

# 无线局域网控制器Splash页重定向配置示例

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[背景信息](#)

[网络设置](#)

[配置](#)

[步骤1.通过Cisco Secure ACS服务器配置RADIUS验证的WLC。](#)

[步骤2.配置Admin和工序部门的WLAN。](#)

[步骤3.配置Cisco Secure ACS支持飞溅页重定向功能。](#)

[验证](#)

[故障排除](#)

[相关信息](#)

## 简介

本文描述如何配置在无线局域网控制器的飞溅页重定向功能。

## 先决条件

### 要求

尝试进行此配置之前，请确保满足以下要求：

- LWAPP安全问题解决方案知识
- 有关如何配置 Cisco Secure ACS 的知识

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 该Cisco 4400系列无线局域网的控制器(WLC)运行固件版本5.0
- Cisco 1232系列轻量级接入点(LAP)
- 运行固件版本4.1的Cisco Aironet 802.a/b/g无线客户端适配器
- 运行版本4.1的Cisco Secure ACS服务器
- 任何第三方外部Web服务器

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## [规则](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

## [背景信息](#)

飞溅页Web重定向是功能介绍与无线局域网控制器版本5.0。使用此功能，在802.1x验证完成后，用户重定向对一个特定的网页。重定向发生，当用户打开浏览器(配置与系统设计的主页)或设法访问URL。在对网页的重定向完成后，用户有对网络的完全权限。

您能指定在远程验证拨入用户服务(RADIUS)服务器的重定向页。应该配置RADIUS服务器返回Cisco AV对url重新定向RADIUS属性到无线局域网控制器在成功的802.1x验证。

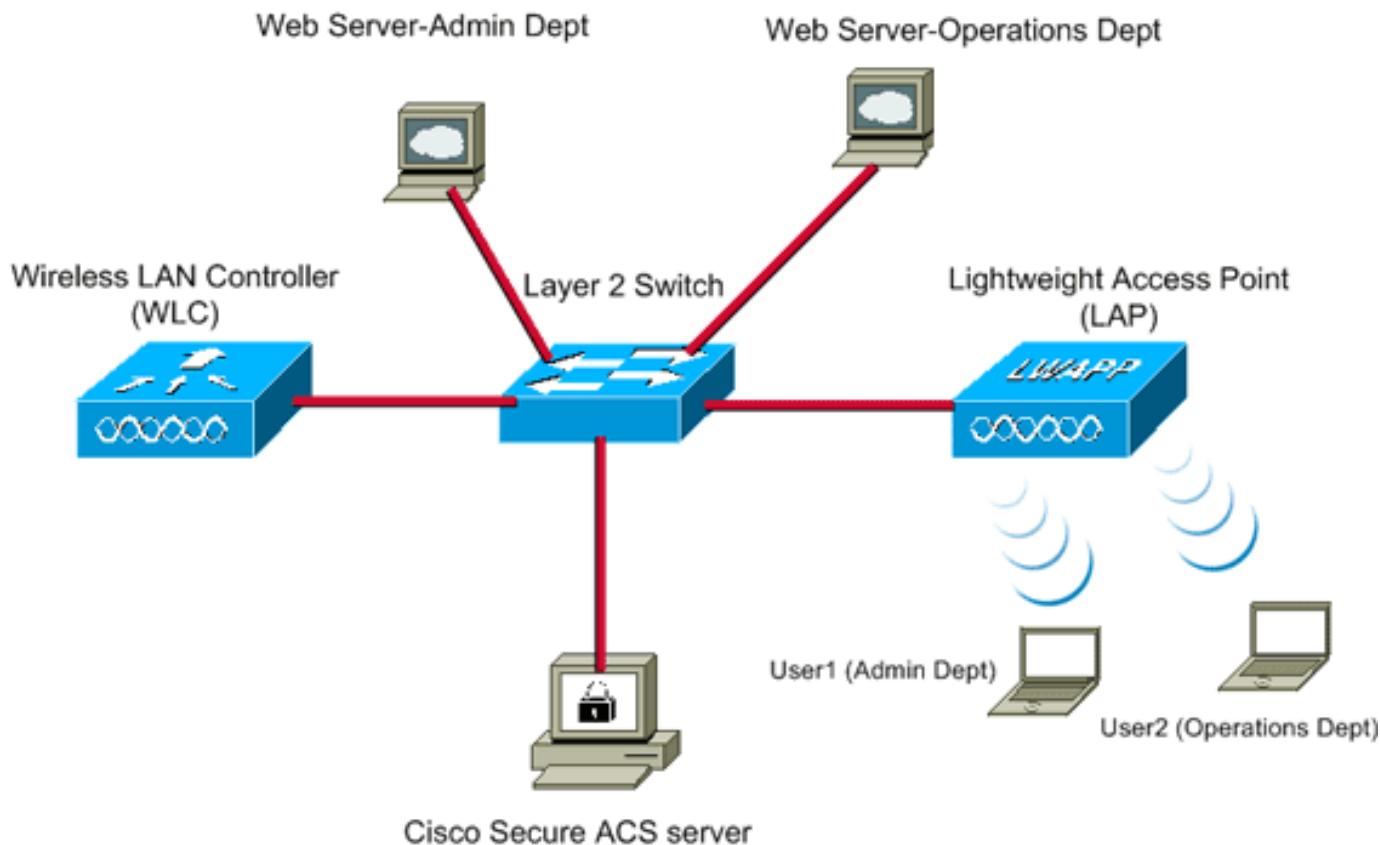
飞溅页Web重定向功能为802.1x或WPA/WPA2第2层安全的配置是仅可用的。

## [网络设置](#)

在本例中，Cisco 4404 WLC和Cisco 1232系列LAP通过第二层交换机连接。作为外部RADIUS服务器)的Cisco Secure ACS服务器(也连接到同一交换机。所有设备都在同一个子网中。

LAP最初注册到控制器。您必须创建两WLAN：一Admin部门用户的和其他工序部门用户的。两无线LAN使用WPA2/ AES (EAP-FAST使用验证)。两WLAN使用飞溅页重定向功能为了重定向用户到适当的主页URL (在外部Web服务器)。

本文档使用以下网络设置：



WLC Management IP address:	10.77.244.204
WLC AP Manager IP address:	10.77.244.205
Wireless Client IP address:	10.77.244.221
Cisco Secure ACS server IP address	10.77.244.196
Subnet Mask used in this example	255.255.255.224

下一部分解释如何为此设置配置设备。

## 配置

本部分提供有关如何配置本文档所述功能的信息。

**注意：** 使用[命令查找工具](#) ( [仅限注册用户](#) ) 可获取有关本部分所使用命令的详细信息。

完成这些步骤为了配置设备使用飞溅页重定向功能：

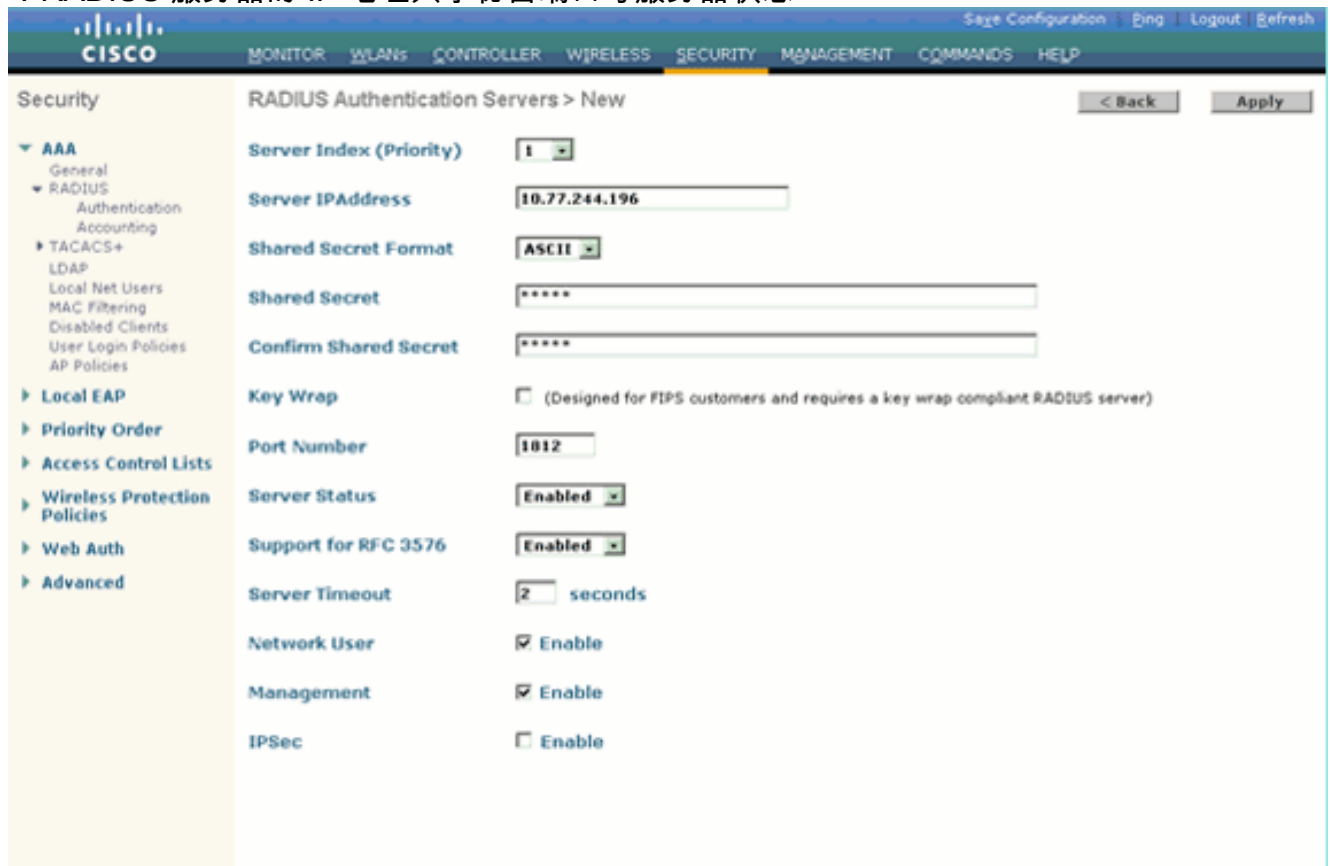
1. [通过Cisco Secure ACS服务器配置RADIUS验证的WLC。](#)
2. [配置Admin和工序部门的WLAN。](#)
3. [配置Cisco Secure ACS支持飞溅页重定向功能。](#)

