

在Cisco 统一无线网络的Wi-Fi Protected Access (WPA)配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[WPA 和 WPA2 支持](#)

[网络设置](#)

[针对 WPA2 企业模式配置设备](#)

[配置 WLC 以便通过外部 RADIUS 服务器进行 RADIUS 身份验证](#)

[针对 WPA2 企业操作模式配置 WLAN](#)

[针对 WPA2 企业模式身份验证 \(EAP-FAST\) 配置 RADIUS 服务器](#)

[针对 WPA2 企业操作模式配置无线客户端](#)

[针对 WPA2 个人模式配置设备](#)

[故障排除](#)

[相关信息](#)

简介

本文档说明如何配置 Cisco 统一无线网络中的 Wi-Fi 安全访问 (WPA)。

先决条件

要求

在尝试进行此配置之前，请确保您已具有以下主题的基础知识：

- WPA
- 无线 LAN (WLAN) 安全解决方案**注意**：有关 Cisco WLAN 安全解决方案的信息，请参阅 [Cisco 无线 LAN 安全概述](#)。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco 1000 系列轻量接入点 (LAP)
- 运行固件 4.2.61.0 的 Cisco 4404 无线 LAN 控制器 (WLC)

- 运行固件 4.1 的 Cisco 802.11a/b/g 客户端适配器
- 运行固件 4.1 的 Aironet Desktop Utility (ADU)
- Cisco Secure ACS 服务器版本 4.1

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](#)。

WPA 和 WPA2 支持

Cisco 统一无线网络支持 Wi-Fi 联盟证书 WPA 和 WPA2。Wi-Fi 联盟于 2003 年引入 WPA。Wi-Fi 联盟于 2004 年引入 WPA2。所有经过 Wi-Fi WPA2 认证的产品都必须能够与经过 Wi-Fi WPA 认证的产品进行互操作。

WPA 和 WPA2 为最终用户和网络管理员提供了高级别的保证, 确保他们的数据保持私密性, 并将对他们网络的访问限制在授权用户范围内。这两种证书都有个人和企业两种操作模式, 可满足两个市场分区的不同需要。每个证书的企业模式使用 IEEE 802.1X 和 EAP 进行身份验证。每个证书的个人模式使用预共享密钥 (PSK) 进行身份验证。Cisco 建议不要使用个人模式进行企业或政府部署, 因为该模式使用 PSK 进行用户身份验证。PSK 对于企业环境并不安全。

WPA 可以解决原始 IEEE 802.11 安全实施中出现的所有已知 WEP 漏洞, 为企业和小型办公室/家庭办公室 (SOHO) 环境中的 WLAN 提供了一种即时安全解决方案。WPA 使用 TKIP 进行加密。

WPA2 是新一代 Wi-Fi 安全证书。它是 Wi-Fi 联盟对已批准的 IEEE 802.11i 标准的可互操作实现。它将计数器模式与密码块链消息身份验证码协议 (CCMP) 结合使用, 实现了美国国家标准与技术研究所 (NIST) 建议的 AES 加密算法。WPA2 促进了政府 FIPS 140-2 标准的实行。

WPA 与 WPA2 的模式类型比较

	WPA	WPA2
企业模式 (企业、政府、教育)	<ul style="list-style-type: none"> • 验证 : IEEE 802.1X/EAP • 加密 : TKIP/MIC 	<ul style="list-style-type: none"> • 验证 : IEEE 802.1X/EAP • 加密 : AES-CCMP
个人模式 (SOHO、家庭/个人)	<ul style="list-style-type: none"> • 验证 : PSK • 加密 : TKIP/MIC 	<ul style="list-style-type: none"> • 验证 : PSK • 加密 : AES-CCMP

在企业操作模式下, WPA 和 WPA2 均使用 802.1X/EAP 进行身份验证。802.1X 为 WLAN 提供客户端与身份验证服务器之间相互的严格身份验证。另外, 802.1X 还可针对每个用户、每个会话提供动态加密密钥, 从而消除了与静态加密密钥相关的管理负担和安全问题。

使用 802.1X, 用于身份验证的证书 (如登录口令) 通过无线介质传输时从不会采用明码或不加密的

形式。尽管 802.1X 身份验证类型为无线 LAN 提供了有力的身份验证，但除 802.1X 以外，加密还需要使用 TKIP 或 AES，因为标准 802.11 WEP 加密容易受到网络攻击。

共有几种 802.1X 身份验证类型，每种类型提供不同的身份验证方法，但它们依靠同一个框架和 EAP 在客户端与接入点之间进行通信。在所有 WLAN 产品中，Cisco Aironet 产品支持的 802.1X EAP 身份验证类型最多。支持的类型包括：

- [Cisco LEAP](#)
- [通过安全隧道的 EAP 灵活身份验证 \(EAP-FAST\)](#)
- EAP 传输层安全 (EAP-TLS)
- [受保护的扩展身份验证协议 \(PEAP\)](#)
- EAP 隧道 TLS (EAP-TTLS)
- EAP 用户身份模块 (EAP-SIM)

802.1X 身份验证的另一个好处是实现 WLAN 用户组的集中管理，包括基于策略的密钥轮换、动态密钥分配、动态 VLAN 分配和 SSID 限制。这些功能会轮换加密密钥。

在个人操作模式下，使用预共享密钥（口令）进行身份验证。个人模式只需要一个接入点和客户端设备，而企业模式通常要求网络中有一个 RADIUS 或其他身份验证服务器。

本文档提供了在 Cisco 统一无线网络中配置 WPA2（企业模式）和 WPA2-PSK（个人模式）的示例。

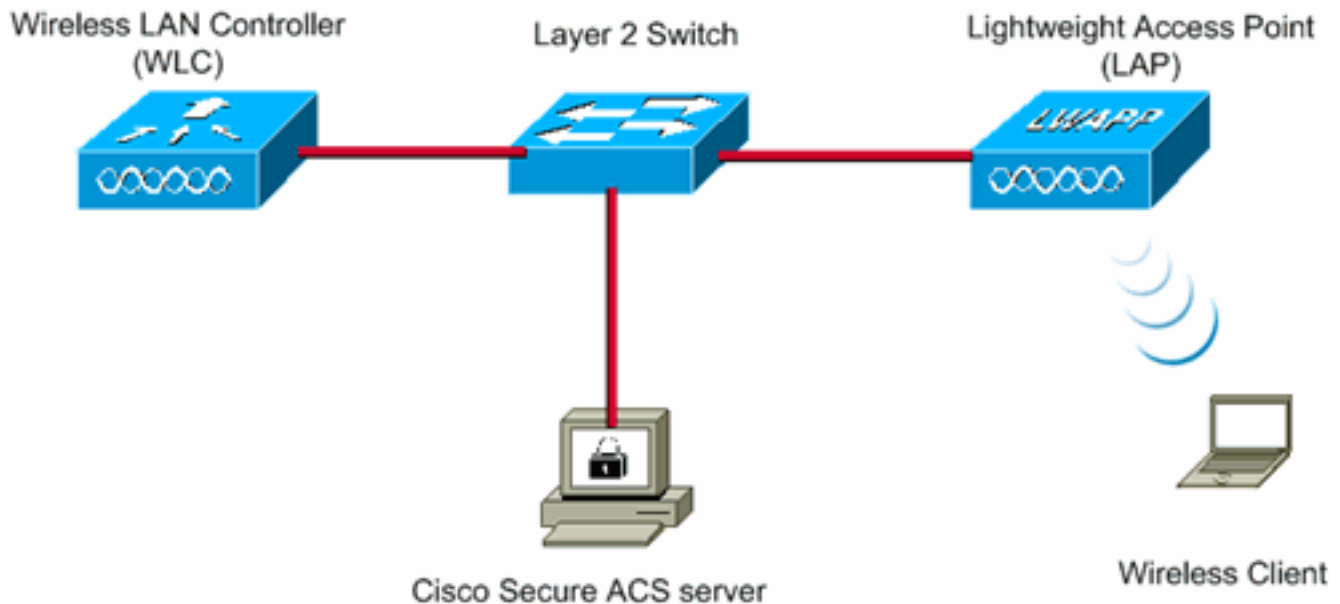
[网络设置](#)

在此设置中，Cisco 4404 WLC 和 Cisco 1000 系列 LAP 通过第 2 层交换机连接起来。还有一个外部 RADIUS 服务器 (Cisco Secure ACS) 也连接到同一个交换机。所有设备都在同一个子网中。接入点 (LAP) 最初在控制器中注册。需要创建两个无线 LAN，一个用于 WPA2 企业模式，另一个用于 WPA2 个人模式。

WPA2 企业模式 WLAN (SSID : WPA2-Enterprise) 将使用 EAP-FAST 对无线客户端和 AES 进行加密身份验证。Cisco Secure ACS 服务器将用作外部 RADIUS 服务器，用于对无线客户端进行身份验证。

WPA2 个人模式 WLAN (SSID : WPA2-PSK)将使用WPA2-PSK验证与预先共享密钥“abcdefghijkl”。

您需要将设备配置为以下设置：



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

针对 WPA2 企业模式配置设备

本部分提供有关如何配置本文档所述功能的信息。

若要针对 WPA2 企业操作模式配置设备，请执行下列步骤：

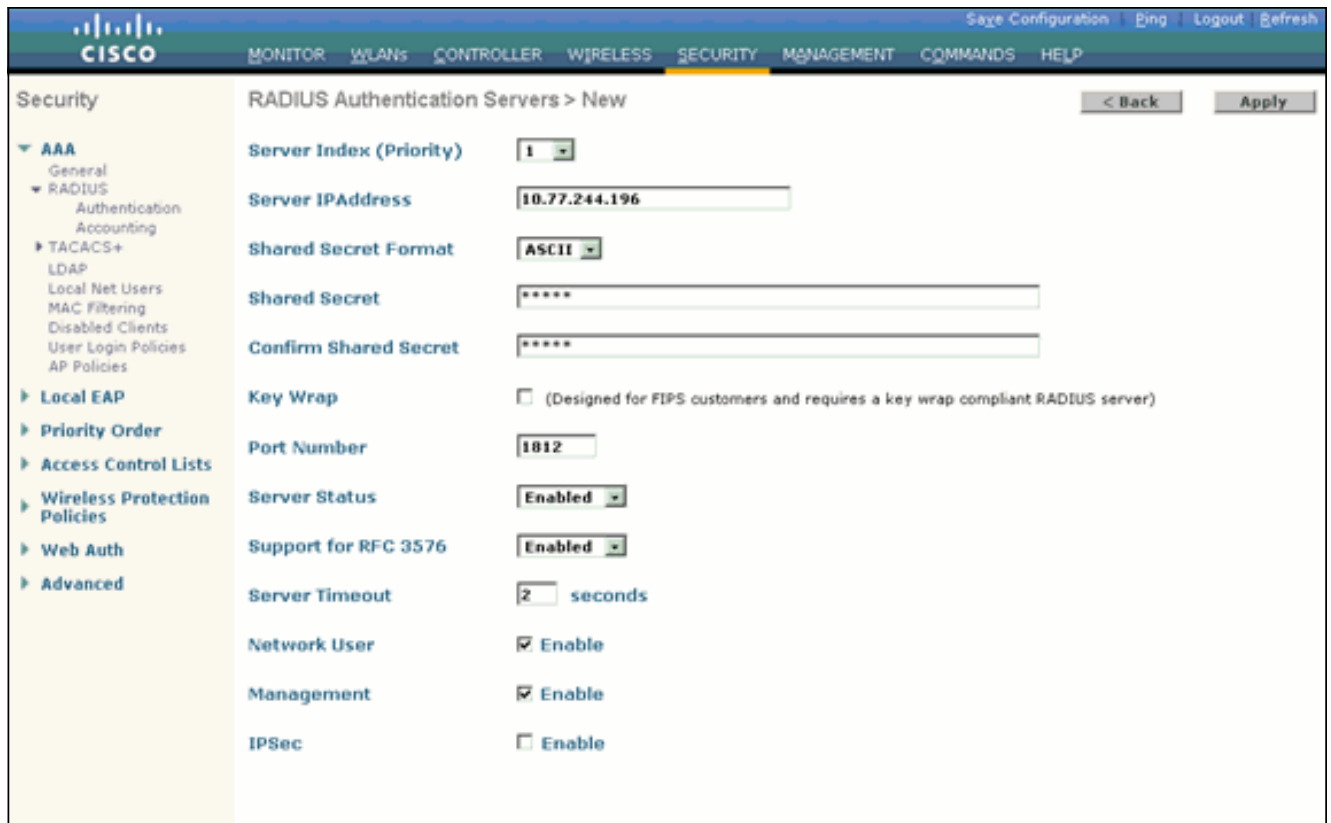
1. [配置 WLC 以便通过外部 RADIUS 服务器进行 RADIUS 身份验证](#)
2. [针对 WPA2 企业模式身份验证 \(EAP-FAST\) 配置 WLAN](#)
3. [针对 WPA2 企业模式配置无线客户端](#)

配置 WLC 以便通过外部 RADIUS 服务器进行 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。随后，外部 RADIUS 服务器使用 EAP-FAST 验证用户凭证，并提供对无线客户端的访问。

完成以下这些步骤，为外部 RADIUS 服务器配置 WLC：

1. 从控制器的 GUI 中选择**安全性**和“**RADIUS 身份验证**”，以便显示“**RADIUS 身份验证服务器**”页。然后，请点击**new**来定义 RADIUS 服务器。
2. 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。



3. 单击 **Apply**。

[针对 WPA2 企业操作模式配置 WLAN](#)

