无线局域网控制器Splash页重定向配置示例

目录

简介

本文档介绍如何在无线LAN控制器上配置启动页重定向功能。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 了解LWAPP安全解决方案
- 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：

- 运行固件版本5.0的Cisco 4400系列无线局域网控制器(WLC)
- 思科1232系列轻型接入点(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

启动页Web重定向是无线LAN控制器5.0版引入的一项功能。通过此功能，用户在802.1x身份验证完成后被重定向到特定网页。当用户打开浏览器（使用默认主页配置）或尝试访问URL时，会发生重定向。完成重定向到网页后，用户即可完全访问网络。

您可以在远程身份验证拨入用户服务(RADIUS)服务器上指定重定向页面。RADIUS服务器应配置为在802.1x身份验证成功后将思科av-pair url-redirect RADIUS属性返回到无线LAN控制器。

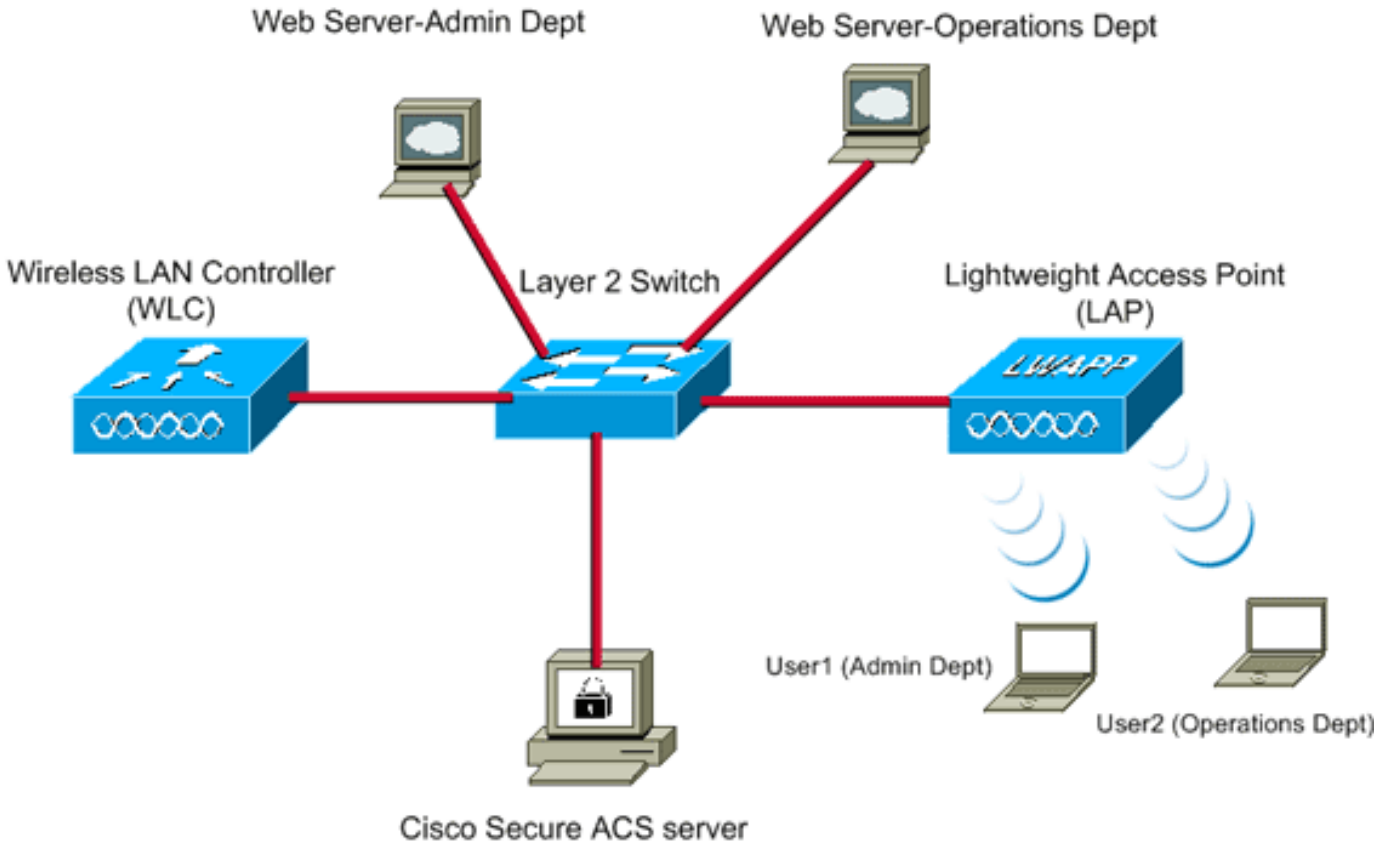
启动页Web重定向功能仅适用于为802.1x或WPA/WPA2第2层安全配置的WLAN。

网络设置

在本示例中，Cisco 4404 WLC和Cisco 1232系列LAP通过第2层交换机连接。Cisco Secure ACS服务器（充当外部RADIUS服务器）也连接到同一台交换机。所有设备都在同一个子网中。

LAP最初注册到控制器。您必须创建两个WLAN：一个用于**管理部**用户，另一个用于**运营部**用户。两个无线LAN都使用WPA2/AES（EAP-FAST用于身份验证）。两个WLAN都使用启动页重定向功能将用户重定向到相应的主页URL（在外部Web服务器上）。

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：要获取此部分中所用命令的更多信息，可使用命令查找工具（仅限已注册客户）。

要配置设备以使用启动页重定向功能，请完成以下步骤：

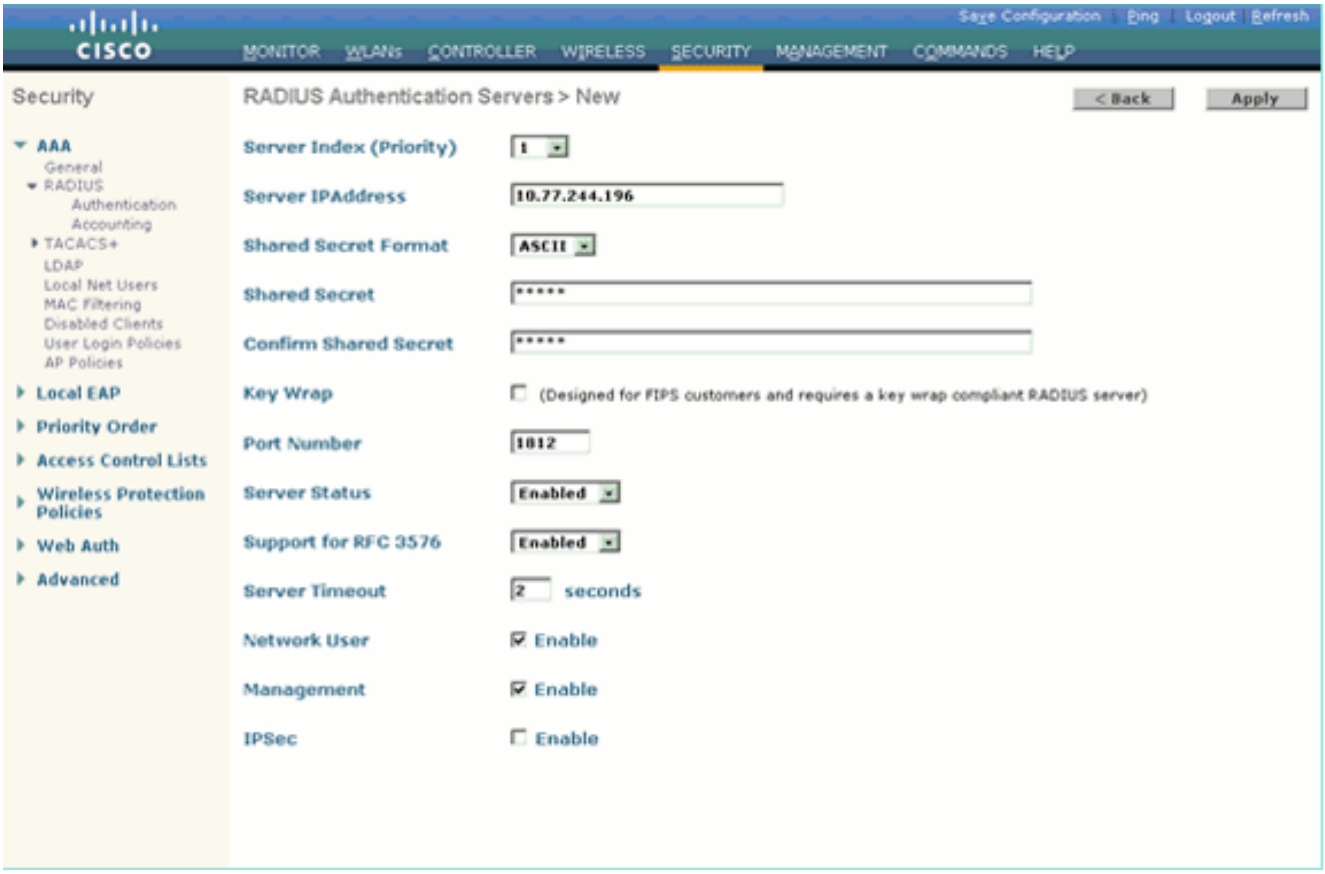
1. 通过Cisco Secure ACS服务器配置WLC进行RADIUS身份验证。
2. 为管理部门和运营部门配置WLAN。
3. 配置Cisco Secure ACS以支持启动页重定向功能。