### [步骤1.通过Cisco Secure ACS服务器配置RADIUS验证的WLC。](#)

需要配置 WLC 以便将用户凭证转发到外部 RADIUS 服务器。

完成以下这些步骤，为外部 RADIUS 服务器配置 WLC：

1. 从控制器GUI选择**安全**和**RADIUS验证**为了显示RADIUS验证服务器页。
2. 单击**新**为了定义RADIUS服务器。
3. 在 **RADIUS Authentication Servers > New** 页上定义 RADIUS 服务器参数。这些参数包括：  
：RADIUS 服务器的 IP 地址共享秘密端口号服务器状态



本文使用IP地址为10.77.244.196的ACS服务器。

4. 单击 **Apply**。

## 步骤2.配置Admin和工序部门的WLAN。

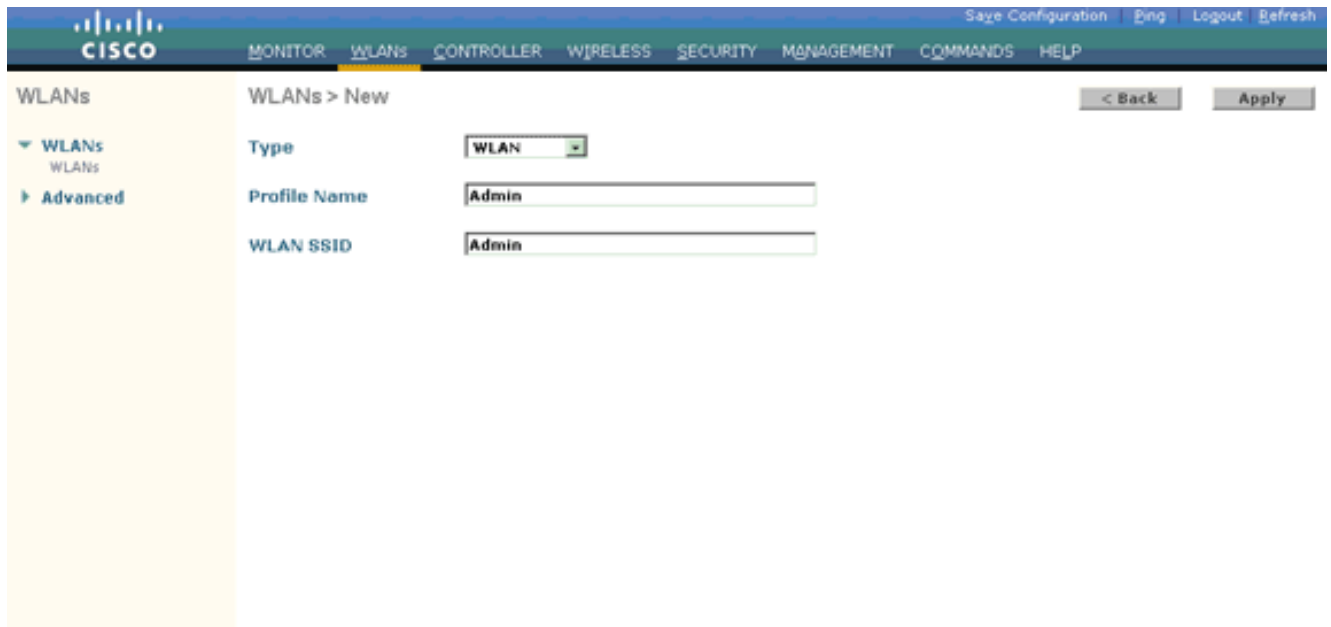
在此步骤，您配置客户端将使用为了连接到无线网络的两WLAN (一Admin部门的和其他工序部门的)。

Admin部门的WLAN SSID将是Admin。工序部门的WLAN SSID将是操作。

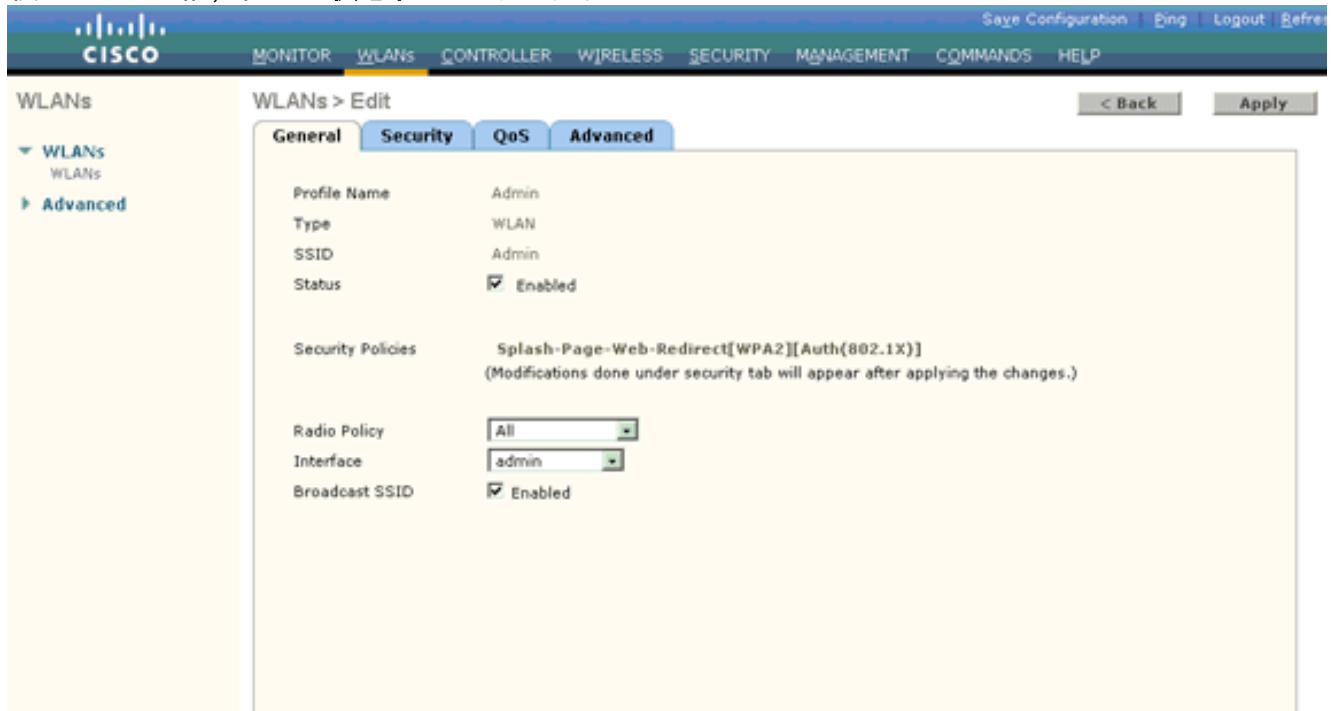
请使用EAP-FAST验证为了启用WPA2作为在两WLAN和Web策略的第2层安全机制-请飞溅页Web重定向功能作为第3层安全方法。