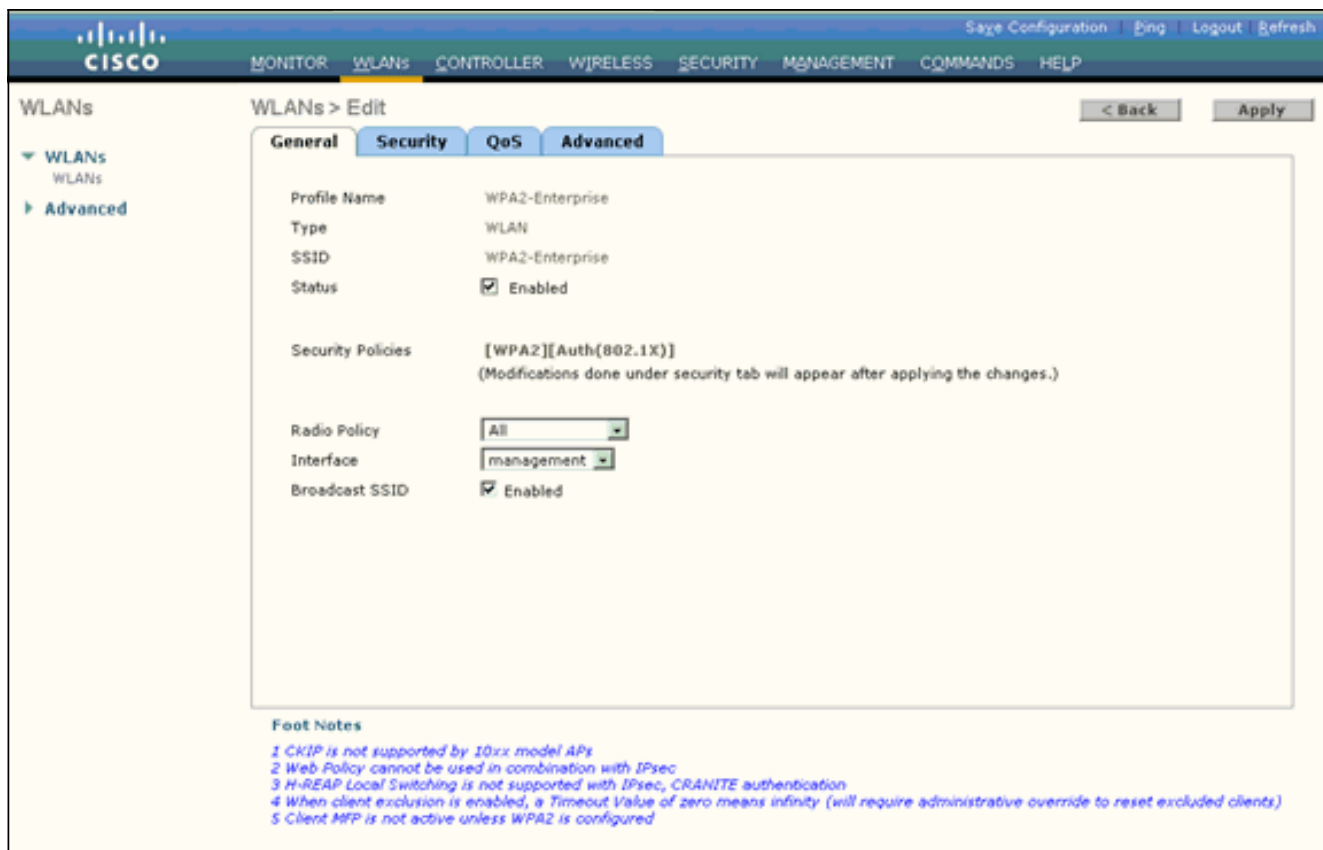
下一步，配置客户端将用于连接到无线网络的 WLAN。用于 WPA2 企业模式的 WLAN SSID 将是 WPA2-Enterprise。本例将此 WLAN 分配到管理接口。

若要配置 WLAN 及其相关参数，请完成下列步骤：

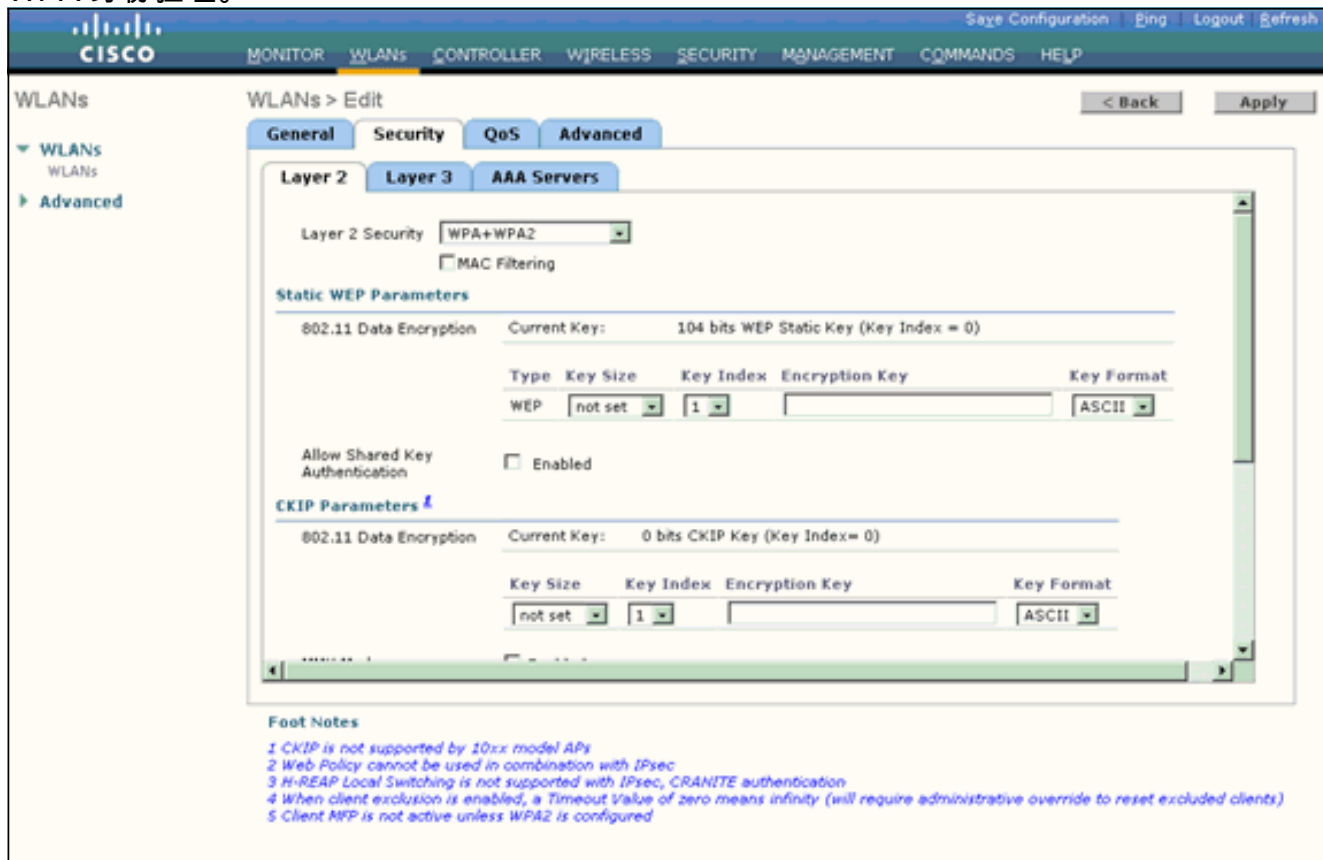
1. 从控制器的 GUI 中单击 **WLAN** 以显示“WLAN”页。此页列出了控制器上现有的 WLAN。
2. 单击 **New** 以创建新的 WLAN。
3. 在 **WLANs > New** 页上输入 WLAN SSID 名称和配置文件名称。然后，单击 **Apply**。本例使用 **WPA2-Enterprise** 作为 SSID。



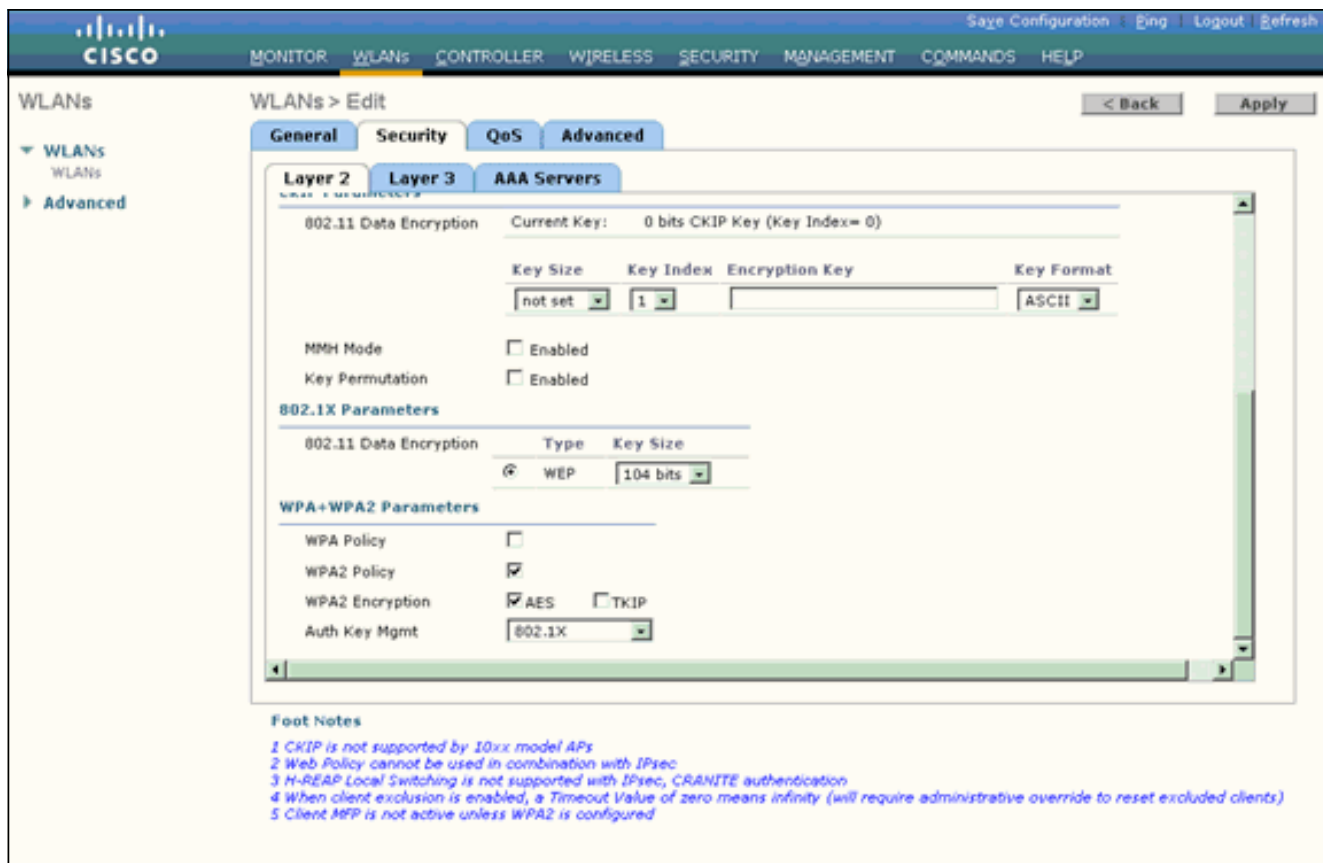
4. 创建新 WLAN 后，就会显示新 WLAN 的 **WLAN > Edit** 页。在此页上，可以定义特定于此 WLAN 的各种参数。其中包括“General Policies”、“Security Policies”、“QOS”策略和“Advanced”参数。
5. 根据一般策略，请检查**状态检查**方框来启用WLAN。



6. 如果希望 AP 在其信标帧中广播 SSID，请选中 **Broadcast SSID** 复选框。
7. 单击 **Security** 选项卡。在“第 2 层安全性”下，选择 **WPA+WPA2**。此操作将启用 WLAN 的 WPA 身份验证。

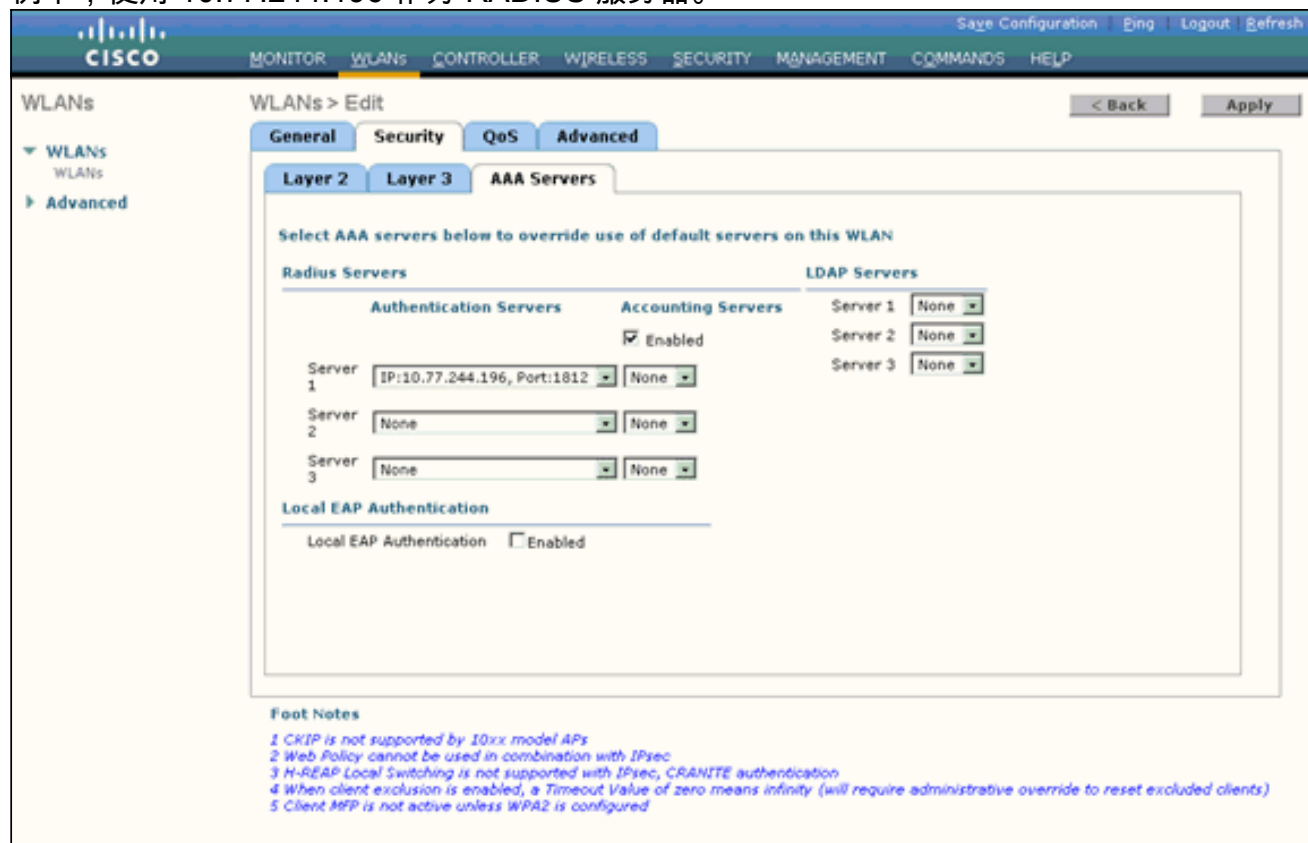


8. 向下滚动页面以修改 **WPA+WPA2 Parameters**。在本例中，选择 WPA2 策略和 AES 加密。



9. 在“Auth Key Mgmt”下，选择 **802.1x**。此操作将为 WLAN 启用采用 802.1x/EAP 身份验证和 AES 加密的 WPA2。

