无线局域网控制器Splash页重定向配置示例

Contents

Introduction

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。

Prerequisites

Requirements

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

Components Used

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

The information in this document was created from the devices in a specific lab environment.All of

the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

背景信息

飞溅页Web重定向是功能被引入无线局域网控制器版本5.0。使用此功能，在802.1x认证完成了后，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(配置有系统设计的主页)或设法访问URL。在对网页的重定向完成后，用户有全部存取对网络。

您在远程验证拨入用户服务(RADIUS)服务器能指定重定向页。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认证。

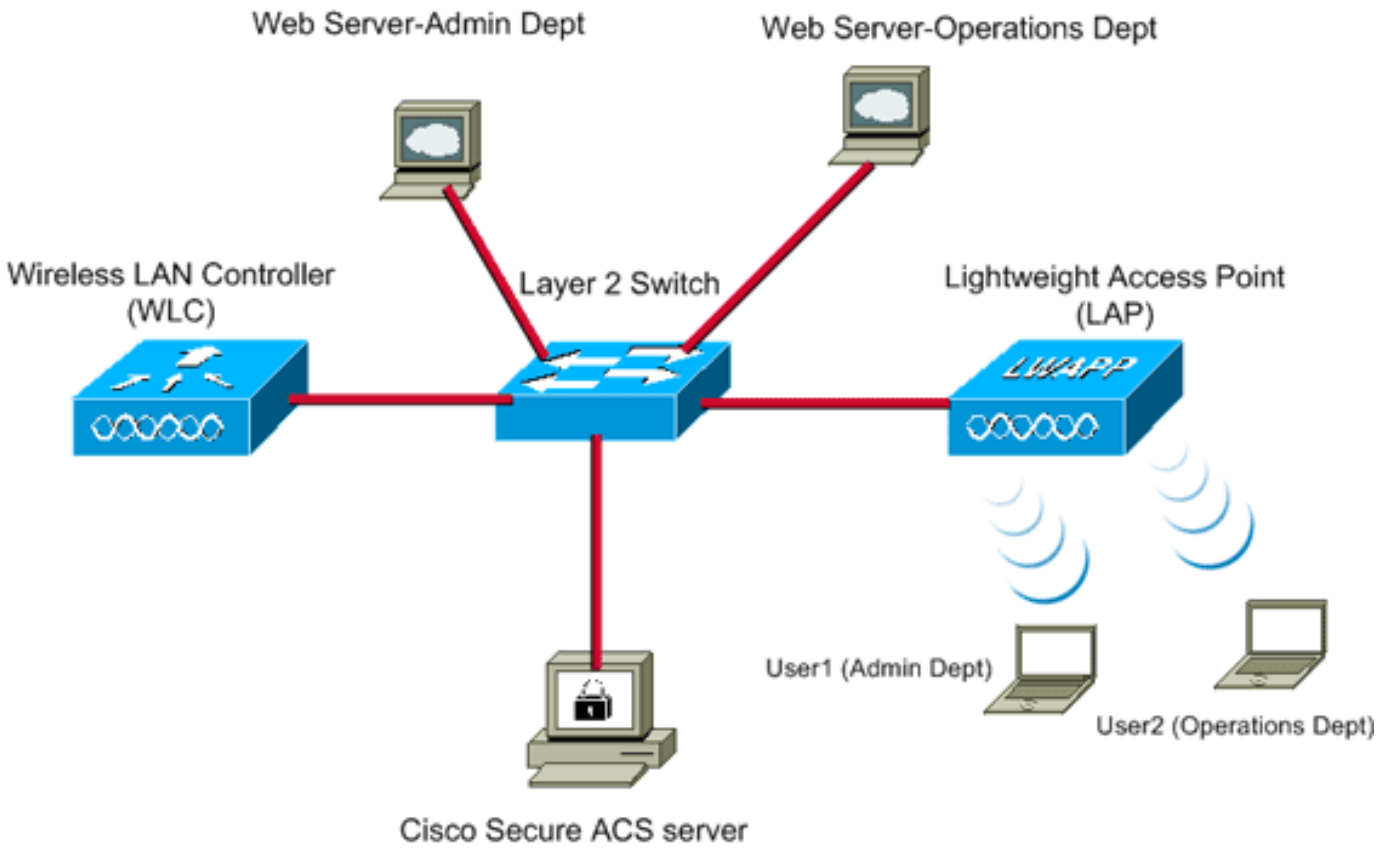
飞溅页Web重定向功能为802.1x或WPA/WPA2第2层安全的配置是仅可用的。

网络设置

在本例中， Cisco 4404 WLC和Cisco 1232系列LAP通过第2层交换机被连接。作为一个外部RADIUS服务器)的Cisco Secure ACS服务器(也被连接到同一台交换机。所有设备在相同子网。

LAP最初注册到控制器。您必须创建两WLANs ：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使用认证)。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。

Configure

本部分提供有关如何配置本文档所述功能的信息。

Note: 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：

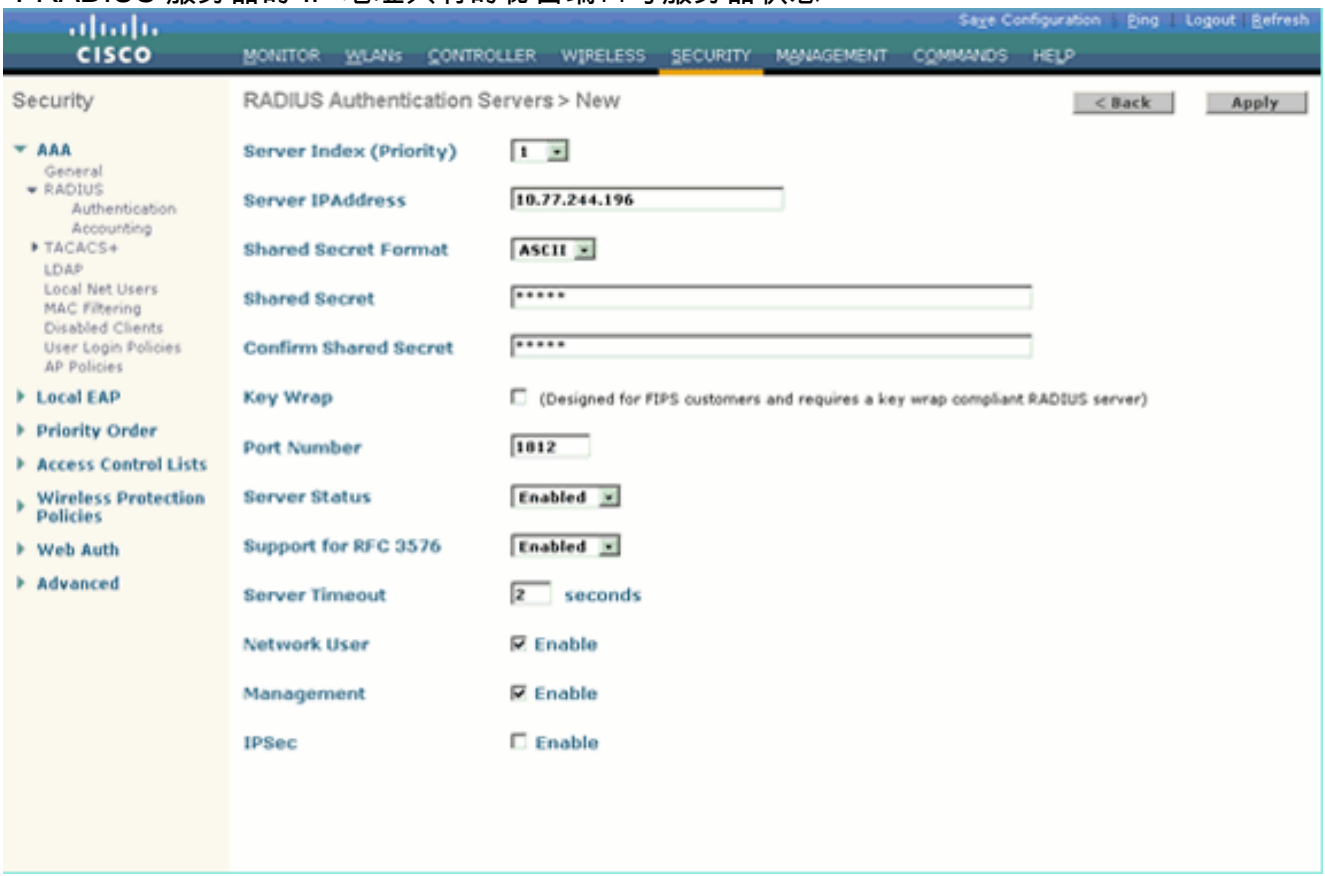
1. 通过Cisco Secure ACS服务器配置RADIUS认证的WLC。
2. 配置Admin和工序部门的WLANs。
3. 配置Cisco Secure ACS支持飞溅页重定向功能。