步骤1:通过Cisco Secure ACS服务器配置WLC进行RADIUS身份验证。

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中选择**Security**和**RADIUS Authentication**以显示“RADIUS Authentication Servers”页。
2. 单击**New**以定义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 地址共享密钥端口号服务器状态



本文使用IP地址为10.77.244.196的ACS服务器。

4. 单击 **Apply**。

第二步：为管理和运营部门配置WLAN。

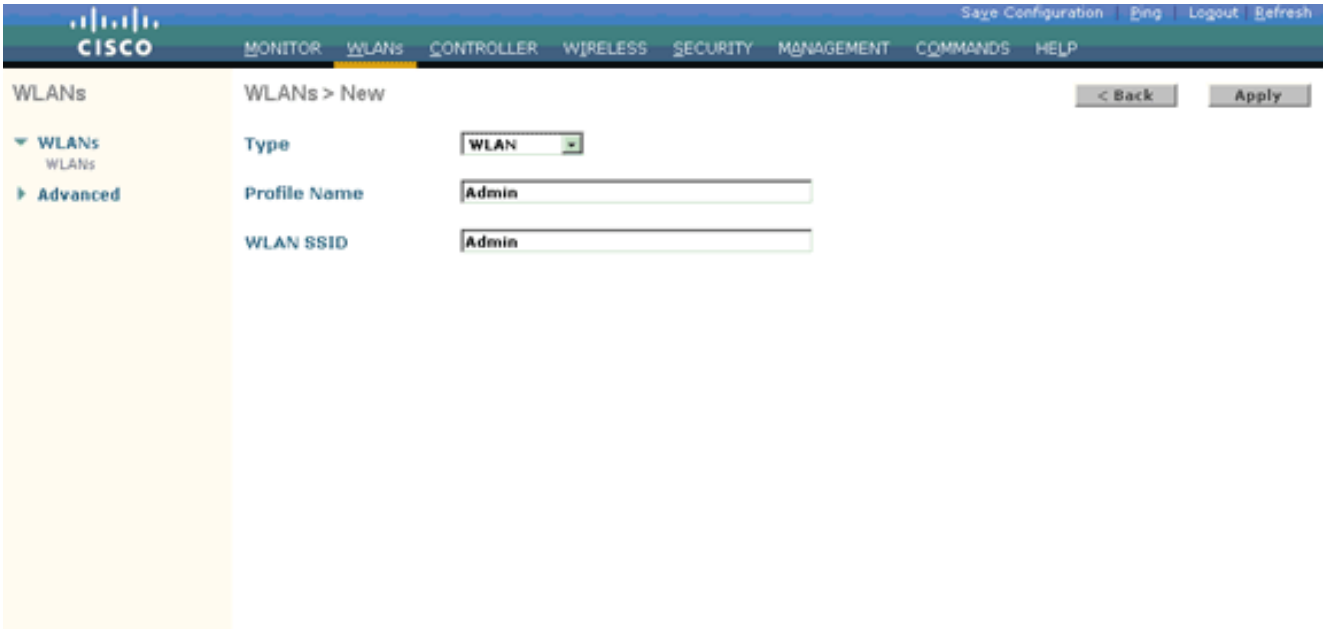
在此步骤中，您将配置客户端用于连接无线网络的两个WLAN（一个用于管理部门，另一个用于运营部门）。

管理部门的WLAN SSID将是*Admin*。运营部门的WLAN SSID为运营。

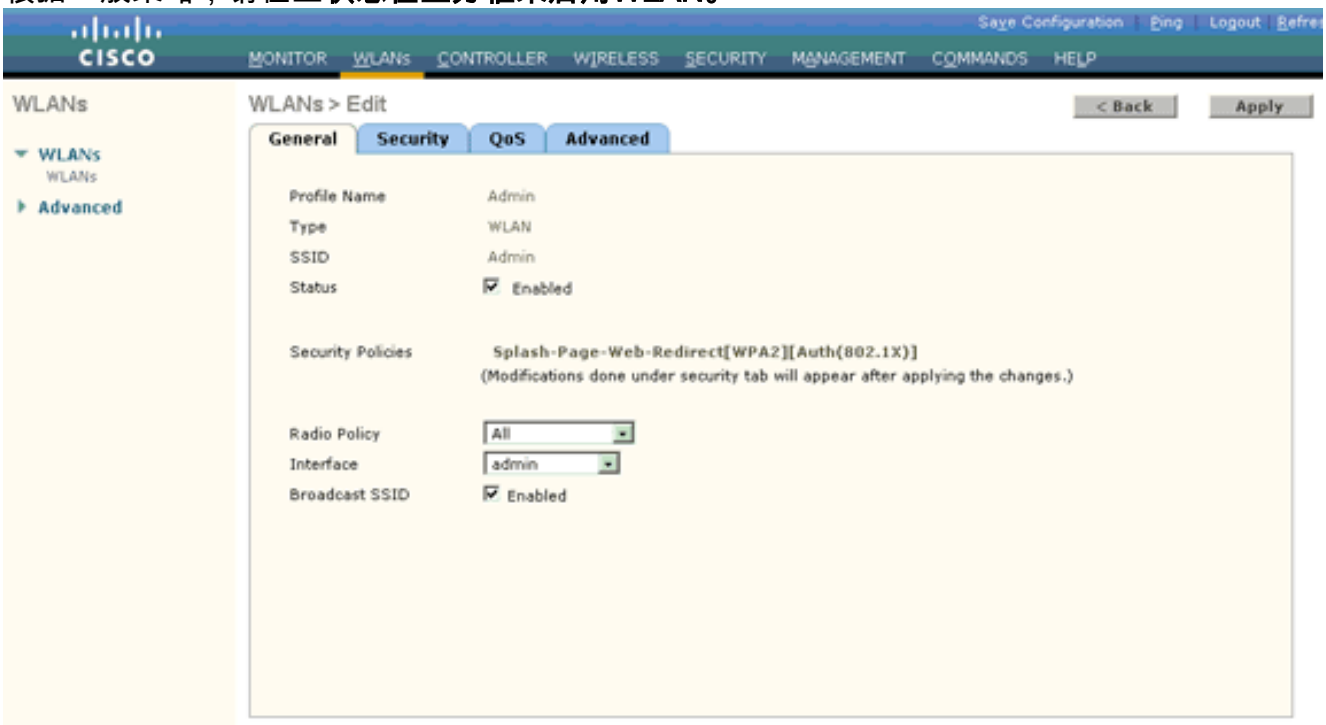
使用EAP-FAST身份验证以启用WPA2作为WLAN上的第2层安全机制，并使用Web策略 — 启动页Web重定向功能作为第3层安全方法。