10. 单击 **AAA Servers** 选项卡。在“Authentication Servers”下，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。



11. 单击 **Apply**。注意：这是针对 EAP 身份验证需要在控制器上配置的唯一 EAP 设置。所有其他特定于 EAP-FAST 的配置需要在 RADIUS 服务器和需要进行身份验证的客户端上完成。

。

针对 WPA2 企业模式身份验证 (EAP-FAST) 配置 RADIUS 服务器

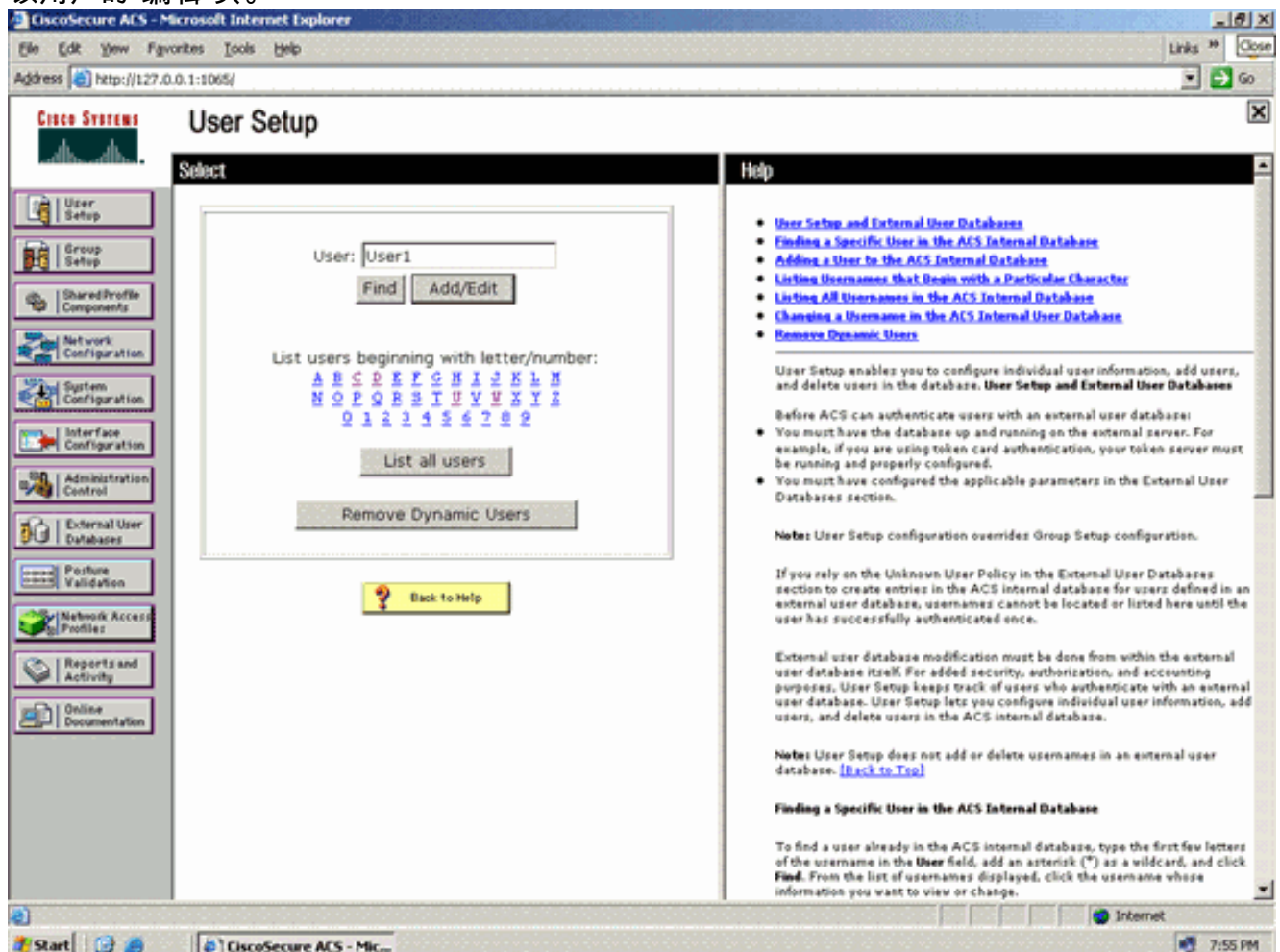
在本例中，使用 Cisco Secure ACS 作为外部 RADIUS 服务器。若要针对 EAP-FAST 身份验证配置 RADIUS 服务器，请执行下列步骤：

1. [创建一个用于对客户端进行身份验证的用户数据库](#)
2. [将 WLC 作为 AAA 客户端添加到 RADIUS 服务器](#)
3. [使用匿名带内 PAC 配置为 RADIUS 服务器配置 EAP-FAST 身份验证](#)注意：配置 EAP-FAST 可以采用匿名带内 PAC 配置，也可以采用经身份验证的带内 PAC 配置。本例使用匿名带内 PAC 配置。有关采用匿名带内 PAC 配置和经身份验证的带内 PAC 配置对 EAP FAST 进行配置的详细信息和示例，请参阅[使用无线 LAN 控制器和外部 RADIUS 服务器的 EAP-FAST 身份验证的配置示例](#)。

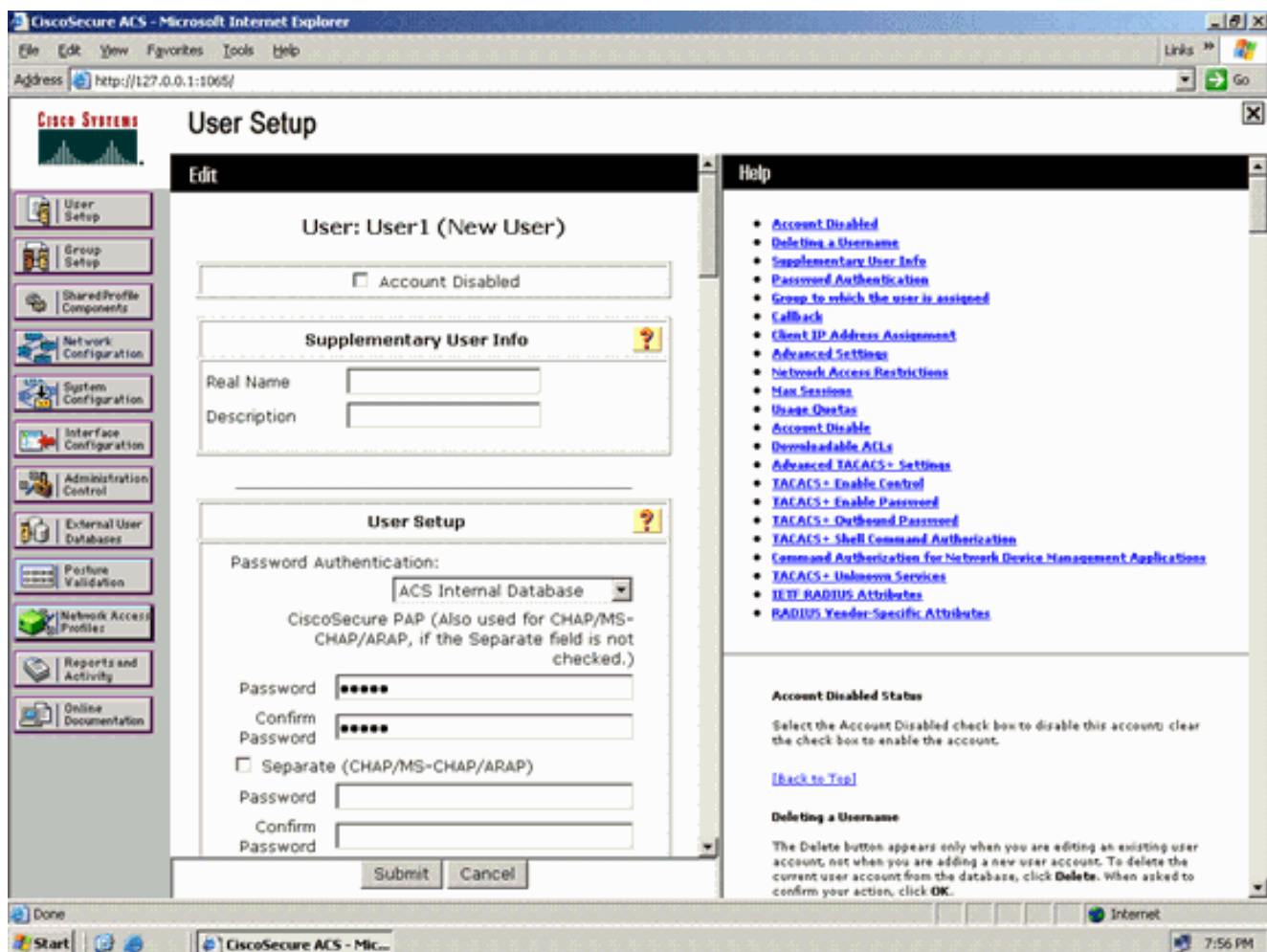
创建一个用于对 EAP-FAST 客户端进行身份验证的用户数据库

若要在 ACS 上为 EAP-FAST 客户端创建一个用户数据库，请完成下列步骤。本例将 EAP-FAST 客户端的用户名和口令分别配置为 User1 和 User1。

1. 从导航栏的 ACS GUI 中选择 **User Setup**。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。



2. 在“User Setup Edit”页中，按本例所示配置“Real Name”、“Description”及“Password”设置。本文档使用 **ACS Internal Database** 作为“Password Authentication”。

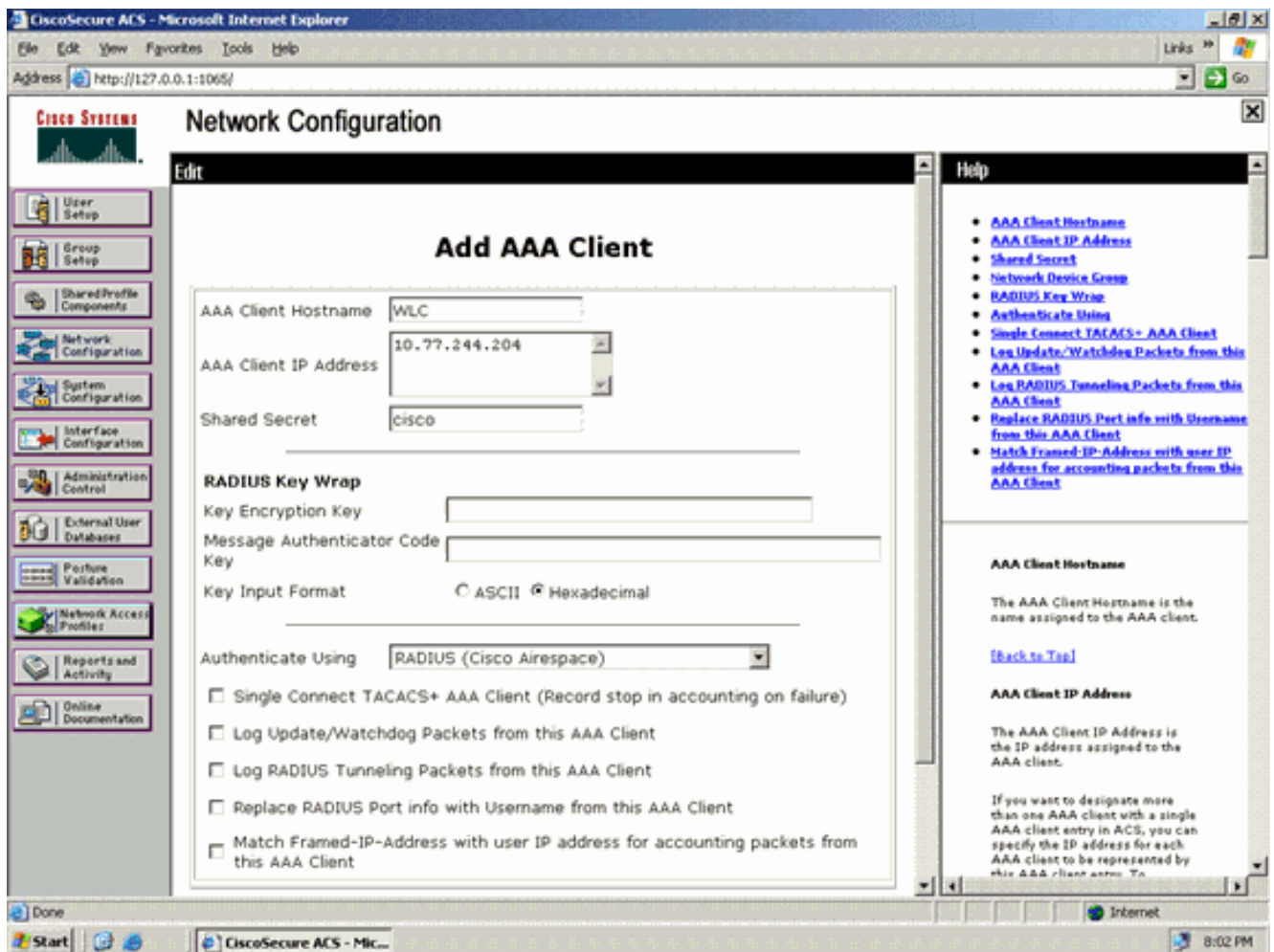


3. 从“Password Authentication”下拉框中选择 **ACS Internal Database**。
4. 配置所需的所有其他参数，然后单击 **Submit**。