步骤1.通过Cisco Secure ACS服务器配置RADIUS认证的WLC。

需要配置WLC为了转发用户凭证到一个外部RADIUS服务器。

完成这些步骤为了配置一个外部RADIUS服务器的WLC ：

1. 从控制器GUI选择**安全**和**RADIUS认证**为了显示RADIUS验证服务器页。
2. 点击**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 地址共有的秘密端口号服务器状态



本文以10.77.244.196的IP地址使用ACS服务器。

4. 单击 **Apply**。

步骤2.配置Admin和工序部门的WLANs。

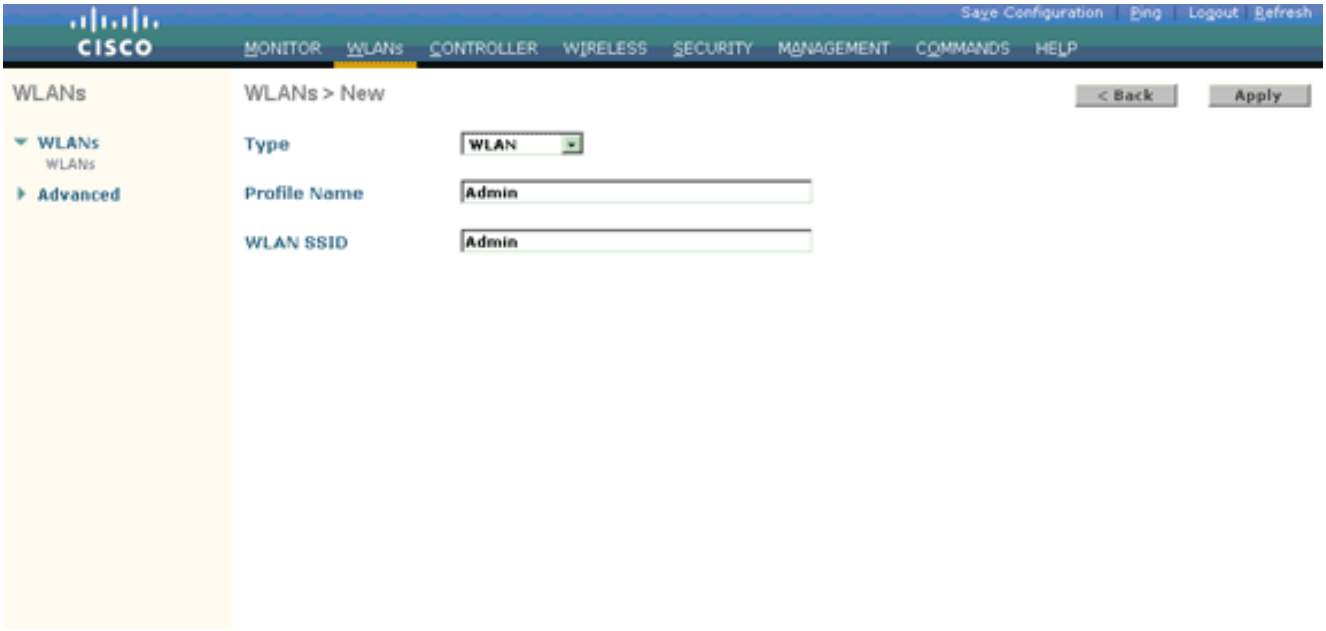
在此步骤，您配置客户端将使用为了连接到无线网络的两个WLANs (一Admin部门的和其他工序部门的)。

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

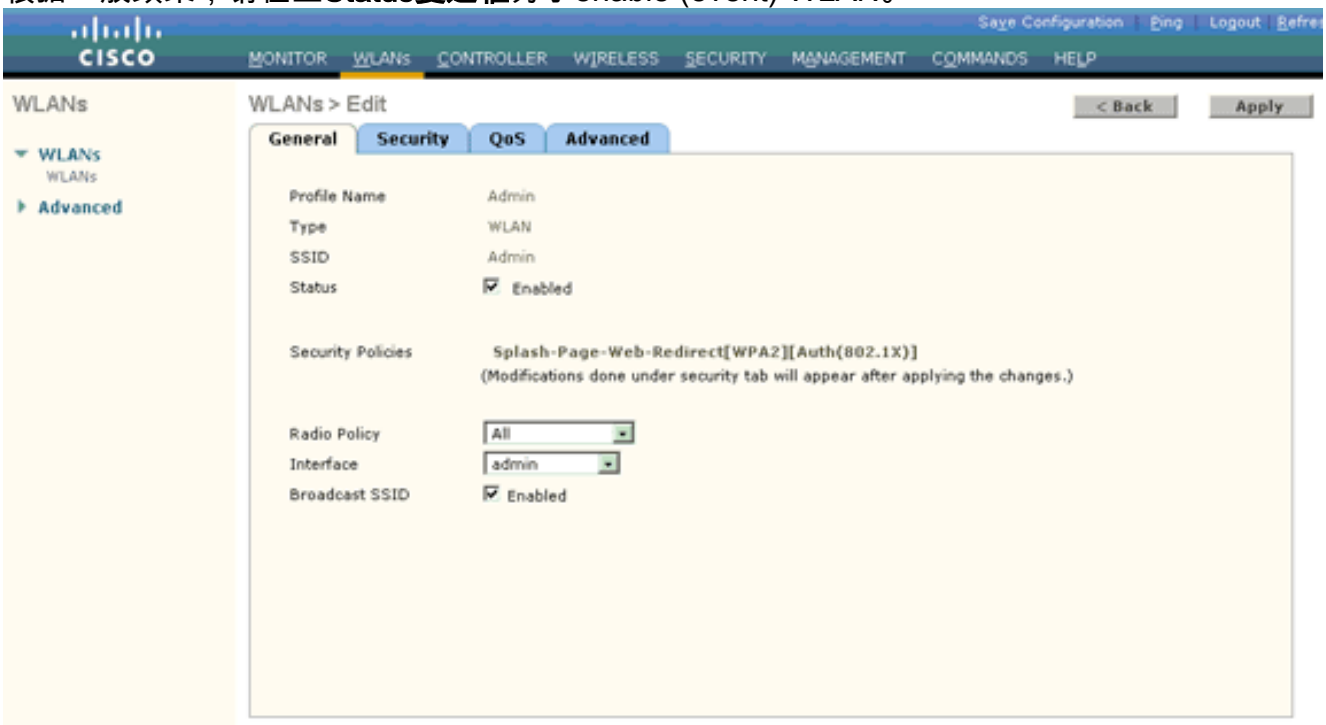
请使用EAP-FAST认证为了enable (event) WPA2作为在WLANs和Web策略的第2层安全机制-请飞溅页Web重定向功能作为第3层安全方法。