若要配置 WLAN 及其相关参数，请完成下列步骤：

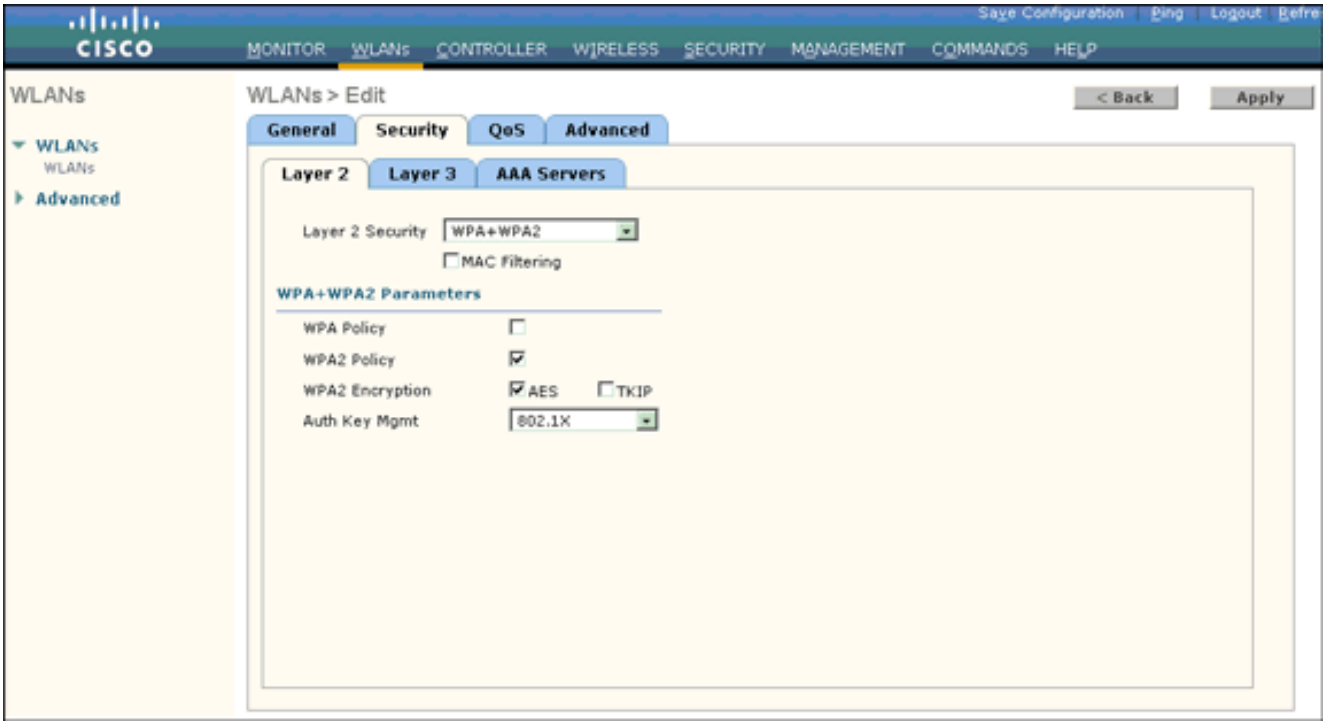
1. 从控制器的 GUI 中单击 **WLAN 以显示“WLAN”页。**此页列出了控制器上现有的 WLAN。
2. 单击 **New 以创建新的 WLAN。**



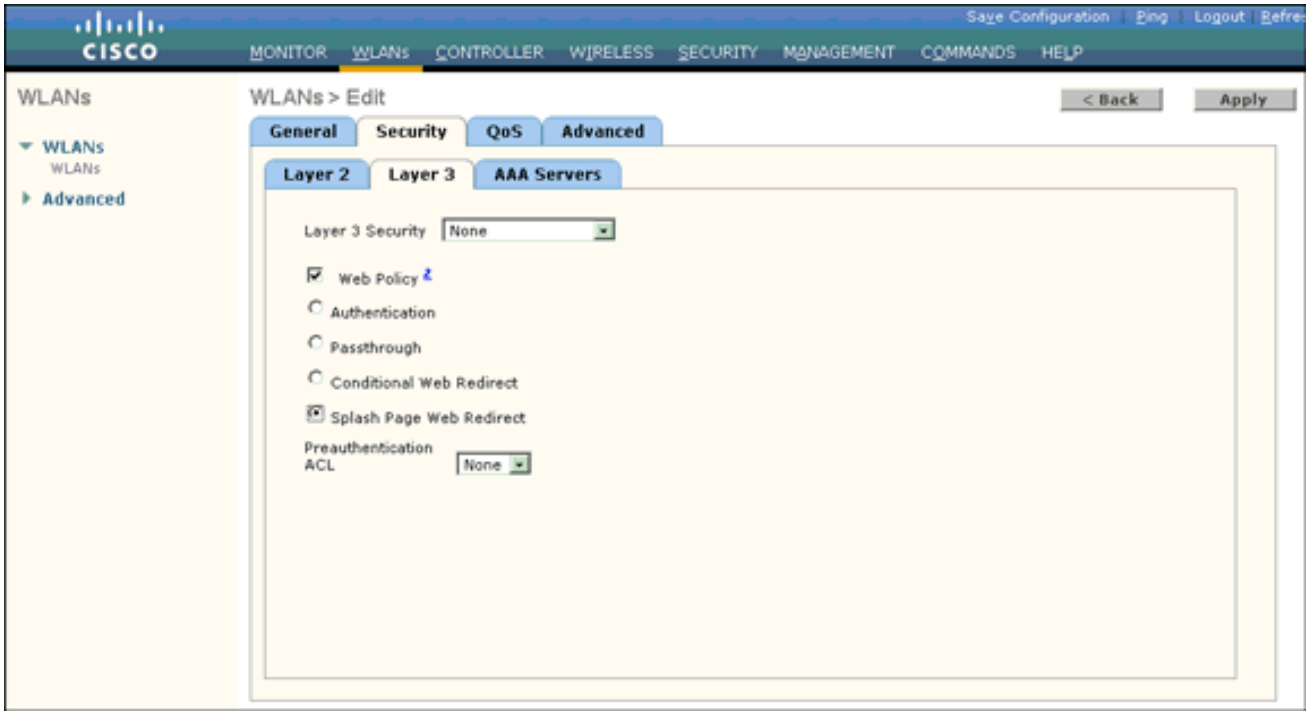
3. 在WLANs > New页面上输入WLAN SSID名称和配置文件名称。
4. 单击 **Apply**。
5. 首先，让我们为管理部门创建WLAN。创建新 WLAN 后，就会显示新 WLAN 的 WLAN > Edit 页。在此页上，可以定义特定于此 WLAN 的各种参数。这包括常规策略、安全策略、QOS策略和高级参数。
6. 根据一般策略，请检查**状态检查方框来启用WLAN。**