若要配置 WLAN 及其相关参数，请完成下列步骤：

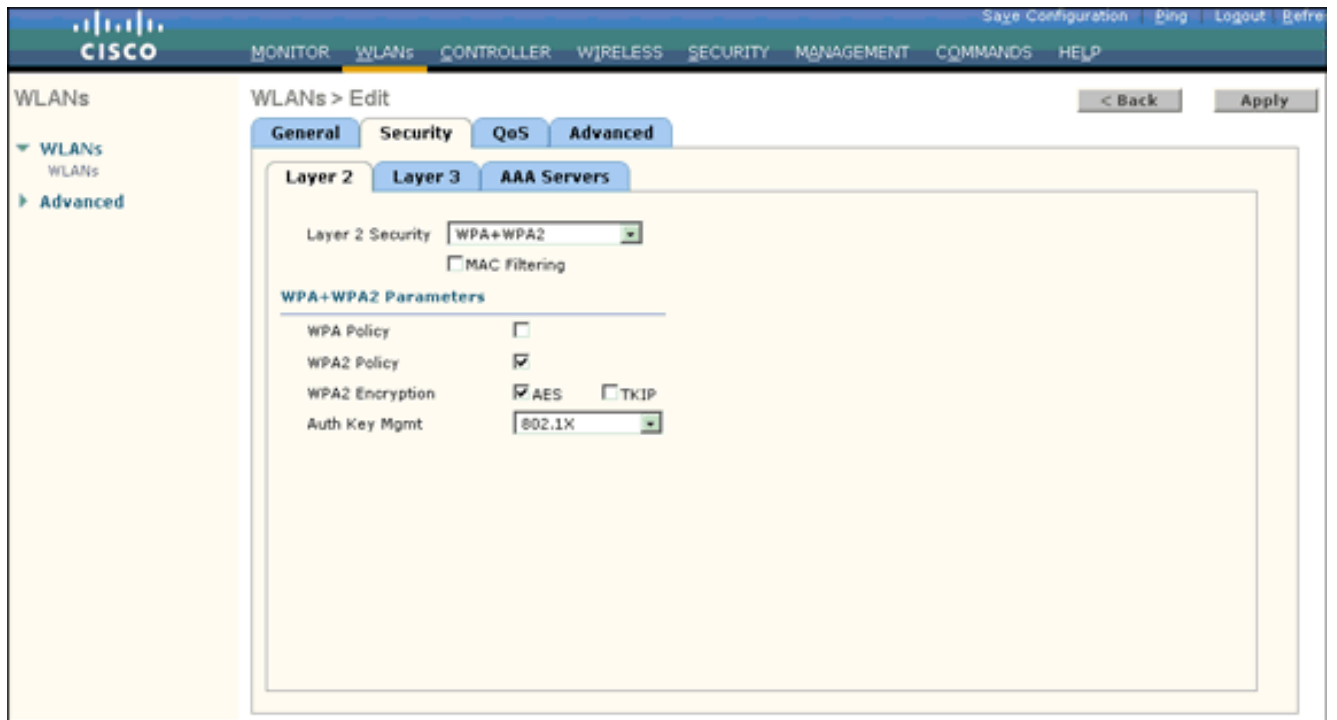
1. 从控制器的 GUI 中单击 **WLAN** 以显示“WLAN”页。此页列出了控制器上现有的 WLAN。
2. 单击 **New** 以创建新的 WLAN。



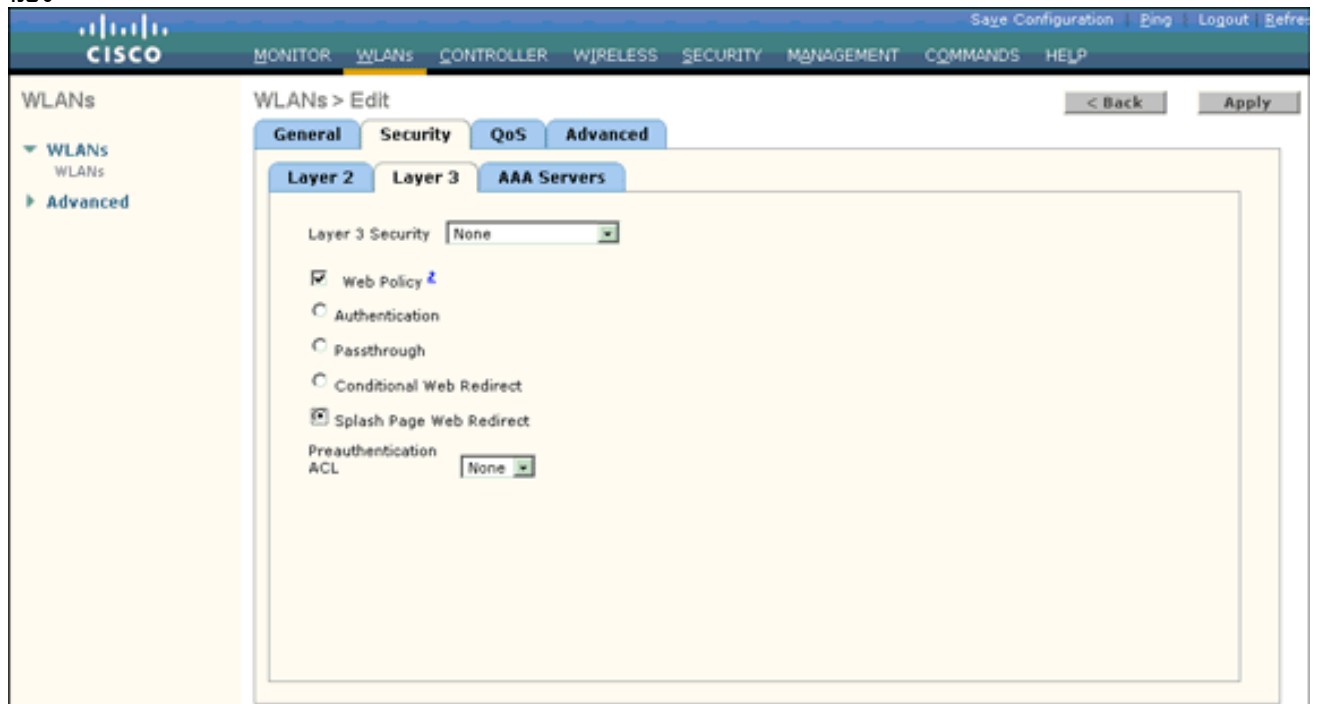
3. 输入WLAN SSID名称和配置文件名称在WLAN >New页。
4. 单击 **Apply**。
5. 首先请让我们创建Admin部门的WLAN。创建新 WLAN 后，就会显示新 WLAN 的 WLAN > Edit 页。在此页上，可以定义特定于此 WLAN 的各种参数。这包括一般策略、安全策略、QoS策略和先进的参数。
6. 根据一般策略，请检查**状态检查**方框来启用WLAN。



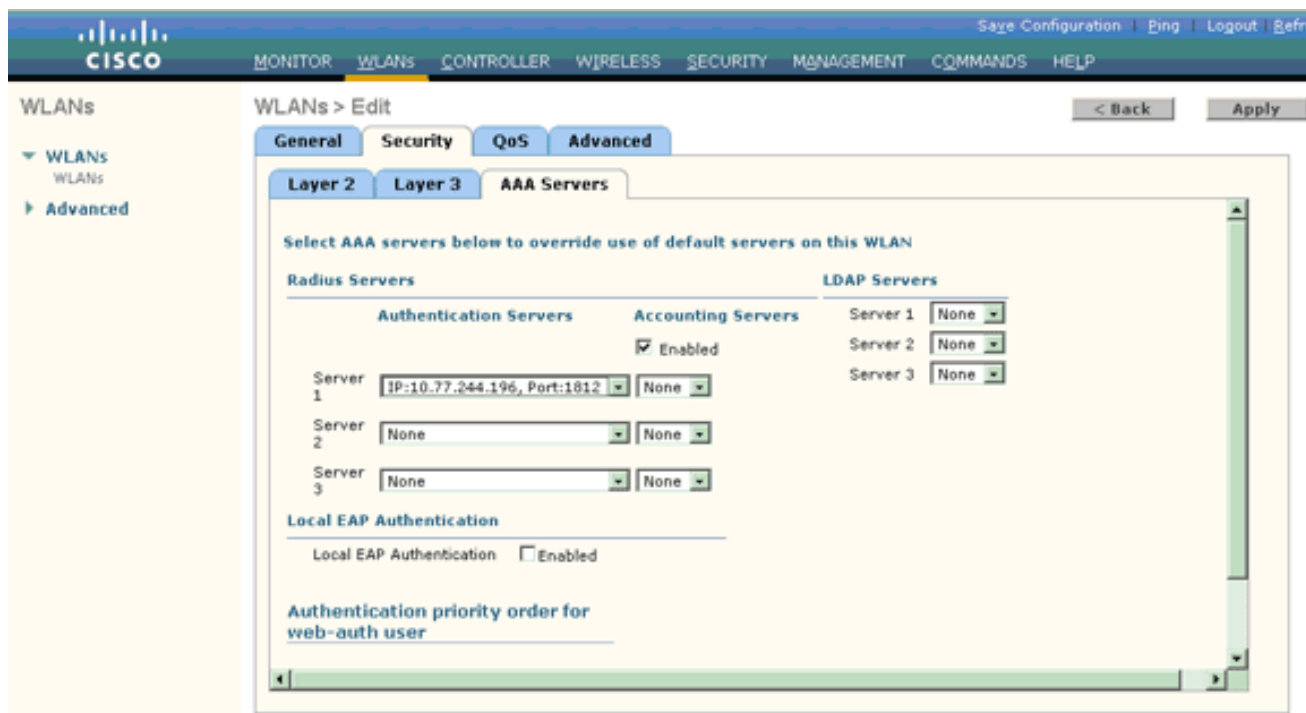
7. 点击**安全选项卡**，然后单击**Layer2选项卡**。
8. 从第2层安全下拉列表选择**WPA+WPA2**。此步骤启用WLAN的WPA验证。
9. 在WPA+WPA2参数下，请检查**WPA2策略**和**AES加密**复选框。



10. 从验证密钥Mgmt下拉列表选择**802.1x**。此选项启用与802.1x/EAP验证的WPA2和WLAN的AES加密。
11. 点击**第3层安全**选项卡。
12. 检查**Web策略**方框，然后单击**飞溅页Web重定向**单选按钮。此选项启用飞溅页Web重定向功能。