若要配置 WLAN 及其相关参数，请完成下列步骤：

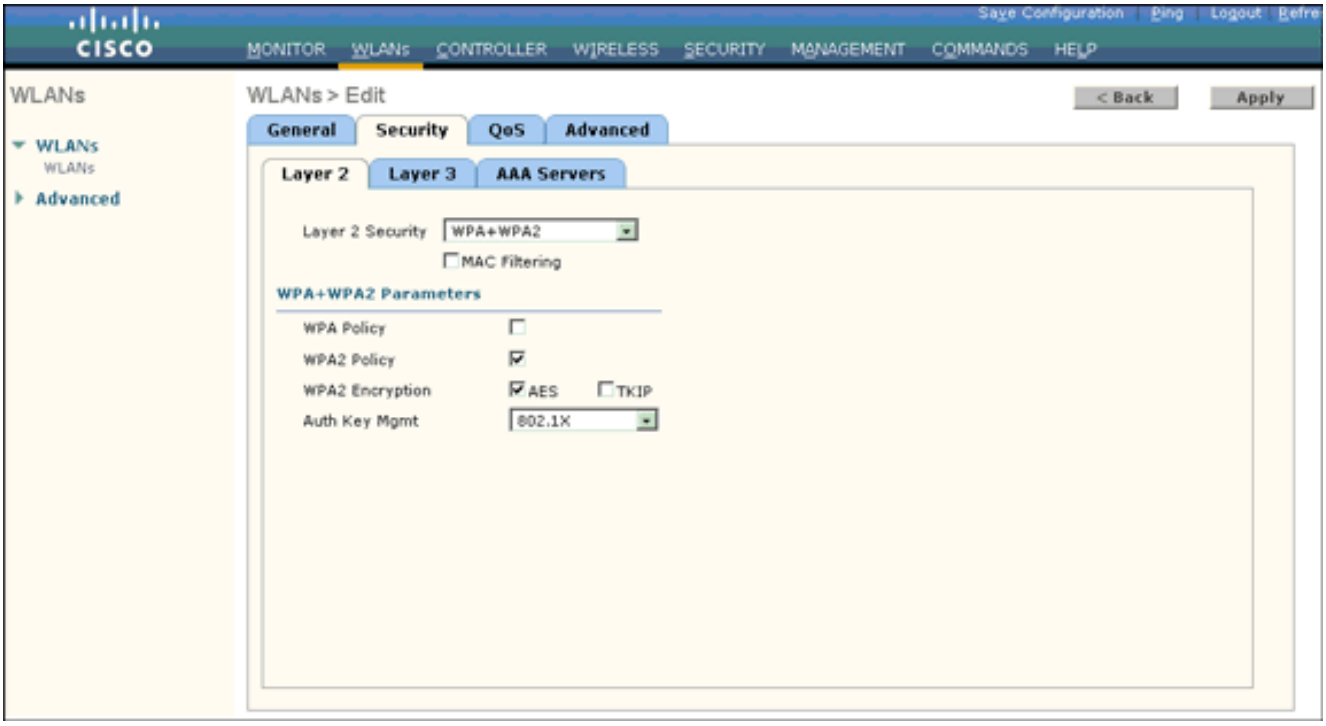
1. 从控制器的 GUI 中单击 **WLAN** 以显示“WLAN”页。此页列出在控制器存在的WLANs。
2. 单击 **New** 以创建新的 WLAN。



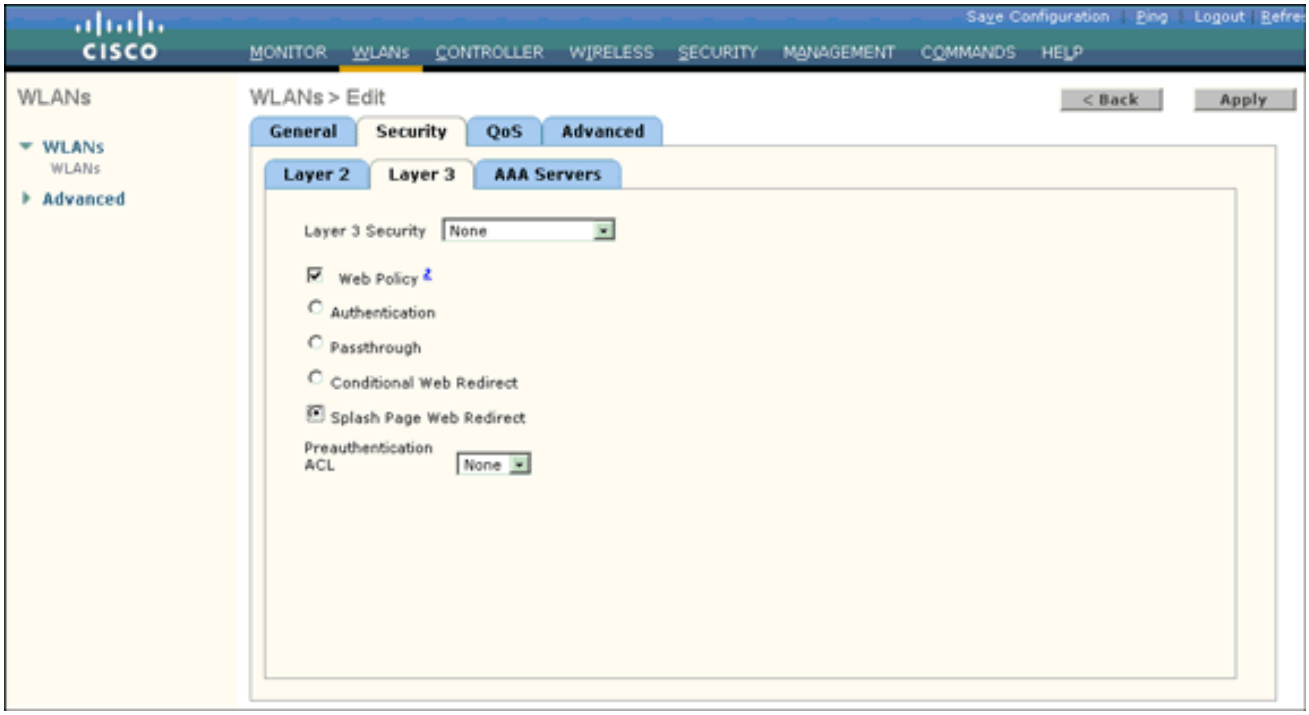
3. 输入WLAN SSID名称和配置文件名字在WLANs >New页。
4. 单击 **Apply**。
5. 首先请让我们创建Admin部门的WLAN。一旦创建一新的WLAN，新的WLAN的WLAN > Edit页出版。在此页上，可以定义特定于此 WLAN 的各种参数。这包括一般政策、安全策略、QoS策略和先进的参数。
6. 根据一般政策，请检查**Status复选框**为了enable (event) WLAN。



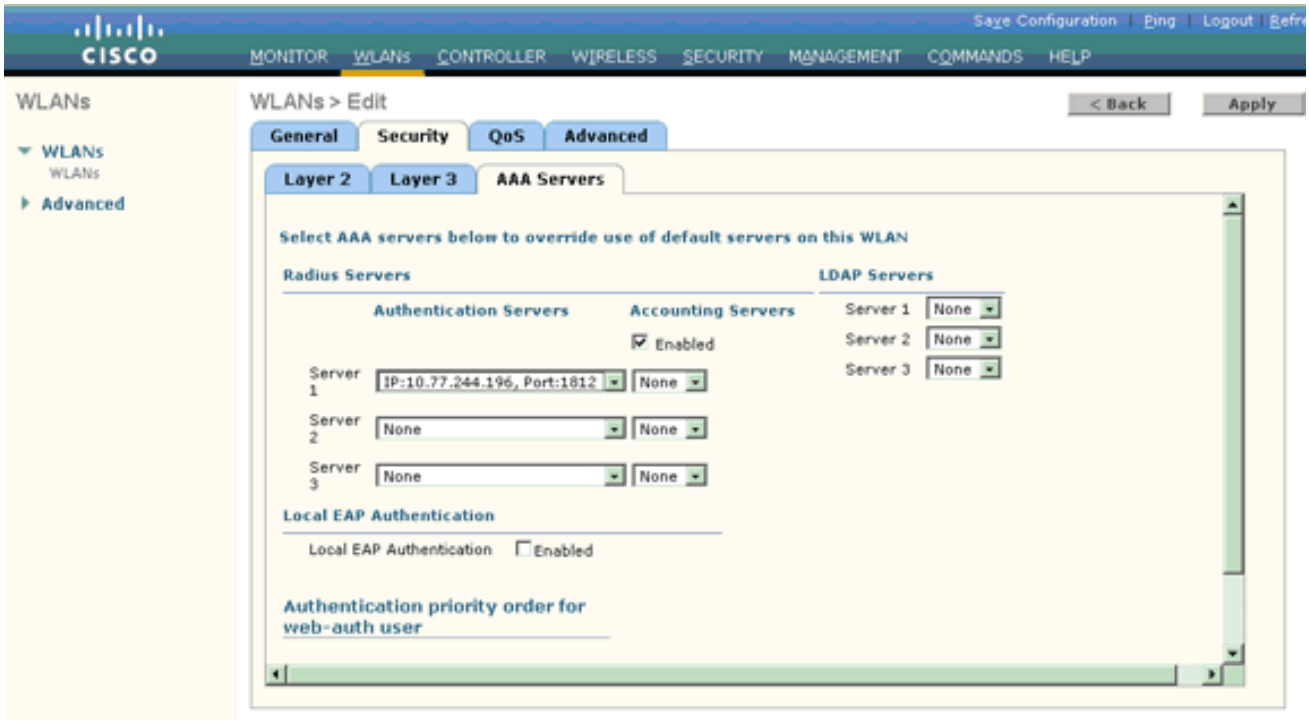
7. 点击**安全**选项，然后点击第**2层**选项。
8. 从第2层安全下拉列表选择**WPA+WPA2**。WLAN的此步骤enable (event) WPA验证。
9. 在WPA+WPA2参数下，请检查**WPA2策略**和**AES加密**复选框。