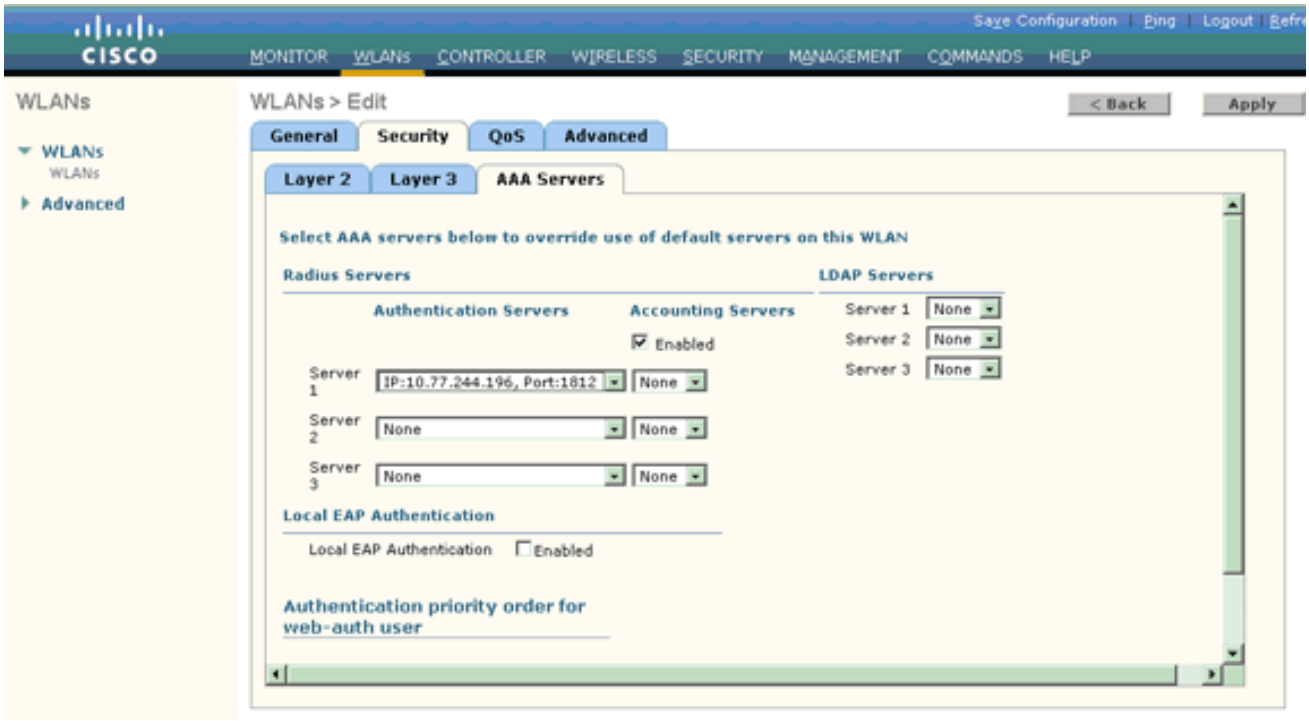
7. 单击**Security**选项卡，然后单击**Layer 2**选项卡。
8. 从Layer 2 Security下拉列表中选择**WPA+WPA2**。此步骤为WLAN启用WPA身份验证。
9. 在WPA+WPA2参数下，选中**WPA2 Policy**和**AES Encryption**复选框。



10. 从Auth Key Mgmt下拉列表中选择**802.1x**。此选项为WLAN启用具有802.1x/EAP身份验证和AES加密的WPA2。
11. 单击**Layer 3 Security**选项卡。
12. 选中**Web Policy**框，然后单击**Splash Page Web Redirect**单选按钮。此选项启用启动页Web重定向功能。



13. 单击 **AAA Servers 选项卡。**
14. 在Authentication Servers下，从Server 1下拉列表中选择适当的服务器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步到第15步，为运营部门创建WLAN。WLAN页面列出您创建的两个WLAN。

请注意，安全策略包括启动页重定向。

第三步：配置Cisco Secure ACS以支持启动页重定向功能。

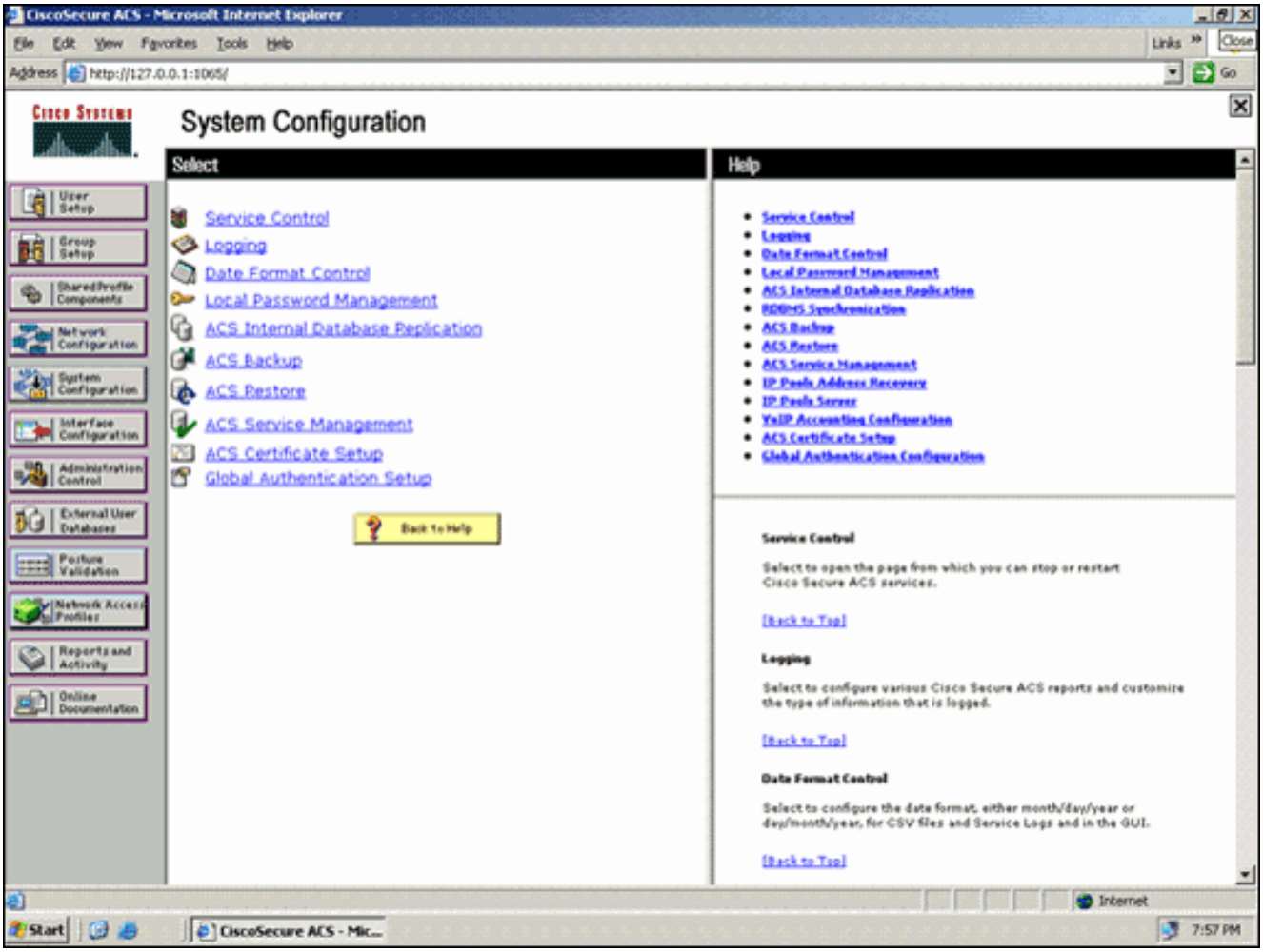
下一步是为此功能配置RADIUS服务器。RADIUS服务器需要执行EAP-FAST身份验证以验证客户端凭证，并在身份验证成功后，将用户重定向到Cisco av-pair ***url-redirect RADIUS属性中指定的*** URL（在外部Web服务器上）。