13. 单击 **AAA Servers** 选项卡。
14. 在认证服务器下，请从Server1下拉列表选择适当的服务器IP地址。



在本例中，使用 10.77.244.196 作为 RADIUS 服务器。

15. 单击 **Apply**。

16. 重复步骤2至15为了创建工序部门的WLAN。WLAN页列出该两的WLAN您创建。



注意安全策略包括飞溅页重定向。

### 步骤3.配置Cisco Secure ACS支持飞溅页重定向功能。

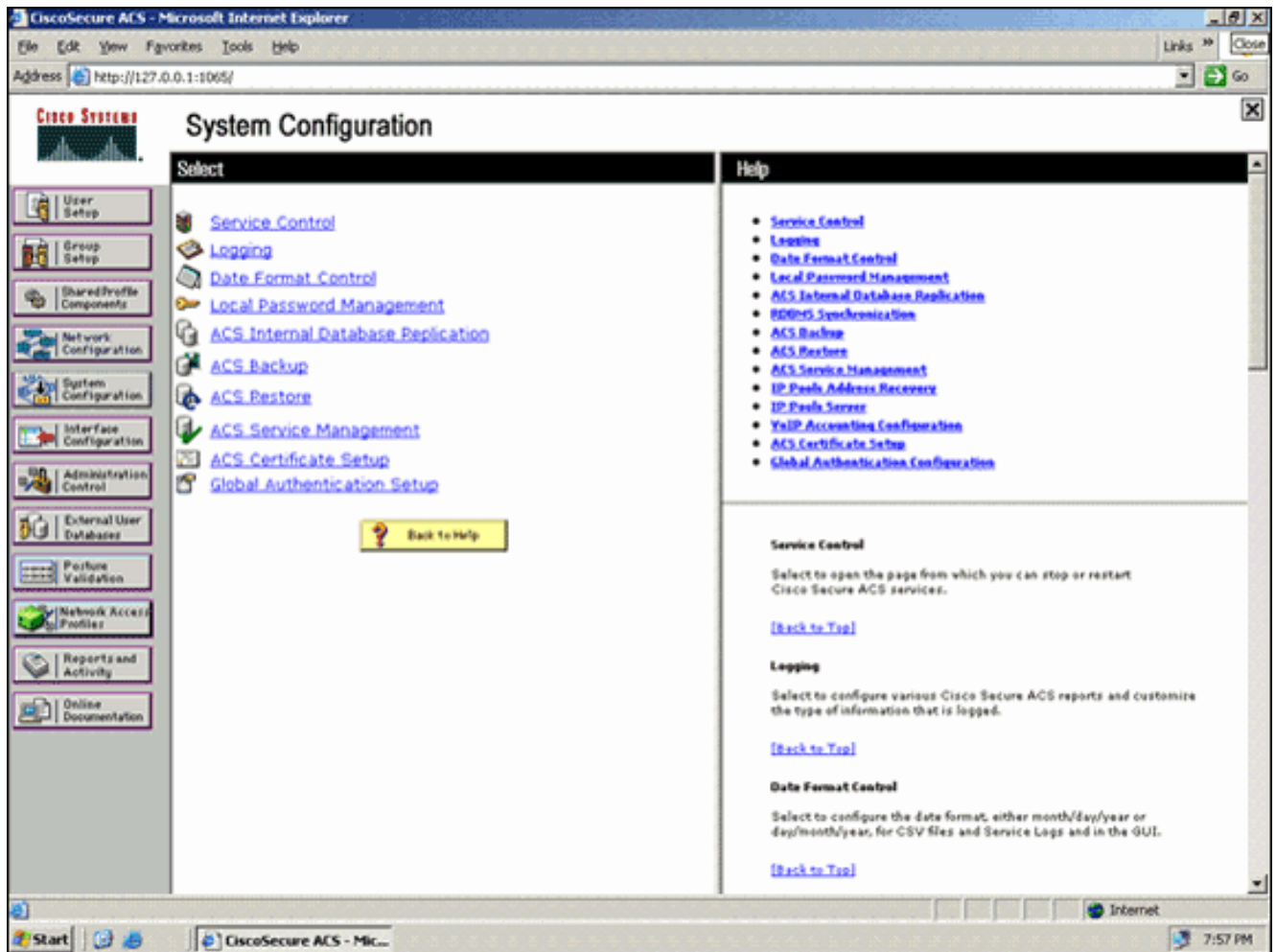
下一步是配置此功能的RADIUS服务器。RADIUS服务器需要执行EAP-FAST验证为了验证客户机证书的，和在成功认证，重定向用户到在Cisco AV对 **url重新定向**RADIUS属性(在外部Web服务器)指定的URL。

#### 配置EAP-FAST验证的Cisco Secure ACS

**注意：** 本文假设，无线局域网控制器被添加到Cisco Secure ACS作为AAA客户端。

完成这些步骤为了配置在RADIUS服务器的EAP-FAST验证：

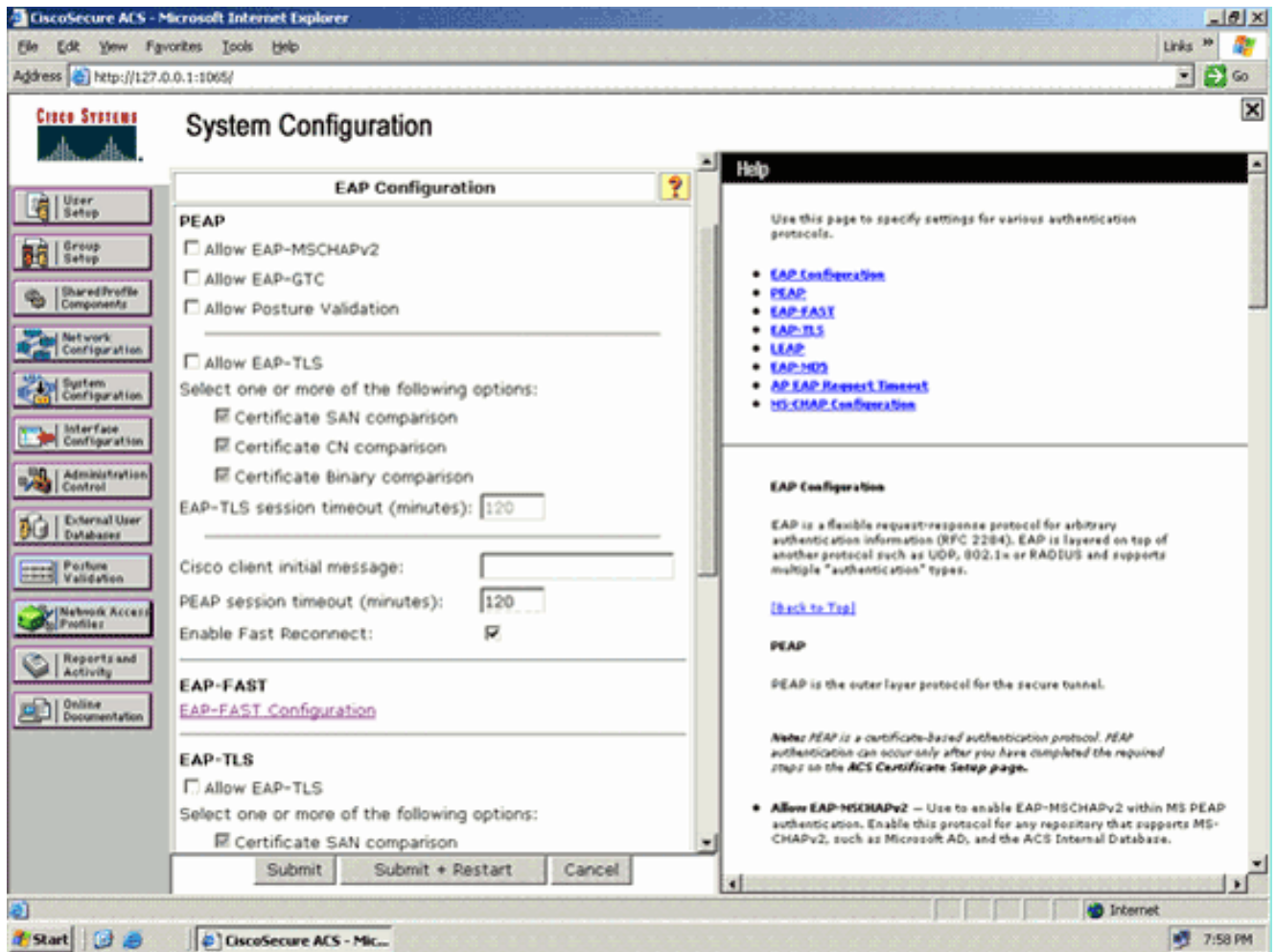
1. 点击从RADIUS服务器GUI的**系统配置**，然后选择从System Configuration Page选择**设置的全局验证**。