10. 从Auth键Mgmt下拉列表选择**802.1x**。与802.1x/EAP认证和AES加密的此选项enable (event) WPA2 WLAN的。
11. 点击**第3层安全**选项。
12. 检查**Web策略**机箱，然后点击**飞溅页Web重定向**单选按钮。此选项enable (event)飞溅页Web重定向功能。

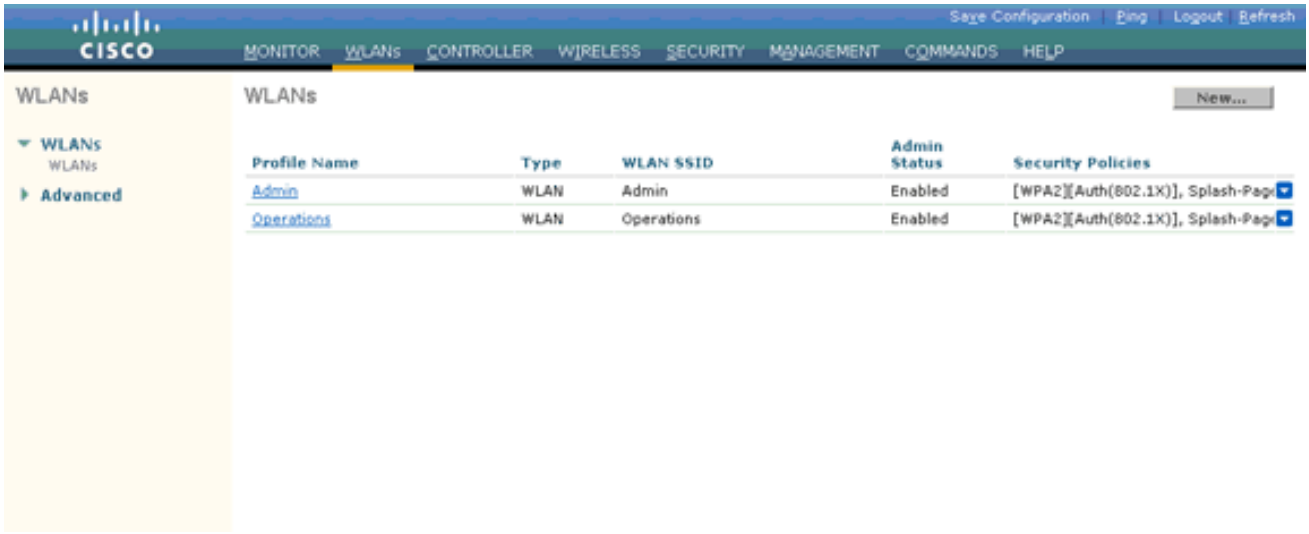


13. 单击 **AAA Servers** 选项卡。
14. 在认证服务器下，从Server1下拉列表请选择适当的服务器IP地址。



在本例中，使用 10.77.244.196 作为 RADIUS 服务器。

15. 单击 **Apply**。
16. 重复第2步至第15步为了创建工序部门的WLAN。WLANs页列出您创建的两个WLANs。



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。

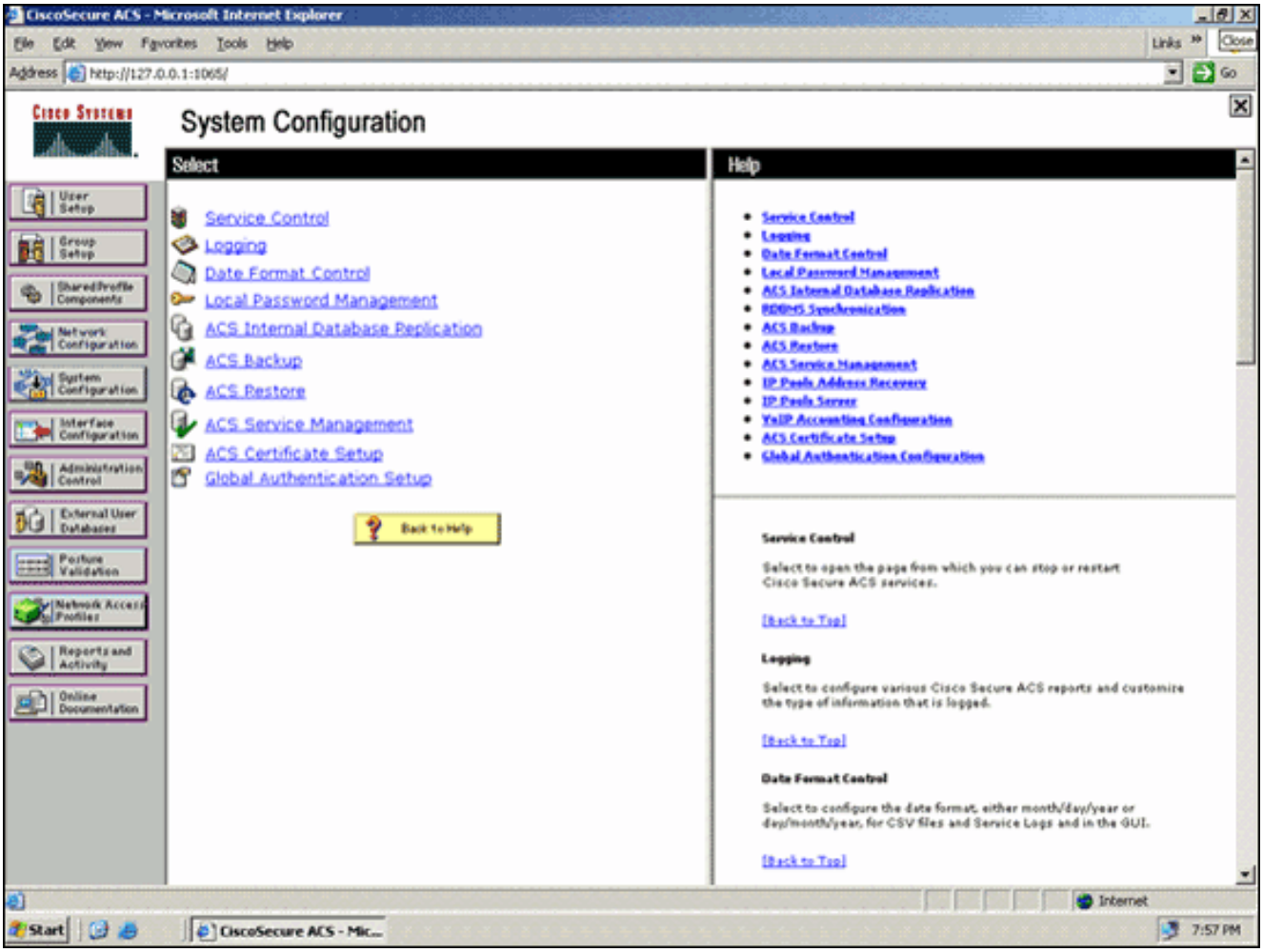
下一步是配置此功能的RADIUS服务器。RADIUS服务器需要进行EAP-FAST认证为了验证客户机证书的，和在成功的验证，重定向用户到URL (在外部Web服务器)指定在Cisco AV对***url重新定向***RADIUS属性。