配置Cisco Secure ACS进行EAP-FAST身份验证

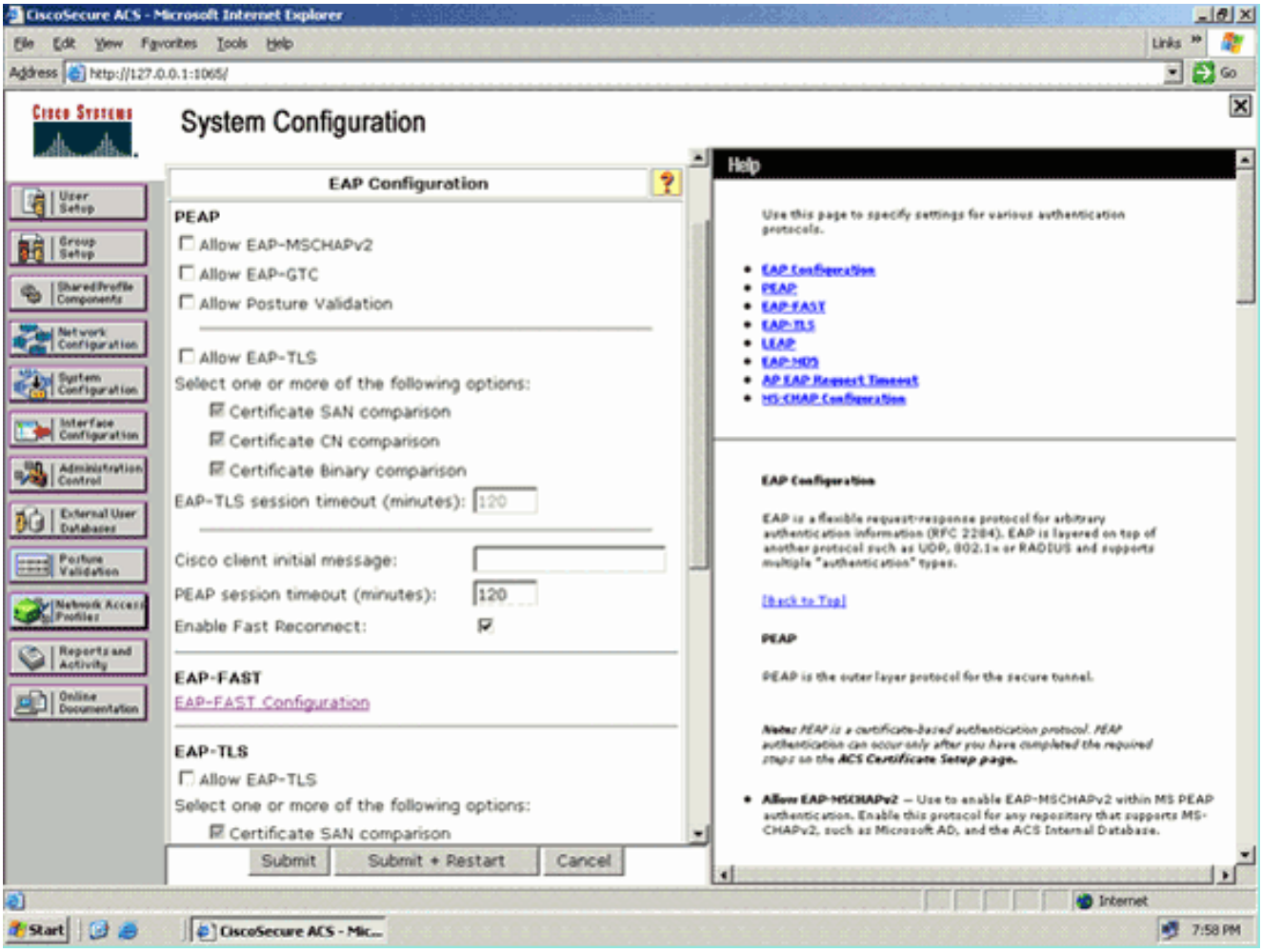
注意：本文档假设无线局域网控制器作为AAA客户端添加到Cisco Secure ACS。

要在RADIUS服务器中配置EAP-FAST身份验证，请完成以下步骤：

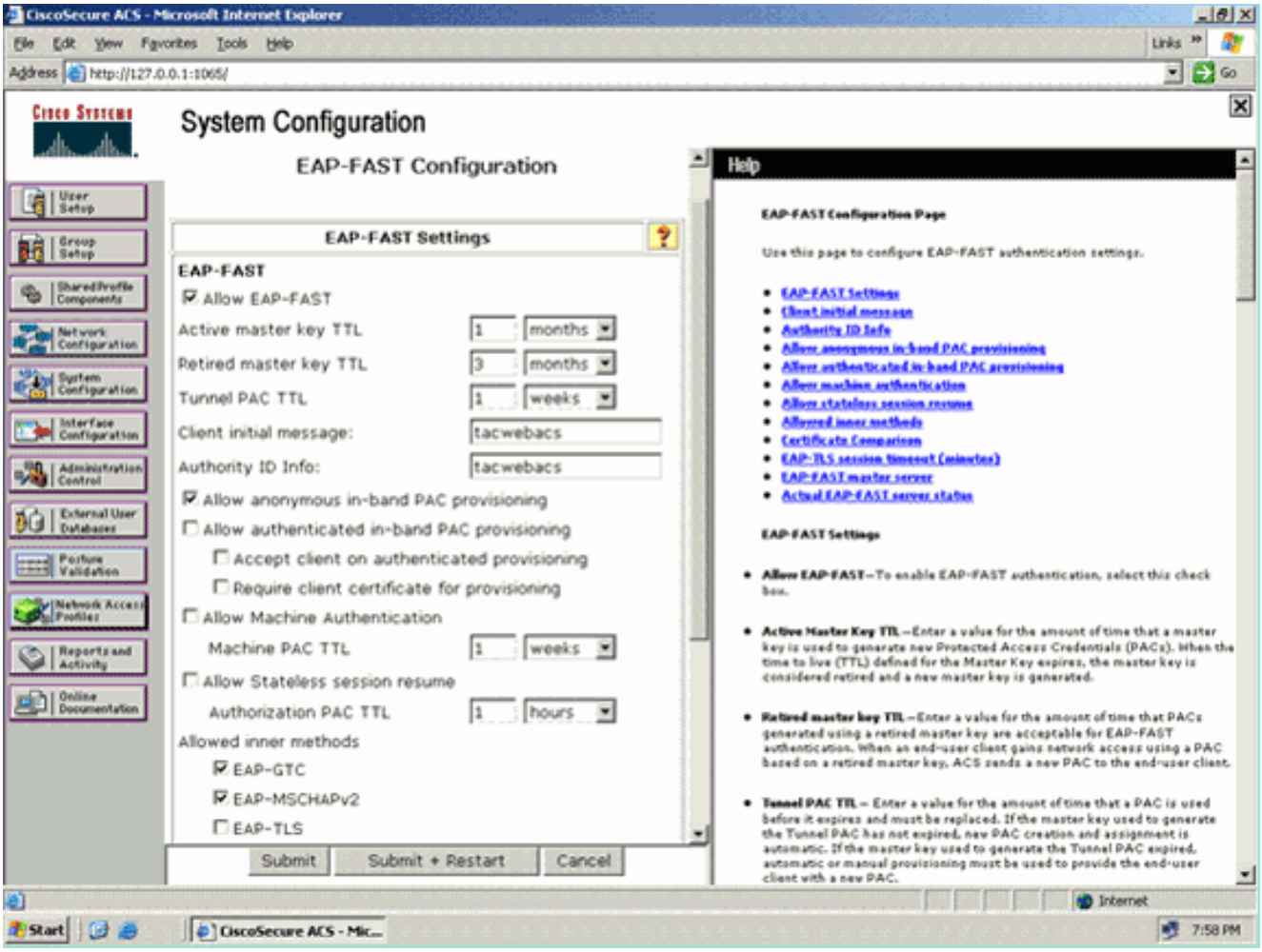
1. 在RADIUS服务器GUI中单击**System Configuration**，然后从System Configuration页面选择**Global Authentication Setup**。