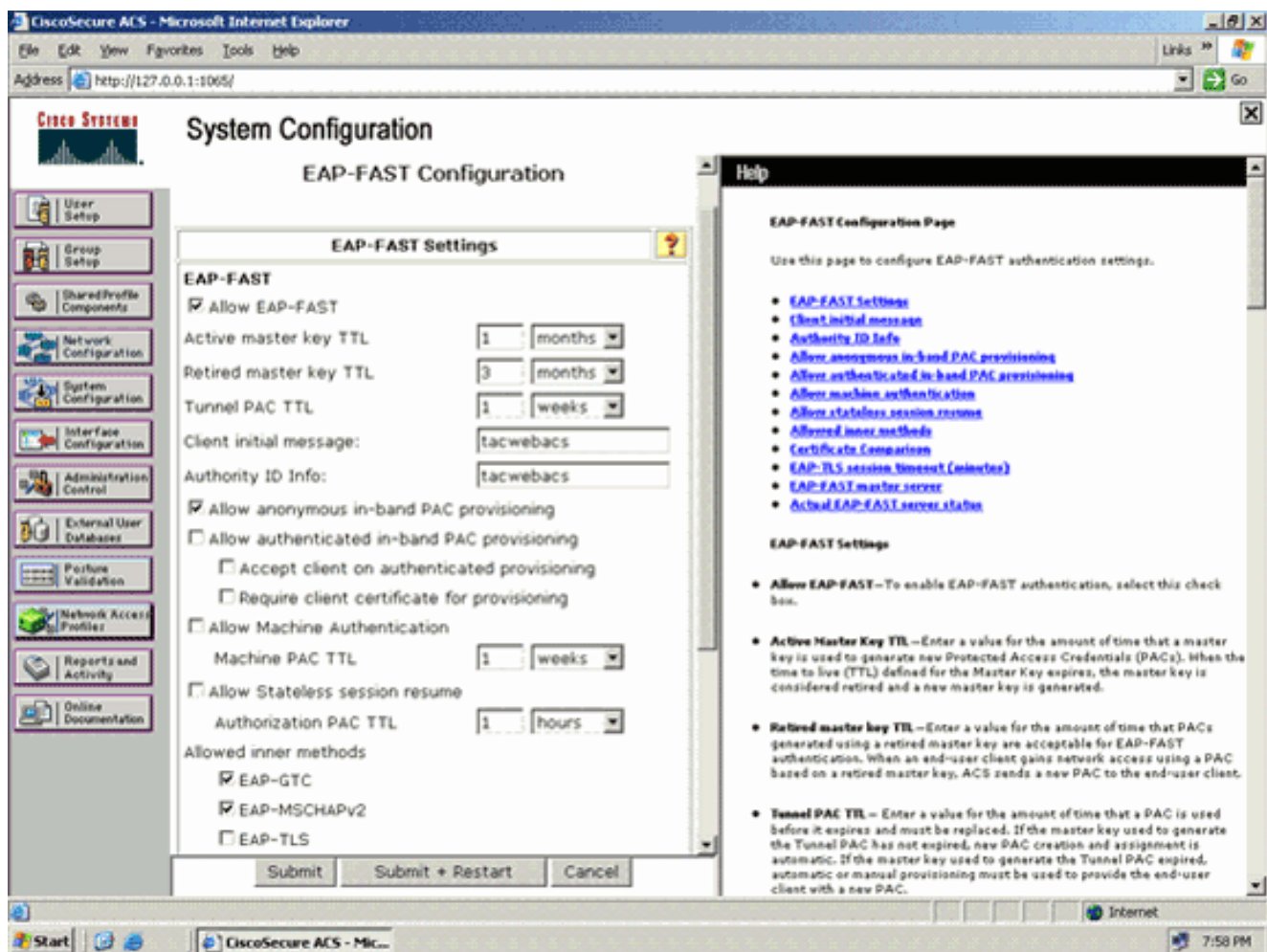
2. 在“Global Authentication”设置页中，单击 **EAP-FAST Configuration** 转到 EAP-FAST 设置页

。





3. 从EAP-FAST Settings页，请检查允许EAP-FAST复选框为了启用在RADIUS服务器的EAP-FAST。



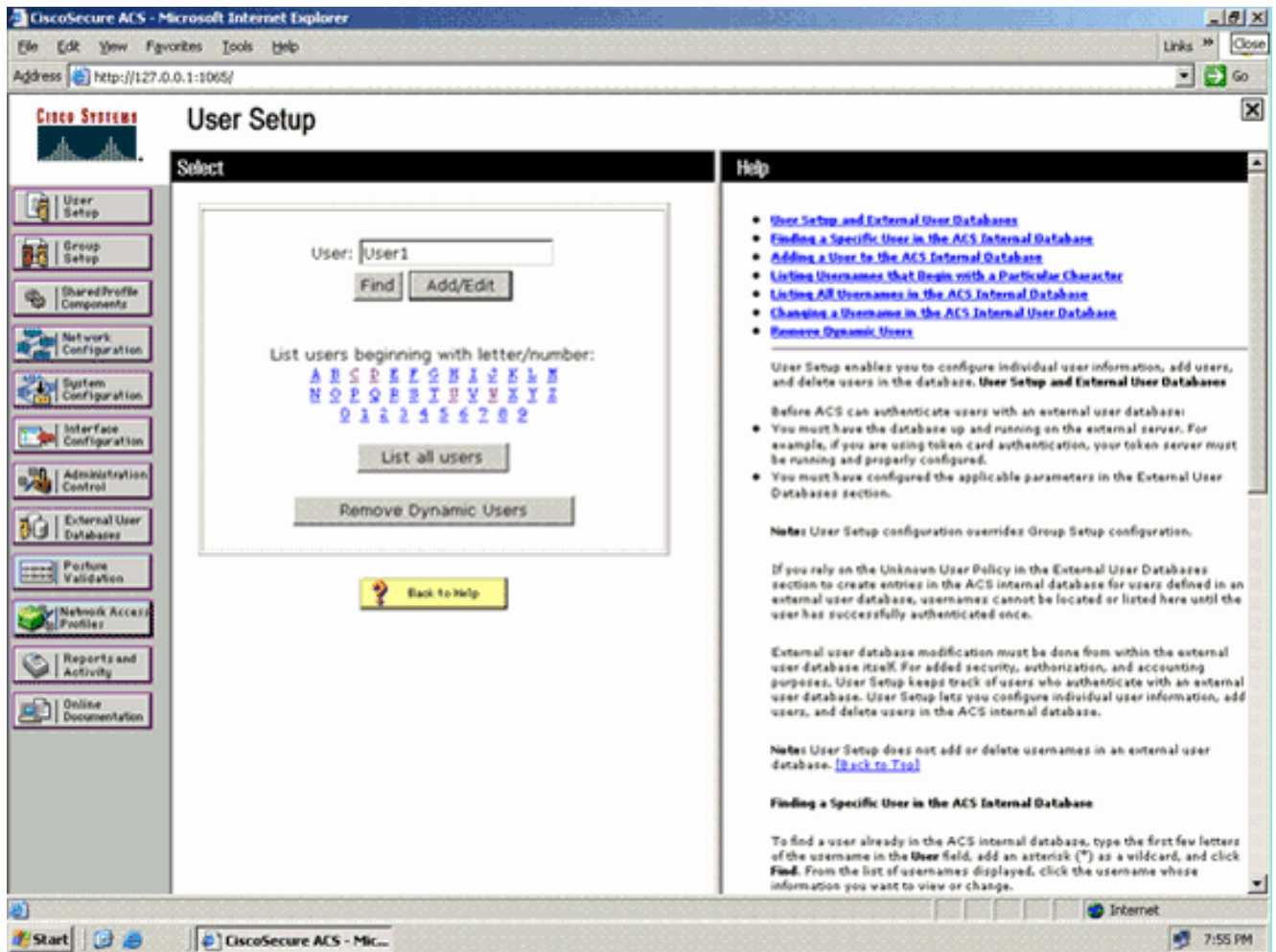
4. 根据需要配置“Active master key TTL”/“Retired master key TTL”（TTL 即存活时间）的值，或按本例所示将其设置为默认值。“Authority ID Info”字段表示此 ACS 服务器的文本身份，最终用户可使用该字段确定要根据哪个 ACS 服务器进行身份验证。必须填写此字段。“Client initial display message”字段用于指定要发送给使用 EAP-FAST 客户端进行身份验证的用户的一条消息。最大长度为 40 个字符。只有最终用户客户端支持显示时，用户才会看到该初始消息。
5. 如果希望 ACS 执行匿名带内 PAC 配置，请选中 **Allow anonymous in-band PAC provisioning** 复选框。
6. 允许内在方法选项确定哪些内在 EAP 方法能运行在 EAP-FAST TLS 通道里面。对于匿名带内配置，必须启用 EAP-GTC 和 EAP-MS-CHAP 以实现向后兼容。如果选择“Allow anonymous in-band PAC provisioning”，则必须选择“EAP-MS-CHAP”（第零阶段）和“EAP-GTC”（第二阶段）。
7. 单击 **submit**。注意：对于详细信息和示例关于如何配置 EAP 法塞特与匿名带内 PAC 设置和已验证在波段之内供应，参考[EAP-FAST 验证与无线局域网控制器和外部 RADIUS 服务器配置示例](#)。