配置EAP-FAST认证的Cisco Secure ACS

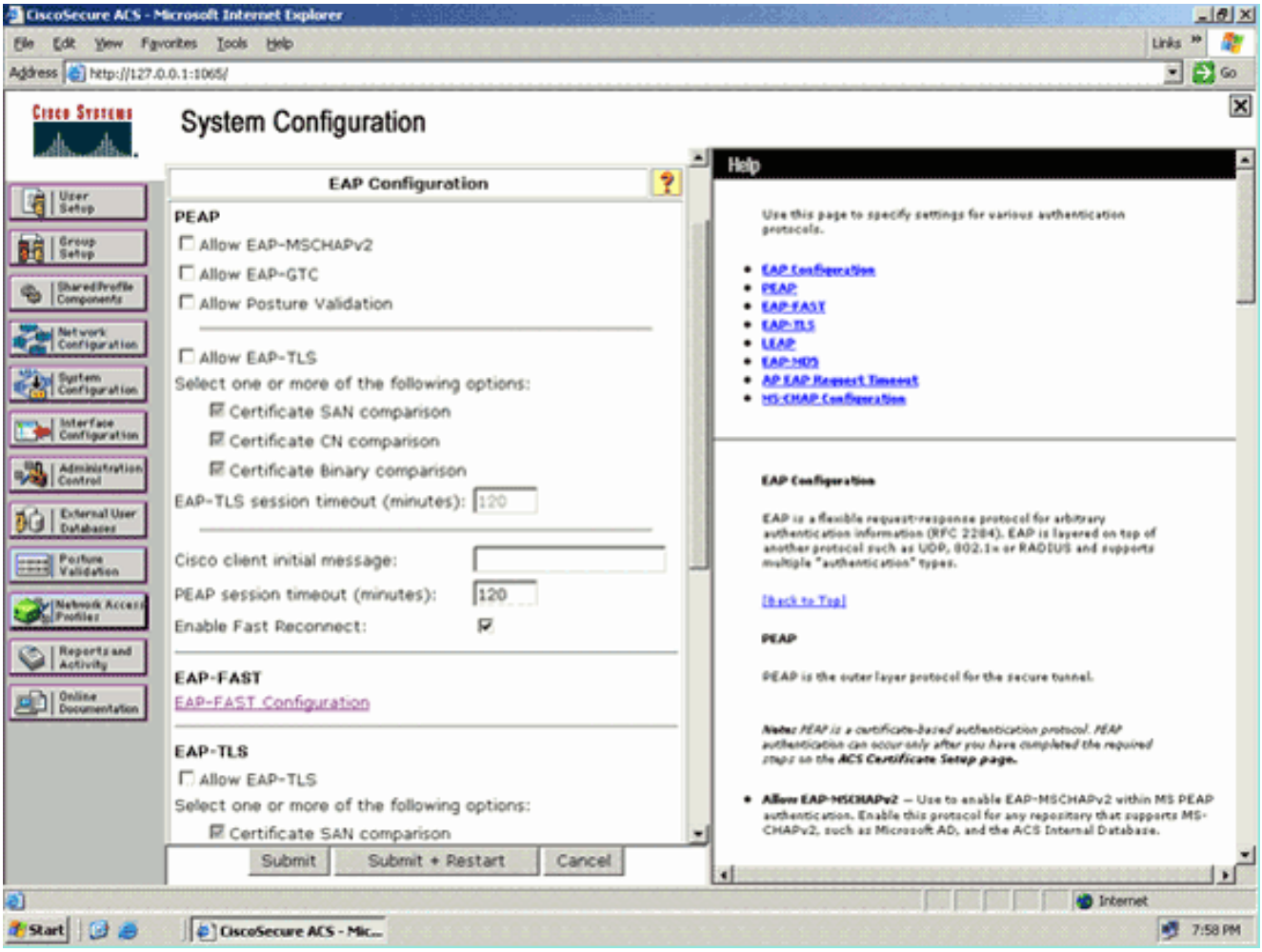
Note: 本文假设，无线局域网控制器被添加到Cisco Secure ACS作为AAA客户端。

完成这些步骤为了配置在RADIUS服务器的EAP-FAST认证：

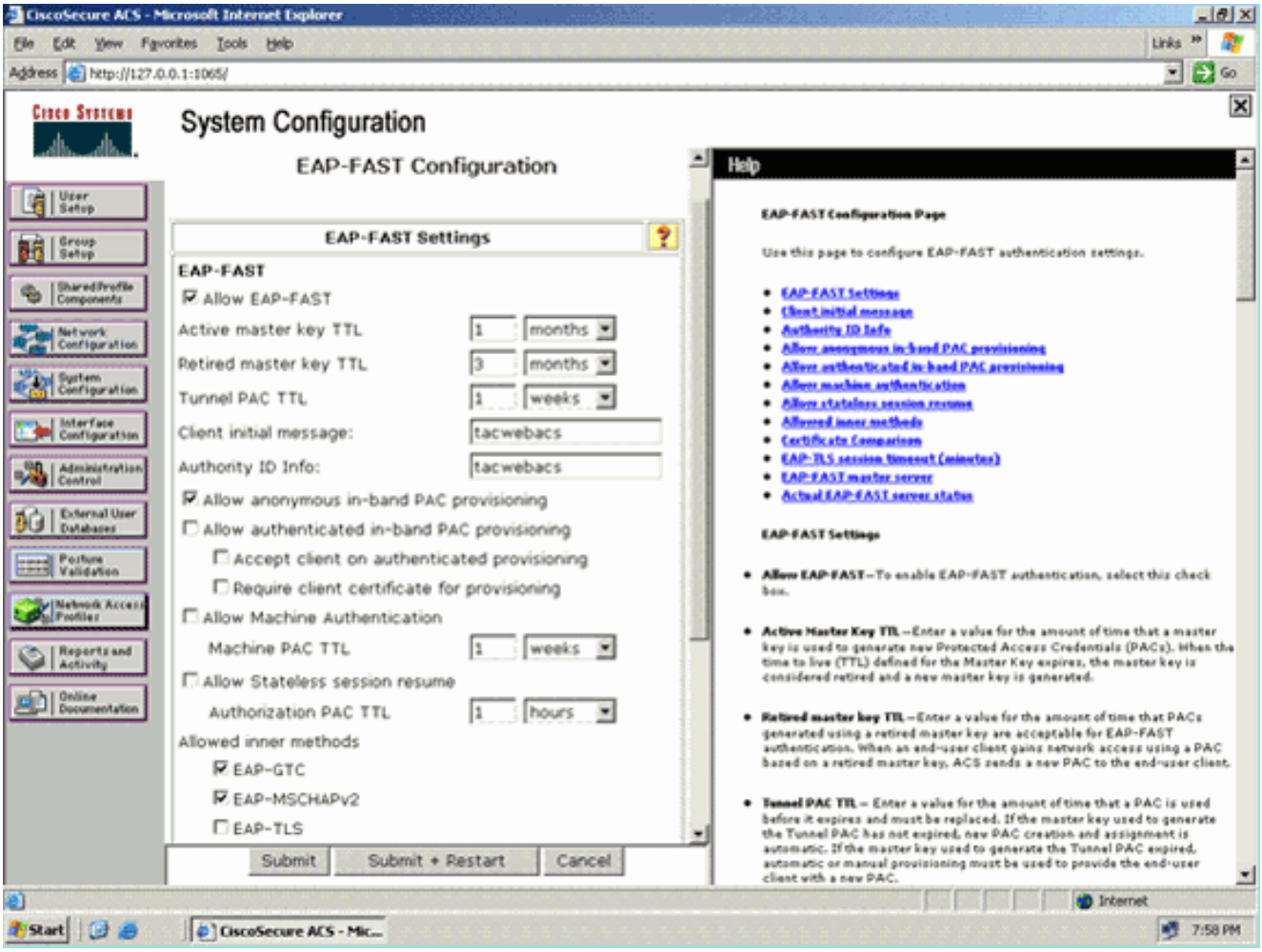
1. 点击从RADIUS服务器GUI的**系统配置**，然后选择从System Configuration Page选择**设置的全局认证。**



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，请检查在RADIUS服务器的**允许EAP-FAST**复选框为了enable (event) EAP-FAST。