将 WLC 作为 AAA 客户端添加到 RADIUS 服务器

若要将控制器定义为 ACS 服务器上的 AAA 客户端，请完成下列步骤：

1. 从 ACS GUI 中单击 **Network Configuration**。在“Network Configuration”页的“Add AAA client”部分下，单击 **Add Entry** 将 WLC 作为 AAA 客户端添加到 RADIUS 服务器。
2. 在“AAA Client”页中，定义 WLC 名称、IP 地址、共享密钥和身份验证方法 (RADIUS/Cisco Airespace)。有关其他非 ACS 身份验证服务器的信息，请参阅制造商提供的文档。



注意：在 WLC 和 ACS 服务器上配置的共享密钥必须匹配。共享密钥区分大小写。

3. 单击 **Submit+Apply**。

[使用匿名带内 PAC 配置为 RADIUS 服务器配置 EAP-FAST 身份验证](#)

匿名带内配置

这是 ACS 与最终用户客户端建立安全连接以便为客户端提供新 PAC 的两种带内配置方法之一。此选项允许在最终用户客户端与 ACS 之间进行匿名 TLS 握手。

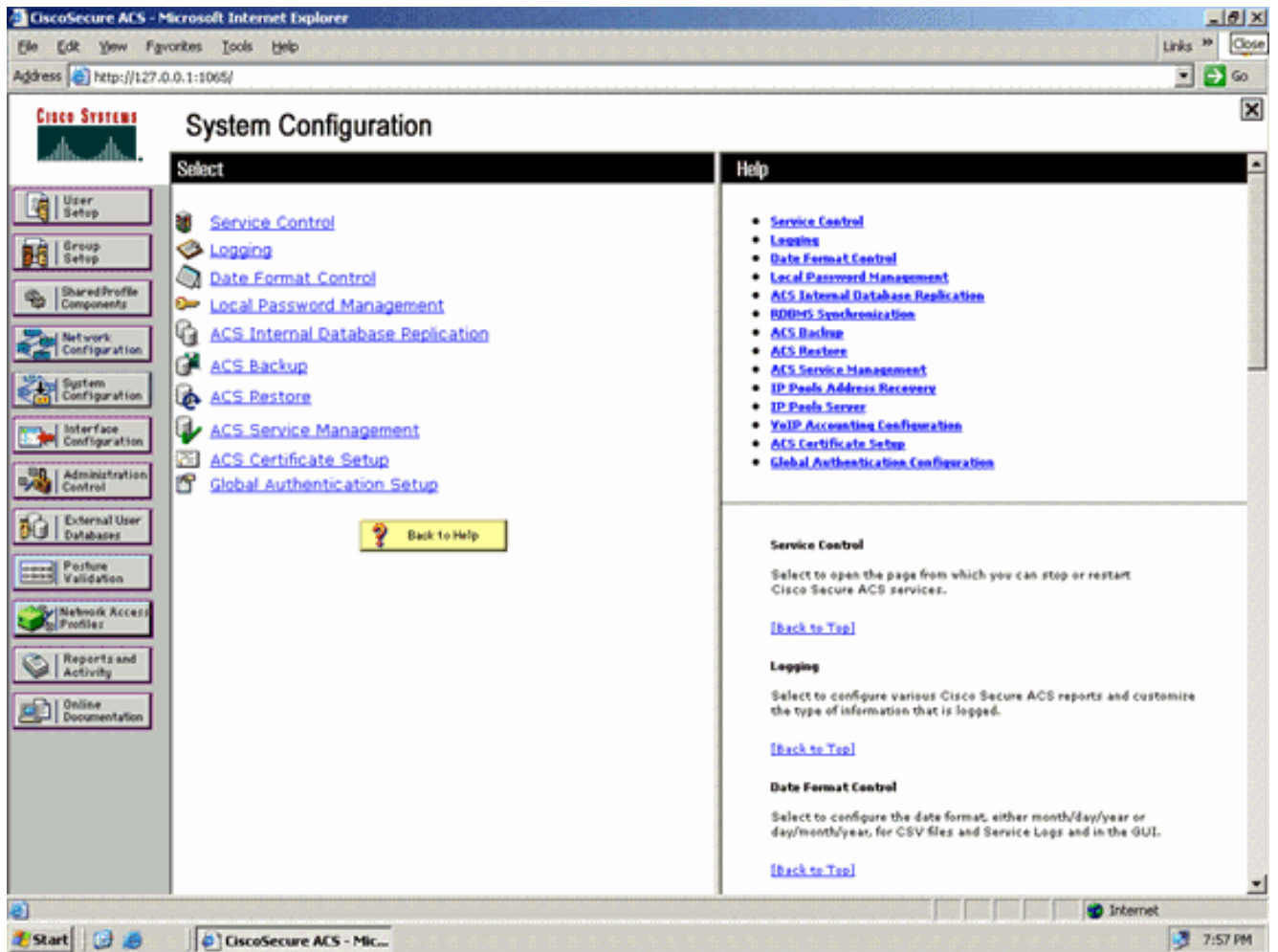
在对等体对 ACS 服务器进行身份验证之前，此方法在经身份验证的 Diffie-HellmanKey 协商协议 (ADHP) 隧道内操作。

随后，ACS 需要对用户进行 EAP-MS-CHAPv2 身份验证。当用户身份验证成功时，ACS 将与最终用户客户端建立一条 Diffie-Hellman 隧道。ACS 为用户生成一个 PAC，并将其与此 ACS 的相关信息一起发送到此隧道中的最终用户客户端。此配置方法在第零阶段使用 EAP-MSCHAPv2 作为身份验证方法，在第二阶段使用 EAP-GTC。

由于配置了未经身份验证的服务器，因此不可能使用纯文本口令。所以，在隧道内只能使用 MS-CHAP 凭证。MS-CHAPv2 用于证明对等体的身份和接收用于后续身份验证会话的 PAC (EAP-MS-CHAP 将仅用作内部方法)。

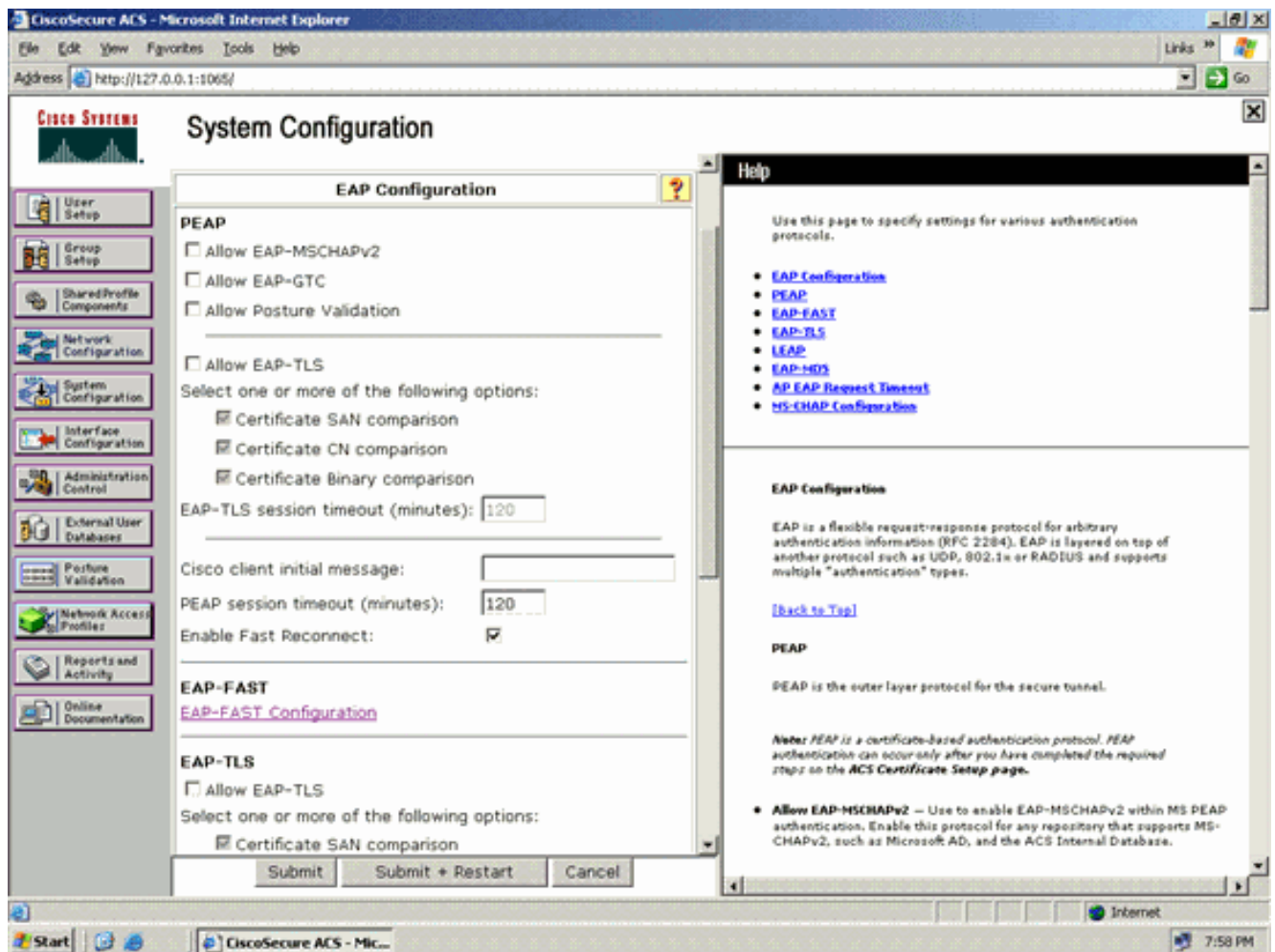
若要采用匿名带内配置为 RADIUS 服务器配置 EAP-FAST 身份验证，请完成下列步骤：

1. 在 RADIUS 服务器 GUI 中单击 **System Configuration**。从“System Configuration”页中选择 **Global Authentication Setup**。