## 配置用户数据库并且定义 url 重新定向 RADIUS 属性

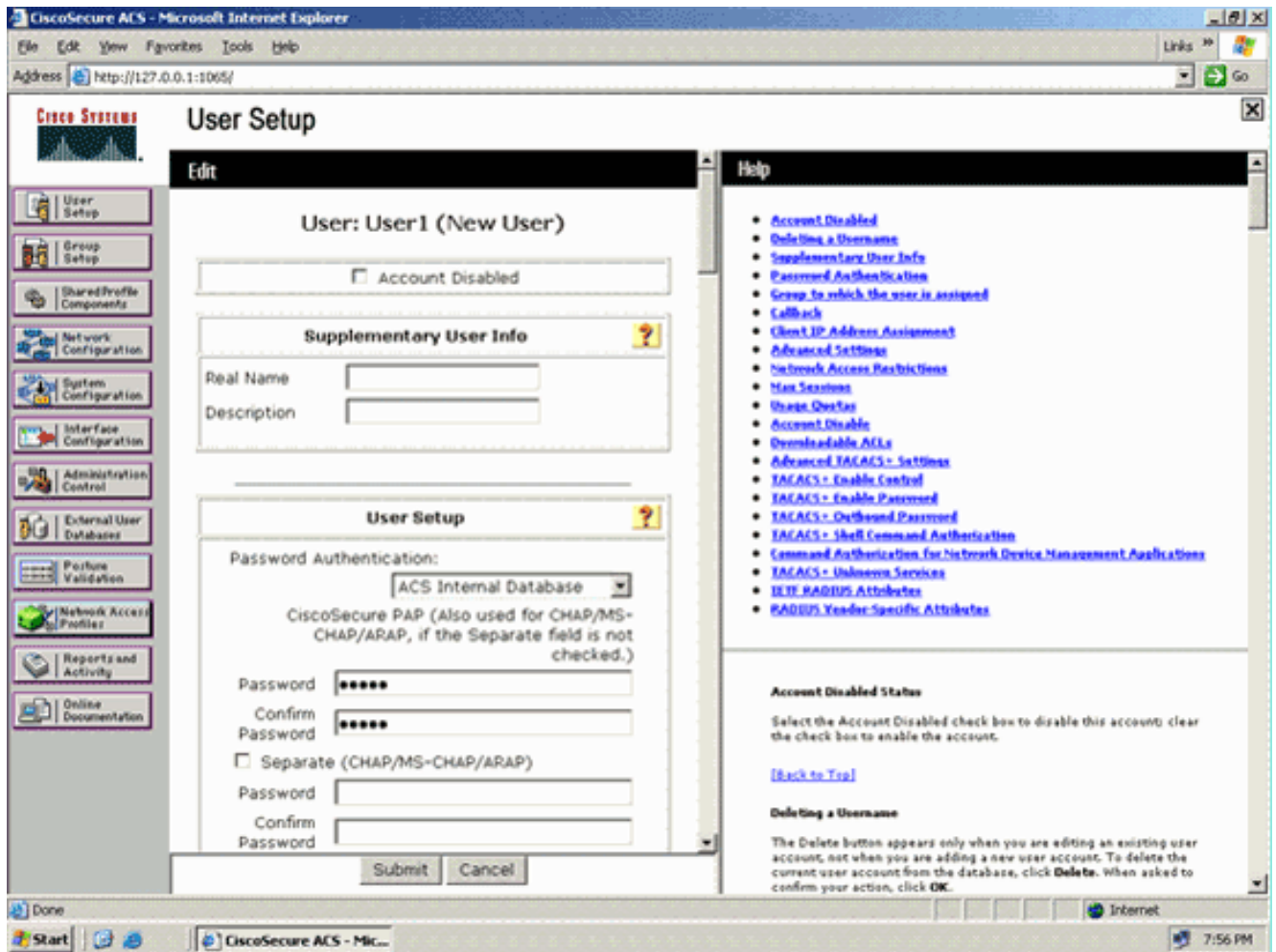
此示例配置无线客户端的用户名和密码作为 User1 和 User1，分别。

完成这些步骤为了创建用户数据库：

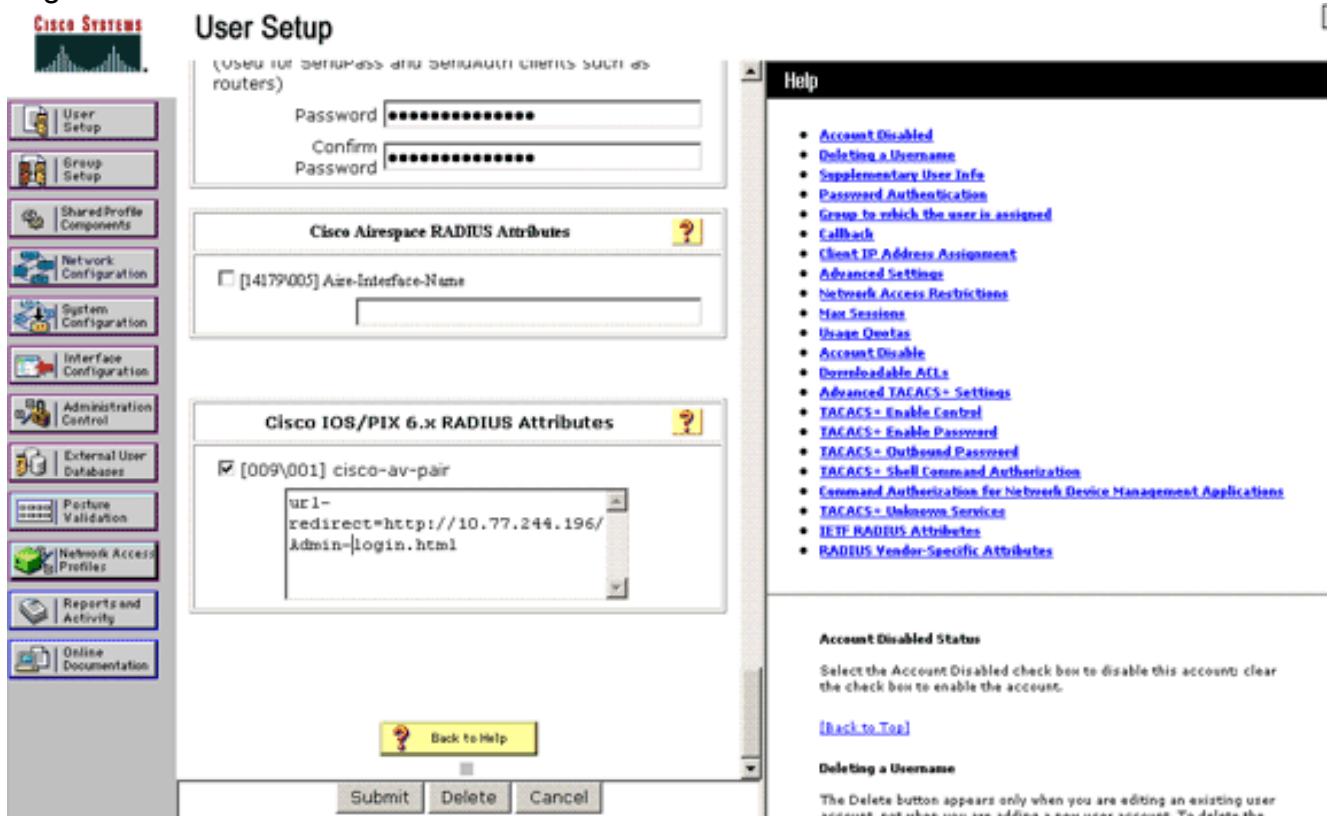
1. 从 ACS GUI 在导航条，请选择 **用户设置**。
2. 创建一个新的无线用户，然后单击 **Add/Edit** 转到该用户的“编辑”页。



3. 如此示例所显示，从Edit页的用户设置，请配置真名和说明，以及密码设置。本文档使用 ACS Internal Database 作为“Password Authentication”。



4. 把页移下来修改RADIUS属性。
5. 检查[009\001] cisco-av-pair复选框。
6. 输入在[009\001] cisco-av-pair编辑框的此Cisco AV对为了指定用户重定向的URL : url-redirect=http://10.77.244.196/Admin-Login.html