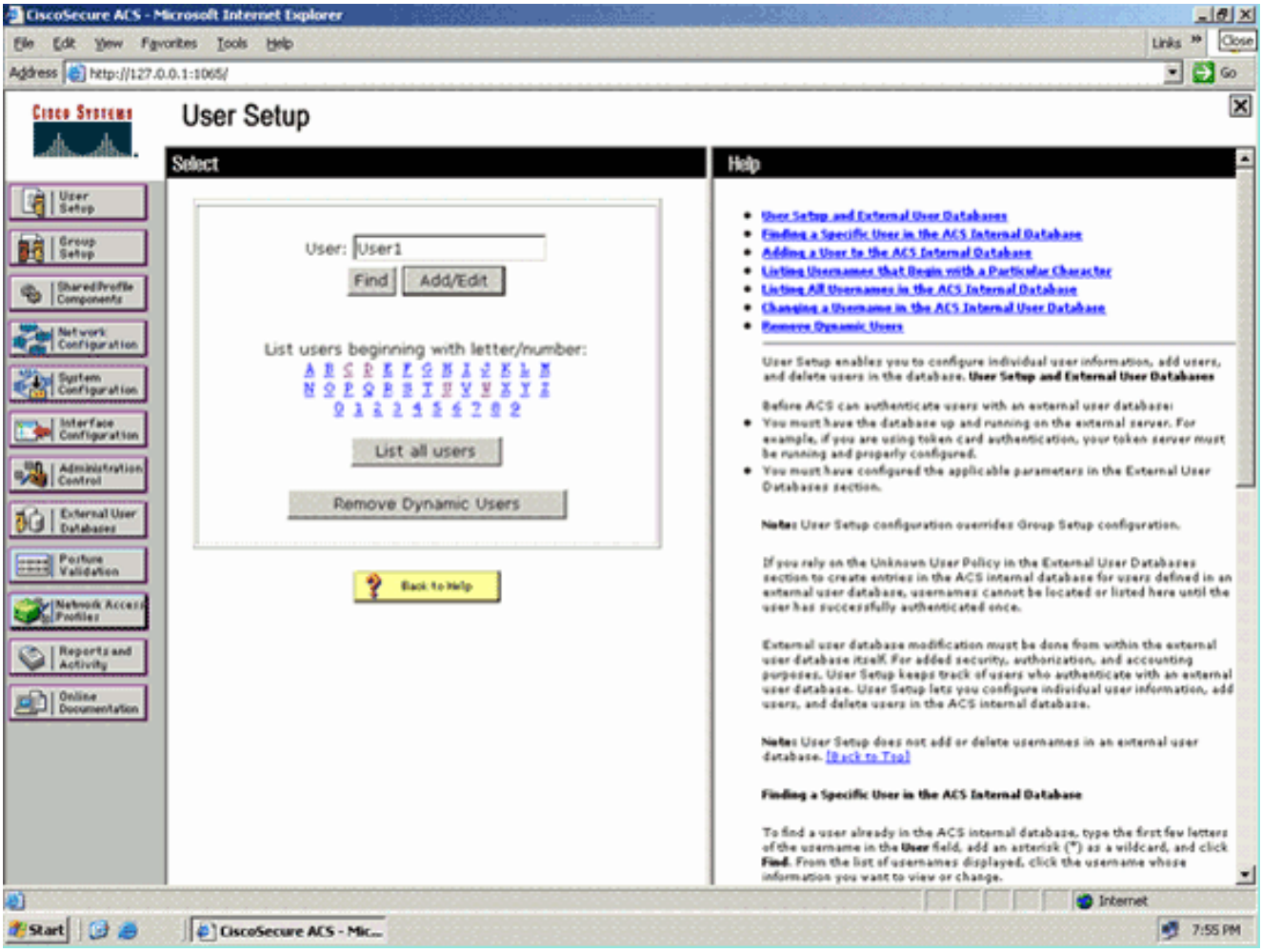
4. 根据需要配置“Active master key TTL”/“Retired master key TTL”（TTL 即存活时间）的值，或按本例所示将其设置为默认值。“Authority ID Info”字段表示此 ACS 服务器的文本身份，最终用户可使用该字段确定要根据哪个 ACS 服务器进行身份验证。必须填写此字段。“Client initial display message”字段用于指定要发送给使用 EAP-FAST 客户端进行身份验证的用户的一条消息。最大长度为 40 个字符。只有最终用户客户端支持显示时，用户才会看到该初始消息。
5. 如果希望 ACS 执行匿名带内 PAC 配置，请选中 **Allow anonymous in-band PAC provisioning** 复选框。
6. *允许的内在方法*选项确定哪些内在EAP方法能运行在EAP-FAST TLS隧道里面。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**。**Note:** 关于详细信息和示例关于如何用匿名在波段之内PAC设置和验证的在波段之内设置快速地配置EAP，请参见EAP-FAST认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

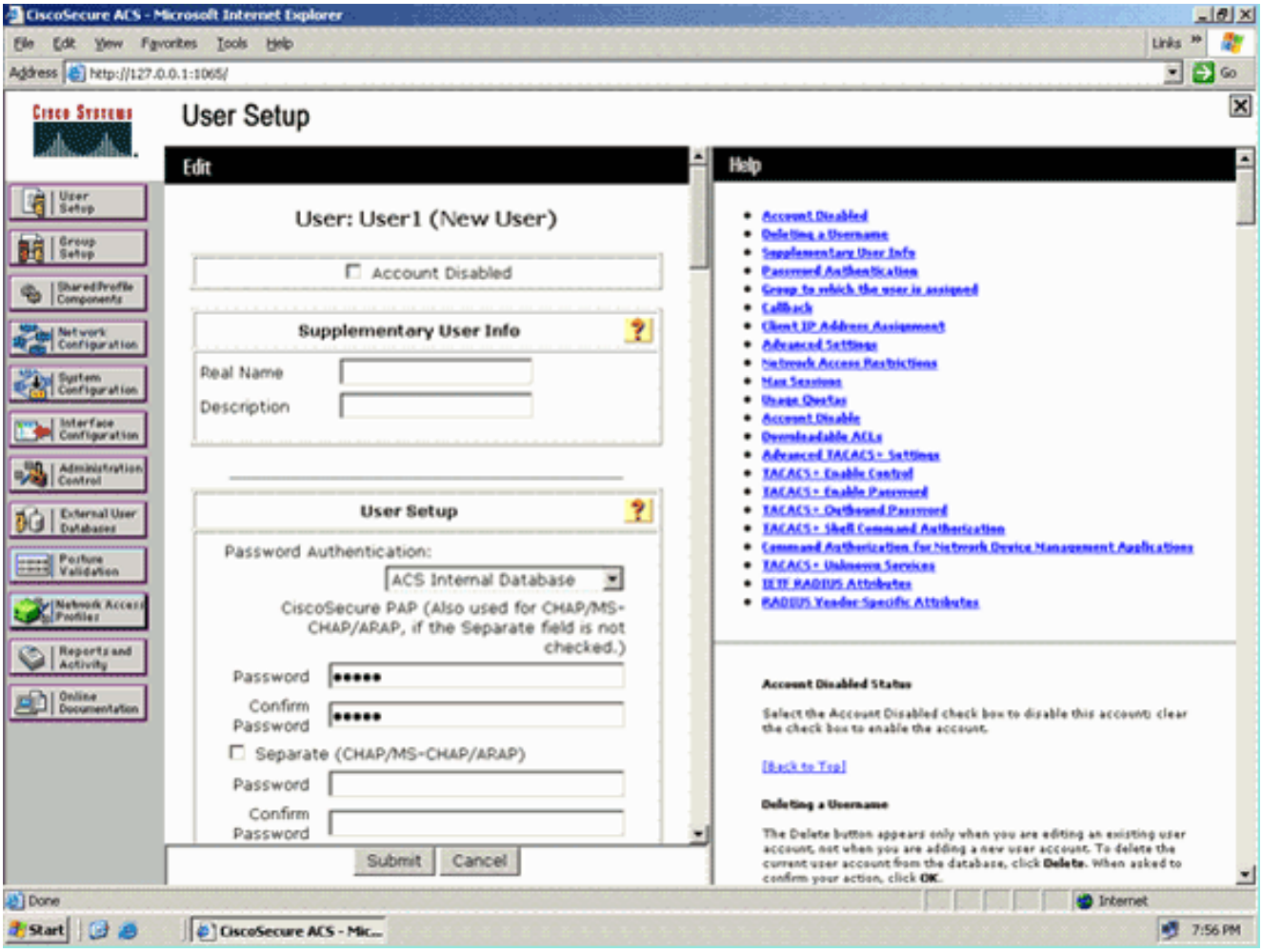
此示例配置无线客户端的用户名和密码作为User1和User1，分别。

完成这些步骤为了创建用户数据库：

1. 从在导航条的ACS GUI，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. 输入此Cisco AV对在[009\001] cisco-av-pair编辑框为了指定用户重定向的URL ：url-redirect=http://10.77.244.196/Admin-Login.html