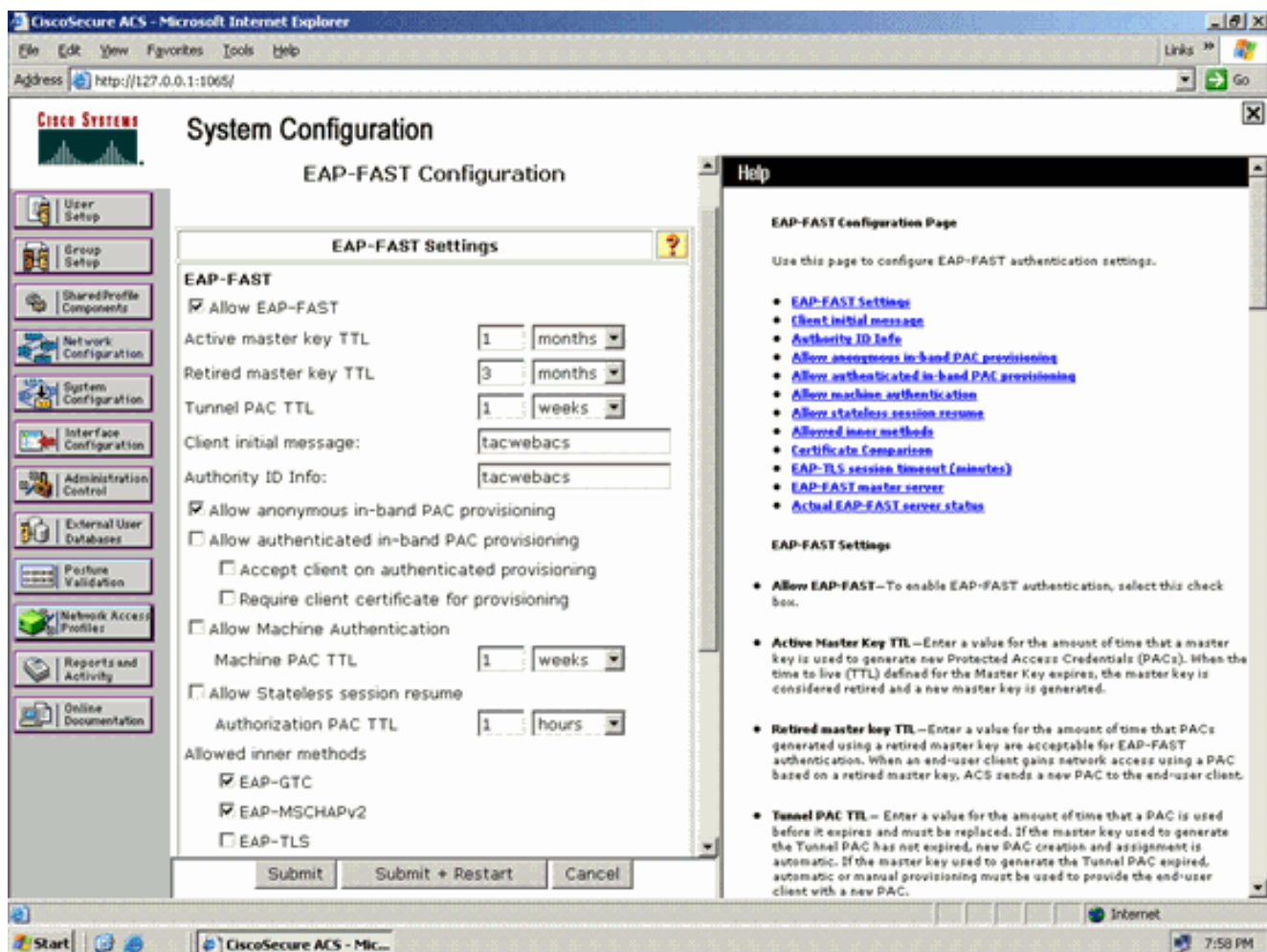


2. 在“Global Authentication”设置页中，单击 **EAP-FAST Configuration** 转到 EAP-FAST 设置页

。



3. 在“EAP-FAST Settings”页中，选中 **Allow EAP-FAST** 复选框以启用 RADIUS 服务器的 EAP-FAST。



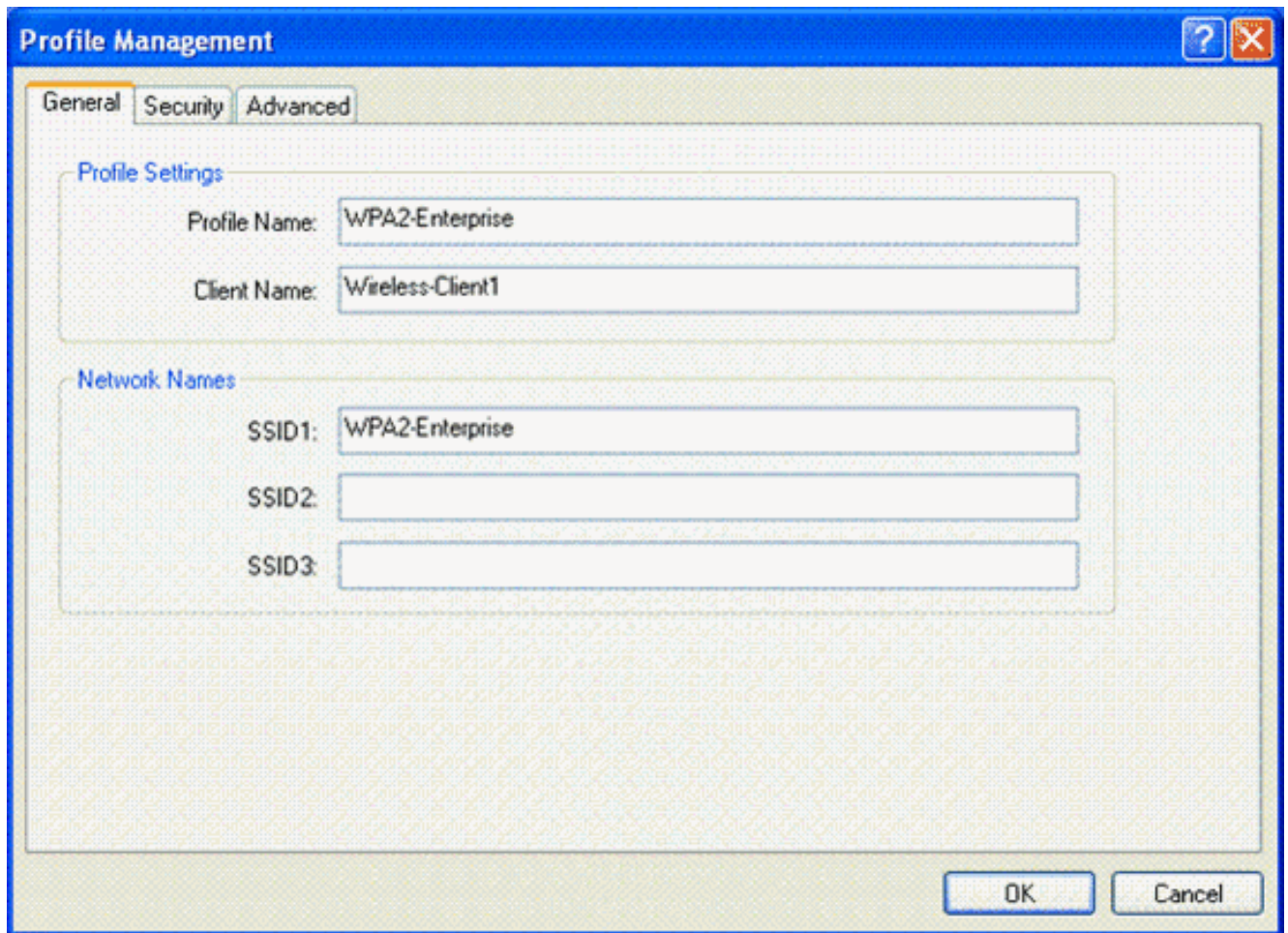
4. 根据需要配置“Active master key TTL”/“Retired master key TTL”（TTL 即存活时间）的值，或按本例所示将其设置为默认值。有关活动和停用的主密钥的信息，请参阅“主密钥”。有关详细信息，另请参阅“主密钥和 PAC TTL”。“Authority ID Info”字段表示此 ACS 服务器的文本身份，最终用户可使用该字段确定要根据哪个 ACS 服务器进行身份验证。必须填写此字段。“Client initial display message”字段用于指定要发送给使用 EAP-FAST 客户端进行身份验证的用户的一条消息。最大长度为 40 个字符。只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**—此选项确定哪些内在 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）。

针对 WPA2 企业操作模式配置无线客户端

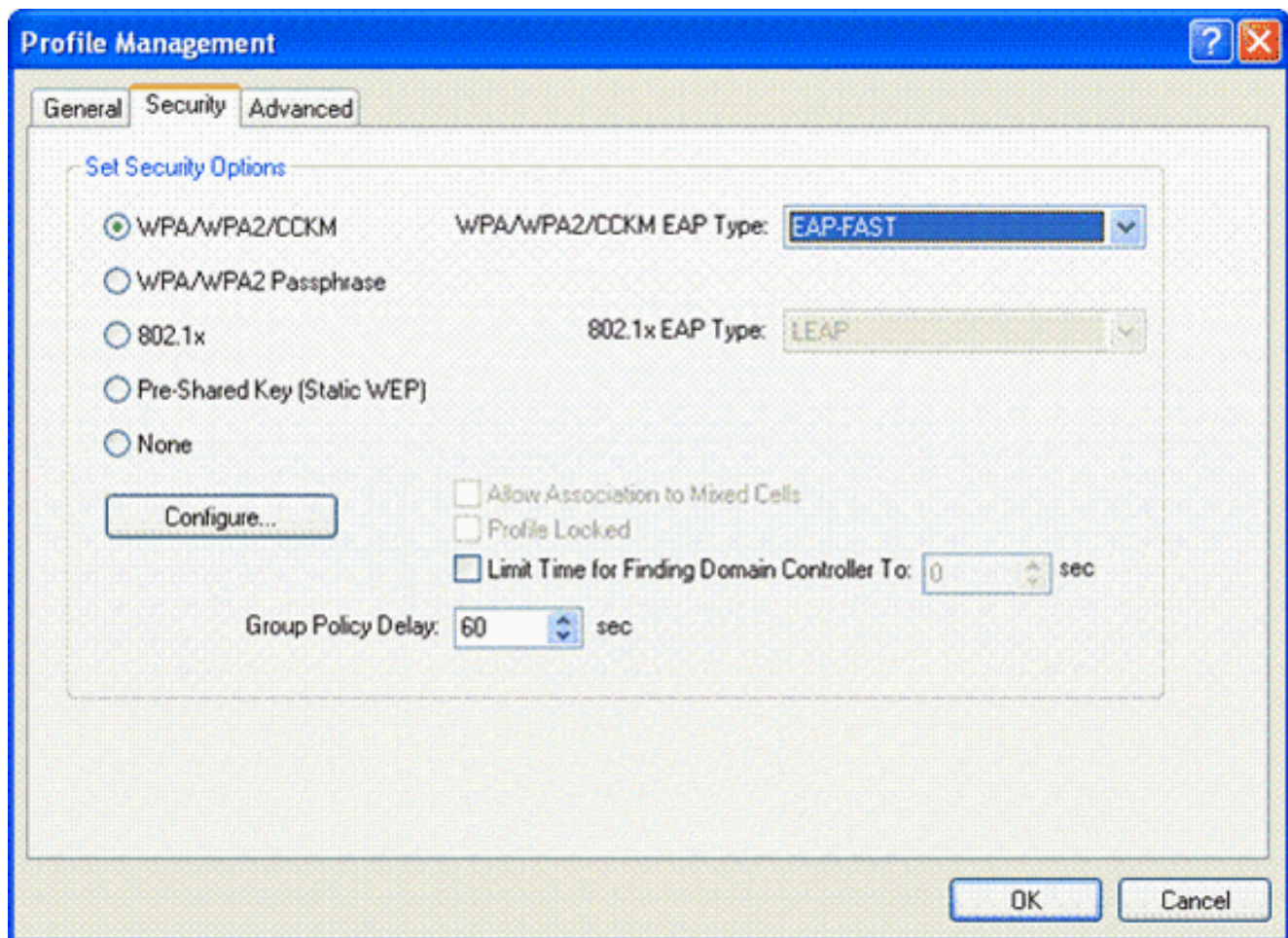
下一步是针对 WPA2 企业操作模式配置无线客户端。

若要针对 WPA2 企业模式配置无线客户端，请完成下列步骤。

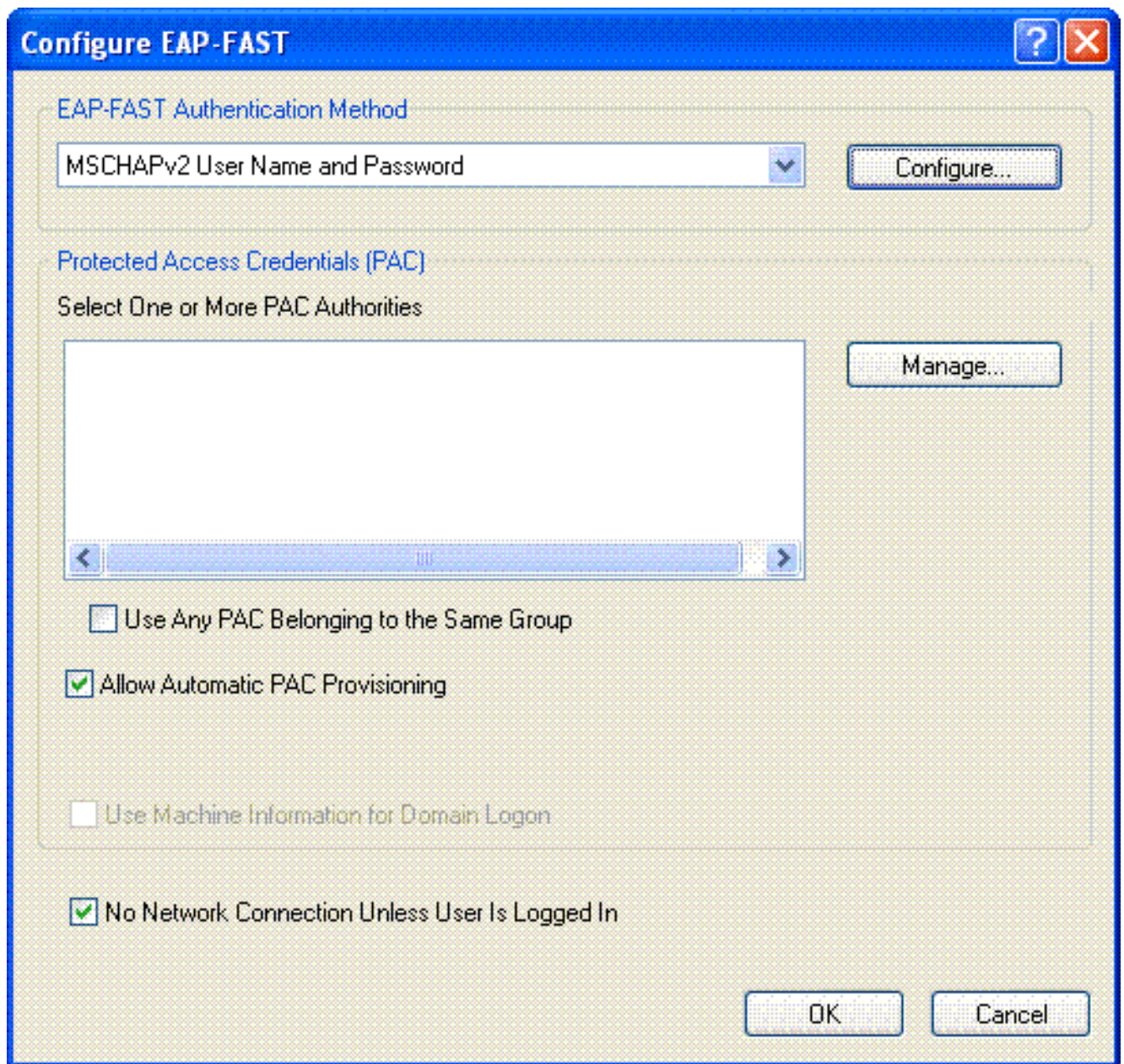
1. 在“Aironet Desktop Utility”窗口中，单击 **Profile Management > New** 为 WPA2-Enterprise WLAN 用户创建一个配置文件。如前所述，本文档使用 WLAN/SSID 名称 **WPA2-Enterprise** 表示无线客户端。
2. 在“Profile Management”窗口中，单击 **General** 选项卡，并按本例所示配置“Profile Name”、“Client Name”和“SSID”名称。然后单击 **OK**。