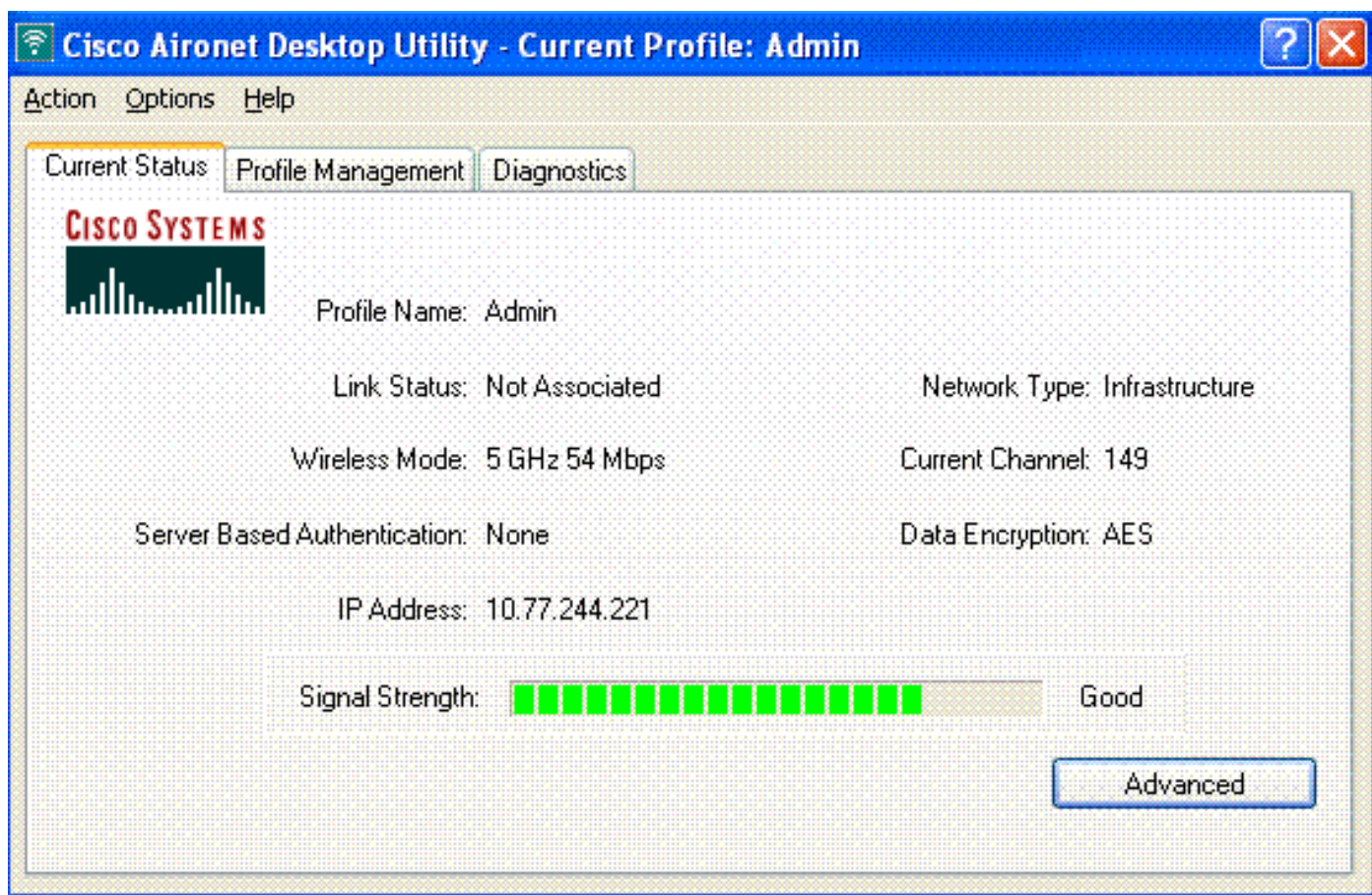
这是Admin部门用户的主页。

7. 单击 **submit**。
8. 重复此步骤为了添加User2 (工序部门用户)。
9. 重复步骤1至6为了添加更多Admin部门用户和工序部门用户到数据库。注意：RADIUS属性可以配置在用户级或社团级别在Cisco Secure ACS。

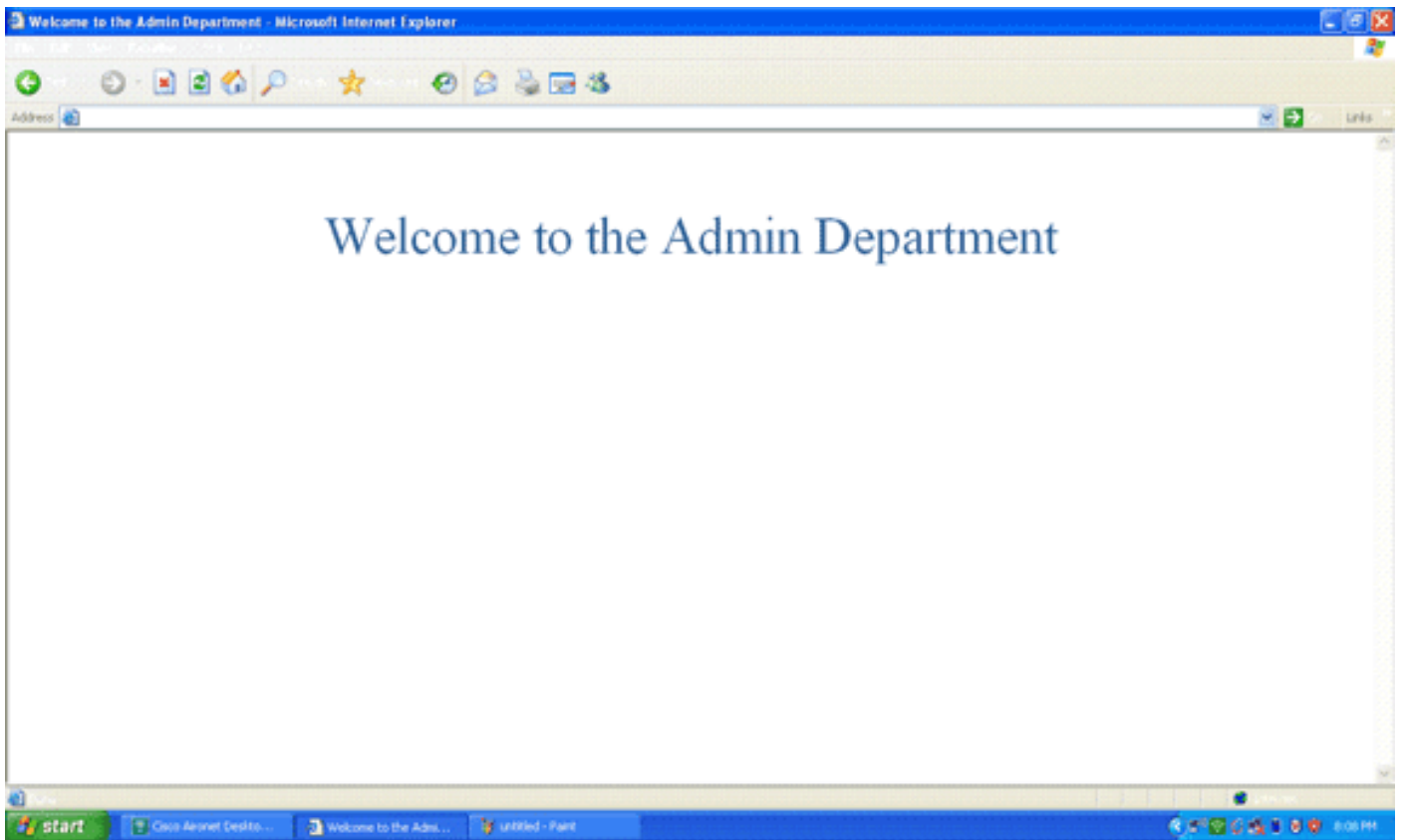
## 验证

为了验证配置，请关联从Admin部门和工序部门的一个WLAN客户端到他们适当的WLAN。

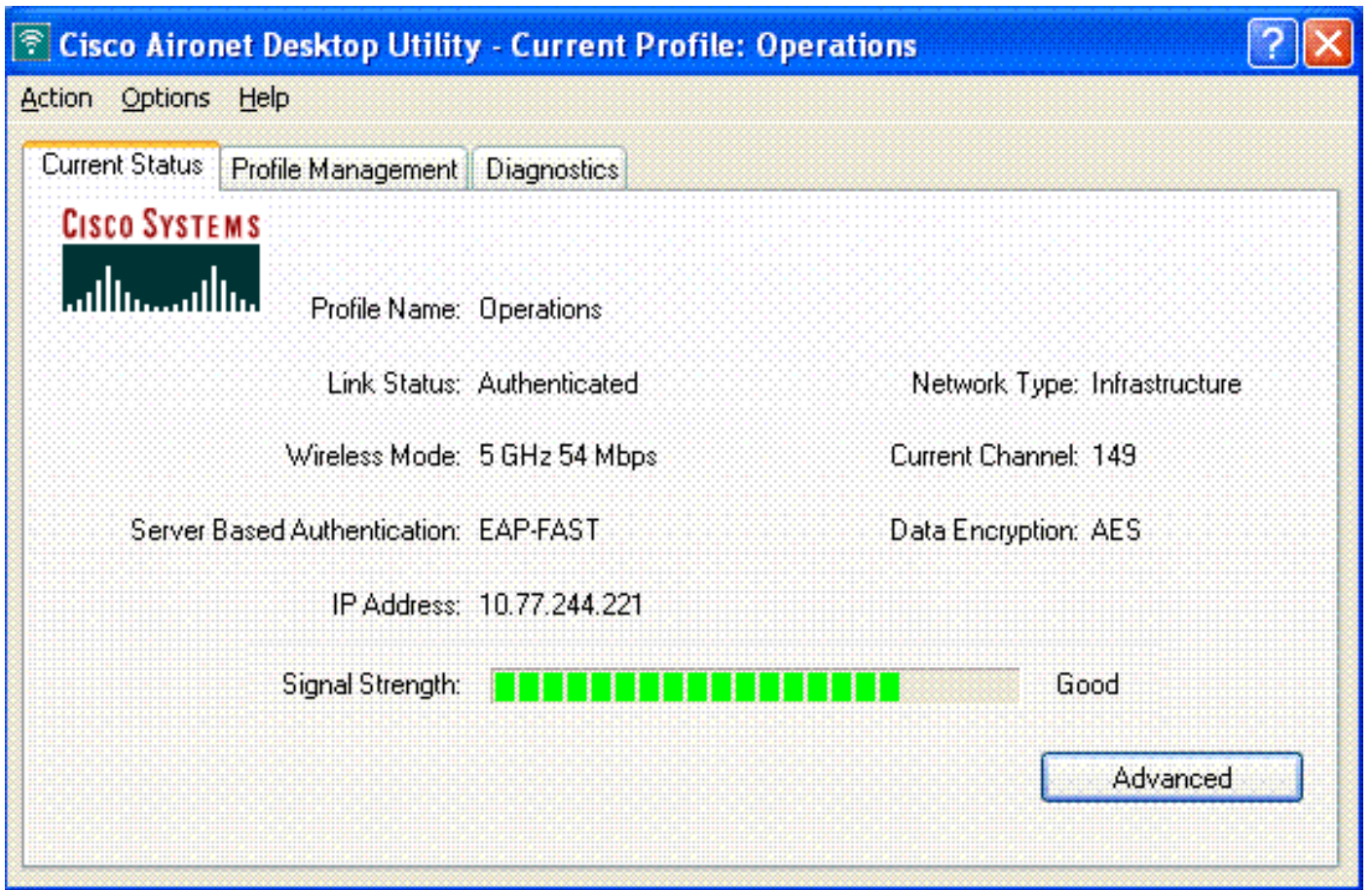
当从Admin部门的一个用户连接对无线局域网Admin时，提示用户输入802.1x凭证(在我们的情况的EAP-FAST凭证)。一旦用户提供凭证，WLC通过那些凭证到Cisco Secure ACS服务器。Cisco Secure ACS服务器验证用户凭据数据库和在成功认证，返回url重新定向属性到无线局域网控制器。验证在此阶段完成。