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



3. 在EAP-FAST Settings页面中，选中**Allow EAP-FAST**复选框以便在RADIUS服务器中启用EAP-FAST。



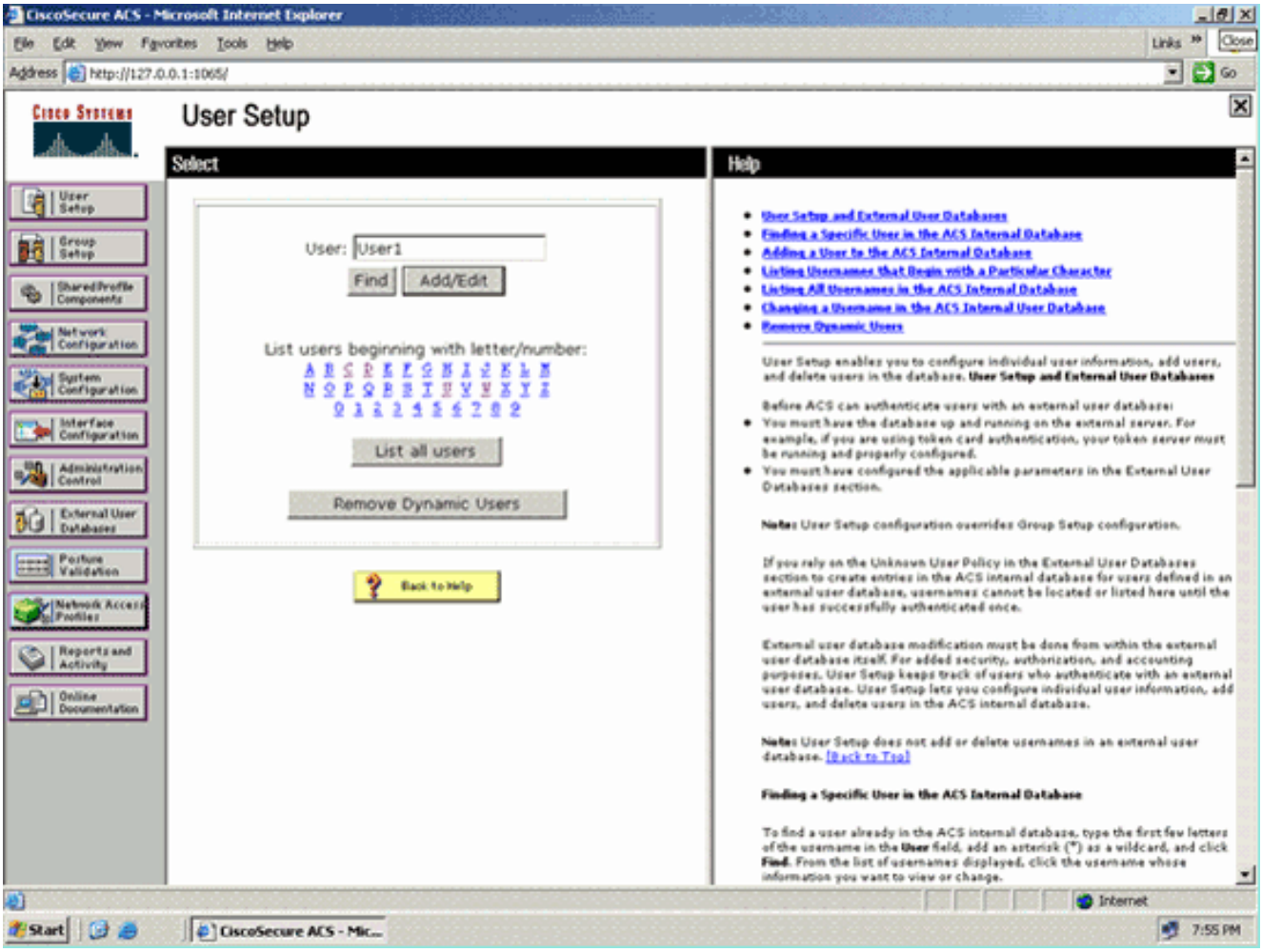
4. 根据需要配置“Active master key TTL”/“Retired master key TTL”（TTL 即存活时间）的值，或按本例所示将其设置为默认值。“Authority ID Info”字段表示此 ACS 服务器的文本身份，最终用户可使用该字段确定要根据哪个 ACS 服务器进行身份验证。必须填写此字段。“Client initial display message”字段用于指定要发送给使用 EAP-FAST 客户端进行身份验证的用户的一条消息。最大长度为 40 个字符。只有最终用户客户端支持显示时，用户才会看到该初始消息。
5. 如果希望 ACS 执行匿名带内 PAC 配置，请选中 **Allow anonymous in-band PAC provisioning 复选框。**
6. *Allowed inner methods*选项确定哪些内部EAP方法可以在EAP-FAST TLS隧道内运行。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：有关如何使用匿名带内PAC调配和经过身份验证的带内调配配置**EAP FAST的详细信息和示例，请参阅使用无线LAN控制器和外部RADIUS服务器配置EAP-FAST身份验证的示例。

配置用户数据库并定义*url-redirect* RADIUS属性

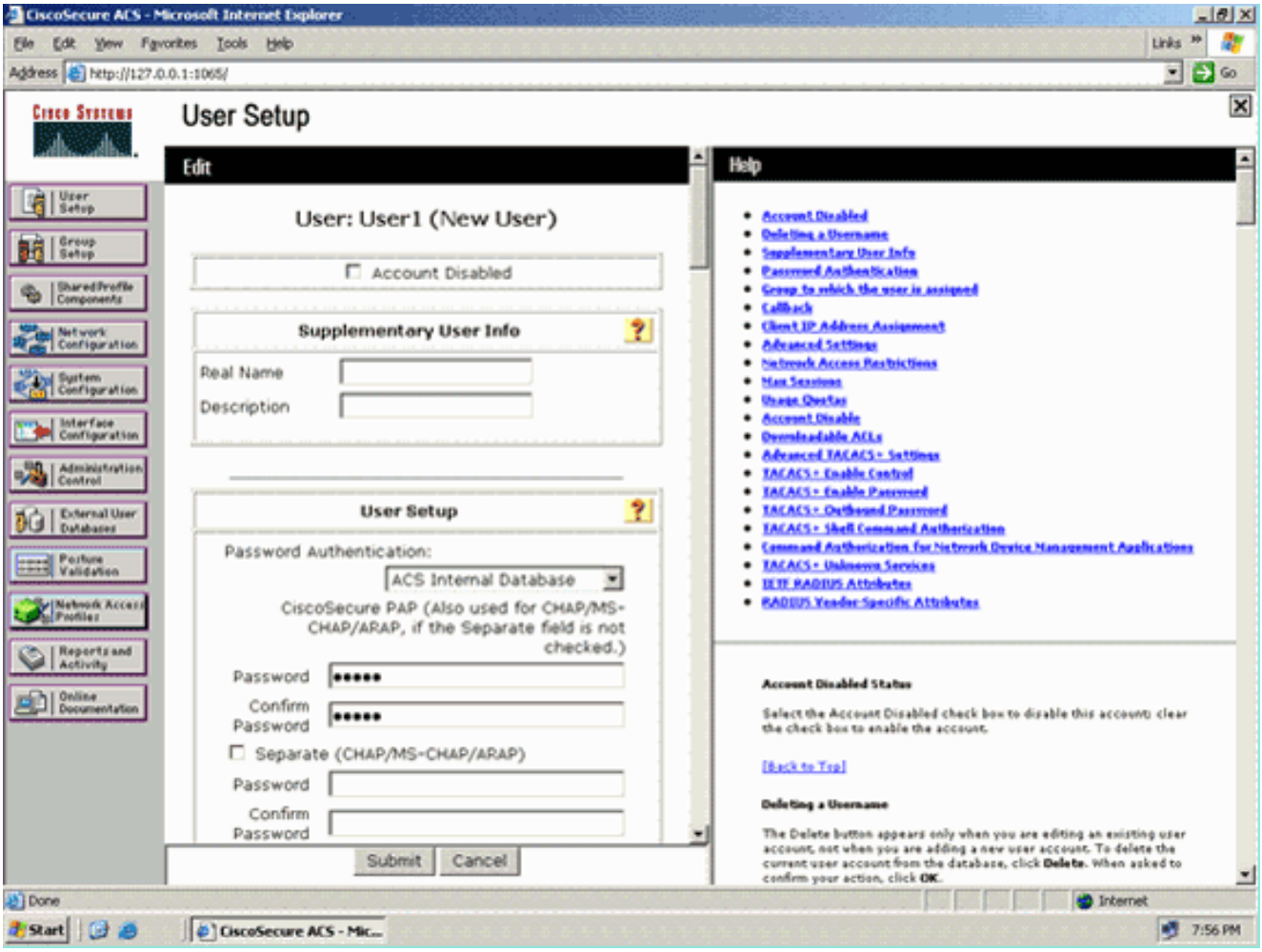
此示例将无线客户端的用户名和密码分别配置为User1和User1。

要创建用户数据库，请完成以下步骤：

1. 从导航栏中的ACS GUI中选择**User Setup**。
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. 在User Setup Edit页面中，配置真实名称和说明以及密码设置，如本示例所示。本文档使用ACS Internal Database 作为“Password Authentication”。



4. 向下滚动页面以修改RADIUS属性。
5. 选中**[009\001] cisco-av-pair**复选框。
6. 在[009\001] cisco-av-pair编辑框中输入此Cisco av-pair以指定用户重定向到的URL:url-redirect=http://10.77.244.196/Admin-Login.html