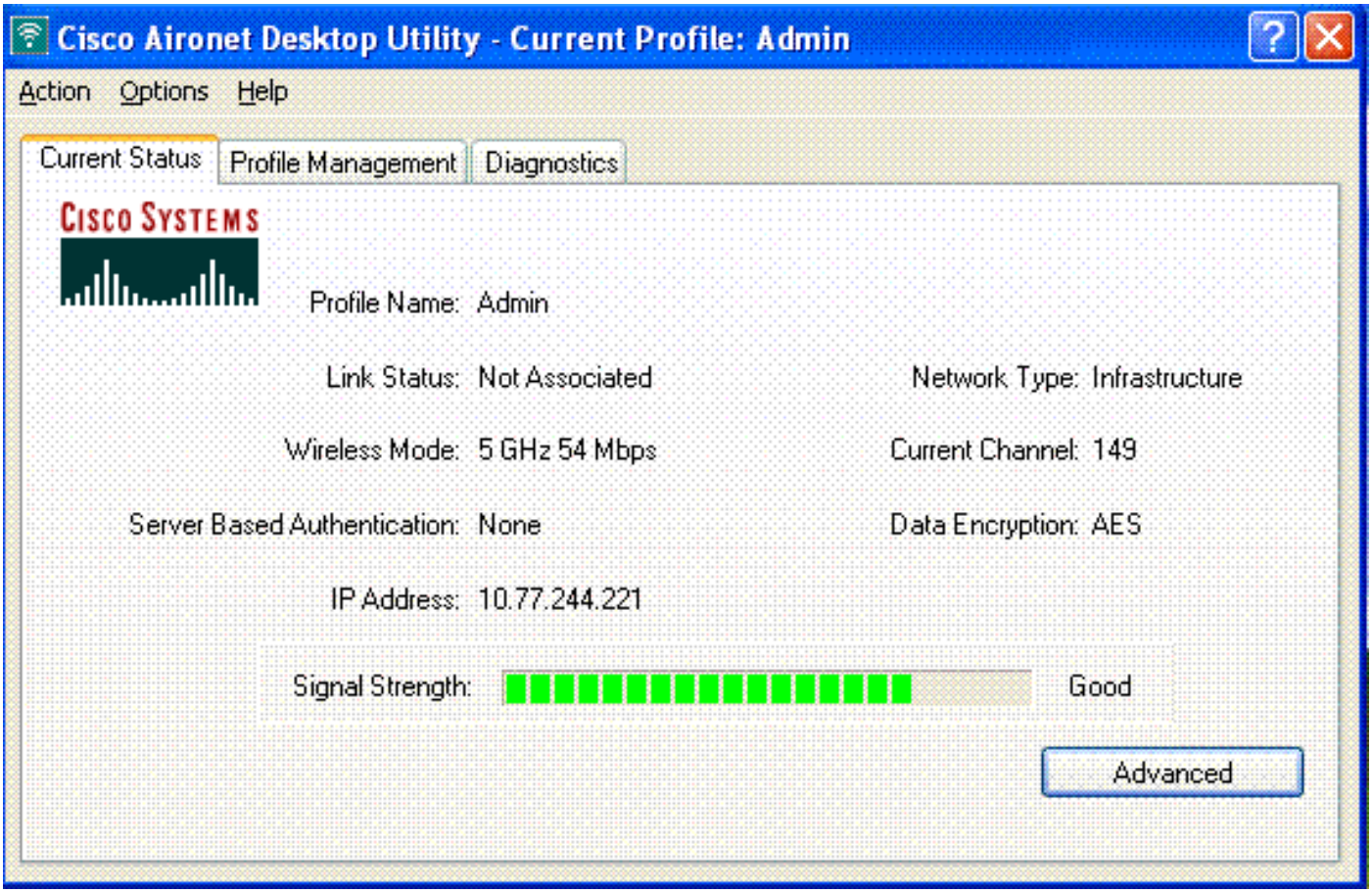
这是Admin部门用户的主页。

7. 单击 **submit**。
8. 重复此程序为了添加User2 (工序部门用户)。
9. 重复第1步至第6步为了添加更多Admin部门用户和工序部门用户到数据库。**Note:** RADIUS属性可以被配置在用户级或社团级别在Cisco Secure ACS。