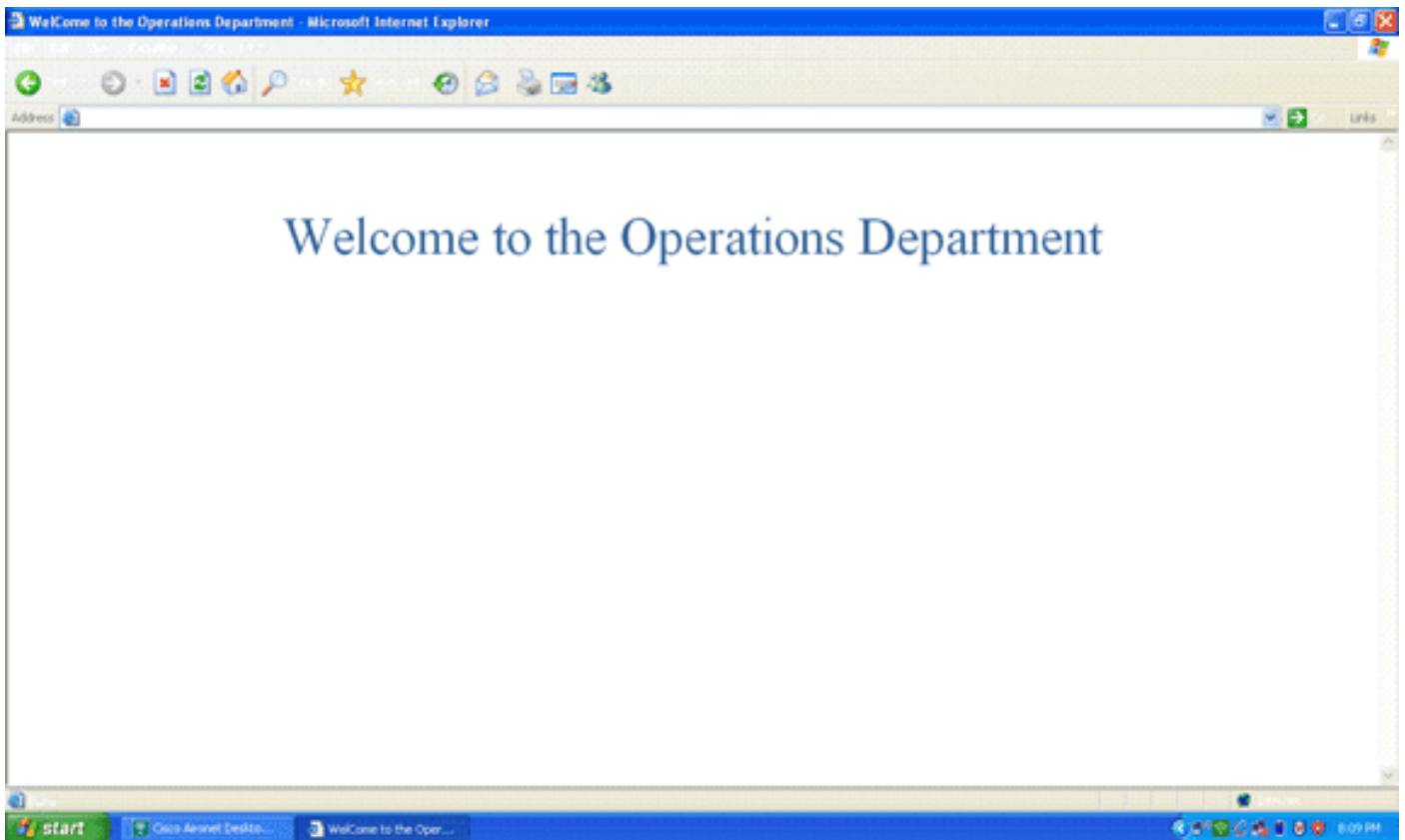


当用户打开Web浏览器时，用户重定向对Admin部门的主页URL。(此URL返回对WLC通过cisco-av-pair属性)。在重定向，用户有对网络后的完全权限。这是屏幕画面：



当从工序部门的一个用户连接对WLAN操作，同样事件顺序出现。





## 故障排除

本部分提供的信息可用于对配置进行故障排除。

**注意：** 使用 `debug` 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

您能使用以下命令排除故障您的配置。

- **显示WLAN wlan\_id** —显示Web重定向功能的状况—特定的WLAN的。示例如下：`WLAN`

```
Identifier..... 1
Profile Name..... Admin
Network Name (SSID)..... Admin
...
Web Based Authentication..... Disabled
Web-Passthrough..... Disabled
Conditional Web Redirect..... Disabled
Splash-Page Web Redirect..... Enabled
```

- **debug dot1x事件enable (event)** —启用802.1x数据包消息调试。示例如下：`Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP Request from AAA to mobile 00:40:96:ac:dd:05 (EAP Id 16) Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAPOL EAPPKT from mobile 00:40:96:ac:dd:05 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAP Response from mobile 00:40:96:ac:dd:05 (EAP Id 16, EAP Type 43) Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Processing Access-Challenge for mobile 00:40:96:ac:dd:05 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Setting re-auth timeout to 1800 seconds, got from WLAN config. Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Station 00:40:96:ac:dd:05 setting dot1x reauth timeout = 1800 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Creating a new PMK Cache Entry for station 00:40:96:ac:dd:05 (RSN 2) Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Adding BSSID 00:1c:58:05:e9:cf to PMKID cache for station 00:40:96:ac:dd:05 Fri Feb 29 10:27:16 2008: New PMKID: (16) Fri Feb 29 10:27:16 2008: [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca fb fa 8e 3c Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Disabling re-auth since PMK lifetime can take care of same. Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP-Success to mobile 00:40:96:ac:dd:05 (EAP Id 17) Fri Feb 29 10:27:16 2008: Including PMKID in M1 (16) Fri Feb 29 10:27:16 2008: [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca fb fa 8e 3c Fri`

Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAPOL-Key Message to mobile  
00:40:96:ac:dd:05 state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00 Fri Feb  
29 10:27:16 2008: 00:40:96:ac:dd:05 Received Auth Success while in Authenticating state for  
mobile 00:40:96:ac:dd:05

- **debug aaa事件enable (event)** —启用所有aaa事件debug输出。示例如下：Thu Feb 28 07:55:18  
2008: 00:40:96:ac:dd:05 Successful transmission of Authentication Packet (id 103) to  
10.77.244.196:1812, proxy state 00:40:96:ac:dd:05-00:00 Thu Feb 28 07:55:18 2008: \*\*\*\*Enter  
processIncomingMessages: response code=11 Thu Feb 28 07:55:18 2008: \*\*\*\*Enter  
processRadiusResponse: response code=11 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-  
Challenge received from RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId =  
3 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of Authentication  
Packet (id 104) to 10.77.244.196:1812, proxy state 00:40:96:ac:dd:05-00:00 Thu Feb 28  
07:55:18 2008: \*\*\*\*Enter processIncomingMessages: response code=2 Thu Feb 28 07:55:18 2008:  
\*\*\*\*Enter processRadiusResponse: response code=2 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05  
Access-Accept received from RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05  
receiveId = 3 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 AAA Override Url-Redirect  
'http://10.77.244.196/Admin-login.html' set Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05  
Applying new AAA override for station 00:40:96:ac:dd:05 Thu Feb 28 07:55:18 2008:  
00:40:96:ac:dd:05 Override values for station 00:40:96:ac:dd:05 source: 4, valid bits: 0x0  
qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1 dataAvgC: -1,  
rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1 vlanIfName: '', aclName: '

## [相关信息](#)

- [Cisco 无线 LAN 控制器配置指南 5.0 版](#)
- [无线局域网控制器 Web 身份验证配置示例](#)
- [使用无线局域网控制器的外部 Web 身份验证配置示例](#)
- [无线支持页](#)
- [技术支持和文档 - Cisco Systems](#)