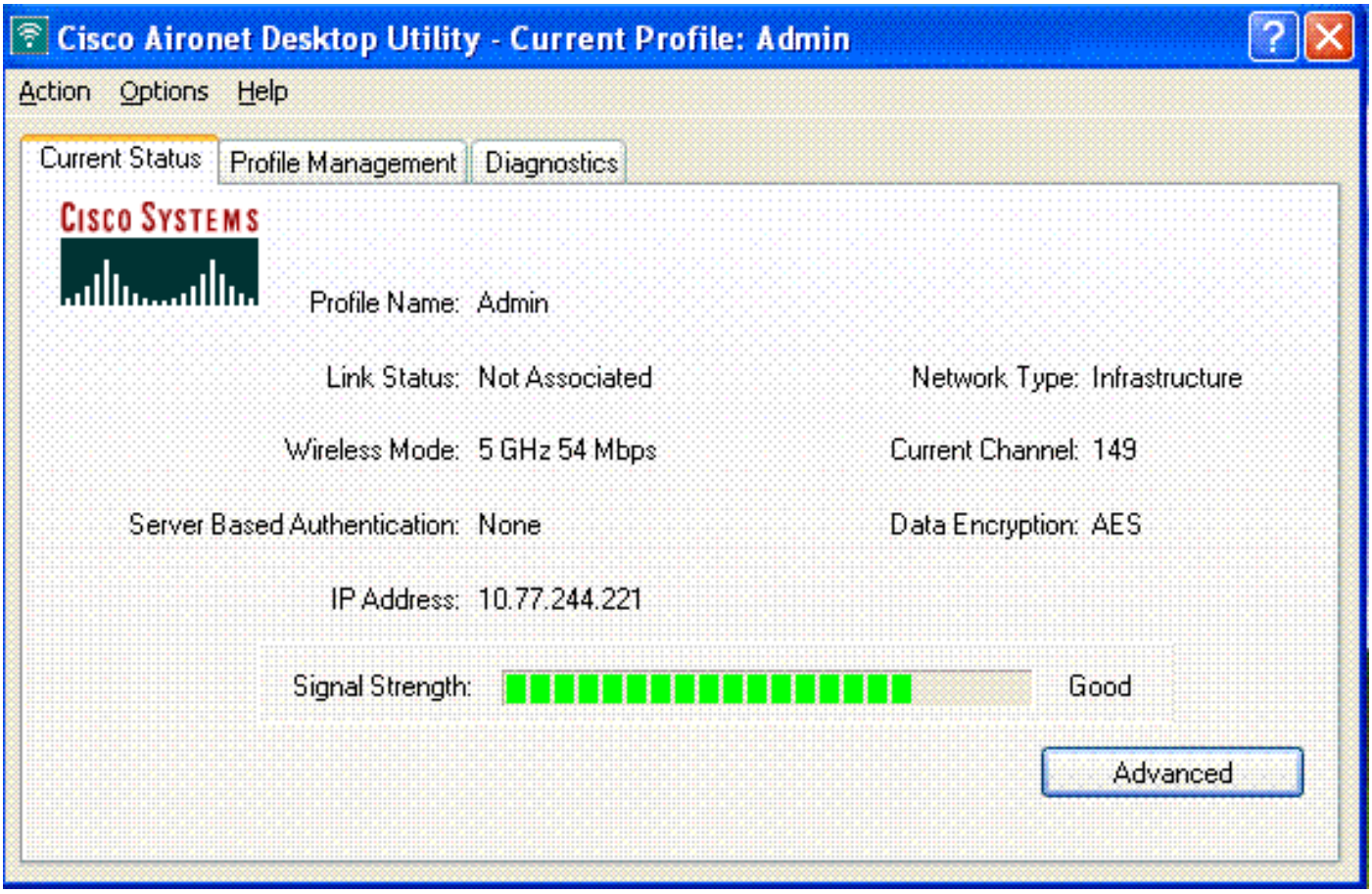
这是管理部门用户的主页。

7. 单击“Submit”。
8. 重复此过程以添加User2（运营部门用户）。
9. 重复第1步到第6步，以便将更多管理员部门用户和运营部门用户添加到数据库。**注意**：RADIUS属性可以在思科安全ACS上的用户级别或组级别进行配置。

