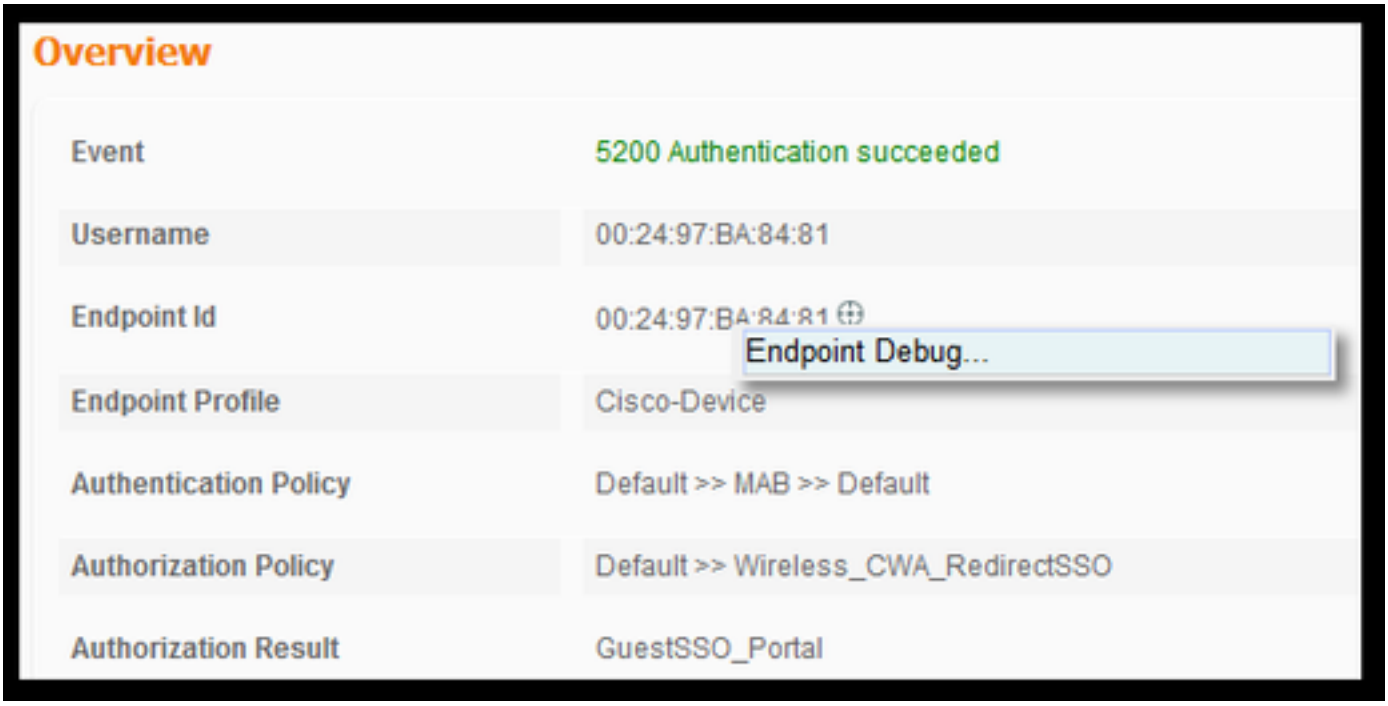
```
RADIUS Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x0 (0)
    Length: 401
    Authenticator: f1eaaffcfaa240270b885a9ba8ccd06d
    [This is a response to a request in frame 1]
    [Time from request: 0.214509000 seconds]
    Attribute Value Pairs
        AVP: l=19 t=User-Name(1): 00-05-4E-41-19-FC
        AVP: l=40 t=State(24): 52656175746853657373696f6e3a30653234396130353030...
        AVP: l=55 t=Class(25): 434143533a30653234396130353030303030616130353536...
        AVP: l=37 t=Vendor-Specific(26) v=ciscoSystems(9)
            VSA: l=31 t=Cisco-AVPair(1): url-redirect-acl=Gues_Redirect
```

```
        AVP: l=195 t=Vendor-Specific(26) v=ciscoSystems(9)
            VSA: l=189 t=Cisco-AVPair(1): url-
redirect=https://ise21a.rtpaaa.net:8443/portal/gateway?sessionId=0e249a0500000aa05565e1c9&portal
=194a5780-5e4e-11e4-b905-005056bf2f0a&action=cwa&token=c6c8a6b0d683ea0c650282b4372a7622
        AVP: l=35 t=Vendor-Specific(26) v=ciscoSystems(9)
```