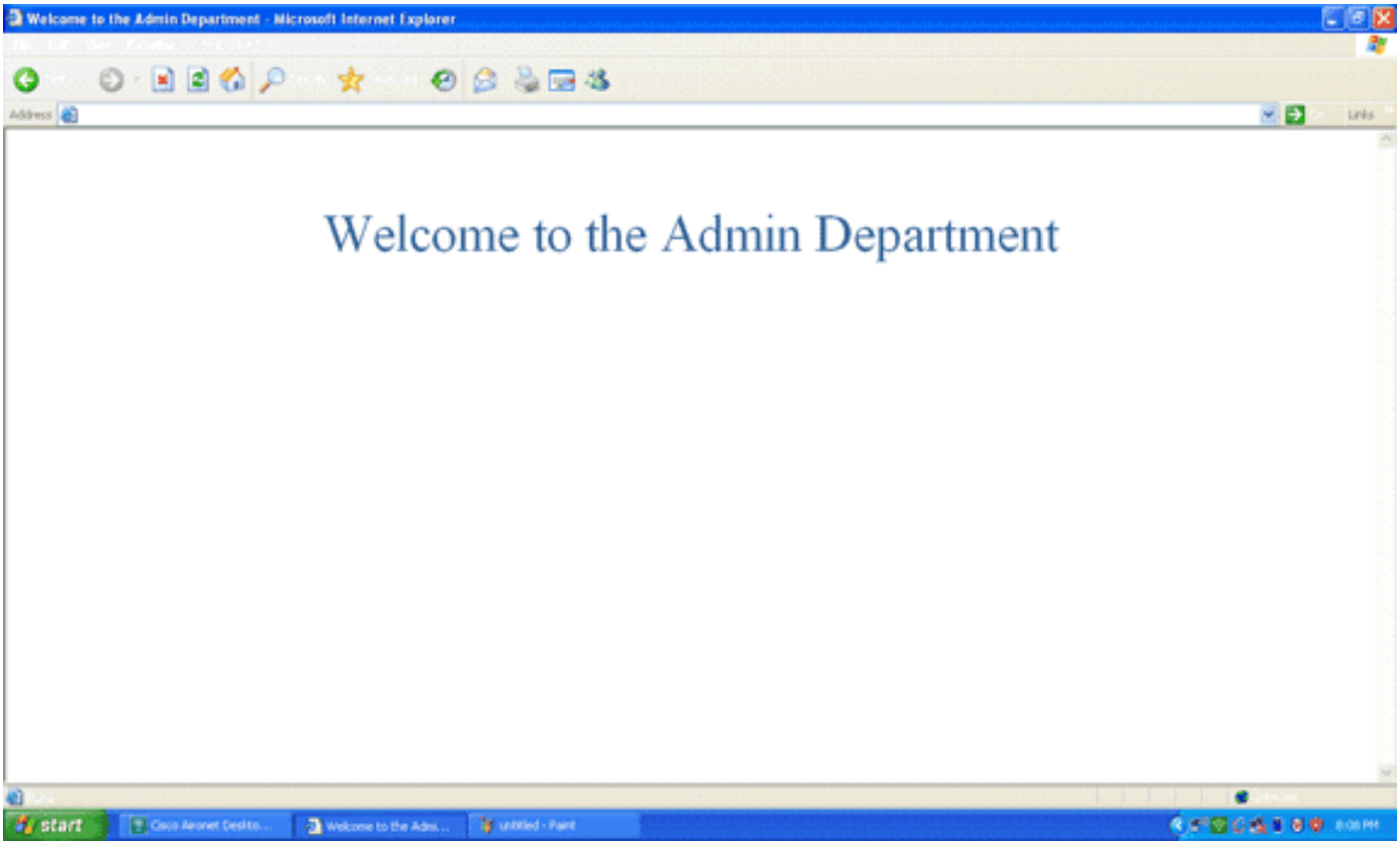
Verify

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

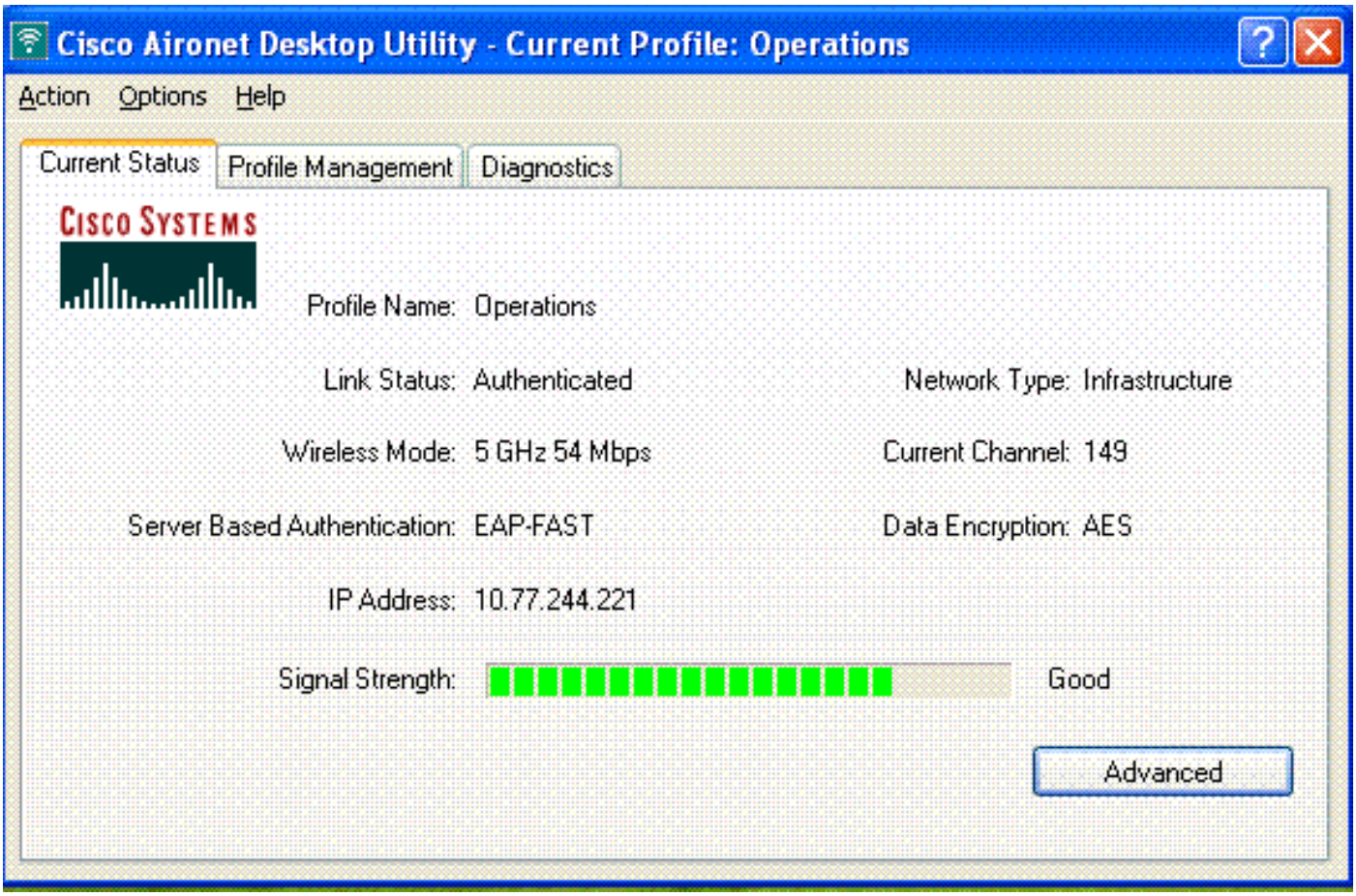
当从Admin部门的一个用户连接到无线局域网Admin时，提示用户输入802.1x证件(在我们的情况的EAP-FAST证件)。一旦用户提供证件， WLC通过那些证件到Cisco Secure ACS服务器。Cisco Secure ACS服务器验证用户凭据数据库和在成功的验证，返回url重新定向属性到无线局域网控制器。认证在此阶段完成。

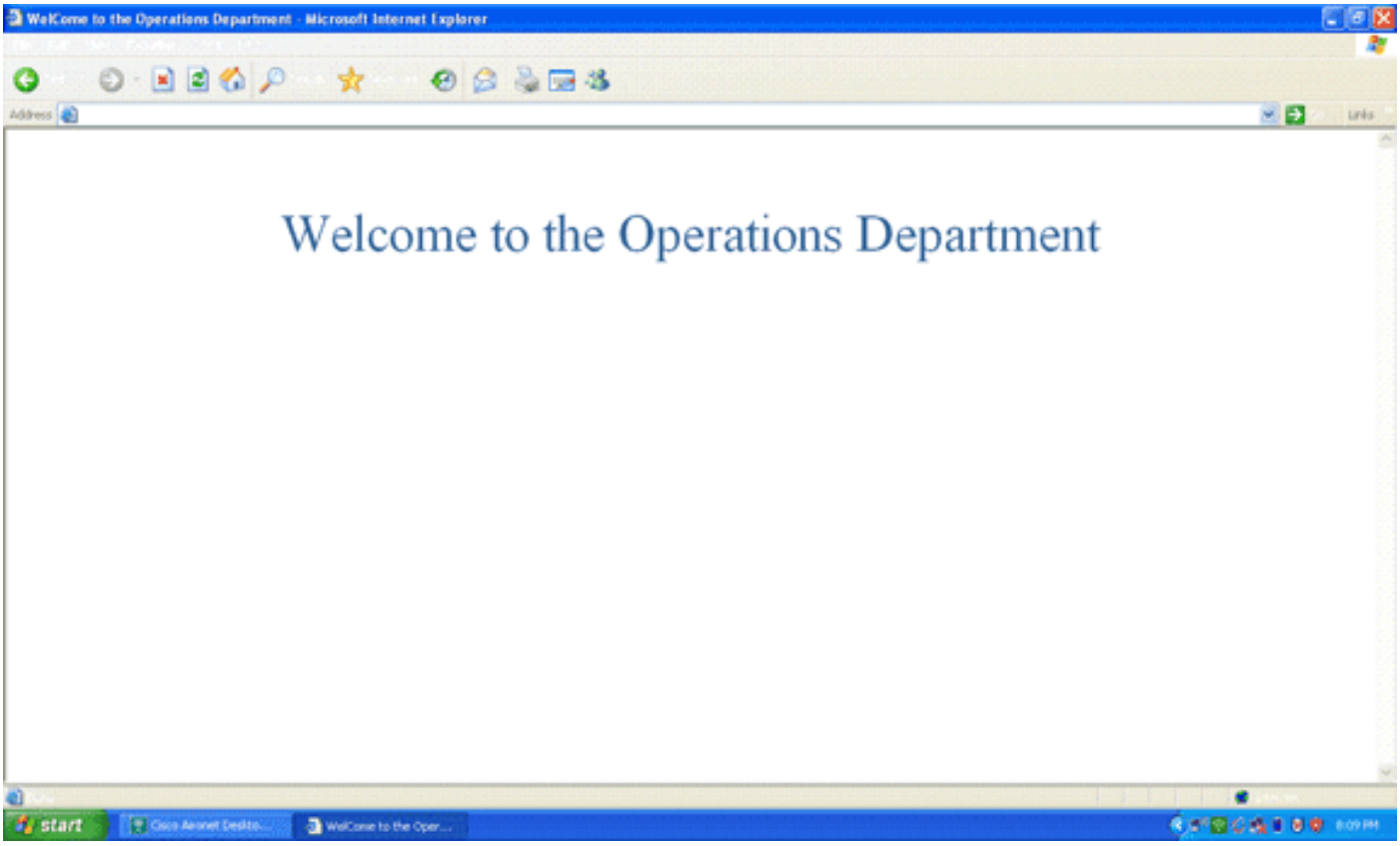


当用户打开Web浏览器时，用户重定向对Admin部门的主页URL。(此URL返回到WLC通过cisco-av-pair属性)。在重定向，用户有全部存取对网络后。这是屏幕画面：



当从工序部门的一个用户连接到WLAN操作，同样事件顺序出现。





Troubleshoot

本部分提供的信息可用于对配置进行故障排除。

Note: 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您的配置故障。

- **显示WLAN wlan_id** —显示Web重定向功能的状况一特定的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)** — Enable (event) 802.1x信息包消息调试。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)** — Enable (event)所有aaa事件的调试输出。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: '
```

Related Information

- 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
- Technical Support & Documentation - Cisco Systems