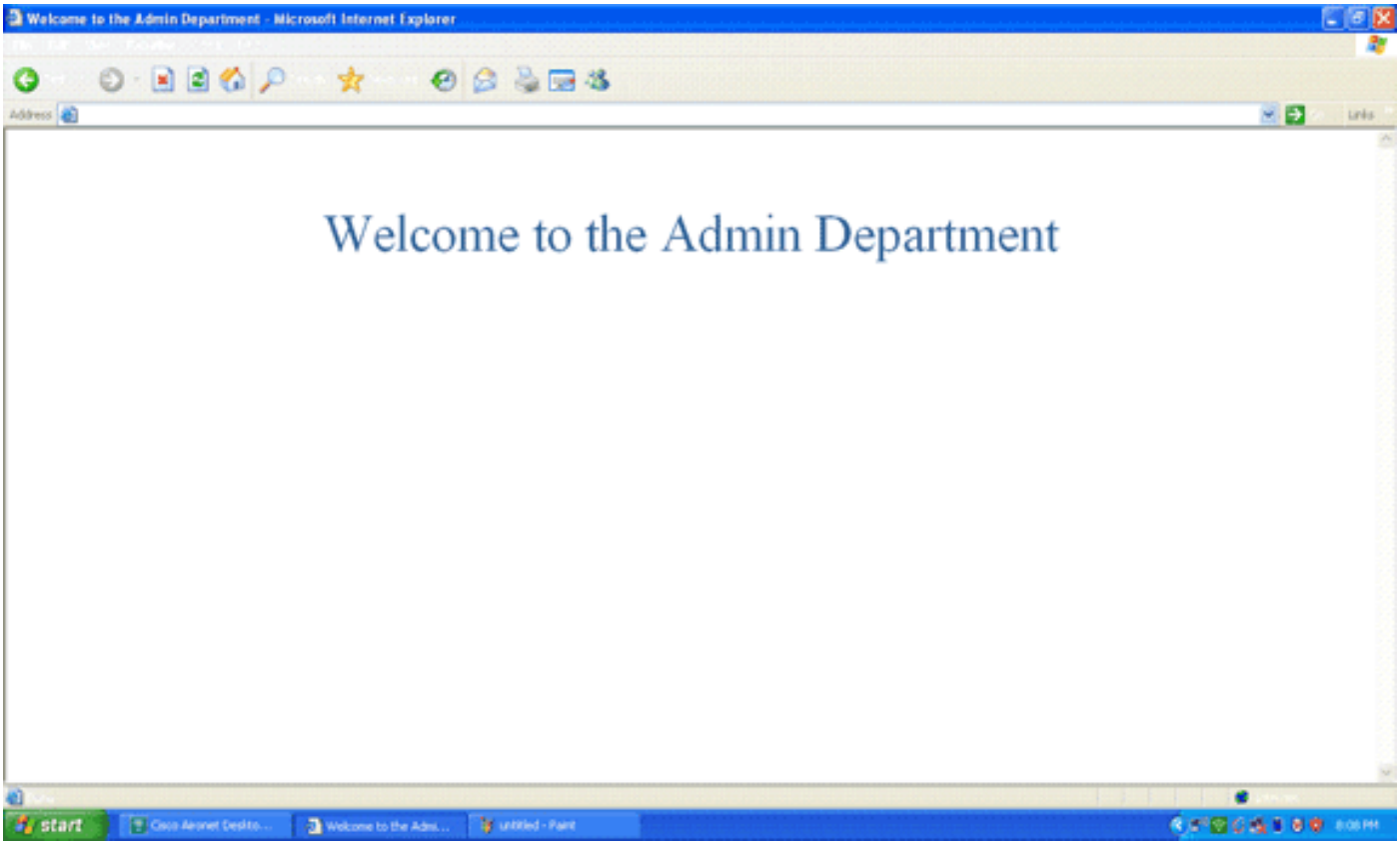
验证

要验证配置，请将管理部门和运营部门的WLAN客户端与其相应的WLAN关联。

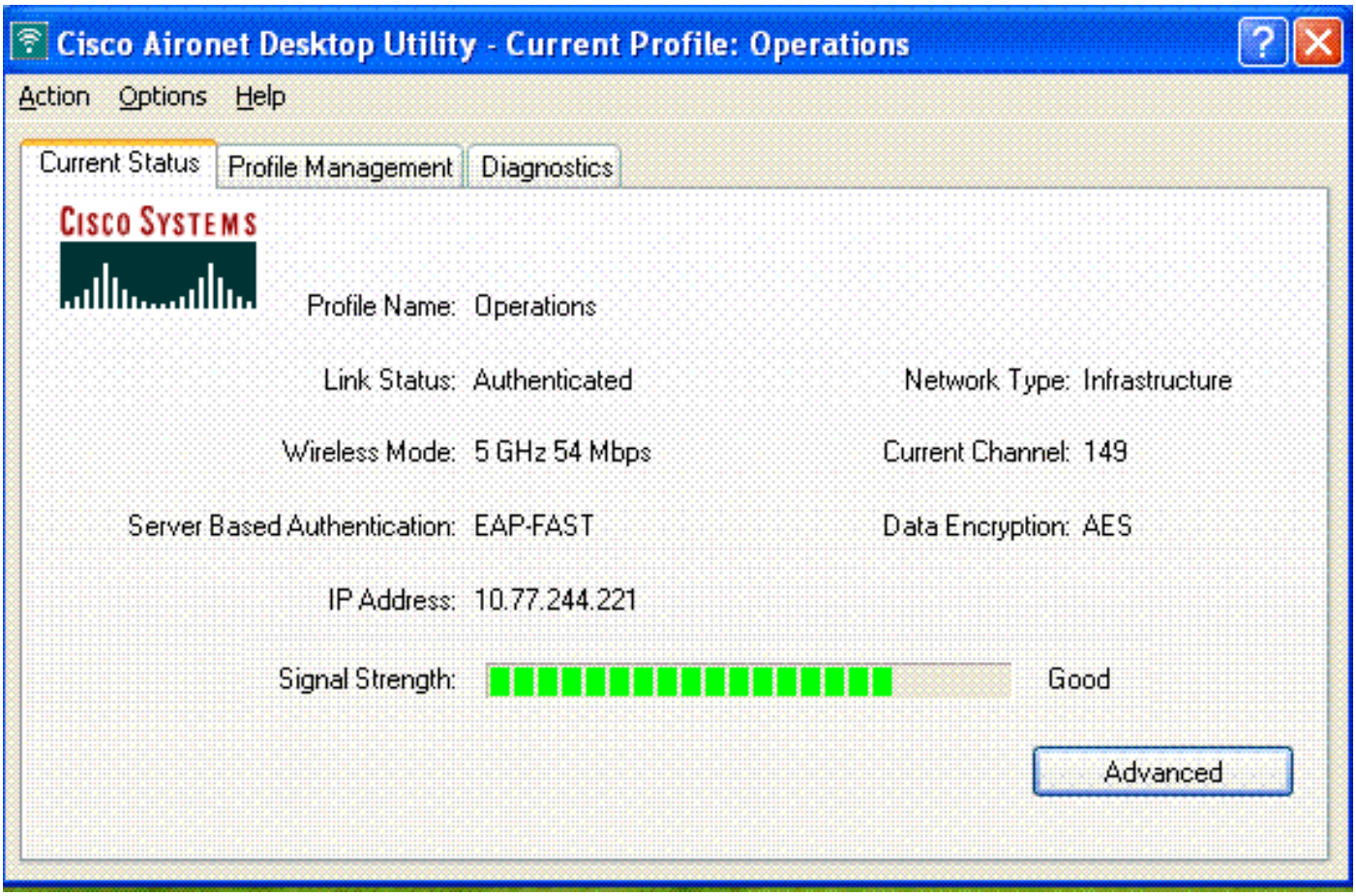
当管理员部门的用户连接到无线LAN管理员时，系统会提示用户输入802.1x凭证（在本例中为EAP-FAST凭证）。用户提供凭证后，WLC会将这些凭证传递到Cisco Secure ACS服务器。Cisco Secure ACS服务器根据数据库验证用户凭证，并在身份验证成功后将url-redirect属性返回至无线LAN控制器。身份验证在此阶段完成。

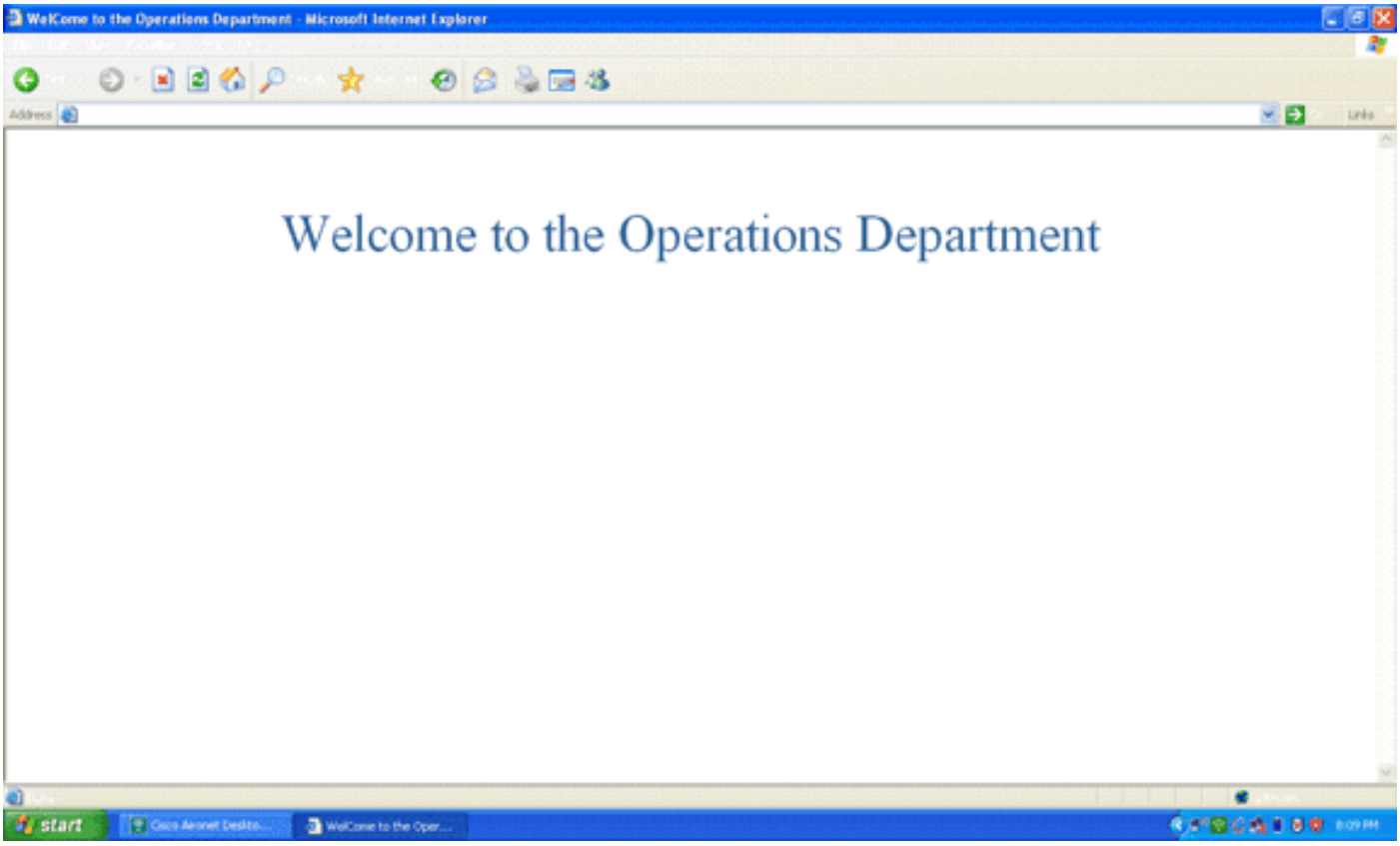


当用户打开Web浏览器时，系统会将用户重定向到管理部门的主页URL。（此URL通过cisco-av-pair属性返回到WLC）。在重定向后，用户具有对网络的完全访问权限。屏幕截图如下：



当操作部门的用户连接到WLAN操作时，也会发生相同的一系列事件。





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。

您可以使用以下命令对配置进行故障排除。

- **show wlan wlan_id** — 显示特定WLAN的Web重定向功能的状态。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 events enable** — 启用802.1x数据包消息的调试。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 events enable** — 启用所有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: '
```

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

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）。