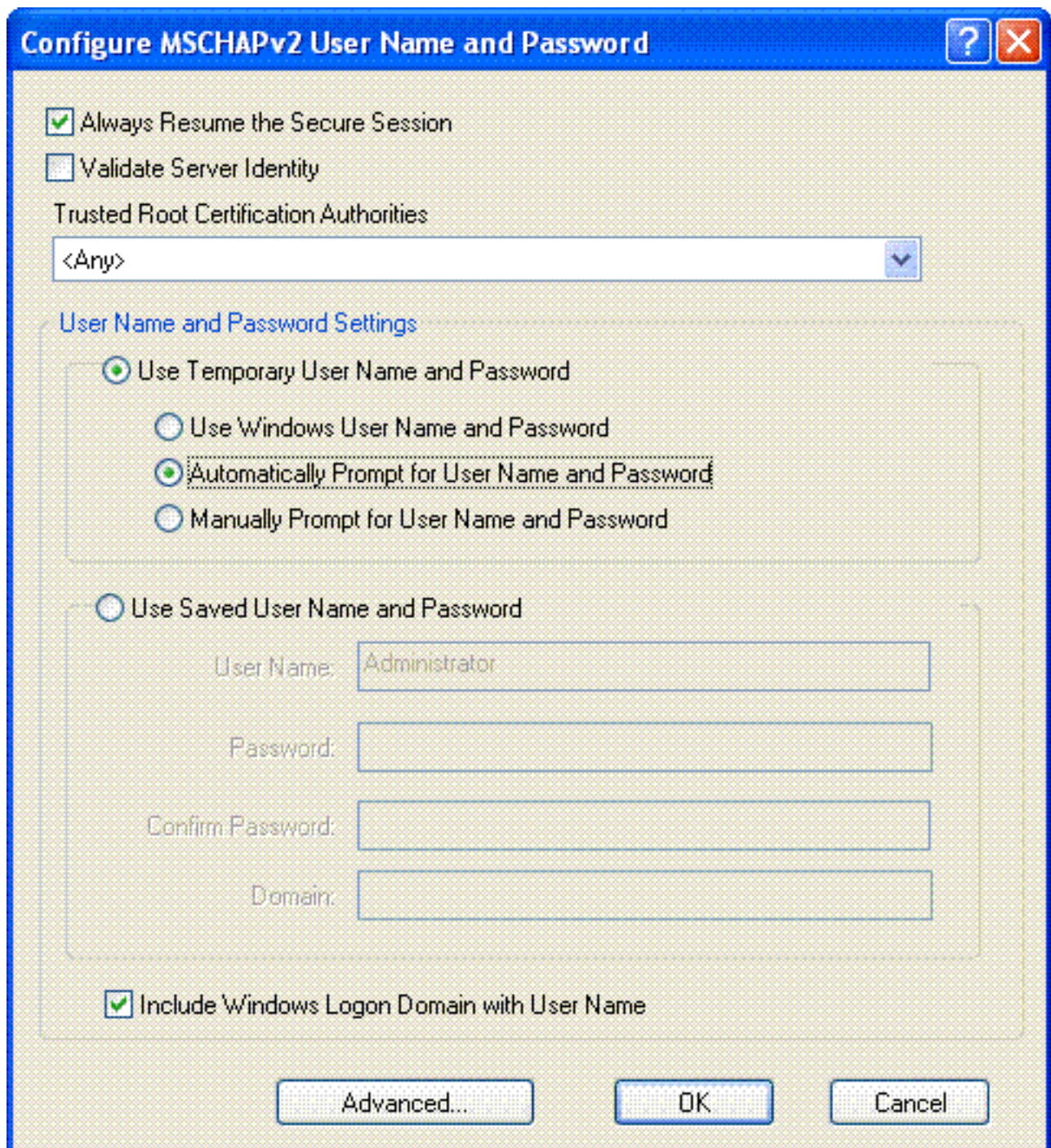
3. 单击 **Security** 选项卡，然后选择“WPA/WPA2/CCKM”以启用 WPA2 操作模式。在“WPA/WPA2/CCKM EAP Type”下，选择 **EAP-FAST**。单击 **Configure** 以配置 EAP-FAST 设置。



4. 在“Configure EAP-FAST”窗口中，选中 **Allow Automatic PAC Provisioning** 复选框。如果要配置匿名 PAC 配置，则会将 EAP-MS-CHAP 用作第零阶段内唯一的内部方法。



5. 从“EAP-FAST Authentication Method”下拉框中选择“MSCHAPv2 User Name and Password”作为身份验证方法。单击 **Configure**。
6. 在“Configure MSCHAPv2 User Name and Password”窗口中，选择适当的用户名和口令设置。本例选择 **Automatically Prompt for User Name and Password**。



在

ACS 应注册相同的用户名和口令。如前所述，本例分别使用 User1 和 User1 作为用户名和口令。另外请注意，这是匿名带内配置。所以，客户端无法验证服务器证书。您需要确保未选中“Validate Server Identity”复选框。

7. 单击 **Ok**。

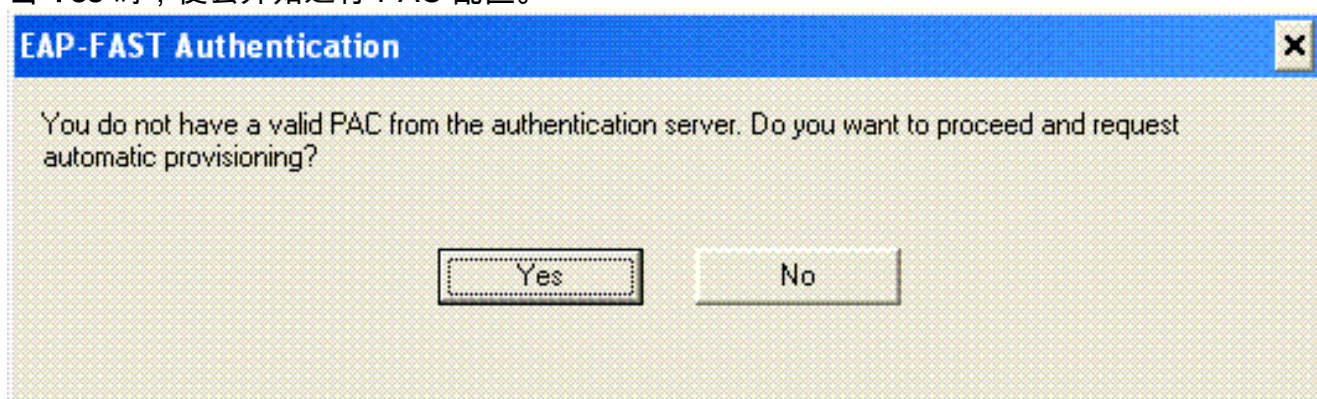
验证 WPA2 企业操作模式

若要验证您的 WPA2 企业模式配置是否工作正常，请完成下列步骤：

1. 在“Aironet Desktop Utility”窗口中，选择配置文件 **WPA2-Enterprise**，然后单击“Activate”以激活无线客户端配置文件。
2. 如果已启用“MS-CHAP ver2”作为身份验证方法，客户端将提示输入用户名和口令。

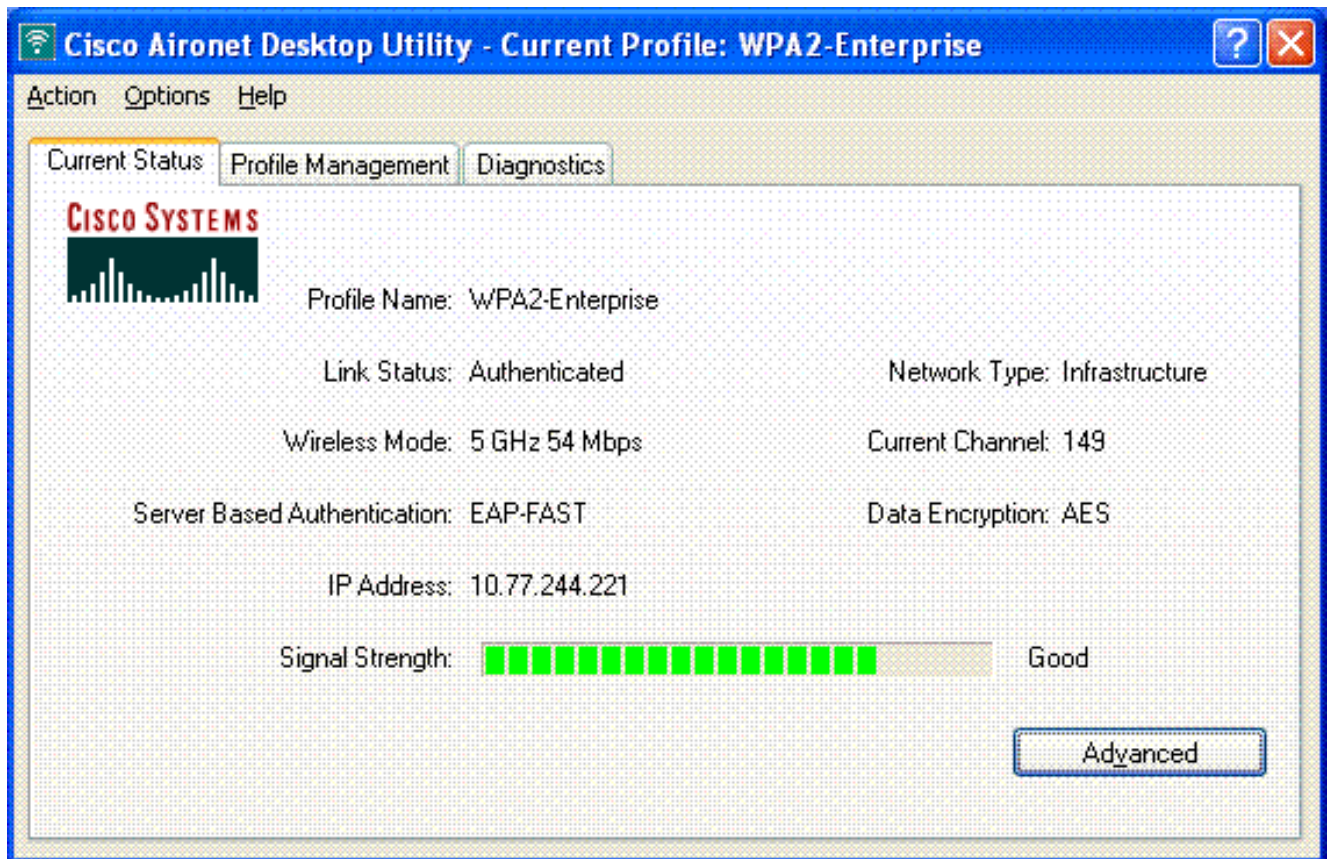


3. 在 EAP-FAST 进行用户处理的过程中，客户端将提示您向 RADIUS 服务器请求 PAC。当您单击 **Yes** 时，便会开始进行 PAC 配置。



4. 在第零阶段的 PAC 配置成功后，接着进行第一阶段和第二阶段，成功完成身份验证过程。身份验证成功时，无线客户端将与 WLAN WPA2-Enterprise 建立关联。下面是屏幕截图

:



您还可以验证 RADIUS 服务器是否收到并验证来自无线客户端的身份验证请求。检查 ACS 服务器上的 Passed Authentications 和 Failed Attempts 报告以完成此操作。在 ACS 服务器上的报表和活动下可获得这些报表。

针对 WPA2 个人模式配置设备

若要针对 WPA2 个人操作模式配置设备，请执行下列步骤：

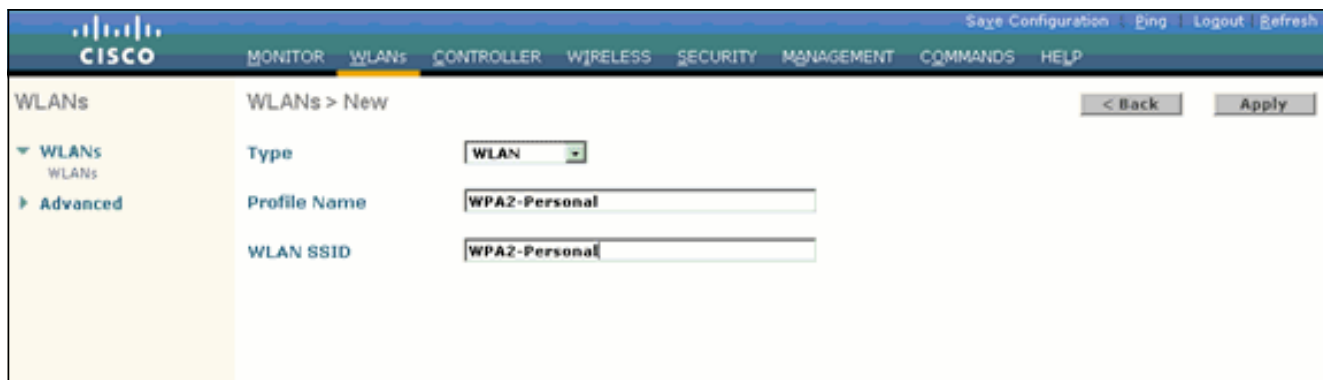
1. [针对 WPA2 个人模式身份验证配置 WLAN](#)
2. [针对 WPA2 个人模式配置无线客户端](#)