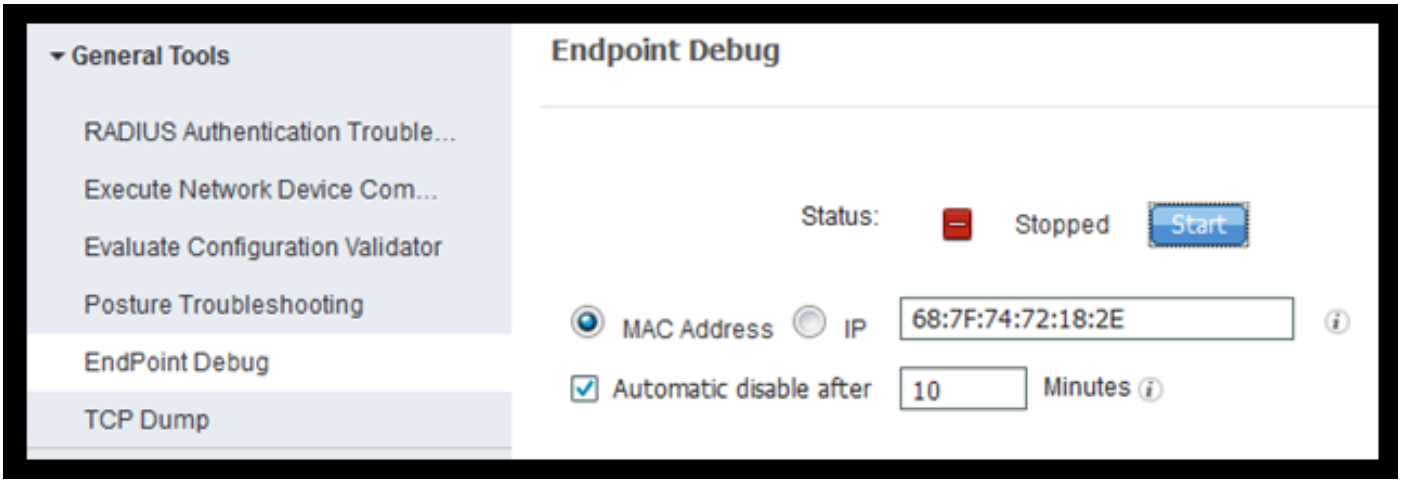
终端调试：

如果您需要深入了解涉及策略决策、门户选择、访客身份验证的ISE流程，CoA处理此问题的最简单方法是启用**Endpoit Debugs**，而不必将完整组件设置为调试级别。

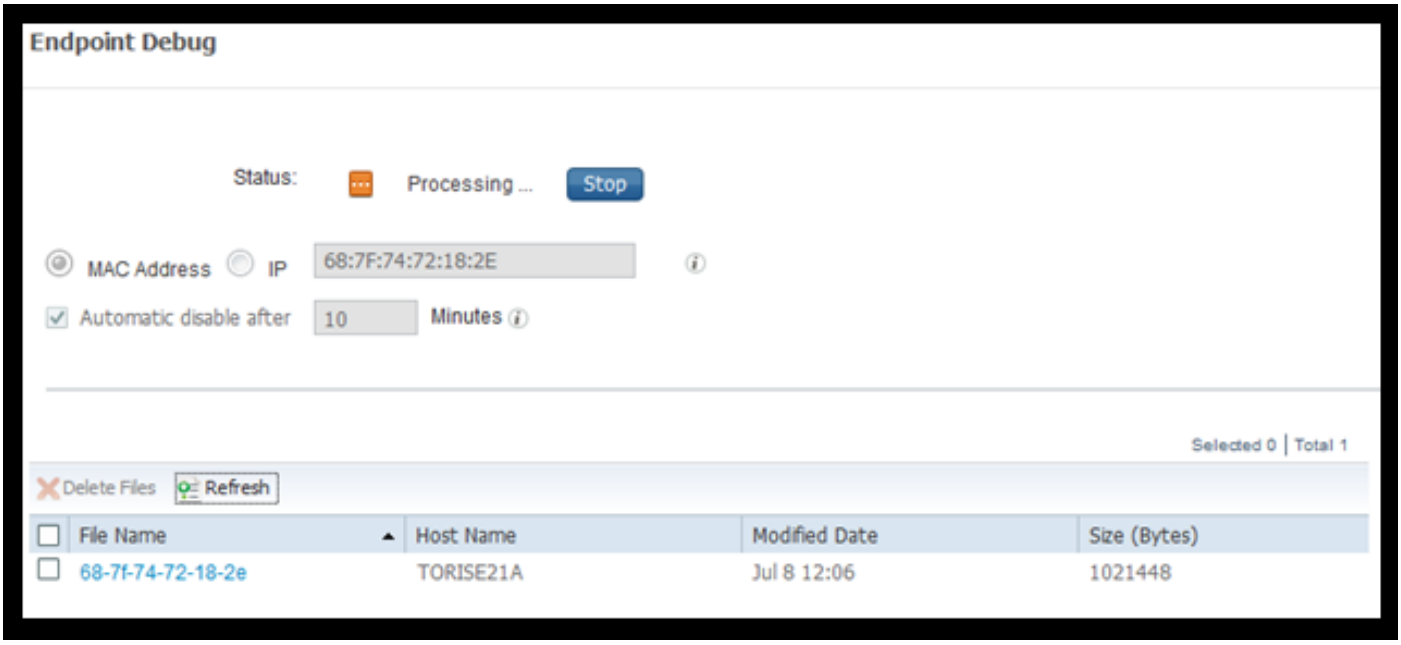
要启用此功能，请导航到**操作>故障排除> DiagnosticTools > General Tools > EndPoint Debug。**



进入终端调试页面后，输入终端MAC地址，并在准备重新创建问题时点击start。



调试停止后，单击标识终端ID的链接以下载调试输出。



相关信息

TAC推荐的AireOS版本

思科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

带身份服务引擎的通用NGWC无线配置

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）。