针对 WPA2 个人操作模式配置 WLAN

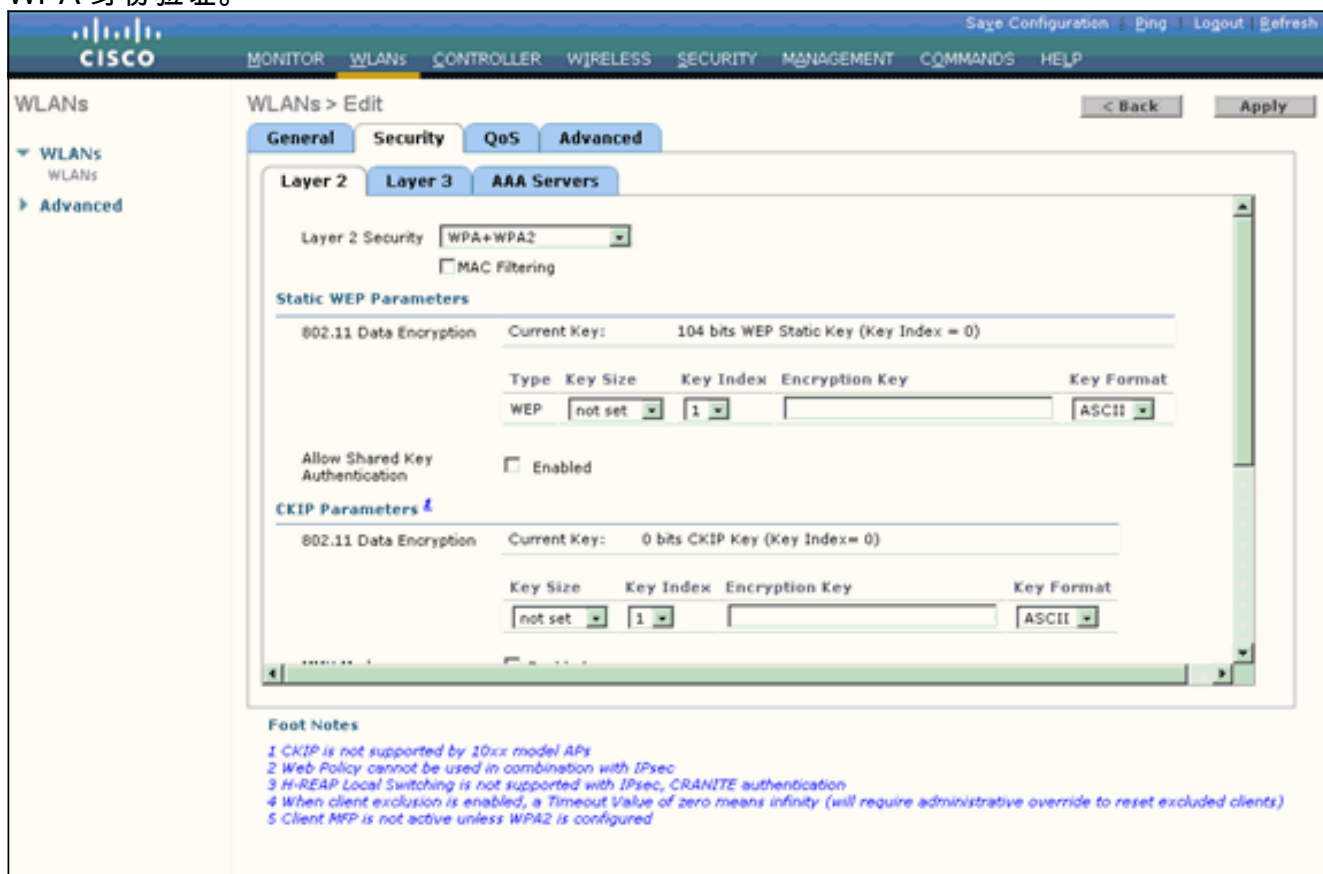
您需要配置客户端将用于连接到无线网络的 WLAN。用于 WPA2 个人模式的 WLAN SSID 将是 WPA2-Personal。本例将此 WLAN 分配到管理接口。

若要配置 WLAN 及其相关参数，请完成下列步骤：

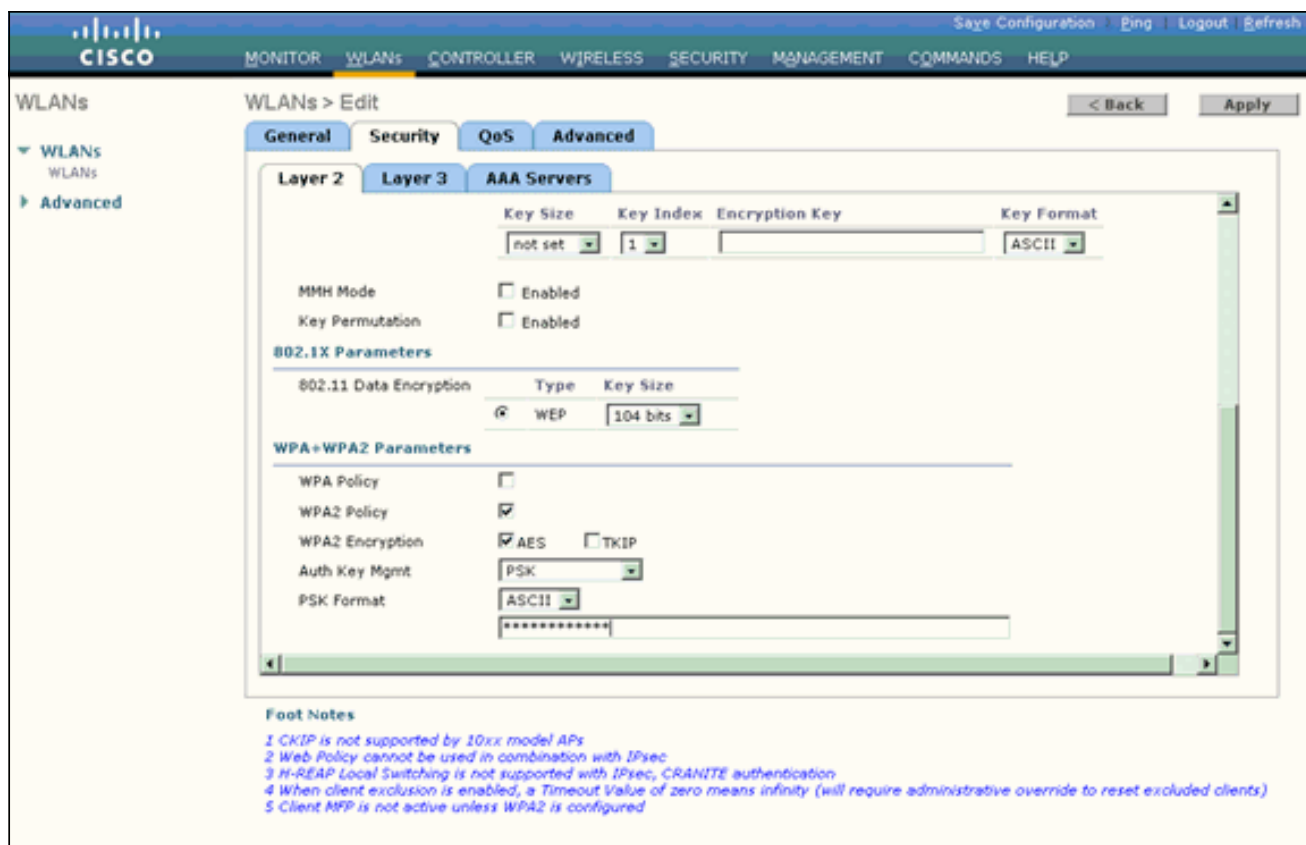
1. 从控制器的 GUI 中单击 **WLAN** 以显示“WLAN”页。此页列出了控制器上现有的 WLAN。
2. 单击 **New** 以创建新的 WLAN。
3. 在“WLANs > New”页上输入“WLAN SSID”名称、“Profile”名称和“WLAN ID”。然后，单击 **Apply**。本例使用 **WPA2-Personal** 作为 SSID。



4. 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。其中包括“General Policies”、“Security Policies”、“QoS”策略和“Advanced”参数。
5. 根据一般策略，请检查**状态检查**方框来启用WLAN。
6. 如果希望 AP 在其信标帧中广播 SSID，请选中 **Broadcast SSID** 复选框。
7. 单击 **Security** 选项卡。在“Layer Security”下，选择 **WPA+WPA2**。此操作将启用 WLAN 的 WPA 身份验证。



8. 向下滚动页面以修改 **WPA+WPA2 Parameters**。在本例中，选择 WPA2 策略和 AES 加密。
9. 在“Auth Key Mgmt”下，选择 **PSK** 以启用 WPA2-PSK。
10. 在适当的字段中输入预共享密钥，如下所示。



注意：用于 WLC 的预共享密钥必须与无线客户端上配置的预共享密钥匹配。

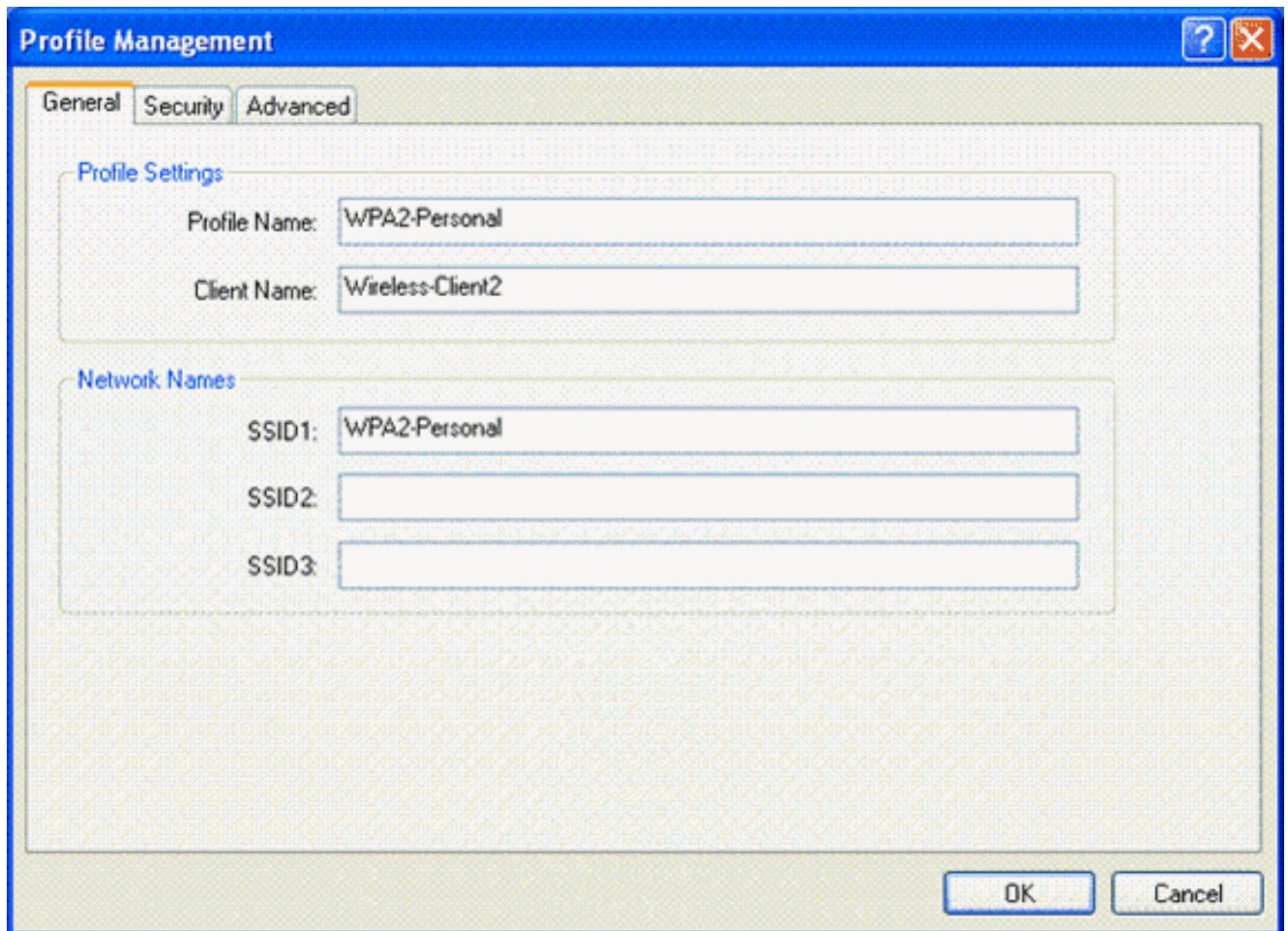
11. 单击 **Apply**。

针对 WPA2 个人模式配置无线客户端

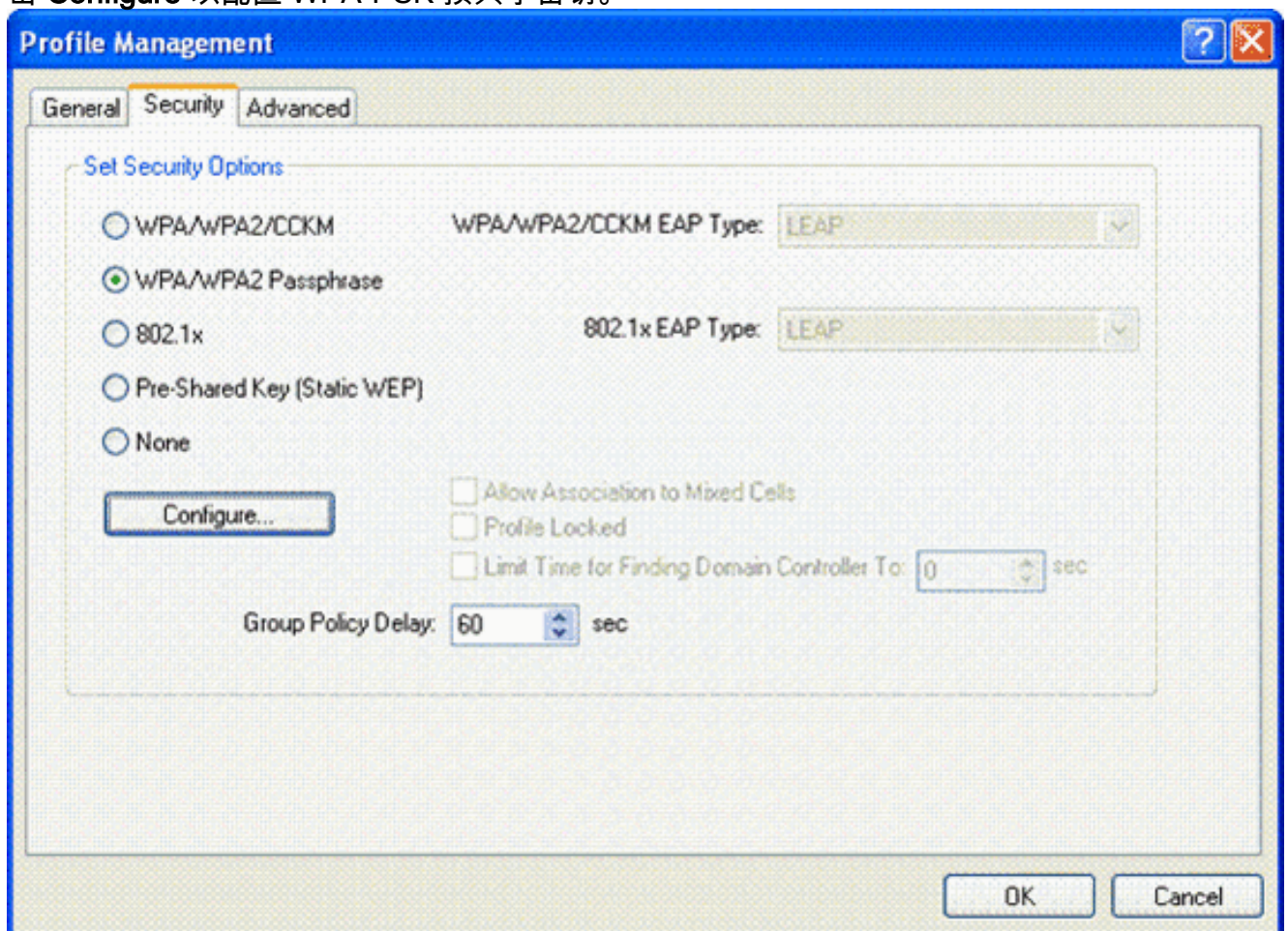
下一步是针对 WPA2 个人操作模式配置无线客户端。

若要针对 WPA2 个人模式配置无线客户端，请完成下列步骤：

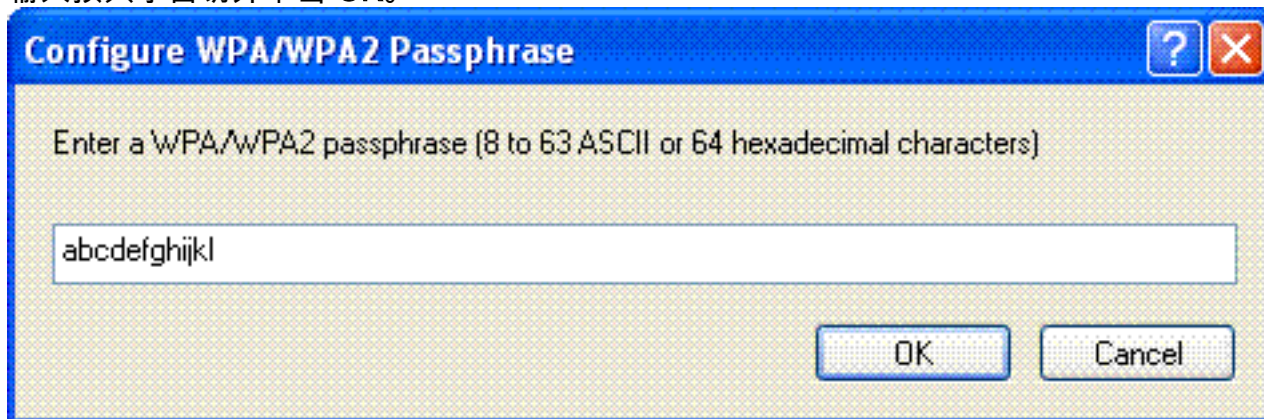
1. 在“Aironet Desktop Utility”窗口中，单击 **Profile Management > New** 为 WPA2-PSK WLAN 用户创建一个配置文件。
2. 在“Profile Management”窗口中，单击 **General** 选项卡，并按本例所示配置“Profile Name”、“Client Name”和“SSID”名称。然后，单击 **OK**。



3. 单击 **Security** 选项卡，然后选择“WPA/WPA2 Passphrase”以启用 WPA2-PSK 操作模式。单击 **Configure** 以配置 WPA-PSK 预共享密钥。



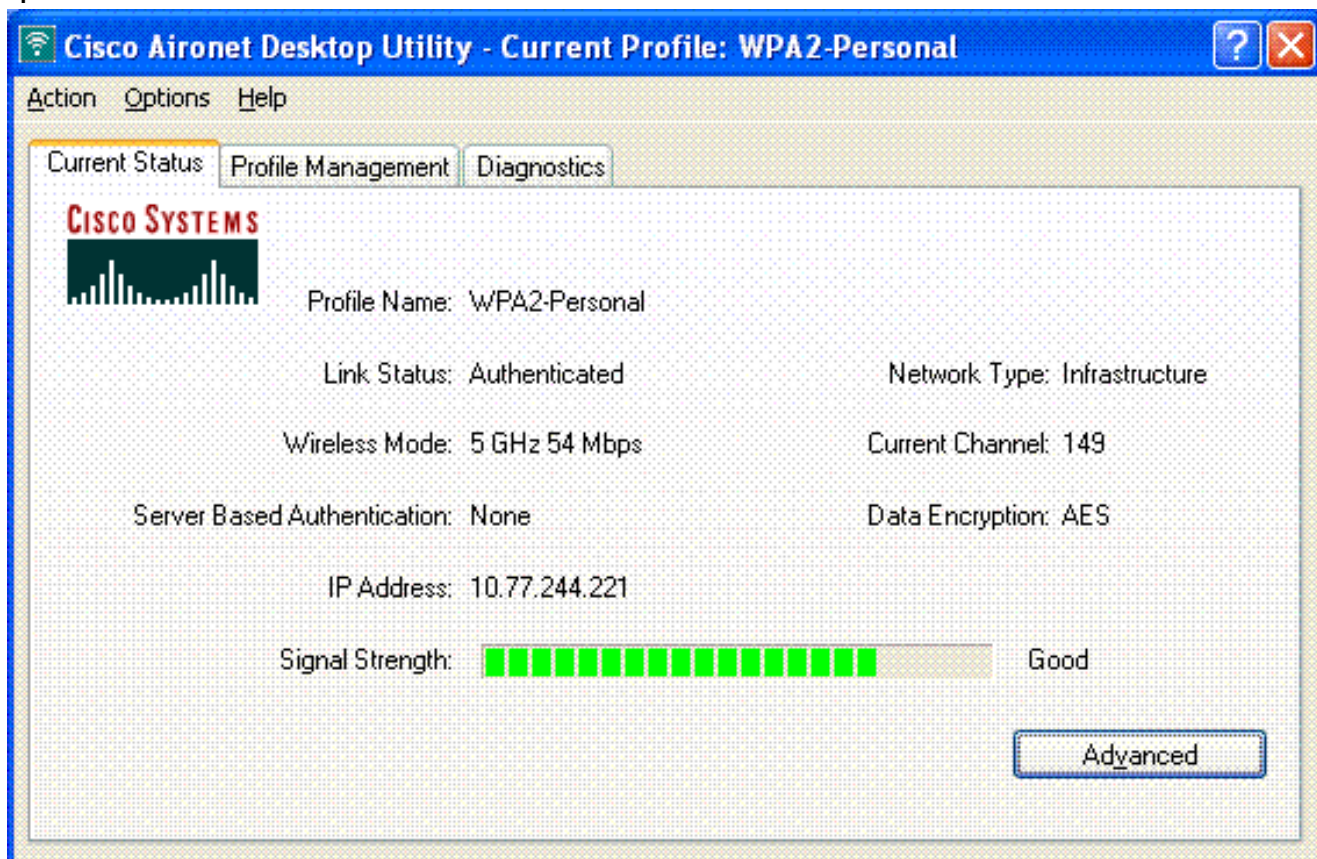
4. 输入预共享密钥并单击 OK。



验证 WPA2 个人操作模式

若要验证您的 WPA2 个人模式配置是否工作正常，请完成下列步骤：

1. 在“Aironet Desktop Utility”窗口中，选择配置文件 **WPA2-Personal**，然后单击“Activate”以激活无线客户端配置文件。
2. 激活配置文件后，无线客户端将在身份验证成功时与 WLAN 建立关联。下面是屏幕截图：



故障排除

本部分提供的信息可用于对配置进行故障排除。

对于配置故障排除，以下 **debug** 命令将十分有用：

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

- **debug dot1x事件enable (event)** —启用所有dot1x事件调试。下面是基于成功身份验证的 debug

输出示例：**注意：**由于空间限制，已将此输出中的一些行移至相应的第二行。(Cisco
Controller)>**debug dot1x events enable** Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Sending
EAP -Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1) Wed Feb 20 14:19:57 2007:
00:40:96:af:3e:93 **Received EAPOL START from mobile 00:40:96:af:3e:93** Wed Feb 20 14:19:57
2007: 00:40:96:af:3e:93 **Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 2)**
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received EAP Response packet with mismatching id
(currentid=2, eapid=1) from mobile 00:40:96:af:3e:93 Wed Feb 20 14:19:57 2007:
00:40:96:af:3e:93 **Received Identity Response (count=2) from mobile 00:40:96:af:3e:93** Wed Feb
20 14:19:57 2007: 00:40:96:af:3e:93 **Processing Access-Challenge for mobile 00:40:96:af:3e:93**
.....
.....
..... Wed Feb 20
14:20:00 2007: 00:40:96:af:3e:93 **Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id**
19, EAP Type 43) Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 **Processing Access-Challenge for**
mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 **Sending EAP Request**
from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20) Wed Feb 20 14:20:01 2007: 00:40:96:af:3e:93
Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43) Wed Feb 20
14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -0 Wed Feb 20 14:20:29
2007: Resetting the group key timer for 3689 seconds on AP 00:0b:85:91:c3:c0 Wed Feb 20
14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -1 Wed Feb 20 14:20:29
2007: Resetting the group key timer for 3696 seconds on AP 00:0b:85:91:c3:c0 Wed Feb 20
14:20:30 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93 Wed Feb
20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93
(EAP Id 22) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received Identity Response (count=3)
from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-
Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 WARNING:
updated EAP-Identifer 22 ==> 19 for STA 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007:
00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 19) Wed
Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93
(EAP Id 19, EAP Type 3) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-
Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending
EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20) Wed Feb 20 14:20:30 2007:
00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type
43) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile
00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA
to mobile 00:40:96:af:3e:93 (EAP Id 21) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received
EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43) Wed Feb 20 14:20:31
2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20
14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93
(EAP Id 22) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile
00:40:96:af:3e:93 (EAP Id 22, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93
Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007:
00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 23) Wed
Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93
(EAP Id 23, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-
Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending
EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 24) Wed Feb 20 14:20:31 2007:
00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type
43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile
00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA
to mobile 00:40:96:af:3e:93 (EAP Id 25) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received
EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43) Wed Feb 20 14:20:31
2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20
14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93
(EAP Id 26) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile
00:40:96:af:3e:93 (EAP Id 26, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93
Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007:
00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 27) Wed
Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93
(EAP Id 27, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-
Reject for mobile00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-

Failure to mobile 00:4096:af:3e:93 (EAP Id 27) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93
Setting quiet timer for 5 seconds for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007:
00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1) Wed
Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile
00:40:96:af:3e:93 (EAP Id 1) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAPOL
START from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-
Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 2) Wed Feb 20 14:20:32 2007:
00:40:96:af:3e:93 Received Identity Response (count=2) from mobile 00:40:96:af:3e:93 Wed Feb
20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 2 ==> 20 for STA
00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA
to mobile 00:40:96:af:3e:93 (EAP Id 20) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received
EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 3) Wed Feb 20 14:20:32 2007:
00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20
14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93
(EAP Id 21) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile
00:40:96:af:3e:93 (EAP Id 21, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93
Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007:
00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 22) Wed
Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93
(EAP Id 22, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-
Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING:
updated EAP-Identifer 22 ==> 24 for STA 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007:
00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 24) Wed
Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93
(EAP Id 24, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Processing Access-
Challenge for mobile 00:40:96:af:3e:93** Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Sending
EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 25)** Wed Feb 20 14:20:32 2007:
00:40:96:af:3e:93 **Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type
43)** Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Processing Access-Accept for mobile
00:40:96:af:3e:93** Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Creating a new PMK Cache Entry
for tation 00:40:96:af:3e:93 (RSN 0)** Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Sending
EAP-Success to mobile 00:40:96:af:3e:93 (EAP Id 25)** Wed Feb 20 14:20:32 2007:
00:40:96:af:3e:93 **Sending default RC4 key to mobile 00:40:96:af:3e:93** Wed Feb 20 14:20:32
2007: 00:40:96:af:3e:93 **Sending Key-Mapping RC4 key to mobile 00:40:96:af:3e:93** Wed Feb 20
14:20:32 2007: 00:40:96:af:3e:93 **Received Auth Success while in Authenticating state for
mobile 00:40:96:af:3e:93**

- debug dot1x数据包enable (event) —启用802.1x数据包消息调试。
- debug aaa事件enable (event) —启用所有aaa事件debug输出。

相关信息

- [WPA2 -Wi-Fi 安全访问 2, Wi-Fi 安全访问 2](#)
- [包含无线局域网控制器和外部 RADIUS 服务器的 EAP-FAST 身份验证配置示例](#)
- [WLAN 控制器 \(WLC\) 中 EAP 身份验证的配置示例](#)
- [WPA 配置概述](#)
- [无线产品支持](#)
- [技术支持和文档 - Cisco Systems](#)